Cyber Threat Advisory

SEPTEMBER 2023

Image Source: Microsoft Crushes OpenAI with Databricks

Contents

September Highlights	1
Ransomware Tracker	7
New Financial Malware 'JanelaRAT' Targets Latin American Users	8
HiatusRAT Malware Resurfaces: Taiwan Firms and U.S. Military Under Attack	10
Reptile Rootkit: Advanced Linux Malware Targeting South Korean Systems	11
Knight Ransomware Distributed in Fake Tripadvisor Complaint E-mails	12
Top Threat Actors	15
Top Exploited Vulnerabilities	15
Security Bulletin	16
Reference Links	23

Monthly Highlights - September

1. **Microsoft Crushes OpenAI with Databricks** – After playing with OpenAI, Microsoft has now moved on to uncovering its flaws, and is looking elsewhere for support and strategic alliance to up its game in generative AI for enterprise. A recent exclusive by The Information might come as a shocker for OpenAI.

   The report said Microsoft is planning to sell a new version of Databricks' software that helps customers make AI apps for their businesses. The tech giant plans to sell it through its Azure cloud-server unit, which can help companies make AI models from scratch or repurpose open-source models as an alternative to licensing OpenAI's proprietary ones.

   Microsoft's actions clearly indicate that everything is not well between the two entities. This seems to be in spite of the fact that OpenAI hasn't done anything to Microsoft which ought to make them unhappy. Instead, it appears that Microsoft's focus has been primarily on its Azure services, which has led to a self-centred approach and possibly contributed to the current state of affairs between the two.

   In the partnership between Microsoft and OpenAI, both parties had their own agendas. While the tech giant needed generative AI push in its cloud services, the ChatGPT creator aimed to secure financial support for building advanced AI systems, and eventually AGI.

   Despite the efforts made by OpenAI, it seems it could not completely gain the trust of enterprises. Large tech companies like Apple, Spotify, Wells Fargo, Samsung, JP Morgan, and Verizon dumped ChatGPT and prohibited their workers from utilizing it. Clearly, the awareness is lacking among enterprise customers.

Ironically, for Azure-Databricks benefit, Microsoft is leveraging OpenAI's innovation to develop a chatbot comparable to ChatGPT. The purpose is to help less tech-savvy users navigate Databricks' software, initially tailored for advanced data scientists. As a result, certain Microsoft clients might find themselves using open-source models instead of the closed-source options from OpenAI. This move by Microsoft indicates that it is moving away from OpenAI and looking out for more partners that can help them make Azure OpenAI services better, especially for its enterprise clients. There's no stopping.

NOT THE FIRST TIME

A few days back, Microsoft posted "Azure ChatGPT" on GitHub (now erased) repository which was promoted as safe, secure and private ChatGPT for enterprise.

The reason Microsoft gave for launching Azure ChatGPT was that ChatGPT risks exposing confidential intellectual property and it would be better to utilize Azure ChatGPT as data remains safe and secure on Azure. Microsoft specified that they would not share any information with OpenAI.

Microsoft did one more thing that put OpenAI's reputation at risk. It collaborated with IBM Consulting. The collaboration with IBM Consulting is centred around helping clients implement and scale Azure OpenAI Service. Notably, IBM also forged a recent partnership with Meta, aiming to integrate Llama 2 into watsonx.ai, a formidable competitor to OpenAI's GPT-4.

WHO IS SPREADING THE RUMOURS?

IBM recently released a blog post cautioning against the use of ChatGPT for enterprise. According to IBM, employing ChatGPT directly within an enterprise context introduces various potential risks and obstacles. These include matters like security vulnerabilities leading to data exposure, issues related to confidentiality and legal responsibility, and the intricate landscape of intellectual property.

OpenAI has taken steps to address this concern by providing clarity. They have explicitly stated in their policy that user data from chat histories is not utilized to train their model in the event that users have disabled the chat history feature. Recently, Sam Altman clarified on X, saying that OpenAI doesn't use API-submitted data to train or improve models unless a user expressly opts in.

In spite of OpenAI's diligent efforts to be transparent, Microsoft's actions appear to undermine their attempts to maintain transparency and integrity.

2. **US hit by major cyberattack, hackers exploit IBM, steal over millions of people's healthcare, personal data** – In one of the biggest hacks or data leaks to have hit the US, healthcare and personal data of over 10 million individuals have been stolen by a group of hackers targeting IBM. The hackers exploited a vulnerability in the super popular MOVEit file transfer software that IBM uses.

   Over millions of people within the US had their private medical information stolen by hackers who found a sneaky way into the super popular MOVEit file transfer software utilized by IBM.

   The Colorado Department of Health Care Policy and Financing (HCPF), the people in charge of Colorado's Medicaid program, got hit hard, and more than 4 million patient records got exposed in the process.

HACKERS TARGET IBM

HCPF had to notify the people affected, clarifying that the data got compromised because IBM, one of their vendors, was utilizing MOVEit to move around HCPF's records. The thing is, no HCPF or Colorado government systems got messed with, but the bad actors did get into some HCPF records on the MOVEit app that IBM was utilizing.

And here's what those records held: full names, birthdays, addresses, Social Security numbers, Medicaid and Medicare ID numbers, money information, medical details like lab results and meds, and health insurance stuff.

All in all, around 4.1 million individuals got caught up in this mess.

HACKERS DID NOT DAMAGE THE NETWORK, JUST STOLE DATA.

This attack on IBM's MOVEit systems also got to Missouri's Department of Social Services (DSS), affecting numerous individuals. Missouri has more than 6 million residents. DSS made it clear that this data breach didn't mess with their systems directly, but it did mess with the data they had. So, names, client numbers, birthdates, benefits information, and medical claims data might've been seized.

3. **AMD 'Zenbleed' exploit can leak passwords and encryption keys from Ryzen CPUs** – A new vulnerability affecting AMD's line of Zen 2 processors — which incorporates prevalent CPUs just like the budget-friendly Ryzen 5 3600 — has been discovered that can be exploited to steal sensitive data like passwords and encryption keys. Google security researcher Tavis Ormandy uncovered the "Zenbleed" bug (recorded as CVE-2023-20593) on his blog this week after reporting the vulnerability to AMD on May 15th.

The entire Zen 2 product stack is impacted by the vulnerability, including all processors within the AMD Ryzen 3000 / 4000 / 5000 / 7020 series, the Ryzen Master 3000 / 4000 series, and AMD's EPYC "Rome" data center processors. AMD has since published its anticipated release timeline for patching out the exploit, with most firmware updates not expected to arrive until later this year.

According to Cloudflare, the Zenbleed exploit doesn't require physical access to a user's computer to attack their system and can even be executed remotely through Javascript on a webpage. If successfully executed, the exploit allows data to be transferred at a rate of 30 kb per core, per second. That's fast enough to steal sensitive data from any software running on the system, including virtual machines, sandboxes, containers, and processes, according to Ormandy. As TomsHardware notes, the adaptability of this exploit could be a particular concern for cloud-hosted services because it may possibly be utilized to spy on clients within cloud instances.

Worse still — Zenbleed can fly beneath the radar since it doesn't require any special system calls or privileges to exploit. "I am not aware of any reliable techniques to detect exploitation," said Ormandy. The bug shares some similarities with the Spectre class of CPU vulnerabilities in that it makes use of flaws withing speculative executions, but it's far easier to execute — making it more like Meltdown family of exploits. The complete technical breakdown of the Zenbleed vulnerability can be found on Ormandy's blog.

AMD has already released a microcode fix for second-generation EPYC 7002 processors, though the next updates for the remaining CPU lines aren't anticipated until October 2023 at the earliest. The company hasn't disclosed if these updates will impact system performance, but a statement AMD provided to TomsHardware proposes it's a plausibility:

Any performance impact will vary depending on workload and system configuration. AMD isn't aware of any known exploit of the described vulnerability outside the research environment.

Ormandy "highly recommends" that affected users apply AMD's microcode update but has provided instructions on his blog for a software workaround that can be applied while we wait for vendors to incorporate a fix into future BIOS upgrades. Ormandy cautions that this workaround may also impact system performance, but at least it's better than having to wait for a firmware update.

4. **WoofLocker Toolkit Hides Malicious Codes in Images to Run Tech Support Scams** – Cybersecurity researchers have detailed an updated version of an advanced fingerprinting and redirection toolkit called WoofLocker that's engineered to conduct tech support tricks.

   The sophisticated traffic redirection scheme was first documented by Malwarebytes in January 2020, leveraging JavaScript embedded in compromised websites to perform anti-bot and web traffic filtering checks to serve next-stage JavaScript that redirects users to a browser locker (aka browlock).

   This redirection mechanism, in turn, makes use of steganographic tricks to conceal the JavaScript code inside a PNG image that's served only when the validation phase is successful. Should a user be detected as a bot or uninteresting traffic, a decoy PNG file without the malicious code is delivered.

   WoofLocker is also known as 404Browlock due to the fact that visiting the browlock URL directly without the appropriate redirection or one-time session token results in a 404 error page.

   The cybersecurity firm's latest analysis shows that the campaign is still ongoing after all these years.

   "The tactics and techniques are very similar, but the infrastructure is now more robust than before to defeat potential takedown attempts," Jérôme Segura, director of threat intelligence at Malwarebytes, said.

   "It is just as difficult to reproduce and study the redirection mechanism now as it was then, especially in light of new fingerprinting checks" to detect the presence of virtual machines, certain browser extensions, and security tools.

   A majority of the sites loading WoofLocker are adult websites, with the infrastructure using hosting providers in Bulgaria and Ukraine that give the threat actors stronger protection against takedowns.

   The primary goal of browser lockers is to get targeted victims to call for assistance to resolve (non-existent) computer issues and gain remote control over the computer to draft an invoice that recommends affected people pay for a security solution to address the issue.

   "Typically, this is handled by third-parties via fraudulent call centers," Segura noted back in 2020. "The threat actor behind the traffic redirection and browlock will get paid for each successful lead."

   The exact identity of the threat actor remains unknown, and there's evidence that arrangements for the campaign have been underway as early as 2017.

   "Unlike other campaigns that depend on purchasing advertisements and playing whack-a-mole with hosting providers and

registrars, WoofLocker is a very stable and low maintenance business," Segura said. "The websites hosting the malicious code have been compromised for years whereas the fingerprinting and browser locker infrastructure appears to be utilizing solid registrar and hosting providers."

The disclosure comes as the company detailed a new malvertising infection chain that involves using bogus ads on search engines to direct users searching for remote access programs and scanners to booby-trapped websites that deploy stealer malware.

What sets this campaign apart is its capacity to fingerprint visitors utilizing the WEBGL_debug_renderer_info API and gather the victim's graphics driver properties to sort genuine browsers from crawlers and virtual machines, then exfiltrate the data to a remote server in order to determine the next course of action.

"By using better filtering before redirecting potential victims to malware, threat actors ensure that their malicious ads and infrastructure remain online longer," Segura said. "Not only does it make it more difficult for defenders to identify and report such events, it also likely has an impact on takedown actions."

The development also follows new research which found that websites belonging to U.S. government agencies, leading colleges, and professional organizations have been hijacked over the last five years and utilized to push scam offers and promotions by means of "poison PDF" files uploaded to the portals.

Many of these scams are aimed at children and attempt to trick them into downloading apps, malware, or submitting personal details in exchange for non-existent rewards in online gaming stages such as Fortnite and Roblox.

5. **Hackers use VPN provider's code certificate to sign malware** – The China-aligned APT (advanced persistent threat) group known as 'Bronze Starlight' was seen targeting the Southeast Asian gambling industry with malware signed using a valid certificate utilized by the Ivacy VPN provider.

   The main benefit of using a valid certificate is to bypass security measures, avoid raising suspicions with system alerts, and blend in with legitimate software and traffic. According to SentinelLabs, which analyzed the campaign, the certificate belongs to PMG PTE LTD, a Singaporean vendor of the VPN item 'Ivacy VPN.'

   The cyberattacks observed in March 2023 are likely a later phase of the 'Operation ChattyGoblin' that ESET recognized in a Q4 2022 – Q1 2023 report.

   Be that as it may, SentinelLabs says it's challenging to associate with particular clusters due to the extensive sharing of devices between Chinese threat actors.

DLL SIDE-LOADING

The attacks begin with dropping .NET executables (agentupdate_plugins.exe and AdventureQuest.exe) on the target framework, likely by means of trojanized chat apps, that fetch password-protected ZIP archives from Alibaba buckets.

The AdventureQuest.exe malware sample was first found by security researcher MalwareHunterteam in May when noted that the code-signing certificate was the same as one utilized for official Ivacy VPN installers.

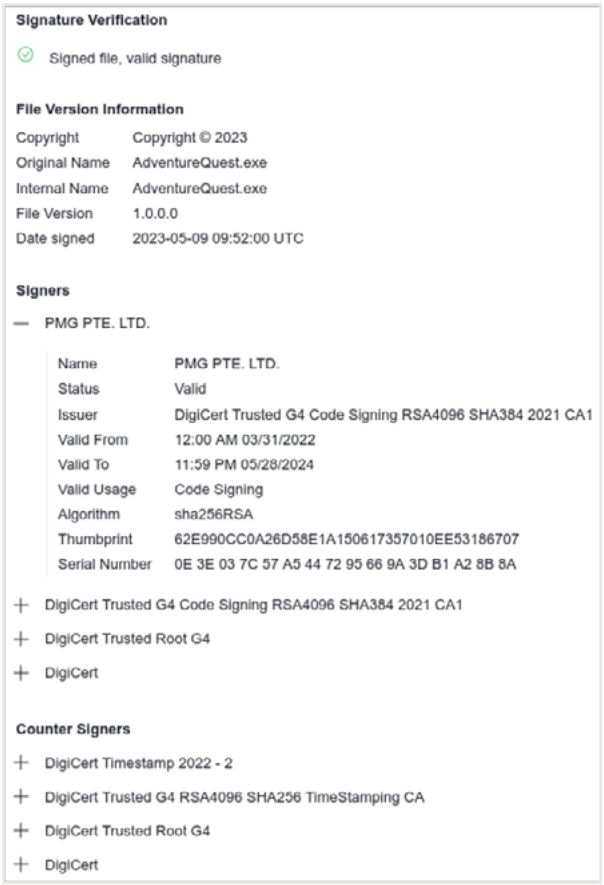
These archives contain vulnerable software versions like Adobe Creative Cloud, Microsoft Edge, and McAfee VirusScan, which are susceptible to DLL hijacking. The Bronze Starlight hackers utilize these vulnerable applications to deploy Cobalt Strike beacons on targeted systems.

The malicious DLLs (libcef.dll, msedge_elf.dll, and LockDown.dll) are packed inside the archives alongside the legitimate program executables, and Windows prioritizes their execution over more secure forms of the same DLL stored in C:\Windows\System32, thus permitting malicious code to run.

Zip archive	Archive content	Final payload
adobe_helper.zip (agentupdate_plugins.exe)	Adobe CEF Helper.exe libcef.dll agent.data (not available)	/
cefhelper.zip (AdventureQuest.exe)	identity_helper.exe msedge_elf.dll agent.data	Cobalt Strike C2: www.100helpchat[.]com
Agent_bak.zip (AdventureQuest.exe)	mfeann.exe LockDown.dll agent.data	Cobalt Strike C2: live100heip[.]com

SentinelLabs notes that the .NET executables include a geofencing restriction that prevents the malware from running in the United States, Germany, France, Russia, India, Canada, or the United Kingdom.

These nations are outside this campaign's target scope and are excluded to evade detection and analysis. In any case, due to an error in the geofencing implementation, it does not work.



ABUSING A VALID CERTIFICATE

An intriguing aspect of the observed attacks is using a code-signing certificate that belongs to PMG PTE LTD, the firm behind Ivacy VPN.

In fact, the same certificate is utilized to sign the official Ivacy VPN installer linked to from the VPN provider's site.

"It is likely that at some point the PMG PTE LTD signing key has been stolen – a commonplace strategy of known Chinese threat actors to enable malware signing," hypothesizes SentinelLabs.

"VPN providers are critical targets since they enable threat actors to potentially gain access to sensitive user data and communications."

If the certificate was stolen, security researchers are concerned about what else threat actors had access to at the VPN provider.

PMG PTE LTD has not responded to this disclosure with a public statement, so the exact means by which the hackers gained access to the certificate remain unclear.

Meanwhile, DigiCert revoked and invalidated the certificate in early June 2023 for breach of the "Baseline Requirements" guidelines.

BleepingComputer contacted Ivacy about their abused code-signing certificate but did not get a response.

6. **Cybercriminals train AI chatbots for phishing, malware attacks** – In the wake of WormGPT, a ChatGPT clone trained on malware-focused data, a new generative AI hacking tool called FraudGPT has emerged, and at least another one is under development that's allegedly based on Google's AI experiment, Bard.

   Both AI-powered bots are the work of the same individual, who appears to be deep in the game of providing chatbots trained specifically for malicious purposes ranging from phishing and social engineering to exploiting vulnerabilities and making malware.

   FraudGPT came out on July 25 and has been promoted on various hacker forums by somebody with the username CanadianKingpin12, who says the tool is intended for fraudsters, hackers, and spammers.

NEXT-GEN CYBERCRIME CHATBOTS

An investigation by researchers at cybersecurity company SlashNext, reveals that CanadianKingpin12 is actively training new chatbots utilizing unrestricted data sets sourced from the dark web or basing them on sophisticated large language models created for battling cybercrime.

In private discussions, CanadianKingpin12 said that they were working on DarkBART - a "dark version" of Google's conversational generative AI chatbot.

The researchers also learned that the advertiser had access to another large language model named DarkBERT, which was developed by South Korean researchers and trained on dark web data to battle cybercrime.

DarkBERT is available to academics based on relevant email addresses, but SlashNext highlights that this criteria is far from a challenge for hackers or malware developers, who can get access to an email address from an academic institution for around $3.

SlashNext researchers shared that CanadianKingpin12 said that the DarkBERT bot is "superior to all in a category of its own specifically trained on the dark web." The malicious version has been tuned for:

- Creating sophisticated phishing campaigns that target people's passwords and credit card details
- Executing advanced social engineering attacks to acquire sensitive information or gain unauthorized access to systems and networks.
- Exploiting vulnerabilities in computer systems, software, and networks.
- Creating and distributing malware.
- Exploiting zero-day vulnerabilities for financial gain or systems disruption.

7. **New acoustic attack steals data from keystrokes with 95% accuracy** – A team of researchers from British universities has trained a deep learning model that can steal data from keyboard keystrokes recorded using a microphone with an accuracy of 95%.

   When Zoom was utilized for training the sound classification algorithm, the prediction accuracy dropped to 93%, which is still dangerously high, and a record for that medium.

   Such an attack severely affects the target's data security, as it could leak people's passwords, discussions, messages, or other sensitive information to malicious third parties.

   In addition, contrary to other side-channel attacks that require special conditions and are subject to data rate and distance limitations, acoustic attacks have become much simpler due to the abundance of microphone-bearing devices that can achieve high-quality audio captures.

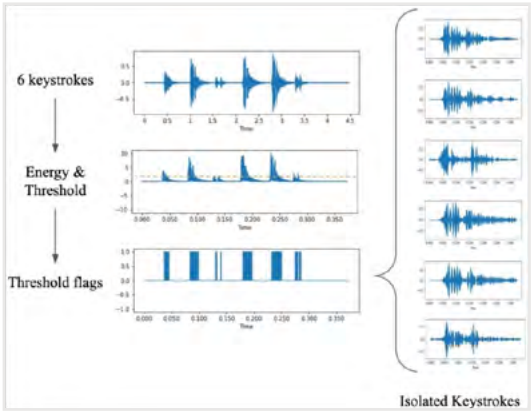
   This, combined with the rapid advancements in machine learning, makes sound-based side-channel attacks feasible and a lot more dangerous than previously anticipated.

LISTENING TO KEYSTROKES

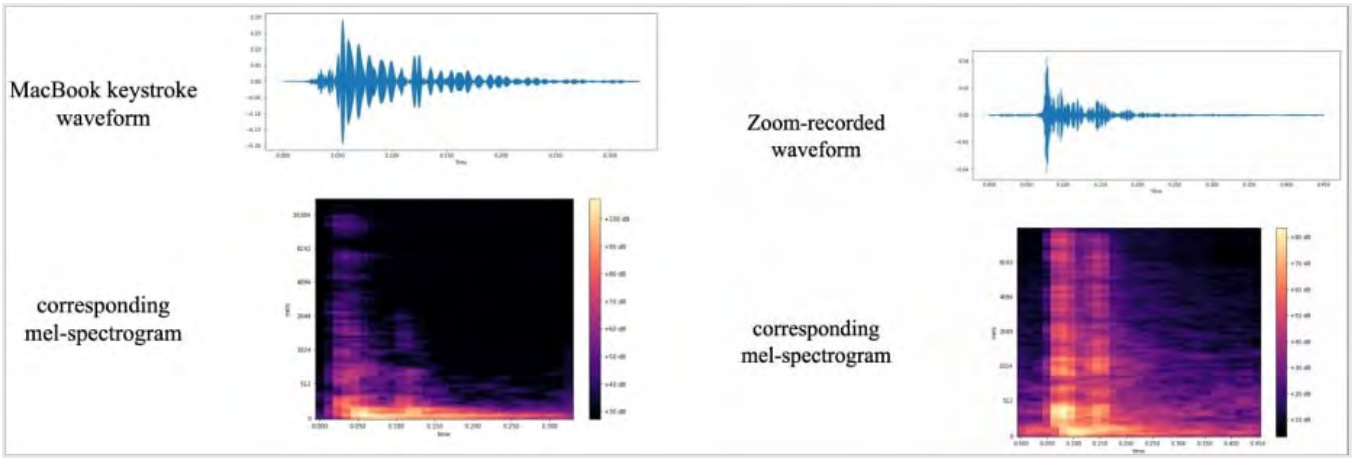
The first step of the attack is to record keystrokes on the target's keyboard, as that data is required for training the prediction algorithm. This can be achieved via a nearby microphone or the target's phone that might have been infected by malware that has access to its microphone.

Alternatively, keystrokes can be recorded through a Zoom call where a rogue participant makes correlations between messages typed by the target and their sound recording.

The researchers gathered training data by pressing 36 keys on a modern MacBook Pro 25 times each and recording the sound created by each press.



At that point, they created waveforms and spectrograms from the recordings that visualize identifiable differences for each key and performed specific data processing steps to augment the signals that can be utilized for identifying keystrokes.

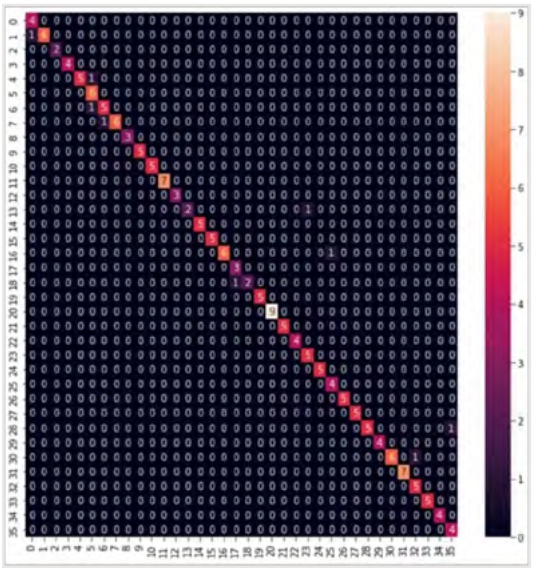


Produced spectrograms

The spectrogram images were utilized to train 'CoAtNet,' which is an image classifier. The process required some experimentation with epoch, learning rate, and data splitting parameters until the best prediction accuracy results could be achieved.

Parameter	Value
Epochs	1100
Batch Size	16
Loss Type	Cross Entropy
Optimiser	Adam
Max Learning Rate	5e-4
Annealing Schedule	Linear
Timeshift Percentage	0.4
Max Mask Percentage	0.1
Number of Masks Per Axis	2
Mel Bands	64
FFT Window Size	1024
Hop Length	225
Data Split	Random
Normalised Data	Yes

Parameters selected for training CoAtNet



Confusion matrix for phone-recorded keystrokes (arxiv.org)

In their experiments, the researchers utilized the same laptop, whose keyboard has been utilized in all Apple laptops for the past two years, an iPhone 13 mini placed 17cm away from the target, and Zoom.

The CoANet classifier accomplished 95% accuracy from the smartphone recordings and 93% from those captured through Zoom. Skype produced a lower but still usable 91.7% precision.

POSSIBLE MITIGATIONS

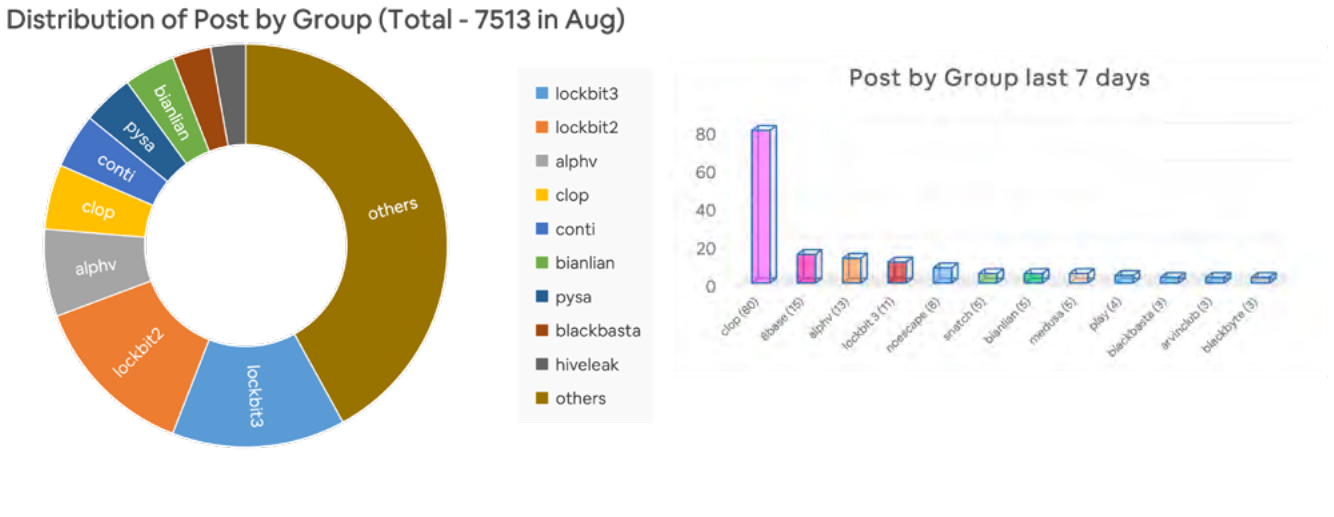
For users who are overly stressed about acoustic side-channel attacks, the paper recommends that they try altering typing styles or utilizing randomized passwords.

Other potential defense measures include using software to reproduce keystroke sounds, white noise, or software-based keystroke audio filters.

Keep in mind, the attack model proved highly effective even against a very silent keyboard, so adding sound dampeners on mechanical keyboards or switching to membrane-based keyboards is unlikely to help.

Ultimately, employing biometric authentication where feasible, and utilizing password managers to circumvent the need to input sensitive information manually, also serve as mitigating factors.

Ransomware Engagement Tracker

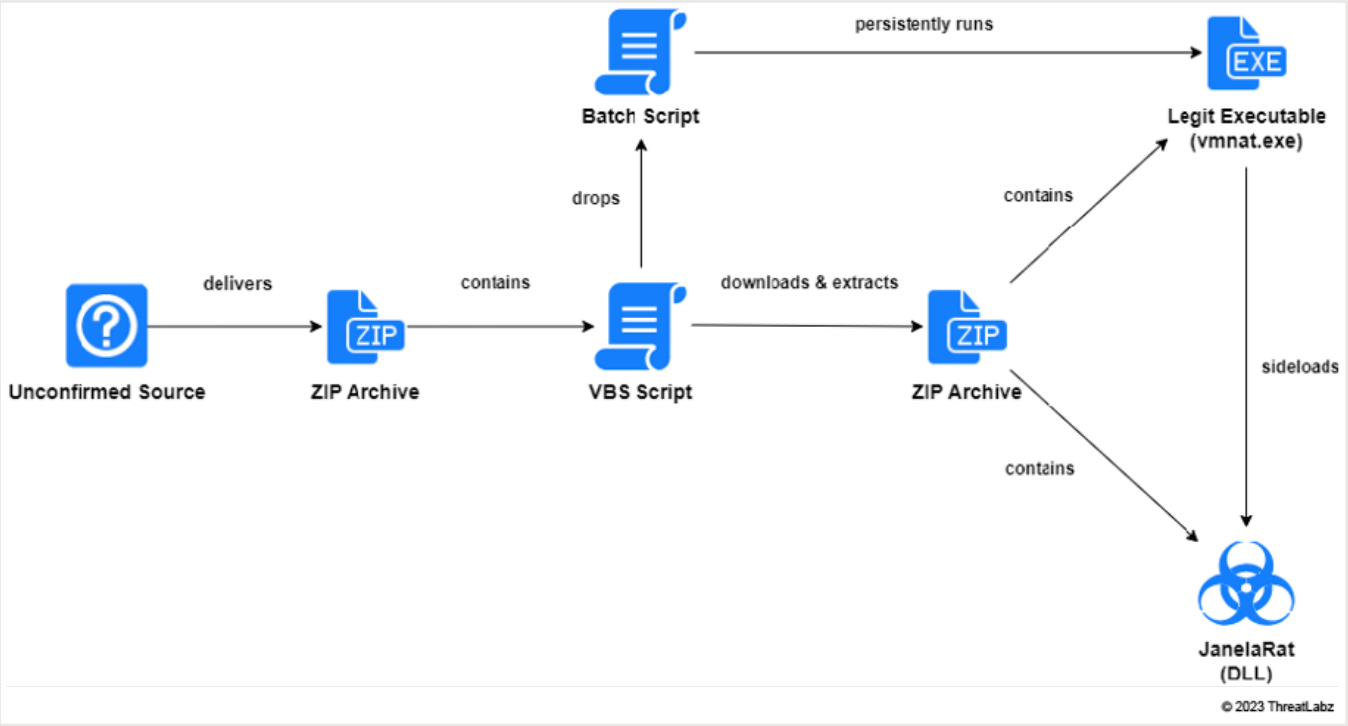


New Financial Malware 'JanelaRAT' Targets Latin American Users

- JanelaRAT is a new financial malware that targets people in Latin America (LATAM), according to Zscaler ThreatLabz. This attack steals private data from infected Microsoft Windows systems.
- Gaetano Pellegrino and Sudeep Singh, researchers from Zscaler ThreatLabz, claim that JanelaRAT primarily targets financial and cryptocurrency data from LATAM banks and financial institutions. JanelaRAT also hides from detection by side-loading trustworthy DLLs from trustworthy sources (like VMware and Microsoft).
- LATAM threat actors frequently employ original or modified commercial Remote Access Trojans (RATs). The stealth and targeted nature of JanelaRAT is highlighted by the fact that it has concentrated on collecting LATAM financial data and extracting window titles for transmission.

Detection

- Unknown methods of infection were used in the campaign; however, the cybersecurity firm found a ZIP archive file containing a Visual Basic Script in June 2023. To keep the infection persistent, VBScript drops a second ZIP archive into a batch file after retrieving it from the attackers' server.
- The JanelaRAT payload and a genuine executable (identity_helper.exe or vmnat.exe) are both included in the ZIP bundle and are utilized to execute the former using DLL side-loading.
- Contrarily, JanelaRAT uses string encryption and enters an idle state when it needs to evade discovery and analysis. Additionally, it is a significantly altered version of the 2014 discovery of BX RAT.
- One of the new features of the trojan is its capacity to record window titles and relay them to the threat actors, but only after the newly infected host has registered with the command-and-control (C2) server. Other capabilities of JanelaRAT enable it to gather system metadata, record keystrokes, capture screenshots, and track mouse actions.



VBScript Evaluation

- For technical investigation, we used the following VBScript with an MD5 hash:
  - 24c6bff8ebfd532f91ebe06dc13637cb
- The VBScript uses extremely basic code obfuscation. Our team was able to determine the VBScript's function after decoding every string in it.

- The following are the key tasks that VBScript performs:
  1. Drops a BAT file with a randomly created 7-character alphanumeric name in the location C:\Users\Public.
  2. Extracts a base64-encoded ZIP package after downloading content from the URL hxxp://zimbawhite.is-certified[.]com:3001/clientes/6.
  3. Base64 decodes the data and stores the ZIP archive with an 8-character alphanumeric file name that is generated at random.
  4. BAT file is run.
  5. Restarts the victim's computer after five seconds of sleep.

Prevention

- Block unknown scripts from running.
- Patch all DLL & script files in production.
- Do not click on the malicious link.
- Use anti-proxy techniques to avoid malicious IP sources.
- Disallow the RDP & SSH feature for unknown connections.
- Do not install unwanted applications from untrusted sources.
- Do not use malicious/free VPN to access web applications or networks.
- Implement packet filtration & IDS/IPD mechanisms through the firewall.
- Enable SSL with SMTP protocol for safe transmission.
- Enable limitations on administrative access or rights.

Remediation

- Monitor event logs.
- Regularly back up data and store backups offline.
- Enable automatic software updates on computers.
- Administrators should limit port proxy usage within environments.
- Download only trusted software from known sites.
- Use post method for sending & retrieving data through communication channels.
- Update your machine & servers on a monthly basis.
- Enable packet filtration through the firewall.
- Configure DLP in environment properly.
- Update the operating system (OS) and all installed programs.
- Use paid VPN to access web applications or networks.
- Use trusted anti-malware & anti-phishing programs.
- Enable two-factor authentication for transferring data packets.

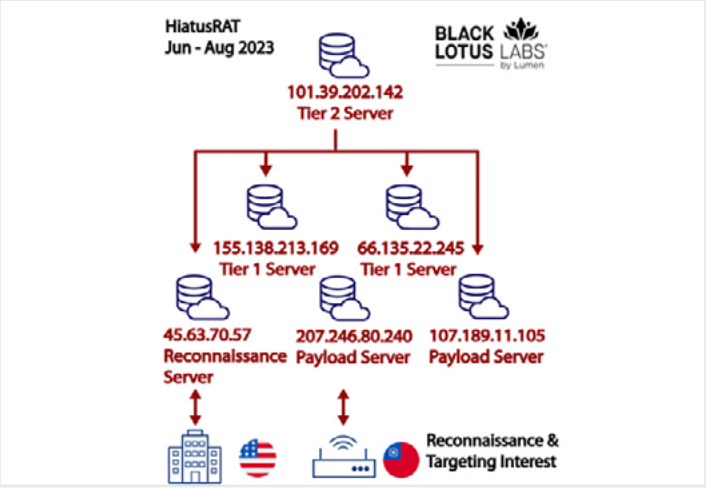
HiatusRAT Malware Resurfaces: Taiwan Firms and U.S. Military Under Attack

Image Source: HiatusRAT Malware Resurfaces: Taiwan Firms and U.S. Military Under Attack

- A new wave of spying and targeting activities has been launched against Taiwanese firms and a U.S. military procurement system by the threat actors responsible for the HiatusRAT malware.
- In a study released last week, Lumen Black Lotus Labs said that the artifacts were hosted on fresh virtual private servers (VPSs) in addition to being recompiled as malware versions for various architectures.
- The activity cluster was referred to by the cybersecurity company as “brazen” and “one of the most audacious,” showing no signs of slowing down. The threat actors’ identities and places of origin are currently unknown.
- Targets included industrial companies like semiconductor and chemical producers, at least one Taiwanese municipal government agency, and a U.S. Department of Defense (DoD) computer.

Detection

- HiatusRAT was initially exposed by the cybersecurity firm in March 2023 as having targeted business-grade routers as part of a campaign that started in July 2022 to discreetly spy on victims who were mostly located in Latin America and Europe.
- Globally, up to 100 edge networking devices were infected with malware that allowed it to passively collect traffic and turn the devices into a command-and-control (C2) infrastructure proxy network.
- The most recent attacks, seen from mid-June through August 2023, make use of HiatusRAT binaries that have already been produced and are optimized for the Arm, Intel 80386, and x86-64 architectures, as well as MIPS, MIPS64, and i386.



- Over 91% of the inbound connections were from Taiwan, according to a telemetry study used to determine connections made to the server hosting the malware, and there looked to be preference for Ruckus-manufactured edge devices.
- Payload and reconnaissance servers that talk directly to the victim networks make up the HiatusRAT infrastructure. Tier 1 servers seize control of these servers, which are then run and maintained by Tier 2 servers.
- The hackers connected to the DoD server on June 13 for almost two hours using two separate IP addresses: 207.246.80[.]240 and 45.63.70[.]57, according to the information available. An estimated 11 MB of bi-directional data was exchanged during that time.
- Although the ultimate objective is unclear, it is believed that the opponent may have been searching for publicly accessible information about current and upcoming military contracts to target them in the future.

Prevention

- Block unknown scripts from running.
- Do not click on the malicious link.
- Use anti-proxy techniques to avoid malicious IP sources.
- Disallow the RDP feature for unknown connections.
- Do not install unwanted applications from untrusted sources.
- Do not use malicious/free VPN to access web applications or networks.

- Implement packet filtration & IDS/IPD mechanisms through the firewall.
- Enable SSL with SMTP protocol for safe transmission.
- Enable limitations on administrative access or rights.

Remediation

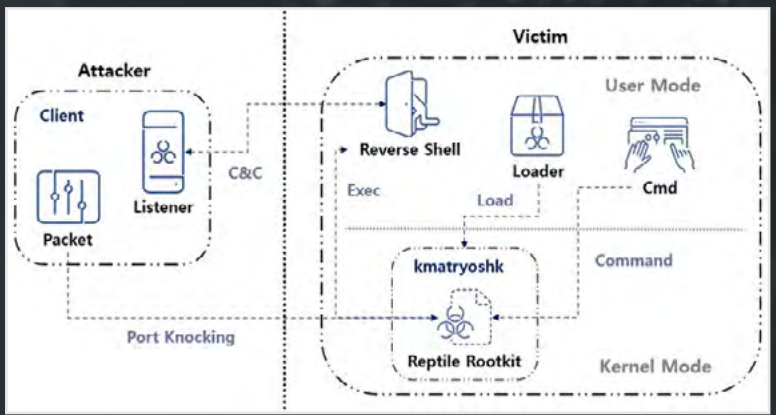
- Monitor event logs.
- Administrators should limit port proxy usage within environments.
- Download only trusted software from known sites.
- Use post method for sending & retrieving data through communication channels.
- Update your machine & servers on a monthly basis.
- Enable packet filtration through the firewall.
- Configure DLP in environment properly.
- Update the operating system (OS) and all installed programs.
- Use paid VPN to access web applications or networks.
- Use trusted anti-malware & anti-phishing programs.
- Enable two-factor authentication for transferring data packets.

Reptile Rootkit: Advanced Linux Malware Targeting South Korean Systems

- The open-source Reptile rootkit is being used by threat actors to target Linux systems in South Korea.
- Reptile offers a reverse shell, which enables threat actors to quickly take control of systems. This is in contrast to other rootkit malware that normally just provides concealing capabilities, according to research released this week by the AhnLab Security Emergency Response Center (ASEC).
- Port knocking is a technique when malware on an infected system opens a certain port and then goes on standby. The magic packet that the threat actor transmits to the system is then utilized as the foundation for a connection to the C&C server.
- A malicious software program called a rootkit is made to grant privileged, root-level access to a computer while hiding its true intentions.

Detection

- The rootkit was first employed by an intrusion set known as Earth Berberoka (also known as GamblingPuppet) in an attack on a gambling website in China. It was discovered that this intrusion set used the malware to conceal connections and processes related to the cross-platform Python trojan known as Pupy RAT.
- Google-owned Mandiant described a series of attacks carried out by a threat actor with a possible connection to China known as UNC3886 that made use of Fortinet device zero-day vulnerabilities to distribute a number of bespoke implants as well as Reptile.
- ExaTrack exposed the usage of a Reptile-based Linux virus named Mélofée by a Chinese hacking outfit. Microsoft found a cryptojacking operation that downloaded Reptile using a shell script backdoor in order to hide its kid.
- A closer look at Reptile reveals the use of a loader, which employs the kmatryoshka tool to decrypt and load the kernel module of the rootkit into memory. Thereafter, it opens a particular port and waits for the attacker to send a magic packet to the host using protocols like TCP, UDP, or ICMP.



- “A reverse shell connects to the C&C server, and the data received through the magic packet contains the C&C server address.”
- It’s important to note that another rootkit called Syslogk previously used magic packets to activate malicious behavior.
- An assault using Reptile that had some tactical parallels to Mélofée was also discovered by the South Korean cybersecurity company.

Prevention

- Block unknown scripts from running.
- Do not click on the malicious link.
- Use anti-proxy techniques to avoid malicious IP sources.
- Disallow the RDP feature for unknown connections.
- Do not install unwanted applications from untrusted sources.
- Do not use malicious/free VPN to access web applications or networks.
- Implement packet filtration & IDS/IPD mechanisms through the firewall.
- Enable limitations on administrative access or rights.

Remediation

- Monitor event logs.
- Administrators should limit port proxy usage within environments.
- Download only trusted software from known sites.
- Use post method for sending & retrieving data through communication channels.
- Update your machine & servers on a monthly basis.
- Enable packet filtration through the firewall.
- Configure DLP in environment properly.
- Update the operating system (OS) and all installed programs.
- Use paid VPN to access web applications or networks.
- Use trusted anti-malware & anti-phishing programs.
- Enable two-factor authentication for transferring data packets.

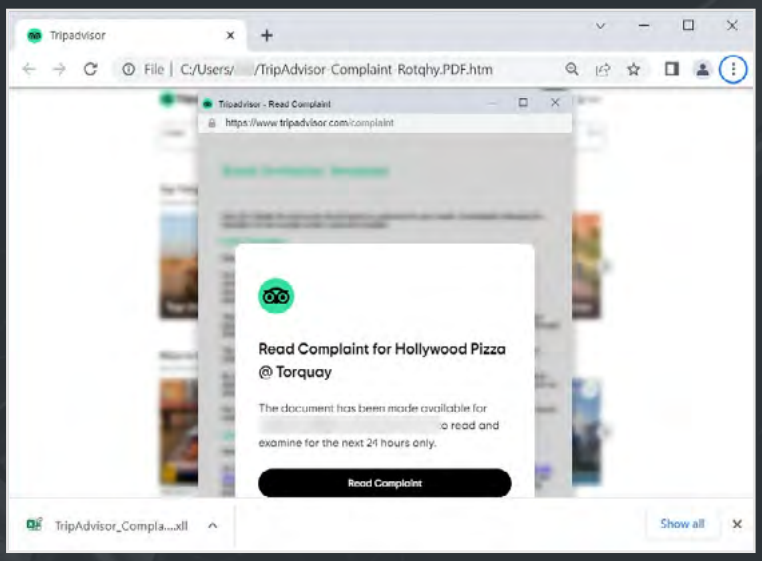
Knight Ransomware Distributed in Fake Tripadvisor Complaint E-mails

- An ongoing spam effort that poses as TripAdvisor complaints is used to spread the Knight ransomware.
- The Cyclop Ransomware-as-a-Service, which changed its name around the end of July 2023, is now known as the Knight ransomware.
- When the operators started looking for affiliates for the new Ransomware-as-a-Service (RaaS) on the RAMP hacker forum in May 2023, the Cyclops ransomware operation officially got underway.
- According to a report by Uptycs, the operation began with encryption software for Windows, macOS, and Linux/ESXi. Additionally, the business makes information-stealing malware for Windows and Linux available to affiliates, which is unusual for RaaS operations.

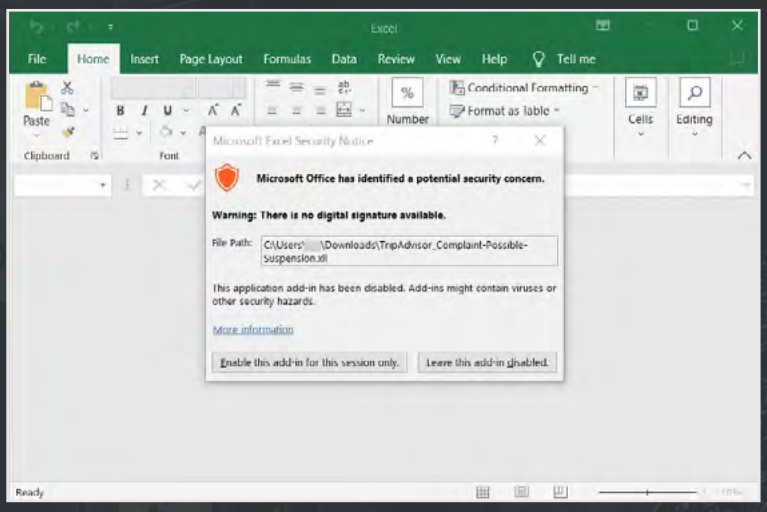
Detection

- Felix claimed that the emails have ZIP file attachments named “TripAdvisorComplaint.zip” that contain an executable file called “TripAdvisor Complaint - Possible Suspension.exe” [VirusTotal], even though the actual emails themselves were not disclosed.
- ‘TripAdvisor-Complaint-[random].PDF.htm’ is an HTML attachment that is part of a more recent version of this campaign that was discovered and examined [VirusTotal].
- When the HTML file is opened, it will open what seems to be a browser window to TripAdvisor using Mr.D0x’s Browser-in-the-Browser phishing technique.

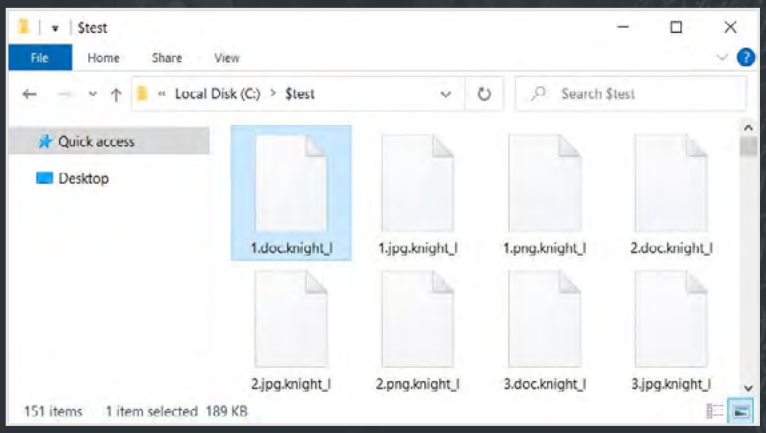
- This false browser window requests that the user review a complaint that has been made about a restaurant. The 'Read Complaint' button, on the other hand, downloads an Excel XLL file with the name 'TripAdvisor_Complaint-Possible-Suspension.xll' [VirusTotal], as seen in the screenshot below.

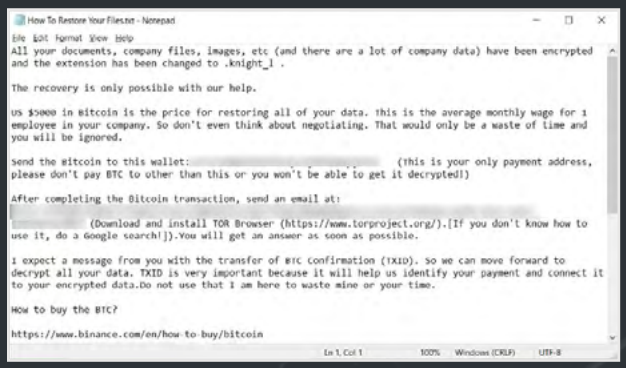


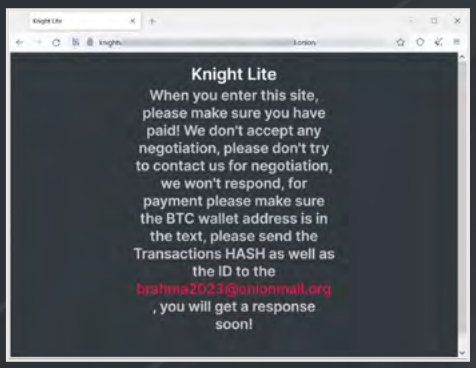
- The malware is executed when this XLL file is opened thanks to Excel-DNA, which integrates.NET into Microsoft Excel.
- Microsoft Excel will recognise the Mark-of-the-Web (MoTW), which is attached to files downloaded from the Internet, including email, when you open the XLL. If it recognises the MoTW, it won't allow the.NET add-in integrated into the Excel document, rendering the attack ineffective until a user releases the file's restrictions.
- Excel will ask the user whether they wish to enable the add-in if there isn't a MoTW flag present on the file, as illustrated below.



- By turning on the add-in, the Knight Lite ransomware encryptor will be injected into a new explorer.exe process and start encrypting your computer's contents.
- It will add the.knight_l extension to encrypted files' names after encryption, where the 'l' part most likely stands for 'light.'







- Additionally, each folder on the computer will get a ransom note called How to Restore Your Files.txt from the ransomware. This campaign's ransom note includes a link to the Knight Tor website and requests $5,000 be delivered to a Bitcoin address provided.
- The same Bitcoin address, "14JJfrWQbud8c8KECHyc9jM6dammyjUb3Z," is used in every ransom note in this campaign that BleepingComputer has seen, making it hard for the threat actor to identify which victim paid the ransom.
- A negotiating panel is not visible while browsing the website because this is a Knight Lite campaign. Instead, it displays a message advising victims to get in touch with the affiliate at brahma2023@onionmail.org once they have paid the ransom demand.
- It is unknown at this moment whether paying a ransom will entitle you to a decryptor from the Knight affiliate.
- Additionally, all the ransom notes that have come across have the same Bitcoin address, making it feasible for someone else to pretend to be you and take your money.

Prevention

- Block unknown scripts from running.
- Do not click on the malicious link.
- Apply filter to accept only trusted HTTPS connections.
- Use anti-proxy techniques to avoid malicious IP sources.
- Disallow the communication feature for unknown connections.
- Do not install unwanted applications from untrusted sources.
- Do not use malicious/free VPN to access web applications or networks.
- Implement packet filtration & IDS/IPD mechanisms through the firewall.
- Enable limitations on administrative access or rights.

Remediation

- Monitor event logs.
- Administrators should limit port proxy usage within environments.
- Download only trusted software from known sites.
- Use post method for sending & retrieving data through communication channels.
- Update your machine & servers on a monthly basis.
- Enable packet filtration through the firewall.
- Configure DLP in environment properly.
- Update the operating system (OS) and all installed programs.
- Use paid VPN to access web applications or networks.
- Use trusted anti-malware & anti-phishing programs.
- Enable two-factor authentication for transferring data packets.

TOP THREAT ACTORS

Threat Actor	IOC Reference
ANTIBOT.PW	https://inquest.net/blog/adversary-on-the-defense-antibot-pw/?web_view=true
QuiteRAT	https://blog.talosintelligence.com/lazarus-quiterat/?&web_view=true
CypherRAT and CraxsRAT	https://cyware.com/news/evlf-dev-knowing-the-creator-of-cypherrat-and-craxsrat-82edf546

TOP EXPLOITED VULNERABILITIES

Threat	Description	Reference Link
Unified Automation UaGateway Certificate Parsing Integer Overflow Denial-of-Service Vulnerability CVE-2023-41185	Vulnerability allows remote attackers to create a denial-of-service condition on affected installations of Unified Automation UaGateway. The specific flaw exists within the processing of client certificates.	https://cve.report/CVE-2023-41185
NETGEAR Orbi 760 SOAP API Authentication Bypass Vulnerability CVE-2023-41183	Vulnerability allows network-adjacent attackers to bypass authentication on affected installations of NETGEAR Orbi 760 routers. The specific flaw exists within the implementation of the SOAP API.	https://therecord.media/netgear-releases-patches-for-two-bugs
D-Link DAP-2622 DDP Set Wireless Info Auth Password Stack-based Buffer Overflow Remote Code Execution Vulnerability CVE-2023-37326	Vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of D-Link DAP-2622 routers. The issue results from the lack of proper validation of the length of user-supplied data prior to copying it to a fixed-length stack-based buffer.	https://www.tenable.com/cve/CVE-2022-37326
Apple macOS ImageIO EXR File Parsing Out-Of-Bounds Write Remote Code Execution Vulnerability CVE-2023-32384	Vulnerability allows remote attackers to execute arbitrary code on affected installations of Apple macOS. Interaction with the ImageIO library is required to exploit this vulnerability, but attack vectors may vary depending on the implementation.	https://www.zerodayinitiative.com/advisories/ZDI-23-1226/
(0Day) LG Simple Editor copyContent Exposed Dangerous Function Remote Code Execution Vulnerability CVE-2023-40501	Vulnerability allows remote attackers to execute arbitrary code on affected installations of LG Simple Editor. The specific flaw exists within the implementation of the copyContent command.	https://www.zerodayinitiative.com/advisories/ZDI-23-1217/
(0Day) Maxon Cinema 4D SKP File Parsing Stack-based Buffer Overflow Remote Code Execution Vulnerability CVE-2023-40485	Vulnerability allows remote attackers to execute arbitrary code on affected installations of Maxon Cinema 4D. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file.	https://www.zerodayinitiative.com/advisories/ZDI-23-1187/
(Pwn2Own) HP Color LaserJet Pro M479fdw CFF Font Parsing Stack-based Buffer Overflow Remote Code Execution Vulnerability CVE-2023-35177	Vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of HP Color LaserJet Pro M479fdw printers. The issue results from the lack of proper validation of the length of user-supplied data prior to copying it to a fixed-length stack-based buffer.	https://support.hp.com/ie-en/document/ish_8651888-8651916-16/hpsbpi03853
7-Zip 7Z File Parsing Integer Underflow Remote Code Execution Vulnerability CVE-2023-31102	Vulnerability allows remote attackers to execute arbitrary code on affected installations of 7-Zip. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of 7Z files.	https://www.suse.com/security/cve/CVE-2023-31102.html
NETGEAR RAX30 UPnP Command Injection Remote Code Execution Vulnerability CVE-2023-40479	Vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of NETGEAR RAX30 routers. The issue results from the lack of proper validation of a user-supplied string before using it to execute a system call.	https://www.cyberveille-sante.gouv.fr/alertes/netgear-cve-2023-40479-2023-08-23
Advantech R-SeeNet Use Of Hard-Coded Credentials Authentication Bypass Vulnerability CVE-2023-2611	Vulnerability allows remote attackers to bypass authentication on affected installations of Advantech R-SeeNet. The specific flaw exists within the configuration of the database.	https://www.cisa.gov/news-events/ics-advisories/icsa-23-173-02
SonicWALL GMS Virtual Appliance Syslog Directory Traversal Remote Code Execution Vulnerability CVE-2023-34129	Vulnerability allows remote attackers to execute arbitrary code on affected installations of SonicWALL GMS Virtual Appliance. Although authentication is required to exploit this vulnerability, the existing authentication mechanism can be bypassed.	https://www.zerodayinitiative.com/advisories/ZDI-23-1154/

Security Bulletin

1. **New Wave of Attack Campaign Targeting Zimbra Email Users for Credential Theft –** JumpCloud, a company that offers identity and access management services in the cloud, responded quickly to a recent cyberattack that affected some of its customers.

   An new "mass-spreading" social engineering campaign is targeting users of the Zimbra Collaboration email server with an aim to collect their login credentials for use in follow-on operations.

   The activity, active since April 2023 and still ongoing, targets a wide range of small and medium businesses and governmental entities, most of which are found in Poland, Ecuador, Mexico, Italy, and Russia. It has not been attributed to any known threat actor or group.

   "At first, the target gets an e-mail with a phishing page in the attached HTML file," ESET researcher Viktor Šperka said in a report. "The e-mail warns the target about an email server update, account deactivation, or similar issue and directs the user to click on the attached file."

   The messages also spoof the from address to seem as if they are coming from a Zimbra administrator in a likely attempt to persuade the recipients to open the attachment.

   The HTML file contains a Zimbra login page tailored to the targeted organization, with the username field prefilled with the victim's email address to make it seem more authentic. Once the credentials are entered, they are collected from the HTML form and sent by means of a HTTPS POST request to an actor–controlled server.

2. **New Apple iOS 16 Exploit Enables Stealthy Cellular Access Under Fake Airplane Mode**

   Cybersecurity researchers have documented a novel post-exploit persistence technique on iOS 16 that could be abused to fly under the radar and maintain access to an Apple device even when the victim believes it is offline.

   The strategy " tricks the victim into thinking their device's Airplane Mode works when, in reality, the attacker (following successful device exploit) has planted an artificial Airplane Mode which edits the UI to display Airplane Mode icon and cuts internet connection to all apps except the attacker application," Jamf Risk Labs analysts Hu Ke and Nir Avraham said in a report shared with The Hacker News.

   Airplane Mode, as the name implies, allows users to turn off wireless features in their devices, effectively preventing them from connecting to Wi-Fi networks, cellular data, and Bluetooth, as well as preventing them from sending or receiving calls and text messages.

   The approach devised by Jamf, in a nutshell, deceives the user into believing that Airplane Mode is on while allowing a malicious actor to stealthily maintain a cellular network connection for a rogue application.

   "When the user turns on Airplane Mode, the network interface pdp_ip0 (cellular data) will no longer display IPv4/IPv6 IP addresses," the researchers explained. "The cellular network is disconnected and unusable, at least to the user space level."

   While the underlying changes are carried out by CommCenter, the user interface (UI) modifications, such as the icon transitions, are taken care of by the SpringBoard.

   The goal of the attack, then, is to devise an artificial Airplane Mode that keeps the UI changes intact but retains cellular connectivity for a malicious payload to be delivered and installed on the device by other means.

   "After enabling Airplane Mode without a Wi-Fi connection, users would expect that opening Safari would result in no connection to the internet," the researchers said. "The typical experience is a notification window that prompts a user to 'Turn Off Airplane Mode.'"

   To pull off the ruse, the CommCenter daemon is utilized to block cellular data access for specific apps and disguise it as Airplane Mode by means of a hooked function that alters the alert window to look like the setting has been turned on.

   It's worth noting that the operating system kernel notifies the CommCenter via a callback routine, which, in turn, notifies the SpringBoard to display the pop-up.

   A closer examination of the CommCenter daemon has also revealed the presence of an SQL database that's used to record the cellular data access status of each app (aka bundle ID), with a flag set to the value "8" if an application is blocked from accessing it.

   "Utilizing this database of installed application bundle IDs, we can now selectively block or allow an app to access Wi-Fi or cellular data," the researchers said.

   "When combined with the other techniques outlined above, the fake Airplane Mode now appears to act just as the real one, except that the internet ban does not apply to non-application processes such as a backdoor trojan."

3. **Windows Defender-Pretender Attack Dismantles Flagship Microsoft EDR**

A newly patched flaw in Windows Defender allows attackers to hijack the signature-update process to sneak in malware, delete benign files, and inflict mayhem on target systems.

Among the 97 CVEs that Microsoft patched in April 2023 was a security feature bypass vulnerability that allows an unprivileged user to hijack Windows Defender and use it to wreak havoc on target systems.

Researchers at SafeBreach—who previously discovered similar vulnerabilities in security products—uncovered the issue with Windows Defender during an attempt take over the antivirus tool's update process.

HIJACKING THE UPDATE PROCESS

The research goal was to verify if the update process could be used to sneak known malware into systems the software is designed to protect. Researchers also wanted to verify if they could get Windows Defender to delete signatures of known threats, and worse, to delete benign files and trigger a denial-of-service condition on a compromised system.

The researchers were able to achieve all three objectives and even develop an automated tool dubbed wd-pretender—for Windows Defender Pretender—that implemented each of the attack vectors. Microsoft assigned a CVE for the issue they discovered—CVE-2023-24934—and issued a fix for it in April.

SafeBreach researchers Tomer Bar and Omer Attias presented a summary of their findings at a Black Hat USA session on Wednesday, entitled "Defender Pretender: When Windows Defender Updates Become a Security Risk."

In a discussion with Dark Reading before their presentation, Bar and Attias say their research was inspired by the sophisticated Flame cyberespionage campaign that targeted organizations in Iran and other countries in the Middle East back in 2012. The nation-state actor behind the campaign inserted themselves into the middle of the Windows update process and used it to deliver the Flame malware tool on previously infected computers.

Bar says the objective with SafeBreach's latest research was to see if they could replicate something similar without a complex man-in-the-middle attack and without a forged certificate—as with the case with the Flame campaign. Altogether, the researchers wanted to see if they would take over the Windows Defender update process as an unprivileged user.

THE DEFENDER UPDATE PROCESS

In considering the Windows Defender update process, Bar and Attias discovered that signature updates are typically contained in a single executable file called the Microsoft Protection Antimalware Front End (MPAM-FE[.]exe). The MPAM file in turn contained two executables and four additional Virtual Device Metadata (VDM) files with malware signatures in compressed—but not encrypted—form. The VDM files worked in tandem to push signature updates to Defender.

The researchers discovered that two of the VDM files were large-sized "Base" files that contained some 2.5 million malware signatures, while the other two were smaller-sized, but more complex, "Delta" files. They determined the Base file was the main file that Defender checked for malware signatures during the update process, while the smaller Delta file defined the changes that needed to be made to the Base file.

At first, Bar and Attias attempted to see if they could hijack the Defender update process by replacing one of the executables in the MPAM file with a file of their own. Defender immediately spotted that the file was not Microsoft-signed and stopped the update process, Bar says.

4. **Microsoft OneDrive a willing and eager 'ransomware double agent'**

There's a rather serious ransomware vulnerability in Microsoft's desktop operating system, according to research out this week. It's nigh undetectable, uses a fully legitimate workflow to encrypt files, and comes pre-installed on all new Windows systems: OneDrive.

As per the discoveries presented by SafeBreach security researcher Or Yair today at Black Hat, OneDrive was a ready and willing double agent Yair was able to turn against the systems it's designed to sync cloud storage for and ostensibly protect.

"Microsoft describes OneDrive as a shield against ransomware," Yair told The Register. "OneDrive is used for ransomware data recovery, and Microsoft even recommends that users store important files in OneDrive because they're better protected in the cloud."

However, as Yair illustrated during his talk, a series of mistakes by both Microsoft and third-party vendors have shown OneDrive to be an easily tricked piece of software eager to encrypt anything it can get a junction to.

THEY LEFT SESSION TOKENS WHERE?

OneDrive, for those unfamiliar with it, is both Microsoft's cloud storage service and the locally run application installed on Windows

devices to synchronize files between a OneDrive directory on said machine and Microsoft's remote servers.

The first thing one would do in order to turn OneDrive into a double agent, then, would be to hijack someone's account¬—a task Yair said was relatively easy once he managed to achieve an initial compromise of a Windows machine.

OneDrive, it turns out, stores all of its log files in a directory for the signed-in user. Those logs, in turn, contain session tokens that Yair said he was able to pull out of the log file once he snagged a copy and parsed it. With the stolen token, Yair was able to get to work.

Getting out of OneDrive's own directories was simple enough. Yair said that while symbolic links can only be created by an administrator (which Yair wasn't operating as during his tests), junctions can be created by anyone, but can only point to a directory, not a specific file.

"Once we create junctions to areas outside of OneDrive's own directory, we achieve a situation where it can create, modify or delete files on a local machine," Yair said.

OneDrive includes features that prevent ransomware from destroying backups by ensuring there are shadow copies of files that can be restored in case of an attack; though, Yair says he was able to subvert those features, too, with the OneDrive app for Android being the weak point in that instance.

An API utilized by the app is different from other OneDrive apps, and those differences allowed Yair to delete the original copies of files that he'd encrypted in such a way that they were unrecoverable, leaving the victim with nothing but encrypted backups of encrypted files.

EDR CAN'T SAVE YOU HERE.

The first response one may have to such a ransomware threat—that a legitimate application would suddenly go rogue and begin encrypting files all over a device—is an understandable one: let endpoint detection and response software handle it.

EDR software, Yair said, should detect such activity, especially the deletion of shadow copies. However, software from several major enterprise vendors failed to spot the OneDrive spy in their midst. CyberReason doesn't detect the vandalism, neither does Microsoft Shield for Endpoint, CrowdStrike Bird of prey, or Palo Alto Cortex XDR, it was claimed.

SentinelOne's software did catch it, and raised a flag about the possibility of a ransomware attack. Unfortunately, it still didn't stop shadow copies from being deleted because the local OneDrive executable is on an allow list.

Since it's a trusted application in multiple EDRs, OneDrive doesn't trip alarms when it alters decoy files, is using known and trusted file extensions for encrypted files, and is allowed to take action in otherwise restricted folders. Since there's no actual malware installed on the target machine, there's no static signature to detect, either.

5. Multiple data center vulnerabilities could cripple cloud services.

Vulnerabilities affect data center services commonly used by organizations and could be exploited by attackers to gain system access and perform remote code execution.

Numerous vulnerabilities in data center infrastructure management systems/power distribution units have the potential to cripple popular cloud-based services. That's according to new findings from the Trellix Advanced Research Center, which revealed four vulnerabilities in CyberPower's Data Center Infrastructure Management (DCIM) platform and five vulnerabilities in Dataprobe's iBoot Power Distribution Unit (PDU).

The vulnerabilities could be utilized to gain full access to these systems and perform remote code execution (RCE) to create device backdoors and an entry point to the broader network, according to the researchers. They are basic, require little expertise or hacking tools, and could be executed in minutes, the team added. At the time of disclosure, Trellix said it had not discovered any malicious use of the exploits in the wild. The research into the vulnerabilities was presented at DEF CON in Las Vegas.

The data center market is seeing rapid growth as businesses turn to digital transformation and cloud services to support new working habits and operational efficiencies. In the US alone, data center demand is expected to reach 35 gigawatts (GW) by 2030, up from 17 GW in 2022, according to analysis from McKinsey & Company. However, today's data centers are a critical attack vector for cybercriminals wanting to spread malware, blackmail businesses for ransom, conduct corporate or foreign espionage, or shut down large swaths of the web.

REMOTE CODE EXECUTION, AUTHENTICATION BYPASS, DOS AMONG RISKS

CyberPower provides power protection and management systems for computer and server technologies. Its DCIM platform allows IT teams to manage, configure, and monitor the infrastructure within a data center through the cloud, serving as a single source of information and control for all devices. "These platforms are commonly used by companies managing on-premises server deployments to larger, co-located data centers— like those from major cloud providers AWS, Google Cloud, Microsoft Azure, etc." the researchers wrote.

The four vulnerabilities Trellix found in CyberPower's DCIM are:

- **CVE-2023-3264: Use of hard-coded credentials (CVSS 6.7).**
- **CVE-2023-3265: Improper neutralization of escape, meta, or control sequences (auth bypass, CVSS 7.2).**
- **CVE-2023-3266: Improperly implemented security check for standard (auth bypass, CVSS 7.5).**
- **CVE-2023-3267: OS command injection (authenticated remote code execution, CVSS 7.5).**

Dataprobe manufactures power management products that assist businesses in monitoring and controlling their equipment. iBoot PDU allows administrators to remotely manage the power supply to their devices and equipment via a web application. Dataprobe has thousands of devices across numerous industries, including deployments in data centers, travel and transportation infrastructure, financial institutions, smart city IoT installations, and government agencies, Trellix said.

The five vulnerabilities Trellix found in Dataprobe's iBoot PDU are:

- **CVE-2023-3259: Deserialization of untrusted data (auth bypass, CVSS 9.8).**
- **CVE-2023-3260: OS command injection (authenticated RCE, CVSS 7.2).**
- **CVE-2023-3261: Buffer overflow (DoS, CVSS 7.5).**
- **CVE-2023-3262: Use of hard-coded credentials (CVSS 6.7).**
- **CVE-2023-3263: Authentication bypass by alternate name (auth bypass, CVSS 7.5).**

MALWARE AT SCALE, DIGITAL ESPIONAGE, POWER OUTAGES POTENTIAL IMPACTS

Attackers can exploit these sorts of vulnerabilities within data center deployments to launch malware at scale, carry out digital espionage, and knock out power altogether, the researchers said. Using these platforms to create a backdoor on the data center equipment provides bad actors a foothold to compromise a huge number of systems and devices. "Some data centers host thousands of servers and connect to hundreds of various business applications. Malicious attackers could slowly compromise both the data center and the business networks connected to it." Malware across such a huge scale of devices could be leveraged for massive ransomware, DDoS, or wiper attacks - potentially even more far reaching than those of SuxNet, Mirai BotNet, or WannaCry, according to Trellix.

Moreover, nation-state sponsored and other advanced persistent threat (APT) actors could leverage these exploits to conduct cyberespionage attacks. "The 2018 concerns of spy chips in data centers would become a digital reality if spyware installed in data centers worldwide were to be leveraged for cyber espionage to inform foreign nation states of sensitive data."

Even the ability to turn the data center off by accessing such power management systems would be significant, the researchers noted. "Websites, business applications, consumer technologies, and critical infrastructure deployments all rely on these data centers to operate. A threat actor could shut that all down for days at a time with the simple "flip of a switch" in dozens of compromised data centers." Furthermore, manipulation of the power management can be used to damage the hardware devices themselves— making them far less effective, if not inoperable, they added.

CHECK FOR INTERNET EXPOSURE, INSTALL LATEST FIRMWARE.

Both Dataprobe and CyberPower have released fixes for the vulnerabilities with CyberPower DCIM version 2.6.9 of their PowerPanel Enterprise software and the latest 1.44.08042023 version of the Dataprobe iBoot PDU firmware. "We strongly urge all potentially impacted customers to download and install these patches immediately," Trellix said. In addition to the official patches, the researchers advised extra steps for any devices or platforms potentially exposed to zero-day exploitation by the vulnerable products.

- Ensure that PowerPanel Enterprise or iBoot PDU are not exposed to the wider internet. Each should be reachable only from within an organization's secure intranet. In the case of the iBoot PDU, Trellix suggested disabling remote access via Dataprobe's cloud service as an added precaution.
- Modify the passwords associated with all user accounts and revoke any sensitive information stored on both appliances that may have been leaked.
- Update to the most recent version of PowerPanel Enterprise or install the latest firmware for the iBoot PDU and subscribe to the relevant vendor's security update notifications.

6. The Vulnerability of Zero Trust: Lessons from the Storm 0558 Hack

While IT security managers in companies and public administrations rely on the concept of Zero Trust, APTS (Advanced Persistent Threats) are putting its practical effectiveness to the test. Analysts, on the other hand, understand that Zero Trust can only be achieved with comprehensive insight into one's own network.

Just recently, an attack believed to be perpetrated by the Chinese hacker group Storm-0558 targeted several government agencies. They used fake digital authentication tokens to access webmail accounts running on Microsoft's Outlook service. In this incident, the

attackers stole a signing key from Microsoft, enabling them to issue functional access tokens for Outlook Web Access (OWA) and Outlook.com and to download emails and attachments. Due to a plausibility check error, the digital signature, which was only intended for private customer accounts (MSA), also worked in the Azure Active Directory for business customers.

EMBRACING THE ZERO TRUST REVOLUTION

According to a report by vendor Okta (State of Zero-Trust Security 2022) 97% of respondents are already engaged in a zero-trust strategy or plan to implement one within the next 18 months. This has increased the percentage of Zero Trust advocates from 24% (2021) to 55% (2022). The security model known as Zero Trust is an overarching security strategy designed to continuously audit and verify access to resources, both internally and externally. Many organizations are embracing this security strategy based on the principle that network devices and users must constantly prove their identity, as they are not automatically trusted.

Zero Trust relies on continuous monitoring and dynamic control for applications, users and devices. It limits access to resources to the absolute minimum and all identities on the platform are evaluated using the same criteria as hosts. The overarching goal is to enhance security by granting access only to those who continuously prove their identity and whose behavior is under constant scrutiny.

PEERING PAST THE PERIMETER: WHAT IS REALLY HAPPENING IN YOUR NETWORK

Identity and access management (IAM) undoubtedly play a fundamental role in Zero Trust. Unfortunately, constant verification of users' identities proves ineffective in cases of stolen identity. Moreover, attackers can bypass these systems by manipulating meta-information, such as the geolocation of a potential login, using a spoofed VPN address. IDS/IPS systems are tasked with detecting suspicious or unauthorized activity, virus infections, malware and ransomware, zero-day attacks, SQL injection and more. However, IDS/IPS systems often only detect known signatures, such as previously identified malicious domains or IP addresses. If a domain hasn't been flagged as malicious beforehand, conventional security solutions may overlook it, allowing attackers to exploit the weak link in the chain. Consequently, traditional cybersecurity systems can sometimes falter when it comes to actualizing Zero Trust in action.

To implement a Zero Trust security strategy effectively, organizations are increasingly turning to network analysis tools, as recently recommended by the analyst firm Forrester ("The Network Analysis and Visibility Landscape, Q1 2023"). According to the Forrester report, security and risk professionals should employ Network Detection and Response (NDR) tools to monitor their networks, search for threats, detect applications and assets, and capture malicious data packets. These actions contribute to the effective detection of threats within IT infrastructures.

NETWORK DETECTION & RESPONSE (NDR): THE UNSUNG HERO OF ZERO TRUST SECURITY

NDR solutions are vital for creating a resilient and effective Zero Trust architecture. They provide real-time visibility into network traffic, monitor user behavior and device activity, and enable swift detection and response to suspicious network operations or anomalous activities. This visibility extends to all operating systems, application servers, and IoT devices.

Forrester has highlighted that the significance of enterprise networks in cyberattacks is often underestimated. Cybercriminals use fake identities or zero-day exploits to infiltrate corporate networks, then move laterally across the network to search for targets, gain access to privileged systems, install ransomware or other malware, and exfiltrate corporate data. NDR facilitates internal reconnaissance—where the attacker surveys potential targets—or lateral movement detection when the attacker is already in the network. NDR systems gather data from all switches and operate entirely without agents, which may not be installable in many environments.

MACHINE LEARNING NDR: THE NEW STANDARD IN ANOMALY DETECTION

With Machine Learning (ML), Network Detection and Response (NDR) systems are capable of detecting traffic anomalies without relying on pre-stored, known "Indicators of Compromise" (IoCs). These ML models are designed to be continuously trained, enabling them to detect new threats and attack techniques. This approach significantly accelerates the detection of malicious activities and enables early attack mitigation. Moreover, it aids in identifying unknown, suspicious behaviour and minimizes the time attackers can dwell unnoticed within a network, thereby enhancing overall security.

HOW EXEONTRACE, A LEADING ML-BASED NDR, ANALYZES META DATA IN ORDER TO PROVIDE NETWORK VISIBILITY, ANOMALY DETECTION AND INCIDENT RESPONSE.

Machine learning algorithms establish the baseline of normal network behavior by analyzing data and algorithms to learn what is "normal" for the network in communication patterns. These algorithms are trained to learn what constitutes "normal" activity for the network, thereby enabling them to detect deviations from this established baseline. Examples of such deviations include suspicious connections, unusual data transfers, traffic patterns that fall outside established norms, lateral movements within the network, data exfiltration, and more.

Exeon is a leading NDR solutions provider headquartered in Switzerland with a strong knowledge base and a foundation rooted in cybersecurity expertise. The NDR platform, Exeon Trace, offers comprehensive network monitoring powered by advanced Machine Learning technology. It enables automated detection of potential cyber threats, making it an essential tool for Security Operations Center (SOC) teams and Chief Information Security Officers (CISOs), who are committed to implementing and maintaining a robust Zero Trust security strategy.

7. Microsoft PowerShell Gallery vulnerable to spoofing, supply chain attacks.

Lax policies for package naming on Microsoft's PowerShell Gallery code repository allow threat actors to perform typosquatting attacks, spoof popular packages and potentially lay the ground for massive supply chain attacks..

PowerShell Gallery is a Microsoft-run online repository of packages uploaded by the wider PowerShell community, hosting a large number of scripts and cmdlet modules for various purposes.

It is a very popular code hosting platform, and some packages on it count tens of millions of monthly downloads.

Aqua Nautilus discovered the problems in the market's policies in September 2022, and even though Microsoft has acknowledged the reception of the corresponding bug reports and PoC exploits, it has not taken action to remediate the flaws.

EASY SPOOFING

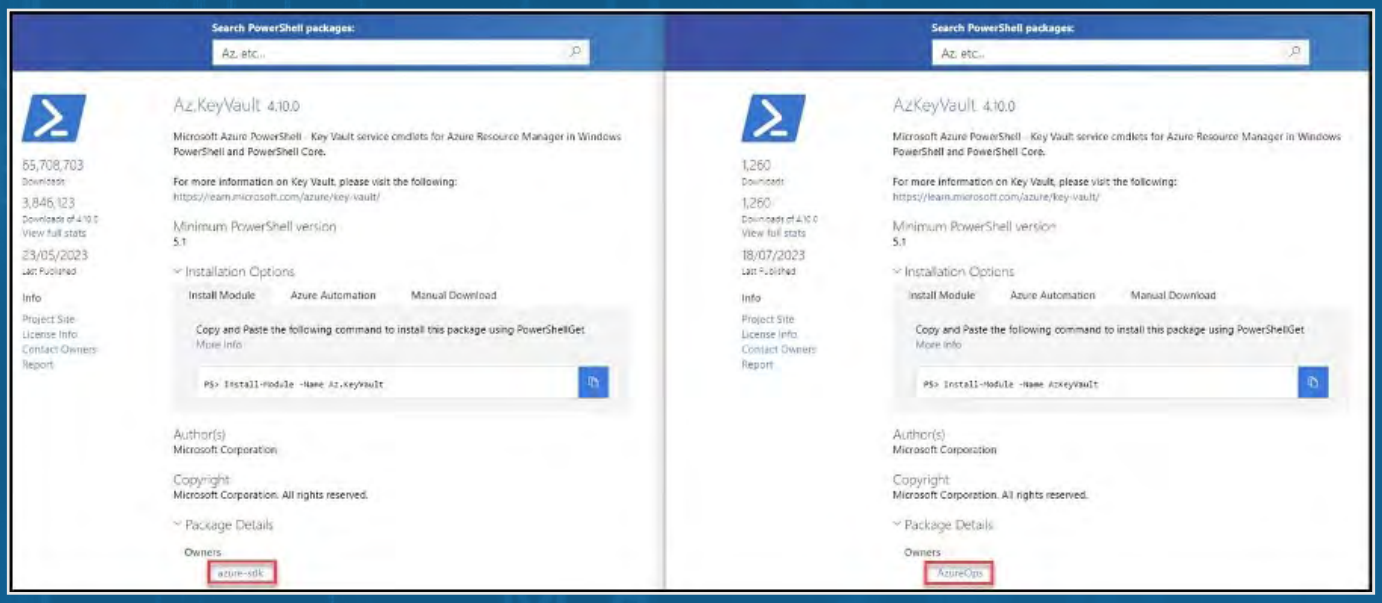
AquaSec's Nautilus team discovered that users can submit to the PS Gallery packages with very similar names to existing repositories, so-called 'typosquatting' when cybercriminals use it for malicious purposes.

A proof-of-concept (PoC) example in the report refers to the popular "AzTable" module with a download count of 10 million, which could be easily impersonated with a new name like 'Az.Table', making it difficult for users to distinguish between them.

Another issue the researchers discovered is the ability to spoof module details, including author and copyright, by copying them from legitimate projects.

Not only would this make the first issue of package typosquatting even more dangerous, but it can also be abused to make arbitrary packages appear as the work of trustworthy publishers.

Moreover, PS Gallery hides by default the more reliable 'Owner' field beneath 'Package Details', which shows the publisher account that uploaded the package.



Spoofed package (left) and real module (right)

EXPOSING HIDDEN PACKAGES

A third imperfection found by AquaSec concerns the ability to expose unlisted packages/modules on the platform, which are normally not indexed by the Gallery's search engine.

To the researchers' surprise, they found on the platform an XML file that provided comprehensive details about both listed and unlisted packages.

"By utilizing the API link located at the bottom of the XML response [...], an attacker can gain unrestricted access to the complete PowerShell package database, including associated versions." clarifies AquaSec's Nautilus team.

"This uncontrolled access provides malicious actors with the ability to search for potentially sensitive information within unlisted packages."

```
Param(
    [Switch] $ToGallery
)

Write-Host "$(Get-Date) Unloading and reloading.."


Write-Host "$(Get-Date)
Remove-Module
Remove-Item                                                    -Force -Recurse
Copy-Item
Recurse

If($ToGallery)
{
    Write-Host "$(Get-Date) Publishing to gallery.."
    Publish-Module -NuGetApiKey "oy2                    e" -Name
}
```

API key of a big tech firm exposed on the unlisted project.

DISCLOSURE AND MITIGATION

AquaSec reported all flaws to Microsoft on September 27, 2022 and was able to replicate them on December 26, 2022, despite Microsoft stating in early November that they had fixed the issues.

On January 15, 2023, Microsoft stated that a short-term solution was implemented until its engineers developed a fix for the name typosquatting and package details spoofing.

AquaSec said that on August 16 the flaws still persisted, indicating that a fix had not been implemented.

Users of the PS Gallery repository are advised to adopt policies that allow execution of only signed scripts, utilize trusted private repositories, regularly scan for sensitive data in module source code, and implement real-time monitoring systems in cloud environments to detect suspicious activity.

REFERENCE LINKS

- https://analyticsindiamag.com/microsoft-crushes-openai-with-databricks/
- https://www.firstpost.com/tech/news-analysis/us-hit-by-major-cyberattack-hackers-exploit-ibm-steal-over-millions-of-peoples-healthcare-personal-data-12999372.html
- https://www.theverge.com/2023/7/25/23806705/amd-ryzen-cpu-processor-zenbleed-vulnerability-exploit-bug
- https://thehackernews.com/2023/08/wooflocker-toolkit-hides-malicious.html
- https://www.bleepingcomputer.com/news/security/hackers-use-vpn-providers-code-certificate-to-sign-malware/
- https://www.bleepingcomputer.com/news/security/cybercriminals-train-ai-chatbots-for-phishing-malware-attacks/
- https://www.bleepingcomputer.com/news/security/new-acoustic-attack-steals-data-from-keystrokes-with-95-percent-accuracy/
- https://thehackernews.com/2023/08/new-wave-of-attack-campaign-targeting.html
- https://thehackernews.com/2023/08/new-apple-ios-16-exploit-enables.html
- https://www.darkreading.com/attacks-breaches/-researchers-detail-vuln-that-allowed-for-windows-defender-update-process-hijack
- https://www.theregister.com/2023/08/10/microsoft_onedrive/
- https://www.csoonline.com/article/649344/multiple-data-center-vulnerabilities-could-cripple-cloud-services.html
- https://thehackernews.com/2023/08/the-vulnerability-of-zero-trust-lessons.html
- https://www.bleepingcomputer.com/news/security/microsoft-powershell-gallery-vulnerable-to-spoofing-supply-chain-attacks/
- https://securereading.com/janelarat-a-new-financial-malware-targets-latin-american-users/#:~:text=According%20to%20Zscaler%20ThreatLabz%20researchers,such%20as%20VMware%20and%20Microsoft).
- https://www.zscaler.com/author/threatlabz?_bt=&_bk=&_bm=&_bn=x&_bg=&utm_source=google&utm_medium=cpc&utm_campaign=google-ads-na&gclid=CjwKCAjw6eWnBhAKEiwADpnw9jIWxCH5KEDSXlsxT_gaC3y9krwUgvcRWw1MR7DomwriHaObDKhiPhoC2SQQAvD_BwE
- https://thehackernews.com/2023/08/hiatusrat-malware-resurfaces-taiwan.html#:~:text=HiatusRAT%20Malware%20Resurfaces%3A%20Taiwan%20Firms%20and%20U.S.%20Military%20Under%20Attack,-%EE%A0%82Aug%2021&text=The%20threat%20actors%20behind%20the,a%20U.S.%20military%20procurement%20system.
- https://thehackernews.com/2023/08/reptile-rootkit-advanced-linux-malware.html
- https://linuxsecurity.com/news/hackscracks/reptile-rootkit-advanced-linux-malware-targeting-south-korean-systems
- https://www.bleepingcomputer.com/news/security/knight-ransomware-distributed-in-fake-tripadvisor-complaint-emails/

About SDG

SDG is a global cybersecurity, identity governance, GRC, risk consulting and advisory firm. SDG's SaaS platform TruOps in combination with its services deliver a comprehensive range of identity, cybersecurity, risk, compliance, and cloud security solutions that enable organizations to identify and mitigate cyber risk, protect cyber assets, and manage their business securely.

To learn how SDG can help ensure the security and compliance of your technology and data infrastructure visit **www.sdgc.com** and **www.truops.com**.

55 North Water Street
Norwalk, CT 06854

203.866.8886

sdgc.com