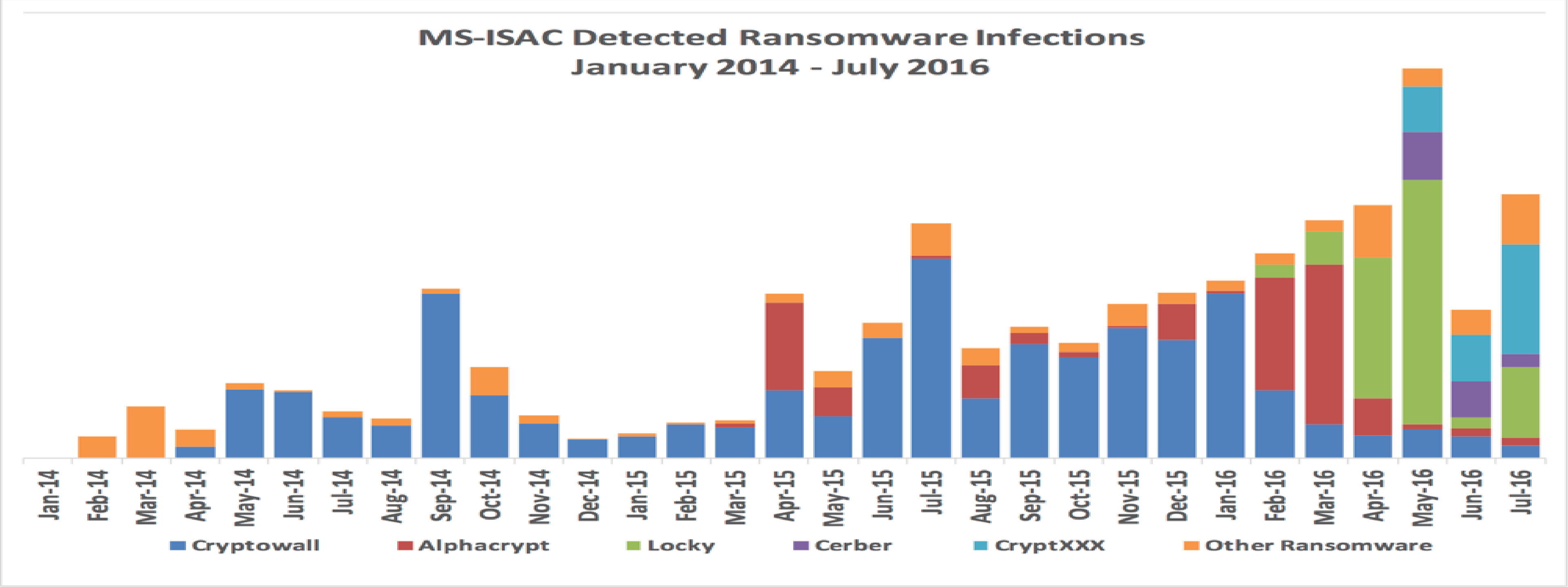
RANSOMWARE: FACTS, THREATS, AND COUNTERMEASURES

RANSOMWARE

Ransomware is a type of malware that has become a significant threat to U.S. businesses and individuals during the past year. General ransomware incidents surged in 2016 and continue to infect victims with overwhelming success. Most of the current ransomware variants encrypt files on the infected system/network (*crypto ransomware*), although a few variants are known to erase files or block access to the system using other methods (*locker ransomware*). Once access to the system is blocked, the ransomware demands a ransom in order to unlock the files, frequently $200 – $1000 in bitcoins, though other currencies, gift cards, and ransoms of several thousand dollars are occasionally reported. Ransomware variants almost always opportunistically target business and home users, infecting an array of devices from computers to smartphones.

Victims are at risk of losing their files, but may also experience financial loss due to paying the ransom, lost productivity, IT costs, legal fees, network modifications, and/or the purchase of credit monitoring services for employees/customers.



INFECTION VECTORS

The majority of ransomware is propagated through user-initiated actions such as clicking on a malicious link in a spam e-mail, search engine results, or website; or through malvertising or drive-by downloads, which do not require user interaction. In early 2016, a ransomware variant was discovered that exploited vulnerabilities in specific content management software and moved laterally within victim networks to infect endpoint machines.

ADDITIONAL CAPABILITIES

In the past several months there have been several ransomware variants that include additional features, such as data exfiltration, participation in distributed denial of service (DDoS) attacks, and anti-detection components. One variant deletes files regardless of whether or not a payment was made. Another variant includes the capability to lock cloud-based backups when systems continuously back up in real-time (a.k.a. during persistent synchronization). Other variants target smartphones and Internet of Things (IoT) devices.

Below are some of the changes in ransomware activity that occurred during July 2016, according to open source reporting:

- Cisco’s Talos group observed a new ransomware variant called Ranscam. Ranscam is not particularly sophisticated and instead of encrypting files it simply deletes all of them. Cisco has not observed any significant campaigns, however they have found a link between the developers of Ranscam and two other destructive variants, Jigsaw and Anonpop.
- TrendMicro reported on a new ransomware family known as CrypMIC, a variant that mimics CryptXXX. Like CryptXXX, CrypMIC is disseminated by the Neutrino Exploit Kit, and uses TCP Port 443 to communicate with command and control (C2) servers. A key difference is that CrypMIC uses weaker encryption and fewer evasion techniques. CrypMIC also leaves file extensions untouched, making it difficult to identify encrypted files.
- The developers of the Petya and Mischa ransomware variants released the variants as a Ransomware-as-a-Service (RaaS) product. This allows users to earn a certain percentage of the ransom paid, determined by how much income they generate for the developers.
- Security researcher BloodDolly identified a variant known as Alfa. There is little information available on Alfa’s distribution or its encryption, however it was developed by the actors behind Cerber.
- Proofpoint identified Bart, a new ransomware from the actors behind Dridex and Locky. Bart does not require a connection to C2 servers in order to begin the encryption process, allowing it to more easily evade detection. Additionally, Bart places each file in its own encrypted ZIP file. A decryptor has been released for Bart.
- Stampado is a RaaS variant identified by Heimdal Security. The developers offer a lifetime license for only $39, putting ransomware well within the financial reach of most malicious cyber threat actors. A decryptor has been released for Stampado.

Although not as common, some variants claim to be from a law enforcement agency and that the user owes a “fee” or “fine” for conducting illegal activities, such as viewing pornography. In an effort to appear more legitimate these variants can use techniques to identify the victim’s rough geographic location in order to use the name of a specific law enforcement agency. *No U.S. law enforcement agency will ever remotely lock or disable a computer and demand a fine to unlock it.*

Paying a ransom does not guarantee an organization will regain access to its data.

SPECIAL CONSIDERATIONS FOR HEALTH INFORMATION

The U.S. Department of Health and Human Services (HHS) issued a fact sheet on ransomware and the applicability of the Health Insurance Portability and Accountability Act (HIPAA) response and reporting requirements. The fact sheet indicates that if "unsecured" electronic Protected Health Information (ePHI) is compromised by ransomware a reportable breach has occurred. The fact sheet also addresses ransomware attack prevention and recovery from a HIPAA perspective.

RECOMMENDATIONS

The following recommendations are provided to help mitigate the risk of ransomware infections. A copy of the recommendations is also available in the printable MS-ISAC Security Primer on Ransomware.

Securing Networks and Systems

- **Have an incident response plan.**
- **Backups are critical.** Perform regular backups of all systems. Use a backup system that allows multiple iterations of the backups to be saved, in case a copy of the backups includes encrypted or infected files. Routinely test backups for data integrity and to ensure it is operational.
- **Use antivirus and anti-spam solutions.** Enable regular system and network scans with antivirus programs enabled to automatically update signatures. Implement an anti-spam solution to stop phishing emails from reaching the network. Consider adding a warning banner to all emails from external sources that reminds users of the dangers of clicking on links and opening attachments.
- **Disable macros scripts in Office**. Consider using Office Viewer software to open Microsoft Office files transmitted via e-mail instead of full office suite applications.
- **Know what is connected to and running on your network.** Keep all hardware, operating systems, software, and applications, including cloud locations and content management systems (CMS), patched and up-to-date. Use a centralized patch management system if possible. Implement application white-listing. Implement software restriction policies (SRP) to prevent the execution of programs in common ransomware locations, such as temporary folders.
- **Restrict Internet access.** Use a proxy server for Internet access and consider ad-blocking software. Restrict access to common ransomware entry points, such as personal email accounts and social networking websites.
- **Apply the principles of least privilege and network segmentation.** Categorize and separate data based on organizational value and where possible, implement virtual environments, and the physical and logical separation of networks and data. Apply the principle of least privilege.
- **Vet and monitor third parties** that have remote access into the organization's network and/or your connections to third parties, to ensure they are diligent with cybersecurity best practices.
- **Participate in cybersecurity information sharing** programs and organizations, such as MS-ISAC and InfraGard.

Securing the End User

- **Provide social engineering and phishing training to employees.** Urge them not to open suspicious emails, not to click on links or open attachments contained in such emails, and to be cautious before visiting unknown websites.
- **Remind users to close their browser when not in use.**
- **Have a reporting plan** that ensures staff know where and how to report suspicious activity.

Responding to a Compromise/Attack

- **Immediately** disconnect the infected system from the network to prevent infection propagation.
- **Determine the affected data** as some sensitive data, such as electronic protected health information (ePHI) may require additional reporting and/or mitigation measures.
- **Restore** files from regularly maintained backups.
- **Report the infection.** It is highly recommended that SLTT government agencies report ransomware incidents to MS-ISAC. Other sectors and home users may report to infections to local Federal Bureau of Investigation (FBI) field offices or to the Internet Crime Complaint Center (IC3) at http://www.ic3.gov.