SentinelOne

# The Rise of Ransomware & How to Defend Against it

## OVERVIEW

Over the last few years, ransomware has emerged as one of the most devastating and costly attacks in the hacker arsenal. Cyber thieves are increasingly using this form of attack to target individuals, corporate entities and public sector organizations alike by holding your system or files for ransom. Unlike other forms of cyber theft that often involve stolen financial or healthcare information, ransomware acts directly in front of the victim, holding their system or data hostage until a ransom payment is made.

Ransomware is a quickly growing threat vector. Recent research published in "Dark Reading" shows that ransomware samples have grown over 127% from mid-2014 to mid-2015, and "SC Magazine" reported that mobile ransomware has increased by 65% over just a single quarter. The attack is also successful in "turning high profits" for hackers. A recent survey conducted by a Cyber Security Research Center at the University of Kent found that over 40% of those infected with Cyptolocker actually agreed to pay the ransom demanded, which is a big incentive for hackers to target more systems.

While many endpoint security products including traditional antivirus, host IPS, clustering and sandbox technologies have tried to prevent ransomware attacks, none of these solutions have been successful in preventing this latest form of attack. SentinelOne is the first and only "Next Generation" Endpoint Protection Platform (EPP) that successfully detects and prevents ransomware-based attacks. We'll now discuss in more depth how ransomware works and how SentinelOne protects against it.

## WHAT IS RANSOMWARE?

Ransomware is a type of malware that infects a computer and takes either control of the core operating system using lockout mechanisms or possession of data files by encrypting them. The program then asks the user to make a "ransom" payment to the malicious individual or organization in order to remove the locks and restore the user's endpoint or files.

Less sophisticated malware simply locks the user out of the system, preventing them from logging in and accessing programs and data on their device. More advanced forms of ransomware will target specific data files such as sensitive documents, spreadsheets, PDF files, pictures and videos. These files are encrypted with advanced cryptographic techniques so that they become inaccessible for use. This more advanced mechanism may also traverse network shares and hold hostage data files that are present on shared drives and online file storage/sharing services. The malware will also use very long encryption keys making it virtually impossible for the user to circumvent the extortion demands. In either case, once infected, a computer or the data files cannot be used without the decryption key. In many cases, even when the ransom has been paid the ransomware will remain, lying dormant on the hard drive which makes this threat even more concerning.


***Fig 1.*** *Reveton ransomware taking over an endpoint, with removal instructions*

## RANSOMWARE EXAMPLES

**Some notable examples of ransomware are:**

### REVETON

This malware did not encrypt files, but rather blocked internet access with a fake law enforcement warning demanding payment to restore access. Reveton falsely warned victims that their computers had been identified by the FBI or Department of Justice as being associated with child pornography websites and other illegal online activity.

### CRYPTOLOCKER

This malware has surfaced in many different variations, and is one of the most recognizable examples of this ransomware attack. CryptoLocker was first was reported in late 2013 and was one of the first to employ the encryption/ransom technique. Originally it also claimed to only allow 72 hours before the decryption key was permanently deleted.

### CRYPTOWALL/CROWTI

This is a recent CryptoLocker variant in this family, and Cryptowall first appeared in 2014. This variant employed more sophisticated attack methods and techniques to hide itself from traditional antivirus software. Cryptowall also attempts to delete shadow copies of files eliminating a common method of lost data recovery and thus making it even more damaging and resistant.

To decrypt the files and allow the victim to recover from an attack, these tools require payment using either cash cards or BitCoin. The threat actors mostly operate out of TOR websites in an effort to obfuscate their identities. Payments typically range from $200 to $500, although it is not uncommon for the extortion scheme to run into tens of thousands of dollars per victim. Once paid, a decryption key may be sent which is used to recover the locked system or files – although as can be expected in a criminal enterprise, this is not guaranteed.


***Fig 2.*** *Cryptolocker is more sophisticated ransomware that selectively encrypts data files*

## HOW DOES RANSOMWARE WORK?

Ransomware follows an attack pattern that consists of 5 steps. In most cases, these steps take less than a few seconds to execute. Even the most benign activities can result in the endpoint becoming a victim of ransomware, and your personal and/or business critical files becoming hostage to extortion.

### **Step 1:** Targeting

Ransomware has primarily targeted endpoints running the Microsoft Windows operating system, although attacks targeting Mac OS X and mobile platforms are on the rise given their increasing popularity. Users in specific geographic regions like Russia, Brazil and of course the US have seen the bulk of ransomware attacks. Because websites are a mechanism for the hackers to initiate the attack through hidden redirects and drive-by-downloads, hackers will also focus their attention on public websites running vulnerable web- or application-servers that they can leverage. This avenue is particularly dangerous if the hacker is able to find vulnerabilities in banking, online commerce or other payment websites.

### **Step 2:** Propagation

Ransomware is usually propagated through the use of spear-phishing emails that have malicious attachments. These attachments are often Trojans in the form of MS Office or Adobe PDF documents, but have the ransomware embedded within them. Also common are websites hosting the malicious ransomware. Users are directed to these websites using fake pretenses and are victimized through "drive-by-download" attacks causing the ransomware to install itself on their device. Very often, ransomware seems to come from legitimate sources, including financial institutions, government entities or for corporate users, from someone within their organization. This could be in the form of email or websites. Some examples that hackers have used include the pretending to be the FBI, the IRS and multinational banks.

### **Step 3:** Exploit

Many hackers today use malware packaged into exploit kits that they covertly place on legitimate websites, or host on fake websites designed to look like a legitimate site. When a potential victim's browser lands on a website hosting such an exploit kit, the kit probes the visitor's system and extracts information like OS, browser type, version information and applications installed to find and exploit vulnerabilities. Once the exploit kit has found a security vulnerability that it can exploit, the attack proceeds to the next step.

### **Step 4:** Infection

In the infection stage, the previous steps are used to download and install a "payload" to the victim's endpoint or mobile device. This payload could be the actual ransomware itself, or it could also be a hidden malicious downloader like Upatre which then creates a backdoor through which multiple types of malware can be downloaded and many different attacks can be executed.

### **Step 5:** Execution

Once the ransomware has been installed on the victim's endpoint, the actual execution of the malicious program starts doing what it is designed to do – which is disable the system's critical operation or find and encrypt the data files on the endpoint. At this point the disruption directs the victim to the hacker's monetization mechanisms with instructions on where to send the ransom, in what form to make the payment (usually BitCoin) and other details to ensure the victim complies with the hacker's instructions.

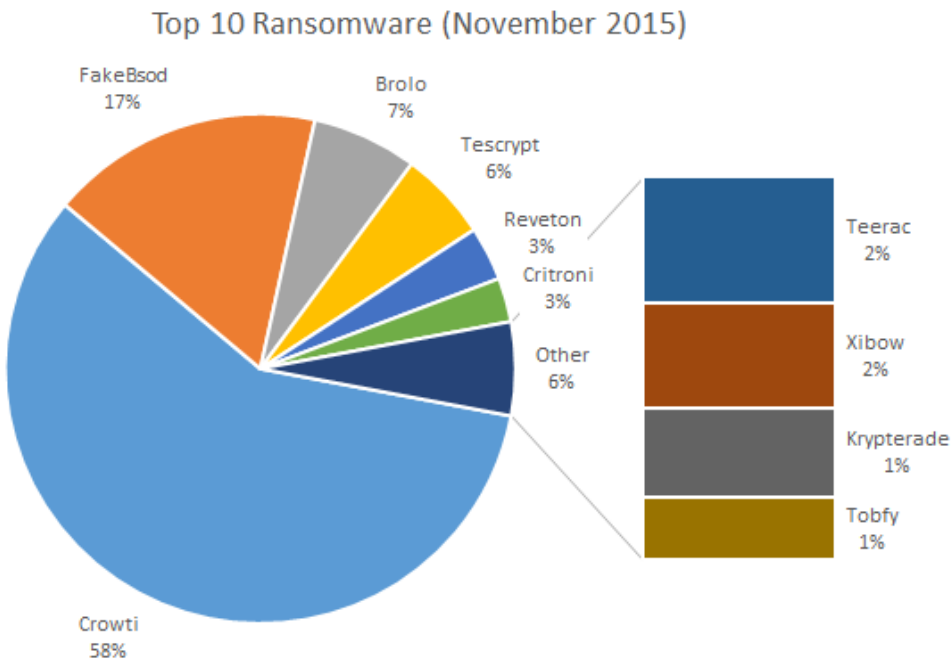



***Fig 3.*** *Crowti/Cryptolocker has recently emerged as the most common form of ransomware (Source: https://www.microsoft.com/security/portal/mmpc/shared/ransomware.aspx)*

## WHAT CAN YOU DO IF YOU'RE INFECTED?

**Unfortunately there is little you can do to recover your files once your system is infected with a ransomware attack, but here are a few tips that can help prevent it from spreading and you to be a victim of a repeat attack.**

### 1 ALERT LAW OFFICIALS.

They probably won't be able to help, but like any ransom activity, they should be informed.

### 2 ISOLATE THE INFECTED MACHINE.

It's important that the system is taken offline, as they essentially own your machine now and can use it to gain access to other systems on the network.

### 3 DON'T PAY THE RANSOM.

As with any form of ransom, you are not guaranteed to get your data back, and you're just encouraging attackers to keep up their lucrative game. In addition, if you pay and actually get your keys once, you may be the target of a repeat (and potentially more costly) ransom attack in the future.

### 4 REMEDIATE.

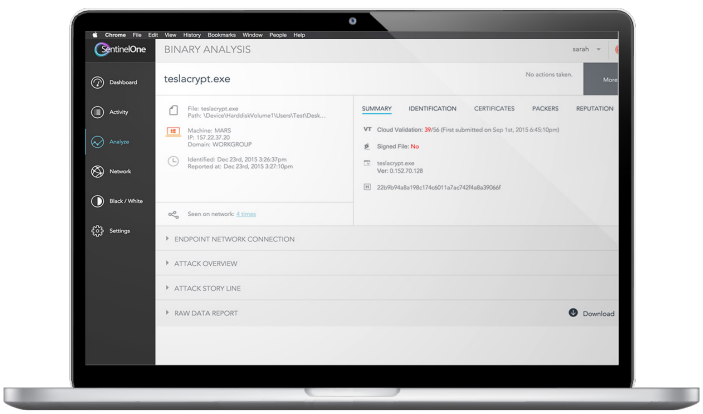
Run endpoint security software to discover and remove the ransomware software. If it cannot detect the threat, wipe your machine.

### 5 RESTORE.

Restore your files with the most recent back-up.

## SENTINELONE: THE ULTIMATE RANSOMWARE DEFENSE

It is obviously best to prevent the ransomware attack from occurring, as recovery is difficult. SentinelOne is the only endpoint security software that protects against unknown forms of ransomware. SentinelOne's EPP uses a groundbreaking Predictive Execution Inspection Engine that goes beyond file based analysis – even mathematical algorithmic analysis – that observes the actual execution of every system process or thread, in real-time. By understanding the execution behavior of all applications, programs and processes in real-time, SentinelOne EPP provides the ultimate defense against ransomware.




**SentinelOne provides the following features for protection against ransomware:**

- **Real-Time Behavioral Detection**: SentinelOne is focused on real-time code execution rather than static markers for threat detection. This execution engine is able to monitor all endpoint processes, add full context for every process and then predict advanced and hidden ransomware attacks based on the execution behavior of the suspicious software. The focus on process execution can find and prevent ransomware that evades static detection techniques, and remains hidden to most other security products.
- **Predictive Execution Inspection**: Unlike static filters that analyze files and persistent elements of the ransomware, SentinelOne's Execution Inspection engine allows and monitors limited execution of all suspicious software, including memory-based and script-based ransomware to understand its behavior. We are able to detect and respond to what is happening on the endpoint as it happens. This allows SentinelOne to find extremely advanced ransomware that does not have any disk or file activity, that does not leave any indicators of compromise and that uses sophisticated embedding techniques to mask its activity.

- **Kernel-Space Operation**: The SentinelOne agent operates in the kernel-space. This allows SentinelOne to perform the protection, detection and response with an extremely small footprint compared to other products. In addition to the performance advantages, the SentinelOne agent provides protection from all vectors while being highly tamper resistant to ransomware attempts that try to evade or disable the agent.
- **Roll-back**: Ransomware among other forms of malware specifically relies on encrypting or obfuscating system and data files as an attack vector. Many of the sophisticated ransomware variants being used today go one step further and eliminate the victim's ability to recover encrypted data by destroying the "shadow copies" created by the operating system. These shadow copies are used in data recovery operations by IT professionals as well as the OS itself e.g. when it recovers from critical system failure. SentinelOne is the only solution that saves and protects the shadow copies of data files, making it uniquely capable of helping victims recover from a ransomware infection.
- **Automatic Response and Mitigation**: SentinelOne is the only solution that provides full Endpoint Protection as well as Endpoint Detection and Response (EDR) in a unified platform. Our ability to provide a single product that covers detection, prevention and response is unique. We have been certified by AV-TEST and are a true replacement for all endpoint security products – including traditional antivirus as well as newer security products.
- **Broad Platform Support**: While ransomware largely targets Windows based endpoints today, other platforms particularly Mac OS X and mobile OSs are becoming more common targets. In addition to Windows, SentinelOne EPP supports Mac OS X, as well Android and iOS mobile devices, providing device coverage across the endpoint attack surface area. SentinelOne EPP also supports a variety of virtual environments and has Linux support in the queue, an increasingly relevant operating system due to the increase of Linux server deployments.

## CONCLUSION

Individuals and corporations alike are struggling with the problem of ransomware. Users continue to bridge the gap between "personal" and "company" devices, and BYOD policies make accessing all kinds of data from any device a reality. At the same time threat actors are pouring their energies into developing increasingly advanced techniques to evade legacy defenses that rely on static signatures as well as new, seemingly innovative solutions to endpoint protection. The only way to ensure ransomware does not hold your device or data hostage for extortion is by using SentinelOne's Endpoint Protection Platform.

For more information on SentinelOne, visit **www.sentinelone.com**