Cyber Threat Advisory

DECEMBER 2023

Contents

Monthly Highlights	1
Ransomware Tracker	3
Gamaredon's LittleDrifter USB Malware Spreads Beyond Ukraine	4
Grayling: Previously Unseen Threat Actor Targets Multiple Organizations in Taiwan	6
Microsoft: Octo Tempest Is One of the Most Dangerous Financial Hackings Groups	8
Toyota Confirms Breach After Medusa Ransomware Threatens to Leak Data	10
Top Threat Actors	11
Top Exploited Vulnerabilities	11-12
Security Bulletin	12-15
Reference Links	16

Monthly Highlights - December

1. **Welltok Data Breach Exposes Data of 8.5 Million US Patients** – Healthcare SaaS provider Welltok has issued a cautionary statement, revealing that approximately 8.5 million patients in the United States had their personal data compromised in a recent data breach. The breach stemmed from a cyber-attack targeting the company's file transfer program.

   In late October, Welltok disclosed the data incident, stating that their MOVEit Transfer server fell victim to a breach on July 26, 2023. Despite promptly implementing security updates provided by the vendor, the breach still occurred.

   Welltok collaborates with healthcare service providers nationwide, overseeing online wellness initiatives, managing databases containing personal patient information, conducting predictive analytics, and supporting healthcare requirements such as medication adherence and pandemic response.

   For some individuals, the compromised information extended to include Social Security Numbers (SSNs), Medicare/Medicaid ID numbers, and specific health insurance details. Welltok did not immediately disclose the exact number of individuals affected, leading to varying estimates.

2. **New 'Looney Tunables' Linux Bug Gives Root on Major Distros** – A new Linux vulnerability, identified as 'Looney Tunables' and tracked as CVE-2023-4911, allows local attackers to acquire root privileges by exploiting a buffer overflow weakness in the GNU C Library's ld.so dynamic loader. As per Security Researchers, successful exploitation of this vulnerability results in full root privileges on major distributions such as Fedora, Ubuntu, and Debian.

   The ease with which the buffer overflow can be transformed into a data-only

attack could allow other research teams to soon produce and release exploits. This could put countless systems at risk, especially given the extensive use of glibc across Linux distributions.

The vulnerability activates when processing the GLIBC_TUNABLES environment variable on default installations of Debian 12 and 13, Ubuntu 22.04 and 23.04, and Fedora 37 and 38 (Alpine Linux, which employs musl libc, remains unaffected).

The GNU C Library (glibc) constitutes the C library for the GNU system and is present in most Linux kernel-based systems, furnishing crucial functionality, encompassing system calls like open, malloc, printf, exit, and others necessary for typical program execution.

Attackers with low privileges can exploit this high-severity vulnerability through low-complexity attacks that do not necessitate user interaction.

Researchers have urged system administrators to promptly apply patches, particularly for users of Fedora, Ubuntu, and Debian, while reassuring Alpine Linux users that they remain unaffected.

Unearthed by the Qualys Threat Research Unit, the flaw had originated in April 2021 with the release of glibc 2.34, introduced via a commit aimed at rectifying SXID_ERASE behavior in setuid programs.

3. **North Korea-Linked Lazarus Apt Laundered Over $900 Million Through Cross-Chain Crime** – The North Korea-linked Lazarus Group laundered $900 million in cryptocurrency between July 2022 and July 2023. According to a report published by Elliptic, the significant rise in cross-chain crime is evident in crypto thefts, scams, Ponzi schemes, and illicit laundering. The Lazarus Group alone is responsible for approximately 1/7th of all cross-chain crime tracked, having laundered over $900 million through these methods.

   Law enforcement operations have recently targeted multiple mixers, prompting threat actors, including both nation-state actors and cybercrime groups, to switch to chain- or asset-hopping typologies to launder stolen assets.

   Additionally, threat actors are exploiting the lack of efficient capabilities in mainstream blockchain analytics solutions to identify and oversee cross-chain activities.

   As per the report, in the past 104 days, the North Korea-linked APT group Lazarus has stolen the majority of $240 million in crypto assets from multiple businesses, including Atomic Wallet ($100 million), CoinsPaid ($37.3 million), Alphapo ($60 million), and Stake.com ($41 million).

4. **File-Transfer Services Containing Valuable Data Like MoveIt, GoAnywhere Are Actively Targeted by Attackers** – MOVEit environments faced a series of attacks in May, leading to downstream consequences persisting for five months. Supply-chain attacks targeted Progress Software's MOVEit, Fortra's GoAnywhere, and IBM Aspera Faspex over a three-month period starting in March.

   Clop ransomware group exploited a zero-day vulnerability in MOVEit and GoAnywhere. Clop was previously responsible for zero-day exploits against Accellion file-transfer devices in 2020 and 2021.

   Managed file-transfer services, like MOVEit, are considered opportunistic attack vectors due to the valuable data they handle. These services contain a "treasure trove" of high-value data beyond credentials, making them attractive for extortion or potential corporate espionage.

   Direct and indirect victims include major financial institutions, education service providers, government agencies, healthcare providers, insurance companies, and law firms.

   Intel 471 documented 17 vulnerabilities in managed file-transfer products since 2018. Out of 136 vulnerabilities impacting managed file transfer software since 2014, 51 are classified as high risk by the National Vulnerability Database.

   Organizations place implicit trust in these file-transfer services, leading to a false sense of security. Consequences from exposure are significant due to the extended period of time in which corporate data is handled by third parties during transfers.

   Managed file-transfer services are crucial for compliance, offering advanced features for monitoring, automation, and enhanced security. Compliance requirements make these services a one-to-many target for threat actors.

   MOVEit and similar services meeting regulatory compliance requirements become widely used for high-volume sensitive file sharing. Clop's attacks exposed private health information, school records, the largest U.S. pension system data, and information held by government contractors and major accounting firms.

5. **Iranian Hackers Exploit PLCs in Attack on Water Authority in U.S.** – The U.S. Cybersecurity and Infrastructure Security Agency (CISA) has reported its active response to a cyberattack involving the exploitation of Unitronics programmable logic controllers (PLCs) targeting the Municipal Water Authority of Aliquippa in western Pennsylvania. This attack has been attributed to the Iranian-backed hacktivist collective known as Cyber Av3ngers.

   The agency disclosed that cyber threat actors are specifically targeting PLCs associated with Water and Wastewater Systems (WWS) facilities, including an identified Unitronics PLC at a U.S. water facility. In reaction to this threat, the affected

municipality's water authority promptly took the system offline and transitioned to manual operations. Importantly, there is currently no known risk to the municipality's drinking water or water supply.

According to reports cited by the Water Information Sharing and Analysis Center (WaterISAC), Cyber Av3ngers allegedly gained control of the booster station responsible for monitoring and regulating pressure in Raccoon and Potter Townships.

The threat actors are believed to have exploited the lax password security and public internet accessibility of the affected device, a Unitronics Vision Series PLC with a Human Machine Interface (HMI).

Given the critical role of PLCs in the Water and Wastewater Treatment sector, where they monitor various stages and processes, disruptive attacks aiming to compromise the integrity of these critical processes can have severe consequences, hindering WWS facilities from providing clean, potable water.

To counter such threats, CISA recommends several measures, including changing the default password for Unitronics PLCs, implementing multi-factor authentication (MFA), disconnecting PLCs from the internet, regularly backing up logic and configurations for swift recovery, and applying the latest updates.

6. **SMBs Being Actively Targeted by Attackers Using Legitimate Tool-Based Attacks** – Threat actors increasingly favor exploiting legitimate tools over conventional malware to blend into network operations and avoid detection. As per a report by Huntress, nearly 3 in 5 incidents targeting SMBs during Q3 2023 were devoid of traditional malware.

   Malware still poses a significant threat, accounting for 44% of all incidents in Q3. However, attackers are more commonly exploiting scripting frameworks and legitimate tools, such as remote monitoring and management (RMM) software, to infiltrate victim networks.

   Almost two-thirds of observed incidents in Q3 involved some form of RMM software credential theft or capture. Third-party instances, like ScreenConnect, were abused to gain access to healthcare organizations' networks, with additional RMM software ensuring persistent access.

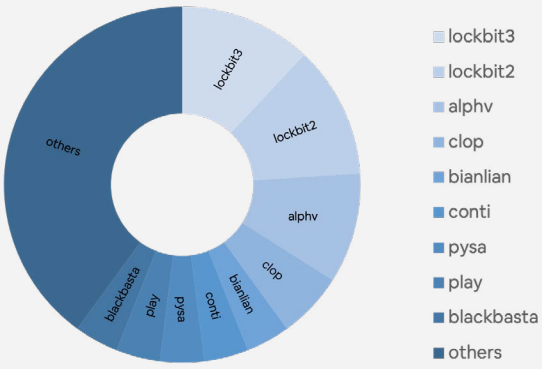
   Legitimate RMM tools like AnyDesk and ScreenConnect (now ConnectWise Control) were exploited in a campaign targeting federal employees since June 2022.

   Financially motivated attacks involved phishing emails posing as help desk communications to trick executive staff into downloading RMM software, leading to money theft from victim bank accounts.

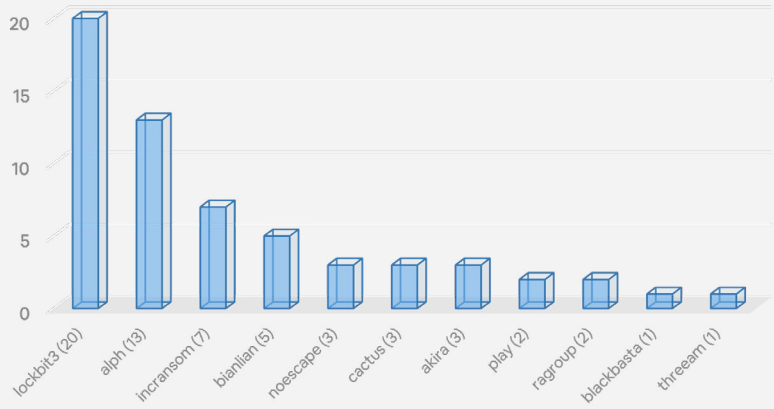
   Cybersecurity and Infrastructure Security Agency (CISA) notes a rising risk from the exploitation of RMM software. Threat actors utilize RMM to infiltrate managed service provider servers, gaining access to thousands of customers' networks.

Ransomware Tracker

Distribution of Post by Group (Total - 8950 in Nov)



Post by Group (Last 7 Days)



Gamaredon's LittleDrifter USB Malware Spreads Beyond Ukraine

The Gamaredon state-sponsored espionage group has been using USB devices to transmit a recently discovered worm known as LittleDrifter, which has infected systems across several nations.

Malware researchers discovered signs of compromise in the US, Ukraine, Germany, Vietnam, Poland, Chile, and Hong Kong. This implies that LittleDrifter, which was meant for unintentional targets, was no longer under the threat group's control.

Check Point analysis indicates that the virus is written in VBS and was created as a variation of Gamaredon's USB PowerShell worm, which spreads via USB sticks.

Gamaredon, sometimes referred to as Shuckworm, Iron Tilden, and Primitive Bear, is a Russian cyber espionage threat group that has been targeting Ukrainian organizations for ten years or more in a variety of industries, including critical infrastructure, government, and defense.

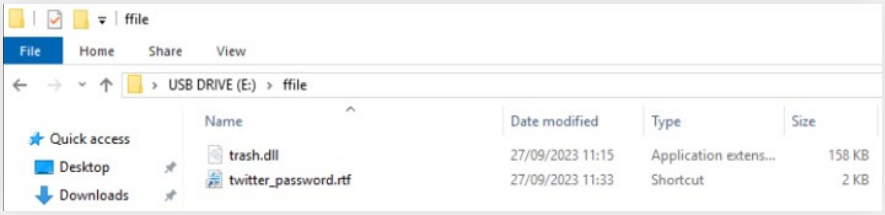
Detection

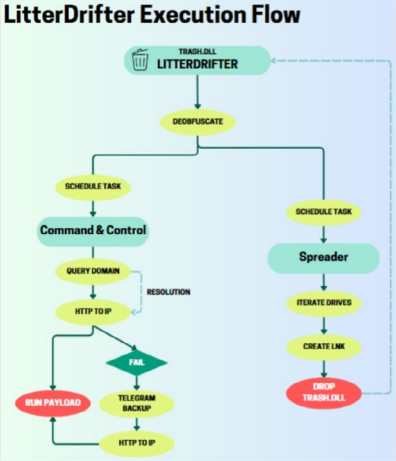
The goal of LitterDrifter is to propagate via USB drives and establish communication with the threat group's command and control (C2) server.

The malware uses two distinct modules, each of which is run by the heavily obfuscated VBS component trash.dll, to accomplish its goal.

Located in the user's "Favourites" directory, LitterDrifter and all its components create persistence through the addition of registry keys and scheduled tasks.

The module in charge of spreading to other systems makes a hidden copy of "trash.dll" and fake LNK shortcuts in addition to keeping an eye out for recently inserted USB drives.





The malware creates shortcuts with arbitrary names to run malicious scripts and uses the Windows Management Instrumentation (WMI) management framework to identify target drives.

According to the researchers, Gamaredon uses domains as stand-in IP addresses for the locations of the C2 servers. The threat group has a "rather unique" strategy from this angle.

```
WMIPath = "winmgmts:{impersonationlevel=impersonate}!\\.\root\cimv2"
WMIQuery = "select * from win32_logicaldisk where mediatype=null"
fileNameList = Array("Bank_account","постанова","Bank_account","службова","compromising_evidence")
wscriptArgs  = " ""trash.dll"" /webm //e:vbScript //b /wm /cal "
iconPath = "%WINDIR%\system32\shell32.dll, 1"
payloadFileName = "\trash.dll"
fileExtension = ".rtf.lnk"
wscriptPath = "%WINDIR%\system32\wscript.exe"
separator = "\"
userProfilePath = "%userprofile%"
Set shellInstance = CreateObject("wscript.shell")
originalScript = shellInstance.expandenvironmentstrings(userProfilePath) + payloadFileName
Set driveQuery = GetObject(WMIPath).execquery(WMIQuery)
For Each drive In driveQuery
    createShortcutsInSubfolders drive.caption , 0
Next
```

The malware searches for a configuration file in the temporary folder before attempting to connect to the C2 server. LittleDrifter uses a WMI query to ping one of Gamaredon's domains if such a file is not present.

As per previous reports on Gamaredon activity, Check Point observes that all domains utilized by the malware are registered under 'REGRU-RU' and utilize the '.ru' top-level domain.

Each IP address used as a C2 in LitterDrifter operations has a typical lifespan of roughly 28 hours, but to avoid being discovered and blocked, the addresses may change several times a day.

LitterDrifter tries to decode and run any additional payloads that the C2 sends on the compromised system. According to CheckPoint, most of the time no additional payloads were downloaded, which might suggest that the attacks are very focused. The malware can also obtain the C2 IP address from a Telegram channel as a fallback.

Because it attempts to establish persistence on the compromised system and waits for the C2 to deliver fresh payloads that would advance the attack, LitterDrifter is probably a component of the initial stage of an attack.

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 VPNs 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.

Grayling: Previously Unseen Threat Actor Targets Multiple Organizations in Taiwan

A previously unreported threat actor with an unclear origin has been connected to several attacks against Taiwanese companies in the IT, manufacturing, and biomedical industries.

The attacks were attributed to an advanced persistent threat (APT) known as Grayling by the Broadcom-owned Symantec Threat Hunter Team. Based on available data, the campaign started in February 2023 and ran through at least May 2023.

A government organization in the Pacific Islands, as well as organizations in Vietnam and the United States, are probably also targets of this activity.

Detection

The use of a unique DLL side-loading method by Grayling, which releases payloads using a customized decryptor, made this activity stand out. It seems that obtaining intelligence is the driving force behind this activity.

After using web shells to gain persistent access, the first foothold into victim environments is said to have been obtained by taking advantage of infrastructure that is visible to the public.

Then, using SbieDll Hook to enable DLL side-loading, the attack chains load a range of payloads, such as Mimikatz, Cobalt Strike, and NetSpy in addition to the Havoc framework. Grayling has also been seen to terminate every process included in a file named processlist.txt.

Many threat actors use the well-liked method of DLL side-loading to evade security measures and fool Windows into launching malicious code on the intended endpoint.

This is often achieved by using the DLL search order mechanism to place a malicious DLL with the same name as a legitimate DLL, which is used by an application in a location where it will load before the legitimate DLL.

After gaining initial access to the victims' computers, the attackers use downloaders, network scanning, and privilege escalation, among other tactics.

It's important to remember that DLL side-loading in relation to SbieDll_Hook and SandboxieBITS.exe was previously noted in the case of Naikon APT attacks against Southeast Asian military institutions.

File Indicators:

SHA256 hashes:
da670d5acf3648b0deaecb64710ae2b7fc41fc6ae8ab8343a1415144490a9ae9 – Havoc framework
79b0e6cd366a15848742e26c3396e0b63338ead964710b6572a8582b0530db17 – Downloader
bf1665c949935f3a741cfe44ab2509ec3751b9384b9eda7fb31c12bfbb2a12ec – Downloader
c2a714831d8a7b0223631eda655ce62ff3c262d910c0a2ed67c5ca92ef4447e3 – Cobalt Strike Beacon
667624b10108137a889f0df8f408395ae332cc8d9ad550632a3501f6debc4f2c – Exploit for CVE-2019-0803
87a7e428d08ecc97201cc8f229877a6202545e562de231a7b4cab4d9b6bbc0f8 – Downloader
90de98fa17294d5c918865dfb1a799be80c8771df1dc0ec2be9d1c1b772d9cf0 – Loader
8b6c559cd145dca015f4fa06ef1c9cd2446662a1e62eb51ba2c86f4183231ed2 – Cobalt Strike Stager
d522bf1fb3b869887eaf54f6c0e52d90514d7635b3ff8a7fd2ce9f1d06449e2c – NetSpy
4fbe8b69f5c001d00bd39e4fdb3058c96ed796326d6e5e582610d67252d11aba – DLL file
9bad71077e322031c0cf7f541d64c3fed6b1dc7c261b0b994b63e56bc3215739 – NetSpy
f2aaedb17f96958c045f2911655bfe46f3db21a2de9b0d396936ef6e362fea1b – Downloader
525417bdd5cdd568605fdbd3dc153bcc20a4715635c02f4965a458c5d008eba9 – Downloader
23e5dfaf60c380837beaddaaa9eb550809cd995f2cda99e3fe4ca8b281d770ae – Downloader
6725e38cbb15698e957d50b8bc67bd66ece554bbf6bcb90e72eaf32b1d969e50 – Downloader
5ef2e36a53c681f6c64cfea16c2ca156cf468579cc96f6c527eca8024bfdc581 – Downloader 12924d7371310c49b1a2150196215
97926ef3c0b4649352e032a884750fab746 – Windump
ab09e8cac3f13dea5949e7a2eaf9c9f98d3e78f3db2f140c7d85118b9bc6125f
c76ba3eb764706a32013007c147309f0be19efff3e6a172393d72d46631f712e
245016ace30eda7650f6bb3b2405761a6a5ff1f44b94159792a6eb64ced023aa
4c44efc7d9f4cd71c43c6596c62b91740eb84b7eb9b8cf22c7034b75b5f432d9
e75f2cee98c4b068a2d9e7e77599998196fd718591d3fa23b8f684133d1715c3
f3e8f2ef4ad949a0ada037f52f4c0e6000d111a4ac813e64138f0ded865e6e31
971ab5d4f0ec58fa1db61622a735a51e14e70ee5d99ab3cd554e0070b248eb1f

Image Source

File Indicators (Continued):

f1764f8c6fc428237ffafeb08eb0503558c68c6ccf6f2510a2ef8c574ba347e0
c24b19e7ccd965dfeed553c94b093533e527c55d5adbc9f0e87815d477924be5
af26d07754c8d4d1cb88195f7dc53e2e4ebee382c5b84fc54a81ba1cee4d0889
1f15c3ae1ce442a67e3d01ed291604bfc1cb196454b717e4fb5ac52daa37ecce
7ea706d8da9d68e1214e30c6373713da3585df8a337bc64fcc154fc5363f5f1f
30130ea1ab762c155289a32db810168f59c3d37b69bcbedfd284c4a861d749d6
74cbde4d4b4ac4cae943831035bff90814fa54fd21c3a6a6ec16e7e3fb235f87
752018c117e07f5d58eed35622777e971a5f495184df1c25041ff525ca72acea
6a8c39e4c543e94f6e4901d0facee7793f932cd2351259d8054981cf2b4da814
803d0d07d64010b102413da61bbf7b4d378891e2a46848b88ef69ca9357e3721
7c1b20de1f170cfaf3e75ebc7e81860378e353c84469795a162cd3cfd7263ba2
a180e67fcaf2254b18eafdc95b83038e9a4385b1a5c2651651d9d288fa0500fe
de500875266fd18c76959839e8c6b075e4408dcbc0b620f7544f28978b852c1c
1ed1b6a06abbab98471d5af33e242acc76d17b41c6e96cce0938a05703b58b91
ba8a7af30e02bd45e3570de20777ab7c1eec4797919bfcd39dde681eb69b9faf
1b72410e8e6ef0eb3e0f950ec4ced1be0ee6ac0a9349c8280cd8d12cc00850f9
dcadcac4c57df4e31dd7094ae96657f54b22c87233e8277a2c40ba56eafcf548
d0e1724360e0ae11364d3ac0eb8518ecf5d859128d094e9241d8e6feb43a9f29
b19ccfa8bc75ce4cf29eb52d4afe79fe7c3819ac08b68bd87b35225a762112ba
6e5d840ddeedc3b691e11a286acd7b6c087a91af27c00044dd1d951da5893068
3acfe90afa3cbb974e219a5ab8a9ee8c933b397d1c1c97d6e12015726b109f1b
5ed10f2564cd60d02666637e9eac36db36f3a13906b851ec1207c7df620d8970

Network Indicators:

Domain
d3ktcnc1w6pd1f.cloudfront[.]net

IP addresses
172.245.92[.]207
3.0.93[.]185

URLs
http://45.148.120[.]23:91/version.dll
http://45.148.120[.]23:91/vmtools.exe

Prevention

- Block unknown scripts from running.
- Patch all .DLL files on production.
- 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 VPNs 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.

Image Source

Microsoft: Octo Tempest Is One of the Most Dangerous Financial Hackings Groups

Microsoft has released a comprehensive profile of a native English-speaking threat actor who targets businesses with ransomware and data extortion. The threat actor, known as Octo Tempest, is well-versed in social engineering techniques.

Since early 2022, Octo Tempest's attacks have gradually changed, focusing on more companies that offer email, tech services, and cable telecommunications. They have also partnered with the ALPHV/BlackCat ransomware group.

Octo Tempest shifted its focus to data theft, social engineering, phishing, and mass password resets for clients of compromised service providers.

The threat group targeted managed service providers (MSPs) and businesses in the gaming, hospitality, retail, manufacturing, technology, and financial sectors earlier this year.

Following its affiliation with ALPHV/BlackCat, Octo Tempest used the ransomware to encrypt and pilfer victim data.

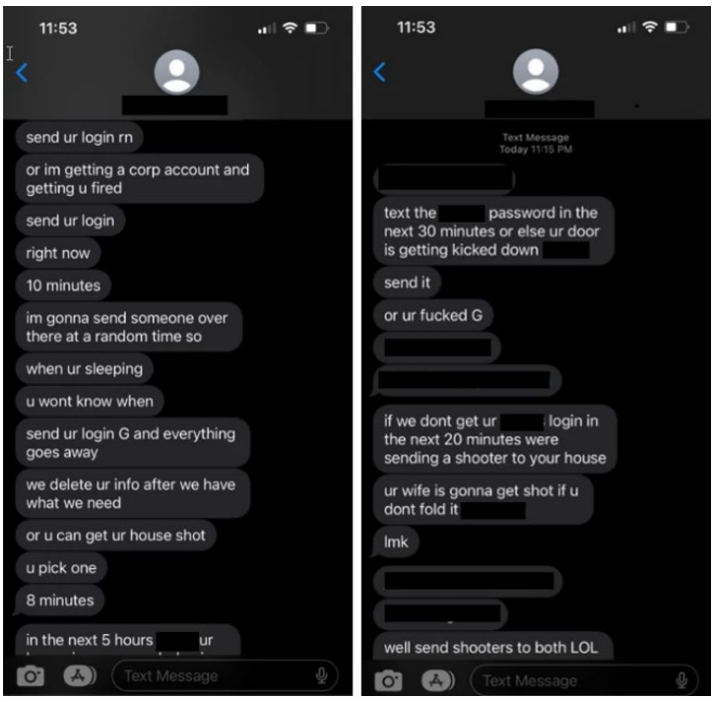
Detection

The group began to monetize intrusions by extorting victims after stealing data, and it also used its accumulated experience to build more sophisticated and aggressive attacks.

According to Microsoft, Octo Tempest has occasionally employed direct physical threats to gain login credentials that would further their attack.

Unexpectedly, Octo Tempest joined the ALPHV/BlackCat ransomware-as-a-service (RaaS) group, according to Microsoft. By June, they began distributing the Linux and Windows ransomware payloads, with a recent focus on VMware ESXi servers.

This group has been targeting businesses in several industries more recently, including gaming, tourism, natural resources, retail, consumer goods, manufacturing, legal services, technology, and financial services.



Octo Tempest TTPs

According to Microsoft, Octo Tempest is a well-run team with several hands-on keyboard operators and members with substantial technical expertise. Advanced social engineering is a common method used by hackers to obtain initial access to accounts belonging to technical administrators who possess sufficient permissions to carry out further attacks.

They conduct research on the business to determine which targets they can mimic in such a way that they can even mimic the person's speech patterns over the phone. Technical administrators are tricked into resetting multi-factor authentication (MFA) methods and passwords.

Other ways to get first access are as follows:

- Misleading the target into installing software for remote management and monitoring
- Obtaining login credentials via phishing websites
- Purchasing session tokens or credentials from other online fraudsters
- Tricking targets by SMS with links to false login portals that collect login credentials
- Call forwarding or SIM swapping
- Explicit threats of violence

After gaining adequate access, Octo Tempest hackers begin the attack's reconnaissance phase by listing all hosts and services and gathering data that would allow them to abuse authorized channels and further the intrusion.

After that, Octo Tempest investigates the infrastructure, listing all the resources and access points for server, backup, and cloud environments as well as code repositories.

The threat actor uses call forwarding, SIM-swapping, or social engineering once more to escalate privileges. They also start the target's account's self-service password reset process.

In this stage, the hackers use compromised accounts and show that they are aware of the company's protocols to gain the victim's trust. They approve requests for more permissions themselves if they have a manager's account.

Octo Tempest keeps searching for new credentials to broaden their reach as long as they have access. They automate the process of searching through code repositories for plaintext keys, secrets, and passwords using tools like Jercretz and TruffleHog.

The hackers also target security personnel's accounts, giving them the ability to disable security features and products while hiding their tracks.

Microsoft claims that Octo Tempest tries to blend in with the network by disabling change alerts and altering mailbox rules to remove emails that might make the victim suspect there has been a breach.

Prevention

- Block unknown scripts from running.
- Do not click on the malicious link.
- Do not share your credentials on fake URLs.
- Use anti-proxy techniques to avoid malicious IP sources.
- Disallow the RDP feature for unknown connections.
- Do not install unwanted applications from untrusted sources.
- 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.

Toyota Confirms Breach After Medusa Ransomware Threatens to Leak Data

Since the announcement of the Medusa ransomware attack on the company, Toyota Financial Services (TFS) has acknowledged that it discovered unauthorized access on several of its systems in Europe and Africa.

Toyota Motor Corporation's subsidiary Toyota Financial Services offers auto financing to its customers globally, operating in 90% of the markets where Toyota sells cars.

The TFS data leak was posted to the dark web by the Medusa ransomware group, who demanded $8,000,000 in exchange for the removal of data they claimed to have stolen from the Japanese company.

Toyota was given 10 days by the threat actors to respond, with the option to extend at an additional $10,000 per day.

Detection

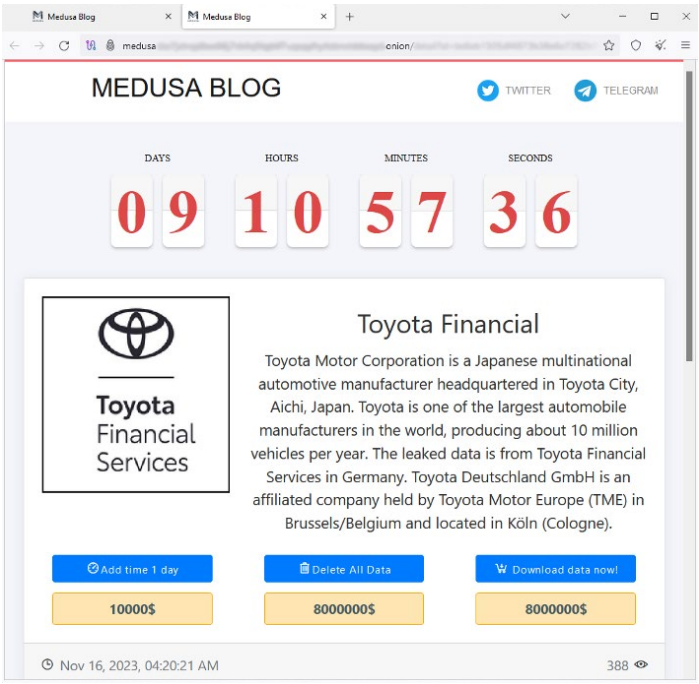
The threat actors claim to have exfiltrated files and threatened a data leak if a ransom is not paid, but Toyota Finance has not confirmed if data was stolen in the attack.

Financial documents, spreadsheets, purchase invoices, hashed account passwords, cleartext user IDs and passwords, agreements, passport scans, internal organization charts, financial performance reports, staff email addresses, and more were all made public by the hackers as examples of the breach.

Additionally, Medusa offers a.TXT file that contains the file tree structure of every piece of information they allege to have taken from Toyota's systems.

Most of the documents are written in German, suggesting that the hackers were able to gain access to the Central European systems that Toyota uses for business.

The spokesperson stated that most countries are currently in the process of bringing their systems back online. This information pertains to the status of the affected systems and when they are expected to resume regular operations.



Prevention

- Block unknown scripts from running.
- Do not click on the malicious link.
- Do not open any malicious .TXT files.
- 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 VPNs 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 a 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
Medusa Ransomware	https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-181a
Oktapus	https://www.microsoft.com/en-us/security/blog/2023/10/25/octo-tempest-crosses-boundaries-to-facilitate-extortion-encryption-and-destruction/
Grayling	https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/grayling-taiwan-cyber-attacks?web_view=true
Lazarus	https://unit42.paloaltonetworks.com/two-campaigns-by-north-korea-bad-actors-target-job-hunters/

TOP EXPLOITED VULNERABILITIES

Threat	Description	Reference Link
ManageEngine Applications Manager SingleSignOn Cross-Site Scripting Remote Code Execution Vulnerability CVE-2023-38333	Vulnerability allows remote attackers to execute arbitrary code on affected installations of ManageEngine Applications Manager. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file.	https://www.manageengine.com/products/applications_manager/security-updates/security-updates-cve-2023-38333.html
NETGEAR ProSAFE Network Management System clearAlertByIds SQL Injection Privilege Escalation Vulnerability CVE-2023-44449	Vulnerability allows remote attackers to escalate privileges on affected installations of NETGEAR ProSAFE Network Management System. The issue results from the lack of proper validation of a user-supplied string before using it to construct SQL queries.	https://vulmon.com/vulnerabilitydetails?qid=CVE-2023-44449
Adobe Acrobat Reader DC Font Parsing Uninitialized Variable Remote Code Execution Vulnerability CVE-2023-44365	Vulnerability allows remote attackers to execute arbitrary code on affected installations of Adobe Acrobat Reader DC. The issue results from the lack of proper initialization of memory prior to accessing it. An attacker can leverage this vulnerability to execute code in the context of the current process.	https://debricked.com/vulnerability-database/vulnerability/CVE-2023-44365
Adobe FrameMaker Publishing Server Authentication Bypass Vulnerability CVE-2023-44324	Vulnerability allows remote attackers to bypass authentication on affected installations of Adobe FrameMaker Publishing Server. The issue results from improper implementation of the authentication algorithm.	https://helpx.adobe.com/security/products/framemaker/apsb23-58.html
GStreamer AV1 Codec Parsing Heap-based Buffer Overflow Remote Code Execution Vulnerability CVE-2023-44429	Vulnerability allows remote attackers to execute arbitrary code on affected installations of GStreamer. Interaction with this library is required to exploit this vulnerability but attack vectors may vary depending on the implementation.	https://access.redhat.com/security/cve/cve-2023-44429
Microsoft Exchange TransportConfigContainer Deserialization of Untrusted Data Information Disclosure Vulnerability CVE-2023-36050	Vulnerability allows remote attackers to disclose sensitive information or relay NTLM credentials on affected installations of Microsoft Exchange. The issue results from the lack of proper validation of user-supplied data, which can result in deserialization of untrusted data.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36050
Microsoft Windows win32kfull UMPDDrvPlgBlt Use-After-Free Local Privilege Escalation Vulnerability CVE-2023-36804	Vulnerability allows local attackers to escalate privileges on affected installations of Microsoft Windows. An attacker must first obtain the ability to execute low-privileged code on the target system to exploit this vulnerability.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36804
NETGEAR CAX30 SSO Stack-based Buffer Overflow Remote Code Execution Vulnerability CVE-2023-44445	Vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of NETGEAR CAX30 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://vulmon.com/vulnerabilitydetails?qid=CVE-2023-44445
TP-Link TL-WR841N ated_tp Command Injection Remote Code Execution Vulnerability CVE-2023-39471	Vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of TP-Link TL-WR841N routers. The issue results from the lack of proper validation of a user-supplied string before using it to execute a system call.	https://vulmon.com/searchpage?q=CVE-2023-39471
Trend Micro Apex One Security Agent Link Following Local Privilege Escalation Vulnerability CVE-2023-47192	Vulnerability allows local attackers to escalate privileges on affected installations of Trend Micro Apex One Security Agent. The specific flaw exists within the Apex One NT RealTime Scan service. By creating a junction, an attacker can abuse the service to create arbitrary files.	https://success.trendmicro.com/dcx/s/solution/000295652?language=en_US
Kofax Power PDF File Parsing Use-After-Free Remote Code Execution Vulnerability CVE-2023-44436	Vulnerability allows remote attackers to execute arbitrary code on affected installations of Kofax Power PDF. 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-23-1608/
Ashlar-Vellum Lithium Uncontrolled Search Path Element Remote Code Execution Vulnerability CVE-2023-44440	Vulnerability allows remote attackers to execute arbitrary code on affected installations of Ashlar-Vellum Lithium. The process loads a library from an unsecured location. An attacker can leverage this vulnerability to execute code in the context of the current process.	https://www.zerodayinitiative.com/advisories/ZDI-23-1598/

TOP EXPLOITED VULNERABILITIES

Threat	Description	Reference Link
VMware vCenter Server Appliance DCE/RPC Protocol Out-Of-Bounds Write Remote Code Execution Vulnerability CVE-2023-34048	Vulnerability allows remote attackers to execute arbitrary code on affected installations of VMware vCenter Server Appliance. The issue results from the lack of proper validation of user-supplied data, which can result in a write before the start of an allocated buffer.	https://www.vmware.com/security/advisories/VMSA-2023-0023.html
Microsoft Azure US Accelarators Synapse SAS Token Incorrect Permission Assignment Authentication Bypass Vulnerability	Vulnerability allows remote attackers to bypass authentication on Microsoft Azure. Authentication is not required to exploit this vulnerability. The specific flaw exists within the permissions granted to an SAS token.	https://vulners.com/zdi/ZDI-23-1588
SolarWinds Network Configuration Manager ExportConfigs Directory Traversal Remote Code Execution Vulnerability CVE-2023-33226	Vulnerability allows remote attackers to execute arbitrary code on affected installations of SolarWinds Network Configuration Manager. The issue results from the lack of proper validation of a user-supplied path prior to using it in file operations.	https://www.solarwinds.com/trust-center/security-advisories/cve-2023-33226
(0Day) Microsoft Exchange ChainedSerializationBinder Deserialization of Untrusted Data Remote Code Execution Vulnerability	Vulnerability allows remote attackers to execute arbitrary code on affected installations of Microsoft Exchange. The issue results from the lack of proper validation of user-supplied data, which can result in deserialization of untrusted data.	https://securityaffairs.com/153599/hacking/microsoft-exchange-zero-day-flaws.html#:~:text=ZDI%2D23%2D1578%20%E2%80%93%20Microsoft,required%20to%20exploit%20this%20vulnerability.
GIMP PSP File Parsing Integer Overflow Remote Code Execution Vulnerability CVE-2023-44443	Vulnerability allows remote attackers to execute arbitrary code on affected installations of GIMP. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file.	https://access.redhat.com/security/cve/cve-2023-44443
Adobe RoboHelp Server UpdateCommandStream XML External Entity Processing Information Disclosure Vulnerability CVE-2023-22274	Vulnerability allows remote attackers to disclose sensitive information on affected installations of Adobe RoboHelp Server. Due to the improper restriction of XML External Entity (XXE) references, a crafted document specifying a URI causes the XML parser to access the URI and embed the contents back into the XML document for further processing.	https://debricked.com/vulnerability-database/vulnerability/CVE-2023-22274

Security Bulletin

1. Kinsing Hackers Exploit Apache ActiveMQ Vulnerability to Deploy Linux Rootkits

Kinsing is a Linux malware that has a track record of focusing on improperly configured, containerized setups for cryptocurrency mining. The threat actors often use compromised server resources to make money illegally.

In order to breach target networks and distribute cryptocurrency miners, the group is also renowned for swiftly changing its strategies to take advantage of recently discovered vulnerabilities in web applications. Aqua revealed earlier this month that the threat actor was attempting to get access to cloud environments by taking advantage of a Linux privilege escalation vulnerability known as Looney Tunables.

The most recent campaign involves the active exploitation of a serious vulnerability in Apache ActiveMQ, CVE-2023-46604 (CVSS score: 10.0), which allows remote code execution and allows an adversary to download and install the Kinsing malware.

Next, further payloads are retrieved from an actor-controlled domain, and concurrent actions are taken to stop rival Bitcoin miners that are already operating on the compromised server.

“Kinsing doubles down on its persistence and compromise by loading its rootkit in /etc/ld.so.preload, which completes a full system compromise,” Girnus stated.

Organizations using impacted versions of Apache ActiveMQ are advised to update to a patched version as soon as feasible in order to reduce potential dangers, given the ongoing exploitation of the bug.

The revelation coincides with a warning from the AhnLab Security Emergency Response Centre (ASEC) regarding cyberattacks that aim to compromise Apache web servers, which are susceptible to a crypto jacking campaign that uses Gh0st RAT or Cobalt Strike to send a Bitcoin miner.

2. DarkGate and PikaBot Malware Resurrect QakBot’s Tactics in New Phishing Attacks

Phishing attempts that distribute malware families like DarkGate and PikaBot employ the same strategies that were previously employed in attacks with the defunct QakBot trojan.

In a study posted with The Hacker News, Cofense stated, "These include URLs with unique patterns that limit user access, hijacked email threads as the initial infection, and an infection chain nearly identical to what we have seen with QakBot delivery. The malware families used also follow suit to what we would expect QakBot affiliates to use."

Earlier in August, QakBot—also known as QBot and Pinkslipbot—was taken offline as part of Operation Duck Hunt, a concerted law enforcement operation.

It is not unexpected that DarkGate and PikaBot are being used in these campaigns; cybercriminals find them both appealing because they can both serve as channels for delivering more payloads to compromised hosts.

Zscaler first drew attention to PikaBot's similarities with QakBot in May 2023 when analyzing the malware, pointing to "distribution methods, campaigns, and malware behaviors."

On the other hand, DarkGate uses sophisticated methods to avoid being discovered by antivirus programs. It also has the ability to record keystrokes, run PowerShell, and set up a reverse shell that lets its operators take control of an infected host from a distance.

"The connection is bidirectional, meaning the attackers can send commands and receive responses in real-time, enabling them to navigate the victim's system, exfiltrate data, or perform other malicious actions," Sekoia stated in a fresh technical report on the spyware.

The high-volume phishing campaign targets a variety of industries, according to Cofense's study of it. The attack chains spread a booby-trapped URL that points to a ZIP archive through hacked email threads.

A JavaScript dropper found in the ZIP file downloads and launches the PikaBot or DarkGate malware by connecting to a second URL.

A significant variation of the assaults has been reported that uses Excel add-in (XLL) files to deliver the payloads instead of JavaScript droppers.

"A successful DarkGate or PikaBot infection could lead to the delivery of advanced crypto mining software, reconnaissance tools, ransomware, or any other malicious file the threat actors wish to install on a victim's machine," Cofense stated.

3. Kansas Courts Confirm Data Theft, Ransom Demand After Cyberattack

In a ransomware attack that has impeded access to records for more than five weeks, cybercriminals broke into the Kansas court system, stole confidential information, and threatened to post it on the dark web, officials said.

Following the state's Judicial Branch's declaration on October 12 that it was stopping electronic filings, computer security experts suspected something, and the announcement of a "sophisticated foreign cyberattack" confirmed their suspicions. State officials have only provided a vague description of the occurrence up until now, calling it a "security incident."

The Judicial Branch said in a statement that the state informed authorities and cut off external access to its court information system as soon as it became aware of the incident. This interrupted all but one county's regular operations, as well as those of the state's appellate courts. The most populated county in the state, Johnson County, has its own computer systems and hasn't migrated to the new internet system yet.

In recent weeks many attorneys have been forced to file motions the old-fashioned way — on paper.

The statement declared, "This attack on the Kansas legal system is evil and criminal. We are deeply sorry that these cybercriminals will cause harm to Kansans today."

According to a preliminary assessment, the stolen material contains potentially sensitive information such as district court case records on appeal. Those impacted will be informed after a thorough study is finished, the statement added.

No information has yet been published on any ransomware group leak site, according to analyst Allan Liska of the cybersecurity company Recorded Future.

A spokesman for the Judicial Branch, Lisa Taylor, said that the statement speaks for itself and declined to respond to inquiries about whether the state paid a ransom nor the identity of the organization that carried out the attack.

According to analyst Brett Callow of the cybersecurity company Emsisoft, data typically starts to surface online in a matter of weeks if firms choose not to pay a ransom. He claimed that although victims who pay receive a "pinkie promise" that their stolen data will be deleted, some are actually extorted twice.

Only a portion of the court documents' accessibility has been restored in the weeks following the attack in Kansas. The Kansas Judicial

Centre in Topeka is home to a public access service center with ten computer terminals.

The Judicial Branch stated that in order to "buttress our systems to guard against future attacks," it would take several weeks to resume regular activities, including electronic filing.

According to state law, a risk assessment of the state's judicial system that was released last year is "permanently confidential." However, shortcomings were found in two recent audits of other state agencies.

"Agency leaders don't know or sufficiently prioritize their IT security responsibilities," said the most current report, which was published in July.

4. Windows Hello Fingerprint Authentication Can Be Bypassed on Popular Laptops

Researchers have discovered a number of vulnerabilities in Windows Hello fingerprint authentication on laptops running Microsoft Surface Pro X, Lenovo ThinkPad T14, and Dell Inspiron 15.

The researchers were tasked with assessing the security of the top three laptop-integrated fingerprint sensors by Microsoft's Offensive Research and Security Engineering (MORSE). They discovered flaws that let them completely get around Windows Hello authentication on each of the three. We kindly point you in the direction of the Black wing researcher's blog, A TOUCH OF PWN - PART I, if you would like to read the complete technical specifics.

Above all, it's critical to understand that the target laptop must have fingerprint authentication enabled in order for these vulnerabilities to be exploited. What kind of calamity may occur if it weren't the case?

All three of the sensors that the researchers examined belonged to the "match on chip" category. This implies that the biometric credentials—in this example, the fingerprints—are stored on a different chip, making hacking nearly impossible.

Microsoft's Secure Device Connection Protocol (SDCP) is used to provide a secure channel for communication between the laptop and the sensor.

SDCP aims to answer three questions about the sensor:

I. How can the laptop be certain it's talking to a trusted sensor and not a malicious one?

II. How can the laptop be certain the sensor hasn't been compromised?

III. How is the raw input from the sensor protected?

1. The input has to be authenticated.
2. The input is fresh and can't be re-playable.

So, what could go wrong?

The communication between the laptops and the sensor might potentially be faked by the researchers. By employing a USB device that masqueraded as a sensor and sent a signal indicating that an authorized person had logged in, they were able to mislead the laptops.

Because the device manufacturers did not fully utilize SDCP, the bypasses are possible:

I. The ELAN sensor that is frequently found in Surface and Dell laptops does not support SDCP and sends security identifiers in clear text.

II. Synaptic sensors, which are utilized by Lenovo and Dell, employed a faulty proprietary Transport Layer Security (TLS) stack to safeguard USB traffic and disabled SDCP by default.

III. Because the Goodix sensors are compatible with Linux and Windows, which do not support SDCP, they might be used instead of the Lenovo and Dell sensors. To tell the sensor which database to use during sensor initialization, the host driver transmits an unauthenticated configuration packet to the sensor.

The researchers' advice to the makers is very clear: while SDCP is a strong protocol, it is useless if it isn't enabled or if other weak links in your system may be used to get around it.

It is in no way implied that other manufacturers have performed better because only three manufacturers were specifically identified. The researchers simply never got around to testing the others.

You should disable fingerprint authentication from your laptop if you, as the user, are concerned about someone utilizing a USB device to access it.

1. In the Windows search box, type, and search [Sign-in options], then select [Open].
2. To remove the fingerprint sign-in option, select [Fingerprint recognition (Windows Hello)] and then click [Remove].

We can't trust that this is a secure authentication technique until the manufacturers have addressed the flaws in their systems.

5. LummaC2 Malware Deploys New Trigonometry-Based Anti-Sandbox Technique

The stealer malware LummaC2 (also known as Lumma Stealer) now has an anti-sandbox method that uses trigonometry, a mathematical concept, to avoid detection and steal important data from compromised hosts.

According to a technical report published with The Hacker News by Outpost24 security researcher Alberto Marin, the strategy is intended to "delay detonation of the sample until human mouse activity is detected."

Since December 2022, LummaC2, which is coded in the C programming language, has been offered for sale in dark web forums. Since then, the virus has been updated repeatedly, making it more difficult to study through control flow flattening and even enabling it to deliver more payloads.

In addition to requiring use of a crypter as an extra concealing method, LummaC2 v4.0 demands users to keep the program from being leaked in its raw form.

The use of trigonometry to identify human behavior on the compromised endpoint is another noteworthy update.

"This technique takes into consideration different positions of the cursor in a short interval to detect human activity, effectively preventing detonation in most analysis systems that do not emulate mouse movements realistically," Marin stated.

In order to accomplish this, following a predetermined 50 millisecond sleep interval, it retrieves the current cursor location five times, then verifies that each captured position differs from the previous one. Until the cursor positions in every subsequent iteration diverge, the process is repeated again.

LummaC2 treats the five cursor positions (P0, P1, P2, P3, and P4) as Euclidean vectors after they all satisfy the necessary conditions. It then determines the angle created between two successive vectors (P01-P12, P12-P23, and P23-P34).

"If all the calculated angles are lower than 45º, then LummaC2 v4.0 considers it has detected 'human' mouse behavior and continues with its execution," Marin stated.

"However, if any of the calculated angles is bigger than 45º, the malware will start the process all over again by ensuring there is mouse movement in a 300-millisecond period and capturing again 5 new cursor positions to process."

The advancement coincides with the introduction of new strains of remote access Trojans and information stealers, like Sayler RAT, BbyStealer, Trap Stealer, Predator AI, Epsilon Stealer, and Nova Sentinel, which are intended to retrieve a variety of sensitive data from infiltrated systems.

Aside from integrating a ChatGPT API to "make the tool easier to use," Predator AI is a noteworthy project that is actively developed. It can be used to attack numerous well-known cloud services, including AWS, PayPal, Razor pay, and Twilio, as Sentinel One reported earlier this month.

"The malware-as-a-service (MaaS) model, and its readily available scheme, remains to be the preferred method for emerging threat actors to carry out complex and lucrative cyberattacks," Marín stated.

"Information theft is a significant focus within the realm of MaaS and represents a considerable threat that can lead to substantial financial losses for both organizations and individuals."

REFERENCE LINKS

- https://thehackernews.com/2023/11/kinsing-hackers-exploit-apache-activemq.html
- https://thehackernews.com/2023/11/darkgate-and-pikabot-malware-resurrect.html
- https://www.malwarebytes.com/blog/news/2023/11/windows-hello-fingerprint-authentication-can-be-bypassed-on-popular-laptops
- https://apnews.com/article/kansas-courts-cyberattack-hack-network-offline-097a11cfa9de552ec5a9ea49b500d3d6
- https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/grayling-taiwan-cyber-attacks?web_view=true
- https://thehackernews.com/2023/10/researchers-uncover-grayling-apts.html
- https://www.microsoft.com/en-us/security/blog/2023/10/25/octo-tempest-crosses-boundaries-to-facilitate-extortion-encryption-and-destruction/
- https://www.healthcareinfosecurity.com/meet-octo-tempest-most-dangerous-financial-hackers-a-23397?&web_view=true
- https://www.bleepingcomputer.com/news/security/new-looney-tunables-linux-bug-gives-root-on-major-distros/
- https://www.bleepingcomputer.com/news/security/welltok-data-breach-exposes-data-of-85-million-us-patients/
- https://www.cybersecuritydive.com/news/file-transfer-services-under-attack/699722/?&web_view=true
- https://www.cybersecuritydive.com/news/smbs-legitimate-tool-attacks/700410/?&web_view=true

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**.

SDG

75 North Water Street
Norwalk, CT 06854

203.866.8886

sdgc.com