How to Protect Your Networks from RANSOMWARE

This document is a U.S. Government interagency technical guidance document aimed to inform Chief Information Officers and Chief Information Security Officers at critical infrastructure entities, including small, medium, and large organizations. This document provides an aggregate of already existing Federal government and private industry best practices and mitigation strategies focused on the prevention and response to ransomware incidents.

Protecting Your Networks from Ransomware

Ransomware is the fastest growing malware threat, targeting users of all types—from the home user to the corporate network. On average, more than 4,000 ransomware attacks have occurred daily since January 1, 2016. This is a 300-percent increase over the approximately 1,000 attacks per day seen in 2015. There are very effective prevention and response actions that can significantly mitigate the risk posed to your organization.

Ransomware targets home users, businesses, and government networks and can lead to temporary or permanent loss of sensitive or proprietary information, disruption to regular operations, financial losses incurred to restore systems and files, and potential harm to an organization's reputation.

Ransomware may direct a user to click on a link to pay a ransom; however, the link may be malicious and could lead to additional malware infections. Some ransomware variants display intimidating messages, such as:

> "Your computer was used to visit websites with illegal content. To unlock your computer, you must pay a $100 fine."

> "You only have 96 hours to submit the payment. If you do not send money within provided time, all your files will be permanently encrypted and no one will be able to recover them."

What is Ransomware?

Ransomware is a form of malware that targets your critical data and systems for the purpose of extortion. Ransomware is frequently delivered through spearphishing emails. After the user has been locked out of the data or system, the cyber actor demands a ransom payment. After receiving payment, the cyber actor will purportedly provide an avenue to the victim to regain access to the system or data. Recent iterations target enterprise end users, making awareness and training a critical preventive measure.

Protecting Your Networks

Educate Your Personnel

Attackers often enter the organization by tricking a user to disclose a password or click on a virus-laden email attachment.

Remind employees to never click unsolicited links or open unsolicited attachments in emails. To improve workforce awareness, the internal security team may test the training of an organization's workforce with simulated phishing emails[1].

Proactive Prevention is the Best Defense

Prevention is the most effective defense against ransomware and it is critical to take precautions for protection. Infections can be devastating to an individual or organization, and recovery may be a difficult process requiring the services of a reputable data recovery specialist.

The U.S. Government (USG) recommends that users and administrators take the following preventive measures to protect their computer networks from falling victim to a ransomware infection:

Preventive Measures

- Implement an awareness and training program. Because end users are targets, employees and individuals should be aware of the threat of ransomware and how it is delivered.
- Enable strong spam filters to prevent phishing emails from reaching the end users and authenticate inbound email using technologies like Sender Policy Framework (SPF), Domain Message Authentication Reporting and Conformance (DMARC), and DomainKeys Identified Mail (DKIM) 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.
- Patch operating systems, software, and firmware on devices. Consider using a centralized patch management system.
- Set anti-virus and anti-malware programs to conduct regular scans automatically.
- Manage the use of privileged accounts based on the principle of least privilege: no users should be assigned administrative access unless absolutely needed; and those with a need for administrator accounts should only use them when necessary.

[1] For additional information on Avoiding Social Engineering and Phishing Attacks, please see US-CERT Security Tip (ST04-014), available at: https://www.us-cert.gov/ncas/tips/ST04-014

- Configure access controls—including file, directory, and network share permissions—with least privilege in mind. If a user only needs to read specific files, the user should not have write access to those files, directories, or shares.
- Disable macro scripts from office files transmitted via email. Consider using Office Viewer software to open Microsoft Office files transmitted via email instead of full office suite applications.
- Implement Software Restriction Policies (SRP) or other controls to prevent programs from executing from common ransomware locations, such as temporary folders supporting popular Internet browsers or compression/decompression programs, including the AppData/LocalAppData folder.
- Consider disabling Remote Desktop protocol (RDP) if it is not being used.
- Use application whitelisting, which only allows systems to execute programs known and permitted by security policy.
- Execute operating system environments or specific programs in a virtualized environment.
- Categorize data based on organizational value and implement physical and logical separation of networks and data for different organizational units.

Business Continuity Considerations

- Back up data regularly. Verify the integrity of those backups and test the restoration process to ensure it is working.
- Conduct an annual penetration test and vulnerability assessment.
- Secure your backups. Ensure backups are not connected permanently to the computers and networks they are backing up. Examples are securing backups in the cloud or physically storing backups offline. Some instances of ransomware have the capability to lock cloud-based backups when systems continuously back up in real time, also known as persistent synchronization. Backups are critical in ransomware recovery and response; if you are infected, a backup may be the best way to recover your critical data.

What to Do If Infected with Ransomware

Should preventive measures fail, the USG recommends that organizations consider taking the following steps upon an infection with ransomware:

- **Isolate the infected computer immediately**. Infected systems should be removed from the network as soon as possible to prevent ransomware from attacking network or share drives.
- **Isolate or power-off affected devices that have not yet been completely corrupted.** This may afford more time to clean and recover data, contain damage, and prevent worsening conditions.

- **Immediately secure backup data or systems by taking them offline.** Ensure backups are free of malware.
- **Contact law enforcement immediately.** We strongly encourage you to contact a local field office of the Federal Bureau of Investigation (FBI) or U.S. Secret Service immediately upon discovery to report a ransomware event and request assistance.
- **If available, collect and secure partial portions of the ransomed data that might exist**.
- **If possible, change all online account passwords and network passwords after removing the system from the network.** Furthermore, change all system passwords once the malware is removed from the system.
- **Delete Registry values and files to stop the program from loading.**

Implement your security incident response and business continuity plan. Ideally, organizations will ensure they have appropriate backups, so their response to an attack will simply be to restore the data from a known clean backup. Having a data backup can eliminate the need to pay a ransom to recover data.

There are serious risks to consider before paying the ransom. USG does not encourage paying a ransom to criminal actors. However, after systems have been compromised, whether to pay a ransom is a serious decision, requiring the evaluation of all options to protect shareholders, employees, and customers. Victims will want to evaluate the technical feasibility, timeliness, and cost of restarting systems from backup. Ransomware victims may also wish to consider the following factors:

- 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 paying a ransom.
- Some victims who paid the demand were targeted again by cyber actors.
- After paying the originally demanded ransom, some victims were asked to pay more to get the promised decryption key.
- Paying could inadvertently encourage this criminal business model.

How Law Enforcement Can Help

Any entity infected with ransomware should contact law enforcement immediately. Law enforcement may be able to use legal authorities and tools that are unavailable to most organizations. Law enforcement can enlist the assistance of international law enforcement partners to locate the stolen or encrypted data or identify the perpetrator. These tools and relationships can greatly increase the odds of successfully apprehending the criminal, thereby preventing future losses.

Federal law enforcement places a priority on conducting cyber investigations in a manner that causes minor disruption to a victim entity's normal operations and seeks to work cooperatively and discreetly with that entity. Federal law enforcement uses investigative measures that avoid unnecessary downtime or displacement of a company's employees. Federal law enforcement closely coordinates its activities with the affected organization to avoid unwarranted disclosure of information.

As an affected entity recovers from a cybersecurity incident, the entity should initiate measures to prevent similar incidents. Law enforcement agencies and the Department of Homeland Security's National Cybersecurity and Communications Integration Center can assist organizations in implementing countermeasures and provide information and best practices for avoiding similar incidents in the future. Additionally, the affected organization should conduct a post-incident review of their response to the incident and assess the strengths and weaknesses of its incident response plan.

Ransomware Variants[2]

Ransomware is a growing criminal activity involving numerous variants. Since 2012 when police locker ransomware variants first emerged, ransomware variants have become more sophisticated and destructive. Some variants encrypt not just the files on the infected device, but also the contents of shared or networked drives, externally attached storage media devices, and cloud storage services that are mapped to infected computers. These variants are considered destructive because they encrypt users' and organizations' files, and render those files useless until a ransom is paid.

Recent federal investigations by the FBI reveal that ransomware authors continue to improve ransomware code by using anonymizing services like "Tor [3]" for end-to-end communication to infected systems and Bitcoin virtual currency to collect ransom payments. Currently, the top five ransomware variants targeting U.S. companies and individuals are CryptoWall, CTB-Locker, TeslaCrypt, MSIL/Samas, and Locky. New ransomware variants are continually emerging.

CryptoWall

CryptoWall and its variants have been actively used to target U.S. victims since April 2014. CryptoWall was the first ransomware variant that only accepted ransom payments in Bitcoin. The ransom amounts associated with CryptoWall are typically between $200 and $10,000. Following the takedown of the CryptoLocker botnet, CryptoWall has become the most successful ransomware variant with victims all over the world. Between April 2014 and June

[2] For more information on Ransomware variants and other resources, visit https://www.us-cert.gov/ncas/alerts/TA16-091A

[3] Tor is free software for enabling anonymous communication. Tor directs Internet traffic through a free, worldwide, volunteer network consisting of more than 7,000 relays to conceal a user's location and usage from anyone conducting network surveillance or traffic analysis. (The name derives from the original software project name, *The Onion Router*.)

2015, IC3 received 992 CryptoWall-related complaints, with victims reporting losses totaling over $18 million.[4] CryptoWall is primarily spread via spam email but also infects victims through drive-by downloads[5] and malvertising[6].

CTB-Locker

CTB-Locker emerged in June 2014 and is one of the first ransomware variants to use Tor for its C2 infrastructure. CTB-Locker uses Tor exclusively for its C2 servers and only connects to the C2 after encrypting victims' files. Additionally, unlike other ransomware variants that utilize the Tor network for some communication, the Tor components are embedded in the CTB-Locker malware, making it more efficient and harder to detect. CTB-Locker is spread through drive-by downloads and spam emails.

TeslaCrypt

TeslaCrypt emerged in February 2015, initially targeting the video game community by encrypting gaming files. These files were targeted in addition to the files typically targeted by ransomware (documents, images, and database files). Once the data was encrypted, TeslaCrypt attempted to delete all Shadow Volume Copies and system restore points to prevent file recovery. TeslaCrypt was distributed through the Angler, Sweet Orange, and Nuclear exploit kits.

MSIL or Samas (SAMSAM)

MSIL or Samas (SAMSAM) was used to compromise the networks of multiple U.S. victims, including 2016 attacks on healthcare facilities that were running outdated versions of the JBoss content management application. SAMSAM exploits vulnerable Java-based Web servers. SAMSAM uses open-source tools to identify and compile a list of hosts reporting to the victim's active directory. The actors then use psexec.exe to distribute the malware to each host on the network and encrypt most of the files on the system. The actors charge varying amounts in Bitcoin to provide the decryption keys to the victim.

Locky

In early 2016, a destructive ransomware variant, Locky, was observed infecting computers belonging to businesses globally, including those in the United States, New Zealand, Australia, Germany and the United Kingdom. Locky propagates through spam emails that include malicious Microsoft Office documents or compressed attachments (e.g., .rar, .zip) that were previously associated with banking Trojans such as Dridex and Pony. The malicious attachments contain macros or JavaScript files to download the Locky files. Recently, this ransomware has also been distributed using the Nuclear Exploit Kit.

---

[4] This number includes additional costs incurred by the victim. Expenses may be associated with network mitigation, network countermeasures, loss of productivity, legal fees, IT services, and the purchase of credit monitoring services for employees or customers.

[5] Drive by download" is the transfer of malicious software to the victim's computer without the knowledge of or any action by the victim.

[6] "Malvertizing," is the use of malicious ads on legitimate websites. These malicious ads contain code that will infect a user's computer without any action from the user (i.e., the user does not have to click on the ad to become infected).

Links to Other Types of Malware

Systems infected with ransomware are also often infected with other malware. In the case of CryptoLocker, a user typically was infected by opening a malicious attachment from an email. This malicious attachment contained Upatre, a downloader, which infected the user with GameOver Zeus. GameOver Zeus was a variant of the Zeus Trojan used to steal banking information and other types of data. After a system became infected with GameOver Zeus, Upatre would also download CryptoLocker. Finally, CryptoLocker encrypted files on the infected system and demanded a ransom payment.

The disruption operation against the GameOver Zeus botnet also affected CryptoLocker, demonstrating the close ties between ransomware and other types of malware. In June 2014, an international law enforcement operation successfully weakened the infrastructure of both GameOverZeus and CryptoLocker.

Federal Government Resources

Reporting

Federal Bureau of Investigation

Cyber Task Forces
www.fbi.gov/contact-us/field

Internet Crime Complaint Center
www.ic3.gov

United States Secret Service

Electronic Crimes Task Force
www.secretservice.gov/investigation/#field

Local Field Offices
www.secretservice.gov/contact/

Mitigation

Department of Homeland Security
United States Computer Emergency Readiness Team (US-CERT)

www.us-cert.gov

NIST Cybersecurity Framework:
http://www.nist.gov/cyberframework/

NSA/IAD Top 10 Information Assurance Mitigations Strategies:
https://www.iad.gov/iad/library/ia-guidance/iads-top-10-information-assurance-mitigation-strategies.cfm