Cyber Threat Advisory

FEBRUARY 2024

Contents

Monthly Highlights - February

1. **Uncovering UAC-0050: Advanced Phishing Tactics Unleash Remcos RAT** – The threat actor identified as UAC-0050 is employing sophisticated phishing tactics to distribute the Remcos RAT, showcasing a high level of adaptability and evasiveness against security measures. In a recent report by Uptycs security researchers Karthickkumar Kathiresan and Shilpesh Trivedi, the group's utilization of the Remcos RAT, a well-known tool for remote surveillance and control, was highlighted as a key component of their espionage operations. Their latest innovation includes the incorporation of a pipe method for inter-process communication, underscoring their advanced capabilities.

   Originating in 2020, UAC-0050 has primarily targeted Ukrainian and Polish entities through social engineering schemes that impersonate legitimate organizations, enticing victims to open malicious attachments. In February 2023, the Computer Emergency Response Team of Ukraine (CERT-UA) linked the group to a phishing campaign aimed at delivering the Remcos RAT. Subsequently, multiple phishing waves have been observed distributing this trojan, with one instance leading to the deployment of the information-stealing malware Meduza Stealer.

   Uptycs' analysis, triggered by the discovery of an LNK file in December 2023, revealed insights into the group's modus operandi. While the exact initial access vector remains undisclosed, suspicions point towards phishing emails targeting Ukrainian military personnel, falsely advertising consultancy roles with the Israel Defense Forces (IDF). The identified LNK file initiates a sequence of actions,

including gathering information about installed antivirus products, retrieving and executing an HTML application from a remote server, and ultimately launching the Remcos RAT.

Upon execution, the Remcos RAT exhibits persistence by creating a duplicate named fmTask_dbg.exe and establishing a shortcut in the Windows Startup folder. Leveraging unnamed pipes for data exchange between processes, the RAT successfully evades detection by antivirus and Endpoint Detection and Response (EDR) systems. This variant of Remcos (version 4.9.2 Pro) is capable of extensive data exfiltration, including system information and login credentials from popular web browsers.

The utilization of covert channels within the Windows operating system highlights UAC-0050's adeptness at circumventing security measures, posing a significant threat to targeted organizations. With their evolving tactics and reliance on sophisticated malware like Remcos, vigilance and robust security protocols are imperative to thwarting their malicious activities.

2. **HealthEC Data Breach Exposes 4.5 Million Individuals to Potential Identity Theft** – HealthEC LLC, a prominent provider of health management solutions, recently fell victim to a significant data breach affecting approximately 4.5 million individuals who received care through one of the company's clients. Specializing in population health management (PHM), HealthEC offers a comprehensive platform for healthcare organizations, encompassing data integration, analytics, care coordination, patient engagement, compliance, and reporting.

   The breach, occurring between July 14 and 23, 2023, came to light on December 22 when the company disclosed unauthorized access to some of its systems. Following an investigation that concluded on October 24, 2023, it was determined that the intruder had accessed files containing sensitive information. The compromised data included personal details such as names, addresses, dates of birth, Social Security numbers, taxpayer identification numbers, medical record numbers, and extensive medical and health insurance information including diagnoses, prescription details, and billing information.

   In response to the breach, HealthEC issued notifications urging affected individuals to remain vigilant against identity theft and fraud. Recommendations included reviewing account statements, explanation of benefits statements, and monitoring free credit reports for any suspicious activity or errors. Individuals were advised to promptly report any suspicious activity to relevant parties, including insurance companies, healthcare providers, and financial institutions.

   Initially undisclosed, the scale of the impact became apparent through a submission to the Attorney General's office in Maine, which indicated that 112,005 individuals were affected specifically related to MD Valuecare. Subsequent updates from the U.S. Department of Health and Human Services revealed a total of 4,452,782 affected individuals, underscoring the widespread consequences of the breach.

   Moreover, 17 healthcare service providers and state-level health systems relying on HealthEC's tech solutions were also affected. This incident highlights the critical importance of robust cybersecurity measures in safeguarding sensitive health information and emphasizes the necessity of collaborative efforts to mitigate the repercussions of such breaches in the healthcare sector.

3. **Orrick Data Breach Exposes Sensitive Information of 637,000 Victims** – Orrick, Herrington & Sutcliffe, a renowned international law firm headquartered in San Francisco, recently faced a significant security incident after the discovery of a data breach in March 2023. The breach exposed sensitive health information belonging to a concerning 637,000 victims.

   The intrusion into Orrick's network compromised a file share, resulting in the exposure of personal information and sensitive health data of 637,620 affected individuals, including 830 residents from Maine. Classified as an external system breach caused by hacking, the incident occurred on 02/28/2023, with its discovery reported on 03/13/2023.

   The stolen data included a wide range of sensitive details such as names, dates of birth, addresses, email addresses, and various government-issued identification numbers like Social Security, passport, driver's license, and tax identification numbers. Additionally, compromised information encompassed medical treatment details, insurance claims information, healthcare insurance numbers, provider details, online account credentials, and credit/debit card numbers.

   In response, Orrick promptly notified affected individuals through written communications on 9/14/2023, 11/16/2023, and 11/17/2023. To mitigate potential fallout, the law firm offered a two-year Kroll identity monitoring service for identity theft protection.

   The data leak from Orrick implicated information related to security incidents at other companies for which Orrick provided legal counsel, including individuals with vision plans from EyeMed Vision Care and dental plans from Delta Dental, as well as data from health insurance company MultiPlan, behavioral health giant Beacon Health Options (now known as Carelon), and the U.S. Small Business Administration.

   In response to inquiries by The Cyber Express (TCE), Orrick expressed regret for the inconvenience caused by the malicious incident and emphasized its commitment to swiftly resolving the matter. The law firm announced the closure of the incident through a settlement within a year and reiterated its ongoing dedication to safeguarding client and firm information.

Additionally, Orrick is in the process of settling a class-action lawsuit arising from the data breach, acknowledging the compromise of clients' personal information. The firm has reached an initial agreement in principle to settle four consolidated lawsuits involving hundreds of thousands of alleged victims, demonstrating its commitment to responsibly addressing the repercussions of the data breach.

4. **New Study Reveals Consumer Trust Plummets After Cyberattacks** – In 2023, businesses encountered a staggering 800,000 cyberattacks, including over 60,000 DDoS attacks and 4,000 ransomware incidents, as per recent research findings. These statistics underscore a concerning trend in cybersecurity, shedding light on the evolving landscape of digital threats.

   Interestingly, the study also delves into consumer perceptions surrounding cybersecurity incidents and their impact on brand trust. It reveals that consumers possess nuanced views on these matters and are often less cognizant of their role in upholding cyber hygiene within a business setting.

   A significant revelation from the research is the pivotal role of brand trust in the digital realm. A striking 75% of consumers express their readiness to sever ties with a brand following any cybersecurity issue. Rebuilding trust post-cyberattack poses a considerable challenge, with 66% of US consumers indicating a reluctance to entrust their data to a company that has suffered a data breach. Moreover, 44% attribute cyber incidents to a company's perceived lack of security measures. Interestingly, there's a degree of leniency shown towards smaller brands grappling with cyberattacks, with 54% expressing more understanding compared to their expectations from larger enterprises.

   These insights, combined with a prevailing lack of awareness regarding the origins of cyberattacks, have led to some concerning consumer behaviors. For instance, 55% of respondents admit to using corporate devices for online shopping, inadvertently posing risks to business infrastructure. Despite this, 35% of consumers believe that impersonating large e-commerce brands is challenging, indicating a gap in understanding the tactics employed by cybercriminals.

   Industry experts have underscored the need for businesses to comprehend their security protocols through the lens of their most vulnerable link—the employees. Advocacy for regular awareness and training sessions across all departments, not just IT and cybersecurity, to foster a culture of vigilance is being conveyed. This inclusive approach aims to empower all employees to recognize and respond to the evolving threat landscape, where social engineering often serves as the entry point for sophisticated ransomware and DDoS attacks.

5. **NIST Raises Alarm on AI Security Risks: Urges Tech Community Action** – The U.S. National Institute of Standards and Technology (NIST) has brought attention to the privacy and security hurdles stemming from the increased adoption of artificial intelligence (AI) systems in recent times.

   NIST underscores security and privacy concerns, including the potential for adversarial manipulation of training data, exploitation of model vulnerabilities, and malicious interactions with models for extracting sensitive information about individuals, the model itself, or proprietary enterprise data.

   As AI systems rapidly integrate into online services, fuelled partly by the rise of generative AI systems like OpenAI ChatGPT and Google Bard, they face a range of threats across different stages of machine learning operations. These threats include tainted training data, vulnerabilities in software components, data model poisoning, supply chain weaknesses, and privacy breaches from prompt injection attacks.

   Apostol Vassilev, a NIST computer scientist, points out that while software developers often seek broader user bases to enhance their products, exposure does not always yield positive outcomes. He highlights that a chatbot, for instance, may produce harmful or toxic information when prompted with carefully crafted language.

   NIST categorizes the attacks into four types:

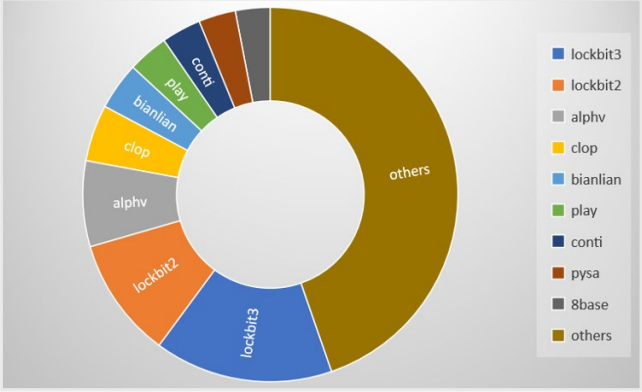
   1. Evasion attacks, which aim to generate adversarial output post-deployment of a model
   2. Poisoning attacks, which target the training phase by introducing corrupt data
   3. Privacy attacks, seeking sensitive details about the system or trained data by posing specific queries
   4. Abuse attacks, compromising legitimate information sources to repurpose the system's intended use

   These attacks can be carried out by threat actors with varying levels of knowledge (white-box, black-box, or grey-box), adding complexity to the taxonomy. NIST underscores the absence of robust mitigation measures and urges the tech community to develop better defenses.

   This development follows the recent issuance of guidelines by the U.K., the U.S., and international partners for the secure development of AI systems. Vassilev underscores how vulnerable AI and machine learning technologies are to attacks, highlighting unresolved theoretical challenges in securing AI algorithms and cautioning against exaggerated claims of complete solutions.

Ransomware Tracker

Distribution of Post by Group (Total - 9697 in Jan)



Post by Group Last 7 Days

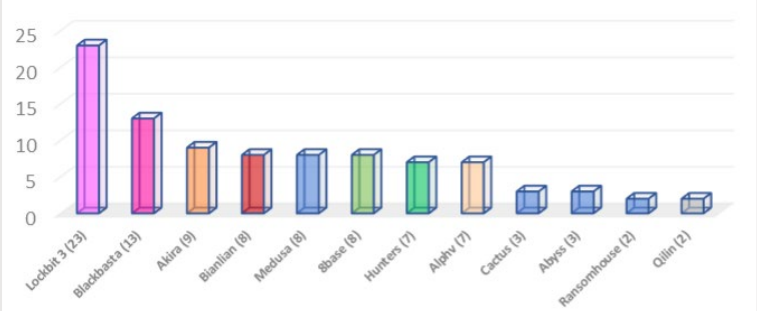


Image Source

Rhysida Ransomware

Targeted Sectors: Rhysida primarily targets organizations in the education, healthcare, manufacturing, IT, and government sectors due to the potential for high-value data and critical systems.

Tactics: Rhysida actors employ a multifaceted approach, exploiting external-facing remote services, utilizing living-off-the-land techniques, and operating within a ransomware-as-a-service (RaaS) model, making attribution challenging.

Initial Access: The threat actors gain initial access through a variety of methods, including compromised credentials acquired through phishing, exploitation of the Zerologon vulnerability (CVE-2020-1472), and successful phishing attempts.

Living off the Land: To remain stealthy, Rhysida leverages native tools like PowerShell, Remote Desktop Protocol (RDP), and VPNs. This approach helps them blend with legitimate Windows activities, making detection more challenging.

Leveraged Tools: The adversaries repurpose both native and third-party tools. Native tools include cmd.exe, PowerShell.exe, and mstsc.exe. They also leverage third-party tools such as PsExec.exe, PuTTY.exe, and PortStarter for lateral movement and maintaining persistence.

Ransomware Characteristics: Rhysida employs a robust 4096-bit RSA encryption key with the ChaCha20 algorithm. Notably, the ransomware engages in “double extortion,” exfiltrating sensitive data before encrypting files and demanding payment in Bitcoin.

Detection

Technical Details:

Initial Access

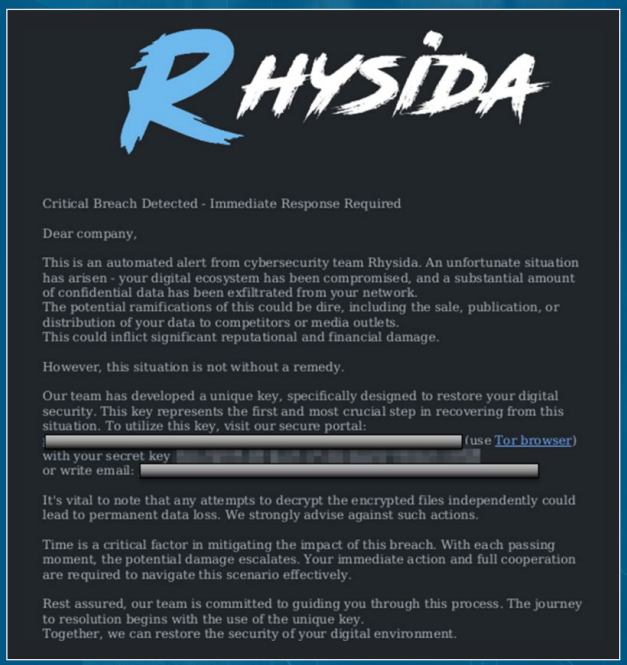
Methods: Rhysida actors successfully compromise credentials, exploit the Zerologon vulnerability, and conduct targeted phishing campaigns.

Observations: The threat actors utilize compromised credentials to authenticate to internal VPNs, exploit Zerologon for rapid domain controller compromise, and employ convincing phishing techniques.

Living off the Land

Techniques: Living-off-the-land techniques involve the use of PowerShell for code execution, RDP for lateral movement, and native tools (ipconfig, whoami, nltest) for reconnaissance.

Tool Repurposing: Legitimate tools like PsExec.exe, PuTTY.exe, and PortStarter are repurposed for malicious activities. This allows the threat actors to move laterally while avoiding suspicion.


RHYSIDA

Critical Breach Detected - Immediate Response Required

Dear company,

This is an automated alert from cybersecurity team Rhysida. An unfortunate situation has arisen - your digital ecosystem has been compromised, and a substantial amount of confidential data has been exfiltrated from your network.
The potential ramifications of this could be dire, including the sale, publication, or distribution of your data to competitors or media outlets.
This could inflict significant reputational and financial damage.

However, this situation is not without a remedy.

Our team has developed a unique key, specifically designed to restore your digital security. This key represents the first and most crucial step in recovering from this situation. To utilize this key, visit our secure portal:
[redacted] (use Tor browser)
with your secret key [redacted]
or write email: [redacted]

It's vital to note that any attempts to decrypt the encrypted files independently could lead to permanent data loss. We strongly advise against such actions.

Time is a critical factor in mitigating the impact of this breach. With each passing moment, the potential damage escalates. Your immediate action and full cooperation are required to navigate this scenario effectively.

Rest assured, our team is committed to guiding you through this process. The journey to resolution begins with the use of the unique key.
Together, we can restore the security of your digital environment.

Leveraged Tools

Native Tools: Rhysida utilizes common native tools such as cmd.exe, PowerShell.exe, and mstsc.exe for remote execution and lateral movement.

Third-Party Tools: The threat actors employ third-party tools like PsExec.exe and PuTTY.exe to facilitate SSH connections and PortStarter for modifying firewall settings.

Ransomware Characteristics

Execution: Rhysida employs various techniques during the execution phase, including the creation of staging directories, deployment of malicious executables (conhost.exe, psexec.exe), and the use of batch scripts for ransomware staging.

Encryption: The ransomware utilizes a robust 4096-bit RSA encryption key with the ChaCha20 algorithm, modifies the registry for persistence, and encrypts data with a .rhysida extension.

Indicators of Compromise (IoCs): Organizations should be vigilant for C2 IP addresses, associated email addresses, and specific files used by Rhysida actors during their campaigns.

Behavioral Indicators: Detection can be enhanced by monitoring for unusual network activity, unexpected use of legitimate tools, and identifying file modifications associated with ransomware activities.

Detailed IOC Link: https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-319a

Prevention

- MFA Implementation: Enforce multi-factor authentication (MFA) for webmail, VPN, and critical system accounts to mitigate the risk of unauthorized access even with compromised credentials.
- Command-Line Restrictions: Disable unnecessary command-line and scripting activities to impede lateral movement and limit the potential for attackers to exploit native tools.
- PowerShell Controls: Tighten controls around PowerShell usage, ensure it is updated to the latest version, and enable enhanced logging to facilitate the detection of malicious activity.
- Network Segmentation: Implement network segmentation to contain and prevent the lateral movement of ransomware, limiting its impact on critical systems.

Remediation

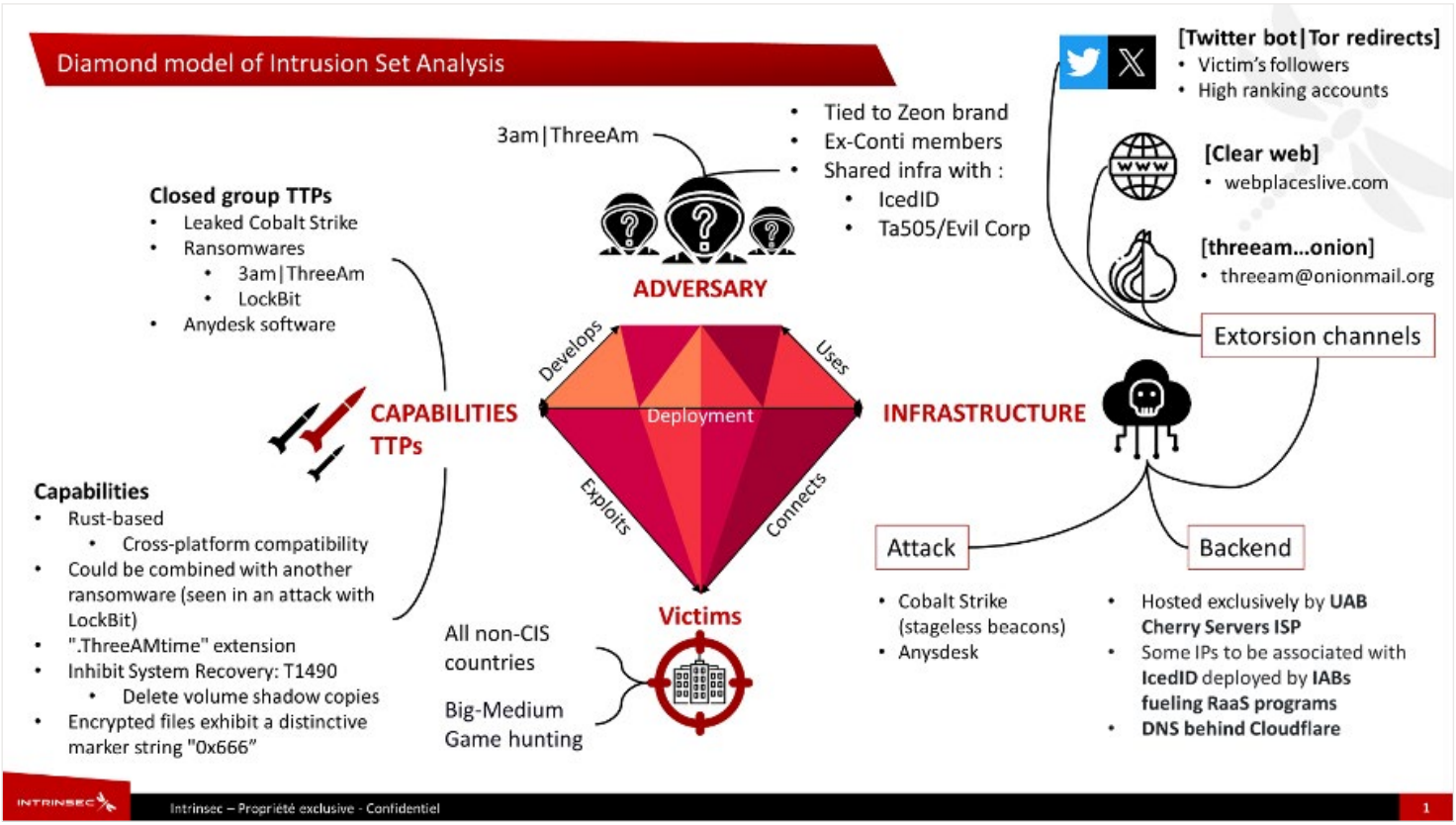
- Regular Patching: Keep systems, software, and firmware up to date to address vulnerabilities, especially the Zerologon vulnerability. Regularly apply patches and updates.
- Backup Best Practices: Maintain offline, encrypted, and immutable backups. Regularly test and restore backups to ensure they are reliable and can be quickly deployed in the event of an attack.
- Security Validation: Continuously test security controls against MITRE ATT&CK techniques associated with Rhysida to ensure the effectiveness of implemented defenses.

Unveiling 3AM Ransomware

- **Emergence of 3AM Ransomware:** A new ransomware family called 3AM or ThreeAM has been identified, initially observed in a limited fashion.
- **Technical Details:** Written in Rust, 3AM is a novel malware family that attempts to stop services on infected computers before encrypting files and deleting Volume Shadow copies. Command-line parameters and encryption methods indicate similarities to Conti ransomware.
- **Attack Preparation:** Attackers deploy reconnaissance tools like gpresult and Cobalt Strike components, attempting privilege escalation and lateral movement. They deploy 3AM after failing to deploy LockBit.
- **Warning Signs:** Researchers have noted an increasing trend of ransomware affiliates deploying multiple ransomware families in a single attack. While new ransomware families often fade quickly, 3AM's use in conjunction with LockBit suggests potential future activity.

Technical Details:

- **Ransomware Characteristics:** 3AM encrypts files, appending them with the ".threeamtime" extension, and attempts to delete Volume Shadow copies. Written in Rust, it uses specific command-line parameters and encryption methods.
- **Attack Tactics:** Attackers utilize reconnaissance commands, privilege escalation tools like PsExec, and lateral movement techniques. They deploy 3AM after initial attempts with LockBit fail.
- **Encryption and Persistence:** 3AM encrypts files using predefined criteria, deletes the original files, and leaves a ransom note named "RECOVER-FILES.txt" in each folder. It adds new users for persistence and exfiltrates files using tools like Wput.



Detection

- **Behavioral Analysis:** Detect 3AM ransomware activity through behavioral analysis. Focus on unusual processes attempting to stop services, delete Volume Shadow copies, and encrypt files.
- **Command-Line Parameters:** Monitor for the specific command-line parameters used by 3AM, including those related to encryption method ("local" or "net") and speed control for encryption ("s").
- **Reconnaissance Activities:** Look for signs of reconnaissance activities such as the use of gpresult, Cobalt Strike components, and commands like whoami, netstat, quser, and net view.

- **IOCs:** Utilize Indicators of Compromise (IOCs)—such as file hashes and network indicators associated with 3AM ransomware activity—for early detection and blocking.
  - **SHA256 file hashes:**
    - 079b99f6601f0f6258f4220438de4e175eb4853649c2d34ada72cce6b1702e22 – LockBit
    - 307a1217aac33c4b7a9cd923162439c19483e952c2ceb15aa82a98b46ff8942e – 3AM
    - 680677e14e50f526cced739890ed02fc01da275f9db59482d96b96fbc092d2f4 – Cobalt Strike
    - 991ee9548b55e5c815cc877af970542312cff79b3ba01a04a469b645c5d880af – Cobalt Strike
    - ecbdb9cb442a2c712c6fb8aee0ae68758bc79fa064251bab53b62f9e7156febc – Cobalt Strike
  - **Network indicators:**
    - 185.202.0[.]111
    - 212.18.104[.]6
    - 85.159.229[.]62

Prevention

- **Security Updates:** Regularly update operating systems and security software to patch vulnerabilities and protect against known exploits used by ransomware attackers.
- **Employee Training:** Educate employees on cybersecurity best practices, including how to identify phishing attempts and avoid downloading malicious attachments or clicking on suspicious links.
- **Network Segmentation:** Implement network segmentation to limit the spread of ransomware in the event of a successful intrusion, isolating critical systems and data from potential compromise.
- **Access Controls:** Enforce least privilege access controls to restrict users' ability to execute arbitrary commands and limit the impact of potential ransomware infections.

Remediation

- **Isolation:** Immediately isolate affected systems from the network to prevent further spread of ransomware and minimize damage to other connected devices and data.
- **Backup Restoration:** Restore encrypted files from secure backups stored offline or in an isolated environment, ensuring the integrity of the data and minimizing downtime for affected systems.
- **Forensic Analysis:** Conduct thorough forensic analysis of affected systems to identify the root cause of the ransomware infection, including potential entry points and lateral movement pathways used by attackers.
- **Incident Reporting:** Report ransomware incidents to relevant authorities and regulatory bodies as required by data protection regulations, ensuring compliance with legal obligations and facilitating coordinated response efforts.
- **Engagement with Experts:** Engage with cybersecurity experts and incident response teams to assist with post-incident remediation efforts, including identifying and addressing vulnerabilities in the organization's security posture.

From Macro to Payload: Decrypting the Sidewinder Cyber Intrusion Tactics

The sophisticated Sidewinder APT group's threat landscape reveals a very capable and tenacious enemy that, in this case, has planned a deliberate campaign against the Nepalese government.

They target not just Nepal but also several South Asian governments. The latest attack revealed an especially complex plan. Researchers have recently discovered that Bhutan is the target of similar attacks.

The way the group operates is by spreading malicious documents that are cleverly disguised as correspondence from the Prime Minister's Office of Nepal.

This dishonest strategy highlights the sophistication of the threat's various methods, such as spear-phishing emails and the use of malicious macros in documents. Given the urgency of the situation, pertinent stakeholders must act quickly and cooperatively.

Detection

A cyber threat group is using a malicious Word document with an embedded macro that asks victims to enable macros when they open it.

When the macro is activated, it starts a sequence of events that include extracting conhost.zip onto the victim's computer, creating and executing BAT and VB scripts, and more. The last payload, the Nim backdoor, is installed at the end of this procedure.

This backdoor's main goal is to connect to the adversaries' command and control (C2) server to enable illegal access. The Sidewinder group is identified as the source of the malicious document, which included the Nim backdoor as its ultimate payload. (also known as Rattlesnake, BabyElephant, APT Q4, APT Q39, Hardcore Nationalist, HN2, RAZOR Tiger, and GroupA21).

The Sidewinder group is thought to have its origins in South Asia, based on information that is currently available. The group's endeavors date back to 2012. The group usually targets military and governmental institutions in different South Asian countries with its attacks.

All the URLs hardcoded in the main payload conhost.exe (Nim Backdoor), according to the OSINT investigation, resolved to the IP address "213[.]109[.]192[.]93."

- http[:]//mail[.]mofa[.]govnp[.]org/mail/AFA/
- http[:]//nitc[.]govnp[.]org/mail/AFA/
- http[:]//dns[.]govnp[.]org/mail/AFA/
- http[:]//mx1[.]Nepal[.]govnp[.]org/mail/AFA/

Analysis

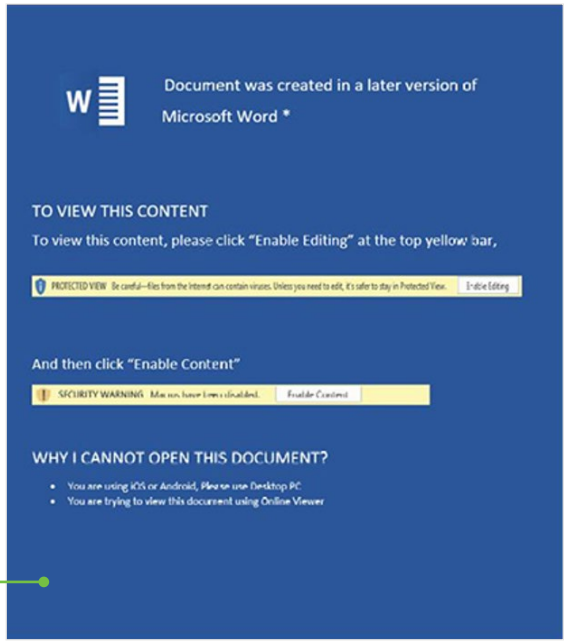
Basic Details:

MD5: E5859B366B93B05414E1E95D65CE7414

SHA256:7459a6106d3562d72c7a4fee62d106064a3ed5b48e16474da2b448aeacc2a333

File Type: Office Open XML Document (Microsoft Word Document)

The e-mail, which might be spear-phished, contains a malicious document. This document contains an embedded malicious macro that is activated and executed upon opening. The victim is tricked when the document asks them to allow editing, as the example to the right illustrates:



The sample's misleading content seems to be connected to the Nepalese government, which may suggest that officials in that country are the target.


नेपाल सरकार
प्रधानमन्त्री तथा मन्त्रिपरिषद्को कार्यालय
सिंहदरबार, काठमाडौं
नेपाल

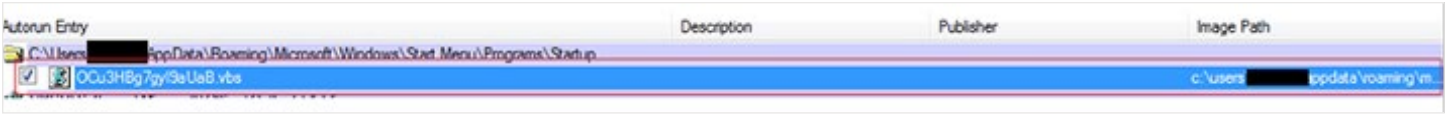
Investigation revealed that the document has an embedded macro in it. The macro was then extracted for additional examination. The macro looks to be a component of a multi-phase assault that aims to carry out malicious payloads, conceal its actions, and establish persistence.

```
A: word/vbaProject.bin
 A1:       560 'PROJECT'
 A2:        71 'PROJECTwm'
 A3:        97 'UserForm1/\x01CompObj'
 A4:       294 'UserForm1/\x03VBFrame'
 A5:        90 'UserForm1/f'
 A6:    678964 'UserForm1/o'
 A7: M   13088 'VBA/ThisDocument'
 A8: m    1455 'VBA/UserForm1'
 A9:      4653 'VBA/_VBA_PROJECT'
A10:      8023 'VBA/__SRP_0'
A11:       290 'VBA/__SRP_1'
A12:      8464 'VBA/__SRP_2'
A13:       396 'VBA/__SRP_3'
A14:       614 'VBA/__SRP_4'
A15:       106 'VBA/__SRP_5'
A16:       814 'VBA/dir'
```

When a document is opened, the Document_Open subroutine is called. Four functions (sch_task, hide_cons, read_shell, and vb_chain) are activated by default when the victim opens the document. Each is in charge of a different facet of the malicious behavior.

```
Attribute VB_Name = "ThisDocument"
Attribute VB_Base = "1Normal.ThisDocument"
Attribute VB_GlobalNameSpace = False
Attribute VB_Creatable = False
Attribute VB_PredeclaredId = True
Attribute VB_Exposed = True
Attribute VB_TemplateDerived = True
Attribute VB_Customizable = True
Sub Document_Open()
sch_task
hide_cons
read_shell
vb_chain
End Sub
```

The sch_task function carries out multiple tasks, including setting up paths and environment variables and creating a VBScript file (OCu3HBg7gyI9aUaB.vbs) for persistence in the Startup folder (C:\Users\UserName\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup).



List of IOCs

SR NO.	INDICATOR	TYPE	REMARKS
1	E5859B366B93B05414E1E95D65CE7414	MD5 File Hash	Malicious Macro Document
2	4319a76108da6dbcc46a8e50dce25bace3dfe518	SHA1 File Hash	Malicious Macro Document
3	7459a6106d3562d72c7a4fee62d106064a3ed5b48e16474da2b448aeacc2a333	SHA256 Hash	Malicious Macro Document
4	777fcc34fef4a16b2276e420c5fb3a73	MD5 File Hash	Conhost.exe
5	5d2e2336bb8f268606c9c8961bed03270150cf65	SHA1 File Hash	Conhost.exe
6	696f57d0987b2edefcadecd0eca524cca3be9ce64a54994be13eab7bc71b1a83	SHA256 Hash	Conhost.exe
7	http://mail.mofa.govnp.org/mail/AFA/	URL	Hardcoded URLs
8	http://nitc.govnp.org/mail/AFA/	URL	Hardcoded URLs
9	http://dns.govnp.org/mail/AFA/	URL	Hardcoded URLs
10	http://mx1.nepal.govnp.org/mail/AFA/	URL	Hardcoded URLs

Mitre Att&ck TTPs

NO.	TACTIC	TECHNIQUE
1	Initial Access (TA0001)	T1566: Phishing T1566.001: Spear phishing Attachment
2	Execution (TA0002)	T1204: User Execution T1204.002: Malicious File
3	Persistence (TA0003)	T1547: Boot or Logon Auto start Execution T1547.001: Registry Run Keys/ Startup Folder
4	Defense Evasion (TA0005)	T1140: Deobfuscate/Decode Files or Information
5	Discovery (TA0007)	T1057: Process Discovery T1082: System Information Discovery
6	Exfiltration (TA0010)	T1041 – Exfiltration Over Command-and-Control Channel
7	Lateral Movement (TA0008)	T1021: Remote Services

Remediation

- Use strong endpoint security solutions with sophisticated threat detection and prevention features to locate and stop malicious activity.
- Make use of trustworthy antivirus and anti-malware software that can quickly identify and eliminate malicious payloads.
- Update operating systems, programs, and security software frequently to fix known vulnerabilities that are frequently used by threat actors.
- Divide your network into sections to prevent lateral movement. This containment technique aids in preventing malware from gaining access to important resources and propagating further.
- Inform staff members about the perils of phishing scams, highlighting the hazards of opening attachments and clicking on links in unsolicited emails.
- Employees can avoid executing malicious files by learning to identify the social engineering techniques used by threat actors and by not falling for shady tactics.

Prevention

- Use behavior-based monitoring to spot odd patterns of behavior, such as suspicious processes trying to connect to unapproved networks.
- Create application whitelisting rules to ensure that only authorized applications can run on endpoints and to stop malicious or unauthorized executables from being executed.
- Keep a careful eye out for any unusual patterns in network traffic, such as large transfers of data to IP addresses that are unknown or questionable.
- Make a thorough incident response plan that outlines what needs to be done if malware is detected. This should entail quickly alerting pertinent stakeholders and isolating impacted systems.
- To proactively identify potential threats, stay informed about the most recent threat intelligence reports and malware-related indicators of compromise.
- Create and implement safety measures by keeping an eye on/blocking IOCs and by fortifying defenses in accordance with the given tactical intelligence and rules.

Google: Russian FSB Hackers Deploy New Spica Backdoor Malware

Google claims that a hacker group backed by Russia's ColdRiver is disseminating backdoor malware that has never been seen before by using payloads that look like PDF decryption tools.

Phishing emails posing as people connected to their targets are used by the attackers to send PDF documents that appear to be encrypted (a tactic first observed in November 2022).

The recipients are sent a link to download what appears to be a PDF decryptor executable (named Proton-decrypter.exe) to view the contents of the lure documents when they respond that they are unable to read the "encrypted" documents.

ColdRiver requests input from the target by posing these documents as a fresh opinion piece or another kind of article that the impersonation account is hoping to publish. The text appears encrypted when the user opens the benign PDF file.

Security researchers with Google's Threat Analysis Group (TAG) have identified a malware strain that the attackers are using, called Spica, to backdoor the victims' devices while pretending to display a fake PDF document.

Even though they were only able to capture one Spica sample while looking into this campaign, the researchers think that there are probably more that match the phishing lures and have different decoy documents.

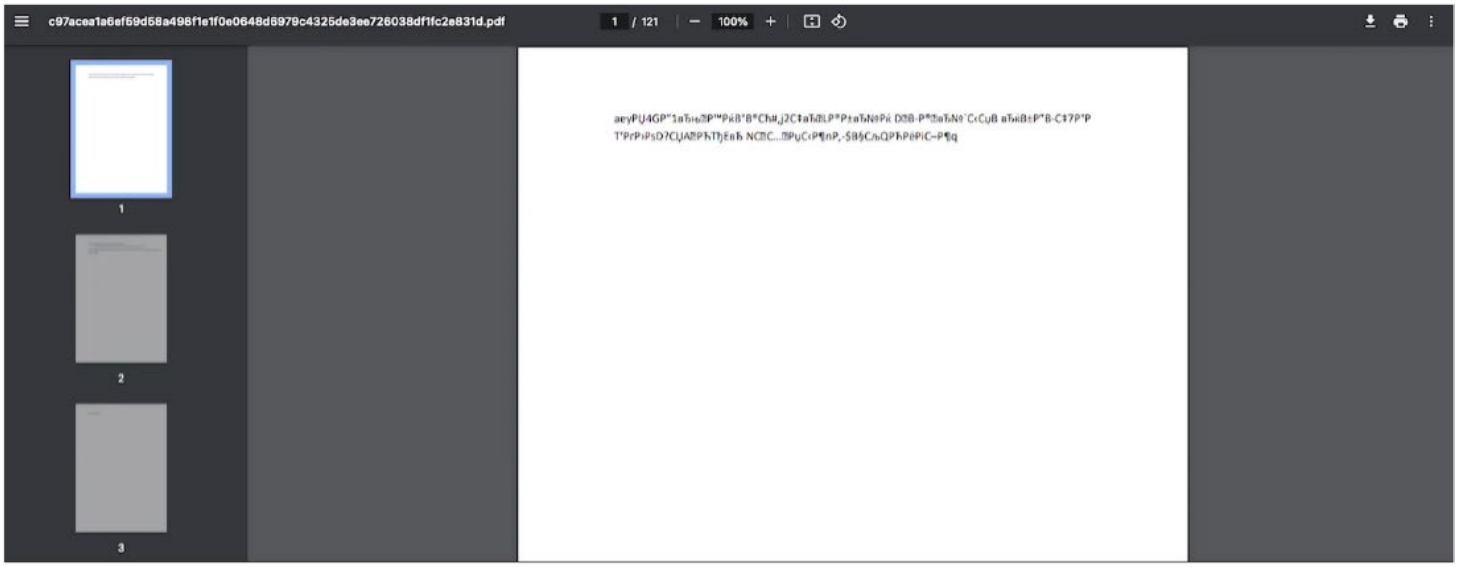
Detection

The Spica Rust malware facilitates the execution of arbitrary shell commands, the theft of cookies from Chrome, Firefox, Opera, and Edge browsers, the uploading and downloading of files, and the exfiltration of documents. It communicates with its command-and-control (C2) server via JSON over websockets.

Upon deployment, Spica will further establish persistence on the compromised devices by launching a scheduled task named "CalendarChecker" through an obfuscated PowerShell command.

TAG believes that ColdRiver has been using the backdoor since at least November 2022, but they have seen Spica being used as early as September 2023.

Although TAG has detected four distinct iterations of the original "encrypted" PDF lure, we have only succeeded in recovering one instance of Spica.



Google has alerted all targeted Google Mail and Workspace users that they were the subject of a government-backed attack and added all domains, web pages, and files used in the incidents to its Safe Browsing phishing attacks protection service.

Prevention

- Block 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

- Monitor remote access tools and implement phishing-resistant multifactor authentication (MFA).
- 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.
- Keep systems and software regularly updated, focusing on patching vulnerabilities.
- Implement network segmentation to control traffic and prevent ransomware spread.
- Use network monitoring and Endpoint Detection and Response (EDR) tools to detect abnormal activities.
- Enhance email security by disabling risky links and encrypting backup data.

TOP THREAT ACTORS

Threat Actor	IOC Reference
Rhysida Ransomware	https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-319a
ColdRiver	https://therecord.media/russia-state-hackers-deploying-malware-nato?&web_view=true
Sidewinder Group	https://www.cyfirma.com/outofband/from-macro-to-payload-decrypting-the-sidewinder-cyber-intrusion-tactics/?web_view=true
ThreeAM	https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/3am-ransomware-lockbit

TOP EXPLOITED VULNERABILITIES

Vulnerability Name	Description	References
Trend Micro Deep Security Improper Access Control Local Privilege Escalation Vulnerability CVE-2023-52337	Vulnerability allows local attackers to escalate privileges on affected installations of Trend Micro Deep Security. An attacker must first obtain the ability to execute low-privileged code on the target system to exploit this vulnerability.	https://success.trendmicro.com/dcx/s/solution/000296337?language=en_US
Paessler PRTG Network Monitor Cross-Site Scripting Authentication Bypass Vulnerability CVE-2023-51630	Vulnerability allows remote attackers to bypass authentication on affected installations of Paessler PRTG Network Monitor. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file.	https://www.paessler.com/prtg/history/stable
Synology RT6600ax Qualcomm LDB Service Improper Input Validation Remote Code Execution Vulnerability CVE-2024-21473	Vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of Synology RT6600ax routers. The specific flaw exists within the Qualcomm LDB service. The issue results from the lack of proper validation of user-supplied data prior to further processing.	https://yanac.hu/2024/01/17/cve-2024-21473-synology-rt6600ax-qualcomm-ldb-service-input-validation/
Ivanti Avalanche WLAvalancheService Stack-based Buffer Overflow Remote Code Execution Vulnerability CVE-2023-46223	Vulnerability allows remote attackers to execute arbitrary code on affected installations of Ivanti Avalanche. The issue results from the lack of proper validation of the length of user-supplied data prior to copying it to a stack-based buffer.	https://www.ivanti.com/blog/new-ivanti-avalanche-vulnerabilities
Trend Micro Apex Central modVulnerabilityProtect Server-Side Request Forgery Information Disclosure Vulnerability CVE-2023-52331	Vulnerability allows remote attackers to disclose sensitive information on affected installations of Trend Micro Apex Central. The specific flaw exists within the modVulnerabilityProtect module. The issue results from the lack of proper validation of a URI prior to accessing resources.	https://success.trendmicro.com/dcx/s/solution/000296153?language=en_US

TOP EXPLOITED VULNERABILITIES

Vulnerability Name	Description	References
D-Link DCS-8300LHV2 RTSP ValidateAuthorizationHeader Username Stack-Based Buffer Overflow Remote Code Execution Vulnerability CVE-2023-51626	Vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of D-Link DCS-8300LHV2 IP cameras. The specific flaw exists within the handling of the Authorization header by the RTSP server, which listens on TCP port 554.	https://supportannouncement.us.dlink.com/announcement/publication.aspx?name=SAP10370
Microsoft Office Word FBX File Parsing Use-After-Free Remote Code Execution Vulnerability CVE-2024-20677	Vulnerability allows remote attackers to execute arbitrary code on affected installations of Microsoft Office Word. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-20677
Microsoft Windows cldflt Integer Overflow Local Privilege Escalation Vulnerability CVE-2024-21310	Vulnerability allows local attackers to escalate privileges on affected installations of Microsoft Windows. An attacker obtains the ability to execute low-privileged code on the target system to exploit this vulnerability. Only systems with long Win32 path support enabled are affected.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21310
Foxit PDF Reader Doc Use-After-Free Remote Code Execution Vulnerability	Vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit PDF Reader. The issue results from the lack of validating the existence of an object prior to performing operations on the object.	https://www.foxit.com/support/security-bulletins.html
Linux Kernel GSM Multiplexing Race Condition Local Privilege Escalation Vulnerability CVE-2023-6546	Vulnerability allows local attackers to execute arbitrary code on affected installations of Linux Kernel. The specific flaw exists within the n_gsm driver. The issue results from the lack of proper locking when performing operations on an object.	https://access.redhat.com/security/cve/cve-2023-6546
Bentley View SKP File Parsing Use-After-Free Remote Code Execution Vulnerability CVE-2023-44430	Vulnerability allows remote attackers to execute arbitrary code on affected installations of Bentley View. The issue results from the lack of validating the existence of an object prior to performing operations on the object.	https://www.bentley.com/advisories/be-2022-0019/
Inductive Automation Ignition ResponseParser Notification Deserialization of Untrusted Data Remote Code Execution Vulnerability CVE-2023-50222	Vulnerability allows remote attackers to execute arbitrary code on affected installations of Inductive Automation Ignition. The issue results from the lack of proper validation of user-supplied data, which can result in deserialization of untrusted data.	https://security.inductiveautomation.com/?tcuUid=fc4c4515-046d-4365-b688-693337449c5b
oFono SMS Decoder Stack-based Buffer Overflow Remote Code Execution Vulnerability CVE-2023-4235	Vulnerability allows remote attackers to execute arbitrary code on affected installations of oFono. The issue results from the lack of proper validation of the length of user-supplied data prior to copying it to a stack-based buffer.	https://bugzilla.redhat.com/show_bug.cgi?id=2255402
X.Org Server ProcXIChangeProperty Heap-based Buffer Overflow Local Privilege Escalation Vulnerability CVE-2023-5367	Vulnerability allows local attackers to escalate privileges on affected installations of X.Org Server. 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 XIChangeDeviceProperty function.	https://lists.x.org/archives/xorg-announce/2023-October/003430.html
SolarWinds Access Rights Manager Hardcoded Credentials Authentication Bypass Vulnerability CVE-2023-40058	Vulnerability allows remote attackers to bypass authentication on affected installations of SolarWinds Access Rights Manager. The specific flaw exists within the configuration of a RabbitMQ instance.	https://www.solarwinds.com/trust-center/security-advisories/cve-2023-40058
Kofax Power PDF BMP File Parsing Out-Of-Bounds Write Remote Code Execution Vulnerability CVE-2023-51569	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 write past the end of an allocated object.	https://docshield.tungstenautomation.com/PowerPDF/en_US/5.0.0-3uoz7ssq2b/print/ReadMe-KofaxPowerPDFAdvanced-5.0.0.16.htm

Security Bulletin

Threat Actor Targets Recruiters with Malware

Recruiters are currently facing a sophisticated threat from a financially motivated actor known as TA4557, as per security researchers. This threat actor employs malicious emails to infect targets, utilizing the More_Eggs backdoor. The More_Eggs backdoor is designed to establish persistence, profile the compromised system, and deploy additional payloads.

TA4557 initially responded to job vacancies on third-party employment platforms in 2022 and early 2023. More recently, the threat actor has shifted to contacting recruiters directly. In a novel attack chain utilizing a direct email technique, the actor replies with a URL leading to an actor-controlled website posing as a candidate's resume after the recipient responds to the initial email.

Alternatively, the actor may respond with a Word or PDF attachment instructing the recipient to visit the fraudulent resume website.

In recent phishing attempts, the threat actor instructs the target to "refer to the domain name of my email address to access my portfolio," aiming to bypass security filters. Visiting the sender's website and following these instructions leads to a CAPTCHA page. Upon completion, a zip file is downloaded, containing a shortcut file (LNK).

Upon execution, the LNK file exploits valid software features in 'ie4uinit.exe' to download and execute a scriptlet from a location specified in the 'ie4uinit.inf' file. After decryption, the scriptlet deposits a DLL in the subdirectory %APPDATA%\Microsoft. Subsequently, it attempts to use Windows Management Instrumentation (WMI) to initiate a new regsrv32 process for running the DLL. If unsuccessful, it employs an alternative strategy using the ActiveX Object Run function.

These "living-off-the-land" techniques are crafted to infect the victim's computer with the More_Eggs backdoor by launching a DLL. To mitigate the threat posed by TA4557, associated with FIN6, Proofpoint recommends that recruiters update their user awareness training. The adoption of this technique by TA4557 may lull recipients into a false sense of trust, making them more susceptible to engaging with and sharing content from the threat actor.

Researchers have noted an increase in threat actors utilizing benign messages to build trust with targets before delivering malicious content. The gang's frequent modification of infrastructure, fake resume domains, and sender emails pose a challenge for automated security systems, as it becomes difficult to identify harmful information

New AeroBlade Hackers Target Aerospace Sector in the U.S.

'AeroBlade,' a previously unidentified cyber espionage hacking gang, was found to be targeting US aerospace industry groups.

The effort was carried out in two stages: a testing phase in September 2022 and a more sophisticated attack in July 2023.

To gain initial access to corporate networks, the assaults employ spear-phishing with weaponized documents, dropping a reverse-shell payload that can be used for file listing and data theft.

The primary objective of this attack was commercial cyber espionage, with a mid to high degree of confidence, to obtain important data.

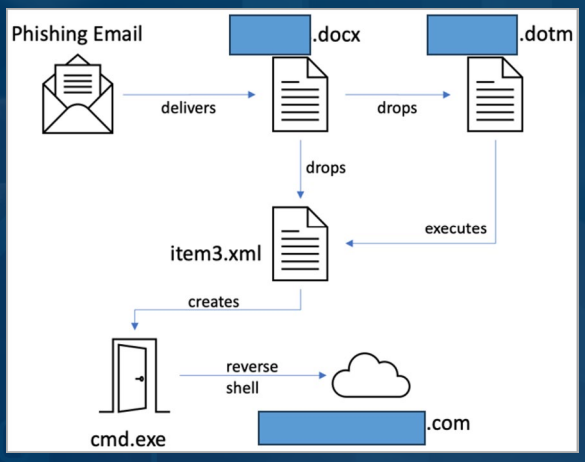
Campaign Details

The first attacks linked to AeroBlade happened in September 2022. The second stage DOTM file was downloaded using phishing emails with a document (docx) attachment that used remote template injection.

To establish a reverse shell on the target's system and connect it to the attacker's command and control (C2) server, the second step of the attack uses malicious macros.

"Once the victim opens the file and executes it by manually clicking the "Enable Content" lure message, the [redacted].dotm document discretely drops a new file to the system and opens it," states BlackBerry.

"The newly downloaded document is readable, leading the victim to believe that the file initially received by email is legitimate."



The reverse shell payload is a massively obfuscated DLL that specifies every directory on the stolen computer, which helps its operators plan their next moves in data theft.

The DLL file incorporates anti-analysis features such as API hashing to conceal Windows function misuse, proprietary string encoding, dead code and control flow obfuscation for disassembly protection, and sandbox detection.

Additionally, the payload adds a process called "WinUpdate2" to the Windows process Scheduler to create persistence on compromised computers even after a system reboot.

Most of the evasion techniques seen in the 2023 samples, as well as the capacity to list folders and exfiltrate data, were absent from the early DLL payload samples.

This suggests that while the 2022 attempts were mostly concerned with testing the intrusion and infection chain, threat actors are

still developing new tools for increasingly complex attacks.

The threat actors utilized identical lure documents in the phishing stage of both operations, and the ultimate payload was a reverse shell connecting to the same C2 IP address.

BlackBerry has not been able to ascertain AeroBlade's source or the exact aim of the attacks.

The researchers hypothesize that the purpose of the data theft was to either sell the knowledge, give it to rival aerospace companies abroad, or use it as leverage to blackmail victims.

North Korea-Linked APT Group Sapphire Sleet Set Up Bogus Skills Assessment Portals in Attacks Aimed at IT Job Seekers

Sapphire Sleet, also known as APT38, BlueNoroff, CageyChameleon, and CryptoCore, is an Advanced Persistent Threat (APT) group linked to North Korea and considered a subset of the Lazarus APT organization. The group primarily targets banks, venture capital firms, and cryptocurrency exchanges in its campaigns. Microsoft researchers have issued a warning to IT job applicants about a recent social engineering campaign orchestrated by Sapphire Sleet, involving the use of fraudulent talent evaluation portals.

According to Microsoft's alerts on X, Sapphire Sleet, known for cryptocurrency theft through social engineering, has shifted its tactics in recent weeks by creating new websites posing as skills assessment portals. The APT group previously employed tools like LinkedIn and lured victims with offers related to competence evaluation. Once contact is established, the threat actors transition to other communication channels such as email or instant messaging apps.

To deceive recruiters into creating accounts, Sapphire Sleet registered multiple domains. The APT group either sent URLs to pages hosted on reputable sites like GitHub or directly transmitted malicious attachments. Microsoft specialists suspect that the group developed its own websites after uncovering Sapphire Sleet's previous strategies.

In a separate discovery, Jamf Threat Labs identified a new macOS malware strain named ObjCShellz and linked it to APT BlueNoroff, associated with North Korea. The RustBucket malware campaign, attributed to the BlueNoroff APT group, shares similarities with the ObjCShellz virus. The use of a domain resembling that of a reputable exchange suggests that threat actors targeted an organization or individual with an interest in the cryptocurrency industry, although specific targets have not been identified.

Elastic Security Labs recently disclosed the use of new KandyKorn macOS malware by the Lazarus APT group, also associated with North Korea. These attacks, directed at blockchain developers, demonstrate the ongoing and evolving threats posed by APT groups in the cybersecurity landscape.

Kinsing Actors Exploiting Recent Linux Flaw to Breach Cloud Environments

Threat actors associated with Kinsing are actively exploiting the Linux privilege escalation vulnerability, Looney Tunables (CVE-2023-4911), in a new experimental campaign. The attackers are demonstrating an expanded focus on cloud-native attacks by extracting credentials from Cloud Service Providers (CSP), a strategic shift from their traditional methods. Kinsing's exploitation of Looney Tunables poses a severe threat, potentially granting the attacker root privileges and compromising cloud environments.

In technical terms, the attackers leverage a Python-based exploit disclosed on X (formerly Twitter) by the researcher bl4sty to probe victim environments for the Looney Tunables vulnerability. After identification, Kinsing executes an additional PHP exploit, initially obscured but revealed to be a JavaScript code upon de-obfuscation. The JavaScript code functions as a web shell, providing backdoor access to the server, enabling file manipulation, command execution, and retrieval of system information.

Organizations are advised to monitor for unusual activities related to Linux systems, especially those indicating exploitation of the Looney Tunables vulnerability. Unexplained changes in system configurations, unauthorized access, or abnormal patterns of cloud credential usage should be thoroughly investigated.

To prevent such attacks, it is crucial to apply the latest security patches to Linux systems promptly to mitigate the risk of Looney Tunables exploitation. Enhance cloud security measures by implementing multi-factor authentication, regularly updating credentials, and monitoring CSP activity for anomalies.

In the event of a suspected compromise, organizations should conduct a thorough review of system logs, focusing on Linux systems and cloud infrastructure. Rotate and strengthen credentials associated with cloud services, limiting potential damage caused by unauthorized access.

This development marks a significant shift in Kinsing's tactics, showcasing a heightened focus on cloud environments and a diversified operational scope. Organizations are urged to bolster their defenses promptly to mitigate the evolving threat landscape posed by Kinsing's latest campaign.

MongoDB Investigates Customer Account Data Breach

MongoDB, a leading database provider, recently faced a security incident involving unauthorized access to specific corporate systems. Lena Smart, MongoDB's Chief Information Security Officer, communicated the issue to clients via email, stating that the breach exposed contact details and metadata from consumer accounts. The incident was detected on December 13, prompting MongoDB to activate its incident response procedures.

MongoDB reassured clients that, as of the latest update, there is no evidence of security breaches involving client data stored in MongoDB Atlas. Despite the breach, the company encouraged customers to be vigilant for potential phishing attempts that may leverage the compromised account details and metadata to appear legitimate.

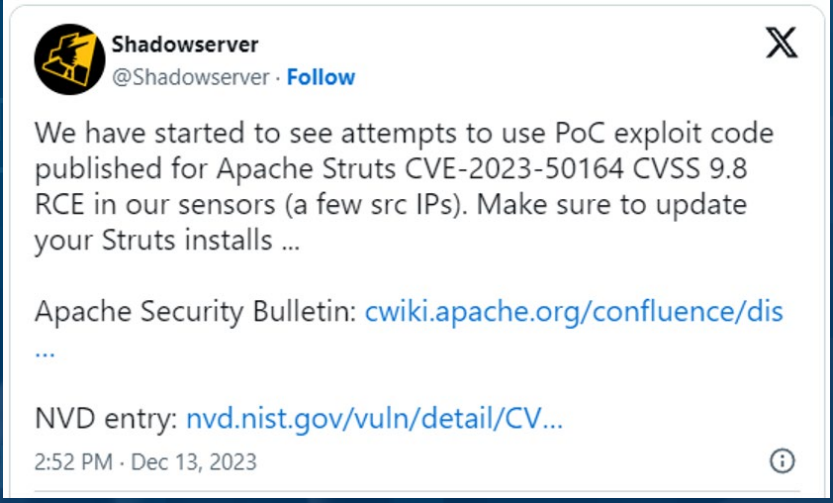
According to Smart, the unauthorized access might have occurred over an extended period before its discovery, and an ongoing active investigation is being conducted to determine the full scope of the incident. Clients were advised to implement phishing-resistant multi-factor authentication (MFA) promptly and consider changing passwords regularly.

A subsequent update from MongoDB clarified that the security breach was unrelated to the recent surge in login attempts causing issues for clients accessing Atlas and its Support Portal. While malicious hackers have historically targeted misconfigured MongoDB databases, leading to data theft and ransom demands, MongoDB hasn't experienced any significant breaches in recent times.

Hackers Are Exploiting Critical Apache Struts Flaw Using Public PoC

Attackers using publicly accessible proof-of-concept exploit code are trying to take advantage of a recently patched major vulnerability (CVE-2023-50164) in Apache Struts that allows for remote code execution.

The Shadowserver scanning platform's researchers saw a modest number of IP addresses involved in exploitation attempts, suggesting that threat actors are still relatively new.



With its form-based interface and powerful integration features, Apache Struts is an open-source web application framework that makes it easier to create Java EE web applications.

Because of the product's effectiveness in creating scalable, dependable, and readily maintained web applications, it is widely utilized in a variety of businesses in both the public and private sectors, including government organizations.

Versions 6.3.0.2 and 2.5.33 of Struts were made available by Apache on December 7 to fix a vulnerability of critical severity that is presently known as CVE-2023-50164.

A path traversal defect, which can be exploited provided specific requirements are met, constitutes the security concern. An attacker may be able to use it to upload malicious files and take control of the target server's remote code execution (RCE). By taking advantage of this vulnerability, a threat actor could alter private files, steal information, interfere with essential services, or

move laterally across the network.

This may result in the following: disruption of vital services; lateral movement inside compromised networks; manipulation or theft of sensitive data; and unauthorized access to web servers.

Struts versions 2.0.0 through 2.3.37 (end of life), 2.5.0 through 2.5.32, and 6.0.0 through 6.3.0 are impacted by the RCE vulnerability.

A technical write-up for CVE-2023-50164 was released on December 10 by a security researcher. It described how a threat actor may taint file upload parameters during an attack. On December 11, the publication of a second write-up included an attack code for the vulnerability.

Cisco Possibly Impacted

Cisco stated in a security alert yesterday that it is looking into CVE-2023-50164 to find out which of its products that use Apache Struts might be impacted and how much.

The Customer Collaboration Platform, Identity Services Engine (ISE), Nexus Dashboard Fabric Controller (NDFC), Unified Communications Manager (Unified CM), Unified Contact Center Enterprise (Unified CCE), and Prime Infrastructure are among the Cisco products that are being examined.

Cisco's security bulletin contains a comprehensive list of potentially affected products; this list is subject to periodic updates with new information.

REFERENCE LINKS

- https://www.cyfirma.com/outofband/from-macro-to-payload-decrypting-the-sidewinder-cyber-intrusion-tactics/?web_view=true
- https://cyware.com/news/decrypting-the-sidewinder-cyber-intrusion-tactics-115065e3
- https://player.fm/series/cyfirma-research/cyfirma-research-from-macro-to-payload-decrypting-the-sidewinder-cyber-intrusion-tactics
- https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-319a
- https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/3am-ransomware-lockbit
- https://www.bleepingcomputer.com/news/security/researchers-link-3am-ransomware-to-conti-royal-cybercrime-gangs/
- https://www.bleepingcomputer.com/news/security/data-breach-at-healthcare-tech-firm-impacts-45-million-patients/?&web_view=true
- https://thehackernews.com/2024/01/uac-0050-group-using-new-phishing.html?&web_view=true
- https://thecyberexpress.com/orrick-data-breach/?&web_view=true
- https://www.helpnetsecurity.com/2024/01/04/consumers-cybersecurity-issue/?web_view=true
- https://thehackernews.com/2024/01/nist-warns-of-security-and-privacy.html?&web_view=true
- https://securityaffairs.com/157769/apt/unc3886-exploits-vcenter-server-zero-day-cve-2023-34048.html?web_view=true
- https://www.helpnetsecurity.com/2024/01/09/delete-stolen-data-ransomware/?web_view=true
- https://www.theregister.com/2024/01/05/swatting_extorion_tactics/?&web_view=true
- https://securityaffairs.com/157079/hacking/cyber-attack-hit-beirut-international-airport.html?web_view=true
- https://securityaffairs.com/157144/cyber-crime/swiss-air-force-data-leak.html?web_view=true
- https://therecord.media/world-council-churches-lutheran-world-federation-cyberattacks?&web_view=true
- https://thehackernews.com/2024/01/turkish-hackers-exploiting-poorly.html?&web_view=true
- https://therecord.media/russia-state-hackers-deploying-malware-nato?&web_view=true

About SDG

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

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

SDG

75 North Water Street
Norwalk, CT 06854

203.866.8886

sdgc.com