Ransomware: Best Practices for Prevention and Response

**MAY 31, 2017 • SEI BLOG**

[*Alexander Volynkin*](https://insights.sei.cmu.edu/author/alexander-volynkin)

[Cyber Missions](https://insights.sei.cmu.edu/sei_blog/cyber-missions/) [Best Practices in Network Security](https://insights.sei.cmu.edu/sei_blog/best-practices-in-network-security/) [Network Situational Awareness](https://insights.sei.cmu.edu/sei_blog/network-situational-awareness/) [Ransomware](https://insights.sei.cmu.edu/sei_blog/ransomware/)

*This blog post is coauthored by Jose Morales and Angela Horneman.*

On May 12, 2017, in the course of a day, the [WannaCry](https://en.wikipedia.org/wiki/WannaCry_ransomware_attack) [ransomware](https://en.wikipedia.org/wiki/Ransomware) attack infected nearly a quarter million computers. WannaCry is the latest in a growing number of ransomware attacks where, instead of stealing data, cyber criminals hold data hostage and demand a ransom payment. WannaCry was perhaps the largest ransomware attack to date, taking over a wide swath of global computers from FedEx in the United States to the systems that power Britain's healthcare system to systems across Asia, [according to the *New York Times*.](https://www.nytimes.com/2017/05/13/technology/hack-ransomware-scam-cyberattacks.html) In this post, we spell out several best practices for prevention and response to a ransomware attack.

**Data Encryption: A Key Component of Malware**

Ransomware, in its most basic form, is self-explanatory. Data is captured, encrypted, and held for ransom until a fee is paid. The two most common forms of ransomware delivery are through email and websites.

Although ransomware has been around in some form or another for decades--[the first known attack is believed to have occurred in 1989](https://en.wikipedia.org/wiki/AIDS_(Trojan_horse))--it has more recently become the modus operandi of cyber criminals across the globe. Ransomware has been continuously evolving in the past decade, in part due to advances in cryptography. The wide availability of advanced encryption algorithms including RSA and AES ciphers made ransomware more robust. While estimates vary, the number of ransomware attacks continues to rise. The [Verizon 2017 Data Breach Investigations Report](https://www.verizondigitalmedia.com/blog/2017/07/2017-verizon-data-breach-investigations-report/) estimates that (pre WannaCry) ransomware attacks around the world grew by 50 percent in the last year. Symantec, in [a separate report](https://thycotic.com/company/blog/2017/04/27/top-takeaways-from-symantecs-internet-security-threat-report-2017/), estimated that the average amount paid by victims had risen to $1,077.

Several factors have fueled the recent rise in ransomware attacks:

* [Bitcoin](https://en.wikipedia.org/wiki/Bitcoin) has been a significant factor in the rise in ransomware attacks. The lack of oversight by any governing body coupled with anonymity makes it an ideal currency in ransomware demands.
* The evolution of [ransomware-as-a-service (RaaS)](http://blog.trendmicro.com/outsourcing-crime-how-ransomware-as-a-service-works/) has also played a significant role in the proliferation of attacks. RaaS has moved the execution of a ransomware attack from "professional" to "[script-kiddie](https://en.wikipedia.org/wiki/Script_kiddie)."
* Operating systems lack runtime detection capabilities that could help stop ransomware execution in the early stages possibly even before actual encryption begins."
* Another reason that ransomware continues to proliferate, despite classic delivery methods such as email, is that users have not been properly trained or made aware of the dangers of opening malicious email attachments. This trend highlights a need among organizations to improve web and email security and user security awareness.  
    
  On a separate-but-related front attackers are getting increasingly skilled at social engineering. Many of the markers that used to be applicable for identifying malicious email (e.g. mis-spellings, bad punctuation, improper capitalization, unknown "from" addresses) are absent in a lot of malicious email today. Advances in online translators and spell-checkers help crafting appealing phishing narratives while it has become increasingly difficult for a user to identify spoofed email addresses.

**An Ounce of Backup**

The single most effective deterrent to ransomware is to regularly back up and then verify your system. More recent ransomware attacks have not only encrypted data files but also [Windows system restore points](https://msdn.microsoft.com/en-us/library/windows/desktop/aa378910(v=vs.85).aspx) and shadow copies, which could be used to partially restore data after a ransomware attack. Backups should be stored on a separate system that cannot be accessed from a network and updated regularly to ensure that a system can be effectively restored after an attack.

Other effective mitigation strategies include the following steps:

* **Educate employees.**Like other malware, ransomware often infects a system through email attachments, downloads, and web browsing. Organizations should conduct regular training to help employees avoid common malware pitfalls.
* **Conduct regular data backups**. This bears repeating. Conduct regular backups of your system and store the backups offline and preferably offsite so that they cannot be accessed through your network (For ransomware, offline is more important. For other events, offsite is more important).  
    
  On a separate-but-related front, it is also important to regularly verify the data backup process to ensure backups are capturing all necessary data and that the restore process works in your environment. At a home/personal level, backup important files as they are modified and be sure that backup media (thumb drives, external hard drives) are not left connected to any networked device. Periodically check that the files can be accessed from the backup device. You don't want to discover that it is defective at the point you need to restore data from it. It is also important to point out that popular online backup solutions may also be vulnerable to a ransomware attack as the backed up data may be overwritten with newer version that is already encrypted by ransomware.
* **Restrict code execution.**If ransomware is designed to execute from temporary and data folders, but it cannot access these folders due to access control, that could be a successful roadblock to data encryption.
* **Restrict administrative and system access.** Some strains of ransomware are designed to use a system administrator account to perform their operations. With this type of ransomware, decreasing user accounts and terminating all default system administrator accounts can create an extra roadblock.
* **Maintain and update software.**Another important yet basic rule for protecting against and/or ensuring early detection of ransomware is to maintain and update software, in particular security and anti-malware software.

**System-Level Protection.**

While it is impossible to completely block ransomware at its two most common points of entry (i.e. email and websites), steps can be taken at the system-level that will reduce (but not completely eliminate) ransomware attacks. First and foremost, it is important to note that current [anti-malware](https://en.wikipedia.org/wiki/Comparison_of_antivirus_software) products *should* be able to detect and block ransomware at the file and process level before data can be compromised. A well-designed anti-malware product *should* also be able to scan email attachments and downloads for malicious content. I emphasize *should* in these statements because ransomware evolves so rapidly that it is not a guarantee that even up-to-date anti-malware products will detect the latest strains.

For email consider the following practices:

* **Robust filtering** is one of the most important steps an organization can take. Logically, chances of an attack will be reduced if employees receive fewer emails that contain spam or potentially malicious attacks.
* **Blocking attachments**is an important step in reducing the attack surface. Ransomware is often delivered as some form of executable attachment: direct executables (e.g. .exe, .js, or anything else that can be executed), Microsoft Office files containing macros, .zip files that either contain executable files or are executable themselves (i.e. named .zip, but really .exe). It is therefore important to have a policy in place that these cannot be sent by email, and that any attachments will be removed by the email security appliance.
* **Reviewing permission-related practices**is an important practice because many of these practices can play an important role in mitigating the impact of a ransomware attack including the following:  
    
  + **Removing local administrative rights**can deter ransomware from running on a local system and prevent its spread by crippling the critical components of any ransomware attack: the power to change system files and directories as well as system registry and storage. The removal of local administrative rights also blocks access to any critical system resources and files that ransomware is targeting for encryption.
  + **Other permission-related practices** include restricting user write capabilities, preventing execution from user directories, whitelisting applications, and limiting access to network storage or shares. Some ransomware requires write access to specific file paths to install or execute. Limiting the write permission to a small number of directories (e.g., User/Document and User/Downloads) will prohibit ransomware variants from successfully carrying out their actions.  
      
    Additionally, ransomware executables can be blocked by the removal of execution permission with those directories. Many organizations use a limited set of applications to conduct business. Non-white-listed applications including ransomware can be blocked from executing by maintenance of a whitelist-only policy for applications.  
      
    A final permissions practice that could blunt the impact of ransomware and prevent it from spreading is to require a login at access points such as local and mapped drives.

**At the Network Level**

At the network level, it has proved more difficult to mitigate and prevent the spread of ransomware. Firewalls that implement whitelisting or robust blacklisting will be a successful deterrent to lessening the likelihood of successful web-based malware downloads and may deter ransomware from connecting to command-and-control servers.

At the network level, firewalls should limit or completely block [remote desktop protocol](https://msdn.microsoft.com/en-us/library/aa383015(v=vs.85).aspx) (RDP) and other remote management services. Also, deploy spam-detection techniques, such as spam lists, to prevent compromised emails from reaching users' inboxes. Another strategy is to limit the types of file extensions that can be delivered via email.

Once an internal host has been infected, preventing the further spread of the ransomware to other computers within the network can prove more difficult. The single most effective method for preventing ransomware from spreading to other computers is to disconnect it as soon as possible including wired connections, Wi-Fi, and Bluetooth connections. Automated backups to local or external storage should also be disabled.

**In the Event of a Ransomware Attack**

While these practices are effective, it is impossible to completely protect your organization from ransomware. If you do believe you have been the victim of a ransomware attack, consider the following steps:

* **Take a snapshot of your system**. Prior to shutting down your system, if it is at all possible, try to capture a snapshot of the system memory. This will help later in locating the ransomware's attack vector, as well as any cryptographic material, which can help with decrypting data.
* **Shut down your system.**To prevent the further spread of the ransomware and inevitable damage to data, shut down the system believed to be infected.
* **Identify the attack vector.**Recall all emails suspected of carrying the ransomware attack to prevent further spread of the attack.
* **Block network access to any identified command-and-control servers used by ransomware.**Ransomware is often blocked from encrypting data without access to these servers.
* **Notify authorities**. Consider informing authorities so they can help with the investigation. While law enforcement can assist with an investigation, it also increases the risk that data may never be recovered. Ransom payments tend to go up as time passes for the payment to be made. Involving law enforcement could also delay and add significant cost to the ransom if ultimately the user(s) decide to pay.

**Wrapping Up and Looking Ahead**

Fueled by easier access and greater financial payoff, the number of ransomware attacks will continue to grow with criminals targeting larger organizations, government, education, and healthcare. Driven by a successful business model that guarantees anonymity, the sophistication of ransomware technologies will also continue to evolve. The level of encryption in ransomware is fast approaching the level of encryption seen in commercial security products.

While law enforcement and government entities continue to work to tackle this problem, employing best practices can help organizations protect against and mitigate ransomware attacks.

**Additional Resources**

View the [SEI Cyber Minute on mitigating ransomware](http://resources.sei.cmu.edu/library/asset-view.cfm?assetid=485786).