CERT-MU Security Alert

CERT-MU

KeRanger – First Ransomware to Target Mac OS X Operating System

Original Issue Date: 08th March, 2016

Severity Rating: High

Systems Affected: Mac OS X

Description:

The KeRanger malware appears to be the first ransomware to target the Mac OS X operating system. KeRanger (OSX.Keranger) was briefly distributed in a compromised version of the installer for the Transmission BitTorrent client. Mac OS X users who downloaded Transmission on March 4 and March 5 2016 may be at risk of being compromised.

KeRanger was signed with a valid Mac Developer ID, which meant that the malware could bypass OS X's Gatekeeper feature, which is designed to block software from untrusted sources. Apple has since revoked the Developer ID used by KeRanger.

Impact of the attack

The KeRanger malware is designed for Mac OS X, its behavior is quite similar to Windows-based ransomware, particularly TeslaCrypt (Trojan.Cryptolocker.N). Once installed, KeRanger will search for approximately 300 different file types and encrypt any it finds. The malware will then display a ransom message, demanding that the victim pay 1 bitcoin (approximately US$408). Payment is made using a website on the anonymous Tor network.

Is your Mac infected?

If you downloaded version 2.90 of Transmission from the open-source project's website then you could be infected.

What to Do if KeRanger Encrypts Your Mac

If your Mac is encrypted, your best option is restore the Mac hard drive from a Time Machine backup.

Recommendations

- Regularly back up any files stored on your computer. If your computer does become infected with ransomware, your files can be restored once the malware has been removed.

- Always keep your security software up to date to protect yourself against any new variants of malware.

- Keep your operating system and other software updated. Software updates will frequently include patches for newly discovered security vulnerabilities that could be exploited by attackers.
- Delete any suspicious-looking emails you receive, especially if they contain links or attachments.

- Be extremely wary of any Microsoft Office email attachment that advises you to enable macros to view its content. Unless you are absolutely sure that this is a genuine email from a trusted source, do not enable macros and instead immediately delete the email.

Please note that the members who do not want to receive the security alert, they can unsubscribe from CERT-MU mailing list by sending an e-mail to the following address: unsubscribe@cert.ncb.mu

For more information please contact CERT-MU team on:

Hotline No: (+230) 800 2378
Fax No: (+230) 208 0119
Gen. Info. : contact@cert.ncb.mu
Incident: incident@cert.ncb.mu
Website: http://cert-mu.org.mu