Clop Ransomware

OVERVIEW

A variant of the CryptoMix, Clop ransomware is spreading via executables with legitimate digital signatures and is targeting entire networks instead of individual users.

OVERVIEW

- CLOP ransomware belongs to CryptoMix ransomware family. The ransom note indicates that the attackers are targeting an entire network rather than an individual computer.
- Clop ransomware uses similar processes like Maze and Revil to steals data before encrypting the company systems, so even if the company refuses to pay the ransom the operators behind them can still make some profit by selling the stolen data on Dark Web markets.

TECHNICAL DETAILS

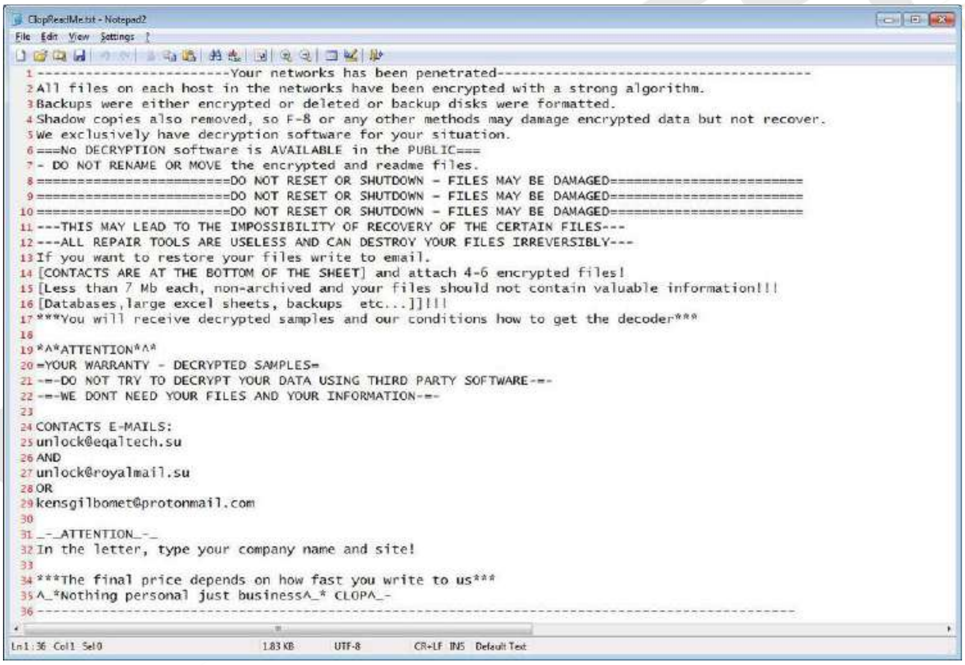
- Clop ransomware's executable code is distributed with legitimate digital signatures. So, the code looks more reliable and may help to bypass some security solutions.
- After execution, Clop will try to search some specific stings in order to stop specific Windows services and processes to disable antivirus software.
- Some other programs are also stopped by Clop including new Windows 10 apps, popular text editors, debuggers, programming languages, terminal programs, and programming IDE software.

ACROBAT.EXE
MEMCACHED.EXE
SKYPEAPP.EXE
ADB.EXE
MICROSOFTEDGE.EXE
SNAGIT32.EXE
CODE.EXE
NOTEPAD++.EXE
TOMCAT7.EXE
CALCULATOR.EXE
POWERPNT.EXE
UEDIT32.EXE
CREATIVE CLOUD.EXE
PYTHON.EXE
WINRAR.EXE
ECLIPSE.EXE
QEMU-GA.EXE
WINWORD.EXE
EVERYTHING.EXE
RUBY.EXE
YOURPHONE.EXE
JENKINS.EXE
SECURECRT.EXE

- Next it disables Windows Defender, by configuring various Registry values that disable behavior monitoring, real time protection, sample uploading to Microsoft, Tamper Protection, cloud detections, and antispyware detections.

```
cmd.exe /C reg add "HKLM\Software\Policies\Microsoft\Windows Defender\Real-Time Protection" /v "DisableBehaviorMonitoring" /t REG_DWORD /d "1" /f
cmd.exe /C reg add "HKLM\Software\Policies\Microsoft\Windows Defender\Real-Time Protection" /v "DisableOnAccessProtection" /t REG_DWORD /d "1" /f
cmd.exe /C reg add "HKLM\Software\Policies\Microsoft\Windows Defender\Real-Time Protection" /v "DisableRealtimeMonitoring" /t REG_DWORD /d "1" /f
cmd.exe /C reg add "HKLM\Software\Policies\Microsoft\Windows Defender\Spynet" /v "SubmitSamplesConsent" /t REG_DWORD /d "2" /f
cmd.exe /C reg add "HKLM\Software\Policies\Microsoft\Windows Defender\Real-Time Protection" /v "DisableScanOnRealtimeEnable" /t REG_DWORD /d "1" /f
cmd.exe /C reg add "HKLM\Software\Microsoft\Windows Defender\Features" /v "TamperProtection" /t REG_DWORD /d "0" /f
cmd.exe /C reg add "HKLM\Software\Policies\Microsoft\Windows Defender" /v "DisableAntiSpyware" /t REG_DWORD /d "1" /f
cmd.exe /C reg add "HKLM\Software\Policies\Microsoft\Windows Defender\MpEngine" /v "MpCloudBlockLevel" /t REG_DWORD /d "0" /f
cmd.exe /C reg add "HKLM\Software\Policies\Microsoft\Windows Defender\Spynet" /v "SpynetReporting" /t REG_DWORD /d "0" /f
```

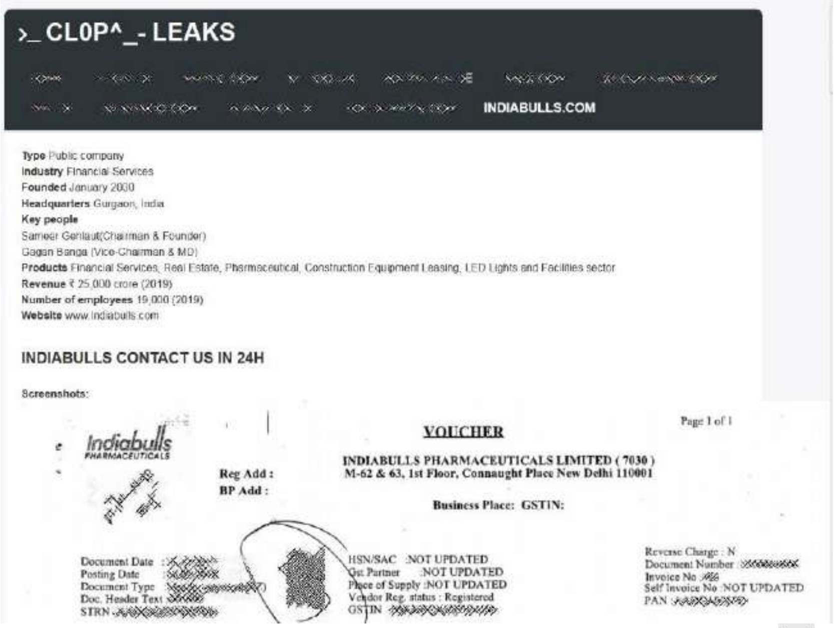
- Clop attackers are using batch script to delete Volume Shadow Copy, resize Volume Shadow Copy to avoid its recovery and to disable recovery option in the boot process.
- The ransomware encrypts files and appends .CLOP or .CIOP extension to the encrypted file's name and creates a ransom note named "ClopReadMe.txt".



```
------------------------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***

*A*ATTENTION*A*
=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

- Like current scenario in ransomware, Clop attackers are also publishing users' personal data on the dark web for sale.
- Recently CLOP ransomware attackers hacked the Indian conglomerate IndiaBulls Group. Attackers leaked samples of stolen data and threatened to release the overall dump within 24 hours if the victim does not pay the ransom.



>_ CL0P^_- LEAKS

[redacted] INDIABULLS.COM

Type Public company
Industry Financial Services
Founded January 2000
Headquarters Gurgaon, India
Key people
Sameer Gehlaut(Chairman & Founder)
Gagan Banga (Vice-Chairman & MD)
Products Financial Services, Real Estate, Pharmaceutical, Construction Equipment Leasing, LED Lights and Facilities sector
Revenue ₹ 25,000 crore (2019)
Number of employees 19,000 (2019)
Website www.indiabulls.com

INDIABULLS CONTACT US IN 24H

Screenshots:

Indiabulls PHARMACEUTICALS

Page 1 of 1

VOUCHER

INDIABULLS PHARMACEUTICALS LIMITED (7030)
Reg Add : M-62 & 63, 1st Floor, Connaught Place New Delhi 110001
BP Add :

Business Place: GSTIN:

Document Date : [redacted]
Posting Date : [redacted]
Document Type : [redacted]
Doc. Header Text : [redacted]
STRN [redacted]

[redacted]

HSN/SAC :NOT UPDATED
Gst Partner :NOT UPDATED
Place of Supply :NOT UPDATED
Vendor Reg. status : Registered
GSTIN [redacted]

Reverse Charge : N
Document Number : [redacted]
Invoice No : [redacted]
Self Invoice No :NOT UPDATED
PAN : [redacted]

Figure 2: IndiaBulls leak on CLOP data leak site

- IndiaBulls had an exposed Citrix Netscaler ADC VPN gateway that was vulnerable to CVE-2019-19781 vulnerability. Exploiting this vulnerability, the attackers could then carry out arbitrary code execution remotely for unauthenticated access, and it could have been the cause of Clop ransomware attack.

INDICATORS OF COMPROMISE

File Hashes (MD5)

0403DB9FCB37BD8CEEC0AFD6C3754314
160FD326A825271E9BD71653BA6F3EE1
227A9F4931342F8B49CB3044F66DBF05
25E11A9EBDE8D2CC26084E3C739273A7
279F5BEEE9D4BF8C54026E78ACBA61B1
35792C5501760071D461E9455AA50730
3FE02FDD243979106F6D91AE2DF8CCFF
569D3ED52F17B12729CEF26018C81FB9
72A76CA18B85E64A8C655C94BE087C5E
738314AA6E07F9A625E4774AC1243A79
73FBFBB0FB34E2696E5F3D9A9D2F6D46
949670DCDED69C76760D87F2271E0631
A09CE9363467F0CDD72714945CF0BF3A
A93B3DAA9460C64C631AD076D8ED126E
AE0C9765CC0BC9F4D2ED8970FF77A8D1
AE5CB860F043CAA84BF4E11CEC758616
B7FD25034019BC0B09242047D2C1D62A
C41A0E1DDEB85B6326A3DC403A5FD0FA
D8DF0EEE17FA5A361E26D67C43E10F28
ED7DB8C2256B2D5F36B3D9C349A6ED0B

Email Addresses

servicedigilogos[at]protonmail[.]com
managersmaers[at]tutanota[.]com

unlock[at]goldenbay[.]su

unlock[at]graylegion[.]su

unlock[at]eqaltech[.]su

unlock[at]royalmail[.]su

kensgilbomet[at]protonmail[.]com

PREVENTIVE AND CORRECTIVE ACTIONS

- **For Organizations**
  - **Preventive Actions**
    - Block the IoCs in the corresponding security devices.
    - All these IoCs are combined in our Threat Intelligence Feed that is integrated with our SOC to provide proactive threat protection to our clients.
    - Employ content scanning and filtering on the organization mail servers. Inbound e-mails should be scanned for known threats and should block any attachment types that could pose a threat.
    - Ensure all systems and software are up-to-date with relevant security patches.
    - Turn off file sharing if not needed. If file sharing is required, use ACLs and password protection to limit access. Disable anonymous access to shared folders. Grant access only to user accounts with strong passwords to folders that must be shared.
    - Limit the number of third-party vendors and employees that have access to RDP connections, create a user group that will be allowed remote access.
    - Use strong passwords and multi-factor authentication on Remote Desktop connection especially on administrator accounts.
    - Ensure anti-virus and anti-malware solutions are set to automatically update and regular scans are conducted.
    - Do not pay the ransom. It only encourages and funds these attackers. Even if the ransom is paid, there is no guarantee that one will be able to regain access to files.
  - **Corrective Actions**
    - If infected, disconnect the affected system from the Network.
    - Inform the Information Security Team.

- Use antivirus or anti-malware software to clean the ransomware.

- **For Individuals**
  - **Preventive Actions**
    - Take regular backups of your data.
    - Do not open mails and mail attachments from unknown people.
    - Do not download or use software cracks and illegal software.
    - Use strong password and multi-factor authentication for your RDP (Remote Desktop Protocol) connection.
    - Make sure your RDP connection is not open to the internet.
    - If not using RDP, close TCP Port 3389 on the computers.
    - Enable network level authentication for RDP.
    - Avoid installing free programs found on the Internet, many of them include viruses.
    - Be careful of the external devices you connect to your computer.
    - Update your antivirus regularly.
    - Regularly monitor your financial transaction, if you notice any suspicious transaction, contact your bank immediately.
  - **Corrective Actions**
    - If infected, disconnect your system from the Network.
    - Perform a full system scan in safe mode to remove any infections.