NOVEMBER 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

### Highest Number of Data Breach Victims Recorded

Q3 saw a massive increase in supply chain attacks and nearly 242 million US breach victims, according to the quarterly report published by the non-profit Identity Theft Resource Center (ITRC). Cyberattacks remained the most common cause of breaches in Q3, with phishing attacks the most popular attack vector, followed by zero-day exploits, ransomware and malware.

Zero-day attacks in particular are on the rise, climbing 1620% in the first three quarters of 2023 versus the whole of 2022.

A persistent concern is the lack of transparency from breached organizations. The ITRC said over half (53%) of reported breaches did not come with any explanation about the initial attack vector.

### Around 400 US Healthcare Institutions Hit By Ransomware

In the last fiscal year, 389 U.S.-based healthcare institutions were successfully hit with ransomware, causing "network closures, systems offline, critical medical operations delayed, and appointments rescheduled," Microsoft said in its recent annual Digital Defense Report. The company did not say how many were successfully attacked last year. Cybercriminals and nation-states are working in greater tandem, with the most prevalent initial access techniques continuing to be social engineering—specifically email phishing, SMS phishing, and voice phishing—but also identity compromise and vulnerability exploitation in public-facing applications or unpatched operating systems.

### Consumer's Personal Financial Data To Be Better Protected

A new Consumer Financial Protection Bureau (CFPB) rule that gives consumers more choice over financial products and services includes significant privacy protections safeguarding individual's data as per the latest announcement. The rule will require that banks and other institutions only use personal financial data for purposes that consumers request, CFPB said. It also blocks third parties from using consumer data to benefit themselves

In the last fiscal year, 389 U.S.-based healthcare institutions were successfully hit with ransomware.

CRITICAL THREAT ALERT

# Focus of the Month: Living Off the Land Attacks

The threat of "Living Off Land Sites" (LOLS), where attackers exploit legitimate websites and services like GitHub for malicious purposes, is growing. This technique poses a significant challenge because it makes it difficult to distinguish between legitimate and malicious activity. Unlike traditional malware attacks, which leverage signature files to carry out the attack plan, LOTL attacks are fileless—meaning they do not require an attacker to install any code or scripts within the target system. Instead, the attacker uses tools already present in the environment, such as PowerShell, Windows Management Instrumentation (WMI) or the password-saving tool, Mimikatz, to carry out the attack.

## Current Attack Tools

1. **Exploit Kits:** A collection of code and commands or data, these are an efficient way to launch a fileless malware attack, such as a LOTL attack, because they can be injected directly into memory without requiring anything to be written to disk. Adversaries can use them to automate initial compromises at scale. Typically, a victim is lured through a phishing email or social engineering
2. **Native Tools:** Adversaries commonly hijack legitimate tools to escalate privileges, access different systems and networks, steal or encrypt data, install malware, set backdoor access points or otherwise advance the attack path. Eg: PsExec , MIMIKATZ, PowerShell , WMI
3. **Registry Resident Malware:** Malware that installs itself in the Windows registry to remain persistent while evading detection. Windows systems are infected through the use of a dropper program that downloads a malicious file
4. **Fileless Malware:** Ransomware attackers are using fileless techniques to embed malicious code in documents through native scripting languages such as macros or to write the malicious code directly into memory through the use of an exploit. The ransomware then hijacks native tools like PowerShell to encrypt hostage files without ever having written a single line to disk.

## Current Trends and Developments in LOL Models

1. **LOLBAS (Living Off the Land Binaries and Scripts):** A wider approach to document binaries, scripts, and libraries, which must be MS-signed files—either OS NATIVE or MS provided—and have functionality that is useful to an APT. Link: https://github.com/LOLBAS-Project/LOLBAS/tree/master
2. **LOLDRIVERS (Living Off the Land Drivers):** Community-driven project to list drivers that communicate with hardware devices. This aims to root out malicious drivers from circulation. Link: https://www.loldrivers.io/
3. **GTFObins:** A curated repo for Unix binaries exploited by threat actors. This invaluable resource meticulously documents legitimate functions of Unix binaries that can be repurposed for malicious activities, including privilege escalation, shell manipulation, and post-exploitation tasks. GTFOBins serves as a guide for defenders to fortify their systems against exploitation and enhance security posture. Link: https://gtfobins.github.io/
4. **Living Off the Orchard:** A curated repo for MacOS ecosystem. This resource provides detailed information on built-in macOS binaries and how they can be potentially misused for various malicious activities. By raising awareness about the potential for abuse, LOOBins helps improve the security posture of macOS devices. Link https://www.loobins.io/binaries/

CRITICAL THREAT ALERT

# Focus of the Month: Living Off the Land Attacks

## Commonly Abused Platforms

Popular online platforms have been exploited for harmful purposes due to their widespread use and trust.

### Social Media Platforms

- **Facebook:** Used for spreading misinformation, phishing scams, and hate speech.
- **Twitter:** A hub for spreading fake news, harassment, and coordinated disinformation campaigns.
- **Instagram:** Often used for catfishing, sextortion, and promoting fraudulent products.

### Messaging Apps

- **WhatsApp:** A popular platform for spreading spam, malware, and scams.
- **Telegram:** Can be used for sharing illegal content, coordinating terrorist activities, and spreading misinformation.

### Online Marketplaces

- **eBay:** Can be used for selling counterfeit goods, stolen items, and illegal products.
- **Amazon:** A platform for promoting fraudulent products, engaging in price gouging, and selling counterfeit items.

### Gaming Platforms

- **Steam:** Used for distributing malware, promoting phishing scams, and engaging in online harassment.
- **Discord:** Can be used for spreading hate speech, coordinating online attacks, and sharing illegal content.

### Email Services

- **Gmail:** A common target for phishing attacks, spam, and malware distribution.
- **Outlook:** Often used for spreading malware, phishing scams, and identity theft.

### Cloud Storage Platforms

- **Dropbox:** Can be used for storing and sharing illegal content, malware, and stolen data.
- **Google Drive:** A platform for sharing and distributing malware, phishing scams, and stolen data.

**Training Data Validation:** Prior to starting model training, all data should be validated to detect and filter out any suspicious or potentially malicious data points. This helps safeguard against the risk of threat actors inserting and later exploiting such data.

**Adversarial Sample Training:** Introducing adversarial samples during the model's training phase is a vital proactive security defense measure to stop many data poisoning attacks. This enables the ML model to correctly classify and flag such inputs as inappropriate.

**Diversity in Data Source:** Using multiple data sources enables an organization to diversify its ML model training data sets, significantly reducing the efficiency of many data poisoning attacks.

**Continuous Monitoring and Auditing:** Like all information systems, AI systems need strict access controls to prevent unauthorized users from accessing them. Apply the principle of least privilege and set logical and physical access controls to mitigate risks associated with unauthorized access. Continuous monitoring and auditing should also focus on the model's performance, outputs, and behavior to detect potential signs of data poisoning.

# Monthly Highlights

## Hybrid Work Exposes New Vulnerabilities in Print Security

**The shift to hybrid work models has revealed new vulnerabilities in corporate print infrastructures, increasing security risks for many organizations. These risks span various issues, including employees using unsecured, unmanaged printers, remote workers transmitting print jobs over public networks, insufficient user authentication, exposed local spools and caches, and inconsistent patching practices.**

A small but consistent number of print-related vulnerabilities have worsened these problems. Recent examples include CVE-2024-38199 (a remote code execution vulnerability in Windows or Line Printer Daemon [LPD] Service), CVE-2024-21433 (a Windows Print Spooler elevation of privilege vulnerability), and CVE-2024-43529 (a similar vulnerability disclosed by Microsoft in its October security update). Importantly, these threats are not limited to Windows. Researchers recently uncovered serious flaws in the Common Unix Printing System (CUPS), a legacy protocol commonly used in Linux, Unix, and mixed environments.

While none of these issues have posed the same level of threat as the 2021 PrintNightmare RCE flaw in the Windows Print Spooler service, they have made managing modern print infrastructure more complex. Attackers, including nation-state actors, have exploited printer software vulnerabilities, such as CVE-2022-38028, to significant effect in their campaigns.

These trends have led to an increase in print-related data breaches. A recent study by Quocirca revealed that 67% of respondents experienced a printer-related security incident in 2024, up from 61% the previous year. Small and mid-sized businesses were hit harder, with 74% reporting printer-related data loss. Additionally, 33% cited unmanaged, employee-owned printers as a major security concern, while 29% identified vulnerabilities in office printing environments as a serious risk. Over a quarter (28%) highlighted the protection of sensitive information as their biggest challenge related to printer security.

While none of these issues have posed the same level of threat as the 2021 PrintNightmare RCE flaw in the Windows Print Spooler service, they have made managing modern print infrastructure more complex.

Casey Ellis, founder and chief strategy officer at Bugcrowd, emphasizes the importance of prioritizing print security. “Printers and print servers are ideal for establishing persistence and gathering business intelligence on a target,” he explains. The CUPS vulnerabilities demonstrated that old or unused printer software can still pose a significant risk, especially for internal attacks or lateral movement.

"If your vulnerability management process lets out-of-sight, out-of-mind thinking dictate priorities, you can easily overlook printer security risks."

Unfortunately, many organizations may be underestimating or ignoring these risks. According to Ellis, the transition to cloud or hybrid print environments has made print infrastructure a more "invisible" issue in terms of vulnerability management. "Let's be honest—the number of people who regularly think about or work with printers is very small," he says. "If your vulnerability management process lets out-of-sight, out-of-mind thinking dictate priorities, you can easily overlook printer security risks."

Ellis's main message is that organizations must stay vigilant about their asset inventory and overall attack surface, ensuring they have processes in place for evaluating risk. The legacy nature of many printer environments is another challenge, as vulnerabilities may go undetected for years. These environments often lack the monitoring tools that are common on other endpoint systems, making them attractive targets for attackers.

Tom Boyer, director of security at Automox, points out that many flaws in print infrastructure arise because print services are often enabled by default, with administrators unaware of their presence. "This allows risks to remain hidden for years, giving adversaries an advantage," he says. "They often know more about the target environment than the company itself."

The Quocirca survey also found that security concerns are the top barrier to adopting cloud print services. "Although many organizations view the cloud as more secure than on-premise environments, security concerns remain a significant obstacle to cloud print adoption," says Nicole Heinsler, chief engineer of security and device management at Xerox. "There is often a disconnect between providers and clients about how the cloud can improve security by handling zero-day threats more effectively, and how data sovereignty can be better managed through cloud policies."

## Nearly 400 US Healthcare Institutions Hit With Ransomware Over Last Year, Microsoft Says

**The ransomware threat has significantly escalated over the past year, with hundreds of healthcare institutions falling victim to attacks, according to a report from Microsoft on Tuesday. Over the past fiscal year, 389 healthcare organizations in the U.S. were successfully targeted by ransomware, leading to "network closures, systems being taken offline, delays in critical medical operations, and rescheduled appointments," Microsoft noted in its annual Digital Defense Report. However, the company did not specify how many attacks were successful the previous year.**

The 114-page report analyzed cybersecurity trends from July 2023 to June 2024, drawing on vast amounts of intelligence data. Microsoft's researchers found an increasing level of coordination between nation-states and cybercriminals. Russia, North Korea, and Iran, in particular, were identified as leveraging ransomware to financially benefit from their cyber operations. This marks a shift from prior strategies, where ransomware appeared financially motivated but was often used for destructive purposes.

Microsoft's researchers found an increasing level of coordination between nation-states and cybercriminals. Russia, North Korea, and Iran, in particular, were identified as leveraging ransomware to financially benefit from their cyber operations.

Among Microsoft's customers, there was a 2.75-fold increase in incidents of human-operated ransomware, which occurs when at least one device within a network is targeted. However, the report highlighted some positive developments: the percentage of ransomware attacks that progressed to the stage of device encryption—where systems are locked—has declined significantly over the past two years.

In cases where systems were encrypted and a ransom demanded, attackers often exploited unmanaged devices within the network to either gain access or encrypt assets remotely at the point of impact. Experts have long warned that the proliferation of internet-of-things (IoT) devices and unauthorized tools introduced into workplaces by employees increases organizations' risk exposure.

"The most common initial access methods remain social engineering tactics—such as phishing via email, SMS, or voice—along with identity compromise and the exploitation of vulnerabilities in public-facing applications or unpatched operating systems," explained Tom Burt, Microsoft's corporate vice president of customer security and trust.

To illustrate the impact of ransomware, Microsoft cited the case of the Church of Sweden, which was attacked by the now-defunct BlackCat ransomware gang in November 2023. The church took two months to recover, which disrupted its fundraising efforts during the Christmas season and affected its ability to conduct funerals and serve its 5.4 million members. The church's data was sold to the

LockBit ransomware gang, which published it after the church refused to pay the ransom.

According to Microsoft, the top ransomware groups tracked were Akira, responsible for 17% of attacks, and LockBit, which accounted for 15%. Other significant groups included Play, BlackCat, and Basta. The report also highlighted some progress in combating ransomware, noting that law enforcement had successfully taken down infrastructure used by LockBit and BlackCat in the past year.

Microsoft also emphasized its efforts to enhance threat-sharing capabilities, stating that it is "actively working to share information, as permitted by law, to fight against the most significant threats to our customers and business." The company showcased its collaborative threat intelligence platform, "Crystal Ball," developed with the Israel National Cyber Directorate and the Cyber Security Council of the United Arab Emirates. This platform is currently used by more than 10 members of the International Counter Ransomware Initiative (CRI) and provides threat intelligence, guides for attribution, deterrence strategies, and methods for nations to collaborate more effectively. Microsoft aims to have all CRI members onboard by the end of the year.

The company showcased its collaborative threat intelligence platform, "Crystal Ball," developed with the Israel National Cyber Directorate and the Cyber Security Council of the United Arab Emirates.

## Majority of Global CISOs Want To Split Roles As Regulatory Burdens Grow

**Research from Trellix reveals that increasing cybersecurity demands from the SEC and other government bodies are pushing CISOs to their limits. According to a report released Tuesday by Trellix and Vanson Bourne, more than 80% of CISOs believe their role should be split into two separate positions, as regulatory and financial responsibilities take up more of their time.**

Most CISOs advocate for dividing the job into two distinct roles: one focused on technical, hands-on security tasks, and another dedicated to regulatory compliance and board-level disclosures. Regulatory changes from the Securities and Exchange Commission (SEC) and other agencies have been both a benefit and a burden for CISOs, explained Harold Rivas, CISO at Trellix.

Nearly 90% of respondents said the evolving regulatory environment is reshaping the role of the CISO, with 80% saying that keeping up with new regulations is becoming unsustainable.

"On the positive side, these changes have raised the profile of cybersecurity and made it a key topic in boardrooms," Rivas said in an email. "However, they have also increased personal liability for CISOs, adding a new layer of stress to the role."

The report is based on a survey of more than 500 CISOs from the Americas, Europe, the Middle East, and the Asia-Pacific region, conducted by Vanson Bourne in August and September. The survey found that CISOs' responsibilities have shifted dramatically due to SEC incident-reporting requirements and broader corporate governance changes. These changes now require CISOs to regularly engage with boards and senior leadership.

A key concern is the increased legal risk for CISOs if their organizations fail to disclose cybersecurity threats. The SEC's ongoing civil fraud case against SolarWinds and its CISO, Timothy Brown, over the alleged failure to disclose cyber risks to investors prior to the 2020 Sunburst attacks, is a prime example of this.

Nearly 90% of respondents said the evolving regulatory environment is reshaping the role of the CISO, with 80% saying that keeping up with new regulations is becoming unsustainable. Close to half of those surveyed reported meeting with their boards every week.

However, Michelle Horton, principal of cyber, risk, and regulatory at PwC US, disagreed with the idea of splitting the CISO role. She suggested that this might reflect a lack of maturity in risk management at some organizations.

"Effective risk management and regulatory compliance should be a collaborative effort across departments such as legal, cybersecurity, risk management, compliance, and internal audit," Horton said in an email. "This isn't necessarily a reason to divide the CISO role."

In June, the Biden administration introduced plans to streamline the growing number of compliance requirements. These regulations call for companies to quickly report major cyberattacks, disclose their cyber resilience strategies, and meet minimum security standards within their respective industries.

## Over 240 Million US Breach Victims Recorded in Q3

**This year is not expected to set a new record for data compromises, despite a significant increase in supply chain attacks and nearly 242 million U.S. breach victims reported in Q3, according to the Identity Theft Resource Center (ITRC). The non-profit organization tracks publicly disclosed U.S. data breaches and accidental leaks for its quarterly reports.**

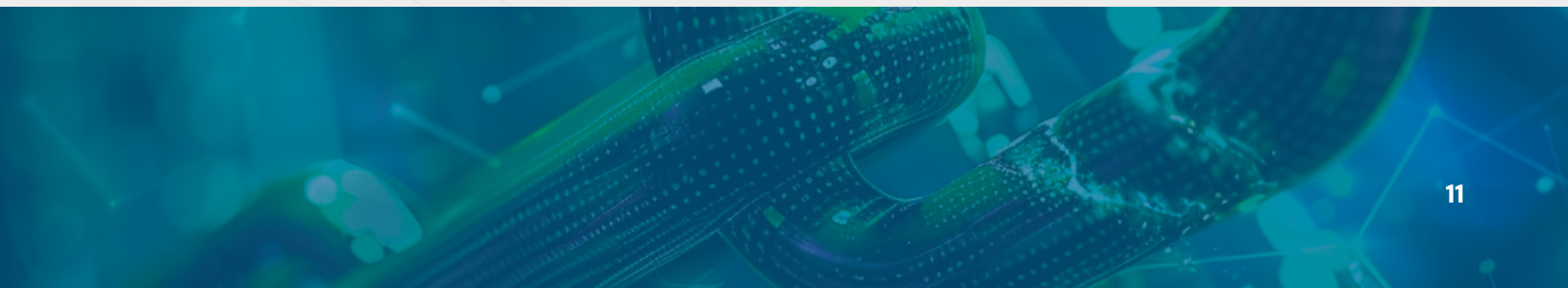
The latest report showed a 77% decrease in the number of data breach and leak victims compared to the previous quarter. However, this drop is mainly due to Q2's unusually high figure of 940 million victims, which was inflated by two major breaches at Ticketmaster and Advanced Auto Parts.

In Q3, the total number of "data compromises"—which includes both breaches and leaks—was 672, reflecting an 8% decline from the previous quarter. However, the report revealed some concerning trends. Notably, supply chain attacks surged by 203% quarter-on-quarter after a decline in the first half of 2024. A total of 31 breaches and data exposures affected 97 entities and nearly one million victims.

"While we may not break the record for data compromises this year like we did in 2023, the Q3 2024 Data Breach Report highlights some notable trends," said Eva Velasquez, CEO of ITRC. "In particular, the growing number of businesses reporting multiple data breaches in the past 12 months and the resurgence of mega-data breaches impacting over 100 million people. These trends emphasize the need for businesses to keep prioritizing data and identity protection, and for consumers to take steps to make their information less valuable to criminals."

One of the major breaches Velasquez referred to involved telecom giant AT&T, where 110 million victims were affected after threat actors downloaded customer data, including call logs, from its Snowflake account.

One of the major breaches Velasquez referred to involved telecom giant AT&T, where 110 million victims were affected after threat actors downloaded customer data, including call logs, from its Snowflake account. Another significant breach in Q3 was an accidental data leak by MC2 Data, a background check company, which left 2.2TB of sensitive data exposed online without password protection. Fortunately, there is no indication that cybercriminals accessed the information before the issue was resolved.



## Sonatype Reports 156% Increase in OSS Malicious Packages

**As the use of open source software (OSS) skyrockets, there has been a 156% increase in open source malware, according to new research from Sonatype. Since 2019, over 704,102 malicious packages have been identified, with 512,847 discovered since November 2023 alone, as highlighted in Sonatype's 10th Annual State of the Software Supply Chain report.**

This year has set a new record for open-source consumption, reaching an estimated 6.6 trillion downloads. JavaScript (npm) alone accounted for an astonishing 4.5 trillion requests in 2024, marking a 70% year-over-year growth. Python (PyPI), spurred by the growth of AI and cloud technologies, is projected to hit 530 billion package requests by the end of 2024, reflecting an 87% increase from the previous year.

Though more than 99% of packages have updated versions available, 80% of application dependencies go un-upgraded for over a year.

Npm and PyPI are package managers for JavaScript and Python, respectively. Despite this massive consumption, organizations are struggling with effective risk mitigation. Sonatype's research shows that while many open source projects are becoming contaminated, vulnerabilities are inevitable in all software, whether open source or commercial.

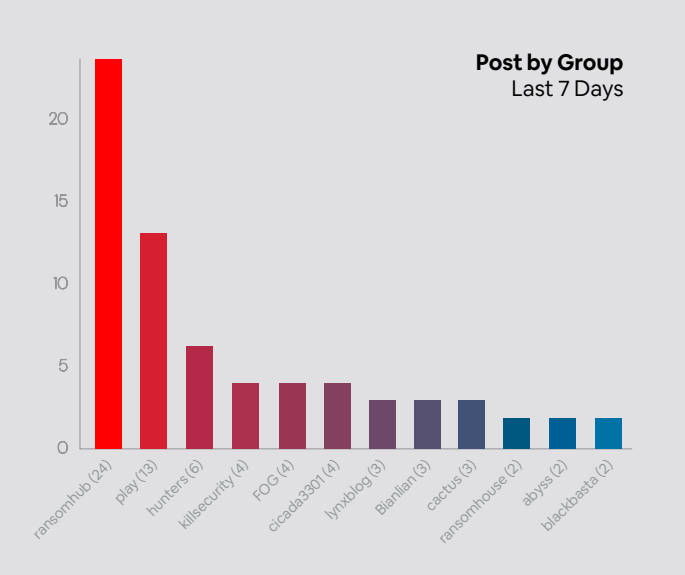
Though more than 99% of packages have updated versions available, 80% of application dependencies go un-upgraded for over a year. Additionally, in 95% of cases where vulnerable components are used, a fixed version is already available. The persistent risk is underscored by the fact that three years after the Log4Shell exposure, 13% of Log4j downloads remain vulnerable.

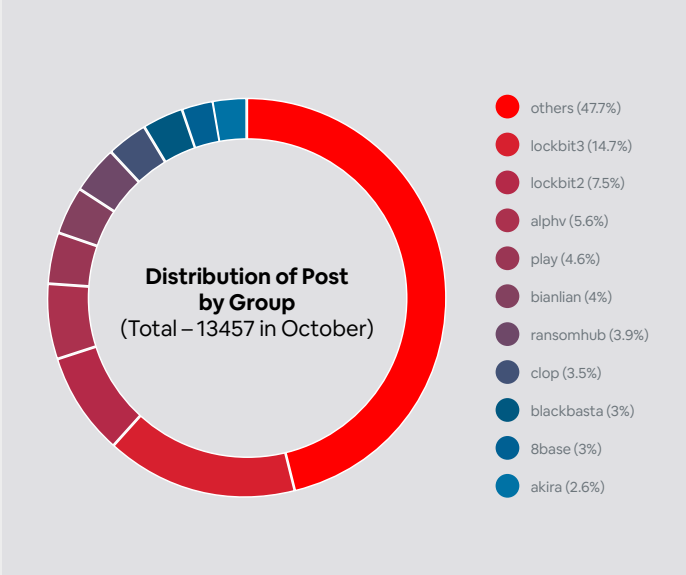
The report also notes that publishers face challenges in addressing Common Vulnerabilities and Exposures (CVEs), with some vulnerabilities taking over 500 days to fix. Between 2013 and 2023, CVEs saw a 463% increase.

Sonatype's report calls on software manufacturers, consumers, and regulators to adopt more rigorous security practices. The balance between innovation and security is now more crucial than ever. Brian Fox, CTO and Co-Founder at Sonatype, emphasized, "Over the past decade, software supply chain attacks have grown in sophistication and frequency, especially with the rise of open source malware, yet publishers and consumers have made limited progress in improving security. To secure the open source ecosystem for the future, we need proactive security measures, heightened vigilance against malware, and comprehensive management of dependencies."

Despite these challenges, regulatory bodies are beginning to catch up. New policies, such as the EU's updated Network and Information Systems Directive (NIS2), set to take effect on October 17, 2024, as well as upcoming regulations in India and Australia, are promoting the adoption of Software Bill of Materials (SBOMs). Over 60,000 SBOMs have been published in the past year, helping to enhance software transparency and security.

# Ransomware Tracker




# Articles

## Storm-0501: Unveiling a Relentless Financially Motivated Threat Actor Exploiting Cloud Services

### Executive Summary

Microsoft has reported a sophisticated, multi-staged attack launched by the threat actor known as Storm-0501, which targeted hybrid cloud environments. This campaign resulted in significant incidents, including data exfiltration, credential theft, ransomware deployment, and persistent backdoor access across various sectors in the United States. This article delves into Storm-0501's tactics, techniques, and procedures (TTPs), their attack methodology, and mitigation strategies for organizations to protect their environments.

### Detection

#### Overview of the attack

- **Threat Actor:** Storm-0501, a financially motivated cybercriminal group.
- **Primary Targets:** U.S. sectors including government, manufacturing, transportation, and law enforcement.
- **Attack Vector:** Multi-staged attack exploiting weak credentials and over-privileged accounts to transition from on-premises systems to cloud environments.

#### Tactics, Techniques, and Procedures (TTPs)

- **Initial Access:**
  - Exploited vulnerabilities in public-facing servers (e.g., CVE-2022-47966 in Zoho ManageEngine, CVE-2023-4966 in Citrix NetScaler).
  - Leveraged access brokers and compromised credentials.
- **Credential Access and Lateral Movement:**
  - Utilized Impacket's SecretsDump module and tools like Cobalt Strike for credential extraction and lateral movement.
  - Employed brute force attacks and methods to gather sensitive files, including KeePass credentials.
- **Data Exfiltration:**
  - Used Rclone masqueraded as legitimate Windows binaries to transfer data to cloud storage services.
- **On-Premises to Cloud Pivot:**
  - Compromised Microsoft Entra Connect Sync accounts to gain persistent access to cloud environments.
  - Exploited cloud session hijacking methods to escalate privileges.

## Indicators of Compromise

| FileName | SHA-256 | Description |
|---|---|---|
| PostalScanImporter.exe, win.exe | efb2f6452d7b0a63f6f2f4d8db49433259249df598391dd79f64df1ee3880a8d | Embargo ransomware |
| win.exe | a9aeb861817f3e4e74134622cbe298909e28d0fcc1e72f179a32adc637293a40 | Embargo ransomware |
| name.dll | caa21a8f13a0b77ff5808ad7725ff3af9b74ce5b67426c84538b8fa43820a031 | Cobalt Strike |
| 248.dll | d37dc37fdcebbe0d265b8afad24198998ae8c3b2c6603a9258200ea8a1bd7b4a | Cobalt Strike |
| cs240.dll | 53e2dec3e16a0ff000a8c8c279eeeca8b4437edb8ec8462bfbd9f64ded8072d9 | Cobalt Strike |
| fel.ocx | 827f7178802b2e92988d7cff349648f334bc86317b0b628f4bb9264285fccf5f | Cobalt Strike |
| theme.ocx | ee80f3e3ad43a283cbc83992e235e4c1b03ff3437c880be02ab1d15d92a8348a | Cobalt Strike |
| hana.ocx | de09ec092b11a1396613846f6b082e1e1ee16ea270c895ec6e4f553a13716304 | Cobalt Strike |
| obfs.ps1 | d065623a7d943c6e5a20ca9667aa3c41e639e153600e26ca0af5d7c643384670 | ADRecon |
| recon.ps1 | c08dd490860b54ae20fa9090274da9ffa1ba163f00d1e462e913cf8c68c11ac1 | ADRecon |

## Prevention

To mitigate the risks associated with Storm-0501's attack methods, organizations should implement the following measures:

### Credential Hygiene

- Apply the principle of least privilege.
- Regularly audit privileged account activities in Microsoft Entra ID environments.

### Conditional Access Policies

- Enable policies to assess every user sign-in attempt, such as device compliance or trusted IP addresses.

### Enhanced Authentication Measures

- Implement Conditional Access authentication strength to require phishing-resistant methods for critical applications.

### Active Directory Federation Services Security

- Follow Microsoft's best practices for securing ADFS.

### Endpoint Detection and Response (EDR)

- Run EDR in block mode to proactively remediate detected threats.

## Remediation

### Incident Response

In the event of an attack:

- I**nvestigation and Remediation:** Enable automated investigation and remediation to promptly respond to alerts.
- **Restoration of Services:** Identify and isolate compromised accounts, ensuring thorough remediation and restoring secure configurations.
- **User Education:** Conduct regular training sessions on identifying phishing attempts and safeguarding credentials.

# CeranaKeeper: A Relentless Threat to Thai Government Institutions

## Executive Summary

- Security researchers discovered a new China-aligned threat actor, CeranaKeeper, targeting governmental institutions in Thailand.
- The group uses updated tools previously attributed to Mustang Panda and has developed new methods for data exfiltration.
- CeranaKeeper exploits popular cloud services (e.g., Dropbox, OneDrive, GitHub) to execute commands and exfiltrate sensitive documents.
- CeranaKeeper has been active since at least early 2022, focusing on government entities in Asia.
- The group's adaptability and innovative tactics, including a stealthy reverse shell using GitHub, highlight its sophistication.

### Key Findings

- CeranaKeeper constantly updates its backdoor to evade detection and uses diversified methods for massive data exfiltration.
- It employs a variety of custom tools, including WavyExfiller, DropboxFlop, OneDoor, and BingoShell, tailored for specific attack vectors.
- The group's operations reveal a systematic approach to compromising networks and harvesting sensitive data.

### Attribution

- Security researchers attribute the activities of CeranaKeeper to a separate threat actor distinct from Mustang Panda, based on technical analysis and operational patterns.

### Compromise Mechanisms

- CeranaKeeper gained access to a Thai government network by conducting brute-force attacks against a domain controller.
- After compromising a machine, the attackers installed their backdoor and used it to deploy additional tools across the network.

### Toolset Aiding Massive Exfiltration

- WavyExfiller: A Python uploader using Dropbox and PixelDrain for document exfiltration.
- DropboxFlop: A backdoor leveraging Dropbox for command execution and file uploads.
- OneDoor: A C++ backdoor utilizing OneDrive for similar purposes.
- BingoShell: A sophisticated backdoor employing GitHub for command-and-control activities.

## Detection

- **Behavioral Analysis:** Monitor for unusual activity related to known cloud services, such as frequent file uploads or command executions from unexpected locations.
- **Threat Intelligence Feeds:** Integrate intelligence on known CeranaKeeper indicators of compromise (IOCs), including file hashes and C&C domains.
- **Log Monitoring:** Review logs for anomalies, particularly regarding user authentication attempts and unusual network traffic patterns.

## Indicators of Compromise

| SHA256 | FileName | Detection | Description |
|---|---|---|---|
| B25C79BA507A256C9CA12A9BD34DEF6A33F9C087578C03D083D7863C708ECA21 | EACore.dll | Win32/Agent.VJO | YK0130 reverse shell. |
| E7B6164B6EC7B7552C93713403507B531F625A8C64D36B60D660D66E82646696 | SearchApp.exe | Python/Agent.AGT | WavyExfiller. |
| 3F81D1E70D9EE39C83B582AC3BCC1CDFE038F5DA31331CDBCD4FF1A2D15BB7C8 | OneDrive.exe | Win32/Agent.VKV | OneDoor. |
| DAFAD19900FFF383C2790E017C958A1E92E84F7BB159A2A7136923B715A4C94F | dropbox.exe | Python/Agent.AQN | PyInstaller DropFlop. |
| 24E12B8B1255DF4E6619ED1A6AE1C75B17341EEF7418450E661B74B144570017 | Update.exe | Python/Agent.AJJ | BingoShell. |
| 451EE465675E674CEBE3C42ED41356AE2C972703E1DC7800A187426A6B34EFDC | oneDrive.exe | Python/Agent.AGP | WavyExfiller PixelDrain variant. |
| E6AB24B826C034A6D9E152673B91159201577A3A9D626776F95222F01B7C21DB | MsOcrRes.orp | Win32/Agent.AFWW | TONESHELL type B. |
| 6655C5686B9B0292CF5121FC6346341BB888704B421A85A15011456A9A2C192A | avk.dll | Win32/Agent.VJQ | TONESHELL variant. |
| B15BA83681C4D2C2716602615288B7E64A1D4A9F4805779CEBDF5E6C2399AFB5 | TurboActivate.dll | Win32/Agent.AFWX | TONESHELL loader. |

| IP | Domain | Hosting Provider | First Seen | Details |
|---|---|---|---|---|
| 104.21.81[.]233<br>172.67.165[.]197 | www.toptipvideo[.]com | CLOUDFLARENET (AS13335) | 20230814 | C&C server for the YK0130 reverse shell. |
| 103.245.165[.]237 | dljmp2p[.]com<br>inly5sf[.]com | Bangmod Enterprise administrator (AS58955) | 20230421 | C&C servers for TONESHELL variants. |
| 103.27.202[.]185 | www.dl6yfsl[.]com | Bangmod Enterprise administrator (AS58955) | 20230810 | C&C server for TONEINS variant. |
| 103.27.202[.]185 | www.uvfr4ep[.]com | Bangmod Enterprise administrator (AS58955) | 20230922 | C&C server for TONEINS variant. |

## Prevention

- **Access Control:** Implement strict access controls to limit administrative access to critical systems.
- **Security Hygiene:** Regularly update and patch systems to mitigate vulnerabilities that CeranaKeeper might exploit.
- **User Training:** Conduct regular training for staff on phishing and social engineering tactics to reduce the risk of initial compromise.

## Remediation

- **Incident Response Plan:** Establish a comprehensive incident response plan that includes identification, containment, eradication, and recovery steps.
- **System Recovery:** Rebuild compromised systems from known good backups and ensure thorough scanning for malware.
- **Continuous Monitoring:** After remediation, maintain heightened monitoring of systems for any signs of reinfection or further unauthorized access.

## Chinese 'Crimson Palace' Espionage Campaign Keeps Hacking Southeast Asian Governments


This year, a complex trio of Chinese cyberespionage groups has been playing a high-stakes game of cat and mouse with defenders. Despite efforts to stop their activities, the hackers have launched a series of attacks on Southeast Asian government institutions.

Sophos researchers have released their second report, titled "Crimson Palace," which details an espionage operation in Southeast Asia that was carried out by Chinese state-sponsored hackers.

Researchers looked at the three groups running the campaign's activities last year—two of which resumed their efforts in the autumn of 2023 and this year.

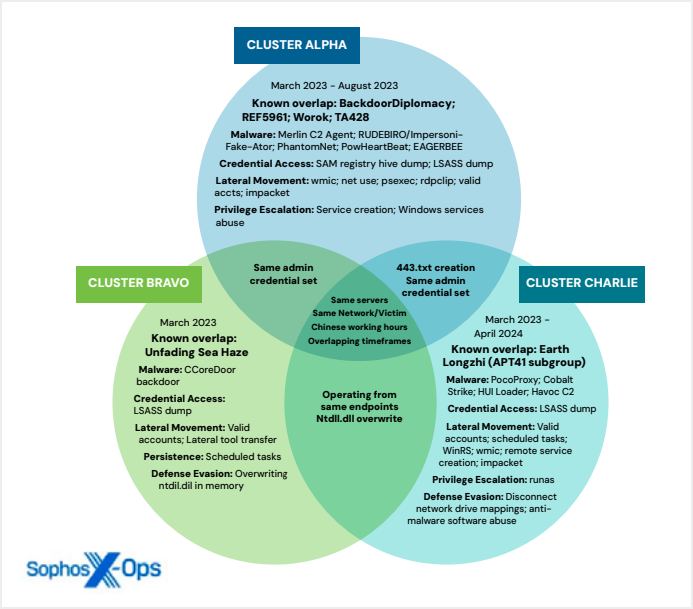
The three groups, which Sophos refers to as Cluster Alpha, Cluster Bravo, and Cluster Charlie, are all associated with Chinese state-backed organizations as well as APT15 and a subgroup of APT41 that some researchers have identified.

### Detection

The organizations continue to carry out attacks and are currently growing their activities to penetrate other Southeast Asian organizations.

The groups shifted to more open-source tools after Sophos detected and blocked many of their proprietary tools, demonstrating "how quickly these attacker groups can adapt and remain persistent."

Additionally, they were seen using a new tool called "Tattletale," which is a malware researcher's tool for "impersonating users who have signed into the system and gathering information related to password policies, security settings, cached passwords, browser information, and storage data."




In addition to continuously trying to re-enter victim networks, the hackers' primary objective in the Crimson Palace campaign remains the exfiltration of information and data.

"They took sensitive documents, cloud infrastructure keys, including backups and disaster recovery keys, other important authentication keys and certificates, and IT and network infrastructure configuration data," Sophos said.

The attackers' main goals were to obtain more information, circumvent security tools, and obtain deeper access to a company's network. Several strategies that Sophos ascribed to the other groups were adopted by Cluster Charlie, supporting their earlier conclusion that they are all part of the same organization.

Sophos MDR once more saw the actors executing a malicious file (C:\ProgramData\mios.exe) on a targeted system using atexec from an unmanaged network device to create internal and external communications:

- **Internal Comms:** C:\Windows\system32\cmd.exe /C "c:\programdata\mios.exe 172.xx.xxx.xx 65211"
- **External Comms:** c:\programdata\mios.exe  178.128.221.202 443 (Digital Ocean, Singapore)

## Indicators of Compromise

| |
|---|
| 103.19.16.248:443 // dmsz.org (geolocated in Philippines) |
| 103.56.5.224:443 // cancelle.net (geolocated in Philippines) |
| 49.157.28.114:443 // gandeste.net (geolocated in Philippines) |

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

## CosmicBeetle Deploys Custom ScRansom Ransomware, Partnering with RansomHub

Attacks targeting small and medium-sized businesses (SMBs) in Europe, Asia, Africa, and South America have introduced a new custom ransomware strain called ScRansom, which was released by the threat actor CosmicBeetle, who is most likely an affiliate of RansomHub.

ESET researcher Jakub Souček stated in a new analysis released that CosmicBeetle replaced its previously used ransomware, Scarab, with ScRansom, which is continuously improved. The threat actor can compromise intriguing targets despite not being very good.

The manufacturing, pharmaceutical, legal, healthcare, education, technology, hospitality, leisure, financial services, and regional government sectors are among the industries targeted by ScRansom attacks.

The most well-known product of CosmicBeetle is Spacecolon, a malicious toolkit that was previously found to be used to spread the Scarab ransomware throughout victim organizations around the world.

### Detection

It is currently unknown who is responsible for the attack or where they are from, although a previous theory suggested that they might be Turkish because they used a unique encryption method in another program called ScHackTool. But according to ESET, the attribution is no longer credible.

Souček noted that the legitimate Disc Monitor Gadget uses the same encryption scheme as ScHackTool. VOVSOFT, the Turkish software company that created the tool, most likely modified this algorithm [from a Stack Overflow thread]. Years later, CosmicBeetle discovered it and utilized it for ScHackTool.

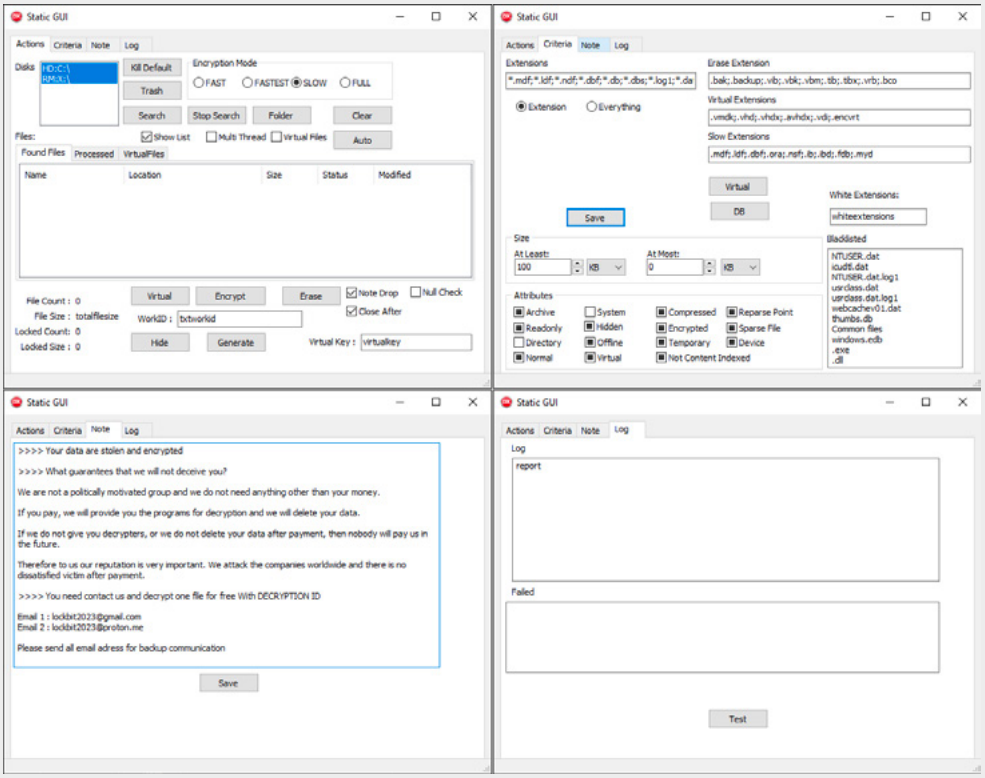
CosmicBeetle frequently breaches its targets using brute-force techniques. The threat actor is also taking advantage of the following vulnerabilities:

- CVE-2017-0144, also known as EternalBlue
- Vulnerability CVE-2023-27532 (a Veeam Backup & Replication component)
- Through noPac, the AD privilege escalation vulnerabilities CVE-2021-42278 and CVE-2021-42287
- CVE-2022-42475 (a FortiOS SSL-VPN vulnerability)
- CVE-2020-1472, also known as Zerologon.

The most frequent victims of this threat actor are SMBs from a wide range of verticals worldwide, as they are the group most likely to use the impacted software and lack effective patch management procedures.

## Technical Analysis

Delphi applications typically have a graphical user interface (GUI), but ransomware does not. A structured GUI is present in every ScRansom sample. The older samples, which the developers typically refer to as "Static," need user intervention to encrypt anything. Given that running such samples in analysis sandboxes does not reveal any malicious activity, this seemingly complicated issue could be one of the reasons ScRansom managed to avoid detection for a while.




The threat actor must be able to access the victim's screen and control their mouse to launch such an encryptor. CosmicBeetle has previously employed this strategy.

ScHackTool is another tool that requires manual interaction and must be run on the victim's computer. We don't know exactly how CosmicBeetle accomplishes this, but based on the other tools we've seen, we think the most likely scenario is using RDP and VPN access with credentials that have already been stolen.

Additionally, CosmicBeetle has experimented with "SSH," a rare variant. The encryptor logic is the same as the other variants, but it encrypts files over FTP rather than local files.

Automation is used in newer builds, but only to simulate clicking the right buttons from code. Typically, these automated builds—dubbed "Auto" by the developers—come with little tools or scripts to remove shadow copies in an MSI installer. This hides the GUI by default.

CosmicBeetle typically has a complicated graphical user interface (GUI) with numerous buttons, some of which are inactive. Although the four-tab GUI appears complicated, the functionality is quite simple. ScRansom encrypts data on all removable, remote, and fixed drives.

# Indicators of Compromise

## Files

| SHA-1 | Filename | Detection | Description |
|---|---|---|---|
| 4497406D6EE7E2EF561C949AC88BB973BDBD214B | auto.exe | Win32/Filecoder.Spacecolon.A | Auto variant of ScRansom. |
| 3C32031696DB109D5FA1A09AF035038BFE1EBE30 | Project1.exe | Win32/Filecoder.Spacecolon.B | Auto variant of ScRansom. |
| 26D9F3B92C10E248B7DD7BE2CB59B87A7A011AF7 | New.exe | Win32/Filecoder.Spacecolon.A | Static variant of ScRansom. |
| 1CE78474088C14AFB8495F7ABB22C31B397B57C7 | Project1.exe | Win32/Filecoder.Spacecolon.B | Auto encryptor variant of ScRansom, Turkish ransom note. |
| 1B635CB0A4549106D8B4CD4EDAFF384B1E4177F6 | Project1.exe | Win32/Filecoder.Spacecolon.A | Static SSH encryptor variant of ScRansom. |
| DAE100AFC12F3DE211BFF9607DD53E5E377630C5 | Project1.exe | Win32/Filecoder.Spacecolon.A | Decryptor variant of ScRansom (oldest). |
| 705280A2DCC311B75AF1619B4BA29E3622ED53B6 | Rarlab_sib.msi | Win32/Filecoder.Spacecolon.A | MSI file with embedded ScRansom, ScKill, BAT script to stop services, and BAT script to delete shadow copies. |

## Network

| IP | Domain | Hosting provider | First seen | Details |
|---|---|---|---|---|
| 66.29.141[.]245 | www.lockbitblog[.]info | Namecheap, Inc. | 2023-11-04 | Fake LockBit leak site. |

# Ransom Notes Fragments

## Email Addresses

| |
|---|
| decservice@ukr[.]net |
| nonamehack2024@gmail[.]com |
| tufhackteam@gmail[.]com |
| nonamehack2023@gmail[.]com |
| nonamehack2023@tutanota[.]com |
| lockbit2023@proton[.]me |
| serverrecoveryhelp@gmail[.]com |
| recoverydatalife@gmail[.]com |
| recoverydatalife@mail[.]ru |

## Tox IDs

| |
|---|
| 91E3BA8FACDA7D4A0738ADE67846CDB58A7E32575531BCA0348EA73F6191882910B72613F8C4 |
| A5F2F6058F70CE5953DC475EE6AF1F97FC6D487ABEBAE76915075E3A53525B1D863102EDD50E |
| F1D0F45DBC3F4CA784D5D0D0DD8ADCD31AB5645BE00293FE6302CD0381F6527AC647A61CB08D |
| 0C9B448D9F5FBABE701131153411A1EA28F3701153F59760E01EC303334C35630E62D2CCDCE3 |

## Tor Links

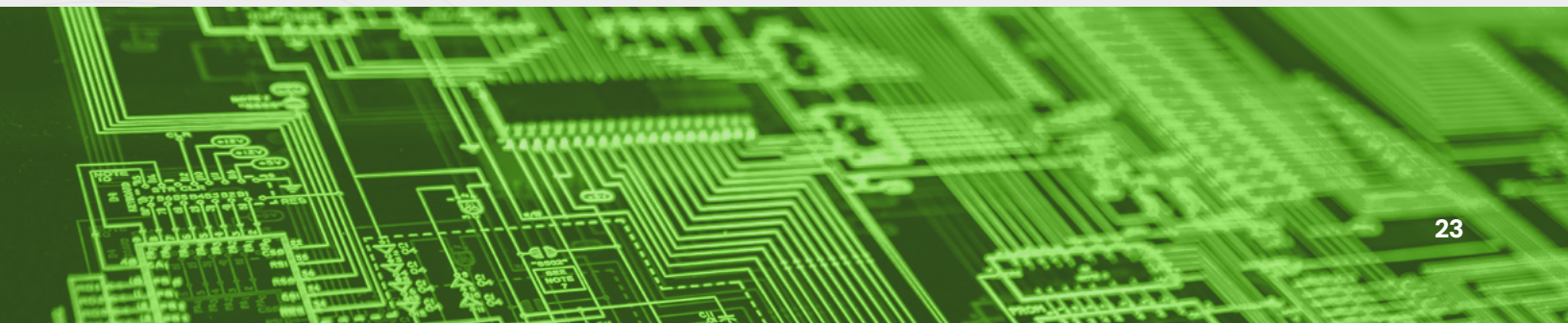
| |
|---|
| http://nonamef5njcxkghbjequlibwe5d3t3li5tmyqdyarnrsryopvku76wqd[.]onion |
| http://noname2j6zkgnt7ftxsjju5tfd3s45s4i3egq5bqtl72kgum4ldc6qyd[.]onion |
| http://7tkffbh3qiumpfjfq77plcorjmfohmbj6nwq5je6herbpya6kmgoafid[.]onion |

## 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.
- To prevent common credential theft methods like LSASS access, adhere to the credential hardening advice in our overview of on-premises credential theft.
- Maintain comprehensive backup and recovery procedures, which is crucial 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.



# Top Exploited Vulnerabilities

| Vulnerability Name | Description | References |
|---|---|---|
| Trimble SketchUp Viewer SKP File Parsing Memory Corruption Remote Code Execution Vulnerability<br>CVE-2024-9730 | Vulnerability allows remote attackers to execute arbitrary code on affected installations of Trimble SketchUp Viewer. The issue results from the lack of proper validation of user-supplied data, which can result in a memory corruption condition. | https://help.sketchup.com/en/release-notes/sketchup-202402 |
| IrfanView SID File Parsing Stack-based Buffer Overflow Remote Code Execution Vulnerability<br>CVE-2024-9261 | Vulnerability allows remote attackers to execute arbitrary code on affected installations of IrfanView. The issue results from the lack of proper validation of the length of user-supplied data prior to copying it to a stack-based buffer. | https://www.irfanview.info/test/iview64_test.zip |
| Tungsten Automation Power PDF JP2 File Parsing Out-Of-Bounds Read Remote Code Execution Vulnerability<br>CVE-2024-9755 | Vulnerability allows remote attackers to execute arbitrary code on affected installations of Tungsten Automation Power PDF. The specific flaw exists within the parsing of JP2 files. | https://esd.tungstenautomation.com/Registrations/ChooseLanguage |
| Wacom Center WTabletServicePro Link Following Local Privilege Escalation Vulnerability<br>CVE-2024-9766 | Vulnerability allows local attackers to escalate privileges on affected installations of Wacom Center. The specific flaw exists within WTabletServicePro process. By creating a symbolic link, an attacker can abuse the service to create a file. | https://www.wacom.com/en-gb/support/product-support/drivers?driver-search=571 |
| SonicWALL Connect Tunnel Link Following Local Privilege Escalation Vulnerability<br>CVE-2024-45316 | Vulnerability allows local attackers to escalate privileges on affected installations of SonicWALL Connect Tunnel. The specific flaw exists within the Secure Mobile Access service. | https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2024-0017 |
| NVIDIA Onyx Directory Traversal Remote Code Execution Vulnerability<br>CVE-2024-0113 | Vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of NVIDIA Onyx switches. When parsing the script query parameter, the process does not properly validate a user-supplied path prior to using it in file operations. | https://nvidia.custhelp.com/app/answers/detail/a_id/5563 |
| Adobe Dimension SKP File Parsing Use-After-Free Remote Code Execution Vulnerability<br>CVE-2024-45146 | Vulnerability allows remote attackers to execute arbitrary code on affected installations of Adobe Dimension. 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/dimension/apsb24-74.html |
| Adobe Substance 3D Stager SKP File Parsing Use-After-Free Remote Code Execution Vulnerability<br>CVE-2024-45138 | Vulnerability allows remote attackers to execute arbitrary code on affected installations of Adobe Substance 3D Stager. 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/substance3d_stager/apsb24-81.html |
| Microsoft Windows win32kfull Use-After-Free Local Privilege Escalation Vulnerability<br>CVE-2024-43556 | Vulnerability allows local attackers to escalate privileges on affected installations of Microsoft Windows. The specific flaw exists within the win32kfull driver. | https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-43556 |
| Ivanti Avalanche Faces ResourceManager Information Disclosure Vulnerability<br>CVE-2024-47011 | Vulnerability allows remote attackers to disclose sensitive information on affected installations of Ivanti Avalanche. The specific flaw exists within the Faces Mojarra component. The issue results from the use of a vulnerable third-party library. | https://forums.ivanti.com/s/article/Ivanti-Avalanche-6-4-5-Security-Advisory?language=en_US |
| Apple macOS AppleVADriver Out-Of-Bounds Write Remote Code Execution Vulnerability<br>CVE-2024-40841 | 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-us/121247 |
| Autodesk Navisworks Freedom DWF File Parsing Heap-based Buffer Overflow Remote Code Execution Vulnerability<br>CVE-2024-7674 | Vulnerability allows remote attackers to execute arbitrary code on affected installations of Autodesk Navisworks Freedom. 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.autodesk.com/trust/security-advisories/adsk-sa-2024-0015 |
| PaperCut NG pc-web-print Link Following Denial-of-Service Vulnerability<br>CVE-2024-8405 | Vulnerability allows local attackers to create a denial-of-service condition on affected installations of PaperCut NG. An attacker must first obtain the ability to execute low-privileged code on the target system to exploit this vulnerability. | https://www.papercut.com/kb/Main/Security-Bulletin-May-2024 |

| | | |
|---|---|---|
| Apple macOS ImageIO PSD File Parsing Heap-based Buffer Overflow Remote Code Execution Vulnerability<br>CVE-2024-40777 | Vulnerability allows remote attackers to execute arbitrary code on affected installations of Apple macOS. Interaction with the ImageIO library is required to exploit this vulnerability but attack vectors may vary depending on the implementation. | https://support.apple.com/en-us/120911 |
| Microsoft Windows Menu DC Path Use-After-Free Local Privilege Escalation Vulnerability<br>CVE-2024-38066 | Vulnerability allows local attackers to escalate privileges on affected installations of Microsoft Windows. The issue results from the lack of validating the existence of an object prior to performing operations on the object. | https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38066 |
| Lenovo Service Bridge Command Injection Remote Code Execution Vulnerability<br>CVE-2024-4696 | Vulnerability allows remote attackers to execute arbitrary code on affected installations of Lenovo Service Bridge. The specific flaw exists within the LscShim module. When parsing a crafted URL, the process does not properly validate a user-supplied string before using it to execute a system call. | https://support.lenovo.com/ca/en/product_security/ps500631-lenovo-service-bridge-vulnerability |
| Foxit PDF Reader Annotation Use-After-Free Remote Code Execution Vulnerability<br>CVE-2024-9254 | Vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit PDF Reader. The issue results from the lack of validating the existence of an object prior to performing operations on the object. | https://www.foxit.com/support/security-bulletins.html |
| Western Digital MyCloud PR4100 ddns-start Heap-based Buffer Overflow Remote Code Execution Vulnerability<br>CVE-2024-22170 | Vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of Western Digital MyCloud PR4100. 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.westerndigital.com/support/product-security/wdc-24005-western-digital-my-cloud-os-5-firmware-5-29-102 |
| Microsoft Windows BeginPaint Brush Use-After-Free Local Privilege Escalation Vulnerability<br>CVE-2024-38249 | Vulnerability allows local attackers to escalate privileges on affected installations of Microsoft Windows. The issue results from the lack of validating the existence of an object prior to performing operations on the object. | https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38249 |
| TeamViewer Missing Authentication Local Privilege Escalation Vulnerability<br>CVE-2024-7481 | Vulnerability allows local attackers to escalate privileges on affected installations of TeamViewer. The specific flaw exists within the TeamViewer service, which listens on TCP port 5939 by default. | https://www.teamviewer.com/en/resources/trust-center/security-bulletins/tv-2024-1006/ |
| (0Day) FastStone Image Viewer GIF File Parsing Out-Of-Bounds Write Remote Code Execution Vulnerability<br>CVE-2024-9114 | Vulnerability allows remote attackers to execute arbitrary code on affected installations of FastStone Image Viewer. The issue results from the lack of proper validation of user-supplied data, which can result in a write past the end of an allocated buffer. | https://www.cve.org/CVERecord?id=CVE-2024-9114 |
| PDF-XChange Editor Doc Object Out-Of-Bounds Read Remote Code Execution Vulnerability<br>CVE-2024-8847 | Vulnerability allows remote attackers to execute arbitrary code on affected installations of PDF-XChange Editor. The specific flaw exists within the handling of Doc objects. | https://www.pdf-xchange.com/index.php/support/security-bulletins.html |
| WinZip Mark-of-the-Web Bypass Vulnerability<br>CVE-2024-8811 | Vulnerability allows remote attackers to bypass the Mark-of-the-Web protection mechanism on affected installations of WinZip. When opening an archive that bears the Mark-of-the-Web, WinZip removes the Mark-of-the-Web from the archive file. | https://notcve.org/view.php?id=CVE-2024-8811 |
| Cohesive Networks VNS3 Command Injection Remote Code Execution Vulnerability<br>CVE-2024-8806 | Vulnerability allows remote attackers to execute arbitrary code on affected installations of Cohesive Networks VNS3. The specific flaw exists within the web service, which listens on TCP port 8000 by default. | https://cohesive.net/support/security-responses/ |

# Security Bulletin

**Growing Use of File Hosting Services for Business Email Compromise:** Microsoft is warning of cyberattack campaigns that abuse legitimate file hosting services such as SharePoint, OneDrive, and Dropbox. This is widely used in enterprise environments as a defense evasion tactic. The end goals of the campaigns are broad and varied, allowing threat actors to compromise identities and devices and conduct business email compromise (BEC) attacks, which ultimately result in financial fraud, data exfiltration, and lateral movement to other endpoints. While these campaigns are generic and opportunistic in nature, they involve sophisticated techniques to perform social engineering, evade detection, and expand threat actor reach to other accounts and tenants," the Microsoft Threat Intelligence team said.

**156% Increase in OSS Malicious Packages:** More than 704,102 malicious packages have been identified since 2019, and 512,847 of these have been discovered since November 2023. This year has been record-breaking year for open-source consumption, according to Sonatype, reaching an estimated 6.6 trillion downloads.

- **(npm)** a package manager for the JavaScript programming language accounted for a staggering 4.5 trillion requests in 2024, representing 70% year-over-year growth in requests.
- **(PyPI)**, package manager for Python driven by AI and cloud adoption, is estimated to reach 530 billion package requests by the end of 2024, up 87% year-over-year, according to Sonatype's findings.

**Facebook Restricted to User Personal Data for Targeted Ads in EU:** Europe's top court has ruled that Meta Platforms must restrict the use of personal data harvested from Facebook for serving targeted ads even when users consent to their information being used for advertising purposes, a move that could have serious consequences for ad-driven companies operating in the region. It's worth noting that Article 5(1)(c) of GDPR necessitates that companies limit the processing to strictly necessary data, preventing the collected personal data about an individual—whether gathered on or outside the platform via third parties—from being aggregated, analyzed, and processed for targeted advertising without time-bound restrictions.

**RSA Encryption Broken by Chinese Researchers Using Quantum Computing:** A team of researchers from China has broken RSA encryption using quantum computing technology. Utilizing D-Wave's advanced quantum annealing systems, this innovative research raises pressing concerns about the security of widely adopted cryptographic methods.

- **Integer Factorization:** By restructuring cryptographic problems, the researchers were able to leverage the D-Wave Advantage system to effectively factor 2,269,753. This is a significant milestone in demonstrating the potential of quantum computing in tackling complex cryptographic challenges.
- **CVP Optimization:** The optimization of the CVP using quantum annealing not only enhances efficiency but also represents a groundbreaking moment in the quest for cracking RSA integers. The team's success in factorizing a 50-bit integer showcases the promise of D-Wave's technology in real-world applications.

# Reference Links


1. https://www.welivesecurity.com/en/eset-research/separating-bee-panda-ceranakeeper-making-beeline-thailand/
2. https://www.darkreading.com/vulnerabilities-threats/hybrid-work-vulnerabilities-print-security?&web_view=true
3. https://therecord.media/ransomware-healthcare-microsoft-last-year?&web_view=true
4. https://www.cybersecuritydive.com/news/global-cisos-want-split-roles-regulatory/729871/?&web_view=true
5. https://www.infosecurity-magazine.com/news/240-million-us-breach-victims-q3/?&web_view=true
6. https://www.infosecurity-magazine.com/news/156-increase-in-oss-malicious/?&web_view=true
7. Crimson Palace returns: New Tools, Tactics, and Targets – Sophos News
8. Chinese 'Crimson Palace' espionage campaign keeps hacking Southeast Asian governments
9. https://www.welivesecurity.com/en/eset-research/cosmicbeetle-steps-up-probation-period-ransomhub/?&web_view=true
10. https://therecord.media/cosmicbeetle-ransomware-group
11. https://thehackernews.com/2024/09/cosmicbeetle-deploys-custom-scransom.html
12. https://thecyberexpress.com/quantum-computing-breaks-rsa-encryption/?&web_view=true
13. https://thehackernews.com/2024/10/eu-court-limits-metas-use-of-personal.html?&web_view=true
14. https://www.infosecurity-magazine.com/news/156-increase-in-oss-malicious/?&web_view=true
15. https://thehackernews.com/2024/10/microsoft-detects-growing-use-of-file.html?&web_view=true


## About SDG

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

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


SDG

75 North Water Street, Norwalk, CT 06854

203.866.8886

sdgc.com