Threat, Vulnerability, and Mitigation Information

1. US-CERT and the Canadian Cyber Incident Response Centre have issued Alert (TA16-091A), entitled “Ransomware and Recent Variants.” Locky and Samas, two ransomware variants, have been observed infecting healthcare facilities and hospitals worldwide. It also has been reported that systems infected with ransomware are infected with other malware (e.g., CryptoLocker and GameOver Zeus). Previously, June 2014, an international law enforcement operation successfully weakened the infrastructure of both GameOver Zeus and CryptoLocker.

2. Researchers have observed a widespread campaign leveraging the Samas/Samsam/MSIL.B/C ransomware variant, thus changing the threat landscape for ransomware delivery. Researchers have also estimated that there are 3.2 million vulnerable machines running unpatched versions of JBoss, which this ransomware variant targets. Information for securing JBoss application servers can found from resources such as this one.

3. Researchers have reported that Manamcrypt (MSIL/Manamcrypt.A, CryptoHost) is a new and severe type of ransomware variant. Manamcrypt is reported to be bundled with “clean” software. It is also reported to not encrypt files, but rather compress files into a password-
protected RAR file. Researchers have provided instructions on how to remove the ransomware, such as here.

4. Security researchers have reportedly developed an online service and a desktop tool for generating a password needed to decrypt a computer which has been infected by Petya ransomware.

5. A security researcher has reportedly developed a tool called “RansomWhere?” to help thwart ransomware attacks against OS X machines.

6. The FBI Cyber Division has released an uncaveated, unclassified document on ransomware (appended to this report). Because ransomware can be highly sophisticated and is constantly evolving, the FBI Cyber Division recommends that organizations have a robust security program with special emphasis on prevention, business continuity, and remediation. The FBI Cyber Division also provides mitigation information in its guidance.

The FBI Cyber Division’s guidance also makes clear that there is no guarantee against exploitation, even with the most robust controls in place. Further, this guidance states that the FBI does not recommend that victims pay the requested ransom. Individuals are encouraged to contact their local FBI Field Office or the FBI’s Internet Crime Complaint Center (IC3) for assistance. Contacting your local FBI Field Office may result in a quicker response.

7. The NSA has released an uncaveated, unclassified document on the Locky variant of ransomware (appended to this report). According to this bulletin, Locky’s main delivery mechanism is through Microsoft Word, Excel, or Outlook attachments. Locky attacks are resilient against countermeasures through updates, code corrections, and new capabilities. Its botnet delivery mechanism has been reported to be similar to the Dridex
trojan horse program. Locky generally evades traditional antivirus defenses. The NSA provides mitigation information, including guidance on application whitelisting, in this bulletin.

8. The FBI has recently issued an announcement about a dramatic increase in business e-mail compromise (“BEC”) targeted companies. According to the FBI, the schemers spoof company e-mail or use social engineering techniques to assume the identity of the company’s CEO, a company attorney, or a trusted vendor. The schemers research who manages money and use language specific to the company which they are targeting and typically request wire transfer payments. From October 2013 through February 2016, it is reported that law enforcement has received reports about BEC from 17,642 victims and that the losses have amounted to more than $2.3 billion. The FBI’s IC3 has issued an alert (I-082715a-PSA) on BEC which provides additional information, including where to turn to if you are a victim.

9. ICS-CERT has issued Alert (IR-ALERT-H-16-056-0), entitled “Cyber-Attack Against Ukrainian Critical Infrastructure.” In this report, the BlackEnergy malware variant is suspected to have played a role in this reported cyber attack. An advanced persistent threat group (BlackEnergy) is said to be the originators of the malware. Of particularly note, ICS-CERT strongly encourages organizations across all sectors to review and employ the mitigation strategies as set forth in this alert.

10. US-CERT has issued Alert (TA16-105A), entitled “Apple Ends Support for QuickTime for Windows; New Vulnerabilities Announced.” In this alert, Trend Micro is reported to have stated that Apple has ended support for Quicktime for Windows. This alert also states that two new vulnerabilities have been discovered. Since this software is no longer supported, it is recommended that this software be uninstalled from machines as a mitigation strategy.
11. Adobe has announced a critical vulnerability (CVE-2016-1019) in Adobe Flash Player 21.0.0.197 and earlier versions for Windows, Macintosh, Linux, and Chrome OS. Successful exploitation may cause a crash and potentially allow an attacker to take control of an affected system. A mitigation introduced in Flash Player 21.0.0.182 currently prevents exploitation of this vulnerability, thereby protecting users running Flash Player 21.0.0.182 and later.

12. Reports of a newly evolved Qakbot/Qbot network-aware worm targeting hospitals and other public institutions have surfaced. According to reports, Qakbot is primarily designed as a credential harvester.

13. As noted in this SANS paper, Remote Desktop Protocol (RDP) connections are common intrusion vectors for botnets and other attackers. The default RDP port is port 3389. By changing this to another unused port, organizations may be able to evade certain attacks. It is important for all organizations to know the difference between normal and suspicious behavior or activity on their systems and networks. Resources such as the SANS DFIR “Find Evil” poster may be helpful.

Research and Reports

1. The 2016 Verizon Data Breach Digest states that insider threat continues to be a problem for the healthcare sector. Source of insider threat problems can be from infected USB drives, rogue employees, and third party partners. Additional detection and mitigation information can be found here (posted with permission).

2. The Gone in Six Characters: Short URLs Considered Harmful for Cloud Services reveals the danger of using shortened uniform resource locators (URLs), especially for sensitive information. Using a brute force technique, online resources which may have been intended to be shared with a few
trusted friends or collaborators may be effectively shared with the public and thus accessible to anyone.

3. The ‘PowerShell’ Deep Dive report states that malware created with Powershell is on the rise. The PowerShell-based malware has been reportedly distributed via social engineering techniques, targeting mainly corporate networks, intellectual property, customer data, and financial data. 13% of the attacks were targeted or advanced attacks. 87% of the attacks were a result of click-fraud, fake antivirus, ransomware, and other opportunistic malware.

4. The Return of Qbot report provides an in-depth technical analysis of the Qbot/Qakbot network-aware worm targeting hospitals and other public institutions. To date, many websites have been compromised, including in the United States. The academic, healthcare, and information technology sectors (e.g., IT service companies) have been victims of this compromise.

Special Announcements

Join the HIMSS Healthcare Cybersecurity Community today! The HIMSS Healthcare Cybersecurity Community provides a monthly forum for thought-leaders (from government, the private sector, and academia) and healthcare constituents to discuss and learn about advancing the state of cybersecurity in our healthcare industry. HIMSS members and non-members are welcome!
Ransomware

Infection Vectors

Ransomware is frequently delivered through phishing e-mails to end users. Early ransomware e-mails were often generic in nature, but more recent e-mails are highly targeted to both the organization and individual, making scrutiny of the document and sender important to prevent exploitation. An e-mail compromise occurs in one of two ways:

1. Receipt of an e-mail containing malicious attachments, including: .pdf, .doc, .xls, and .exe file extensions. These attachments are described as something that appears legitimate, such as an invoice or electronic fax, but contain malicious code.

2. Receipt of an e-mail that appears legitimate but contains a link to a website hosting an exploit kit.

When the user opens the malicious file or link in the phishing e-mail, the most frequent end result is the rapid encryption of files and folders containing business-critical information and data. Recent ransomware campaigns have employed robust encryption that prevents most attempts to break the encryption and recover the data.

Another infection method involves adversaries hacking a known website to plant the malware. End users are infected when visiting the compromised website while using outdated browsers, browser plugins, and other software.

After infection, the malware usually calls home to command and control (C2) infrastructure to obtain encryption keys from the adversary. Once keys are obtained, the malware begins rapidly encrypting files and folders on local drives, attached drives, and network shares to which the infected user has access. Organizations are generally not aware that they have been infected until users are no longer able to access data or begin to see messages advising them of the attack and demanding a ransom payment.

While the FBI normally recommends organizations invest in measures to prevent, detect, and remediate cyber exploitation, the key areas to focus on with ransomware are prevention, business continuity, and remediation. It is very difficult to detect a successful ransomware compromise before it is too late. The best approach is to focus on defense in depth, or several layers of security, as there is no single method to prevent a compromise. As ransomware techniques and malware continue to evolve and become more sophisticated, even with the most robust prevention controls in place, there is no guarantee against exploitation. This fact makes contingency and remediation planning crucial to business recovery and continuity, and those plans should be tested regularly to ensure the integrity of sensitive data in the event of a compromise.
Prevention Considerations

• Focus on awareness and training. Since end users are targeted, employees should be made aware of the threat of ransomware, how it is delivered, and trained on information security principles and techniques.

• Patch the operating system, software, and firmware on devices. All endpoints should be patched as vulnerabilities are discovered. This can be made easier through a centralized patch management system.

• Ensure anti-virus and anti-malware solutions are set to automatically update and regular scans are conducted.

• Manage the use of privileged accounts. Implement the principle of least privilege. No users should be assigned administrative access unless absolutely needed. Those with a need for administrator accounts should only use them when necessary; and they should operate with standard user accounts at all other times.

• Implement least privilege for file, directory, and network share permissions. If a user only needs to read specific files, they should not have write access to those files, directories, or shares. Configure access controls with least privilege in mind.

• Disable macro scripts from office files transmitted via e-mail. Consider using Office Viewer software to open Microsoft Office files transmitted via e-mail instead of full office suite applications.

• Implement software restriction policies (SRP) or other controls to prevent the execution of programs in common ransomware locations, such as temporary folders supporting popular Internet browsers, or compression/decompression programs, including those located in the AppData/LocalAppData folder.

Business Continuity Considerations

• Regularly back up data and verify its integrity.

• Secure your backups. Ensure backups are not connected to the computers and networks they are backing up. Examples might be securing backups in the cloud or physically storing them 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; if you are infected, backups may be the best way to recover your critical data.

Other Considerations

Some other considerations that can be highly dependent on organizational budget and system configuration include:

• Implement application whitelisting. Only allow systems to execute programs known and permitted by security policy.

• Use virtualized environments to execute operating system environments or specific programs.

• Categorize data based on organizational value, and implement physical/logical separation of networks and data for different organization units. For example, sensitive research or business data should not reside on the same server and/or network segment as an organization’s e-mail environment.

• Require user interaction for end user applications communicating with websites uncategorized by the network proxy or firewall. Examples include requiring users to type information or enter a password when their system communicates with a website uncategorized by the proxy or firewall.

The Ransom

The FBI does not advocate paying a ransom to an adversary. 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. Paying a ransom emboldens the adversary to target other organizations for profit and provides a lucrative environment for other criminals to become involved. Finally, by paying a ransom, an organization is funding illicit activity associated with criminal groups, including potential terrorist groups, who likely will continue to target an organization. While the FBI does not advocate paying a ransom, there is an understanding that when businesses are faced with an inability to function, executives will evaluate all options to protect their shareholders, employees, and customers.

In all cases, the FBI encourages organizations to contact their local FBI Cyber Task Force immediately to report a ransomware event and request assistance. The FBI works with federal, state, local, and international partners to pursue cyber actors globally and assist victims of cyber crime. Victims are also encouraged to report cyber incidents to the FBI's Internet Crime Complaint Center (www.ic3.gov).

Contact the Cyber Task Forces at www.fbi.gov/contact-us/field and the Internet Crime Complaint Center at www.ic3.gov
**What is Locky?**

Locky is a multi-staged ransomware that restricts access to files on a compromised system until a ransom is paid. Cyber actors tempt victims into opening and clicking attachments in socially engineered spam e-mails. In many cases, these emails contain capabilities that harvest the victim’s credentials and gather personal details from the victim’s host. Locky’s main delivery mechanism is through Microsoft Word, Excel, or Outlook attachments.

Known Locky targets include various private citizens, hospitals, and Government networks. Observed techniques against hospitals included a fake invoice which entices the recipient to click on the attachment prompting the user to enable macros. Once executed, it contacts one of the command and control servers resulting in the delivery of ransomware to the host. It then encrypts files on the infected host and provides instructions on how to pay the ransom.

**Growth and External Incidents**

Locky attacks have continued to be resilient against countermeasures through updates, code corrections, and the addition of new capabilities. Attack analysis reveals a planned phased attack cycle with observed pauses during each phase, as each consecutive phase grows exponentially. As reported by Trustwave, over a seven day period, the number of targeted emails grew by 200,000 with Locky representing nearly 18% of all spam delivered email during that period. At the height of infection, 1,000 devices per hour were calling back to the C2 servers. Currently, approximately 1,000 devices per day are observed.

Locky revealed a significant change in ransomware TTPs by targeting hospitals. Several hospitals have been infected to very likely include Flint Michigan, Hollywood Presbyterian Medical Center in Los Angeles, three German hospitals and at least one hospital in Canada. Hollywood Presbyterian paid a 40 bitcoin ransom ($17,000 USD) to regain network functionality. Two hospitals in Germany were reported to have paid ransoms while the Flint Michigan hospital and one German hospital were able to recover functionality through rapid mitigation to include successful reimaging of devices.

**Locky Behavior**

Locky has been observed using the same botnet delivery mechanism as other ransomware, such as Dridex. Variants typically employ a multi-staged payload dropping system designed to modularize the delivery of malware, obfuscate analysis, and evade typical enterprise AV defenses. Nearly all variants utilize an email attachment that contains obfuscated JavaScript, or macro-enabled Word documents that drop and then execute the 1st stage JavaScript downloader. When the 2nd Stage windows executable is downloaded and executed, a second executable is unpacked from the resource section of the 2nd Stage executable and further executed. Some variants will download additional resources in the form of a 3rd Stage executable. The following chart highlights the common functionality of Locky variants.

Locky loads itself into memory, sets persistence mechanisms, encrypts files and documents while renaming them with a custom extension, deletes VSS snapshots, and alters the desktop wallpaper.
Ransomware: Locky

Mitigations

- In order to reduce the attack surface, ensure proper network segmentation is in place.
- Educate users about common spear phishing tactics and how to recognize, as well as prevent, infection. Hold users accountable for poor security practices.
- Regularly perform backups and keep the copies off-site: Locky has the capability to encrypt your network based backup file; therefore, it is recommended to not only backup each system within the domain but also store the copies off-site.
- Ensure a robust application whitelisting (AWL) strategy that includes rules that prevent any execution from user writable file locations, specifically %TEMP% locations (e.g. c:\users\*\appdata\local\temp). Most AWL products have "default" rules that preclude %TEMP% directories from allowing execution, but organizations should also ensure that any location that is whitelisted is also preventing users from writing to those folders.
- Ensure that HIPS rules that deny unknown executables from running are in place, well-tuned, and set to block. For example, McAfee’s HBSS rules 3905 and 2297 deny execution from common malware locations (e.g. temp directories). Rules 7010, 7011, and 7035 are similar rules with additional optimization for DoD environments. Custom rules could be created that deny the creation of the registry key "HKEY_CURRENT_USER\Software\Locky".
- If permissible, implement a registry access protection rule to block registry key/value creation under “HKCU\Software\locky”.
- Identify infected network users: If .locky extension files are shown in network shares, look up the file owner on the "_Locky_recover_instructions.txt" file in each folder. This will assist in determining the infected user.
- Disable macros in email attachments: After an extreme prevalence of infections in the past, Microsoft has deliberately disabled macros on word documents automatically as a security measure. Do not turn it on.

Before and After Compromise of Host System

The screenshots (located right) are a demonstration of what occurs if a user enables macros in the infected word document, which automatically compromises the host system. It should be noted that an additional method of compromising hosts consists of sending JavaScript file attachments that have been designed to evade AV detection.