

Advanced Security Operations Center Telelink Business Services www.tbs.tech



Monthly Security Bulletin

June 2023



This security bulletin is powered by Telelink Business Services' <u>Advanced Security Operations Center</u>

The modern cybersecurity threat landscape is constantly evolving. New vulnerabilities and zero-day attacks are discovered every day. The old vulnerabilities still exist. The tools to exploit these vulnerabilities are applying more complex techniques. But are getting easier to use.

Mitigating modern cyber threats require solutions for continuous monitoring, correlation, and behavior analysis that are expensive and require significant amount of time to be implemented. Moreover, many organizations struggle to hire and retain the expensive security experts needed to operate those solutions and provide value by defending the organizations.

The ASOC by Telelink allows organizations get visibility, control, and recommendations on improving their security posture for a fixed and predictable monthly fee.



LITE Plan 425 EUR/mo

- Gain visibility on the security posture of all your company's IT infrastructure
- Analysis of up to 2 GB/day log data
- Optional emergency response team (ERT) and user and endpoint behavior analytics (UEBA)

Get visibility on the cyber threats targeting your company!

PROFESSIONAL Plan

1225 EUR/mo

- Gain visibility on your company's security posture and recommendations on how to deal with security threats, risks, and actors
- Analysis of up to 5 GB/day log data and 100 GB/day network data
- Optional ERT and UEBA

Start to mitigate cyber threats and minimize the risk!

Why Advanced Security Operations Center (ASOC) by Telelink?

- Delivered as a service, which guarantees fast implementation, clear responsibility in the Supplier and ability to cancel the contract on a monthly basis.
- Built utilizing state of the art leading vendor's solutions.
- Can be sized to fit small, medium, and large business needs.
- No investment in infrastructure, team, trainings or required technology.
- Flexible packages and add-ons that allow pay what you need approach.
- Provided at a fraction of the cost of operating your own SOC.

ADVANCED Plan 2 575 EUR/mo

- Gain complete visibility, deep analysis, recommendations, and security awareness trainings for your employees
- Analysis of up to 10 GB/day log data and 200 GB/day network data
- Included ERT and optional UEBA

Complete visibility, deep analysis, and cyber threat mitigation!



Log Analysis and Correlation	Health Monitoring	Asset Identification and Prioritization	Infrastructure Security Assessment	Infrastructure Security Audit	Automatic Asset Discovery and Service Mapping	Network Devices Configurations Backup
Monthly External Vulnerability Scan and Reports	External Vulnerability Analysis	Monthly Internal Vulnerability Scan and Reports	Internal Vulnerability Analysis	Advanced Vulnerability Analysis	Recommendations for Security Patch Management	
Automatic Attack and Breach Detection	Human Triage	Threat Hunting				
Recommendations and Workarounds	Recommendations for Future Mitigation					
Attack Vector Identification	Reports	Security Surface Exposure	Likelihood Analysis	Impact Analysis		
Network Forensics	Server Forensics	Endpoint Forensics				
Monthly Security Bulletin	Emerging Threats Bulletins	Tailored Bulletin for Customer's Critical Assets	Security Awareness Training			
				Lite Plan	Professional Plan (incl. all from Lite)	Advanced Plan (incl. all from Professional)

What is inside:

- Infrastructure Security Monitoring the essential minimum to cybersecurity and to detect anomalies is to monitor your infrastructure 24x7x365
- Vulnerability Management get visibility on the risks new or old vulnerabilities are posing to your IT infrastructure and get recommendations on how to reduce or mitigate those risks
- Attack Detection get data from state-of-the-art cybersecurity tools, detect attacks and breaches, and involve our ASOC Analytics Team to perform human triage and threat hunting to precisely define the risks of the attack
- Reports and Recommendations get detailed tailored reports with structured recommendations on how to prevent malicious activities (attacks) and take preventive measures
- Advanced Attack Analysis get information on the attack vector, the attack surface, potential threat actors, and their objectives and motives for the attack
- Forensic Analysis in case of severe cybercrimes the ASOC team can perform forensic analysis and/or support the authorities
- Bulletins, Training and Awareness be timely informed on critical vulnerabilities with tailored and emerging threats bulletins and security awareness trainings to stop people being the weakest link



Table of Contents

1. Wha	at does ChatGPT know about phishing?4
2.	Cyber-Risk Declines But 78% of Organizations Predict Successful Attacks in
Comin	g Year15
3.	New Cactus ransomware encrypts itself to evade antivirus17
4.	FBI nukes Russian Snake data theft malware with self-destruct command22
5.	Plenty of Phish in the Sea—Your Guide to Spotting Phishing Emails and Scams24
6.	New phishing-as-a-service tool "Greatness" already seen in the wild
7.	Top 5 Password Cracking Techniques Used by Hackers42
8.	Airline exposes passenger info to others due to a 'technical error'
9.	Open-source Cobalt Strike port 'Geacon' used in macOS attacks51
10.	Parental control app with 5 million downloads vulnerable to attacks
11.	KeePass exploit helps retrieve cleartext master password, fix coming soon57
12.	Android phones are vulnerable to fingerprint brute-force attacks
13.	Mobile Spyware—How You Can Keep Stalkers Off Your Phone66
14.	Why Are Some Countries Banning TikTok?70
15.	How I Got Started: White Hat Hacker72
16.	Three Reasons You Need a VPN74
17.	Brute-Forcing a Fingerprint Reader77
18.	Android apps with spyware installed 421 million times from Google Play78
19.	What is the Dark Web? The Answer Can Help You Stay Safer Online
20.	RomCom malware spread via Google Ads for ChatGPT, GIMP, more
21.	Microsoft finds macOS bug that lets hackers bypass SIP root restrictions



1. What does ChatGPT know about phishing?

Can ChatGPT detect phishing links?

Hearing all the buzz about the amazing applications of ChatGPT and other language models, our team could not help but ask this question. We work on applying machine learning technologies to cybersecurity tasks, specifically models that analyze websites to detect threats such as phishing. What if all our complex, multi-layered detection systems are now obsolete, and a single LLM (large language model) to rule them all can fight cybercriminals better than we do?

To answer this question, we conducted an experiment to see how good ChatGPT is at recognizing overtly malicious links. In this article, we provide a practical example of how an LLM can be applied to a real, albeit simplified, cybersecurity task, and describe all the interesting things we learned along the way. Since we didn't have any illusions that ChatGPT could actually be used as a detection method, our primary goal was to find out how much cybersecurity knowledge ChatGPT has learned from its training data and how it could possibly assist a human analyst in their job.

Why URL classification?

An analyst's trained eye can spot an obviously malicious link in a split second (and you probably can too):

hxxp://caseld-10xxxx.info/1/Office365/Offlce3.6.5/live/login.php

This is not the Office365 login link, is it?

(links in the article are partially masked with x)

A rule of thumb for finding tasks to which ML can be applied is that if a person can do it instantly, almost without thinking, it's probably a good candidate. Still, building a machine-learning system requires a lot of effort, from gathering data and crafting features to preparing the infrastructure. The promise of replacing all that with a single interface configured via natural language sounds too good to be true, but just how far is it from being a reality?

When conducting this experiment, we were well aware of the limitations of large language models, as well as the fact that OpenAl asks that this emerging technology not be applied to any high-risk area, and state the following regarding GPT-4's cybersecurity applications in the system card:

However, GPT-4 has significant limitations for cybersecurity operations due to its "hallucination" tendency and limited context window.

It is natural to assume that GPT-3.5-turbo will exhibit these limitations to a greater extent.



We chose the URL classification task because:

- Unlike a whole HTML page, a URL fits easily into an LLM, because modern LLMs, such as ChatGPT, can only consume a limited number of symbols (more precisely, tokens) at a time (they have a fixed context window, in LLM-speak).
- Obviously malicious links are easy to detect, but the task is still non-trivial, because it requires world knowledge (for example, knowing the names of popular web services).
- URLs are still text, and LLMs are good at processing text.

So here is what we did.

Let's talk?

First of all, we opened the ChatGPT web interface and checked if what we wanted was even possible:

Judging by the URL, is this link a phishing attempt? Please explain why. Link: hxxp://caseld-10xxxx.info/1/Office365/0fflce3.6.5/live/login.php

Yes, it is likely a phishing attempt.

The URL appears to be intentionally deceptive, as it contains several red flags:

- The domain name "caseld-10xxxx.info" is not associated with any reputable or recognizable entity, and it looks like a random sequence of letters and numbers.
- The URL uses the term "Office365" which is a popular productivity suite, and it is a common target for phishing attacks. Cybercriminals often use this tactic to lure unsuspecting victims into clicking on a link and disclosing sensitive information.
- The word "live" in the URL could be used to imply that the page is an official Microsoft Office365 login page, as Microsoft has used "live" in the past in some of its services.
- The misspelling of "Office" as "Office" is another red flag as it is a common tactic used by phishers to trick users into believing the website is legitimate.
- The ".php" extension at the end of the URL suggests that it is a PHP script running on a server, which is commonly used in phishing attacks to harvest login credentials.

Therefore, it is advisable to avoid clicking on such links and to always check the URL's legitimacy before entering any personal information or credentials.

This is a pretty reasonable explanation. Aside from the fact that the model shows some distrust of PHP (well, who doesn't?), it is good at recognizing the target organization, a homographic attack (Office), and even points out why "live" might have been used. This is an explanation worthy of a junior analyst.

To gather a corpus of explanations, we used OpenAl API to query the model called GPT-3.5turbo, which is the backend for ChatGPT. It is fast and cheap (we check a lot of links), but still



powerful enough. For the test corpus, we gathered a few thousand links that our detection technologies deemed phishing, and threw in a few thousand safe URLs.

Attempt 1. Is it phishing?

ChatGPT is great at providing the answer in the form that you require – from poems:

And lastly, "Office" it doth spell amiss,

A trick oft used by phishers with a hiss.

Beware, dear user, and take great care,

Lest thou fall victim to this cyber snare.

to machine-readable formats. It can also do more than one thing at once. This means that in addition to the yes/no answer to the question about link safety, we could ask ChatGPT to format the response as JSON and also to include a rationale, as well as the possible target. So, after a few iterations, we settled on the following prompt:

We use a system prompt here (according to practitioners and docs, this is less important than the user input) that portrays ChatGPT as a cybersecurity chatbot and ask for its verdict in the user prompt. Frankly, the fact that it is so easy to get the desired output from ChatGPT is awe-inspiring.

It took us two nights to get about 6,000 verdicts (probably because we ran the experiment at the peak of all the hype), and once we got the data, we proceeded to parse the results.

Unfortunately, while most of the outputs could be parsed as is, some were corrupted: some contained additional text, such as "Note: be careful when opening links..." or just a dot at the end, others had unnecessary escape characters. All in all, less than 0.5% of JSONs were broken beyond automated fixes or contained text such as:

I am sorry, but as an AI language model, I am not able to access the internet or browse the website provided. However, as per the standard industry practices, you can check the legitimacy of the website by running it through a reputable online phishing detection service/provider. Additionally, if there are any official reports of phishing attacks or scams associated with the target company, it further increases the likelihood of the link leading to a phish website.



Which is still a reasonable answer.

All in all, after all the errors and rejections, we were left with a dataset of 2322 phish and 2943 safe URLs. The resulting metrics are:

- Detection rate: 87.2%
- False positive rate: 23.2%

While the detection rate is very high, the false positive rate is unacceptable. Imagine if every fifth website you visit was blocked? Sure, no machine learning technology on its own can have a zero false positive rate, but this number is too high. To put this in perspective, in a well-known paper called URLnet, where Le et al. solved a very similar task, the authors managed to achieve about the same level of detection rate (~85%) with a false positive rate of about 0.4% with a specially crafted convolutional neural network. A more recent URLTran paper by Maneriker et al. uses Transformers (the same architecture that powers ChatGPT) to achieve an even lower FPR.



ROC curve from Le et al., 2018, illustrating achievable TPR (DR)/FPR values

Unfortunately, there are no miracles here. This is also where we met the first limitation – we can't adjust the threshold to trade FPR for DR. Or can we?

Security Bulletin, June 2023



The second experiment: 'Is it safe?'

Our prompt was probably too specific and cued the language model to view the link with suspicion. Instead of asking if the link is phishing, we could ask if it is safe to visit, and maybe the LLM would behave less suspiciously. This led us to the second prompt:

Differences from the previous prompt:

- Gone is the 'cybersecurity guru', who by nature should be suspicious of random links
- We don't ask for the target, so as not to alert the model that this is a phishing detection task
- We do, however, ask for confidence. Though this is very unlikely, confidence may prove useful.

The results were quite discouraging:

- Detection rate: 93.8%
- False positive rate: 64.3%

It turns out that the more general prompt is more likely to prompt a verdict that the link is dangerous. This is how the links from the safe subset of data changed the assigned verdicts, compared to the previous cybersecurity guru prompt:

Internet security assistant chatbot verdicts (safe data) CyberGPT cybersecurity guru verdicts (safe data)	safe	unsafe
safe	1049	1210
phish	2	682

Interestingly, the confidence choices are more like human-assigned confidence in the sense that round numbers like 90% occur most often:





TOP 5 probabilities that the model chose. Note that they are rounded to 0.1

At least the ROC curve looks alright, but there is no point at which this prompt would outperform the cybersecurity guru from the previous attempt:



ROC Curve (AUC=0.7060)

ROC curve based on probabilities provided by ChatGPT



To conclude, it is hard to predict the behavior of the LLM based on human reasoning about the prompt. Probably the "safety" of a link is a vaguer concept than "phish". Understanding why the first prompt won by a large margin is difficult, and choosing the best prompt at this time, despite the emergence of new prompt engineering techniques, is more art than science.

Verdict stability

An important fact about LLMs is that the generation process is random. While you can coerce an LLM to be almost deterministic by setting its temperature parameter, which actually controls the output randomness, to 0 (there are still numerical sources of non-determinism), it usually leads to poor performance (such as the tendency to repeat the same phrase over and over again). As a result, for each token (a word or its part) that the network generates, it has a few alternatives among the choices (also controllable by parameters).

Non-deterministic verdicts are not the top feature you expect from a detection system. To measure its impact on the results, we conducted another small experiment in which we chose 200 random URLs (100 safe and 100 phish) and gathered verdicts with the same simplified prompt:

This is how the results of these two identical runs compare (the responses are not postprocessed and answer the question of whether the link is safe):

Run 2 Run 1	no	unknown	yes
no	145	2	3
yes	4	0	46

So, the verdict for 4.5% percent of the URLs changed due to the randomness of the LLM, with the variation in verdicts between runs on safe URLs being 7%. Again, while this can be remedied by tweaking the temperature, it's an important factor to keep in mind when using LLMs.

Organization extraction

The most striking aspect of ChatGPT's performance was the extraction of the potential phishing target. When attackers craft their samples, they try to trick users into believing that the URL is



genuine and belongs to a company, while also obfuscating it enough to fool automated analysis. Extracting the attack target can be useful in many scenarios.

ChatGPT has enough real-world knowledge to know about many internet and financial services and with only a small post-processing step (e.g., merging "Apple" and "iCloud" or removing "LLC" and "Inc") it does a very good job at extracting them. It was able to identify a target more than half the time. Note that not every URL contains a reference to a target organization. Among the identified companies, there were major tech portals like Facebook, TikTok and Google, marketplaces such as Amazon and Steam, lots of banks from all over the world, from Australia to Russia, cryptocurrency and delivery services.

Some interesting examples include:

URL: hxxps://steancxxxmuunity.com/profiles/765xxxxxxx175

Organization: Steam

Reasoning: The domain name 'steancxxxmuunity.com' appears to be a typo-squatting attempt. The correct spelling of the domain should be 'steamcommunity.com'. The website is trying to impersonate Steam Community, a popular gaming platform...

URL: <u>https://cxxxxxxr.com/wp-</u> includes/js/jcrop/cgi/BOfA/Validation/login.php?cmd=login_submit

Organization: Bank of America

Reasoning: The link is suspicious and indicates a phishing attempt because the domain name is not related to the possible targeted company (Bank of America), the URL is also suspicious containing additional characters such as '/wp-includes/js/jcrop/cgi'...

URL: http://caseld-10xxxx.info/1/Office365/0fflce3.6.5/live/login.php

Organization: Microsoft

Reasoning: The link's domain name (caseld-10xx93.info) does not appear to be related to Microsoft's Office 365 service. The URL path also contains a misspelled version of the word 'office' (Office) and a suspiciously old version number (3.6.5).

URL: http://adobexxxsignxxxx.duckdns.org/ees/

Organization: Adobe

Reasoning: The domain name 'duckdns.org' is a free dynamic DNS provider which is often used by cyber criminals for hosting phishing sites or other malicious content. Additionally, the subdomain adobexxxsignxxxx in the URL appears to imitate the legitimate Adobe service 'Adobe Sign', which suggests that the attackers may be targeting Adobe's customers for information theft or fraud.



Here we see that ChatGPT detects homographic attacks (although it can confuse them with typo-squatting), and correctly states that the domains are not related to the companies. While it fails to untangle that "3.6.5" is an imitation of 365, the explanations are quite reasonable.

Implicit knowledge: reasoning analysis

The examples above are cherry-picked. When cherry-picking with the opposite intention, some funny things happen. The explanations that ChatGPT provides may include:

- References to WHOIS, which the model doesn't have access to:
 - Finally, if we perform a WHOIS lookup for the domain name, it was registered very recently (2020-10-14) and the registrant details are hidden.
- References to content on a website that the model doesn't have access to either:
 - the website is asking for user credentials on a non-Microsoft website. This is a common tactic for phishing attacks.
 - Additionally, the webpage's layout and design are inconsistent with eBay's official website, indicating that it may be a fake website designed to impersonate eBay.
 - There is also no information available on the website's security and privacy policy. A secure website should provide that information transparently to users.
- References to SSL certificate expiration:
 - The domain 'duckdns.org' is not owned by Netflix, and the SSL Certificate is invalid.
- Misstatements:
 - The domain 'sxxxxxp.com' is not associated with Netflix and the website uses 'http' protocol instead of 'https' (the website uses https)
- Revelatory nuggets of cybersecurity information:
 - The domain name for the URL 'yxxxx3.com' appears to be registered in Korea which is a red-flag.

These are funny and highlight the limitations of an LLM: while it can generate reasonable explanations, it is also prone to hallucinations – such as imagining contexts that it does not have access to, or coming up with facts that are just plain wrong.

In general, however, we see that the model demonstrates a non-trivial understanding of the task. Analyzing all the explanations by hand would be laborious, so we do some distant reading here to get a bird's-eye overview of the reasonings it generates by applying a little bit of old-school NLP.

First of all, we noticed that the model used mostly short, terse sentences with one point per sentence in its explanations. We split the statements into sentences using the NLTK Punkt tokenizer. The resulting sentences were then vectorized using MPNet from the Sentence-Bert package, and then visualized using UMAP. To color the resulting plot, we used DBSCAN clustering. A few iterations of hyperparameter tweaking yield the following result:



UMAP projection of explanation embeddings



Cluster analysis of explanations provided by ChatGPT. Semantically close reasons form dense clusters.

These dense clusters reveal the most popular phrases that the model provides as explanations. Some of these clusters are:

- Mentions of particular target companies.
- Recommendations not to click the link.
- Certain statements about the website being phish or not.
- Statements of uncertainty.
- References to HTTPS (or lack thereof) or SSL (usually hallucinations)
- Sentences like "This is a common tactic..."

However, some of them reveal "common tactics":



- Use of IPFS: "The URL looks suspicious and appears to be hosted on IPFS which can be used to host malicious content."
- Suspicious elements in path, including homographic attacks: "This link is an example of a homograph attack also known as 'IDN homograph attack'."
- Elements in path or domain that are related to security and urgency: "Lastly, the URL has a sense of urgency to it, indicating that the user needs to click immediately."
- Use of dynamic DNS: "The domain name 'duckdns.org' is a free dynamic DNS provider that can be used by anyone to create custom subdomains, which makes it easy for attackers to use for phishing emails or websites impersonating legitimate companies".
- An email in the parameters: "Additionally, the email address used as a query parameter may indicate a potential phishing attempt."
- Mention of an organization in the path or subdomain while the domain is not related to the organization: "The link appears suspicious as it contains a subdomain that is not related to Amazon."
- Elements in the domain that look autogenerated: "Also, the path 'bafyxxxxxxxxxxxxx43ky' suggests that this is an autogenerated link."

These points make a lot of sense. This means that the training data for ChatGPT contained enough cybersecurity material for the LLM to learn the telltale signs of phishing attempts and use this knowledge to analyze specific cases, which is very impressive.

Conclusion

As we have seen, for a zero-shot system the results are amazing – it is hard to argue with, even for a die-hard sceptic. Anecdotal examples, especially the cherry-picked ones, are also very impressive. This is why, when we talk about real-world performance, a screenshot from Twitter is not a solid basis for decision-making. This is especially true in cybersecurity, where applying automated scenarios to our tasks means going far beyond "good" or even "impressive" performance.

As with many other use cases, the core detection task is only part of the problem. Creating signatures or blocklist records, validating and testing them, delivering them, ensuring quality of service is less glamorous, but just as important, and here we need a lot of hard work done by humans to get things rolling.

Moreover, the use of LLM means applying a whole new set of skills. We could have improved the results, both in detection, target organization extraction and reasoning, by trying various things:

- Using a stronger model, such as GPT-4
- Using special prompt-designing patterns, such as Chain-of-Thought-prompting or Reflect-Critique-Improve
- Feeding parts of the HTML along with the URL
- Adjusting the system prompt and sampling parameters, such as temperature, etc.



However, this means abandoning the hope of a zero-shot AI that "just works". Also, using LLMs means dealing with their current idiosyncrasies, such as the demonstrated tendency to hallucinate (manifested by coming up with imaginary explanations and referring to page texts it has never seen), randomness of output, as well as possible prompt injection attacks.

On the other hand, if we look at the organization extraction and reasoning, we have to admit that it performs on par with what we would expect from an intern-level phishing analyst: it is good, but never leave it without supervision! Therefore, it is possible to use this type of technology to assist flesh-and-blood analysts by highlighting suspicious parts of the URL and suggesting possible attack targets. It could also be used in weak supervision pipelines to improve classic ML pipelines.

All in all, while impressive, ChatGPT and LLMs are not yet ready to radically change the cybersecurity game, at least as far as phishing detection is concerned. At Kaspersky, we continue to investigate cutting-edge technologies and study their potential impact on both cyberattackers and defenders. Let's see what happens next.

Source: https://securelist.com/chatgpt-anti-phishing/109590/

2. Cyber-Risk Declines But 78% of Organizations Predict Successful Attacks in Coming Year

DALLAS, May 2, 2023 /PRNewswire/ -- Trend Micro Incorporated (TYO: 4704; TSE: 4704), a global cybersecurity leader, today announced that cyber-risk levels have improved from "elevated" to "moderate" for the first time, but that insiders represent a persistent threat for global organizations.

o read a full copy of the Trend Micro Cyber Risk Index (CRI) 2H 2022*, please visit: https://www.trendmicro.com/en_us/security-intelligence/breaking-news/cyber-risk-index

Jon Clay, VP of threat intelligence at Trend Micro: "For the first time since we've been running these surveys, we saw the global cyber-risk index not only improve but move into positive territory at +0.01. It means that organizations may be taking steps to improve their cyber-preparedness. There is still much to be done, as employees remain a source of risk. The first step to managing this is to gain complete and continuous attack surface visibility and control."

The CRI found that cyber-preparedness improved in Europe and APAC but declined slightly in North and Latin America over the past six months. At the same time, threats declined in every region bar Europe.

Most organizations are still pessimistic about their prospects over the coming year. The CRI found that most respondents said it was "somewhat to very likely" they'd suffer a breach of customer data (70%) or IP (69%) or a successful cyber-attack (78%).



These figures represent declines of just 1%, 2%, and 7%, respectively, from the last report.

The top four threats listed by respondents in the CRI 2H 2022 remained the same from the previous report:

- Clickjacking
- Business Email Compromise (BEC)
- Ransomware
- Fileless attacks

"Botnets" replaced "login attacks" in fifth place.

Global respondents also named employees as representing three of their top five infrastructure risks:

- Negligent insiders
- Cloud computing infrastructure and providers
- Mobile/remote employees
- Shortage of qualified personnel
- Virtual computing environments (servers, endpoints)

Dr. Larry Ponemon, chairman and founder of Ponemon Institute, said: "As the shift to hybrid working gathers momentum, organizations are rightly concerned about the risk posed by negligent employees and the infrastructure used to support remote workers. They will need to focus not only on technology solutions but people and processes to help mitigate these risks."

Based on the global survey results, the greatest areas of concern for businesses related to cyber-preparedness are:

People: "My organization's senior leadership does not view security as a competitive advantage."

Process: "My organization's IT security function doesn't have the ability to unleash countermeasures (such as honeypots) to gain intelligence about the attacker."

Technology: "My organization's IT security function does not have the ability to know the physical location of business-critical data assets and applications."

*The six-monthly Cyber Risk Index was compiled by the Ponemon Institute from interviews with 3729 global organizations. The index is based on a numerical scale of -10 to 10, with -10 representing the highest level of risk. It is calculated by subtracting the score for cyber threats from the score for cyber-preparedness.

About Trend Micro

Trend Micro, a global cybersecurity leader, helps make the world safe for exchanging digital information. Fueled by decades of security expertise, global threat research, and continuous



innovation, Trend Micro's cybersecurity platform protects hundreds of thousands of organizations and millions of individuals across clouds, networks, devices, and endpoints. As a leader in cloud and enterprise cybersecurity, the platform delivers a powerful range of advanced threat defense techniques optimized for environments like AWS, Microsoft, and Google, and central visibility for better, faster detection and response. With 7,000 employees across 65 countries, Trend Micro enables organizations to simplify and secure their connected world. www.TrendMicro.com.

Source: <u>https://newsroom.trendmicro.com/2023-05-02-Cyber-Risk-Declines-But-78-of-</u> Organizations-Predict-Successful-Attacks-in-Coming-Year

3. New Cactus ransomware encrypts itself to evade antivirus

A new ransomware operation called Cactus has been exploiting vulnerabilities in VPN appliances for initial access to networks of "large commercial entities."

The Cactus ransomware operation has been active since at least March and is looking for big payouts from its victims.

While the new threat actor adopted the usual tactics seen in ransomware attacks - file encryption and data theft - it added its own touch to avoid detection.

Encrypted configuration twist

Researchers at Kroll corporate investigation and risk consulting firm believe that Cactus obtains initial access into the victim network by exploiting known vulnerabilities in Fortinet VPN appliances.

The assessment is based on the observation that in all incidents investigated the hacker pivoted inside from a VPN server with a VPN service account.

What sets Cactus apart from other operations is the use of encryption to protect the ransomware binary. The actor uses a batch script to obtain the encryptor binary using 7-Zip.

The original ZIP archive is removed and the binary is deployed with a specific flag that allows it to execute. The entire process is unusual and the researchers that this is to prevent the detection of the ransomware encryptor.

In a technical report, Kroll investigators explain that there are three main modes of execution, each one selected with the use of a specific command line switch: setup (-s), read configuration (-r), and encryption (-i).



The -s and -r arguments allow the threat actors to setup persistence and store data in a C:\ProgramData\ntuser.dat file that is later read by the encryptor when running with the -r command line argument.

For the file encryption to be possible, though, a unique AES key known only to the attackers must be provided using the -i command line argument.

This key is necessary to decrypt the ransomware's configuration file and the public RSA key needed to encrypt files. It is available as a HEX string hardcoded in the encryptor binary.

```
bash> strings -td -n1628 cactus.exe
4227632 d3d3d5aa22a2e5a2d8c8b9267360a7752c41f1e00827fcc31ff64aaf166e10908a04afe904c39a7
```

Hex string for encrypted Cactus ransomware configuration

source: Kroll

Decoding the HEX string provides a piece of encrypted data that unlocks with the AES key.

"CACTUS essentially encrypts itself, making it harder to detect and helping it evade antivirus and network monitoring tools," Laurie Iacono, Associate Managing Director for Cyber Risk at Kroll, told Bleeping Computer.

Running the binary with the correct key for the -i (encryption) parameter unlocks the information and allows the malware to search for files and start a multi-thread encryption process.

Kroll researchers provided the diagram below to better explain the Cactus binary execution process as per the selected parameter.





Cactus ransomware binary execution flow

source: Kroll

19



Ransomware expert Michael Gillespie also analyzed how Cactus encrypts data and told BleepingComputer that the malware uses multiple extensions for the files it targets, depending on the processing state.

When preparing a file for encryption, Cactus changes its extension to .CTS0. After encryption, the extension becomes .CTS1.

However, Gillespie explained that Cactus can also has a "quick mode," which is akin to a light encryption pass. Running the malware in quick and normal mode consecutively results in encrypting the same file twice and appending a new extension after each process (e.g. .CTS1.CTS7).

Kroll observed that the number at the end of the .CTS extension varied in multiple incidents attributed to Cactus ransomware.

Cactus ransomware TTPs

Once in the network, the threat actor used a scheduled task for persistent access using an SSH backdoor reachable from the command and control (C2) server.

According to Kroll investigators, Cactus relied on SoftPerfect Network Scanner (netscan) to look for interesting targets on the network.

For deeper reconnaissance, the attacker used PowerShell commands to enumerate endpoints, identify user accounts by viewing successful logins in Windows Event Viewer, and ping remote hosts.

The researchers also found that Cactus ransomware used a modified variant of the open-source PSnmap Tool, which is a PowerShell equivalent of the nmap network scanner.

To launch various tools required for the attack, the investigators say that Cactus ransomware tries multiple remote access methods through legitimate tools (e.g. Splashtop, AnyDesk, SuperOps RMM) along with Cobalt Strike and the Go-based proxy tool Chisel.

Kroll investigators say that after escalating privileges on a machine, Cactus operators run a batch script that uninstalls the most commonly used antivirus products.

Like most ransomware operations, Cactus also steals data from the victim. For this process, the threat actor uses the Rclone tool to transfer files straight to cloud storage.

After exfiltrating data, the hackers used a PowerShell script called TotalExec, often seen in BlackBasta ransomware attacks, to automate the deployment of the encryption process.

Gillespie told us that the encryption routine in Cactus ransomware attacks is unique.Despite this, it does not appear to be particular to Cactus as a similar encryption process has also been adopted recently by the BlackBasta ransomware gang.





Cactus ransomware tactics, techniques, and procedures

source: Kroll

At the moment there is no public information about the ransoms that Cactus demands from its victims but BleepingComputer has been told by a source that they are in the millions.

Even if the hackers do steal data from victims, it appears that they have not set up a leak site like other ransomware operations involved in double-extortion.

However, the threat actor does threaten victims with publishing the stolen files unless they get paid. This is explicit in the ransom note:



```
CAcTuS.readme.txt
Your systems were accessed and encrypted by Cactus.
To recover your files and prevent data disclosure contact us via email:
Your unique ID reference: <redacted>
Backup contact: TOX (https://tox.chat/):
<redacted>
```

Cactus ransom note threatens with publishing stolen data

source: Kroll

Extensive details about the Cactus operation, the victims they target, and if the hackers keep their word and provide a reliable decryptor if paid, are not available at this time.

What is clear is that the hackers' incursions so far likely leveraged vulnerabilities in the Fortinet VPN appliance and follow the standard double-extortion approach by stealing data before encrypting it.

Applying the latest software updates from the vendor, monitoring the network for large data exfiltration tasks, and responding quickly should protect from the final and most damaging stages of a ransomware attack.

Source: <u>https://www.bleepingcomputer.com/news/security/new-cactus-ransomware-encrypts-itself-to-evade-antivirus/</u>

4. FBI nukes Russian Snake data theft malware with self-destruct command

Cybersecurity and intelligence agencies from all Five Eyes member nations took down the infrastructure used by the Snake cyber-espionage malware operated by Russia's Federal Security Service (FSB).

The development of the Snake malware started under the name "Uroburos" in late 2003, while the first versions of the implant were seemingly finalized by early 2004, with Russian state hackers deploying the malware in attacks immediately after.

The malware is linked to a unit within Center 16 of the FSB, the notorious Russian Turla hacking group, and was disrupted following a coordinated effort named Operation MEDUSA.

Among the computers ensnared in the Snake peer-to-peer botnet, the FBI also found devices belonging to NATO member governments.

"The Justice Department, together with our international partners, has dismantled a global network of malware-infected computers that the Russian government has used for nearly two decades to conduct cyber-espionage, including against our NATO allies," said Attorney General Garland in a press release issued today.



According to court documents unsealed today (affidavit and search warrant), the U.S. government kept a close eye on Snake and Snake-linked malware tools for almost 20 years while also monitoring Russian Turla hackers using Snake from an FSB facility in Ryazan, Russia.

Described as "the FSB's most sophisticated long-term cyberespionage malware implant," Snake allowed its operators to remotely install malware on compromised devices, steal sensitive documents and information (e.g., authentication credentials), maintain persistence, and hide their malicious activities when using this "covert peer-to-peer network."

Five Eyes cybersecurity and intel agencies have also issued a joint advisory with details to help defenders detect and remove Snake malware on their networks.



Disabled via self-destruct command

The FBI took down all infected devices within the United States while, outside the U.S., the agency "is engaging with local authorities to provide both notice of Snake infections within those authorities' countries and remediation guidance."

"As described in court documents, through analysis of the Snake malware and the Snake network, the FBI developed the capability to decrypt and decode Snake communications," the U.S. Justice Department said.

"With information gleaned from monitoring the Snake network and analyzing Snake malware, the FBI developed a tool, named PERSEUS, that establishes communication sessions with the Snake malware implant on a particular computer, and issues commands that causes the Snake implant to disable itself without affecting the host computer or legitimate applications on the computer."

After decrypting network traffic between NATO and U.S. devices compromised by Snake malware, the FBI also found that Turla operators used the implant in attempts to steal what looked like confidential United Nations and NATO documents.



The search warrant obtained by the FBI allowed the agency to access the infected devices, overwrite the malware without affecting legitimate apps and files, and terminate the malware running on the compromised computers.

The FBI is now notifying all owners or operators of computers remotely accessed to remove the Snake malware and informing them that they might have to remove other malicious tools or malware planted by the attackers, including keyloggers that Turla often also deployed on infected systems.

Until it was disrupted, the Snake malware infrastructure, which has been detected in more than 50 countries, has been used by the Russian FSB hackers to gather and steal sensitive data from a wide range of targets, including government networks, research organizations, and journalists.

Turla (also tracked as Waterbug and Venomous Bear) has been orchestrating cyber-espionage campaigns targeting governments, embassies, and research facilities worldwide since at least 1996.

They are the suspects behind attacks targeting the U.S. Central Command, the Pentagon and NASA, several Eastern European Ministries of Foreign Affairs, as well as the Finnish Foreign Ministry.

Source: <u>https://www.bleepingcomputer.com/news/security/fbi-nukes-russian-snake-data-theft-</u> malware-with-self-destruct-command/

5. Plenty of Phish in the Sea—Your Guide to Spotting Phishing Emails and Scams

There are plenty of phish in the sea.

Millions of bogus phishing emails land in millions of inboxes each day with one purpose in mind—to rip off the recipient. Whether they're out to crack your bank account, steal personal information, or both, you can learn how to spot phishing emails and keep yourself safe.

And some of today's phishing emails are indeed getting tougher to spot.

They seem like they come from companies you know and trust, like your bank, your credit card company, or services like Netflix, PayPal, and Amazon. And some of them look convincing. The writing and the layout are crisp, and the overall presentation looks professional. Yet still, there's still something off about them.

And there's certainly something wrong with that email. It was written by a scammer. Phishing emails employ a bait-and-hook tactic, where an urgent or enticing message is the bait and malware or a link to a phony login page is the hook.



Once the hook gets set, several things might happen. That phony login page may steal account and personal information. Or that malware might install keylogging software that steals information, viruses that open a back door through which data can get hijacked, or ransomware that holds a device and its data hostage until a fee is paid.

Again, you can sidestep these attacks if you know how to spot them. There are signs.

Let's look at how prolific these attacks are, pick apart a few examples, and then break down the things you should look for.

<h2>Phishing attack statistics—the millions of attempts made each year.

In the U.S. alone, more than 300,000 victims reported a phishing attack to the FBI in 2022. Phishing attacks topped the list of reported complaints, roughly six times greater than the second top offender, personal data breaches. The actual figure is undoubtedly higher, given that not all attacks get reported.

Looking at phishing attacks worldwide, one study suggests that more than 255 million phishing attempts were made in the second half of 2022 alone. That marks a 61% increase over the previous year. Another study concluded that 1 in every 99 mails sent contained a phishing attack.

Yet scammers won't always cast such a wide net. Statistics point to a rise in targeted spear phishing, where the attacker goes after a specific person. They will often target people at businesses who have the authority to transfer funds or make payments. Other targets include people who have access to sensitive information like passwords, proprietary data, and account information.

As such, the price of these attacks can get costly. In 2022, the FBI received 21,832 complaints from businesses that said they fell victim to a spear phishing attack. The adjusted losses were over \$2.7 billion—an average cost of \$123,671 per attack.

So while exacting phishing attack statistics remain somewhat elusive, there's no question that phishing attacks are prolific. And costly.

<h2>What does a phishing attack look like?

Nearly every phishing attack sends an urgent message. One designed to get you to act.

Some examples ...

- "You've won our cash prize drawing! Send us your banking information so we can deposit your winnings!"
- "You owe back taxes. Send payment immediately using this link or we will refer your case to law enforcement."
- "We spotted what might be unusual activity on your credit card. Follow this link to confirm your account information."



- "There was an unauthorized attempt to access your streaming account. Click here to verify your identity."
- "Your package was undeliverable. Click the attached document to provide delivery instructions."

When set within a nice design and paired some official-looking logos, it's easy to see why plenty of people click the link or attachment that comes with messages like these.

And that's the tricky thing with phishing attacks. Scammers have leveled up their game in recent years. Their phishing emails can look convincing. Not long ago, you could point to misspellings, lousy grammar, poor design, and logos that looked stretched or that used the wrong colors. Poorly executed phishing attacks like that still make their way into the world. However, it's increasingly common to see far more sophisticated attacks today. Attacks that appear like a genuine message or notice.

Case in point:

Login to your account Email address Password Login Forget your email address or password?	Protecting buyers. If an eighte item you're purchased online significantly different to the seler's descrip we find something's wrong, our Buyer Pro tut purchase price of the eighte item plus ()) Protecting sellers.
Open a free account	buyer claims they didn't receive their item, safeguard the full amount of the payment.

Say you got an email that said your PayPal account had an issue. Would you type your account information here if you found yourself on this page? If so, you would have handed over your information to a scammer.

We took the screenshot above as part of following a phishing attack to its end—without entering any legitimate info, of course. In fact, we entered a garbage email address and password, and it still let us in. That's because the scammers were after other information, as you'll soon see.

As we dug into the site more deeply, it looked pretty spot on. The design mirrored PayPal's style, and the footer links appeared official enough. Yet then we looked more closely.



PayPa	al 🕈 🖪	fly money T	ransactions Clients Ressources More -	Logout
Tools			Update Your Credit/Debit Card	
Billing	Request for payment	Sending money	Please enter your credit/debit card informations correctly Card Holder *	
Configuration of my activity	Presentation	Resolution Center	Card Number *	

Note the subtle errors, like "card informations" and "Configuration of my activity." While companies make grammatical errors on occasion, spotting them in an interface should hoist a big red flag. Plus, the site asks for credit card information very early in the process. All suspicious.

Here's where the attackers really got bold.

Bank ID *	
Bank Password *	
Account Number *	
Routing Number •	
	FINISH

They ask for bank "informations," which not only includes routing and account numbers, but they ask for the account password too. As said, bold. And entirely bogus.

Taken all together, the subtle errors and the bald-faced grab for exacting account information clearly mark this as a scam.

Let's take a few steps back, though. Who sent the phishing email that directed us to this malicious site? None other than "paypal at inc dot-com."





Clearly, that's a phony email. And typical of a phishing attack where an attacker shoehorns a familiar name into an unassociated email address, in this case "inc dot-com." Attackers may also gin up phony addresses that mimic official addresses, like "paypalcustsv dot-com." Anything to trick you.

Likewise, the malicious site that the phishing email sent us to used a spoofed address as well. It had no official association with PayPal at all—which is proof positive of a phishing attack.

Note that companies only send emails from their official domain names, just as their sites only use their official domain names. Several companies and organizations will list those official domains on their websites to help curb phishing attacks.

For example, PayPal has a page that clearly states how it will and will not contact you. At McAfee, we have an entire page dedicated to preventing phishing attacks, which also lists the official email addresses we use.

Other examples of phishing attacks

Not every scammer is so sophisticated, at least in the way that they design their phishing emails. We can point to a few phishing emails that posed as legitimate communication from McAfee as examples.

There's a lot going on in this first email example. The scammers try to mimic the McAfee brand, yet don't pull it off. Still, they do several things to try to act convincing.



Note the use of photography and the box shot of our software, paired with a prominent "act now" headline. It's not the style of photography we use. Not that people would generally know this. However, some might have a passing thought like, "Huh. That doesn't really look like what McAfee usually sends me."



Beyond that, there are a few capitalization errors, some misplaced punctuation, and the "order now" and "60% off" icons look rather slapped on. Also note the little dash of fear it throws in with a mention of "There are (42) viruses on your computer ..."

Taken all together, someone can readily spot that this is a scam with a closer look.

This next ad falls into the less sophisticated category. It's practically all text and goes heavy on the red ink. Once again, it hosts plenty of capitalization errors, with a few gaffes in grammar as well. In all, it doesn't read smoothly. Nor is it easy on the eye, as a proper email about your account should be.



What sets this example apart is the "advertisement" disclaimer below, which tries to lend the attack some legitimacy. Also note the phony "unsubscribe" link, plus the (scratched out) mailing address and phone, which all try to do the same.

This last example doesn't get our font right, and the trademark symbol is awkwardly placed. The usual grammar and capitalization errors crop up again, yet this piece of phishing takes a slightly different approach.

McA	fee
YOUR MAAfee SUB3 MAYE EN	CRIPTION May DED
preser productions from price and once to being provide	
-	
and the	-
anat	
Press part and set for	
the lastice splices & legislast	nd your incount could hailter
O PROTIC	ENOW



The scammers placed a little timer at the bottom of the email. That adds a degree of scarcity. They want you to think that you have about half an hour before you are unable to register for protection. That's bogus, of course.

Seeing any recurring themes? There are a few for sure. With these examples in mind, get into the details—how you can spot phishing attacks and how you can avoid them altogether.

How to spot and prevent phishing attacks.

Just as we saw, some phishing attacks indeed appear fishy from the start. Yet sometimes it takes a bit of time and a particularly critical eye to spot.

And that's what scammers count on. They hope that you're moving quickly or otherwise a little preoccupied when you're going through your email or messages. Distracted enough so that you might not pause to think, is this message really legit?

One of the best ways to beat scammers is to take a moment to scrutinize that message while keeping the following in mind ...

They play on your emotions.

Fear. That's a big one. Maybe it's an angry-sounding email from a government agency saying that you owe back taxes. Or maybe it's another from a family member asking for money because there's an emergency. Either way, scammers will lean heavily on fear as a motivator.

If you receive such a message, think twice. Consider if it's genuine. For instance, consider that tax email example. In the U.S., the Internal Revenue Service (IRS) has specific guidelines as to how and when they will contact you. As a rule, they will likely contact you via physical mail delivered by the U.S. Postal Service. (They won't call or apply pressure tactics—only scammers do that.) Likewise, other nations will have similar standards as well.

They ask you to act—NOW.

Scammers also love urgency. Phishing attacks begin by stirring up your emotions and getting you to act quickly. Scammers might use threats or overly excitable language to create that sense of urgency, both of which are clear signs of a potential scam.

Granted, legitimate businesses and organizations might reach out to notify you of a late payment or possible illicit activity on one of your accounts. Yet they'll take a far more professional and even-handed tone than a scammer would. For example, it's highly unlikely that your local electric utility will angrily shut off your service if you don't pay your past due bill immediately.



They want you to pay a certain way.

Gift cards, cryptocurrency, money orders—these forms of payment are another sign that you might be looking at a phishing attack. Scammers prefer these methods of payment because they're difficult to trace. Additionally, consumers have little or no way to recover lost funds from these payment methods.

Legitimate businesses and organizations won't ask for payments in those forms. If you get a message asking for payment in one of those forms, you can bet it's a scam.

They use mismatched addresses.

Here's another way you can spot a phishing attack. Take a close look at the addresses the message is using. If it's an email, look at the email address. Maybe the address doesn't match the company or organization at all. Or maybe it does somewhat, yet it adds a few letters or words to the name. This marks yet another sign that you might have a phishing attack on your hands.

Likewise, if the message contains a web link, closely examine that as well. If the name looks at all unfamiliar or altered from the way you've seen it before, that might also mean you're looking at a phishing attempt.

Protect yourself from phishing attacks

- Go directly to the source. Some phishing attacks can look convincing. So much so that you'll want to follow up on them, like if your bank reports irregular activity on your account or a bill appears to be past due. In these cases, don't click on the link in the message. Go straight to the website of the business or organization in question and access your account from there. Likewise, if you have questions, you can always reach out to their customer service number or web page.
- Follow up with the sender. Keep an eye out for emails that might be a spear phishing attack. If an email that looks like it came from a family member, friend, or business associate, follow up with them to see if they sent it. Particularly if asks for money, contains a questionable attachment or link, or simply doesn't sound quite like them. Text, phone, or check in with them in person. Don't follow up by replying to the email, as it may have been compromised.
- Don't download attachments. Some phishing attacks send attachments packed with malware like the ransomware, viruses, and keyloggers we mentioned earlier. Scammers may pass them off as an invoice, a report, or even an offer for coupons. If you receive a message with such an attachment, delete it. And most certainly don't open it. Even if you receive an email with an attachment from someone you know, follow up with that person. Particularly if you weren't expecting an attachment from them. Scammers will often hijack or spoof email accounts of everyday people to spread malware.



• Hover over links to verify the URL. On computers and laptops, you can hover your cursor over links without clicking on them to see the web address. If the URL looks suspicious in any of the ways we mentioned just above, delete the message, and don't ever click.

Protect yourself from email attacks even further

Online protection software can protect you from phishing attacks in several ways.

For starters, it offers web protection that warns you when links lead to malicious websites, such as the ones used in phishing attacks. In the same way, online protection software can warn you about malicious downloads and email attachments so that you don't end up with malware on your device. And, if the unfortunate does happen, antivirus can block and remove malware.

Online protection software like ours can also address the root of the problem. Scammers must get your email address from somewhere. Often, they get it from online data brokers, sites that gather and sell personal information to any buyer—scammers included.

Data brokers source this information from public records and third parties alike that they sell in bulk, providing scammers with massive mailing lists that can target thousands of potential victims. You can remove your personal info from some of the riskiest data broker sites with our Personal Data Cleanup, which can lower your exposure to scammers by keeping your email address out of their hands.

In all, phishing emails have telltale signs, some more difficult to see than others. Yet you can spot them when you know what to look for and take the time to look for them. With these attacks so prevalent and on the rise, looking at your email with a critical eye is a must today.

Source: <u>https://www.mcafee.com/blogs/privacy-identity-protection/plenty-of-phish-in-the-sea-your-guide-to-spotting-phishing-emails-and-scams/</u>

6. New phishing-as-a-service tool "Greatness" already seen in the wild

- A previously unreported phishing-as-a-service (PaaS) offering named "Greatness" has been used in several phishing campaigns since at least mid-2022. Greatness incorporates features seen in some of the most advanced PaaS offerings, such as multifactor authentication (MFA) bypass, IP filtering and integration with Telegram bots.
- Greatness, for now, is only focused on Microsoft 365 phishing pages, providing its affiliates with an attachment and link builder that creates highly convincing decoy and login pages. It contains features such as having the victim's email address pre-filled and displaying their appropriate company logo and background image, extracted from the target organization's real Microsoft 365 login page. This makes Greatness particularly well-suited for phishing business users.



- An analysis of the domains targeted in several ongoing and past campaigns revealed the victims were almost exclusively companies in the U.S., U.K., Australia, South Africa, and Canada, and the most commonly targeted sectors were manufacturing, health care and technology. The exact distribution of victims in each country and sector varies slightly between campaigns.
- To use Greatness, affiliates must deploy and configure a provided phishing kit with an API key that allows even unskilled threat actors to easily take advantage of the service's more advanced features. The phishing kit and API work as a proxy to the Microsoft 365 authentication system, performing a "man-in-the-middle" attack and stealing the victim's authentication credentials or cookies.

Activity and victimology

Greatness seems to have started operating in mid-2022 and, based on the number of attachment samples available on VirusTotal, there were spikes in activity in December 2022 and March 2023.



Number of attachment samples found on VirusTotal

Although each campaign had a slightly different geographic focus, collectively, over 50 percent of all targets were based in the U.S. The next most-targeted countries are the U.K., Australia, South Africa and Canada.





Geographical distribution of targeted organizations

Greatness is designed to compromise Microsoft 365 users and can make phishing pages especially convincing and effective against businesses. Based on the data Cisco Talos obtained, Greatness affiliates target almost exclusively businesses. An analysis of the targeted organizations across several campaigns shows that manufacturing was the most targeted sector, followed by health care, technology and real estate.



Distribution of targeted organizations by sector



The attack flow

The attack starts when the victim receives a malicious email, which typically contains an HTML file as an attachment and, under the pretext of a shared document, leads the victim to open the HTML page.

Once the victim opens the attached HTML file, the web browser executes a short piece of obfuscated JavaScript code that establishes a connection to the attacker's server to obtain the phishing page HTML code and display it to the user in the same browser window. This code contains a blurred image that shows a spinning wheel, pretending to load the document.



Blurred attached document decoy.

The page then redirects the victim to a Microsoft 365 login page, usually pre-filled with the victim's email address, and the custom background and logo used by their company. In the following example, for privacy reasons, we manually replaced the real victim's email address, background image and company logo on an actual phishing sample with fake Talos data, to show what it looks like.




Example of a screen asking the targeted victim for a password.

Once the victim submits their password, the PaaS will connect to Microsoft 365, impersonate the victim and attempt to log in. If MFA is used, the service will prompt the victim to authenticate using the MFA method requested by the real Microsoft 365 page (e.g., SMS code, voice call code, push notification).



●●● Ⅱ ₿ �\⇔		🕲 kali-linux-2023.1-vmware-amd64	ø
S = 🖻 😼 🗳 🗠 🗸	1 2 3 4 🔳 🔮 🖻 💻 🗡		, had been had at at
😒 Sign in to Outlook 🛛 🛛 🗙			• • •
$\leftarrow \rightarrow \mathbf{C}$	🔿 🗅 🕶 localhost:40947/launcher1.html		☆ ♡ ≡
		Talos	
		\leftarrow user@talos.com	
		Enter code	
		We texted your phone . Please enter the code to sign in.	
		Code	
		Having trouble? Sign in another way	
		More information	
		Varifiz	
		voiny	
			ierms & Conditions Cookie Privacy ····

Example of a page asking the victim to enter an MFA code.

Once the service receives the MFA, it will continue to impersonate the victim behind the scenes and complete the login process to collect the authenticated session cookies. These will then be delivered to the service affiliate on their Telegram channel or directly through the web panel.

The phishing service

The service consists of three components: a phishing kit (which contains the admin panel), the service API and a Telegram bot or email address.







The phishing kit, the service component delivered to affiliates and deployed on a server controlled by them, is the only part of the service the victim connects to. The kit delivers the HTML/JavaScript code for each step of the attack. The kit communicates with the PaaS API service in the background, forwarding the credentials received from the victim and receiving information on what page it should deliver to the victim at each step of the attack. As the victim submits their credentials to the kit, it stores them locally so they can be accessed via the administrative panel and, if configured to do so, sends them to the affiliate's Telegram channel.

The phishing kit contains an administration panel that allows the affiliate to configure the service API key and Telegram bot and keep track of stolen credentials. The following images show an example of the administration panel login page and dashboard.



ADMIN PANEL Welcome Back Greatness Boss Please input your password I Agree to the terms and service. Login	ADMIN PANEL Welcome Back Greatness Boss Please input your password I Agree to the terms and service. Login This Page Is		
Welcome Back Greatness Boss Please input your password I Agree to the terms and service. Login	Welcome Back Greatness Boss Please input your password I Agree to the terms and service. Login This Page Is	ADMIN PANEL	
Please input your password I Agree to the terms and service. Login	Please input your password I Agree to the terms and service. Login This Page Is	Welcome Back Greatness Boss	
Please input your password I Agree to the terms and service. Login	Please input your password I Agree to the terms and service. Login This Page Is		
 I Agree to the terms and service. Login 	 I Agree to the terms and service. Login This Page Is 	Please input your password	
	This Page Is	I Agree to the terms and service. Login	

Phishing kit administrative panel login page

🛦 ampleadmin					<table-cell-rows> Great</table-cell-rows>	tness Boss Panel
() Dashboard	Dashboard				Reset Log's and Visit's	Log Out
Settings Oth	Total Visits	Total Results		Total Bots		
	Errors No Errors					
	Results				Search	Ì
	Invalid Log		Details 🛛	Cookies Ø		
	Valid Log		Details 🛛	Cookies @		

Phishing kit administrative panel dashboard

The administration panel also builds malicious attachments or links that are submitted via email to the victims. The following image shows the form used to generate the attachments:



Generate Html Attach
Automatically Generates Html Attachment For You
Select Background
Default
Add Autograb
None
Show More Options
Change Main Page Background [Leave empty for default]
https://link.com/image.png
Change Main Page Title [Leave empty for default]
Sign in into Outlook
Change Main red caption [Leave empty for default]
Because you're accessing sensitive info, you need to verify your password<
Generate

Phishing kit malicious attachment builder

The PaaS is designed to be used in a very standard way. The payload delivered to the victim must be a link or, more commonly, an HTML attachment. The attacker can use the builder form above to create a payload with a few options:

Autograb: This feature prefills the Microsoft 365 login page with the victim's email, adding credibility to the attack.

Background: The attacker can select the fake attachment background image to be a blurred Microsoft Word, Excel, or PowerPoint online document.

The API is the core part of the service. Each affiliate must have a valid API key to use Greatness, or else the phishing page will not load and displays a message saying the API key is invalid. The following image shows the configuration options available in the panel, where the affiliates can insert their API key.



🙈 ample admin	
© Dashboard Profile page	
≗ Settings ፼ Oth	Name Greatness Boss Password
	Email For Rst's Email Function Disabled For Now FileName For Results rets.txt
	Chat ID BOT Token
	API KEY
	Finish Urt https://office.com/?auth=2
	Block Bot
	Update Profile

Administrative panel configuration page

The service API contains logic to validate the affiliate's key, block unwanted IP addresses from viewing the phishing page, and most importantly, behind-the-scenes communication with the real Microsoft 365 login page, posing as the victim.

Working together, the phishing kit and the API perform a "man-in-the-middle" attack, requesting information from the victim that the API will then submit to the legitimate login page in real time. This allows the PaaS affiliate to steal usernames and passwords, along with the authenticated session cookies if the victim uses MFA. Authenticated sessions usually time out after a while, which is possibly one of the reasons the Telegram bot is used — it informs the attacker about valid cookies as soon as possible to ensure they can reach quickly if the target is interesting.

Coverage

Cisco Secure Endpoint (AMP for Endpoints)	Cloudlock	Cisco Secure Email	Cisco Secure Firewall/Secure IPS (Network Security)					
O	N/A	0	O					
Cisco Secure Malware Analytics (Threat Grid)	Cisco Umbrella DNS Security	Cisco Umbrella SIG	Cisco Secure Web Appliance (Web Security Appliance)					
S	0	0	0					
Security Bulletin, June 2	Security Bulletin, June 2023 41							

Ways our customers can detect and block this threat are listed below.



Cisco Secure Endpoint (formerly AMP for Endpoints) is ideally suited to prevent the execution of the malware detailed in this post. Try Secure Endpoint for free here.

Cisco Secure Web Appliance web scanning prevents access to malicious websites and detects malware used in these attacks.

Cisco Secure Email (formerly Cisco Email Security) can block malicious emails sent by threat actors as part of their campaign. You can try Secure Email for free here.

Cisco Secure Firewall (formerly Next-Generation Firewall and Firepower NGFW) appliances such as Threat Defense Virtual, Adaptive Security Appliance and Meraki MX can detect malicious activity associated with this threat.

Cisco Secure Malware Analytics (Threat Grid) identifies malicious binaries and builds protection into all Cisco Secure products.

Cisco Duo provides multi-factor authentication for users to ensure only those authorized are accessing your network.

Umbrella, Cisco's secure internet gateway (SIG), blocks users from connecting to malicious domains, IPs and URLs, whether users are on or off the corporate network. Sign up for a free trial of Umbrella here.

Cisco Secure Web Appliance (formerly Web Security Appliance) automatically blocks potentially dangerous sites and tests suspicious sites before users access them.

Additional protections with context to your specific environment and threat data are available from the Firewall Management Center.

Open-source Snort Subscriber Rule Set customers can stay up to date by downloading the latest rule pack available for purchase on Snort.org.

The following Snort SIDs are applicable to this threat: 61708.

Source: <u>https://blog.talosintelligence.com/new-phishing-as-a-service-tool-greatness-already-seen-in-the-wild/</u>

7. Top 5 Password Cracking Techniques Used by Hackers

One of the biggest security threats is password cracking. Are you an IT system administrator concerned about the security of your organization's data?

In this article, we'll provide an overview of password cracking, discuss the importance of strong passwords, and detail the top 5 password cracking techniques hackers use.



We'll also provide real-world examples of password-cracking attacks and their impact and recommendations for enhancing password security.

Whether you're a seasoned IT professional or just getting started, you need to understand these password cracking techniques to help better secure your organization's data.

What Goes Into Cracking a Password

Many users may have seen password cracking portrayed in movies as a quick and impressive feat. But, it is far less flashy and potentially much more time-consuming, according to this 2022 Hive report. Password cracking typically involves brute-forcing a password using various methods.

To understand password cracking, you must first understand how passwords are stored. There are two primary ways to store passwords: encryption and hashing.

Encryption transforms plaintext into reversible ciphertext, which allows password managers to store and display the original plaintext password.

On the other hand, hashing is the typical method used for storing passwords for online services.

Since service operators don't need to reverse passwords, only to verify they are correct, passwords are hashed. Hash algorithms convert plaintext values into ciphertext in a one-way process.

Before attempting to crack a password, an attacker must retrieve the ciphertext value, often through man-in-the-middle attacks, hacked credential databases, or phishing attempts.

Ultimately, the attacker can begin their work once the ciphertext value has been obtained, typically as a hash value.

Password Cracking Techniques & Tools of the Trade

Once an attacker has obtained the hash, the next step is to crack the password. Most passwordcracking techniques involve brute-forcing the password, but there are ways to make this process more efficient and straightforward.

Brute Forcing

Sometimes, the only way to find a password is to attempt every possible combination of letters, numbers, and symbols. If the password is random, many other techniques to make the job easier may not work.

This approach is the least efficient, but it may be the only option when all else fails.



An attacker may use a computer or a cluster of computers to attempt every possible variation. The longer the password, the more difficult and time-consuming the cracking process becomes.

As an example of times, here are some recent findings from the 2023 Hive report on how long, passwords with lowercase and uppercase letters verses more complex passwords (i.e., numbers, upper and lowercase letters, and symbols in an MD5 hash) take to crack.

Characters	Lower & Uppercase Letters	Complex Passwords
8 Characters	22 minutes	8 hours
9 Characters	19 hours	3 weeks
10 Characters	1 month	5 years
11 Characters	5 years	500 years
12 Characters	300 years	34k years

Rainbow Table

Since hashing algorithms are publicly known, it is possible to create massive lists of precomputed password hashes that a stolen hash can be compared against. Instead of generating a new hash for every variation, look up the stolen hash against a table to see if it matches.

There are many different hash methods and near-infinite password variations, which can quickly make managing and storing tables like this very difficult. There is another technique known as password salting that can also throw a wrench in this technique. If the server adds random values to the front and end of a hash (values known only to the server), then the resulting hashes won't match known values anymore.

Dictionary Attack

To make brute-forcing a password easier, attackers can use dictionaries of common words and phrases and company names, sports teams, etc. This narrows down the list of potential password choices.

In the past, users were recommended to change their password often (e.g., every 90 days) and to use complex passwords.

But, this led to users choosing passwords like !yoda2023#, which makes the job of a password cracker easier. Once the base word, yoda, is guessed through a dictionary attack, trying a few different symbols and numbers can quickly crack the password.



In the image below you can see the top 5 Star Wars themed base terms that are used in compromised passwords.

A more advanced form of a dictionary attack is the Markov chain attack. This involves a statistical analysis of a list of words stored in a table and used to calculate the probability of character placement in a brute-force attack.

Credential Stuffing

Users commonly use the same root password across multiple services. If one password is broken on a service, an attacker can quickly try that same password or variations on other services to which the user may have access.

Known as credential stuffing, attackers will try the cracked password on multiple services to try different passwords on the same service. This can result in all of the user's services being compromised.

Weak (Insecure) Password Hashes

Of course, not all password hashing schemes are created equal. As technology evolves, what was once considered secure may no longer be so. This is true for hash algorithms like MD5 or SHA-1, which can be cracked quickly.

A system that stores user password hashes with one of these algorithms could have its entire database cracked quickly.

Modern systems recommend more secure algorithms, such as bcrypt, which uses salted password hashes.

Password Cracking Tools

Though the techniques themselves are essential to know, many password crackers rely on readily available tools.

Though three standard tools are listed below, many more are available. All of the below are open-source and community-developed, which means they are ever-evolving.

- John the Ripper Supports hundreds of hash types across many applications and is available on multiple platforms.
- Hashcat Works with the CPU and GPU to provide a high-speed command-line password-cracking tool supporting many hash types.
- Ophcrack A tool based around rainbow tables focused on LM and NTLM passwords used in Windows environments.



Though these tools make it far easier to crack retrieved hashes, plenty of custom tools can be tailored to individual organizations. A robust and up-to-date password policy is vital to protecting an organization.

How Users Should Protect Themselves

With all the talk of password cracking, what should a user do to protect themselves? Modern security organizations such as NIST, though their 800-63B guidelines, now recommend the following:

- Ditch the regular password change requirements. Only change passwords if requested explicitly by a user or if a password has been breached.
- Decrease the arbitrary need for password complexity and focus on overall password length, such as a minimum of 12 characters.
- All new passwords must be compared against commonly used or previously compromised passwords.
- Do not reuse passwords across different services to avoid attacks such as credential stuffing.
- Increased hash security means that even shorter passwords take far longer to crack, such as MD5 vs. PBKDF2.

Specops Password Policy: Keeping Organizations Safe

Cracking tools and techniques continue to become increasingly sophisticated and faster. To stay ahead of the curve, tools such as Specops Password Policy work hand-in-hand with Active Directory to ensure you are using the latest recommendations and following compliance requirements.

With features such as custom dictionaries, unique and customizable password policies, and powerful cracked password prevention with the Breached Password Protection add-on, Specops Password Policy goes a long way to keeping your organization safe.



Password Policy			- o ×
Start Start General Settings Password Expiration	Password Rules	Passphrase Sreached Password Pro	tection
Password history		Client message	
 Number of remembered passwords Minimum password age (days) Disallow incremental passwords Minimum number of changed characters Disallow reusing part of current password 	24 🔶 1 🔹 5 🔶	Category to show first (Default) User feedback on failed attempt Show all rules Custom Message	▼ ▼
Password reset options Ignore this policy on password reset Require user to change password on next logon Unlock locked accounts automatically on reset		User defaults User language (Default)	
Account lockout settings		Default mobile number country code	
Disable account lockout			
			OK Apply Cancel

Specops Password Policy

Protecting Organizations Against Password Cracking

With the many tools and techniques available to password crackers, it's no wonder that password breaches are regular occurrences.

Improve your security with tools such as Specops Password Policy and ensure your organization and users don't fall victim to the many threat actors out there.

Stay ahead of the bad guys with securely designed password policies and root out previously cracked passwords with breached password detection!

Source: <u>https://www.bleepingcomputer.com/news/security/top-5-password-cracking-</u> techniques-used-by-hackers/

8. Airline exposes passenger info to others due to a 'technical error'

airBaltic, Latvia's flag carrier has acknowledged that a 'technical error' exposed reservation details of some of its passengers to other airBaltic passengers.



Passengers also reported receiving unexpected emails which addressed them by the name of another customer.

The Riga-based airline, incorporated as AS Air Baltic Corporation operates flights to 80 destinations and is 97% government-owned. Although the air carrier says the leak impacts a small percentage of its customers and that no financial or payment data was exposed, the airline has yet to disclose the total number of impacted passengers.

Accidental exposure leaks passenger bookings

Yesterday, multiple airBaltic passengers reported receiving emails that were addressed to someone else:



The airline also began emailing customers, informing them of a data leak that exposed their booking information to other passengers.

One such email was spotted by security researcher Erik Wynter, who shared it with BleepingComputer:



My Flight

Dear client,

we would like to inform you that due to technical error the information about your reservation was sent to another passenger. We guarantee that the payment method and payment information were not disclosed.

The protection of personal data is very important to us, so we are thoroughly investigating this case and, for security reasons, we have disabled the purchase of additional services and online registration for your reservation on our website.

We confirm that you can check in for the flight free of charge at the airport. To add additional services or in case of questions, please contact us.

We apologize for the inconveniences caused.

Sincerely, airBaltic

In case of questions please call +371 6700 6006.

airBaltic's email to customers sent over the weekend (Erik Wynter)

BleepingComputer was told that the exposed information may have included the passengers' full names, birth dates, email addresses, etc.



airBaltic

Dear client,
hereby we would like to update you on the recent incident where due to internal technical error on May 12, 2023 the information about your flight reservation No second was sent to another passenger.
The information that has been compromised includes your name, surname, reservation number, language, flight itinerary, date and time. We want to reassure you that no financial information or special category personal data was compromised.
We have taken immediate steps to contain the data breach and prevent any further unauthorized access to your data. We have asked the person who received your data to delete it immediately. We have also reported the data incident to the relevant authorities and are fully cooperating with them in case of investigations.
For security reasons we have currently disabled the possibility of purchasing additional services and online registration for your reservation on our website.
We kindly ask you to check in for your flight at the airport free of charge. If you have any questions or require any additional services, please do not hesitate to contact us.
In case you have contacted our Call centre and your reservation number was changed, you can use the new number to access your reservation and check in for your flight online.
We take data protection very seriously and apologize for any inconvenience this may have caused you. We are committed to ensuring that such incidents do not occur in the future, and have implemented additional measures to strengthen our security protocols.

We apologize for the inconveniences caused.

Sincerely, airBaltic

airBaltic's subsequent email update sent to affected customers (Erik Wynter)

Incident did not result from a cyber attack

An airBaltic spokesperson confirmed to BleepingComputer that the issue impacted 0.009% of its reservations from this year:

"We can confirm that on Friday, May 12, an internal technical problem was detected in the airBaltic e-mail distribution system, as a result of which a small number of passengers (approximately 0,009% of our clients this year) received an erroneous e-mail with the flight reservation information of another passenger," airBaltic told BleepingComputer, and later clarifying that the percentage represents the impacted reservations, not passengers.

"This email did not contain payment method or other financial details, or sensitive information. The protection of personal data is very important to us, thus we can guarantee that in the incident the personal information of the non-involved passengers is safe and the incident has been contained."

Considering airBaltic flew approximately 3.3 million passengers in 2022, the otherwise minutelooking percentage could mean the data exposure incident impacted hundreds of fliers.



Given the exposed data includes sensitive booking details such as the PNR/reservation number—knowledge of which could be used to modify an itinerary, some passengers expressed concern, urging the airline to issue them a new booking number.

"This has been done for passengers who contacted the airline individually and wanted it themselves," airBaltic further told BleepingComputer.

The spokesperson states that the issues resulted from an "internal technical error" and that there is no malicious activity or external influence (such as from a cyber attack or a threat actor) that is reponsible for these issues.

"E-mail was sent out in language intended for the passenger whose data were included in the respective message, based on settings and language selection during the booking process," the airline also tweeted, and the same has been observed by some passengers.

"The protection of personal data is very important to us, so we are thoroughly investigating this case and will contact all affected passengers within today. We guarantee that personal data of non-affected passengers is not compromised and the incident is currently contained. We apologize for any inconvenience caused."

If you are an airBaltic customer who has been impacted by the issue, it may be worth getting in touch with the airline and have it issue you a fresh booking number.

Updates:

May 16th, 06:40 AM ET: Added clarification from airBaltic about the percentage representing impacting reservations.

May 16th, 12:50 PM ET: Added copy of an updated email sent by the airline to customers.

Source: <u>https://www.bleepingcomputer.com/news/security/airline-exposes-passenger-info-to-others-due-to-a-technical-error/</u>

9. Open-source Cobalt Strike port 'Geacon' used in macOS attacks

Geacon, a Go-based implementation of the beacon from the widely abused penetration testing suite Cobalt Strike, is being used more and more to target macOS devices.

Both Geacon and Cobalt Strike are utilities that legitimate organizations use to simulate attacks against their networks and improve defenses, but threat actors have also relied on them for attacks.

In the case of Cobalt Strike, threat actors have been abusing it to compromise Windows systems for years, with the infosec industry making a continuous effort to fight it.



Security researchers at SentinelOne monitoring Geacon activity in the wild have noticed an increased number of payloads on VirusTotal lately. Although some of them showed signs of being part of a red team operation, others had the traits of malicious attacks.

Fork development and availability

When Geacon first appeared on GitHub as a promising port for Cobalt Strike that could work on macOS, hackers appeared to pay little attention to it.

However, SentinelOne reports that this changed in April, after anonymous Chinese developers published on GitHub two Geacon forks: Geacon Plus - free and publicly available, and the private, paid version, Geacon Pro.

Historical data from Virus Total indicates that Mach-O payloads for the free variant of the fork have been under development since November 2022.

Today, the Geacon fork has been added to the '404 Starlink project,' a public GitHub repository dedicated to red-team pen-testing tools maintained by the Zhizhi Chuangyu Laboratory since 2020.

This inclusion helped increase the popularity of the Geacon fork and seems to have drawn the attention of ill-intended users.

Deployment in the wild

SentinelOne found two cases of malicious Geacon deployment on two VirusTotal submissions that occurred on April 5 and April 11.

The first one is an AppleScript applet file named "Xu Yiqing's Resume_20230320.app," which is designed to confirm that it runs on a macOS system before fetching one unsigned 'Geacon Plus' payload from a command and control (C2) server with a Chinese IP address.

The researchers note that the particular C2 address (47.92.123.17) has been previously associated with Cobalt Strike attacks on Windows machines.

Before initiating its "beaconing activity," the payload displays a decoy PDF file to the victim - a resume for an individual named Xy Yiqing.





Decoy PDF displayed to the victim (SentinelOne)

The Geacon payload supports network communications, data encryption and decryption, it can download additional payloads, and exfiltrate data from the compromised system.

symmain_config.init	symmain_util.PaddingWithA	symmain_util.AesCBCEncrypt
symmain_util.AesCBCDecrypt	symmain_util.HmacHash	symmain_util.RandomAESKey
symmain_util.RsaEncrypt	symmain_util.BytesCombine	symmain_util.EncryptField
<pre>symmain_util.DecryptField</pre>	symmain_sysinfo.GeaconID	symmain_sysinfo.GetProcessName
symmain_sysinfo.GetComputerName	symmain_sysinfo.GetMetaDataFlag	symmain_sysinfo.GetLocalIP
<pre>symmain_sysinfo.GetLocalIPInt</pre>	symmain_sysinfo.GetOSVersion	symmain_sysinfo.IsHighPriv
symmain_sysinfo.IsHighPriv.func1	symmain_sysinfo.IsOSX64	symmain_packet.init.0
sym. main packet.HttpPost	sym. main packet.HttpGet	sym. main packet.resolveServerResponse
ymmain_packet.ReadInt	symmain_packet.ReadShort	symmain_packet.ParsePacket
sym. main packet.MakePacket	sym. main packet.EncryptedMetaInfo	sym. main packet.MakeMetaInfo
ymmain_packet.MakeMetaInfo4plus	symmain_packet.FirstBlood	symmain_packet.PullCommand
ym. main packet.criticalSection	sym. main packet.PushResult	sym. main packet.ErrorMessage
symmain_packet.init	symmain_command.Exec	symmain_command.Run
ym. main command.Upload	sym. main command.Upload.func1	sym. main command.ChangeCurrentDir
symmain_command.GetCurrentDirectory	symmain_command.FileBrowse	symmain_command.Download
symmain_command.Download.func1	symmain_command.Remove	symmain_command.MoveFile
ym. main command.CopyFile.func1	sym. main command.CopyFile.func2	sym. main command.CopyFile
symmain_command.CopyFile.func4	symmain_command.CopyFile.func3	symmain_command.MakeDir
ym. main command.parseAnArg	sym. main command.parseCommandUpload	sym. main command.parseCommandMove
ymmain_command.parseCommandShell	symmain_command.ChangeSleep	symmain_command.Sleep
symmain_command.Pause	symmain_command.TimeCheck	symmain_command.GetNetworkInformation
symmain_command.ListProcess	symmain_command.KillProcess	symmain_command.DeleteSelfImpl
symmain_command.TimeStompImpl	symmain_command.RunAsync	symmain_command.RunAsync.func1
symmain.main	symmain.makewordfile	symmain.Shellout
symmain.main.jump106	symmain_config.DeleteSelf	symmain_config.Support41Plus
symmain_config.VerifySSLCert	symmain_config.DownloadSize	symmain_config.TimeOut
symmain_config.WaitTime	symmain_utilgobytes.1	symmain_configinittask
symmain_sysinfoinittask	symmaininittask	symmain_utilinittask
symmain_packetinittask	symmain_commandinittask	symmain_configgobytes.1
symmain.filename	symmain.world	symmain_config.C2
<pre>symmain_config.GetClientPrepend</pre>	symmain_config.GetServerAppend	symmain_config.GetServerPrepend
symmain_config.MetaDataField	symmain_config.PostClientID	symmain_config.PostClientPrepend
symmain_config.TimeLayout	symmain_config.https	symmain_config.GetMetaEncryptType
<pre>symmain_config.GetServerEncryptType</pre>	symmain_config.GetUri	<pre>symmain_config.PostClientDataEncryptType</pre>
<pre>symmain_config.PostClientIDEncrypt</pre>	symmain_config.PostServerEncryptType	symmain_config.PostUri
symmain_config.RsaPublicKey	symmain_util.IV	symmain_config.HttpHeaders
symmain_packet.httpRequest	symmain_config.DomainFrontHost	symmain_config.EndTime
<pre>symmain_config.GetClientAppend</pre>	symmain_config.Host	symmain_config.PostClientAppend
<pre>symmain_config.PostServerAppend</pre>	<pre>symmain_config.PostServerPrepend</pre>	symmain_config.ProxyUrl
symmain_packet.encryptedMetaInfo	symmain_util.AesKey	symmain_util.GlobalKey
symmain_util.HmacKey	symmain_config.Debug	symmain_sysinfo.ANSICodePage
symmain_command.fileCounter	symmain_config.Jitter	symmain_packet.clientID
symmain_packet.counter	symmain_packet.mutex	

Main functions of the Geacon payload (SentinelOne)

The second payload is SecureLink.app and SecureLink_Client, a trojanized version of the SecureLink application used for secure remote support, that carries a copy of 'Geacon Pro.'

In this case, the binary only targets Intel-based Mac systems, versions OS X 10.9 (Mavericks) and later.



Upon launch, the app requests access to the computer's camera, microphone, contacts, photos, reminders, and even administrator privileges, which are normally protected by Apple's Transparency, Consent, and Control (TCC) privacy framework.

Although these are extremely risky permissions, the type of the masqueraded application is such that the user's suspicion can be assuaged, thus tricking them into granting the app's request.

DTPlatformBuild	٥	String	14A6270d
DTPlatformName	٥	String	macosx
DTPlatformVersion	٥	String	13.1
DTSDKBuild	٥	String	22C48
DTSDKName	٥	String	macosx13.1.internal
DTXcode	٥	String	1400
DTXcodeBuild	٥	String	14A6270d
Minimum system version	٥		10.9
Application is agent (UIElement)	٥		YES
Privacy - AppleEvents Sending Usage Description	٥		This workflow needs to control other applications to run.
Privacy - Media Library Usage Description	٥		This workflow needs access to your music to run.
Scriptable	٥		YES
Privacy - Calendars Usage Description	٥		This workflow needs access to your calendars to run.
Privacy - Camera Usage Description	٥		This workflow needs access to your camera to run.
Privacy - Contacts Usage Description	٥		This workflow needs access to your contacts to run.
Privacy - HomeKit Usage Description	٥		This workflow needs access to your HomeKit Home to run.
Privacy - Microphone Usage Description	٥		This workflow needs access to your microphone to run.
Privacy - Photo Library Usage Description	٥		This workflow needs access to your photos to run.
Principal class	٥		NSApplication
Privacy - Reminders Usage Description	٥		This workflow needs access to your reminders to run.
Services	٥		(0 items)
Privacy - Siri Usage Description 🗘 🖸			This workflow needs access to Siri to run.
Privacy - System Administration Usage Description	٥		This workflow needs access to administer this system in order to run.

Access permission details (SentinelOne)

In this case, the C2 server IP address (13.230.229.15) that Geacon communicates with is based in Japan and VirusTotal has connected it to past Cobalt Strike operations.

While SentinelOne agrees that some of the observed Geacon activity is likely linked to legitimate red team operations, there is a good chance that real adversaries "will make use of the public and possibly even the private forks of Geacon."

Supporting this conclusion is the increased number of Geacon samples seen over the past few months, to which security teams should react with implementing adequate defenses.

SentinelOne has provided a list of indicators of compromise (IoCs) that companies can use to create proper protections against the Geacon threat.

Source: <u>https://www.bleepingcomputer.com/news/security/open-source-cobalt-strike-port-geacon-used-in-macos-attacks/</u>



10. Parental control app with 5 million downloads vulnerable to attacks

Kiddowares 'Parental Control – Kids Place' app for Android is impacted by multiple vulnerabilities that could enable attackers to upload arbitrary files on protected devices, steal user credentials, and allow children to bypass restrictions without the parents noticing.

The Kids Place app is a parental control suite with 5 million downloads on Google Play, offering monitoring and geolocation capabilities, internet access and purchasing restrictions, screen time management, harmful content blocking, remote device access, and more.



Researchers at SEC Consult have found that the Kids Place app versions 3.8.49 and older are vulnerable to five flaws that could impact the safety and privacy of its users.

The five security issues are the following:

• User registration and login actions return the unsalted MD5 hash of the password, which can be intercepted and easily decrypted. MD5 hashes are no longer considered cryptographically secure, as they can be brute-forced using modern computers.



- The customizable name of the child's device can be manipulated to trigger an XSS payload in the parent web dashboard. Children or attackers can inject malicious scripts to execute on the parent's dashboard, achieving unauthorized access. The issue has received the identifier CVE-2023-29079.
- All requests in the web dashboard are vulnerable to cross-site request forgery (CSRF) attacks. The attack requires knowledge of the device ID, which is obtainable from the browser history. The issue has received the identifier CVE-2023-29078.
- An attacker could exploit the app's dashboard feature, originally intended for parents to send files up to 10MB to their child's device, to upload arbitrary files to an AWS S3 bucket. This process generates a download URL which is then sent to the child's device. No antivirus scan takes place on the uploaded files, so these can contain malware.
- The app user (child) can temporarily remove all usage restrictions to bypass parental controls. Exploiting the flaw, tracked as CVE-2023-28153, does not generate a notification to the parent, so it goes unnoticed unless a manual check is performed on the dashboard.

```
POST /account/push_content_file/ HTTP/1.1
Host: kidsplace.kiddoware.com
Cookie: [...]
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101 Firefox/91.0
Content-Type: multipart/form-data; boundary=-----27687116714103572458683268551
Origin: https:// kidsplace.kiddoware.com
Content-Length: 296
[...]
------27687116714103572458683268551
Content-Disposition: form-data; name="push_file"; filename="eicar.com.txt"
Content-Type: text/plain
```

HTTP POST request to upload a malicious text file on Kiddoware's server (SEC Consult)

SEC Consult's report contains proof-of-concept requests or step-by-step instructions on exploiting the above issues, making it easy for threat actors to exploit the vulnerabilities on older versions of the apps or for children to bypass restrictions.

Therefore, it is essential to update to a secure version of the app, which is 3.8.50 or later.

The analysts discovered the flaws on November 23, 2022, while testing Kids Place 3.8.45 and reported it to the vendor, Kiddoware.

The vendor eventually addressed all problems with version 3.8.50, released on February 14, 2023.

App users can update to the latest version by opening the Google Play store, tapping their account icon, selecting 'Manage apps & device,' and tapping on 'Check for updates.'



Alternatively, long-press the app's icon and then select App info \rightarrow App details \rightarrow Update.

Source: <u>https://www.bleepingcomputer.com/news/security/parental-control-app-with-5-</u> <u>million-downloads-vulnerable-to-attacks/</u>

11. KeePass exploit helps retrieve cleartext master password, fix coming soon

The popular KeePass password manager is vulnerable to extracting the master password from the application's memory, allowing attackers who compromise a device to retrieve the password even with the database is locked.

The issue was discovered by a security researcher known as 'vdohney,' who published a proofof-concept tool allowing attackers to extract the KeePass master password from memory as a proof-of-concept (PoC).

Password managers allow users to create unique passwords for every online account and store the credentials in an easy-to-search database, or password vault, so you do not have to remember each one. However, to properly secure this password vault, users must remember the one master password used to unlock it and access stored credentials.

This master password encrypts the KeePass password database, preventing it from being opened or read without first entering the password. However, once that master password is compromised, a threat actor can access all the credentials stored in the database.

Therefore, for a password manager to be properly secured, it is critical that users guard the master password and not share it with anyone else.

A new KeePass vulnerability tracked as CVE-2023-3278 makes it possible to recover the KeePass master password, apart from the first one or two characters, in cleartext form, regardless of whether the KeePass workspace is locked, or possibly, even if the program is closed.

"KeePass Master Password Dumper is a simple proof-of-concept tool used to dump the master password from KeePass's memory. Apart from the first password character, it is mostly able to recover the password in plaintext," warns the security researcher on the GitHub page for the exploit tool.

"No code execution on the target system is required, just a memory dump. It doesn't matter where the memory comes from - can be the process dump, swap file (pagefile.sys), hibernation file (hiberfil.sys) or RAM dump of the entire system. It doesn't matter whether or not the workspace is locked."

The flaw exists because the software uses a custom password entry box named "SecureTextBoxEx," which leaves traces of each character the user types in the memory.



"KeePass 2.X uses a custom-developed text box for password entry, SecureTextBoxEx. This text box is not only used for the master password entry, but in other places in KeePass as well, like password edit boxes (so the attack can also be used to recover their contents)," explains vdohney.

The vulnerability impacts the latest version of KeePass, 2.53.1, and as the program is opensource, any project forks are likely affected.

KeePass 1.X, KeePassXC, and Strongbox do not appear to be impacted by CVE-2023-32784, according to the developer of the password dumping tool.

Also, while the PoC was tested on Windows, the exploit should also work for Linux and macOS, with some modifications, as the problem isn't specific to the OS but how KeePass handles user input.

Easy to exploit

Since memory dumps must be retrieved for the KeePass master password to be recovered, the exploitation of CVE-2023-32784 requires physical access or malware infection on the target machine.

However, information-stealing malware could quickly check if KeePass exists on a computer or is running, and if so, dump the program's memory and send it and the KeePass database back to the attacker for offline retrieval of the cleartext password from the memory dump.

BleepingComputer tested vdohney's 'keepass-password-dumper' tool by installing KeePass on a test device and creating a new database with the master password 'password123,' as shown below.



	Create Master Key				×	
KeePass	Create N C:\Users\c	laster Key us\Documents\Da	atabase.kdbx			X
File Gro	Specify a new master key	which will be used to	encrypt the database			
: L O — ma	A master key consists of or be required to open the da anymore.	ne or more of the fo tabase. If you lose of	llowing components. A one component, you wi	Il components that yo Il not be able to oper	ou specify will 1 the database	
	Master password:	password123			•••	
	Repeat password:					
	Estimated quality:		17 bits		11 ch.	
	Show expert options:					
						/
						/
-						
0 of 0 select						
	Help			ОК	Cancel	

Creating a test KeePass database

Source: BleepingComputer

We then locked our KeePass workspace, which prevents access to it unless you enter the master password again.

In our tests, you can use Process Explorer to dump the memory of the KeePass project, but it requires a full memory dump, and not a minidump, to work correctly. No elevated privileges are needed to dump the processes' memory.

After compiling vdohney's tool using Visual Studio, we executed it against our memory dump, and it quickly recovered most of our cleartext password, with just the first two letters missing.





Extracting most of the KeePass master password

Source: BleepingComputer

While this is not the complete password, determining what characters are missing would be fairly easy.

The researcher also warns that master passwords used in the past can remain in memory, so they can be retrieved even if KeePass is no longer running on the breached computer.

Fix coming soon

The developer of KeePass, Dominik Reichl, received the bug report and promised to roll out a fix for CVE-2023-32784 on version 2.54, expected sometime in July 2023.

However, Reichl told BleepingComputer that KeePass version 2.54 is more likely to be released to users in about two weeks, so it should be out by early June.

Based on a discussion where Reichl developed his thoughts on the security flaw and the potential mitigation strategies, two security enhancements are mentioned for the upcoming KeePass version:

- Perform direct API calls for getting/setting the text of the text box, avoiding the creation of managed strings in memory that can leak secrets.
- Create dummy fragments containing random characters in the process memory that will have approximately the same length as the user's master password, obfuscating the real key.

KeePass 2.54 for Windows will have both, while macOS and Linux versions will only get the second enhancement.

The developer has released a test version with the new security enhancements that mitigate the issue, so those who can accept unstable behavior can source it from here.



The creator of the PoC has confirmed that he can no longer reproduce the attack with the two security enhancements in place, so the fix appears to be effective.

Even after the new version is released, the master password may still be stored in memory files. The researcher warns that to be 100% safe that it is not lurking on the system, you would need to delete your system's swap and hibernation files, format your hard drive using the "overwrite data" mode to prevent data recovery, and do a fresh OS install.

For most, though, restarting the computer, clearing your swap file and hibernation files, and not using KeePass until the new version is released are reasonable safety measures for the time being.

Even then, for the best protection, be super vigilant about not downloading programs from untrusted sites and beware of phishing attacks that may infect your devices, giving threat actors remote access to your device and your KeePass database.

Source: <u>https://www.bleepingcomputer.com/news/security/keepass-exploit-helps-retrieve-</u> <u>cleartext-master-password-fix-coming-soon/</u>

12. Android phones are vulnerable to fingerprint bruteforce attacks

Researchers at Tencent Labs and Zhejiang University have presented a new attack called 'BrutePrint,' which brute-forces fingerprints on modern smartphones to bypass user authentication and take control of the device.

Brute-force attacks rely on many trial-and-error attempts to crack a code, key, or password and gain unauthorized access to accounts, systems, or networks.

The Chinese researchers managed to overcome existing safeguards on smartphones, like attempt limits and liveness detection that protect against brute-force attacks, by exploiting what they claim are two zero-day vulnerabilities, namely Cancel-After-Match-Fail (CAMF) and Match-After-Lock (MAL).

The authors of the technical paper published on Arxiv.org also found that biometric data on the fingerprint sensors' Serial Peripheral Interface (SPI) were inadequately protected, allowing for a man-in-the-middle (MITM) attack to hijack fingerprint images.

BrutePrint and SPI MITM attacks were tested against ten popular smartphone models, achieving unlimited attempts on all Android and HarmonyOS (Huawei) devices and ten additional attempts on iOS devices.





BrutePrint attack diagram (arxiv.org)

How BrutePrint works

The idea of BrutePrint is to perform an unlimited number of fingerprint image submissions to the target device until the user-defined fingerprint is matched.

The attacker needs physical access to the target device to launch a BrutePrint attack, access to a fingerprint database that can be acquired from academic datasets or biometric data leaks, and the necessary equipment, costing around \$15.



Equipment required for launching BrutePrint (arxiv.org)

Contrary to how password cracking works, fingerprint matches use a reference threshold instead of a specific value, so attackers may manipulate the False Acceptance Rate (FAR) to increase the acceptance threshold and create matches more easily.

BrutePrint stands in between the fingerprint sensor and the Trusted Execution Environment (TEE) and exploits the CAMF flaw to manipulate the multi-sampling and error-canceling mechanisms of fingerprint authentication on smartphones.



CAMF injects a checksum error in the fingerprint data to stop the authentication process at a pre-mature point. This allows the attackers to try out fingerprints on the target device while its protection systems won't register failed attempts, hence giving them infinite tries.



CAMF vulnerability attack logic (arxiv.org)

The MAL flaw enables the attackers to infer authentication results of the fingerprint images they try on the target device, even if the latter is in "lockout mode."



Keyguard exception introduced by device vendors causing MAL (arxiv.org)

The lockout mode is a protection system activated after a certain number of failed consecutive unlock attempts. During the lockout "timeout," the device shouldn't accept unlocking attempts, but MAL helps bypass this restriction.

The final component of the BrutePrint attack is using a "neural style transfer" system to transform all fingerprint images in the database to look like the target device's sensor scanned them. This makes the images appear valid and thus have better chances of success.



Source		-unify	$\rightarrow D_X$	
Target		- refine		
	A			
(a) C	Capacitive	(b) Optical	(c) Ultra-thin	(d) Ultrasonic

Refining the images (top) based on the sensor type (bottom) (arxiv.org)

Tests on devices

The researchers conducted experiments on ten Android and iOS devices and found that all were vulnerable to at least one flaw.

Device				Sensor		Attempt Limit		
Manuf./Model	OS/Ver.	TEE	r_{max}	Manuf.	Туре	ScreenLock ¹	Payment ²	Privacy ³
Xiaomi Mi 11 Ultra	Android 11	QTEE	5	Goodix	Optical (ultra-thin)*	5×4	5×4	5
Vivo X60 Pro	Android 11	Kinibi	5	Goodix	Optical*	5	∞	5
OnePlus 7 Pro	Android 11	QTEE	5	Goodix	Optical*	5	5	5
OPPO Reno Ace	Android 10	OTEE	5	Goodix	Optical*	5×4	5×4	5×4
Samsung Galaxy S10+	Android 9	Knox	4	Qualcomm	Ultrasonic*	5×10	5	5×10
OnePlus 5T	Android 8	QTEE	5	Goodix	Capacitive	5×4	5×4	5×4
Huawei Mate30 Pro 5G	HarmonyOS 2	TrustedCore	5	Goodix	Optical*	5×4	$5 \times \infty$	5×∞
Huawei P40	HarmonyOS 2	TrustedCore	5	Novatek	Optical*	5×4	$5 \times \infty$	$5 \times \infty$
Apple iPhone SE	iOS 14.5.1	Secure Enclave	5	AuthenTec	Capacitive	5	5	5
Apple iPhone 7	iOS 14.4.1	Secure Enclave	5	AuthenTec	Capacitive	5	5	5

Details of tested devices (arxiv.org)

The tested Android devices allow infinite fingerprint tryouts, so brute-forcing the user's fingerprint and unlocking the device is practically possible given enough time.

On iOS, though, the authentication security is much more robust, effectively preventing bruteforcing attacks.

	Attributes					Attacks			
	Samples	Cancel	Hot-Plug	Decode	f _{SPI} (MHz)	Vulnerability	Bypassing	Hijacking	Brute-force
Xiaomi Mi 11 Ultra	2	~	~	~	32	CAMF, MAL	(∞,∞,∞)	~	(1.1.1)
Vivo X60 Pro	3	V	~	~	25	CAMF, MAL	(∞,∞,∞)	~	(V.V.V)
OnePlus 7 Pro	4	V	~	~	25	CAMF	(∞,∞,∞)	~	$(\mathbf{V},\mathbf{V},\mathbf{V})$
OPPO Reno Ace	3	V	~	V	25	CAMF	(∞,∞,∞)	~	$(\mathbf{V},\mathbf{V},\mathbf{V})$
Samsung Galaxy S10+	2~4*	V	~	V	24	CAMF	(∞,∞,∞)	~	(V.V.V)
OnePlus 5T	2	~	~	~	4.8	CAMF	(∞,∞,∞)	~	(1,1,1)
HUAWEI Mate30 Pro 5G	2	N/A [†]	~	~	23	MAL	(∞,∞,∞)	~	(1.1.1)
HUAWEI P40	2	N/A [†]	~	~	23	MAL	(∞,∞,∞)	~	(V, V, V)
Apple iPhone SE	3	~	~	×	7.7	CAMF	(15,15,15)	×	(X , X , X)
Apple iPhone 7	3	~	~	×	7.7	CAMF	(15,15,15)	×	$(\mathbf{X}, \mathbf{X}, \mathbf{X})$

Test results table (arxiv.org)



Although the researchers found that iPhone SE and iPhone 7 are vulnerable to CAMF, they could only increase the fingerprint tryout count to 15, which isn't enough to brute-force the owner's fingerprint.

Regarding the SPI MITM attack that involves hijacking the user's fingerprint image, all tested Android devices are vulnerable to it, while iPhones are again resistant.

The researchers explain that the iPhone encrypts fingerprint data on the SPI, so any interception has little value in the context of the attack.

In summary, the conducted experiments showed that the time it takes to complete BrutePrint against vulnerable devices successfully ranges between 2.9 and 13.9 hours when the user has enrolled one fingerprint.

When multiple fingerprints are enrolled on the target device, the brute-forcing time drops to just 0.66 to 2.78 hours as the likelihood of producing matching images increases exponentially.



Time to brute-force the fingerprint (arxiv.org)

Conclusion

At first glance, BrutePrint may not seem like a formidable attack due to requiring prolonged access to the target device. However, this perceived limitation should not undermine its value for thieves and law enforcement.

The former would allow criminals to unlock stolen devices and extract valuable private data freely.

The latter scenario raises questions about privacy rights and the ethics of using such techniques to bypass device security during investigations.

This constitutes a rights violation in certain jurisdictions and could undermine the safety of certain people living in oppressive countries.



Source: <u>https://www.bleepingcomputer.com/news/security/android-phones-are-vulnerable-to-</u> <u>fingerprint-brute-force-attacks/</u>

13. Mobile Spyware—How You Can Keep Stalkers Off Your Phone

When you wind up with mobile spyware, you may wind up with a stalker on your phone.

In its most malicious forms, mobile spyware can steal information like text messages and photos, capture passwords as you tap them in, secretly turn on your microphone or camera for recording, and track your movements using GPS.

Figuratively speaking, it's like going about your day with a stalker peering over your shoulder.

If that doesn't sound creepy enough, it can get worse. More than just providing attackers with a live feed of your activity, spyware can record and archive your actions. From there, it can "phone home," meaning it sends stolen information back to cybercriminals so they can hoard it for later use.

That stolen information can lead to identity fraud and theft, such as when a cybercriminal raids your existing bank accounts, sets up entirely new lines of credit in your name, or impersonates you in several other ways. In darker scenarios, stolen photos, files, and information can lead to blackmail and harassment.

Without question, a case of mobile spyware can get serious quite quickly. Yet, it is highly preventable when you know how it can end up on your phone—and the steps you can take to keep that from happening.

How do phones get mobile spyware?

Malicious apps. They account for much of mobile spyware today.

Whether they're downloaded from a third-party app store or even from Google Play or Apple's App Store, the ruse remains the same: a malicious app poses as legitimate app. These apps may present themselves as games, wallpapers, productivity apps, exercise apps, utility apps, and even security apps. Instead, they're loaded with spyware.

Google Play does its part to keep its virtual shelves free of malware-laden apps with a thorough submission process as reported by Google and through its App Defense Alliance that shares intelligence across a network of partners, of which we're a proud member. Further, users also have the option of running Play Protect to check apps for safety before they're downloaded.

Apple's App Store has its own rigorous submission process for submitting apps. Likewise, Apple deletes hundreds of thousands of malicious apps from its store each year.



Yet, bad actors find ways to sneak malware into the store. Sometimes they upload an app that's initially innocent and then push malware to users as part of an update. Other times, they'll embed malicious code such that it only triggers once it's run in certain countries. They will also encrypt malicious code in the app that they submit, which can make it difficult for reviewers to sniff out.

Unique to Android phones, Android gives people the option to download apps from thirdparty app stores. These stores may or may not have a thorough app submission process in place. As a result, they can be far less secure than Google Play. Moreover, some third-party app stores are fronts for organized cybercrime gangs, built specifically to distribute malware, making third-party download that much riskier.

Other ways spyware can end up on your phone

Someone can install it directly.

In this case, a bad actor needs physical access to your phone. If they know the passcode or if the phone is unlocked, they can tamper with the phone's settings and install the spyware themselves. This requires access, time, and effort, yet some bad actors certainly take this approach.

Surprisingly, we've also seen cases where malware comes pre-installed on phones. A recent case estimated that some 9 million smartphones had spyware installed in them somewhere along the supply chain. Reportedly, the spyware could steal personal information from the phone or possibly take it over entirely for a short stretch of time.

You can spot signs of tampering on an Android phone by heading to Settings and searching for "Install Unknown Apps." If you see any sources that you didn't set to the "On" position or a third-party website you don't recognize, it indicates that apps from outside official app stores could have been installed in the device. Such apps are generally riskier than apps from official sources like Google Play. While not an outright indication of spyware, you should set those to "Off."

On an iPhone, directly installing spyware takes a bit more effort. Typically, it requires "jailbreaking" the phone. This process tampers with the operating system and removes software restrictions so the iPhone can access third-party app stores and download unapproved apps. Both are highly risky activities and the reason why Apple's iOS enforces such restrictions in the first place.

Put plainly, "jailbreaking" is not safe.

In the hands of bad actors, they can install an app called "Cydia" on a jailbroken iPhone. Cydia is an unapproved app store that offers potentially dangerous modifications and apps. If you spot Cydia on your iPhone, it's certain sign of tampering.



The signs of mobile spyware

Not long ago, you could often see or even feel if your smartphone was infected with spyware. It could run hot, like it was left out on blanket at the beach, because the spyware ate up computing cycles while it ran in the background. It could drain batteries or lead to sluggish performance. That's not always the case anymore. Spyware has become leaner and more efficient in recent years, so cybercriminals can better mask their attacks.

Some signs that are better indicators of spyware include:

Spikes in data use.

Whether through your phone's data connection or through a Wi-Fi connection, unexpected increases in usage could be a sign that your phone is communicating with a third party.

Difficulty logging into your accounts the first time.

A phone infected with spyware may communicate your activity to a third party, rather than to the legitimate login. The legitimate site or service never receives the first login attempt, forcing you to log in again.

Difficulty logging into your accounts at all.

This may be a sign that a cybercriminal already hacked your password, logged in under your name, and then changed the password to one of their own. (Note that this could also be a sign of a compromised or stolen password and not necessarily a sign of spyware.)

Other apps like antivirus and online protection software get shut down.

Some types of spyware can gain administration-level privileges to your phone and drop its defenses, leaving you yet more vulnerable.

You spot signs of fraud or theft.

Above we mentioned how cybercriminals use spyware to gain login credentials to banks and credit cards, and even steal personal items like files and photos. If you spot any unusual activity or find yourself threatened with demands, it's possible that spyware could be a possible cause among others.

Seven steps to protect yourself from mobile spyware

1. Update your phone's operating system.

Security Bulletin, June 2023



Along with installing security software, keeping your phone's operating system up to date can greatly improve your security. Updates can fix vulnerabilities that hackers rely on to pull off their malware-based attacks. It's another tried and true method of keeping yourself safe—and for keeping your phone running great too.

2. Avoid third-party app stores.

As mentioned above, Google Play has measures in place to review and vet apps to help ensure that they are safe and secure. Third-party sites may very well not, and they may intentionally host malicious apps as part of a front. Further, Google is quick to remove malicious apps from their store once discovered, making shopping there safer still.

3. Review apps carefully.

Check out the developer—have they published several other apps with many downloads and good reviews? A legit app typically has quite a few reviews, whereas malicious apps may have only a handful of (phony) five-star reviews. Lastly, look for typos and poor grammar in both the app description and screenshots. They could be a sign that a hacker slapped the app together and quickly deployed it.

4. Go with a strong recommendation.

Yet better than combing through user reviews yourself is getting a recommendation from a trusted source, like a well-known publication or from app store editors themselves. In this case, much of the vetting work has been done for you by an established reviewer. A quick online search like "best fitness apps" or "best apps for travelers" should turn up articles from legitimate sites that can suggest good options and describe them in detail before you download.

5. Keep an eye on app permissions.

Another way hackers weasel their way into your device is by getting permissions to access things like your location, contacts, and photos—and they'll use malicious apps to do it. If an app asks for way more than you bargained for, like a simple puzzle game that requests access to your camera or microphone, it might be a scam. On Android, recent spyware usually requests REQUEST_IGNORE_BATTERY_OPTIMIZATIONS permission to execute the malicious behavior in the background. If you see behaviors like these, delete the app.

6. Tidy up.

Remove old, unused, and underused applications that could be future vectors of attacks.

Along this line, we've seen where mobile applications change ownership (whether they get sold or others take over its operations), and the new owners don't have the same standard operating procedures as the founders.

7. Lock your phone—and keep an eye on it too.



As mentioned above, some bad actors will install spyware on phones themselves. However, this requires access, time, and effort to pull off. Locking your phone and always keeping it close can help prevent bad actors from infecting your phone this way.

8. Protect your phone.

Comprehensive online protection software can secure your phone in the same ways that it secures your laptops and computers. Installing it can protect your privacy, keep you safe from attacks on public Wi-Fi, and automatically block unsafe websites and links, just to name a few things it can do.

Source: <u>https://www.mcafee.com/blogs/mobile-security/mobile-spyware-how-you-can-keep-stalkers-off-your-phone/</u>

14. Why Are Some Countries Banning TikTok?

Waiting in the checkout line. Waiting to fall asleep. Waiting for your boring work call to finally end.

When you find yourself in these situations, do you usually have your phone in hand? And does it usually include scrolling through videos on TikTok? You're far from alone! The app has 150 million users in the United States and more than a billion daily users worldwide.1

However, governments around the world believe that while you're exploring the world through short-form video, unscrupulous characters are lurking in the background collecting your personal data. Here's the real story behind TikTok bans and what they mean for you and your online privacy.

Why Is TikTok Banned?

TikTok is owned by ByteDance, a Chinese company. Much of the data privacy unease surrounding TikTok is ByteDance's opacity in their data mining practices. It's unknown how much data it collects on users and what it does with that information. Since the Chinese government has a hand in many of the businesses based in the country, it's unclear if the government is party to the mined data. Because many countries are tense politically with China, some governments are being cautious about limiting ByteDance's access to personal information and potentially government secrets.

So far, various countries have banned TikTok from the work phones of government employees, including the United States, Australia, Canada, Taiwan, and various European Union members.2 India completely banned the app in the country in 2020. Various other countries with strict limits on self-expression have also attempted to forbid their citizens from accessing TikTok.



Montana became the first state to ban TikTok in May 2023. The governor cited "protecting Montanans' personal and private data" as the reason behind the new bill, which is set to go into effect in January 2024.3

What Do the Bans Mean for You?

For the general population, bans of TikTok on government-issued devices will not affect your access to the platform Even for government employees, this just means that you can't access the app from your work phone, laptop, or tablet. On your own time and your personal devices, you can still scroll to your heart's content.

Montana's TikTok bill could pick up steam with other states claiming to protect the PII of their citizens; however, the Montana law and any similar ones that may arise are likely to be scrutinized as a violation of freedom of speech. As of now, it's unclear whether the bill – and future ones like it – will be invalidated due to a violation of the First Amendment.

How these TikTok bans and the news headlines may affect you is that they emphasize the necessity of social media best practices and guarding your personally identifiable information (PII) more closely.

How to Maintain Your Privacy on TikTok

Because it's unclear how much and with whom TikTok is gathering and sharing your data, it's best to play it safe and limit the amount you reveal about yourself on the app. Here are a few tips to give you peace of mind and improve your online privacy:

1. Turn off geo-tagging.

This is a good practice on any social media platform. Geo-tagging is a function where the app uses GPS to track your location and then publish it alongside your post. This feature may put your personal safety at risk, since stalkers can use the geotag, context clues, and video background to guess at your location.

2. Disable tracking and targeted ads.

TikTok, Facebook, Instagram, and gaming apps depend on advertisers' dollars to make money. To provide users with the most relevant ads (and improve their chances of making a sale), companies gather information about you and build a profile based on your online comings and goings. Most apps that allow tracking must ask your permission first to do so. Always uncheck this box and disable ad tracking, because there's no guarantee that the PII the ad company collects will stay a secret. Did you know that 98% of people have their personal information up for sale on the internet? Personal Data Cleanup is an excellent tool to erase your private details from the internet and keep it out of the hands of strangers.

3. Keep your life a mystery.


Oversharing on social media may leave you vulnerable to social engineering schemes. This happens when a scammer gathers details about you and then tailor-makes a scam that's likely to get your attention. For example, if your social media profiles make it clear that you're an animal lover, a scammer may write a heartfelt post about needing donations to save their beloved pet.

4. Use a VPN.

A virtual private network (VPN) scrambles your online traffic, making it very difficult for someone to digitally eavesdrop on you or pinpoint your location. Plus, a VPN works on any device, not just desktops. So, while you scroll on a computer, tablet, or smartphone, a VPN can keep your internet traffic a secret.

Enjoy TikTok Safely

Don't worry: TikTok – the constant companion in times of boredom, transit, and when you're in need of a laugh – isn't going anywhere anytime soon. For the general population in most parts of the world, the app is staying put.

However, just because it's not banned doesn't mean that it's 100% safe for your online privacy. Keep our tips in mind the next time you scroll through or post. To fully cover your bases and give you peace of mind, partner with McAfee+ Ultimate. This all-in-one service includes unlimited VPN for all your devices, Personal Data Cleanup, and more.

Laugh, cry, learn, and explore the world through TikTok with confidence in the security of your online privacy!

1TikTok, "Celebrating our thriving community of 150 million Americans"

2Associated Press, "Here are the countries that have bans on TikTok"

3CNN, "Montana governor bans TikTok"

Source: <u>https://www.mcafee.com/blogs/privacy-identity-protection/why-are-some-countries-banning-tiktok/</u>

15. How I Got Started: White Hat Hacker

White hat hackers serve as a crucial line of cyber defense, working to identify and mitigate potential threats before malicious actors can exploit them. These ethical hackers harness their skills to assess the security of networks and systems, ultimately helping organizations bolster their digital defenses. But what drives someone to pursue a career as a white hat hacker, and how do you get started in leveraging so-called "evil" skills for the greater good??

In this exclusive Q&A, we spoke with seasoned white hat hacker Gilit Saporta, Director of Analytics for DoubleVerify's Fraud Lab. Gilit has helped out with and stopped some of the



world's sneakiest ad fraudsters across streaming, the open web, mobile, etc. Before her role as Director of Analytics at DV, she worked at Simplex as a Fraud Fighting Team Leader and Head of Fraud Intelligence. Prior to that, Gilit was Head of Training for Forter, and for nearly seven years, led analytics and risk science initiatives at PayPal.

Did you go to college? What did you go to school for?

As an adopted daughter to parents who immigrated to Israel a few years after World War II, I was honored to be the first person in my extended family to attend university in Israel. I graduated from Tel Aviv University, where I majored in Theatre Arts (BA summa cum laude, valedictorian and MFA summa cum laude). I was lucky enough to be able to pursue my passion for art in parallel to my work in tech for a couple of years and even had a few of my plays produced in fringe theaters in Tel Aviv.

What was your first role in tech?

Going way back, as a teenager I had a summer vacation job for a telephone company, where I physically maintained analog phone line routing systems back in the 1990s.

But to be a bit more focused on high-tech, as an IDF military intelligence officer, I started to learn code and build logic for innovative defense products at the age of 18. This experience probably landed me my first "real" role in tech: a student position at the age of 21 catching early attacks on e-commerce sites for a startup called FraudSciences, that was later acquired by PayPal. I was looking for an interesting part-time job I could do to help fund my university studies, and in a way, I almost fell into it. Today, I love hearing my kids tell people that their mom has been "catching bad people online for over 20 years."

What is the most valuable skill you learned in your role?

Keeping an open mind and a curious mindset was and remains the core of my skill set. Through my first roles, I learned that being curious about the endless research options of the data around you will allow you to work with the most intelligent — and fun — people. Plus, you'll get the rush of feeling that there's always another hill to climb.

I've always loved solving puzzles, so learning that the passion for digging into data quirks is in itself a skill was a huge revelation for me.

What soft skills do you think make a person successful in tech, fraud protection and cybersecurity?

Stay humble, knowing that there's lots to learn from newcomers with a fresh perspective. This is a soft skill that all researchers should possess, especially when it comes to growing into leadership roles. I see that by continuously encouraging others to express even their "hunch"



about potential theories is a strong asset for the team's creativity and that great discoveries are made thanks to this culture.

Any parting thoughts or final piece of advice to someone looking into your type of role?

These days, there are ample learning opportunities and reading materials available about any flavor of cybersecurity and fraud protection products. I recommend not only reading samples of this ocean of information but also interacting with the community of fraud fighters whenever possible — conferences, meetups, professional social media and beyond. Contribute your own thoughts and questions to the community, hypothesize about scams and schemes that you would imagine are happening, get some feedback and gradually become a master of storytelling — since the story of the attack is often just as important as the quantitative analysis.

Source: <u>https://securityintelligence.com/articles/how-i-got-started-white-hat-hacker/</u>

16. Three Reasons You Need a VPN

You know what a VPN is, but the question remains—why do you need a VPN?

There's one good reason. Your privacy. Because it's a commodity on today's internet.

For starters, you have advertisers and internet service providers (ISPs) that want to know what you're doing, when you're doing it, where you're doing it, and even for how long you're doing it. They gather and use this information to create targeted ad profiles. And sometimes, they sell that information to third parties.

Next, there are the hackers and identity thieves out there. They take an even greater interest in what you're doing online—like your shopping, banking, and finances. Even your insurance and medical matters. Primarily they want that information so they can turn a buck by hijacking your accounts or impersonating you to get medical care. In more extreme cases, they might use stolen information to impersonate you in other ways. That might include opening entirely new lines of credit or getting a driver's license in your name.

A VPN can prevent this kind of snooping from happening.

VPNs and privacy—blocking ads and data collection

As for data collection and ads, that activity should come as no surprise. Particularly for anyone who's seen uncannily targeted ads follow them around on the internet. Search for "summer cargo pants" one time and suddenly the sites you visit are full of ads for pants, pants, and more pants.

Aside from gathering your online activity for advertising purposes, ISPs might also sell the data they gather to third parties. They can gather that data while you're on your home network, and



they might gather it while you're using public Wi-Fi. (Some ISPs provide free Wi-Fi in public places that allows them to collect data from people who aren't their regular customers.)

This practice varies by region and the data privacy laws that are in place in each one.

For example, the European Union has strict data privacy laws that prevent this type of sale. (Thanks to the enactment of the GDPR, General Data Protection Regulation.) However, there are few such protections in the U.S. There, an ISP can sell the browsing history of an internet user to a third party—provided the data has been anonymized.

"Anonymized" is a key term here. It refers to the process of stripping away personal identifiers that connect a person to a set of stored data. It might also include adding "noise" to the data, which obscures personal identifiers. For example, that might remove an exact birthdate and replace it with a broad range of dates. So, "March 31, 1957" becomes "January – June 1957."

At issue is that this anonymized data can get de-anonymized rather easily.

Researchers in 2019 found that "99.98% of Americans would be correctly re-identified in any dataset using 15 demographic attributes." And when you consider how much data is collected about you, 15 attributes are only drops in the ocean.

Marketing and analytics companies collect hundreds and hundreds of data points on people and their households. That might include information about their mortgage, if they are allergy sufferers, whether they own cats or dogs, where they do most of their grocery shopping, and more—in addition to other information like their age and address.

What happens when that information gets breached, or published accidentally, as it did when 123 million records of U.S. households were made public back in 2017? It gives bad actors plenty of data that can potentially harm others.

Internet browsing activity doesn't account for all the data points that these companies collect. However, the thought of your ISP tracking your time online and selling it to others might leave you feeling uncomfortable. Whether that data gets anonymized or not.

VPNs, privacy, and identity theft

The other threat to your privacy online comes from bad actors—like hackers and identity thieves. By targeting insecure networks, lurking on unsecured public Wi-Fi, or setting up phony public Wi-Fi hotspots themselves, they'll snoop on the people using it.

On insecure networks, bad actors can watch as you log into your bank account, read your email, and see what you're doing on the internet in general. They can steal any passwords and logins you're using along the way, giving them access to those accounts.

In truth, this kind of snooping is more than a threat to your privacy. It enters the realm of identity theft, making the risk to your data and personal information that much greater.



Three reasons to use a VPN

With your privacy and personal identity in mind, here are three specific examples that make the case for using a VPN:

1. You value your privacy.

As outlined above, the internet has increasingly become less private. Advertisers and ISPs will track you when and where they can. When you use a VPN, you can hide several things from your ISP, like the websites and apps you use, the time spent on them, your search history, and downloads. As for websites and apps, a VPN can hide your IP address and your location, all of which can thwart ad tracking on those sites and apps.

2. You work remotely.

Many larger businesses and organizations offer (and sometimes require) a VPN for their employees who work outside the office. Smaller businesses use them less so, which makes them subject to attacks like data breaches. According to FBI reports, the average cost of a data breach for a business in 2022 was well over \$150,000. Moreover, cybercriminals increasingly wage these attacks against businesses with revenues of \$500,000 or less, which makes the thought of a six-figure loss even more devastating.

A VPN encrypts and protects company data in transit, whether you're connecting from home, the airport, or anywhere outside the office. Using one protects you and the business or organization you work for.

3. You want extra protection while you bank, shop, or handle any sensitive matters online.

A strong VPN service like ours uses bank-grade encryption to keep your data and information secure. With a VPN, a snoop bad actor would only see garbled content thanks to your VPN's encryption functionality.

Another popular reason for a VPN—streaming shows and content

If you're traveling, you can access the sites and services you typically use at home. For example, some video streaming services aren't available in foreign locations. By using a VPN, you can still access content by connecting through the proxy servers that VPNs use. These are servers in other locations that can make requests on your behalf. So, even if you are out of the country, you can connect to a proxy server in the U.S. and access your services as usual.

Where can I get a VPN?

If you have online protection with us, like our McAfee+ plans, you have a VPN ready to go. If not, McAfee+ offers a great way to get one.



It's completely private and independently audited to ensure your sensitive info stays secure. We don't log or track what you do online, so your online activity remains private.

By design, we made it simple to use. You can set it to automatically turn on if you're on an unprotected network. Or you can also choose to keep it on all the time for an even safer online experience. With nearly 50 server locations worldwide, you can get a fast and stable VPN connection wherever you go.

And because it comes with our online protection software, you get other identity, privacy, and device security features that can keep you even safer online.

Bottom line, a VPN makes you more private and secure.

And that kind of protection is called for nowadays. Ad trackers, data collectors, hackers, and thieves—they all want to know what you're doing online. And with a VPN, you can keep all that to yourself, making your time online more private and secure than before.

Source: <u>https://www.mcafee.com/blogs/privacy-identity-protection/three-reasons-you-need-a-vpn/</u>

17. Brute-Forcing a Fingerprint Reader

It's neither hard nor expensive:

Unlike password authentication, which requires a direct match between what is inputted and what's stored in a database, fingerprint authentication determines a match using a reference threshold. As a result, a successful fingerprint brute-force attack requires only that an inputted image provides an acceptable approximation of an image in the fingerprint database. BrutePrint manipulates the false acceptance rate (FAR) to increase the threshold so fewer approximate images are accepted.

BrutePrint acts as an adversary in the middle between the fingerprint sensor and the trusted execution environment and exploits vulnerabilities that allow for unlimited guesses.

In a BrutePrint attack, the adversary removes the back cover of the device and attaches the \$15 circuit board that has the fingerprint database loaded in the flash storage. The adversary then must convert the database into a fingerprint dictionary that's formatted to work with the specific sensor used by the targeted phone. The process uses a neural-style transfer when converting the database into the usable dictionary. This process increases the chances of a match.

With the fingerprint dictionary in place, the adversary device is now in a position to input each entry into the targeted phone. Normally, a protection known as attempt limiting effectively locks a phone after a set number of failed login attempts are reached. BrutePrint can fully bypass this limit in the eight tested Android models, meaning the adversary device can try an



infinite number of guesses. (On the two iPhones, the attack can expand the number of guesses to 15, three times higher than the five permitted.)

The bypasses result from exploiting what the researchers said are two zero-day vulnerabilities in the smartphone fingerprint authentication framework of virtually all smartphones. The vulnerabilities—-one known as CAMF (cancel-after-match fail) and the other MAL (matchafter-lock)—result from logic bugs in the authentication framework. CAMF exploits invalidate the checksum of transmitted fingerprint data, and MAL exploits infer matching results through side-channel attacks.

Depending on the model, the attack takes between 40 minutes and 14 hours.

Also:

The ability of BrutePrint to successfully hijack fingerprints stored on Android devices but not iPhones is the result of one simple design difference: iOS encrypts the data, and Android does not.

Source: <u>https://www.schneier.com/blog/archives/2023/05/brute-forcing-a-fingerprint-</u> <u>reader.html</u>

18. Android apps with spyware installed 421 million times from Google Play

A new Android malware distributed as an advertisement SDK has been discovered in multiple apps, many previously on Google Play and collectively downloaded over 400 million times.

Security researchers at Dr. Web discovered the spyware module and tracked it as 'SpinOk,' warning that it can steal private data stored on users' devices and send it to a remote server.

The antivirus company says SpinkOk demonstrates a seemingly legitimate behavior, using minigames that lead to "daily rewards" to spark user interest.

"On the surface, the SpinOk module is designed to maintain users' interest in apps with the help of mini games, a system of tasks, and alleged prizes and reward drawings," explains Doctor Web's report.

In the background, though, the trojan SDK checks the Android device's sensor data (gyroscope, magnetometer) to confirm that it's not running in a sandboxed environment, commonly used by researchers when analyzing potentially malicious Android apps.

The app then connects to a remote server to download a list of URLs opened used to display expected minigames.





Mini-games displayed by SDK

Source: Dr.Web

While the minigames are displayed to the apps' users as expected, Dr. Web says that in the background, the SDK is capable of additional malicious functionality, including listing files in directories, searching for particular files, uploading files from the device, or copying and replacing clipboard contents.

The file exfiltration functionality is particularly concerning as it could expose private images, videos, and documents.

In addition, the clipboard modification functionality code allows the SDK's operators to steal account passwords and credit card data, or hijack cryptocurrency payments to their own crypto wallet addresses.

Dr. Web claims this SDK was found in 101 apps that were downloaded for a cumulative total of 421,290,300 times from Google Play, with the most downloaded listed below:

- Noizz: video editor with music (100,000,000 downloads)
- Zapya File Transfer, Share (100,000,000 downloads; Dr. Web says the trojan module was present in version 6.3.3 to version 6.4 and is no longer present in current version 6.4.1)
- VFly: video editor&video maker (50,000,000 downloads)
- MVBit MV video status maker (50,000,000 downloads)
- Biugo video maker&video editor (50,000,000 downloads)
- Crazy Drop (10,000,000 downloads)
- Cashzine Earn money reward (10,000,000 downloads)
- Fizzo Novel Reading Offline (10,000,000 downloads)



- CashEM: Get Rewards (5,000,000 downloads)
- Tick: watch to earn (5,000,000 downloads)

All but one of the above apps have been removed from Google Play, indicating that Google received reports about the malicious SDK and removed the offending apps until the developers submitted a clean version.

A complete list of the apps reportedly using the SDK can be found on Dr. Web's site.

It is unclear if the publishers of the trojanized apps were deceived by the SDK's distributor or knowingly included it in their code, but these infections commonly result from a supply-chain attack from a third party.

If you use any of the apps listed above, you should update to the latest version available via Google Play, which should be clean.

If the app isn't available on Android's official app store, it is recommended to uninstall them immediately and scan your device with a mobile antivirus tool to ensure that any spyware leftovers are removed.

BleepingComputer has reached out to Google for a statement on this massive infection base, but a comment wasn't available by publication time.

Source: <u>https://www.bleepingcomputer.com/news/security/android-apps-with-spyware-installed-421-million-times-from-google-play/</u>

19. What is the Dark Web? The Answer Can Help You Stay Safer Online.

The dark web. The name raises all kinds of questions. What is the dark web, really? Where is it? Can anyone hop on it?

Answering these questions can help you stay safer online.

The story of the dark web is a complicated one. It's a small and highly anonymous layer of the internet. As a result, it has a reputation for harboring criminal activity. We often mention the dark web in our blogs, typically when the conversation turns to identity theft, data breaches, and stolen personal information. Rightfully so. Plenty of cybercrime can get traced right back to the dark web.

Yet cybercriminals didn't create the dark web. And they're far from the only people who use it. News outlets like the BBC and the New York Times have a presence there, as does the U.S. Central Intelligence Agency (CIA). Journalists, activists, and everyday citizens use it as well, often to work around oppressive censorship. Even Facebook is there, providing people access to the social media site in regions where it's blocked.



Anonymity reigns on the dark web. It was designed to work that way. With that, it's home to a mixed bag of activity, legitimate and illicit alike. Yet that anonymity doesn't stop us from putting a face onto the dark web—from understanding what it is, where it is, and what transpires there.

That starts with a look at the internet and the two primary layers that make it up.

The layers of the internet: The surface web and the deep web

If you visualize the internet as an ocean, you'll find it populated with websites and collections of data at all depths. Yet, the typical internet user only has access to the first few feet, a layer of the internet known as the surface web.

The sights you'll see within the surface web will look familiar. It's all the blogs, shops, social media sites, and so on that you visit regularly. And it's easy to get to. You only need to fire up your browser and go. All the sites are public facing. With a quick search, you can find them.

In all, the surface web contains any destination you can reach through search. To put it more precisely, the surface web accounts for areas of the internet that search engines can "crawl" and index for search. Estimates vary, yet the surface web accounts for roughly 4 to 5% of the internet.

Now, enter the deep web, the next 95% of the internet that is not searchable. Yet, that's not to say that you don't travel down into its depths from time to time. In fact, you likely do it daily. Any time you go through a paywall or use a password to access internet content, you're entering the deep web. The content found there is hidden from search. Examples include logging into your bank account, accessing medical records through your healthcare provider, or using corporate web pages as part of your workday. Even streaming a show can involve a trip to the deep web. None of that content is searchable.

As such, the overwhelming majority of activity within the deep web is legitimate. So while this layer of the internet runs deep, it isn't necessarily dark. The dark web is something altogether different.

What is the dark web?

The dark web lives within the deep web. Like the other depths of the deep web, it's not searchable. The people behind the websites and data collections on the dark web intentionally keep them hidden from search. And the reasons vary. Some of them are entirely legitimate, others questionable, and several are outright illegal in nature.

Its origins go back to the 1990s, when the U.S. Department of Defense developed the dark web as a means of anonymous and encrypted communications. That story might sound familiar. It's quite like the origin story for the broader internet. That had its roots in the Department of



Defense as well. So, just as the broader internet eventually became available to the public, so did the dark web as well.

Getting there requires a special browser because the protocols for the dark web differ from the surface web. Moreover, these browsers strip web traffic of identifiable information, encrypt it, and send it through a series of server jumps. The browsing traffic will appear to go through a server in one country, then a different server in another, and then another.

These steps make it highly difficult to identify the person using the browser. On the flip side, it makes it difficult to identify the people hosting the sites and services on the dark web as well.

Without question, privacy is everything on the dark web. For good and for bad.

Legitimate uses of the dark web

While the notion of the dark web typically gets raised in the context of cybercrime and other illegal activity, it has legitimate uses. Some of these use cases include:

Circumventing censorship

Well-regarded news outlets such as the BBC and Pro Publica maintain a presence on the dark web to ensure that anyone can access their reporting. This includes people in nations and regions where certain news sources are censored.

Private communication

For the particularly privacy-conscious, the dark web hosts several resources for encrypted communication. That includes email clients, internet chat, and even social media sites.

Whistleblowing

Anonymous tips are a part of national security, law enforcement, and journalism as well. The private nature of the dark web confers an additional degree of anonymity to tipsters.

The dark web isn't a place everyday internet users will need, or even want, to go. It's far more complicated than the surface web—and going in without taking several security measures can make the trip a risky one.

The dark web as a marketplace for cybercrime

This is where the rubber meets the road from an online protection standpoint. The dark web is also a marketplace for hackers and bad actors. In several ways—as a place to purchase and rent malware, a repository for stolen information, and a place to communicate and coordinate attacks.



For starters, the dark web is populated with dark marketplaces. And difficult-to-trace cryptocurrency is the coin of the realm. With dark web stores stocked with ready-made malware kits, bad actors can launch attacks with little need for technical expertise. Others have done the work for them.

Cybercrime groups of all sizes prop up these shops, which they also use to rent out other services for attacks. For example, a small-time bad actor could easily lease a botnet to wage an attack that slows a targeted website to a crawl. Some cybercrime groups will provide hackers who can run attacks on someone else's behalf, creating a mercenary "hacker for hire" gig economy.

Likewise, information stolen from a data breach can end up in dark web marketplaces as well. The personal information posted in these marketplaces can range anywhere from emails and passwords to in-depth information like tax numbers, health information, and driver's license numbers. Some of it goes up for sale. Some of it gets dumped there for free. With the right information in hand, cybercriminals can commit acts of identity theft. That includes claiming unemployment benefits and tax refunds in someone else's name. In extreme cases, it can lead to bad actors can outright impersonate their victims, racking up debts and criminal records along the way.

Some hacking groups sell hacked accounts outright. For a couple hundred dollars, they offer up login and password information for bank accounts that have a couple thousand dollars in them. Also available, pre-hacked email, social media, and online payment accounts. If it's hackable and has value, it's likely for sale on the dark web.

Protect yourself from hackers and bad actors on the dark web

With all this shady activity on the dark web, you might wonder how you can protect yourself. In fact, you can take several steps to help prevent your information from finding its way there. And you also can take other steps if your information unfortunately does end up on the dark web.

Installing online protection software is the first step. Online protection software can help prevent many of the attacks bad actors can purchase on the dark web. It protects against ransomware, adware, spyware, and all manner of malware, whether it's pre-existing or entirely new.

Yet today's online protection goes far beyond antivirus. Comprehensive protection like ours protects your privacy and identity as well. It can monitor your identity and credit, create strong passwords, and clean up your personal information online.

Monitor your identity:

An identity monitoring service can actively scan the dark web for personal info like your date of birth, email addresses, credit card numbers, personal identification numbers, and much



more. In the event you fall victim to identity theft, our identity theft coverage and restoration can provide up to \$1 million in coverage to cover the costs. Plus, it provides the services of a recovery expert with limited power of attorney to help you repair the damage done.

Keep an eye on your credit:

If you spot unusual or unfamiliar charges or transactions in your account, bank, or debit card statements, follow up immediately. That might indicate improper use. In general, banks, credit card companies, and many businesses have countermeasures to deal with fraud. Moreover, they have customer support teams that can help you file a claim if needed.

Given all the accounts you likely have a credit monitoring service can help. McAfee's credit monitoring service can help you keep an eye on changes to your credit score, report, and accounts with timely notifications and provide guidance so you can take action to tackle identity theft.

Create and maintain strong, unique passwords:

With the high number of accounts you need to protect, creating strong, unique passwords for each one can get time consuming. Further, updating them regularly can become a time-consuming task. That's where a password manager comes in.

A password manager does the work of creating strong, unique passwords for your accounts. These will take the form of a string of random numbers, letters, and characters. They will not be memorable, but the manager does the memorizing for you. You only need to remember a single password to access the tools of your manager.

Close old, risky accounts:

The more online accounts you keep, the greater the exposure you have to data breaches. Each account will have varying degrees of personal and financial information linked to it. And that means each one carries a varying degree of risk if it gets breached. Moreover, some sites and services protect data better than others, which adds another dimension of risk. Closing old and particularly risky accounts can decrease the risk of your personal and financial information winding up in the hands of an identity thief.

With security and savings in mind, McAfee created Online Account Cleanup. It finds and requests the deletion of unused accounts and protects your personal data from data breaches as a result. Monthly scans across your online accounts show a risk level for each account and help you decide which ones to delete.

Use two-factor authentication:

Two-factor authentication is an extra layer of defense on top of your username and password. It adds a one-time-use code to access your login procedure, typically sent to your smartphone



by text or call. Together, that makes it tougher for a crook to hack your account if they get hold of your username and password. If any of your accounts support two-factor authentication, the few extra seconds it takes to set up is more than worth the big boost in protection you'll get.

Protect yourself from cybercriminals on the dark web

The "dark" in the dark web stands for anonymity. And with anonymity, all kinds of activity follow. Good and bad.

From a security standpoint, the dark web is a haven for all manner of cybercriminals. Understanding how they use the dark web can help you protect yourself from their activities. You have tools for prevention, and you have resources available if your information ends up there or leads to identity theft.

By putting a face on the dark web, you put a face on cybercrime and can help reduce the risk of it happening to you.

Source: <u>https://www.mcafee.com/blogs/privacy-identity-protection/what-is-the-dark-web-the-answer-can-help-you-stay-safer-online/</u>

20. RomCom malware spread via Google Ads for ChatGPT, GIMP, more

A new campaign distributing the RomCom backdoor malware is impersonating the websites of well-known or fictional software, tricking users into downloading and launching malicious installers.

The latest campaign was uncovered by Trend Micro, who have followed RomCom since the summer of 2022. The researchers report that the threat actors behind the malware have escalated its evasion by using payload encryption and obfuscation and expanded the tool's capabilities by introducing new and powerful commands.

Most websites used for distributing RomCom to victims concern remote desktop management applications, which increases the likelihood of attackers employing phishing or social engineering to approach their targets.

RomCom linked to Cuba ransomware

The first documented use of RomCom was reported in August 2022 by Palo Alto Networks, attributing the attacks to a Cuba ransomware affiliate they named 'Tropical Scorpius.' Trend Micro uses 'Void Rabisu' to track the same actor.

In October 2022, Ukraine's CERT-UA reported that the RomCom malware was being used in attacks against critical networks in the country.



Another report published almost simultaneously by BlackBerry claimed the association with Cuba ransomware but confirmed the attacks in Ukraine while also indicating there were malware victims in the United States, Brazil, and the Philippines.

A subsequent BlackBerry report in November 2022 illustrated how RomCom impersonated legitimate software, including SolarWinds Network Performance Monitor (NPM), the KeePass password manager, and PDF Reader Pro.

The current campaign

Trend Micro's report on the latest RomCom activity lists several examples of websites used by the malware operators between December 2022 and April 2023 that impersonate legitimate software, like Gimp, Go To Meeting, ChatGPT, WinDirStat, AstraChat, System Ninja, Devolutions' Remote Desktop Manager, and more.



One of the malicious website that's still online (BleepingComputer)

Some of the malicious sites used in the said time period are:

- gllmp.com (offline) Impersonates the free and open-source image editor
- gotomeet.us (offline) Impersonates the cloud video meeting and conferencing app
- singularlabs.org (offline) Impersonates a PC-cleaning tool
- chatgpt4beta.com (online) Impersonates the AI-powered chatbot platform
- astrachats.com (offline) Impersonates the secure chat software
- devolutionrdp.com (online) Impersonates a remote desktop management tool



- cozy-sofware.com (offline) Impersonates a remote desktop management tool
- vectordmanagesoft.com (offline) Impersonates a remote desktop management tool
- devolrdm.com (online) Impersonates a remote desktop management tool
- dirwinstat.com (online) Impersonates a disk usage viewer and cleanup tool

These fake sites are promoted through Google advertisements and highly targeted phishing emails, with most of the victims based in Eastern Europe.

The websites distribute MSI installers that impersonate the promised app but are trojanized with a malicious DLL file ("InstallA.dll").

This file extracts another three DLLs onto the victim's %PUBLIC%\Libraries folder, which handles command and controll server communications and command execution.



Infection process (Trend Micro)

The latest version of the RomCom payload analyzed by Trend Micro shows that its authors have worked towards implementing additional malicious commands, with their number of commands growing from 20 to 42.

Some of the highlighted commands that can be pushed to a device infected with RomCom are:

- Start cmd.exe
- Drop a file onto the victim's computer to introduce more payloads.
- Spawn a process with PID spoofing to make it appear legitimate.
- Exfiltrate data from the compromised system.
- Set up a proxy via SSH.
- Update the malware on the device.



- Run AnyDesk on a hidden window.
- Compress a given folder and send it to the attackers' server.

These commands already give the attackers extensive capabilities, but the cybersecurity company reports having seen several cases of additional malware payloads being installed through RomCom.

Stealer components downloaded by RomCom on compromised devices include:

- PhotoDirector.dll A screenshot-snapping tool that compresses images in ZIP archives for exfiltration.
- procsys.dll A web browser (Chrome, Firefox, Edge) cookies stealer.
- wallet.exe A cryptocurrency wallet stealer.
- msg.dll An instant messenger chat stealer.
- FileInfo.dll An FTP credentials stealer that uploads data to an FTP server.



C2 communications diagram (Trend Micro)

Enhanced evasion

RomCom's authors now use the VMProtect software for code protection and anti-VM capabilities. Also, it uses encryption for the payload, the key for which is not hard coded but fetched by an external address.

The malware uses null bytes in its C2 communication to evade detection from network monitoring tools.

Finally, the software downloaded from the malicious websites is signed by seemingly legitimate companies supposedly based in the U.S. and Canada, the websites of which are filled with fake or plagiarized content.



RomCom has been associated with ransomware, espionage, and warfare, and the exact goals of its operators remain murky. Whatever the case, it is a versatile threat that can cause significant damage.

Trend Micro has provided a comprehensive list of indicators of compromise (IoCs) for the latest RomCom campaign and Yara rules to help defenders detect and stop the attacks.

Source: <u>https://www.bleepingcomputer.com/news/security/romcom-malware-spread-via-google-ads-for-chatgpt-gimp-more/</u>

21. Microsoft finds macOS bug that lets hackers bypass SIP root restrictions

Apple has recently addressed a vulnerability that lets attackers with root privileges bypass System Integrity Protection (SIP) to install "undeletable" malware and access the victim's private data by circumventing Transparency, Consent, and Control (TCC) security checks.

Discovered and reported to Apple by a team of Microsoft security researchers, the flaw (dubbed Migraine) is now tracked as CVE-2023-32369.

Apple has patched the vulnerability in security updates for macOS Ventura 13.4, macOS Monterey 12.6.6, and macOS Big Sur 11.7.7, released two weeks ago, on May 18.

System Integrity Protection (SIP), also known as 'rootless,' is a macOS security mechanism that prevents potentially malicious software from altering certain folders and files by imposing restrictions on the root user account and its capabilities within protected areas of the operating system.

SIP operates under the principle that only processes signed by Apple or those possessing special entitlements, such as Apple software updates and installers, should be authorized to alter macOS-protected components.

It's also important to note that there's no method to disable SIP without restarting the system and booting off of macOS Recovery (the built-in recovery system)—which requires having physical access to an already compromised device.

However, Microsoft's researchers found that attackers with root permissions could bypass SIP security enforcement by abusing the macOS Migration Assistant utility, a built-in macOS app that uses the systemmigrationd daemon with SIP-bypassing capabilities stemming from its com.apple.rootless.install.heritable entitlement.

The researchers demonstrated that attackers with root permissions could automate the migration process with AppleScript and launch a malicious payload after adding it to SIP's exclusions list without restarting the system and booting from macOS Recovery.



"By focusing on system processes that are signed by Apple and have the com.apple.rootless.install.heritable entitlement, we found two child processes that could be tampered with to gain arbitrary code execution in a security context that bypasses SIP checks," the Microsoft Threat Intelligence team said.

Arbitrary SIP bypasses come with significant risks, especially when exploited by malware creators, as it enables malicious code to have far-reaching effects, including creating SIP-protected malware that can't be removed via standard deletion methods.

They also greatly expand the attack surface and could allow attackers to tamper with system integrity through arbitrary kernel code execution and potentially install rootkits to hide malicious processes and files from security software.

Bypassing SIP protection also enables a complete bypass of Transparency, Consent, and Control (TCC) policies, enabling threat actors to replace TCC databases and gaining granting unrestricted access to the victim's private data.

This is not the first such macOS vulnerability reported by Microsoft researchers in recent years, with another SIP bypass dubbed Shrootless reported in 2021, allowing attackers to perform arbitrary operations on compromised Macs, escalate privileges to root, and potentially install rootkits on vulnerable devices.

More recently, Microsoft principal security researcher Jonathan Bar Or also found a security flaw known as Achilles that attackers could exploit to deploy malware via untrusted apps capable of bypassing Gatekeeper execution restrictions.

He also discovered powerdir, another macOS security bug that can let attackers bypass Transparency, Consent, and Control (TCC) technology to access users' protected data.

Source: <u>https://www.bleepingcomputer.com/news/security/microsoft-finds-macos-bug-that-lets-hackers-bypass-sip-root-restrictions/</u>



If you want to learn more about ASOC and how we can improve your security posture, **contact us at tbs.sales@tbs.tech**.

This Bulletin contains information, articles, news, reports or other materials from external sources (links to website sources stated herein above). All information and materials are provided "as is" and TELELINK BUSINESS SERVICES makes no warranty or representations, expressed or implied, for their accuracy, completeness, fitness for particular use, reliability, legality or non-infringement of copyrights.

The content in this Bulletin is provided for informational purposes only do not constitute or represent TELELINK BUSINESS SERVICES's expressed or implied endorsement, recommendation, advertisement, merchandising or solicitation to purchase any of the products or services, described therein, or making any other investment decisions.

TELELINK BUSINESS SERVICES is not responsible for the contents of any linked site or any link contained in a linked site. The hypertext links provided herein are meant only as a convenience and the inclusion of any link does not imply endorsement of or by the referenced site.