Ransomware: A Billion Dollars a Year Cyber Crime

secpod

Ransomware is a form of malware that renders a computer, or personal data stored in it, inaccessible to its owner. A perpetrator uses ransomware to infect a computer and hold the user hostage by making all data inaccessible to its legitimate owner by encrypting the data. Ransomware can enter a system in multiple ways. These include exploitation of vulnerabilities, misconfigurations, and social engineering.

Ransomware Overview

The most virulent form of ransomware is based on the concept of Cryptovirology introduced by Young and Yung in a 1996 IEEE paper. This paper discusses the use of public key cryptography to demonstrate how encryption mechanisms can be misused by miscreants. The paper highlighted how asymmetric key encryption is used to encrypt the data on the victim's computer. The key to decrypt the data is with the perpetrator. The perpetrator then demands a ransom to provide the key for decrypting the data. There is no guarantee that the key will be provided to the user after paying the ransom. CryptoLocker, CryptoWall, Petya, Locky, and Zepto are typical ransomware.

Variants of ransomware include Trojans that lock the Microsoft Windows system, and demand a ransom to unlock the system. Some forms of ransomware exploit social engineering to trick victims into paying ransoms. One variation of this works by locking the victim's system. It then claims that the law enforcement agency has locked the system and the lock will be released upon payment of a fine. Reveton, a major ransomware Trojan, has used this method to extort money from victims.

A recent CNN report estimates that cybercriminals collected over $209 million in the first three months of 2016. Ransomware is turning out to be a *more than a billion dollars a year cybercrime.* This figure does not include losses associated with recovery and other related losses. Many victims do not report the ransom they paid and are just keen on getting their system back as soon as possible.

Cybercriminals collected over $209 million in the first three months of 2016 - CNN

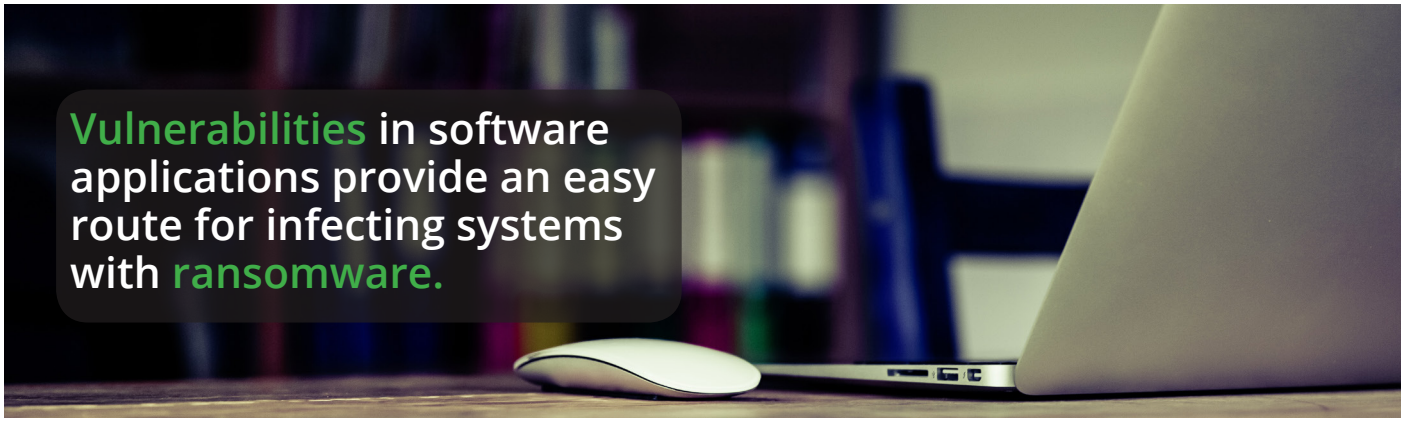
How Ransomware Enters the System

Ransomware uses multiple strategies to gain access to the victim's system. Vulnerabilities in software applications provide an easy route for infecting systems with ransomware. Many exploit kits include ransomware and are actively used to attack systems.

While the latest data shows ransomware exploiting vulnerabilities in Adobe Flash Player and Microsoft Silverlight, many vulnerabilities in other applications continue to be used by perpetrators to attack systems using ransomware.

Ransomware can also enter the system through the lack of adherence to compliance rules within an organization. For example, perpetrators can easily exploit the auto-run option of USB drives to execute ransomware, if it is not blocked by the organization.

Another common strategy adopted by ransomware to gain access to systems is by email. Through phishing attacks, the user receives email with an attachment that looks genuine. The attachment contains a hidden executable that installs and runs the ransomware.



Preventing Ransomware Attacks

Ransomware can impact normal business in many ways. If an attacked endpoint is connected to network drives, files in those drives may get encrypted as well. It is important to ensure risk to endpoint systems and enterprise resources is reduced. The following simple steps will help reduce the risk of a ransomware security breach.

1. Keep all endpoint systems up to date by applying the latest patches

A significant percentage of ransomware attacks take place by exploiting vulnerabilities in applications. The risk of a ransomware attack can be substantially minimised by keeping systems up to date by applying the latest patches available from the vendor.

2. Have strong policies, and ensure that all endpoint systems comply with policies

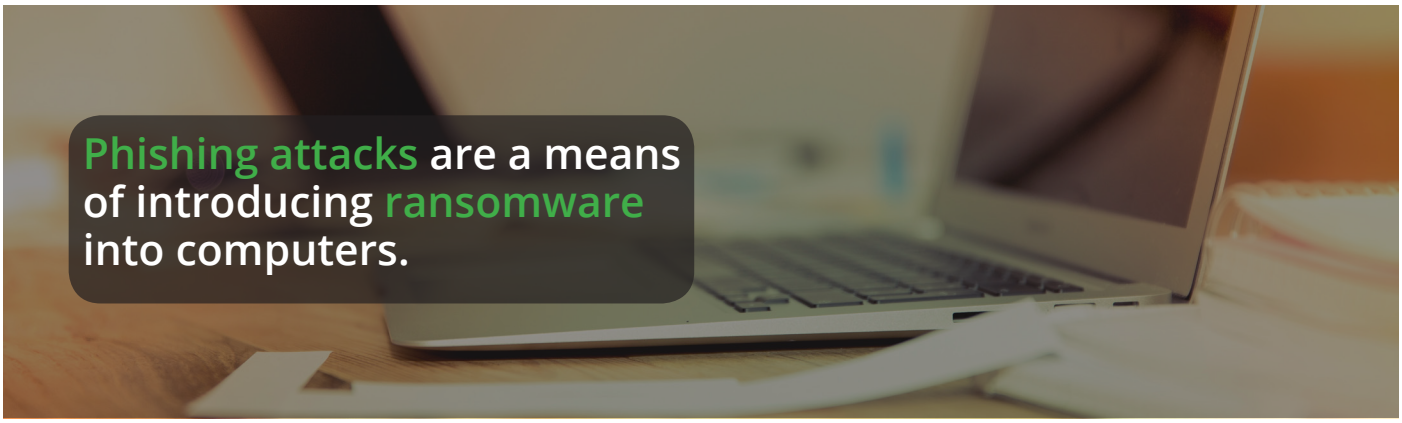
Misconfigurations and weak security policies provide a potential entry point for ransomware. For example, if "autorun" is enabled for USB drives, it can be potentially used by ransomware to install and execute malware. Having strict policies and ensuring compliance with policies reduces the risk of ransomware.

3. Keep an off-line, up-to-date backup of all files in the system

When a successful ransomware attack has been carried out, the personal files on the system are compromised and encrypted. This makes it impossible to read the files unless the decryption key is available. One easy way of recovering from an attack of this nature is to keep an up-to-date backup of all files on the system so that data can be recovered.

4. Stay informed about phishing techniques

Phishing attacks are a means of introducing ransomware into computers. It is important for everyone to be aware of common phishing emails, and the dos and don'ts of what to do when a suspicious email is received.



The Saner Solution to Prevent, Detect, and Respond to Ransomware

Prevention is the first step to reduce the risk of a ransomware breach. However, prevention alone is not sufficient in the case of ransomware. Attacks can happen when a user clicks on an innocuous-looking email attachment. Detecting such attacks in real time is critical to security. Limiting the potential damage and protecting systems from future attacks is critical to ensuring the security of the enterprise.

Saner uses a multipronged approach to detect and respond to ransomware attacks. Saner is an endpoint security platform that provides continuous visibility and control over endpoints. Saner stresses prevention and achieves a reduction in security incidents by ensuring all endpoint systems are constantly kept up to date with the latest patches. This ensures malware cannot exploit known vulnerabilities. Saner also detects threats and includes a variety of remediation measures to instantaneously contain or block an attack. Threat Intelligence Feeds automatically detect Indicators of Compromise in seconds.

➢ Prevention

Saner's first level of defence is prevention. Saner remediates endpoint systems to remove all known vulnerabilities. Removal of vulnerabilities effectively blocks the ability of ransomware to exploit known vulnerabilities. Since known vulnerabilities provide a major gateway, this substantially reduces the entry point and opportunity for ransomware attacks.

Often ransomware exploits lax compliance with strict hardening rules to attack endpoint systems. Saner's compliance management component ensures that endpoint systems are hardened and stay compliant with defined policies. Deviations are monitored and corrected in real time. This further reduces the risk of ransomware by eliminating potentially easy paths through which ransomware can enter the system.

➢ Detection

Often ransomware enters systems as an attachment to an email, through a phishing attack. The user clicks the attachment — which triggers the ransomware attack. The attachment is usually innocuous-looking – made to appear as a genuine artefact from a company or somebody he or she corresponds with regularly. However, the attachment is actually an executable that launches the ransomware.

When ransomware enters a system through this channel, it is of utmost importance to detect the launch immediately. Saner detects ransomware using an up-to-date threat intelligence database that contains the latest ransomware threat feed. If an attacker is successful in getting through with an email attachment, Saner uses the threat feed to detect the ransomware.

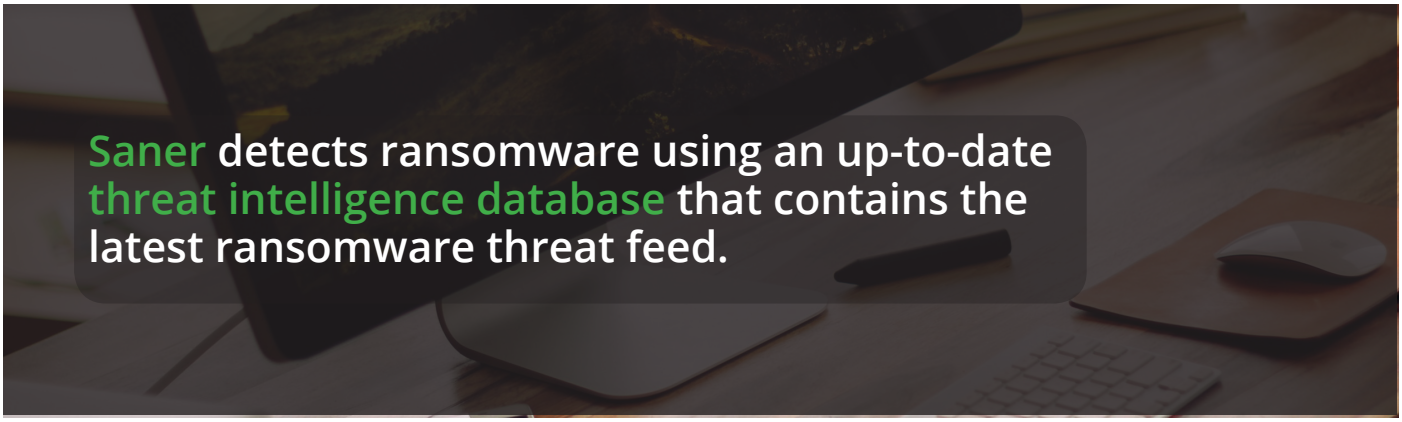
In addition to threat intelligence, Saner uses known behavioural patterns of ransomware to detect an ongoing attack. Such behaviour includes connecting to a server to procure the key for encryption, modifying certain registry keys, and creating new registry keys. Additionally, if the attack is actually in progress, a large number of files with specific extensions are updated. Some variants create files with a new extension. For example, Locky ransomware creates files with an extension .locky. Saner detects these events in real time.

With this multipronged approach, Saner reduces the risk of ransomware infecting a system and helps contain damage.

➢ Impact Analysis and Containment

Saner's ability to detect and alert the administrator to an ongoing attack is a crucial part of a response strategy. With its admin interface, Viser, the administrator is quickly alerted to an ongoing ransomware attack. In such cases, the administrator can prevent greater damage by responding to those incidents before the ransomware has a chance to encrypt the contents of the network file systems. This significantly reduces damage from ransomware by preventing encryption of files on network drives connected to the affected computer.

In the event of a successfully launched attack, enterprises should be in a position to minimise the damage it causes. Successfully launched ransomware can wreak havoc by encrypting not only files on the user's disk, but also files on network drives connected to the system. Responding to such an attack requires reliable information about what has transpired in the affected systems, and the risk faced by other systems in the enterprise. Saner produces comprehensive reports by running relevant queries. This information is crucial for the enterprise to assess the extent of damage to systems and the potential for damage. These reports help in creating a meaningful response strategy.



Conclusion

Ransomware is quickly becoming ubiquitous, and the choice tool for cybercriminals.

In this whitepaper, we presented an in-depth look at how ransomware enters a system and four ways to prevent it. We saw how ransomware exploits vulnerabilities, misconfigurations, and social engineering. We have understood how detection and prevention reduce the risk of ransomware infecting a system and how to protect endpoints.

Ransomware can arrive via emails, downloads or other techniques. To avoid becoming a victim of ransomware it is imperative to improve security, apply basic security practices to protect confidential and sensitive data. Apart from this, always:

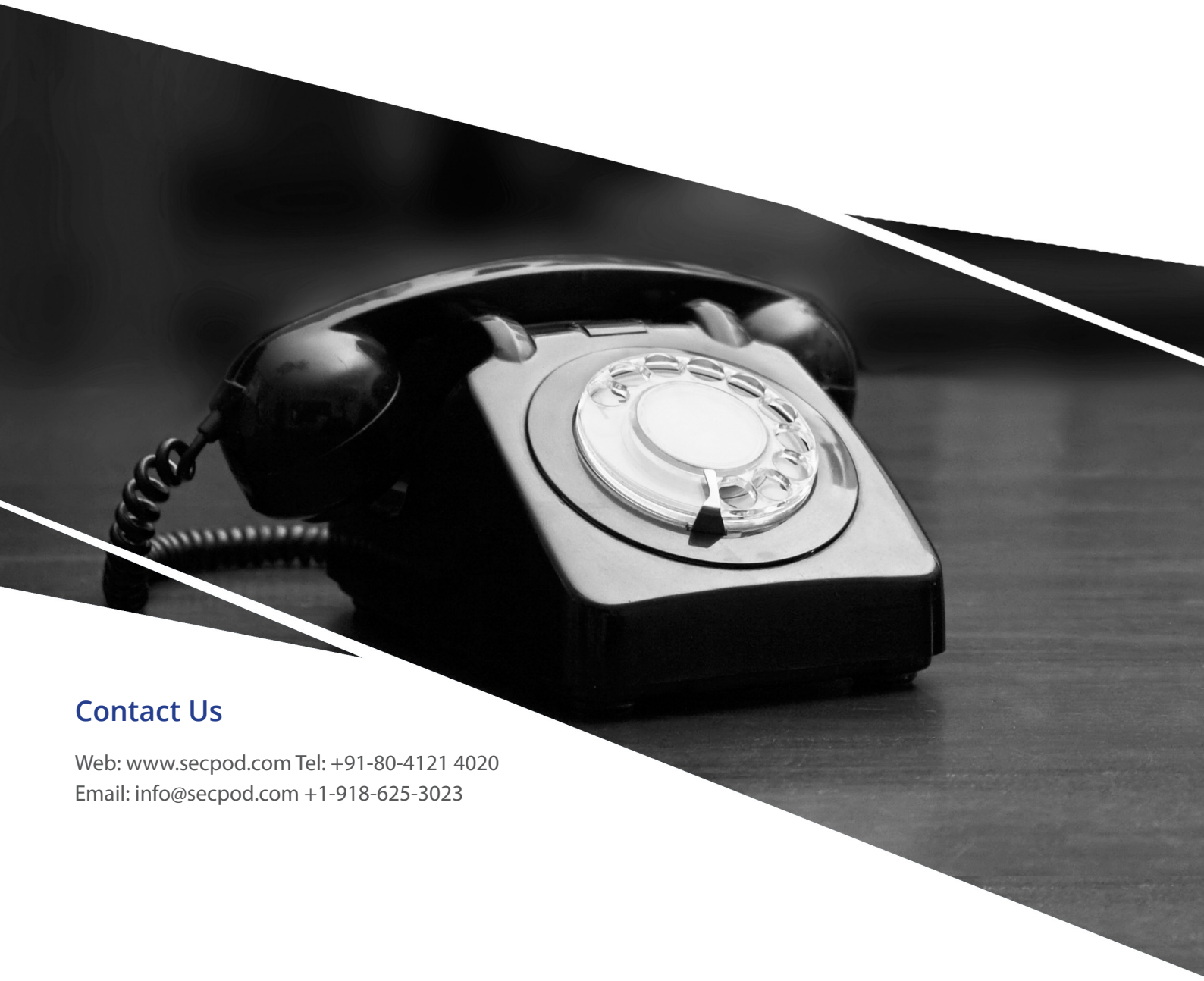
- Fix vulnerabilities with SecPod's Saner endpoint security solution
- Backup important data
- Continuously monitor detection of such attacks through Saner
- Apply a response strategy provided by Saner to prevent or contain attacks

References

SC Magazine: Hackers shift to Neutrino exploit kit to spread CryptXXX ransomware
Dark Reading: Here are 4 Vulnerabilities Ransomware Attacks Are Exploiting Now
IEEE: Cryptovirology: Extortion-Based Security Threat and Countermeasures
CNN: Cyber-extortion losses skyrocket says FBI
SecPod Technologies: SecPod Solution

About Us

Founded in 2008 and headquartered in Bangalore with operations in USA, SecPod Technologies creates cutting edge products to ensure endpoint security. We strongly believe in the principle 'Strong Defense, Not a Weak Cure' and our product Saner Business reflects this ideology by proactively detecting and eliminating vulnerabilities before they can be exploited. We have been entrusted by Enterprise and mid level organizations in various verticals including Government, Healthcare and IT/ITES .



Contact Us

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