Understanding and Responding to Ransomware Attacks

secpod

Introduction - Ransomware

Ransomware is a malware, which prevents users from accessing the system or personal files by locking the system or by encrypting the personal files unless a ransom is paid.

Types of Ransomware

1. Encrypting ransomware: Encrypts files then asks for a ransom.
   Eg: CryptoLocker, Locky, CryptoWall
2. Locker ransomware: Locks OS then asks for a ransom.
   Eg: Winlocker
3. Master Boot Record (MBR) ransomware: Locks MBR and asks for a ransom.
   Eg: Petya, Satana

Ransomware Distribution and Spreading Methods

1. Spam emails with malicious links or attachments
2. Through vulnerable software
3. Malicious websites
4. Legitimate websites with malicious code injected
5. Drive-by-downloads
6. Social engineering
7. Self-propagation
8. Malvertising

In most of the above spreading techniques except social engineering, ransomware uses a security hole in the software applications called vulnerability. Malware/Ransomware exploit these vulnerabilities to get into the system.

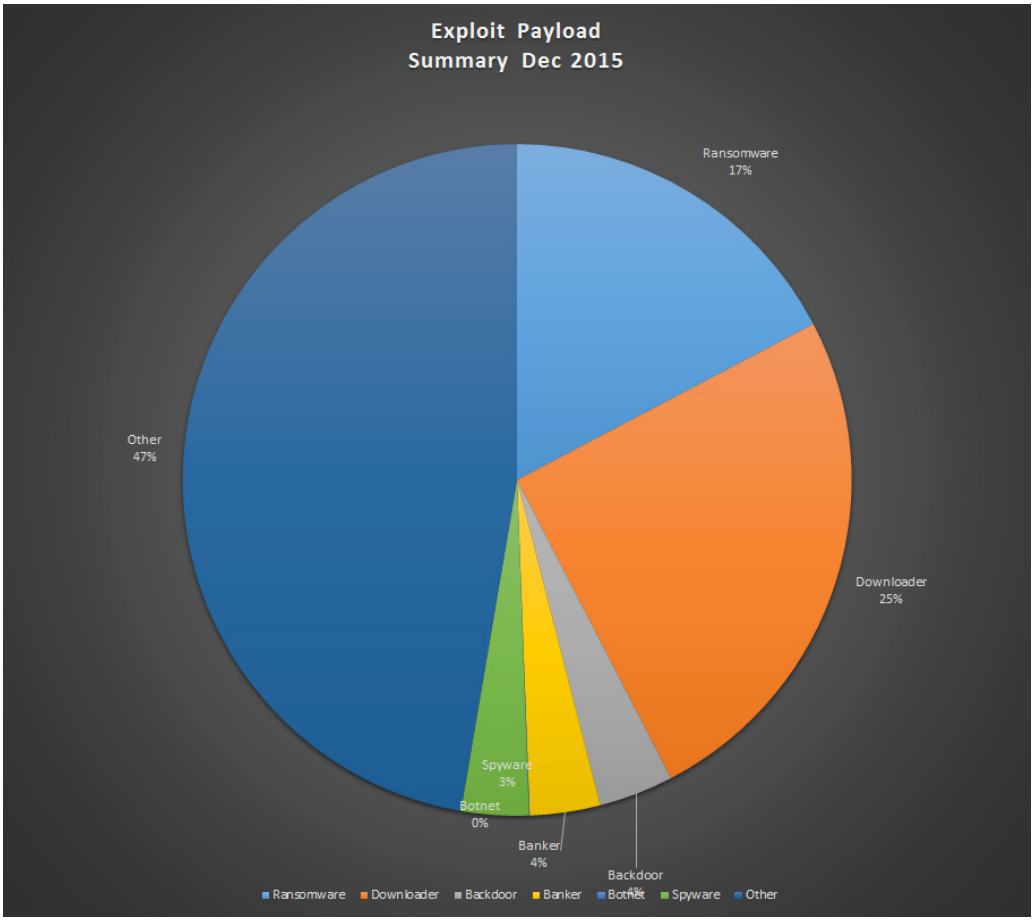
How Ransomware Infects System

1. The attacker sends an email which includes a malicious link or a malicious attachment. To convince the victim, the attacker will make their email look like it came from someone whom the victim knows or trusts such as a friend or a recognized company.
2. When the victim opens the malicious link or attachment, it exploits a vulnerability in the system. The downloader gets downloaded and is kept on the infected system.
3. The downloader contacts list of domains or C&C (Command and Control) servers hosted by an attacker to download the ransomware.
4. The C&C server sends the requested ransomware onto the infected host.
5. The downloaded ransomware starts encrypting the whole hard disk.
6. Once encryption is done, ransomware pops up on the screen with an instruction on how to get the data back or how to get the decryption key by paying ransom, mostly in terms of bitcoins.

How Saner Prevents and Detects Ransomware Attacks

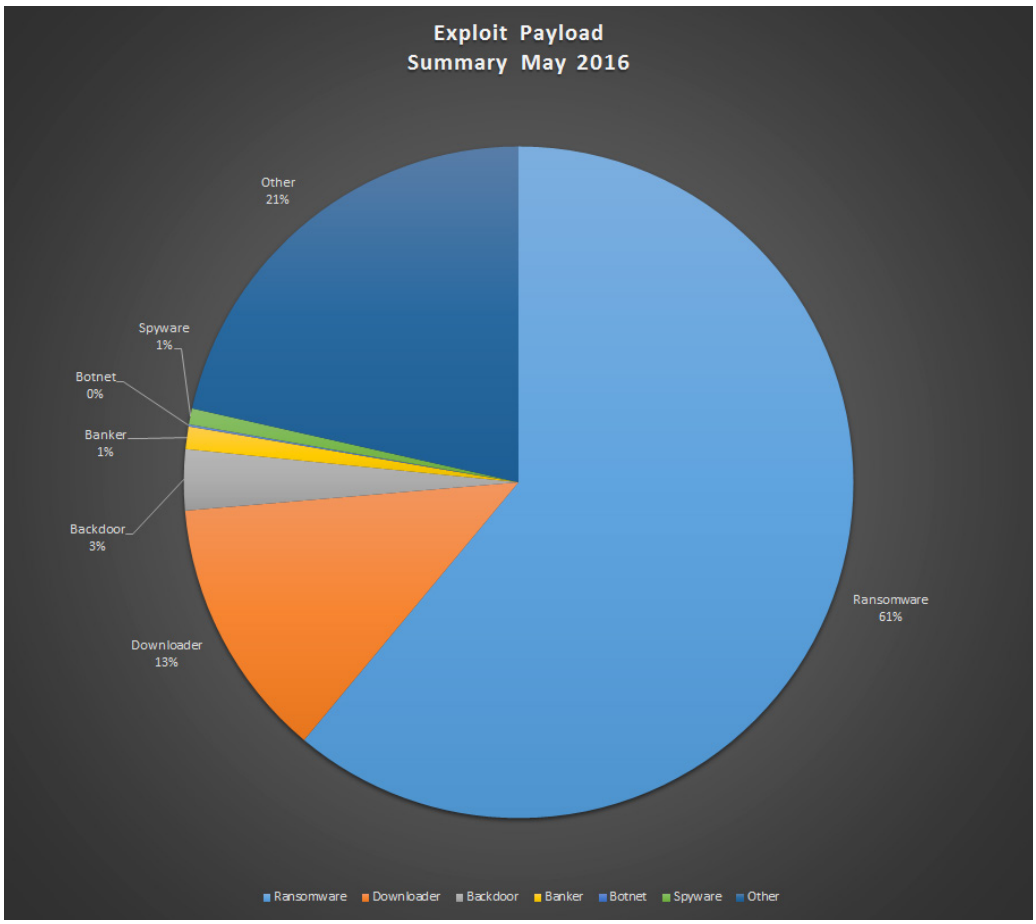
1) Prevention - vulnerability mitigation, any statistics to substantiate this?

Most of the ransomware attacks are driven through exploit kits which use vulnerabilities to get into the system. According to Malwarebytes, in 2015 ransomware payload distribution in exploit kits was only 17% as shown in the image below.



Source: Malwarebytes

In mid-2016, ransomware payload soared from 17% to 61%, which is 259 percent increase of ransomware being dropped by exploit kits.



Source: Malwarebytes

More statistics on ransomware can be found at https://blog.barkly.com/ransomware-statistics-2016

Saner identifies and remediates the vulnerabilities in the system thus defending most of the ransomware attacks. Saner automates this process by scheduling the vulnerability scanning and remediation.

2) Do most ransomware use existing vulnerabilities to get into the system?

Yes, ransomware indirectly (through exploit kits) and few directly exploit vulnerabilities to get into the system. The other more popular method is social engineering attacks.

We can stop most of the ransomware infection by remediating vulnerabilities by applying security patches. Another important step is to educate employees on techniques employed in social engineering attacks.

Security updates is a very important security layer to keep away ransomware and other malware. Below are few cases where ransomware exploits vulnerabilities to get into the system.

Here Are 4 Vulnerabilities Ransomware Attackers Are Exploiting Now

10 Shocking New Facts About Ransomware

3) Detection: How is our detection, do we cover most ransomware?

We cover most of the crucial and common ransomware such as Locky, Petya, CryptoLocker, CryptoWall, just to name a few. We are also creating new detection methods.

4) Do we perform early detection?

Partially yes, Saner detects as soon as the ransomware creates indicators like creating a specific process, file or registry in real time. Also, Saner detects if malware tries to contact C&C server to download a ransomware or any other malware, which will help to detect attacks early. Saner allows execution of actions such as killing connection to C&C server, killing and blocking the process as a possible ransomware response strategy. Using Saner, one can see complete security posture of the system and network.

5) Is there a value in detection if the system is already compromised?

Yes. Ransomware may not have encrypted all the data (it takes more time to encrypt whole hard disk), Saner detects and terminates the malicious process or terminates the malicious connection to C&C server. It can also help with preventing ransomware from spreading to other systems.

Fighting Against Ransomware

1. Apply security updates for OS and all the installed application and remove unwanted applications from the system.
2. Use strong security hardening policies.
3. Use web filtering to avoid infection vectors.
4. Stop and disable unwanted services.
5. Install and run security software and keep them up-to-date.
6. Educate employees on ransomware attacks.
7. Don't open emails or attachments from an unknown or suspicious sender.
8. Always use the system as a normal user instead of a power user.
9. Segregate the network for important systems with sensitive data.
10. Back your data offline or in a secure place.

How Saner Solution Fights Against Ransomware

1. Saner detects vulnerabilities in systems and provides ways to remediate those vulnerabilities. Saner provides immunity against most of the ransomware infections.
2. Saner automates vulnerability detection and remediation simplifying the process.
3. Saner detects infected systems in the network based on the indicator of attack/compromise. This information will be useful to move the infected system to a quarantine zone to avoid further infection.
4. Saner helps to remove or block unwanted software from the systems reducing the attack surface.
5. Saner helps to harden the system configuration settings making it hard for ransomware to infect the system with unknown methods.

About Us

SecPod Technologies creates cutting edge products to ensure endpoint security. SecPod's deep information security expertise exceptionally positions the company to help solve complex endpoint security challenges. Headquartered in Bangalore with operations in USA, SecPod's products are deployed across diversified verticals.

Contact Us

Web: www.secpod.com Tel: +91-80-4121 4020
Email: info@secpod.com +1-918-625-3023