United States Secret Service & Homeland Security Investigations

10 May 2016

What is Ransomware?

Ransomware is a type of malware that restricts access to infected computers and requires victims to pay a ransom in order to regain full access to their data. Ransomware is typically spread through spear phishing emails or by unknowingly visiting an infected website. This type of malware attempts to extort money from victims by displaying an on-screen alert. These alerts often state that the computer has been locked or that all files have been encrypted, and demand that a ransom is paid to restore access. Typical ransoms are in the range of $100–$300 dollars, and are often demanded in the form of digital currency, such as Bitcoin. In addition to the potential significant financial losses, ransomware infections can cause temporary or permanent loss of sensitive data, disrupt daily operations, and cause damage to the reputation of the affected organizations.

Prevention & Mitigation are Essential

Prevention and mitigation are the key to limiting the risk posed by ransomware. Response and recovery options are extremely limited if an enterprise does not have back-ups in place. Companies should ensure their Continuity of Operations plan (COOP) includes having appropriate back-ups in place to avoid being in a circumstance where payment of the ransom may be the only option to recover the data.

Law Enforcement

The U.S. Secret Service and U.S. Immigration and Customs Enforcement/Homeland Security Investigations (ICE/HSI) discourages the paying of extortion demands. Unfortunately, we are currently not aware of any particular means to recover the data encrypted by current versions of major ransomware families, without access to the private key, or restoring the withheld data from an available back-up. Accordingly, companies should ensure they have appropriate backups in place to avoid being placed in this dilemma. Whatever a business's decision, it should report the crime and coordinate its approach with an appropriate law enforcement agency. Paying the ransom may recover the data in some cases, but it also has risks, including:

- It may encourage criminals to re-target the victim with higher ransom demands,
- In some cases it does not recover the data,
- It may contribute to increasing the prevalence of this criminal scheme, and
- Paying the ransom may result in further legal or reputation risks to the business.

In all cases of extortion immediately contact an appropriate law enforcement agency, whether Federal, State, or Local, to report a ransomware event and request assistance. The United States Secret Service's Electronic Crimes Task Forces and ICE/HSI field offices are available to respond and investigate significant ransomware cases.

Federal Law Enforcement Contact Information

United States Secret Service
Electronic Crimes Task Force
www.secretservice.gov/investigation/#field
Local Field Offices
www.secretservice.gov/contact/

U.S. Immigration and Customs Enforcement
Homeland Security Investigations (ICE/HSI)
HSI Tip Line: Call 866-DHS-2-ICE (866-347-2423)
https://www.ice.gov/webform/hsi-tip-form
HSI Field Offices
https://www.ice.gov/contact/hsi

Questions to assess preparedness

Have we identified our most valuable data? Is it backed up or protected through extra measures, including isolating your critical data from other networks and encryption?

Does my organization have, and regularly, test a cyber incident response plan?

How do we coordinate and implement cyber incident response planning across the enterprise?

Does my organization have a cybersecurity policy in place?

What are the risks to the critical functions of our organization if data was compromised or withheld? How would it affect our bottom line?

How have we linked our physical security team with our cybersecurity team?

Do we know when we will call law enforcement or DHS for assistance, and who we will call?

US-CERT Preparedness Recommendations

The U.S. Computer Emergency Readiness Team (US-CERT)published a recent alert which includes the following recommendations:

- Employ a **data backup and recovery plan** for all critical information and back up your data on a regular basis. Ideally, this data should be kept on a separate device and should be stored offline.
- **Update software and operating systems** with the latest patches. Out of date applications and operating systems are the low hanging fruit of most malicious actors.
- **Restrict users' ability (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 your network.
- Remind employees to **never click unsolicited links or open unsolicited attachments** in emails.

Follow safe practices when browsing the Internet. Read Good Security Habits and Safeguarding Your Data for additional details.