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

Monthly Security Bulletin

February 2023

This security bulletin is powered by Telelink Business Services'

Advanced Security Operations Center

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

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.

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

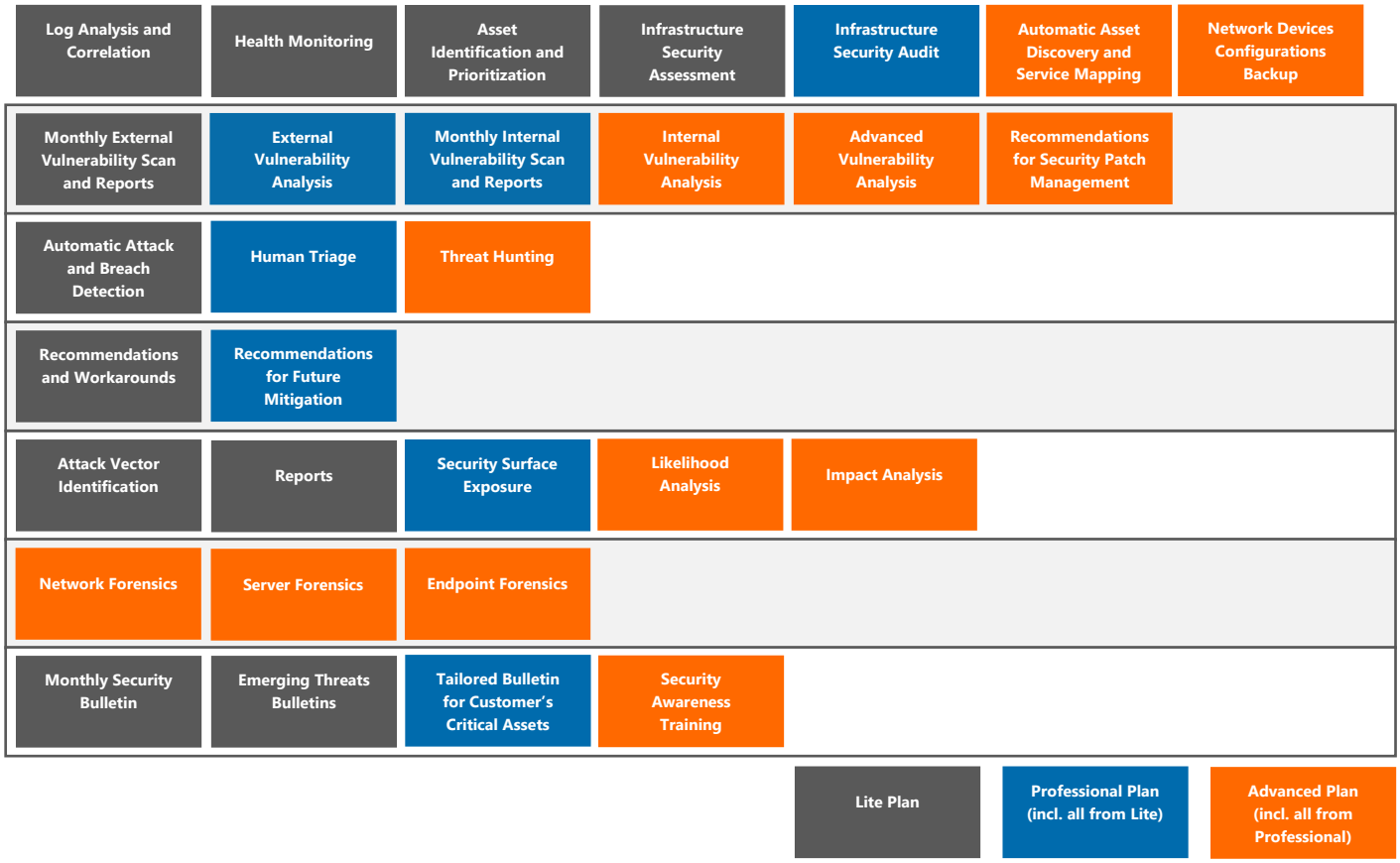
Start to mitigate cyber threats and minimize the risk!

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!



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. PyTorch discloses malicious dependency chain compromise over holidays

PyTorch has identified a malicious dependency with the same name as the framework's 'torchtriton' library. This has led to a successful compromise via the dependency confusion attack vector.

PyTorch admins are warning users who installed PyTorch-nightly over the holidays to uninstall the framework and the counterfeit 'torchtriton' dependency.

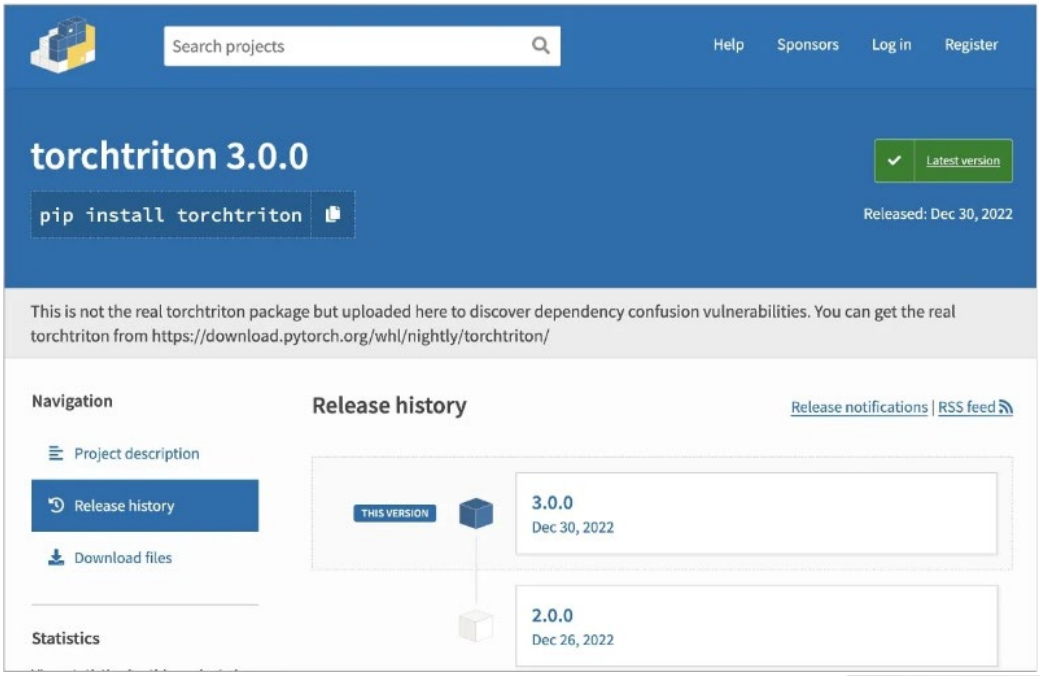
From computer vision to natural language processing, the open source machine learning framework PyTorch has gained prominence in both commercial and academic realms.

Malicious library targets PyTorch-nightly users

Between December 25th and December 30th, 2022, users who installed PyTorch-nightly should ensure their systems were not compromised, PyTorch team has warned.

The warning follows a 'torchtriton' dependency that appeared over the holidays on the Python Package Index (PyPI) registry, the official third-party software repository for Python.

"Please uninstall it and **torchtriton** immediately, and use the latest nightly binaries (newer than Dec 30th 2022)," advises PyTorch team.



Malicious PyTorch dependency 'torchtriton' on PyPI (BleepingComputer)

The malicious 'torchtriton' dependency on PyPI shares name with the official library published on the PyTorch-nightly's repo. But, when fetching dependencies in the

Python ecosystem, PyPI normally takes precedence, causing the malicious package to get pulled on your machine instead of PyTorch's legitimate one.

"Since the PyPI index takes precedence, this malicious package was being installed instead of the version from our official repository. This design enables somebody to register a package by the same name as one that exists in a third party index, and **pip** will install their version by default," writes PyTorch team in a disclosure published yesterday.

At the time of writing, BleepingComputer observed the malicious 'torchtriton' dependency had exceeded 2,300 downloads in the past week.

This type of supply chain attack is known as "dependency confusion," as first reported by BleepingComputer in 2021, just as the attack vector was popularized by ethical hacker Alex Birsan.

PyTorch states, users of the PyTorch **stable** packages are unaffected by this issue.

Hacker steals sensitive files, claims ethical research

Not only does the malicious 'torchtriton' survey your system for basic fingerprinting info (such as IP address, username, and current working directory), it further steals sensitive data:

- Gets system information
  - nameservers from **/etc/resolv.conf**
  - hostname from **gethostname()**
  - current username from **getlogin()**
  - current working directory name from **getcwd()**
  - environment variables

- Reads the following files
  - /etc/hosts
  - /etc/passwd
  - The first 1,000 files in $HOME/*
  - $HOME/.gitconfig
  - $HOME/.ssh/*

It then uploads all of this data, including file contents, to the h4ck.cfd domain via encrypted DNS queries using the wheezy.io DNS server.

PyTorch explains, the malicious 'triton' binary contained within the counterfeit 'torchtriton' is only executed when the user imports 'triton' package in their build. This would require explicit code and is not PyTorch's default behavior.

The notice on the h4ck.cfd domain **implies** the whole operation is ethical research, but the analysis strongly indicates otherwise.

> *"Hello, if you stumbled on this in your logs, then this is likely because your Python was misconfigured and was vulnerable to a dependency confusion attack. To identify companies that are vulnerable the script sends the metadata about the host (such as its hostname and current working directory) to me. After I've identified who is vulnerable and [reported] the finding all of the metadata about your server will be deleted."*

Contrary to the wording of the notice, the binary not only collects "metadata," but steals aforementioned secrets including your SSH keys, **gitconfig, hosts** and **passwd** files, and the contents of the first 1,000 files in your HOME directory.

BleepingComputer obtained a copy of the malicious binary which, according to VirusTotal, shows a clean reputation at the time of writing. But, don't be fooled.

We observed, unlike several research packages and PoC exploits that are conspicuous in their intent and behavior, 'torchtriton' employs known anti-VM techniques to evade detection. More importantly, the malicious payload is obfuscated and contained entirely in the binary format, i.e. Linux ELF files, all of which makes the library an outlier when juxtaposed with ethical dependency confusion exploits of the past shipped in plaintext.

We also noticed the sample reads **.bash_history** or a list of commands and inputs the user has typed into the terminal, which is yet another trait exhibited by malware.

This won't be the first time either when a hacker claims that their actions constitute ethical research, just as they are caught exfiltrating secrets.

In mid 2022, hugely popular Python and PHP libraries, respectively, 'ctx' and 'PHPass' were hijacked and altered to steal AWS keys. The researcher behind the attack later claimed that this was ethical research.

For the avoidance of doubt, we approached the owner of h4ck.cfd for comment. Public records show the domain was registered with Namecheap on December 21st, just days prior to this incident.

Given below is the complete statement we received from the domain owner, who also appears to be behind the wheezy.io domain.

Note, the mention of "Facebook" below is relevant given PyTorch's conception at Meta AI.

> *"Hey, I am the one who claimed torchtriton package on PyPi. Note that this was not intended to be malicious!*
>
> *I understand that I could have done a better job to not send all of the user's data. The reason I sent more metadata is that in the past when investigating dependency confusion issues, in many cases it was not possible to identify the victims by their hostname, username and CWD. That is the reason this time I decided to send more data, but looking back this was wrong decision and I*

should have been more careful.

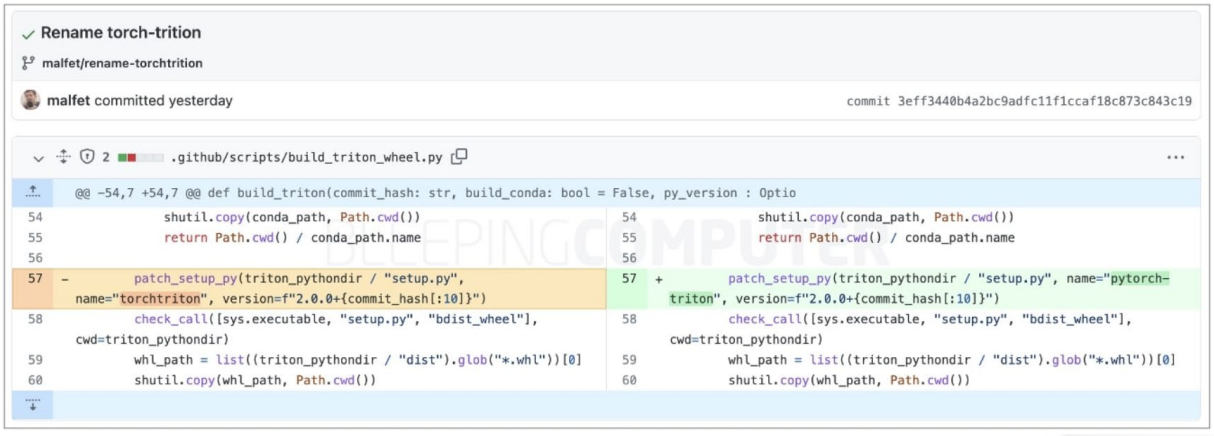
I accept the blame for it and apologize. At the same time I want to assure that it was not my intention to steal someone's secrets. I already reported this vulnerability to Facebook on December 29 (almost three days before the announcement) after having verified that the vulnerability is indeed there. I also made numerous reports to other companies who were affected via their HackerOne programs. Had my intents been malicious, I would never have filled any bug bounty reports, and would have just sold the data to the highest bidder.

I once again apologize for causing any disruptions, I assure that all of the data I received has been deleted.

By the way in my bug report to Facebook I already offered to transfer the PyPi package to them, but so far I haven't received any replies from them."

Mitigations

PyTorch team has renamed the 'torchtriton' dependency to 'pytorch-triton' and reserved a dummy package on PyPI to prevent similar attacks. The group seeks to claim ownership of the existing 'torchtriton' on PyPI to defuse the current attack.



PyTorch renames dependency to prevent further attacks (BleepingComputer)

To uninstall the malicious dependency chain, users should run the following command:

```
$ pip3 uninstall -y torch torchvision torchaudio torchtriton
$ pip3 cache purge
```

Running the following command will look for the presence of malicious binary and reveal if you are impacted:

```
python3 -c "import pathlib;import
importlib.util;s=importlib.util.find_spec('triton');
affected=any(x.name == 'triton' for x in
(pathlib.Path(s.submodule_search_locations[0]
if s is not None else '/' ) / 'runtime').glob('*'));
print('You are {}affected'.format('' if affected else 'not
'))"
```

The SHA256 hash of the 'triton' ELF binary
is: 2385b29489cd9e35f92c072780f903ae2e517ed422eae67246ae50a5cc738a0e.

Source: https://www.bleepingcomputer.com/news/security/pytorch-discloses-malicious-dependency-chain-compromise-over-holidays/

2. Ransomware gang apologizes, gives SickKids hospital free decryptor

The LockBit ransomware gang has released a free decryptor for the Hospital for Sick Children (SickKids), saying one of its members violated rules by attacking the healthcare organization.

SickKids is a teaching and research hospital in Toronto that focuses on providing healthcare to sick children.

On December 18th, the hospital suffered a ransomware attack that impacted internal and corporate systems, hospital phone lines, and the website.

While the attack only encrypted a few systems, SickKids stated that the incident caused delays in receiving lab and imaging results and resulted in longer patient wait times.

On December 29th, SickKids announced that it had restored 50% of its priority systems, including those causing diagnostic or treatment delays.

LockBit gang apologizes for attack

As first noted by threat intelligence researcher Dominic Alvieri, two days after SickKids' latest announcement, the LockBit ransomware gang apologized for the attack on the hospital and released a decryptor for free.

"We formally apologize for the attack on sikkids.ca and give back the decryptor for free, the partner who attacked this hospital violated our rules, is blocked and is no longer in our affiliate program," stated the ransomware gang.

BleepingComputer has confirmed that this file is available for free and claims to be a Linux/VMware ESXi decryptor. As there is no additional Windows decryptor, it indicates that the attacker could only encrypt virtual machines on the hospital's network.

Apology to SickKids on the LockBit data leak site
Source: BleepingComputer

The LockBit operation runs as a Ransomware-as-a-Service, where the operators maintain the encryptors and websites, and the operation's affiliates, or members, breach victims' networks, steal data, and encrypt devices.

As part of this arrangement, the LockBit operators keep approximately 20% of all ransom payments and the rest goes to the affiliate.

While the ransomware operation allows its affiliates to encrypt pharmaceutical companies, dentists, and plastic surgeons, it prohibits its affiliates from encrypting "medical institutions" where attacks could lead to death.

"It is forbidden to encrypt institutions where damage to the files could lead to death, such as cardiology centers, neurosurgical departments, maternity hospitals and the like, that is, those institutions where surgical procedures on high-tech equipment using computers may be performed," explains the ransomware operation's policies.

The stealing of data from any medical institution is allowed per the policies.

According to the ransomware gang, as one of its affiliates encrypted the hospital's devices, they were removed from the operation, and a decryptor was offered for free.

However, this does not explain why LockBit did not provide a decryptor sooner, with patient care being impacted and SickKids working to restore operations since the 18th.

Furthermore, LockBit has a history of encrypting hospitals and not providing decryptors, as was seen in its attack against the Center Hospitalier Sud Francilien (CHSF) in France, where a $10 million ransom was demanded, and patient data eventually leaked.

The attack on the French hospital led to referring patients to other medical centers and postponing surgeries, which could have led to significant risk to patients.

BleepingComputer had contacted LockBit at the time to understand why they were demanding a ransom from CHSF, even though it was against policies, but never received a response.

This is not the first time a ransomware gang has provided a free decryptor to a healthcare organization.

In May 2021, the Conti Ransomware operation provided a free decryptor to Ireland's national health service, the HSE, after facing increased pressure from international law enforcement.

Source: https://www.bleepingcomputer.com/news/security/ransomware-gang-apologizes-gives-sickkids-hospital-free-decryptor/

3. How Can the White House's New IoT Labels Improve Security?

The White House's National Security Council (NSC) is working on an ambitious project to improve consumer Internet of Things (IoT) security through industry-standard labeling. If successful, the labeling system will replace existing frameworks across the globe.

Modeled after the EPA's Energy Star labeling program, the IoT labeling initiative should have two effects: to educate and inform consumers, and to provide a strong incentive to manufacturers to make their products more secure.

The government wants the program to roll out in the Spring of 2023. But what must these labels address from the perspective of cybersecurity specialists?

Why Consumer IoT Matters to Cybersecurity Professionals

IoT devices represent a special kind of security threat. Consumers buy fun or useful gadgets with a focus on the price, features or convenience, often without considering security. After all, how threatening could a toaster, security camera, smart doorbell, smart light switch, air-quality monitor or fitness dog collar really be?

This perception issue is the main problem with consumer IoT. A "smart light bulb" sounds innocent. But all IoT devices are, by definition, nonstandard microprocessor-based computers that run software and send data over a network.

In fact, the majority of "computers" in the world are IoT devices rather than servers, laptops or desktops. Billions of devices come in thousands of types. This combination of ubiquity and variety causes even more issues for cybersecurity.

Operating systems manufacturers and application vendors stay vigilant for new security threats and issue regular patches and updates. But is the maker of smart home smoke detectors performing those tasks? The new labels should light a fire to get IoT makers to focus more on security.

The Dissolving Security Perimeter

The IoT concept has been around since 1999. Until recently, the distinction between consumer IoT and industrial or enterprise IT was far more defined. This distinction is still important, of course. But from a cybersecurity perspective, well, things have changed.

Employees are working from home, and not just full-time remote workers and hybrid workers. Even full-time office workers are now logging on from home in the evenings and weekends. These employees are connecting over the same networks their consumer IoT devices operate on.

The dissolution of the perimeter in enterprise computing means that IoT devices inside and outside corporate offices share the same status as potential security risks to be managed — hence the need for zero trust architectures. But the difference is that consumer devices are far less likely to offer security features, such as regular security-enhancing firmware updates.

Zero trust is necessary. But consumer devices with greater security would also help a lot.

In Search of a Global Standard

The White House is working with the European Union to unify labeling standards with the hope that they'll be applied globally.

As a preview of the White House's initiative, Carnegie Mellon University developed 47 "key factors" for privacy and security, working with 22 groups, and tested with real consumers. They concluded that the main facts should be plainly displayed on the box each device comes in, along with a QR code linking to additional details and a URL for accessing the company's privacy policy.

The researchers divided the highest-priority types of security information into five categories:

1. Security updates
2. Access control
3. Sensor types

4. Data storage locations
5. Data Sharing.

The NSC can also look at Singapore's example. That country launched its Cybersecurity Labelling Scheme (CLS) in October 2020, and much of that effort was adopted by Finland. Singapore also proposed an international standard, ISO 27404, which defines a Universal Cybersecurity Labelling Framework (UCLF) for consumer IoT.

And so, the NSC labeling system can succeed in all its aims if it's "user friendly" enough for the mass consumer marketplace, improves upon existing initiatives from the likes of Carnegie Mellon and Singapore and also offers the right kind of restrictions and coverage.

Clarity, Transparency and Security

From a cybersecurity point of view, the best ideas are clear labels that address:

- How often manufacturers deploy patches, with a requirement for manufacturers to stick to their promises on frequency
- Whether or not devices connect to the internet without a password and other access control issues
- Whether it supports multi-factor authentication, especially for devices that come with consumer-facing apps that directly connect with devices
- Lists of all sensors capable of capturing data, including microphones and cameras, and what the purpose of those sensors are
- Whether harvested data is available to employees or third-party companies
- Whether harvested data is stored on the device, the cloud or both, and who has access to the cloud-stored data
- What exactly is done with the data generated by the device? For example, does it have an expiration date? Is it available to consumers? Can anyone share or duplicate it, and what is to become of the data should the company go out of business or change management?

Cybersecurity professionals want the White House initiative to succeed wildly. It could make their jobs just a little bit easier. But to succeed, the new labels must hit all of the major threat points inherent in the nature of the IoT beast.

Source: https://securityintelligence.com/articles/how-white-house-new-iot-labels-improve-security/

4. Poland warns of attacks by Russia-linked Ghostwriter hacking group

A The Polish government is warning of a spike in cyberattacks from Russia-linked hackers, including the state-sponsored hacking group known as GhostWriter.

In an announcement on Poland's official site, the government claims that hostile cyber-activities have intensified, targeting public domains and state organizations, strategic energy and armament providers, and other crucial entities.

The Polish believe Russian hackers target their country due to the continued support they have provided Ukraine in the ongoing military conflict with Russia.

Recent cyberattacks

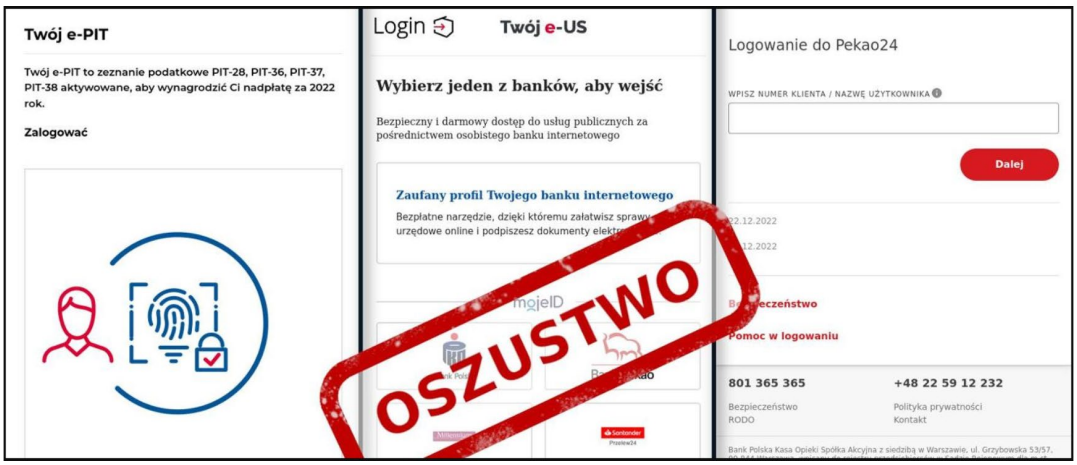
The first case highlighted by the Polish government post is a DDoS (distributed denial of service) attack against the parliament website ('sejm.gov.pl'), attributed to the pro-Russian so-called hacktivists' NoName057(16).'

The attack unfolded the day after the parliament adopted a resolution recognizing Russian as a state sponsor of terrorism, rendering the website inaccessible to the public.

Another notable incident mentioned in the announcement is a phishing attack attributed to the 'GhostWriter' group, which the European Union has associated with the GRU, Russia's military intelligence service. Cybersecurity firm Mandiant has also linked the hacking group to the Belarusian government.

According to the Polish, the Russian hackers set up websites that impersonate the gov.pl government domain, promoting fake financial compensation for Polish residents allegedly backed by European funds.

Clicking on the embedded button to learn more about the program takes victims to a phishing site where they are requested to pay a small fee for verification.



December '22 campaign impersonating the Polish tax administration (gov.pl)

"More and more often cyberattacks are used in order to spread Russian disinformation and serve Russian special services to gather data and vulnerable information," explained the Polish government.

"The operation that is carried out using simultaneously both of these methods is the GhostWriter campaign."

GhostWriter has been active since at least 2017, previously observed impersonating journalists from Lithuania, Latvia, and Poland, to disseminate false information and anti-NATO narratives to local audiences.

The announcement warns that GhostWriter has been focusing on Poland recently, attempting to breach email accounts to collect information, and taking control of social media accounts to spread false information.

In response to the growing cyber threats, Poland's Prime Minister has increased the cybersecurity threat level to 'CHARLIE-CRP,' introducing various measures like maintaining a 24-hour roster in designated offices and public administration organizations.

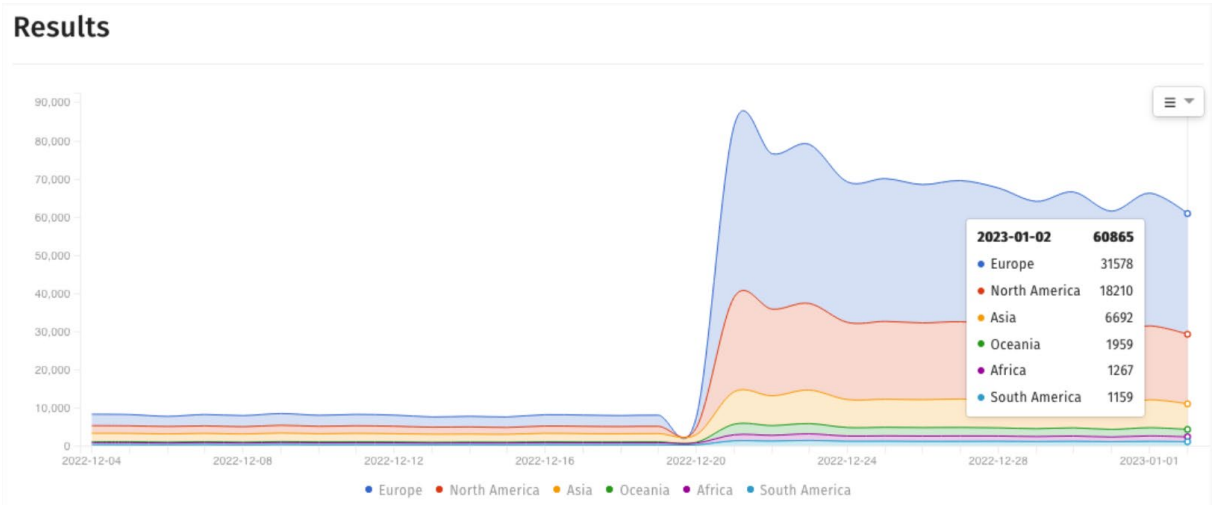
Source: https://www.bleepingcomputer.com/news/security/poland-warns-of-attacks-by-russia-linked-ghostwriter-hacking-group/

5. Over 60,000 Exchange servers vulnerable to ProxyNotShell attacks

More than 60,000 Microsoft Exchange servers exposed online are yet to be patched against the CVE-2022-41082 remote code execution (RCE) vulnerability, one of the two security flaws targeted by ProxyNotShell exploits.

According to a recent tweet from security researchers at the Shadowserver Foundation, a nonprofit organization dedicated to improving internet security, almost 70,000 Microsoft Exchange servers were found to be vulnerable to ProxyNotShell attacks according to version information (the servers' x_owa_version header).

However, new data published on Monday shows that the number of vulnerable Exchange servers has decreased from 83,946 instances in mid-December to 60,865 detected on January 2nd.



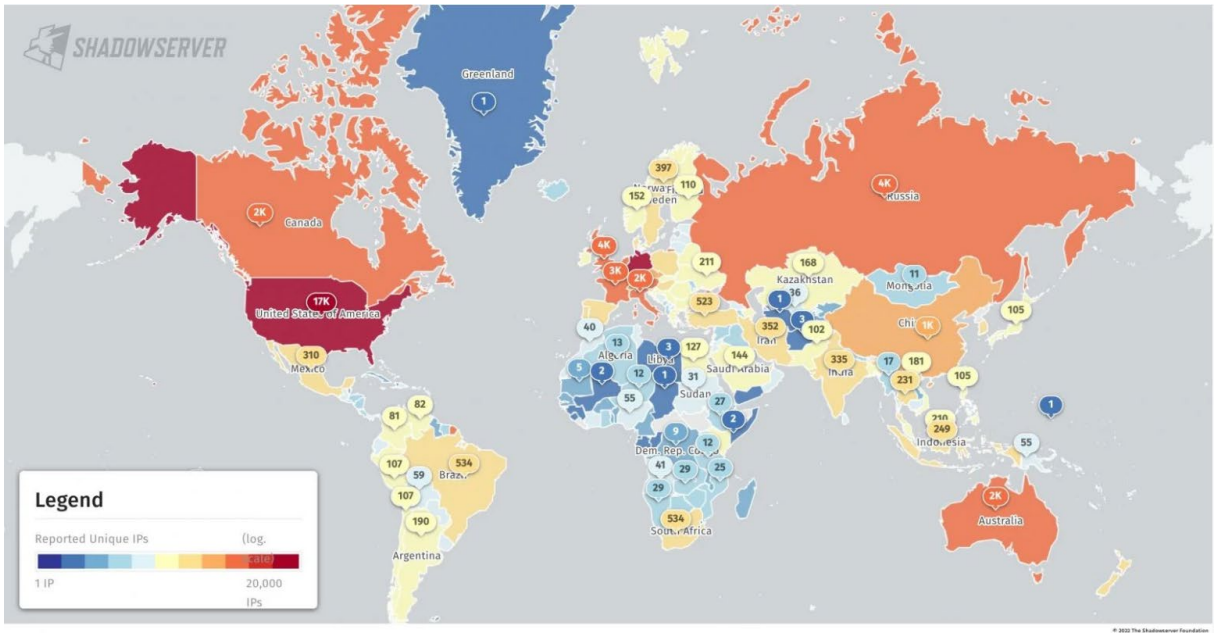
Exchange servers vulnerable to ProxyNotShell attacks (Shadowserver Foundation)

These two security bugs, tracked as CVE-2022-41082 and CVE-2022-41040 and collectively known as ProxyNotShell, affect Exchange Server 2013, 2016, and 2019.

If successfully exploited, attackers can escalate privileges and gain arbitrary or remote code execution on compromised servers.

Microsoft released security updates to address the flaws during the November 2022 Patch Tuesday, even though ProxyNotShell attacks have been detected in the wild since at least September 2022.

Threat intelligence company GreyNoise has been tracking ongoing ProxyNotShell exploitation since September 30th and provides information on ProxyNotShell scanning activity and a list of IP addresses linked to the attacks.



Map of Exchange servers unpatched against ProxyNotShell (Shadowserver Foundation)

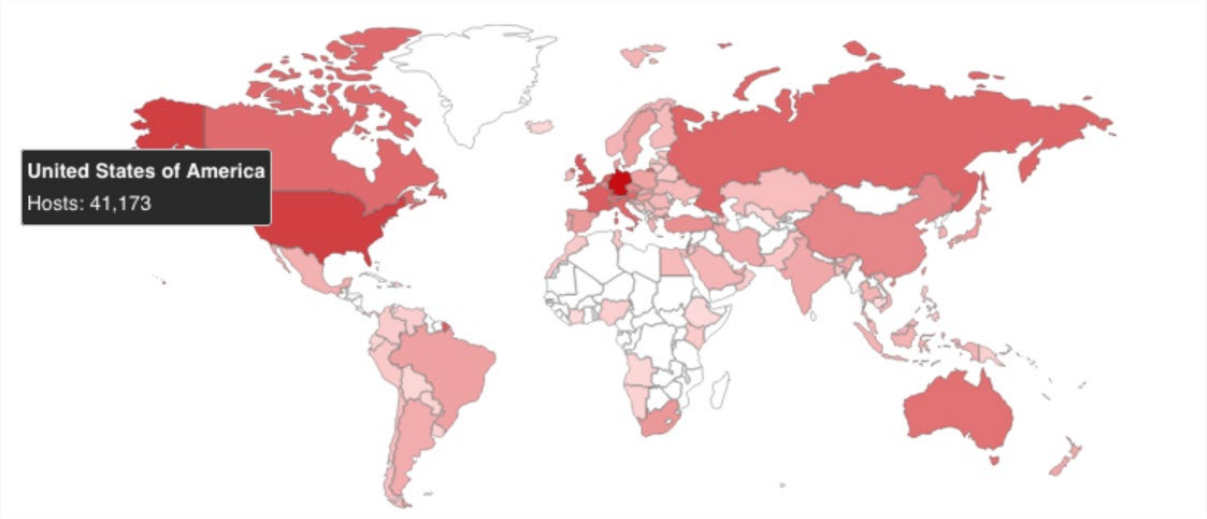
Thousands also exposed to ProxyShell and ProxyLogon attacks

In order to protect your Exchange servers from incoming attacks, you have to apply the ProxyNotShell patches released by Microsoft in November.

While the company also provided mitigation measures, these can be bypassed by attackers, meaning that only fully patched servers are secure from compromise.

As reported by BleepingComputer last month, Play ransomware threat actors are now using a new exploit chain to bypass ProxyNotShell URL rewrite mitigations and gain remote code execution on vulnerable servers through Outlook Web Access (OWA).

To make things even worse, a Shodan search reveals a significant number of Exchange servers exposed online, with thousands left unpatched against ProxyShell and ProxyLogon vulnerabilities that made it into the top most exploited vulnerabilities in 2021.



Exchange servers exposed online (Shodan)

Exchange servers are valuable targets, as demonstrated by the financially motivated FIN7 cybercrime group which has developed a custom auto-attack platform known as Checkmarks and designed to breach Exchange servers.

According to threat intelligence firm Prodaft, which discovered the platform, it scans for and exploits various Microsoft Exchange remote code execution and privilege elevation vulnerabilities, such as CVE-2021-34473, CVE-2021-34523, and CVE-2021-31207.

FIN7's new platform has already been used to infiltrate 8,147 companies, primarily located in the United States (16.7%), after scanning over 1.8 million targets.

Source: https://www.bleepingcomputer.com/news/security/over-60-000-exchange-servers-vulnerable-to-proxynotshell-attacks/

6. Meta to fight €390 million fine for breaching EU data privacy laws

The Irish Data Protection Commission (DPC) has fined Meta a total of €390 million after finding that it forced Facebook and Instagram users to consent to personal data processing for targeted advertising.

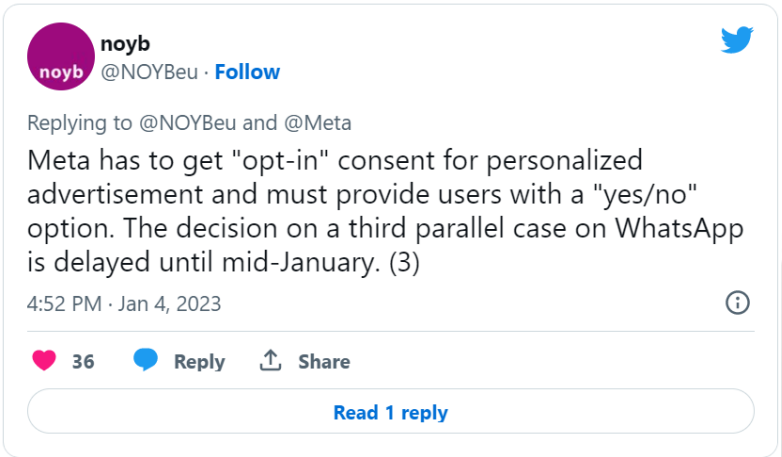
Today's decision comes after the conclusion of two investigations into Meta's data processing operations prompted by complaints filed by the noyb non-profit organization on behalf of Austrian and Belgian users on May 25, 2018, when the EU's General Data Protection Regulation (GDPR) data privacy and security law came into operation.

"Having previously relied on the consent of users to the processing of their personal data in the context of the delivery of the Facebook's and Instagram's services (including behavioural advertising), Meta Ireland now sought to rely on the 'contract' legal basis for most (but not all) of its processing operations," the Irish data watchdog said.

"If they wished to continue to have access to the Facebook and Instagram services following the introduction of the GDPR, existing (and new) users were asked to click "I accept" to indicate their acceptance of the updated Terms of Service. (The services would not be accessible if users declined to do so)."

The DPC imposed a €210 million administrative fine on Meta Ireland for GDPR breaches related to its Facebook service and a €180 million one for violations linked to Instagram services.

The DPC also ordered Meta to bring its current data processing operations into compliance with GDPR's regulations within the next three months, likely meaning that the company would no longer be able to process its users' personal information for personalized advertising until they opt-in.



Meta rejects DPC's findings and will appeal the fines

However, Meta also published today a statement in reaction to DPC's announcement of the €390 million fine, claiming that its approach respects GDPR and blaming the decision on a "lack of regulatory clarity."

The company added that it would appeal the fines and reassured businesses and users that they would be able to "continue to benefit" from personalized ads on Meta's platforms across the EU.

"We strongly believe our approach respects GDPR, and we're therefore disappointed by these decisions and intend to appeal both the substance of the rulings and the fines," Meta said.

"These decisions do not prevent personalised advertising on our platform. Advertisers can continue to use our platforms to reach potential customers, grow their business and create new markets."

"Facebook and Instagram are inherently personalised, and we believe that providing each user with their own unique experience – including the ads they see – is a necessary and essential part of that service."

In November, Meta was also fined €265 million ($275.5 million) by the Irish data watchdog for failing to protect Facebook users' data from scrapers after data belonging to 533 million was leaked on a hacker forum.

Source: https://www.bleepingcomputer.com/news/security/meta-to-fight-390-million-fine-for-breaching-eu-data-privacy-laws/

7. Toyota, Mercedes, BMW API flaws exposed owners' personal info

Almost twenty car manufacturers and services contained API security vulnerabilities that could have allowed hackers to perform malicious activity, ranging from unlocking, starting, and tracking cars to exposing customers' personal information.

The security flaws impacted well-known brands, including BMW, Roll Royce, Mercedes-Benz, Ferrari, Porsche, Jaguar, Land Rover, Ford, KIA, Honda, Infiniti, Nissan, Acura, Hyundai, Toyota, and Genesis.

The vulnerabilities also affected vehicle technology brands Spireon, Reviver, and SiriusXM Connected Vehicle Services.

The discovery of these API flaws comes from a team of researchers led by Sam Curry, who previously disclosed Hyundai, Genesis, Honda, Acura, Nissan, Infinity, and SiriusXM security issues in November 2022.

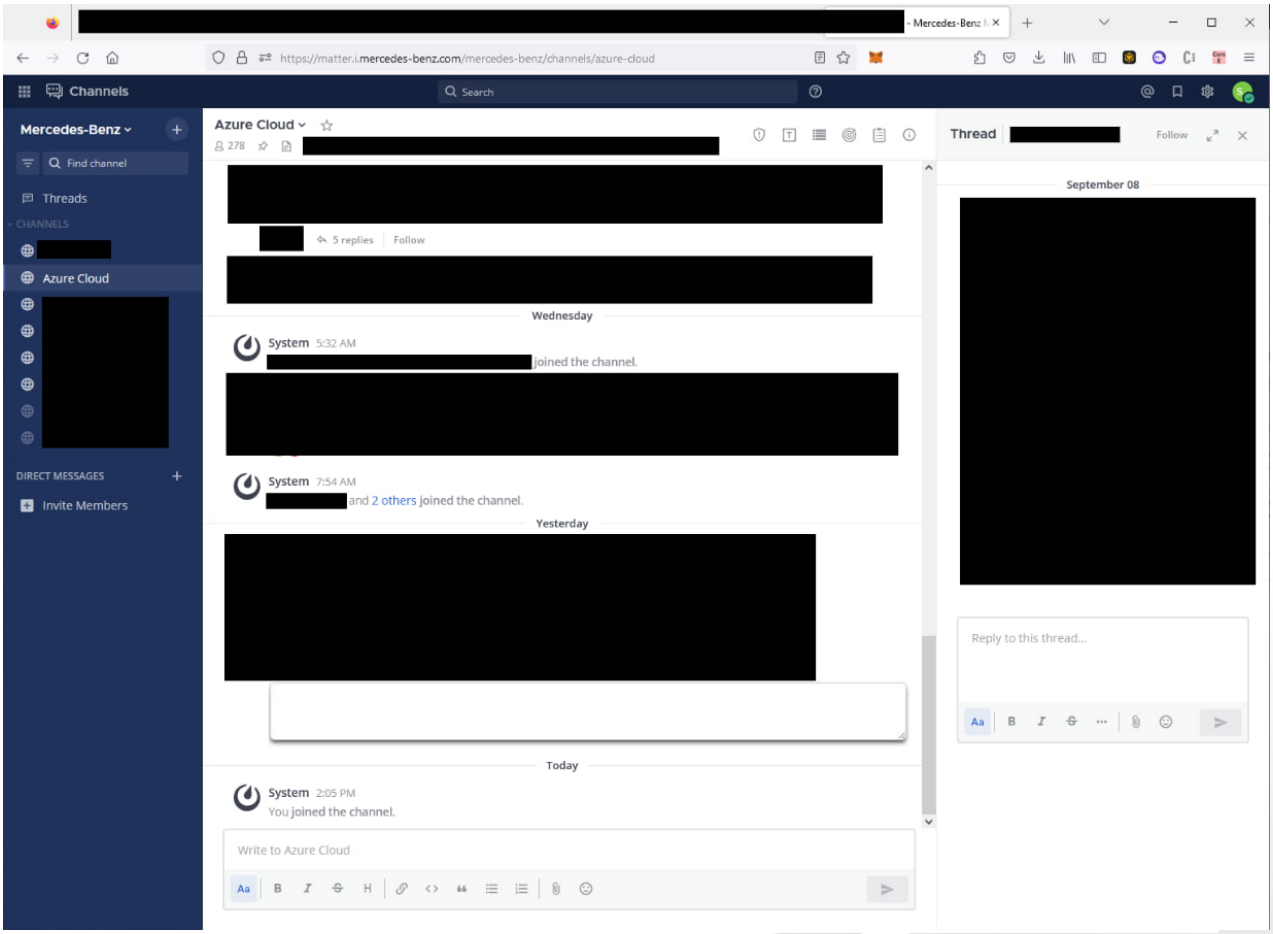
While Curry's previous disclosure explained how hackers could use these flaws to unlock and start cars, now that a 90-day vulnerability disclosure period has passed since reporting these issues, the team has published a more detailed blog post about the API vulnerabilities.

The impacted vendors have fixed all issues presented in this report, so they are not exploitable now.

Accessing internal portals

The most severe API flaws were found in BMW and Mercedes-Benz, which were affected by company-wide SSO (single-sign-on) vulnerabilities that enabled attackers to access internal systems.

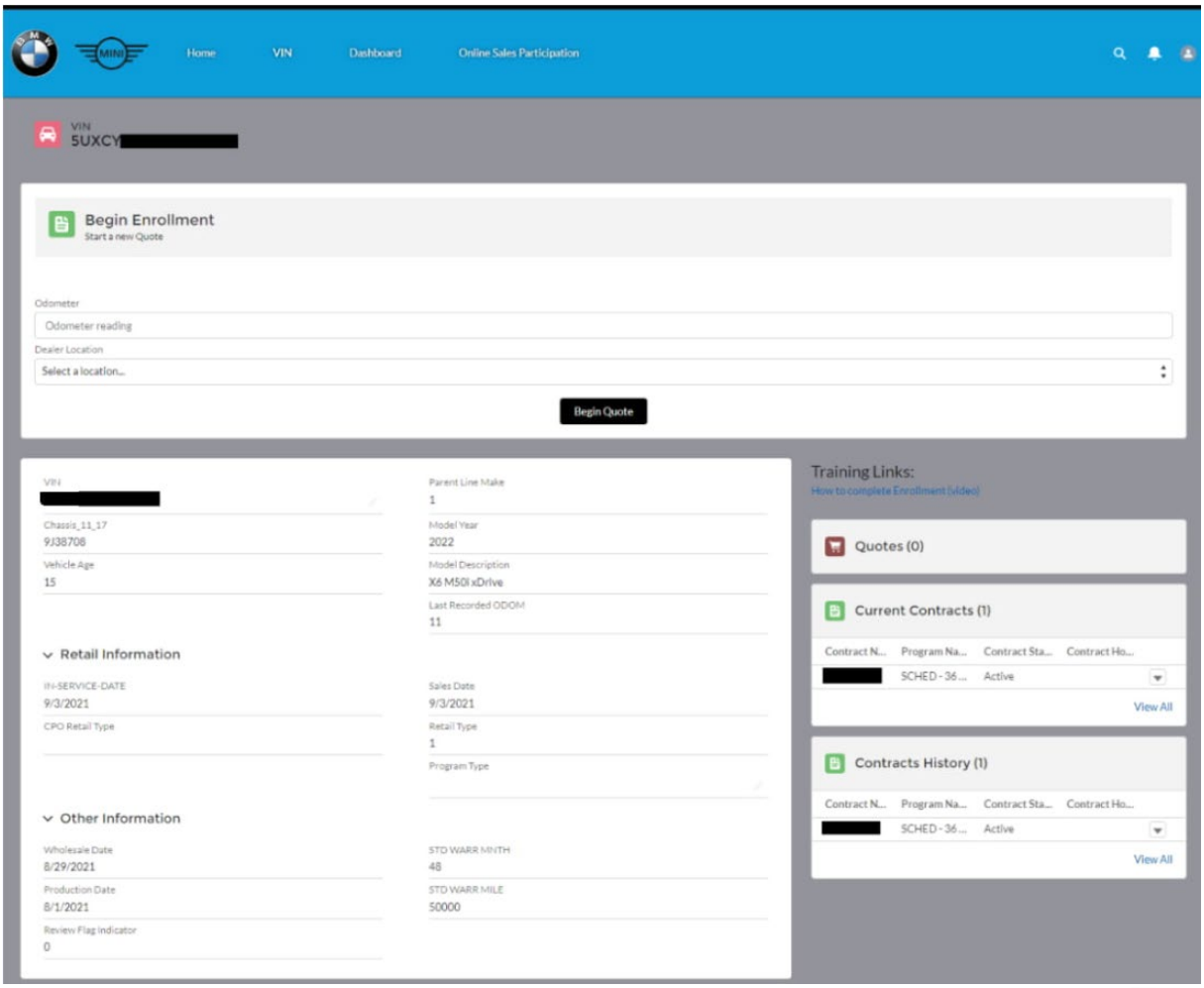
For Mercedes-Benz, the analysts could access multiple private GitHub instances, internal chat channels on Mattermost, servers, Jenkins and AWS instances, XENTRY systems that connect to customer cars, and more.



Internal Mercedes-Benz portal
Source: Sam Curry

For BMW, the researchers could access internal dealer portals, query VINs for any car, and retrieve sales documents containing sensitive owner details.

Additionally, they could leverage the SSO flaws to log in as any employee or dealer and access applications reserved for internal use.



Accessing vehicle details on the BMW portal
Source: Sam Curry

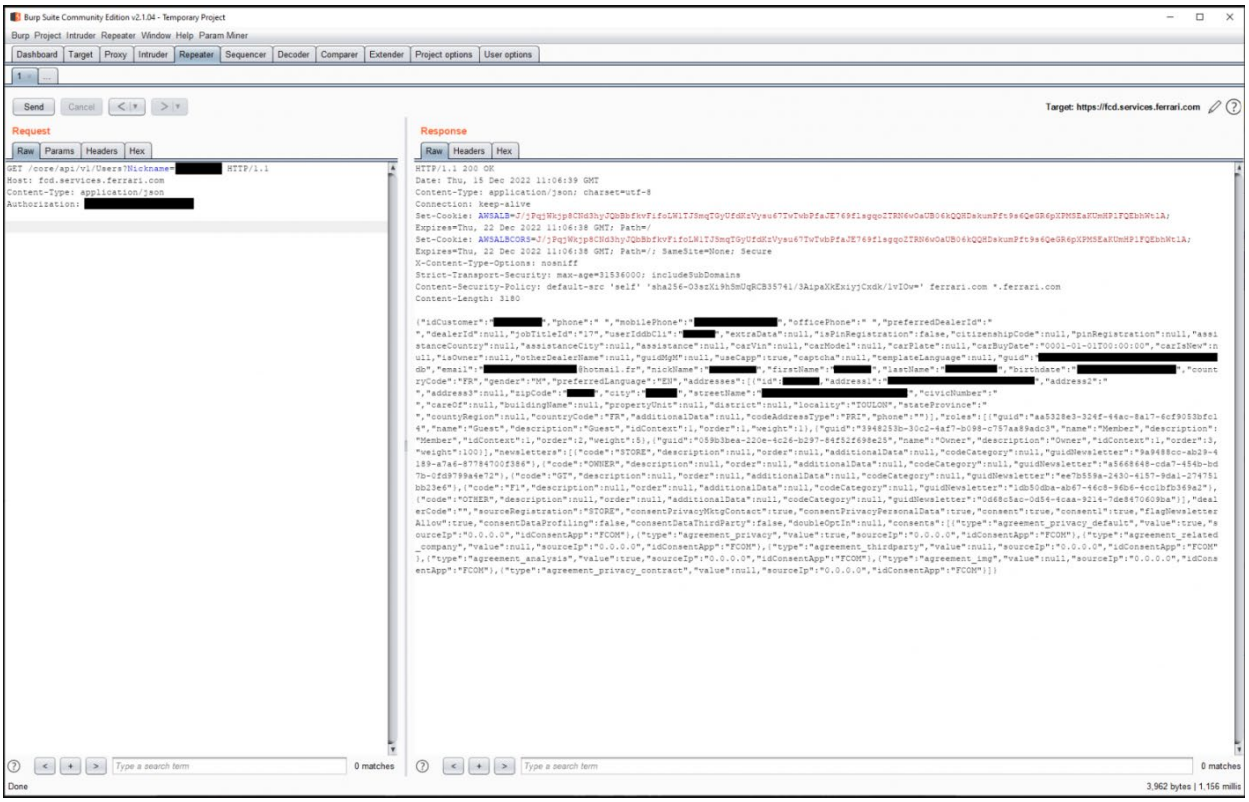
Exposing owner details

Exploiting other API flaws allowed the researchers to access PII (personally identifiable information) for owners of KIA, Honda, Infiniti, Nissan, Acura, Mercedes-Benz, Hyundai, Genesis, BMW, Roll Royce, Ferrari, Ford, Porsche, and Toyota cars.

In the cases of ultra-expensive cars, disclosing owner information is particularly dangerous as, in some cases, the data includes sales information, physical location, and customer addresses.

Ferrari suffered from poorly implemented SSO on its CMS, exposing backend API routes and making it possible to extract credentials from JavaScript snippets.

An attacker could exploit these flaws to access, modify, or delete any Ferrari customer account, manage their vehicle profile, or set themselves as car owners.



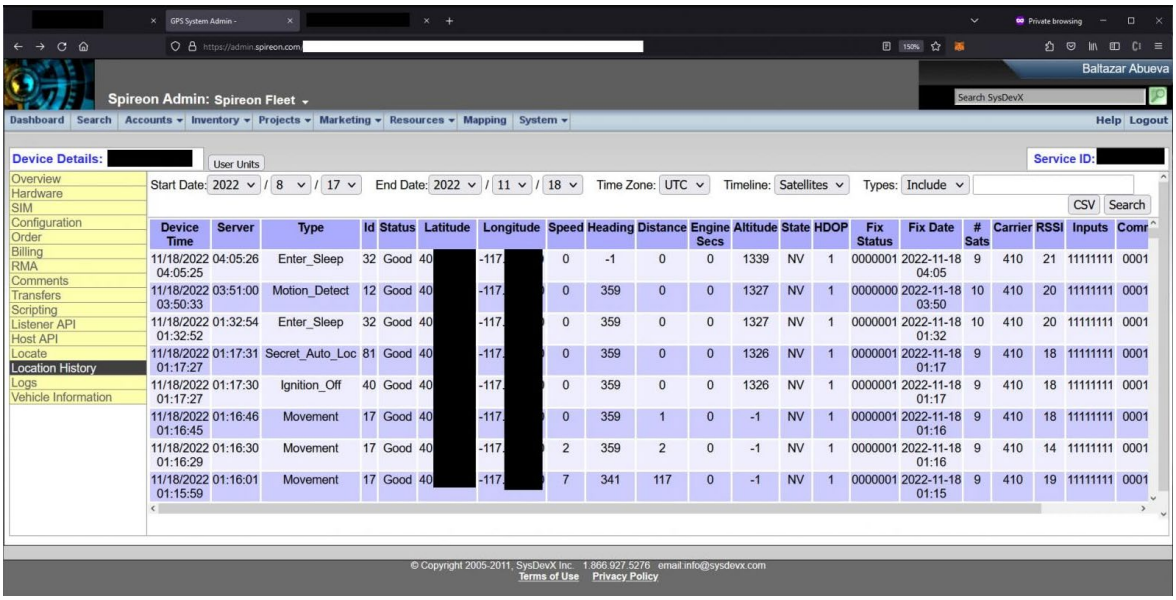
Disclosing Ferrari user data details
Source: Sam Curry

Tracking vehicle GPS

These vulnerabilities could have also allowed hackers to track cars in real time, introducing potential physical risks and impacting the privacy of millions of car owners.

Porsche was one of the impacted brands, with flaws in its telematic systems enabling attackers to retrieve vehicle locations and send commands.

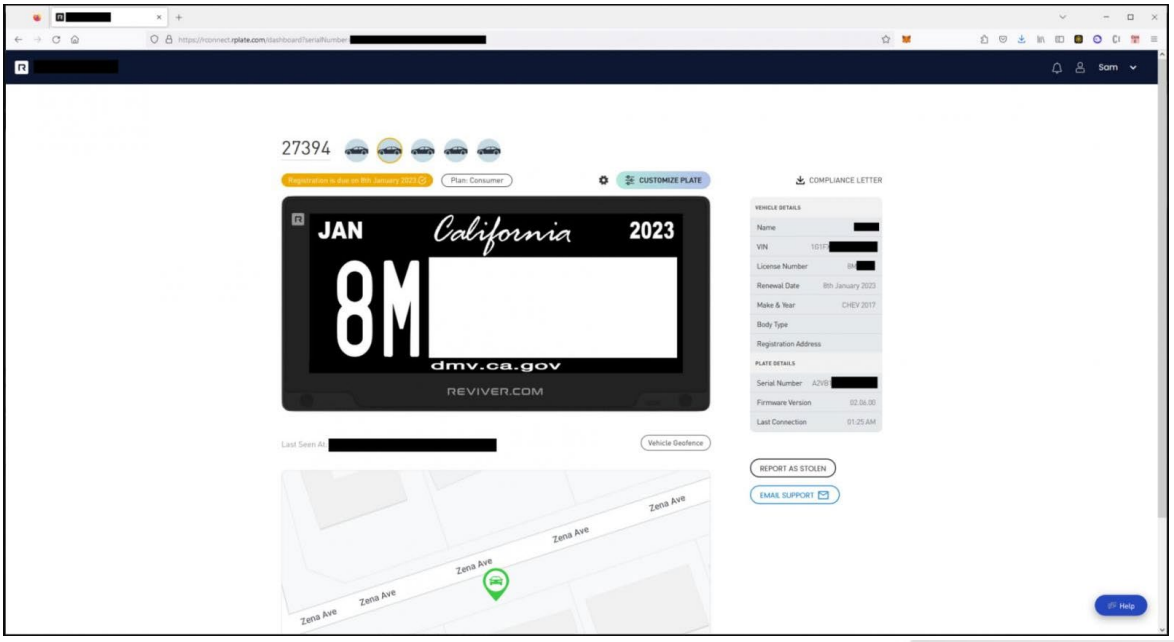
GPS tracking solution Spireon was also vulnerable to car location disclosure, impacting 15.5 million vehicles using its services and even letting full administration access to its remote management panel, enabling attackers to unlock cars, start the engine, or disable the starter.



Historic GPS data on the Spireon admin panel
Source: Sam Curry

The third impacted entity is Reviver, a digital license plate maker that was vulnerable to unauthenticated, remote access to its admin panel that could have given anyone access to GPS data and user records, the ability to change license plate messaging, and more.

Curry illustrates how these flaws allowed them to mark a vehicle as "STOLEN" on the Reviver panel, which would automatically inform the police about the incident, putting the owner/driver at unnecessary risk.



Modifying Reviver plates remotely
Source: Sam Curry

Minimizing exposure

Car owners can protect themselves from these types of vulnerabilities by limiting the amount of personal information stored in vehicles or mobile companion apps.

It is also essential to set in-car telematics to the most private mode available and read privacy policies to understand how data is being used.

Sam Curry also shared the following advice with BleepingComputer that owners should follow when purchasing a car.

"When purchasing a used car, make sure that the prior owner's account has been removed. Use strong passwords and set up 2FA (two-factor authentication) if possible for apps and services which link to your vehicle," warned Curry in a statement to BleepingComputer.

Update 1/4 - A Spireon spokesperson has sent BleepingComputer the following comment:

> *Our cybersecurity professionals met with the security researcher to discuss and evaluate the purported system vulnerabilities and immediately implemented remedial measures to the extent required.*
>
> *We also took proactive steps to further strengthen the security across our product portfolio as part of our continuing commitment to our customers as a leading provider of aftermarket telematics solutions.*
>
> *Spireon takes all security matters seriously and utilizes an extensive industry leading toolset to monitor and scan its products and services for both known and novel potential security risks.*

Update 1/11 - A Reviver spokesperson has sent BleepingComputer the following comment:

> *We were recently contacted by a cybersecurity researcher regarding potential application vulnerabilities in the auto industry. Our team immediately investigated this report, met with the researcher, and, out of an abundance of caution, engaged leading data security and privacy professionals to assist.*
>
> *We are proud of our team's quick response, which patched our application in under 24 hours and took further measures to prevent this from occurring in the future.*
>
> *Our investigation confirmed that this potential vulnerability has not been misused. Customer information has not been affected, and there is no evidence of ongoing risk related to this report.*

As part of our commitment to data security and privacy, we also used this opportunity to identify and implement additional safeguards to supplement our existing, significant protections.

Cybersecurity is central to our mission to modernize the driving experience and we will continue to work with industry-leading professionals, tools, and systems to build and monitor our secure platforms for connected vehicles.

Source: https://www.bleepingcomputer.com/news/security/toyota-mercedes-bmw-api-flaws-exposed-owners-personal-info/

8. 200 million Twitter users' email addresses allegedly leaked online

A data leak described as containing email addresses for over 200 million Twitter users has been published on a popular hacker forum for about $2. BleepingComputer has confirmed the validity of many of the email addresses listed in the leak.

Since July 22nd, 2022, threat actors and data breach collectors have been selling and circulating large data sets of scraped Twitter user profiles containing both private (phone numbers and email addresses) and public data on various online hacker forums and cybercrime marketplaces.

These data sets were created in 2021 by exploiting a Twitter API vulnerability that allowed users to input email addresses and phone numbers to confirm whether they were associated with a Twitter ID.

The threat actors then used another API to scrape the public Twitter data for the ID and combined this public data with private email addresses/phone numbers to create profiles of Twitter users.

Though Twitter fixed this flaw in January 2022, multiple threat actors have recently begun to leak the data sets they collected over a year ago for free.

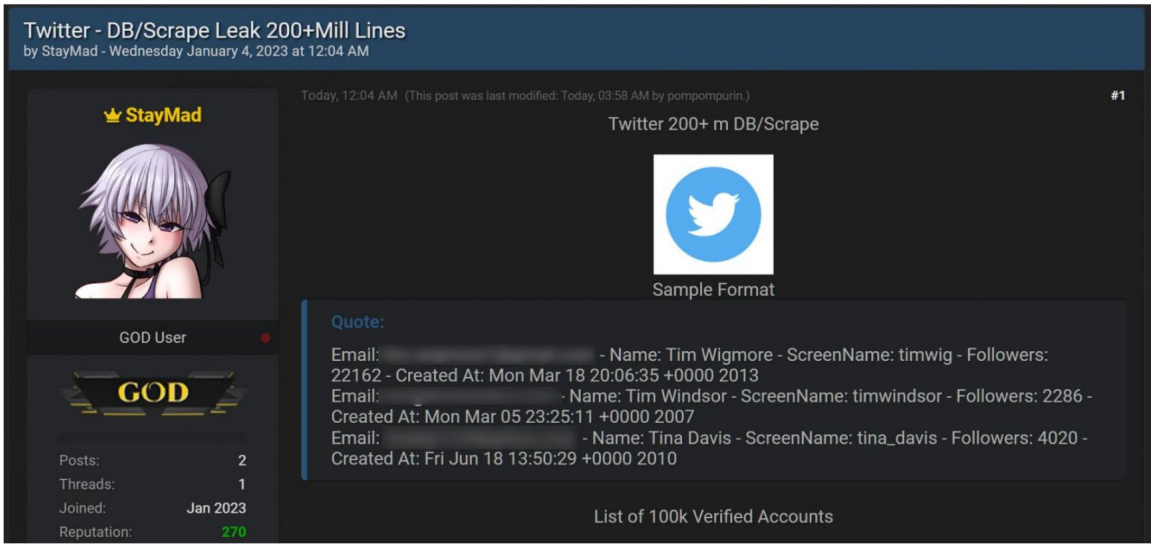
The first data set of 5.4 million users was put up for sale in July for $30,000 and ultimately released for free on November 27th, 2022. Another data set allegedly containing the data for 17 million users was also circulating privately in November.

More recently, a threat actor began selling a data set that they claimed contained 400 million Twitter profiles collected using this vulnerability.

200 million lines of Twitter profiles released for free

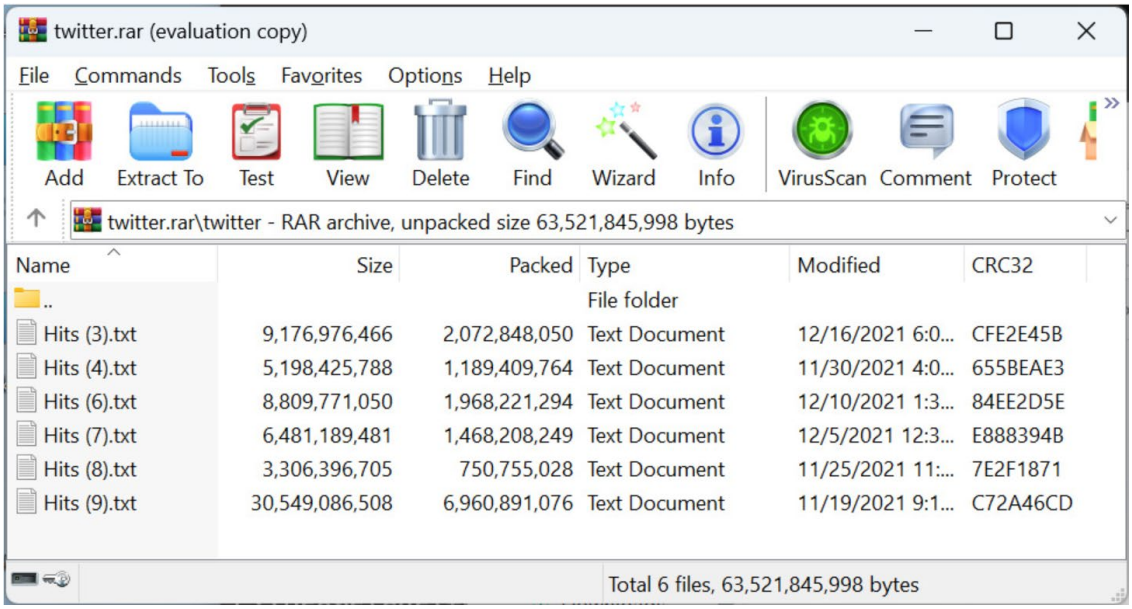
Today, a threat actor released a data set consisting of 200 million Twitter profiles on the Breached hacking forum for eight credits of the forum's currency, worth approximately $2.

This data set is allegedly the same as the 400 million set circulating in November but cleaned up to not contain duplicates, reducing the total to around 221,608,279 lines. However, BleepingComputer's tests have also confirmed duplicates in this latest leaked data.



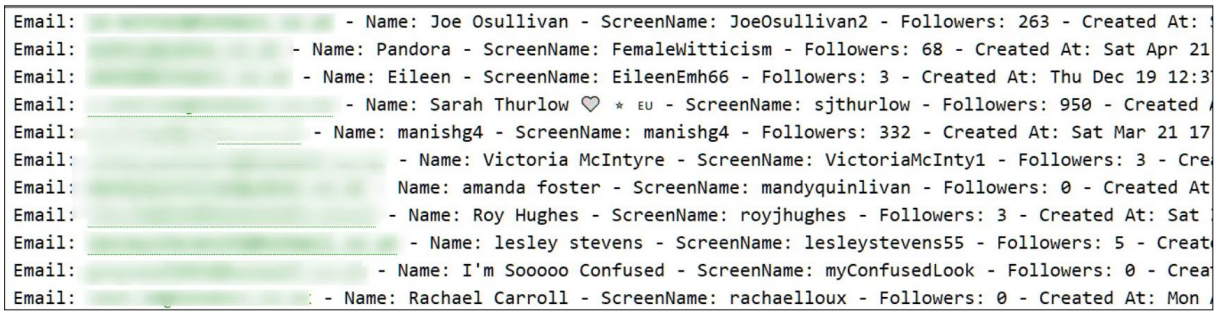
The initial sale of Facebook data in June 2020
Source: BleepingComputer

The data was released as a RAR archive consisting of six text files for a combined size of 59 GB of data.



RAR archive containing leaked Twitter data
Source: BleepingComputer

Each line in the files represents a Twitter user and their data, which includes email addresses, names, screen names, follow counts, and account creation dates, as shown below.



Sample of leaked Twitter data
Source: BleepingComputer

Unlike previously leaked data collected using this Twitter API flaw, today's leak does not indicate whether an account is verified.

While BleepingComputer has been able to confirm that the email addresses are correct for many of the listed Twitter profiles, the full data set has obviously not been confirmed.

Furthermore, the data set is far from complete, as there were many users who were not found in the leak.

Whether or not your information is in this data set highly depends on whether your email address was exposed in previous data breaches.

In 2021, the threat actors created massive lists of email addresses and phone numbers that were exposed in previous data breaches.

The scrapers then fed these lists into the API bug to see if your number or email address was associated with a corresponding Twitter ID with the email or phone number.

If your email address is only used at Twitter or was not in many data breaches, it would not have been fed into the API bug and added to this data set.

BleepingComputer has contacted Twitter regarding this leaked data but has not received a response to this or our previous emails.

Is your email in the leak?

Data breach notification service Have I Been Pwned (HIBP) has added the Twitter data leak to its system and has begun notifying subscribers if their email was found in the data set.

Troy Hunt, the creator of HIBP, told BleepingComputer that there is a total of 211,524,284 unique email addresses in the leak, down from the original number of 221,608,279 lines.

To check if your email is part of the Twitter leak, you can visit Have I Been Pwned and search with your email. If your email is part of the leak, HIBP will notify you with the list of detected data breaches, including the Twitter one, shown below.

Have I Been Pwned result for the 200 million user Twitter leak
Source: BleepingComputer

What should you do if your listed?

Even though this data leak only contains email addresses, it could be used by threat actors to conduct phishing attacks against accounts, especially verified ones.

Verified accounts with large followers are highly valued as they are often used to steal cryptocurrency through online scams.

This leak is also a significant privacy concern, especially for Twitter users who tweet anonymously. With this leak, it may be possible to identify anonymous Twitter users and expose their real identities.

All Twitter users should be on the lookout for targeted phishing scams that attempt to steal your passwords or other sensitive information.

Unfortunately, if you are concerned about your identity being revealed by a leaked email address, there is not much you can do.

Update 1/5/23: Twitter users can now search on Have I Been Pwned to see if they are in the leak.

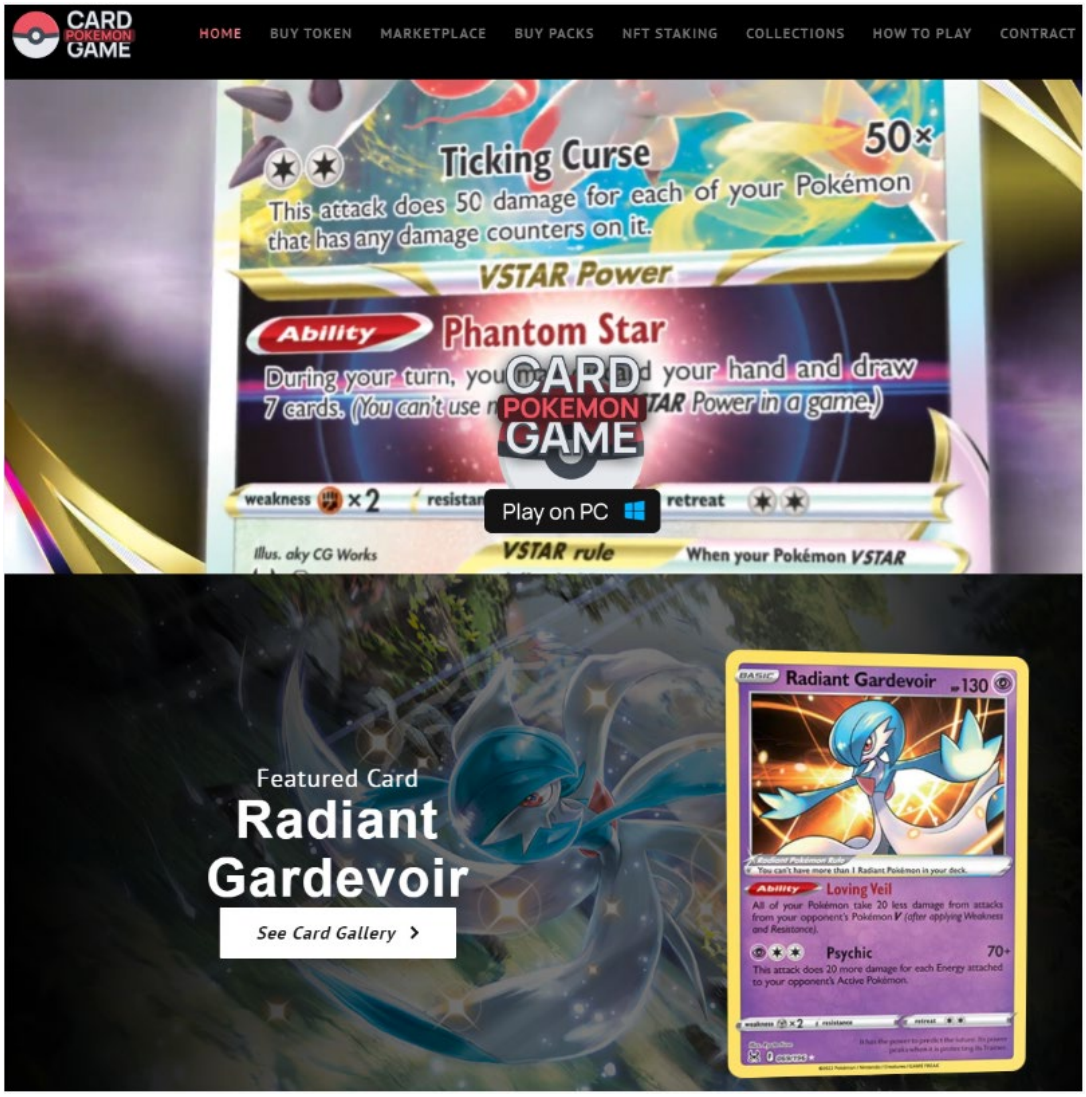
Source: https://www.bleepingcomputer.com/news/security/200-million-twitter-users-email-addresses-allegedly-leaked-online/

9. Hackers push fake Pokemon NFT game to take over Windows devices

Threat actors are using a well-crafted Pokemon NFT card game website to distribute the NetSupport remote access tool and take control over victims' devices.

The website "pokemon-go[.]io," which is still online at the time of writing, claims to be home to a new NFT card game built around the Pokemon franchise, offering users strategic fun together with NFT investment profits.

Considering the popularity of both Pokemon and NFTs, it shouldn't be hard for the operators of the malicious portal to draw an audience to the site through malspam, social media posts, etc.



Site promoting a fake Pokemon NFT game (BleepingComputer)

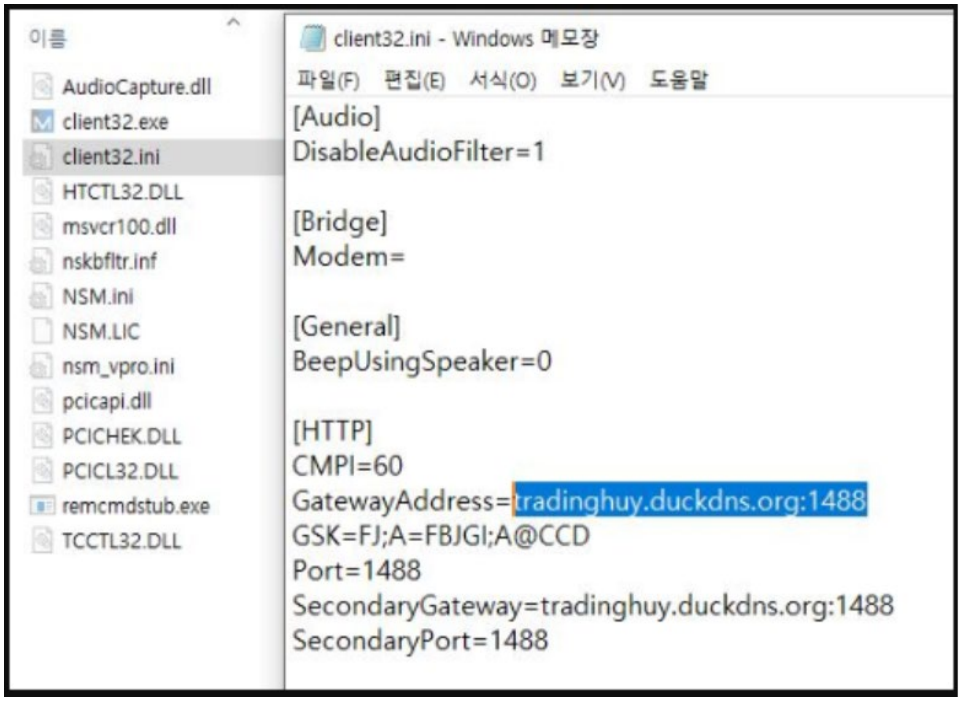
Those who click on the "Play on PC" button download an executable that looks like a legitimate game installer but, in reality, installs the NetSupport remote access tool (RAT) on the victim's system.

The operation was uncovered by analysts at ASEC, who reports there was also a second site used in the campaign, at "beta-pokemoncards[.]io," but it has since been taken offline.

This campaign's first signs of activity appeared in December 2022, while earlier samples retrieved from VirusTotal showed that the same operators pushed a fake Visual Studio file instead of the Pokemon game.

Dropping the NetSupport RAT

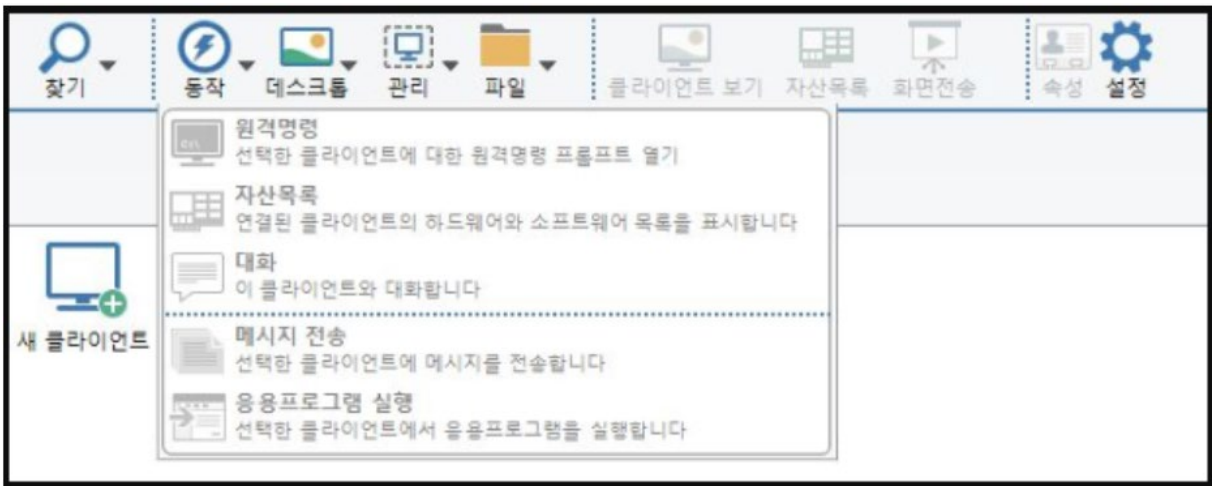
The NetSupport RAT executable ("client32.exe") and its dependencies are installed in a new folder in the %APPDATA% path. They are set to "hidden" to help evade detection from victims performing manual inspections on the file system.



Dropped files and contents of the configuration file (ASEC)

Moreover, the installer creates an entry in the Windows Startup folder to ensure the RAT will execute upon system boot.

As NetSupport RAT (NetSupport Manager) is a legitimate program, threat actors commonly use it in the hopes it will evade security software.



NetSupport RAT interface (ASEC)

The threat actors can now remotely connect to a user's device to steal data, install other malware, or even attempt to spread further on the network.

While NetSupport Manager is a legitimate software product, it is commonly used by threat actors as part of their malicious campaigns.

In 2020, Microsoft warned about phishing actors using COVID-19-themed Excel files that dropped NetSupport RAT onto the recipients' computers.

In August 2022, a campaign targeting WordPress sites with fake Cloudflare DDoS protection pages installed NetSupport RAT and Raccoon Stealer on victims.

NetSupport Manager supports remote screen control, screen recording, system monitoring, remote system grouping for better control, and plenty of connectivity options, including network traffic encryption.

That said, the consequences of such an infection are broad and severe, mainly concerning unauthorized access to sensitive user data and downloading further malware.

Source: https://www.bleepingcomputer.com/news/security/hackers-push-fake-pokemon-nft-game-to-take-over-windows-devices/

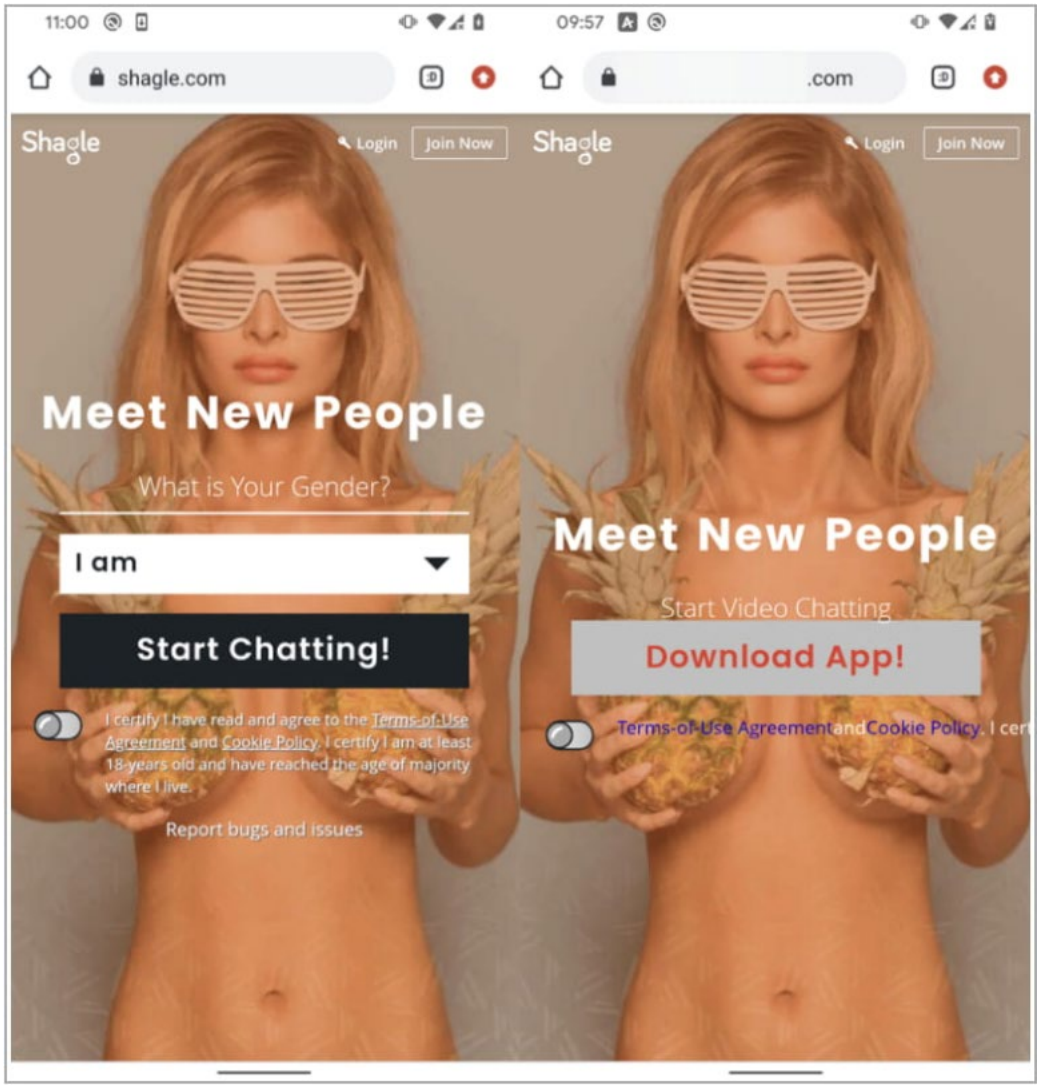
10. StrongPity hackers target Android users via trojanized Telegram app

The StrongPity APT hacking group is distributing a fake Shagle chat app that is a trojanized version of the Telegram for Android app with an added backdoor.

Shagle is a legitimate random-video-chat platform allowing strangers to talk via an encrypted communications channel. However, the platform is entirely web-based, not offering a mobile app.

StrongPity has been found using a fake website since 2021 that impersonates the actual Shagle site to trick victims into downloading a malicious Android.

Once installed, this app enables the hackers to conduct espionage on the targeted victims, including monitoring phone calls, collecting SMS texts, and grabbing contact lists.



The real site is on the left. The fake site is on the right
Source: ESET

StrongPity, also known as Promethium or APT-C-41, was previously attributed to a campaign that distributed trojanized Notepad++ installers and malicious versions of WinRAR and TrueCrypt to infect targets with malware.

The latest StrongPity activity was discovered by ESET researchers who attributed the campaign to the espionage APT group based on code similarities with past payloads.

Additionally, the Android app is signed with the same certificate the APT used to sign an app that mimicked the Syrian e-gov Android application in a 2021 campaign.

Trojanizing the Android Telegram app

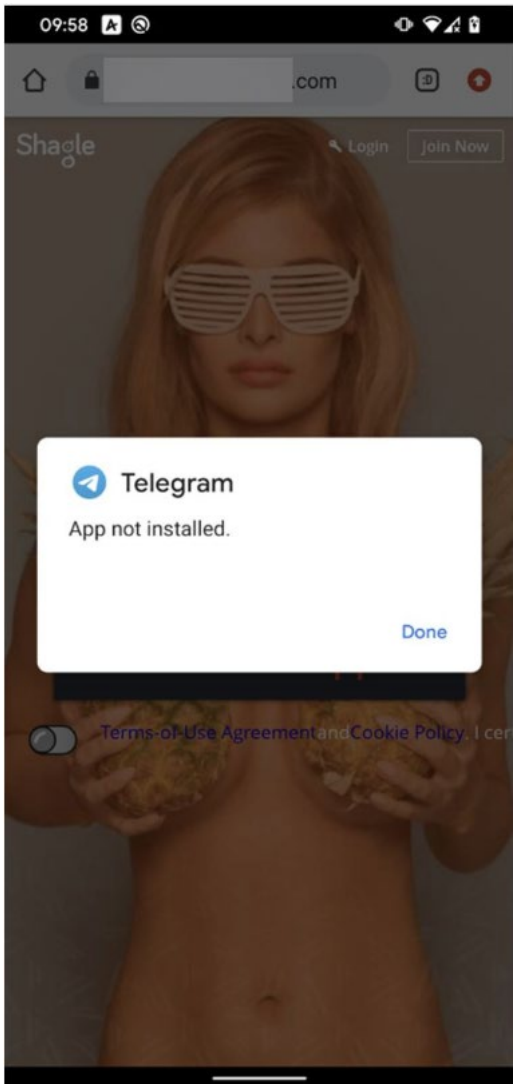
The malicious Android application distributed by StrongPity is an APK file named "video.apk," the standard Telegram v7.5.0 (February 2022) app modified to impersonate a Shagle mobile app.

ESET couldn't determine how victims arrive on the fake Shagle website, but it's likely through spear phishing emails, smishing (SMS phishing), or instant messages on online platforms.

The malicious APK is provided directly from the fake Shagle site and has never been made available on Google Play.

ESET says the cloned site first appeared online on November 2021, so the APK has likely been under active distribution since then. However, the first confirmed detection in the wild came in July 2022.

One drawback of using Telegram as the basis for the hacking group's fake app is that if the victim already has the real Telegram app installed on their phones, the backdoored version won't be installed.



Malicious app won't install as Telegram installed already
Source: ESET

Currently, the API ID used in the captured samples has been limited due to overuse, so the trojanized app will no longer accept new user registrations; hence, the backdoor won't work.

ESET believes this indicates that StrongPity has successfully deployed the malware on targeted victims.

Backdoor designed to spy on victims

Upon installation, the malware requests access to Accessibility Service and then fetches an AES-encrypted file from the attacker's command and control server.

This file consists of 11 binary modules extracted to the device and used by the backdoor to perform various malicious functionality.

```
kali:/data/data/org.telegram.messenger/files/.li # ls -l
total 86
drwxrwxrwt 2 u0_a1003 u0_a1003 3488 2022-07-21 15:26 __MACOSX
-rwxrwxrwt 1 u0_a1003 u0_a1003 5007 2022-07-21 15:26 libarm.jar
-rwxrwxrwt 1 u0_a1003 u0_a1003 3466 2022-07-21 15:26 libmpeg4.jar
-rwxrwxrwt 1 u0_a1003 u0_a1003 9081 2022-07-21 15:26 local.jar
drwxrwxrwt 2 u0_a1003 u0_a1003 3488 2022-07-21 15:27 oat
-rwxrwxrwt 1 u0_a1003 u0_a1003 4415 2022-07-21 15:26 phone.jar
-rwxrwxrwt 1 u0_a1003 u0_a1003 4205 2022-07-21 15:26 resources.jar
-rwxrwxrwt 1 u0_a1003 u0_a1003 5868 2022-07-21 15:26 services.jar
-rwxrwxrwt 1 u0_a1003 u0_a1003 6761 2022-07-21 15:26 systemui.jar
-rwxrwxrwt 1 u0_a1003 u0_a1003 3215 2022-07-21 15:26 timer.jar
-rwxrwxrwt 1 u0_a1003 u0_a1003 5607 2022-07-21 15:26 toolkit.jar
-rwxrwxrwt 1 u0_a1003 u0_a1003 3643 2022-07-21 15:26 watchkit.jar
-rwxrwxrwt 1 u0_a1003 u0_a1003 4220 2022-07-21 15:26 wearkit.jar
```

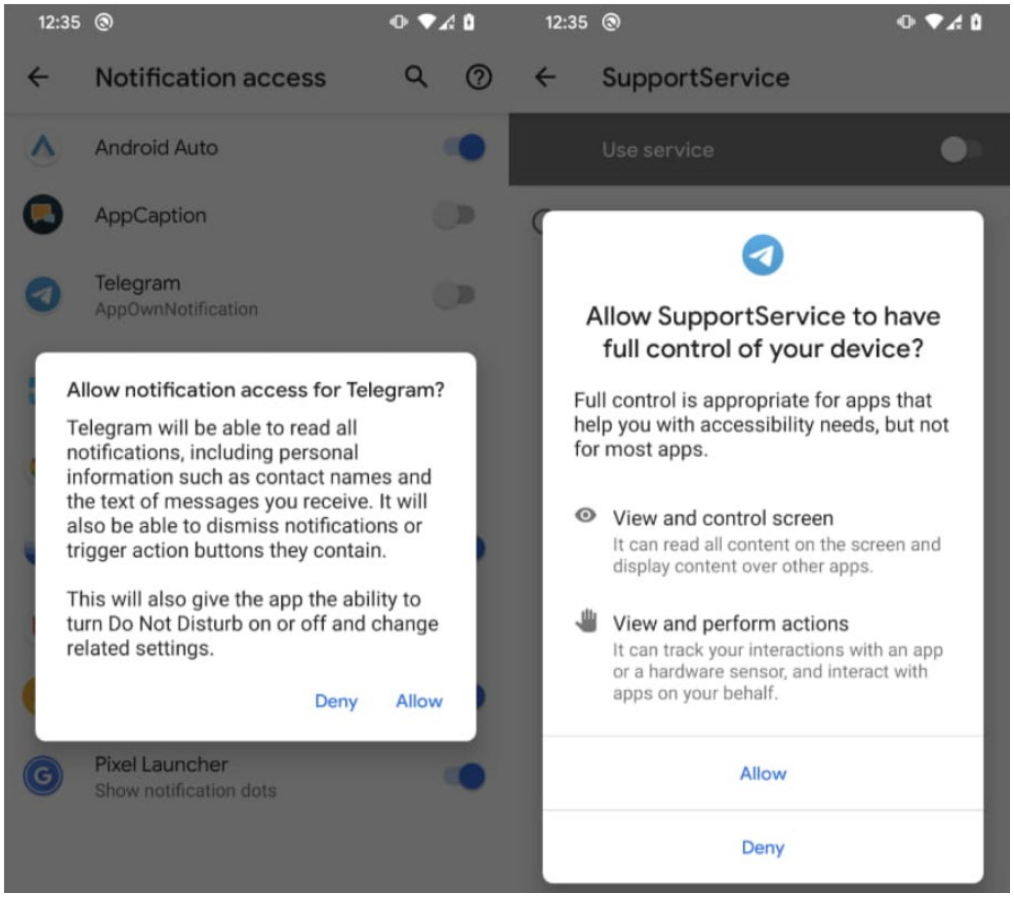
The 11 modules fetched from the C2
Source: ESET

Each module performs an espionage function and is triggered as needed. The complete list of the malicious spyware modules is listed below:

- libarm.jar – records phone calls
- libmpeg4.jar – collects text of incoming notification messages from 17 apps
- local.jar – collects file list (file tree) on the device
- phone.jar – misuses accessibility services to spy on messaging apps by exfiltrating contact name, chat message, and date
- resources.jar – collects SMS messages stored on the device
- services.jar – obtains device location
- systemui.jar – collects device and system information
- timer.jar – collects a list of installed apps
- toolkit.jar – collects contact list
- watchkit.jar – collects a list of device accounts
- wearkit.jar – collects a list of call logs

The gathered data is stored in the app's directory, encrypted with AES, and eventually sent back to the attacker's command and control server.

By abusing the Accessibility Service, the malware can read notification content from Messenger, Viber, Skype, WeChat, Snapchat, Tinder, Instagram, Twitter, Gmail, and more.



Trojan app requesting dangerous permissions
Source: ESET

In rooted devices where the regular user has administrator privileges, the malware automatically grants itself permission to perform changes on security settings, write on the filesystem, perform reboots, and perform other dangerous functions.

The StrongPity hacking group has been active since 2012, commonly hiding backdoors in legitimate software installers. Based on ESET's report, the threat actor continues to employ the same tactic after a decade.

Android users should be cautious with APKs sourced outside Google Play and pay attention to permission requests while installing new apps.

Source: https://www.bleepingcomputer.com/news/security/strongpity-hackers-target-android-users-via-trojanized-telegram-app/

11. ChatGPT-Written Malware

I don't know how much of a thing this will end up being, but we are seeing ChatGPT-written malware in the wild.

> …within a few weeks of ChatGPT going live, participants in cybercrime forums—some with little or no coding experience—were using it to write software and emails that could be used for espionage, ransomware, malicious spam, and other malicious tasks.
>
> "It's still too early to decide whether or not ChatGPT capabilities will become the new favorite tool for participants in the Dark Web," company researchers wrote. "However, the cybercriminal community has already shown significant interest and are jumping into this latest trend to generate malicious code."
>
> Last month, one forum participant posted what they claimed was the first script they had written and credited the AI chatbot with providing a "nice [helping] hand to finish the script with a nice scope."
>
> The Python code combined various cryptographic functions, including code signing, encryption, and decryption. One part of the script generated a key using elliptic curve cryptography and the curve ed25519 for signing files. Another part used a hard-coded password to encrypt system files using the Blowfish and Twofish algorithms. A third used RSA keys and digital signatures, message signing, and the blake2 hash function to compare various files.

Check Point Research report.

ChatGPT-generated code isn't that good, but it's a start. And the technology will only get better. Where it matters here is that it gives less skilled hackers—script kiddies—new capabilities.

Source: https://www.schneier.com/blog/archives/2023/01/chatgpt-written-malware.html

12. Over 1,300 fake AnyDesk sites push Vidar info-stealing malware

A massive campaign using over 1,300 domains to impersonate the official AnyDesk site is underway, all redirecting to a Dropbox folder recently pushing the Vidar information-stealing malware.

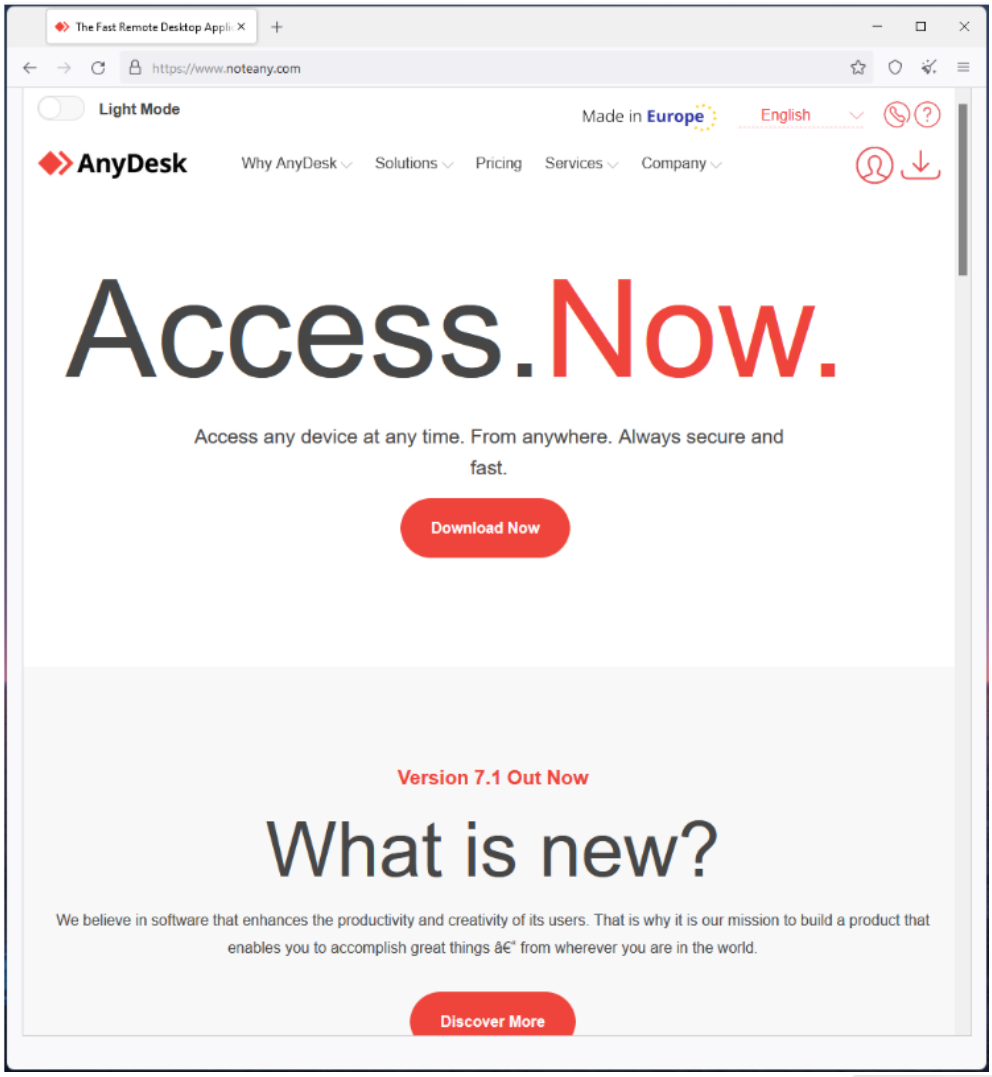
AnyDesk is a popular remote desktop application for Windows, Linux, and macOS, used by millions of people worldwide for secure remote connectivity or performing system administration.

Due to the tool's popularity, malware distribution campaigns often abuse the AnyDesk brand. For example, in October 2022, Cyble reported that the operators of Mitsu Stealer were using an AnyDesk phishing site to push their new malware.

The new ongoing AnyDesk campaign was spotted by SEKOIA threat analyst crep1x, who warned about it on Twitter and shared the complete list of the malicious hostnames. All of these hostnames resolve to the same IP address of 185.149.120[.]9.

The list of the hostnames includes typosquats for AnyDesk, MSI Afterburner, 7-ZIP, Blender, Dashlane, Slack, VLC, OBS, cryptocurrency trading apps, and other popular software.

However, regardless of the name, they all lead to the same AnyDesk clone site, shown below.



Fake AnyDesk site used in Vidar distribution (BleepingComputer)

At the time of writing this, most domains are still online, while others have been reported and taken offline by the registrars or are blocked by AV tools. Even for the sites that are up, their Dropbox links no longer work after the malicious file was reported to the cloud storage service.

However, as this campaign all point to the same site, the threat actor can easily fix this by updating the download URL to another site.

All sites lead to Vidar Stealer

In the newly discovered campaign, the sites were distributing a ZIP file named 'AnyDeskDownload.zip' [VirusTotal] that pretended to be an installer for the AnyDesk software.

However, instead of installing the remote access software, it installs Vidar stealer, an information-stealing malware circulating since 2018.

When installed, the malware will steal victims' browser history, account credentials, saved passwords, cryptocurrency wallet data, banking information, and other sensitive data. This data is then sent back to the attackers, who could use it for further malicious activity or sell it to other threat actors.

Instead of hiding the malware payload behind redirections to evade detection and takedowns, the recent Vidar campaign used the Dropbox file hosting service, which is trusted by AV tools, to deliver the payload.

BleepingComputer has recently seen Vidar being pushed by a campaign relying on over 200 typosquatting domains that impersonated 27 software brands.

Another campaign pushing Vidar via Google Ads abuse was spotted by Guardio Labs at the end of December 2022, also abusing the AnyDesk brand among others.

A few days ago, SEKOIA published a report revealing another massive info-stealer distribution campaign using 128 websites that promote cracked software.

Users typically end up on these sites after searching Google for pirated versions of software and games. They are then led to 108 second-stage domains that redirect them to the final destination of 20 domains that deliver the malicious payloads.

However, as the researcher told BleepingComputer, there's no overlap between the two campaigns.

Users are advised to bookmark the sites they use for downloading software, avoid clicking on promoted results (ads) in Google Search, and find the official URL of a software project from their Wikipedia page, documentation, or your OS's package manager.

Source: https://www.bleepingcomputer.com/news/security/over-1-300-fake-anydesk-sites-push-vidar-info-stealing-malware/

13. Twitter claims leaked data of 200M users not stolen from its systems

Twitter finally addressed reports that a dataset of email addresses linked to hundreds of millions of Twitter users was leaked and put up for sale online, saying that it found no evidence the data was obtained by exploiting a vulnerability in its systems.

"In response to recent media reports of Twitter users' data being sold online, we conducted a thorough investigation and there is no evidence that data recently being sold was obtained by exploiting a vulnerability of Twitter systems," the company said.

In August, the company confirmed that a data leak impacting 5.4 million Twitter users resulted from threat actors exploiting a vulnerability fixed in January 2022.

This flaw enabled the attackers to link email addresses and phone numbers to Twitter users' accounts.

Today, Twitter said that another dataset containing email addresses linked to 200 million Twitter users that reportedly got leaked online earlier this month was not obtained by exploiting the vulnerability patched in January 2022.

"[The] 200 million dataset could not be correlated with the previously reported incident or any data originating from an exploitation of Twitter systems," Twitter said.

"None of the datasets analyzed contained passwords or information that could lead to passwords being compromised."

The company added that "based on information and intel analyzed to investigate the issue, there is no evidence that the data being sold online was obtained by exploiting a vulnerability of Twitter systems. The data is likely a collection of data already publicly available online through different sources."

However, Twitter failed to explain in today's statement how the Twitter users' leaked data was accurately linked to email addresses associated with their accounts.

Twitter added that it's currently in contact with Data Protection Authorities and other relevant data regulator bodies in multiple countries to provide additional details regarding the "alleged incidents."

In December 2022, the Irish Data Protection Commission (DPC) announced that it launched an inquiry and "raised queries in relation to GDPR compliance" following news reports that the personal information of 5.4 million Twitter users was leaked online.

Two years before, in December 2020, the DPC fined Twitter €450,000 (~$550,000) after it failed to notify the data watchdog of a breach within the 72-hour timeframe required by EU's General Data Protection Regulation (GDPR).

Source: https://www.bleepingcomputer.com/news/security/twitter-claims-leaked-data-of-200m-users-not-stolen-from-its-systems/

14. Royal Mail cyberattack linked to LockBit ransomware operation

A cyberattack on Royal Mail, UK's largest mail delivery service, has been linked to the LockBit ransomware operation.

Yesterday, the Royal Mail disclosed that they suffered a cyber incident that forced them to halt international shipping services.

"Royal Mail is experiencing severe service disruption to our international export services following a cyber incident," disclosed Royal Mail in a service update.

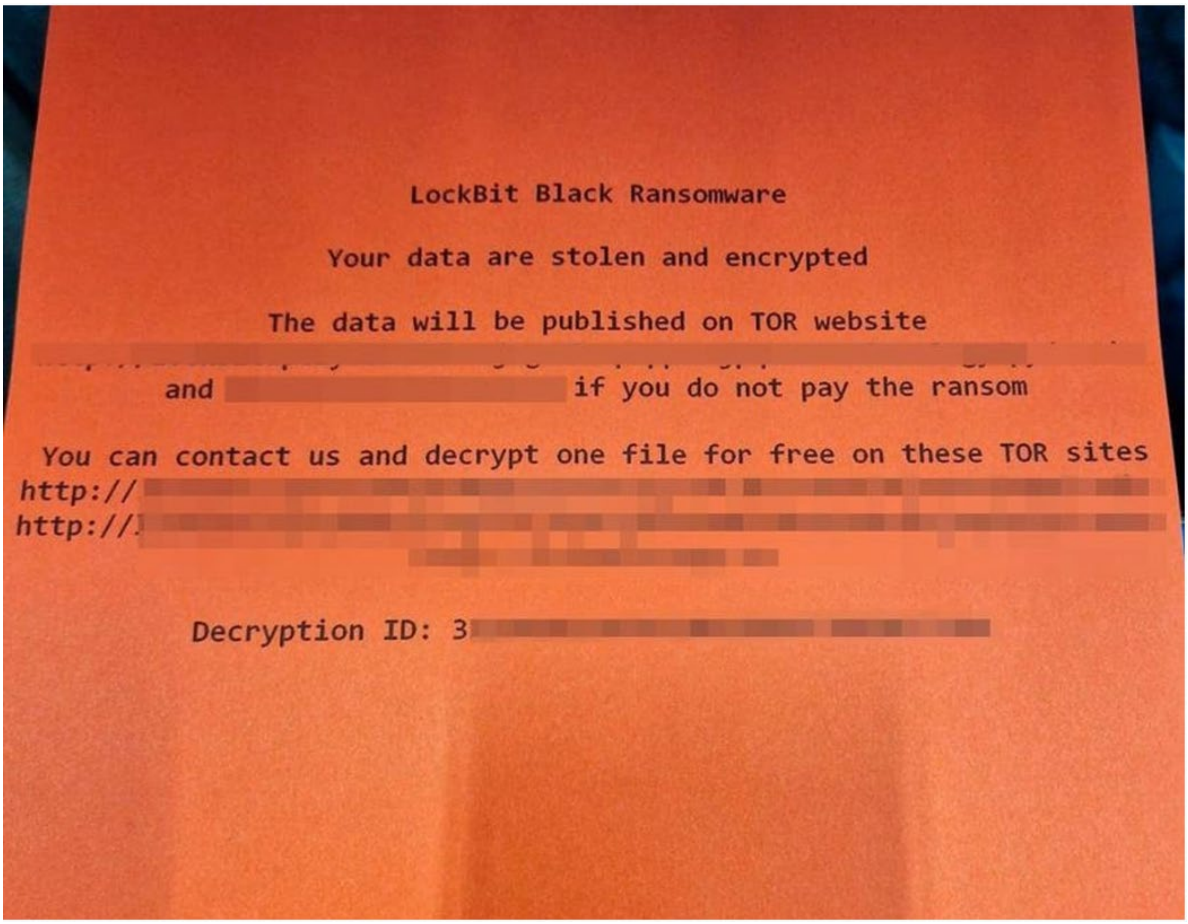
While Royal Mail did not provide any details on the cyberattack, they said they were working with external cybersecurity experts and have notified UK regulators and law enforcement.

LockBit ransomware encryptor used in the attack

As first reported by The Telegraph, the attack on Royal Mail is now confirmed to be a ransomware attack by the LockBit operation, or at least someone using their encryptors.

The Telegraph reports that the ransomware attack encrypted devices used for international shipping and caused ransom notes to be printed on printers used for customs dockets.

BleepingComputer has seen an unredacted version of the printed ransom notes and can confirm that they include the Tor websites for the LockBit ransomware operation.



LockBit 3.0 ransom note printed during Royal Mail cyberattack
Source: Daniel Card on Twitter

The ransom note states it was created by "LockBit Black Ransomware," which is the operation's latest encryptor name as it includes code and features from the now-shut down BlackMatter ransomware gang.

The note also contains multiple links to the LockBit ransomware operation's Tor data leak sites and negotiation sites, including a 'Decryption ID' required to log in to chat with the threat actors.

However, BleepingComputer has been told by multiple security researchers that this "Decryption ID" does not work.

It is unclear if the ransomware gang deleted the ID after news of the circulating ransom notes or if they moved negotiations to a new ID to avoid scrutiny by researchers and journalists.

BleepingComputer reached out to LockBitSupport, the public-facing representative of the ransomware operation, and was told that they did not attack Royal Mail and they blamed it on other threat actors using their leaked builder.

In September, the LockBit 3.0 ransomware builder was leaked on Twitter. This allowed other threat actors to launch ransomware operations based on the LockBit's encryptor.

LockBitSupp's explanation does not explain why Royal Mail's ransom notes included links to LockBit's Tor negotiation and data leak sites rather than the other threat actor's sites who are allegedly using the builder.

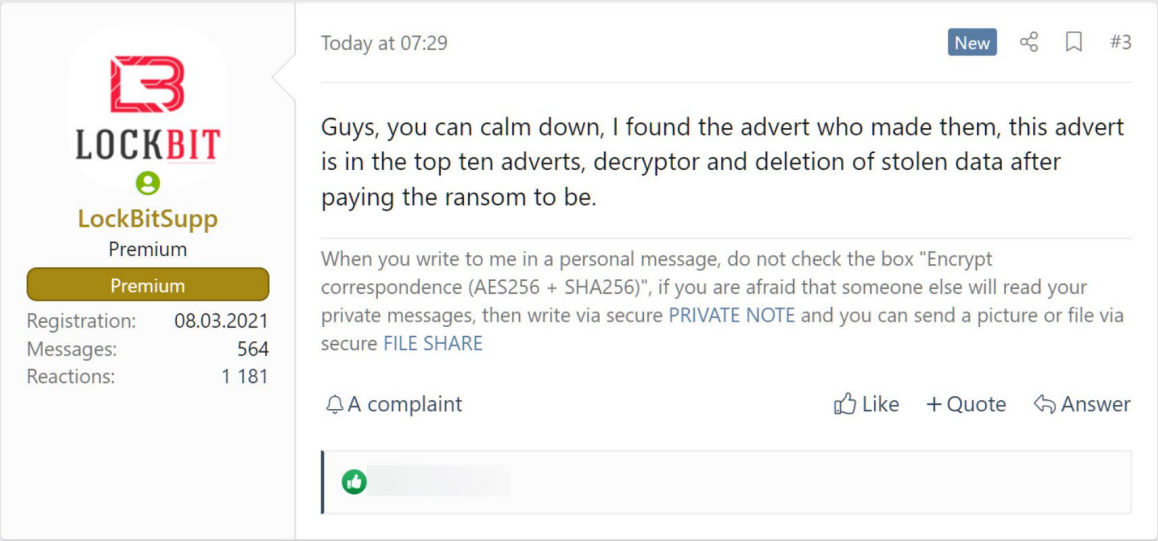
However, if LockBitSupp is telling the truth and other threat actors used the leaked builder in the attack, then it would mean this was likely a destructive attack rather than one for personal gain, as there is no way to contact the actual attackers.

Update 1/14/22 01:25 PM ET:

The LockBit operation has confirmed that it is behind the attack on Royal Mail in a post to a Russian-speaking hacking forum.

The ransomware operator known as LockBitSupp states that they determined which affiliate conducted the attack and will only provide a decryptor and delete stolen data after a ransom is paid.

"Guys, you can calm down, I found the advert who made them, this advert is in the top ten adverts, decryptor and deletion of stolen data after paying the ransom to be,"
LockBitSupp said in a translated posted to a hacking forum.



Post from LockBitsupp on a hacking forum
Source: BleepingComputer

While the LockBit representative implies that data was stolen in the cyberattack again Royal Mail, there is information on how much data was stolen and what it contains.

Source: https://www.bleepingcomputer.com/news/security/royal-mail-cyberattack-linked-to-lockbit-ransomware-operation/

15. TikTok slapped with $5.4 million fine over cookie opt-out feature

France's data protection authority (CNIL) has fined TikTok UK and TikTok Ireland €5,000,000 for making it difficult for users of the platform to refuse cookies and for not sufficiently informing them about their purpose.

This design behavior was deemed a violation of Article 82 of France's data protection laws (DPA), a national regulation that conforms with the GDPR (General Data Protection Regulation) framework enforced throughout Europe.

The €5 million fine was determined by the severity of the violations, including the number of impacted individuals, which include children, and the number of times CNIL had to repeat its warnings to TikTok on the need to adhere to France's Data Protection Act.

As CNIL explains in the announcement, it inspected the TikTok website in June 2021. It found that while the platform offered a button to allow users to immediately accept cookies, rejecting them wasn't as easy.

Instead, CNIL says users would have to perform several targeted clicks to refuse all cookies, which was discouraging, naturally leading to most visitors on the TikTok site clicking on the "Accept all" button.

Article 82 of France's DPA not only requires services to secure users' consent for the storage of cookies but also presupposes the users' freedom to give that consent. Hence, the cookie consent dialogs must offer a balanced approach to how the options are presented to the user, which wasn't the case on TikTok sites.

Despite CNIL's repeated warnings to TikTok, it took the company until February 2022 to implement a "Reject all" button and give it a prominent position in the cookie consent prompt.

The second violation, also a breach of Article 82 of the DPA, is the insufficient description of the objectives of the cookies on the banner. CNIL says users who clicked on the banner link to learn more still didn't get enough details about the purpose of the cookies.

It's worth noting that aggressive data collection strategies are common among major online platforms, which CNIL recently penalized with heavy fines, including Apple receiving an $8.5M fine, Facebook $68M, and Google $170M.

A TikTok spokesperson sent BleepingComputer the following comment regarding the CNIL fine:

> *"These findings relate to past practices that we addressed last year, including making it easier to reject non-essential cookies and providing additional information about the purposes of certain cookies.*
>
> *The CNIL itself highlighted our cooperation during the course of the investigation and user privacy remains a top priority for TikTok."*

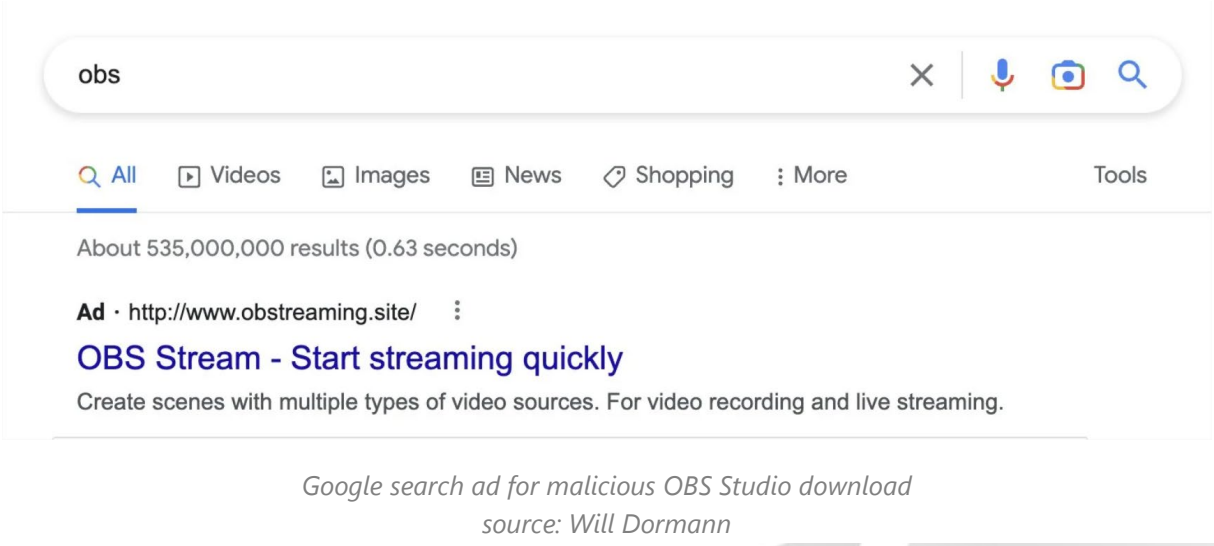
Source: https://www.bleepingcomputer.com/news/security/tiktok-slapped-with-54-million-fine-over-cookie-opt-out-feature/

16. Hackers turn to Google search ads to push info-stealing malware

Hackers are setting up fake websites for popular free and open-source software to promote malicious downloads through advertisements in Google search results.

At least one prominent user on the cryptocurrency scene has fallen victim to the campaign, claiming it allowed hacker hackers steal all their digital crypto assets along with control over their professional and personal accounts.

Over the weekend, crypto influencer Alex, better known by their online persona NFT God, was hacked after launching a fake executable for the Open Broadcaster Software (OBS) video recording and live streaming software they had downloaded from a Google ad in search results.



Google search ad for malicious OBS Studio download
source: Will Dormann

"Nothing happened when I clicked the EXE," Alex wrote in a Twitter thread recounting their experience over the weekend. However, a few hours later friends alerted them that their Twitter account had been hacked.

Unbeknownst to Alex, this was likely an information-stealing malware that stole their saved browser passwords, cookies, Discord tokens, and cryptocurrency wallets and sent them to a remote attacker.

Soon, Alex found that their account at the OpenSea NFT marketplace had also been compromised and a different wallet was listed as the owner of one of their digital assets.

"I knew at that moment it was all gone. Everything. All my crypto and NFTs ripped from me," NFT God says in the thread.

Soon, Alex discovered that their Substack, Gmail, Discord, and cryptocurrency wallets suffered the same fate and were controlled by the hackers.

Crypto influencer NFT God's online accounts hacked
source: NFT God

While this is not a new stratagem, threat actors appear to use it more often. In October last year, BleepingComputer reported on a massive campaign that relied on more than 200 typosquatting domains for over two dozen brands to mislead users.

The distribution method was unknown at the time but separate reports in December from cybersecurity companies Trend Micro and Guardio revealed that hackers were abusing the Google Ads platform to push malicious downloads in search results.

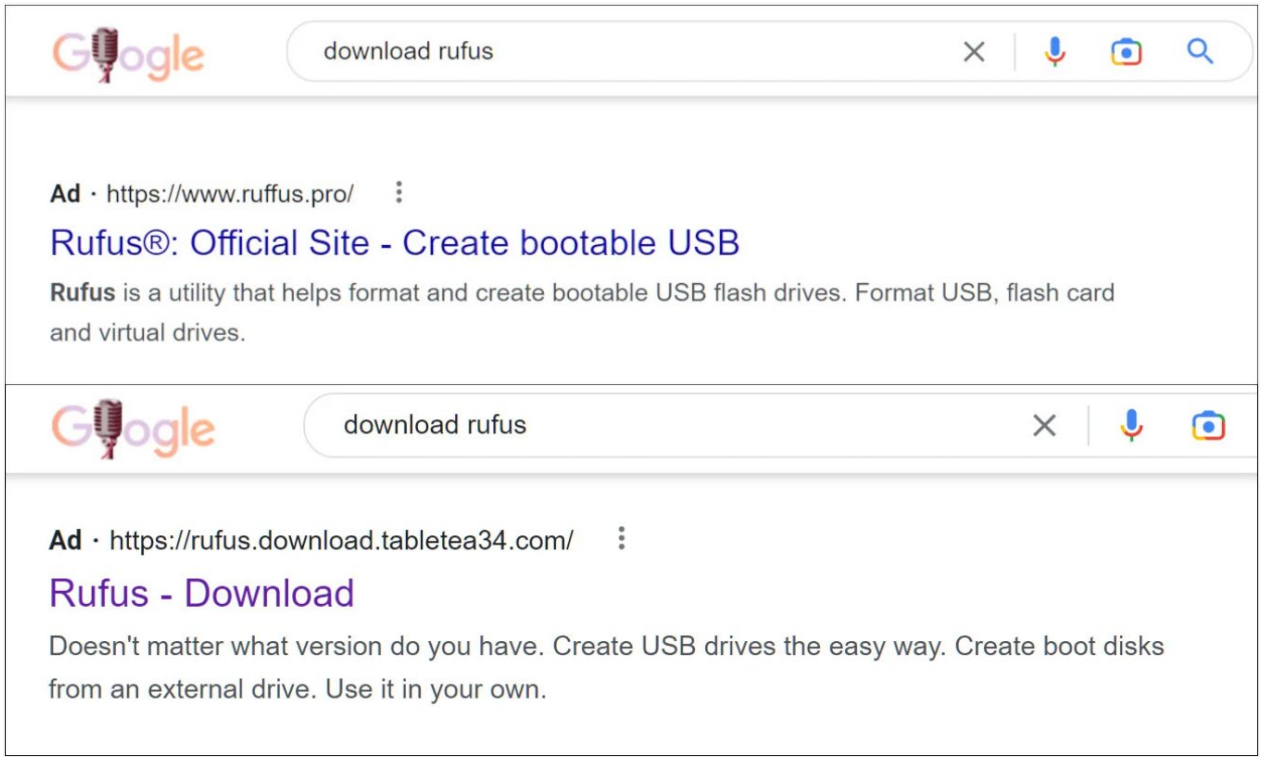
Flurry of malicious ads in Google search results

Following NFT God's thread, BleepingComputer conducted its own research and uncovered that OBS is one in a long list of software that threat actors impersonate to push malicious downloads in Google Ads search results.

One example we found is a Google Ad search result for Rufus, a free utility for creating bootable USB flash drives.

The threat actor registered domains that resemble the official one and copied the main part of the legitimate site up to the download section.

In one case, they used the generic top-level domain "pro," likely in an attempt to pique victim interest and attract with the promise of a wider set of program features.

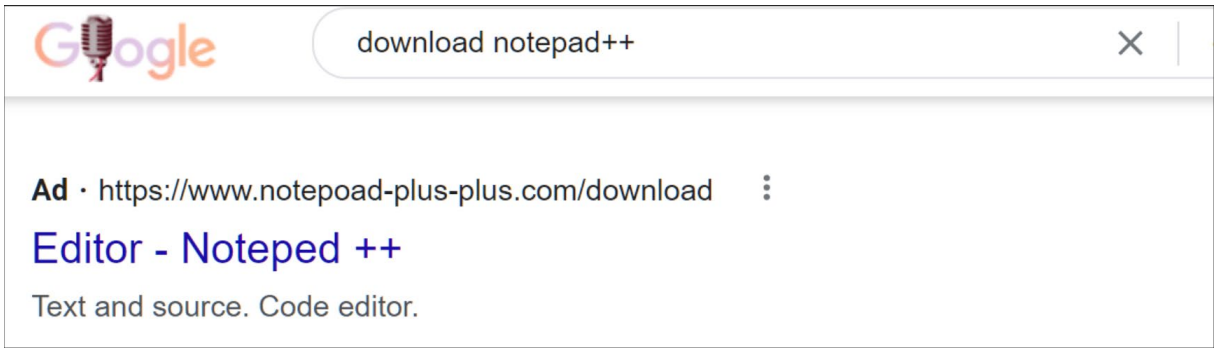


Malicious Rufus download pushed via ads in Google search results
source: BleepingComputer

To note, there is no advanced variant of Rufus. There is only one edition available as an installable or portable variant hosted on GitHub.

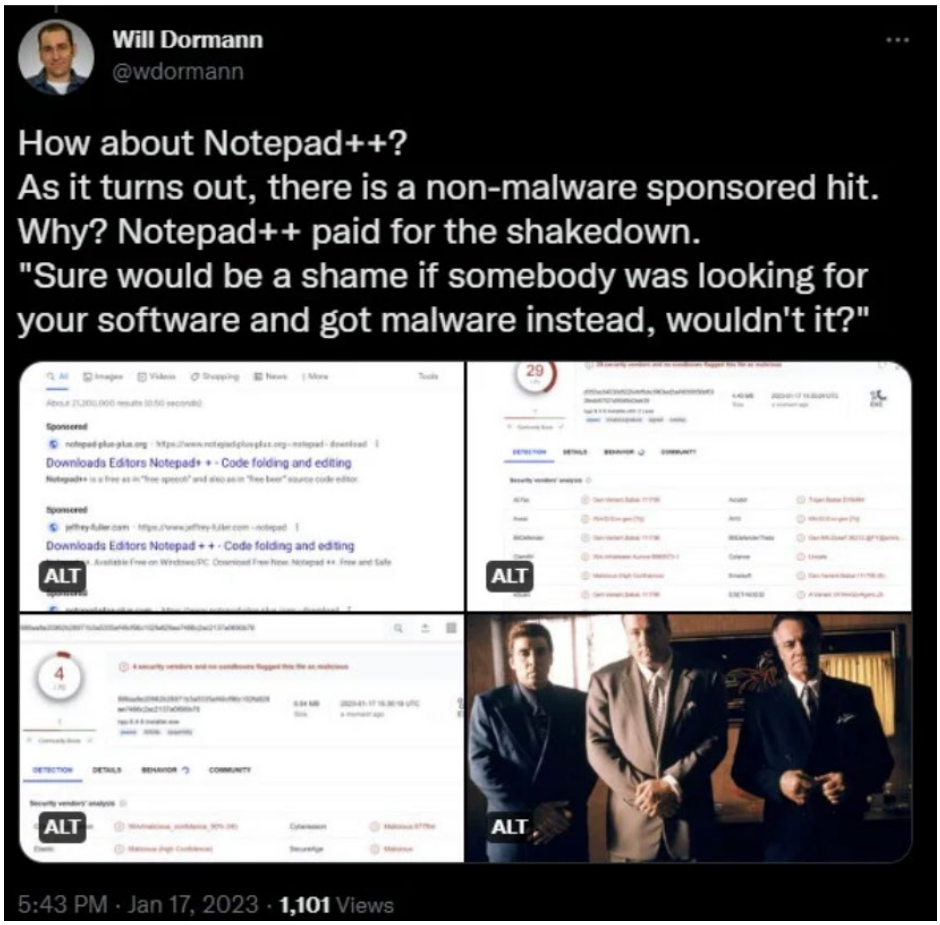
For the malicious version, the download goes to a file transfer service. Because it is an archive bomb, many antivirus engines do not detect it as a threat.

Another popular program impersonated is the text and source code editor Notepad++. The threat actor used typosquatting to create a domain similar to the legitimate one from the official developer.



Ad in Google Search for malicious Notepad++ download
source: BleepingComputer

Security researcher Will Dormann found that fake Notepad++ downloads in the sponsored section of Google search were available from additional URLs, all files being marked as malicious by various antivirus (AV) engines on the Virus Total scanning platform.

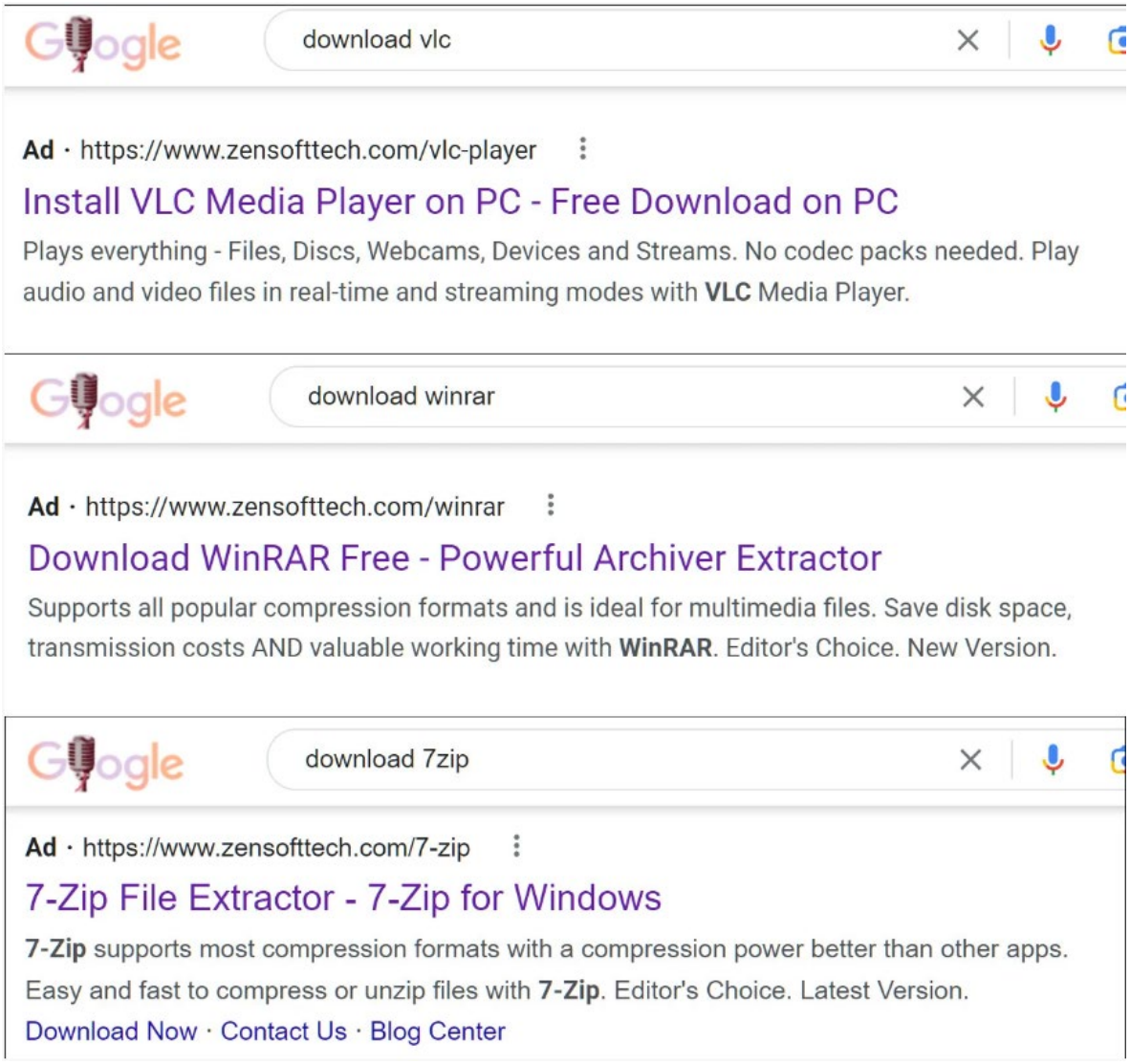


Malicious Notepad++ ad in Google search results
source: Will Dormann

BleepingComputer also found a website filled with fake software downloads distributed solely via Google Ads search results. The website impersonates what appears to be a legitimate web design company in India called Zensoft Tech.

Unfortunately, we could not verify if the downloads were malicious but given that the domain is a typosquatted URL, the site blocks search engines from indexing content and promoting the downloads only through ads in search results, there is a strong indication of malicious activity.

Among the pieces of software we discovered on the website are the file compression utilities 7-ZIP and WinRAR, and the widely used media player VLC.

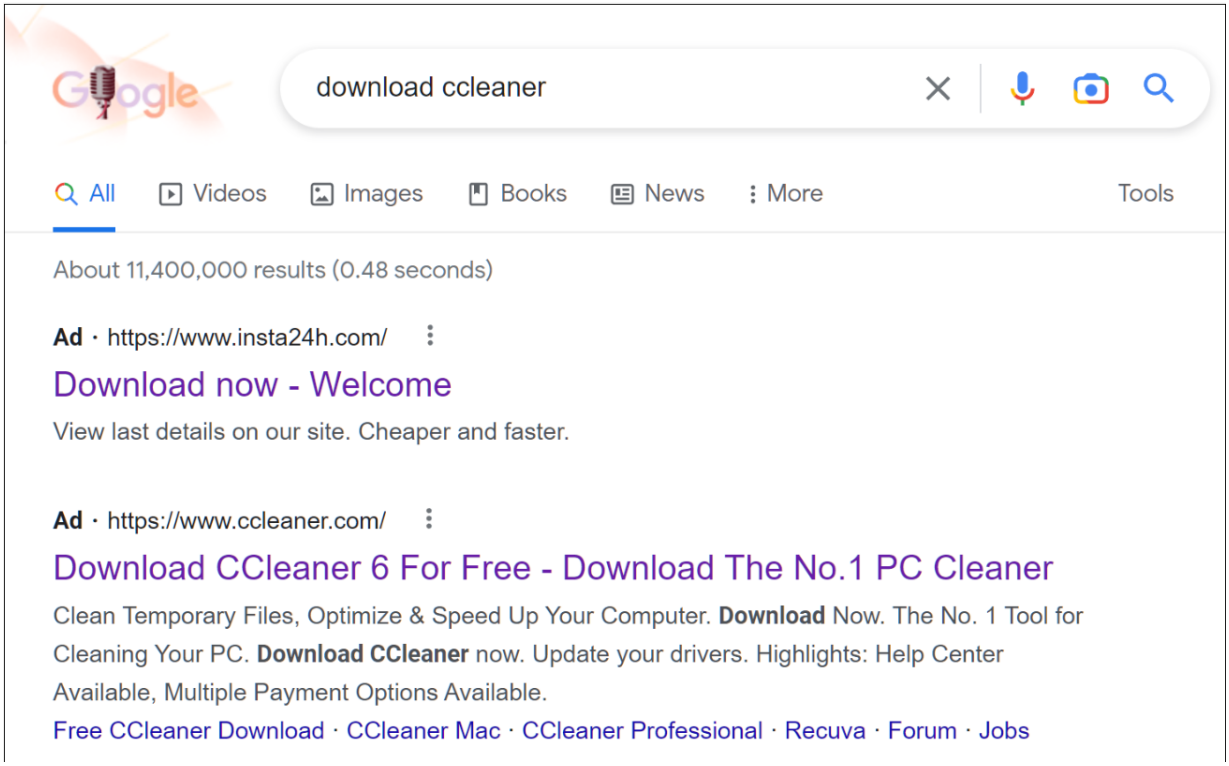


Malicious downloads for WinRAR, 7-ZIP, VLC in sponsored ads on Google search source: BleepingComputer

From a different domain, threat actors provided a malicious version of the CCleaner utility for removing potentially unwanted files and invalid Windows Registry entries.

It appears that the hackers made an effort to outbid the legitimate developer and thus have their ad in the top position. As seen in the image below, the official CCleaner website is

displayed under the malicious advertisement. This site offered a CCleaner.zip file that installed Redline information-stealing malware.



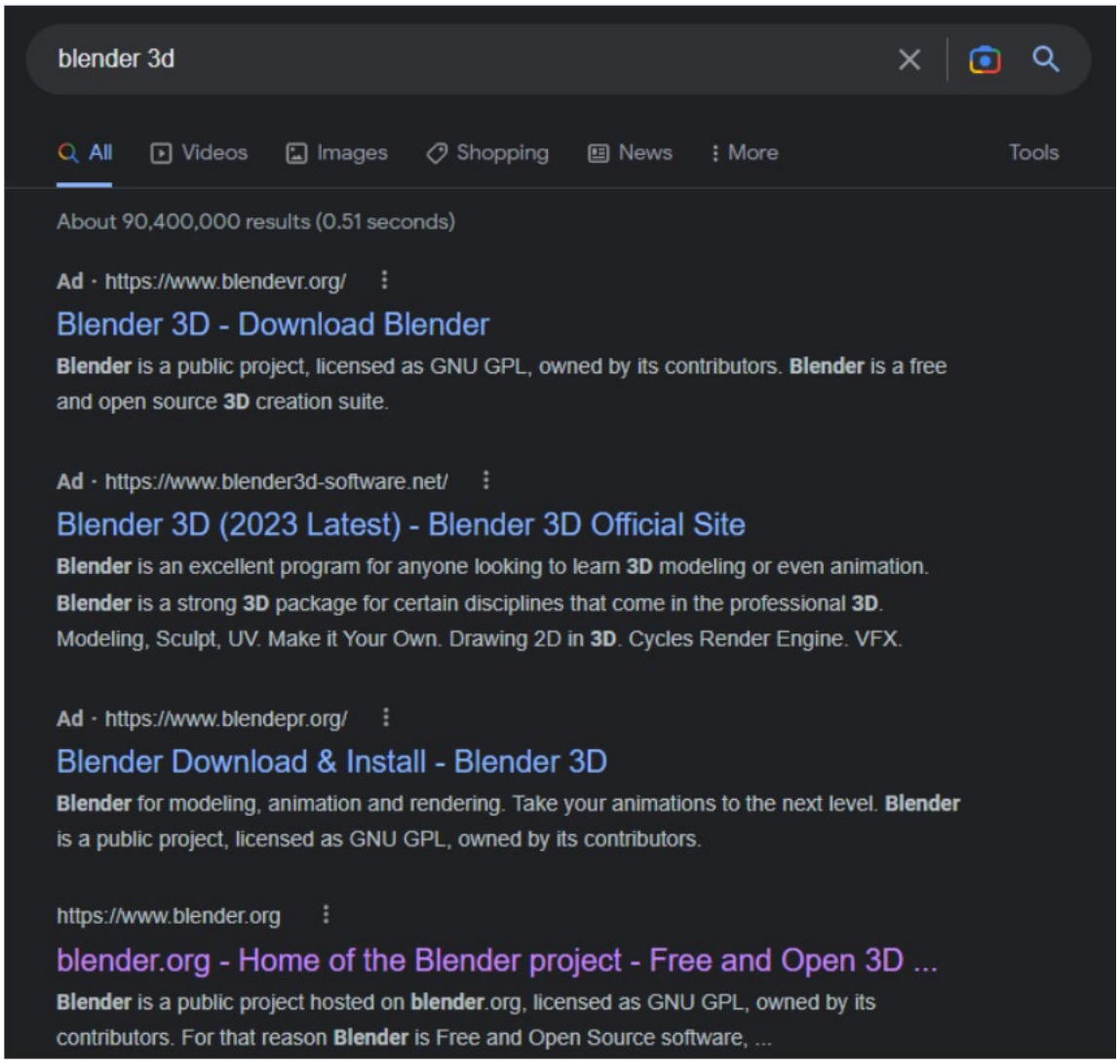
CCleaner malicious download pushed via Google ads
source: BleepingComputer

Several security researchers (mdmck10, MalwareHunterTeam, Will Dormann, Germán Fernández) have uncovered additional URLs hosting malicious downloads impersonating free and open-source software, confirming that luring users through sponsored results on Google search is a more common approach for cybercriminals.

Germán Fernández of cybersecurity company CronUp provides a list of 70 domains that are distributing malware through Google Ads search results by impersonating legitimate software.

The websites are replicas of the official ones and either provide fake software or redirect to another download location. Many of them offer Audacity and some are for VLC and the image editor GIMP.

One user almost fell for the trick when looking to get the Blender 3D open-source 3D creation suite. A tweet from MalwareHunterTeam shows that three malicious ads for this product preceded the link from the official developer.



Malicious Blender 3D downloads take top ad spot in Google search results
source: Nox Scimitar

Looking at one of the samples flagged as malicious by some AV products, security researcher Will Dormann noticed that it had an invalid signature from cybersecurity company Bitdefender.

Although BleepingComputer could not check in all cases the malware delivered this way, in some instances the payload was the RedLine Stealer we saw in the fake CCleaner site.

This malware collects sensitive data from browsers (credentials, credit card, autocomplete info), details about the system (username, location, hardware, security software available), and cryptocurrency.

Fernández found that one threat actor distributed the .NET-based remote access trojan SectoRAT, also known as Arechclient2, via fake downloads for the Audacity digital audio editor.

The researcher also came across the Vidar info-stealer delivered via malicious downloads for Blender 3D advertised in Google Search. Vidar is focused on collecting sensitive info from browsers and can also steal cryptocurrency wallets.

After publishing this article, researchers at HP Wolf Security released a report about similar campaigns, noting that the first one they analyzed dated from November 2022.

Some of the malware they saw delivered through fake software malvertising includes the IcedID trojan, Vidar, Rhadamanthys Stealer and BatLoader.

At the moment, BleepingComputer and multiple security researchers have seen malicious ads in Google search results for the following software:

- 7-Zip
- Blender 3D
- Capcut
- CCleaner
- Notepad++
- OBS
- Rufus
- VirtualBox
- VLC Media Player
- WinRAR
- Putty

BleepingComputer has shared some of these findings with Google and a company representative told us that the platform's policies are designed and enforced to prevent brand impersonation.

"We have robust policies prohibiting ads that attempt to circumvent our enforcement by disguising the advertiser's identity and impersonating other brands, and we enforce them vigorously. We reviewed the ads in question and have removed them" – Google

At the time of writing this article, Google said it would check if additional advertisements and sites reported violated their policies and would take appropriate action if needed. The company has completed this process and removed the reported malicious ads.

Ad-blockers could increase protection

Using sponsored ads in search results as a malware delivery channel has been flagged by the FBI in an alert last year before Christmas.

The agency warned that "these advertisements appear at the very top of search results with minimum distinction between an advertisement and an actual search result" and they link to a website that "looks identical to the impersonated business's official webpage."

Because of this, cybercriminals have a better chance of spreading their malware to a larger pool of unsuspecting users.

Checking the URL of a download source is always good advice. Coupled with the use of an ad-blocker, the level of protection against this type of threat should decrease drastically.

Ad-blockers are available as extensions in most web browsers and, as their name says, they stop advertisements from being loaded and displayed on a web page, including search results.

Apart from adding to more comfortable use of the internet, ad-blockers also step up privacy by preventing tracking cookies in advertisements from collecting data about your browsing habits.

In this case, however, such extensions could make the difference between losing access to your sensitive information or online accounts and getting digital resources from legitimate vendors.

Update [January 18, 2023]: Article updated to reflect that Google reviewed additional malicious ads reported and removed them after publishing this article. Initially, the company received only a smaller set of malicious ads and removed them from the platform.

Added new details from HP Wolf Security research finding other malware delivered through fake software advertising campaigns since November 2022.

Source: https://www.bleepingcomputer.com/news/security/hackers-turn-to-google-search-ads-to-push-info-stealing-malware/

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