telelink
BUSINESS SERVICES

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

Monthly Security Bulletin

November 2021

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 predictable monthly fee.

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

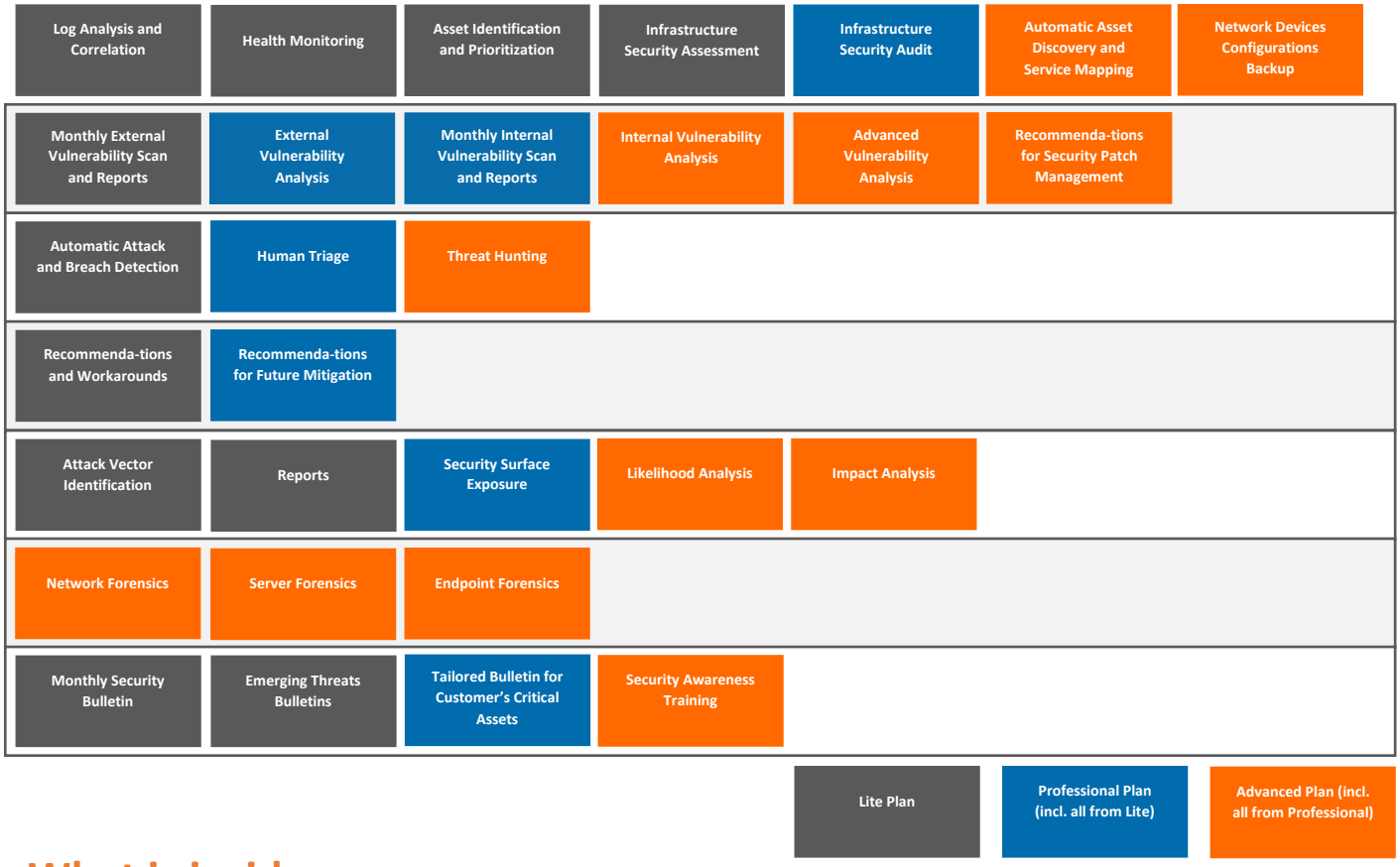
Start to mitigate cyber threats and minimize the risk!

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. Hydra malware targets customers of Germany's second largest bank

The Hydra banking trojan is back to targeting European e-banking platform users, and more specifically, customers of Commerzbank, Germany's second-largest financial institution.

MalwareHunterTeam has spotted the two-year-old malware in a new distribution campaign that targets German users with a malicious APK named 'Commerzbank Security' and using the same icon as the official app.

This sparked the interest of Cyble researchers, who sampled the file for a more in-depth analysis which revealed a powerful phishing tool with extensive access to permissions.

A galore of permissions

Cyble has found that the Hydra-laced app requests 21 permissions, most notably the 'BIND-ACCESSIBILITY_PERMISSION' and 'BIND_DEVICE_ADMIN,' two extremely risky permissions. The former ensures that the app is always running in the background, monitoring and intercepting all data that comes and goes to and from the device. The latter is practically giving the trojan admin privileges on the device, so a wide range of exploitation possibilities opens up.

Other risky permissions used by the trojan include:

Permission Name	Description
CHANGE_WIFI_STATE	Modify Device's Wi-Fi settings
READ_CONTACTS	Access to phone contacts
READ_EXTERNAL_STORAGE	Access device external storage
WRITE_EXTERNAL_STORAGE	Modify device external storage
READ_PHONE_STATE	Access phone state and information
CALL_PHONE	Perform call without user intervention
READ_SMS	Access user's SMSs stored in the device
REQUEST_INSTALL_PACKAGES	Install applications without user interaction
SEND_SMS	Allows the app to send SMS messages
SYSTEM_ALERT_WINDOW	Allows the display of system alerts over other apps

These permissions can be abused to access SMS content, send SMSs, display system alerts, modify device settings, perform calls, write and read external storage, modify WiFi settings, install additional apps, and more.

None of these activities requires interaction by the victimized user, so once the malware has infected the device, it's already too late.

New features and enhancements appear

The fake Commerzbank app sends bulk SMS to the victim's contact list, creates overlays on other apps, screencasts the device screen back to the actor's system, hides its icon, and steals OTPs (one-time passwords) as well as the screen lock PIN.

A notable new feature is the incorporation of TeamViewer relying on the abuse of the Accessibility service, which has not been documented in previous Hydra variants.

New enhancements that aim to make the detection of the trojan harder include the use of encrypted TOR communications, enabling SOCKS Proxy for redirection, and disabling Play Protect, Android's default security component.

A large pool of targets

Commerzbank serves 13 million customers in Germany and another 5 million people in Central and Eastern Europe. This makes up for a total of 18 million potential targets, which is always a critical consideration for malware distributors.

Typically, the threat actors use SMS, social media, and forum posts to lure their prospective victims to malicious landing pages that drop the APK onto German smartphones.

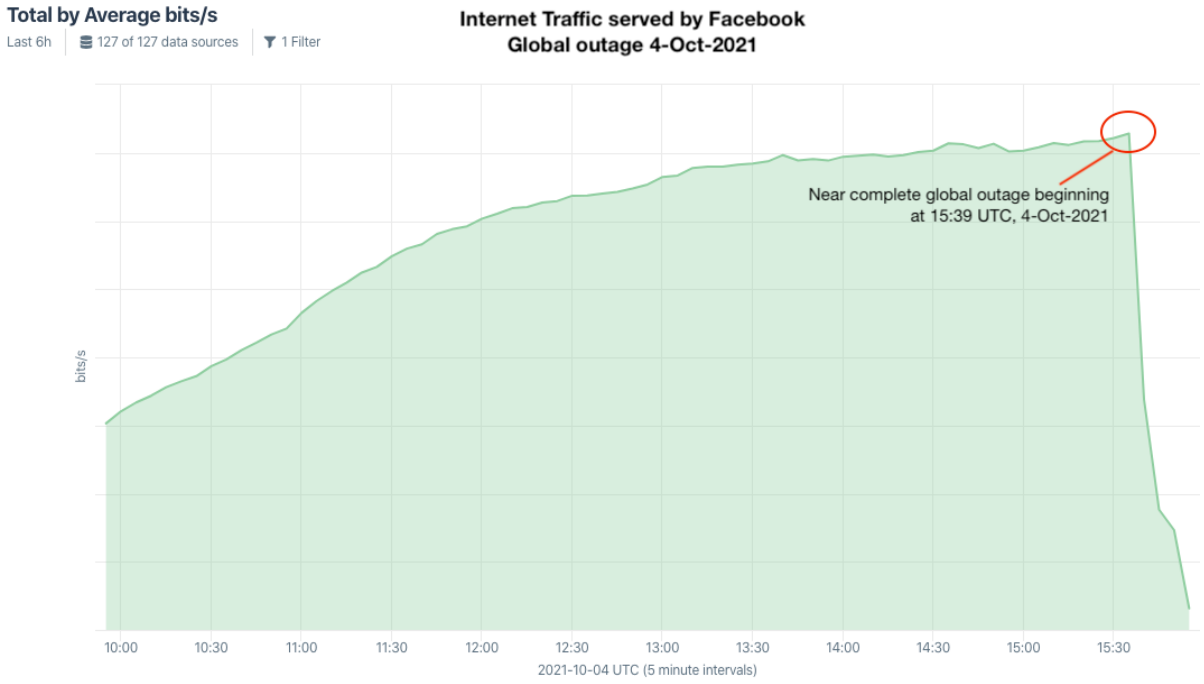
If you think you may have fallen in Hydra's trap already, it is recommended that you clean your device with a security tool from a reputable vendor and even perform a factory reset afterwards.

In general, you should only install APKs from trustworthy sources (the bank's website or Google Play), activate 2FA on your online banking account, and keep your device's OS and AV up to date.

Source: https://www.bleepingcomputer.com/news/security/hydra-malware-targets-customers-of-germanys-second-largest-bank/

2. What Happened to Facebook, Instagram, & WhatsApp?

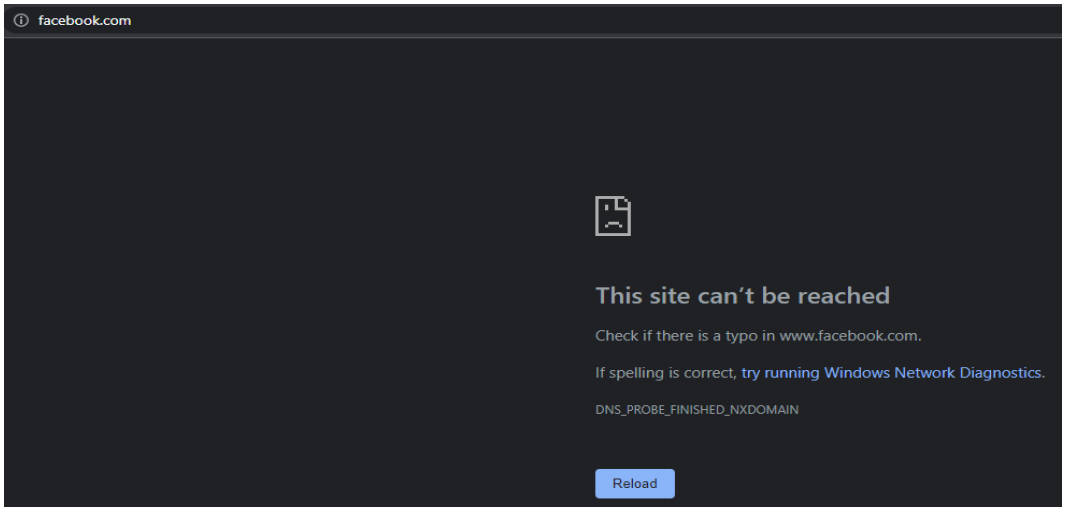
Facebook and its sister properties **Instagram** and **WhatsApp** are suffering from ongoing, global outages. We don't yet know why this happened, but the how is clear: Earlier this morning, something inside Facebook caused the company to revoke key digital records that tell computers and other Internet-enabled devices how to find these destinations online.



Kentik's view of the Facebook, Instagram and WhatsApp outage.

Doug Madory is director of internet analysis at **Kentik**, a San Francisco-based network monitoring company. Madory said at approximately 11:39 a.m. ET today (15:39 UTC), someone at Facebook caused an update to be made to the company's Border Gateway Protocol (BGP) records. BGP is a mechanism by which Internet service providers of the world share information about which providers are responsible for routing Internet traffic to which specific groups of Internet addresses.

In simpler terms, sometime this morning Facebook took away the map telling the world's computers how to find its various online properties. As a result, when one types Facebook.com into a web browser, the browser has no idea where to find Facebook.com, and so returns an error page.



In addition to stranding billions of users, the Facebook outage also has stranded its employees from communicating with one another using their internal Facebook tools. That's because Facebook's email and tools are all managed in house and via the same domains that are now stranded.

"Not only are Facebook's services and apps down for the public, its internal tools and communications platforms, including Workplace, are out as well," New York Times tech reporter **Ryan Mac** tweeted. "No one can do any work. Several people I've talked to said this is the equivalent of a 'snow day' at the company."

The outages come just hours after **CBS's 60 Minutes** aired a much-anticipated interview with **Frances Haugen**, the Facebook whistleblower who recently leaked a number of internal Facebook investigations showing the company knew its products were causing mass harm, and that it prioritized profits over taking bolder steps to curtail abuse on its platform — including disinformation and hate speech.

We don't know how or why the outages persist at Facebook and its other properties, but the changes had to have come from inside the company, as Facebook manages those records internally. Whether the changes were made maliciously or by accident is anyone's guess at this point.

Madory said it could be that someone at Facebook just screwed up.

"In the past year or so, we've seen a lot of these big outages where they had some sort of update to their global network configuration that went awry," Madory said. "We obviously can't rule out someone hacking them, but they also could have done this to themselves."

Update, 4:37 p.m. ET: Sheera Frenkel with The New York Times tweeted that Facebook employees told her they were having trouble accessing Facebook buildings because their employee badges no longer worked. That could be one reason this outage has persisted so long: Facebook engineers may be having trouble physically accessing the computer servers needed to upload new BGP records to the global Internet.

Update, 6:16 p.m. ET: A trusted source who spoke with a person on the recovery effort at Facebook was told the outage was caused by a routine BGP update gone wrong. The source explained that the errant update blocked Facebook employees — the majority of whom are working remotely — from reverting the changes. Meanwhile, those with physical access to Facebook's buildings couldn't access Facebook's internal tools because those were all tied to the company's stranded domains.

Update, 7:46 p.m. ET: Facebook says its domains are slowly coming back online for most users. In a tweet, the company thanked users for their patience, but it still hasn't offered any explanation for the outage.

Update, 8:05 p.m. ET: This fascinating thread on Hacker News delves into some of the not-so-obvious side effects of today's outages: Many organizations saw network disruptions and slowness thanks to billions of devices constantly asking for the current coordinates of Facebook.com, Instagram.com and WhatsApp.com. **Bill Woodcock**, executive director of the Packet Clearing House, said his organization saw a 40 percent increase globally in wayward DNS traffic throughout the outage.

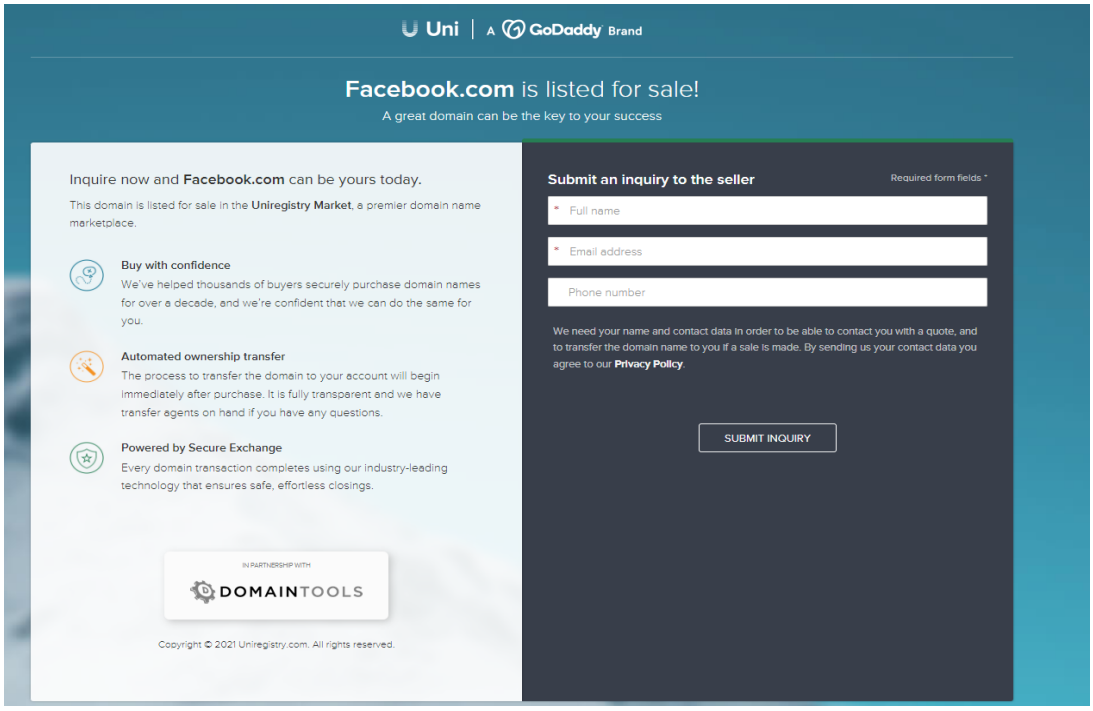
Update, 8:32 p.m. ET: Cloudflare has published a detailed and somewhat technical writeup on the BGP changes that caused today's outage. Still no word from Facebook on what happened.

Update, 11:32 p.m. ET: Facebook published a blog post saying the outage was the result of a faulty configuration change:

"Our engineering teams have learned that configuration changes on the backbone routers that coordinate network traffic between our data centers caused issues that interrupted this communication," Facebook's **Santosh Janardhan** wrote. "This disruption to network traffic had a cascading effect on the way our data centers communicate, bringing our services to a halt."

"We want to make clear at this time we believe the root cause of this outage was a faulty configuration change," Janardhan continued. "We also have no evidence that user data was compromised as a result of this downtime."

Several different domain registration companies today listed the domain Facebook.com as up for sale. This happened thanks to automated systems that look for registered domains which appear to be expired, abandoned or recently vacated. There was never any reason to believe Facebook.com would actually be sold as a result, but it's fun to consider how many billions of dollars it could fetch on the open market.



Source: https://krebsonsecurity.com/2021/10/what-happened-to-facebook-instagram-whatsapp/

3. Massive Twitch hack: Source code and payment reports leaked

Twitch source code, as well as streamers' and users' sensitive information, was allegedly leaked online by an anonymous user on the 4chan imageboard.

The leaker shared a torrent link leading to a 125GB archive containing data allegedly stolen from roughly 6,000 internal Twitch Git repositories.

"Their community is also a disgusting toxic cesspool, so to foster more disruption and competition in the online video streaming space, we have completely pwned them, and in part one, are releasing the source code from almost 6,000 internal Git repositories," the post reads.

According to the anonymous 4chan user, the leaked Twitch data contains:

- The entirety of twitch.tv, with commit history going back to its early beginnings
- Mobile, desktop, and video game console Twitch clients
- Various proprietary SDKs and internal AWS services used by Twitch
- Every other property that Twitch owns, including IGDB and CurseForge

- An unreleased Steam competitor from Amazon Game Studios
- Twitch SOC internal red teaming tools (lol)
- Creator payout reports from 2019 until now.

The anonymous poster named his thread "twitch leaks part one," which hints at further stolen Twitch data likely being leaked in the future.

BleepingComputer downloaded a portion of the leaked data and can confirm that it looks authentic and matches what was disclosed by the hacker.

The leak was likely a direct reply to Twitch's lack of response and effective tools to fend off hate raids targeting streamers in August, given that the anonymous leaker also used the #DoBetterTwitch hashtag.

This hashtag was used on Twitter by streamers who shared how their Twitch stream chats were being flooded with harrassment bots.

Twitch eventually acknowledged the issue and said it will launch account verification and channel level ban evasion detection tools later this year.

"Thank you to everyone who shared these difficult experiences. We were able to identify a vulnerability in our proactive filters, and have rolled out an update to close this gap and better detect hate speech in chat.," the company said.

A Twitch spokesperson confirmed over email that "a breach has taken place" after this article was published.

Source: https://www.bleepingcomputer.com/news/security/massive-twitch-hack-source-code-and-payment-reports-leaked/

4. European Parliament calls for ban on AI-powered mass surveillance

The EU Parliament has voted in favor of a resolution that bans the adoption of AI-powered biometric mass surveillance technologies such as facial recognition systems in the continent.

A big "no" to mass surveillance

The MEPs (members of the European parliament) are worried about discrimination, bias, and injustice that arise from AI-based predictive policing, and their concerns are based on numerous real examples. For history, 377 MEPs voted in favor, 248 against, and 62 were absent.

Vendors of AI-based facial recognition solutions have admitted that algorithm bias has plagued their systems for years and have made efforts to solve the problem through diverse data sets and machine learning optimizations. However, the discriminatory rates are still too high to be acceptable in any important deployment context.

With today's decision, the European Parliament asks for a permanent ban on the automated recognition of individuals in public spaces, and the prohibition of predicting policing based on behavioral data.

The only exception in the ban are cases of criminal suspects, but even then, the use of facial recognition databases should be excluded from the available tools used for justifying or proving that person's culpability. Clearview AI is specifically mentioned as an example of what is to be avoided.

Finally, the MEPs ask for higher levels of transparency like using open source code for the detection algorithms, allowing public scrutiny in all aspects of these systems.

Petar Vitanov, the lead MEP on the issue, has stated the following:

"Fundamental rights are unconditional. For the first time ever, we are calling for a moratorium on the deployment of facial recognition systems for law enforcement purposes, as the technology has proven to be ineffective and often leads to discriminatory results.

We are clearly opposed to predictive policing based on the use of AI as well as any processing of biometric data that leads to mass surveillance. This is a huge win for all European citizens."

AI systems still on the way

Although this is an important development and a strong step towards the protection of human rights in Europe, the case with AI-deployment is not closed.

The 'Artificial Intelligence Act' is still being negotiated and drafted, so the EU Parliament's decision merely plays a catalytic role right now. The MEPs are sending a message of what will be acceptable and where they would like to see more safeguards introduced.

In a relevant report published today, the European Commission states they intend to boost private and public investment in AI technologies to €20 billion per year.

While legislation underpinning this massive rollout will need to ensure that all potential abuse, discrimination, and human rights violations are addressed, AI-powered systems are still on their way to becoming omnipresent in Europe.

In the U.S., AI-assisted policing and mass-scale facial recognition systems are still not audited by a central authority or controlled by a comprehensive legislation, and at the same time, the adoption rates on both public and private sectors are now booming.

Source: https://www.bleepingcomputer.com/news/technology/european-parliament-calls-for-ban-on-ai-powered-mass-surveillance/

5. Phishing campaign uses math symbols to evade detection

Phishing actors are now using mathematical symbols on impersonated company logos to evade detection from anti-phishing systems.

One notable case spotted by analysts at INKY involves the spoofing of Verizon, a large U.S.-based telecommunication service provider.

In this case, the actors are using a square root symbol, a logical NOR operator, or the checkmark symbol itself, all helping to create a slight optical differentiation that could trick AI-based spam detectors.

For many people who don't keep up with the latest logo changes though, these slightly altered logos look good enough, so the delivery success and user engagement rates have better chances of staying high.

You have fake voicemail

All three spoofing types masquerade as voicemail notifications containing an embedded 'Play' button, that when clicked, take the user to a phishing portal that was crafted to look like a Verizon website.

The landing domain is clearly not part of Verizon's official webspace, with one example given in the report being sd9-08[.]click.

The actors bet on the carelessness of the target, as otherwise, the spoofed site looks pretty convincing. Also, Inky has found that this phishing campaign relied on recently-registered domains that were unreported.

The logo on the cloned site is the genuine one as the phishing actors stole most of the HTML and CSS elements from the real Verizon site.

Scrolling down on the fake page, the visitor will find the alleged voicemail, but they are only allowed to access it if they provide their Office365 account credentials on the sign-in form.

The first attempt will result in getting an "incorrect password" message, while the second attempt is generating a bogus error that ends the login procedure.

This is done for the phishing actors to ensure that the victim hasn't mistyped their password in the first attempt, so it's essentially a "quality assurance" step.

When you receive email of this kind, proper scrutiny is an important factor to not falling victims to these scams. Never click on embedded buttons, always validate the URL of the site you're about to enter any credentials, and finally, consider the realism of the situation.

In this case, a message from Verizon is urging recipients to enter their Office365 credentials, which does not make sense in this situation. If the contents of an email do not make sense for whatever reason, it's usually phishing and the email should be junked.

Source: https://www.bleepingcomputer.com/review/security/phishing-campaign-uses-math-symbols-to-evade-detection/

6. Don't Let Old Accounts Haunt You: How to Maintain Your Digital Graveyard

What was the first online service that you signed up for? Perhaps it was your middle school email address ("soccerloveR1450@hotmail.com" anyone?) or your very first Tumblr or Myspace account. Whatever it was, it's likely that you haven't used these accounts in years — but did you ever actually delete the account?

Over the past decade, you've likely collected various online accounts that you no longer use. But just because you stop using an account doesn't mean that it doesn't exist — and your data is likely still floating around on the World Wide Web. These old "zombie" accounts haunt your digital graveyard and are easy pickings for cybercriminals.

The Haunting of Accounts Past

Today, most websites and apps either require or strongly encourage their visitors to create user accounts. Almost always, exchanging an email address for an exclusive offer seems a fair tradeoff. As a result, consumers quickly accumulate accounts, many of which they may not even remember creating.

According to Digital Guardian, 70% of consumers have more than 10 password-protected online accounts, and 30% have too many to keep track of. These accounts are comprised of free trials, stores that you no longer purchase from, one-time accounts that you create to buy something, gaming platforms, and apps that you only used a few times. While they may have once served a purpose, you no longer need them.

The problem with zombie accounts is that they contain credentials at risk of exposure. Say that you sign up for a free week trial of a meal kit delivery service. When creating your account, you include information like your email address, password, phone number, delivery address, and credit card information. Once your trial expires, you decide not to sign up for a membership, but your account information remains online. If the meal kit company is involved in a data breach, your personal data could be leaked and exploited by cybercriminals. And if you happen to reuse the same credentials across multiple accounts, a criminal could use credential stuffing techniques (where they use email and password combinations to hack into online profiles) to break into your other accounts.

How to Gain Control of Your Data

So, how can you keep protect your online data and prevent a zombie account apocalypse? Follow these cybersecurity best practices to help keep your information secure:

Track down and close old accounts

Don't remember which accounts you made and no longer use? No worries! If you browse with Google Chrome, check under chrome > settings > passwords. This will show all the accounts and passwords you've used and saved. Other browsers like Firefox and Safari have similar settings. If you use a password manager, this will also keep a record of your credentials. Once you've identified the online accounts you no longer used (or completely forgot you had), close the account for good! This may take some patience, as some websites require multiple steps to close an account. But it will be worth knowing that your information is safer from online exposure.

Make sure all your passwords are strong and unique

Having a strong, unique password for each of your online accounts helps protect them from credential stuffing. By using different passwords for your online accounts, you can take comfort in knowing that the majority of your data is secure if one of your accounts is vulnerable.

Update your credentials when necessary

If you realize a company you buy from fell victim to a data breach, start investigating. A tool like McAfee Identity Protection Service can help you monitor multiple email addresses that allow you to see if you were impacted by a breach. If your credentials were potentially exposed, update them on the company's website immediately.

Use multifactor authentication

Multifactor authentication is an online safety measure where more than one method of identity verification is needed to access the valuable information that lies within password-protected accounts. This can prevent a criminal from breaking into your online profile by providing an added layer of security.

Invest in protection

McAfee Total Protection will help protect your personal information and privacy and provides identity restoration services and invaluable peace of mind. Ninety-two percent of Canadians are concerned about the protection of their privacy and 37% are extremely concerned, reports the Canadian Centre for Cybersecurity. All it takes is a few changes to your online habits and arming yourself with the right tools to feel secure about your online presence.

The post Don't Let Old Accounts Haunt You: How to Maintain Your Digital Graveyard appeared first on McAfee Blogs.

Source: https://www.mcafee.com/blogs/consumer-cyber-awareness/dont-let-old-accounts-haunt-you-how-to-maintain-your-digital-graveyard/

7. Ransomware as a Service: Defend by Reinvesting in the Fundamentals

Ransomware as a service (RaaS) is a business model designed for criminals, by criminals that lowers the technical barrier for entry into cybercrime. Instead of having to learn the skills needed to code ransomware or access a network, aspiring criminals can buy access and components – sometimes with a monthly subscription comparable to a streaming movie service. While in many ways this makes life easier for cybercriminals, there's a silver lining for defenders: Less sophisticated cybercriminals can often be stopped by following best practices and consistently introducing basic roadblocks. In the second installment of this two-part series, I cover how reinvesting in the fundamentals and being sure to use a defense in depth strategy can ensure that rookie cybercriminals looking for a quick payout have a very frustrating day when they encounter your network.

Starting Points for Defense in Depth against RaaS

In no particular order, I've listed a few areas that I believe are good jumping-off points to start conversations in your organization about defense in-depth strategies.

Authentication

Keeping attackers out – and limiting what they can do if they do get in – is a great place to start. If we objectively look at how compromises occur most predominantly these days, it's typically through the use of legitimate credentials or tricking users into running malware directly via phishing. Exploitation of vulnerabilities as an initial vector into organizations is usually less than ideal given how easy it is to get access through the human side of things. However, if the attackers do leverage exploits, they find it exponentially more difficult to continue lateral movement and navigate the internals of your network without credentials. This is where we can view every account and authentication point as potential roadblocks to hinder or slow attackers.

- Implement stronger password policies involving complexity and how frequently credentials get rotated.
- Place restrictions on access – who can access data, and where and when, especially in the context of administrative access.
- Use multi-factor authentication.

While these roadblocks will help, they become even more effective when you combine them with auditing and aggressive monitoring for usage anomalies – but the benefits of proactive security are a separate discussion.

Attack Surface Reduction

A singular truism exists in every cyberattack, which is that there must be an entry point. Within the context of our digital lives, this entry point is usually accessible through internet-connected systems. As such, building successful roadblocks here will be to know what is actually exposed. What is your digital footprint on the internet, and what types of connectivity does it offer?

Due to the global COVID-19 pandemic, remote work has taken off and companies have rushed to situate themselves in a way that facilitates supporting employees who now unexpectedly find themselves working from home. This has increased the opportunity for threat actors to take shots at VPNs and remote access solutions as a quick way into the internal network. But what about the webserver you migrated from six years ago but never got around to retiring? You don't know what you don't know, so making sure you have a good, frequently updated assessment of your network perimeter is key to reducing the attack surface. Breaking it down into exposed services and remote access opportunities helps prioritize where you can implement more robust controls.

Patching and Vulnerability Management

Vulnerabilities are being weaponized at a record pace these days, and the game of whack-a-mole with patches continues unabated. Sometimes even before patches are released, just the announcement of the vulnerability and breadcrumbs on social media are enough to create the exploits. This makes this one of the hardest "back to basics" guidance there is. Still, the bottom line is that attackers have only become more efficient in their rapid exploitation of vulnerabilities, while most organizations continue to stagnate with unpatched environments.

Closing these holes makes the attacker's life more difficult. It places the onus back on the attackers to be clever and crafty enough to circumvent these roadblocks without the use of vulnerability exploitation, removing a strong tool from their arsenal.

- Conduct comprehensive accounting of missing patches throughout your environment, both for the infrastructure and end user systems, to more easily identify problem areas.
- Reduce the time systems remain vulnerable from patch release to deployment. There is no one size fits all solution for this problem; every organization has to determine acceptable timelines based on their level of risk, but at the end of the day, the faster, the better.
- Where patches can't be deployed, identify compensating mechanisms to protect vulnerable systems or users.

Network Segmentation and Microsegmentation

I'm a firm believer in the power of segmentation, both logically and physically, as it creates a distinct boundary for access controls and monitoring. In the context of this article, network segmentation would be barriers between things like end users and data center servers, whereas microsegmentation would be logical barriers between things such as SAN servers and database servers. At its core, this is just another foundational concept – Zero Trust.

By creating roadblocks that restrict the traversal of network traffic from all directions (West to East, North to South) and coupling this with other security controls, you are better positioned to create the roadblocks that severely hamper less technical threat actors.

Expect a High Return on Investment for Defense in Depth

My hope is that this article serves in some capacity to be a catalyst for taking a step back and trying to identify what proactive roadblocks you can construct when it comes to defending your networks and data. RaaS is here to stay, and the lessons learned through its evolution will be an example to cybercriminals on the commoditization of every aspect of cyberattacks. The silver lining is that we'll likely see the technical sophistication of threat actors decrease while the refocusing of our defensive efforts on core security concepts, such as defense in depth, will provide a higher return on investment in the long run.

Learn more about making a plan for defending against ransomware attacks.

Jeff White is a principal threat researcher for the Unit 42 Threat Intelligence team. This is the second of a two-part series on ransomware as a service.

The post Ransomware as a Service: Defend by Reinvesting in the Fundamentals appeared first on Palo Alto Networks Blog.

Source: https://www.paloaltonetworks.com/blog/2021/10/raas-defense-in-depth

8. Massive campaign uses YouTube to push password-stealing malware

Widespread malware campaigns are creating YouTube videos to distribute password-stealing trojans to unsuspecting viewers.

Password stealing trojans are malware that quietly runs on a computer while stealing passwords, screenshots of active windows, cookies, credit cards stored in browsers, FTP credentials, and arbitrary files decided by the threat actors.

When installed, the malware will communicate with a Command & Control server, where it waits for commands to execute by the attacker, which could entail the running of additional malware.

Malicious YouTube videos gone wild

Threat actors have long used YouTube videos as a way to distribute malware through embedded links in video descriptions.

However, this week has Cluster25 security researcher Frost told BleepingComputer that there has been a significant uptick in malware campaigns on YouTube pushing various password-stealing Trojans.

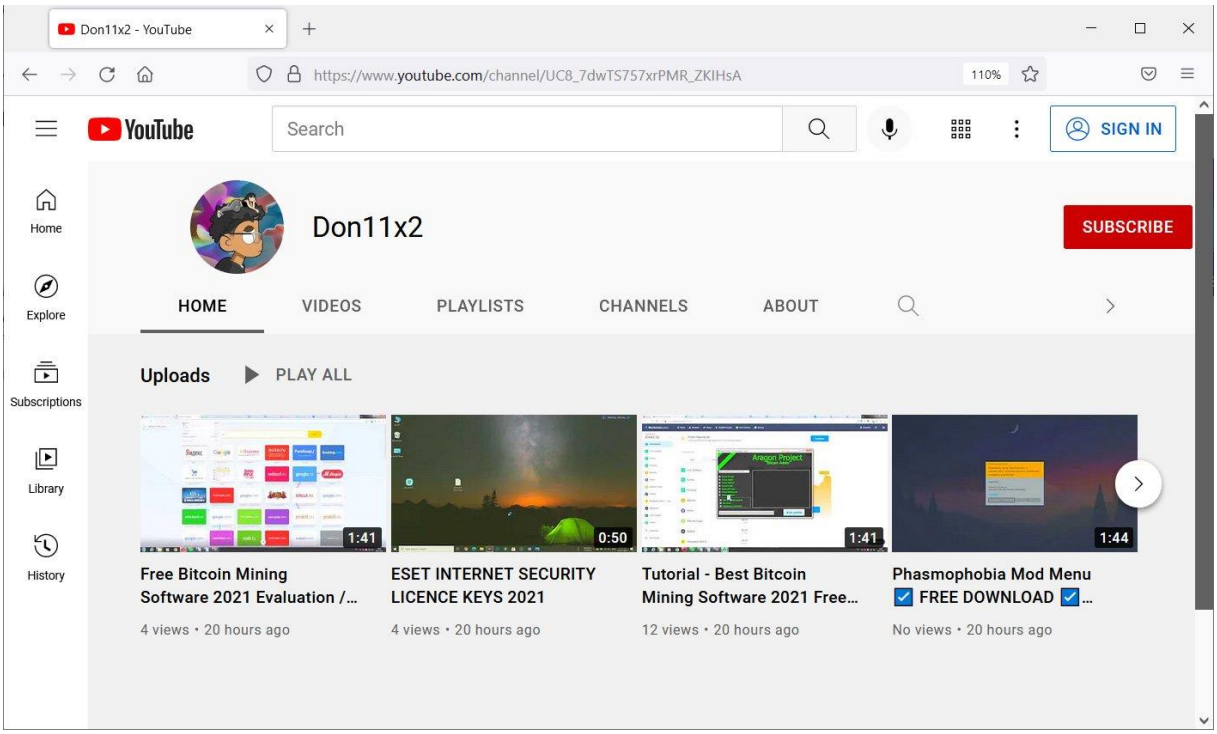
Frost told BleepingComputer that it is likely two clusters of malicious activity being conducted simultaneously - one pushing the RedLine malware and the other pushing Racoon Stealer.

The researcher said that thousands of videos and channels had been made as part of this massive malware campaign, with 100 new videos and 81 channels created in just twenty minutes.

Frost explained that the threat actors use the Google accounts they steal to launch new YouTube channels to spread malware, creating a never-ending and ever-growing cycle.

"The threat actors have thousands of new channels available because they infect new clients every day. As part of these attacks, they steal victim's Google credentials, which are then used to create new YouTube Videos to distribute the malware," Frost told BleepingComputer.

The attacks start with the threat actors creating numerous YouTube channels filled with videos about software cracks, licenses, how-to guides, cryptocurrency, mining, game cheats, VPN software, and pretty much any other popular category.



Example of a malicious YouTube channel

These videos contain content that explains how to perform a task using a specific program or utility. Additionally, the YouTube video's description includes an alleged link to the associated tool used to distribute the malware.

Once a user becomes infected, the malware will proceed to scan all installed browsers and the computer for cryptocurrency wallets, credit cards, passwords, and other data and upload it back to the attacker.

Google told BleepingComputer that they are aware of the campaign and are taking action to disrupt the activity.

"We are aware of this campaign and are currently taking action to block activity by this threat actor and flagging all links to Safe Browsing. As always, we are continuously improving our detection methods and investing in new tools and features that automatically identify and stop threats like this one. It is also important that users remain aware of these types of threats and take appropriate action to further protect themselves." - Google.

Google also disclosed this week a phishing campaign that distributed password-stealing trojans used to steal the accounts of YouTube Creators. These accounts were then sold on dark web markets or used to perform cryptocurrency scams.

Downloading software can be dangerous.

These campaigns illustrate how important it is not to download programs from the Internet haphazardly, as sites like YouTube can not vet every link added by video publishers.

Therefore, a user should research a site before downloading and installing anything from it to determine if they have a good reputation and can be trusted. Even then, it is always suggested that you first upload the program to a site like VirusTotal to confirm if it's safe to run.

If you have accidentally fallen for this attack and installed a program from a similar link, it is strongly suggested that you scan your computer with an antivirus program.

After you have removed any malware detected in a virus scan, you should immediately change any passwords saved in your browsers.

Source: https://www.bleepingcomputer.com/news/security/massive-campaign-uses-youtube-to-push-password-stealing-malware/

9. Threat Actors Abuse Discord to Push Malware

The platform's Content Delivery Network and core features are being used to send malicious files—including RATs--across its network of 150 million users, putting corporate workplaces at risk.

Threat actors are abusing the core features of the popular Discord digital communication platform to persistently deliver various types of malware—in particular remote access trojans (RATs) that can take over systems–putting its 150 million users at risk, researchers have found.

RiskIQ and CheckPoint both discovered multi-functional malware being sent in messages across the platform, which allows users to organize Discord servers into topic-based channels in which they can share text, image or voice files or other executables. Those files are then stored on Discord's Content Delivery Network (CDN) servers.

Researchers warn, "many files sent across the Discord platform are malicious, pointing to a significant amount of abuse of its self-hosted CDN by actors by creating channels with the sole purpose of delivering these malicious files," according to a report published Thursday by Team RiskIQ.

Initially Discord attracted gamers, but the platform is now being used by organizations for workplace communication. The storage of malicious files on Discord's CDN and proliferation of malware on the platform mean that "many organizations could be allowing this bad traffic onto their network," RiskIQ researchers wrote.

RATs and Miscellaneous Malware

Features of the latest malware found on the platform include the capability to take screenshots, download and execute additional files, and perform keylogging, CheckPoint researchers Idan Shechter and Omer Ventura disclosed in a separate report also published Thursday.

CheckPoint also found that the Discord Bot API—a simple Python implementation that eases modifications and shortens the development process of bots on the platform–"can easily turn the bot into a simple RAT" that threat actors can use "to gain full access and remote control on a user's system."

Discord bots are becoming an increasingly integral part of how users interact with Discord, allowing them to integrate code for enhanced features to facilitate community management, researchers said.

"Discord bots appear to be powerful, friendly and highly time-saving," Shechter and Ventura wrote. "However, with great power also comes great responsibility, and Discord's bot framework can be easily used for malicious intent."

CheckPoint researchers discovered several malicious repositories among GitHub that are relevant for the Discord platform. These repositories include malware based on Discord API and malicious bots with different functionalities, they said.

Exploiting Discord Channels

Meanwhile, RiskIQ researchers examined Discord CDN URLs containing .exe, DLL and various document and compressed files, discovering upon review of the hashes on VirusTotal that more than 100 were delivering malicious content. Eighty files were from 17 malware different families, with trojans comprising the most common malware observed on the platform, researchers said.

Specifically, RiskIQ researchers took a deeper dive into how Discord CDN uses a Discord domain through links that use [hxxps://cdn.discordapp[.]com/attachments/{ChannelID}/{AttachmentID}/{filename}] as the format to discover malware, they said.

Researchers detected links and queried Discord channel IDs used in these links, which enabled them to identify domains containing web pages that link out to a Discord CDN link with a specific channel ID, they said.

"For example, the RiskIQ platform can query the channel IDs associated with zoom[-]download[.]ml," researchers explained. "This domain attempts to spoof users into downloading a Zoom plug-in for Microsoft Outlook and instead delivers the Dcstl password stealer hosted on Discord's CDN."

In another example, RiskIQ discovered that the channel ID for a URL containing a Raccoon password stealer file returned a domain for Taplink, a site that provides users with micro landing pages to direct individuals to their Instagram and other social media pages, they explained.

"A user likely added the Discord CDN link to their Taplink page," researchers explained. "Querying these IDs enables RiskIQ users to understand which Discord files and associated infrastructure are concerning and where they are across the web."

The technique enabled researchers to determine the date and time Discord channels were created, linking ones created within a few days before the first observation of a file in VirusTotal to channels with the sole purpose of distributing malware, they said. Ultimately, they uncovered and cataloged 27 unique malware types hosted on Discord's CDN.

Security Holes Persist

The latest research isn't the first time Discord has been called out for a malware problem. In July researchers from Sophos revealed that the number of Discord malware detections rose sharply compared to last year, also observing abuse of the CDN to host malicious files. Researchers also said at the time that Discord's API was being leveraged to exfiltrate stolen data and facilitate hacker command-and-control channels.

The findings unsurprisingly raised an alarm among security experts, who said they demonstrate numerous holes with platforms that people widely use to communicate and share files that rely on the use of encrypted traffic for security.

However, as has been observed many times before, encrypting traffic on APIs alone is not sufficient to keep malware off a content delivery network, noted one security professional.

"API abuse is best defended by ensuring that only genuine software clients can use the API, thus preventing malicious scripts and malware doing damage to the platform, David Stewart, CEO of security firm Approov, said in an email to Threatpost.

The discovery also highlights a key problem in the development of communication platforms—the emphasis on functionality rather than security, said another security professional.

"This is an example of an exploitation that probably could have been addressed with a better software design," Saryu Nayyar, CEO of security firm Gurucul, said in an email to Threatpost.

That said, Discord's developers need to think about adding a way to collect and analyze data in real time from the platform to discover and quickly remediate unusual activity, she said.

"Absent a redesign of the Discord software, this is the only realistic way of detecting malware is to look for activities that are out of the ordinary," Nayyar observed.

Source: https://threatpost.com/threat-actors-abuse-discord-to-push-malware/175663/

10. Attackers Hijack Craigslist Emails to Bypass Security, Deliver Malware

Manipulated Craigslist emails that abuse Microsoft OneDrive warn users that their ads contain "inappropriate content."

Musical instruments, motorcycle parts and now malware — Craigslist really does have it all.

The Craigslist internal email system was hijacked by attackers this month to deliver convincing messages, ultimately aimed at avoiding Microsoft Office security controls in order to deliver malware.

Sent from an authentic Craigslist IP address, the emails informed users that one of their published ads included inappropriate content and violated Craigslist's terms and conditions, giving false instructions on how to avoid having their accounts deleted.

Researchers at INKY discovered that the attackers manipulated the email's HTML into a customized document with a malware-download link uploaded to a Microsoft OneDrive page. That page impersonated major brands like DocuSign, Norton and Microsoft.

That also allowed the campaign to slip past standard email authentication.

"Since the URL to resolve the issue hosted a customized document placed on Microsoft OneDrive, it did not appear on any threat intelligence feed, allowing it to slip past most security vendors," the researchers noted in a posting this week.

Abusing Anonymity

Craigslist is more than one gigantic yard sale. Its internal email system also lets interested buyers and sellers contact each other anonymously. According to INKY's report, threat actors were able to abuse that Craigslist email system so as to deliver authentic-looking phishing emails to users who were actively trying to sell something on the site.

That means victims were likely already fielding random inquiries from the Craigslist system, so the malicious emails simply blended in.

"Craigslist knows the identities of everyone, but unless a correspondent discloses details, they are perfectly anonymous to others on the system," the INKY report said. "This situation suits phishers just fine. They can shoot their poisoned arrows from behind a local mail proxy. And shoot they did — a number of times in early October."

The phishing emails looked like a notice from Craigslist that the user's ad contained inappropriate content. The letter then threatened to ban the user from the platform unless they filled out a form, accessed by a malicious link.

Craigslist Phishing Emails Flag 'Inappropriate Content'

"Our platform's content publishing policy explicitly prohibits inappropriate content, your ad has received many red flags," the email read. "A more detailed description of the problem is available in this form. It will be available 24 hours."

Clicking on the "form" took users to a Microsoft OneDrive document, INKY explained.

"It appears as if bad actors were able to manipulate the email's HTML to create that button and link it to OneDrive," the researchers wrote. "Hovering over the link revealed a Russian domain (myjino[.]ru)."

Clicking on the link initiated a .ZIP file download containing a macro-enabled spreadsheet that delivered malware. To get around Microsoft Office security controls and run the macros, the malicious documents prompted victims to click on a button to "Enable Editing" or "Enable Content," INKY said.

"The spreadsheet impersonated DocuSign and also used Norton and Microsoft logos to imply that the file was safe," according to the report. "DocuSign does not in fact have a service called 'DocuSign Protect Service.'"

When the INKY team tried to get the malware to work it led to a 404 error message, which the team surmised is either a mistake by the attackers, or an indication that they had already been found out and taken down by the host.

Nonetheless, the INKY team said this Craigslist-hosted attack could have been used to install a remote access tool (RAT), launch a ransomware attack, implement a first-stage implant like TrickBot, exfiltrate sensitive data or deploy a keylogger.

INKY advised Craigslist users to be on the lookout for these kinds of attacks, and added that any emails that seem unusual should be viewed as potentially malicious.

"Another red flag is the mixing of platforms," the analysts added. "It doesn't make sense to resolve a Craigslist issue through a document uploaded to OneDrive."

Source: https://threatpost.com/attackers-hijack-craigslist-email-malware/175754/

11. EU's Green Pass Vaccination ID Private Key Leaked

UPDATE: French & Polish authorities found no sign of cryptographic compromise in the leak of the private key used to sign the vaccine passports and to create fake passes for Mickey Mouse and Adolf Hitler, et al.

As of Thursday morning Eastern time, Adolf Hitler and Mickey Mouse could still validate their digital Covid passes, SpongeBob Squarepants was out of luck, and the European Union was investigating a leak of the private key used to sign the EU's Green Pass vaccine passports.

Two days earlier, on Tuesday, several people reported that they'd found a QR code online that turned out to be a digital Covid certificate with the name "Adolf Hitler" written on it, along with a date of birth listed as Jan. 1, 1900.

On Wednesday, the Italian news agency ANSA reported that several underground vendors were selling passes signed with the stolen key on the Dark Web, and that the EU had called "several high-level meetings" to investigate whether the theft was an isolated incident.

The private key used to verify Hitler's pass was reportedly revoked as of Wednesday, but there were multiple reports of working certificates still being sold online. Threatpost confirmed this on Thursday morning by using the official Verifica C19 app to scan a QR code that had been shared on Twitter by a penetration tester.

Adolf's certificate got the green light, as shown in the screen capture below:

Other QR codes posted to GitHub turned up a validly signed certificate for Mickey Mouse, though SpongeBob's certificate has since been turned away as the key(s) gets revoked.

As of Thursday, the certificate for Adolf Hitler was also still being accepted by Germany's Covid app "CovPass," where the private certificate itself appears to originate from France.

Serious Repercussions of a Leaked Private Certificate

Dirk Schrader, global vice president of security research at New Net Technologies (NNT), now part of change management software provider Netwrix, told Threatpost on Thursday that this leak is likely going to be a big issue as travelers increasing require proof of vaccination.

"A leaked private certificate is a likely a big issue as other nations, specially non-EU nations, might require additional proof for any traveler, once the full scope of this incident unfolds," he said via email. "The market for such fake vaccination certificates seems to be promising, as the use of Mickey Mouse and other fictitious and historic names certainly is used as a proof and assurance for potential buyers."

Authentic EU Digital Passports Could Be Invalidated

The worst potential outcome of this, Schrader pointed out, would be revocation of that private key – an outcome that could affect 278 million EU citizens.

Joseph Carson, chief security scientist and Advisory CISO at ThycoticCentrify, a Washington D.C. based provider of cloud identity security solutions, said the news of the leak is "shocking,"

"It is a major concern that the private keys have been reportedly leaked/sold and actively being used to create forged EU Digital COVID passports," he told Threatpost on Thursday. "This leak could, in fact, invalidate existing authentic EU Digital Passports unless a full incident response and root cause analysis is determined that could minimize any potential damage this could cause."

Carson pointed out that aach country is responsible for their private keys, so one country being compromised "would not be a major surprise."

That, however, isn't the case: multiple countries are being reported, which is going to damage the trust that the EU Digital Passport provides and which "could force a revamp on travel restrictions or trust in the passport," Carson said.

"The whole trust is based on keeping those private keys secured and protected, and I just hope that the impacted countries have minimized the risks and [are] not dependent on a single set of private keys for all EU Digital Passports," he continued.

"[Determining] how the private keys have been compromised should be a top priority," while reducing the risks of such a leak reoccurring should mean that security and protection of the keys will be significantly improved, he said.

A 'Growing Black Market' in Forged Vaccine Passports

Besides fictional or dead characters, the penetration tester who shared the QR code – @reversebrain – noted that this is no laughing matter. "This is worrying," they said. "If the leak would be confirmed, this means that fake EU Digital COVID Certificate can be forged to any person."

It wouldn't be the first time. In June, Germany set up a police task force to battle what the BBC called a growing black market in forged vaccine certificates, as scammers communicated via the encrypted Telegram messaging service to dupe people into paying about €100 (£86; $122) for a whole lot of nothing.

Telegram is again featuring in the forged certificates this time around. GitHub user Emanuele Laface said on Tuesday that the encrypted messenger service is where most of the forged Green Passes are being passed around:

Laface suggested that the leak could encompass more than just one private key. Rather, it could be that a database of private keys was compromised: a possibility that "may [end] up in a break of the chain of trust in the Green Pass architecture," they noted.

That chain of trust could be broken in a lot of places: According to BleepngComputer, the fake certificates circulating online have been issued from countries including France,

Germany, Italy, Netherlands, North Macedonia, Poland, and more, "indicating the issue could very well impact the entire EU."

EU (Slowly) Moves to Block Bogus Certificates

102821 13:05 UPDATE: The European Commission told Threatpost on Thursday that it's in contact with the relevant Member States authorities that are investigating and which are putting remedial actions in place.

A spokesperson said that Member States in the eHealth Network decided on Wednesday to coordinate their actions on the incident. As a first step, he said, "Member States have agreed to block the two fraudulent certificates so that they will be shown as invalid by the verifying apps."

The Commission didn't give a timeline for when the certificates will be blocked, nor why Threatpost and others could still validate some of the bogus certificates on Thursday.

But the Commission did say that Member States and the Commission are working at the national and European level on improving invalidation and revocation systems, "to be able to react to any such cases even more quickly."

The Commission condemned the private key theft: "The Member States and the Commission condemn this malicious act in the strongest possible terms, which comes at a time when health services in all Member States are under pressure fighting the pandemic."

Cryptographic Keys Not Compromised

The Commission's statement said that the certificates were apparently generated "by persons with valid credentials to access the national IT systems, or a person misusing such valid credentials."

An investigation now being conducted by authorities in France and Poland is looking into possible causes of the fraudulent activity, including potential forgery of documents and identity theft.

At this point, the investigation has ruled out a compromise of the cryptographic keys used to sign certificates, according to the Commission:

"According to the information available, the cryptographic keys used to sign certificates have not been compromised. This incident is caused by an illegal activity and not by a technical failure. Together with the Member States, we reaffirm our full trust in the EU Digital COVID Certificate system."

Source: https://threatpost.com/eus-green-pass-vaccination-id-private-key-leaked/175857/

12. TrickBot malware dev extradited to U.S. faces 60 years in prison

A Russian national believed to be a member of the TrickBot malware development team has been extradited to the U.S. and is currently facing charges that could get him 60 years in prison.

38-year old Vladimir Dunaev, also known as FFX, was a malware developer that supervised the creation of TrickBot's browser injection module, the indictment alleges.

He is the second malware developer associated with the TrickBot gang that the Department of Justice arrested this year. In February, Latvian national Alla Witte, a.k.a. Max, was arrested for writing code related to the control and deployment of ransomware.

Old member of the gang

Dunaev was arrested in South Korea in September as he was trying to leave the country. He had been forced to stay there for more than a year due to Covid-19 travel restrictions and his passport expired. The extradition completed on October 20.

Dunaev is believed to have been involved with the TrickBot gang since mid-2016 following a recruitment test that involved creating an application that simulated a SOCKS server and altering a copy of the Firefox browser.

He passed both tests with flying colors, showing skills that the TrickBot gang needed. "He's capable of everything. Such a person is needed," reads a conversation between two members of the gang responsible for recruiting developers.

Starting June 2016, the defendant created, modified, and updated code for the TrickBot malware gang, the indictment alleges.

Between October 19, 2017, and March 3, 2018, members of the TrickBot gang that included Dunaev and Witte successfully wired more than $1.3 million from victim bank accounts.

Large, well-organized group

According to the indictment, the TrickBot gang has at least 17 members, each with specific attributes within the operation:

- Malware Manager - who outlines the programming needs, manages finances, deploys TrickBot
- Malware Developer - who develops TrickBot modules and hands them to others to encrypt
- Crypter - who encrypt the TrickBot modules so that they evade antivirus detection

- Spammer - who use distribute TrickBot through spam and phishing campaigns

  Created from the ashes of the Dyre banking trojan in 2015, TrickBot focused on stealing banking credentials initially, via web injection and logging the victim user's keystrokes.

  Later, it developed into modular malware that could also distribute other threats. These days, the gang has a preference for dropping ransomware on company networks, Conti in particular.

  TrickBot is believed to have infected millions of computers, enabling its operators to steal personal and sensitive information (logins, credit cards, emails, passwords, dates of birth, SSNs, addresses) and steal funds from victims' banking accounts.

  The malware has impacted businesses in the United States, United Kingdom, Australia, Belgium, Canada, Germany, India, Italy, Mexico, Spain, and Russia.

  Apart from Dunaev and Witta, the DoJ has indicted other members of the TrickBot gang whose names have not been revealed and are located in various countries, Russia, Belarus, and Ukraine among them.

  Dunaev is currently facing multiple counts of aggravated identity theft, wire fraud, bank fraud. as well as conspiracy to commit computer fraud, aggravated identity theft, and money laundering.

  All the charges against him come with a maximum penalty of 60 years in a federal prison.

  Source: https://www.bleepingcomputer.com/news/security/trickbot-malware-dev-extradited-to-us-faces-60-years-in-prison/

13. All Windows versions impacted by new LPE zero-day vulnerability

A security researcher has disclosed technical details for a Windows zero-day privilege elevation vulnerability and a public proof-of-concept (PoC) exploit that gives SYSTEM privileges under certain conditions.

A public proof-of-concept (PoC) exploit and technical details for an unpatched Windows zero-day privilege elevation vulnerability has been disclosed that allows users to gain SYSTEM privileges under certain conditions.

The good news is that the exploit requires a threat actor to know another user's user name and password to trigger the vulnerability, so it will likely not be widely abused in attacks.

The bad news is that it affects all versions of Windows, including Windows 10, Windows 11, and Windows Server 2022.

Researcher releases bypass to patched vulnerability

August, Microsoft released a security update for a "Windows User Profile Service Elevation of Privilege Vulnerability" tracked as CVE-2021-34484 and discovered by security researcher Abdelhamid Naceri.

After examining the fix, Naceri found that the patch was not sufficient and that he was able to bypass it with a new exploit that he published on GitHub.

"Technically, in the previous report CVE-2021-34484. I described a bug where you can abuse the user profile service to create a second junction," Naceria explains in a technical writeup about the vulnerability and the new bypass.

"But as I see from ZDI advisory and Microsoft patch, the bug was metered as an arbitrary directory deletion bug."

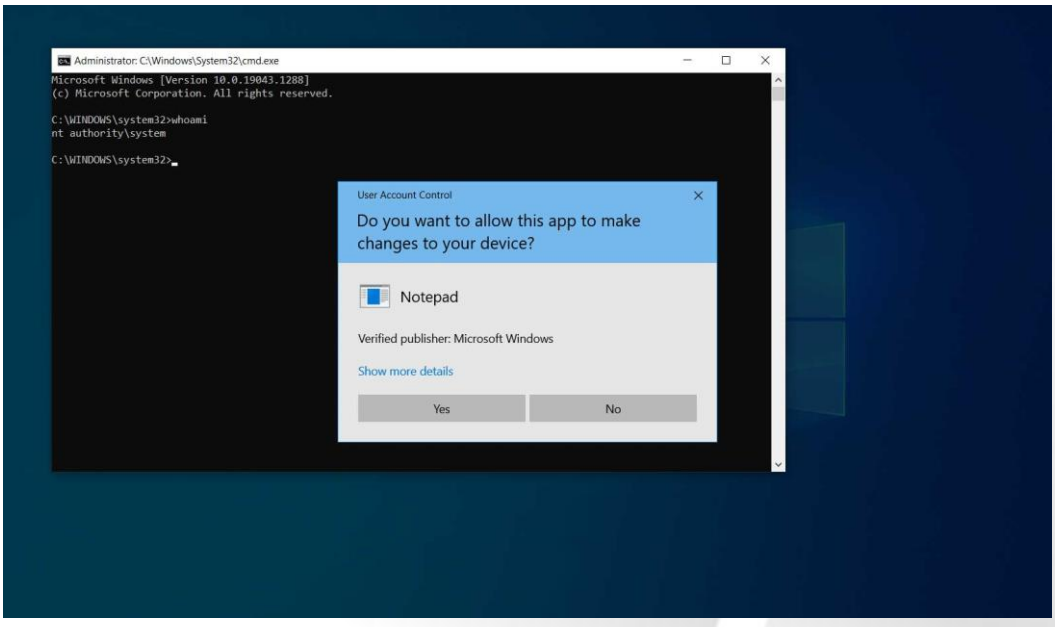
"Microsoft didn't patch what was provided in the report but the impact of the PoC. Since the PoC I wrote before was horrible, it could only reproduce a directory deletion bug."

Naceri says that since they only fixed the symptom of his bug report and not the actual cause, he could revise his exploit to make a junction elsewhere and still achieve privilege elevation.

This exploit will cause an elevated command prompt with SYSTEM privileges to be launched while the User Account Control (UAC) prompt is displayed.

Will Dormann, a vulnerability analyst for CERT/CC, tested the vulnerability and found that while it worked, it was temperamental and did not always create the elevated command prompt.

When BleepingComputer tested the vulnerability, it launched an elevated command prompt immediately, as shown below.



As this bug requires a threat actor to know a user name and password for another user, it will not be as heavily abused as other privilege elevation vulnerabilities we have seen recently, such as PrintNightmare.

"Definitely still a problem. And there may be scenarios where it can be abused. But the 2 account requirement probably puts it in the boat of NOT being something that will have widespread use in the wild," Dormann told BleepingComputer.

However, Naceri told BleepingComputer that a threat actor only needs another domain account to exploit the vulnerability, so it should still be something to be concerned about.

Microsoft said they are aware of the issue and are looking into it.

"We are aware of the report and will take appropriate action to keep customers protected." – a Microsoft spokesperson.

Source: https://www.bleepingcomputer.com/news/security/all-windows-versions-impacted-by-new-lpe-zero-day-vulnerability/

14. Police arrest hackers behind over 1,800 ransomware attacks

The Europol has announced the arrest of 12 individuals who are believed to be linked to ransomware attacks against 1,800 victims in 71 countries.

According to the law enforcement report, the actors have deployed ransomware strains such as LockerGoga, MegaCortex, and Dharma, as well as malware like Trickbot and post-exploitation tools like Cobalt Strike.

LockerGoga first appeared in the wild in January 2019, when it hit 'Altran Technologies', a French engineering and R&D consultant, part of the Capgemini group.

LockerGoga and MegaCortex infections culminated during that year, with a report from the National Cyber Security Centre (NCSC) in the Netherlands attributing 1,800 infections to Ryuk and the two strains.

The most notable case linked to the suspects is a 2019 attack against Norsk Hydro, the Norwegian aluminum production giant, causing severe and lengthy disruption in the company's operations.

Today, the Norwegian police posted a relevant announcement saying that they never stopped hunting for the threat actors, working with foreign counterparts to bring them down.

The arrests took place in Ukraine and Switzerland on October 26, 2021, and as a result of the simultaneous raids, the police seized five luxury vehicles, electronic devices, and $52,000 in cash.

As Europol explains, the arrested individuals are considered high-value targets in the sense that they're thought to have spearheaded multiple high-profile ransomware cases.

As such, the forensic examination and the interrogations that follow the action will be extensive and may very likely bring up new investigative leads.

Highly organized cybercrime organization

The cyber-criminals fulfilled specialized roles in a highly organized criminal organization, with each person being responsible for distinct operational aspects.

Some engaged in network penetration, others in brute force attacks, while others performed SQL injections or handled credential phishing operations.

In the post-infection stage, their roles were transposed to a new domain, with the actors deploying malware, network reconnaissance, and lateral movement tools, carefully stealing data while staying undetected.

Eventually, the actors encrypted the compromised systems and left ransom notes demanding the victims to pay exorbitant amounts of money in Bitcoin in exchange for decryption keys.

Some of the individuals who were arrested now are thought to be in charge of the money laundering operation, using Bitcoin mixing services to obscure the money trace.

This operation is a massive law-enforcement success, made possible thanks to more than 50 investigators from seven European police departments, six Europol specialists, and members of the FBI and the US Secret Service.

Source: https://www.bleepingcomputer.com/news/security/police-arrest-hackers-behind-over-1-800-ransomware-attacks/

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.