CLOP Poses Ongoing Risk to HPH Organizations

Executive Summary

CLOP is a ransomware variant associated with the FIN11 threat actor group and the double extortion tactic, it has previously been used to target several U.S. HPH organizations. Researchers have also identified the CLOP operators combining the "spray and pray" approach to compromising targets with a more targeted approach, suggesting that the operators have some discretion when selecting victims. In December 2020, CLOP operators discovered multiple zero-day vulnerabilities affecting the Accellion File Transfer Appliance (FTA) product and began targeting its users. CLOP should be treated the same as any other ransomware/extortion cybercrime group when it comes to safeguarding against their attacks. Mitigations for the HPH sector can be found at the end of the report.

Report

On November 12, 2020, the ACSC released an alert noting "increased targeting activity against the Australian Health sector by actors using the SDBBot Remote Access Tool… SDBBot is a known precursor of the Clop ransomware." CLOP, also known as CL0P (spelled with a zero instead of an "o"), is an active ransomware variant using the popular double extortion ransomware strategy. This technique occurs when a cybercriminal gang first steals an organization's information before encrypting it. The actors then demand payment to decrypt the data and to ensure they do not leak the organization's data. Should a victim fail to pay, their data will appear on CLOP's ransomware website, CLOP^_- LEAKS. Researchers at Mandiant FireEye have also observed the operators of CLOP combining the "spray and pray" approach to compromising targets with a more targeted approach by operating large scale phishing campaigns and then selecting which of the networks it compromises to target for monetization.
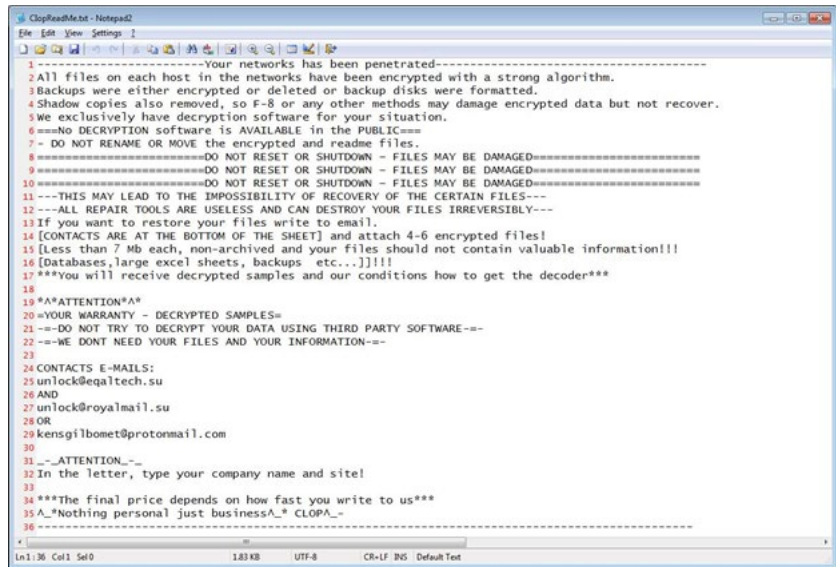

Figure 1 CLOP ransom note, Source: BleepingComputer

The CryptoMix ransomware variant CLOP began circulating in February 2019 and initially behaved very similarly to other CryptoMix variants. However, in March 2019 security researchers noted that the variant changed behavior and began disabling services for enterprise software like Microsoft Exchange, Microsoft SQL Server, MySQL, and BackupExec. CLOP also changed its ransom note to indicate that entire networks were compromised by the ransomware rather than individual devices. The December 2019 variant of CLOP built out this functionality further, targeting and killing 663 processes on the device before beginning the encryption process.

BleepingComputer tied CLOP to threat actor group TA505, a financially motivated threat group active since at least 2014, and later to the TA505 spinoff group FIN11. In 2020, FIN11 began using CLOP to target HPH companies, including:

- April 2020: ExecuPharm, Inc., a U.S.-based pharmaceutical research company
- May 2020: Carestream Dental LLC, a U.S.-based provider of dental equipment
- November 2020: Nova Biomedical, a U.S.-based medical device manufacturer

The group has also targeted HPH organizations in Canada and Sweden. Mandiant researchers following FIN11 have assessed with moderate confidence that the group operates from somewhere within the Commonwealth of Independent States (CIS), which comprise most of the former Soviet Union countries. This assessment is based on FIN11's avoidance of systems utilizing CIS-country keyboard layouts and the use of Russian-language file metadata. Researchers believe that FIN11 outsources many of their services via underground, criminal communities. This includes using bulletproof hosting services, signed certificates, publicly available malware, and domain registration services. Attribution efforts are hampered when a cybercrime organization uses many of the same publicly available services as other cybercriminals.

After the discovery of four zero-day vulnerabilities affecting the Accellion FTA product, CLOP began targeting Accellion customers. Accellion supplied a hotfix on December 22, 2020, but at least one customer, cloud-based security services supplier Qualys, had data published on CLOP's ransomware blog despite applying the fix. According to Mandiant, the link between CLOP/FIN11 and the threat actors behind the Accellion attack is unknown.

CLOP should be treated the same as any other ransomware/extortion cybercrime group when it comes to safeguarding against their attacks. The Cybersecurity and Infrastructure Security Agency (CISA) has published Alert (AA20-302A) - Ransomware Activity Targeting the Healthcare and Public Health Sector, in conjunction with the Department of Health and Human Services and the Federal Bureau of Investigations. This end of this Alert contains a section titled 'General Ransomware Mitigations – HPH Sector' and contains numerous best practices regarding ransomware along with points of contact should you become a victim. The link to this alert is in the References section.

References

"Alert (AA20-302A) Ransomware Activity Targeting the Healthcare and Public Health Sector," Cybersecurity and Infrastructure Security Agency. October 28, 2020. https://us-cert.cisa.gov/ncas/alerts/aa20-302a

"Clop Ransomware Also Follows the Trend - Leaks Data After Failed Ransom Attempt," Cyware. May 6, 2020. https://cyware.com/news/clop-ransomware-also-follows-the-trend-leaks-data-after-failed-ransom-attempt-5d624968

"Ransomware in Australia," Australian Signals Directorate's Australian Cyber Security Centre. October 2, 2020. https://www.cyber.gov.au/acsc/view-all-content/publications/ransomware-australia

"TA505," MITRE ATT&CK. June 23, 2020. https://attack.mitre.org/groups/G0092/

Abrams, Lawrence. "Clop Ransomware Now Kills Windows 10 Apps and 3rd Party Tools," Bleeping Computer. January 3, 2020. https://www.bleepingcomputer.com/news/security/clop-ransomware-now-kills-windows-10-apps-and-3rd-party-tools/

Paganini, Pierluigi. "Clop ransomware gang leaks data allegedly stolen from cybersecurity firm Qualys," Security Affairs. March 3, 2021. https://securityaffairs.co/wordpress/115250/data-breach/qualys-clop-ransomware.html

Scroxton, Alex. "Qualys caught up in Accellion FTA breach," Computer Weekly. March 4, 2021. https://www.computerweekly.com/news/252497263/Qualys-caught-up-in-Accellion-FTA-breach

Seals, Tara. "Accellion FTA Zero-Day Attacks Show Ties to Clop Ransomware, FIN11," Security Weekly. February 22, 2021. https://threatpost.com/accellion-zero-day-attacks-clop-ransomware-fin11/164150/

Stark, Genevieve et al. "FIN11: Widespread Email Campaigns as Precursor for Ransomware and Data Theft," FireEye. October 14, 2020. https://www.fireeye.com/blog/threat-research/2020/10/fin11-email-campaigns-precursor-for-ransomware-data-theft.html

Townsend, Kevin. "FIN11 Spun Out From TA505 Umbrella as Distinct Attack Group," Security Week. October 14, 2020. https://www.securityweek.com/fin11-spun-out-ta505-umbrella-distinct-attack-group

We want to know how satisfied you are with our products. Your answers will be anonymous, and we will use the responses to improve all our future updates, features, and new products. Share Your Feedback