SEPTEMBER 2024

Cyber Threat Advisory

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

sdgc.com

Table of Contents

Key Cybersecurity Trends

CXO Summary

Increase in Abuse of URL Rewriting in Phishing

- **Trend:** In recent months, cybercriminals have started abusing URL rewriting, which is a protection feature that replaces links in emails.
- **Impact:** Attackers make sure phishing links appear to be from trusted security vendors and therefore go unnoticed.

Result: This has led to an upsurge of advanced phishing attacks. The very tools that are intended to prevent these attacks are instead being used to enable them.

Healthcare Under Siege by Ransomware

- **Statistics:** In a year, over 21 percent of ransomware attacks were pointed towards healthcare systems. This is up from 18 percent the previous year.
- **Incidents:** There were 200 reported ransomware incidents between August 2023 and July 2024.

Momentum for 'Secure by Design'

- **Initiative:** This was proposed by CISA during this year's RSA to try to curb security gaps and improve efficiency of security.

- **Adoption:** The number of firms that have pledged to impose security on their products has increased

from 70 firms to 200 firms.

Increase in DDoS Attack Volume

- **Statistics:** The total DDoS attacks recorded within the first 6 months of 2024 were at 830,000, an increase of 46% when compared to the first 6 months of 2023.
- **Peak Power:** Peak attack power increased from 1.6 Tbs in the second half of 2023 to 1.7 Tbs in 2024.
- **Targeted Sectors:** Attacks were mostly aimed at the gaming (49%), technology (15%), financial services (12%), and telecommunications (10%) industries.

CRITICAL THREAT ALERT

Focus of the Month: Fileless Malware / Memory Attacks

Fileless malware is a class of cyber threat that does not write traditional files to a victim's system; therefore, it is hard to detect and analyze. Instrumental in performing its payload through exploitation of system memory, fileless malware leverages legitimate tools or employs features that are part of the operating system.

Current Trends and Developments in Fileless Malware:

1. **Higher Sophistication:** Fileless malware attacks are becoming increasingly sophisticated. Attackers now exploit advanced techniques that help hide activities and avoid detection, such as abusing PowerShell, Windows Management Instrumentation, and other scripting languages.
2. **New Techniques:** New ways through which fileless malware can be deployed continue to emerge. For example, attackers could exploit vulnerabilities in web browsers or leverage malicious macros embedded in documents to run their payloads.
3. **Industrial Targeting:** Fileless malware now targets sectors like finance, healthcare, and critical infrastructure, where wide disruption or theft of sensitive information can be caused.
4. **Evasion Strategies:** State-of-the-art fileless malware is excellent at evading traditional antivirus. It mostly resides in memory and often uses legitimate system processes that are difficult to identify with traditional file-based scanning methods.
5. **Ransomware Integration:** Recently, several fileless ransomware attacks have surged. In this category, fileless malware is used for the advanced penetration of a system to deliver ransomware, encrypt files, and then demand a ransom.

Risks and Mitigation:

The risks associated with fileless malware are huge:

- **Data Exfiltration:** Fileless malware can be employed in the theft of extremely sensitive data, such as intellectual property, customers' information, or financial records, with attendant risks of causing financial loss, reputational management, and liability at law.
- **Operation Disruption:** The malware can cause system crashes, network outages, and other connected problems that hurt business continuity. It can result in a lack of productivity, loss of revenue, and customer dissatisfaction.
- **Regulatory Compliance Violations:** In case of one vulnerability, the exploited systems can easily contribute to non-compliance with industry regulations like GDPR and HIPAA, which can result in stiff fines, legal actions, and reputation damage.
- **Indirect Consequences:** Fileless malware may have a ripple effect further than the original breach, using the system as a platform to launch other attacks, including ransomware or supply chain attacks. In turn, this can imply added data breaches, financial losses, and even operational disruption of the organization.

CRITICAL THREAT ALERT

Focus of the Month: Fileless Malware / Memory Attacks

The following strategies should, therefore, be implemented to mitigate the risks of fileless malware:

- **Advanced Threat Detection:** Implement advanced security solutions to identify memory-based threats through anomalous behavior and event correlation across different security layers. These will be driven by behavioral analytics, machine learning, and artificial intelligence techniques that help detect and respond to new threats.
- **Network Segmentation:** Isolate critical systems and data to limit the possible extent of impact in case of a breach. Break the network down into smaller, isolated segments based on function or sensitivity with rigid controls between segments to stop the sideways movement of malware.
- **Keep Systems Updated:** Whether operating systems, applications, or libraries, ensure systems are regularly updated with the latest security patches. This will help close potential vulnerabilities that fileless malware could exploit.
- **Application Whitelisting:** Only allow execution of predefined, trusted applications. This will limit the chances of unauthorized code execution or the execution of malware in a system. Also implement behavior-based intrusion detection; observe the behavior of the system to identify the signs that tell if a malicious attack is occurring. This way, even if it evades otherwise traditional signature-based detection, fileless malware is still detected.
- **Memory Forensics:** Extracting and analyzing memory dumps can help identify and investigate fileless malware attacks. It gives extremely useful information about the tactics and techniques of the attacker.
- **Threat Intelligence Sharing:** Sharing intelligence about emerging threats and best practices for prevention and response enables organizations to stay ahead of the latest threats and improve security postures.
- **Incident Response Planning:** To effectively respond to fileless malware attacks, an organization needs to create a robust incident response plan. This includes activities that would be conducted in case of a breach, such as containing, eradicating, recovering, and conducting a post-incident analysis.
- **Employee Training and Awareness:** Employees should be trained on the risks of fileless malware and how to be secure in general. This will include ways and means to identify and report suspicious activity, avoid phishing activities, and use strong passwords

Monthly Highlights

Email Attacks Skyrocket 293%

Email attacks have skyrocketed by 293% in the first half of 2024 compared to the same period in 2023, according to Acronis. Ransomware detections also surged, with a 32% increase from Q4 2023 to Q1 2024.

In Q1 2024, Acronis identified 10 new ransomware groups responsible for 84 cyberattacks worldwide. Among the top 10 most active ransomware families during this period, three groups—LockBit, Black Basta, and PLAY—were particularly notable, accounting for 35% of all attacks.

The report also highlights the increasing targeting and compromise of Managed Service Providers (MSPs). Notably, phishing, social engineering, vulnerability exploits, credential compromises, and supply chain attacks were identified as the most effective methods for breaching MSPs' cybersecurity defenses.

"As we continue to uncover the growing volume and complexity of cyber threats in the current landscape, it is crucial for MSPs to adopt a holistic approach to securing their customers' data, systems, and unique digital infrastructures," said Irina Artioli, Cyber Protection Evangelist at the Acronis Threat Research Unit.

"To do this effectively, we recommend that MSPs implement a comprehensive security strategy, including mandatory security awareness training and incident response planning, as well as deploying advanced endpoint protection solutions such as extended detection and response (XDR), multi-factor authentication, and more," Artioli added.

Additionally, the report emphasizes emerging cybersecurity trends, particularly the increasing use of generative artificial intelligence (AI) and large language models (LLMs) by threat actors. Specifically, it highlights the growing use of AI in social engineering and automation attacks. The most commonly detected AI-generated attacks include malicious emails, deepfake business email compromise (BEC), deepfake extortion, KYC bypass, and the generation of scripts and malware.

Researchers have identified two main types of AI threats: AI-generated threats, where malware is created using AI techniques but does not use AI in its operations, and AI-enabled malware, which incorporates AI into its functionality.

The top five most frequently observed MITRE ATT&CK techniques in the first half of the year were PowerShell, Windows Management Instrumentation, Process Injection, Data Manipulation, and Account Discovery.

Organizations experienced a 25% increase in email communications, coinciding with a 47% rise in email attacks targeting them. Phishing attempts through malicious URLs affected 26% of users. Social engineering attacks rose by 5% compared to H1 2023, while malware attacks decreased from 11% in H1 2023 to 4% in H1 2024.

Cybercriminals continue to exploit malicious AI tools like WormGPT and FraudGPT. While AI can aid attackers at every stage of the cyberattack kill chain, it also serves as a powerful defense mechanism, enabling around-the-clock detection of attacks and alerting experts to take appropriate response actions to ensure business continuity.

CrowdStrike Outage Renews Supply Chain Concerns, Federal Officials Say

The White House and the U.S. Government Accountability Office (GAO) are expressing concerns about the resilience of the software supply chain and vulnerabilities related to memory safety.

Federal officials have highlighted that the global IT outage caused by a flawed CrowdStrike software update has brought renewed attention to the security of the software supply chain. On Tuesday, the GAO released a report discussing the July 19 outage, which disrupted 8.5 million Microsoft Windows systems. The report noted that the CrowdStrike incident has reignited concerns like those raised during the state-sponsored supply chain attack on SolarWinds in 2020.

The White House, on Thursday, underscored that the CrowdStrike incident emphasizes specific warnings about memory safety issues in software development. These comments build upon a February report that questioned the connection between memory safety concerns and software vulnerabilities.

A spokesperson for the Office of the National Cyber Director (ONCD) told Cybersecurity Dive via email that ONCD has been actively addressing the complex challenge of safeguarding the nation's cybersecurity. As part of implementing the National Cybersecurity Strategy, ONCD is continuing to examine the issue of memory safety vulnerabilities.

In February, ONCD released a report urging the tech industry to adopt memory-safe programming languages and memory-safe chip architectures. The report also called on the research community to enhance the ability to diagnose and measure software security.

Several companies, including SAP, Palantir, and Hewlett Packard Enterprise, have supported the administration's push for memory-safe coding practices.

Microsoft and CrowdStrike are conducting thorough reviews of the outage to determine how such a significant disruption could have been avoided and are exploring ways to prevent similar incidents in the future. Microsoft confirmed in a blog post on Saturday that the faulty software update in CrowdStrike's Falcon platform was linked to a read-out-of-bounds memory safety error in the CSagent.sys driver developed by CrowdStrike.

In February, ONCD released a report urging the tech industry to adopt memory-safe programming languages and memory-safe chip architectures.

CrowdStrike reported that a rapid response content update was released on July 19 to gather more information on new adversary techniques. This content was distributed to Windows hosts running sensor version 7.11 and above, according to CrowdStrike's update. Unfortunately, the update included problematic content that caused affected Windows systems to crash due to an out-of-bounds memory read.

The Cybersecurity and Infrastructure Security Agency (CISA) stated that it is collaborating with government and industry partners to assess the impact of the IT outage and provide additional support.

Beware of Fake AI Tools Masking Very Real Malware Threats

Generative AI (GenAI) is gaining significant attention worldwide, but its rising popularity has also attracted cybercriminals, leading to various cyber threats. While much of the discussion around tools like ChatGPT has focused on how the technology can be exploited to create convincing phishing messages, generate malicious code, or identify vulnerabilities, there is less talk about GenAI being used as bait or a Trojan horse to deliver malware.

Examples of this threat are not hard to find. Last year, for instance, a campaign tricked Facebook users into trying what seemed to be the latest version of Google's legitimate AI tool, "Bard." However, the ads were a front for a malicious fake tool. Such campaigns represent a concerning trend that isn't going away. It's crucial to understand how these schemes work, recognize warning signs, and take precautions to protect your identity and finances.

Cybercriminals have several tactics to trick you into installing malware disguised as GenAI apps, including:

Phishing Sites

In the second half of 2023, ESET blocked over 650,000 attempts to access malicious domains containing "chapgpt" or similar text. Victims often reach these sites by clicking links on social media or in emails and mobile messages. Some of these phishing pages may lead to malware disguised as GenAI software.

Web Browser Extensions

ESET's H1 2024 threat report highlighted a malicious browser extension that users were tricked into installing after being lured by Facebook ads claiming to lead to the official websites of OpenAI's Sora or Google's Gemini. The extension, masquerading as Google Translate, was actually an infostealer known as "Rilide Stealer V4," designed to steal Facebook credentials.

Fake Apps

There have been numerous reports of fake GenAI apps, particularly in mobile app stores. Many of these apps contain malware designed to steal sensitive information such as login credentials, personal identification details, and financial information. Others are scams that generate revenue for developers by promising advanced AI capabilities for a fee, but these apps often bombard users with ads, solicit in-app purchases, or require subscriptions for services that are non-existent or of poor quality.

Malicious Ads

Cybercriminals are leveraging the popularity of GenAI tools to deceive users into clicking on malicious ads, particularly on platforms like Facebook. Meta warned that many of these campaigns are designed to compromise businesses with access to ad accounts across the internet. Attackers hijack legitimate accounts or pages, change their profile information to resemble official ChatGPT or other GenAI-branded pages, and use them to run fake ads. These ads link to supposed new versions of GenAI tools but actually deploy infostealer malware, according to researchers.

The Art of the Lure

Humans are social creatures who are often eager to believe what we're told. We also have a desire to get the latest gadgets and apps, which

cybercriminals exploit by playing on our greed, curiosity, and fear of missing out. To get us to click on malicious links or download malware-infected apps, what's offered must be enticing and believable, often containing a kernel of truth. Social engineers excel at this, persuading us to click on sensational news stories or tempting offers, sometimes even using GenAI to craft stories seamlessly across multiple languages.

How to Avoid Malicious GenAI Lures

- **Install Apps Only from Official App Stores:** Google Play and the Apple App Store have strict vetting processes and regularly monitor for malicious apps. Avoid downloading apps from third-party websites or unofficial sources, as they are more likely to host malicious software.

Before downloading an app, verify the developer's credentials, review other apps they've created, and read user reviews.

- **Double-Check Developers and Reviews:** Before downloading an app, verify the developer's credentials, review other apps they've created, and read user reviews. Suspicious apps often have poorly written descriptions, limited developer history, and negative feedback.
- **Be Wary of Clicking on Digital Ads:** Digital ads, especially on social media, are common vectors for distributing malicious apps. Instead of clicking ads, search for the app or tool in your official app store to ensure you're getting the legitimate version.
- **Check Web Browser Extensions Before Installing:** Web browser extensions can enhance your browsing experience but also pose security risks. Check the developer's background and read reviews before installing. Stick to well-known developers with high ratings and positive feedback.
- **Use Comprehensive Security Software:** Install reputable security software on your PC and mobile devices for real-time protection against malware, phishing, and other online threats.
- **Be Aware of Phishing:** Phishing remains a significant threat. Be cautious of unsolicited messages prompting you to click links or open attachments. Verify the sender's identity before interacting with any suspicious email, text, or social media message.
- **Enable Multi-Factor Authentication (MFA):** MFA adds an extra layer of security to your online accounts by requiring multiple verification methods. Enable MFA wherever possible to protect your accounts even if your password is compromised.
- **Stay Vigilant:** Cybercriminals often exploit the excitement around new releases. If you see an offer to download a new GenAI tool, verify its availability through official channels before proceeding.

Blue Report 2024 Reveals 40% of Environments Exposed to Full Takeover

Each year, cybersecurity evolves, bringing new threats and challenges to the forefront. The Blue Report 2024 takes a comprehensive look at these developments, particularly focusing on the complexities of threat exposure management. Compiled by Picus Labs, this annual study analyzed over 136 million attack simulations to evaluate the effectiveness of current security measures. In this post, we highlight key findings from the report and explain why it's essential reading for cybersecurity professionals and decision-makers.

40% of Environments at Risk of Complete Takeover: A Serious Warning

Imagine an intruder gaining full access to your home with a master key. Now, picture that scenario within your organization's IT infrastructure. The Blue Report 2024 reveals that 40% of tested environments had vulnerabilities that could lead to domain administrator access. "Just like a chain reaction starting from a single domino, minor gaps in cybersecurity can escalate into significant breaches," says Dr. Suleyman Ozarslan, co-founder of Picus Security and VP of Picus Labs. Domain administrator access enables attackers to control user accounts, security settings, and even the entire network, effectively handing cybercriminals the keys to the kingdom.

Prevention is Up, But Detection is Down: A Cyber Defense Paradox

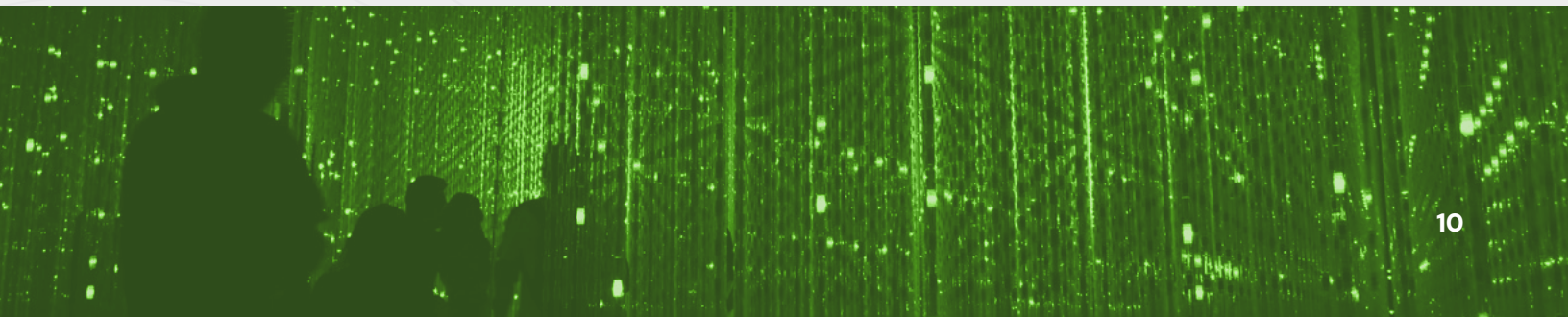
While the effectiveness of preventive measures has improved—from 59% in 2023 to 69% in 2024—detection capabilities have declined, with alert scores dropping from 16% to 12%. This indicates that although we are becoming better at preventing certain attacks, our ability to detect them promptly is still lacking. This highlights the urgent need for a balanced, proactive approach to security.

macOS: The Overlooked Vulnerability in Cybersecurity

The report also uncovers a significant gap in the protection of macOS systems. Security controls on macOS endpoints prevented only 23% of attacks, compared to 62% and 65% for Windows and Linux, respectively. "Although Macs are often perceived as less vulnerable, our findings suggest that security teams are not dedicating enough resources to protect these systems," observes Volkan Ertürk, co-founder and CTO of Picus Security. This is a clear call to action for security teams to bolster defenses for macOS environments.

Ongoing Struggles with Common Passwords and Ransomware

It's alarming to discover that 25% of environments still use easily crackable passwords based on common words. The struggle against ransomware is equally concerning, with organizations managing only a 17% success rate against threats like BlackByte. These findings emphasize the pressing need for more robust and effective cybersecurity measures.



IBM: Cost of a Breach Reaches Nearly $5 Million, With Healthcare Being Hit the Hardest

Businesses that experience a data breach can now expect an average financial impact of nearly $5 million, marking a 10% increase from the previous year, according to IBM's latest annual cybersecurity report. The tech giant, in collaboration with the Ponemon Institute, analyzed 604 organizations affected by data breaches between March 2023 and February 2024. These breaches spanned 17 industries across 16 countries and regions, with records leaked ranging from 2,100 to 113,000 per incident. Additionally, the researchers interviewed 3,556 security and C-suite business leaders who had firsthand knowledge of the breaches within their organizations.

One of the most striking findings in IBM's report is the significant increase in the global average cost of a data breach, which climbed to $4.88 million—the largest spike since the onset of the pandemic. In 2023, the average cost was $4.45 million.

More than half of the organizations surveyed indicated that they are passing these rising breach-related costs on to customers through increased prices for goods and services. "Businesses are now trapped in an ongoing cycle of breaches, containment, and recovery," said Kevin Skapinetz, Vice President at IBM Security. "This cycle frequently involves investing in stronger security measures and transferring breach expenses to consumers—making cybersecurity a new business expense."

IBM arrived at the $4.88 million figure by considering four key activities: detecting the breach, notifying victims, conducting post-breach response efforts, and the lost business resulting from the breach. Costs included those for forensic experts, hotline support, and free credit monitoring—along with indirect expenses such as in-house investigations and potential customer losses.

The report highlights that operational downtime, customer attrition, staffing customer service help desks, and increased regulatory fines have all seen cost increases over the past year. Lost business and post-breach activities alone accounted for $2.8 million, the highest combined figure in the last six years.

More than 45% of the breaches examined involved the compromise of customer personal data, such as tax identification numbers, emails, and addresses. Additionally, intellectual property was exposed in 43% of the breaches.

The report also investigated breaches related to ransomware attacks. Organizations that involved law enforcement during these incidents saw cost savings of up to $1 million, not including any potential ransom payments. Notably, two-thirds of organizations impacted by ransomware chose to involve law enforcement and did not pay ransoms.

Healthcare Sectors See Significant Impacts

The healthcare industry continues to lead all sectors in breach costs, with an average of $9.77 million per incident—maintaining its top position since 2011. The industrial sector experienced the largest year-over-year increase, with breach costs rising by $830,000 on average. This sector, which includes chemical processing, engineering, and manufacturing, is heavily regulated and particularly vulnerable to the effects of operational downtime.

Among the 16 countries and regions studied, the United States reported the highest breach costs for the 14th consecutive year, with an average of $9.36 million. While Canada and Japan saw decreases in their average breach costs, Italy and countries in the Middle East experienced significant increases.

The majority of breaches were traced back to phishing attacks or compromised credentials, with breaches resulting from phishing costing an average of $4.88 million and those from compromised credentials costing $4.81 million.

Most CISOs Feel Unprepared for New Compliance Regulations

With the introduction of stringent new regulations, such as the SEC's cybersecurity disclosure rules in the USA and the Digital Operational Resilience Act (DORA) in the EU, many organizations are facing significant challenges, according to Onyxia Cyber.

The Evolving Role of the CISO

The role of the Chief Information Security Officer (CISO) has undergone a significant transformation in recent years. What was once a primarily technical position focused on cybersecurity has now expanded to include a stronger emphasis on security strategy and the assessment and mitigation of business risks. As compliance regulations tighten and the cost of data breaches continues to rise, executives are increasingly recognizing the importance of giving cybersecurity leaders a seat at the decision-making table.

Despite this recognition, 67% of CISOs report feeling unprepared for these new compliance regulations, and 52% acknowledge needing more knowledge about how to report cyberattacks to government authorities.

"As cyber threats intensify and regulations impose heavy penalties for non-compliance, it's crucial for CISOs to reassess and strengthen their security programs in a data-driven manner. Our survey highlights critical industry benchmarks, revealing areas of strength as well as significant gaps that require urgent attention," said Sivan Tehila, CEO of Onyxia. "CISOs must enhance their preparedness, improve security hygiene, and embrace new technologies like AI to maximize the effectiveness of their existing security tools and better protect their organizations."

Incident Response and Communication Challenges

The survey also revealed that 56% of CISOs are uncomfortable with their current incident response strategies, indicating a significant need for improvement in handling cyber incidents effectively.

As regulations evolve, many organizations struggle with inadequate guidance and unclear definitions, such as what constitutes a "material" incident.

Furthermore, 67% of CISOs report difficulties in effectively convincing the C-suite of the importance of their security strategies and securing buy-in for their initiatives. Interestingly, only 19% of CISOs with over five years of experience find it very easy to communicate their strategy to the executive board, compared to 40% of less experienced CISOs.

Potential of AI in Cybersecurity

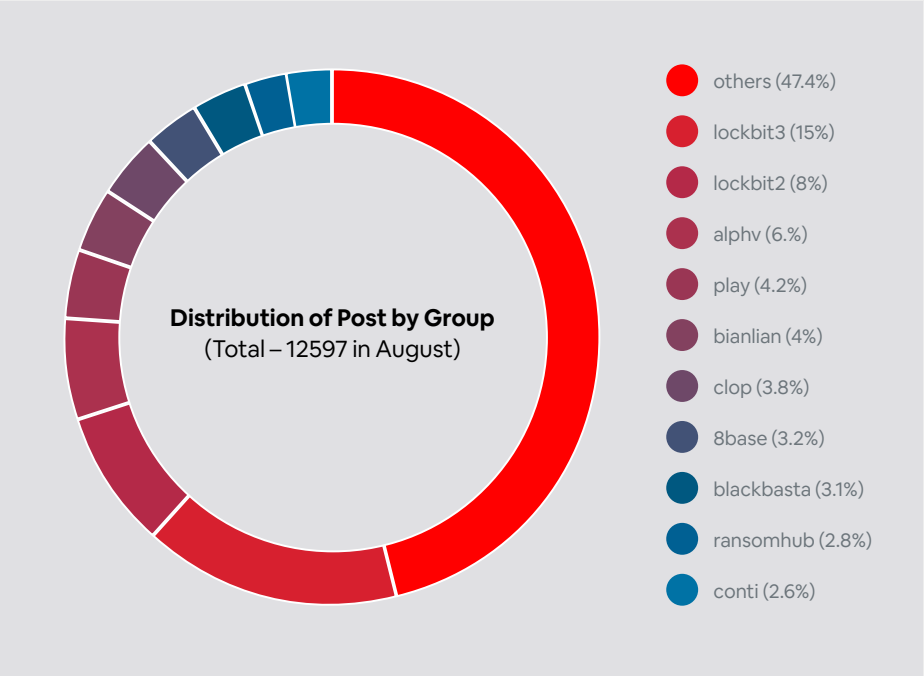
Basic security measures, such as multi-factor authentication (MFA) and strong passwords, are still not universally implemented. On average, CISOs consider 11% of user accounts with weak passwords and 13% without MFA as acceptable, highlighting areas needing improvement.

Despite relying heavily on manual methods, such as spreadsheets and analysts, to measure the effectiveness of their security programs, CISOs are increasingly optimistic about the potential of AI.

A substantial 97% of CISOs believe that AI can enhance risk management, with 54% seeing AI as a tool to identify gaps and redundancies in their security stack, and 42% anticipating AI's role in automating business-level risk reporting.

"Our industry is in a phase of evolution," said Chris Roberts, Onyxia Cyber CISO Advisor. "We are at a point where business drivers, leadership discussions, and legal, compliance, and regulatory accountability are taking center stage over other concerns. This report provides an honest assessment of where we stand, the progress we've made, and the challenges that remain ahead."

Ransomware Tracker



Articles

#StopRansomware: Phobos Ransomware

The Phobos ransomware has been a source of concern for government and critical infrastructure entities. U.S. cybersecurity and intelligence agencies have issued warnings about the threat actors' varied strategies and methods for spreading the malware that encrypts files.

The Phobos ransomware operates on a ransomware-as-a-service (RaaS) model. Its attackers have successfully held several million dollars in ransom by targeting various entities such as emergency services, education, public healthcare, and critical infrastructure.

These attacks succeeded in holding several million dollars in ransom for emergency services, public healthcare, education, local and county governments, and other vital infrastructure organizations.

According to the agencies, Phobos actors have been seen exploiting built-in Windows API functions to generate new processes that escalate privileges by utilizing the SeDebugPrivilege process, steal tokens, and get around access controls. Up until they gain domain administrator access, Phobos actors try to authenticate on victim computers using password hashes that have been cached.

Detection

Open-source reporting indicates that similar TTPs found in Phobos intrusions are probably connected to many variants of the ransomware, such as Elking, Eight, Devos, Backmydata, and Faust.

The Phobos ransomware functions in tandem with multiple open-source tools, including Bloodhound, Cobalt Strike, and Smokeloader. Given their accessibility and ease of use across multiple operating systems, these tools—as well as their related variants—are a preferred option for numerous threat actors.

Reconnaissance and Initial Access

Phobos actors usually use one of these methods to get initial access to vulnerable networks: either they use phishing campaigns to drop hidden payloads, or they use IP scanning tools like Angry IP Scanner to look for vulnerable ports on the Remote Desktop Protocol (RDP), or they use RDP on Microsoft Windows environments.

The actors use free and open-source brute force tools to break into an RDP server once they find one. After successfully authenticating via RDP in the intended environment, Phobos actors conduct open-source research to construct a victim profile and link the targeted IP addresses to the businesses that are connected to them.

Execution and Privilege Escalation

Phobos actors utilize executables such as cmd.exe or 1saas.exe to launch extra Phobos payloads that are enabled for elevated privileges. The aforementioned commands can also be used by Phobos actors to carry out different Windows shell tasks.

Threat actors can take control of different parts of a system with the Windows command shell, since different commands require different permission levels.

Persistence and Privilege Escalation

The Phobos ransomware reportedly makes use of commands like Exec.exe and the bcdedit[.] exe control mechanism, according to reports from open sources. In order to stay persistent in compromised environments, Phobos has also been seen to use Windows Startup folders and Run Registry Keys like C:/Users\Admin\AppData\ Local\directory.

Furthermore, Phobos actors have been seen exploiting SeDebugPrivilege process to create new processes, circumvent access controls, and steal tokens through built-in Windows API functions. Up until they gain domain administrator access, Phobos actors try to authenticate on victim computers using password hashes that have been cached.

Discovery and Credential Access

Phobos actors count the active directory using open-source tools like Bloodhound and Sharphound. Additionally, NirSoft and Mimikatz have been utilized, along with Remote Desktop Passview for exporting browser client credentials. The Phobos ransomware can also encrypt user files, list all connected storage devices, and list active processes.

Exfiltration

Mega.io and WinSCP have been seen to be used by Phobos actors for file exfiltration. They connect straight to an FTP server they control via a victim network using WinSCP. Via the installation of Mega.io, Phobos actors can export victim files straight to a cloud storage service. Usually, data is archived as a zip or RAR file so it can be later exfiltrated. They look for frequently used password management software in databases, financial records, technical documents (including network architecture), and legal documents.

Impact

The Phobos actors then search for backups following the exfiltration stage. In Windows environments, they find and remove volume shadow copies using the Windows Management Instrumentation command-line utility (WMIC) and vssadmin.exe. This keeps victims from being able to recover files once encryption has occurred.

On the target host, Phobos.exe has the ability to encrypt all connected logical drives. Unique build identifiers (IDs), affiliate IDs, and an embedded ransom note are all present in every Phobos ransomware executable.

Indicators of Compromise (IOCs):

Associated Phobos Domains
adstat477d[.]xyz
demstat577d[.]xyz [12]
serverxlogs21[.]xyz
Shell Commands
vssadmin delete shadows /all /quiet
netsh advfirewall set currentprofile state off
wmic shadowcopy delete
netsh firewall set opmode mode=disable

bcdedit /set {default} bootstatuspolicy ignoreallfailures
bcdedit /set {default} recoveryenabled no
wbadmin delete catalog -quiet
mshta C:\%USERPROFILE%\Desktop\info.hta
mshta C:\%PUBLIC%\Desktop\info.hta
mshta C:\info.hta

Registry Keys

HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\<Phobos exe name>
C:/Users\Admin\AppData\Local\directory

Email Addresses

AlbetPattisson1981@protonmail[.]com	henryk@onionmail[.]org
atomicday@tuta[.]io	info@fobos[.]one
axdus@tuta[.]io	it.issues.solving@outlook[.]com
barenuckles@tutanota[.]com	JohnWilliams1887@gmx[.]com
Bernard.bunyan@aol[.]com	jonson_eight@gmx[.]us
bill.g@gmx[.]com	joshuabernandead@gmx[.]com
bill.g@msgsafe[.]io	LettoIntago@onionmail[.]com
bill.g@onionmail[.]org	Luiza.li@tutanota[.]com
bill.gTeam@gmx[.]com	MatheusCosta0194@gmx[.]com
blair_lockyer@aol[.]com	mccreight.ellery@tutanota[.]com
CarlJohnson1948@gmx[.]com	megaport@tuta[.]io
cashonlycash@gmx[.]com	miadowson@tuta[.]io
chocolate_muffin@tutanota[.]com	MichaelWayne1973@tutanota[.]com
claredrinkall@aol[.]com	normanbaker1929@gmx[.]com
clausmeyer070@cock[.]li	nud_satanakia@keemail[.]me
colexpro@keemail[.]me	please@countermail[.]com
cox.barthel@aol[.]com	precorpman@onionmail[.]org
crashonlycash@gmx[.]com	recovery2021@inboxhub[.]net
everymoment@tuta[.]io	recovery2021@onionmail[.]org
expertbox@tuta[.]io	SamuelWhite1821@tutanota[.]com
fastway@tuta[.]io	SaraConor@gmx[.]com
fquatela@techie[.]com	secdatltd@gmx[.]com
fredmoneco@tutanota[.]com	skymix@tuta[.]io

getdata@gmx[.]com	sory@countermail[.]com
greenbookBTC@gmx[.]com	spacegroup@tuta[.]io
greenbookBTC@protonmail[.]com	stafordpalin@protonmail[.]com
helperfiles@gmx[.]com	starcomp@keemail[.]me
helpermail@onionmail[.]org	xdone@tutamail[.]com
helpfiles@onionmail[.]org	xgen@tuta[.]io
helpfiles102030@inboxhub[.]net	xspacegroup@protonmail[.]com
helpforyou@gmx[.]com	zgen@tuta[.]io
helpforyou@onionmail[.]org	zodiacx@tuta[.]io

Telegram Username
@phobos_support

Wickr Address
Vickre me
IP Address
194.165.16[.]4
45.9.74[.]14
147.78.47[.]224
185.202.0[.]111

Phobos Ransomware SHA 256 Malicious Trojan Executable File Hashes
518544e56e8ccee401ffa1b0a01a10ce23e49ec21ec441c6c7c3951b01c1b19c
9215550ce3b164972413a329ab697012e909d543e8ac05d9901095016dd3fc6c
482754d66d01aa3579f007c2b3c3d0591865eb60ba60b9c28c66fe6f4ac53c52
c0539fd02ca0184925a932a9e926c681dc9c81b5de4624250f2dd885ca5c4763

Phobos Ransomware SHA 256 File Hashes
58626a9bfb48cd30acd0d95debcaefd188ae794e1e0072c5bde8adae9bccafa6
f3be35f8b8301e39dd3dffc9325553516a085c12dc15494a5e2fce73c77069ed
518544e56e8ccee401ffa1b0a01a10ce23e49ec21ec441c6c7c3951b01c1b19c
32a674b59c3f9a45efde48368b4de7e0e76c19e06b2f18afb6638d1a080b2eb3
2704e269fb5cf9a02070a0ea07d82dc9d87f2cb95e60cb71d6c6d38b01869f66
fc4b14250db7f66107820ecc56026e6be3e8e0eb2d428719156cf1c53ae139c6
a91491f45b851a07f91ba5a200967921bf796d38677786de51a4a8fe5ddeafd2

Remediation

- Secure remote access software.
- Implement application controls to manage and control execution of software, including allowlisting remote access programs.
- Use intrusion detection systems and best practices for log collection to protect the organization from threat actors.
- Strictly limit use of RDP and other remote desktop services.
- Turn off permissions and command-line and scripting operations
- Check for new or unfamiliar accounts on domain controllers, servers, workstations, and active directories.
- Examine user accounts that possess administrative privileges and set up access controls based on the least privilege principle.
- Diminish the risk of compromised credentials
- Put time-based access controls in place for admin-level and above accounts.
- Create a recovery plan to ensure that servers and sensitive or proprietary data are kept in multiple copies.

Prevention

- Keep offline data backups and periodically perform backup and restoration (at least once a day or once a week).
- Make it mandatory for all accounts requiring a password to adhere to guidelines for creating and maintaining password policies.
- Make all services subject to phishing-resistant multifactor authentication (MFA).
- Install antivirus software on all hosts, keep it up to date, and allow real-time detection.
- Turn off any unused protocols and ports.
- Think about including a banner when receiving emails from individuals outside of your company.
- Turn off hyperlinks in emails you've received.
- Make sure every backup file is unchangeable, encrypted, and encompasses the entire data infrastructure of the company.

APT41's Global Cyber Espionage Campaign: A Comprehensive Analysis

Executive Summary

- **Threat Actor:** APT41, a Chinese state sponsored group, targeted multiple global sectors.
- **Affected Sectors:** Shipping and logistics, media and entertainment, technology, and automotive sectors.
- **Geographic Spread:** Targeted victims primarily located in Italy, Spain, Taiwan, Thailand, Turkey, and the UK.
- **Intrusion Techniques:** Utilized ANTSWORD and BLUEBEAM web shells, DUSTPAN dropper, and DUSTTRAP plugin framework for prolonged access.
- **Data Exfiltration:** Employed SQLULDR2 and PINEGROVE to export and exfiltrate sensitive data.
- **Operational Sophistication:** Used stolen code signing certificates and advanced persistence techniques.

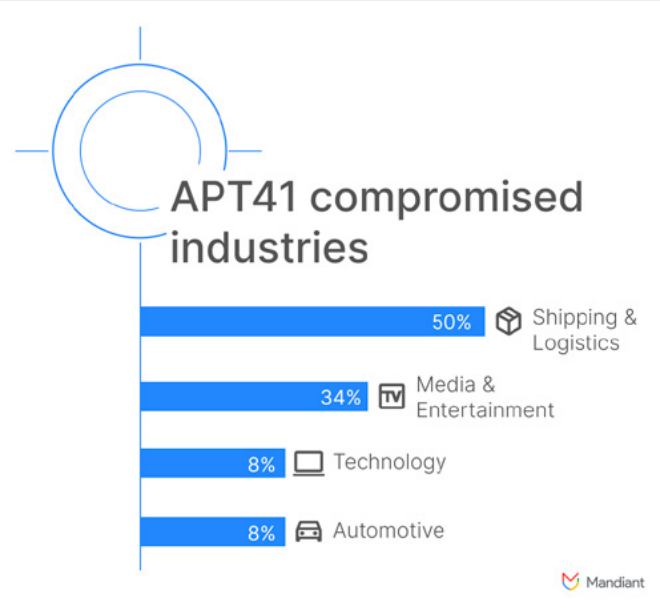


Figure 1. Sectors impacted by APT41's DUSTTRAP campaigns in 2024
Source: Mandiant

Detection

Web Shell Deployment

APT41 utilized ANTSWORD and BLUEBEAM web shells on Tomcat Apache Manager servers, active since 2023. These were used to execute `certutil.exe` to download the DUSTPAN dropper, which stealthily loaded the BEACON backdoor.

DUSTTRAP Deployment

APT41 escalated their tactics by deploying the DUSTTRAP dropper, which decrypted a payload to establish C&C communication with either APT41 infrastructure or compromised Google Workspace accounts. These accounts were later remediated.

Reconnaissance and Victimology

APT41 targeted organizations across multiple continents, with specific interest in the shipping and logistics sectors in Europe and the Middle East and media and entertainment sectors in Asia. Reconnaissance activities were also directed at similar organizations in other regions, such as Singapore.

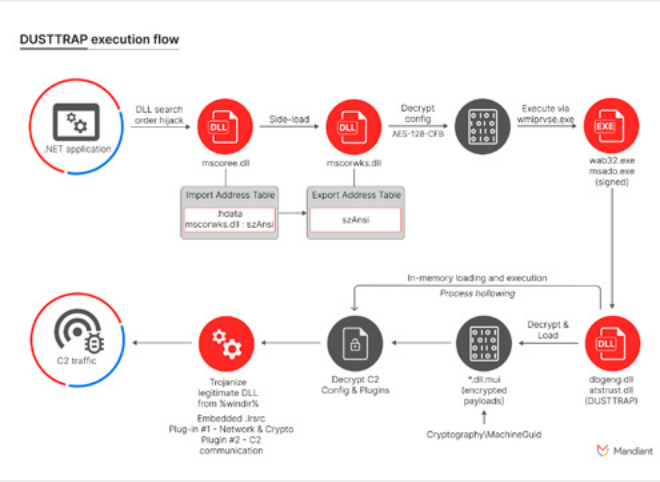


Figure 2. Full execution flow of DUSTTRAP
Source: Mandiant

Indicators of Compromise (IOCs):

Filename	MD5	Family
sqluldr.exe	fcff642268898fcf65702a214aefbf9e	SQLULDR2
OneDriveUploader.exe	ac125aea0b703de37980779599438b4a	PINEGROVE
aclui.dll	17d0ada8f5610ff29f2e8eaf0e3bb578	DUSTPAN
dbgeng.dll	9991ce9d2746313f505dbf0487337082	DUSTTRAP
dbgeng.dll	c33247bc3e7e8cb72133e47930e6ddad	DUSTTRAP
hostfxr.dll	cfce85548436fb89a83bf34dc17f325d	DUSTTRAP
dbgeng.dll	e98b9e21928252332edf934f3d18ac21	DUSTTRAP
dbgeng.dll	8222352a61eacca3a1c6517956aa0b55	DUSTTRAP
-	dc725f5e9b1ae062fbec86ee4d816b45	DUSTTRAP
Sbiedll.dll	d72f202c1d684c9a19f075290a60920f	DUSTTRAP
atstrust.dll	393065ef9754e3f39b24b2d1051eab61	DUSTTRAP
-	0e74285f3359393e57f5d49c156aca47	DUSTTRAP
conn.exe	35f650c94faf6a2068e8238dd99edbea	DUSTPAN
PrintWorkflowUserSvc_	3bb44c0dd7f424864d76d4df09538cb6	DUSTPAN
a0c15f9d.dll / cbi.dll		
dbgeng.dll	aca5c6daecf463012a09564764584937	DUSTTRAP
-	336a0d6f8cc92bf9740ce17de600463b	DUSTTRAP
-	6bc4a92ff4d2cfc9da91ae6a5d2ad3d5	DUSTTRAP
-	a689e182fe33b9d564dddc35412ea0a7	DUSTTRAP
-	e4a4aafb49b8c86a5ac087ae342c0ee6	DUSTTRAP
-	e584119a4766e6cf49093c666965c8be	DUSTTRAP
-	f1769ad5a9dc44794895275c656ed484	DUSTTRAP

Value	Family	Comment
ns2[.]akacur[.]tk	BEACON	-
ns1[.]akacur[.]tk	BEACON	-
orange-breeze-66bb[.]tezsfsoikdvd[.]workers[.]dev	BEACON	-
www[.]eloples[.]com	DUSTTRAP	First observed at 2024-02-21Last observed at 2024-07-16
95.164.16[.]231	-	Related to DUSTTRAP FQDN www[.]eloples[.]com
152.89.244[.]185	-	Used to deliver DUSTPAN
		First activity observed at 2023-03-21
hxxp://152.89.244[.]185/conn.exe	-	Used to deliver DUSTPAN
		First activity observed at 2023-03-21

Prevention

- **Restrict Web Shell Activity:** Regularly scan and monitor web servers for unauthorized web shells, particularly on critical infrastructure like Tomcat Apache Manager servers.
- **Enhance EDR Solutions:** Ensure EDR systems are updated to detect sophisticated malware like DUSTPAN and DUSTTRAP, which use advanced evasion techniques.
- **Secure Database Access:** Limit access to critical databases and monitor for unusual data export activities, especially using tools like SQLULDR2.
- **Strengthen Cloud Security:** Implement strict controls and monitoring on cloud services like Google Workspace and OneDrive to prevent unauthorized data exfiltration.

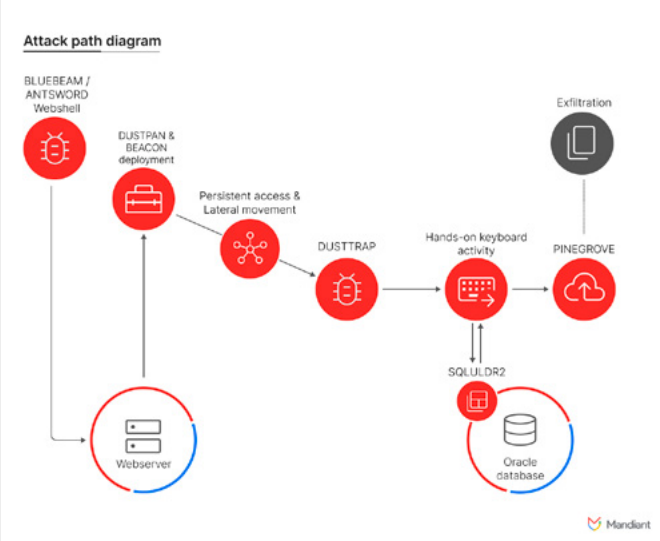


Figure 3. Attack path diagram of observed APT41 attack
Source: Mandiant

Remediation

- **Web Shell Removal:** Identify and remove all instances of ANTSWORD and BLUEBEAM web shells from compromised servers.
- **DUSTPAN and DUSTTRAP Eradication:** Use memory forensic tools to detect and remove DUSTPAN and DUSTTRAP from infected systems. Ensure that these tools are configured to detect fileless malware and in-memory payloads.
- **Data Exfiltration Mitigation:** Investigate and halt any ongoing data exfiltration using SQLULDR2 and PINEGROVE, and secure all affected cloud accounts.
- **Certificate Revocation:** Revoke any compromised code signing certificates and update software to remove any reliance on these certificates.

APT41's campaign highlights the evolving nature of cyber threats, particularly those from state sponsored actors who blend espionage with financially motivated activities. Organizations must adopt a proactive and layered defense strategy to detect, prevent, and remediate such sophisticated intrusions. Continued vigilance and collaboration among security researchers and organizations are key to mitigating the risks posed by threat actors like APT41.

Understanding and Defending Against North Korean Cyber Espionage and Ransomware Operations - Andariel

Executive Summary

Source: ASEC

- The RGB 3rd Bureau, a North Korean state-sponsored cyber group, also known as Andariel, Onyx Sleet, DarkSeoul, Silent Chollima, and Stonefly/Clasiopa, poses a significant threat to global industries, particularly in defense, aerospace, nuclear, and engineering sectors.
- This group is known for its sophisticated cyber espionage and ransomware operations. They exploit vulnerabilities like Log4j to gain initial access and use a range of custom and dual use tools for execution, lateral movement, and data exfiltration.
- Organizations are advised to apply timely patches, protect web servers, monitor endpoints, and strengthen authentication measures to defend against these threats.

Threat Overview

RGB 3rd Bureau, operating from North Korea, targets high-value sectors to advance military and nuclear objectives. The group's activities include:

- **Cyber Espionage:** Targeting sensitive information related to defense, aerospace, nuclear, and engineering sectors.
- **Ransomware Operations:** Funding espionage activities through ransomware attacks on U.S. healthcare entities.

Detection

Initial Access

- **Exploitation of Vulnerabilities:** The group exploits known vulnerabilities in web servers, such as Log4j (CVE202144228), to deploy web shells and gain access. They also use phishing tactics with malicious attachments (e.g., LNK files, HTA scripts).

Execution

- **Command Line and Scripting:** Utilization of native tools and commands like `netstat` and `curl` for system enumeration and execution.
- **Custom Malware:** Deployment of malware such as MagicRAT and AndarLoader for remote access and lateral movement.

Defense Evasion

- **Malware Packing:** Use of VMProtect and Themida to obscure malware, making detection more challenging.

Credential Access

- **Credential Theft Tools:** Use of Mimikatz and ProcDump to extract credentials and access additional systems.

Discovery and Lateral Movement

- **File System Enumeration:** Use of custom .NET tools and SMB protocol for directory and file enumeration.
- **RDP Usage:** Use of Remote Desktop Protocol (RDP) for lateral movement.

Command and Control

- **Tunneling Techniques:** Use of 3Proxy, PLINK, and Stunnel to disguise and tunnel C2 traffic.

Collection and Exfiltration

- **Data Exfiltration Methods:** Use of WinRAR and WinSCP for data collection and transfer to cloud services or North Korea controlled servers.

Indicators Of Compromise (IOCs):

Type	Hashes
SHA256	ed8ec7a8dd089019cfd29143f008fa0951c56a35d73b2e1b274315152d0c0ee6
SHA256	db6a9934570fa98a93a979e7e0e218e0c9710e5a787b18c6948f2eedd9338984
SHA256	773760fd71d52457ba53a314f15dddb1a74e8b2f5a90e5e150dea48a21aa76df
SHA256	05e9fe8e9e693cb073ba82096c291145c953ca3a3f8b3974f9c66d15c1a3a11d
SHA256	e3027062e602c5d1812c039739e2f93fc78341a67b77692567a4690935123abe
SHA256	1962ebb7bf8d2b306c6f3b55c3dcd69a755eeff1a17577b7606894b781841c3a
SHA256	f226086b5959eb96bd30dec0ffcbf0f09186cd11721507f416f1c39901addafb
SHA256	6db57bbc2d07343dd6ceba0f53c73756af78f09fe1cb5ce8e8008e5e7242eae1
SHA256	b7435d23769e79fcbe69b28df4aef062685d1a631892c2354f96d833eae467be
SHA256	66415464a0795d0569efa5cb5664785f74ed0b92a593280d689f3a2ac68dca66
SHA256	def2f01fbd4be85f48101e5ab7ddd82efb720e67daa6838f30fd8dcda1977563
SHA256	323cbe7a3d050230cfaa822c2a22160b4f8c5fe65481dd329841ee2754b522d9
SHA256	74529dd15d1953a47f0d7ecc2916b2b92865274a106e453a24943ca9ee434643
SHA256	1e4de822695570421eb2f12fdfe1d32ab8639655e12180a7ab3cf429e7811b8f
SHA256	8ce219552e235dcaf1c694be122d6339ed4ff8df70bf358cd165e6eb487ccfc5
SHA256	c2904dc8bbb569536c742fca0c51a766e836d0da8fac1c1abd99744e9b50164f
SHA256	dda53eee2c5cb0abdbf5242f5e82f4de83898b6a9dd8aa935c2be29bafc9a469
SHA256	90fb0cd574155fd8667d20f97ac464eca67bdb6a8ee64184159362d45d79b6a4
SHA256	452ca47230afd4bb85c45af54fcacbfa544208ef8b4604c3c5caefe3a64dcc19
SHA256	199ba618efc6af9280c5abd86c09cdf2d475c09c8c7ffc393a35c3d70277aed1
SHA256	2eb16dbc1097a590f07787ab285a013f5fe235287cb4fb948d4f9cce9efa5dbc

SHA256	ce779e30502ecee991260fd342cc0d7d5f73d1a070395b4120b8d300ad11d694
SHA256	db6a9934570fa98a93a979e7e0e218e0c9710e5a787b18c6948f2eedd9338984
SHA256	c28bb61de4a6ad1c5e225ad9ec2eaf4a6c8ccfff40cf45a640499c0adb0d8740
SHA256	34d5a5d8bec893519f204b573c33d54537b093c52df01b3d8c518af08ee94947
SHA256	664f8d19af3400a325998b332343a9304f03bab9738ddab1530869eff13dae54
SHA256	772b06f34facf6a2ce351b8679ff957cf601ef3ad29645935cb050b4184c8d51
SHA256	aa29bf4292b68d197f4d8ca026b97ec7785796edcb644db625a8f8b66733ab54
SHA256	9a5504dcfb7e664259bfa58c46cfd33e554225daf1cedea2ec2a9d83bbbfe238
SHA256	c2500a6e12f22b16e221ba01952b69c92278cd05632283d8b84c55c916efe27c
SHA256	8aa6612c95c7cef49709596da43a0f8354f14d8c08128c4cb9b1f37e548f083b
SHA256	38f0f2d658e09c57fc78698482f2f638843eb53412d860fb3a99bb6f51025b07

Prevention

Mitigating Exploits

- **Patch Management:** Apply patches for vulnerabilities, especially Log4j-related issues, promptly.
- **Web Server Protection:** Implement Web Application Firewalls (WAFs) and use reverse proxies for web-facing servers.

Endpoint Protection

- **Endpoint Monitoring:** Deploy endpoint security tools and monitor for unusual activities.
- **Network Segmentation:** Segment networks to prevent lateral movement from compromised systems.

Authentication and Access Control

- **Multi-Factor Authentication:** Use MFA for remote access services to enhance security.

Command Line and Remote Access Monitoring

- **Monitor Command-Line Activity:** Monitor for suspicious command-line activity and unauthorized use of dual-use tools.

Packing Detection

- **Anti-Packing Measures:** Be aware of malware packed with commercial tools like VMProtect and Themida.

Remediation

Incident Response

- **Detection and Response:** Follow best practices for incident detection and response as outlined in relevant advisories.
- **Data Encryption:** Encrypt sensitive data and update passwords if compromised.

Reporting and Alerts

- **Report Suspicious Activities:** Notify relevant authorities of any suspected North Korean cyber activities.
- **Rewards for Justice:** U.S. and ROK governments offer rewards for information on DPRK cyber operations through the Rewards for Justice program.

Top Exploited Vulnerabilities

Vulnerability Name	Description	References
Autel MaxiCharger AC Elite Business C50 AppAuthenExchangeRandomNum Stack-Based Buffer Overflow Remote Code Execution Vulnerability CVE-2024-7795	Vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of Autel MaxiCharger AC Elite Business C50 EV chargers. 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://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2024-7795
Autodesk AutoCAD DWF File Parsing Out-Of-Bounds Write Remote Code Execution Vulnerability CVE-2024-7305	Vulnerability allows remote attackers to execute arbitrary code on affected installations of Autodesk AutoCAD. 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://www.autodesk.com/trust/security-advisories/adsk-sa-2024-0014
Ivanti Avalanche deleteSkin Directory Traversal Arbitrary File Deletion Vulnerability CVE-2024-38652	Vulnerability allows remote attackers to delete arbitrary files on affected installations of Ivanti Avalanche. The issue results from the lack of proper validation of a user-supplied path prior to using it in file operations.	https://forums.ivanti.com/s/article/Security-Advisory-Ivanti-Avalanche-6-4-4-CVE-2024-38652-CVE-2024-38653-CVE-2024-36136-CVE-2024-37399-CVE-2024-37373?language=en_US
Microsoft Office PowerPoint PPTX File Parsing Use-After-Free Remote Code Execution Vulnerability CVE-2024-38171	Vulnerability allows remote attackers to execute arbitrary code on affected installations of Microsoft Office PowerPoint. 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-2024-38171
Microsoft Office Visio VSDX File Parsing Out-Of-Bounds Write Remote Code Execution Vulnerability CVE-2024-38169	Vulnerability allows remote attackers to execute arbitrary code on affected installations of Microsoft Office Visio. 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://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38169
Adobe Substance 3D Stager SKP File Parsing Use-After-Free Remote Code Execution Vulnerability CVE-2024-39388	Vulnerability allows remote attackers to execute arbitrary code on affected installations of Adobe Substance 3D Stager. The specific flaw exists within the parsing of SKP files.	https://helpx.adobe.com/security/products/substance3d_stager/apsb24-60.html
Adobe Dimension SKP File Parsing Out-Of-Bounds Write Remote Code Execution Vulnerability CVE-2024-34124	Vulnerability allows remote attackers to execute arbitrary code on affected installations of Adobe Dimension. 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://helpx.adobe.com/security/products/dimension/apsb24-47.html
Adobe Bridge AVI FIle Parsing Out-Of-Bounds Write Remote Code Execution Vulnerability CVE-2024-39386	Vulnerability allows remote attackers to execute arbitrary code on affected installations of Adobe Bridge. The issue results from the lack of proper validation of user-supplied data, which can result in a write past the end of an allocated buffer.	https://helpx.adobe.com/security/products/bridge/apsb24-59.html
Adobe Acrobat Reader DC AcroForm Use-After-Free Remote Code Execution Vulnerability CVE-2024-41831	Vulnerability allows remote attackers to execute arbitrary code on affected installations of Adobe Acrobat Reader DC. The issue results from the lack of validating the existence of an object prior to performing operations on the object.	https://helpx.adobe.com/security/products/acrobat/apsb24-57.html
Magnet Forensics AXIOM Command Injection Remote Code Execution Vulnerability CVE-2024-7448	Vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of Magnet Forensics AXIOM. The specific flaw exists within the Android device image acquisition functionality.	https://docs.magnetforensics.com/docs/axiom/release_notes.html
Samsung MagicInfo Server getFileFromMultipartFile Directory Traversal Remote Code Execution Vulnerability CVE-2024-7399	Vulnerability allows remote attackers to execute arbitrary code on affected installations of Samsung MagicInfo Server. The specific flaw exists within the getFileFromMultipartFile method.	https://security.samsungtv.com/securityUpdates
Foxit PDF Reader AcroForm Use-After-Free Remote Code Execution Vulnerability CVE-2024-7725	Vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit PDF Reader. The specific flaw exists within the handling of AcroForms.	https://www.foxit.com/support/security-bulletins.html
(Pwn2Own) QNAP TS-464 Netmgr Endpoint Command Injection Remote Code Execution Vulnerability CVE-2024-32765	Vulnerability allows remote attackers to execute arbitrary code on affected installations of QNAP TS-464 NAS devices. The specific flaw exists within the legacy_api endpoints, resulting from the lack of proper validation of a user-supplied string before using it to execute a system call.	https://www.qnap.com/en/security-advisory/qsa-24-14

Continued on next page >

Top Exploited Vulnerabilities

Apple macOS AppleVADriver Out-Of-Bounds Write Remote Code Execution Vulnerability CVE-2024-27829	Vulnerability allows remote attackers to execute arbitrary code on affected installations of Apple macOS. The issue results from the lack of proper validation of user-supplied data, which can result in a write past the end of an allocated buffer.	https://support.apple.com/en-ca/120903
Apple macOS AMDRadeonX6000MTLDriver KTX Parsing Out-Of-Bounds Write Remote Code Execution Vulnerability CVE-2024-27857	Vulnerability allows remote attackers to execute arbitrary code on affected installations of Apple macOS. The specific flaw exists within the AMDRadeonX6000MTLDriver. Crafted data in a KTX file can trigger a write past the end of an allocated buffer.	https://support.apple.com/en-ca/120906
Logsign Unified SecOps Platform Directory Traversal Arbitrary Directory Deletion Vulnerability CVE-2024-7603	Vulnerability allows remote attackers to delete arbitrary directories on affected installations of Logsign Unified SecOps Platform. The specific flaw exists within the HTTP API service, which listens on TCP port 443 by default.	https://support.logsign.net/hc/en-us/articles/20617133769362-07-08-2024-Version-6-4-23-Release-Notes
Apache OFBiz resolveURI Authentication Bypass Vulnerability CVE-2024-38856	Vulnerability allows remote attackers to bypass authentication on affected installations of Apache OFBiz. Authentication is not required to exploit this vulnerability.	https://lists.apache.org/thread/olxxjk6b13sl3wh9cmp0k2dscvp24l7w
SMARTBEAR SoapUI unpackageAll Directory Traversal Remote Code Execution Vulnerability CVE-2024-7565	Vulnerability allows remote attackers to execute arbitrary code on affected installations of SMARTBEAR SoapUI. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file.	https://www.soapui.org/downloads/latest-release/release-notes/
(0Day) Microsoft GitHub Dev-Containers Improper Privilege Management Privilege Escalation Vulnerability	Vulnerability allows remote attackers to escalate privileges on Microsoft GitHub. The specific flaw exists within the configuration of Dev-Containers. The application does not enforce the privileged flag within a devcontainer configuration.	https://vulners.com/zdi/ZDI-23-1044
Microsoft Windows Menu DC Color Space 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 in order to exploit this vulnerability.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-30082
NoMachine Uncontrolled Search Path Element Local Privilege Escalation Vulnerability CVE-2024-7253	Vulnerability allows local attackers to escalate privileges on affected installations of NoMachine. The specific flaw exists within nxnode.exe. The process loads a library from an unsecured location.	https://kb.nomachine.com/TR07V11184
Google Chrome Updater DosDevices Local Privilege Escalation Vulnerability CVE-2023-7261	Vulnerability allows local attackers to escalate privileges on affected installations of Google Chrome. By creating a DOS device redirection, an attacker can abuse the update mechanism to launch an executable from an untrusted location.	https://issues.chromium.org/issues/40064602
PaperCut NG web-print-hot-folder Link Following Local Privilege Escalation Vulnerability CVE-2024-3037	Vulnerability allows local attackers to escalate privileges on affected installations of PaperCut NG. The specific flaw exists within the PCWebService. By creating a symbolic link, an attacker can abuse the service to delete a file.	https://www.papercut.com/kb/Main/Security-Bulletin-May-2024
PDF-XChange Editor PDF File Parsing Out-Of-Bounds Write Remote Code Execution Vulnerability CVE-2024-7352	Vulnerability allows remote attackers to execute arbitrary code on affected installations of PDF-XChange Editor. 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://www.pdf-xchange.com/product/pdf-xchange-editor/history#Build%2010.3.0.386
Microsoft Windows NTFS Junction Heap-based Buffer Overflow Local Privilege Escalation Vulnerability CVE-2024-21371	Vulnerability allows local attackers to escalate privileges on affected installations of Microsoft Windows. The issue results from the lack of proper validation of the length of user-supplied data prior to copying it to a heap-based buffer.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21371
NI VeriStand DataLoggingServer Deserialization of Untrusted Data Remote Code Execution Vulnerability CVE-2024-6793	Vulnerability allows remote attackers to execute arbitrary code on affected installations of NI VeriStand. The specific flaw exists within the processing of service requests in the DataLoggingServer component.	https://www.ni.com/en/support/security/available-critical-and-security-updates-for-ni-software/deserialization-of-untrusted-data-vulnerabilities-in-ni-veristand.html

Continued on next page >

Top Exploited Vulnerabilities

Trend Micro VPN Proxy One Pro Link Following Local Privilege Escalation Vulnerability CVE-2024-41183	Vulnerability allows local attackers to escalate privileges on affected installations of Trend Micro VPN Proxy One Pro. The specific flaw exists within the DEP Manager. By creating a symbolic link, an attacker can abuse the service to delete a folder.	https://helpcenter.trendmicro.com/en-us/article/tmka-14460
SolarWinds Access Rights Manager deleteTransferFile Directory Traversal Arbitrary File Deletion and Information Disclosure Vulnerability CVE-2024-28992	Vulnerability allows remote attackers to delete arbitrary files and disclose sensitive information on affected installations of SolarWinds Access Rights Manager. The issue results from the lack of proper validation of a user-supplied path prior to using it in file operations.	https://documentation.solarwinds.com/en/success_center/arm/content/release_notes/arm_2024-3_release_notes.htm
(Pwn2Own) Docker Desktop extension-manager Exposed Dangerous Function Privilege Escalation Vulnerability CVE-2024-6222	Vulnerability allows local attackers to escalate privileges on affected installations of Docker Desktop. The specific flaw exists within the the implemention of the Docker Extensions functionality. The issue results from an exposed dangerous function.	https://docs.docker.com/desktop/release-notes/#4290
(Pwn2Own) Linux Kernel io_uring Buffer List Race Condition Local Privilege Escalation Vulnerability CVE-2024-35880	Vulnerability allows local attackers to escalate privileges on affected installations of Linux Kernel. The specific flaw exists within the handling of the io_uring buffer list. The issue results from the lack of proper locking when performing operations on an object.	https://lore.kernel.org/linux-cve-announce/2024051944-CVE-2024-35880-6ffb@gregkh/#r
Linux Kernel ksmbd ACL Inheritance Heap-based Buffer Overflow Remote Code Execution Vulnerability CVE-2023-52755	Vulnerability allows remote attackers to execute arbitrary code on affected installations of Linux Kernel. The specific flaw exists within the processing of ACL attributes, resulting from lack of proper validation of the length of user-supplied data prior to copying it to a fixed-length heap-based buffer.	https://lore.kernel.org/all/20231124172008.838629931@linuxfoundation.org/
Autodesk AutoCAD X_T File Parsing Out-Of-Bounds Write Remote Code Execution Vulnerability CVE-2024-23146	Vulnerability allows remote attackers to execute arbitrary code on affected installations of Autodesk AutoCAD. The specific flaw exists within the parsing of X_T files, resulting from lack of proper validation of user-supplied data, which can result in a write past the end of an allocated object.	https://www.autodesk.com/trust/security-advisories/adsk-sa-2024-0009
Delta Electronics CNCSoft-G2 DPAX File Parsing Out-Of-Bounds Write Remote Code Execution Vulnerability CVE-2024-39881	Vulnerability allows remote attackers to execute arbitrary code on affected installations of Delta Electronics CNCSoft-G2. The specific flaw exists within the parsing of DPAX files.	https://www.cisa.gov/news-events/ics-advisories/icsa-24-191-01

Security Bulletin

Privilege Escalation in Azure Kubernetes Services: Kubernetes can be difficult to harden. Enforcing authentication for internal services, applying granular Network Policies, and restricting unsafe workloads with Pod Security are now table stakes for preventing post-exploitation activity that can compromise an entire cluster.

Cybercriminals Exploit File-Sharing Services to Advance Phishing Attacks: A file-sharing phishing attack is a unique type of phishing threat in which a cybercriminal poses as a known colleague or a familiar file-hosting or e-signature solution and sends a target a malicious email containing a link to what appears to be a shared file or document. Should the recipient click on the link, it initiates the second phase of the attack, which varies depending on the cybercriminal's desired outcome—e.g., stealing login credentials or infecting the target's device with malware.

Google Fixes High-Severity Chrome Flaw Actively Exploited in the Wild Google has rolled out security fixes to address a high-severity security flaw in its Chrome browser that has come under active exploitation in the wild. Tracked as CVE-2024-7971, the vulnerability has been described as a type of confusion bug in the V8 JavaScript and WebAssembly engine. Type confusion in V8 in Google Chrome prior to 128.0.6613.84 allowed a remote attacker to exploit heap corruption via a crafted HTML page.

Microsoft Patches Zero-Day Flaw Exploited by North Korea's Lazarus Group: A newly patched security flaw in Microsoft Windows was exploited as a zero-day by Lazarus Group, a prolific state-sponsored actor affiliated with North Korea. The security vulnerability, tracked as CVE-2024-38193 (CVSS score: 7.8), has been described as a privilege escalation bug in the Windows Ancillary Function Driver (AFD.sys) for WinSock. "An attacker who successfully exploited this vulnerability could gain SYSTEM privileges," Microsoft said in an advisory for the flaw last week. It was addressed by the tech giant as part of its monthly Patch Tuesday update.

Reference Links

1. https://cloud.google.com/blog/topics/threat-intelligence/apt41-arisen-from-dust?&web_view=true
2. https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-207a
3. https://ransomwatch.telemetry.ltd/
4. https://www.helpnetsecurity.com/2024/08/06/email-attacks-h1-2024/?web_view=true
5. https://www.cybersecuritydive.com/news/crowdstrike-outage-supply-chain/723198/?&web_view=true
6. https://www.welivesecurity.com/en/cybersecurity/beware-fake-ai-tools-masking-very-real-malware-threat/?&web_view=true
7. https://www.picussecurity.com/resource/blog/blue-report-2024-reveals-40-percent-of-environments-exposed-to-full-take-over?&web_view=true
8. https://therecord.media/ibm-breach-report-cost-rise-to-5-million?&web_view=true
9. https://www.helpnetsecurity.com/2024/07/26/cisos-compliance-regulations-preparedness/?web_view=true
10. https://thehackernews.com/2024/08/microsoft-patches-zero-day-flaw.html

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