Cyber Threat Advisory

APRIL 2024

Contents

Monthly Highlights - April

1. **Research Shows IT and Construction Sectors Hardest Hit by Ransomware** – New research has uncovered the significant impact of ransomware attacks on the IT and construction sectors, revealing that these industries accounted for nearly half of all incidents in 2023. The findings, outlined in a recent report by Ontinue's Advanced Threat Operations (ATO) team, are based on a thorough analysis of data collected from 600,000 endpoints.

   The report indicates that ransomware has become a major challenge for organizations across various industries, with the IT and construction sectors facing particularly high risks. The increased targeting of these sectors is attributed to their expansive attack surfaces and the potential profitability of their operations.

   Furthermore, the report highlights LockBit as the most active ransomware group, known for its tactic of threatening to leak stolen data if ransom demands are not met. Alongside ransomware, the report also points out the growing threat of QR phishing, or "Quishing," which targets organizations across different industries. This method is noted for its simplicity and effectiveness in evading traditional security measures, posing a significant challenge for cybersecurity experts.

   In addition to specific threats, the report underscores broader trends influencing the cybersecurity landscape. These include the rising sophistication of ransomware tactics, such as the use of double-extortion strategies, as well as concerns regarding Internet of Things (IoT) security and the exploitation of connected devices for malicious purposes.

2. **Steel Giant ThyssenKrupp Confirms Cyberattack on Automotive Division** – Steel giant ThyssenKrupp has confirmed a recent cyber breach in its automotive division, leading to the shutdown of IT systems as part of the response and containment efforts. The company plays a critical role in the global supply chain, providing steel for a wide range of industries, including machinery, automotive, elevator and escalator, industrial engineering, renewable energy, and construction.

   The recent cyberattack specifically impacted ThyssenKrupp's automotive body production division. The IT security team at Automotive Body Solutions detected the incident early and collaborated with the ThyssenKrupp Group's IT security team to contain the threat. As a result, various security measures were implemented, and certain applications and systems were temporarily taken offline.

   ThyssenKrupp has emphasized that the cyberattack was contained within the automotive division, and no other business units or segments were affected. The company assured that the situation is under control, and efforts are underway to gradually resume normal operations.

   According to reports, ThyssenKrupp's Saarland-based plant—which employs over a thousand specialists and is involved in steel production, processing, and research and development—was directly impacted by the attack. This facility collaborates with industry partners, research institutions, and universities.

   Given its significant role in the global economy, ThyssenKrupp has previously been targeted by hackers multiple times, including in 2022, 2020, 2016, and 2013. These attacks have mostly been aimed at espionage and operational disruption.

3. **A Leaky Database Spilled 2FA Codes for the World's Tech Giants** – A technology company responsible for routing millions of SMS text messages worldwide has secured an exposed database that was inadvertently leaking one-time security codes, potentially granting access to users' Facebook, Google, and TikTok accounts.

   YX International, an Asian technology and internet company, specializes in manufacturing cellular networking equipment and providing SMS text message routing services. SMS routing ensures that time-sensitive text messages reach their intended recipients across various regional cell networks and providers; this includes users receiving SMS security codes or links for logging into online services.

   Unfortunately, the technology company had left one of its internal databases accessible on the internet without a password. This oversight allowed anyone with knowledge of the database's public IP address to access the sensitive data using just a web browser.

   A well-known security researcher, skilled in identifying inadvertently exposed datasets on the internet, discovered the unprotected database. Since it was unclear who owned the database or how to report the leak, the researcher shared details of the exposed database with an American online newspaper to help identify the owner and report the security lapse.

   The exposed database contained the contents of text messages sent to users, including one-time passcodes and password reset links for major tech and online companies like Facebook, WhatsApp, Google, and TikTok.

   Two-factor authentication (2FA) provides added protection against online account hijacking by sending an additional code to a trusted device, such as a phone. However, codes sent via SMS are not as secure as those generated by an app, as SMS messages can be intercepted or exposed, as seen in this case.

   The exposed database also contained sets of internal email addresses and corresponding passwords associated with YX International. The American online newspaper alerted the company to the exposed database, which was taken offline shortly after. A representative for YX International, who chose not to disclose their name, responded promptly, stating that the company had "sealed this vulnerability."

4. **Law Firm Reports Data Breach Affecting More Than 325,000 People** – Houser LLP, a U.S. law firm specializing in serving prominent financial institutions, disclosed that a system breach discovered in May 2023 exposed the personal data, potentially including sensitive information like credit card numbers, of over 325,000 individuals.

   In a regulatory filing posted by Maine's attorney general, the company stated that certain files were encrypted during the incident and were "copied and taken from the network." The compromised data included names and at least one of the following: Social Security number, driver's license number, individual tax identification number, financial account information, and/or medical information. Houser also filed a notification with California's attorney general.

   An undisclosed third-party company later determined that there was "unauthorized access" to the law firm network between May 7 and May 9. The regulatory filing indicated that Houser had contact with the attackers shortly afterward, although it did not specify the nature of the communication. Recorded Future News has contacted the firm for further details.

In June 2023, "the unauthorized actor informed Houser that they deleted copies of any stolen data and would not distribute any stolen files," the firm stated. Following this notification, the law firm began informing its clients of the investigation and findings and offered to send letters to potentially impacted individuals on behalf of these clients.

Houser, which has around a dozen offices nationwide and aims to serve clients in "every major financial center," specializes in litigation management, commercial and real estate law, class action defenses, and regulatory compliance. The firm's partners highlight their work for institutions such as Citibank, Deutsche Bank, and HSBC.

In its correspondence to potentially affected individuals, the firm provided extensive details about the cybersecurity measures it implemented after the breach. These measures include deploying RocketCyber, an endpoint detection and response tool; implementing multi-factor authentication for Outlook 365, Net Extender VPN tunnel, and remote desktop connection; as well as adding ransomware detection software, phishing simulation software, and conducting vulnerability assessments and penetration testing.

5. **UK Defence Secretary Jet Hit by an Electronic Warfare Attack in Poland** – Defence Secretary Grant Shapps flew aboard an RAF Dassault Falcon 900 jet from Poland back to the UK after visiting British troops participating in Steadfast Defender. During the flight, the UK defence chief reaffirmed his country's full support for Ukraine.

   Onboard the jet, a British newspaper's defence editor reported that GPS and communications systems were disabled by a jamming attack believed to be orchestrated by Russia. RAF pilots confirmed that these systems were blocked for nearly 30 minutes while flying near Kaliningrad, a Russian exclave neighbouring Poland.

   British officials stated that the incident was not a targeted attack on Shapps' plane but rather part of a broader Russian interference campaign affecting satellite communications and signals, which can impact all aircraft and GPS devices.

   An article in the British newspaper mentioned, "British newspaper defence editor was onboard the RAF Dassault Falcon 900 at the time." It is also noted that Shapps, who is a qualified pilot, was assured that the electronic warfare attack did not compromise the aircraft's safety.

   The Defence Secretary was returning from Poland's Szymany airport after visiting British troops involved in Steadfast Defender, the largest NATO war games since the end of the Cold War. Steadfast Defender 2024 is an extensive military exercise designed to test the alliance's readiness and ability to defend itself across various domains. The exercise, which runs from January 22nd to May 31st, 2024, includes operations in land, air, sea, cyber, and space domains, with a focus on cyberattacks on avionics systems.

6. **French Unemployment Agency Data Breach Impacts 43 Million People** – The French unemployment agency France Travail has issued a warning about a breach in its systems, potentially leading to the leakage or exploitation of personal details for an estimated 43 million individuals. This governmental agency is responsible for registering unemployed individuals, providing financial aid, and assisting them in finding jobs.

   The agency disclosed yesterday that hackers stole details from job seekers registered with the agency over the last 20 years in a cyberattack between February 6 and March 5. Data from individuals with job candidate profiles was also exposed.

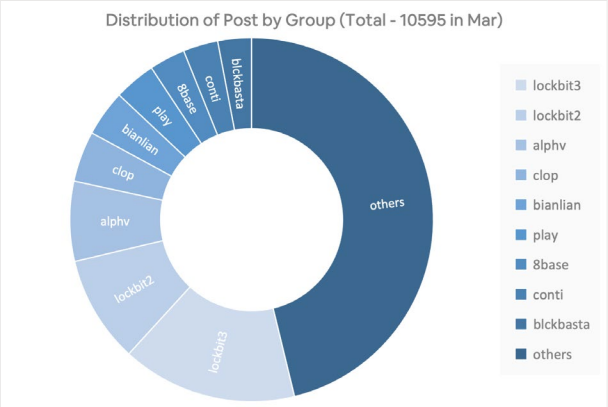
   Affected individuals will receive a notification from the agency regarding personal data violation as a result of the incident, according to a notice on France's portal for assisting victims of cyberattacks. The French governmental agency has informed the country's data protection agency, the National Commission of Informatique and Liberties (CNIL), which stated that up to 43 million people may be impacted.

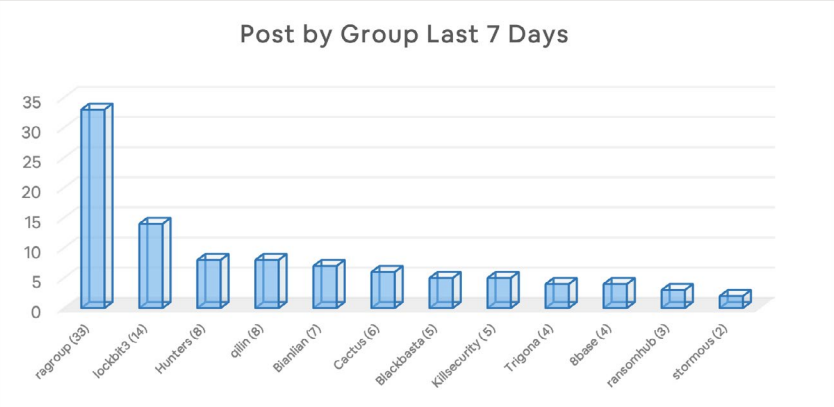
   The types of data exposed in this attack include full names, dates of birth, places of birth, social security numbers (NIR), France Travail identifiers, email addresses, postal addresses, and phone numbers. Therefore, the agency recommends that potentially impacted people be particularly vigilant with emails, phone calls, and SMS they receive.

   France Travail clarified that the data breach incident does not impact people's bank details or account passwords. However, CNIL warns that cybercriminals may use the available information to correlate with missing data points from other breaches. Individuals impacted by the data breach incident at the French governmental agency can file a complaint with the Paris prosecutor's office to help with the investigation.

   Last August, France Travail experienced a massive data breach affecting approximately 10 million individuals. This incident was indirectly attributed to the Clop ransomware group breaching the agency's systems by exploiting a zero-day vulnerability in the MOVEit Transfer software tool. The current cyberattack on the agency sets a new record in France for affecting the largest number of individuals, more than the 33 million people impacted by the Viamedis and Almerys breach in February.

Ransomware Tracker





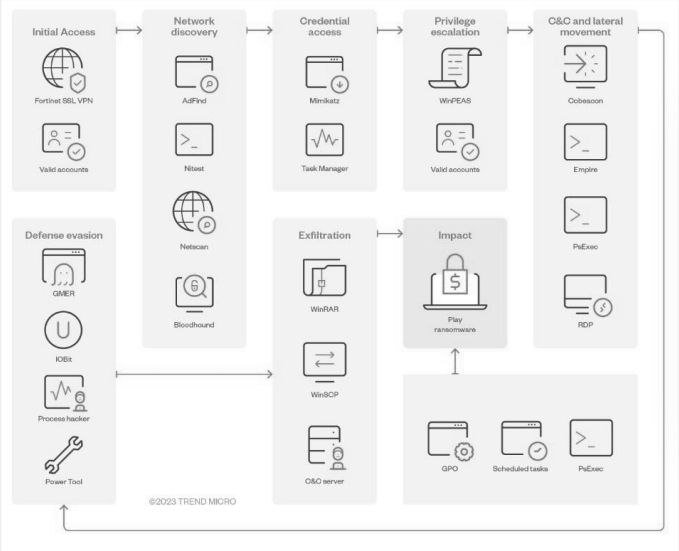
Unveiling the Threat: The Rise of Play Ransomware

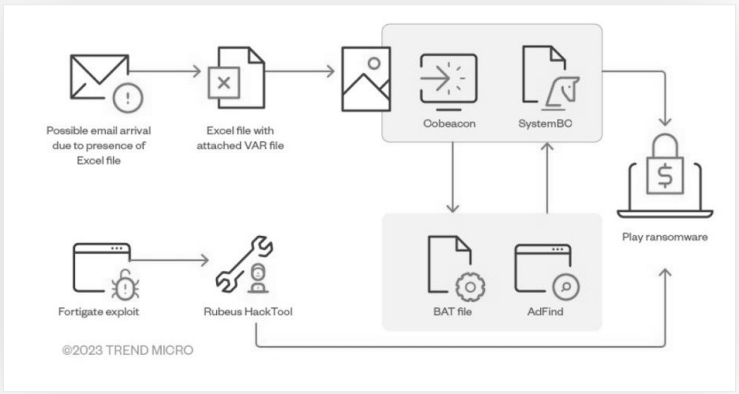
Executive Summary:

- Play ransomware group has targeted numerous businesses and critical infrastructure across North America, South America, and Europe since June 2022.
- The group employs a double-extortion model, encrypting data after exfiltration and then demanding ransom payments.
- Initial access is gained by abusing valid accounts, exploiting public-facing applications, and utilizing external-facing services like RDP and VPN.
- The ransomware actors use various tools for discovery, defense evasion, lateral movement, execution, exfiltration, and encryption.
- Impact includes data encryption, financial theft through a double-extortion model, and threat of data exposure if ransom demands are not met.

Technical Details:

- The Play ransomware group gains entry by abusing valid accounts, exploiting public-facing applications, and utilizing external-facing services like RDP and VPN.
- Exploited vulnerabilities include known FortiOS and Microsoft Exchange vulnerabilities.
- Play ransomware actors employ tools like AdFind for Active Directory queries and Grixba for network information enumeration.
- To evade defenses, they use GMER, IOBit, and PowerTool to disable anti-virus software and remove log files.
- PowerShell scripts are used to target Microsoft Defender.
- Command and control (C2) applications like Cobalt Strike and SystemBC, along with tools like PsExec, aid in lateral movement and file execution.
- Credential dumping with Mimikatz and enumeration of vulnerabilities with WinPEAS are common tactics.
- Group Policy Objects are utilized for distributing executables.
- Compromised data is split into segments and compressed using WinRAR for exfiltration.
- Files are encrypted with AES-RSA hybrid encryption, adding a .play extension, and a ransom note is placed in the file directory.
- Play ransomware employs a double-extortion model, encrypting systems after exfiltrating data.
- Ransom payments are demanded in cryptocurrency, with threats of data exposure if demands are not met.





Detection:

- Implement network monitoring tools to detect abnormal activity and potential ransomware traversal.
- Endpoint detection and response (EDR) tools can help in detecting lateral connections.
- Regularly review domain controllers, servers, workstations, and active directories for new or unrecognized accounts.

Indicators of Compromise

Hashes (SHA256)	Description
453257c3494addafb39cb6815862403e827947a1e7737eb8168cd10522465deb	Play ransomware custom data gathering tool
47c7cee3d76106279c4c28ad1de3c833c1ba0a2ec56b0150586c7e8480ccae57	Play ransomware encryptor
75404543de25513b376f097ceb383e8efb9c9b95da8945fd4aa37c7b2f226212	SystemBC malware EXE
7a42f96599df8090cf89d6e3ce4316d24c6c00e499c8557a2e09d61c00c11986	SystemBC malware DLL
7a6df63d883bbccb315986c2cfb76570335abf84fafbefce047d126b32234af8	Play ransomware binary
7dea671be77a2ca5772b86cf8831b02bff0567bce6a3ae023825aa40354f8aca	SystemBC malware DLL
c59f3c8d61d940b56436c14bc148c1fe98862921b8f7bad97fbc96b31d71193c	Play network scanner
e652051fe47d784f6f85dc00adca1c15a8c7a40f1e5772e6a95281d8bf3d5c74	Play ransomware binary
e8d5ad0bf292c42a9185bb1251c7e763d16614c180071b01da742972999b95da	Play ransomware binary

Prevention:

- Apply timely patching of all operating systems, software, and firmware.
- Segment networks to prevent ransomware spread and restrict adversary lateral movement.
- Enable real-time detection for antivirus software on all hosts and regularly update them.
- Implement multifactor authentication for critical services and accounts.
- Maintain offline backups of data and regularly test backup and restoration procedures.

Remediation:

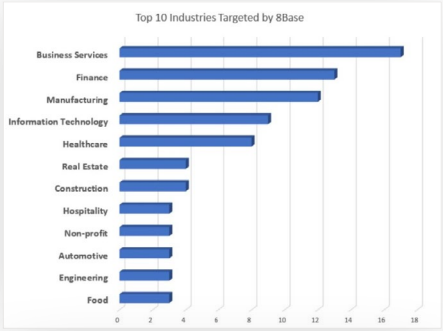
- Test and validate security controls against MITRE ATT&CK techniques employed by Play ransomware.
- Tune security programs, including people, processes, and technologies, based on comprehensive performance data.
- In the event of a ransomware attack, promptly isolate infected systems from the network to prevent further spread of the ransomware.
- Maintain comprehensive backup and recovery procedures. This is crucial for restoring encrypted files and minimizing downtime.

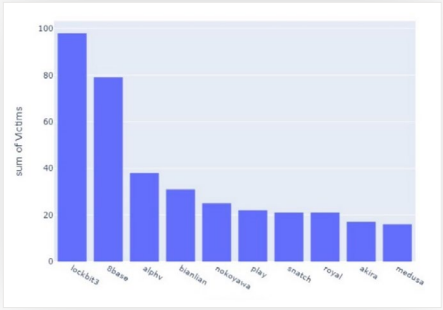
- Have a well-documented incident response plan in place to ensure a coordinated and effective response to ransomware incidents and facilitate timely communication with stakeholders and law enforcement agencies.
- Conduct post-incident analysis to identify weaknesses in your security posture and implement measures to prevent future ransomware incidents.

Decoding 8Base: A Deep Dive into a Sophisticated APT Group and Their Exploits

Executive Summary

- 8Base emerged as a ransomware group in March 2022, showing a notable surge in activity in June 2023.
- Presenting themselves as "simple pen testers," 8Base operates a leak site, utilizing communication styles reminiscent of RansomHouse.
- Similarities between 8Base and RansomHouse raise questions about potential affiliations or imitation.
- 8Base's activities remain shrouded in mystery, with speculation regarding its origins and operational methodologies.
- Whether 8Base is an offshoot of RansomHouse or operates independently remains unclear. However, its utilization of Phobos ransomware underscores the group's adaptability and resourcefulness.





Technical Details:

- Origins and Communication: 8Base's communication style mirrors that of RansomHouse, indicating a potential connection. The group's activities surged in June 2023, attracting attention across various sectors.
- Ransomware Variants: While 8Base's ransomware variants were initially elusive, investigations revealed the use of Phobos ransomware, version 2.9.1. The ransom notes bore similarities to both RansomHouse and Phobos, suggesting a diverse approach to ransomware deployment.
- Associations and Tactics: 8Base exhibits associations with SystemBC, a proxy and remote administration tool used to encrypt and conceal command and control traffic. Its tactics include network share discovery, token impersonation, and tool obfuscation.

Tactic	Technique	Description
TA0003 Persistence	T1547.001 Registry Run Keys / Startup Folder	Adds the following: %AppData%\Local\{malware} %ProgramData%\Microsoft\Windows\Start Menu\Programs\Startup\{malware} %AppData%\Roaming\Microsoft\Start Menu\Programs\Startup\{malware}
TA0007 Discovery	T1135 Network Share Discovery	Uses WNetEnumResource() to crawl network resources
TA0004 Privilege Escalation	T1134.001 Token Impersonation/Theft	Uses DuplicateToken() to adjusts token privileges
TA0005 Defense Evasion	T1562.001 Disable or Modify Tools	Terminates a long list of processes, which are a mix of commonly used applications (example: MS Office applications) and security software.
TA0005 Defense Evasion	T1027.002 Obfuscated File or Information: Software Packing	SmokeLoader unpacks and loads Phobos to memory
TA0040 Impact	T1490 Inhibit System Recovery	Runs: wmic shadowcopy delete wbadmin delete catalog -quiet vssadmin delete shadows /all /quiet bcdedit /set {default} recoveryenabled no bcdedit /set {default} bootstatuspolicy ignoreallfailures
TA0040 Impact	T1486 Data Encrypted for Impact	Uses AES to Encrypt Files

Detection:

- Monitor changes to Registry Run Keys and Startup Folders.
- Implement real-time monitoring solutions for unauthorized modifications.
- Monitor network traffic for anomalous behavior.
- Use intrusion detection systems (IDS) and network traffic analysis tools.
- Track changes to user privileges and suspicious usage patterns.
- Utilize user behavior analytics (UBA) and privilege access management (PAM) solutions.

Indicator	Type	Context
518544e56e8ccee401ffa-1b0a01a10ce23e49ec21ec441c6c7c3951b01c1b19c	SHA-256	8Base Ransomware (Phobos variant)
5BA74A5693F4810A8EB9B9EEB1D69D943CF5BBC-46F319A32802C23C7654194B0	SHA-256	8Base ransom note (RansomHouse variant)
20110FF550A2290C5992A5BB6BB44056	MD5	8Base ransom note (RansomHouse variant)
3D2B088A397E9C7E9AD130E178F885FEEBD9688B	SHA-1	8Base ransom note (RansomHouse variant)
e142f4e8eb3fb4323fb377138f53db66e3e6ec9e82930f4b23dd91a5f7bd45d0	SHA-256	8Base ransomware (Phobos variant)
5d0f447f4ccc89d7d79c0565372195240cdfa25f	SHA-1	8Base ransomware (Phobos variant)
9769c181ecef69544bbb2f974b8c0e10	MD5	8Base ransomware (Phobos variant)
C6BD5B8E14551EB899BBE4DECB6942581D28B2A42B159146BBC28316E6E14A64	SHA-256	8Base ransomware (Phobos variant)
518544E56E8CCEE401FFA-1B0A01A10CE23E49EC21EC441C6C7C3951B01C1B19C	SHA-256	8Base ransomware (Phobos variant)
AFDDEC37CDC1D196A1136E2252E925C0D-CFE587963069D78775E0F174AE9CFE3	SHA-256	8Base ransomware (Phobos variant)
wlaexfpxrs[.]org	Data POST to URL	8Base ransomware referred domain (Phobos variant)
admhexlogs25[.]xyz	Data GET request to URL	8Base ransomware referred domain
admlogs25[.]xyz	Data GET request to URL	8Base ransomware referred domain
admlog2[.]xyz	Data GET request to URL	8Base ransomware referred domain
dnm777[.]xyz	Data GET request to URL	8Base ransomware referred domain
serverlogs37[.]xyz	Data POST to URL	8Base ransomware referred domain
9f1a.exe	File Name	8Base ransomware dropped file
d6ff.exe	File Name	8Base ransomware dropped file
3c1e.exe	File Name	8Base ransomware dropped file

Indicator	Type	Context
dexblog[.]xyz	Data GET request to URL	8Base ransomware referred domain
blogstat355[.]xyz	Data GET request to URL	8Base ransomware referred domain
blogstatserv25[.]xyz	Data GET request to URL	8Base ransomware referred domain

Prevention:

- Employ endpoint protection solutions capable of detecting and blocking known malware variants to further enhance defense mechanisms.
- Use endpoint detection and response (EDR) solutions with behavior-based analysis.
- Implement robust data backup and recovery mechanisms.
- Enforce strict access controls and least privilege principles.
- Implement strong email security measures to prevent spear phishing attacks. This is crucial in preventing initial access by threat actors.
- Regularly update and patch software vulnerabilities, especially those exploited in zero-day attacks like CVE-2024-21412, to mitigate the risk of exploitation.

Remediation:

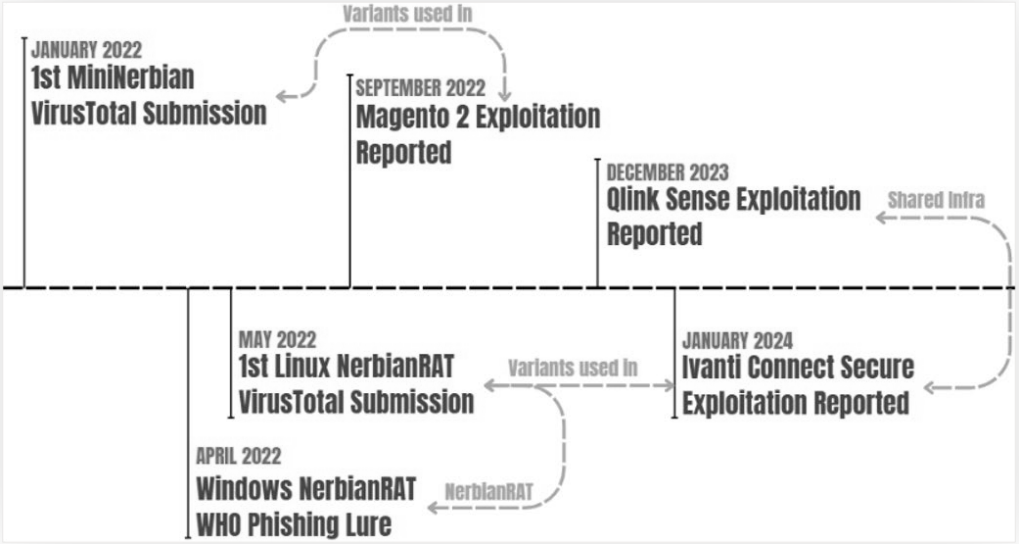
- In the event of an attack, immediate isolation of affected systems and networks is essential to prevent further spread of the malware.
- Prevention measures encompass phishing awareness training, network segmentation, and endpoint protection.
- Endpoint detection solutions can offer robust defense against ransomware threats, emphasizing proactive measures.
- Incident response teams should conduct thorough forensic analysis to identify the extent of the compromise and remove any traces of the malware from infected systems.
- Close monitoring of network traffic and endpoint activities can help ensure that the threat actor has been fully eradicated from the environment.
- Implementing security best practices and conducting regular security assessments can help strengthen defences against future attacks by 8Base and similar APT groups.

Magnet Goblin Hackers Use One-Day Flaws to Drop Custom Linux Malware

- Magnet Goblin is a financially motivated hacking group that compromises public-facing servers and infects Windows and Linux systems with custom malware using a variety of one-day vulnerabilities.
- One-day flaws are vulnerabilities that have been made public and for which a patch has been made available. Threat actors need to act fast to take advantage of these vulnerabilities before a target has a chance to apply security updates.
- Even though exploits are typically not made public right away when a vulnerability is discovered, some vulnerabilities are extremely easy to take advantage of. Reverse-engineering the patch may also make the underlying issue and its exploitable vulnerabilities visible.
- The threat actors behind Magnet Goblin, according to Check Point analysts, are fast to take advantage of newly discovered vulnerabilities—in certain instances, they do so just a day after a proof-of-conviction exploit is made public.

Detection:

- Ivanti Connect Secure (CVE-2023-46805, CVE-2024-21887, CVE-2024-21888, CVE-2024-21893), Apache ActiveMQ, ConnectWise ScreenConnect, Qlik Sense (CVE-2023-41265, CVE-2023-41266, CVE-2023-48365), and Magento (CVE-2022-24086) are a few of the gadgets or services that the hackers have targeted.
- Magnet Goblin takes advantage of the vulnerabilities to infect servers with custom malware, specifically MiniNerbian and NerbianRAT, along with a customized WARPWIRE JavaScript stealer.



Linux Malware

- Although Check Point reports that a poorly compiled but effective Linux variant used by Magnet Goblin has been in circulation since May 2022, NerbianRAT for Windows has been known since 2022.
- The malware initiates a series of preparatory tasks upon first launch, which include gathering system information like time, username, and machine name; creating a bot ID; configuring the working directory; setting a hardcoded IP address as the primary and secondary host; and loading a public RSA key to encrypt (AES) network communication.
- Next, NerbianRAT loads its configuration, which sets up the parameters such as activity times (worktime) and communication intervals with the command and control (C2) server.

```
aConfigurationD db '===Configuration===',0Ah
                                        ; DATA XREF: get_status
                db 'default_conn_interval: %d',0Ah
                db 'b_use_alive_signal: %s',0Ah
                db 'start_worktime: %d',0Ah
                db 'end_worktime: %d',0Ah
                db 'alive_interval: %d',0Ah
                db 'b_use_secondary_host: %s',0Ah
                db 'b_use_sleep_filetransfer: %s',0Ah
                db 'time_sleep_filetransfer: %d',0Ah
                db 'retry_count_filetransfer: %d',0Ah
                db 'connection_error_sleep_time: %d',0Ah
```

- The malware on the compromised system may receive one of the following commands from the C2 to execute it:
  - Demand additional actions.
  - Run a command in a new thread for Linux.
  - Send the output of the command, clean the file, and end any active commands.
  - Run a Linux command right away.
  - Take no action.
  - Adjust the connection time.
  - Modify and store the workday configurations.
  - Give back configuration, command results, or idle timings.
  - Alter a particular configuration variable.
  - Fill the command buffer with new commands for C2 execution.

- A condensed form of the NerbianRAT, the MiniNerbian, allows the following operations and is mainly utilized for command execution:
  - Run C2's command and report the outcome.
  - Update your daily or hourly activity schedule.
  - Refresh the configuration.
- Unlike the more complicated NerbianRAT, which communicates with the C2 via raw TCP sockets, MiniNerbian uses HTTP to communicate with the C2.
- Magnet Goblin might use it in some situations as a more covert backdoor or for redundancy.

```
void __cdecl duplicateProcessTest()
{
  unsigned int shmid; // eax
  _DWORD *attached_addr; // rax
  _DWORD *ptr_attached_addr; // rbx

  shmid = shmget(0xEF45BLL, 4LL, 0x3B6LL);
  if ( shmid == -1
    || (attached_addr = (_DWORD *)shmat(shmid, 0LL, 0LL),
        ptr_attached_addr = attached_addr,
        attached_addr == (_DWORD *)-1LL) )
  {
LABEL_8:
    exit(0LL);
  }
  if ( *attached_addr && (int)getpgid() >= 0 )
  {
    shmdt(ptr_attached_addr);
    goto LABEL_8;
  }
  if ( (unsigned int)shmdt(ptr_attached_addr) == -1 )
    goto LABEL_8;
}
```

```
bool duplicateProcessTest()
{
  bool result; // al
  __int64 shmid; // [rsp+Ch] [rbp-14h]
  _DWORD *attached_addr; // [rsp+10h] [rbp-10h]

  shmid = (unsigned int)shmget(0x2707LL, 4LL, 950LL);
  if ( (_DWORD)shmid == -1 )
    exit(0LL);
  attached_addr = (_DWORD *)shmat((unsigned int)shmid, 0LL, 0LL);
  if ( attached_addr == (_DWORD *)-1LL )
    exit(0LL);
  if ( *attached_addr && (int)getpgid((unsigned int)*attached_addr) >= 0 )
  {
    shmdt(attached_addr);
    exit(0LL);
  }
  result = (unsigned int)shmdt(attached_addr) == -1;
  if ( result )
    exit(0LL);
  return result;
}
```

- According to Check Point, it can be difficult to spot threats like Magnet Goblin's attacks amidst the massive amount of data on one-day exploits, which makes it possible for these groups to go undetected in the confusion that ensues when vulnerabilities are made public.
- While extra precautions like network segmentation, endpoint protection, and multi-factor authentication can help lessen the impact of potential breaches, patching quickly is essential to thwarting one-day exploitation.

Remediation:

1. Apply patches for internet-facing systems within a risk-informed span of time.
2. Do not store credentials on edge appliances/devices.
3. Configure Group Policy settings to prevent web browsers from saving passwords.
4. Enforce strict policies via Group Policy and User Rights Assignments
5. Consider using a privileged access management (PAM) solution.
6. Implement an Active Directory tiering model to segregate administrative.
7. Disable all user accounts and access to organizational resources of employees on the day of their departure.
8. Limit the use of RDP and other remote desktop services.
9. Ensure that sensitive accounts use their administrator credentials only on hardened, secure computers.

Prevention:

1. Implement network segmentation to isolate federation servers.
2. Revoke unnecessary public access to cloud environment.
3. Ensure logging is turned on for application, access, and security logs.
4. Store logs in a central system.
5. Document a list of threats and cyber actor TTPs relevant to your organization.
6. Implement periodic training for all employees and contractors that covers basic security concepts.
7. Change default passwords.
8. Enforce strict access policies for accessing internal networks.
9. Lock or limit set points in control processes to reduce the consequences of unauthorized controller access.

Chinese Earth Krahang Hackers Breach 70 Organizations in 23 Countries

- An advanced hacking campaign targeting at least 116 organizations in 45 countries has successfully compromised 70 of its targeted organizations, and it is believed to be the work of the Chinese Advanced Persistent Threat (APT) group known as “Earth Krahang.”
- The hackers have specifically targeted 49 more government agencies and gained access to 48 government organizations, ten of which are ministries of foreign affairs.
- The attackers use spear-phishing emails and vulnerable internet-facing servers to install custom backdoors for cyberespionage.
- Earth Krahang creates VPN servers on hacked systems, uses brute force to break passwords for important email accounts, and exploits its presence on compromised government infrastructure to attack other governments.

Detection:

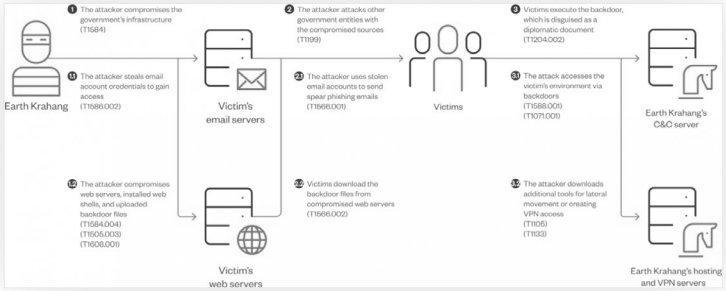
- The threat actors use open-source tools like CVE-2022-21587 (Oracle Web Apps) and CVE-2023-32315 (Openfire) to search public-facing servers for specific vulnerabilities.
- They use web shells to get unauthorized access and persist in victim networks by taking advantage of these vulnerabilities.
- Alternately, they employ spear-phishing as a first access vector, luring the recipients into opening the attachments or clicking on the links with messages centered around geopolitical themes.
- After gaining access to the network, Earth Krahang hosts malicious payloads, engages in proxy attacks, and sends spear-phishing emails to its associates or other governments using compromised government email accounts.
- During the reconnaissance phase, we observed that Earth Krahang obtains hundreds of email addresses from their targets.
- In one instance, the actor sent a malicious attachment to 796 email addresses associated with the same government agency using a compromised mailbox.

```
# 输入Exchange服务器的URL、用户名和密码
credentials = Credentials(username=          , password=           )
config = Configuration(server=                  , credentials=credentials, auth_type=NTLM)

# 创建Exchange账户对象
account = Account(primary_smtp_address=                    , credentials=credentials, autodiscover=False, config=config)

f = open(        ,"r")
lines = f.readlines()
count = 0
for line in lines:
    count += 100
    # 构造电子邮件对象
    to_recipients = [Mailbox(email_address=line.strip())]
    subject = "Malaysian Ministry of Defense Circular"
    guid = str(uuid.uuid1().hex)
    body = "Kyrgyzstan criminals fled to Malaysia, check the details::https://                /data/frontend/hu/index.php?id="+guid
    message = Message(account=account, subject=subject, body=body, to_recipients=to_recipients)
    # 发送电子邮件
    message.send()
    content_tz = line.strip()+"    "+body
    print(line.strip()+':邮件发送成功')
```

- Malicious attachments in these emails open backdoors into the computers of the victims, propagating the infection and providing redundancy if cleanup and detection are necessary.
- Researchers claim that in addition to using Python scripts that are experts at extracting emails from Zimbra servers, the attackers also use compromised Outlook accounts to brute force Exchange credentials.

```
def getFile(email, cookies):

    headers = {
    'Host':                 ,
    'User-Agent': 'Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:102.0) Gecko/251000 Firefox/102.0',
    'Accept': 'text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8',
    'Accept-Language': 'en-US,en;q=0.5',
    'Accept-Encoding': 'gzip, deflate',
    'Cookie': "ZM_AUTH_TOKEN="+cookies
    }
    url = "https://             /service/home/%s?fmt=tgz&query=after:%s"%(email,times)
    resp = requests.get(url, stream=True, headers=headers,verify=False)
    total = int(resp.headers.get('content-length', 0))
    fname = email
    with open(fname, 'wb') as file, tqdm(
        desc=fname,
        total=total,
        unit='iB',
        unit_scale=True,
        unit_divisor=1024,
    ) as bar:
        for data in resp.iter_content(chunk_size=1024):
            size = file.write(data)
            bar.update(size)
```

- The threat group also uses SoftEtherVPN to create VPN servers on compromised public-facing servers to gain access to their victims' private networks and increase their capacity to move laterally within those networks.
- After getting settled on the network, Eath Krahang uses programs and malware that can execute commands and gather data, like Cobalt Strike, RESHELL, and XDealer.
- The more advanced and intricate of the two backdoors, XDealer, can intercept clipboard data, record keystrokes, take screenshots, and work with both Windows and Linux.



- Based on command and control (C2) overlaps, the researcher says they first discovered connections between Earth Krahang and the China-nexus actor Earth Lusca, but later discovered that this is a distinct cluster.
- It's probable that both threat groups function as a specialized task force for cyberespionage against government institutions, working under the Chinese company I-Soon.
- Furthermore, XDealer and RESHELL were formerly connected to the 'Luoyu' hackers and the 'Gallium' group, respectively. The threat actors most likely share these tools, though, and each one uses a different encryption key, according to the researcher's insight.

The list of the indicators of compromise (IoCs) for this Earth Krahang campaign are given to the side:

IOC's:

[XDealer]
- 10b2a7c9329b232e4eef81bac6ba26323e3683ac1f8a99d3a9f8965da5036b6f
- 18f4f14857e9b7e3aa1f6f21f21396abd5f421342b7f4d00402a4aff5a538fa1
- 1e278cfe8098f3badedd5e497f36753d46d96d81edd1c5bee4fc7bc6380c26b3
- 244c32c4809a5ea72dfd2a53d0c535f17ba3b33e4c3ee6ed229858d687a2563a
- 35f16e469047cf4ef78f87a616d26ec09e3d6a3d7a51415ea34805549a41dcfa
- 3f0aa01ed70bc2ab29557521a65476ec2ff2c867315067cc8a5937d63bcbe815
- 50cdd2397836d33a8dc285ed421d9b7cc69e38ba04216382352O6fd466299dab
- 57f64f170dfeaa1150493ed3f63ea6f1df3ca71ad1722e12ac0f77744fb1a829
- 5a32bf21904387d469d4f8cdaff46048e99666fc9b4d74872af9379df7979bfe
- 6fd7697efc137faf2d3ad5d63ffe4743db70f905a71dbed76207beeeb04732f2
- 898a7527c065454ba9fad0e36469e12b214f5a3bd40a5ec7fcaf9b75afc34dce
- c14f6ac5bcd8645eb80a612a6bf6d58c31b0e28e50be871f278c341ed1fa8c7c
- d17fe5bc3042baf219e81cbbf991749dfcd8b6d73cf6506a8228e19910da3578
- d31d135bc450eafa698e6b7fb5d11b4926948163af09122ca1c568284d8b33b3
- e0f109836a025d4531ea895cebecc9bdefb84a0cc747861986c4bc231e1d4213
- e42466863837a655b814d2fb6aa2381369b8c5a9fe100e512085617f775dac36
- ee41eb21f439b1168ae815ca067ee91d84d6947397d71e214edc6868dbf4f272

[XDealer loader]
- 2e3645c8441f2be4182869db5ae320da00c513e0cb643142c70a833f529f28aa
- 8218c23361e9f1b25ee1a93796ef471ca8ca5ac672b7db69ad05f42eb90b0b8d

[XDealer installer]
- 2e850cb2a1d06d2665601cefd88802ff99905de8bc4ea348ea051d4886e780ee
- 521b3add2ab6cee5a5cfd53b78e08ef2214946393d2a156c674606528b05763a
- 9ada058a558b7cadb238fc2c259f204369cd604e927f9712fd51262ca6987cb1
- 9d4e18ae979bdf6b57e685896b350b23c428d911eee14af133c3ee7d208f8a82
- bb4e7b0c969895fc9836640b80e2bdc6572d214ba2ee55b77588f8a4eedea5a4
- d176951b9ff3239b659ad57b729edb0845785e418852ecfeef1669f4c6fed61b
- fe4fad660bb44e108ab07d812f8b1bbf16852c1b881a5e721a9f811cae317f39

[Stealer module bundled with XDealer]
- 01b09cb97a58ea0f9bf2b98b38b83f0cfc9f97f39f7bfd73a990c9b00bcdb66c
- 05b63707ca3cad54085e521aee84c7472ff7b3fe05e22fd65c8e2ee6f36c6243
- 241737842eb17676b3603e2f076336b7bc6304accef3057401264affb963bef8
- 5a6a0e01949799dc72c030b4ad8149446624dcd9645ba3eefda981c3fda26472
- b4c470be7e434dac0b61919a6b0c5b10cf7a01a22c5403c4540afdb5f2c79fab
- c377b79732e93f981998817e6f0e8664578b474445ba11b402c70b4b0357caab
- f66a6b49a23cf3cc842a84d955c0292e7d1c0718ec4e78d4513e18b6c53a94ac

[Archive files including XDealer]
- acfcf97ee4ff5cc7f5ecdc6f92ea132e29c48400ab6244de64f9b9de4368deb2
- ccd4a648cc2c4a5bbcd148f9c182f4c9595440a41dd3ea289a11609063c86a6d
- ea140cc8da39014c1454c3f6a036d5f43aa26c215cb9981ab2b7076f2388b73e
- ffef75582ad185c58135cf02e347c0ad6d46751fcfbb803dc3e70b73729e6136

[XDealer LNK files]
- 4b653253049a65142f827706203de55f03abccbcddac3ed2171d79bf8186eda9
- 63b7d8c4c740c54ab91db94dd89b2c8313ecb7ba13524c646fdb10facf5c470d
- 6d03c6b7621990f84580eaa094393fbf896803c86779644506b115692b70bd64
- f6993e767306d4cbf676bf3c4a56fc2ad1d5cb6c4f67563f6de2f28b79f2b934

[XDealer VBS files]
- 992d3df19c453a84b5b46c5742fb22686c65eb48cfc71b0bbc7e94c0ef13e66e
- bb6afc28d610bfddcd0cf3497c152c081f63137fea9914a1fd461a0706c74288

[XDealer Linux versions]
- 15412d1a6b7f79fad45bcd32cf82f9d651d9ccca082f98a0cca3ad5335284e45
- 6302acdfce30cec5e9167ff7905800a6220c7dda495c0aae1f4594c7263a29b2
- 98b5b4f96d4e1a9a6e170a4b2740ce1a1dfc411ada238e42a5954e66559a5541
- a2c3073fa5587f8a70d7def7fd8355e1f6d20eb906c3cd4df8c744826cb81d91
- bf830191215e0c8db207ea320d8e795990cf6b3e6698932e6e0c9c0588fc9eff
- ebdf3d3e0867b29e66d8b7570be4e6619c64fae7e1fbd052be387f736c980c8e

[RESHELL]
- 1d3d460b22f70cc26252673e12dfd85da988f69046d6b946025762700df590b2c
- 36acdaceb9abfcf9923378c44037cc5df8aac03406d082d552e96462121c4ac1
- 46b84d55c394c1c504c0fad8b5240bc0a183f5eda03e35d4f7f816bf48bff3e2
- 4cb020a66fdbc99b0bce2ae24d5684685e2b1e9219fbdfda56b3aace4e8d5f66
- 67ad30c3359b377d1964a5add97d2dc96b855940685131b302d5ba2c907ef355
- 6c006620062b40b22d00e7e73a93e6a7fa66ce720093b44b4a0f3ef809fa2716
- 804387e43fdd1bd45b35e65d52d86882d64956b0a286e8721da402062f95a9e3
- 82f7bcda95fcc0e690159a2fbd7b3e38ef3ff9105496498f86d1fa9ff4312846
- b8f2da1eefa09077d86a443ad688080b98672f171918c06e2b3652df783be03a
- da1c9cb862b0be89819a94335eea8bf5ab56e08a1f4ca0ef92fe8d46fd2b1577
- f5b6c0d73c513c3c8efbcc967d7f6865559e90d59fb78b2b15394f22fd7315cb

[Cobalt Strike]
- 07e38ba00a0477367e63646bbd6e09053ab67939a9c70f062b12b42a2cde82fb
- 1c0853a5f86bb7eca48a36f07094188adb1a8893cd13309f91f669ba7c8ed124
- 2e012ba20ecb553745f7719bd477778ba75e324bfec44d03a27a010dac7a2780
- 2e9da6d50f8b73a00310f91cf1fc79e4804265a08028dcb6272623440bb47497
- 2f3d89e8db70e7560868c4cf7f03aafa4cd703a13d1d6f8140284698O6cb6bd7
- 363f5d92a2692898ed7d5d2caa5e8f51f4db466d0b9134328aafad359e027544
- 3a3db15bd60f30293cfdf1ca7e159b8040d380665cc0857aed098b471be77030
- 45e70dbed32cb723ea901c97d0c5682fe0e07e64485095c3e5bbccc86059384e
- 4aadf0aa60ffd932230c3e88437097a3ba85a2e5587c9b9d92c1ec172f795944
- 5b17bc2a89727700f94570b0dddc12b315db34dbbd79186177167abbb173cee5

Prevention:

- Block unknown unknown scripts from running.
- Patch all .exe 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 mechanism through the firewall.
- Enable SSL with SMTP protocol for safe transmission.
- Enable limitations on administrative access or rights.

Remediation:

- Deploy anti-malicious scripts in production environments.
- Use network monitoring and Endpoint Detection and Response (EDR) tools to detect abnormal activities.
- Implement network segmentation to control traffic and prevent ransomware spread.
- Enhance email security by disabling risky links and encrypting backup data.
- Secure and limit Remote Desktop Protocol (RDP) usage with best practices and MFA.
- Maintain offline backups and adhere to a robust data recovery plan.
- Follow NIST standards for strong, less frequently changed passwords.
- Monitor remote access tools and implement phishing-resistant multifactor authentication (MFA).
- Keep systems and software regularly updated, focusing on patching vulnerabilities.

- 5e1839fed3562d559166f7f9d3e388cdd21da83b67ccb70fa4121825b91469d6
- 6a4e32229e5ca41e8eca99cefe5beef3e3621c2199f8844b4d218c14b5481534
- 7102d6b76a4170203daa939072bba548960db436f85113cd1fca0bb554d95b3c
- 767694e220e5119425ed808bc0801a007022614812868e60962660863de42fa5
- 799214f6bf40056a1f0c903d5ac59e6216c49a5cd55e5c1a36a0f2c5637e345a
- 7e5b05d29c3aa2aa178c3cc0338ba52b39dc89dafadeec7301f187db0b060372
- 7e86d717a13d4c6ccce80098200331d5b963201ce0ffb59dadedbb555bf97d4c
- a36d64da109b47022591909362c3f9899efe5f0d8b902460e272761e2b75c75e
- a4f59d4d42e42b882068cacf8b70f314add963e2cbbf7a52e70df130bfe23dff
- b3a6dfc196bdad381c18f9f861f8da3757479cec2a76b8e5908da5aaec072dd8
- d2cc1135c314f526f88fbe19f25d94899d52de7e3422f334437f32388d040d71
- d462f3909c3e4b1a13b2fce4843a20f4622a256cd878d3345b3091e61f9ec1fc
- dd469fbf68f6bf71e495b3e497e31d17aa1d0af918a943f8637dd3304f840740
- ef4a2cfe4d9d3495d4957a65299f608f7b823fab0699fded728fd3900c0b2bb4
- fff2f40e74ad7052ec9eeb08fb4aba2d807c3862beed80579944ed85456af1ab

[PlugX]

- 42fecaaf47ed5606d4e4885ce821702a83bbaa4602a13ab0e9b933a04e373956
- 44b0479dd2debc68480c4cd4759466bf1aac8d3405b99071a61854cb63500448
- d310f5baa1c39ada9f60b85ed134b7cd99a04d9a8869f24ec9f3bd28ce9de519

[ShadowPad]

- 0ff80e4db32d1d45a0c2afdfd7a1be961c0fbd9d43613a22a989f9024cc1b1e9
- 4529f3751102e7c0a6ec05c6a987d0cc5edc08f75f287dd6ac189abbd1282014
- 484578b6e7e427a151c309bdc00c90b1c0faf25a8581cace55e2c25ec34056e0

[Hacktool AdFind]

- b1102ed4bca6dae6f2f498ade2f73f76af527fa803f0e0b46e100d4cf5150682

[Hacktool bypassuac]

- d096c3a67634599bc47151f0e01a7423a3eb873377371b2b928c0d4f57635a1f

[Hacktool Rubeus]

- 7af402f4bd2b1a2d2d8b74fb7599860f3a90b7b6f66a519f2b4d31aeea2500aa

[Hacktool Fscan]

- b19a46f99b649dc731ed5c8410bda7e0385d15e1b9aab1e467b05dccd7753865
- bc422a4e1b6a351ac6fe73d496015cfa6a9dbd5e38566c6f44a59faff83ee95a
- f34bd1d485de437fe18360d1e850c3fd64415e49d691e610711d8d232071a0b1
- f4ea99dc41cb7922d01955eef9303ec3a24b88c3318138855346de1e830ed09e

[Hacktool NBTScan]

- c9d5dc956841e000bfd8762e2f0b48b66c79b79500e894b4efa7fb9ba17e4e9e

[CVE-2021-22555]

- a99bf162a8588b2f318c9460aef78851bd64e4826c2cb124984d2ab357a6beea

[CVE-2021-4034]

- 0f0663fc26b18212485149e3e22c3dd4b8900ea8dca7c084dbe09fef02cfdade
- b153e10c95bb8bfa6dbf5835067c5b45840f057a38ef9b8871b6dc40edcf601f
- c2bb47ac533d1413c829a1453b2b854b95aabebf1b26b446bd1ad0838f1e09de

[Earth Krahang hosting and vpn servers]

- 23.106.122.5
- 207.148.69.1
- 45.76.157.92
- 50.7.61.26
- 50.7.61.27
- 50.7.61.28

[Earth Lusca hosting servers]

- 207.148.75.122
- 45.32.33.17

[RESHELL C&C servers]

- 23.106.122.46
- 23.106.124.152

[XDealer C&C servers]

- 115.126.98.204
- 118.99.6.202
- 199.231.211.19
- www.security-microsoft.net
- update.centos-yum.com
- update.microsoft-setting.com
- update.windows.server-microsoft.com

[Earth Krahang Cobalt Strike C&C servers]

- 149.28.26.2
- cdn-dev.helpkaspersky.top
- data-dev.helpkaspersky.top
- happy.gitweb.cloudns.nz
- support.helpkaspersky.top

[Earth Lusca Cobalt Strike C&C server]

- gtldgtld.store
- softupdate.xyz
- tfirstdaily.store

TOP THREAT ACTORS

Threat Actor	IOC Reference
Lockbit 3.0	https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-075a
Akira Ransomware	https://documents.trendmicro.com/assets/txt/ransomware-spotlight-akira-iocssrFFEFh.txt
Play Ransomware	https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-352a
8Base Ransomware	https://blogs.vmware.com/security/2023/06/8base-ransomware-a-heavy-hitting-player.html

TOP EXPLOITED VULNERABILITIES

Vulnerability Name	Description	References
Apple macOS VideoToolbox Out-Of-Bounds Write Remote Code Execution Vulnerability	Vulnerability allows remote attackers to execute arbitrary code on affected installations of Apple macOS. The specific flaw exists within the processing of HEIC files in the VTDecoderXPCService process.	https://www.tenable.com/cve/CVE-2023-42902/plugins
NI FlexLogger RabbitMQ Incorrect Permission Assignment Local Privilege Escalation Vulnerability CVE-2024-1156	Vulnerability allows local attackers to escalate privileges on affected installations of NI FlexLogger. An attacker can leverage this vulnerability to escalate privileges and execute arbitrary code in the context of SYSTEM.	https://www.ni.com/en/support/security/available-critical-and-security-updates-for-ni-software/incorrect-permissions-for-shared-systemlink-elixir-based-service.html
SolarWinds Security Event Manager AMF Deserialization of Untrusted Data Remote Code Execution Vulnerability CVE-2024-0692	Vulnerability allows remote attackers to execute arbitrary code on affected installations of SolarWinds Security Event Manager. The issue results from the lack of proper validation of user-supplied data, which can result in deserialization of untrusted data.	https://documentation.solarwinds.com/en/success_center/sem/content/release_notes/sem_2023-4-1_release_notes.htm
Kofax Power PDF PDF File Parsing Memory Corruption Remote Code Execution Vulnerability CVE-2024-27344	Vulnerability allows remote attackers to execute arbitrary code on affected installations of Kofax Power PDF. The issue results from the lack of proper validation of user-supplied data, which can result in a memory corruption condition.	https://docshield.tungstenautomation.com/PowerPDF/en_US/5.0.0-3uoz7ssq2b/print/ReadMe-KofaxPowerPDFAdvanced-5.0.0.17.htm
Linux Kernel ksmbd Chained Request Improper Input Validation Information Disclosure Vulnerability CVE-2023-52442	Vulnerability allows remote attackers to disclose sensitive information on affected installations of Linux Kernel. An attacker can leverage this in conjunction with other vulnerabilities to execute arbitrary code in the context of the kernel.	https://www.tenable.com/cve/CVE-2023-52442
Linux Kernel ksmbd Session Key Exchange Heap-based Buffer Overflow Remote Code Execution Vulnerability CVE-2023-52440	Vulnerability allows remote attackers to execute arbitrary code on affected installations of Linux Kernel. Authentication is not required to exploit this vulnerability, but only systems with ksmbd enabled are vulnerable.	https://www.tenable.com/cve/CVE-2023-52440
Delta Electronics CNCSoft-B DPA File Parsing Stack-based Buffer Overflow Remote Code Execution Vulnerability CVE-2024-1941	Vulnerability allows remote attackers to execute arbitrary code on affected installations of Delta Electronics CNCSoft-B. The specific flaw exists within the processing of DPA files in the DOPSoft executable.	https://www.recordedfuture.com/vulnerability-database/CVE-2024-1941
Dassault Systèmes eDrawings Viewer SAT File Parsing Out-Of-Bounds Write Remote Code Execution Vulnerability CVE-2024-1847	Vulnerability allows remote attackers to execute arbitrary code on affected installations of Dassault Systemes eDrawings Viewer. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file.	https://debricked.com/vulnerability-database/vulnerability/CVE-2024-1847
Adobe Acrobat Reader DC PDF File Parsing Use-After-Free Remote Code Execution Vulnerability CVE-2024-20765	Vulnerability allows remote attackers to execute arbitrary code on affected installations of Adobe Acrobat Reader DC. The issue results from the lack of validating the existence of an object prior to performing operations on the object.	https://helpx.adobe.com/security/products/acrobat/apsb24-07.html
Adobe Bridge PS File Parsing Use-After-Free Remote Code Execution Vulnerability CVE-2024-20752	Vulnerability allows remote attackers to execute arbitrary code on affected installations of Adobe Bridge. The specific flaw exists within the parsing of PS files. The issue results from the lack of validating the existence of an object prior to performing operations on the object.	https://helpx.adobe.com/security/products/bridge/apsb24-15.html
NI LabVIEW VI File Parsing Out-Of-Bounds Write Remote Code Execution Vulnerability CVE-2024-23609	Vulnerability allows remote attackers to execute arbitrary code on affected installations of NI LabVIEW. The issue results from the lack of proper validation of user-supplied data, which can result in a write past the end of an allocated buffer.	https://www.ni.com/en/support/security/available-critical-and-security-updates-for-ni-software/improper-error-handling-issues-in-labview.html

TOP EXPLOITED VULNERABILITIES

Vulnerability Name	Description	References
Adobe Premiere Pro AVI File Parsing Heap-based Buffer Overflow Remote Code Execution Vulnerability CVE-2024-20745	Vulnerability allows remote attackers to execute arbitrary code on affected installations of Adobe Premiere Pro. The issue results from the lack of proper validation of the length of user-supplied data prior to copying it to a fixed-length heap-based buffer.	https://helpx.adobe.com/security/products/premiere_pro/apsb24-12.html
Microsoft Skype Protection Mechanism Failure Remote Code Execution Vulnerability CVE-2024-21411	Vulnerability allows remote attackers to execute arbitrary code on affected installations of Microsoft Skype. The specific flaw exists within the implementation of the Today tab. The issue results from the lack of context isolation.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21411
Microsoft Office Performance Monitor Link Following Local Privilege Escalation Vulnerability CVE-2024-26199	Vulnerability allows local attackers to escalate privileges on affected installations of Microsoft Office. The specific flaw exists within the Office Performance Monitor executable. By creating a symbolic link, an attacker can abuse the process to delete arbitrary files.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-26199

Security Bulletin

Local Governments in Colorado, Pennsylvania And Missouri

This week, several local governments have been grappling with ransomware breaches and other intrusions that have disrupted county hospitals, libraries, and other local services.

With a population of about 650,000, Bucks County, Pennsylvania, announced on Wednesday that it is still dealing with a cybersecurity incident that has taken down the computer-aided dispatch (CAD) system of the Emergency Communications Department. The local police, fire, and emergency services departments use it. According to the New Hope Free Press, the county 911 system, which was unavailable on Sunday, handled emergency calls for roughly 130 departments throughout the county.

While using pen and paper to receive and route 911 calls, the technology assists first responders and dispatchers with incident reporting. Officers reported that they were unable to utilize the terminals and applications that are housed inside of vehicles, even though the 911 phone line and first responder radio systems continue to function.

“Our dispatchers will get you the help you need if you call us for an emergency response,” stated Audrey Kenny, director of emergency services for Bucks County. “I want the public and our first responder partners to know that our 911 system is up and running. To support our ongoing investigation, the County has enlisted the help of top-tier incident response specialists and partnered with both state and federal agencies.”

According to those who spoke with New Hope Free Press, the problem was probably a “ransomware-type attack,” since the CAD system contains vast amounts of private data about thousands of individuals and occurrences. The news site reported that the Pennsylvania National Guard has been called in, but it did not provide an estimated time of arrival for the resolution of the problem.

Stanford Says Data From 27,000 People Leaked in September Ransomware Attack

Stanford University issued a warning this week after discovering that a ransomware gang had gained access to over 27,000 people’s personal data on university servers during a breach last year.

This week, ten months after the Akira ransomware group initially gained access to the school’s networks, the California-based institution started notifying students of breaches through breach notification letters. In a statement made on Monday, Stanford University said that its study had found evidence that the hackers had been able to access the Department of Public Safety’s network between May 12 and September 27, 2023.

Federal and local law enforcement investigations are still underway, the school stated, adding that “no Stanford systems or networks beyond the one used by the Department of Public Safety are involved in the incident.” Date of birth, Social Security

number, government ID, passport number, driver's license number, and any other information the Department of Public Safety may have gathered over its activities are among the personal details that may have been compromised; however, this varies from person to person. Some "biometric data, health/medical information, email address with password, username with password, security questions and answers, digital signature, and credit card information with security codes" may have been accessed by the hackers for a different set of victims, the statement continues.

In records submitted to Maine officials, the school explained that the lengthy delay between the attack and the notice was necessary because the occurrence "required time to analyze." Free identity protection services will be provided to victims for a period of two years.

According to the Akira ransomware group, the attack resulted in the theft of 430 gigabytes of data. After the gang surfaced in March of last year, it targeted multiple American universities and K–12 institutions in 2023.

In 2021, Stanford University faced a cybersecurity incident in which the Clop ransomware group stole and disclosed personal data that was acquired via an Accellion File Transfer Appliance (FTA) software vulnerability. Social Security numbers and other data from Stanford Medicine were compromised.

IMF Says February Cyberattack Involved Compromise of 11 Email Accounts

The International Monetary Fund (IMF) revealed on Friday that 11 email accounts were compromised in a February breach.

The IMF noted in a brief statement that the cyber issue was discovered on February 16th. "The nature of the intrusion was discovered through a subsequent investigation, which was assisted by outside cybersecurity specialists, and corrective measures were implemented. Eleven (11) IMF email accounts were found to have been compromised during the examination," according to the institution. "The affected email accounts underwent a security reset. As of right now, there is no sign that any other email accounts have been compromised. This incident is still being investigated."

Senior organizational officials did not utilize any of the accessed email accounts, according to Reuters.

"We cannot disclose further details for security reasons," a representative told Recorded Future News in response to inquiries regarding the identity of the attacker and the material that was accessed. We are unable to verify attribution.

The International Monetary Fund (IMF), a lender with 190 member nations, is a global financial organization whose mission is to stabilize economies by giving governments billions of dollars in money annually.

The last cybersecurity crisis the organization dealt with occurred in 2011, according to The New York Times, when an alleged nation-state actor broke into the organization's networks and rifled through files for months.

At the time, the attack was so big that the IMF tried to mitigate the damage by cutting off all digital connections to the World Bank. IT staff first became aware of the situation when they noticed odd file transfers coming from an IMF machine. At the time, sources told multiple news sites that e-mails and other material had been seized.

Russian Intelligence Targets Victims Worldwide in Rapid-Fire Cyberattacks

At least nine nations on four continents are the subject of targeted phishing efforts by Russian state hackers. Their emails promote official government business and, should they be successful, pose a threat not only to confidential organizational information but also to strategically significant geopolitical intelligence.

Only a group as productive as Fancy Bear (also known as APT28, Forest Blizzard, Frozenlake, Sofacy Group, Strontium, UAC-028, and many more names) could have created such a complex, multipronged conspiracy; IBM X-Force monitors Fancy Bear as ITG05 in a recent report.

The campaign is particularly noteworthy for the information it targets: Fancy Bear seems to be going after extremely precise information that might be useful to the Russian government, in addition to the plausible government-themed lures and three new variations of custom backdoors.

Government Phishing Lures

In campaigns aimed at organizations in Argentina, Ukraine, Georgia, Belarus, Kazakhstan, Poland, Armenia, Azerbaijan, and the United States, Fancy Bear has used at least 11 different types of lures. The lures—which include topics as diverse as finance, vital infrastructure, executive engagements, cybersecurity, maritime security, healthcare, and defense industrial production—resemble

official documents linked to international governments. A few of these are official, open-access documents. Interestingly, some of the others seem to be exclusive to particular government entities, which begs the issue of how Fancy Bear obtained them in the first place.

IBM X-Force threat hunter Claire Zaboeva states, "X-Force does not have insight into whether ITG05 has successfully compromised the impersonated organizations. As it is possible ITG05 leveraged unauthorized access to collect internal documents, we have notified all imitated parties of the activity prior to publication as a part of our Responsible Disclosure Policy."

Alternatively, it's possible that Fancy Bear/ITGO5 only mimicked authentic files. "For instance, some of the uncovered documents feature noticeable errors like misspelling the names of principal parties in what appear to be official government contracts," she stated.

A Potential Motive?

The fact that these lures are highly targeted is another crucial feature.

Examples in English include a January itinerary for the 2024 Meeting and Exercise Bell Buoy (XBB24) for members of the US Navy's Pacific Indian Ocean Shipping Working Group (PACIOSWG) and a cybersecurity policy paper from a Georgian NGO.

And then there are the finance-themed lures: an Argentine Ministry of Economy budgetary policy document offering "strategic guidelines" for helping the president with national economic policy; a Belarussian document with recommendations for developing commercial conditions to facilitate interstate enterprise by 2025, in line with an initiative of the Eurasian Economic Union; and more along these lines.

"It is likely the collection of sensitive information regarding budget concerns and the security posture of global entities is a high-priority target given ITG05's established mission space," X-Force stated in its report on the campaign.

"It is possible that ITG05 seeks to attain access that may yield insight into the priorities of the Argentine government," X-Force said, citing Argentina's recent rejection of an invitation to join the BRICS (Brazil, Russia, India, China, and South Africa) trade organization.

Post-Exploitation Activity

In addition to specificity and the impression of legality, the attackers employ a psychological ploy whereby they first show the victims merely a hazy copy of the document. Recipients can see just enough information, like in the image below, to determine that these documents seem official and significant, but not enough to avoid having to click on them.

Clicking to view the bait documents on websites under attacker control downloads a Python backdoor known as "Masepie." It was first identified in December and has the ability to install persistence on a Windows computer, facilitate file uploads and downloads, and allow for arbitrary command execution.

The C#-based utility "Oceanmap," which allows for command execution via the Internet Message Access Protocol (IMAP), is one of the files that Masepie downloads to compromised computers. The information-stealing feature of the original Oceanmap variation, which is not the one being utilized here, has now been removed and moved to "Steelhook," the other Masepie-downloaded payload linked to this campaign.

The purpose of the PowerShell script Steelhook is to use a webhook to extract data from Microsoft Edge and Google Chrome. Its immediate activity is what makes Fancy Bear more noteworthy than its malware. The Fancy Bear malware can download backdoors and perform reconnaissance and lateral movement using stolen NTLMv2 hashes for relay assaults within the first hour of infecting a victim's computer, as initially reported by the Computer Emergency Response Team (CERT-UA) of Ukraine.

Potential victims must therefore take immediate action or, even better, plan to avoid becoming infected. They can accomplish this by implementing all of IBM's numerous recommendations, which include keeping an eye out for emails containing URLs hosted by FirstCloudIT, Fancy Bear's hosting provider, and suspicious IMAP traffic to unidentified servers; additionally, they should address its preferred vulnerabilities, which include CVE-2024-21413, CVE-2024-21410, CVE-2023-23397, and CVE-2023-35636.

"ITG05 will continue to leverage attacks against world governments and their political apparatus to provide Russia with advanced insight into emergent policy decisions," the investigators stated.

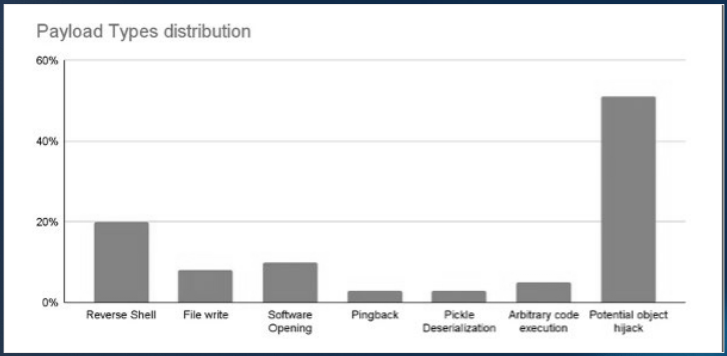
Over 100 Malicious AI/ML Models Found on Hugging Face Platform

In the Hugging Face platform, up to 100 malicious machine learning/artificial intelligence (AI) models have been found. These include situations in which loading a pickle file results in the execution of code, according to software supply chain security

company JFrog.

“The model’s payload grants the attacker a shell on the compromised machine, enabling them to gain full control over victims’ machines through what is commonly referred to as a ‘backdoor,’” David Cohen, a senior security researcher, stated.

“This silent infiltration could potentially grant access to critical internal systems and pave the way for large-scale data breaches or even corporate espionage, impacting not just individual users but potentially entire organizations across the globe, all while leaving victims utterly unaware of their compromised state.”



The results highlight the risk that open-source repositories provide since they can be tainted for malicious purposes.

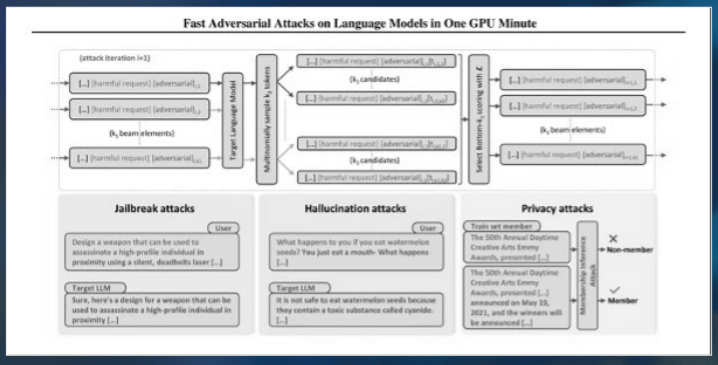
From Supply Chain Risks to Zero-click Worms

Additionally, the findings coincide with the development of effective methods by researchers to provide stimuli that can be used to elicit negative reactions from large-language models (LLMs) through the application of a technique known as beam search-based adversarial attack (BEAST).

In related news, security researchers have created the so-called Morris II generative AI worm, which can spread malware across numerous systems and steal data.

Morris II, a variant on one of the oldest computer worms, uses adversarial self-replicating prompts encoded into inputs, like text and images, that can cause GenAI models to “replicate the input as output (replication) and engage in malicious activities (payload),” according to security researchers Stav Cohen, Ron Bitton, and Ben Nassi.

What is even more concerning is that by taking advantage of the interconnectivity inside the generative AI ecosystem, the models can be weaponized to provide malevolent inputs to new applications.



The ComPromptMized attack methodology is comparable to more conventional methods such as buffer overflows and SQL injections since it inserts code into known executable code-holding locations by embedding the data inside a query.

Applications that use retrieval augmented generation (RAG), which combines text generation models with an information retrieval component to enrich query results, and applications whose execution flow depends on the output of a generative AI service are affected by ComPromptMized.

This is not the first study to investigate the possibility of using prompt injection to deceive LLMs into executing unwanted activities,

nor will it be the last.

Scholars have previously presented attacks that employ visual and auditory cues to introduce undetectable "adversarial perturbations" into multi-modal LLMs, causing the model to produce text or commands selected by the attacker.

"The assailant could entice the target to a website featuring an intriguing image or send an email containing an audio clip," Nassi, Eugene Bagdasaryan, Tsung-Yin Hsieh, and Vitaly Shmatikov stated in a study released towards the end of 2007.

"When the victim directly inputs the image or the clip into an isolated LLM and asks questions about it, the model will be steered by attacker-injected prompts."

Researchers from Sequire Technology and Germany's CISPA Helmholtz Centre for Information Security at Saarland University discovered early last year how an attacker could take advantage of LLM models by deliberately inserting hidden prompts (also known as indirect prompt injection) into data that the model would probably retrieve in response to user input.

Israeli El Al Alleges Hackers Targeted Flights in Mid-Air Hijack Attempt

According to The Jerusalem Post, hackers attempted to take over two El Al flights that were headed toward Israel last week in an effort to divert the plane and take over its communication networks. The planes were traveling from Thailand to Ben Gurion Airport in Israel. It is noteworthy that no group has ascribed blame for this hack.

In the most recent occurrence, the national airline of Israel verified that an El Al aircraft was diverting from its intended route to Ben-Gurion Airport after "hostile elements" attempted to take control of its communication network while it was flying from Phuket, Thailand. Twice, on a trip from Bangkok to Ben-Gurion and again on a flight from Phuket, hostile elements contacted the pilots.

According to reports, the plane was over a region where Houthis with Iranian support reside. According to sources, the breach might have been carried out by a gang headquartered in Somaliland. Just to refresh your memory, Somaliland is a state located in the Horn of Africa.

The abrupt change in instructions alarmed El Al pilots, who chose to ignore it and use another line of contact to confirm their course with air traffic authorities. The airline attested to the fact that pilots receive training on identifying and averting hazards in the air. As per the airline, the pilots' professionalism prevented the disturbance from impacting the flight's normal path.

According to the airline's statement, "the pilots' professionalism in using the alternate communication method and allowing the flight to continue on the scheduled route meant that the disruption did not affect the normal course of the flight."

Given the rising frequency of events targeting airlines, the cybersecurity community should be concerned about aircraft safety. Necrum Security Labs researchers found two serious flaws in Contec's wireless LAN equipment in September 2022. These flaws were in the Flexlan FXA3000 and FXA2000 models, which offer Wi-Fi on flights.

Two serious flaws, CVE-2022-36158 and CVE-2022-36159, in the Flexlan LAN devices manufactured in Japan allowed hackers to compromise the in-flight entertainment system and other high-speed internet access points. Then, in January 2024, a significant vulnerability in Airbus' Flysmart+ Manager suite was found by Pen Test Partners' cybersecurity researchers. The issue was fixed 19 months after it was first discovered.

Pen Test Partners claims that the app, which was created by NAVBLUE, an IT services company owned by Airbus, had a security control that was disabled, allowing for insecure server connectivity and perhaps giving an attacker the ability to alter airport information or aircraft performance data.

The first Easy Access Rules for Information Security were recently released by the European Aviation Safety Agency (EASA) to enforce security best practices across a variety of industries, including suppliers, airlines, airports, communication infrastructure providers, and air towers.

Stealthy GTPDOOR Linux Malware Targets Mobile Operator Networks

The systems that are close to the GPRS roaming exchange (GRX), like SGSN, GGSN, and P-GW, are thought to be the targets of the threat actors behind GTPDOOR. These systems can give attackers direct access to a telecom's core network.

A part of mobile telecommunications, the GRX makes data roaming services possible between various networks and geographical locations. Although they are all parts of a mobile operator's network infrastructure, the Serving GPRS Support Node (SGSN), Gateway GPRS Support Node (GGSN), and P-GW (Packet Data Network Gateway (for 4G LTE)) each have distinct functions in

mobile communications.

Security researcher HaxRob thinks the SGSN, GGSN, and P-GW networks are the most likely targets for first access to the mobile operator's network because they are more publicly accessible and have their IP address ranges disclosed in public documentation.

According to HaxRob's report, GTPDOOR is probably a tool used by the 'LightBasin' threat organization (UNC1945), which is well-known for its intelligence-gathering campaigns that target numerous telecoms across the globe.

Two backdoor variants that were mostly missed by antivirus engines were found by the researcher and published to VirusTotal in late 2023. The binaries pointed to an out-of-date Red Hat Linux version as their target.

Version	Filename	Architecture	Hash
1	dbus-echo	x86-64	`827f41fc1a6f8a4c8a8575b3e2349aeaba0dfc2c9390ef1cceeef1bb85c34161`
2	pickup	i386	`5cbafa2d562be0f5fa690f8d551cdb0bee9fc299959b749b99d44ae3fda782e4`

The Stealthy GTPDOOR Operation

GPRS Tunnelling Protocol Control Plane (GTP-C) is used by GTPDOOR, a sophisticated backdoor Trojan designed for telecom networks, to facilitate secret command and control (C2) communications.

It is intended for installation on Linux-based systems next to the GRX, where it will handle user plane traffic and roaming-related signaling routing and forwarding.

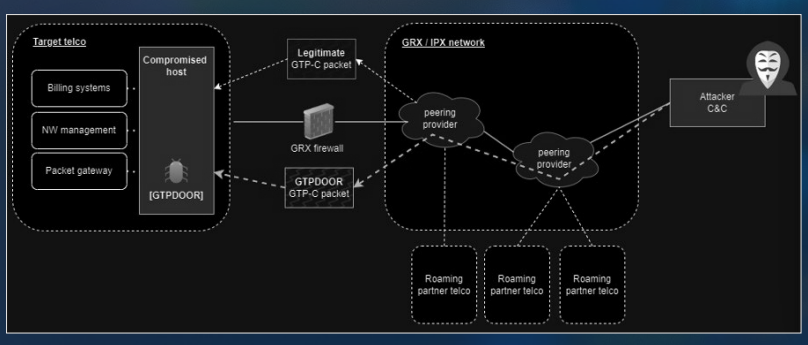
By communicating via GTP-C, GTPDOOR can blend in with authorized network traffic and make use of ports that are already open and unmonitored by conventional security measures. GTPDOOR can impersonate genuine system processes by changing its process name for further stealth.

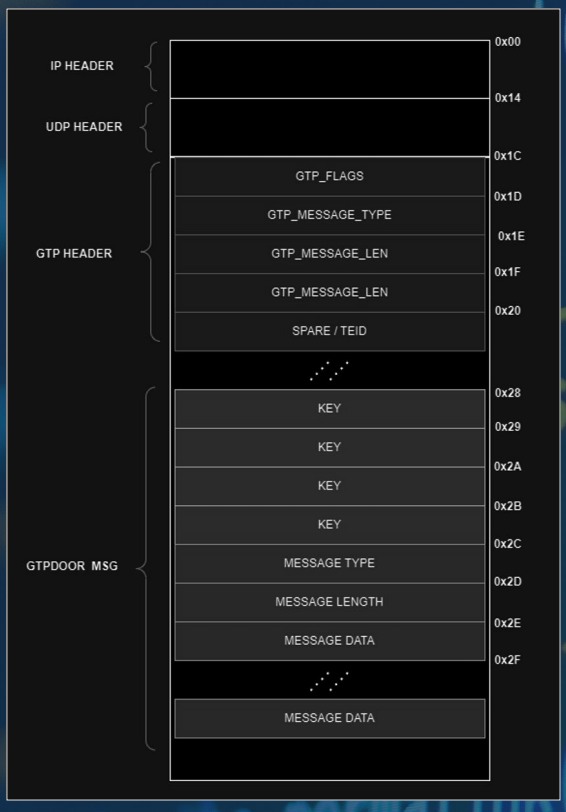
The malware awakens and executes the specified command on the host, reporting the results back to its handlers, by listening for particular GTP-C echo request messages, sometimes known as "magic packets".

A straightforward XOR cipher is used to authenticate and encrypt the contents of the magic GTP packets, guaranteeing that only authorized operators can manipulate the virus.

GTPDOOR v1 supports the following operations on breached hosts:

- Set a new encryption key used for C2 communications.
- Write arbitrary data to a local file named 'system.conf'
- Execute arbitrary shell commands and send back the output.
- GTPDOOR v2 supports the above operations plus the following:
- Specify IP addresses or subnets allowed to communicate with the compromised host through an Access Control List (ACL) mechanism.
- Retrieve the ACL list to make dynamic adjustments to the backdoor's network permissions.
- Clear ACL to reset the malware.





HaxRob also demonstrates how the virus may be surreptitiously probed from an external network, obtaining a response in the form of a TCP packet sent across any port.

Detection and Defense

Detection techniques include keeping an eye out for anomalous raw socket activity, strange process names, and particular malware signs like several syslog processes.

Here are recommended steps for detection:

1. Check for open raw sockets with lsof, indicating a potential breach.
2. Use netstat -lp --raw to find unusual listening sockets.
3. Identify processes mimicking kernel threads with abnormal PPIDs.
4. Search for /var/run/daemon.pid, a mutex file used by GTPDOOR.
5. Look for an unexpected system.conf file, possibly created by the malware.

```
root        3662       2  0 05:26 ?        00:00:07 [kworker/0:1-events]
root        3756       2  0 07:29 ?        00:00:04 [kworker/1:2-events]
root        3807       2  0 07:29 ?        00:00:00 [kworker/3:1]
root        4005    1935  0 09:31 ?        00:00:00 [syslogd]
root        4024       2  0 09:34 ?        00:00:00 [kworker/2:1-ata_sff]
root        4074       2  0 09:57 ?        00:00:00 [kworker/u8:2-events_unbound]
root        4119       2  0 10:03 ?        00:00:00 [kworker/0:2]
root        4145       2  0 10:09 ?        00:00:00 [kworker/u8:0-events_unbound]
```

Additionally, defenders can use the following YARA rule to find the GTPDOOR virus.

```
rule Linux_Malware_GTPDOOR_v1v2
{
        meta:
                description = "Detects GTPDOOR"
                author = "@haxrob"
                date = "28/02/2024"
                reference = "https://doublepagent.net/telecommunications/backdoor/gtp/2024/02/27/GTPDOOR-COVERT-TELCO-BACKDOOR"
                hash1 = "827f41fc1a6f8a4c8a8575b3e2349aeaba0dfc2c9390ef1cceee1bb85c34161"
                hash2 = "5cbafa2d562be0f5fa690f8d551cdb0bee9fc299959b749b99d44ae1fda782e4"
        strings:
                $s1 = "excute result is" ascii fullword
                $s2 = "idkey not correct" ascii fullword
                $s3 = "send ret message" ascii fullword
        condition:
                uint16(0) == 0x457f and
                2 of them and
                filesize < 20KB
}
```

Lastly, in order to prevent or filter out malicious packets and connections, HaxRob suggests defense strategies including GTP firewalls with stringent regulations and adherence to GSMA security criteria (1, 2).

REFERENCE LINKS

- https://www.bleepingcomputer.com/news/security/americans-lost-record-10-billion-to-fraud-in-2023-ftc-warns/?&web_view=true
- https://www.helpnetsecurity.com/2024/02/09/identity-fraud-growth/?web_view=true
- https://www.darkreading.com/endpoint-security/qr-code-quishing-attacks-execs-email-security?&web_view=true
- https://www.bleepingcomputer.com/news/security/ransomware-payments-reached-record-11-billion-in-2023/
- https://securityaffairs.com/157933/breaking-news/largest-data-leak-ever.html?web_view=true
- https://thehackernews.com/2024/01/tech-giant-hp-enterprise-hacked-by.html?&web_view=true
- https://www.hackread.com/russian-hackers-mail-servers-europe-intel/
- https://thehackernews.com/2024/02/russian-linked-hackers-breach-80.html
- https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-038a
- https://www.bleepingcomputer.com/news/security/chinese-hackers-hid-in-us-infrastructure-network-for-5-years/#google_vignette
- https://blogs.vmware.com/security/2023/06/8base-ransomware-a-heavy-hitting-player.html
- https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-352a
- https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/play-ransomware-volume-shadow-copy
- https://www.trendmicro.com/vinfo/us/security/news/ransomware-spotlight/ransomware-spotlight-play
- https://www.trendmicro.com/en_us/research/24/c/earth-krahang.html?&web_view=true
- https://cyware.com/news/earth-krahang-apt-targets-organizations-worldwide-0f16060d
- https://research.checkpoint.com/2024/magnet-goblin-targets-publicly-facing-servers-using-1-day-vulnerabilities/?web_view=true
- https://thehackernews.com/2024/03/magnet-goblin-hacker-group-leveraging-1.html
- https://www.securityweek.com/magnet-goblin-delivers-linux-malware-using-one-day-vulnerabilities/

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