MegaCortex Version 4

Summary: MegaCortex Version 4 is the latest version of the ransomware first detected on 11/04/19. Version 4 is a modification of the version 2 where the malware contain the key embedded into the loader, and the ransomware contain two components, loader and main module. Version 4 has a few significant changes in the ransomware. The ransomware separate the encryption code into their own module (Payload 1 & 2), in addition, the ransomware also change the style of ransom notes where once the ransomware change the user’s password, the ransomware log the user off and display the ransom notes in the Logon’s screen.

**Signatures:**

File Access:

* C:\\qibfmqkeM5.log
* C:\.log
* C:\Windows\temp\qibfmqkeM5-0.cmd
* C:\Windows\temp\qibfmqkeM5-1.cmd
* C:\Windows\temp\qibfmqkeM5-2.cmd

Processes:

* Net user [username] [random\_password]

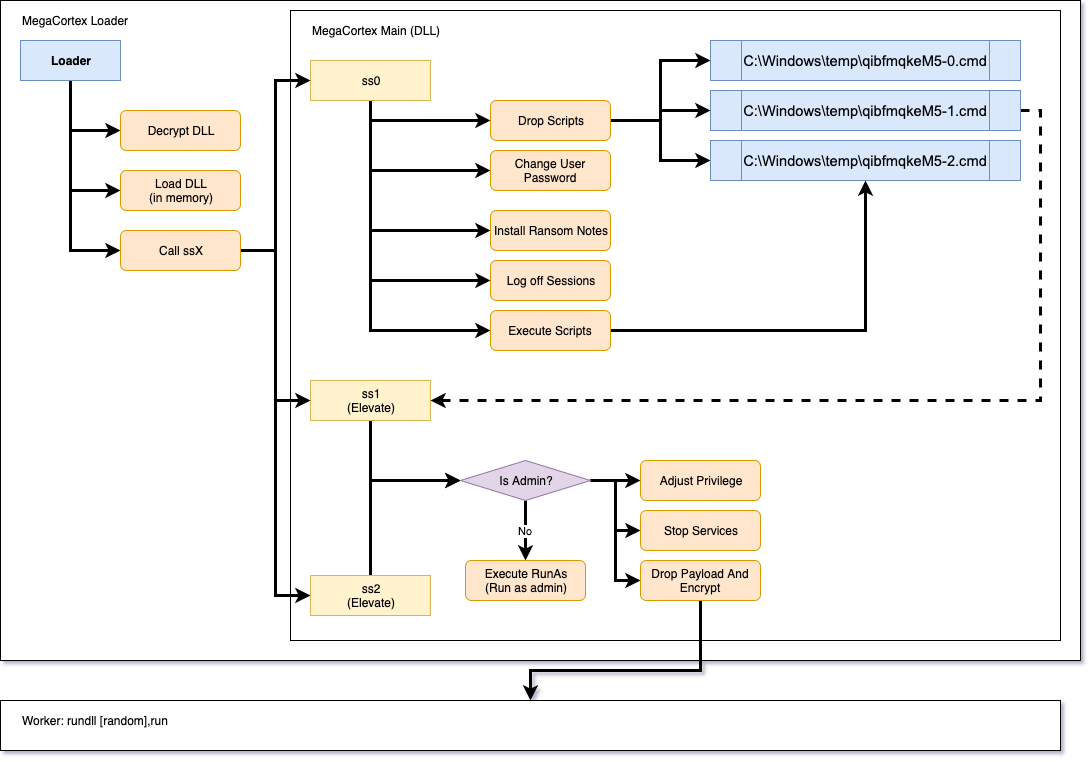
Registry:

* HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\legalnoticecaption=”Locked By MegaCortex”

**Malware Analysis:**

**Overview:**

Summary: MegaCortex Version 4 is the latest version of the ransomware first detected on 11/04/19. Version 4 is a modification of the version 2 where the malware contain the key embedded into the loader, and the ransomware contain two components, loader and main module. Version 4 has a few significant changes in the ransomware. The ransomware separate the encryption code into their own module (Payload 1 & 2), in addition, the ransomware also change the style of ransom notes where once the ransomware change the user’s password, the ransomware log the user off and display the ransom notes in the Logon’s screen. Below are the overview of MegaCortex Version 4.



**File Information:**

**Loader**:

MD5: 174b579b9577253b29269d6ceb289156

SHA256: ca0d1e770ca8b36f6945a707be7ff1588c3df2fd47031aa471792a1480b8dd53

File Type: Win32 Executable

VT: <https://www.virustotal.com/gui/file/ca0d1e770ca8b36f6945a707be7ff1588c3df2fd47031aa471792a1480b8dd53/details>

**Main Module**:

MD5: eb31747adbf69fda5930874e3b39a44d

SHA-256: efee6ffa542bd3db168cb810b68a547e9b298471a29ff57b63c7cb5a648452a5

File Type: Win32 DLL

**Payload 1:**

MD5: 68e0d3f36228240b95bdcd363f254231

SHA256: e362d6217aff55572dc79158fae0ac729f52c1fc5356af4612890b9bd84fbcde

File Type: Win32 DLL

**Payload 2:**

MD5: 3c38cfce20262b064070e30fd99b9406

SHA256: 5ff14746232a1d17e44c7d095e2ec15ede4bd01f35ae72cc36c2596274327af9

File Type: Win32 DLL

Decryption Key:

* /tTOwekJG0kQaKVAu1y4O8yhwZ8i0PImZ9apFajLFlY=

**Loading Method:**

Once the loader is executed, the loader would decrypt the malware and execute the payload in memory. The function get executed are based on the arugment provided to the loader. Version 4 loader can be executes with three options. Below are the possible arguments.

* No argument - the loader execute “ss0” function in the main payload.
* + - the loader execute “ss1” function in the main payload.
* - - the loader execute “ss2” function in the main payload.

cmd:> Loader [+|-]

**Drop Scripts:**

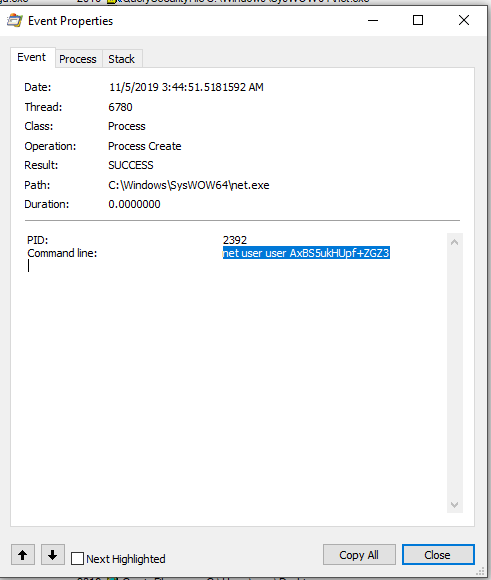
Once execute, the malware drop three script into the Windows temporary directory. Below are the list of file.

* C:\Windows\temp\qibfmqkeM5-0.cmd
* C:\Windows\temp\qibfmqkeM5-1.cmd
* C:\Windows\temp\qibfmqkeM5-2.cmd

**File Extensions:**

* m3gac0rtx

**Change User Password:**

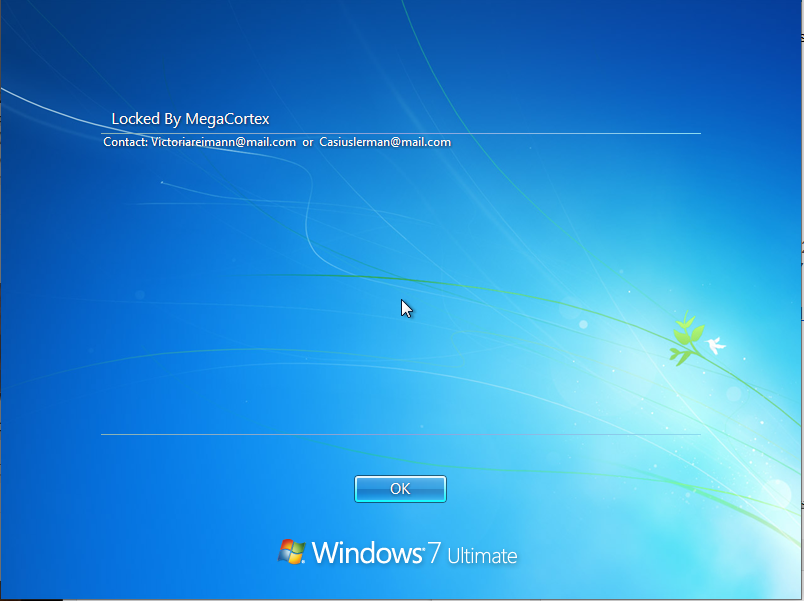


Ransom Notes:

The malware modify the login screen with the following commands.

* reg add HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System /f /t REG\_SZ /v legalnoticetext /d "Contact:
* reg add HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System /f /t REG\_SZ /v legalnoticecaption /d "Locked By MegaCortex"

Once the malware encrypt the files, the malware log the user off and display the ransom notes in the log in screen.



The following email address of the actor:

* [Victoriareimann@mail.com](mailto:Victoriareimann@mail.com)
* Casiuslerman@mail.com