United States Secret Service [INFO]

May 9, 2019

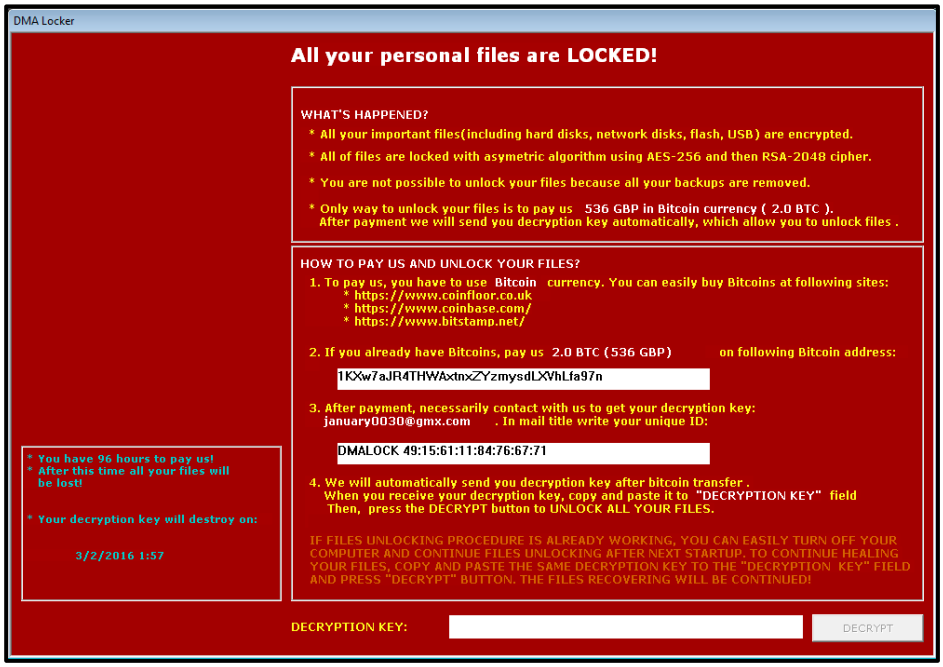
[INFO] Information Only Alert – GIOC Reference #19-007-I
TLP Green

Ransomware: Prevention and Response to an Attack

The GIOC has recently observed an increase in notifications concerning ransomware events. Ransomware is a type of malicious software cyber actors use to deny access to systems or data. In these events, a malicious cyber actor holds systems or data hostage until a ransom is paid. Frequently, after the initial infection, the ransomware attempts to spread to shared storage drives and other accessible systems. If ransom demands aren't met, the system or encrypted data remains unavailable or data may be erased.

This type of malware attempts to extort money from victims by displaying an on-screen alert advising the victim that their computer has been locked or that their files have been encrypted (typically using RSA 2048 encryption) and demand that a ransom is paid to restore access. The system remains encrypted until the victim pays the ransom, in exchange for a decryption key, which allows the user to regain access.

Recent statistics show the average ransom demand is $522. However, this amount can be substantially higher if the target is a business or organization and not an individual. Increasingly, ransom is demanded via virtual currency, such as payment to a Bitcoin address.



Example of ransomware on-screen alert

[INFO] - Indicates informational or educational content.

RESPONDING TO A RANSOMWARE ATTACK

Victims should reach out to law enforcement ***before*** making contact with the bad actor. Once initial contact is made, this potentially starts the clock, which will reduce the allowable time to respond.

The USSS does ***not*** encourage victims to pay the demand.

- Paying a ransom does not guarantee an organization will regain access to their data; in fact, some individuals or organizations were never provided with decryption keys after having paid a ransom while others have been continually extorted by new demands.
- On average, paying the ransom results in decryption of 77% of the network data.

The following are instructions and advice an investigator can provide to the victim to help mitigate this type of network attack.

- Advise the victim to isolate the compromised portion of their network as soon as possible, but ***do not power down*** or shutoff any system affected by the ransomware (this includes both wired and wireless networks).
- Determine if communication has occurred with the attacker; if yes, by whom (if the victim is a large corporation, often it will be a company's attorney).
- Collect all available log information.
- Try to discover the characteristics of the malware infection to determine the investigative response:
    - Non-encrypting ransomware locks the screen (restricts access to files but does not encrypt them).
    - Ransomware that encrypts the Master Boot Record (MBR) prevents the victims' computers from being booted up in a live environment (what most people consider a ransomware attack).
    - Leakage or "extortionware" exfiltrates data that the attackers threaten to release if ransom is not paid
    - Mobile Device Ransomware (infects cell-phones through drive-by downloads or fake apps).

- Ransomware attacks are the result of poor or defective security standards, therefore, the entire system should not be trusted. Advise the victim that all communications regarding the compromise, should be "out-of-band" i.e. via phone and not email.

- If the victim has multiple backups, use the oldest back-up to restore the system -the infection should be considered to be temporal.

The below list is an example of key data to collect when responding to a ransomware event. This list is not exhaustive and every situation will be unique, but it provides a starting point for most situations.

1) Detailed victim information to include organization name, sector, systems affected, technical POC, and loss amount.
2) If available, ransomware variant name.
3) Original email(s) with full headers and any attachments (if the attack was executed by phishing).
4) Copies of any executables or other files dropped onto the system after accessing malicious attachments, including splash page.
5) Any domains or IP addresses communicated with just prior to or during infection.
6) The Bitcoin address (or other requested virtual currency address) to which payment is requested, and the amount being requested.
7) Was the ransom paid? If so, the amount and the Bitcoin address to which the payment was made.
8) If available, any forensic analysis or incident response reports completed.
9) If available, any memory captures taken during execution of the malware.
10) Status of the infection.

This information and other relevant reports related to a ransomware attack can be sent to the GIOC at gioc@usss.dhs.gov, to be collected for criminal intelligence purposes.

Additionally, the victim can file an IC3 complaint at www.ic3.gov/complaint.

PREVENTING A RANSOMWARE ATTACK

The following measures can make a system or network more secure against malware or similar types of attacks:

- Update software and operating systems with the latest patches. This one of the most common vulnerabilities that is easily fixable.
- Restrict users' permissions to install and run software applications, and apply the principle of "least privilege"

to all systems and services. Restricting these privileges may prevent malware from running or limit its capability to spread through a network.

- Use application whitelisting to allow only approved programs to run on a network.
- Enable strong spam filters to prevent phishing emails from reaching the end users and authenticate inbound email to prevent email spoofing.
- Scan all incoming and outgoing emails to detect threats and filter executable files from reaching end users.
- Configure firewalls to block access to known malicious IP addresses.

Any questions relating to this alert can be directed to the GIOC at gioc@usss.dhs.gov or 202-406-6009.

[INFO] - Indicates informational or educational content.