Health Sector Cybersecurity Coordination Center (HC3)
Analyst Note
November 16, 2020 **TLP: WHITE** **Report: 202011160840**

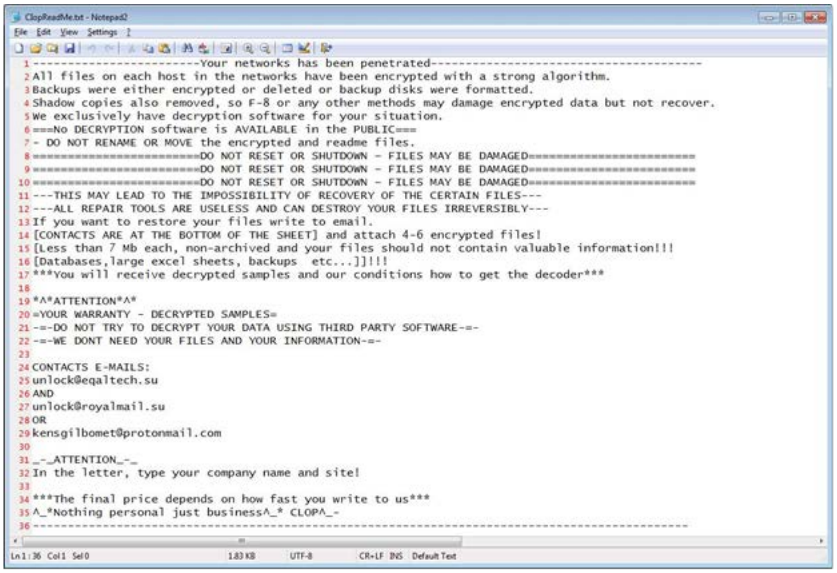
CLOP Poses Ongoing Risk to HPH Organizations

Executive Summary

CLOP, a ransomware variant associated with the FIN11 threat actor group and the double extortion tactic, has previously targeted several U.S. healthcare and public health (HPH) organizations. The Australian Cyber Security Center (ACSC) published an alert notifying the Australian HPH sector of the danger posed by the SDBBot Remote Access Tool and CLOP ransomware. 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. 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 12th, 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 CLOP (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.



```
-----------------------Your networks has been penetrated--------------------------------------
All files on each host in the networks have been encrypted with a strong algorithm.
Backups were either encrypted or deleted or backup disks were formatted.
Shadow copies also removed, so F-8 or any other methods may damage encrypted data but not recover.
We exclusively have decryption software for your situation.
===No DECRYPTION software is AVAILABLE in the PUBLIC===
- DO NOT RENAME OR MOVE the encrypted and readme files.
=======================DO NOT RESET OR SHUTDOWN - FILES MAY BE DAMAGED=======================
=======================DO NOT RESET OR SHUTDOWN - FILES MAY BE DAMAGED=======================
=======================DO NOT RESET OR SHUTDOWN - FILES MAY BE DAMAGED=======================
---THIS MAY LEAD TO THE IMPOSSIBILITY OF RECOVERY OF THE CERTAIN FILES---
---ALL REPAIR TOOLS ARE USELESS AND CAN DESTROY YOUR FILES IRREVERSIBLY---
If you want to restore your files write to email.
[CONTACTS ARE AT THE BOTTOM OF THE SHEET] and attach 4-6 encrypted files!
[Less than 7 Mb each, non-archived and your files should not contain valuable information!!!
[Databases,large excel sheets, backups  etc...]]!!!
***You will receive decrypted samples and our conditions how to get the decoder***

*^*ATTENTION*^*
=YOUR WARRANTY - DECRYPTED SAMPLES=
-=-DO NOT TRY TO DECRYPT YOUR DATA USING THIRD PARTY SOFTWARE-=-
-=-WE DONT NEED YOUR FILES AND YOUR INFORMATION-=-

CONTACTS E-MAILS:
unlock@eqaltech.su
AND
unlock@royalmail.su
OR
kensgilbomet@protonmail.com

_-_ATTENTION_-_
In the letter, type your company name and site!

***The final price depends on how fast you write to us***
^_*Nothing personal just business^_* CLOP^_-
----------------------------------------------------------------------------------------------
```

Figure 1 CLOP ransom note, Source: BleepingComputer

The CryptoMix ransomware variant CLOP began circulating in February 2019 and initially behaved very similar 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:

- 20200430: ExecuPharm, Inc., a U.S-based pharmaceutical research company
- 20200505: Carestream Dental LLC, a U.S.-based provider of dental equipment Carestream Dental LLC
- 20201106: 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.

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) recently 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

https://us-cert.cisa.gov/ncas/alerts/aa20-302a
https://www.cyber.gov.au/acsc/view-all-content/publications/ransomware-australia
https://www.bleepingcomputer.com/news/security/clop-ransomware-now-kills-windows-10-apps-and-3rd-party-tools/
https://www.fireeye.com/blog/threat-research/2020/10/fin11-email-campaigns-precursor-for-ransomware-data-theft.html
https://attack.mitre.org/groups/G0092/
https://www.securityweek.com/fin11-spun-out-ta505-umbrella-distinct-attack-group
hxxp://ekbgzchl6x2ias37[.]onion
https://cyware.com/news/clop-ransomware-also-follows-the-trend-leaks-data-after-failed-ransom-attempt-5d624968