FALL 2016 E-NEWSLETTER

At Digital Mountain we assist our clients with their cybersecurity, computer forensics and e-discovery needs. For this E-Newsletter, we focus on the topic of ransomware and the information security, legal and financial impact it has on organizations.

TECHNICAL INTRICACIES OF RANSOMWARE AND SAFEGUARDING STRATEGIES

Ransomware is the online equivalent to crooks changing the door locks to your house and then demanding payment for the keys. Ransomware is malicious software that holds critical data and systems hostage through encryption and requires payment for the decryption key. If payment is not received according to the ransom terms, depending on the type of ransomware, the files may be deleted, altered, or the charitable cybercriminal may provide additional time to meet the demand.

Ransomware - Variants and Victims

The variants of ransomware have multiplied dramatically. Shadowlock, a particularly inhumane ransomware, forces users to complete consumer surveys of products and services as the ransom payment (Hey, time is money, right?). The most disturbing variants of ransomware, however, are the ransomware-as-a-service products, such as CerberRing, which provides less-tech savvy criminals a corridor into cybercrime, and yields criminal affiliates (often tasked with distributing the ransomware) a healthy portion of the profits.

The typical victim of ransomware has also changed. Although cybercriminals are notorious for launching attacks against broad numbers of victims, focused attacks are now prevalent. High-value targets, such as key executives and key data systems, are specific and frequent targets because they control high-value data. Understandably, high-value data held hostage reaps a premium ransom payment.

How Ransomware Works - Infecting and Executing in the Shadows

Because ransomware infects computers much like other forms of malware, cybercriminals seek to compromise targets through traditional system vulnerabilities, especially human vulnerabilities. Systems are often compromised through spear phishing (infected e-mails that appear legitimate), and through malicious advertisements placed on legitimate websites.

Spear phishing attacks either infect email attachments with malicious macros (programs embedded into files such as Word and PDF that execute when the document is opened) or include hyperlinks directing users to websites that run malicious exploit kits that search for vulnerabilities on the local system, download ransomware into the local system, and execute the ransomware.

Because ransomware's initial program commands are usually designed to hide the ransomware from the system (often by running in the background in system memory), defending against ransomware is problematic. For example, ransomware targeting Windows systems masks malicious activity behind the volume shadow copies (snapshots of data on the local system). The typical masked steps of ransomware include:

1. Executing the malicious program from within a volume shadow copy;
2. Linking the volume shadow copy to a Windows system folder; and
3. Deleting the original volume shadow copy.

Thanks to the deceptive masking of ransomware, to an untrained eye the malicious program appears as a standard executable for a Windows system. The program continues to execute, encrypting predetermined and often valuable files, such as system files and documents (e.g., Word, Excel, and PDF).

When All is Not Lost - Methodologies for Interrupting Ransomware Attacks

For now, most ransomware does not complete its encryption process without further commands from its cybercriminal controllers. For example, ransomware often requires that the local system communicate back to the cybercriminal's host server in order to create the decryption key and transmit it to the cybercriminal.

Consequently, it's possible for experts to thwart the creation and transmission of the decryption key by disabling the network functionality of the local machine. It is also possible to interrupt the process by cutting power to the systems—though this is less desirable because when the systems are powered down evidence critical to tracking down the perpetrator will be lost. The challenges with the aforementioned techniques are that organizations need to train personnel to recognize the warning signs of ransomware (e.g., CPU utilization mysteriously increasing) and to react immediately and correctly to a specific variant of malware that is likely designed to hide itself from users.

Thus, because ransomware is difficult to detect, the key is to prevent ransomware from ever entering your systems, and if it does enter your systems, take countermeasures to stop it from proliferating throughout.

For end users that means:

- Be skeptical of emails and links that have the following characteristics: an unknown sender; received at an odd time; and contains misspelled words or incorrect grammar. One tactic you can employ is to hover over links to determine whether it's pointing to the same location as the hyperlink text (though this tactic is difficult to perform on mobile devices).

- Install the latest antivirus / malware protection software and set it to update your library automatically with the new variants of malware defense.

At the organization level, IT staff should:

- Harden operating systems by locking down the key attack vectors, such as changing default passwords, removing unnecessary and outdated login credentials, and updating software versions.
- Segment your systems in a way that quarantines ransomware infection of a single device to prevent infecting your entire system.
- Implement a robust backup plan that utilizes different backup methods, such as traditional backup tapes and cloud-based backups. Taking this critical prevention step strikes a blow to cybercriminals because there's minimal leverage to demand a ransom when it's likely cheaper to restore an infected machine to its malware-free state than pay a ransom.

Again, the best defense against ransomware is to be aware of its variants and take proactive measures to prevent infection. In addition to providing assistance with the requisite system hardening to defend against ransomware and ensuring that cybercriminals have not made any additional changes to your systems, Digital Mountain can also locate alternative access to the system when under attack (imagine dropping into the house through the skylight rather than having to deal with the locked door).

UPCOMING INDUSTRY EVENTS

October 2016
Privacy + Security Forum,
Washington, DC: October 24-26

The Sedona Conference Working Group 1 on Electronic Document Retention,
Atlanta: October 27-28

November 2016
Georgetown Law's The Advanced EDiscovery Institute,
Washington, DC: November 10-11

December 2016
Association of Defense Counsel Annual Meeting,
San Francisco: December 8-9

Click here to see more upcoming events and links

Digital Mountain, Inc. Founder and CEO, Julie Lewis, will be presenting at various upcoming industry events. Please send requests for speaker or panel participation for her to marketing@digitalmountain.com.

DIGITAL MOUNTAIN, INC.
4633 Old Ironsides Drive, Suite 401
Santa Clara, CA 95054

Contact us today!

866.DIG.DOCS

www.digitalmountain.com

FOLLOW US AT: