Elusive MegaCortex Ransomware Found - Here is What We Know

bleepingcomputer.com/news/security/elusive-megacortex-ransomware-found-here-is-what-we-know/

Lawrence Abrams

By
Lawrence Abrams

- July 19, 2019
- 03:00 AM
- 0

A sample of the ransomware called MegaCortex that is known to target the enterprise in targeted attacks has been found and analyzed. In this article, we will provide a brief look at the MegaCortex Ransomware and how it encrypts a computer.

When modern ransomware were first released, attackers would distribute the malware in a wide net in order to catch as many victims as possible. Over the past year, ransomware has evolved into more targeted enterprise attacks that have been earning extremely large payouts. Due to these payouts, we continue to see new players in the targeted ransomware scene.

While Ryuk, BitPaymer, and Sodinokibi (REvil) have become commonly known as "enterprise ransomware", the MegaCortex Ransomware less known. This article will hopefully shed some light on how it operates.

Installed via targeted attacks

We first heard about MegaCortex when Sophos reported that victims contacted them about being infected with a new ransomware called MegaCortex.

When Sophos analyzed the victim's computers, they found that the attackers were gaining access to a network and then compromising the Windows domain controller. Once the domain controller was compromised the attackers would install Cobalt Strike in order to open a reverse shell back to the attackers.

Now that the attackers had full access to the network, they would use PsExec to distribute a batch file and the ransomware named as winnit.exe to the rest of the computers on the network. It would then execute this batch file in order to encrypt the various compromised workstations.

```
424 sc config VeeamTransportSvc start= disabled
425 sc config W3Svc start= disabled
426 sc config wbengine start= disabled
427 sc config WRSVC start= disabled
428 sc config MSSQL$VEEAMSQL2008R2 start= disabled
429 sc config SQLAgent$VEEAMSQL2008R2 start= disabled
430 sc config VeeamHvIntegrationSvc start= disabled
431 sc config swi_update start= disabled
432 sc config SQLAgent$CXDB start= disabled
433
434 iisreset /stop
435 c:\windows\temp\winnit.exe [redacted]==
```

Portion of batch file

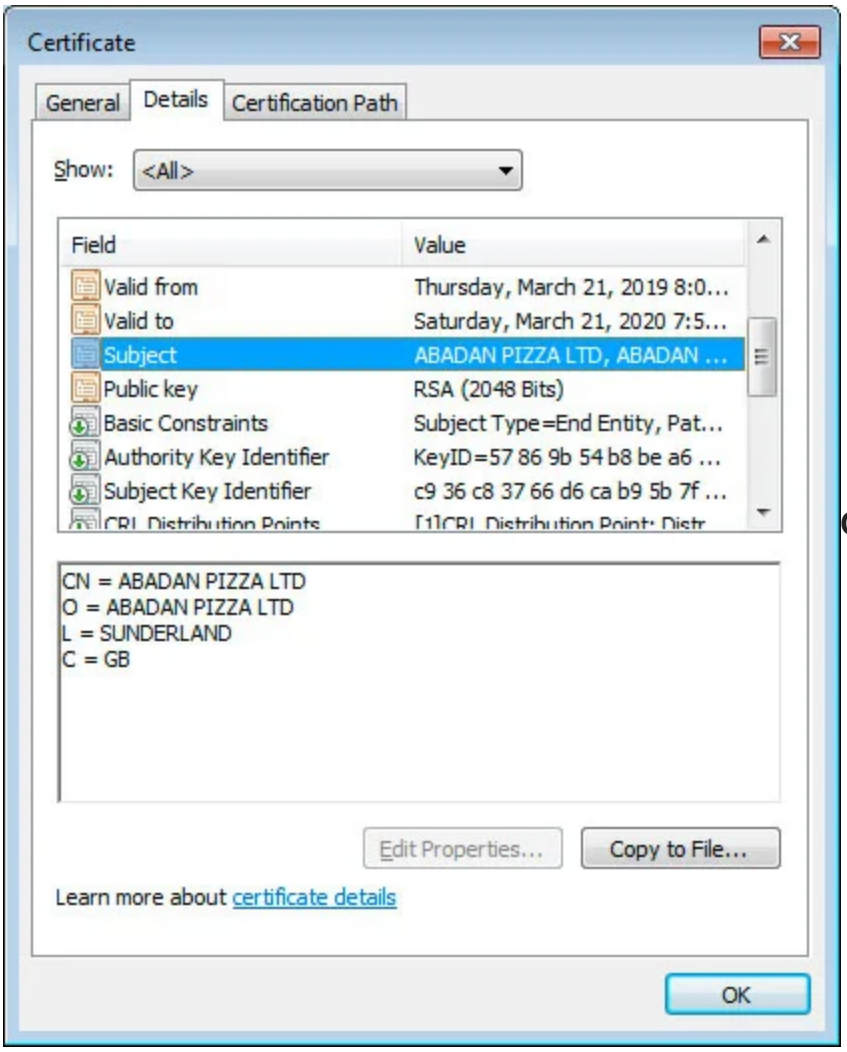
When launching the winnit.exe executable, a particular base64 encoded string would need to be provided in order for the ransomware to extract and inject a DLL into memory. This DLL is the main ransomware component that encrypts a computer.

It is not known exactly how the attackers gained access to a network, but Sophos stated that the Emotet or Qakbot Trojans were present on networks also infected with MegaCortex.

The MegaCortex encryption process

In a sample of MegaCortex discovered by MalwareHunterTeam, analyzed by Vitali Kremez, and shared with BleepingComputer, we are able to gain new insight into how the ransomware operates.

The particular sample that was found is code signed with a certificate from a UK company named "ABADAN PIZZA LTD". This company was probably abandoned and then claimed by the attackers under their own aliases in order to purchase a certificate.



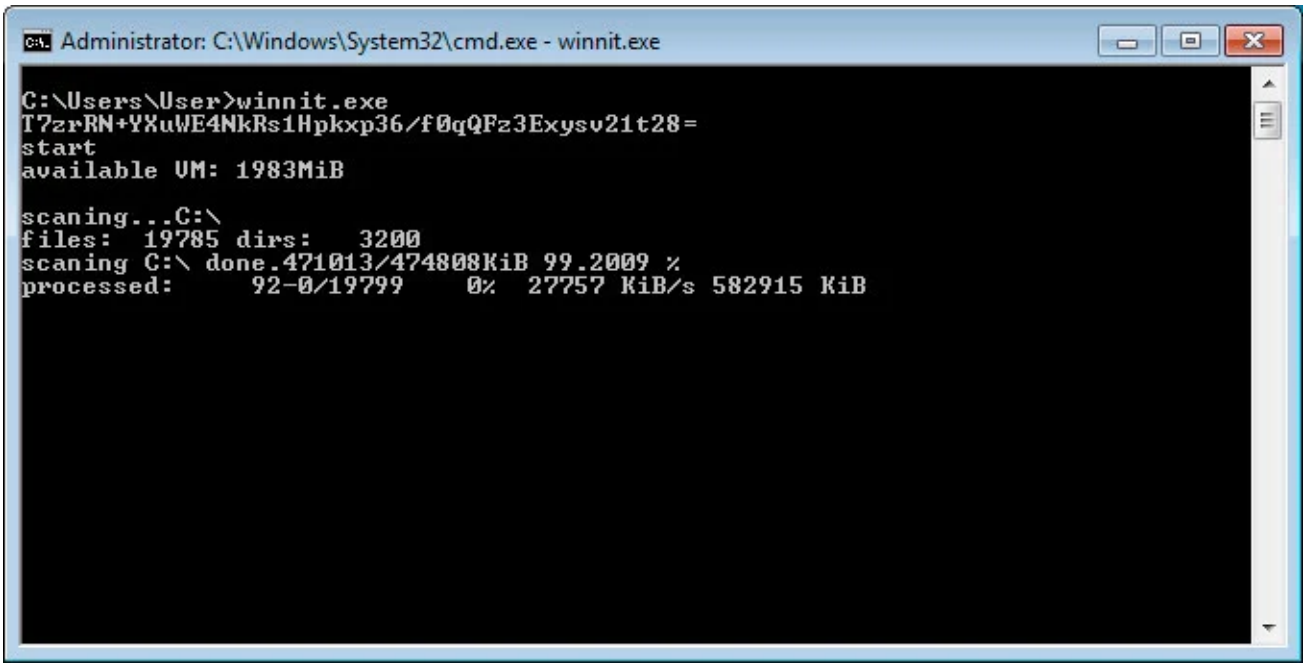
Certificate used to sign ransomware

In this sample, it is no longer necessary to provide a special base64 encoded string for the DLL payload to be unpacked and injected into memory. Now you can simply run the executable and the ransomware will begin encrypting the computer.

Kremez thinks this change was made in order to increase the scale of their operations and to simplify its execution.

"I think they are trying to scale their ops and reach more victims Simplifying their approach without multiple layered script execution" Kremez told BleepingComputer.

When executed, MegaCortex will display a running output of the files processed and its current stage of operation. As you can see by the output of the ransomware below, MegaCortex was designed to be monitored by a live attacker and then cleaned up after execution is finished.



MegaCortex Encrypting Files

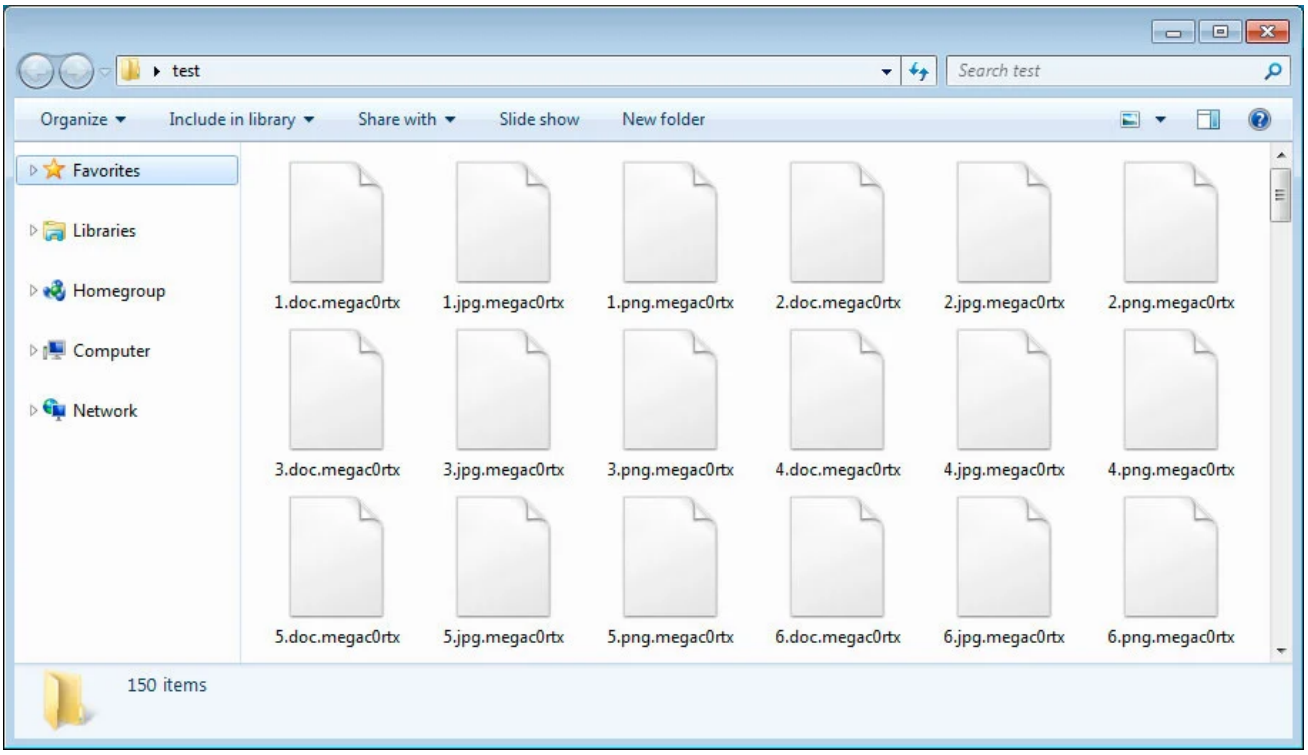
Kremez told BleepingComputer that when the executable is launched it will terminate or disable 1,396 different Windows services and processes. These processes include security software, database servers, mail servers, and backup software. A full list of disabled services and terminated processes can be found in Kremez's GitHub repository.

This termination process was previously done in a batch file, but is now integrated into the ransomware itself.

The ransomware will then begin to encrypt files on the victim's hard drives. When encrypting files, it will not encrypt any of the following types of files, file names, or files under listed folders.

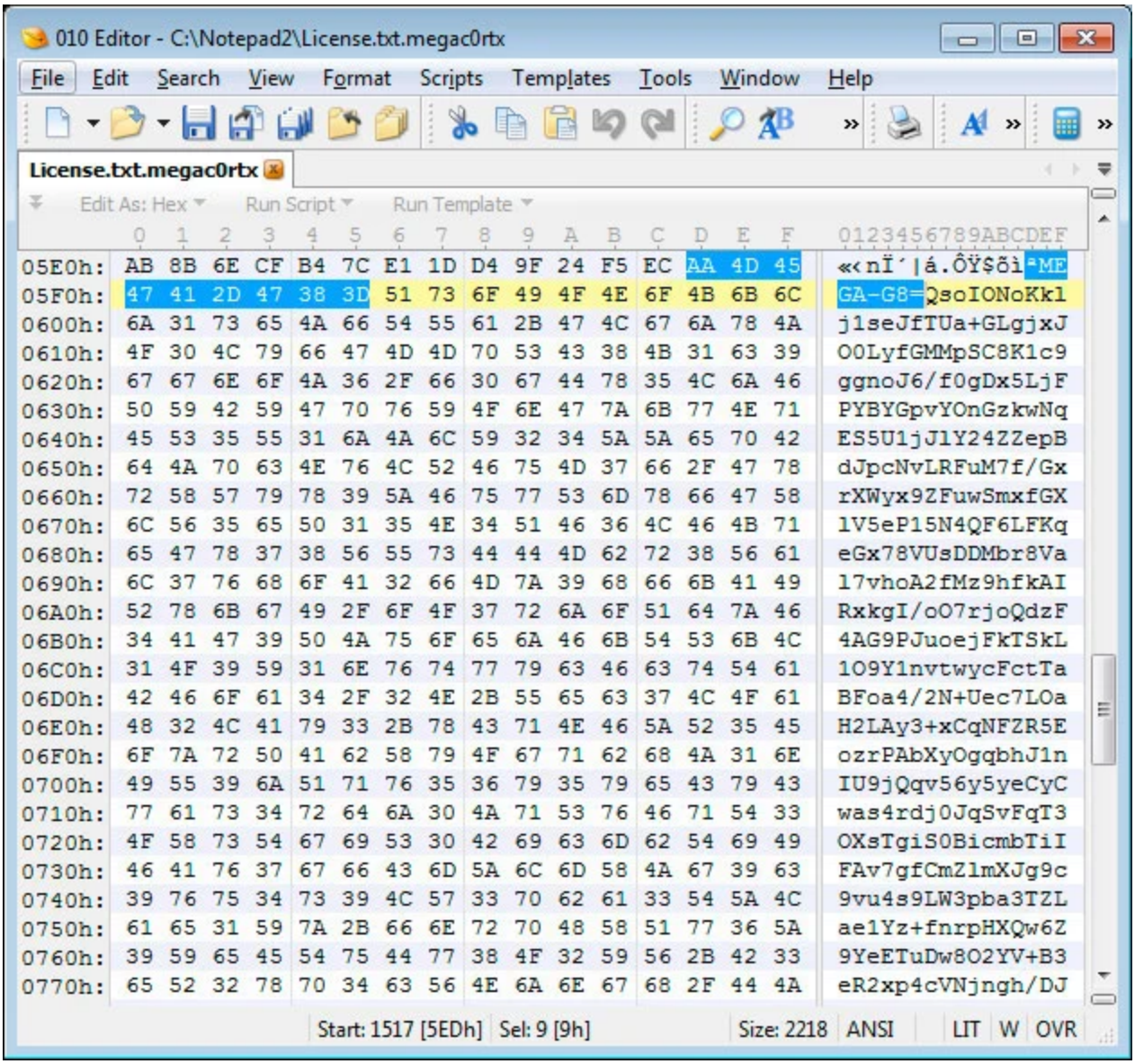
```
.dll
.exe
.sys
.mui
.tmp
.lnk
.config
.manifest
.tlb
.olb
.blf
.ico
.regtrans-ms
.devicemetadata-ms
.settingcontent-ms
.bat
.cmd
.ps1
desktop.ini
iconcache.db
ntuser.dat
ntuser.ini
ntuser.dat.log1
ntuser.dat.log2
usrclass.dat
usrclass.dat.log1
usrclass.dat.log2
bootmgr
bootnxt
temp\
.+\\Microsoft\\(User Account Pictures|Windows\\(Explorer|Caches)|Device
Stage\\Device|Windows)\\
```

As the ransomware encrypts a file it will append the **.megac0rtx** extension to the encrypted file's name. For example, test.jpg will be encrypted and renamed to test.jpg.megac0rtx.



Folder of MegaCortex Encrypted Files

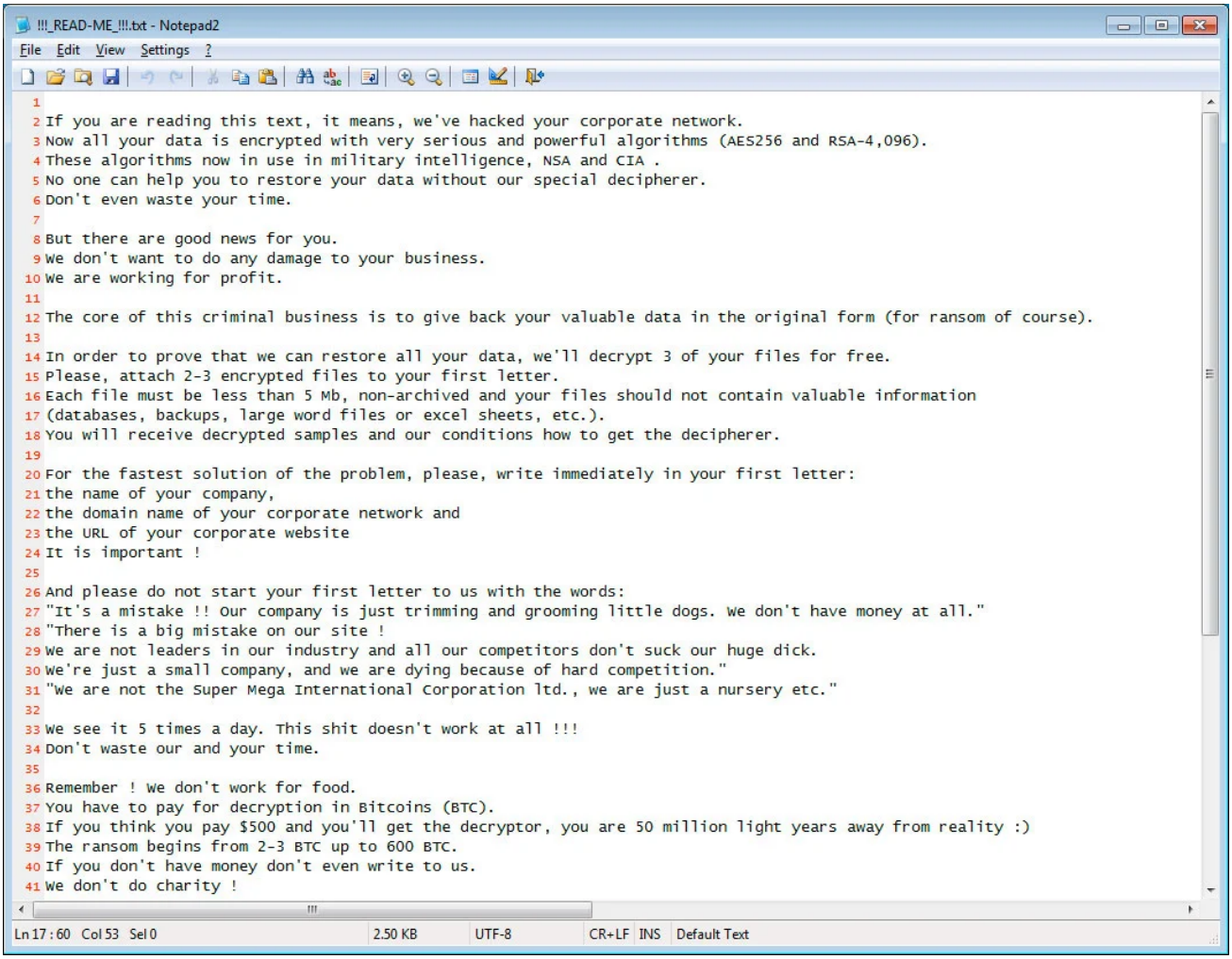
Each file that is encrypted, will also include the **MEGA-G8=** file marker as shown below.



File Marker in Encrypted Files

As its encrypting, the ransomware will also create a log file at **C:\x5gj5_gmG8.log** that will contain a list of files that could not be encrypted by the ransomware.

When done encrypting files the ransomware will create a ransom note named **!!!_READ-ME_!!!.txt** and save it on the victim's desktop. This ransom note contains emails that the victim can use to contact the attackers to find out payment instructions. The note states that ransom amounts range anywhere from 2-3 bitcoins to 600 BTC.



MegaCortex Ransom Note

During its execution, the ransomware will also delete Shadow Volume Copies using the `vssadmin delete shadows /all /for=C:\` command.

In addition, Kremez told BleepingComputer that there are references to the Windows `Cipher /W:` command, which is used to overwrite deleted data so that it cannot be recovered using file recovery software.

Now that a sample has been found, the ransomware's encryption algorithm will be analyzed by researchers for weaknesses. If anything new develops, we will update this article.

Ransom note may detract payments

We have seen a lot of ransom notes here at BleepingComputer and I can say that the language used in MegaCortex's is one of the most aggressive ones I have seen to date.

Most ransomware will try to walk a victim through the payment process and display almost sympathetic undertones to their requests. Instead, the MegaCortex ransom note goes the complete opposite direction.

They point blank say they do not negotiate, do not care about your hardships, and have no sympathy that they encrypted your files.

And please do not start your first letter to us with the words:
"It's a mistake !! Our company is just trimming and grooming little dogs. We don't have money at all."
"There is a big mistake on our site !
We are not leaders in our industry and all our competitors don't suck our huge **ck.
We're just ? small company, and we are dying because of hard competition."
"We are not the Super Mega International Corporation ltd., we are just a nursery etc."

We see it 5 times a day. This sh*t doesn't work at all !!!
Don't waste our and your time.

Remember ! We don't work for food.
You have to pay for decryption in Bitcoins (BTC).
If you think you pay $500 and you'll get the decryptor, you are 50 million light years away from reality :)
The ransom begins from 2-3 BTC up to 600 BTC.
If you don't have money don't even write to us.
We don't do charity !

Whether or not this tone will do the ransomware developer's any favors is hard to determine. What I do no know is that ransomware victims feel violated, hurt. and angry and this ransom note won't make them feel any better.

IOCs:

Hashes:

```
77ee63e36a52b5810d3a31e619ec2b8f5794450b563e95e4b446d5d3db4453b2
```

Associated Files:

```
winnit.exe
x5gj5_gmG8.log
payload.dll
!!!_READ-ME_!!!.txt
```

Ransom Note Text:

If you are reading this text, it means, we've hacked your corporate network.
Now all your data is encrypted with very serious and powerful algorithms (AES256 and RSA-4,096).
These algorithms now in use in military intelligence, NSA and CIA .
No one can help you to restore your data without our special decipherer.
Don't even waste your time.

But there are good news for you.
We don't want to do any damage to your business.
We are working for profit.

The core of this criminal business is to give back your valuable data in original form (for ransom of course).

In order to prove that we can restore all your data, we'll decrypt 3 of your files for free.
Please, attach 2-3 encrypted files to your first letter.
Each file must be less than 5 Mb, non-archived and your files should not contain valuable information
(databases, backups, large word files or excel sheets, etc.).
You will receive decrypted samples and our conditions how to get the decipherer.

For the fastest solution of the problem, please, write immediately in your first letter:
the name of your company,
the domain name of your corporate network and
the URL of your corporate website
It is important !

And please do not start your first letter to us with the words:
"It's a mistake !! Our company is just trimming and grooming little dogs. We don't have money at all."
"There is a big mistake on our site !
We are not leaders in our industry and all our competitors don't suck our huge **ck.
We're just ? small company, and we are dying because of hard competition."
"We are not the Super Mega International Corporation ltd., we are just a nursery etc."

We see it 5 times a day. This sh*t doesn't work at all !!!
Don't waste our and your time.

Remember ! We don't work for food.
You have to pay for decryption in Bitcoins (BTC).
If you think you pay $500 and you'll get the decryptor, you are 50 million light years away from reality :)
The ransom begins from 2-3 BTC up to 600 BTC.
If you don't have money don't even write to us.
We don't do charity !

One more time :

1.(In first letter) write the name of your company, the domain name of your corporate network and the URL of your corporate website
2. Attach 2-3 encrypted files (we'll show you some magic)
3. Use Google in order to find out how to buy bitcoins fast

```
As soon as we get bitcoins you'll get all your decrypted data back.

Contact emails:
MckinnisKamariyah91@mail.com
or
ThomassenVallen1999@mail.com

Man is the master of everything and decides everything.
```

Associated Email addresses:

```
MckinnisKamariyah91@mail.com
ThomassenVallen1999@mail.com
```

- Enterprise
- MegaCortex
- 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

You may also like: