ICIT | Institute for Critical Infrastructure Technology

Cerber & KeRanger: The Latest Examples of Weaponized Encryption

Authors:

James Scott, Sr Fellow at the Institute for Critical Infrastructure Technology

Drew Spaniel, Visiting Scholar, Carnegie Mellon University

Copyright 2016 – Institute for Critical Infrastructure Technology (ICIT)

Contents

Copyright 2016 – Institute for Critical Infrastructure Technology (ICIT)

Introduction:

Ransomware is an unsophisticated cyber-attack vector that weaponizes encryption algorithms against the systems belonging to unsuspecting victims, in an attempt to extort a payment in exchange for safe return of the victim's data, files, and systems. Ransomware succeeds when either the attackers successfully pressures the victim into paying the ransom or when the victim fails to mitigate the risk by not creating a system backup and therefore has no option to recover the file other than to pay the ransom. The sheer lack of cybersecurity hygiene makes the American population easy targets in this ever-evolving threat landscape. Kaspersky, Trend Micro, Forcepoint, Securonix, Covenant Security Solutions, GRA Quantum, and numerous other information security firms predicted that ransomware attacks would significantly increase in 2016 and they were correct. By March 2016, the media covered at least one major ransomware attack every few days. ICIT addressed the rising threat of ransomware in our March 2016 publication, "The ICIT Ransomware Report: 2016 Will Be the Year Ransomware Holds America Hostage." Afterward, two new variants of ransomware, Cerber and KeRanger, began attacking Windows and Mac hosts respectively. This report analyzes these groups with the intent of informing readers and anticipating potential evolution of the ransomware form.

Cerber:

The Cerber ransomware surfaced from Russian underground malware forums around March 4, 2016. Cerber exhibits characteristics of a Ransomware as a Service tool, in which a sophisticated malware developer outsources deployment of their tool for a commission of each paid ransom, to less sophisticated, but more numerous attackers. Though Cerber's distribution vector is not yet known, RaaS is often distributed through botnets, spam email, and drive-by-downloads.

When the downloader executes, the malware identifies the victim's country of origin (by IP Geolocation). If the victim host is located in one of 12 former soviet nations (Armenia, Azerbaijan, Belarus, Georgia, Kyrgyzstan, Kazakhstan, Moldova, Russia, Turkmenistan, Tajikistan, Ukraine, or Uzbekistan) then the malware terminates itself and will not encrypt data on the computer. Otherwise, Cerber installs itself in %AppData%\{2ED2A2FE-872C-D4A0-17AC-E301404F1CBA}\ folder and names itself after a random Windows executable. The malware configures Windows to automatically boot into Safe Mode with Networking on the next reboot. Cerber configures itself to start automatically when the user logs into Windows, to execute as the screensaver when the system is idle, and to set a task to execute itself every minute to display fake system alerts until the computer is restarted. The system will reboot into Safe Mode with Networking (for a yet unknown reason) and will then shut down and reboot

Copyright 2016 – Institute for Critical Infrastructure Technology (ICIT)

again in normal mode. The ransomware will execute at login and begin encrypting the victim's files.

Cerber uses a JSON configuration file to determine what extensions to target, what nationalities of victims to not target, what files and folders to leave unencrypted, and other configuration information. Cerber will ignore files namd bootsect.bak, iconcache.db, thumbs.db, or wallet.dat, along with other select file paths. Cerber scans the victim's connected drives for files matching certain file extensions, encrypts each file using AES-256 encryption, encrypts the file name, and appends the .CERBER extension to it. For example, according to security researcher Lawrence Abrams, test.doc might become Zu0ITC4HoQ.cerber after encryption. Cerber has the capability to scan and enumerate unmapped Windows shared networks as well and spread onto those machines; however the feature is disabled in samples discovered in circulation.

To ensure that the victim receives the ransom demand, the malware generates three ransom notes (# DECRYPT MY FILES #.html, # DECRYPT MY FILES #.txt, and # DECRYPT MY FILES #.vbs) on the victim desktop and in every folder that is encrypted. The VBS file causes the computer to repeatedly speak a message out load notifying the victim that their data is encrypted. The vocal reminder intensifies the implementation of anxiety necessary to influence human emotion, thus in many cases prompting a quicker pay cycle. Ransomware is less about technical savvy and more about emotional manipulation. Further, it means that even if somehow the malware does not encrypt all of its target files, the victim may still be inconvenienced into paying the ransom by the relentless reminders (unless every VBS file is removed). The files contain notification about the attack and instructions to access Tor to make a payment to retrieve the decryptor. Each note ends with "Quod me non necat me fortiorem facit"/ "That which does not kill me makes me stronger." Inclusion of this tag and the incessant vocal reminder that files are encrypted could indicate that the developer lacks a level of maturity found in other cyber-criminals because the two actions could be perceived as gloating or chiding the victim.

Victims are asked to follow a link (for example: decrypttozxybarc.onion) to a Tor site that acts as the payment and decryption service. The site is available in 12 languages. After selecting a language, victims are asked to enter a capcha, and are then directed to an information page that lists the ransom amount of 1.24 bitcoins (~$500), information on how to pay the ransom, and a warning that the ransom will double within 7 days if left unpaid. Each victim payment can be seen in a Payment History section. Once the full ransom has been paid, the victim will receive a download link for a decryptor unique to their system and files. Aside from restoring files from a backup, there is no way to recover files encrypted by Cerber other than by paying the ransom.

Copyright 2016 – Institute for Critical Infrastructure Technology (ICIT)

KeRanger:

On March 4, 2016, Palo Alto Networks discovered that the Transmission 2.90 BitTorrent installer for OS X was infected with the KeRanger ransomware. Transmission is an open source BitTorrent client. Attackers infected two Transmission 2.90 installers with infected DMG files in hopes that users would infect their own systems by installing the program from the official website. . Around 6,500 systems were infected with the ransomware between 11:00 am PST, March 4, 2016 and before 7:00pm PST, March 5, 2016. According to Transmission representative John Clay, the ransomware was added to the disk-image of the software after cyber-attackers compromised a Transmission's main server. Security on the server has increased since the incident was discovered.

Apple protects its OS X systems with the Gatekeeper security feature. User application installations are restricted to reduce the likelihood that malware will inadvertently be installed and executed on the machine. The malicious Transmission installers used a valid Apple Developer certificate to bypass the OS X gatekeeper feature. The certificate belonged to POLISAN BOYA SANAYI VE TICARET ANONIM SIRKETI (a Turkish company) with the ID Z7276PX673, which differed from the certificate used on earlier versions of Transmission. The installers were generated and signed on March 4, 2016. They included the traditional Transmission installers, along with an extra file named General.rtf in the Transmission.app/Contents/Resources directory. The code in General.rtf reveals that its main function is to encrypt and ransom user data. While the icon of General.rtf masqueraded as a RTF file, it was actually a Mach-O format executable file packed with UPX 3.91. When users ran the installer, this file would be copied to their ~/Library/kernel_services directory, where it execute as "kernel_service." After the infected application was installed, it ran an embedded executable on the host system to install KeRanger. Upon its initial execution, three files, "kernel_pid", "kernel_time", and "kernel_complete" are created under the ~/Library directory. The current time is written to "kernel_time" and a sleep timer is set to three days. The ransomware is configured to wait three days before contacting its command and control infrastructure over the Tor anonymizer network. Palo Alto Networks notes that while this variant sleeps for the full three days, a different sample of KeRanger made requests to the C2 servers every five minutes during this time. The malware collects the host's model name, and UUID and uploads the information to a C2 server. The servers' domains are all sub-domains of onion[.]link or onion[.]nu, which are only accessible via the Tor network. The malware keeps attempting to connect until the server responds with two lines of encrypted data. The malware decodes these two lines, an RSA public key and a line of text written to "README_FOR_DECRYPT.txt", lines using Base64.

After contact is made, an encryption key is sent and the malware begins encrypting specific file types on the host system. The malware uses a statically linked open source

Copyright 2016 – Institute for Critical Infrastructure Technology (ICIT)

encryption library called mbed TLS (formerly Polar SSL) to encrypt files corresponding to 300 different file extensions found under the /Users and /Volumes directories on the host system. KeRanger begins by creating an encrypted version of each file that appends the .encrypted file extension onto the file name. For example, an encrypted file, test.doc, would become test.doc.encrypted. KeRanger encrypt each file by generating a random number (RN) and encrypting the RN with the RSA key. It then stores the encrypted RN at the beginning of the resulting file. Next, it generates an initialization vecor (IV) using the file's original contents and stores the IV in the resulting file. The RN and the IV are combined to generate an AES encryption key, which is then used on the contents of the target file and written to the encrypted file. Additionally, developmental features (functions named "_creare_tcp_socket", "_execute_cmd", and "_encrypt_timemachine") in the malware suggest that it also tries to encrypt Time Machine backup files so that users cannot simply avoid the ransom demand by restoring from a back-up point. The victim then receives a ransom demand of 1 Bitcoin (~$420) in order to recover their files. A link in the ransom demand guides victims on how and where to purchase bitcoins, while a separate section directs them to an address (for example "1PGAUBqHNcwSHYKnpHgzCrPkyxNxvsmEof") to make the payment. Victims attempting to pay the ransom are taken to a page to enter their assigned bitcoin address. After the address is entered, the victim is taken to a page that contains a list of the support requests that were created by the victim. At the top of every page on the payment site is the option to decrypt one file, of the victim's choice, for free, a reminder of the ransom amount, how much has been paid already, and the bitcoin address to which payments should be forwarded. According to security researcher Lawrence Abrams, the decryption feature is currently non-operational. Victims can also navigate to an FAQ about bitcoins and how to pay the ransom. In the event that the victim pays, a "Download Decryption Pack" button on the page will be enabled so that they can download a decryptor tool unique to their system and files.

In response to the incident, Apple revoked abused certificates on March 4, 2016 and Gatekeeper now blocks the malicious installers. Additionally, Apple updated the XProtect signatures on all Mac computers to recognize the known variants. If a user tries to open an infected version of Transmission, a warning dialog stating that "Transmission.app will damage your computer. You should move it to the Trash." or "Transmission can't be opened. You should eject the disk image." will be displayed. On March 5, 2016, Transmission removed the malicious installers from the website. Users who downloaded Transmission from the official website after 11:00 am PST, March 4, 2016 and before 7:00pm PST, March 5, 2016 may be infected with the KeRanger ransomware. Users could also be infected by downloading Transmission from third party websites. Users of older versions of Transmission were unaffected by the incident. Transmission has since increased security on its servers and released two updated versions of the Transmission application. The former, version 2.91 is a clean installation of the application and has since been replaced by version 2.92, which also removes the KeRanger malware.

Copyright 2016 – Institute for Critical Infrastructure Technology (ICIT)

Palo Alto Networks suggests that potential victims check their systems and remove the malware if infected. Indicators of compromise include detecting the General.rtf file, detecting a running “kernel_service”, or detecting “kernel_pid”, “kernel_time”, “kernel_comple”, or “kernel_service” in the ~/Library directory. General.rtf can be detected by running a search of /Applications/Transmission.app/Contents/Resources/ General.rtf or /Volumes/Transmission/Transmission.app/Contents/Resources/ General.rtf in Terminal or Finder. If either file is detected, then Transmission is infected and will need to be deleted. The “kernel_service” can be detected by checking the Activity Monitor preinstalled in OS X. If the service is running, the user should navigate to “OpenFiles and Ports”, checking whether there is a file name “/Users/<username>/Library/kernel_service”, and terminating it with “Quit->Force Quit”. Finally, if any of the files exist in the ~/Library directory, they should be deleted. In the event that a system is already infected, Lawrence Abrams has created a tool that quarantines the files associated with the KeRanger infection and creates a list of encrypted files. The tool does not decrypt the files. At this time, the only ways to recover encrypted files is by restoring the system from a backup or by paying the ransom.

Conclusion:

The optimal solution to preventing ransomware, and all malware, infections for individuals and organizations alike is to anticipate an attack and to prepare accordingly by practicing good cyber hygiene. Systems and critical data should be regularly backed up on external and redundancy systems to prevent ever having to pay a ransom demand. Ransomware is only a valid attack vector because some percentage of victims inevitably pay. If society improves its cyber-hygiene to prevent infections or to remediate the consequences without engaging with the attackers, then the effectiveness and profitability of the attack vector will decrease. According to the theory of broken windows, as fewer attacks result in profitable outcomes, fewer attackers will enter the market.

Ransomware is less sophisticated than most malware. Instead of spreading through complex attack vectors, it typically spreads through the exploitation of human nature. Users need to learn how to recognize and ignore malicious emails, how to avoid suspicious websites, and how to recognize suspicious activity on the network and engage qualified information security personnel. After users are made dependable, the network can be supported with technical controls such as white-listed firewalls, IDS/IPS, UBA, and other hardware and software solutions. Only trusted software and services should be downloaded onto a system. Finally, it is critical for users and security professionals to observe evolutions in the tools that attackers develop and to anticipate a mitigation strategy.

The Cerber ransomware is similar to other ransomware in operation and function; however, it is peculiar in its adoption of text-to-speech as a means of coercing victims to pay the

Copyright 2016 – Institute for Critical Infrastructure Technology (ICIT)

ransom. A device squawking that you made a mistake and that you need to take immediate action instills a 'setting off the car alarm' type of anxiety and stress. Imagine if Cerber evolved to infect other Windows or even Linux based devices. For example, how many phone users would pay a low fee, say $0.99, to cease their phone from emitting a blusterous "your files have been infected message"? Security vendors need to begin thinking about mobile and IoT security solutions that prevent ransomware infections and that prevent exploitation of this feature to deter the evolution of this vector.

Similarly, the KeRanger ransomware grabbed the media attention because it is one of the first ransomware to target Mac systems and it may be the first to succeed in infecting Mac hosts. The misconception made by the public is that Mac systems are in any way more secure from malware threats than Windows systems. They are not. Apple does some wonderful things, such as Gatekeeper and XProtector, to deter malware campaigns, but ultimately, if an attacker dedicated enough resources to targeting these devices, they would succeed. Macs are targeted less because it is more profitable for attackers to target Windows hosts because Microsoft has a larger market segment for personal computers than Apple. However, as the Windows attack surface saturates and as more users switch to Mac, attackers will inevitably begin developing malware to specifically target Apple products. KeRanger is one of the first, but it will not be the last. Because the iPhone is the leading mobile device, mobile malware and ransomware targeting Apple products will probably popularize before other variants. If the KeRanger attack infected 6,500 systems in a day, by infecting only a moderately popular torrenting client and only infecting novel downloads, imagine how many systems could be infected if a the same style attack succeeded on a popular mobile application such as Facebook, Tinder, etc. Organizations, users, and security vendors must begin to anticipate these attacks by practicing exceptional cyber-hygiene and by developing comprehensive solutions before the threats emerge. Great cybersecurity is not accomplished through empty kneejerk reactions to the latest breach. There will always be a 'latest threat' via a new and creative attack vector. The only true and meaningful way to thwart ongoing threats is with a cultural renaissance focused on cybersecurity hygiene. This starts with education, compounded by technologically evolving layers of detection and response strategies.

Copyright 2016 – Institute for Critical Infrastructure Technology (ICIT)

Cerber Technical Details:

Indicators of Compromise:
Files associated with Cerber Ransomware:

HKCU\Control Panel\Desktop\SCRNSAVE.EXE "%AppData%\{2ED2A2FE-872C-D4A0-17AC-E301404F1CBA}\[random].exe"

HKCU\Software\Microsoft\Command Processor\AutoRun "%AppData%\{2ED2A2FE-872C-D4A0-17AC-E301404F1CBA}\[random].exe"

HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\Run
"%AppData%\{2ED2A2FE-872C-D4A0-17AC-E301404F1CBA}\[random].exe"

HKCU\Software\Microsoft\Windows\CurrentVersion\Run\[random]
"%AppData%\{2ED2A2FE-872C-D4A0-17AC-E301404F1CBA}\[random].exe"

HKCU\Software\Microsoft\Windows\CurrentVersion\RunOnce\[random]
"%AppData%\{2ED2A2FE-872C-D4A0-17AC-E301404F1CBA}\[random].exe"

Registry Entries Associated with Cerber Ransomware:
"%AppData%\{2ED2A2FE-872C-D4A0-17AC-E301404F1CBA}\[random].exe"

Files and File Paths Skipped by Cerber:
bootsect.bak

concache.db

thumbs.db

wallet.dat

:\$recycle.bin\

:\$windows.~bt\

:\boot\

Copyright 2016 – Institute for Critical Infrastructure Technology (ICIT)

:\drivers\

:\program files\

:\program files (x86)\

:\programdata\

:\users\all users\

:\windows\

\appdata\local\

\appdata\locallow\

\appdata\roaming\

\public\music\sample music\

\public\pictures\sample pictures\

\public\videos\sample videos\

\tor browser\

Targeted File Extensions:

.contact, .dbx, .doc, .docx, .jnt, .jpg, .mapimail, .msg, .oab, .ods, .pdf, .pps, .ppsm, .ppt, .pptm, .prf, .pst, .rar, .rtf, .txt, .wab, .xls, .xlsx, .xml, .zip, .1cd, .3ds, .3g2, .3gp, .7z, .7zip, .accdb, .aoi, .asf, .asp, .aspx, .asx, .avi, .bak, .cer, .cfg, .class, .config, .css, .csv, .db, .dds, .dwg, .dxf, .flf, .flv, .html, .idx, .js, .key, .kwm, .laccdb, .ldf, .lit, .m3u, .mbx, .md, .mdf, .mid, .mlb, .mov, .mp3, .mp4, .mpg, .obj, .odt, .pages, .php, .psd, .pwm, .rm, .safe, .sav, .save, .sql, .srt, .swf, .thm, .vob, .wav, .wma, .wmv, .xlsb, .3dm, .aac, .ai, .arw, .c, .cdr, .cls, .cpi, .cpp, .cs, .db3, .docm, .dot, .dotm, .dotx, .drw, .dxb, .eps, .fla, .flac, .fxg, .java, .m, .m4v, .max, .mdb, .pcd, .pct, .pl, .potm, .potx, .ppam, .ppsm, .ppsx, .pptm, .ps, .pspimage, .r3d, .rw2, .sldm, .sldx, .svg, .tga, .wps, .xla, .xlam, .xlm, .xlr, .xlsm, .xlt, .xltm, .xltx, .xlw, .act, .adp, .al, .bkp, .blend, .cdf, .cdx, .cgm, .cr2, .crt, .dac, .dbf, .dcr, .ddd, .design, .dtd, .fdb, .fff, .fpx, .h, .iif, .indd, .jpeg, .mos, .nd, .nsd, .nsf, .nsg, .nsh, .odc, .odp, .oil, .pas, .pat, .pef, .pfx, .ptx, .qbb, .qbm, .sas7bdat, .say, .st4, .st6, .stc, .sxc, .sxw, .tlg, .wad, .xlk, .aiff, .bin, .bmp, .cmt, .dat, .dit, .edb, .flvv, .gif, .groups, .hdd, .hpp, .log, .m2ts, .m4p, .mkv, .mpeg, .ndf, .nvram, .ogg, .ost, .pab, .pdb, .pif, .png, .qed, .qcow, .qcow2, .rvt, .st7, .stm, .vbox, .vdi, .vhd, .vhdx, .vmdk, .vmsd, .vmx, .vmxf, .3fr, .3pr, .ab4, .accde, .accdr, .accdt, .ach, .acr, .adb, .ads, .agdl, .ait, .apj, .asm, .awg, .back, .backup, .backupdb, .bank, .bay, .bdb, .bgt, .bik, .bpw, .cdr3, .cdr4, .cdr5, .cdr6, .cdrw,

Copyright 2016 – Institute for Critical Infrastructure Technology (ICIT)

.ce1, .ce2, .cib, .craw, .crw, .csh, .csl, .db_journal, .dc2, .dcs, .ddoc, .ddrw, .der, .des, .dgc, .djvu, .dng, .drf, .dxg, .eml, .erbsql, .erf, .exf, .ffd, .fh, .fhd, .gray, .grey, .gry, .hbk, .ibank, .ibd, .ibz, .iiq, .incpas, .jpe, .kc2, .kdbx, .kdc, .kpdx, .lua, .mdc, .mef, .mfw, .mmw, .mny, .moneywell, .mrw, .myd, .ndd, .nef, .nk2, .nop, .nrw, .ns2, .ns3, .ns4, .nwb, .nx2, .nxl, .nyf, .odb, .odf, .odg, .odm, .orf, .otg, .oth, .otp, .ots, .ott, .p12, .p7b, .p7c, .pdd, .pem, .plus_muhd, .plc, .pot, .pptx, .psafe3, .py, .qba, .qbr, .qbw, .qbx, .qby, .raf, .rat, .raw, .rdb, .rwl, .rwz, .s3db, .sd0, .sda, .sdf, .sqlite, .sqlite3, .sqlitedb, .sr2, .srf, .srw, .st5, .st8, .std, .sti, .stw, .stx, .sxd, .sxg, .sxi, .sxm, .tex, .wallet, .wb2, .wpd, .x11, .x3f, .xis, .ycbcra, .yuv

Copyright 2016 – Institute for Critical Infrastructure Technology (ICIT)

KeRanger Technical Details:

Indicators of Compromise:

Samples of Ransomware.OSX.KeRanger

d1ac55a4e610380f0ab239fcc1c5f5a42722e8ee1554cba8074bbae4a5f6dbe1 Transmission-2.90.dmg

e3ad733cea9eba29e86610050c1a15592e6c77820927b9edeb77310975393574 Transmission

31b6adb633cff2a0f34cefd2a218097f3a9a8176c9363cc70fe41fe02af810b9 General.rtf

d7d765b1ddd235a57a2d13bd065f293a7469594c7e13ea7700e55501206a09b5 Transmission

2.90.dmg

ddc3dbee2a8ea9d8ed93f0843400653a89350612f2914868485476a847c6484a Transmission

6061a554f5997a43c91f49f8aaf40c80a3f547fc6187bee57cd5573641fcf153 General.rtf

Targeted File Extensions:

.3dm, .3ds, .3g2, .3gp, .7z, .ab4, .accdb, .accde, .accdr, .accdt, .ach, .acr, .act, .adb, .ads, .ai, .ait, .al, .apj, .arw, .asf, .asm, .asp, .asx, .avi, .back, .backup, .bak, .bank, .bay, .bdb, .bgt, .bik, .bkf, .bkp, .blend, .bpw, .cdb, .cdf, .cdr, .cdx, .ce1, .ce2, .cer, .cfp, .cgm, .class, .cls, .cmt, .cnv, .cpi, .cpp, .cr2, .craw, .crt, .crw, .cs, .csh, .csl, .csv, .dac, .db, .db3, .dbf, .dbr, .dbs, .dc2, .dcr, .dcs, .dcx, .ddd, .ddoc, .dds, .der, .des, .design, .dgc, .djvu, .dng, .doc, .docm, .docx, .dot, .dotm, .dotx, .drf, .drw, .dtd, .dwg, .dxb, .dxf, .dxg, .ebd, .edb, .eml, .eps, .erf, .exf, .fdb, .ffd, .fff, .fh, .fhd, .fla, .flac, .flv, .fm, .fp7, .fpx, .fxg, .gdb, .gray, .grey, .grw, .gry, .hbk, .hpp, .ibd, .idx, .iif, .indd, .java, .jpe, .jpeg, .jpg, .kdbx, .kdc, .key, .laccdb, .lua, .m4v, .maf, .mam, .maq, .mar, .maw, .max, .mdb, .mdc, .mde, .mdf, .mdt, .mef, .mfw, .mmw, .mos, .mov, .mp3, .mp4, .mpg, .mpp, .mrw, .mso, .myd, .ndd, .nef, .nk2, .nrw, .ns2, .ns3, .ns4, .nsd, .nsf, .nsg, .nsh, .nwb, .nx1, .nx2, .nyf, .obj, .odb, .odc, .odf, .odg, .odm, .odp, .ods, .odt, .oil, .one, .orf, .otg, .oth, .otp, .ots, .ott, .p12, .p7b, .p7c, .pages, .pas, .pat, .pbo, .pcd, .pct, .pdb, .pdd, .pdf, .pef, .pem, .pfx, .php, .pip, .pl, .plc, .pot, .potm, .potx, .ppam, .pps, .ppsm, .ppsx, .ppt, .pptm, .pptx, .prf, .ps, .psafe3, .psd, .pspimage, .ptx, .pub, .puz, .py, .qba, .qbb, .qbm, .qbw, .qbx, .r3d, .raf, .rar, .rat, .raw, .rdb, .rm, .rtf, .rwz, .sas7bdat, .say, .sd0, .sda, .sdf, .snp, .sql, .sr2, .srf, .srt, .srw, .st4, .st5, .st6, .st7, .st8, .stc, .std, .sti, .stw, .stx, .svg, .swf, .sxc, .sxd, .sxg, .sxi, .sxm, .sxw, .tex, .tga, .thm, .tlg, .txt, .vob, .vsd, .vsx, .vtx, .wav, .wb2, .wbk, .wdb, .wll, .wmv, .wpd, .wps, .x11, .x3f, .xla, .xlam, .xlb, .xlc, .xlk, .xll, .xlm, .xlr, .xls, .xlsb, .xlsm, .xlsx, .xlt, .xltm, .xltx, .xlw, .xpp, .xsn, .yuv, .zip, .tar, .tgz, .gzip, .tib, .sparsebundle

Copyright 2016 – Institute for Critical Infrastructure Technology (ICIT)

Domains

lclebb6kvohlkcml.onion[.]link

lclebb6kvohlkcml.onion[.]nu

bmacyzmea723xyaz.onion[.]link

bmacyzmea723xyaz.onion[.]nu

nejdtkok7oz5kjoc.onion[.]link

nejdtkok7oz5kjoc.onion[.]nu

Copyright 2016 – Institute for Critical Infrastructure Technology (ICIT)

Sources:

Bleeping Computer:

http://www.bleepingcomputer.com/news/security/information-about-the-keranger-os-x-ransomware-and-how-to-remove-it-/

http://www.bleepingcomputer.com/news/security/the-cerber-ransomware-not-only-encrypts-your-data-but-also-speaks-to-you/

CSO Online:

http://www.csoonline.com/article/3040619/security/cerber-ransomware-sold-as-a-service-speaks-to-victims.html

IB Times:

http://www.ibtimes.co.uk/cerber-terrifying-russian-ransomware-speaks-bitcoin-demand-blackmail-victims-out-loud-1547592

NDTV:

http://www.ndtv.com/world-news/mac-ransomware-caught-before-large-number-of-computers-infected-1284845

Palo Alto Networks:

http://researchcenter.paloaltonetworks.com/2016/03/new-os-x-ransomware-keranger-infected-transmission-bittorrent-client-installer/

Reuter:

http://in.reuters.com/article/apple-ransomware-idINL1N16F17Q

Slate:

http://www.slate.com/blogs/future_tense/2016/03/07/keranger_ransomware_strikes_mac_os_x_through_transmission_update.html

Copyright 2016 – Institute for Critical Infrastructure Technology (ICIT)