**Incident Report:** CH-15101-Challenge-Ransomware-Attack

**Date:** 10-25-2022

**Executive Summary:**

The main computer at the local General Dentist office was infected with Jigsaw Ransomware, a malicious program written in .NET that uses AES encryption on locally-stored data and begins deleting files if Bitcoin payment is not received within one hour of installation.

**Initial Observations:**

* The desktop screen displays a persistent pop-up with scrolling text, a countdown clock, and an image of the puppet from the “Saw” movie series.
* The ransom note gives information about where the victim can access Bitcoin currency (localbitcoin), the attacker’s Bitcoin wallet address, and a link to click once Bitcoin payment has been secured.
* There is also a link to view the files that have been encrypted:
  + Clicking on this link leads to another pop-up window with a list of locally-stored files across all folders within the device directory.
  + Files of varying types appear to be infected, including .doc, .pdf, .xml, .ppt, .png, etc.
* Moving the pop-up screen window down with the mouse reveals several files stored on the desktop, all of which have had their file extensions appended to .fun.
* When the timer on the pop-up runs out, the ransomware will delete a certain amount of files depending on how many times the counter has run (i.e. how many hours have passed). Each time it resets, a greater number of files are deleted.
* Restarting the computer also restarts the timer, and 1,000 files are deleted as punishment.

**Attack Analysis:**

In order to study this program further, a copy of its executable was run in a Windows 10 virtual environment using the following analysis tools:

* PeStudio
* dotPeek
* Regshot
* Process Hacker
* Wireshark

**Static Analysis:**

* MD5: 2773e3dc59472296cb0024ba7715a64e
* SHA-1: 27d99fbca067f478bb91cdbcb92f13a828b00859
* SHA256: 3ae96f73d805e1d3995253db4d910300d8442ea603737a1428b613061e7f61e7
* File-type: 64-bit .NET EXE
* Configuration details:
  + Encrypted file extension: .fun
  + Maximum size of files it can encrypt: 10000000 bytes
  + Encryption password: “OoIsAwwF23cICQoLDA0ODe==”
    - Uses 192-bit encryption

**Dynamic Analysis:**

* Gets and sets %AppData% path upon execution
* Replicates into two executables:
  + drpbx.exe
  + firefox.exe
* Associated file paths:
  + %AppData$\Roaming\Frfx\firefox.exe
  + AppData\Local\Drpbx\drpbx.exe
* Persists on Startup and reboots:
  + HKCU\Software\Microsoft\Windows\CurrentVersion\Run firefox.exe=C:\Users\admin.admin-PC\AppData\Roaming\Frfx\firefox.exe
* Queries when payment link is clicked: <http://btc.blockr.io/>
  + API call to the Bitcoin address to check if payment has been received
  + If received → Decryption code sent

**Attack Narrative:**

Also known as BitcoinBlackmailer, Jigsaw Ransomware uses spam email or internet adware as an attack vector on devices running Windows OS. The malicious attachment includes an installer that will activate once the file is opened. Once executed, the payload replicates itself into two different .exe files, each taking the name of commonly-used applications so as to deceive users (firefox.exe and drpbx.exe). A launching command is also executed to ensure its persistence on Startup and reboot.

192-bit AES Encryption of files stored on the infected device occurs as soon as the program has been installed. This ransomware does not move laterally, limiting the scope of the encrypted data to the computer on which it was installed.

A ransom note appears on screen via a pop-up window once the encryption process has been completed. The note contains scrolling instructions to deliver a bitcoin payment of $150 to an identified Bitcoin address within the next hour or files will begin to be deleted. It then threatens to perform additional file deletions every hour at an increasing rate for up to 72 hours, at which point the computer will be wiped entirely.

Encrypted files contain the .fun file extension. A running log of the files being deleted is available to view by accessing the associated link on the ransom note pop-up.

**Resolution:**

The malicious executables (firefox.exe and drpbx.exe) are viewable processes within the Task Manager of the infected device. Terminating them will remove the pop-up window and stop the ransomware from running. Running msconfig and disabling firefox.exe will ensure that the ransomware does not run again on Startup.

To decrypt compromised files, download and run the open-source Jigsaw Decrypter on the infected device.