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

Monthly Security Bulletin

July 2023

This security bulletin is powered by Telelink Business Services' Advanced Security Operations Center

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

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

The ASOC by Telelink allows organizations get visibility, control,

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

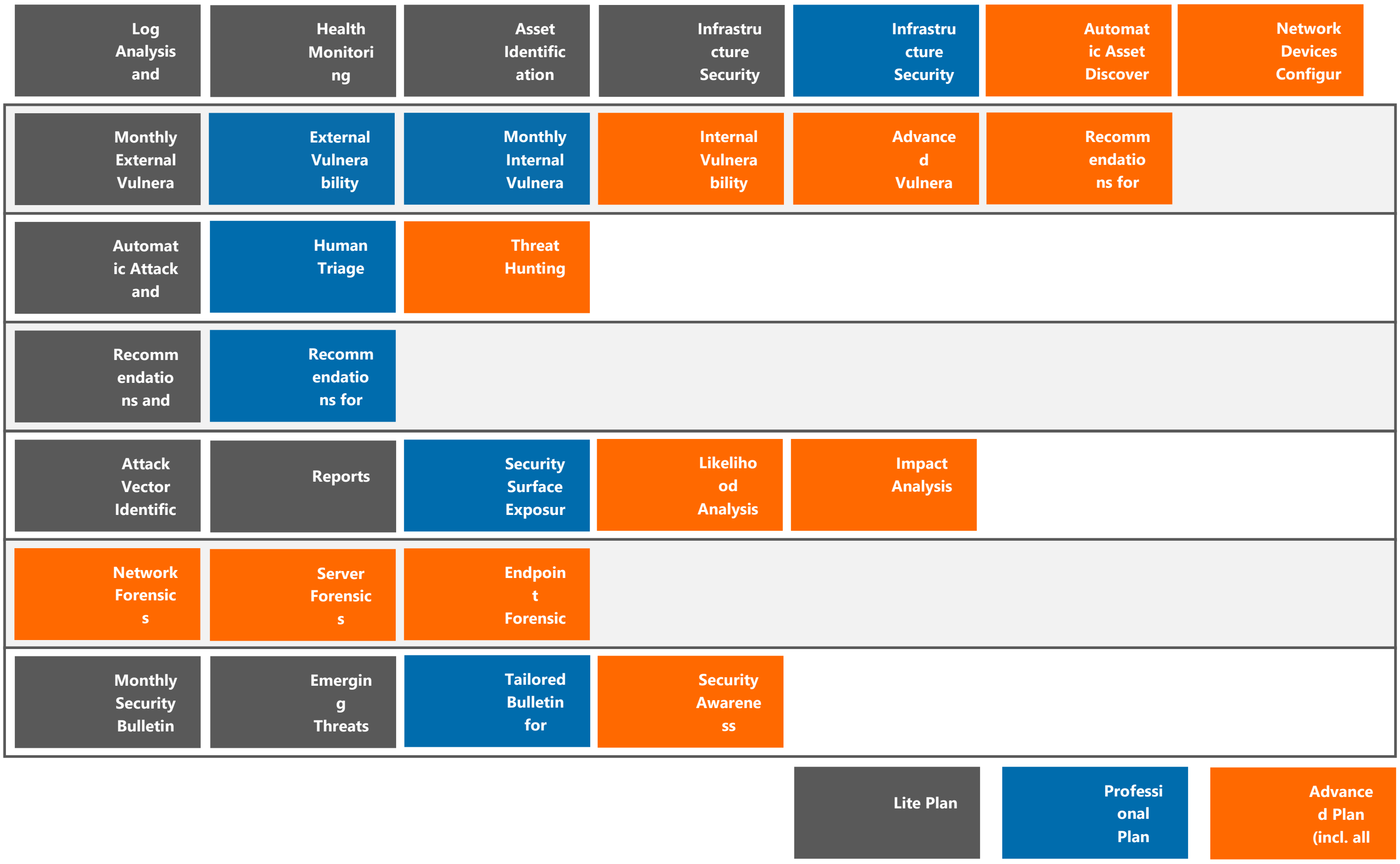
Start to mitigate cyber threats and minimize the risk!

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!



⬛ Log Analysis and	⬛ Health Monitoring	⬛ Asset Identification	⬛ Infrastructure Security	🟦 Infrastructure Security	🟧 Automatic Asset Discover	🟧 Network Devices Configur
⬛ Monthly External Vulnera	🟦 External Vulnerability	🟦 Monthly Internal Vulnera	🟧 Internal Vulnerability	🟧 Advanced Vulnera	🟧 Recommendations for	
⬛ Automatic Attack and	🟦 Human Triage	🟧 Threat Hunting				
⬛ Recommendations and	🟦 Recommendations for					
⬛ Attack Vector Identific	⬛ Reports	🟦 Security Surface Exposur	🟧 Likelihood Analysis	🟧 Impact Analysis		
🟧 Network Forensics	🟧 Server Forensics	🟧 Endpoint Forensic				
⬛ Monthly Security Bulletin	⬛ Emerging Threats	🟦 Tailored Bulletin for	🟧 Security Awareness			

⬛ Lite Plan 🟦 Professional Plan 🟧 Advanced Plan (incl. all

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. U.K. Cyber Thug “PlugwalkJoe” Gets 5 Years in Prison

Joseph James “PlugwalkJoe” O’Connor, a 24-year-old from the United Kingdom who earned his 15 minutes of fame by participating in the July 2020 hack of Twitter, has been sentenced to five years in a U.S. prison. That may seem like harsh punishment for a brief and very public cyber joy ride. But O’Connor also pleaded guilty in a separate investigation involving a years-long spree of cyberstalking and cryptocurrency theft enabled by “SIM swapping,” a crime wherein fraudsters trick a mobile provider into diverting a customer’s phone calls and text messages to a device they control.

On July 16, 2020 — the day after some of Twitter’s most recognizable and popular users had their accounts hacked and used to tweet out a bitcoin scam — KrebsOnSecurity observed that several social media accounts tied to O’Connor appeared to have inside knowledge of the intrusion. That story also noted that thanks to COVID-19 lockdowns at the time, O’Connor was stuck on an indefinite vacation at a popular resort in Spain.

Joseph “PlugwalkJoe” O’Connor, in a photo from a Globe Newswire press release Sept. 02, 2020, pitching O’Connor as a cryptocurrency expert and advisor

Not long after the Twitter hack, O’Connor was quoted in The New York Times denying any involvement. “I don’t care,” O’Connor told The Times. “They can come arrest me. I would laugh at them. I haven’t done anything.”

Speaking with KrebsOnSecurity via Instagram instant message just days after the Twitter hack, PlugwalkJoe demanded that his real name be kept out of future blog posts here. After he was told that couldn’t be promised, he remarked that some people in his circle of friends had been known to hire others to deliver physical beatings on people they didn’t like.

O’Connor was still in Spain a year later when prosecutors in the Northern District of California charged him with conspiring to hack Twitter. At the same time, prosecutors in the Southern District of New York charged O’Connor with an impressive array of cyber offenses involving the exploitation of social media accounts, online extortion, cyberstalking, and the theft of cryptocurrency then valued at nearly USD $800,000.

In late April 2023, O’Connor was extradited from Spain to face charges in the United States. Two weeks later, he entered guilty pleas in both California and New York, admitting to all ten criminal charges levied against him. On June 23, O’Connor was sentenced to five years in prison.

PlugwalkJoe was part of a community that specialized in SIM-swapping victims to take over their online identities. Unauthorized SIM swapping is a scheme in which fraudsters trick or bribe employees at wireless phone companies into redirecting the target's text messages and phone calls to a device they control.

From there, the attackers can reset the password for any of the victim's online accounts that allow password resets via SMS. SIM swapping also lets attackers intercept one-time passwords needed for SMS-based multi-factor authentication (MFA).

O'Connor admitted to conducting SIM swapping attacks to take control over financial accounts tied to several cryptocurrency executives in May 2019, and to stealing digital currency currently valued at more than $1.6 million.

PlugwalkJoe also copped to SIM-swapping his way into the Snapchat accounts of several female celebrities and threatening to release nude photos found on their phones.

Victims who refused to give up social media accounts or submit to extortion demands were often visited with "swatting attacks," wherein O'Connor and others would falsely report a shooting or hostage situation in the hopes of tricking police into visiting potentially lethal force on a target's address.

Prosecutors said O'Connor even swatted and cyberstalked a 16-year-old girl, sending her nude photos and threatening to rape and/or murder her and her family.

In the case of the Twitter hack, O'Connor pleaded guilty to conspiracy to commit computer intrusions, conspiracy to commit wire fraud, and conspiracy to commit money laundering.

On July 16, 2020 — the day after some of Twitter's most recognizable and popular users had their accounts hacked and used to tweet out a bitcoin scam — KrebsOnSecurity observed that several social media accounts tied to O'Connor appeared to have inside knowledge of the intrusion. That story also noted that thanks to COVID-19 lockdowns at the time, O'Connor was stuck on an indefinite vacation at a popular resort in Spain.

Not long after the Twitter hack, O'Connor was quoted in **The New York Times** denying any involvement. "I don't care," O'Connor told The Times. "They can come arrest me. I would laugh at them. I haven't done anything."

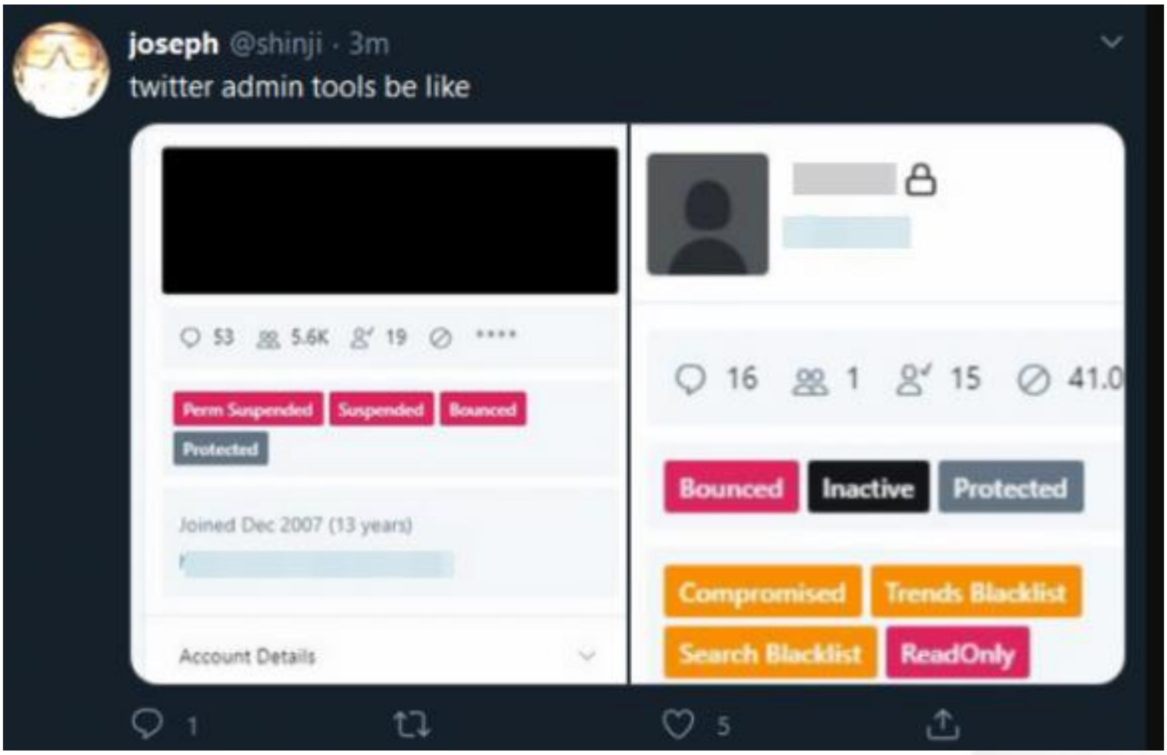
Speaking with KrebsOnSecurity via Instagram instant message just days after the Twitter hack, PlugwalkJoe demanded that his real name be kept out of future blog posts here. After he was told that couldn't be promised, he remarked that some people in his circle of friends had been known to hire others to deliver physical beatings on people they didn't like.

O'Connor was still in Spain a year later when prosecutors in the Northern District of California charged him with conspiring to hack Twitter. At the same time, prosecutors in the Southern District of New York charged O'Connor with an impressive array of cyber offenses involving the exploitation of social media accounts, online extortion, cyberstalking, and the theft of cryptocurrency then valued at nearly USD $800,000.

In late April 2023, O'Connor was extradited from Spain to face charges in the United States. Two weeks later, he entered guilty pleas in both California and New York, admitting to all ten criminal charges levied against him. On June 23, O'Connor was sentenced to five years in prison.

PlugwalkJoe was part of a community that specialized in SIM-swapping victims to take over their online identities. Unauthorized SIM swapping is a scheme in which fraudsters trick or bribe employees at wireless phone companies into redirecting the target's text messages and phone calls to a device they control.

The account "@shinji," a.k.a. "PlugWalkJoe," tweeting a screenshot of Twitter's internal tools interface, on July 15, 2020.



joseph @shinji · 3m

twitter admin tools be like

From there, the attackers can reset the password for any of the victim's online accounts that allow password resets via SMS. SIM swapping also lets attackers intercept one-time passwords needed for SMS-based multi-factor authentication (MFA).

O'Connor admitted to conducting SIM swapping attacks to take control over financial accounts tied to several cryptocurrency executives in May 2019, and to stealing digital currency currently valued at more than $1.6 million.

PlugwalkJoe also copped to SIM-swapping his way into the Snapchat accounts of several female celebrities and threatening to release nude photos found on their phones.

Victims who refused to give up social media accounts or submit to extortion demands were often visited with "swatting attacks," wherein O'Connor and others would falsely report a shooting or hostage situation in the hopes of tricking police into visiting potentially lethal force on a target's address.

Prosecutors said O'Connor even swatted and cyberstalked a 16-year-old girl, sending her nude photos and threatening to rape and/or murder her and her family.

In the case of the Twitter hack, O'Connor pleaded guilty to conspiracy to commit computer intrusions, conspiracy to commit wire fraud, and conspiracy to commit money laundering.

Fake extortionists are piggybacking on data breaches and ransomware incidents, threatening U.S. companies with publishing or selling allegedly stolen data unless they get paid.

Sometimes the actors add the menace of a distributed denial-of-service (DDoS) attack if the message recipient does not comply with the instructions in the message.

Bad actors

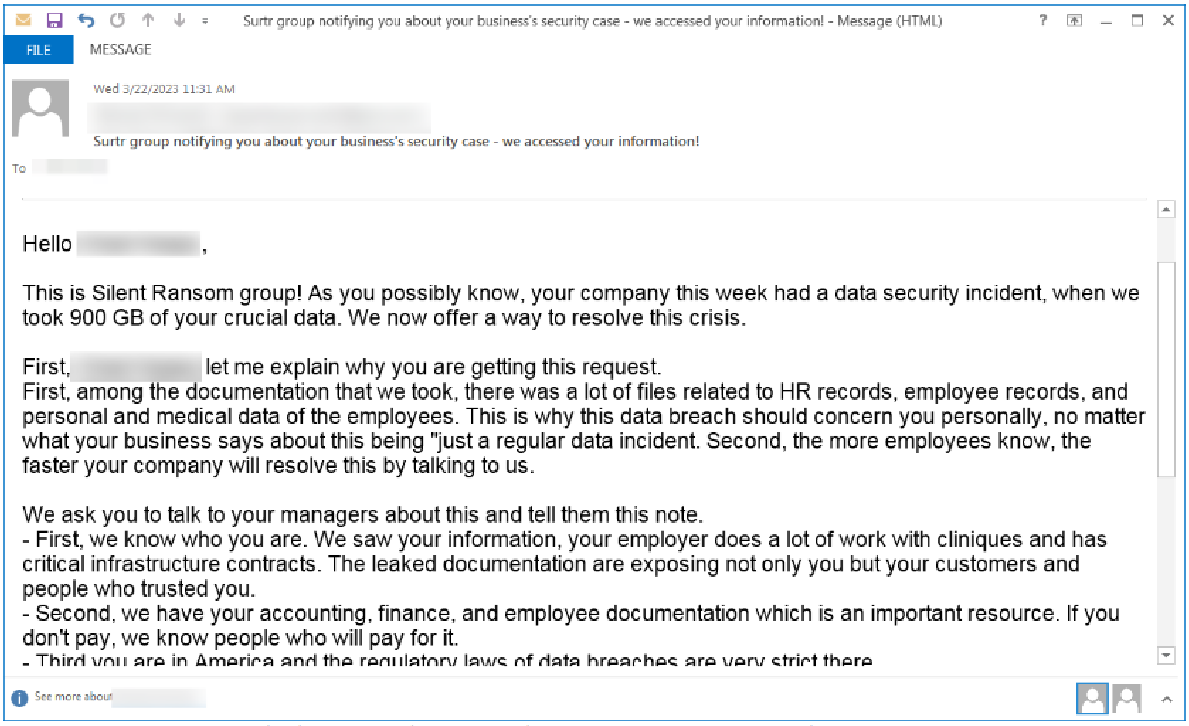
The attackers behind this activity use the name Midnight and started targeting companies in the U.S. since at least March 16.

They have also impersonated some ransomware and data extortion gangs in emails and claimed to be the authors of the intrusion, stealing hundreds of gigabytes of important data.

In one email to the employee of a holding company in the industry of petroleum additives, the threat actor claimed to be the Silent Ransom Group (SRG) - a splinter of the Conti syndicate focused on stealing data and extorting the victim, also known as Luna Moth. The same message, however, used in the subject line the name of another threat actor, the Surtr ransomware group, first seen to encrypt company networks in December 2021.

To resolve the case against him in New York, O'Connor pleaded guilty to conspiracy to commit computer intrusion, two counts of committing computer intrusions, making extortive communications, two counts of stalking, and making threatening communications.

In addition to the prison term, O'Connor was sentenced to three years of supervised release, and ordered to pay $794,012.64 in forfeiture.



Surtr group notifying you about your business's security case - we accessed your information! - Message (HTML)

FILE MESSAGE

Wed 3/22/2023 11:31 AM

[redacted]

Surtr group notifying you about your business's security case - we accessed your information!

To [redacted]

Hello [redacted],

This is Silent Ransom group! As you possibly know, your company this week had a data security incident, when we took 900 GB of your crucial data. We now offer a way to resolve this crisis.

First, [redacted] let me explain why you are getting this request.
First, among the documentation that we took, there was a lot of files related to HR records, employee records, and personal and medical data of the employees. This is why this data breach should concern you personally, no matter what your business says about this being "just a regular data incident. Second, the more employees know, the faster your company will resolve this by talking to us.

We ask you to talk to your managers about this and tell them this note.
- First, we know who you are. We saw your information, your employer does a lot of work with cliniques and has critical infrastructure contracts. The leaked documentation are exposing not only you but your customers and people who trusted you.
- Second, we have your accounting, finance, and employee documentation which is an important resource. If you don't pay, we know people who will pay for it.
- Third you are in America and the regulatory laws of data breaches are very strict there

See more about [redacted]

Midnight Group impersonating Surtr ransomware and Silent Ransom

source: BleepingComputer

The account "@shinji," a.k.a. "PlugWalkJoe," tweeting a screenshot of Twitter's internal tools interface, on July 15, 2020.

To be clear, the Twitter hack of July 2020 did not involve SIM-swapping. Rather, Twitter said the intruders tricked a Twitter employee over the phone into providing access to internal tools. Three others were charged along with O'Connor in the Twitter compromise. The alleged mastermind of the hack, then 17-year-old Graham Ivan Clarke from Tampa, Fla., pleaded guilty in 2021 and agreed to serve three years in prison, followed by three years probation.

This story is good reminder about the need to minimize your reliance on the mobile phone companies for securing your online identity. This means reducing the number of ways your life could be turned upside down if someone were to hijack your mobile phone number.

Most online services require users to validate a mobile phone number as part of setting up an account, but some services will let you remove your phone number after the fact. Those services that do you let you remove your phone number or disable SMS/phone calls for account recovery probably also offer more secure multi-factor authentication options, such as app-based one-time passwords and security keys. Check out 2fa.directory for a list of multi-factor options available across hundreds of popular sites and services.

Source: https://krebsonsecurity.com/2023/06/u-k-cyber-thug-plugwalkjoe-gets-5-years-in-prison/

2. SMS Phishers Harvested Phone Numbers, Shipment Data from UPS Tracking Tool

The United Parcel Service (UPS) says fraudsters have been harvesting phone numbers and other information from its online shipment tracking tool in Canada to send highly targeted SMS phishing (a.k.a. "smishing") messages that spoofed UPS and other top brands. The missives addressed recipients by name, included details about recent orders, and warned that those orders wouldn't be shipped unless the customer paid an added delivery fee.

In a snail mail letter sent this month to Canadian customers, UPS Canada Ltd. said it is aware that some package recipients have received fraudulent text messages demanding payment before a package can be delivered, and that it has been working with partners in its delivery chain to try to understand how the fraud was occurring.

In April 2022, KrebsOnSecurity heard from Alex, the CEO of a technology company in Canada who asked to leave his last name out of this story. Alex reached out when he began receiving the smishing messages almost immediately after ordering two sets of Airpods directly from Apple's website.

What puzzled Alex most was that he'd instructed Apple to send the Airpods as a gift to two different people, and less than 24 hours later the phone number he uses for his Apple account received two of the phishing messages, both of which contained salutations that included the names of the people for whom he'd bought Airpods.

"I'd put the recipient as different people on my team, but because it was my phone number on both orders I was the one getting the texts," Alex explained. "That same day, I got text messages referring to me as two different people, neither of whom were me."

Alex said he believes UPS Canada either doesn't fully understand what happened yet, or it is being coy about what it knows. He said the wording of UPS's response misleadingly suggests the smishing attacks were somehow the result of hackers randomly looking up package information via the company's tracking website.

Alex said it's likely that whoever is responsible figured out how to query the UPS Canada website for only pending orders from specific brands, perhaps by exploiting some type of application programming interface (API) that UPS Canada makes or made available to its biggest retail partners.

"It wasn't like I put the order through [on Apple.ca] and some days or weeks later I got a targeted smishing attack," he said. "It was more or less the same day. And it was as if [the phishers] were being notified the order existed."

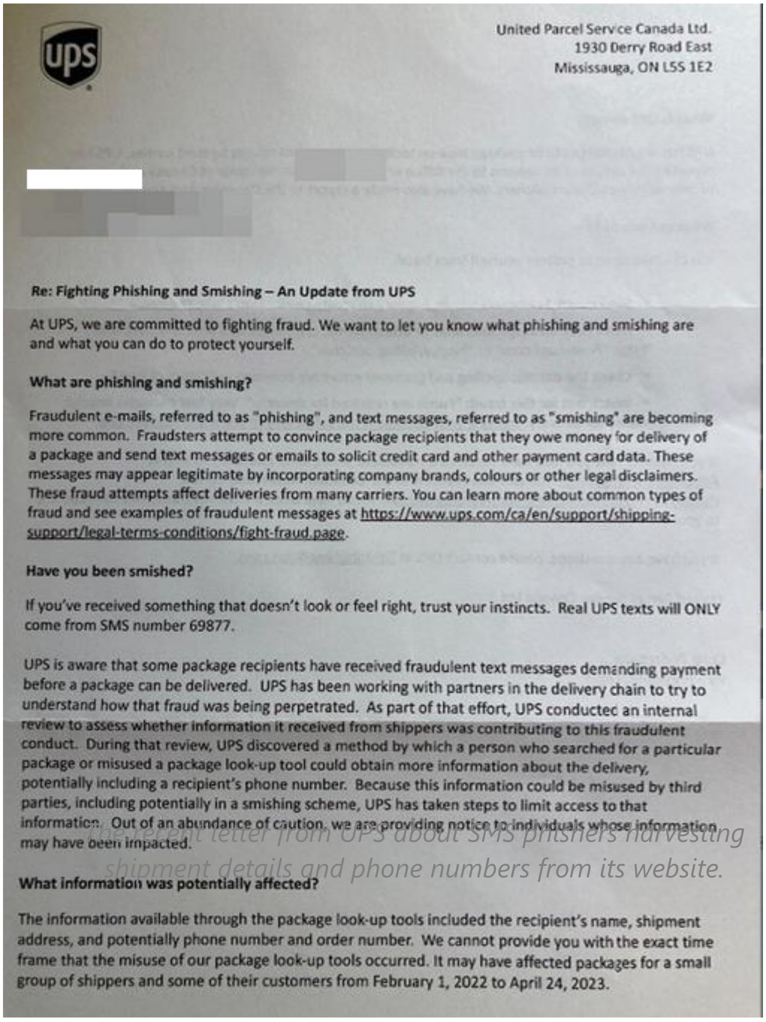
The letter to UPS Canada customers does not mention whether any other customers in North America were affected, and it remains unclear whether any UPS customers outside of Canada may have been targeted.

In a statement provided to KrebsOnSecurity, Sandy Springs, Ga. based UPS [NYSE:UPS] said the company has been working with partners in the delivery chain to understand how that fraud was being perpetrated, as well as with law enforcement and third-party experts to identify the cause of this scheme and to put a stop to it.

“Law enforcement has indicated that there has been an increase in smishing impacting a number of shippers and many different industries,” reads an email from Brian Hughes, director of financial and strategy communications at UPS.

“Out of an abundance of caution, UPS is sending privacy incident notification letters to individuals in Canada whose information may have been impacted,” Hughes said. “We encourage our customers and general consumers to learn about the ways they can stay protected against attempts like this by visiting the UPS Fight Fraud website.”

“During that review, UPS discovered a method by which a person who searched for a particular package or misused a package look-up tool could obtain more information about the delivery, potentially including a recipient’s phone number,” the letter reads. “Because this information could be misused by third parties, including potentially in a smishing scheme, UPS has taken steps to limit access to that information.”



United Parcel Service Canada Ltd.
1930 Derry Road East
Mississauga, ON L5S 1E2

[redacted]

Re: Fighting Phishing and Smishing – An Update from UPS

At UPS, we are committed to fighting fraud. We want to let you know what phishing and smishing are and what you can do to protect yourself.

What are phishing and smishing?

Fraudulent e-mails, referred to as "phishing", and text messages, referred to as "smishing" are becoming more common. Fraudsters attempt to convince package recipients that they owe money for delivery of a package and send text messages or emails to solicit credit card and other payment card data. These messages may appear legitimate by incorporating company brands, colours or other legal disclaimers. These fraud attempts affect deliveries from many carriers. You can learn more about common types of fraud and see examples of fraudulent messages at https://www.ups.com/ca/en/support/shipping-support/legal-terms-conditions/fight-fraud.page.

Have you been smished?

If you’ve received something that doesn’t look or feel right, trust your instincts. Real UPS texts will ONLY come from SMS number 69877.

UPS is aware that some package recipients have received fraudulent text messages demanding payment before a package can be delivered. UPS has been working with partners in the delivery chain to try to understand how that fraud was being perpetrated. As part of that effort, UPS conductec an internal review to assess whether information it received from shippers was contributing to this fraudulent conduct. During that review, UPS discovered a method by which a person who searched for a particular package or misused a package look-up tool could obtain more information about the delivery, potentially including a recipient’s phone number. Because this information could be misused by third parties, including potentially in a smishing scheme, UPS has taken steps to limit access to that information. Out of an abundance of caution, we are providing notice to individuals whose information may have been impacted.

What information was potentially affected?

The information available through the package look-up tools included the recipient’s name, shipment address, and potentially phone number and order number. We cannot provide you with the exact time frame that the misuse of our package look-up tools occurred. It may have affected packages for a small group of shippers and some of their customers from February 1, 2022 to April 24, 2023.

The recent letter from UPS about SMS phishers harvesting shipment details and phone numbers from its website.

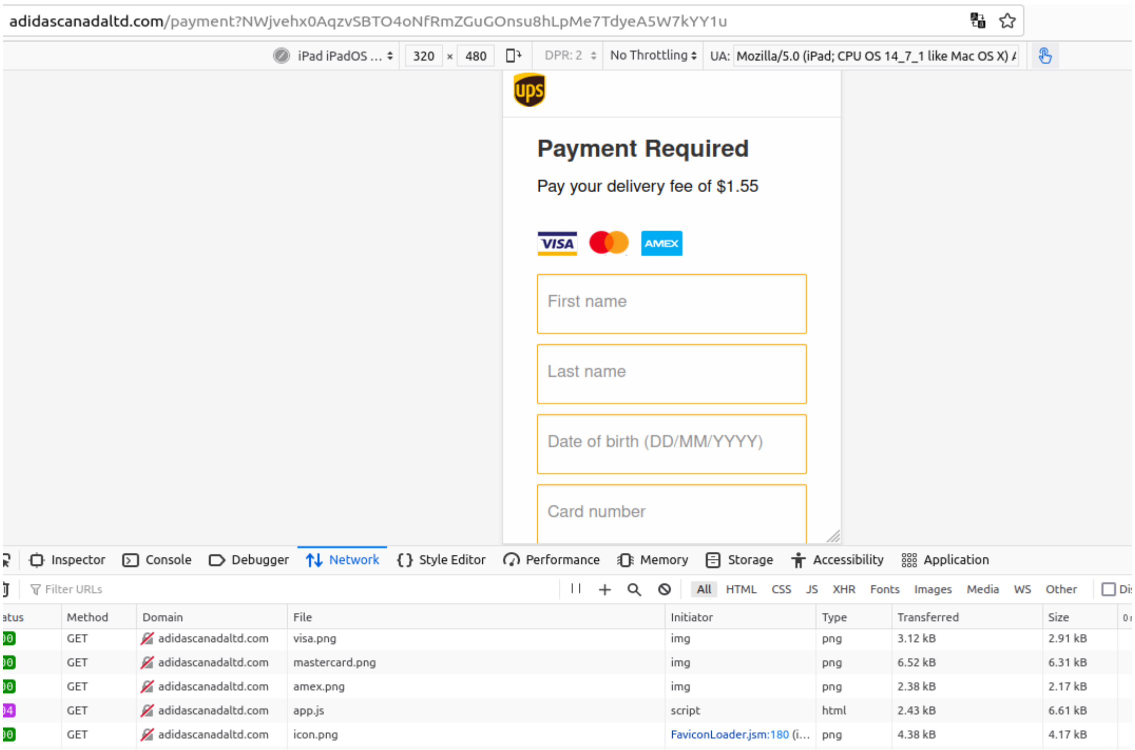
The written notice goes on to say UPS believes the data exposure “affected packages for a small group of shippers and some of their customers from February 1, 2022 to April 24, 2023.”

As early as April 2022, KrebsOnSecurity began receiving tips from Canadian readers who were puzzling over why they’d just received one of these SMS phishing messages that referenced information from a recent order they’d legitimately placed at an online retailer.

In March, 2023, a reader named Dylan from British Columbia wrote in to say he'd received one of these shipping fee scam messages not long after placing an order to buy gobs of building blocks directly from Lego.com. The message included his full name, phone number, and postal code, and urged him to click a link to mydeliveryfee-ups[.]info and pay a $1.55 delivery fee that was supposedly required to deliver his Legos.

"From searching the text of this phishing message, I can see that a lot of people have experienced this scam, which is more convincing because of the information the phishing text contains," Dylan wrote. "It seems likely to me that UPS is leaking information somehow about upcoming deliveries."

Josh is a reader who works for a company that ships products to Canada, and in early January 2023 he inquired whether there was any information about a breach at UPS Canada.



adidascanadaltd.com/payment?NWjvehx0AqzvSBTO4oNfRmZGuGOnsu8hLpMe7TdyeA5W7kYY1u

iPad iPadOS … 320 × 480 DPR: 2 No Throttling UA: Mozilla/5.0 (iPad; CPU OS 14_7_1 like Mac OS X) A

Payment Required

Pay your delivery fee of $1.55

VISA AMEX

First name

Last name

Date of birth (DD/MM/YYYY)

Card number

atus	Method	Domain	File	Initiator	Type	Transferred	Size
00	GET	adidascanadaltd.com	visa.png	img	png	3.12 kB	2.91 kB
00	GET	adidascanadaltd.com	mastercard.png	img	png	6.52 kB	6.31 kB
00	GET	adidascanadaltd.com	amex.png	img	png	2.38 kB	2.17 kB
04	GET	adidascanadaltd.com	app.js	script	html	2.43 kB	6.61 kB
00	GET	adidascanadaltd.com	icon.png	FaviconLoader.jsm:180 (i…	png	4.38 kB	4.17 kB

A smishing website targeting Canadians who recently purchased from Adidas online. The site would only load in a mobile browser.

"We've seen many of our customers targeted with a fraudulent UPS text message scheme after placing an order," Josh said. "A link is provided (often only after the customer responds to the text) which takes you to a captcha page, followed by a fraudulent payment collection page."

Pivoting on the domain in the smishing message sent to Dylan shows the phishing domain shared an Internet host in Russia [91.215.85-166] with nearly two dozen other smishing related domains, including upsdelivery[.]info, legodelivery[.]info, adidascanadaltd[.]com, crocscanadafee[.]info, refw0234apple[.]info, vista-printcanada[.]info and telus-ca[.]info.

The inclusion of big-name brands in the domains of these UPS smishing campaigns suggests the perpetrators had the ability to focus their lookups on UPS customers who had recently ordered items from specific companies.

Attempts to visit these domains with a web browser failed, but loading them in a mobile device (or in my case, emulating a mobile device using a virtual machine and Developer Tools in Firefox) revealed the first stage of this smishing attack. As Josh mentioned, what first popped up was a CAPTCHA; after the visitor solved the CAPTCHA, they were taken through several more pages that requested the user's full name, date of birth, credit card number, address, email and phone number.

Source: https://krebsonsecurity.com/2023/06/sms-phishers-harvested-phone-numbers-shipment-data-from-ups-tracking-tool/

3. Swiss government warns of ongoing DDoS attacks, data leak

Microsoft has released Sysmon 15, converting it into a protected process and adding the new 'FileExecutableDetected' option to log when executable files are created.

For those not familiar with Sysmon (or System Monitor), it is a free Microsoft Sysinternals tool that can monitor and block malicious/suspicious activity and log events to the Windows Event Log.

By default, Sysmon monitors basic events such as new process creation and the termination of processes. However, it is possible to create advanced configuration files that let you monitor various behavior, such as file deletions, Windows clipboard changes, and detecting and blocking the shredding of files.

Users can find the complete list of directives in the Sysmon schema, which can be viewed by running the sysmon -s command at the command line.

Yesterday, Microsoft released Sysmon 15.0, which includes two new features - the hardening of the program by turning it into a protected process and the ability to detect when executable files are created on the monitored system.

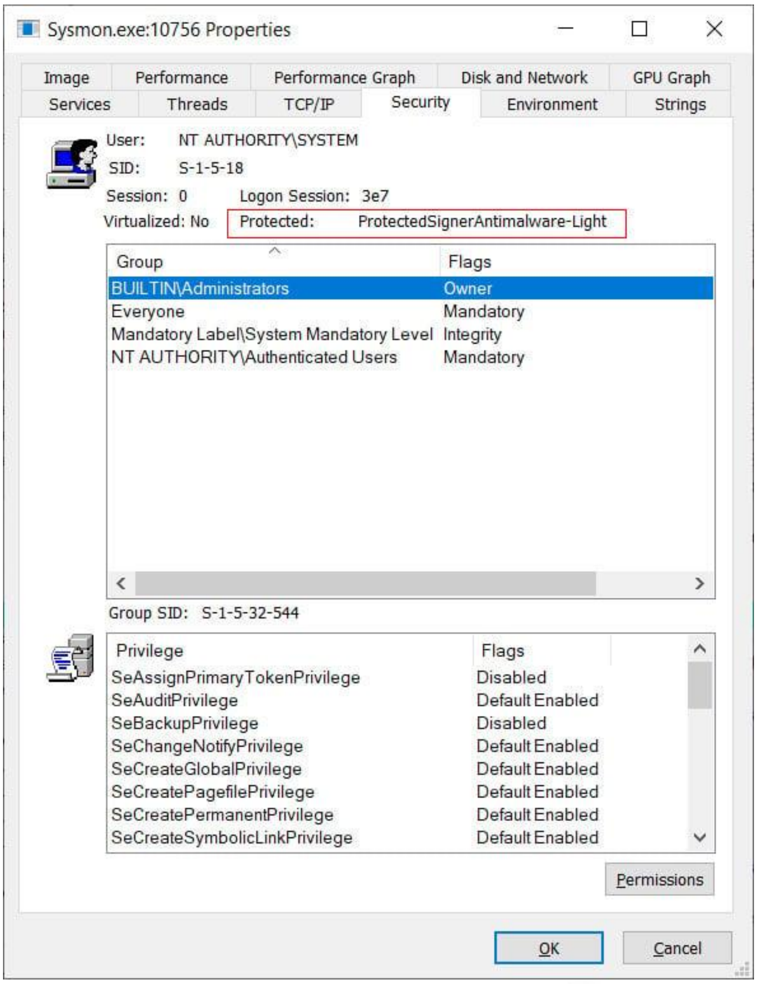
Sysmon is now a protected process

As Sysmon is commonly used to detect malicious behavior, it is in threat actors’ best interest to tamper with or disable the software.

With this release, Microsoft converted the Sysmon.exe executable into a protected process to prevent malicious code from being injected into the process.

"In Windows 8.1, a new concept of protected service has been introduced to allow anti-malware user-mode services to be launched as a protected service," explains a Microsoft article about the feature.

"After the service is launched as protected, Windows uses code integrity to only allow trusted code to load into the protected service. Windows also protects these processes from code injection and other attacks from admin processes."



User: NT AUTHORITY\SYSTEM
SID: S-1-5-18
Session: 0 Logon Session: 3e7
Virtualized: No Protected: ProtectedSignerAntimalware-Light

Group	Flags
BUILTIN\Administrators	Owner
Everyone	Mandatory
Mandatory Label\System Mandatory Level	Integrity
NT AUTHORITY\Authenticated Users	Mandatory

Group SID: S-1-5-32-544

Privilege	Flags
SeAssignPrimaryTokenPrivilege	Disabled
SeAuditPrivilege	Default Enabled
SeBackupPrivilege	Disabled
SeChangeNotifyPrivilege	Default Enabled
SeCreateGlobalPrivilege	Default Enabled
SeCreatePagefilePrivilege	Default Enabled
SeCreatePermanentPrivilege	Default Enabled
SeCreateSymbolicLinkPrivilege	Default Enabled

Sysmon running as a PPL process
Source: BleepingComputer

After Sysmon is launched, you can see it is a protected process by using Process Explorer and examining its Security properties, as shown below.

Source: [*https://www.bleepingcomputer.com/news/security/irs-authorized-efilecom-tax-return-software-caught-serving-js-malware/*](https://www.bleepingcomputer.com/news/security/irs-authorized-efilecom-tax-return-software-caught-serving-js-malware/)

4. Satacom delivers browser extension that steals cryptocurrency

Satacom downloader, also known as LegionLoader, is a renowned malware family that emerged in 2019. It is known to use the technique of querying DNS servers to obtain the base64-encoded URL in order to receive the next stage of another malware family currently distributed by Satacom. The Satacom malware is delivered via third-party websites. Some of these sites do not deliver Satacom themselves, but use legitimate advertising plugins that the attackers abuse to inject malicious ads into the webpages. The malicious links or ads on the sites redirect users to malicious sites such as fake file-sharing services.

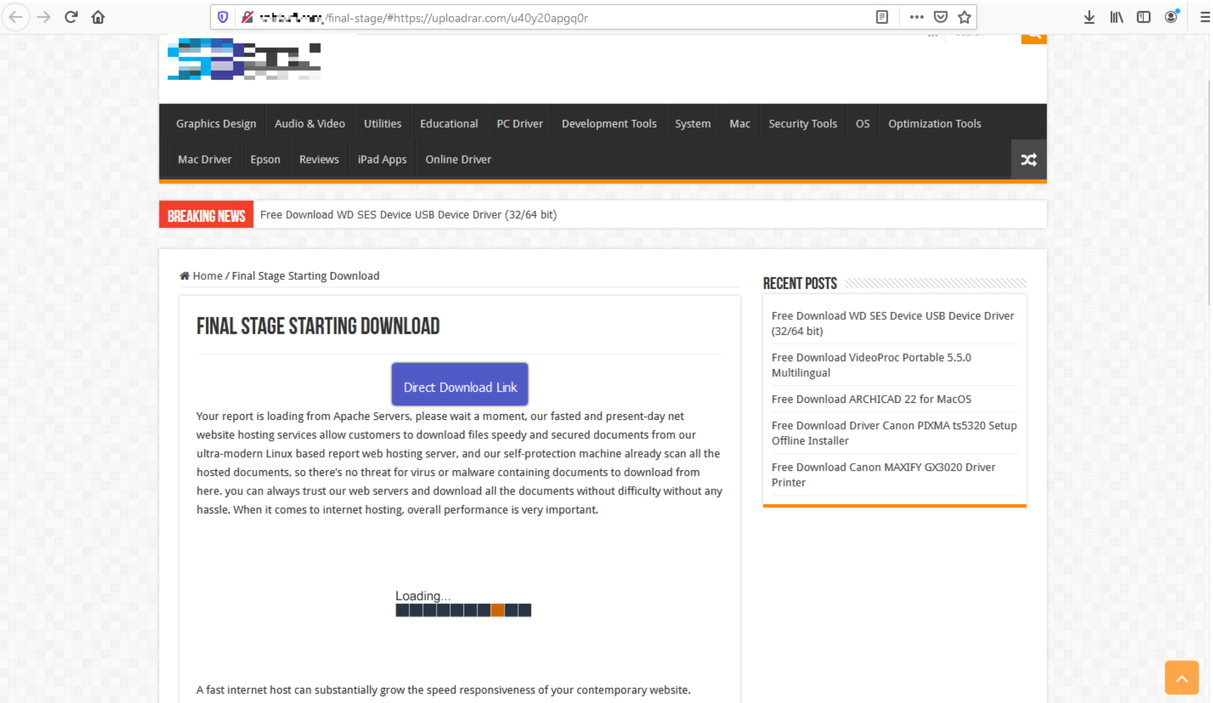
In this report we cover a recent malware distribution campaign related to the Satacom downloader. The main purpose of the malware that is dropped by the Satacom downloader is to steal BTC from the victim's account by performing web injections into targeted cryptocurrency websites. The malware attempts to do this by installing an extension for Chromium-based web browsers, which later communicates with its C2 server, whose address is stored in the BTC transaction data.

The malicious extension has various JS scripts to perform browser manipulations while the user is browsing the targeted websites, including enumeration and manipulation with cryptocurrency websites. It also has the ability to manipulate the appearance of some email services, such as Gmail, Hotmail and Yahoo, in order to hide its activity with the victim's cryptocurrencies shown in the email notifications.

Satacom technical analysis

The initial infection begins with a ZIP archive file. It is downloaded from a website that appears to mimic a software portal that allows the user to download their desired (often cracked) software for free. The archive contains several legitimate DLLs and a malicious Setup.exe file that the user needs to execute manually to initiate the infection chain.

Various types of websites are used to spread the malware. Some of them are malicious websites with a hardcoded download link, while others have the "Download" button injected through a legitimate ad plugin. In this case, even legitimate websites may have a malicious "Download" link displayed on the webpage. At the time of writing, we saw the QUADS plugin being abused to deliver Satacom.



[redacted]/final-stage/#https://uploadrar.com/u40y20apgq0r

Graphics Design | Audio & Video | Utilities | Educational | PC Driver | Development Tools | System | Mac | Security Tools | OS | Optimization Tools | Mac Driver | Epson | Reviews | iPad Apps | Online Driver

BREAKING NEWS Free Download WD SES Device USB Device Driver (32/64 bit)

Home / Final Stage Starting Download

FINAL STAGE STARTING DOWNLOAD

Direct Download Link

Your report is loading from Apache Servers, please wait a moment, our fasted and present-day net website hosting services allow customers to download files speedy and secured documents from our ultra-modern Linux based report web hosting server, and our self-protection machine already scan all the hosted documents, so there's no threat for virus or malware containing documents to download from here. you can always trust our web servers and download all the documents without difficulty without any hassle. When it comes to internet hosting, overall performance is very important.

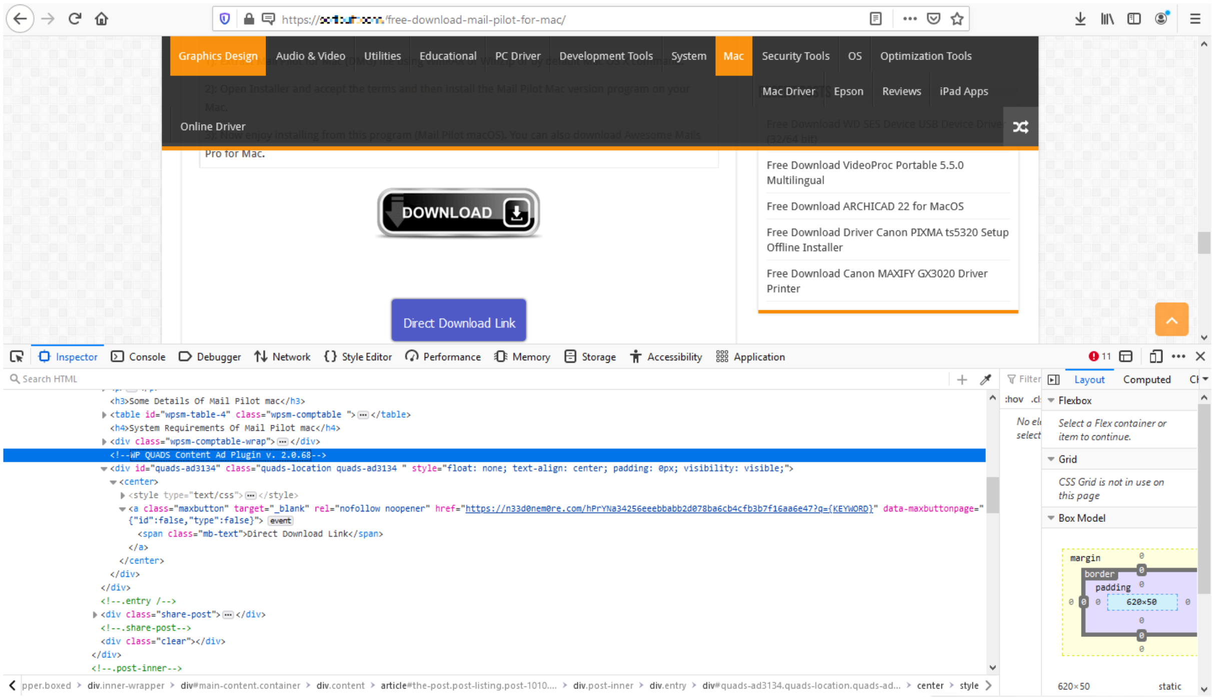
Loading...

A fast internet host can substantially grow the speed responsiveness of your contemporary website.

RECENT POSTS

- Free Download WD SES Device USB Device Driver (32/64 bit)
- Free Download VideoProc Portable 5.5.0 Multilingual
- Free Download ARCHICAD 22 for MacOS
- Free Download Driver Canon PIXMA ts5320 Setup Offline Installer
- Free Download Canon MAXIFY GX3020 Driver Printer

Websites with embedded QUADS ad plugin



https://[redacted]/free-download-mail-pilot-for-mac/

Graphics Design | Audio & Video | Utilities | Educational | PC Driver | Development Tools | System | Mac | Security Tools | OS | Optimization Tools | Mac Driver | Epson | Reviews | iPad Apps | Online Driver

Pro for Mac.

DOWNLOAD

Direct Download Link

- Free Download VideoProc Portable 5.5.0 Multilingual
- Free Download ARCHICAD 22 for MacOS
- Free Download Driver Canon PIXMA ts5320 Setup Offline Installer
- Free Download Canon MAXIFY GX3020 Driver Printer

```
<h3>Some Details Of Mail Pilot mac</h3>
<table id="wpsm-table-4" class="wpsm-comptable ">…</table>
<h4>System Requirements Of Mail Pilot mac</h4>
<div class="wpsm-comptable-wrap">…</div>
<!--WP QUADS Content Ad Plugin v. 2.0.68-->
<div id="quads-ad3134" class="quads-location quads-ad3134 " style="float: none; text-align: center; padding: 0px; visibility: visible;">
  <center>
    <style type="text/css">…</style>
    <a class="maxbutton" target="_blank" rel="nofollow noopener" href="https://n33d0nem0re.com/hPrYNa34256eeebbabb2d078ba6cb4cfb3b7f16aa6e47?q={KEYWORD}" data-maxbuttonpage="
    {"id":false,"type":false}"> event
      <span class="mb-text">Direct Download Link</span>
    </a>
  </center>
</div>
</div>
<!--.entry /-->
<div class="share-post">…</div>
<!--.share-post-->
<div class="clear"></div>
</div>
<!--.post-inner-->
```

pper.boxed > div.inner-wrapper > div#main-content.container > div.content > article#the-post.post-listing.post-1010.... > div.post-inner > div.entry > div#quads-ad3134.quads-location.quads-ad... > center > style

WP QUADS ad plugin within the website’s content

After the user clicks on the download button or link, there’s a chain of redirects that automatically takes them through various servers to reach a website masquerading as a file-sharing service to distribute the malware. In the screenshot below, we can see examples of websites that are the final destinations of the redirection chains.

After the user downloads and extracts the ZIP archive, which is about 7MB in size, a few binaries, EXE and DLL files are revealed. The DLLs are legitimate libraries, but the 'Setup.exe' file is a malicious binary. It is about 450MB, but is inflated with null bytes to make it harder to analyze. The original size of the file without the added null bytes is about 5MB and it is an Inno Setup type file.

Inno Setup installers usually work as follows: at runtime the binary extracts a child installer to a temporary folder with the name 'Setup.tmp'. Then it runs the child installer 'Setup.tmp' file that needs to communicate with the primary installer with arguments pointing to the location of the original 'Setup.exe' and its packages in order to retrieve the BIN data inside the 'Setup.exe' file for the next step of the installation.

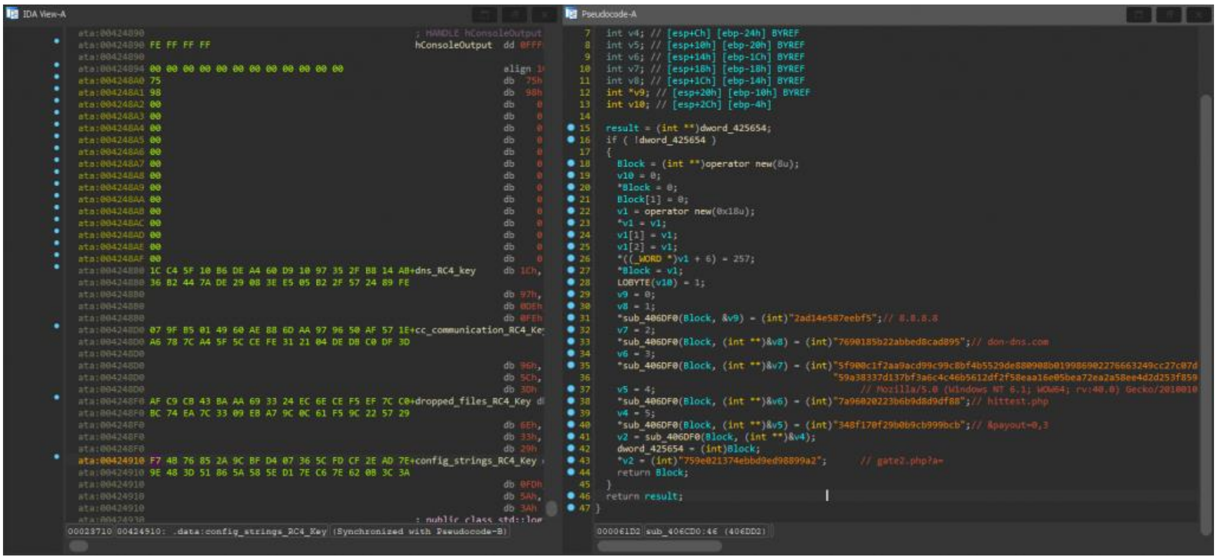
In the case of the Satacom installer, the Setup.tmp file, once running, creates a new PE DLL file in the Temp directory. After the DLL is created, the child installer loads it into itself and runs a function from the DLL.

It then decrypts the payload of Satacom and creates a new sub-process of 'explorer.exe' in order to inject the malware into the 'explorer.exe' process.

Based on the behavior we observed, we can conclude that the malware performs a common process injection technique on the remote 'explorer.exe' process called process hollowing. This is a known technique used to evade detection by AV applications.

The malicious payload that's injected into the 'explorer.exe' process uses the RC4 encryption implementation to decrypt its configuration data, communication strings and data for the other dropped binaries on the victim's machine. The encrypted data is stored inside the malicious payload.

The malware uses different hardcoded keys to decrypt the data at each step. There are four different RC4 keys that the malware uses to perform its actions, first decrypting the HEX string data to use it for its initial communication purposes.



```
ata:00424890                                                    ; HANDLE hConsoleOutput
ata:00424890 FE FF FF FF                                        hConsoleOutput  dd 0FFF
ata:00424890
ata:00424894 00 00 00 00 00 00 00 00 00 00 00 00                align 1
ata:004248A0 75                                                 db  75h
ata:004248A1 98                                                 db  98h
ata:004248A2 00                                                 db    0
ata:004248A3 00                                                 db    0
ata:004248A4 00                                                 db    0
ata:004248A5 00                                                 db    0
ata:004248A6 00                                                 db    0
ata:004248A7 00                                                 db    0
ata:004248A8 00                                                 db    0
ata:004248A9 00                                                 db    0
ata:004248AA 00                                                 db    0
ata:004248AB 00                                                 db    0
ata:004248AC 00                                                 db    0
ata:004248AD 00                                                 db    0
ata:004248AE 00                                                 db    0
ata:004248AF 00                                                 db    0
ata:004248B0 1C C4 5F 10 B6 DE A4 60 D9 10 97 35 2F B8 14 A8+dns_RC4_key     db 1Ch,
ata:004248B0 36 B2 44 7A DE 29 08 3E E5 05 B2 2F 57 24 89 FE
ata:004248B0                                                    db 97h,
ata:004248B0                                                    db 0DEh
ata:004248B0                                                    db 0FEh
ata:004248D0 07 9F B5 01 49 60 AE B8 6D AA 97 96 50 AF 57 1E+cc_communication_RC4_Ke
ata:004248D0 A6 78 7C A4 5F 5C CE FE 31 21 04 DE DB C0 DF 3D
ata:004248D0
ata:004248D0                                                    db 96h,
ata:004248D0                                                    db 5Ch,
ata:004248D0                                                    db 3Dh
ata:004248F0 AF C9 CB 43 BA AA 69 33 24 EC 6E CE F5 EF 7C C0+dropped_files_RC4_Key d
ata:004248F0 BC 74 EA 7C 33 09 E8 A7 9C 0C 61 F5 9C 22 57 29
ata:004248F0                                                    db 6Eh,
ata:004248F0                                                    db 33h,
ata:004248F0                                                    db 29h
ata:00424910 F7 48 76 85 2A 9C BF D4 07 36 5C FD CF 2E AD 7E+config_strings_RC4_Key
ata:00424910 9E 48 3D 51 86 5A 58 5E D1 7E C6 7E 62 0B 3C 3A
ata:00424910                                                    db 0FDh
ata:00424910                                                    db 5Ah,
ata:00424910                                                    db 3Ah
ata:00424930                                                 ; public class std::lo
00023710 00424910: .data:config_strings_RC4_Key (Synchronized with Pseudocode-B)
```

```
int v4; // [esp+Ch] [ebp-24h] BYREF
int v5; // [esp+10h] [ebp-20h] BYREF
int v6; // [esp+14h] [ebp-1Ch] BYREF
int v7; // [esp+18h] [ebp-18h] BYREF
int v8; // [esp+1Ch] [ebp-14h] BYREF
int *v9; // [esp+20h] [ebp-10h] BYREF
int v10; // [esp+2Ch] [ebp-4h]

result = (int **)dword_425654;
if ( !dword_425654 )
{
  Block = (int **)operator new(8u);
  v10 = 0;
  *Block = 0;
  Block[1] = 0;
  v1 = operator new(0x18u);
  *v1 = v1;
  v1[1] = v1;
  v1[2] = v1;
  *((_WORD *)v1 + 6) = 257;
  *Block = v1;
  LOBYTE(v10) = 1;
  v9 = 0;
  v8 = 1;
  *sub_406DF0(Block, &v9) = (int)"2ad14e587eebf5";// 8.8.8.8
  v7 = 2;
  *sub_406DF0(Block, (int **)&v8) = (int)"7690185b22abbed8cad895";// don-dns.com
  v6 = 3;
  *sub_406DF0(Block, (int **)&v7) = (int)"5f900c1f2aa9acd99c99c8bf4b5529de880908b01998690227666 3249cc27c07d
                                         "59a38337d137bf3a6c4c46b5612df2f58eaa16e05bea72ea2a58ee4d2d253f859
                                                    // Mozilla/5.0 (Windows NT 6.1; WOW64; rv:40.0) Gecko/2010010
  v5 = 4;
  *sub_406DF0(Block, (int **)&v6) = (int)"7a96020223b6b9d8d9df88";// hittest.php
  v4 = 5;
  *sub_406DF0(Block, (int **)&v5) = (int)"348f170f29b0b9cb999bcb";// &payout=0,3
  v2 = sub_406DF0(Block, (int **)&v4);
  dword_425654 = (int)Block;
  *v2 = (int)"759e021374ebbd9ed98899a2";      // gate2.php?a=
  return Block;
}
return result;
}
000061D2 sub_406CD0:46 (406DD2)
```

RC4 keys (left pane) and encrypted HEX strings (right pane)

In the screenshot above, the left pane shows the four RC4 hardcoded keys as HEX strings, and in the right pane we can see the HEX strings that are decrypted using the RC4 'config_strings' key to get the strings for the first initialization of communication with the C2. If we decrypt the strings ourselves using the key, we get the result shown in the screenshot.

Once the HEX strings are decrypted, 'explorer.exe' initiates its first communication. To do so, it performs a DNS request to don-dns[.]com (a decrypted HEX string) through Google DNS (8.8.8.8, another decrypted string) and it queries for the TXT record.

Source: https://securelist.com/satacom-delivers-cryptocurrency-stealing-browser-extension/109807/

5. Cracking the Code — How Machine Learning Supercharges Threat Detection

In the second episode of the "This Is How We Do It" series, we dive further into the dynamics of security operations centers (SOCs) with Devin Johnstone, a senior staff security engineer (SOC Ops Specialist) at Palo Alto Networks. David Szabo, sales enablement consultant, conducts the interview, discussing the structure of SOC teams and their essential players. Johnstone shares his experience working in SOC teams of various sizes and explains how to build a new SOC from scratch.

The needs of a security team may vary depending on the organization, according to Johnstone. At Palo Alto Networks, the SOC started with just two managers and three analysts six years ago, but a lot has changed:

“As companies grow and mature, it does usually happen that IT and security will separate. That happened for us around that 2017 timeframe and now we've grown to he 22 full-time employees that we have here in the SOC today. And of those 22, 10 are in the traditional analyst role where they're actually looking at alerts coming off the technology and doing threat hunting. And then the rest of us on the team support those analysts by enabling tooling, logging — giving them the alert data and the insights they need in order to be successful.”

Palo Alto Networks employs a red team, a group of full-time employees dedicated to attacking the company's systems, also known as “penetration testing.” They operate quarterly exercises where they select a target and attempt to breach it without the SOC's knowledge. If the SOC identifies a potential attack during the exercise, they consult with the red team to avoid wasting resources on internal investigations. The red team provides valuable feedback and insights to help the SOC improve their defenses.

“Our red team are full-time employees whose job is to test our defenses. They'll pick a target. It's always new, so they're not repeating something that's going to be easy and something that the SOC is going to find fast. They first get approval for it because they want to make sure that leadership is going to be okay with them potentially attacking an internal system, and they go pretty far.”

They're that good sometimes that we are even reaching that point and questioning, ‘Is this them or not?’ And they'll go about their attack in secret as long as they can for three months. If we find something in the SOC, on the blue team side of the house, and determine it might be the red team, we check with them to confirm, so we don't spend too much time chasing down our own internal team and then either stop the exercise or finish. At the end of the exercise, we do a debrief where they report on everything that they did, which gives us in the SOC a literal checklist where we can go back and say, ‘We saw this, we didn't see this, we need to build a new alert here. We need to build new automation here.’ And we get that feedback.”

In addition to automation capabilities in cybersecurity, the advancement of artificial intelligence (AI) has sparked both excitement and concern. ChatGPT, a language-based machine learning model, is not exempt from this discussion. While ChatGPT presents promising opportunities in cybersecurity, it also raises ethical considerations. Adversarial attacks, where malicious actors manipulate AI systems to deceive or exploit them, are a real concern.

Johnstone also highlights the rise of supply chain attacks, such as the SolarWinds incident, where attackers target organizations connected to the true victims. Palo Alto Networks aims to protect not only itself, but also its customers by preventing the company from becoming a gateway to widespread attacks.

When it comes to threat actors, the Palo Alto Networks Unit 42 Threat Intelligence team is monitoring the evolving landscape. Johnstone says:

> *"Our Unit 42 team publishes regular reports on the type of threat activity that they're seeing out in the wild, and it is ever-changing. There are certain groups that trend year over year. I won't name any in particular, but there is an ever-changing pool of those groups, and we have Unit 42 to help us keep tabs on them and even track activity that doesn't affect us. We want to know what they are doing in other parts of the world, so we can be aware and then also share that with all of our customers "*

Part of the work we do at Palo Alto Networks is showing our customers the information that is important to them to help them make decisions. And in those cases where we come across threat intelligence or actions of specific groups or nations or individuals that might be valuable to us or our customers, we want to share that as proudly as possible."

Palo Alto Networks uses its own products extensively within their SOC, acting as the first customer. They also collaborate closely with product teams, providing feedback and shaping roadmap decisions. The SOC relies on Cortex XSOAR as the central platform for incident management and threat intelligence. Additionally, they use a range of sensors and enforcement points, such as next-generation firewalls and Cortex XDR to monitor network activity and endpoints. The Prisma suite of products helps secure cloud services, while Cortex Xpanse provides visibility into external exposures and potential vulnerabilities:

> *"And then we've also got Cortex Xpanse which gives us the outside-in view. So, we've got a lot of sensors inside, showing us what we already know about. But because we've grown by acquisition, there's always the chance that we've got environments still lingering out on somebody else's cloud account or shadow. It is a big concern. The stuff that we don't know about we can't protect. Cortex Xpanse is going out into the cloud and finding all of those exposures that we may not have known were out there and allowing us to get control of them before they become a problem."*

Before acquiring Cortex Xpanse, Palo Alto Networks had gaps in asset discovery and monitoring. With Xpanse, we have gained the ability to identify traffic and track potential attacks, even if they weren't directly targeted. This proved invaluable during incidents like the SolarWinds attack, where Palo Alto Networks could proactively assist compromised customers.

Source: https://www.paloaltonetworks.com/blog/2023/06/cracking-the-code-how-machine-learning-supercharges-threat-detection/

6. Operation Triangulation: Zero-Click iPhone Malware

Kaspersky is reporting a zero-click iOS exploit in the wild. Mobile device backups contain a partial copy of the filesystem, including some of the user data and service databases. The timestamps of the files, folders and the database records allow to roughly reconstruct the events happening to the device. The mvt-ios utility produces a sorted timeline of events into a file called “timeline.csv,” similar to a super-timeline used by conventional digital forensic tools.

Using this timeline, we were able to identify specific artifacts that indicate the compromise. This allowed to move the research forward, and to reconstruct the general infection sequence:

- The target iOS device receives a message via the iMessage service, with an attachment containing an exploit
- Without any user interaction, the message triggers a vulnerability that leads to code execution.
- The code within the exploit downloads several subsequent stages from the C&C server, that include additional exploits for privilege escalation.
- After successful exploitation, a final payload is downloaded from the C&C server, that is a fully-featured APT platform.
- The initial message and the exploit in the attachment is deleted

The malicious toolset does not support persistence, most likely due to the limitations of the OS. The timelines of multiple devices indicate that they may be reinfected after rebooting. The oldest traces of infection that we discovered happened in 2019. As of the time of writing in June 2023, the attack is ongoing, and the most recent version of the devices successfully targeted is iOS 15.7.

Source: https://www.schneier.com/blog/archives/2023/06/operation-triangulation-zero-click-iphone-malware.html

7. AI as Sensemaking for Public Comments

It’s become fashionable to think of artificial intelligence as an inherently dehumanizing technology, a ruthless force of automation that has unleashed legions of virtual skilled laborers in faceless form. But what if AI turns out to be the one tool able to identify what makes your ideas special, recognizing your unique perspective and potential on the issues where it matters most?

You’d be forgiven if you’re distraught about society’s ability to grapple with this new technology. So far, there’s no lack of prognostications about the democratic doom that AI may wreak on the US system of government. There are legitimate reasons to be concerned that AI could spread misinformation, break public comment processes on regulations, inundate legislators with artificial constituent outreach, help to automate corporate lobbying, or even generate laws in a way tailored to benefit narrow interests.

But there are reasons to feel more sanguine as well. Many groups have started demonstrating the potential beneficial uses of AI for governance. A key constructive-use case for AI in democratic processes is to serve as discussion moderator and consensus builder.

To help democracy scale better in the face of growing, increasingly interconnected populations—as well as the wide availability of AI language tools that can generate reams of text at the click of a button—the US will need to leverage AI's capability to rapidly digest, interpret and summarize this content.

There are two different ways to approach the use of generative AI to improve civic participation and governance. Each is likely to lead to drastically different experience for public policy advocates and other people trying to have their voice heard in a future system where AI chatbots are both the dominant readers and writers of public comment.

For example, consider individual letters to a representative, or comments as part of a regulatory rulemaking process. In both cases, we the people are telling the government what we think and want.

For more than half a century, agencies have been using human power to read through all the comments received, and to generate summaries and responses of their major themes. To be sure, digital technology has helped.

In 2021, the Council of Federal Chief Data Officers recommended modernizing the comment review process by implementing natural language processing tools for removing duplicates and clustering similar comments in processes governmentwide. These tools are simplistic by the standards of 2023 AI. They work by assessing the semantic similarity of comments based on metrics like word frequency (How often did you say "personhood"?) and clustering similar comments and giving reviewers a sense of what topic they relate to.

Think of this approach as collapsing public opinion. They take a big, hairy mass of comments from thousands of people and condense them into a tidy set of essential reading that generally suffices to represent the broad themes of community feedback. This is far easier for a small agency staff or legislative office to handle than it would be for staffers to actually read through that many individual perspectives.

But what's lost in this collapsing is individuality, personality, and relationships. The reviewer of the condensed comments may miss the personal circumstances that led so many commenters to write in with a common point of view, and may overlook the arguments and anecdotes that might be the most persuasive content of the testimony.

Most importantly, the reviewers may miss out on the opportunity to recognize committed and knowledgeable advocates, whether interest groups or individuals, who could have long-term, productive relationships with the agency.

These drawbacks have real ramifications for the potential efficacy of those thousands of individual messages, undermining what all those people were doing it for. Still, practicality tips the balance toward of some kind of summarization approach. A passionate letter of advocacy doesn't hold any value if regulators or legislators simply don't have time to read it.

There is another approach. In addition to collapsing testimony through summarization, government staff can use modern AI techniques to explode it. They can automatically recover and recognize a distinctive argument from one piece of testimony that does not exist in the thousands of other testimonies received. They can discover the kinds of constituent stories and experiences that legislators love to repeat at hearings, town halls and campaign events. This approach can sustain the potential impact of individual public comment to shape legislation even as the volumes of testimony may rise exponentially.

In computing, there is a rich history of that type of automation task in what is called outlier detection. Traditional methods generally involve finding a simple model that explains most of the data in question, like a set of topics that well describe the vast majority of submitted comments. But then they go a step further by isolating those data points that fall outside the mold—comments that don't use arguments that fit into the neat little clusters.

State-of-the-art AI language models aren't necessary for identifying outliers in text document data sets, but using them could bring a greater degree of sophistication and flexibility to this procedure. AI language models can be tasked to identify novel perspectives within a large body of text through prompting alone. You simply need to tell the AI to find them.

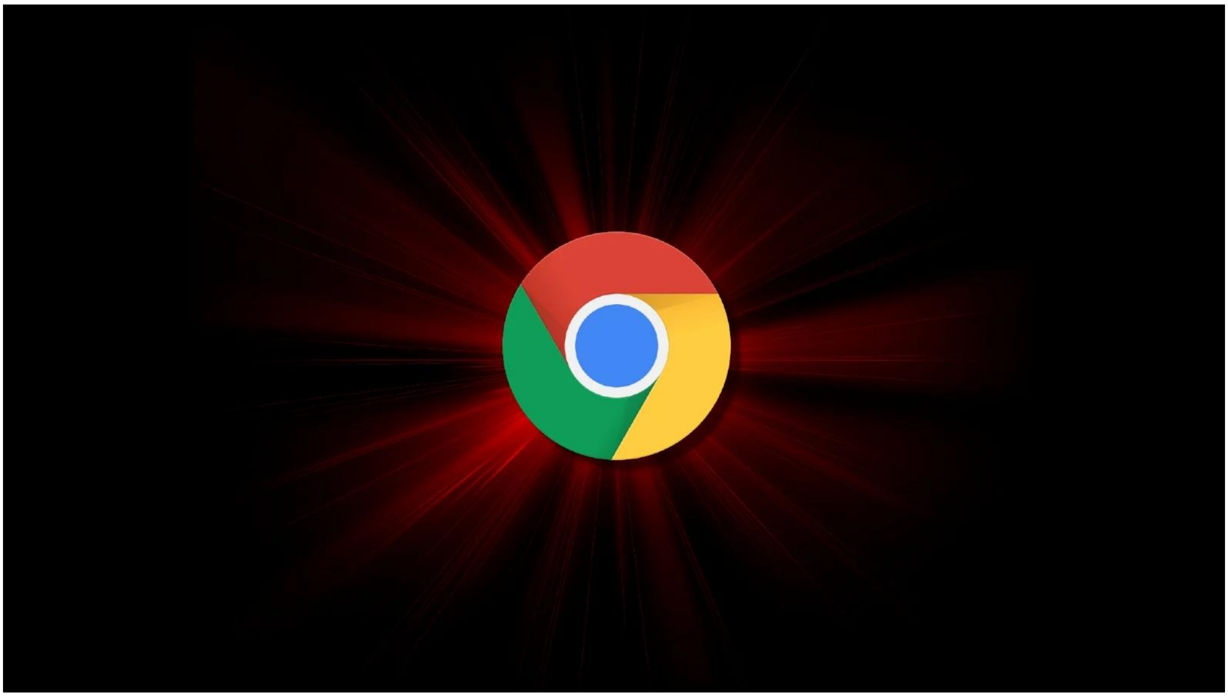
In the absence of that ability to extract distinctive comments, lawmakers and regulators have no choice but to prioritize on other factors. If there is nothing better, "who donated the most to our campaign" or "which company employs the most of my former staffers" become reasonable metrics for prioritizing public comments. AI can help elected representatives do much better.

If Americans want AI to help revitalize the country's ailing democracy, they need to think about how to align the incentives of elected leaders with those of individuals. Right now, as much as 90% of constituent communications are mass emails organized by advocacy groups, and they go largely ignored by staffers. People are channeling their passions into a vast digital warehouses where algorithms box up their expressions so they don't have to be read. As a result, the incentive for citizens and advocacy groups is to fill that box up to the brim, so someone will notice it's overflowing.

A talented, knowledgeable, engaged citizen should be able to articulate their ideas and share their personal experiences and distinctive points of view in a way that they can be both included with everyone else's comments where they contribute to summarization and recognized individually among the other comments. An effective comment summarization process would extricate those unique points of view from the pile and put them into lawmakers' hands.

Source: https://www.schneier.com/blog/archives/2023/06/ai-as-sensemaking-for-public-comments.html

8. Malicious Chrome extensions with 75M installs removed from Web Store



Google has removed from the Chrome Web Store 32 malicious extensions that could alter search results and push spam or unwanted ads. Collectively, they come with a download count of 75 million.

The extensions featured legitimate functionality to keep users unaware of the malicious behavior that came in obfuscated code to deliver the payloads.

Cybersecurity researcher Wladimir Palant analyzed the PDF Toolbox extension (2 million downloads) available from Chrome Web Store and found that it included code that was disguised as a legitimate extension API wrapper.

In a write-up in mid-May, the researcher explains that the code allowed the "serasearchtop[.]com" domain to inject arbitrary JavaScript code into any website the user visited.

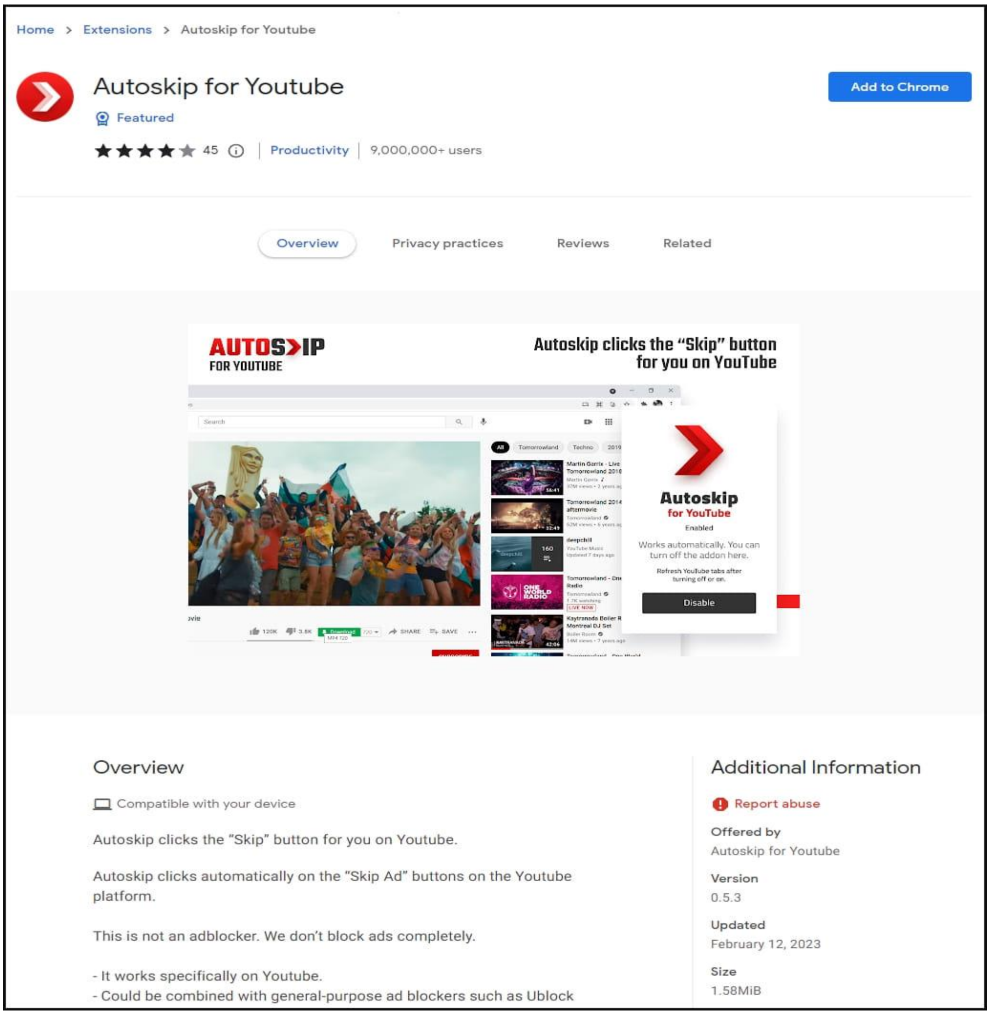
The potential for abuse ranges from inserting ads into webpages to stealing sensitive information. However, Palant didn't observe any malicious activity, so the code's purpose remained unclear.

The researcher also noticed that the code was set to activate 24 hours after installing the extension, a behavior that is typically associated with malicious intentions.

A few days ago, Palant published a follow-up post on the case to alert that he had discovered the same suspicious code in another 18 Chrome extensions with a total download count of 55 million. Some examples include:

- Autoskip for Youtube – 9 million active users
- Soundboost – 6.9 million active users
- Crystal Ad block – 6.8 million active users
- Brisk VPN – 5.6 million active users
- Clipboard Helper – 3.5 million active usersMaxi Refresher – 3.5 million active users

At the time of Palant publishing the second post, all of the extensions were still available in the Chrome Web Store.



Autoskip for Youtube

Autoskip clicks the "Skip" button for you on YouTube

Autoskip for YouTube

Enabled

Works automatically. You can turn off the addon here.

Refresh YouTube tabs after turning off or on.

Overview

Compatible with your device

Autoskip clicks the "Skip" button for you on Youtube.

Autoskip clicks automatically on the "Skip Ad" buttons on the Youtube platform.

This is not an adblocker. We don't block ads completely.

- It works specifically on Youtube.
- Could be combined with general-purpose ad blockers such as Ublock

Additional Information

Offered by
Autoskip for Youtube

Version
0.5.3

Updated
February 12, 2023

Size
1.58MiB

Continuing his investigation, Palant found two variants of the code: one masquerading as Mozilla's WebExtension browser API Polyfill, and another posing as the Day.js library.

However, both versions featured the same arbitrary JS code injection mechanism involving serasearchtop[.]com.

Although the researcher did not observe any clear malicious activity, he noted that there are numerous user reports and reviews on the Web Store indicating that the extensions were performing redirections and search result hijacking.

Despite his attempts to report the suspicious extensions to Google, they continued to be available to users from the Chrom Web Store.

Earlier today, though, cybersecurity company Avast said that it reported the extensions to Google after confirming their malicious nature, and expanded the list to 32 entries. Collectively, these boasted 75 million installs.

Avast says that while the extensions appear harmless to unsuspecting users, they are adware that hijacks search results to display sponsored links and paid results, sometimes even serving malicious links.

Responding to a request for comment from BleepingComputer before Avast published its findings, a Google spokesperson said that the "reported extensions have been removed from the Chrome Web Store."

“We take security and privacy claims against extensions seriously, and when we find extensions that violate our policies, we take appropriate action.”

> *“The Chrome Web Store has policies in place to keep users safe that all developers must adhere to," the Google representative told BleepingComputer”*

Avast highlights the significant impact of the extensions, which targeted tens of thousands of its customers, and potentially millions worldwide.

For its customers, Avast selectively neutralized only the malicious elements within the extensions, letting the legitimate features continue operating without disruption.

While the 75 million downloads looks worrying, the company suspects that the count was "artificially inflated." A complete list of the malicious extensions (IDs) can be found on Avast’s report.

Users should note that the removal of the extensions from the Chrome Web Store does not automatically deactivate or uninstall them from their browsers, so manual action is required to eliminate the risk.

Source: https://www.bleepingcomputer.com/news/security/malicious-chrome-extensions-with-75m-installs-removed-from-web-store/

9. New Horabot campaign takes over victims Gmail, Outlook accounts

A previously unknown campaign involving the Horabot botnet malware has targeted Spanish-speaking users in Latin America since at least November 2020, infecting them with a banking trojan and spam tool.

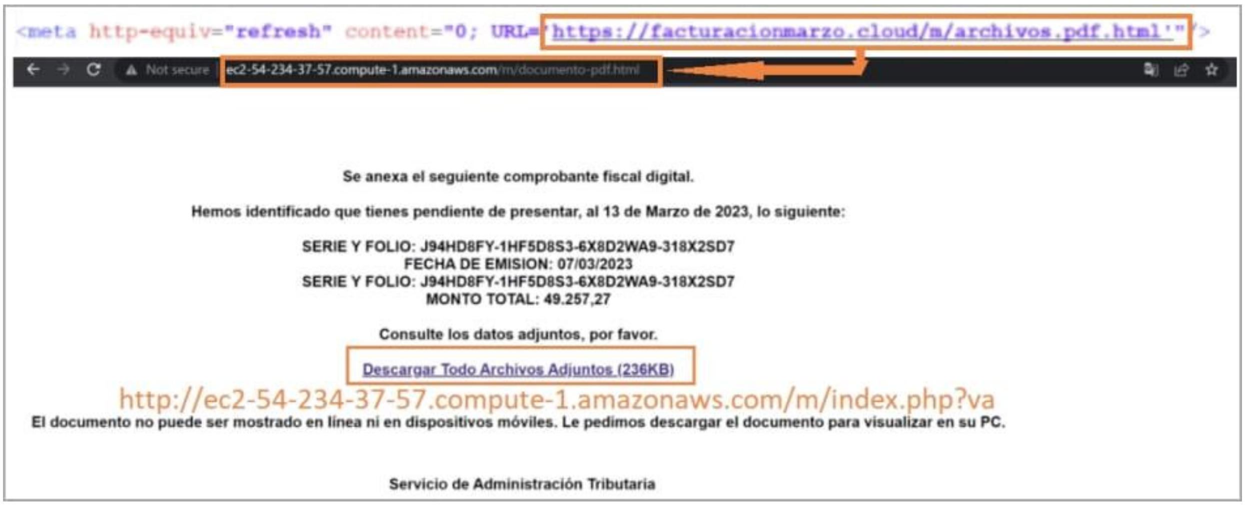
The malware enables the operators to take control of the victim's Gmail, Outlook, Hotmail, or Yahoo email accounts, steal email data and 2FA codes arriving in the inbox, and send phishing emails from the compromised accounts.

The new Horabot operation was discovered by analysts at Cisco Talos, who report that the threat actor behind it is likely based in Brazil.

Starts with phishing

The multi-stage infection chain begins with a tax-themed phishing email sent to the target, with an HTML attachment that is supposedly a payment receipt.

Opening the HTML launches a URL redirection chain that lands the victim on an HTML page hosted on an attacker-controlled AWS instance.



```
<meta http-equiv="refresh" content="0; URL='https://facturacionmarzo.cloud/m/archivos.pdf.html'"/>
```

Not secure
ec2-54-234-37-57.compute-1.amazonaws.com/m/documento-pdf.html

Se anexa el seguiente comprobante fiscal digital.

Hemos identificado que tienes pendiente de presentar, al 13 de Marzo de 2023, lo siguiente:

SERIE Y FOLIO: J94HD8FY-1HF5D8S3-6X8D2WA9-318X2SD7
FECHA DE EMISION: 07/03/2023
SERIE Y FOLIO: J94HD8FY-1HF5D8S3-6X8D2WA9-318X2SD7
MONTO TOTAL: 49.257,27

Consulte los datos adjuntos, por favor.

Descargar Todo Archivos Adjuntos (236KB)

http://ec2-54-234-37-57.compute-1.amazonaws.com/m/index.php?va

El documento no puede ser mostrado en línea ni en dispositivos móviles. Le pedimos descargar el documento para visualizar en su PC.

Servicio de Administración Tributaria

The victim clicks on the hyperlink on the page and downloads a RAR archive that contains a batch file with a CMD extension, which downloads a PowerShell script that fetches trojan DLLs and a set of legitimate executables from the C2 server.

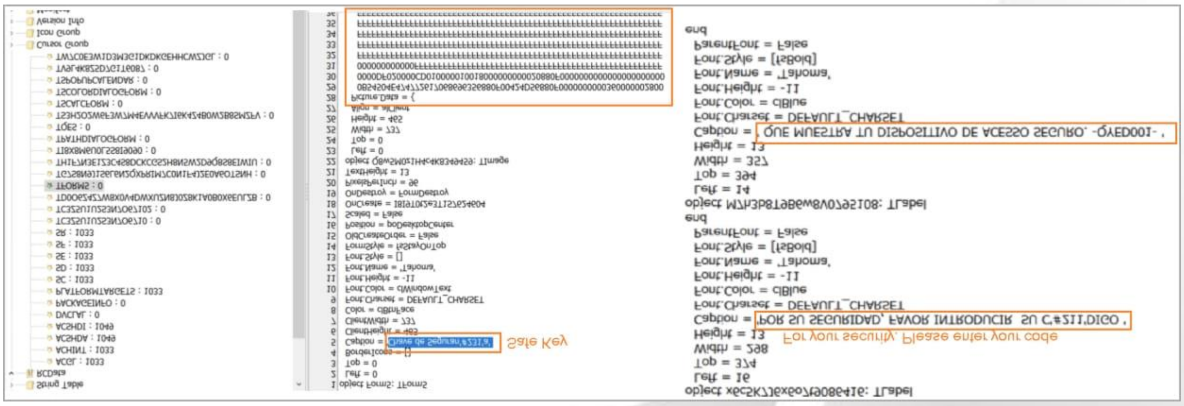
These trojans execute to fetch the final two payloads from a different C2 server. One is a PowerShell downloader script, and the other is the Horabot binary.

Banking trojan

One of the DLL files in the downloaded ZIP, "jli.dll," which is sideloaded by the "kinit.exe" executable, is a banking trojan written in Delphi.

It targets system info (language, disk size, antivirus software, hostname, OS version, IP address), user credentials, and activity data.

Moreover, the trojan also offers its operators remote access capabilities like performing file actions and can also conduct keylogging, screenshot snapping, and mouse event tracking. When the victim opens an application, the trojan overlays a fake window on top of it to trick victims into entering sensitive data like online banking account credentials or one-time codes.



```
object Form5: TForm5
  Left = 0
  Top = 0
  BorderIcons = []
  Caption = 'Clave de Seguran'#231'a'
  ClientHeight = 465
  ClientWidth = 737
  Color = clBtnFace
  Font.Charset = DEFAULT_CHARSET
  Font.Color = clWindowText
  Font.Height = -11
  Font.Name = 'Tahoma'
  Font.Style = []
  FormStyle = fsStayOnTop
  OldCreateOrder = False
  Position = poDesktopCenter
  Scaled = False
  OnCreate = 18I9T0t2e3T1S27e24e04
  OnDestroy = FormDestroy
  PixelsPerInch = 96
  TextHeight = 13
  object Q8wSM0zIH4c4K8349459: TImage
    Left = 0
    Top = 0
    Width = 737
    Height = 465
    Align = alClient
    Picture.Data = {
      0B54504E474772617068696332880F00424D56880F000000000003E0000002800
      0000DF020000CD01000001001800000000002088 0F000000000000000000000000
      000000000000FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
      FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
      FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
      FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
      FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
```

Safe Key

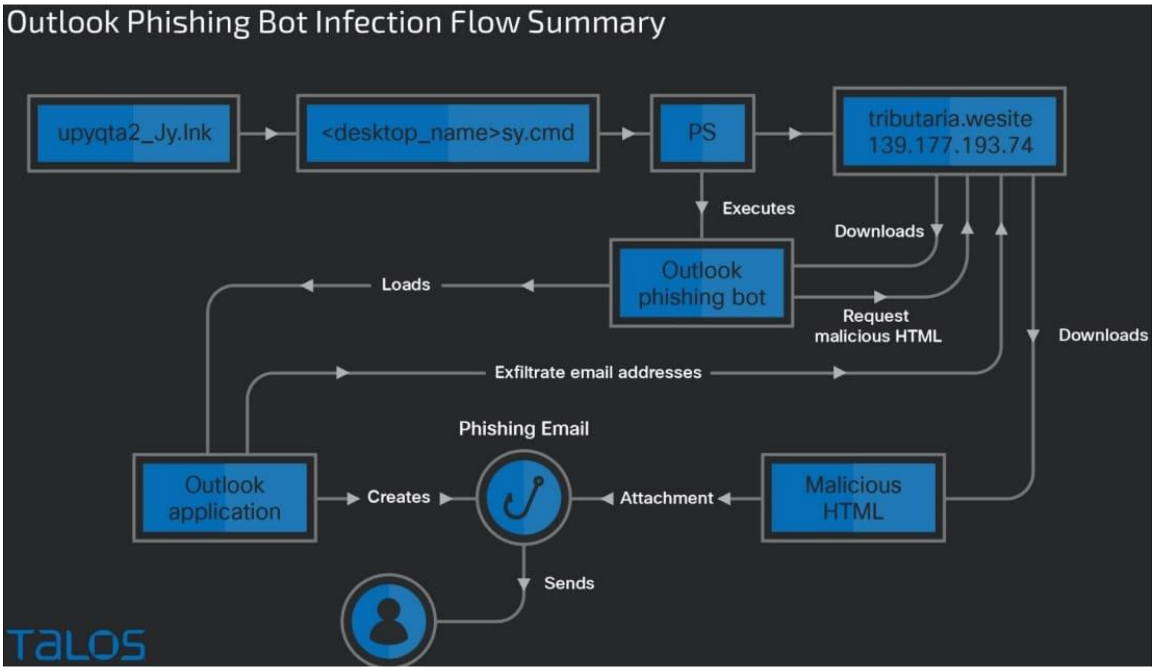
```
object xec5K71ex6o7f9086416: TLabel
  Left = 16
  Top = 374
  Width = 298
  Height = 13
  Caption = 'POR SU SEGURIDAD, FAVOR INTRODUCIR  SU C'#211'DIGO '
  Font.Charset = DEFAULT_CHARSET
  Font.Color = clBlue
  Font.Height = -11
  Font.Name = 'Tahoma'
  Font.Style = [fsBold]
  ParentFont = False
end
object M7H3b8T9Bem8V0795108: TLabel
  Left = 14
  Top = 394
  Width = 327
  Height = 13
  Caption = ' QUE MUESTRA TU DISPOSITIVO DE ACESSO SEGURO.  -QYED001- '
  Font.Charset = DEFAULT_CHARSET
  Font.Color = clBlue
  Font.Height = -11
  Font.Name = 'Tahoma'
  Font.Style = [fsBold]
  ParentFont = False
end
```

For your security, Please enter your code

Code for creating phishing forms (Cisco)

All extracted email addresses are written into an ".Outlook" file and then encoded and exfiltrated to the C2 server.

Finally, the malware creates an HTML file locally, fills it with content copied from an external resource, and sends phishing emails to all extracted email addresses individually.



All extracted email addresses are written into an ".Outlook" file and then encoded and exfiltrated to the C2 server.

Finally, the malware creates an HTML file locally, fills it with content copied from an external resource, and sends phishing emails to all extracted email addresses individually.

Source: *https://www.bleepingcomputer.com/news/security/new-horabot-campaign-takes-over-victims-gmail-outlook-accounts/*

10. Lazarus hackers linked to the $35 million Atomic Wallet Heist

The notorious North Korean hacking group known as Lazarus has been linked to the recent Atomic Wallet hack, resulting in the theft of over $35 million in crypto.

This attribution is from the blockchain experts at Elliptic, who have been tracking the stolen funds and their movements across wallets, mixers, and other laundering pathways.

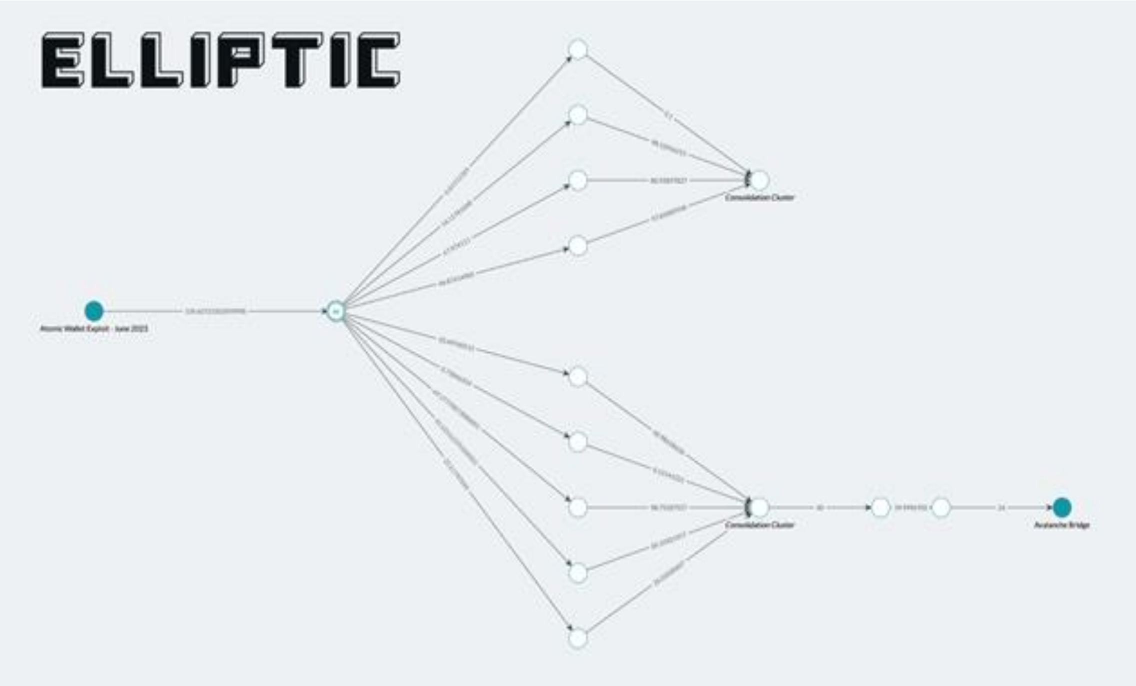
The attack on Atomic Wallet occurred last weekend when numerous users reported that their wallets were compromised and their funds had been stolen.

While the investigation into the incident was underway, crypto-analyst ZachXBT calculated the losses to be over $35 million, with the largest single victim losing almost 10% of the stolen total.

Yesterday, Elliptic reported that its analysis points to Lazarus Group as the threat actors responsible for the attack, making this the hackers'hackers' first major crypto heist for 2023.

Last year, the FBI attributed to Lazarus the Harmony Horizon Bridge hack in June 2022, which resulted in the theft of $100 million, and also the March 2022 hack of Axie Infinity, from which the North Koreans siphoned $620 million in crypto.

The latest attack on Atomic Wallet shows that the threat actors remain laser-focused on monetary goals, which experts have said are directly used to fund North Korea's weapons development program.



Tracing the transactions

The first evidence pointing to the Lazarus group is the observed laundering strategy, which matches patterns seen in previous attacks by the particular threat actor. The second attribution element is using the Sinbad mixer for laundering the stolen funds, which the threat group also used in the Harmony Horizon Bridge hack.

Elliptic has previously said that North Korean hackers have passed tens of millions of USD through Sinbad, demonstrating confidence and trust in the new mixer. The third and most significant proof of Lazarus' involvement in the Atomic Wallet hack is that substantial portions of the stolen cryptocurrency ended up in wallets that hold the proceeds of previous Lazarus hacks and are assumed to belong to group members.As last year's attacks have shown, successfully stealing cryptocurrency only accomplishes half the objective.

The rise of blockchain monitoring firms, coupled with the enhanced capabilities of law enforcement agencies, has significantly complicated the laundering process and subsequently cashing out the stolen assets. As victims notify exchanges of wallet addresses containing stolen funds, preventing them from being exchanged for other crypto or fiat, it causes the hackers to turn to less scrupulous exchanges that take a hefty commission to launder the money.

Source: https://www.bleepingcomputer.com/news/security/lazarus-hackers-linked-to-the-35-million-atomic-wallet-heist/

11. Russia says US hacked thousands of iPhones in iOS zero-click attacks

Russian cybersecurity firm Kaspersky says some iPhones on its network were hacked using an iOS vulnerability that installed malware via iMessage zero-click exploits.

The delivery of the message exploits a vulnerability that leads to code execution without requiring any user interaction, leading to the download of additional malicious from the attackers' server. Subsequently, the message and attachment are wiped from the device. At the same time, the payload stays behind, running with root privileges to collect system and user information and execute commands sent by the attackers.

Kaspersky says the campaign started in 2019 and reports the attacks are still ongoing. The cybersecurity firm has named the campaign "Operation Triangulation" and is inviting anyone who knows more about it to share information.

Russia accuses NSA of attacks

In a statement coinciding with Kaspersky's report, Russia's FSB intelligence and security agency claims that Apple deliberately provided the NSA with a backdoor it can use to infect iPhones in the country with spyware. The FSB alleges that it has discovered malware infections on thousands of Apple iPhones belonging to officials within the Russian government and staff from the embassies of Israel, China, and several NATO member nations in Russia.

Despite the seriousness of the allegations, the FSB has provided no proof of its claims. The Russian state has previously recommended that all presidential administration employees and members switch from using Apple iPhones and, if possible, give up American-made technology entirely.

Kaspersky confirmed to BleepingComputer that the attack impacted its headquarters office in Moscow and employees in other countries. Still, the company stated it's in no position to verify a link between its finding and FSB's report, as they do not have the technical details of the government's investigation. However, Russia's CERT released an alert linking FSB's statement to Kaspersky's report.

BleepingComputer has contacted Apple to request a comment on both Kaspersky's findings and FSB's allegations, but we are still waiting to receive a response.

Source:*https://www.bleepingcomputer.com/news/security/russia-says-us-hacked-thousands-of-iphones-in-ios-zero-click-attacks/*

12. American Airlines, Southwest Airline disclose data breaches affecting pilots

American Airlines and Southwest Airlines, two of the largest airlines in the world, disclosed data breaches on Friday caused by the hack of Pilot Credentials, a third-party vendor that manages multiple airlines' pilot applications and recruitment portals.

Both airlines were informed of the Pilot Credentials incident on May 3, which was limited solely to the systems of the third-party vendor, with no compromise or impact on the airlines' own networks or systems.

An unauthorized individual gained access to Pilot Credentials' systems on April 30 and stole documents containing information provided by certain applicants in the pilot and cadet hiring process.

According to breach notifications filed on Friday with Maine's Office of the Attorney General, American Airlines said the data breach affected 5745 pilots and applicants, while Southwest reported a total of 3009.

> "Our investigation determined that the data involved contained some of your personal information, such as your name and Social Security number, driver's license number, passport number, date of birth, Airman Certificate number, and other government-issued identification number(s),"
> - *American Airlines revealed.*

Although no evidence indicating that the pilots' personal information was specifically targeted or exploited for fraudulent or identity theft purposes was found, the airlines will, from now on, direct all pilot and cadet applicants to self-managed internal portals.

> *"We are no longer utilizing the vendor, and, moving forward, Pilot applicants are being directed to an internal portal managed by Southwest,"*
> *-Southwest Airlines said.*

American Airlines and Southwest Airlines have also notified relevant law enforcement authorities of the breaches and are fully cooperating with their ongoing investigation into the matter.

American Airlines hit by other breaches in recent years

The disclosures come after American Airlines disclosed another data breach in September 2022 that impacted over 1,708 American Airlines customers and team members following a July 2022 phishing attack that led to the compromise of a number of employee email accounts.

As disclosed at the time, personal information exposed in the July 2022 breach may have included employees' and customers' names, dates of birth, mailing addresses, phone numbers, email addresses, driver's license numbers, passport numbers, and/or certain medical information.

A subsequent investigation also indicated that the attackers used the employees' compromised accounts to send more phishing emails.

American Airlines was also hit by a data breach in March 2021 after global air information tech giant SITA disclosed that hackers breached its servers and accessed the Passenger Service System (PSS) used by multiple airlines worldwide.

American Airlines is the world's largest airline by fleet size (with over 1,300 aircraft in its mainline), operates almost 6,700 flights daily to roughly 350 destinations in over 50 countries, and has more than 120,000 employees.

Southwest Airlines is the world's largest low-cost carrier, has nearly 70,000 employees, and is present in over 121 airports across 11 countries.

Source: https://www.bleepingcomputer.com/news/security/american-airlines-southwest-airlines-disclose-data-breaches-affecting-pilots/

13. Grafana warns of critical auth bypass due to Azure AD integration

Grafana has released security fixes for multiple versions of its application, addressing a vulnerability that enables attackers to bypass authentication and take over any Grafana account that uses Azure Active Directory for authentication.

Grafana is a widely used open-source analytics and interactive visualization app that offers extensive integration options with a wide range of monitoring platforms and applications. Grafana Enterprise, the app's premium version with additional capabilities, is used by well-known organizations such as Wikimedia, Bloomberg, JP Morgan Chase, eBay, PayPal, and Sony.

> *"This can enable a Grafana account takeover and authentication bypass when Azure AD OAuth is configured with a multi-tenant Azure AD OAuth application," reads Grafana's advisory.*

The bug is caused by Grafana authenticating Azure AD accounts based on the email address configured in the associated 'profile email' setting. However, this setting is not unique across all Azure AD tenants, allowing threat actors to create Azure AD accounts with the same email address as legitimate Grafana users and use them to hijack accounts.

> *"If exploited, the attacker can gain complete control of a user's account, including access to private customer data and sensitive information."*

The bug is caused by Grafana authenticating Azure AD accounts based on the email address configured in the associated 'profile email' setting. However, this setting is not unique across all Azure AD tenants, allowing threat actors to create Azure AD accounts with the same email address as legitimate Grafana users and use them to hijack accounts.

> *"This can enable a Grafana account takeover and authentication bypass when Azure AD OAuth is configured with a multi-tenant Azure AD OAuth application," reads Grafana's advisory.*

"If exploited, the attacker can gain complete control of a user's account, including access to private customer data and sensitive information."

Source: https://www.bleepingcomputer.com/news/security/grafana-warns-of-critical-auth-bypass-due-to-azure-ad-integratio

14. EncroChat takedown led to 6,500 arrests and $979 million seized

Europol announced today that the takedown of the EncroChat encrypted mobile communications platform has led to the arrest of over 6,600 people and the seizure of $979 million in illicit funds. EncroChat phones ran a special, hardened version of Android that promised users unbreakable encryption, anonymity, and no traceability.

The service also provided message self-destruction features, panic device wipe, tamper-proofing booting, and a brute force resistant FIPS 140-2 certified hardware cryptographic engine. These features were valued by criminals who wanted to communicate securely, so tens of thousands paid €1,500 ($1,635) for a six-month subscription with global coverage and 24/7 support.

The EncroChat phones themselves were sold for a one-time payment of €1,000 ($1,090) and were remotely erasable if needed.

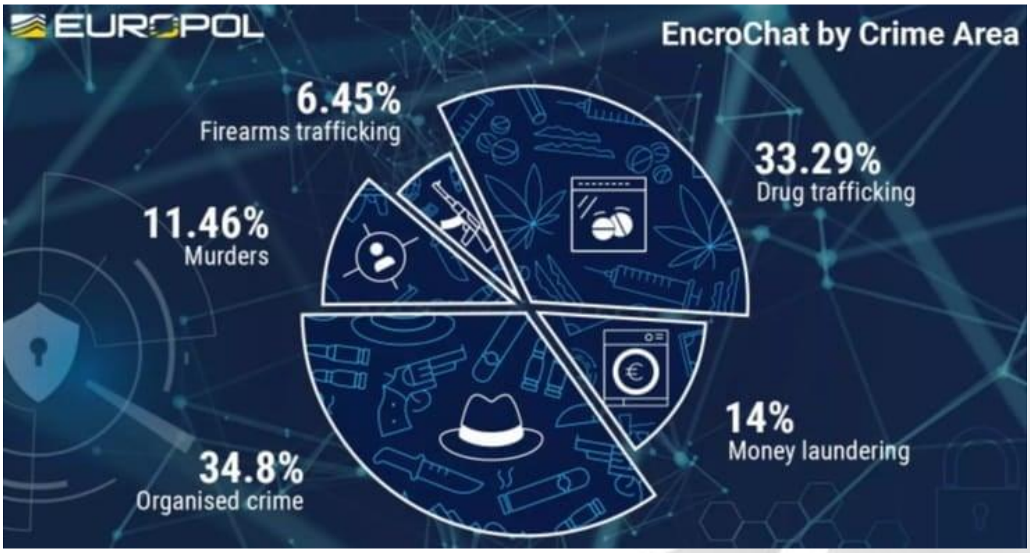
Secretly monitoring communications

In 2020, a large-scale European law enforcement operation quietly infiltrated the EncroChat platform and was able to analyze millions of messages shared between its users after breaking the encryption algorithm.

Since then, police units in France and the Netherlands working in coordination with their peers in other countries have arrested 6,558 individuals, users of EncroChat, including 197 high-value targets. This was made possible thanks to the analysis of 115 million conversations between roughly 60,000 users of the platform.

Utilizing this data, the police managed to locate and seize 270 tons of drugs, 971 vehicles, 271 properties, 923 weapons, 68 explosives, 40 planes, and 83 boats.

Additionally, law enforcement agents sized €740 million ($807 million) in cash and froze another €154 million ($168 million).



Europol says that most EncroChat users were either members of organized crime (34.8%) or performed drug trafficking (33.3%). The rest engaged in money laundering (14%), murders (11.5%), and firearms trafficking (6.4%).

The arrested EncroChat users have so far been convicted to a total of 7,134 years of imprisonment, though not all of them have been sentenced yet. It is worth noting that after the takedown of EncroChat, many of its users migrated to an alternative service called 'Sky ECC,' which was operating as a legal entity. Europol and investigators from various European cyber-police units broke the encryption of Sky ECC and monitored the communications between roughly 70,000 users.

Information stealers are a malware category that targets account data stored on applications such as email clients, web browsers, instant messengers, gaming services, cryptocurrency wallets, and others. These types of malware are known to steal credentials saved to web browsers by extracting them from the program's SQLite database and abusing the CryptProtectData function to reverse the encryption of the stored secrets. These credentials, and other stolen data, are then packaged into archives, called logs, and sent back to the attackers' servers for retrieval.

Source: https://www.bleepingcomputer.com/news/security/encrochat-takedown-led-to-6-500-arrests-and-979-million-seized/

15. Over 100,000 ChatGPT accounts stolen via info-stealing malware

More than 101,000 ChatGPT user accounts have been stolen by information-stealing malware over the past year, according to dark web marketplace data. Cyberintelligence firm Group-IB reports having identified over a hundred thousand info-stealer logs on various underground websites containing ChatGPT accounts, with the peak observed in May 2023, when threat actors posted 26,800 new ChatGPT credential pairs.

Regarding the most targeted region, Asia-Pacific had almost 41,000 compromised accounts between June 2022 and May 2023, Europe had nearly 17,000, and North America ranked fifth with 4,700.

> "Many enterprises are integrating ChatGPT into their operational flow," comments Group-IB's Dmitry Shestakov. "*Employees enter classified correspondences or use the bot to optimize proprietary code. Given that ChatGPT's standard configuration retains all conversations, this could inadvertently offer a trove of sensitive intelligence to threat actors if they obtain account credentials.*"

. If you input sensitive data on ChatGPT, consider disabling the chat saving feature from the platform's settings menu or manually delete those conversations as soon as you are done using the tool.

ChatGPT accounts, alongside email accounts, credit card data, cryptocurrency wallet information, and other more traditionally targeted data types, signify the rising importance of AI-powered tools for users and businesses. Because ChatGPT allows users to store conversations, accessing one's account might mean gaining insights into proprietary information, internal business strategies, personal communications, software code, and more.

However, it should be noted that many information stealers snap screenshots of the infected system or perform keylogging, so even if you do not save conversations to your ChatGPT account, the malware infection could still lead to a data leak. Unfortunately, ChatGPT has already suffered a data breach where users saw other users' personal information and chat queries.

Therefore, those working with extremely sensitive information shouldn't trust inputting it on any cloud-based services, but only on secured locally-built and self-hosted tools.

Source: https://www.bleepingcomputer.com/news/security/over-100-000-chatgpt-accounts-stolen-via-info-stealing-malware/

16. As Data Gravity Goes Up, are Clouds Becoming Black Holes?

The more data in one place, the more data it attracts.

This “data gravity” is a familiar function for enterprises, even if the term isn’t. As the number of applications hosted on local servers increases, so too does the amount of data necessary for them to operate. Add more data and more applications are required to manage this data. Over time, the cycle repeats again and again as data gravity builds.

Now, this gravity is shifting to the cloud. With companies making the move to cloud storage, analytics and compute services, the volume of data — and its commensurate gravity — is on the rise. But are the very same clouds designed to boost performance at risk of becoming data black holes?

What is Data Gravity?

Coined in 2010 by Dave McCrory, data gravity is an analog for its physical counterpart. In the world around us, large objects attract smaller masses. It’s why we don’t fly off the Earth and why the Earth rotates around the sun. Moving large objects away from a center of mass is difficult — this is why sending shuttles into space requires thousands and thousands of tons of rocket fuel to break free from our planet’s gravitational pull.

In the digital world, data gravity refers to the tendency of large data “masses” to attract and retain more data. For example, if a company uses a cloud-based ERP system, this system naturally attracts data related to customer histories, transaction details and key business operations. These data types are themselves governed by applications such as CRM solutions or eCommerce portals, which are carried along toward the data center. These applications also come with their own data and, in turn, the applications required to manage that data — and on and on it goes.

The result is a growing data mass that picks up attractive speed the more data it brings in. This mass also makes it prohibitively time and resource-expensive to run functions outside the center. Consider a security control located at the edge of company networks. Because data must travel back and forth between the control and the central storage mass, the time required to complete key processes goes up. In addition, data may be compromised on its journey to or from the center, in turn lowering the efficacy of these edge tools.

To address this loss of performance and increase in lag time, many companies are now centralizing key services in the cloud — creating even bigger data masses.

From Shared Responsibility to Shared Fate

In a shared responsibility model, ensuring cloud services were available and secure was the role of the provider. Cloud customers, meanwhile, were responsible for configuring and using the cloud — and for any issues that arose due to this configuration and use.

The problem? According to research firm Gartner, cloud customers are the primary driver of cloud security failures. In fact, Gartner estimates that by 2025, 99% of cloud security failures will be the customers' fault.

To combat this challenge, companies like Google are moving to a "shared fate" model that takes a more active role in cloud configurations with guidance, tools and blueprints to help customers succeed. IBM, meanwhile, has developed solutions such as Continuous Cloud Delivery which help companies create and implement cloud application toolchains that enhance app management and ensure process repeatability.

While the primary impact of this effort is reduced cloud misconfigurations, it also comes with a knock-on effect: increased gravitational pull. If companies know that providers are willing to take on additional responsibilities for data protection and service operation, they're more likely to accelerate their move to the cloud.

Laws of Attraction: Navigating the Cloud Paradox

If enough physical mass is concentrated in one area, the pressure of the system converts it into a black hole. Not only do these holes in space consume everything around them, but once mass goes past the event horizon, there's no coming back.

This is the cloud paradox. As providers recognize the shift toward all-in cloud models, they're creating solutions that make it possible for enterprises to shift every aspect of their IT framework into the cloud. Underpinned by evolving solutions such as softwaredefined networking (SDN), powerful data analytics and artificial intelligence, it's now possible for cloud services to outpace on-premises options when it comes to everything from security to performance to collaboration.

The challenge? The more data in the same place, the harder it is to leave. While storing services and data across multiple providers increases complexity, it also lowers the overall escape velocity of data. Put simply; it's much easier for companies to leave a cloud they use only for a few services or applications. It's much more difficult to make the switch if critical functions and data are housed in a single cloud. The time and effort required to move increase exponentially as more services are added.

Breaking Free

When it comes to black hole clouds, the solution lies not in avoidance but in agility. As noted above, cloud providers are moving to a shared fate model as they recognize the role of data gravity in enterprise operations. To bring businesses on board, they're both reducing prices and improving performance, making data attractors hard to resist.

To make the most of these solutions without drifting past the point of no return, companies need to create comprehensive and consistent policies around which data and applications belong in large clouds, which are better served by specialized providers and should stay on-site. For example, a financial institution might shift its client demographic analysis to a large-scale cloud provider and make use of its computational power. The same company might procure cybersecurity services — such as threat intelligence and incident detection and response — from a provider that specializes in these solutions. Finally, they might opt to keep core financial data in-house and under lock and key.

Put simply? Data gravity is growing. To avoid being caught in cloud black holes, enterprises need to identify their IT needs, determine the best-fit location for disparate data sources and deploy specialty providers where appropriate to keep operational data in orbit.

Source: https://securityintelligence.com/articles/as-data-gravity-goes-up-are-clouds-becoming-black-holes/

17. The Great Exodus to Telegram: A Tour of the New Cybercrime Underground

The world of cybercrime is moving quickly. Threat actors, ransomware gangs, malware developers, and others are increasingly and rapidly moving off of the "traditional" dark web (Tor sites) and onto illicit Telegram channels specializing in cybercrime.

This Flare article will examine the reasons why threat actors are shifting from Tor and provide detailed guidance for best practices in monitoring Telegram channels.

Why Are Threat Actors Moving from Tor to Telegram?

Today we see a majority of cybercrime activity occurring off of the traditional dark web and on modern social media applications.

There are a myriad of reasons for the switch including the commodification of cybercrime, increasing law enforcement scrutiny on Tor sites, and the general slowness of Tor. We'll cover each in turn.

Lack of Exit Scams

One of the biggest upsides and downsides to traditional dark web marketplaces is that the marketplace acts as a clearinghouse.

Typically, there is a 14 day hold on transactions in which the marketplace holds onto cryptocurrency and in which the buyer can request recourse if they are scammed.

The challenge becomes that in many cases marketplace owners may be holding millions of dollars in crypto at any given time, creating a strong incentive to exit scam and steal the money being held.

Amenities of Modern Social Media

Compared to Tor sites, Telegram has an advantage in these following areas:

Telegram is fast, and has many of the amenities that modern social media applications have such as emojis, direct private chats, a phone application, and other nice to haves

Level of technical proficiency to find cybercrime channels and successfully make purchases is even lower than Tor, creating a democratization of cybercrime data

Many channels exist which provide free "samples" of credentials, stealer logs, data from breaches, and other data which can provide an easy way for users to "validate" the effectiveness of the vendors offerings

Perceived Anonymity

It's no secret that Tor marketplaces, forums, and sites are heavily monitored by law enforcement organizations. Users know when they make a forum post or marketplace listing will likely be seen by enterprise security teams, dozens of law enforcement agencies, and many others.

Conversely Telegram provides perceived anonymity given the thousands of channels specializing in cybercrime, the lack of IP tracking available to security and LE professionals, and the seeming ephemeral nature of messages.

Types of Cybercrime Telegram Channels

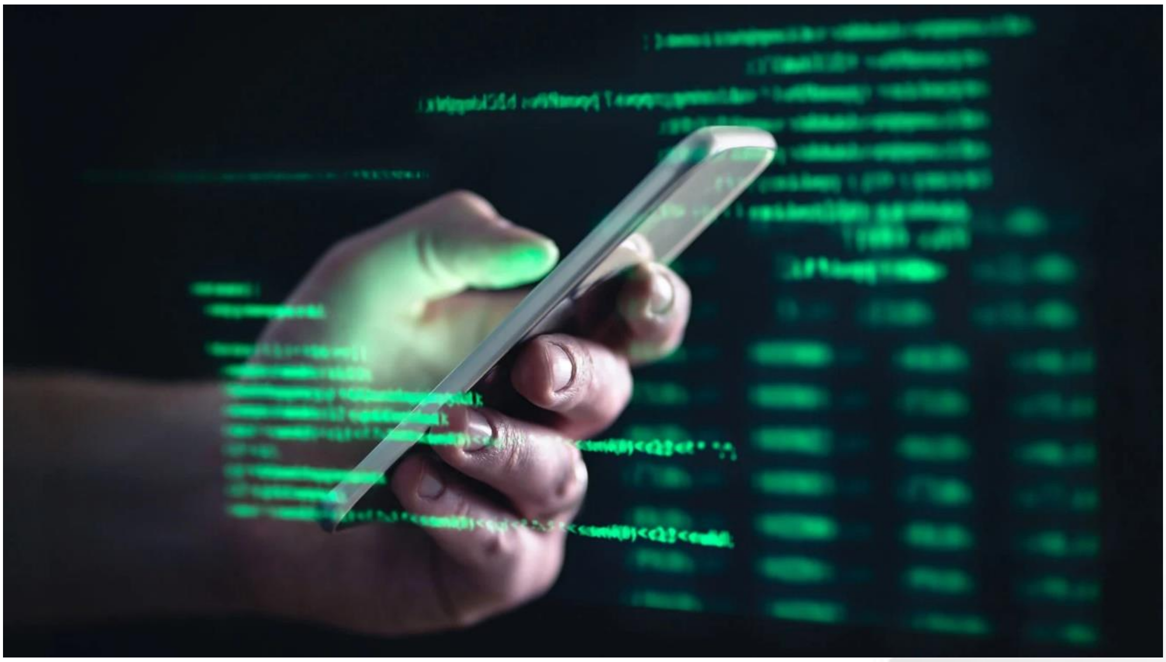
Compared to legacy dark web marketplaces, Telegram channels tend to specialize in one particular type of criminal activity. A dark web marketplace may offer a criminal the ability to buy drugs, guns, credit card numbers, combolists and dozens of other illicit goods.

Telegram channels by contract act as a single shop for a single type of goods and can be classified based on what they are offering.

The following categories we've identified are not exhaustive:

Stealer Log Distribution

Stealer logs represent data from devices infected with infostealer malware. They typically include the browser fingerprint, saved passwords in the browser, clipboard data, credit card data saved in the browser, cryptocurrency wallet information, and relevant information.



An individual log ›represents data from one computer. Stealer log channels on Telegram come in two types:

Open Access Stealer Log Channels

These channels routinely distribute megabyte-gigabyte sized files that contain hundreds, thousands, or in some cases hundreds of thousands of individual stealer logs.

These can be seen as an extended advertisement for private, invite only log channels and as a way for the vendors to prove that the logs they are providing are high-quality and contain valuable credentials.

VIP Stealer Log Channels

VIP stealer logs channels provide a limited number of threat actors access to "premium" logs which are supposedly directly from the source and untouched by other threat actors. Typically the price for access to these channels ranges from $200-$400 a month paid in Monero.

We suspect that many initial access brokers sift through logs posted in these channels to identify specific logs that have corporate access, validate the access, and then resell the access on top-tier cybercrime forums such as Exploit or XSS.

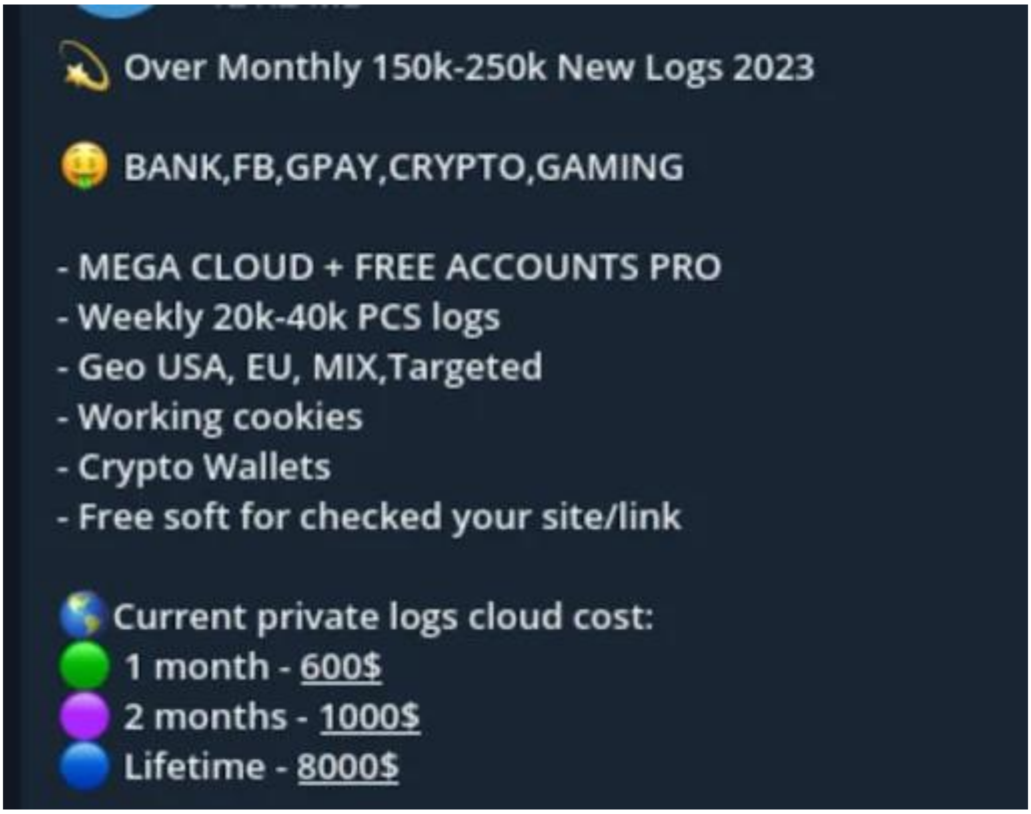
Financial Fraud

Another type of channel we commonly see are financial fraud channels in which bank account, credit card, and refund information is given out in bulk. These channels typically sub-specialize in their particular "type" of crime for example:

- Credit Card Numbers
- Bank Accounts
- Refunding Guides
- SIM Swapping
- Gift Card Fraud
- Combolists & Credentials

Another common and critical type of channel to monitor are channels providing combolists. Combolists are "curated" lists of stolen usernames and passwords, sometimes accompanied by names, emails and other identifying information that criminals use to attempt account takeover attacks. Combolists can be created based on geography, industry, account access and other features that make them high-value for threat actors.

In many cases usernames, emails, and passwords are pasted directly into the Telegram chat. In other cases threat actors may provide files that contain thousands or tens of thousands of data points (and often are accompanied by malware).



💫 Over Monthly 150k-250k New Logs 2023

🤑 BANK,FB,GPAY,CRYPTO,GAMING

- MEGA CLOUD + FREE ACCOUNTS PRO
- Weekly 20k-40k PCS logs
- Geo USA, EU, MIX,Targeted
- Working cookies
- Crypto Wallets
- Free soft for checked your site/link

🌎 Current private logs cloud cost:
🟢 1 month - 600$
🟣 2 months - 1000$
🔵 Lifetime - 8000$

Nation State Hacktivism

The last category of channels that is particularly relevant for cybersecurity teams are nation-state hacktivist channels. Channels such as Bloodnet, Killnet, Noname47, Anonymous Sudan, and others have exploded in popularity, particularly since the beginning of the war in Ukraine.

These channels typically pick specific targets, often critical infrastructure in NATO countries and attempt to deface websites, DDoS vital services, and leak data from companies.

Source: https://www.bleepingcomputer.com/news/security/the-great-exodus-to-telegram-a-tour-of-the-new-cybercrime-underground/

18. Ukrainian hackers take down service provider for Russian banks

A group of Ukrainian hackers known as the Cyber.Anarchy.Squad claimed an attack that took down Russian telecom provider Infotel JSC on Thursday evening. Among other things, Moscow-based Infotel provides connectivity services between the Russian Central Bank and other Russian banks, online stores, and credit institutions.

Following yesterday's attack, multiple major banks across Russia had their access cut off from the country's banking systems so that they can no longer make online payments, as Ukrainian news site Economichna Pravda first reported.

Infotel has confirmed the incident on its website, saying that it's currently working on restoring systems that were damaged following what it described as a "massive" attack.

> "We would like to inform you that as a result of a massive hacker attack on the network of Infotel JSC, some of the network equipment was damaged," the Russian company said.

"Restoration work is currently underway. Additional deadlines for completing the work will be announced. We hope for your understanding and further cooperation."

While Infotel or their attackers are yet to share a timeline of the attacks, Georgia Tech's Internet Outage Detection and Analysis (IODA) project shows that the Central Bank of Russia's Internet provider went down on June 8, around 11:00 AM UTC.

IODA also confirms that the Russian company is working on restoring its systems, and it was still offline 34 hours after it was knocked down.

> *"All their infrastructure was destroyed, nothing living was left there," said the Ukrainian hacktivists on their Telegram channel when they announced the attack yesterday.*
>
> *"In total, the company has about four hundred clients, a quarter of them are banks, the rest are credit institutions, car dealerships."*

As proof of their attacks, they released screenshots of alleged access to Infotel's network, including a network diagram and what appears to be a compromised email account. This is a recurring pattern for the Cyber.Anarchy.Squad Ukrainian hacking group, which has targeted other Russian companies since it surfaced after Russia invaded Ukraine.

Notably, last year, the group leaked online databases stolen from the breached systems of a Russian retailer and a jewelry manufacturer. The leaked databases contained millions of records with information belonging to the companies' employees and customers, as well as internal company emails.

Source: https://www.bleepingcomputer.com/news/security/ukrainian-hackers-take-down-service-provider-for-russian-banks/

19. Three reasons to Think Twice About Enabling Location Sharing

Do you remember the days of printing out directions from your desktop? Or the times when passengers were navigation co-pilots armed with a 10-pound book of maps? You can thank location services on your smartphone for today's hassle-free and paperless way of getting around town and exploring exciting new places.

However, location services can prove a hassle to your online privacy when you enable location sharing. Location sharing is a feature on many connected devices – smartphones, tablets, digital cameras, smart fitness watches – that pinpoints your exact location and then distributes your coordinates to online advertisers, your social media following, or strangers.

While there are certain scenarios where sharing your location is a safety measure, in most cases, it's an online safety hazard. Here's what you should know about location sharing and the effects it has on your privacy.

The Benefits of Location Sharing

Location sharing is most beneficial when you're unsure about new surroundings and want to let your loved ones know that you're ok. For example, if you're traveling by yourself, it may be a good idea to share the location of your smartphone with an emergency contact. That way, if circumstances cause you to deviate from your itinerary, your designated loved one can reach out and ensure your personal safety.

The key to sharing your location safely is to only allow your most trusted loved one to track the whereabouts of you and your connected device. Once you're back on known territory, you may want to consider turning off all location services, since it presents a few security and privacy risks.

The Risks of Location Sharing

In just about every other case, you should definitely think twice about enabling location sharing on your smartphone. Here are three risks it poses to your online privacy and possibly your real-life personal safety:

Ad tracking

Does it sometimes seem like your phone, tablet, or laptop is listening to your conversations? Are the ads you get in your social media feeds or during ad breaks in your gaming apps a little too accurate? When ad tracking is enabled on your phone, it allows online advertisers to collect your personal data that you add to your various online accounts to better predict what ads you might like. Personal details may include your full name, birthday, address, income, and, thanks to location tracking, your hometown and regular neighborhood haunts.

If advertisers kept these details to themselves, it may just seem like a creepy invasion of privacy; however, data brokerage sites may sell your personally identifiable information (PII) to anyone, including cybercriminals. The average person has their PII for sale on more than 30 sites and 98% of people never gave their permission to have their information sold online. Yet, data brokerage sites are legal.

One way to keep your data out of the hands of advertisers and cybercriminals is to limit the amount of data you share online and to regularly erase your data from brokerage sites. First, turn off location services and disable ad tracking on all your apps. Then, consider signing up for McAfee Personal Data Cleanup, which scans, removes, and monitors data brokerage sites for your personal details, thus better preserving your online privacy.

Stalkers

Location sharing may present a threat to your personal safety. Stalkers could be someone you know or a stranger. Fitness watches that connect to apps that share your outdoor exercising routes could be especially risky, since over time you're likely to reveal patterns of the times and locations where one could expect to run into you.

Additionally, stalkers may find you through your geotagged social media posts. Geotagging is a social media feature that adds the location to your posts. Live updates, like live tweeting or real-time Instagram stories, can pinpoint your location accurately and thus alert someone on where to find you.

Social Engineering

Social engineering is an online scheme where cybercriminals learn all there is about you from your social media accounts and then use that information to impersonate you or to tailor a scam to your interests. Geotagged photos and posts can tell a scammer a lot about you: your hometown, your school or workplace, your favorite café, etc.

With these details, a social engineer could fabricate a fundraiser for your town, for example. Social engineers are notorious for evoking strong emotions in their pleas for funds, so beware of any direct messages you receive that make you feel very angry or very sad. With the help of ChatGPT, social engineering schemes are likely going to sound more believable than ever before. Slow down and conduct your own research before divulging any personal or payment details to anyone you've never met in person.

Live Online Anonymously

Overall, it's best to live online as anonymously as possible, which includes turning off your location services when you feel safe in your surroundings. McAfee+ offers several features to improve your online privacy, such as a VPN, Personal Data Cleanup, and Online Account Cleanup.

Source: https://www.mcafee.com/blogs/internet-security/3-reasons-to-think-twice-about-enabling-location-sharing/

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.