Recent Ransomware Trends

Mass Market Ransomware

- Source code for ransomware variants typically cost thousands of dollars. Mass market ransomware is available at a lower cost and is designed for non-technical users.
    - Stampado ransomware is available for 39 USD and comes with the source code, lifetime support, and upgrades.

Alternate Encryption Methods

- This type of ransomware attempts to encrypt an alternate service, such as the master boot record or web server, rather than encrypting individual files.

Ransomware as a Service (RaaS)

- RaaS offers individuals an opportunity to purchase ransomware at a lower cost, but splits the ransom profits between the attacker and developer of the ransomware.

Core Mitigation Strategy

- Do not open suspicious emails or attachments. Ransomware and other malware typically are installed via social engineering techniques.

- Create multiple security layers to help mitigate vulnerabilities.
    - Regularly back up and maintain critical files separate from the corporate network. This enables victims of ransomware to wipe their systems clean and restore critical files.

    - Disable macros to ensure that malicious documents do not automatically run.

    - Maintain up-to-date firewall settings that will block malicious activity and known IPs associated with malware campaigns.

    - Create policies to establish strong passwords, password length, and password expiration requirements.

- Conduct secondary verification of emails containing attachments or links received by coworkers to ensure they are legitimate.

- Report ransomware infections to the Internet Crime Complaint Center (IC3)[1]. Reporting helps authorities attribute ransomware attacks to threat actors.

[1] http://www.ic3.gov/

Post Infection Strategy

- Attempt to identify the ransomware variant that is affecting the computer.
- Determine if there is an application designed to decrypt the files. This is known as a decryptor.
- If a decryptor is available, decrypt affected files, remove the infected system from the network, and reimage the machine.
    - If a decryptor is not available, the victim will need to utilize backups in order to properly restore encrypted files. The machine should be reimaged before restoring files.
- Paying the ransom does not guarantee receiving a decryptor. Threat actors often take the ransom payment without giving a decryption key in return.

Ransomware Chart

The ransomware variants defined below are the most common according to NCFTA intelligence. This chart provides initial indicators and if a means to decrypt files exists online[2].

Ransomware Name:	File Extension Given to Encrypted Files:	Decryptor available:	Encryption Algorithm:
Cerber	.cerber	Yes	AES
Cryptolocker	.encrypted	Yes	RSA
CTB Locker	.ctbl	No	AES
HDD Cryptor	.cry	No	Custom (net shares) XTS-AES (disk)
Locky	.locky, .zepto, .odin, .shit	No	AES128
Petya	random 4 characters (.7GP3), random 8 character	Yes	Salsa20
Samas	.encryptedAES, .encryptedRSA, .encedRSA	Yes	AES256 RSA 2096
Satan	.satan	Yes	AES256 RSA2096
Stampado	.locked	Yes	AES256
Teslacrypt	.mp3, .micro, .xxx, .ttt	Yes	AES256 ECHD + SHA1

[2] http://www.nomoreransom.org/