



DECEMBER 2024

# Cyber Threat Advisory

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

[sdgc.com](https://sdgc.com)

# Table of Contents

---

Key Cybersecurity Trends	3
Focus of the Month: Data Breaches	4
Monthly Highlights	5
Ransomware Tracker	13
Articles	
IcePeony: Emerging China-Nexus APT Group Targeting Asian Nations	11
Unmasking Tenacious Pungsan: Malicious npm Packages and DPRK's Contagious Interview Campaign	15
Breaking Down Earth Estries' Persistent TTPs in Prolonged Cyber Operations	18
China-Aligned MirrorFace Hackers Target EU Diplomats with World Expo 2025 Bait	24
Top Exploited Vulnerabilities	26
Security Bulletin	28
Reference Links	Back Page

---

# Key Cybersecurity Trends

## CXO Summary

### Identity Data Breaches Cost More Than Average Incidents

40% of respondents reported an identity-related security breach. Of those, 66% reported it as a severe event that affected their organization. 44% estimated that the total costs of identity-related data breaches exceeded the cost of a typical data breach.

### AI Key Assets in Future Cybersecurity Measures

80% of security community felt that AI will do more to empower cybersecurity than abet cybercriminals over the next five years, with nearly as many organizations (79%) planning to implement some AI in their cybersecurity stack within the next year.



Entertainment, finance, and retail were the likeliest sectors to implement some form of AI in the next year.

Highly regulated industries are among the most likely to have plans to implement AI in their cybersecurity stacks.

### Inculcating Security in Work Culture Is More of an Art Than Science

Simply disbursing guidelines to the employees won't bring the desired cultural shift. The focus has to be more on changing the mindset of the employees. While a change is highly appreciable, it is just a stepping stone to what is actually required. Given the present state of cyberspace, organizations can no longer afford for their departments to work in silos when it comes to cybersecurity. A cultural shift from the bottom to the top of the organizational pyramid is required, covering every nook and corner of all echelons wherein every individual employee of the organization maintains an optimum cyber hygiene

---

Given the **present state of cyberspace**, organizations can no longer afford for their departments **to work in silos** when it comes to cybersecurity.

---

**CRITICAL THREAT ALERT**

# Focus of the Month: Data Breaches

Data breaches are a growing danger, with incidents escalating in both number and severity. To safeguard critical data, we must understand the current landscape of cyber threats.

## Average Data Breach Jumps to \$4.88 Million

- Breach costs increased 10% from the prior year, the largest yearly jump since the pandemic, as 70% of breached organizations reported that the breach caused significant or very significant disruption.
- 40% of breaches involved data stored across multiple environments including public cloud, private cloud, and on-prem. These breaches cost more than \$5 million on average and took the longest to identify and contain (283 days).
- 42% of breaches were detected by an organization's own security team or tools compared to 33% the prior year.

## 47% of Corporate Data on Cloud Is Sensitive

- 44% of organizations have experienced a cloud data breach with 14% reporting an incident in the last 12 months.
- Human error and misconfiguration continued to be the top root cause of these breaches (31%), followed by exploiting known vulnerabilities (28%), and failure to use multi-factor authentication (17%).

## 94% Outages Due to Ransomware

- Within the last 12 months, 48% of organizations identified evidence of a successful breach within their environment.

- 66% of organizations that suffered a data breach in the last year chose to publicly disclose information regarding the incidents, while 30% only disclosed their breaches to impacted parties.

## One Third of Breaches Go Undetected

- As hybrid cloud environments grow in complexity and bad actors launch a barrage of unseen attacks, 65% of respondents believe that their existing solutions cannot effectively detect breaches.
- 31% of organizations only detected a recent breach when they received an extortion threat from the adversary.

## 98% of Breaches Linked to Third-Party Breaches

- Healthcare and financial services emerged as the sectors most heavily impacted by third-party breaches, with healthcare accounting for 35% of total breaches and financial services accounting for 16%.
- 75% of external business-to-business (B2B) relationships that enabled third-party breaches involved software or other technology products and services.
- The three most widely exploited vulnerabilities (MOVEit, CitrixBleed, and Proself) were involved in 77% of all third-party breaches involving a specified vulnerability.



## Monthly Highlights

### Cybercriminals Exploit Weekend Lull to Launch Ransomware Attacks

**Ransomware groups are increasingly exploiting weekends and holidays to launch attacks, taking advantage of reduced cybersecurity staffing during these times, according to Semperis' latest report.**


The 2024 **Ransomware Holiday Risk Report**, released on November 20, 2024, revealed that 86% of respondents who experienced ransomware attacks were targeted on weekends or holidays when staff availability is lower. Despite 96% of surveyed organizations maintaining 24/7 Security Operations Centres (SOCs), 85% reported reducing SOC staffing by up to 50% during these periods.

Dan Lattimer, Area VP EMEA West at Semperis, explained to Infosecurity that maintaining a fully staffed SOC is costly. "You might only have three or four people working, which isn't sufficient for true 24/7 coverage. Without adequate resources or budget, continuous monitoring is impossible," he said.

Some organizations scale back monitoring during weekends due to perceived lower risks, such as fewer employees being online. Others may assume they are unlikely targets because they haven't been attacked previously. However, ransomware gangs are aware of these vulnerabilities and capitalize on them. "If I'm trying to maximize my chances of being paid, I'll attack when defences are weakest—like weekends or holidays," Lattimer noted.

This lack of vigilance allows attackers more time to navigate networks undetected, encrypt files, and steal sensitive data. The report highlighted that 78% of finance sector respondents and 75% from manufacturing and utilities confirmed ransomware incidents during weekends or holidays.

Another trend from the report showed 63% of participants experienced ransomware attacks



Some organizations scale back monitoring during weekends due to perceived lower risks, such as fewer employees being online.

following major corporate events, such as mergers, acquisitions, or workforce restructuring.

Alarmingly, many organizations may overestimate their readiness against identity-related threats. While 81% of respondents felt confident in their expertise to defend against identity attacks, 83% reported falling victim to ransomware in the last year. Semperis, which specializes in Active Directory (AD) security, revealed that 40% of organizations lack—or are uncertain about having—adequate budgets to protect core identity systems like AD. This shortfall leaves significant gaps in Identity Threat Detection and Response (ITDR) strategies.

The report, based on a global study of 900 IT and security leaders from the US, UK, France, and Germany, underscores the critical need for better defenses and investments in identity security and 24/7 threat monitoring.

## Identity-Related Data Breaches Cost More Than Average Incidents

**Identity-related data breaches are more costly and severe compared to standard incidents, according to a report by RSA. Among the respondents, 40% reported experiencing an identity-related security breach, with 66% classifying it as a severe event impacting their organization. Additionally, 44% estimated that the costs of these breaches exceeded those of typical data breaches. These findings highlight the importance of investing in advanced security measures to mitigate the financial and operational impacts of identity-related breaches.**

Looking ahead, 80% of respondents believe artificial intelligence (AI) will play a more significant role in strengthening cybersecurity than aiding cybercriminals over the next five years. Nearly 79% of organizations plan to integrate AI into their cybersecurity frameworks within the next year, with entertainment, finance, and retail sectors leading the charge. Highly regulated industries also rank among the top adopters of AI in cybersecurity strategies.

However, there is skepticism surrounding passwordless technologies in enterprise settings due to unclear definitions of “passkeys” and concerns about their suitability for professional use.

Password management remains a pain point for many employees, with 51% needing to input their passwords six or more times daily. This friction, coupled with the high cost of identity breaches, is driving 61% of organizations to explore passwordless authentication within the next year

to bolster security against phishing and similar attacks. However, there is skepticism surrounding passwordless technologies in enterprise settings due to unclear definitions of “passkeys” and concerns about their suitability for professional use.

The report also revealed differing attitudes toward installing corporate security software on personal devices. While 73% of Identity and Access Management (IAM) professionals and 60% of cybersecurity specialists were open to such measures, only 39% of generalists shared this sentiment.

Hybrid environments, which combine on-premises and cloud applications, are now the norm, with 70% of organizations operating in such setups. This trend underscores the need for security solutions that seamlessly span diverse environments.

Sector-specific insights showed that agriculture and aerospace organizations face the highest costs from identity-related breaches, with 50% and 43% of respondents, respectively, reporting damages exceeding \$10 million. The United States had the largest share of breaches surpassing \$10 million and reported the highest severity levels globally.

These findings emphasize the urgency for organizations to enhance identity security, adopt AI-driven cybersecurity tools, and address vulnerabilities in authentication strategies to better safeguard their systems and data.

## Enterprise Executives Cite AI-Assisted Attacks as Top Emerging Risk, Gartner Finds

**A recent survey by Gartner highlights growing concerns about potential scenarios where artificial intelligence (AI) could play a significant role in cyberattacks. Although these risks remain largely theoretical, the anxiety around them is mounting.**

### Key Findings

- **AI-Enhanced Attacks as Top Risk:** AI-assisted malicious attacks were identified as the leading emerging business risk during the first three quarters of the year. Four out of five executives surveyed in Q3 ranked it as their top concern.
- **Broader Risk Landscape:** Other prominent risks include AI-driven misinformation, increasing political polarization, globally consequential events, and mismatches in organizational talent profiles.

The survey, based on responses from 286 senior risk and assurance executives, focuses on speculative risks—scenarios that have not yet materialized but could have a significant impact in the future.

### AI in Cyberattacks: Speculation vs. Reality

Despite widespread speculation, there is no concrete evidence of AI-engineered cyberattack campaigns. “I don’t see any evidence of it yet,” said Charles Carmakal, CTO of Mandiant Consulting, during the RSA Conference earlier this year. However, he acknowledged the likelihood of such attacks in the future.

Mandiant’s Chief Analyst, John Hultquist, identified that the main concern is attackers potentially leveraging AI for social engineering and overcoming language barriers, which could make phishing and other tactics more effective.

For now, security leaders at major firms like Google Cloud are optimistic that AI will offer defenders an edge over attackers.

For now, security leaders at major firms like Google Cloud are optimistic that AI will offer defenders an edge over attackers.

### New Risks Emerge

Gartner’s report also highlighted AI-driven misinformation and escalating political polarization as emerging risks. These reflect growing concerns about global elections and their potential impacts on enterprises.

“Organizations struggle to assess the risk implications of various scenarios surrounding the upcoming U.S. election,” said Zachary Ginsburg, senior director of research at Gartner’s Risk and Audit Practice.

### Implications for Enterprises

While AI has not yet been weaponized in significant ways by threat actors, organizations are increasingly bracing for potential risks tied to its misuse. These findings emphasize the importance of proactive risk management and strategic planning to address emerging threats in the evolving technological and geopolitical landscape.

## T-Mobile Breached in Major Chinese Cyberattack on Telecoms

**T-Mobile has been breached in a large-scale cyber espionage campaign attributed to Salt Typhoon, a Chinese state-sponsored hacking group. The attack targeted major U.S. telecommunications providers, including AT&T, Verizon, and Lumen Technologies, as well as international telecom firms.**

### Key Details of the Breach:

- Hackers infiltrated critical telecom systems used for law enforcement surveillance, compromising sensitive communications.
- Salt Typhoon exploited vulnerabilities in telecom infrastructure, such as Cisco Systems routers, to access call records, unencrypted messages, and audio communications of targeted individuals.
- The campaign is believed to have lasted at least eight months, leveraging advanced artificial intelligence to enhance intelligence-gathering efforts.

The national security risks are profound.

T-Mobile has stated that no significant impacts on its systems or customer data have been identified. However, federal agencies and security experts remain concerned about the breach's potential severity. Paul Bischoff, consumer privacy advocate at Comparitech, noted, "We won't know the full impact until T-Mobile discloses what information was stolen. Metadata like call times is worrisome, but theft of texts and audio messages would be far more alarming."

The breach raises additional concerns due to T-Mobile's history of cybersecurity challenges. Just last month, the company settled for \$31.5 million over multiple data breaches spanning three years.

### National Security Concerns:

Victims reportedly include U.S. government officials involved in national security and policymaking, amplifying fears of counterintelligence risks. Investigators have uncovered:

- Access to telecom systems used for wiretap surveillance.
- Compromised call logs and private communications of high-ranking officials.
- Potential mapping of critical infrastructure for future attacks.

Tom Kellermann, SVP of cyber strategy at Contrast Security, warned of the broader implications: "The Chinese hacker will use T-Mobile to island-hop into government agencies and critical infrastructures. The national security risks are profound. This is the third telecom provider compromised by Chinese hackers in the past year."

### Broader Implications and Response:

The breach underscores significant vulnerabilities across the telecommunications sector, classified as critical infrastructure under U.S. federal law. The Biden administration has described the attack as "broad and significant," while federal agencies like the FBI and CISA continue their investigations.

Telecom companies are now ramping up security measures. T-Mobile is reportedly working to implement a zero-trust architecture and phishing-resistant authentication to bolster its defenses. The breach highlights the urgent need for strengthened cybersecurity protocols across the telecommunications industry to safeguard against future state-sponsored attacks.



## 81% of Bank CEOs Identify Cybersecurity, Talent Shortage as Key Growth Challenges for the Sector

**As banks worldwide increasingly prioritize investments in emerging technologies, 81% of Chief Executive Officers (CEOs) in the banking sector identify cybercrime and cybersecurity as critical threats likely to impede organizational growth over the next three years. This finding comes from the latest Banking CEO Report by KPMG in India.**

The rapid evolution of technology, particularly artificial intelligence (AI), has heightened associated risks. While only 43% of CEOs express confidence in their organization's cybersecurity measures keeping pace with AI advancements, 72% are boosting investments in cybersecurity to mitigate AI-related risks.

The survey also reveals that 81% of CEOs view generative AI (Gen AI) as a top investment priority. However, only 53% feel adequately prepared to address cybersecurity challenges, a slight dip from 54% in 2023. Encouragingly, the proportion of those feeling unprepared has dropped significantly—from 21% last year to just 3% now. Meanwhile, 44% of leaders describe their readiness as neutral, up from 23% in the previous year.

Very soon, your ability to work faster and meet evolving client expectations will be critical. Addressing technology challenges and building the necessary capabilities must start now," emphasized Francisco Uría, Global Head of Banking and Capital Markets at KPMG International. He also stressed the importance of investing in data governance, workforce skills, and internal exploration channels to stay competitive.

The report, based on interviews with 120 banking leaders worldwide, found that 76% believe experimentation is essential for unlocking Gen AI's potential, actively encouraging employee participation. Additionally, 66% of organizations are equipping employees with upskilling programs to harness Gen AI benefits effectively.

While 66% of banking CEOs remain optimistic about the growth prospects of the banking and capital markets industry over the next three years, talent management continues to be a pressing concern. The sector is striving to attract and retain professionals with the skills necessary for technology-driven transformation, amid geopolitical and macroeconomic uncertainties.

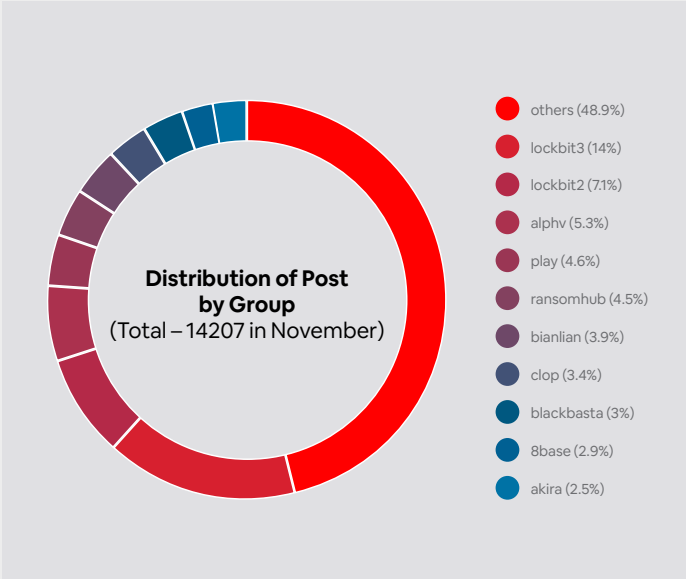
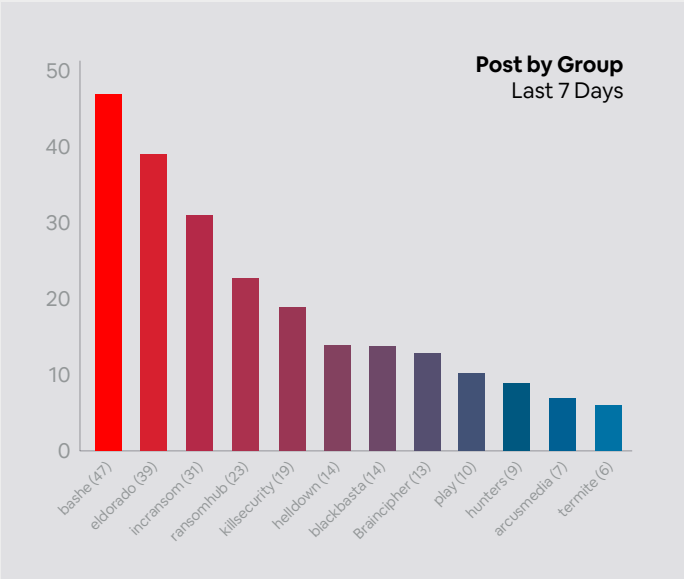
The skills gap across critical areas is evident. Banks now find themselves competing for new capabilities in a challenging global and domestic marketplace," noted Hemant Jhahhria, Partner and Head of Consulting at KPMG in India.

Interestingly, there has been a sharp decline in preference for hybrid work models, with only 10% of leaders favoring this arrangement compared to 34% in 2023. A significant 86% expect employees in traditional office roles to return to in-office work within the next three years, and 92% are likely to reward employees who work on-site with favorable assignments or promotions.

Uría highlighted the changing workforce dynamics, noting that next-generation talent prioritizes personal mobility, flexibility, and supportive workplace cultures. The survey identified knowledge transfer, increasing retirements, and a growing skills gap between older and younger employees as major labor market concerns.

The report also underscored the growing significance of environmental, social, and governance (ESG) factors. CEOs view ESG as vital for driving growth, with 58% expecting significant returns on ESG investments within three to five years.

# Ransomware Tracker

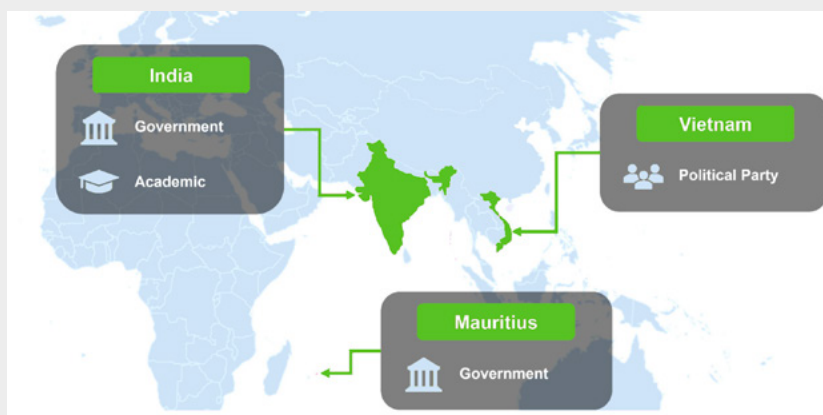


## Articles

### IcePeony: Emerging China–Nexus APT Group Targeting Asian Nations

#### Executive Summary

- **Discovery:** IcePeony is a previously unknown APT group linked to China, active since at least 2023.
- **Targets:** Focused on government agencies, academic institutions, and political organizations in India, Vietnam, and Mauritius.
- **Attack Vector:** SQL injection as an initial compromise method, followed by deployment of custom malware, including IceCache and IceEvent.
- **Unique Tools:** Utilizes tools like StaX (a custom variant of Stowaway), ProxyChains, and rootkits like Diamorphine.
- **Attribution:** Likely operates under China's national interests, potentially tied to their maritime strategy.



#### Key Findings

- Over 200 SQL injection attempts on Indian government websites recorded.
- IcePeony utilizes custom malware, IceCache and IceEvent, to establish persistence and exfiltrate data.
- Operational oversight exposed attacker resources, revealing details about tools, tactics, and work conditions.
- Indicators suggest attackers work under a strict “996 working hour system” (9 AM–9 PM, six days a week).

#### Intrusion Tactics and Timeline

##### Attack Flow:

1. **Initial Compromise:** Exploits SQL vulnerabilities on publicly accessible web servers.
2. **Payload Deployment:** Installs web shells or IceCache malware upon successful exploitation.
3. **Credential Theft:** Primary goal is to steal sensitive credentials for further exploitation.

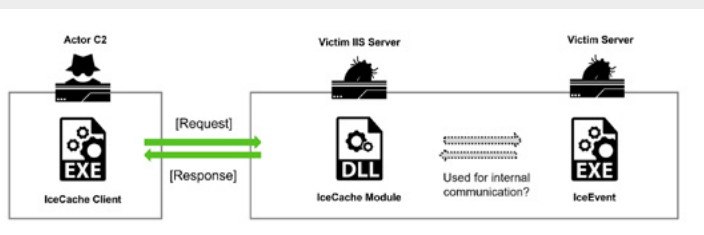
## 14-Day Operational Timeline:

- **Day 1:** SQL injection attacks government websites; successful exploits lead to IceCache installation.
- **Day 4:** Configures proxy rules using IceCache.
- **Day 6:** Uses advanced tools like StaX and Diamorphine.
- **Day 11:** Leverages craXcel to unlock password-protected Microsoft Office files.
- **Day 12–14:** Explores further hosts and exfiltrates information.

## Tools and Malware

### 1. IceCache:

- Customized malware based on reGeorge for IIS servers.
- Features SOCKS proxy functions, command execution, and file transfer capabilities.



### 2. IceEvent:

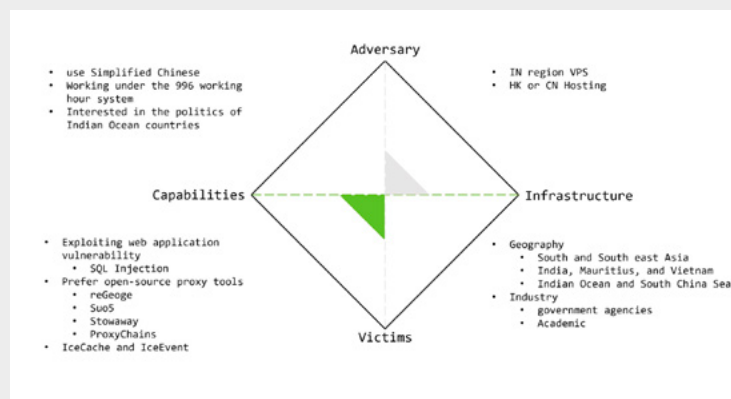
- Passive backdoor used for establishing persistence.
- Shares similarities with IceCache, including XOR-based data encoding.

### 3. StaX:

- Modified proxy tool based on Stowaway.
- Adds encryption (Custom Base64 and AES) for secure communication.

## 4. Other Tools:

- ProxyChains for script execution.
- Diamorphine rootkit for stealth operations.



## Detection

### Indicators of Compromise (IOCs):

- SQL injection attempts targeting public-facing servers.
- Presence of IceCache modules with commands like EXEC, SOCKS\_CONNECT, and FILE\_UPLOAD.
- Traces of Diamorphine and StaX in compromised environments.

### Artifacts:

- Files with PDB paths revealing development environments:
- C:\Users\power\documents\visual studio 2017\Projects\cachsess

### Command Usage:

- Insights from zsh\_history logs exposing attacker workflows.



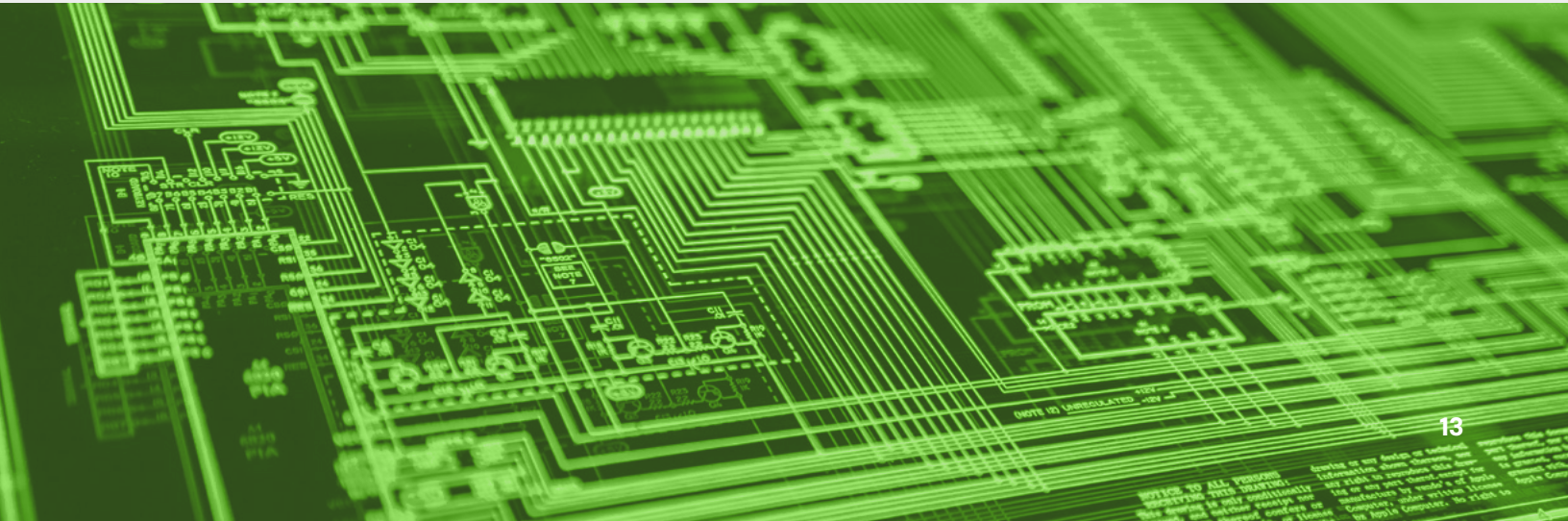
Indicators of Compromise

IP
165[.]22.211.62
64[.]227.133.248
173[.]208.156.19
173[.]208.156.144
154[.]213.17.225
103[.]150.186.219
63[.]141.255.16
204[.]12.205.10
107[.]148.37.63
103[.]99.60.119
154[.]213.17.237
45[.]195.205.88
154[.]213.17.244
103[.]99.60.93
149[.]115.231.17
149[.]115.231.39
103[.]99.60.108

Domain
d45qomwkl[.]online
k9ccin[.]com
k8ccyn[.]com
88k8cc[.]com
googlesvn[.]com

IceCache
484e274077ab6f9354bf71164a8edee4dc4672fcfbf05355958785824fe0468f
5b16d1533754c9e625340c4fc2c1f76b11f37eb801166ccfb96d2aa02875a811
ceb47274f4b6293df8904c917f423c2f071f31416b79f3b42b6d64e65dcfe1b
e5f520d95cbad6ac38eb6badbe0ad225f133e0e410af4e6df5a36b06813e451b
d1955169cd8195ecedfb85a3234e4e6b191f596e493904ebca5f44e176f3f950
11e90e2458a97957064a3d3f508fa6dadae19f632b45ff9523b7def50ebacb63
de8f58f008ddaa60b5cflb729ca03f276d2267e0a80b584f2f0723e0fac9f76c
b8d030ed55bfb6bc4fdc9fe34349ef502561519a79166344194052f165d69681
535586af127e85c5561199a9ala3254d554a6cb97200ee139c5ce23e68a932bd
0b8b10a2ff68cb2aa3451eedac4a8af4bd147ef9ddc6eb84fc5b01a65fca68fd
5fd5e99fc503831b71f4072a335f662d1188d7bc8ca2340706344fb974c7fe46
3eb56218a80582a79f8f4959b8360ada1b5e471d723812423e9d68354b6e008c
a66627cc13f827064b7fcea643ab31b34a7cea444d85acc4e146d9f2b2851cf6
0eb60e4c5dc7b06b719e9dbd880eb5b7514272dc0d1e4760354f8bb44841f77

IceEvent
80e831180237b819e14c36e4af70304bc66744d26726310e3c0dd95f1740ee58
9a0b0439e6fd2403f764acf0527f2365a4b9a98e9643cd5d03cccc3825a732e
9aba997bbf2f38f68ad8cc3474ef68eedd0b99e8f7ce39045fld770e2af24fea
bc94da1a066cbb9bdee7a03145609d0f9202b426a52aca19cc8d145b4175603b



## Prevention

### Web Application Security:

- Regularly patch and monitor public-facing servers for vulnerabilities.
- Employ Web Application Firewalls (WAFs) to block SQL injection attempts.

### Credential Security:

- Implement multi-factor authentication (MFA).
- Regularly rotate administrative credentials.

### Endpoint Hardening:

- Restrict execution of unauthorized scripts and tools.
- Monitor for installation of IIS-based malware.

## Remediation

### Incident Response:

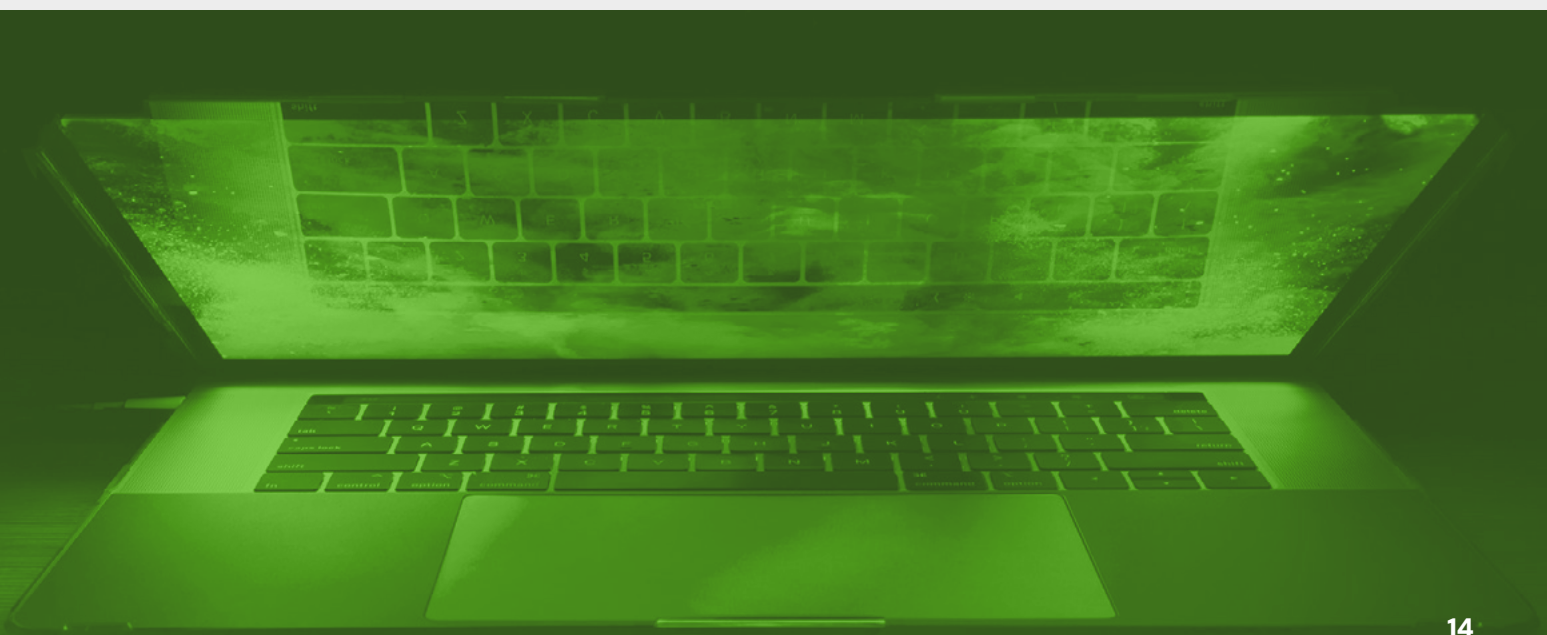
- Isolate affected systems and analyze for IceCache and IceEvent.
- Remove web shells, backdoors, and unauthorized user accounts.

### Forensic Analysis:

- Leverage zsh\_history or similar command history files for attacker timeline reconstruction.

### Future Readiness:

- Conduct regular penetration tests to identify vulnerabilities.
- Enhance detection capabilities for known IcePeony tools and tactics.



## Unmasking Tenacious Pungsan: Malicious npm Packages and DPRK's Contagious Interview Campaign

### Executive Summary

- **Discovery:** In September 2024, three malicious npm packages — passports-js, bcrypts-js, and blockscan-api — were identified by security researchers.
- **Downloads:** These packages were downloaded 323 times before removal.
- **Associated Malware:** All three packages contained BeaverTail, a JavaScript-based infostealer and downloader malware linked to DPRK (North Korea).
- **Campaign Linkage:** These malicious packages are connected to the Contagious Interview campaign targeting job-seekers in the US tech and blockchain industries.
- **Threat Actor:** Activity is attributed to a North Korean threat actor, referred to as Tenacious Pungsan, employing name squatting tactics to compromise npm users.

### Key Findings

#### 1. Malicious Packages Identified:

- passports-js – Mimics the legitimate passport package.
- bcrypts-js – Name squats the legitimate bcryptjs library.
- blockscan-api – A backdoored copy of the etherscan-api.

#### 2. Attack Tactics:

- Use of name squatting to deceive developers into downloading malicious packages.
- Incorporation of obfuscated JavaScript to conceal malware within the packages.

#### 3. Malware Characteristics:

- **BeaverTail Malware:** Steals cryptocurrency wallet data, browser caches, and Login Keychain credentials.
- **Second Stage:** Downloads and runs a Python backdoor named InvisibleFerret from command-and-control (C2) servers.

#### 4. Campaign Links:

- Shared infrastructure and techniques with previously reported Contagious Interview campaigns.
- Targeting blockchain developers and Node.js developers through npm repositories.

## Background

The open-source software ecosystem has become a frequent target for supply chain attacks. Malicious actors exploit platforms like npm to publish counterfeit packages, often resembling legitimate ones. Name squatting remains a prominent tactic, misleading developers into installing compromised packages.

Security researchers continue to monitor npm and PyPI repositories for malicious activity, employing tools like GuardDog to detect suspicious code and behaviors.

## Technical Analysis

### 1. Discovery and Analysis:

- GuardDog Detection: Flagged passports-js on September 11, 2024, revealing

obfuscated JavaScript embedded in the package.

- Similar obfuscated code was later identified in bencrypts-js and blockscan-api, all linked to BeaverTail malware.

### 2. Campaign Infrastructure:

- All identified malware communicated with a C2 server at 95.164.17[.]24 on port 1224.
- Consistent directory structure (/uploads, /pdown, /client/<ID>) reused across campaigns.

### 3. BeaverTail Capabilities:

- Exfiltrates sensitive data from cryptocurrency wallets, browser extensions, and macOS Keychain.
- Employs campaign-specific IDs to differentiate targeted victim groups.

## Detection

- **Obfuscated Code Patterns:** Tools like GuardDog can detect unusual obfuscation in package source files.
- **C2 Communication:** Monitor outbound traffic to known malicious IPs (95.164.17[.]24) and ports (1224).
- **Behavioral Analysis:** Look for signs of credential theft, browser data exfiltration, and second-stage payload deployment.





## Indicators of Compromise

Package	Purpose
passports-js-v0.7.0.zip	Initial payload
passports-js-v0.7.1.zip	Initial payload
bcrypts-js-v2.4.4.zip	Initial payload
blockscan-api-v1.3.1.zip	Initial payload

IP addresses	Purpose	Note
95.164.17[.]24	Data exfiltration, InvisibleFerret download	Reused from previous campaign documented by Unit42

NPM authors	Email	Packages published
superdev727	austin27ahn@outlook.com	passports-js, bcrypts-js
intelliman	g65492036@gmail.com	blockscan-api

## Prevention

- **Dependency Verification:** Always cross-check the legitimacy of npm packages before installing.
- **Security Tools:** Use static and dynamic analysis tools to scan dependencies for malicious behaviors.
- **Educate Developers:** Provide training to recognize name squatting attacks and supply chain threats.

## Remediation

### Immediate Actions:

- Remove compromised packages (passports-js, bcrypts-js, and blockscan-api) from affected systems.
- Revoke any credentials potentially exposed during the infection period.

### Network Hardening:

- Block traffic to known malicious IPs and domains linked to the campaign.
- Regularly update firewall and intrusion detection system (IDS) rules.

### Long-Term Measures:

- Conduct a comprehensive review of your software supply chain security.
- Use tools like GuardDog for continuous monitoring of package repositories.

## Breaking Down Earth Estries' Persistent TTPs in Prolonged Cyber Operations

Breaking Down Earth Estries' Persistent TTPs in Prolonged Cyber Operations describes the advanced strategies employed by the cyber group Earth Estries during their extended campaigns.

They employ two main attack chains: one that uses CAB files to leverage PsExec and tools like Hemigate, Crowdoor, and Trillclient, and another that uses cURL downloads to deliver malware like SnappyBee and Zingdoor. Both chains take advantage of flaws in network management software and Microsoft Exchange servers.

Earth Estries uses lateral movement, backdoors, and ongoing tool updates to stay persistent. They use proxies to hide their activities while exfiltrating data using Trillclient and cURL. They frequently send stolen data to anonymized file-sharing services.

### Detection:

Earth Estries employs several Cobalt Strike installations with Crowdoor backdoors, which are distributed via CAB file packages, as well as an installation of QConvergeConsole, a web-based management tool for setting up and overseeing QLogic Fibre Channel Adapters, as one of its entry methods in the first attack scenario. Although the backdoors themselves are also utilized for lateral movement, PSEXec is heavily used in the early phases of the attacks.

To increase its network presence, Earth Estries still uses Trillclient to steal user credentials from browser caches. Since the threat actor specifically downloaded documents from the target's internal web-based document management system using wget, they also demonstrated a deep understanding of the target's environment and methodology.

### Initial access

The group has been seen exploiting QConvergeConsole installations on target servers that are either weak or improperly configured to obtain access to their system. Cobalt Strike can be installed on a

target computer, and network discovery can be carried out by the installed remote application agent (c:\program files\qlogic corporation\nqagent\netqlremote.exe).

#### Commands

```
C:\Windows\system32\cmd.exe /C net group "domain admins" /domain

C:\Windows\system32\cmd.exe /C copy C:\users\public\music\go4.cab \\
{HostName}\c$\programdata\microsoft\drm

C:\Windows\system32\cmd.exe /C expand -f:* \\
{HostName}\c$\programdata\microsoft\drm\go4.cab \\
{HostName}\c$\programdata\microsoft\drm

C:\Windows\system32\cmd.exe /C c:\users\public\music\PSEXec.exe -accepteula
\\172.16.xx.xx "c:\ProgramData\Microsoft\DRM\g2.bat"
```

Secondly, they exploited a flaw in Apache Tomcat6 that was included with QConvergeConsole (c:\program files (x86)\qlogic corporation\qconvergeconsole\tomcat-x64\apache-tomcat-6.0.35\bin\tomcat6.exe) to carry out lateral movement tasks and run tools at a later stage.

## Backdoor

The first-stage backdoor, Cobalt Strike, is used to execute lateral movement and open the second-stage backdoor. HemiGate served as the second-stage backdoor in their prior operation, allowing them to continue accessing compromised computers. Nevertheless, Earth Estries launched this attack using a brand-new backdoor called Crowdoor.

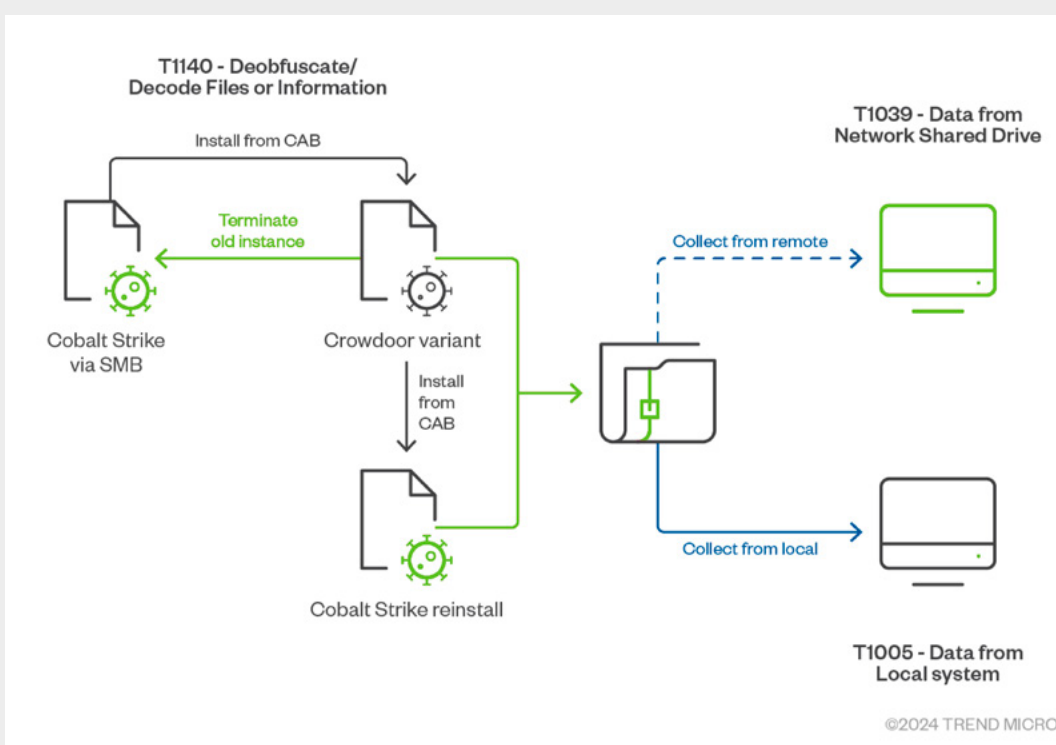
The Cobalt Strike installation has been observed interacting with the new backdoor variant, Crowdoor,

in accordance with Earth Estries' tools, tactics, and procedures (TTPs) involving reinstalling and cleaning up tools. The reinstalled Cobalt Strike and the Crowdoor instances were both brought in as CAB files by earlier instances.

### Commands

```
C:\Windows\system32\cmd.exe /C wmic /node:172.16.xx.xx process call create "cmd.exe /c c:\ProgramData\Microsoft\DRM\182.bat"

C:\Windows\system32\cmd.exe /C C:\Users\Public\Music\rar.exe a -m5 C:\Users\Public\Music\pdf0412.rar C:\Users\Public\Music\temp\*.pdf
```



Old Crowdoor variant	New Crowdoor variant	Functions
0x2347135	0x11736212	Initial connection C2
0x2347136	0x11736213	Collect ComputerName,Username, OS version and hostnet or IP information
0x2347137	0x11736214	Remote shell
0x234713B	0x11736218	Delete malware files, persistence and exit
0x2347140	0x1173621D	File related Operation
0x2347141	0x1173621E	Open/ReadFile
0x2347142	0x1173621F	Open/WriteFile

0x2347144	0x11736221	Collect drive information
0x2347145	0x11736222	Search File
0x2347148	0x11736225	CreateDirectory
0x2347149	0x11736226	Rename file or directory
0x234714A	0x11736227	Delete file or Directory
0x234714A	0x11736228	Communication with C&C server

## Collection via Backdoor

Earth Estries archives information of interest from both nearby and distant locations—using the Crowdoor and Cobalt Strike installations for collection routines. Here are a few instances of collection commands in action:

Example command	Functions
<code>rar.exe a -m5 &lt;install path&gt;\322.rar \\&lt;remote machine&gt;\c\$\&lt;remote path&gt;</code>	Gather information collected by an older generation of infection from a remote machine
<code>rar.exe a -m5 &lt;install path&gt; \his231.rar "C:\Users\&lt;username&gt;\AppData\Local\Google\Chrome\User Data\Default\History"</code>	Collect browser history files, which are of interest to the attackers to be able to compromise more credentials
<code>rar.exe a &lt;install path&gt;\0311.rar C:\users\&lt;user name&gt;\Desktop\* C:\users\&lt;user name&gt;\Downloads\* C:\users\&lt;user name&gt;\Documents\* -r -y -ta&lt;cutoff date&gt;</code>	Collect more recent files and/or documents interacted with by a local user

Telemetry indicates that they were exfiltrated using the same techniques as the collection command, either by using the same initial access method to control these tools or by using the command-and-control (C&C) channels of their backdoors.

Earth Estries used tools like Cobalt Strike, Hemigate, and Crowdoor that are distributed via CAB file packages to take advantage of flaws in web-based adapter management software like QConvergeConsole. These backdoors allowed lateral movement across the network in addition to PsExec. The group's all-encompassing strategies to strengthen their position in the target environment are further demonstrated using Trillclient for credential harvesting from browser caches.

## Indicators of Compromise

[File] [SHA256]	[Detection name]
42d4eb7f0411631891379c5cce55480d2d9d2ef8feaf1075e1aed0c52df4bb9	Backdoor.Win32.ZINGDOOR.ZHKH
95062728536f23b1335756a61d68f1df22d58594ece9998cae6b73772fd49f	Trojan.MSIL.DULLOAD.ZHKL
6a4de5c7787e212dea5f033f8f7cd39aefc93e7c83c8564dc2204813e8e76ff2	Backdoor.Win32.COBEACON.ZHKL.enc
27042218e8d1a0491525b35a6dc2fc0737841bcaed65b751e78769eadea9751	Trojan.Win32.DULLOAD.ZHKL
c32156a7de42a61f5d584e82dfbced690d23fd72080024c14a9143e5f20f0ad8	Backdoor.Win32.COBEACON.ZHKL
a298031b1c28f11f00d3b9f631fbfae881d6c789e70c4bc5e6ccdf8165b94c6	Backdoor.Win32.CRYPTMERLIN.ZHKL
cdde7878ed0529f9ef3ad58aa3084f1df6e2fb371807b15539187539b060fed2	TrojanSpy.Win64.NINJACOPY.ZYLA
6f274955b1fb58cc9a60476bc5a9cd9d54c962cc29e73db41b7786148cb74505	Trojan.Win64.DRACULoader.ZBLD
09abc579097b0bd8d115702bb1eeb546d2401373c83385a52386ad4243f945e8	Backdoor.Win64.ZINGDOOR.ZBKJ



292f70bff5717608c289f4146febcc06a2c5d8192529a8c51e18ec0f7b44dlcf	Backdoor.Win64.ZINGDOOR.ZBKJ
cd8630f8e07e16203195f563457a84beb08112fcb4d9ee1056a788174cf8f6b	Backdoor.Win32.CROWDOOR.ZCLC
98ddf03ca6ade4770cc06ac8034b3468bd94094f5813d28b74885e-5ca6958895	Backdoor.Win32.CROWDOOR.ZTLC
03365cce37db511fdfaf8d77a14f806a2d822a111aa8cc032b5b341c0b0064a5	Trojan.Win32.DULLOAD.ZCLB
1378bde3aee0057ca2a5854fee4d18447949lec624a3bbf215098afaa6b82299	Trojan.Win32.DRACULoader.ZCLB
bl7660d1a4c0258739024187497be0b11530791d1307d9e5556f04f0ac58d42f	Trojan.Win32.DULLOAD.ZCLB
b450311b5fc4333b26955f7c709ca61fcfd8a168f1a8839a93979a892a8c22cc	Trojan.Win32.DRACULoader.ZAKH
39f1c7095e1db05944eeda08a2e1c1b8c513ea581bfc0cb36ad106e3a8f38b5f	Trojan.Win32.DRACULoader.ZALJ
0c8c0b2837fbb9c15dalbf904ed3f3903e2d4d49c999394068f274b014a09dd	Trojan.Win32.DRACULoader.ZALJ
a113c637bb81f9bbd39731672b242a8da5915ef4b5e93d72cc9a7454b5e120bd	Trojan.Win64.DRACULoader.ZCLJ
4aeaa0d954268d4fc7179ec7578258c3459ee95b82698363e0cafb700c05181a	Trojan.Win64.DRACULoader.ZBLJ
d0575b3ced944dc627d047c60f23d25bd3aa0c4deab69f-784b9a80aae50fbd7b	Trojan.Win64.DRACULoader.ZCLJ
25b9fdef3061c7dfea744830774ca0e289dba7c14be85f0d4695d382763b409b	Trojan.Win32.SNAPPYBEE.ZMLJ
6d64643c044fe534dbb2c1158409138fcded757e550c6f79eada15e69a7865bc	Trojan.Win32.SNAPPYBEE.ZOLK

[Network Type]	[Indicators]
IP address	103.159.133[.]209
IP address	45.192.178[.]208
IP address	38.54.71[.]140 (Snappybee)
IP address	103.159.133[.]205
IP address	103.103.131[.]40
IP address	103.15.28[.]228
IP address	154.220.3[.]17
IP address	156.255.2[.]202
IP address	103.103.128[.]121
IP address	162.19.135[.]182
Domain	cdglobalclouds[.]com
Domain	broadmediacloud[.]com
Domain	zmail.broadmediacloud[.]com (CrowDoor)
Domain	www.nodtecloud[.]com
Domain	mail2-Oda8aa1c.oxcdntech[.]com (Zingdoor)
Domain	helpdesk.athenatechlabs[.]com (CrowDoor)
Domain	supports.flarecastdns[.]com (CrowDoor)
Domain	ns.starkaero[.]com (Cobeacon)
Domain	pay.johannesburghotel[.]net (CRYPTMERLIN)
Domain	kidshomeworkabc.global.ssl.fastly[.]net (Cobeacon)
Domain	ap.missmichiko[.]com (Zingdoor)
Domain	portal[.]spokemon[.]com (Zingdoor)
Domain	svn.truecdnnetwork[.]com (Cobeacon)
Domain	lync.realtxholdem[.]com

Domain	globalnetzone.b-cdn[.]net
Domain	amazoncdns[.]com
Domain	www[.]euphemismscase[.]site
Domain	www[.]dbacloudsupport[.]com
Domain	www[.]cloudshappen[.]com
Domain	www[.]amazoncdns[.]com
Domain	supports[.]dbacloudsupport[.]com
Domain	ssl3[.]awsdns-531[.]com
Domain	soffice[.]offices-analytics[.]com
Domain	services[.]offices-analytics[.]com
Domain	resource[.]offices-analytics[.]com
Domain	redsquare[.]redcrossco[.]com
Domain	portal[.]techmersion[.]com
Domain	portal[.]cdglobalclouds[.]com
Domain	opengl[.]cloudshappen[.]com
Domain	ns108[.]cloudshappen[.]com
Domain	ns101[.]awsdns-531[.]com
Domain	ms119[.]newsfreecloud[.]com
Domain	ms101[.]cloudshappen[.]com
Domain	mail[.]euphemismscase[.]site
Domain	llnw-dd[.]awsdns-531[.]com
Domain	images[.]dbacloudsupport[.]com
Domain	helpdesk[.]cloudshappen[.]com
Domain	helpdesk[.]athenatechlabs[.]com
Domain	global[.]techmersion[.]com
Domain	ge[.]huseinhbz[.]click
Domain	ftp[.]techmersion[.]com
Domain	euphemismscase[.]site
Domain	emv1[.]techmersion[.]com
Domain	emv1[.]cdglobalclouds[.]com
Domain	de[.]huseinhbz[.]click
Domain	credits[.]offices-analytics[.]com
Domain	cloudsrv[.]cloudfrontsrv[.]com
Domain	cdn181[.]awsdns-531[.]com
Domain	cdn101[.]cloudflaresrv[.]com
Domain	cdglobalclouds[.]com
Domain	cas04[.]awsdns-531[.]com
Domain	cachecloud[.]cloudflaresrv[.]com
Domain	cache10[.]newsfreecloud[.]com
Domain	c11r[.]awsdns-531[.]com
Domain	blog[.]techmersion[.]com
Domain	auth[.]boxlibraries[.]com

**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 cloud environment.

**Remediation:**

- In the event of an attack, isolate affected systems and networks immediately to prevent further spread of the malware.
- Secure external-facing services
- Implement prevention measures including phishing awareness training, network segmentation, and endpoint protection.
- Emphasize proactive measures like endpoint detection solutions, which can offer a robust defense against ransomware threats.
- Employ incident response teams to conduct thorough forensic analysis identifying the extent of the compromise and remove any traces of the malware from infected systems.
- Closely monitor network traffic and endpoint activities to help ensure that 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.

## China-Aligned MirrorFace Hackers Target EU Diplomats with World Expo 2025 Bait

MirrorFace, the China-affiliated threat actor, was seen attacking a diplomatic institution in the European Union, the first time the hacking team has targeted a regional organization.

According to ESET's APT Activity Report for the April–September 2024 period, “the threat actor used the upcoming World Expo, which will be held in 2025 in Osaka, Japan, as a lure during this attack.”

APT10, an umbrella group that includes clusters tracked as Earth Tengshe and Bronze Starlight, is thought to include MirrorFace, also known as Earth Kasha. Since at least 2019, it has been well-known for targeting Japanese organizations, but in early 2023, a new campaign was noticed that broadened its operations to include Taiwan and India.

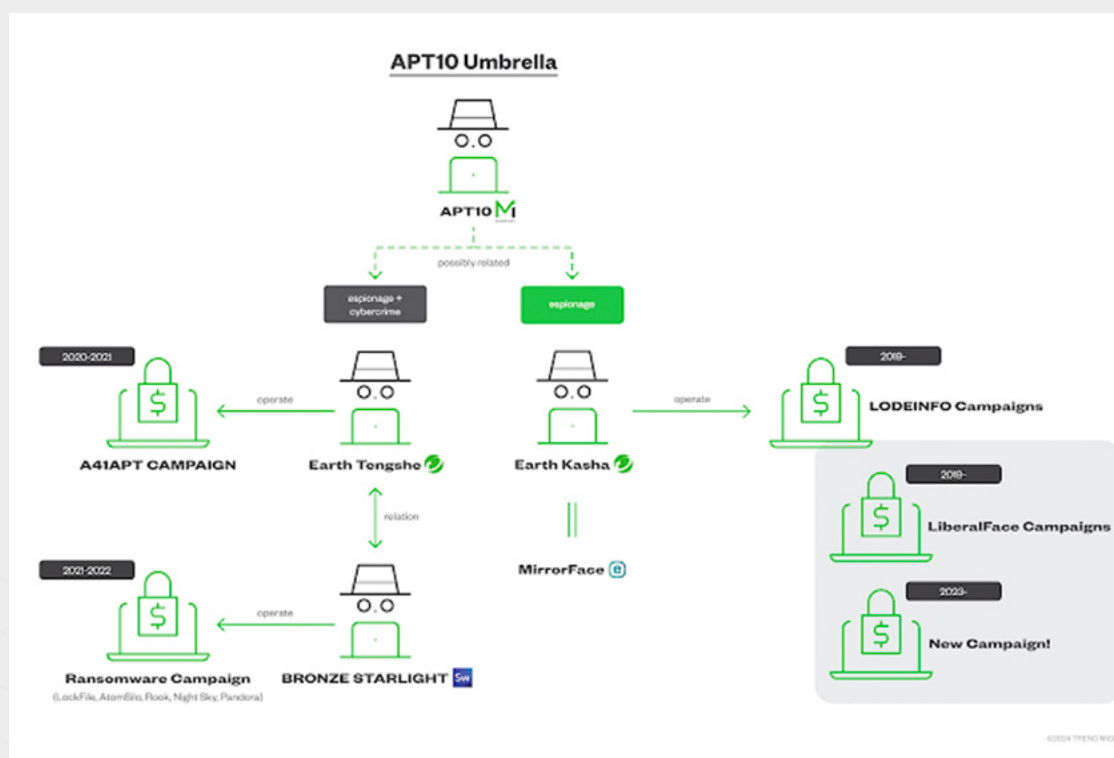
### Detection

Backdoors like ANEL (also known as UPPERCUT), LODEINFO, and NOOPDOOR (also known as HiddenFace) have been added to the hacking team's malware arsenal over time, along with a credential stealer called MirrorStealer.

MirrorFace attacks are highly targeted, according to ESET, which typically receives “less than 10 attacks per year.” Data theft and cyber espionage are the ultimate objectives of these intrusions. The threat actor has previously targeted diplomatic organizations.

The victim received a spear-phishing email with a link to a ZIP archive (“The EXPO Exhibition in Japan in 2025.zip”) hosted on Microsoft OneDrive in the most recent attack identified by the Slovak cybersecurity firm.

A Windows shortcut file (“The EXPO Exhibition in Japan in 2025.docx.lnk”) contained in the archive file was used to launch an infection sequence that eventually deployed ANEL and NOOPDOOR.





Around the end of 2018 or the beginning of 2019, ANEL vanished from the scene, and it was thought that LODEINFO had taken its place, making an appearance later in 2019. Thus, it's intriguing to see ANEL making a comeback after nearly five years.

The development coincides with the discovery that Chinese threat actors, such as Webworm, Granite Typhoon, and Flax Typhoon, are increasingly depending on the open-source, multi-platform SoftEther VPN to keep access to victims' networks.

### 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.
- 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.

### Remediation:

- Use Microsoft Defender XDR to find ransomware attacks that are operated by humans.

# Top Exploited Vulnerabilities

Vulnerability Name	Description	References
(ODay) G DATA Total Security Incorrect Permission Assignment Local Privilege Escalation Vulnerability CVE-2024-6871	Vulnerability allows local attackers to escalate privileges on affected installations of G DATA Total Security. The issue results from incorrect permissions set on folders.	<a href="https://linuxsecurity.com/advisories/ubuntu/ubuntu-6871-l-linux-kernel-hwe-security-advisory-updates-gqclpo32jgu8">https://linuxsecurity.com/advisories/ubuntu/ubuntu-6871-l-linux-kernel-hwe-security-advisory-updates-gqclpo32jgu8</a>
(ODay) Trimble SketchUp Viewer SKP File Parsing Memory Corruption Remote Code Execution Vulnerability CVE-2024-9731	Vulnerability allows remote attackers to execute arbitrary code on affected installations of Trimble SketchUp Viewer. Issue results from the lack of proper validation of user-supplied data, which can result in a memory corruption condition	<a href="https://www.cve.org/CVERecord?id=CVE-2024-9731">https://www.cve.org/CVERecord?id=CVE-2024-9731</a>
Panda Security Dome PSANHost Link Following Local Privilege Escalation Vulnerability CVE-2024-8424	Vulnerability allows local attackers to escalate privileges on affected installations of Panda Security Dome. The specific flaw exists within the Application Host Service. By creating a symbolic link, an attacker can abuse the service to delete a file.	<a href="https://www.watchguard.com/wgrd-psirt/advisory/wgsa-2024-00017">https://www.watchguard.com/wgrd-psirt/advisory/wgsa-2024-00017</a>
Delta Electronics DIAScreen DPA File Parsing Stack-based Buffer Overflow Remote Code Execution Vulnerability CVE-2024-39354	Vulnerability allows remote attackers to execute arbitrary code on affected installations of Delta Electronics DIAScreen. The issue results from the lack of proper validation of the length of user-supplied data prior to copying it to a fixed-length stack-based buffer.	<a href="https://www.cisa.gov/news-events/ics-advisories/icsa-24-312-02">https://www.cisa.gov/news-events/ics-advisories/icsa-24-312-02</a>
Delta Electronics InfraSuite Device Master _gExtrInfo Deserialization of Untrusted Data Remote Code Execution Vulnerability CVE-2024-10456	Vulnerability allows remote attackers to execute arbitrary code on affected installations of Delta Electronics InfraSuite Device Master. The specific flaw exists within the handling of the _gExtrInfo attribute.	<a href="https://www.cisa.gov/news-events/ics-advisories/icsa-24-303-03">https://www.cisa.gov/news-events/ics-advisories/icsa-24-303-03</a>
Linux Kernel nftables Improper Validation of Array Index Local Privilege Escalation Vulnerability	Vulnerability allows local attackers to escalate privileges on affected installations of the Linux Kernel. The specific flaw exists within the handling of packet filtering tables.	<a href="https://cdn.kernel.org/pub/linux/kernel/v5.x/ChangeLog-5.10.221">https://cdn.kernel.org/pub/linux/kernel/v5.x/ChangeLog-5.10.221</a>
Linux Kernel Net Scheduler ATM Queuing Discipline Use-After-Free Local Privilege Escalation Vulnerability	Vulnerability allows local attackers to escalate privileges on affected installations of Linux Kernel. The issue results from the lack of validating the existence of an object prior to performing operations on the object.	<a href="https://git.kernel.org/pub/scm/linux/kernel/git/stable/linux.git/commit/?h=v6.1.113&amp;id=09038f47e45cd5dbb02315db2134403a6b160ceb">https://git.kernel.org/pub/scm/linux/kernel/git/stable/linux.git/commit/?h=v6.1.113&amp;id=09038f47e45cd5dbb02315db2134403a6b160ceb</a>
X.Org Server XkbSetCompatMap Heap-based Buffer Overflow Privilege Escalation Vulnerability CVE-2024-9632	Vulnerability allows local attackers to escalate privileges on affected installations of X.Org Server. The specific flaw exists within the handling of XkbSetCompatMap requests.	<a href="https://bugzilla.redhat.com/show_bug.cgi?id=2317233">https://bugzilla.redhat.com/show_bug.cgi?id=2317233</a>
Autodesk AutoCAD CATPART File Parsing Memory Corruption Remote Code Execution Vulnerability CVE-2024-8592	Vulnerability allows remote attackers to execute arbitrary code on affected installations of Autodesk AutoCAD. The specific flaw exists within the parsing of CATPART files.	<a href="https://www.autodesk.com/trust/security-advisories/adsk-sa-2024-0020">https://www.autodesk.com/trust/security-advisories/adsk-sa-2024-0020</a>
Apple macOS ICC Profile Parsing Out-Of-Bounds Write Remote Code Execution Vulnerability CVE-2024-44284	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.	<a href="https://support.apple.com/en-us/121564">https://support.apple.com/en-us/121564</a>
Apple Scene Kit Improper Validation of Array Index Remote Code Execution Vulnerability CVE-2024-44218	Vulnerability allows remote attackers to execute arbitrary code on affected installations of Apple macOS. Interaction with the Scene kit framework is required to exploit this vulnerability but attack vectors may vary depending on the implementation.	<a href="https://support.apple.com/en-us/121564">https://support.apple.com/en-us/121564</a>
Nikon NEF Codec Thumbnail Provider NRW File Parsing Heap-based Buffer Overflow Remote Code Execution Vulnerability CVE-2024-8025	Vulnerability allows remote attackers to execute arbitrary code on affected installations of Nikon NEF Codec. The specific flaw exists within the parsing of NRW files.	<a href="https://downloadcenter.nikonimglib.com/en/download/sw/259.html">https://downloadcenter.nikonimglib.com/en/download/sw/259.html</a>

Continued on next page &gt;

VMware HCX list Extensions SQL Injection Remote Code Execution Vulnerability CVE-2024-38814	Vulnerability allows remote attackers to execute arbitrary code on affected installations of VMware HCX. The issue results from the lack of proper validation of a user-supplied string before using it to construct SQL queries.	<a href="https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/O/25019">https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/O/25019</a>
Trend Micro Deep Security Improper Access Control Local Privilege Escalation Vulnerability CVE-2024-48903	Vulnerability allows local attackers to escalate privileges on affected installations of Trend Micro Deep Security. The specific flaw exists within the Anti-Malware Solution Platform. The issues result from insufficient access control on a sensitive folder.	<a href="https://success.trendmicro.com/en-US/solution/KA-0017997">https://success.trendmicro.com/en-US/solution/KA-0017997</a>
Trend Micro Cloud Edge REST API Command Injection Remote Code Execution Vulnerability CVE-2024-48904	Vulnerability allows remote attackers to execute arbitrary code on affected installations of Trend Micro Cloud Edge. The specific flaw exists within the REST API, which listens on TCP port 8443 by default.	<a href="https://success.trendmicro.com/en-US/solution/KA-0017998">https://success.trendmicro.com/en-US/solution/KA-0017998</a>
Schneider Electric Zelio Soft 2 ZM2 File Parsing Use-After-Free Remote Code Execution Vulnerability CVE-2024-8422	Vulnerability allows remote attackers to execute arbitrary code on affected installations of Schneider Electric Zelio Soft 2. The specific flaw exists within the parsing of ZM2 files.	<a href="https://www.cisa.gov/news-events/ics-advisories/icsa-24-284-14">https://www.cisa.gov/news-events/ics-advisories/icsa-24-284-14</a>
Oracle VirtualBox TPM Heap-based Buffer Overflow Local Privilege Escalation Vulnerability CVE-2024-21259	Vulnerability allows local attackers to escalate privileges on affected installations of Oracle VirtualBox. The specific flaw exists within the implementation of the virtual TPM device.	<a href="https://www.oracle.com/security-alerts/cpuoct2024verbose.html">https://www.oracle.com/security-alerts/cpuoct2024verbose.html</a>
QEMU SCSI Use-After-Free Local Privilege Escalation Vulnerability CVE-2024-6519	Vulnerability allows local attackers to escalate privileges on affected installations of QEMU. The specific flaw exists within the implementation of the virtual LSI53C895A SCSI Host Bus Adapter.	<a href="https://access.redhat.com/security/cve/CVE-2024-6519">https://access.redhat.com/security/cve/CVE-2024-6519</a>
PostHog database_schema Server-Side Request Forgery Information Disclosure Vulnerability CVE-2024-9710	Vulnerability allows remote attackers to disclose sensitive information on affected installations of PostHog. The specific flaw exists within the implementation of the database schema method.	<a href="https://github.com/PostHog/posthog/pull/25388">https://github.com/PostHog/posthog/pull/25388</a>
Tungsten Automation Power PDF JP2 File Parsing Out-Of-Bounds Read Remote Code Execution Vulnerability 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.	<a href="https://esd.tungstenautomation.com/Registrations/ChooseLanguage">https://esd.tungstenautomation.com/Registrations/ChooseLanguage</a>
VMware vCenter Server Heap-Based Buffer Overflow Vulnerability CVE-2024-38812	Vulnerability allows a malicious actor with network access to vCenter Server can trigger this vulnerability by sending a specially crafted network packet potentially leading to remote code execution.	<a href="https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/O/24968">https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/O/24968</a>
Progress Kemp LoadMaster OS Command Injection Vulnerability CVE-2024-1212	Vulnerability allows unauthenticated remote attackers to access the system through the LoadMaster management interface, enabling arbitrary system command execution.	<a href="https://community.progress.com/s/article/Release-Notice-LMOS-7-2-59-2-7-2-54-8-7-2-48-10-CVE-2024-1212">https://community.progress.com/s/article/Release-Notice-LMOS-7-2-59-2-7-2-54-8-7-2-48-10-CVE-2024-1212</a>
Palo Alto Networks PAN-OS Management Interface Authentication Bypass Vulnerability CVE-2024-0012	An authentication bypass in Palo Alto Networks PAN-OS software enables an unauthenticated attacker with network access to the management web interface to gain PAN-OS administrator privileges to perform administrative actions, tamper with the configuration, or exploit other authenticated privilege escalation vulnerabilities like CVE-2024-9474	<a href="https://security.paloaltonetworks.com/CVE-2024-0012">https://security.paloaltonetworks.com/CVE-2024-0012</a>

## Security Bulletin

**vCenter RCE Actively Exploited:** Broadcom has issued an urgent warning that two critical vulnerabilities in VMware vCenter Server are now being actively exploited in the wild. The more severe of the two flaws is a remote code execution (RCE) vulnerability tracked as CVE-2024-38812, which carries a maximum CVSSv3 score of 9.8. The second vulnerability, CVE-2024-38813, allows attackers to escalate privileges to root by sending maliciously crafted network packets. It has a CVSSv3 score of 7.5.

**DDoS Attacks Growing Bigger:** Distributed Denial of Service (DDoS) attacks are escalating at an alarming rate, as unveiled in a revelation by Cloudflare researchers. The recent data indicates that these attacks pose an increasingly severe threat to online services and infrastructure worldwide.

As per Cloudflare researchers, exponential increase is observed across multiple metrics: –

- ✎ **Bits per second (bps):** Skyrocketed from 309 Gbps in 2013 to a staggering 5.6 Tbps in 2024, marking a 20-fold increase.
- ✎ **Packets per second (pps):** Surged from 230 Mpps in 2015 to 2,100 Mpps in 2024, a 10-fold rise.
- ✎ **Requests per second (rps):** Experienced the most dramatic growth, soaring from 6 Mrps in 2020 to an unprecedented 201 Mrps in September 2024, representing a 70-fold increase since 2014.

**URL Rewriting Abused in Phishing Attack:** Cybercriminals have found a new way to exploit email security measures, turning them into tools for their malicious activities. Since mid-June 2024, threat actors have been increasingly abusing URL rewriting features, which are designed to protect users from phishing threats, to carry out sophisticated attacks. The process involves replacing original URLs with modified links that first direct recipients to the vendor's servers for threat scanning before allowing access to the web content.

**DocuSign Targeting Organizations Working with Govt Agencies:** A new wave of sophisticated phishing attacks exploiting DocuSign has emerged, specifically targeting businesses that regularly interact with state, municipal, and licensing authorities. Cybersecurity researchers have reported a staggering 98% increase in DocuSign phishing URLs between November 8 and 14, compared to the entirety of September and October. These attacks are particularly dangerous as they exploit the trusted relationships between businesses and regulatory bodies. These phishing attempts often involve time-sensitive requests, such as licensing renewals, change orders, or compliance issues, pressuring victims to act quickly without proper verification.

## Reference Links

1. [https://www.infosecurity-magazine.com/news/cybercriminals-exploit-weekend/?web\\_view=true](https://www.infosecurity-magazine.com/news/cybercriminals-exploit-weekend/?web_view=true)
2. [https://www.helpnetsecurity.com/2024/11/06/identity-related-data-breaches-cost/?web\\_view=true](https://www.helpnetsecurity.com/2024/11/06/identity-related-data-breaches-cost/?web_view=true)
3. [https://www.cybersecuritydive.com/news/ai-assisted-attacks-top-emerging-risk-gartner/731874/?web\\_view=true](https://www.cybersecuritydive.com/news/ai-assisted-attacks-top-emerging-risk-gartner/731874/?web_view=true)
4. <https://www.infosecurity-magazine.com/news/tmobile-breached-chinese/>
5. <https://www.outlookbusiness.com/news/81-of-bank-ceos-identify-cybersecurity-talent-shortage-as-key-growth-challenges-for-the-sector>
6. <https://cybersecuritynews.com/new-docusign-attacks-targeting-organizations/>
7. <https://cybersecuritynews.com/ddos-attack-growing-bigger/>
8. <https://nao-sec.org/2024/10/lcePeony-with-the-996-work-culture.html>
9. <https://securitylabs.datadoghq.com/articles/tenacious-pungsan-dprk-threat-actor-contagious-interview/>
10. <https://ransomwatch.telemetry.ltd/#/stats>
11. Breaking Down Earth Estries Persistent TTPs in Prolonged Cyber Operations | Trend Micro (US)
12. <https://social.cyware.com/news/breaking-down-earth-estries-persistent-ttps-in-prolonged-cyber-operations-cc7cae47>
13. [https://community.gurukul.com/articles/ThreatResearch/Breaking-Down-Earth-Estries-Persistent-13-11-2024?\\_gl=1\\*1s79upt\\*\\_gcl\\_au\\*MTg4NTAxNDZy4xNzMyNjA2NjMw\\*\\_ga\\*MTE4OTE4NTgyLjE3MzI2MDY2MzI.\\*\\_ga\\_XK6L3BZR7J\\*MTczMjYwNjYzMi4xLjAuMTczMjYwNjYzMi42MC4wLjA](https://community.gurukul.com/articles/ThreatResearch/Breaking-Down-Earth-Estries-Persistent-13-11-2024?_gl=1*1s79upt*_gcl_au*MTg4NTAxNDZy4xNzMyNjA2NjMw*_ga*MTE4OTE4NTgyLjE3MzI2MDY2MzI.*_ga_XK6L3BZR7J*MTczMjYwNjYzMi4xLjAuMTczMjYwNjYzMi42MC4wLjA)
14. China-Aligned MirrorFace Hackers Target EU Diplomats with World Expo 2025 Bait
15. <https://therecord.media/china-linked-hackers-tasked-with-japanese-targets-pursue-through-europe>
16. <https://social.cyware.com/news/china-aligned-mirrorface-hackers-target-eu-diplomats-with-world-expo-2025-bait-9404bc54>

## 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](http://www.sdgc.com) and [www.truops.com](http://www.truops.com).



■ 75 North Water Street, Norwalk, CT 06854  
 ■ 203.866.8886  
 ■ [sdgc.com](http://sdgc.com)