certTonga

Tonga National Computer
Emergency Response
Team

Viro Botnet Ransomware

Dear Constituents,

The Viro Botnet Ransomware (also seen as Virii Ransomware) is a file cryptor program developed by threat actors who are believed to be based in France. Samples of the Viro Botnet Ransomware were submitted for analysis online on September 15th, 2018 and appear to feature a ransom message written in French. The Viro Botnet Ransomware is packed as an encryption Trojan that is based on the HiddenTear open-source Ransomware. The Viro Botnet Ransomware is known to run as 'Office Updater.exe' on compromised systems and attempt to use the Outlook email solution by Microsoft with the aim to infect saved contacts on the user's PC.

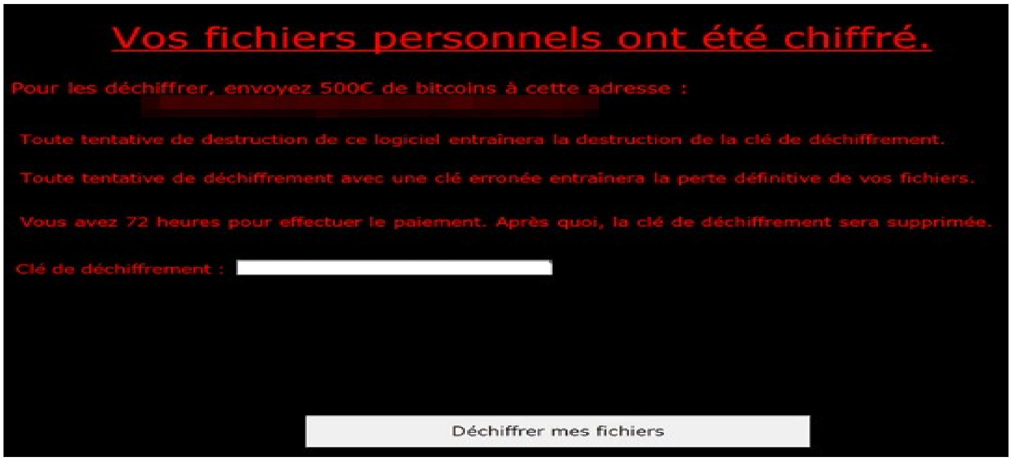
How it works

1. Once, the file named “Ransom_VIBOROT.THIAHAH” is installed on system, it directly goes for checking registry keys, to see whether the system is encrypted or not.

2. After this, it creates an encryption and decryption key with cryptographic Random Number Generator. As soon as the key is generated, Viro botnet starts gathering information from system and simultaneously keeps sending the data to its host server through POST.

3. Following to which, it begins with encryption process via RSA encryption technique.

4. Once, the system is encrypted, it shows a ransom message, which is written in French.



Vos fichiers personnels ont été chiffré.

Pour les déchiffrer, envoyez 500C de bitcoins à cette adresse :

[redacted]

Toute tentative de destruction de ce logiciel entrainera la destruction de la clé de déchiffrement.

Toute tentative de déchiffrement avec une clé erronée entrainera la perte définitive de vos fichiers.

Vous avez 72 heures pour effectuer le paiement. Après quoi, la clé de déchiffrement sera supprimée.

Clé de déchiffrement :

1. Viro Botnet comes in a file name “Ransom_VIBOROT.THIAHAH” with .exe extension. This botnet gathers information from registries, and directly attacks machine GUID for it.

2. It collects:

- Machine GUID
- Machine name
- User name
- Other details

3. For sending and receiving information, it redirects and connects system to website with URL “http://viro.m{BLOCKED}ier.fr”, which is hosted by attacker’s server. It can also redirect users to other malicious websites as well, which are:

- hxxps://viro(.)mleydier(.)fr
- hxxps://viro(.)mleydier(.)fr/noauth/order/
- hxxps://viro(.)mleydier(.)fr/noauth/keys/
- hxxps://viro(.)mleydier(.)fr/noauth/attachment/
- hxxps://viro(.)mleydier(.)fr/noauth/attachment/

4. This ransomware is capable of doing lots of other things as well, which are:

- Downloads and executes a file
- Propagate
- Log Keystrokes
- Makes the infected system imitate as a Botnet to send spam emails
- Can encrypt files in fixed, removable and network drives
- Once, the files are encrypted, it shows a message with the ransom text written in French

5. Viro Botnet can encrypt files with the following extensions:

.asp, .aspx, .csv, .doc, .docx, .html, .jpg, .mdb, .odt, .odt, .pdf, .php, .png, .ppt, .pptx, .psd, .sln, .sql, .swp, .txt , .xls, .xlsx, .xml

6. Viro Botnet can also be present with alias name, that is “HEUR:Trojan.Win32.Generic”. It is currently active in United States and is only targeting Windows users for now.

What to do

1. Keep applications and operating systems running at the current released patch level
2. Ensure anti-virus software and associated files are up to date
3. Verify, through a separate channel, the legitimacy of any unsolicited email attachments - delete without opening if you can not validate
4. Search for existing signs of the indicated IOCs in your environment
5. Block all URL and IP based IoCs at the firewall, IDS, web gateways, routers or other perimeter-based devices

Reference

https://blog.trendmicro.com/trendlabs-security-intelligence/virobot-ransomware-with-botnet-capability-breaks-through/

https://exchange.xforce.ibmcloud.com/collection/Viro-Botnet-Ransomware-dfb236340e7f5a7e55c6434f056ebcc2

Please for more information you can contact us:

Tonga National CERT

Ministry of MEIDECC
OG Sanft Building Level 2
Nuku'alofa
Tel: 2378 (CERT)
email: report@cert.to
web: www.cert.to

Disclaimer Notice:
The information in this notice is intended solely for public knowledge and awareness, and not intending to harm, fright or disturb any person(s), legal entity or the receiver of this information. Under no circumstances shall the Ministry of MEIDECC be liable for any indirect, incidental, consequential, special or exemplary damages arising out of or in connection with your access or use of or inability to access or use the information and any third party content and services.