[redacted]

INTEL471

[redacted]

ANNOUNCEMENT

# Executive Intelligence Update – Dec. 23, 2024

Published: Today 05:16:38 UTC

Intel 471's Executive Intelligence Update gives CISOs and security teams insight into trends, threats, risks and regulations. This will be the last Executive Intelligence Update for this year. We'll resume publishing Jan. 13, 2025. In this issue:

- CLOP exploits attacks file transfer software again
- CISA sent more ransomware warnings than ever
- Raccoon infostealer developer sentenced to five years
- Signal group chats offer intelligence collection opportunities

## 1. CLOP exploits file transfer software again

**What's happening**: The **CLOP** ransomware and extortion group has been exploiting vulnerabilities in managed file transfer software from the vendor Cleo as part of suspected extortion attempts. The number of organizations affected could range from dozens to hundreds.

**Backdoor deployed: CLOP** is a ransomware and data extortion group that has specialized in targeting vulnerabilities in managed file transfer systems. **CLOP** is believed to have first exploited CVE-2024-50623 — an unrestricted file upload with dangerous type vulnerability impacting Cleo's Harmony, VLTrader versions and LexiCom products. Cleo patched that flaw on Oct. 29, 2024. However, Huntress Labs wrote in early December 2024 that it appeared the software was still being exploited, possibly because that patch didn't mitigate the issue. According to a rundown by Bleeping Computer, Rapid7 then discovered a second similar but different vulnerability, CVE-2024-55956, which is an unauthenticated file write vulnerability. Cleo has now patched that issue. Both of the flaws could allow an unauthenticated user to import bash or PowerShell scripts leveraging the default settings of autorun directories. The security vendor Artic Wolf writes that the attackers deployed a PowerShell stager, which was then used to upload a Java-based cross-platform backdoor it calls Cleopatra that supports in-memory file storage.

Bleeping Computer reached **CLOP** after which the group confirmed that it had been exploiting CVE-2024-50623 and CVE-2024-55956. The group purportedly told the publication it had exploited "a lot" of organizations. On Dec. 15, 2024, **CLOP** wrote on their victim-shaming blog that "due to recent events (attack of CLEO)" they allegedly would delete data pertaining to older attacks from their server and "will work only with new companies." These latest attacks add to several other mass breaches **CLOP** has exploited in managed file transfer software, including Accellion's FTA, Fortra's GoAnywhere MFT and Progress Software's MOVEit Transfer software.

**Intel 471's view: CLOP**'s recent claim of compromising organizations through the newly disclosed Cleo vulnerabilities likely are credible given the striking parallels with their previous exploitation of file transfer software. It is plausible that **CLOP** had prior knowledge of several vulnerabilities in Cleo's platforms, enabling the group to breach and extract data from victim organizations systematically long before the vendor issued a public security advisory. By timing their public disclosures and media engagement, the group likely intends to maximize the pressure on victims and amplify the overall impact of these attacks. In the short term, additional reports of **CLOP**-related breaches are anticipated, especially as the group has prepared to accommodate new victims on their extortion site. It is likely that proof-of-concept exploit code for these vulnerabilities will be publicly released, which can be expected to trigger further malicious activity from other threat groups.

## 2. CISA sent more ransomware warnings than ever

**What's happening:** The U.S. Cybersecurity and Infrastructure Security Agency (CISA) sent 2,131 notifications to organizations as of November 2024 warning them of impending ransomware attacks, giving them time to kick threat actors out of their networks.

**Trusted intermediary:** The notifications are part of CISA's Pre-Ransomware Notification Initiative (PRNI), which launched in 2023. Since the start of the program, PRNI has sent about 3,368 notifications, most of which were sent in 2024. It allows researchers, infrastructure providers and security companies to pass on cyber threat intelligence through a trusted intermediary. The nature of how ransomware attacks take shape means that security companies, email providers, cyber threat intelligence firms, infrastructure companies and others may gain visibility into potential targets. Ransomware actors often purchase credentials from underground markets, and the advertisements for those credentials can give a clue as to which organization may be targeted next. Email security providers may be monitoring phishing campaigns targeted at

[redacted]

companies. Threat actors may post screenshots from inside compromised organizations as proof of their intrusions but also revealing the identity of the victim. Security companies also sometimes gain access to ransomware gangs' systems and subsequently learn about infected organizations. But warning organizations can be difficult, particularly if two parties have no pre-existing relationship. Ironically, some organizations that receive warnings sometimes suspect that they've been compromised by the party doing the reporting. Outreach by security companies – even if it is genuine – maybe misinterpreted as a commercial pitch rather than an earnest heads-up. Most often, such warnings are simply ignored. CISA says its notifications were sent to "hundreds of K-12 school districts; state, local, tribal and territorial government entities; healthcare organizations and hospitals; and other critical infrastructure." CISA also said it used its administrative subpoena powers to drive mitigation of more than 1,200 devices used in critical infrastructure such as power plants and water utilities, up from about 690 in 2023.

**Intel 471's view:** The ransomware threat has not receded in 2024. In fact, the threat appears to loom greater than ever, although there are anecdotal signs fewer organizations may be paying. The PRNI is an example of the type of public-private partnerships that drive better security outcomes. A program such as this administered on an international level could perhaps help even more organizations undertake mitigation action before a ransomware or data extortion attack occurs.

# 3. Raccoon infostealer developer sentenced to five years

**What's happening:** Ukrainian Mark Sokolovsky was sentenced to five years in prison and will pay $910,000 in restitution after pleading guilty to charges related to Raccoon stealer, which was the top information stealer (infostealer) malware for several years.

**Admin fled Ukraine:** Raccoon stealer launched around 2019. It was sold as a malware-as-a-service model, where customers pay a subscription fee. With that fee came a unique version of Raccoon stealer and the related software and administration panels to run campaigns. Customers of Raccoon stealer found it dead easy to use, and it had great customer support. Users often became infected through emails with malicious attachments or links. Once on a computer, Raccoon would steal usernames, passwords, financial data, cryptocurrency wallet data, session tokens and more. After Raccoon pilfered the data, it would delete itself, with the user none the wiser that their sensitive data had been stolen.

Sokolovsky fled Ukraine with his girlfriend when Russia launched a full-scale invasion in February 2022. Sokolovsky didn't know it at the time, but he was facing charges in the U.S. In November 2021, a grand jury in federal court in Texas returned an indictment that charged him with being the administrator of Raccoon stealer. As part of its investigation, the FBI recovered at least 50 million sets of unique login credentials and other types of data, including bank accounts details, cryptocurrency addresses, credit card numbers and four million email addresses. All told, it's believed that more than two million devices were infected. Sokolovsky was arrested in the Netherlands in March 2022. He fought extradition but lost and was extradited to the state of Texas. In October 2024, he pleaded guilty to one count of conspiracy to commit computer intrusion. For more information about Raccoon stealer, please see episode 8 of Intel 471's Cybercrime Exposed podcast, which can be found on Spotify and Apple.

**Intel 471's view**: Infostealer malware is a sought after product amongst the cybercriminal underground, and since the demise of Raccoon stealer, several others are now commonly seen infecting systems. Infostealer "logs" — which are batches of data comprising stolen credentials, financial data and other sensitive information — are high-demand commodities traded on underground forums. One of the most prominent of these is the Russian Market, a well-established platform among Russian cybercriminals extensively used by threat actors worldwide. Russian Market serves as a platform for selling logs from six different stealer families at the time of this report — Lumma, Raccoon, RisePro, RedLine, Stealc and Vidar.

# 4. Signal group chats offer intel collection opportunities

**What's happening:** Intel 471 has added group chats on Signal to its intelligence messaging platform intelligence collection, as threat actors have expressed interest in alternative messaging platforms to increase operational security (OPSEC).

**Worries about Telegram:** For several years, cybercriminals have been expanding the number of platforms and messaging services they use. Cybercriminals began gravitating to messaging applications throughout 2021 and 2022 following a handful of data breaches and leaks impacting well-known cybercrime forums (see: Friendly fire: Four well-known cybercriminal forums dealing with breaches). The leaks revealed users' private messages, contact names, and email addresses, likely driving some forum users to seek alternatives. Discord and Telegram shaped up to be the most popular platforms for cybercriminals (see: Why cybercriminals are flocking to Telegram). Telegram offers near real-time encrypted communication between individuals, groups chats up to 200,000 users, and channels to broadcast to an unlimited number of viewers. Both Telegram and Discord also have functionality that enables actors to automate parts of their malware operations and store stolen data. Telegram's reputation, however, became somewhat tarnished after the service said it would divulge data such as IP addresses and phone numbers in response to lawful legal requests. This announcement came from Telegram co-founder and CEO on Sept. 23, 2024, about a month after he was indicted by French authorities. Durov, who frequently positioned Telegram as a platform free of censorship, was indicted on charges including the sale of malicious hacking tools, fraud, money laundering and child sexual abuse material. The suggestion that Telegram was willing to be more accommodating to legal requests caused a shiver through the cybercriminal world.

Underground chatter indicated some threat actors planned to move to different platforms. However, four months on, Telegram still is a hotbed of activity, and we track more than 6,600 Telegram channels although not all of those are active.

**Intel 471's view:** Compared to Telegram, Signal today is not a significant hub for cybercrime, but our collection of relevant Signal chat groups has steadily increased since we added our initial batch of groups. Signal is attractive to those seeking privacy because it minimizes the amount of data it collects from its users. Messages and calls are end-to-end encrypted. It's free, so there's no payment related data. Users must register with a phone number, but once an account is registered, that phone number can be hidden from other users, a new, privacy-enhancing feature. Instead, users can find one another with a username rather than a phone number, and the username can also be changed. All of these are good OPSEC features. But there are limits that might make it less appealing for cybercriminals seeking a large market that is possible on Telegram. For example, group chats are limited to just 1,000 people. Signal also lacks Telegram's application protocol interfaces that have allowed infostealer developers to use Telegram to automate the exfiltration of stolen data (see: How cybercriminals are using messaging apps to launch malware schemes). However, Signal group chats meet the needs of threat actors who primarily need a private and secure alternative for communicating, coordinating and planning their next attacks. For more information and an intelligence report covering how threat actors are using different messaging services including Tox, Session, Jabber (XMPP), Matrix, Telegram and Signal, please contact us.