Defending Against

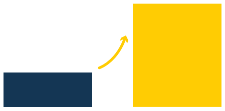
Ransomware

SEP

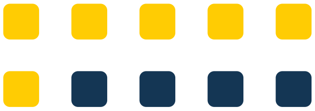
Contents

Introduction

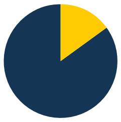
Ransomware is today's number one security threat. The U.S. is still the country most affected by ransomware, followed by Japan, Italy, India, Germany, Netherlands, UK, Australia, Russia, and Canada. And now each version seems to be more powerful, destructive, and difficult to detect and eliminate than the last.



The number of ransomware attacks on businesses tripled during 2016, jumping from one attack every two minutes in the first quarter to one every 40 seconds by the third quarter.



Ransomware is the malware of choice. Six out of every ten malware payloads were ransomware in the first quarter of 2017.



Fifteen percent or more of businesses in the top ten industry sectors have been attacked, with education being the highest at 23 percent.

4.3x

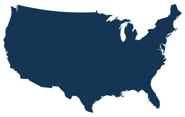
There were 4.3 times more new ransomware variants in the first quarter of 2017 than in the first quarter of 2016.

5MM

In May 2017, a new Ransomware variant called Jaff was involved in nearly 5 million attack emails per hour.

$5B

Global ransomware damages exceeded $5 billion in 2017.



The United States continues to be the country most targeted with ransomware during 2017 and into 2018, accounting for approximately 29 percent of all infections.

What Is Ransomware?

Ransomware is malicious software that either encrypts or scrambles files on a computer or completely locks out the user. Ransomware hackers then demand a ransom (hence the name) to deliver a decryption key that allows you to recover your data. But that is not always the case. Some Ransomware has been around for a long time and both the original authors and the keys may be missing. So paying the ransom will not assure that the affected parties will ever recover their data.

The first recorded ransomware attack happened in 1989, when evolutionary biologist Joseph Popp deliberately infected floppy disks with the AIDS Trojan and distributed them to fellow researchers. The malware was programmed to wait until users booted their computers 90 times before activating. At that point, all system files were encrypted and became unusable. Popp then asked users to pay a grand sum of $189 to unlock their files. Instead, system experts were able to develop tools to unlock the files and remove the malware.

Ransomware is not a virus; the two infectors operate differently. Viruses infect software or files and can replicate your data. Ransomware scrambles files and renders them unusable, until ransom is paid.

How Can SEP Help?

SEP Software, the technology leader providing high-performance hybrid backup and disaster recovery solutions, is an expert in the disaster recovery preparedness and business community. SEP can advise companies on how to avoid such situations, and provide expert assistance creating a thorough backup and disaster recovery strategy to eliminate the possibility of blackmail in the event of a cyber-attack.

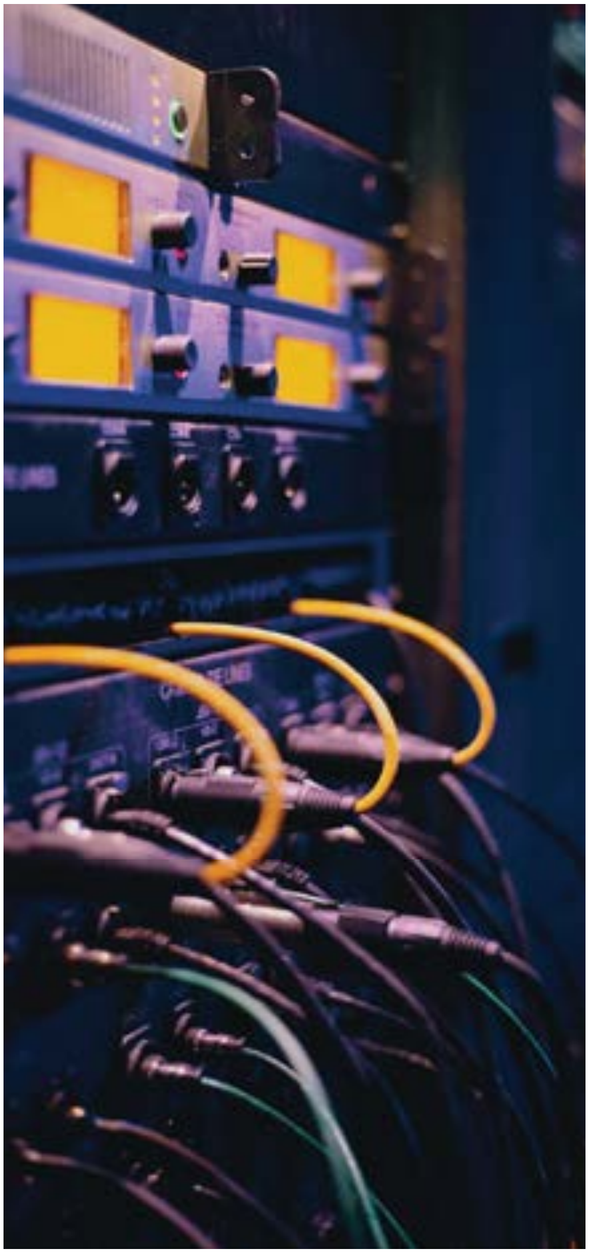
Using SEP as your backup software, a company can confidently restore all critical data after a ransomware attack. When businesses first recognize they have been the victim of a cyber-attack, it is too late to prevent critical data loss or data held ransom by unauthorized encryption. Most often, virus protection software either failed to recognize the intrusion or recognized it after encryption was already in progress.

After an attack, a reliable and safe analysis of the infected data must take place before the system can be brought back online. In order to accomplish this, a robust and reliable backup and disaster recovery solution must be in place prior to the attack.

Multi-Platform Data Protection & Business Continuity

By implementing a business continuity strategy against ransomware utilizing both SEP backup software solutions and SEP Bare Metal Recovery (BMR), users can restore entire physical and virtual servers, operating systems, databases, and applications quickly and easily. This recovery method can be achieved within minutes, regardless of the type of hardware in use. SEP BMR is fully integrated into the SEP interface to ensure a fast and complete system recovery. The data flow for the entire enterprise data recovery operation can be controlled from a single management console.

The SEP Bare Metal Recovery (BMR) solution guarantees a fast and secure recovery of all company data. SEP ensures that in the event of a disaster, all data and information can be recovered to completely recreate the original environment.



Developing and Testing a Disaster Recovery Plan

- Do you have a Recovery Time Objective plan? How long would it take to restore all of your data? Could you be back up-and-running within a few hours if you had to restore everything?
- Do you have a Recovery Point Objective plan? When was your last backup completed? How much data would you lose if an attack occurred X hours in between backups?
- Are you certain that you would get all of your data back exactly how you need it?

Implementing a multi-layer security strategy – including anti-malware, personal firewall, hard disk and file encryption, DLP and more – is critical to protecting against growing cybersecurity threats.

Have An Information Security Program

Consider taking the following steps to put an effective security program in place.

1. Know where critical data is stored.
2. Inventory systems to discern the weakest link for intrusions.
3. Assess risk.
4. Implement workflow automation and simple IT use policies.
5. Monitor the effectiveness of your security policy.
6. Educate all users.

Protect Data

Network security is a good first line of defense in guarding against ransomware attacks. By implementing effective technology best practices, organizations can further protect their data and IT infrastructure.

1. Employ a multi-faceted security solution that includes keeping all systems and software updated with relevant patches, and protecting against file-based threats, employing download protection, browser protection, and firewall protection.
2. Define and employ a comprehensive prevention policy that includes endpoint and network policies and protection products (antivirus, antispyware, firewall, etc.). This policy should also limit the execution of unapproved programs on workstations, and limit a program's write capabilities.
3. Take volume level snapshots every 15 minutes and store them for a long time. Perform a system backup every 24 hours.
4. Implementing a strategy is only half the battle. Test your backups often and test your disaster recovery plan. Make sure your data is where you need it, when you need it. Using SEP BMR is easy. Use the SEP GUI to schedule periodic restores to confirm data veracity and that all systems are being backed up as planned.
5. Be sure all employees are educated on actions to take and not take when they receive suspicious emails or other communications.

Secure the Endpoint

Educating everyone who touches your data on good security habits is essential to keeping your business data secure. Much of this training is simple common sense.

1. Do not open attachments unless they are expected and from a trusted source.
2. Do not execute software downloaded from the internet unless it has been scanned for malware.
3. Be cautious when clicking links in emails or social media, even when received from trusted sources.
4. Encourage employees to report any suspicious behavior, emails, communications, or attachments right away.

What Can SEP Do After An Attack?

SEP backup software provides snapshot backups which can be restored to any type of media at any location, on-site, off-site, or in the cloud, using BMR. The data repository can be selected using a disk-to-disk or disk-to-disk-to-tape strategy. After a system has been infected with ransomware, all infected computers on the network must be disconnected and cannot be brought back online until the ransomware has been completely removed.

A replacement server, completely cleaned (scrubbed) of any ransomware must be used to restart the recovery process. The computer is loaded with the SEP software and all data can be restored to the new backup server. Once this is accomplished, you can reconnect the 'cleaned' servers, workstations, etc. to the network and begin to restore the data through the network. Last, the desired saveset is selected and the automated recovery to the selected servers begins.

Steps taken after the attack

If you become the victim of a ransomware attack, SEP can get you back up and running safely and quickly. After the attack is discovered, determine when the attack began and if any infected data was included in a backup. SEP is able to restore all data from any chosen backup point-in-time to a protected system. This protected system must be clean and free of all viruses and must not be connected to the network. Using the Read-Only-Mode, SEP can restore data to 'cleaned' servers, where your antivirus program has been used to rid the virus from infected computers. As the data is restored, it is checked by the anti-virus software to ensure that the infection will not be reintroduced into the new environment.

In the event the encryption command from the cybercriminals has not yet been executed and the data can still be read, SEP supports forensic Linux distributions, like KALI, that have been developed specifically for analysis after a cyber-attack. This provides the capability to check every backup, regardless of the source, e.g. on Linux, Windows Backup Servers, or Remote Device Servers. Any file can be opened and screened for the virus. The malware does not have any ability to re-infect the system during the forensic analysis.

Once the last uninfected backup data set is determined, SEP will restore all systems in a clean and usable state. Safety and anti-virus mechanisms must be updated and verified to prevent another attack. All systems can be restored and processes can return to normal.

Restoration and Rehabilitation Procedures after a Cyber Attack

The infection has occurred and has been detected by the IT Administrator.

1. Determine when the virus entered the system by analyzing recent full and incremental backups. Pinpoint the last successful set of backups before the infection. Using a forensic Linux program like KALI on a protected server, find the infected files by comparing backup records, begin to analyze the virus and remove it from all servers.
    - The backed up data will be restored from removable devices, like removable disk or tape, to the cleaned system disk drives and mounted using Read-Only-Mode.
    - Compare data sets from various points-in-time.
    - Restore data sets that have been confirmed to be clean of the virus.
2. Check that all systems safety and anti-virus mechanisms are updated and verified to prevent another attack.
3. Restart the systems and resume regular operations.
4. Continue regular backups and test restores to maintain the integrity of your data.

Conclusion

Cybersecurity has become a global epidemic as a consequence of unsecure corporate and customer data. With the explosion of ransomware attacks, it's doesn't make sense that some businesses are not taking the necessary precautions to protect themselves from these increasing attacks. Stay ahead of the curve and secure your critical data. If you haven't seen our product, this is a great opportunity to take a look.

Supporting the widest range of operating systems, databases, and applications, SEP is the perfect solution for IT professionals managing data protection and business continuity. SEP replaces multiple backup software products with a single solution for hybrid IT environments – physical, virtual and cloud.

SEP is incredibly simple to install and can be integrated into any system in a matter of hours. For more information, visit www.sepusa.com.

Appendix 1: Types of Ransomware

Ransomware varies in size and levels of damage they can cause, but they all have a single common factor: the ransom.

- **Crypto malware or encryptors** - These are the most common type of ransomware. The WannaCry variant of ransomware put thousands of lives at risk when it hit hospitals around the world and blocked medical staff from accessing patient files, and managed to extort over $50,000.
- **Lockers** - This variant infects operating systems to completely lock users out of their own computer and makes it impossible to access any apps or files.
- **Scareware** - This form of ransomware is fake software which claims to have found issues on a computer and demands money to fix them. Some variants lock the computer completely while others flood the screen with annoying alerts and pop-ups, making it almost impossible to use the computer.
- **Doxware** - Also called leakware, this variant threatens to publish the information it has gathered online unless payment is made.
- **RaaS (Ransomware as a Service)** - This is malware hosted by a hacker who handles everything – distributing the ransomware, collecting payments, managing decryptors – in exchange for a cut of the ransom.

Appendix 2: How Is Ransomware Spread?

Ransomware is spread through various means, called infection vectors. Let's briefly examine each of the popular vectors.

- **Email** - Email continues to be the primary distribution channel for ransomware. Botnets are used to send out large spam campaigns, often daily. The emails use simple social-engineering tactics to trick recipients into compromising their computers:
  - Open a malicious attachment that directly installs the ransomware.
  - Open a malicious attachment that initiates a second stage delivery through a downloader that downloads and installs the ransomware.
  - Click a link that initiates a download and installation of the ransomware.
  - Click a link that points to an exploit kit which will ultimately lead to the malware being installed on the computer.
- **Exploit Kits** - These work by exploiting vulnerabilities in software in order to install malware. Exploit kit attackers compromise third-party web servers and inject iframes into the web pages hosted on them. The iframes direct browsers to the exploit kit servers. Attackers can redirect users to exploit kits in a number of different ways:
  - Malicious links in spam email or social media posts
  - Malvertisements
  - Redirected web traffic from traffic distribution services
- **Self-Propagation** - The new variants of WannaCry and Petya employed self-propagation. Once one Windows system is affected on a Windows network, self-propagating ransomware will propagate, or spread, itself and infect other unpatched machines without any human interaction. The cybersecurity industry refers to this type of super-vigorous ransomware as a Ransomworm.
- **Malvertising** - Malicious ads are placed through ad networks whose ads are distributed through trusted websites with a high volume of visitors. The visitor doesn't even have to click on the ad in some cases, as simply loading the web page hosting the malvertisement will lead to infection, often through redirection to an exploit kit.
- **Brute-Forcing Passwords** - This is an emerging tactic for spreading ransomware and is often used on servers that host cloud-based software. Brute-forcing is a trial and error method used by application programs to decode encrypted data such as passwords or Data Encryption Standard (DES) keys. It simply uses exhaustive efforts (using brute force) rather than employing intellectual strategies.
- **Exploiting Server Vulnerabilities** - Attackers will always target vulnerable software running on servers to gain access to an organization's network. These can include abusing database features, deployment errors, a lack of data segregation, SQL injections, and sub-standard key management.
- **SMS Messages and Third-Party App Stores** - An example of this can be seen with Android. Lockdroid.E, which poses as a pornographic video player on third-party app stores. Instead of playing adult videos, the app snaps a picture of the victim using the device's camera and includes the image as part of the ransom note.