Secureworks®
a SOPHOS company

THREAT INTELLIGENCE EXECUTIVE REPORT

Volume 2025, Number 1

Presented by the
Counter Threat Unit™ (CTU)
Research Team

Executive Summary

The Secureworks® Counter Threat Unit™ (CTU) research team analyzes security threats to help organizations protect their systems. Based on observations in November and December, CTU™ researchers identified the following noteworthy issues and changes in the global threat landscape:

- Clop ransomware group targets Cleo file transfer systems
- Ransomware threat remains high
- Chinese compromises continue

Clop ransomware group targets Cleo file transfer systems

It's unlikely that GOLD TAHOE's data theft attacks on Cleo managed file transfer systems will be the last example of this type of activity.

File transfer systems have proven a valuable and often highly accessible source of sensitive data for the GOLD TAHOE threat group, which operates the Clop ransomware. The group has used zero-day vulnerabilities to target these systems, including Accellion FTA in 2021 and MOVEit Transfer in 2023. The MOVEit Transfer attacks alone impacted over 2,500 victims by the end of 2023. Based on this history, it's unsurprising that GOLD TAHOE exploited vulnerabilities in Cleo MFT products in early December 2024.

There were initially questions about attribution for the Cleo attacks, but GOLD TAHOE claimed responsibility in a December 15 message posted to their dark web leak site. The threat actors started to list victims on the Clop leak site at the end of December, confirming a return to activity after rarely posting victims since August 2023. The group initially listed over 65 partially obscured names of Cleo MFT victims. By mid-January 2025, the names were unobscured, but only 59 were listed. The reduced number suggests that some victims may have paid ransom.

CTU researchers always recommend prompt patching of systems that can be accessed from outside the corporate network. However, GOLD TAHOE typically exploits zero-day vulnerabilities. In addition, there is little an organization can do to prevent a breach of a trusted third party, especially via a zero-day vulnerability in the vendor's platform.

To minimize the risk and impact of these types of incidents, organizations should implement best practices such as requiring data to be encrypted at rest, password protecting data, applying data-retention policies, and auditing data flows through the system. Monitoring systems to alert on unexpected data flows is also essential.

What You Should Do Next

Review policies and procedures specific to secure managed file transfer solutions. Aim to minimize the time data resides on these solutions and apply additional layers of data security if necessary.

Ransomware threat remains high

Law enforcement actions have successfully disrupted some ransomware operations, but the threat persists as other ransomware groups have taken their place.

While GOLD TAHOE appeared to return to normal operations in late 2024, the wider ransomware ecosystem experienced significant changes as the year drew to a close. These changes were largely the result of law enforcement's actions against the LockBit name-and-shame ransomware-as-a-service (RaaS) scheme throughout 2024 and the shuttering of the BlackCat (also known as ALPHV) RaaS scheme in March.

Unfortunately, those law enforcement successes did not mean a slowdown in attacks. Leak site listings only provide an approximate view of ransomware activity as they do not include victims who paid the ransom. Yet the numbers remained elevated, with November ranking the most active month of the year at 663 victims. December was not much lower (542), giving it the third-highest monthly total in 2024.

What did change was threat actor affiliation and the level of fragmentation in the ransomware ecosystem. LockBit and BlackCat affiliates shifted to other ransomware operations, many of which emerged in the aftermath of the LockBit takedown and BlackCat shuttering. Forty-six new name-and-shame ransomware schemes launched between March and the end of November. While 32 groups listed victims in January 2024, 49 posted victim names in November and 52 posted in December. The RansomHub scheme operated by GOLD HUBBARD emerged in late February, and the victim tally on its leak site steadily increased to the highest number of victims of any scheme in November and the second highest in December, after Clop.

Some displaced affiliates likely joined existing schemes such as Akira or Play, while others may have gone solo. Secureworks incident responders have noticed an increase in the number of ransomware attacks conducted by threat actors who do not use branding associated with established groups and may be operating independently.

Successful defense against ransomware attacks remains the same despite these changes. Organizations should regularly patch internet-facing devices, implement phishing-resistant multi-factor authentication (MFA) as part of a conditional access policy, and monitor their network and endpoints for malicious activity.

What You Should Do Next
Ensure you have an incident response plan in place in case a ransomware attack happens.

Chinese compromises continue

As more information is released about Chinese cyberattacks on Western organizations, keeping on top of patching and other good security practices is even more essential.

November and December brought further revelations about the scale of the threat that Chinese cyberespionage groups pose to U.S. and other Western entities. In particular, it became clearer that Salt Typhoon, which compromised major U.S. telecommunications providers, has had a broader impact than initially thought. During a White House press briefing on December 4, U.S. deputy national security advisor Anne Neuberger stated that Salt Typhoon had breached telecommunications companies in dozens of countries over a period of one to two years. A U.S. Cybersecurity and Infrastructure Security Agency (CISA) spokesperson told the media on December 3 that it was not possible to “say with certainty that the adversary has been evicted, because we still don't know the scope of what they're doing.” During the compromises, China was allegedly able to access information from systems used by the U.S. federal government for court-authorized wiretapping related to criminal and national security investigations. Details about the telecommunications systems used by the U.S. and its allies, particularly call detail records (CDRs), are likely of value to China.

At the end of December, news broke that the U.S. Treasury Department’s network had been breached in a supply chain attack by a Chinese state-sponsored threat group, later identified as Silk Typhoon. This breach was a result of the compromise of BeyondTrust in early December. The group was likely searching for information about possible sanctions of Chinese interests or U.S. government plans to control Chinese investments in the U.S.

In these incidents, Silk Typhoon and Salt Typhoon likely gained initial access by exploiting vulnerabilities. Chinese threat groups consistently take advantage of vulnerable perimeter devices, exploiting them to access corporate networks or to conduct supply chain attacks. As demonstrated by Chinese threat group Volt Typhoon, the threat actors may also recruit the devices into botnets for use in other attacks. As demonstrated by Chinese threat group Volt Typhoon, the threat actors may also recruit the devices into botnets for use in other attacks.

In the press briefing, Neuberger also said that “if the companies had in place minimum [security] practices… that would make it far riskier, harder, and costlier for the Chinese to gain access and maintain access.” This sentiment and the exploitation of vulnerabilities in perimeter devices are not new, nor are they unique to Chinese threat groups. In August 2023, Secureworks incident responders investigated a network compromise in which a Russian threat actor obtained access to dozens of perimeter routers, modified them, and redirected a copy of network traffic to a remote IP address.

Protecting the perimeter is one of the most essential elements of cybersecurity for organizations in every sector.

✓ **What You Should Do Next**

Prioritize perimeter devices in your patching program.

Conclusion

Anne Neuberger's emphasis on the importance of basic security practices bears constant repetition and reinforces the CTU research team's frequent guidance. Promptly patching vulnerabilities, encrypting data at rest and in transit, and avoiding exposing device management interfaces to the internet unless access control and strong authentication are implemented are all examples of good practices that will help protect organizations against attacks by cybercriminals and state-sponsored threat groups.

A Glance at the CTU Research Team

CTU researchers frequently serve as expert resources for the media, publish technical analyses for the security community, and speak about emerging threats at security conferences. Leveraging Secureworks' advanced security technologies and a network of industry contacts, the CTU research team tracks threat actors and analyzes anomalous activity, uncovering new attack techniques and threats. This process enables CTU researchers to identify threats as they emerge and develop countermeasures that protect customers before damage can occur.

Research

Understanding the nature of threats customers face, and creating countermeasures to address and protect.

Intelligence

Providing information that extends the visibility of threats beyond the edges of a network.

Integration

Infusing CTU intelligence into the Secureworks Taegis XDR platform, managed solutions, and security consulting practices.

Secureworks®
a **SOPHOS** company

Secureworks, a Sophos company, is a global cybersecurity leader that protects customer progress with Taegis™, an AI-native security analytics platform built on more than 20 years of real-world threat intelligence and research, improving customers' ability to detect advanced threats, streamline and collaborate on investigations, and automate the right actions.

If you need immediate assistance, call our 24x7 **Global Incident Response Hotline:**

+1-770-870-6343