



AUGUST 2024

Cyber Threat Advisory

Third-party cyberattacks exploit
supplier access to compromise sensitive
information and critical systems.

sdgc.com


Table of Contents

Executive Cyber Risk Rundown	3
Focus of the Month: Ransomware Resurgence	4
Monthly Highlights	5
Ransomware Tracker	9
Articles	10
Velvet Ant: A Detailed Analysis of a Prolonged Cyber Espionage Campaign	10
Emergent Threat: The Rise of RansomHub Ransomware	15
Investigating APT40: Analysis of a Sophisticated Cyber Espionage Campaign	18
Turla: A Master’s Art of Evasion	21
Top Exploited Vulnerabilities	25
Security Bulletin	27
Reference Links	Back Page

Executive Cyber Risk Rundown

CXO Summary

- **Ransomware threats severely rising:** The latest Thales 2024 data threat report states a 47% rise in ransomware attacks with 10% of cases paying out for demands and only 20% having a formal plan in place.
- **Kaspersky to close business in USA:** Russian Cybersecurity company and antivirus software provider Kaspersky Lab will start shutting down operations in the United States on July 20 due to sanctions imposed on its employees for reportedly working in the Russian Tech industry.

 **Fully embracing security automation:** The industry is now beginning to fully embrace the powers of automation in security analysis to protect against regular attacks and lower the investigation time.

- **Embrace third-party cyber risk management:** With supply chains facing cyberattacks, 62% of companies have identified cyber risk management as their top priority in 2024. Financial institutions have also been asked by regulatory bodies to implement this framework.

Ransomware's rising toll: Ransomware payments surged

from **\$1.1 million** in 2020 to **\$1 billion** in 2023.

CRITICAL THREAT ALERT

Focus of the Month: Ransomware Resurgence

Ransomware has seen a major comeback with record-breaking payments and a substantial increase in the scope and complexity of attacks — a significant reversal from the decline observed in 2022.

1. Increased Ransomware Activity
2. Tools and Tactics
3. Rapid Deployment
4. Global Impact

Ransomware actors intensified their operations, targeting high-profile institutions and critical infrastructures, including hospitals, schools, and government agencies. Major ransomware supply chain attacks were carried out exploiting the ubiquitous file transfer software MOVEit, impacting companies ranging from the BBC to British Airways. As a result of these attacks and others, ransomware gangs reached an unprecedented milestone, surpassing \$1 billion in extorted cryptocurrency payments from victims.

Last year's developments highlight the evolving nature of this cyber threat and its increasing impact on global institutions and security at large.

Impact of Ransomware Resurgence

The ransomware threat landscape continues to expand rapidly, making comprehensive tracking and analysis challenging. The volume of ransom payments, often executed in cryptocurrencies, is difficult to quantify precisely. Available data suggests conservative estimates, with the likelihood of underreporting due to the emergence of new ransomware addresses over time.

Geopolitical tensions, such as the Russia-Ukraine conflict, have significantly influenced the ransomware ecosystem. While disrupting some cybercriminal operations, these events have also diverted the focus of certain threat actors towards politically motivated cyberattacks, including espionage and sabotage, rather than solely financial gain.

The frequent rebranding of ransomware groups, particularly those behind high-profile attacks, underscores the dynamic nature of this threat. Despite the proliferation of ransomware strains, the underlying criminal network is relatively smaller than it appears.

The ransomware landscape underwent a dramatic transformation in 2023. Threat actors demonstrated increased sophistication, with a shift towards more aggressive tactics, the rapid spread of Ransomware-as-a-Service (RaaS) models, and accelerated attack execution times. The fluidity of affiliate relationships within the ransomware underworld highlights the constant pursuit of more profitable extortion schemes.



Monthly Highlights

92% of Organizations Hit by Credential Compromise from Social Engineering Attacks

According to a new report by Barracuda, over **92%** of organizations faced an average of six credential compromises due to email-based social engineering attacks in 2023. Scamming and phishing accounted for **86%** of these attacks.

Several notable trends emerged in how attackers use social engineering techniques:

- 1. Conversation Hijacking:** Attackers gain access to business accounts through phishing and then monitor these accounts to understand business operations, deals, and payment procedures. They use this information to craft convincing messages from the compromised domains, tricking victims into wiring money or updating payment information. Although conversation hijacking comprised only **0.5%** of social engineering attacks in 2023, it saw a nearly **70%** increase from 2022.
- 2. Business Email Compromise (BEC):** In these attacks, hackers impersonate executives to deceive employees into transferring money, often via gift cards or wire transfers. BEC made up **10.6%** of social engineering attacks last year, up from **8%** in 2022.
- 3. Extortion:** Hackers threaten to expose sensitive or embarrassing content to victims' contacts unless a ransom is paid.

The report also highlighted the evolving use of legitimate services in these attacks. Gmail was the

most used email domain for social engineering attacks, accounting for **22%** of incidents. Other commonly used free webmail services included Outlook (**2%**), Hotmail (**1%**), iCloud (**1%**), and Mail.com (**1%**), with other domains making up **73%** of attacks. Over **50%** of Gmail attacks were BEC-related, while **43%** were scamming.

Cybercriminals are increasingly using commercial URL shortening services to embed malicious links in phishing emails. These services disguise the true nature and destination of the links, making them appear legitimate. Bit.ly was the most widely used URL shortening service in 2023, appearing in nearly **40%** of attacks with shortened URLs. X (formerly Twitter) was used in **16%** of such attacks, a significant change from 2020, when X's service was used in **64%** of attacks and bit.ly in just **3%**.

Another trend in late 2023 was a rise in QR code phishing attacks, targeting about **5%** of mailboxes in the last quarter. In these attacks, QR codes in phishing emails prompt users to scan the code and visit a fake page mimicking a trusted service or application, often leading to malware downloads or credential theft. QR code attacks are challenging to detect with traditional email filters since they lack embedded links or malicious attachments. These attacks also divert victims from corporate machines to personal devices, such as phones or iPads, which are not protected by corporate security software.

Cyberattacks That Compromise OT Systems Are on the Rise

A survey revealed that **49%** of respondents experienced an intrusion in 2023 that impacted either OT systems only or both IT and OT systems. But this year, **73%** of organizations are being impacted. The survey data also shows a year-over-year increase in intrusions that only impacted OT systems (from **17%** to **24%**). Given the rise in attacks, **46%** of respondents indicate that they measure success based on the recovery time needed to resume normal operations.

As threats grow more sophisticated, the report suggests that most organizations still have blind spots in their environment. Respondents claiming that their organization has complete visibility of OT systems within their central security operations decreased since last year, dropping from **10%** to **5%**.

AT&T Says Hackers Breached 'Nearly All' Customer Data in 2022, Assures Exposed Data Not Publicly Available

AT&T disclosed that a 2022 data breach exposed "nearly all" call and text records of tens of millions of customers. The US telecom giant revealed that from mid-to-late 2022, records of calls and text messages involving tens of millions of its cellphone customers, as well as many non-AT&T customers, were compromised.

The breach affected data including the telephone numbers of "nearly all" of its cellular customers and those of other wireless providers using AT&T's network, covering the period from May 1, 2022, to October 31, 2022. The stolen logs included records of every number AT&T customers called or texted, including those from other networks, detailing the frequency of interactions and call durations. However, the breach did not include the content of calls and text messages, nor the specific times of these communications.

Additionally, AT&T reported that the records of a "very small number" of customers from January 2, 2023, were also compromised. The Federal Communications Commission (FCC) announced on X that they are conducting an ongoing investigation into the AT&T breach and coordinating with law enforcement partners.

For further information on the AT&T breach please go to a detailed advisory issued by SDG:

https://resources.sdgc.com/hubfs/CTA%20Critical%20Alert%207.17.24.pdf?utm_source=hs_email&utm_medium=email&_hsenc=p2ANqtz-8JlzviUiYwrqyplJbYEzxbHPpMXrB2jQL_mQRq5QBbZpUEwSaUyQM32_q4X6VKWKJkk3M1

Quarter of Firms Suffer an API-Related Breach

Digital transformation projects seem to be progressing more rapidly than organizations' efforts to secure them. According to Salt Security, nearly a quarter (**23%**) of organizations admitted to experiencing a breach via production APIs in the past year. The security vendor surveyed 250 individuals from various job roles, industries, and company sizes globally to create its State of API Security Report, 2024.

In addition to breaches, almost all respondents (**95%**) reported encountering API security issues over the past year, including vulnerabilities (**37%**), sensitive data exposure (**38%**), authentication problems (**38%**), denial of service (**21%**), and account misuse (**24%**).

The report noted a 167% increase in the number of APIs over the past year, with two-thirds (**66%**) of respondents managing more than 100 APIs. However, security measures are not being strengthened to handle this growing attack surface. Only **8%** of respondents consider their API security strategy to be "advanced," while nearly two-fifths

(**37%**) do not have a strategy at all. Furthermore, only **58%** have processes in place to discover all APIs in their environment, despite nearly half (**46%**) stating that API security is a topic of discussion at the C-level within their organization.

"Attackers continue to exploit vulnerabilities within APIs to carry out malicious attacks and gain access to company and customer data," said Roey Eliyahu, co-founder and CEO of Salt Security. "As bad actors continuously refine their tactics to discreetly launch API attacks, often through legitimate means, organizations need to adopt a more sophisticated approach to securing APIs. This approach should include robust API discovery capabilities, a governance strategy for API posture, and the ability to quickly and efficiently detect active threats and malicious API traffic."

Only **21%** of respondents believe their current API security measures, such as web app firewalls and API gateways, are effective against attacks. Additionally, **70%** expressed significant concern over "zombie" APIs, up from **54%** in 2023.

Cloud Breaches Impact Nearly Half of Organizations

According to the Thales 2024 Cloud Security Study, nearly half (**44%**) of organizations have experienced a cloud data breach, with **14%** having reported an incident in the past year. The leading causes of these breaches were human error and misconfigurations, occurring in **31%** of cases, a significant decrease from last year's **55%**. Exploitation of known vulnerabilities accounted for **28%** of breaches, a seven-point increase from 2023, while zero-day vulnerabilities were responsible for **24%** of breaches. Additionally, the failure to use multi-factor authentication (MFA) was a factor in **17%** of incidents.

The primary cloud targets identified were SaaS applications (**31%**), cloud storage (**30%**), and cloud management infrastructure (**26%**). Among those targeting cloud management infrastructure, **72%** reported an increase in attacks. The report also highlighted that **66%** of organizations use over 25 SaaS applications, and **47%** of corporate data in the cloud is sensitive, yet less than **10%** of enterprises have encrypted **80%** or more of their cloud data. Nearly half of respondents agreed that managing compliance and privacy is increasingly

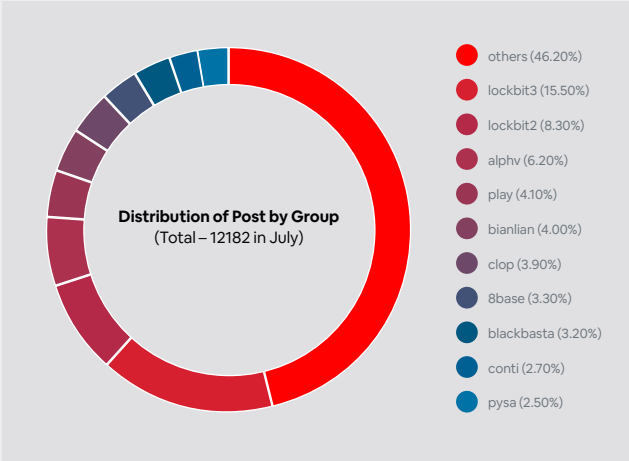
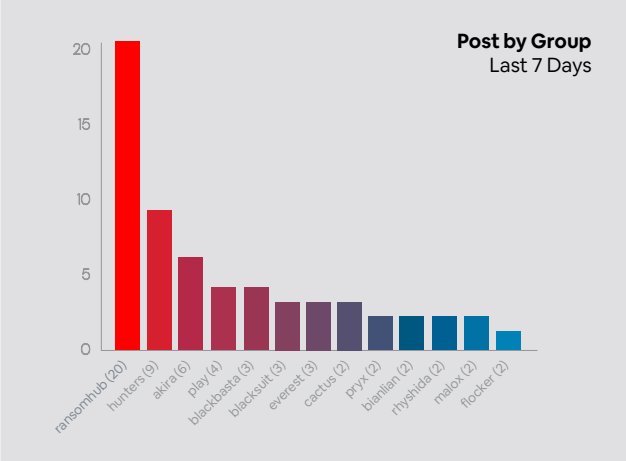
difficult due to cloud complexity, a trend consistent with previous reports.

This complexity also affects encrypted content management, with **53%** of respondents using five or more key management systems, increasing the risk of human error.

Sebastien Cano, Senior Vice President for Cloud Protection and Licensing at Thales, stated, "The scalability and flexibility of the cloud are highly compelling for organizations, making it central to their security strategies." He added, "As the cloud attack surface expands, it's crucial for organizations to understand the data stored in the cloud, the encryption keys in use, and to have visibility into data access and usage. Addressing these challenges is vital, especially as data sovereignty and privacy have become top concerns in this year's research."

Furthermore, **65%** of respondents identified cloud security as a current concern, and it was the top category of security spending for **33%** of all respondents.

Ransomware Tracker

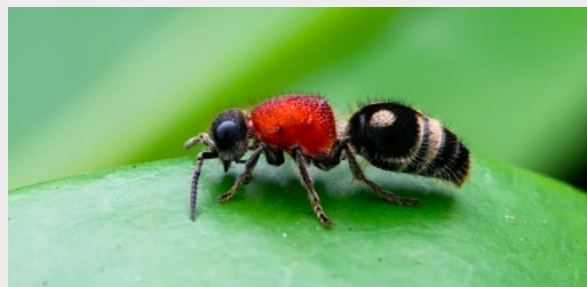


Articles

Velvet Ant: A Detailed Analysis of a Prolonged Cyber Espionage Campaign

Executive Summary

- ✎ **Attack Overview:** In late 2023, Velvet Ant, a Chinese state-sponsored threat actor, infiltrated a major organization.
- ✎ **Duration:** The attackers maintained a presence in the on-premises network for three years.
- ✎ **Primary Goal:** The group focused on espionage, leveraging multiple footholds for prolonged access.
- ✎ **Main Techniques:**
 - Utilized a legacy F5 BIG-IP appliance as an internal Command and Control (C&C) server.
 - Employed PlugX malware, known for its stealthy remote access capabilities.
 - Adapted quickly to remediation efforts, indicating high operational sophistication.



Source: Ryanpictures Via Shutterstock

Detection

Persistent Presence: Velvet Ant established multiple footholds within the network, using a legacy F5 BIG-IP appliance as an internal Command and Control (C&C) server. The PlugX execution chain in this network consisted of three files: 'iviewers.exe', 'iviewers.dll' and 'iviewers.dll.ui'.

Swift Adaptation: Despite remediation efforts, Velvet Ant quickly pivoted to other entry points within the network.

Initial Compromise with PlugX

PlugX Malware: Security researchers identified the use of PlugX, a remote access Trojan. Techniques included DLL search order hijacking and DLL side-loading.

Legacy Systems: The malware was found on systems such as legacy Windows Server 2003 machines, lacking modern Endpoint Detection and Response (EDR) products.

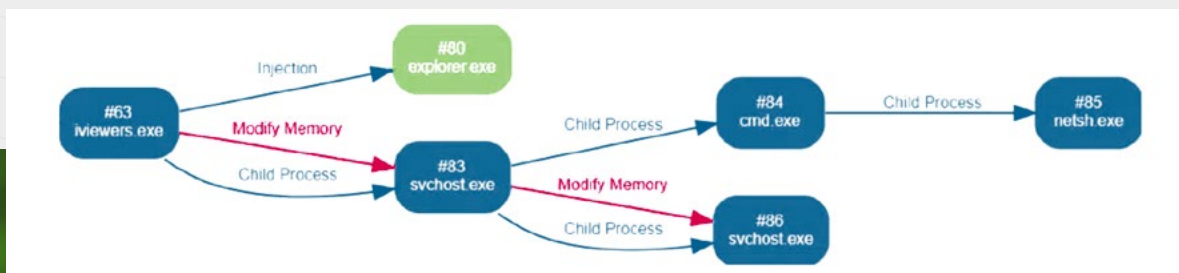


Figure 1. Snippet from VMRay sandbox, showing a process graph for an execution of 'iviewers.exe'.

Persistence and Lateral Movement

Impacket's wmiexec.py: Used for lateral movement and code execution.

Operational Security: Velvet Ant tampered with EDR products before deploying PlugX on newer Windows versions. Memory dumps revealed harvested credentials and executed commands.

Command and Control (C&C) Mechanisms

Initial C&C Server: Velvet Ant used an external C&C server, later blocked by remediation efforts.

Internal C&C Adaptation: After blocking external communications, Velvet Ant used an internal file server, channeled through a compromised F5 load balancer.

F5 BIG-IP Appliance Compromise

Vulnerable Appliances: The organization's outdated F5 BIG-IP appliances were exploited, providing critical network services.

Reverse SSH Tunnel: Forensic analysis revealed reverse SSH tunnel connections to the C&C server, bypassing corporate firewalls.

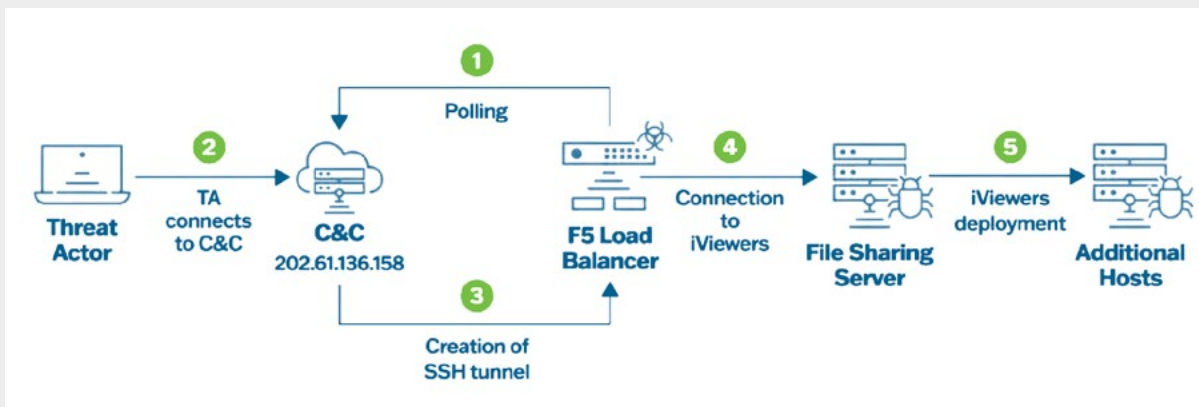


Figure 2. Diagram showing how the F5 appliance was leveraged by the threat actor

Indicators of Compromise

Value	Type	Description
d1e6767900c85535f300e08d76aac9ab	MD5	iviewers.exe
4a0f328e7672ee7ba83f265d48a6077a0c9068d4	SHA1	iviewers.exe
91f6547bcdddfb2f241570ac82c00de700e311e4a38dea60d8619638f1ed3520	SHA256	iviewers.exe
Od5abbe83e5eeb2cb79630caba3a33c7	MD5	iviewers.exe
d80427c922db5fcd8cf490a028915485ff833666	SHA1	iviewers.exe
d663b323d132a3c811bb53a48a686ea85c6bf8faeef3b48dfa93528be8f4133b	SHA256	iviewers.exe
977a7e48f8b05c12249a28dbc4054d78	MD5	iviewers.exe

291bcceef6e03a9f4f0c524f1dd3a4b77d870cd8	SHA1	iviewers.exe
9a7a24b1c785b3c7c39f7e33e99897290165693deaf46ed4f3c7919aef93928	SHA256	iviewers.exe
4cdeffe8c379e6b702f2d22160c59ccf	MD5	iviewers.exe
f07272762b322ceald8cc0845718371flafObd4a	SHA1	iviewers.exe
75fa71e65344b61a80f0e598349b735912be39d04a7e2159748423bd860d3454	SHA256	iviewers.exe
dacfc13d17cda55e58fab7d66d5417d1	MD5	iviewers.exe
37d3665d3b803eaddfad245c0e96172b9c3e8a29	SHA1	iviewers.exe
be852d7a59ba168d93eb975fbed652617046433e6fdc177d0087331f9a095f02	SHA256	iviewers.exe
74a6c8bb6fb08c68d0ff4a6efad64242	MD5	iviewers.exe
2c5d678948938de4d10095db35390c064305413c	SHA1	iviewers.exe
0acc25396ef78c00631c64df538678a323982115bafbf7487a4370d4b4129ac	SHA256	iviewers.exe
cefb71fd132df7fb913ec747080da7c	MD5	iviewers.exe
6003f8042d375ec5c6d56ald6e363e2d2cc9eb67	SHA1	iviewers.exe
859c823eb3e7420e0db234ba224764faa62d391bddd25e9ad415b1ld853741f9	SHA256	iviewers.exe
ababde83c740651f014d9671d4dab557	MD5	iviewers.exe
1fc7b986e55f116d92e77e3b2bee86b720ffa155	SHA1	iviewers.exe
9b9d2da73b510276d38d1698f3b87671958e338b40230e6a004ccaf3dcceb03b	SHA256	iviewers.exe
ad2d2126fe198b35a657804c7cbbf84f	MD5	iviewers.exe
0b400eb4451c3148fa48bc72cb8a84fdcf4461d3	SHA1	iviewers.exe
b4d71b0ac0bc1495789501f9afce6f950b601a36c0836534294640f2db6b2f40	SHA256	iviewers.exe
654349edf1ac14dabce9bec435f06f98	MD5	iviewers.exe
49d2e3dfabd2led4a1lc6fca6236ced7b17fa97e	SHA1	iviewers.exe
3a6a5b1d76dfcac5920e6e9163c08543304ba013425eb2c2e64071b15d26996e	SHA256	iviewers.exe
113779c96c005ac50729462ec1b81f96	MD5	iviewers.exe
e6bd682c47f1a9d564f45a54427100b42e19d2e9	SHA1	iviewers.exe
bdf8a8c7f0298484dc95895dbddf367689ca361618453597129343838b94debb	SHA256	iviewers.exe
0b0b592ec201605503b4a245f024b37c	MD5	iviewers.exe
fc06519154e3a4b28fe16606dec05ec02dd2f647	SHA1	iviewers.exe
7c9336afd7530576b6a0f2e978b36955e8f264fee429d810309ce157a4918aaa	SHA256	iviewers.exe
7266fb2e71fc97036ad642fb592d3444	MD5	iviewers.exe
ca7331e0c8dda90054eb941a2fdd0cc943a04fc4	SHA1	iviewers.exe
c456747731141c2ea0f8e69f89193e8bb823da4667527fe90b614b97f1d425ae	SHA256	iviewers.exe
c5af1894f9806fafc6eae449a4021362	MD5	iviewers.exe
61a382b2139512f8c816ceae93ec823c88bd6eed	SHA1	iviewers.exe

55d6c4a95b5172ea47381ab66ea9ea37fa0afb53b9bb10aid752ac4acc8f6cd4	SHA256	iviewers.exe
52692f03f7c14bc6a6bd35679beb7fab	MD5	iviewers.exe
8e722b2c6b114b69bd71c37759dc3410a32b7594	SHA1	iviewers.exe
527df166af23cd0d139ebad9d219f125137b5a7b619fa50e5e245ccaf8c0b7d6	SHA256	iviewers.exe
b9a46c2960ddbceca5fc4db1a810d92	MD5	iviewers.exe
35e0cbec56e6ad052c3cf53a052b254490995453	SHA1	iviewers.exe
4965f809b71ffb71fe8456d88dcd0a80a99fa6aa4ffd6ba96e1ald810d41bbd0	SHA256	iviewers.exe
805fa6261f5fb268e56fd911fd13e01	MD5	iviewers.exe
7dc223a47fa35011d9e5ed8ef0bbeaf7bd08500f	SHA1	iviewers.exe
b5aa86fd97624a317945d110541a07fc80b83dd960fbf16642720fc275d8f04f	SHA256	iviewers.exe
f0293d80323383dcb494b12ceb313105	MD5	iviewers.exe
0667f44b8dc20d0d1b8f1a5c2fe2f8011204664b	SHA1	iviewers.exe
9092cdd52109531f9f58c28bda25b0c3f82d9bd2d261ce5fcb0137873dbb0868	SHA256	iviewers.exe
3e32bcdcl6db8baf98065b29faeaa18d	MD5	iviewers.exe
86a219232410f236665c51854425fbe5e37b07b3	SHA1	iviewers.exe
bcbcb3184756a6cacfd5ca2b879708cfd015e84050c9b9ede096cfb70282f870c	SHA256	iviewers.exe
5312ba28ce0105cf4563279508bf83fa	MD5	iviewers.exe
3faf065a9987ade102f20dd1ac6b857c7c191b97	SHA1	iviewers.exe
febe116a87860e42bbcf7c6e2c710446f33bdacc56e990f69493837c01f1059	SHA256	iviewers.exe
d8a1805843925a0394d64d1574b15388	MD5	iviewers.exe
2b3b897dd7ef6a54bc038a9afc9d79d5989b6c5f	SHA1	iviewers.exe
7e118a6c4d6f162d8c6a53faf972bd3e675da7f9d0a0b67a1988b4e2102ebb53	SHA256	iviewers.exe
f26edb1d8a61d6bee6da5b5214cce77e	MD5	iviewers.exe
44e2b73f6f5ec010681cblfa5681ca0903f0a080	SHA1	iviewers.exe
cc48a02f06066a37c90d063b6d28ae17d9503e4ba6df69aef1b55b5fa5a5ff48	SHA256	iviewers.exe
9003d7c01c4f2b2e2632a86815eb40a2	MD5	iviewers.exe
ddb59cf25b40273ef0f394c6f164923b6872d7cf	SHA1	iviewers.exe
562974ea1325a88c916a55719fb9263eb6c710ba281fdee4ba7e9a98a3f4a5a8	SHA256	iviewers.exe
ad9267c5c64390d1ed2d6cfa498b5339	MD5	iviewers.dll
1f2e03650afbbd10b9cff21116b7b8d9b192cee3	SHA1	iviewers.dll
92b2535373e55b16b6f3b2d134a1d5545e837d3c19fff4cead4e92558e302b6e	SHA256	iviewers.dll
c5a873b83798a7ad21990eff4c90cb98	MD5	iviewers.dll
3a5ea30f0ff6928a26c4e67352d0adf44dd978da	SHA1	iviewers.dll
a9556cc05422cae960e36f76eeff7168b8e3cfebl6a20855a93d4f2ed4a65a8b	SHA256	iviewers.dll

9f128f604a3e57a92381457e6552f886	MD5	VELVETSTING (PMCD)
ef22dfed358bf35f702af4a14f7a646375123e05	SHA1	VELVETSTING (PMCD)
821d0cdc3e8a735976045ecblafdlc0170bf39701d2da118b9533a45383a9ebe	SHA256	VELVETSTING (PMCD)
d8958e44fa0499a5fbde99b71207184b	MD5	VELVETTAP (MCDP)
553674972e59e7b37a63d19556152b13bf785d71	SHA1	VELVETTAP (MCDP)
436f35dc69bbe7cb8cf5430b52c3aedace099730245de57e004dc1f6531ae262	SHA256	VELVETTAP (MCDP)
2666a1f1f38ba3bd261c908f14d588c7	MD5	ESRDE
0e7c4f374009ff3e264d299dfc1c279bff5b6b4b	SHA1	ESRDE
13f3c05cc348ecb47c4e86dlfb522fdf499a6fb23e0cc6370f4618137f055b04	SHA256	ESRDE
d313dd345d5ea37bc1c431a53d1af91d	MD5	SAMRID
baaa29799bdbb6c1f3fc70e25c0aee4b033f8c8	SHA1	SAMRID
3d9aaac0a8e5c7eadd79d8d5c16119d04f4e9db7107fc44ale32a8746alec375	SHA256	SAMRID
202.61.136[.]158	IP Address	C&C
103.138.13[.]31	IP Address	C&C

Prevention

- **Restrict Outbound Traffic:** Limit outbound connections to prevent C&C communication.
- **Control Lateral Movement:** Implement stringent controls to detect and prevent lateral movement within the network.
- **Update and Patch:** Regularly update and patch all network devices, including legacy systems and appliances.
- **Enhance Monitoring:** Increase monitoring of network traffic and endpoints for unusual activity.

Remediation

- **Identify and Isolate:** Quickly identify compromised systems and isolate them from the network.
- **Clean and Restore:** Clean infected systems and restore them from backups.
- **Continuous Monitoring:** Maintain ongoing monitoring to detect any signs of reinfection or new threats.

Emergent Threat: The Rise of RansomHub Ransomware

Executive Summary

- **Emergence:** RansomHub, a new Ransomware-as-a-Service (RaaS), surfaced in February 2024, becoming a significant threat.
- **Origins:** Likely a rebranded version of the Knight ransomware, utilizing its leaked source code.
- **Impact:** Rapidly grew to become one of the largest ransomware groups, targeting various sectors globally.
- **Technical Details:** Written in Go and C++, targets multiple operating systems including Windows, Linux, and ESXi.
- **Attack Methods:** Uses sophisticated techniques, including exploiting cloud storage backups and vulnerabilities like Zerologon.
- **Attraction:** Offers high commission rates to affiliates, drawing in experienced cybercriminals.



SOURCE: Tripwire.com

```
ransomhub:~# index/ archive/ about/ contact/

About
=====
Our team members are from different countries and we are not interested in anything else, we are only interested in dollars.

We do not allow CIS, Cuba, North Korea and China to be targeted.

Re-attacks are not allowed for target companies that have already made payments.

We do not allow non-profit organizations to be targeted.
```

Figure 2. RansomHub's About Page

RansomHub's Growth and Affiliates

Expansion: Despite its recent emergence, RansomHub quickly became the fourth most prolific ransomware operator within three months, partly by attracting affiliates from defunct groups like Noberus (BlackCat).

Victim Profile: Targets high-value sectors such as IT, leveraging high commission rates (up to 90%) to recruit seasoned affiliates.

Notable Incidents: Involved in high-profile attacks, including a significant data breach at Change Healthcare, showcasing its capacity to handle and exploit large volumes of stolen data.

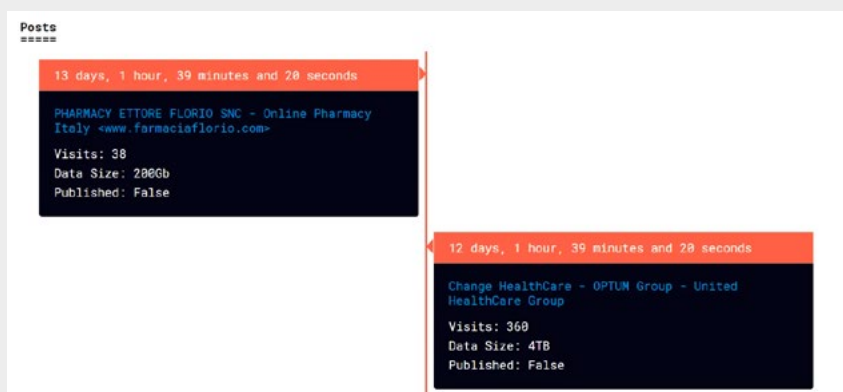


Figure 3. Snippet from RansomHub's Victim Listing Page

Detection

Initial Indicators:

- Infections often begin with the exploitation of known vulnerabilities like Zerologon (CVE-2020-1472).
- Common tools used include Atera, Splashtop for remote access, and NetScan for network reconnaissance.
- Command-line activities include stopping IIS services with `iisreset.exe /stop``.

Technical Similarities:

- High code overlap with Knight ransomware.
- Uses unique obfuscation techniques where critical strings are encoded with unique keys and decoded at runtime.
- Nearly identical command-line help menus with minor differences such as the addition of a sleep command in RansomHub.

Ransom Notes:

- Similar in phrasing to Knight's notes, indicating minimal changes from the original text.

Indicators of Compromise

SHA-256 hash	Description
02e9f0fbb7f3acea4fcf155dc7813e15c1c8d1c77c3ae31252720a9fa7454292	RansomHub
34e479181419efd0c00266bef0210f267beaa92116e18f33854ca420f65e2087	RansomHub
7539bd88d9bb42d280673b573fc0f5783f32db559c564b95ae33d720d9034f5a	RansomHub
8f59b4f0f53031c555ef7b2738d3a94ed73568504e6c07aaf3fa3f1fd786de7	RansomHub
ea9f0bd64a3ef44fe80ce1a25c387b562a6b87c4d202f24953c3d9204386cf00	RansomHub
104b22a45e4166a5473c9db924394e1fe681ef374970ed112edd089c4c8b83f2	Knight
2f3d82f7f8bd9ff2f145f9927belab16f8d7d61400083930e36b6b9ac5bbe2ad	Knight
36e5be9ed3ec960b40b5a9b07ba8e15d4d24ca6cd51607df21ac08cda55a5a8e	Knight
595cd80f8c84bc443eff619add01b86b8839097621cdd148f30e7e2214f2c8cb	Knight
7114288232e469ff368418005049cf9653fe5c1cdcfcd63d668c558b0a3470f2	Knight
e654ef69635ab6a2c569b3f8059b06aee4bce937afb275ad4ec77c0e4a712f23	Knight
fb9f9734d7966d6bcl5cce5150abb63aadd4223924800f0b90dc07a311fb0a7e	NetScan
f1a6e08a5fd013f96facc4bb0d8dfb6940683f5bdfc161bd3a1de8189dea26d3	Splashtop
a96a0ba7998a6956c8073b6eff9306398cc03fb9866e4cabf0810a69bb2a43b2	Atera

Prevention

Network Security:

- Segment networks to prevent lateral movement.
- Implement robust endpoint detection and response (EDR) systems with YARA and Sigma rules.

Access Controls:

- Enforce least privilege access and multi-factor authentication for remote access.
- Regularly audit and patch systems to close vulnerabilities.

Backup Strategies:

- Regularly back up critical data and store it offline or in isolated segments.
- Evaluate and ensure secure configurations of cloud storage and backup solutions.

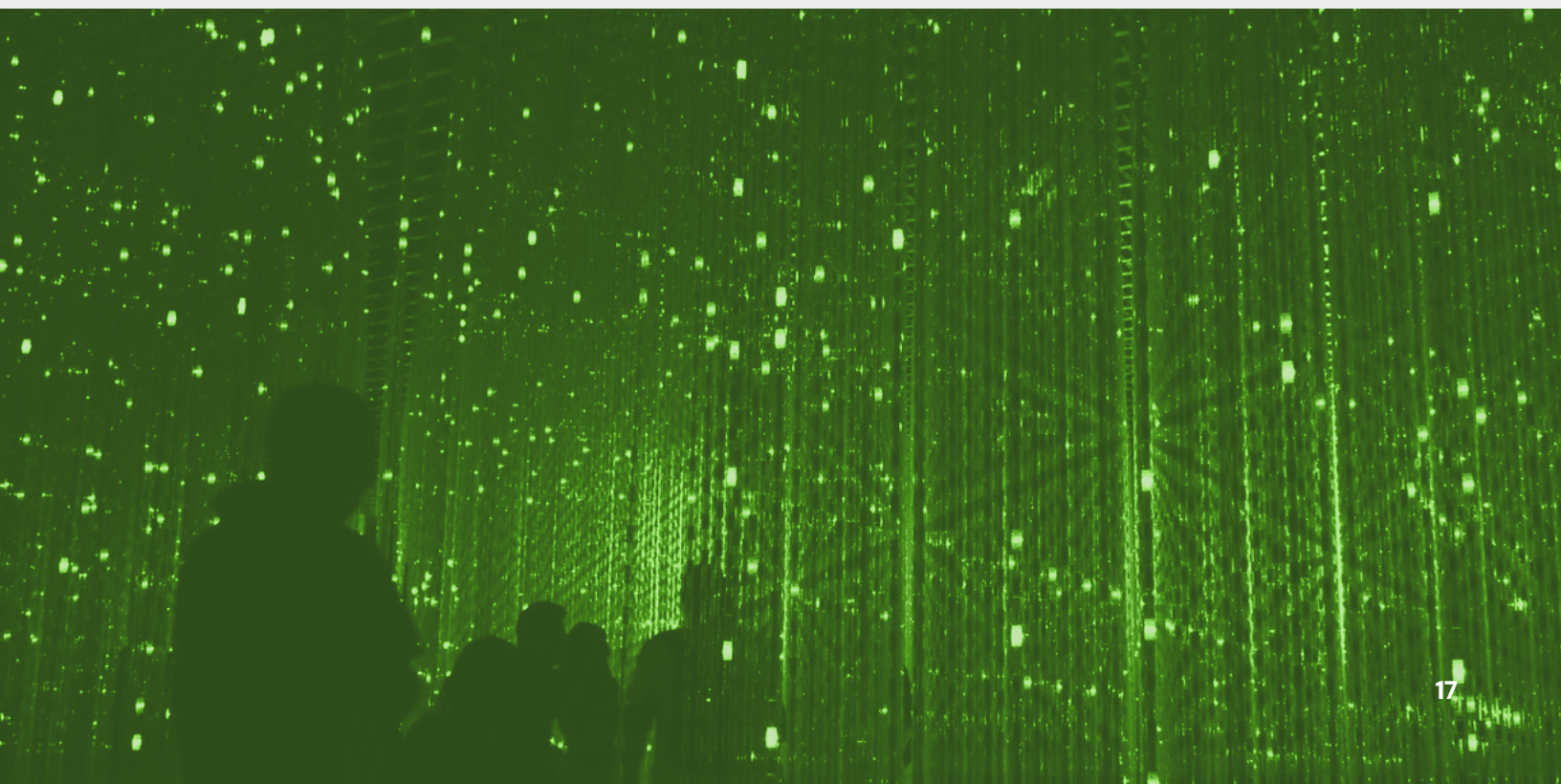
Remediation

Incident Response:

- Isolate infected systems immediately to prevent further spread.
- Use SIEM systems for centralized logging and real-time threat detection.
- Employ network isolation techniques to limit the ransomware's impact.

Recovery:

- Restore systems from clean, verified backups.
- Conduct a thorough investigation to understand the breach and prevent future incidents.



Investigating APT40: Analysis of a Sophisticated Cyber Espionage Campaign

Executive Summary

- **Attack Overview:** APT40 compromised the organization's network through vulnerabilities in the remote access login portal, exploiting them for extensive data exfiltration.
- **Duration:** Initial compromise detected in April 2022; ongoing persistence and lateral movement until May 2022.
- **Primary Goal:** Gain unauthorized access to sensitive corporate resources and data for espionage purposes.
- **Main Techniques:**
 - Exploitation of remote code execution (RCE) vulnerabilities in internet-facing applications.
 - Use of web shells and compromised credentials for command execution and persistence.
 - Collection of hundreds of legitimate username-password pairs and multi-factor authentication (MFA) tokens.

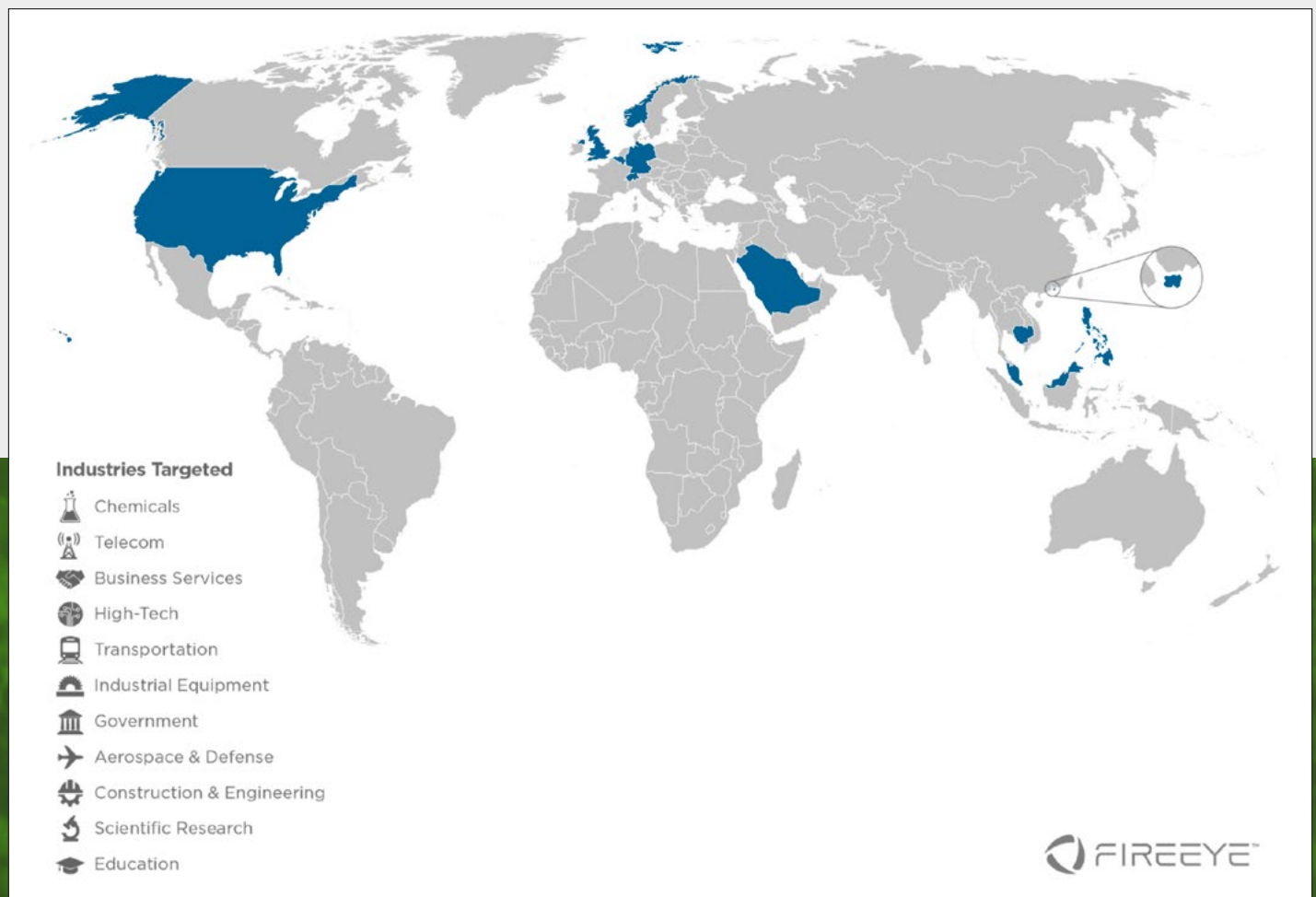


Figure 1. Countries and industries targeted by APT 40

Detection

Host Enumeration: APT40 mapped the organization's network to identify targets for exploitation.

Exploitation: Initial access gained through exploitation of RCE vulnerabilities in the compromised remote access login portal.

Credential Harvesting: Captured hundreds of username–password pairs and MFA tokens, leveraging compromised authentication processes.

Initial Compromise

RCE Exploitation: APT40 exploited known vulnerabilities in the remote access login portal to establish initial access.

Web Shell Deployment: Utilized web shells for command execution and persistence on compromised appliances.

Persistence and Lateral Movement

Web Shell Usage: Deployed multiple web shells on compromised appliances for persistent access and command execution.

Credential Abuse: Leveraged captured credentials to move laterally across the network, including mounting SMB shares.



Figure 2: TTP Flowchart for APT40 activity

Command and Control (C&C) Mechanisms

Web Shell Communication: Used web shells over HTTPS for command and control operations.

Credential Theft: Captured JWTs and other authentication artifacts to maintain unauthorized access.

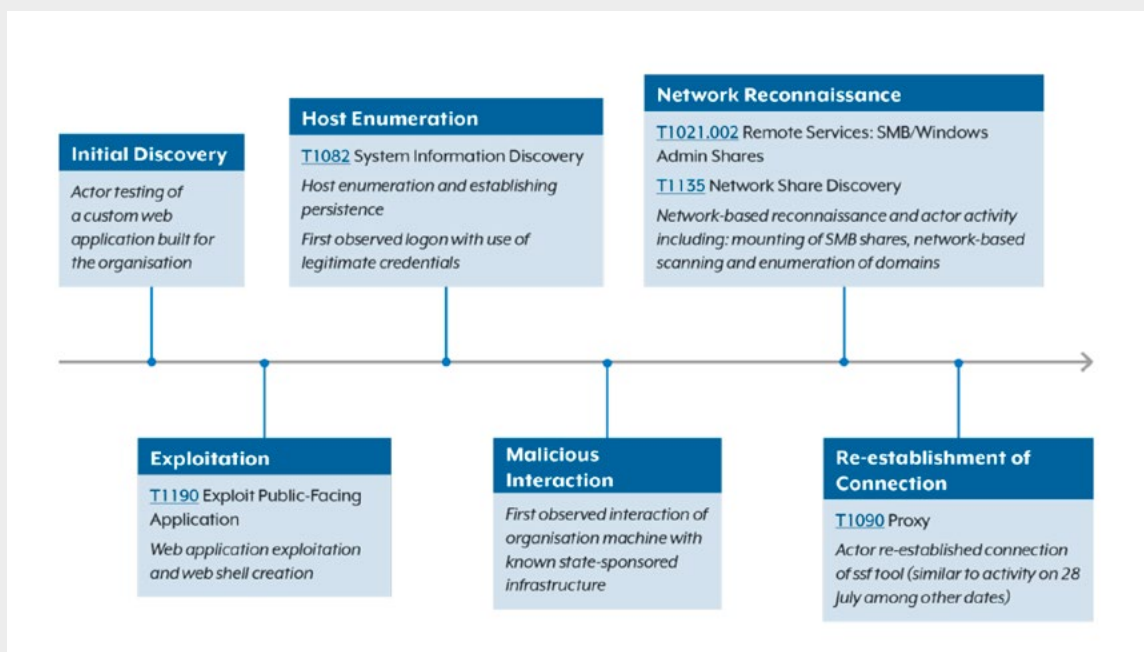


Figure 3. The above timeline provides a broad overview of the key phases of malicious actor activity observed on the victim organization's network.

Prevention

Patch Management: Promptly apply patches to internet-facing servers and applications to mitigate known vulnerabilities.

Network Segmentation: Segment networks to restrict lateral movement and isolate critical services.

Enhanced Monitoring: Implement comprehensive logging and monitoring to detect anomalous activities and potential compromises.

Use of MFA: Enforce multi-factor authentication (MFA) for all remote access services to mitigate credential theft.

Remediation

Incident Response: Quickly identify and isolate compromised hosts to prevent further spread.

System Cleanup: Clean infected systems and restore from secure backups to eliminate malicious presence.

Continuous Monitoring: Maintain ongoing monitoring to detect any signs of reinfection or new attack attempts.

Turla: A Master's Art of Evasion

In a system, a shortcut file is a reference in the user interface that gives the user the convenience of executing a file or resource that is in a different folder. But what if it becomes a weapon in the hands of threat actors? On May 9, 2024, GDATA analysts noticed what may be a new campaign using a malicious shortcut file that takes advantage of Microsoft's application development platform to introduce a fileless backdoor into the machine.

To further strengthen its ability to evade, it also uses memory patching, gets around AMSI, and turns off the system's event logging features. Since they were involved in one of the initial analyses of this malware, which originated in Russia, more than ten years ago, G DATA researchers are familiar with Turla, also going by other names like "Uroburos."

About Uroburos

An encrypted virtual file system and a driver make up the rootkit known as Uroburos. A machine that has been infected can be taken over by the rootkit, which can also conceal system activity and run random commands. Not only can it intercept network traffic, but it can also steal data, most notably files. It is not only extremely sophisticated but also extremely flexible and dangerous due to its modular structure, which makes adding new features easy. The driver component of a robot is incredibly intricate, discrete, and challenging to identify.

Detection

A feature of Uroburos is its peer-to-peer mode of operation; compromised machines can communicate with one another under the direction of remote attackers.

The malware can infect additional machines in the network, even those without an Internet connection, by taking control of one compromised machine. By relaying the exfiltrated data through the infected devices to a single machine with an Internet connection, it can spy on every single compromised machine and send the information back to the attackers.

This type of malware propagation behavior is common in networks belonging to large corporations or government agencies. The attackers employ this tactic as a sort of workaround because they anticipate that their target's computers are disconnected from the Internet.

Microsoft Windows 32- and 64-bit systems are supported by Uroburos. We believe that this rootkit is intended for use against governments because of the intricacy of the malware and the purported spying methods it employs.

Technical Analysis

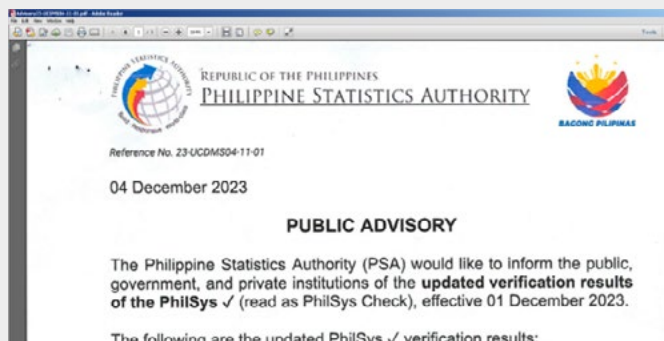
Upon entering the system, the malicious shortcut file assumes the appearance of a typical PDF document shortcut file. The reference number of the Philippine Statistic Authority (PSA) Public Advisory is represented by the filename Advisory23-USDMSO4-11-01.pdf.lnk. National accounts compilation, as well as all national surveys and censuses, are within the purview of the PSA.

The malicious shortcut file will cause a PowerShell script to run, dropping the following files when it is executed:

%temp%\ChromeConnection

%temp%\ Advisory23-USDMSO4-11-01.pdf

The PSA Public Advisory is contained in the benign file Advisory23-USDM504-11-01.pdf, as seen in the figure below:



This paper serves as a ruse to draw attention away from the malicious actions that ChromeConnection is carrying out in the background. Executed file is a malicious MSBuild project file that a PowerShell script will trigger, causing msbuild.exe to load it.

The project file indicates that the assembly file is in the Microsoft.Net Framework64 directory, which means it will only function on 64-bit operating systems. The malware's persistence mechanism involves creating a scheduled task as soon as the project file "ChromeConnection" is executed using msbuild.exe:

```
/create /sc MINUTE /mo 30 /st 07:00:00
/tn "ChromeConnection" /tr "cmd /c
start /min %windir%\Microsoft.NET\
Framework64\v4.0.30319\MSBuild %temp%\
ChromeConnection" /f
```



An MSIL-compiled binary serves as the backdoor. It is safeguarded by a potent obfuscation tool called SmartAssembly, which guards against reverse engineering and disassembly. Additionally, some of its codes are hidden, which is part of its anti-debugging techniques.

About Backdoor

When the system's Event Tracing for Windows (ETW) is disabled, backdoors like this one can avoid detection. It is possible to track and record events produced by kernel-mode drivers and user-mode applications with this feature.

As a part of its anti-detection strategy, the backdoor also patches memory on a few of the in-memory system module components. The manipulation of Windows Antimalware Scan Interface (AMSI), a security feature that allows programs and services to interact with any antimalware program installed on a system, is another aspect of this plan.

Using various URLs, a connection is made to its command and control server (c2 server). The malicious software will first connect to the following URL:

[hxxp://files.philbendeck.com/file/<computed string encoded ID>.jsp](https://files.philbendeck.com/file/<computed string encoded ID>.jsp)

This URL leads to a compromised personal website of an individual. Depending on the server's response, this connection will check if the backdoor's operation continues uninterrupted.

Backdoor Commands

The following actions are carried out by the PowerShell runspace that ps creates:

- Disables the ETW to turn off the system's event-related features.
- Disables event-related module functions with memory patching of in-memory system module components.
- Disables the AMSI scan feature by memory patching the in-memory amsi.dll.
- Runs a script in PowerShell that you downloaded from the server.
- Shuts down PowerShell runspace.
- Reports the backdoor's timeout, reconnects, and sleeps.
- Generates a file with the username as the filename, in which the content is downloaded from the server.

The URL `hxxp://files.philbendeck.com/article/.jsp` will receive all these logs.

Indicators of Compromise

SHA256	Filename
cac4d4364d20fa343bf681f6544b31995a57d8f69ee606c4675db60be5ae8775	Advisory23-CDMS04-11-01.pdf.lnk
c2618fb013135485f9f9aa27983df3371dfdc7beecde86d02cee0c258d5ed7f	Advisory23-UCDMS04-11-01.pdf.zip
b6abbab6e000036c6cdfc57c096d796397263e280ea264eba73ac5bab39441	ChromeConnection
7091ce97fb5906680c1b09558bafdf9681a81f5f524677b90fd0f7fc0a05bc00	None (extracted embedded binary)

URL	Description
<code>hxxps://ies.inquirer.com.ph/advprod03/assets/images/Advisory23-UCDMS04-11-01.zip</code>	Origin of the malicious lnk file's package
<code>hxxp://files.philbendeck.com/file/<computed string encoded ID>.jsp</code>	malware server used for connection verification
<code>hxxp://files.philbendeck.com/help/<computed string encoded ID>.jsp</code>	malware server used for backdoor commands
<code>hxxp://files.philbendeck.com/article/<computed string encoded ID>.jsp</code>	malware server used for reporting of disabling system event features and script execution result
<code>hxxp://files.philbendeck.com/about/<computed string encoded ID>.jsp</code>	malware server used for reporting of time of malware's reconnection, sleep and receive timeout

Prevention

- Set the PowerShell execution policy to run only scripts that have been signed.
- PowerShell can be uninstalled from systems when it's not needed, but since it can be used for a variety of acceptable reasons and administrative tasks, an evaluation should be done to determine the environmental impact.
- To aid in preventing the use of PowerShell for remote execution, disable or restrict the WinRM Service.
- If MSBuild.exe is not being used, it may not be required in the environment and must be deleted.
- If msbuild.exe is not needed for a particular system or network, use application control setup to prevent its execution from happening to stop potential adversary abuse.

Remediation

- Use Microsoft Defender XDR to find ransomware attacks that are operated by humans.
- Turn on restricted folder access.
- Verify that Microsoft Defender for Endpoint has tamper protection turned on.
- Activate Microsoft Defender for Endpoint's network protection.
- To prevent common credential theft methods like LSASS access, adhere to the credential hardening advice in our overview of on-premises credential theft.
- Set up a fully automated mode for investigation and remediation to enable Microsoft Defender for Endpoint to respond quickly to alerts and address breaches, thereby lowering the volume of alerts.
- Activate endpoint detection and response (EDR) in block mode to enable Microsoft Defender for Endpoint to stop malicious artifacts even if your non-Microsoft antivirus program is in passive mode or fails to identify the threat.
- Activate cloud-delivered protection in Microsoft Defender Antivirus or its equivalent.

Top Exploited Vulnerabilities

Vulnerability Name	Description	References
Parse Server literalizeRegexPart SQL Injection Information Disclosure Vulnerability CVE-2024-27298	Vulnerability allows remote attackers to disclose sensitive information on affected installations of Parse Server. The issue results from the lack of proper validation of a user-supplied string before using it to construct SQL queries.	https://github.com/parse-community/parse-server/security/advisories/GHSA-6927-3vr9-fxf2
Centreon testServiceExistence SQL Injection Remote Code Execution Vulnerability CVE-2024-39841	Vulnerability allows remote attackers to execute arbitrary code on affected installations of Centreon. Issue results from the lack of proper validation of a user-supplied string before using it to construct SQL queries.	https://vulmon.com/vulnerabilitydetails?qid=CVE-2024-39841
ESET Smart Security Premium Link Following Local Privilege Escalation Vulnerability CVE-2024-2003	Vulnerability allows local attackers to escalate privileges on affected installations of ESET Smart Security Premium. An attacker can leverage this vulnerability to escalate privileges and execute arbitrary code in the context of SYSTEM.	https://support.eset.com/en/ca8674-link-following-local-privilege-escalation-vulnerability-in-quarantine-of-eset-products-for-windows-fixed
Trend Micro Apex One modOSCE SQL Injection Remote Code Execution Vulnerability CVE-2024-39753	Vulnerability allows remote attackers to execute arbitrary code on affected installations of Trend Micro Apex One. An attacker can leverage this in conjunction with other vulnerabilities to execute code in the context of IUSR.	https://success.trendmicro.com/dcx/s/solution/000298063?language=en_US
Parse Server literalizeRegexPart SQL Injection Authentication Bypass Vulnerability CVE-2024-39309	Vulnerability allows remote attackers to bypass authentication on affected installations of Parse Server. The issue results from the lack of proper validation of a user-supplied string before using it to construct SQL queries.	https://github.com/parse-community/parse-server/security/advisories/GHSA-c2hr-cqg6-8j6r
Progress Software WhatsUp Gold CommunityController Unrestricted File Upload Remote Code Execution Vulnerability CVE-2024-4884	Vulnerability allows remote attackers to execute arbitrary code on affected installations of Progress Software WhatsUp Gold. The issue results from the lack of proper validation of user-supplied data, which can allow the upload of arbitrary files.	https://community.progress.com/s/article/WhatsUp-Gold-Security-Bulletin-June-2024
Zen Cart findPluginAdminPage Local File Inclusion Remote Code Execution Vulnerability CVE-2024-5762	Vulnerability allows remote attackers to execute arbitrary code on affected installations of Zen Cart. The issue results from the lack of proper validation of user-supplied data prior to passing it to a PHP include function.	https://docs.zen-cart.com/release/whatsnew_2.0.0
VMware vCenter Server Appliance License Server Uncontrolled Memory Allocation Denial-of-Service Vulnerability CVE-2024-37087	Vulnerability allows remote attackers to create a denial-of-service condition on affected installations of VMware vCenter Server Appliance. The issue results from the lack of proper validation of user-supplied data, which can result in an uncontrolled memory allocation.	https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/24505
(Pwn2Own) Ubiquiti Networks EV Station changeUserPassword Missing Authentication Remote Code Execution Vulnerability CVE-2024-29208	Vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of Ubiquiti Networks EV Station. The issue results from the lack of proper validation of the old password before setting a new password.	https://community.ui.com/releases/Security-Advisory-bulletin-039-039/44e24007-2c2c-4ac0-bebf-3f19b9b24f09
(Pwn2Own) Sony XAV-AX5500 WMV/ASF Parsing Stack-based Buffer Overflow Remote Code Execution Vulnerability CVE-2024-23934	Vulnerability allows remote attackers to execute arbitrary code on affected installations of Sony XAV-AX5500 devices. A crafted Extended Content Description Object in a WMV media file can trigger an overflow of a fixed-length stack-based buffer.	https://www.sony.com/electronics/support/mobile-cd-players-digital-media-players-xav-series/xav-ax5500/software/00274156
(Pwn2Own) Silicon Labs Gecko OS HTTP GET Request Handling Stack-based Buffer Overflow Remote Code Execution Vulnerability CVE-2024-23973	Vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of Silicon Labs Gecko OS. The specific flaw exists within the handling of HTTP GET requests.	https://community.silabs.com/a45Vm0000000Atp
(Pwn2Own) Phoenix Contact CHARX SEC-3100 ClientSession Use-After-Free Remote Code Execution Vulnerability CVE-2024-26005	Vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of Phoenix Contact CHARX SEC-3100 devices. The specific flaw exists within the handling of ClientSession objects in the CharxControllerAgent service.	https://cert.vde.com/en/advisories/VDE-2024-011/
(Pwn2Own) Autel MaxiCharger AC Elite Business C50 DLB_HostHeartBeat Stack-based Buffer Overflow Remote Code Execution Vulnerability CVE-2024-23957	Vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of Autel MaxiCharger AC Elite Business C50 charging stations. Authentication is not required to exploit this vulnerability. The specific flaw exists within the DLB_HostHeartBeat handler of the DLB protocol implementation.	https://vuldb.com/?id.269461

Top Exploited Vulnerabilities

Vulnerability Name	Description	References
(Pwn2Own) Alpine Halo9 prh_l2_sar_data_ind Use-After-Free Remote Code Execution Vulnerability CVE-2024-23923	Vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of Alpine Halo9 devices. The issue results from the lack of validating the existence of an object prior to performing operations on the object.	https://www.tenable.com/cve/CVE-2023-23923
Linux Kernel ICMPv6 Router Advertisement Race Condition Remote Code Execution Vulnerability CVE-2023-6200	Vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of Linux Kernel. The issue results from the lack of proper locking when performing operations on an object.	https://bugzilla.redhat.com/show_bug.cgi?id=2250377
(Pwn2Own) Wyze Cam v3 Realtek Wi-Fi Driver Heap-Based Buffer Overflow Remote Code Execution Vulnerability CVE-2024-6246	Vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of Wyze Cam v3 IP cameras. The specific flaw exists within the Realtek Wi-Fi kernel module.	https://forums.wyze.com/t/security-advisory/289256
(Pwn2Own) Synology BC500 synocam_param.cgi Stack-based Buffer Overflow Remote Code Execution Vulnerability CVE-2024-39349	Vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of Synology BC500 cameras. The specific flaw exists within the synocam_param.cgi module.	https://www.synology.com/en-id/security/advisory/Synology_SA_23_15
(Pwn2Own) Samsung Galaxy S23 Instant Plays Improper Input Validation Remote Code Execution Vulnerability CVE-2023-42581	Vulnerability allows remote attackers to execute arbitrary code on affected installations of Samsung Galaxy S23 smartphones. The specific flaw exists within the implementation of the samsungapps URI scheme. The issue results from a logical error when checking the safety of URIs.	https://security.samsungmobile.com/serviceWeb.smsb?year=2023&month=12
(Pwn2Own) QNAP TS-464 Improper Validation Authentication Bypass Vulnerability CVE-2024-32766	Vulnerability allows remote attackers to bypass authentication on affected installations of QNAP TS-464 NAS devices. The specific flaw exists within the authentication logic. The issue results from improper validation of the password.	https://www.qnap.com/en-us/security-advisory/qlsa-24-09
(Pwn2Own) HP Color LaserJet Pro MFP 4301fdw CFF Parsing Stack-based Buffer Overflow Remote Code Execution Vulnerability CVE-2024-0794	Vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of HP Color LaserJet Pro MFP 4301fdw printers. The issue results from the lack of proper validation of the length of user-supplied data prior to copying it to a fixed-length stack-based buffer.	https://support.hp.com/us-en/document/ish_10174031-10174074-16/hpsbpi03917
Windscribe Directory Traversal Local Privilege Escalation Vulnerability CVE-2024-6141	Vulnerability allows local attackers to escalate privileges on affected installations of Windscribe. An attacker must first obtain the ability to execute low-privileged code on the target system to exploit this vulnerability.	https://github.com/Windscribe/Desktop-App/blob/90a5cc3c1f50f6545f83969c2ace6b4ac2c91c4e/client/common/changelog.txt#L23
VIPRE Advanced Security Incorrect Permission Assignment Local Privilege Escalation Vulnerability CVE-2024-5930	Vulnerability allows local attackers to escalate privileges on affected installations of VIPRE Advanced Security. The specific flaw exists within the Anti Malware Service.	https://success.vipre.com/en_US/home-windows-release-notes/home-windows-release-notes-20240227
Microsoft Windows Menu DC Bitmap Use-After-Free Local Privilege Escalation Vulnerability CVE-2024-30082	Vulnerability allows local attackers to escalate privileges on affected installations of Microsoft Windows. An attacker must first obtain the ability to execute low-privileged code on the target system to exploit this vulnerability. The specific flaw exists within the win32kfull driver.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-30082
Toshiba e-STUDIO2518A unzip Directory Traversal Remote Code Execution Vulnerability CVE-2024-3497	Vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of Toshiba e-STUDIO2518A printers. The specific flaw exists within the unzip method.	https://www.toshibatec.com/information/20240531_01.html

Security Bulletin

The notorious FIN7 hacking group has been spotted selling its custom “AvNeutralizer” tool, used to evade detection by killing enterprise endpoint protection software on corporate networks. “AvNeutralizer uses a combination of drivers and operations to create a failure in some specific implementations of protected processes, ultimately leading to a denial-of-service condition,” explains SentinelOne.

Malicious actors have demonstrated that AI can be weaponized for cyberattacks. In 2023, we witnessed new techniques for penetrating systems and outsmarting cyber defenses which continue to mature in 2024. Examples of such methods include highly deceptive phishing emails, deep fake recordings, and other fraudulent documents.

Top recommended controls:

1. **AI technology and machine learning to recognize anomalies and threats.**
2. **Automated monitoring and alerting.**
3. **Automated penetration testing.**

Prudential Financial, a global financial services company, has revealed that over 2.5 million people had their personal information compromised in a February data breach. Prudential is the second-largest life insurance company in the United States, with 40,000 employees worldwide and reported revenues of over \$50 billion in 2023. In May 2023, the personal information of an additional 320,000 Prudential customers—including names, addresses, dates of birth, phone numbers, and Social Security numbers—was also exposed after the Clop cybercrime gang hacked into the MOVEit Transfer file-sharing platform of Pension Benefit Information (PBI), a third-party vendor handling the data.

The Cybersecurity and Infrastructure Security Agency (CISA), National Security Agency (NSA), and Federal Bureau of Investigation (FBI) assess that People’s Republic of China (PRC) state-sponsored cyber actors are seeking to pre-position themselves on IT networks for disruptive or destructive cyberattacks against U.S. critical infrastructure in the event of a major crisis or conflict with the United States.

CISA, NSA, FBI and the following partners are releasing this advisory to warn critical infrastructure organizations about this assessment, which is based on observations from the U.S. authoring agencies’ incident response activities at critical infrastructure organizations that have been compromised by the PRC state-sponsored cyber group known as Volt Typhoon (also known as Vanguard Panda, BRONZE SILHOUETTE, Dev-O391, UNC3236, Voltzite, and Insidious Taurus)

Reference Links

1. <https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-038a>
2. <https://www.bleepingcomputer.com/news/security/notorious-fin7-hackers-sell-edr-killer-to-other-threat-actors/>
3. <https://bleepingcomputer.com/news/security/prudential-financial-now-says-25-million-impacted-by-data-breach/>
4. <https://www.hindustantimes.com/world-news/us-news/att-says-hackers-breached-nearly-all-customer-data-in-2022-assures-exposed-data-not-publicly-available-101720820377786.html>
5. <https://ransomwatch.telemetry.ltd/>
6. https://www.helpnetsecurity.com/2024/07/05/cloud-environments-security-priority/?web_view=true
7. https://www.infosecurity-magazine.com/news/cloud-breaches-half-organizations/?&web_view=true
8. https://www.infosecurity-magazine.com/news/quarter-firms-suffer-api-related/?&web_view=true
9. https://www.infosecurity-magazine.com/news/credential-compromise-social/?&web_view=true
10. https://www.cybersecuritydive.com/news/mfa-multi-factor-authentication-cisco-talos-cyber/719254/?&web_view=true
11. https://www.gdatasoftware.com/blog/2024/07/37977-turla-evasion-lnk-files?&web_view=true

About SDG

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

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



■ 75 North Water Street, Norwalk, CT 06854
■ 203.866.8886
■ sdgc.com