Secureworks®

Threat Intelligence Executive Report

Volume 2022, Number 1

Presented by the
Counter Threat Unit™ (CTU)
research team

Executive Summary

The Secureworks® Counter Threat Unit™ (CTU) research team analyzes security threats and helps organizations protect their systems. During November and December 2021, CTU™ researchers observed notable developments in threat behaviors, the global threat landscape, and security trends, and identified lessons to consider.

- Log4j flaws highlight security concerns about third-party code
- Chinese threat groups share tactics and increase sophistication
- Some ransomware groups debut, others persist or return

Log4j flaws highlight security concerns about third-party code

Not all organizations will fall victim to exploitation of a high-profile vulnerability. However, every security team must be able to identify and patch affected systems in their environment, including those using third-party code, often at short notice.

December 2021 was exceptionally busy for cybersecurity teams, thanks to the ostensibly easy-to-exploit Log4j vulnerability CVE-2021-44228 (also known as Log4Shell). Nearly all organizations have Java applications running Log4j in their environment. The subsequent disclosure of four additional Log4j vulnerabilities (CVE-2021-45105, CVE-2021-45046, CVE-2021-44832, and CVE-2021-4104) added to the pressure, even though they were considered less severe than Log4Shell.

Threat actors responded quickly, beginning extensive scanning immediately following the December 9 disclosure. Yet the number of actual compromises remains low compared to the level of scanning activity. This discrepancy suggests that successful exploitation, even of vulnerabilities that are characterized as ‘trivial to exploit’, is often much harder on complex real-world enterprise systems than in test environments.

The low number of compromises is not a reason for complacency. Identifying systems that use the Log4j code library, especially in third-party code; checking if vulnerable servers were compromised; and patching systems all created a significant burden for affected organizations. But this attention to detail was necessary due to the potential severity of the vulnerabilities.

The challenge isn't over. Organizations will be confronted with Log4j-related risks until they have identified and updated all vulnerable systems. Meanwhile, threat actors will continue to attempt exploitation.

This will not be the last time organizations have to address vulnerabilities that they cannot easily pinpoint in their systems. To improve their ability to respond, organizations should implement processes that identify third-party code and include the results in risk assessments. They must also develop compensating controls, such as limiting or stopping backend servers from communicating with the internet, and implementing comprehensive network and endpoint monitoring.

✓ **If you do just one thing after reading this:**
Review your incident response procedures to ensure they work as planned during times of reduced staffing over the holidays, when threat actors often strike.

Chinese threat groups share tactics and increase sophistication

Chinese government-sponsored threat groups continue to enhance operational security and technical sophistication. Network defenders must respond to these increasingly complex attacks while remembering that groups with similar geographical targets often share tradecraft.

Analysis of Chinese government-sponsored threat group activity during November and December 2021 provided a reminder that tracking geopolitical activity can predict and provide information about cyber activity. Chinese People's Liberation Army (PLA) reforms announced in 2015 introduced five regional theater commands: Northern, Western, Central, Eastern, and Southern. Overlaps in infrastructure and malware, as well as collaboration among specific Chinese threat groups targeting China's adjacent countries, are consistent with these PLA theater commands.

For example, the evolution of activity involving the modular ShadowPad malware demonstrates its proliferation across theater commands. The Chinese government-sponsored BRONZE ATLAS threat group has used ShadowPad since at least 2017. In 2019, a growing list of other Chinese threat groups began deploying it globally in attacks against organizations in multiple industry verticals. CTU researchers analyzed ShadowPad activity that appears linked to the Northern, Southern, and Western theater commands.

Cyberattacks by Chinese groups observed in November and December support the evidence that these threat groups are improving their tradecraft. Their activity included complex execution chains involving multiple steps. The threat actors also increasingly used infrastructure within target countries during their attacks to disguise their origin, and continued to exploit known vulnerabilities rather than zero-day vulnerabilities. To address these threats, network defenders must implement security controls that provide the visibility and defense-in-depth to prevent, detect, and remediate attacks involving complex execution chains.

Organizations will likely encounter multiple Chinese threat groups using tactics, techniques, and procedures (TTPs) that were previously exclusive to a distinct group. As a result, an organization's threat modeling of a specific threat group should include the TTPs of other groups operating in the same theater command. Timely patching of perimeter devices helps organizations defend against Chinese threat group activity, even as the threat actors evolve their tradecraft and sophistication.

✓ **If you do just one thing after reading this:**
Remain vigilant to geopolitical developments affecting regions where your organization operates.

Some ransomware groups debut, others persist or return

The ransomware landscape is ever-changing. Despite temporary setbacks for some groups, the overall number of attacks is still increasing.

For a short while after the May 2021 Colonial Pipeline attack by the Darkside ransomware group, it seemed as if ransomware groups had overreached and were on the retreat. However, the name-and-shame activity in November and December conclusively spoiled that theory. In November, leak sites monitored by CTU researchers cumulatively listed the greatest number of victim names for the year. In December, a record number of threat groups listed victims. Of course, leak sites only provide a partial view of the ransomware landscape. Many victims pay the ransom before they are listed, and many ransomware groups do not maintain leak sites.

The most prolific name-and-shame groups in November and December were LockBit and Conti. The Sabbath and Entropy groups emerged in November, and the ALPHV (also known as Blackcat), Bl@ckt0r, RobinHood, and ROOK groups emerged in December.

The most active 'new' group appeared to be Karakurt, which seems to be an extortion-only group that does not encrypt a victim's files. It listed 33 victims on its leak site in December. However, there are indications that Karakurt may have carried out attacks as early as September but just launched its leak site in December.

The Snatch name-and-shame group resumed activity in November 2021. It was the first group to create a leak site, posting six victims in May 2019 before going dormant. By the end of December, the number of victims listed on its leak site had grown to 23 victims. On the other hand, some groups remained dormant. The GOLD SOUTHFIELD threat group that operated the REvil ransomware has not posted victims since October.

Ransomware is a many-headed hydra. Individual groups may disappear or go quiet, but new ones quickly emerge. In 2021, the number of victims listed on leak sites per month never dropped lower than the total for January 2021, despite strong law enforcement action. Further, the number of publicly named victims in 2021 was more than double 2020's total. The November reemergence of longstanding ransomware precursor Emotet will likely spawn another increase of victims in 2022. Organizations cannot afford to drop their guard.

✓ **If you do just one thing after reading this:**
Reduce ransomware risk by protecting access to all internet-facing servers with multi-factor authentication.

Conclusion

As ransomware and government-sponsored threat groups grow in sophistication, stealth, and effectiveness, they will remain eager to leverage high-profile vulnerabilities. The prevalence of third-party code adds to the burdens of vulnerability management and network defense for organizations. It is increasingly important to leverage detection systems and security controls that can identify, stop, or ideally prevent intrusions from both types of threat group.

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 research and intelligence into Secureworks managed security services and security consulting practices.

Secureworks®

Secureworks® (NASDAQ: SCWX) is a leading global cybersecurity company that protects organizations in the digitally connected world. We combine visibility from thousands of customers, aggregate and analyze data from any source, anywhere, to prevent security breaches, detect malicious activity in real time, respond rapidly, and predict emerging threats. We offer our customers a cyber-defense that is Collectively Smarter. Exponentially Safer.™

Corporate Headquarters

United States
1 Concourse Pkwy NE #500
Atlanta, GA 30328
www.secureworks.com

Asia Pacific

Australia
Building 3, 14 Aquatic Drive Frenchs
Forest, Sydney NSW Australia 2086

Japan
Otemachi One Tower 17F, 2-1,
Otemachi 1-chome, Chiyoda-ku,
Tokyo 100-8159,
Japan
www.secureworks.jp

Europe & Middle East

France
8 avenue du Stade de France 93218
Saint Denis Cedex

Germany
Main Airport Center,
Unterschweinstiege 10 60549
Frankfurt am Main Germany

United Kingdom
One Creechurch Place,
1 Creechurch Ln
London EC3A 5AY
United Kingdom

1 Tanfield
Edinburgh EH3 5DA
United Kingdom

United Arab Emirates
Building 15, Dubai Internet City Dubai,
UAE PO Box 500111

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

+1-770-870-6343