JANUARY 2025

# 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

### More Than 50% of Office Workers Bypass Security To Boost Productivity

In a recent survey by CyberArk, more than 50% of employees reported having some kind of privileged access to get the job done. Additionally, 80% of employees can access work applications from personal devices and 65% of office workers surveyed admitted they've found ways to get around cybersecurity policies in the name of productivity. 27% of those surveyed use one password across multiple accounts to avoid aggravation, while 20% say they use personal devices as Wi-Fi hotspots.

### AI Adoption Creating New Attack Surface

With the majority of workers already adopting AI tools for work, data leakage scenarios are more likely because using many AI tools often involves inputting sensitive data.

**50% of respondents said they don't always adhere to company policies about adding sensitive or confidential information to AI tools—or that their company doesn't have an AI policy.**

### Digital Operation Resilience Act

Come January 17, 2025, EU-based financial institutions need to be compliant with the new DORA regulations which will reshape the financial sector approach to cybersecurity and operational resilience. It demands more than just technical upgrades—it calls for a strategic shift in mindset and practices.

27% of those surveyed use one password across multiple accounts to avoid aggravation.

CRITICAL THREAT ALERT

# Focus of the Month: AI-Leveraged Attacks

AI-powered attacks can be challenging for cybersecurity professionals and security teams. Some of the consequences of AI-generated attacks include data security breaches and other significant impacts on individuals and society. AI-generated attacks exploit machine learning and language models' capabilities to craft personalized phishing emails that are difficult to detect. By analyzing vast amounts of data and human intelligence, AI-enabled tools can generate highly convincing emails containing minimal grammatical errors and using authentic language. The aim is to successfully deceive individuals and gain access to their personal or sensitive information.

## Average AI-Leveraged Attacks Tune to $3.84 Million

- Social Media and Online Platform Manipulation: AI can be used to manipulate social media and online platforms
- Phishing Emails: AI can generate personalized phishing emails that are hard to detect.
- DDoS Attacks: AI can analyze network traffic data to identify the best time to launch an attack, making it difficult for traditional defenses to keep up

## Challenges for Security Teams

The rise of AI-powered attacks is making it increasingly difficult for security teams to protect organizations from cyber threats. It can deceive the most vigilant users and bypass advanced security systems.

## Some key challenges security teams face in defending against AI-generated cyberattacks:

- Highly Dynamic Threats: AI attacks can continuously modify tactics, techniques, and procedures to avoid detection. This makes it hard to build an effective static defense.
- Detection Evasion: AI allows attackers to optimize malware, phishing lures, network traffic, and more to hide from rules, signatures, and training data. It's increasingly difficult to spot anomalies.
- Increased Scale & Speed: AI dramatically boosts the automation and efficiency of attacks. Human analysts struggle to keep up.
- Blind Spots in Modelling: AI models have gaps in detecting novel attacks not represented in training data. Attackers exploit these blind spots.
- Difficulty Attributing Attacks: AI makes it harder to attribute attacks to specific groups based on TTPs, which are constantly changing.
- Skill Gaps: Defending against AI attacks requires specialized data science and ML skills that security teams often lack. Finding talent is difficult.
- Lack of Labelled Training Data: Defensive AI relies on large volumes of representative, labeled data on attacks, which is hard to come by.
- Data Isolation: Defensive insights learned from attacks in one organization aren't shared to benefit other defenses.

# Monthly Highlights

## Security Risks Persist in Open-Source Ecosystem

**A recent report by the Linux Foundation, OpenSSF, and Harvard University highlights significant security risks in open-source software practices. Based on data from the CENSUS III project, which analyzed 12 million observations of free and open-source software (FOSS) libraries used by over 10,000 companies, the findings underscore critical cybersecurity challenges in the FOSS ecosystem.**

The project builds on the earlier CENSUS I and II reports from 2015 and 2022, aiming to shed light on structural vulnerabilities threatening open-source software. Among the key issues identified is the continued reliance on Python 2, despite its official discontinuation in 2008. High usage rates in sectors like data analysis (29%), computer graphics (24%), and DevOps (23%) present significant risks, as Python 2 no longer receives security updates or support.

Another longstanding concern is the lack of a standardized naming scheme for software components. The report describes naming conventions as "unique, individualized, and inconsistent," complicating efforts to improve software security and supply chain transparency. Without standardized naming, sharing software security information on a global scale becomes increasingly difficult, hampering strategies like Software Bills of Materials (SBOM) and other security measures.

A major finding from CENSUS III is that the security management of open-source projects often rests on a small number of contributors. In 2023, 17% of projects had one developer responsible for over 80% of commits, while 40% of projects relied on just one or two developers for the same proportion of contributions. Furthermore, many software packages are hosted under individual developer accounts, which typically lack robust protections like multifactor authentication (MFA) or advanced permission controls, increasing vulnerability to account takeovers.

Legacy software remains another critical challenge in the open-source ecosystem. While theoretically easier to replace than hardware, legacy software often has incompatible APIs or functionality, making transitions difficult. As fewer developers maintain older software, the risks of unpatched vulnerabilities grow.

### On a positive note, the report highlights a 500% increase in the use of Rust components since CENSUS II.

This shift reflects growing adoption of memory-safe programming languages, driven in part by US federal efforts to move away from memory-unsafe languages like C and C++. Rust's package management system facilitates dependency tracking, making it a popular choice for secure software development.

"The significant rise in Rust adoption marks a step forward in integrating memory-safe languages into open-source software," the researchers noted, emphasizing its role in improving security across the ecosystem.

## Ransomware Costs Manufacturing Sector $17B in Downtime

**Ransomware attacks have inflicted an estimated $17 billion in downtime losses on manufacturing companies since 2018, according to new data from Comparitech. These attacks have disrupted operations at 858 manufacturers worldwide, with each day of downtime costing an average of $1.9 million.**

The financial toll stems from widespread production halts, compromised customer orders, strained business relationships, and extended recovery periods. Comparitech's report highlights a sharp resurgence in ransomware activity in 2023, with 194 confirmed cases, up from 109 in 2022.

On average, ransomware incidents cause 11.6 days of downtime, though durations can range from hours to as long as 129 days.

The manufacturing sector has also experienced a dramatic increase in data breaches, with 43.9 million records exposed in 2023—over 40 times the number in 2022. Significant incidents include VF Corporation's breach of 35.5 million records and PharMerica's 5.8 million records. Despite these attacks, ransom payment disclosures remain rare, with only eight of the 858 affected companies confirming payments. Boeing notably refused to pay a $200 million ransom in 2023, leading to the public release of 43 GB of data.

On average, ransomware incidents cause 11.6 days of downtime, though durations can range from hours to as long as 129 days. Using the $1.9 million daily downtime figure, researchers estimate that ransomware-induced disruptions cost manufacturers billions of dollars annually. The average ransom demand since 2018 stands at $10.7 million, with individual demands ranging from $5,000 to $200 million. LockBit, the ransomware group behind the Boeing attack, has been particularly active in recent years.

Transportation and automotive manufacturing, with 130 attacks, and food and beverage production, with 124 attacks, are among the hardest-hit sectors.

As of October 2024, there have been 137 confirmed ransomware incidents in manufacturing, with average downtimes of 11 days per attack. Experts warn that the total number of attacks in 2024 could rival or surpass 2023 levels.

The staggering financial and operational impact of ransomware attacks on manufacturing underscores the urgent need for stronger cybersecurity measures and proactive strategies to minimize disruptions during such incidents.

## Five Ransomware Groups Responsible for 40% of Cyberattacks in 2024

**Five ransomware groups, including RansomHub and LockBit 3.0, were responsible for 40% of all cyberattacks in Q3 2024, reflecting the growing complexity and competition within the ransomware landscape, according to Corvus Insurance's latest research.**

The Q3 2024 Cyber Threat Report, titled The Ransomware Ecosystem is Increasingly Distributed, revealed that the overall ransomware threat level remained high. During the quarter, 1257 victims were reported on leak sites, a slight 0.7% increase from Q2's total of 1248 victims.

The report highlighted the impact of law enforcement efforts, such as Operation Cronos, which disrupted LockBit's infrastructure and shifted the ransomware ecosystem toward smaller-scale operations. Filling this gap, RansomHub emerged as a dominant player, with over 290 victims across various sectors in 2024. Research by Symantec in October also identified RansomHub as the leading ransomware group in terms of successful attacks. Its success is attributed to recruiting skilled affiliates for its ransomware-as-a-service model.

LockBit 3.0, on the other hand, saw a sharp decline in activity, with victim counts dropping from 208 in Q2 to 91 in Q3, likely due to increased law enforcement pressure.

A significant driver of ransomware attacks in Q3 was the exploitation of virtual private network (VPN) vulnerabilities and weak passwords, accounting for nearly 30% of incidents. Corvus explained that outdated software and poorly secured VPN accounts were commonly exploited by attackers. Default usernames like "admin" or "user," coupled with the absence of multi-factor authentication (MFA), left accounts susceptible to brute-force attacks, enabling cybercriminals to gain network access with minimal effort.

A significant driver of ransomware attacks in Q3 was the exploitation of virtual private network (VPN) vulnerabilities and weak passwords, accounting for nearly 30% of incidents.

"Attackers prioritize the path of least resistance, and in Q3, VPNs were the primary entry point," said Jason Rebholz, Chief Information Security Officer at Corvus.

"As businesses look ahead, they must adopt multi-layered security strategies that go beyond MFA. Today, MFA is a baseline requirement and must be supplemented with secure access controls to address both current and emerging vulnerabilities," Rebholz added.

## Over 145,000 Industrial Control Systems Across 175 Countries Found Exposed Online

**A recent study uncovered over 145,000 internet-exposed Industrial Control Systems (ICS) across 175 countries, with the U.S. accounting for more than one-third of these exposures. The research, conducted by attack surface management firm Censys, revealed that 38% of these devices are in North America, followed by Europe (35.4%), Asia (22.9%), Oceania (1.7%), South America (1.2%), and Africa (0.5%).**

Many of these protocols, dating back to the 1970s, lack modern security updates, posing significant risks to critical infrastructure.

The countries with the highest ICS exposures include the U.S. (over 48,000 devices), Turkey, South Korea, Italy, Canada, Spain, China, Germany, France, the U.K., Japan, Sweden, Taiwan, Poland, and Lithuania. These exposures stem from commonly used ICS protocols like Modbus, IEC 60870-5-104, CODESYS, and OPC UA. Regional trends highlight differences in protocol usage, with Modbus, S7, and IEC 60870-5-104 more prevalent in Europe, while Fox, BACnet, and ATG are common in North America. Shared protocols between the regions include EIP, FINS, and WDBRPC.

The report also revealed that 34% of C-more human-machine interfaces (HMIs) relate to water and wastewater management, while 23% are tied to agricultural processes. Many of these protocols, dating back to the 1970s, lack modern security updates, posing significant risks to critical infrastructure.

"The security of ICS devices is crucial for safeguarding national critical infrastructure," noted Zakir Durumeric, co-founder and chief scientist at Censys. "Understanding how these devices are exposed and vulnerable is key to protecting them."

Although targeted ICS cyberattacks remain relatively rare—only nine malware strains have been identified—there has been an increase in ICS-specific malware in recent years, especially since the Russo-Ukrainian conflict began. For instance, in July 2024, the energy sector in Ukraine was targeted by FrostyGoop (also known as BUSTLEBERM), a Windows-based malware exploiting Modbus TCP communications to disrupt operational technology (OT) networks. The malware can manipulate any Modbus TCP-compatible ICS device, enabling denial-of-service (DoS) attacks.

Between September 2 and October 2, 2024, telemetry data revealed that 1,088,175 Modbus TCP devices were exposed to the internet. Threat actors have also targeted other critical infrastructure sectors. For example, in 2023, attackers breached the Municipal Water Authority of Aliquippa, Pennsylvania, by exploiting internet-exposed programmable logic controllers (PLCs) to display anti-Israel messages.

The increasing availability of HMIs online to enable remote access has further compounded security risks. The U.S. leads in exposed HMIs, followed by Germany, Canada, France, Austria, and others. Most HMIs and ICS services are hosted on mobile or business-grade ISPs, such as Verizon and Deutsche Telekom, offering little metadata to identify users. Censys emphasized the need for cooperation from telcos to address these challenges.

The broad attack surface of ICS and OT networks requires urgent action. Organizations must secure exposed devices, update default credentials, and monitor networks for malicious activity. The rise in botnet malware like Aisuru, Kaiten, and Gafgyt underscores the urgency, as these strains exploit weak OT credentials for distributed denial-of-service (DDoS) attacks and data wiping.

Most HMIs and ICS services are hosted on mobile or business-grade ISPs, such as Verizon and Deutsche Telekom, offering little metadata to identify users.

In related findings, cybersecurity firm Forescout recently identified medical devices, including DICOM workstations and PACS systems, as some of the most vulnerable in healthcare environments. These devices, widely used on the Internet of Medical Things (IoMT), are frequently exposed online, particularly in the U.S., India, Germany, Brazil, Iran, and China. Daniel dos Santos, head of security research at Forescout, stressed the importance of asset identification, network segmentation, and continuous monitoring to safeguard sensitive patient data and healthcare systems.

## 65% of Office Workers Bypass Cybersecurity to Boost Productivity

**High-risk access is prevalent across nearly every job role, signaling a pressing need for organizations to rethink their approach to workforce security, according to a CyberArk report.**

**The study surveyed 14,003 employees from the UK, USA, France, Germany, Australia, and Singapore to identify workforce behaviors that challenge security teams. It revealed that nearly all employees require access to sensitive or privileged resources to perform their jobs effectively.**

### Key Findings:

- All respondents reported using corporate devices to access work applications, including collaboration tools like Teams, Slack, and Outlook (52%), IT admin tools (41%), and customer-facing applications (34%). These are critical systems containing sensitive and privileged data.
- 80% also accessed work applications from personal devices, expanding the organization's attack surface.

### Risky behaviors further increase vulnerabilities:

- Personal Device Usage: 60% admitted using personal devices for work-related apps, emails, or systems in the past year.
- Policy Circumvention: 65% of office workers said they bypass cybersecurity policies to maintain productivity.
- Weak Password Practices: 27% use a single password across multiple accounts, and 30% share work-related credentials with colleagues. Additionally, 36% reuse login credentials for both personal and work accounts.

### The growing use of AI in the workplace adds another layer of complexity:

- 72% of respondents use AI tools for work, often inputting sensitive data.
- 50% admitted to either disregarding company policies regarding AI or working in organizations without an AI policy, increasing exposure to potential data leaks.

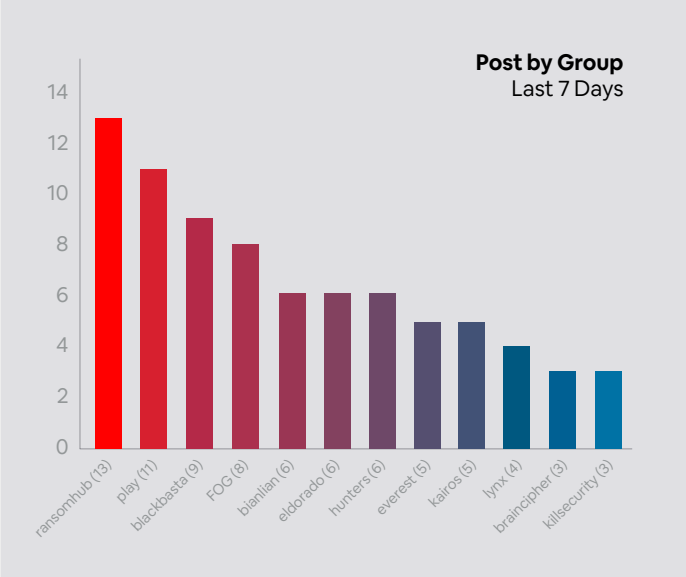
### Phishing and patch management challenges:

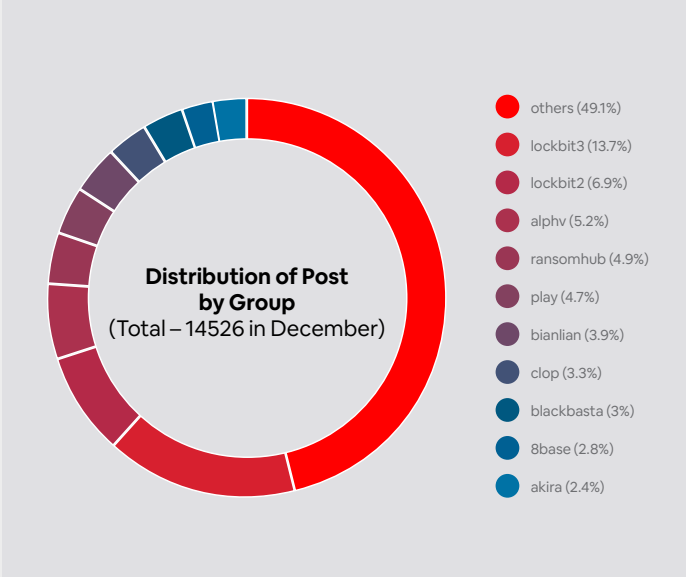
- C-level executives are particularly susceptible to phishing attacks, with 62% admitting to clicking on phishing email links, compared to 25% of entry-level staff.
- 36% of employees do not immediately install security patches or updates on personal devices, leaving vulnerabilities unaddressed.

These risky shortcuts often stem from good intentions but highlight the urgent need for robust identity security strategies. Organizations must create systems that enable employees to work efficiently while minimizing security risks.

By prioritizing secure access controls, enforcing password best practices, and educating employees about safe behaviors, companies can better protect their sensitive assets in today's dynamic work environment.

# Ransomware Tracker




# Articles

## Operation Digital Eye: Uncovering Targeted Cyber Espionage on Critical Sectors

### Executive Summary

- **Operation Overview:** Operation Digital Eye is a sophisticated cyberespionage campaign attributed to a Chinese APT group. It targets high-value entities in Europe, focusing on exploiting Visual Studio Code Remote Tunnels.
- **Tool Utilization:** The campaign employed mimCN tools, including bK2o.exe and custom Mimikatz variants, for lateral movement and credential theft.
- **Infrastructure Insights:** M247 infrastructure and geographically proximate cloud services were leveraged to manage targeted attacks effectively.
- **Attribution:** The operation is likely linked to the Chinese APT ecosystem, involving shared tools and methodologies suggestive of centralized digital quartermaster involvement.

### Detection

Organizations can detect activities associated with Operation Digital Eye by monitoring the following indicators:

#### 1. Tool Signatures and Behavior:

- Identify use of custom mimCN tools like mim221, bK2o.exe, wsx.exe, and simplify_32.exe.
- Look for unusual processes, especially those reflecting credential theft behaviors linked to Mimikatz variants.

#### 2. Visual Studio Code Tunneling:

- Monitor network traffic for connections to Visual Studio Code Remote Tunnels.
- Detect abnormal use of trusted development tools, such as LNK files deploying Visual Studio Code.

#### 3. Infrastructure Indicators:

- Track usage of M247 infrastructure, particularly in geographic proximity to targeted entities.
- Identify suspicious activity originating from cloud services often used by attackers.

#### 4. Temporal Patterns:

- Analyse activity logs for timestamps indicating operations during Chinese work hours (9 a.m. to 9 p.m. CST).
- Look for consistent inactivity during typical Chinese lunch hours (11 a.m. to 1 p.m. CST).

## Prevention

To prevent similar campaigns, organizations should implement the following measures:

1. **Security Hardening:**
   - Regularly update and patch systems, including development tools like Visual Studio Code.
   - Deploy endpoint detection and response (EDR) tools to flag abnormal behavior linked to credential theft or reflective image loading.
2. **Infrastructure Security:**
   - Limit access to remote tunneling features in development tools unless explicitly required.
   - Implement network segmentation and restrict external access to critical systems.
3. **Threat Intelligence Integration:**
   - Incorporate threat intelligence feeds to detect indicators associated with mimCN tools and infrastructure.
   - Share findings with industry peers to stay updated on evolving tactics.
4. **User Awareness and Training:**
   - Train staff on identifying phishing attempts that could lead to tool deployment.
   - Emphasize the risks of downloading and executing unverified development tools or scripts.

## Remediation

If indicators of compromise (IOCs) are detected, organizations should follow these steps:

1. **Containment:**
   - Isolate affected systems to prevent lateral movement.
   - Disable Visual Studio Code tunneling and related remote access tools.
2. **Incident Response:**
   - Perform forensic analysis to identify the scope and source of the intrusion.
   - Analyze logs for unusual activity patterns, particularly around mimCN tools.
3. **Credential Reset:**
   - Reset credentials for all accounts accessed during the breach.
   - Deploy multifactor authentication (MFA) to strengthen account security.
4. **Tool Removal:**
   - Remove malicious executables and associated DLLs, such as AddSecurityPackage64.dll and getHashFlsa64.dll.
   - Reimage affected systems if necessary to ensure complete eradication.
5. **Post-Incident Review:**
   - Conduct a thorough review to identify gaps in defense that allowed the breach.
   - Update security policies and incident response plans to address identified vulnerabilities.

## Conclusion

Operation Digital Eye demonstrates the persistent and evolving threats posed by Chinese APT groups. Their strategic targeting of high-value entities and reliance on innovative tactics, such as abusing trusted development tools, highlights the need for robust security measures. By enhancing detection, prevention, and remediation strategies, organizations can better protect themselves against sophisticated cyberespionage campaigns.

# APT35's Cyber Campaign: Exploiting Fake Recruitment Sites and VPN Tools to Target Aerospace and Semiconductor Industries

## Executive Summary

APT35, also known as Magic Hound, Cobalt Illusion, and Charming Kitten, is a threat actor group with ties to Iran and suspected affiliation with the Islamic Revolutionary Guard Corps (IRGC). Active since 2014, APT35 primarily targets the energy, government, and technology sectors across the Middle East, United States, and other regions. Recent analyses by security researchers have uncovered their use of forged recruitment and corporate websites, leveraging legitimate internet resources like OneDrive and Google Cloud to conduct targeted attacks on aerospace and semiconductor industries. These operations involve sophisticated malware delivery mechanisms designed to evade detection and compromise victim systems.

### Key Findings:

- Targets include aerospace and semiconductor industries, with attacks observed in the United States, Thailand, UAE, and Israel.
- Utilization of fake recruitment sites hosting mixed legitimate and malicious components.
- Deployment of malware leveraging legitimate resources like OneDrive and GitHub.
- Indicators of Compromise (IOCs) include hardcoded credentials, malicious DLL modules, and callback mechanisms to compromised domains.

## Detection

To identify and mitigate threats associated with APT35, consider the following detection measures:

### 1. Network Monitoring:

- Monitor traffic to known malicious domains such as xboxapicenter.com and msdnhelp.com.
- Identify unusual activity involving legitimate platforms like OneDrive and GitHub, particularly drive.google.com or raw.githubusercontent.com.

### 2. Endpoint Analysis:

- Look for the presence of renamed malicious files in %LOCALAPPDATA%\Microsoft\WindowsInsights\workstation.
- Detect registry modifications under SOFTWARE\Microsoft\Windows\CurrentVersion\Run\OneDrive for unauthorized auto-start entries.

### 3. Malware Indicators:

- Analyze modules such as secur32.dll and Qt5Core.dll for hardcoded credentials or GUID generation mechanisms.
- Identify static detection evasion techniques, including string reconstruction and obfuscation.

### 4. IOC-Based Detection:

- Utilize threat intelligence feeds to detect known IOCs, including IP addresses, domains, and file hashes associated with APT35 campaigns.

## Prevention

Proactive measures can help prevent attacks from APT35:

### 1. User Awareness and Training:

- Educate employees about phishing techniques, especially those involving fake recruitment or corporate websites.
- Highlight risks associated with downloading unauthorized software or accessing unknown websites.

### 2. Access Controls:

- Implement robust access restrictions for sensitive roles, particularly in aerospace and semiconductor sectors.
- Enforce multi-factor authentication (MFA) for accessing critical systems and resources.

### 3. Endpoint Security:

- Deploy advanced endpoint protection solutions with real-time monitoring and malware detection capabilities.
- Regularly update and patch all software to mitigate vulnerabilities exploited by APT35.

### 4. Network Security:

- Restrict outbound connections to domains and IPs not explicitly approved.
- Implement DNS filtering to block access to malicious or suspicious domains.

## Remediation

If a compromise is detected, follow these remediation steps:

### 1. Isolation:

- Immediately isolate affected systems to prevent lateral movement.
- Disconnect compromised endpoints from the network.

### 2. Incident Response:

- Conduct a thorough forensic analysis to determine the scope of the breach.
- Retrieve and analyze logs from affected endpoints and servers.

### 3. IOC Cleanup:

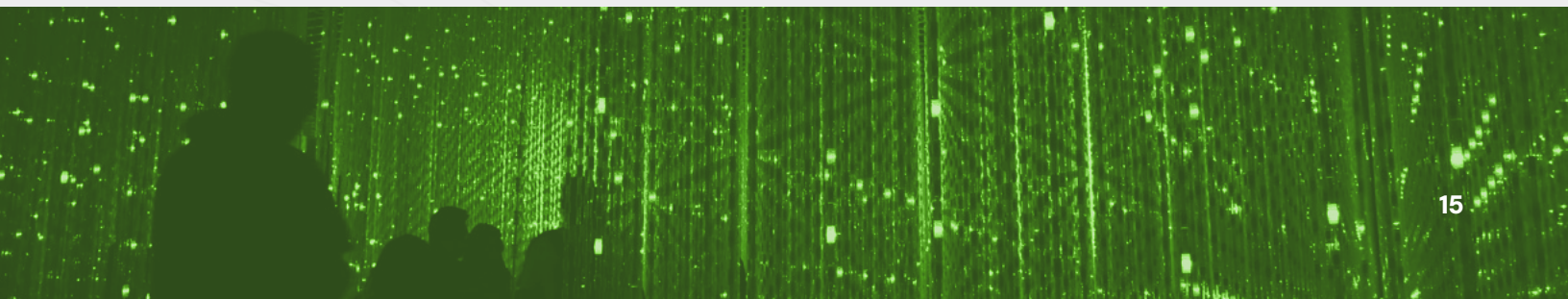
- Remove malicious files and registry entries identified during detection.
- Block malicious domains and IPs at the firewall and network level.

### 4. System Recovery:

- Rebuild compromised systems from known good backups.
- Change credentials for all affected accounts, including hardcoded ones identified in malware.

### 5. Post-Incident Actions:

- Share IOCs and findings with threat intelligence sharing platforms.
- Enhance security policies and practices based on lessons learned from the incident.



## Unveiling WolfsBane: Gelsemium's Linux Counterpart to Gelsevirine

'WolfsBane' is a new Linux backdoor that has been found and is thought to be a port of Windows malware used by the Chinese hacker collective 'Gelsemium'.

According to ESET security researchers who examined WolfsBane, it is a full-fledged malware tool with a backdoor, launcher, and dropper. To avoid detection, it also makes use of a modified open-source rootkit.

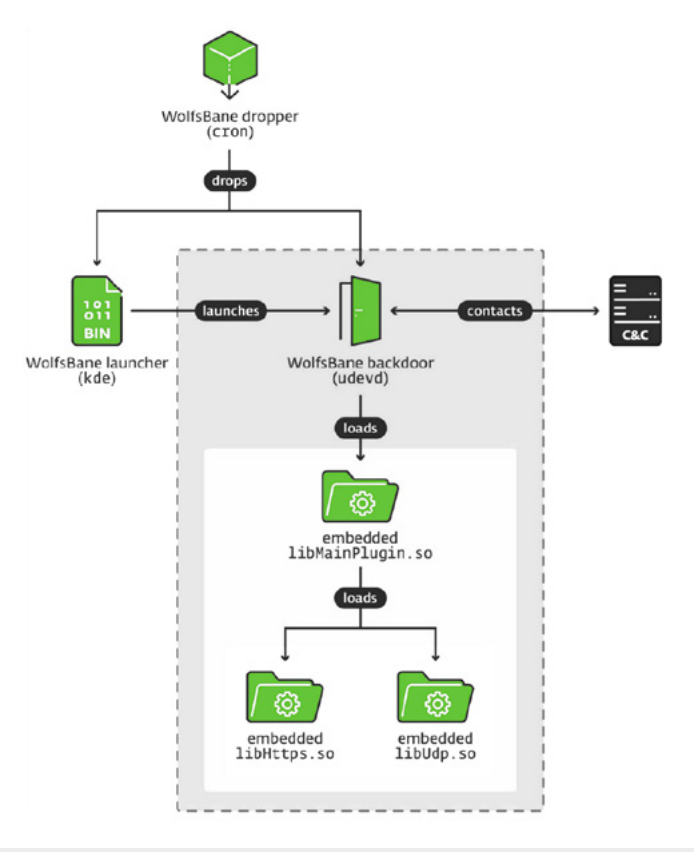
'FireWood,' another Linux malware that seems to be connected to the 'Project Wood' Windows malware, was also found by the researchers.

Nevertheless, FireWood is not an exclusive/private tool developed by Gelsemium, but rather a shared tool utilized by several Chinese APT groups.

The two malware families, which have both been listed on VirusTotal in the past year, according to ESET, are part of a larger trend in which APT groups are increasingly targeting Linux platforms as Windows security becomes more robust.

### Detection

Targets are introduced to WolfsBane through a dropper called 'cron,' which drops the launcher component with a KDE desktop component disguised as it.




It establishes persistence by either creating system service files, changing user configuration files, or disabling SELinux, depending on the privileges it runs with.

The launcher loads 'udevd,' the privacy malware component, which loads three encrypted libraries with its command and control (C2) communication configuration and essential functions.

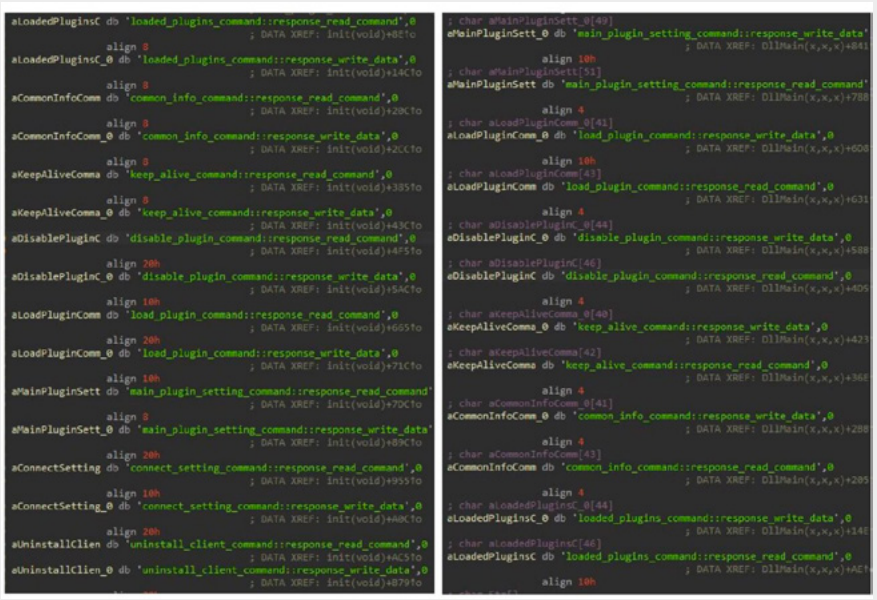
To help conceal processes, files, and network traffic associated with WolfsBane's operations, a modified version of the BEURK userland rootkit is loaded via '/etc/ld.so.preload' for system-wide hooking.

Numerous fundamental standard C library functions, including open, stat, readdir, and access, are hookable by the WolfsBane Hider rootkit.

These hooked functions filter out any results associated with the WolfsBane malware, even though they still invoke the original ones.

Like its Windows counterpart, WolfsBane's primary function is to use predefined command-function mappings to execute commands received from the C2 server.

Gelsemium has complete control over compromised systems thanks to these commands, which include file operations, data exfiltration, and system manipulation.




## Indicators of Compromise

### Files

| SHA-1 | Filename | Detection | Description |
|---|---|---|---|
| 0FEF89711DA11C550D3914DEBC0E663F5D2FB86C | dbus | Linux/Agent.WF | FireWood backdoor. |
| 44947903B2BC760AC2E736B25574BE33BF7AF40B | libselinux.so | Linux/Rootkit.Agent.EC | WolfsBane Hider rootkit. |
| 0AB53321BB9699D354A032259423175C08FEC1A4 | udevd | Linux/Agent.WF | WolfsBane backdoor. |
| 8532ECA04C0F58172D80D8A446AE33907D509377 | kde | Linux/Agent.WF | WolfsBane launcher. |
| B2A14E77C96640914399E5F46E1DEC279E7B940F | cron | Linux/Agent.WF | WolfsBane dropper. |
| 209C4994A42AF7832F526E09238FB55D5AAB34E5 | ccc | Linux/Agent.WF | Privilege escalation helper tool. |
| F43D4D46BAE9AD963C2EB05EF43E90AA3A5D88E3 | ssh | Linux/SSHDoor.IC | Trojanized SSH client. |
| FD601A54BC622C041DF0242662964A7ED31C6B9C | a.jsp | Java/Agent.BP | JSP webshell. |
| 9F7790524BD759373AB57EE2AAFA6F5D8BCB918A | yy1.jsp | Java/JSP.J | icesword webshell. |
| 238C8E8EB7A732D85D8A7F7CA40B261D8AE4183D | login.jsp | Java/Webshell.AM | Modified AntSword JSP webshell. |
| F1DF0C5A74C9885CB5934E3EEE5E7D3CF4D291C0 | virus.tgz | Linux/Agent.WF | VirusTotal archive. |
| B3DFB40336C2F17EC74051844FFAF65DDB874CFC | virus-b.tgz | Linux/Agent.WF | VirusTotal archive. |
| 85528EAC10090AE743BCF102B4AE7007B6468255 | CHINA-APT-Trojan.zip | Java/Agent.BP | VirusTotal archive. |
| CDBBB6617D8937D17A1A9EF12750BEE1CDDF4562 | CHINA-APT-Trojan.zip | Linux/Rootkit.Agent.EC | VirusTotal archive. |
| 843D6B0054D066845628E2D5DB95201B20E12CD2 | CHINA-APT-Trojan.zip | Linux/Rootkit.Agent.EC | VirusTotal archive. |
| BED9EFB245FAC8CFFF8333AE37AD78CCFB7E2198 | Xl1.zip | Linux/Rootkit.Agent.EC | VirusTotal archive. |
| 600C59733444BC8A5F71D41365368F3002465B10 | CHINA-APT-Trojan.zip | Linux/Rootkit.Agent.EC | VirusTotal archive. |
| 72DB8D1E3472150C1BE93B68F53F091AACC2234D | virus.tgz | Linux/Agent.WF | VirusTotal archive. |

### Network

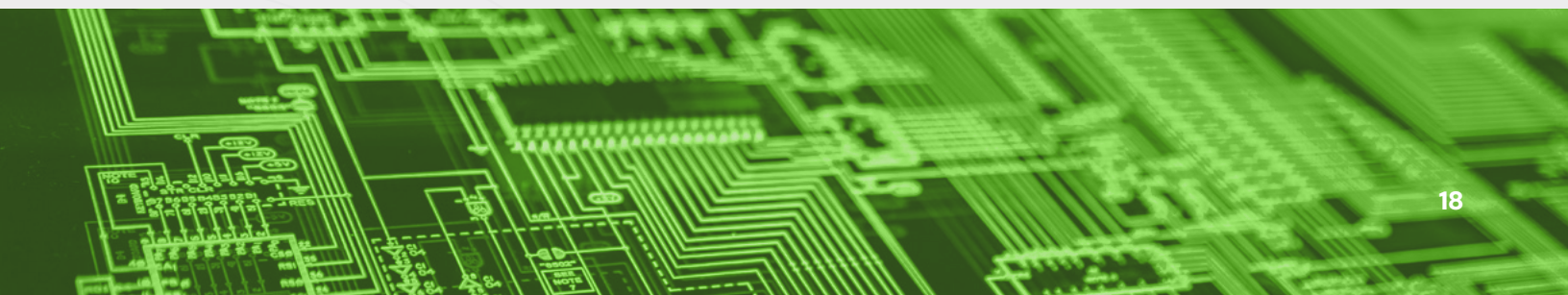
| IP | Domain | Hosting provider | First seen | Details |
|---|---|---|---|---|
| N/A | dsdsei[.]com | N/A | 2020-08-16 | WolfsBane backdoor C&C server. |
| N/A | asidomain[.]com | N/A | 2022-01-26 | FireWood backdoor C&C server. |

## Prevention

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

## Remediation

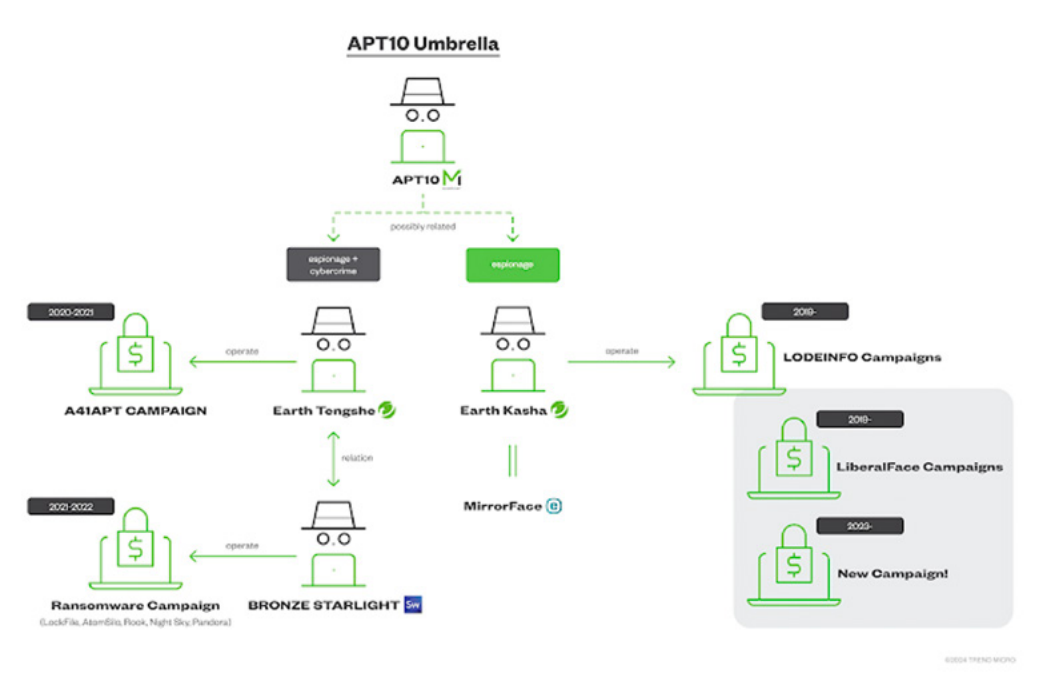
- Use Microsoft Defender XDR to find ransomware attacks that are operated by humans.
- Turn on restricted folder access.
- Activate Microsoft Defender for Endpoint's network protection.
- Adhere to the credential hardening advice in our overview of on-premises credential theft to prevent common credential theft methods like LSASS access.
- Maintain comprehensive backup and recovery procedures for restoring encrypted files and minimizing downtime.
- Activate endpoint detection and response (EDR) in block mode to enable Microsoft Defender for Endpoint to stop malicious artifacts even if your non-Microsoft antivirus program is in passive mode or fails to identify the threat.
- Activate cloud-delivered protection in Microsoft Defender Antivirus or its equivalent.
- Conduct post-incident analysis to identify weaknesses in security posture and implement measures to prevent future ransomware incidents.



## Spot the Difference: Earth Kasha's New LODEINFO Campaign and the Correlation Analysis with the APT10 Umbrella

Since 2019, the malware LODEINFO has been used in attacks primarily against Japan. The band has been monitored by Trend Micro under the name Earth Kasha. Some vendors, however, believe that APT10 may be the actor using LODEINFO.

Although they may be connected, we currently consider APT10 and Earth Kasha to be distinct entities. We use the new term "APT10 Umbrella" to refer to a collection of intrusion sets associated with APT10 (including APT10 itself) to prevent name confusion.

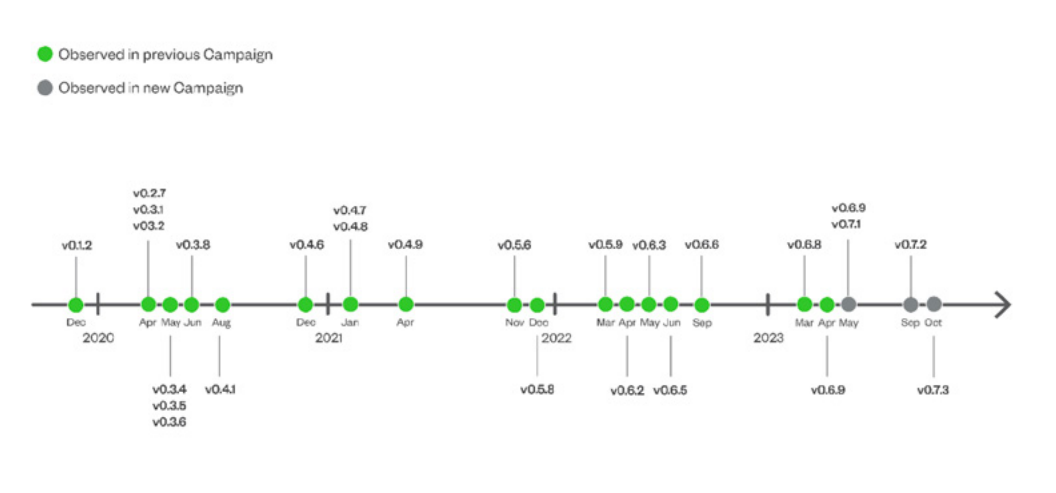



During their inception, Earth Kasha has been identified as using spear-phishing emails to target academics and public institutions. However, we found a new campaign that made substantial changes to their strategy, tactics, and arsenals between early 2023 and early 2024.

### Detection

LODEINFO is the main backdoor that Earth Kasha has been using exclusively since 2019. Its versatility is demonstrated by the fact that it is only one choice among many in this new campaign.

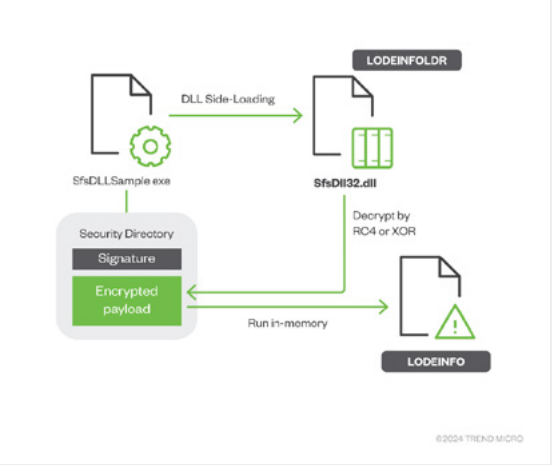
LODEINFO has undergone constant updates since its launch, as evidenced by its version numbers. Versions v0.6.9, v0.7.1, v0.7.2, and v0.7.3 have been seen in this campaign.



Additionally, Earth Kasha has been updating a procedure to execute LODEINFO with the increasing version number. Three components were installed on the victim's computer. They made the legitimate application a scheduled task, causing the malicious DLL to load side-loaded.

An encrypted payload embedded in the loaded process's digital signature is extracted by this malicious DLL, which we named LODEINFOLDR, and decrypted using RC4 or XOR.

The legitimate digital signature is compromised by abusing MS13-098/CVE-2013-3900 to embed the encrypted payload.




## Indicators of Compromise

| SHA256 | malware |
|---|---|
| 9c681493c81581995e6a48b96411a7004fe77558d7ca863e26398538ad78f385 | NOOPLDR (DLL) |
| 8574a494425825958c1e978ca7f66a467954fa90c7c898eebac49928519f0eae | LODEINFOLDR (Type 2) |
| 87fd4cf002e4d3867462c7a08124cba154750ae78785009a9f213c7479241eef | LODEINFOLDR (Type 2) |

| domain/IP | malware | comment |
|---|---|---|
| ns1[.]tlsart[.]com | Cobalt Strike | |
| {DGA}[.]hopto[.]org | NOOPDOOR | DDNS, blocking all sub-domains is not recommended |
| {DGA}[.]gotdns[.]ch | NOOPDOOR | DDNS, blocking all sub-domains is not recommended |
| {DGA}[.]myftp[.]org | NOOPDOOR / LODEINFO | DDNS, blocking all sub-domains is not recommended |
| {DGA}[.]tw8sl[.]com | NOOPDOOR | |
| {DGA}[.]srmbr[.]com | NOOPDOOR | |
| 45[.]76[.]197[.]236 | NOOPDOOR / LODEINFO | IP related to the domain used by NOOPDOOR and LODEINFO |

### Prevention

- Employ endpoint protection solutions capable of detecting and blocking known malware variants to further enhance defense mechanisms.
- Use endpoint detection and response (EDR) solutions with behavior-based analysis.
- Implement robust data backup and recovery mechanisms.
- Enforce strict access controls and least privilege principles.
- Regularly update and patch software vulnerabilities, especially those exploited in zero-day attacks, to mitigate the risk of exploitation.
- Store logs in a central system
- Revoke unnecessary public access to the cloud environment.

### Remediation

- In the event of an attack, immediately isolate affected systems and networks to prevent further spread of the malware.
- Secure external-facing services
- Implement the following prevention measures: phishing awareness training, network segmentation, and endpoint protection.
- Enable endpoint detection solutions for a robust defense against ransomware threats, emphasizing proactive measures.
- Mobilize incident response teams to conduct thorough forensic analysis, identifying the extent of the compromise and removing any traces of the malware from infected systems.
- Closely monitor network traffic and endpoint activities to ensure the threat actor has been fully eradicated from the environment.
- Implement security best practices and conduct regular security assessments to help strengthen defenses against future attacks.

# Top Exploited Vulnerabilities

| Vulnerability Name | Description | References |
|---|---|---|
| Ivanti Avalanche FileStoreConfig Unrestricted File Upload Remote Code Execution Vulnerability CVE-2024-37373 | Vulnerability allows remote attackers to execute arbitrary code on affected installations of Ivanti Avalanche. The issue results from the lack of proper validation of user-supplied data, which can allow the upload of arbitrary files. | 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 PC Manager MSPCManagerService Link Following Local Privilege Escalation Vulnerability | Vulnerability allows local attackers to escalate privileges on affected installations of Microsoft PC Manager. By creating a symbolic link, an attacker can abuse the service to create arbitrary files. | https://msrc.microsoft.com/update-guide/en-us/acknowledgement/online |
| Dell Avamar Web Restore Login Action SQL Injection Information Disclosure Vulnerability CVE-2024-47484 | Vulnerability allows remote attackers to disclose sensitive information on affected installations of Dell Avamar. The issue results from the lack of proper validation of a user-supplied string before using it to construct SQL queries. | https://www.dell.com/support/kbdoc/en-us/000258636/dsa-2024-489-security-update-for-dell-avamar-and-dell-avamar-virtual-edition-security-update-for-multiple-vulnerabilities |
| Linux Kernel ksmbd PreviousSessionId Race Condition Remote Code Execution Vulnerability | Vulnerability allows remote attackers to execute arbitrary code on affected installations of Linux Kernel. The issue results from the lack of proper locking when performing operations on an object. | https://lore.kernel.org/all/CAKYAXd_MPF9WiFoOwnPBiPvwMKDjGJ4BX4u-UnGymFM4sp3YMQ@mail.gmail.com/T/ |
| Progress Software WhatsUp Gold GetFilterCriteria SQL Injection Privilege Escalation Vulnerability CVE-2024-46908 | Vulnerability allows remote attackers to escalate privileges on affected installations of Progress Software WhatsUp Gold. The issue results from the lack of proper validation of a user-supplied string before using it to construct SQL queries. | https://cve.enginsight.com/2024/46908/index.html |
| Wacom Center WTabletServicePro Link Following Local Privilege Escalation Vulnerability CVE-2024-12552 | Vulnerability allows local attackers to escalate privileges on affected installations of Wacom Center. By creating a symbolic link, an attacker can abuse the service to create an arbitrary file. | https://cdn.wacom.com/u/productsupport/drivers/win/professional/releasenotes/Windows_6.4.8-2.html |
| Tungsten Automation Power PDF JPF File Parsing Out-Of-Bounds Write Remote Code Execution Vulnerability CVE-2024-12547 | Vulnerability allows remote attackers to execute arbitrary code on affected installations of Tungsten Automation 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/5.1.1-x2ki7a3ycc/print/ReadMe-TungstenPowerPDFBusiness-5.1.1.2.htm |
| ManageEngine Analytics Plus getOAToken Exposed Dangerous Method Privilege Escalation Vulnerability CVE-2024-52323 | Vulnerability allows remote attackers to escalate privileges on affected installations of ManageEngine Analytics Plus. The issue results from an exposed dangerous method. | https://www.manageengine.com/analytics-plus/CVE-2024-52323.html |
| AutomationDirect C-More EA9 EAP9 File Parsing Memory Corruption Remote Code Execution Vulnerability CVE-2024-11611 | Vulnerability allows remote attackers to execute arbitrary code on affected installations of Automation Direct C-More EA9. The issue results from the lack of proper validation of user-supplied data, which can result in a memory corruption condition. | https://certvde.com/en/bulletins/bulletins/2182-automationdirect-c-more-ea9-programming-software/ |
| GFI Archiver Telerik Web UI Remote Code Execution Vulnerability CVE-2024-11948 | Vulnerability allows remote attackers to execute arbitrary code on affected installations of GFI Archiver. The issue results from the use of a vulnerable version of Telerik Web UI. | https://www.tenable.com/cve/CVE-2024-11948/cpes |
| Veritas Enterprise Vault Deserialization of Untrusted Data Remote Code Execution Vulnerability CVE-2024-53911 | Vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of Veritas Enterprise Vault. The issue results from the lack of proper validation of user-supplied data, which can result in deserialization of untrusted data. | https://www.veritas.com/support/en_US/security/VTS24-014 |
| Microsoft Edge File Extension Spoofing Remote Code Execution Vulnerability CVE-2024-49041 | Vulnerability allows remote attackers to execute arbitrary code on affected installations of Microsoft Edge. A crafted file name can cause the true file extension to be hidden, misleading the user into believing that the file type is harmless. | https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-49041 |
| Delta Electronics CNCSoft-G2 DPAX File Parsing Heap-based Buffer Overflow Remote Code Execution Vulnerability CVE-2024-47964 | Vulnerability allows remote attackers to execute arbitrary code on affected installations of Delta Electronics CNCSoft-G2. The issue results from the lack of proper validation of the length of user-supplied data prior to copying it to a fixed-length heap-based buffer. | https://www.cisa.gov/news-events/ics-advisories/icsa-24-284-21 |
| Rockwell Automation Arena Simulation DOE File Parsing Out-Of-Bounds Read Remote Code Execution Vulnerability CVE-2024-12130 | Vulnerability allows remote attackers to execute arbitrary code on affected installations of Rockwell Automation Arena Simulation. The issue results from the lack of proper validation of user-supplied data, which can result in a read past the end of an allocated buffer. | https://www.cisa.gov/news-events/ics-advisories/icsa-24-345-06 |

Continued on next page >

| | | |
|---|---|---|
| Linux Kernel Bluetooth HCI Request Race Condition Local Privilege Escalation Vulnerability | Vulnerability allows local attackers to escalate privileges on affected installations of Linux Kernel. The issue results from the lack of proper locking when performing operations on an object. | https://git.kernel.org/pub/scm/linux/kernel/git/bluetooth/bluetooth-next.git/commit/?id=92048ab2e2e6 |
| BlueZ Classic HID Missing Authentication Remote Code Execution Vulnerability CVE-2024-8805 | Vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of BlueZ. The specific flaw exists within the implementation of Classic HID connections. | https://git.kernel.org/pub/scm/linux/kernel/git/bluetooth/bluetooth-next.git/commit/?id=370e38c32529e0899b-b387a70d5d92dfb5a2b3c5 |
| Epic Games Launcher Incorrect Default Permissions Local Privilege Escalation Vulnerability CVE-2024-11872 | Vulnerability allows local attackers to escalate privileges on affected installations of Epic Games Launcher. The product applies incorrect default permissions to a sensitive folder. | https://trello.com/c/tcS6Jcfy/578-epic-games-launcher-1720 |
| Progress Software WhatsUp Gold WriteDataFile Directory Traversal Remote Code Execution Vulnerability CVE-2024-46909 | Vulnerability allows remote attackers to execute arbitrary code on affected installations of Progress Software WhatsUp Gold. The issue results from the lack of proper validation of a user-supplied path prior to using it in file operations. | https://community.progress.com/s/article/WhatsUp-Gold-Security-Bulletin-September-2024 |
| (Pwn2Own) iXsystems TrueNAS tarfile.extractall Directory Traversal Remote Code Execution Vulnerability CVE-2024-11944 | Vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of iXsystems TrueNAS devices. The specific flaw exists within the tarfile.extractall method. | https://www.truenas.com/docs/core/13.0/gettingstarted/corereleasenotes/#130-u63 |
| Intel Computing Improvement Program PyInstaller Local Privilege Escalation Vulnerability CVE-2023-49797 | Vulnerability allows local attackers to escalate privileges on affected installations of Intel Computing Improvement Program. The issue results from the use of a vulnerable version of PyInstaller. | https://github.com/pyinstaller/pyinstaller/security/advisories/GHSA-9w2p-rh8c-v9g5 |
| XnSoft XnView Classic RWZ File Parsing Integer Underflow Remote Code Execution Vulnerability CVE-2024-11950 | Vulnerability allows remote attackers to execute arbitrary code on affected installations of XnSoft XnView Classic. The issue results from the lack of proper validation of user-supplied data, which can result in an integer underflow before writing to memory. | https://ogma.in/cve-2024-11950-mitigating-xnsoft-xnview-classic-rwz-file-parsing-vulnerability |
| Hewlett Packard Enterprise Insight Remote Support Process Attachment DataStream Directory Traversal Remote Code Execution Vulnerability CVE-2024-53676 | Vulnerability allows remote attackers to execute arbitrary code on affected installations of Hewlett Packard Enterprise Insight Remote Support. The specific flaw exists within the implementation of the processAtatchmentDataStream method. | https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbgn04731en_us&docLocale=en_US |
| (0Day) Fuji Electric Tellus Lite V-Simulator 5 V8 File Parsing Out-Of-Bounds Write Remote Code Execution Vulnerability CVE-2024-11803 | Vulnerability allows remote attackers to execute arbitrary code on affected installations of Fuji Electric Tellus Lite. The specific flaw exists within the parsing of V8 files in the V-Simulator 5 component. | https://www.tenable.com/cve/CVE-2024-11803/cpes |
| Intel Driver & Support Assistant Log Folder Link Following Local Privilege Escalation Vulnerability CVE-2024-36488 | Vulnerability allows local attackers to escalate privileges on affected installations of Intel Driver & Support Assistant. By creating a symbolic link, an attacker can abuse the service to create an arbitrary directory with weak permissions. | https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-01200.html |
| Luxion KeyShot ABC File Parsing Heap-based Buffer Overflow Remote Code Execution Vulnerability CVE-2024-11580 | Vulnerability allows remote attackers to execute arbitrary code on affected installations of Luxion KeyShot. 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://ogma.in/mitigating-cve-2024-11580-secure-luxion-keyshot-against-heap-based-buffer-overflow-attacks |
| IrfanView SVG File Parsing Heap-based Buffer Overflow Remote Code Execution Vulnerability CVE-2024-11509 | Vulnerability allows remote attackers to execute arbitrary code on affected installations of IrfanView. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. | https://debricked.com/vulnerability-database/vulnerability/CVE-2024-11509 |
| Microsoft SharePoint Server FindSpecific Unsafe Reflection Remote Code Execution Vulnerability CVE-2024-38024 | Vulnerability allows remote attackers to execute arbitrary code on affected installations of Microsoft SharePoint Server. The process does not properly restrict a user-supplied argument before using it to create an instance of an object. | https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38024 |
| 7-Zip Zstandard Decompression Integer Underflow Remote Code Execution Vulnerability CVE-2024-11477 | Vulnerability allows remote attackers to execute arbitrary code on affected installations of 7-Zip. Interaction with this library is required to exploit this vulnerability but attack vectors may vary depending on the implementation. | https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/cve-2024-11477-7-zip-flaw-allows-remote-code-execution/ |
| WordPress Core maybe_unserialize Deserialization of Untrusted Data Remote Code Execution Vulnerability CVE-2024-31210 | Vulnerability allows remote attackers to execute arbitrary code on affected installations of WordPress Core. Issue results from the lack of proper validation of user-supplied data, which can result in deserialization of untrusted data. | https://wordpress.org/documentation/wordpress-version/version-6-4-3/ |

# Security Bulletin

### Federal Agencies Advise Against SMS-Based Two-Factor Authentication

The FBI and the Cybersecurity and Infrastructure Security Agency (CISA) have issued advisories urging users to discontinue receiving two-factor authentication (2FA) codes via SMS. This recommendation follows a significant telecommunications breach, attributed to Chinese actors, compromising major networks including AT&T, T-Mobile, and Verizon. Due to the unencrypted nature of SMS messages, intercepted codes are susceptible to malicious exploitation. CISA recommends using encrypted messaging applications like Signal or WhatsApp, authentication apps, or FIDO authentication and passkeys for enhanced security. Users are also advised to maintain strong passwords, use password managers, set device PINs, and keep devices updated.

### Concerns Rise Over Potential Impact on U.S. Cybersecurity Agency

Employees at the U.S. Cybersecurity and Infrastructure Security Agency (CISA) have expressed apprehension regarding potential changes under the incoming administration. Established during the previous term, CISA's future initiatives may face uncertainty due to proposed reductions in government spending and corporate regulation. Staff are particularly concerned about the potential dismantling of current cybersecurity initiatives, the undermining of secure-by-design campaigns, and a reduction in the agency's regulatory powers, all of which could impede their mission to safeguard U.S. infrastructure.

### Unidentified Drones Observed in New Jersey and New York

Over recent weeks, numerous sightings of unidentified drones have been reported across New Jersey, New York City, and parts of Pennsylvania. Observed primarily at night, the origins and intentions of these drones remain unknown, prompting investigations by local, state, and federal authorities, including the FBI and FAA. Speculations regarding their purpose range from military projects to foreign adversaries; however, no concrete explanations have been provided. Officials have called for thorough investigations to provide transparency and reassure the public.

### Fortinet Leads Cybersecurity Sector with Significant Stock Rally

Fortinet, a prominent cybersecurity firm, has been recognized as the IBD Stock of the Day following a 67% stock rally in 2024, closing at 97.62. This performance is attributed to positive third-quarter earnings and favorable analyst evaluations. Despite challenges such as slowing product revenue growth, Fortinet's innovations and strategic market positioning have garnered positive outlooks from analysts. The company's robust growth metrics, including a Composite Rating of 99 and a Relative Strength Rating of 92, underscore its resilience amid competitive pressures and market dynamics.

### Data Breach Settlements Offer Compensation to Affected Individuals

Individuals impacted by data breaches at Lansing Community College, Elekta Inc., Northwestern Memorial Healthcare, and Ticketmaster may be eligible for compensation from settlements totaling millions of dollars. Affected parties are required to submit valid claims by specified deadlines and provide documentation of losses to receive compensation. These settlements highlight the ongoing challenges organizations face in protecting sensitive information and the financial repercussions of data breaches.

### Microsoft's AI Tool 'Recall' Raises Privacy Concerns

Microsoft's AI tool, Recall, designed to capture screenshots every five seconds, has been found to inadvertently save sensitive information, including credit card and Social Security numbers, despite implemented safeguards. This issue raises significant privacy and security concerns, emphasizing the need for stringent data protection measures in AI tools.

### Warnings Issued Against Illegal Streaming Due to Cybersecurity Risks

Cybersecurity experts have issued warnings to Amazon Fire Stick owners against illegally streaming events, such as the Fury vs Usyk fight, due to significant cybersecurity risks. Illegal streaming platforms may harbor malware capable of stealing personal information and granting hackers access to home networks, potentially leading to financial losses. Users are advised to utilize legal channels to access content and avoid severe security risks.

### Krispy Kreme Experiences Cybersecurity Breach Impacting Online Services

Krispy Kreme is addressing a cybersecurity incident that has disrupted its online ordering services in the U.S. since November 29th. The company detected unauthorized access to its systems and is collaborating with cybersecurity experts to resolve the issue. While physical stores remain operational, the breach is expected to have financial implications due to the costs associated with cybersecurity measures. Krispy Kreme has cybersecurity insurance and anticipates no long-term material impact on its overall financial condition.

### U.S. Cyber Official Warns of Chinese Hackers Preparing for Potential Conflict

Chinese hackers are infiltrating U.S. critical infrastructure IT networks in preparation for potential conflicts, according to U.S. Cyber Command. These cyber operations aim to establish advantages in case of significant disputes. Recent incidents include the "Salt Typhoon" hack, compromising telecommunications networks and accessing sensitive data. The U.S. is responding with coordinated defensive and offensive measures, including exposing operations and applying sanctions. China denies involvement in these cyber activities.

### UK's Cybersecurity Chief Warns of Increasing Vulnerability to Cyberattacks

The UK's National Cyber Security Centre (NCSC) has raised concerns about the nation's growing vulnerability to cyberattacks and a perceived complacency towards hacker threats. National defenses have not kept pace with the rise in hostile cyber activities from nations like Russia and China. Recent cyberattacks have disrupted services in various sectors, with most incidents being ransomware attacks predominantly linked to Russian groups. The NCSC emphasizes the urgency of enhancing cyber-resilience across critical infrastructure and the economy.

# Reference Links


1. https://www.infosecurity-magazine.com/news/security-risks-open-source/?&web_view=true
2. https://www.infosecurity-magazine.com/news/ransomware-manufacturing-dollar17b/?&web_view=true
3. https://www.infosecurity-magazine.com/news/five-ransomware-groups-40-of/?&web_view=true
4. https://thehackernews.com/2024/11/over-145000-industrial-control-systems.html?&web_view=true
5. https://www.helpnetsecurity.com/2024/12/04/employees-privileged-access-security-risk/?web_view=true
6. https://threats.wiz.io/all-incidents/gelsemiums-shift-to-linux-malware-with-wolfsbane-and-firewood
7. https://www.bleepingcomputer.com/news/security/chinese-gelsemium-hackers-use-new-wolfsbane-linux-malware/
8. https://x.com/ESET/status/1859619244868059194
9. https://www.eset.com/int/about/newsroom/press-releases/research/eset-research-discovers-wolfsbane-new-linux-cyberespionage-backdoor-by-china-aligned-gelsemium/
10. Unveiling WolfsBane: Gelsemium's Linux counterpart to Gelsevirine
11. https://community.gurucul.com/articles/ThreatResearch/Spot-the-Difference-Earth-Kasha-s-New-22-11-2024?_gl=1*1tr8h5*_gcl_au*MTg4NTAxNDAzNy4xNzMyNjA2NjMw*_ga*MTExOTE4NTgyLjE3MzI2MDY2MzI.*_ga_XK6L3BZR7J*MTczNDY5MTgwOC4yLjAuMTczNDY5MTgxNC41NC4wLjA.
12. https://gurucul.com/latest-threats/spot-the-difference-earth-kashas-new-lodeinfo-campaign-and-the-correlation-analysis-with-the-apt10-umbrella/
13. https://x.com/780thC/status/1858836730985533919
14. Spot the Difference: Earth Kasha's New LODEINFO Campaign And The Correlation Analysis With The APT10 Umbrella | Trend Micro (US)
15. https://www.trendmicro.com/en_in/research/24/k/lodeinfo-campaign-of-earth-kasha.html
16. Feds issue another warning about texting dangers - the scary reason to stop using two-factor authentication now
17. CISA Cuts: Cybersecurity Concerns Under New Administration
18. What We Know About the Mysterious New Jersey Drone Sightings
19. Fortinet Leads Cybersecurity Sector Amidst Robust Market Growth
20. Data Breach Settlements: What You Need to Know
21. Microsoft's AI Tool 'Recall' Sparks Privacy Debate
22. Illegal Streaming Risks Highlighted in Security Warning
23. Krispy Kreme Faces Cybersecurity Breach
24. Chinese Hackers Target U.S. Critical Infrastructure
25. UK's Cybersecurity Chief Warns of Growing Threats
26. https://www.sentinelone.com/labs/operation-digital-eye-chinese-apt-compromises-critical-digital-infrastructure-via-visual-studio-code-tunnels/?&web_view=true
27. https://threatbook.io/blog/id/1095?&web_view=true

## About SDG

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

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


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