CYBERARK®

Mitigate the Risks of Ransomware with Privileged Account Security

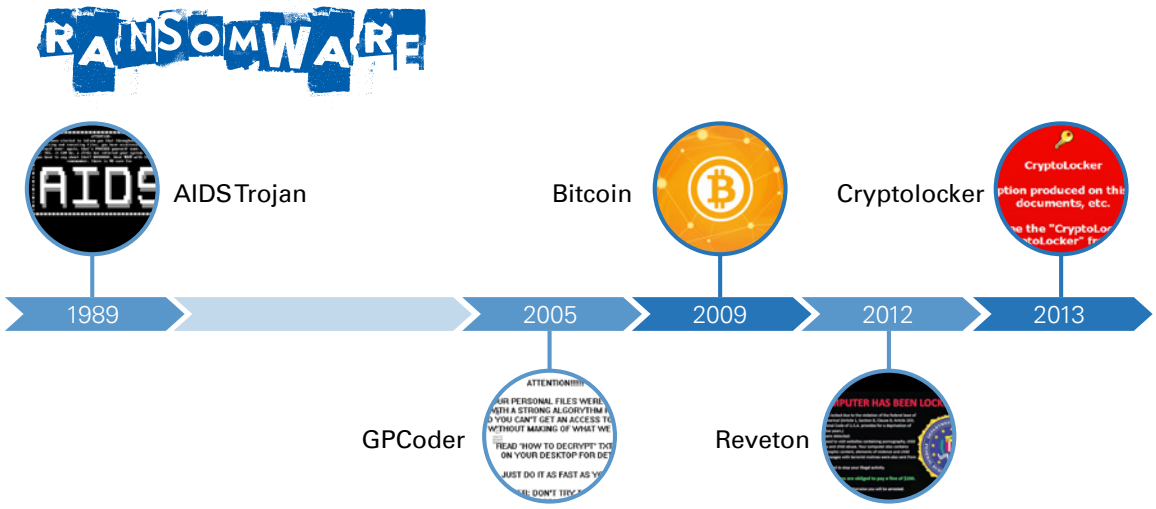
Solution Brief

Ransomware attacks are one of the latest trends in cyber security. Victims discover that they've been compromised by ransomware when an extortion message appears on their screen informing them that their files and data have been encrypted. Next, the attacker demands a fee in return for decrypting the files and too often, the victims' only option for recovering files is to pay attackers.

Ransomware yesterday, today, and tomorrow

Yesterday

A brief look at how ransomware has developed over the past few decades:



1989 – AIDS Trojan

The first known ransomware is introduced in 1989. Victims of the AIDS trojan received a disk in the mail titled "AIDS Information Introductory Diskette." Upon inserting the disk, the trojan encrypts file names on the C drive and hides directories making the operating system essentially unusable. In order to reverse the effects of the trojan, victims are instructed to send $189 USD to a P.O. Box in Panama.[1]

1 https://en.wikipedia.org/wiki/AIDS_(Trojan_horse)

2005 – GPCoder

In the mid-2000s multiple ransomware families are discovered in the wild including GPCoder, which encrypts files with a strong RSA encryption algorithm. Victims of GPCoder have to pay between $100 and $300 USD to an e-gold or Liberty Reserve account in order to decrypt the files.[2]

2009 – Bitcoin

Most ransomware variants start demanding payment in Bitcoin and include instructions on how to purchase Bitcoins and transfer them to the attacker. Bitcoin is the first decentralized digital currency. This anonymous currency is perfect for extortion because a new account can be created for every transaction, which means it's essentially impossible to trace payments.[3]

2012 – Reveton

The Reveton Trojan family impersonates the U.S. Federal Bureau of Investigation and locks victims out of their machine until they pay a "fine" to avoid prosecution for supposedly downloading child pornography and pirated content.

Symantec estimates that ransomware generates at least $5M per year by the end of 2012[4]

2013 – Cryptolocker

Cryptolocker compromises machines via phishing. Originally targeting consumers, the ransomware encrypts personal files and photos, and demands between $250 and $500 (an amount that most households are willing to pay).[5]

Today

There are thousands of ransomware variants in the wild today and new strings are discovered every day. Despite the proliferation of crypto families, there are some commonalities among most types of ransomware. First, they follow a common attack pattern:

Infiltration and installation. Ransomware enters the network via phishing or spam and quietly installs itself on the compromised machine.

Key exchange. Encryption occurs via an asymmetric key pair. The public key is sent to the compromised machine and the private key is hosted on the master server. The master server (run by the attacker) generates a unique encryption key for every compromised machine. This prevents multiple victims from paying the ransom once and sharing a decryption key.

Encryption. Within seconds, ransomware will scan and encrypt entire directories and files on the compromised machine.

Extortion. Once files are encrypted, the ransomware displays an extortion message in a local language that dictates a price and sets a timer, usually for only 48 to 72 hours. The message can also include instructions on how to acquire Bitcoin and transfer them to the attacker in return for decryption.

2 http://rump2008.cr.yp.to/6b53f0dad2c752ac2fd7cb80e8714a90.pdf
3 https://en.wikipedia.org/wiki/Bitcoin
4 http://www.symantec.com/connect/blogs/ransomware-how-earn-33000-daily
5 http://arstechnica.com/security/2013/10/youre-infected-if-you-want-to-see-your-data-again-pay-us-300-in-bitcoins/

In addition to the rise in popularity of these attacks, there is a shift in the target market for ransomware attacks. These attacks began by targeting individuals; ransomware encrypted photos and personal files, and attackers demanded a few hundred dollars for the decryption key. In the constantly evolving attack landscape, ransomware attacks have shifted from typically targeting individuals to now frequently targeting organizations. From one phishing attack, ransomware can compromise multiple endpoints within an organization and encrypt a wide range and large quantity of highly valuable data. With sensitive data at stake and encrypted files across potentially thousands of machines, organizations are able and willing to pay more than individuals, so attackers demand ransoms that can total tens of thousands to hundreds of thousands of dollars. According to the FBI, ransomware criminals have collected $209 million USD in just the first three months of 2016.[6]

Tomorrow

Ransomware attacks will continue to grow in severity as they target organizations and expand the scope of their attacks. Cyber attackers only need one compromised machine to begin an attack. A single compromised endpoint provides a valuable foothold for an attacker to move laterally and gain additional access to a network. As attackers continue to advance their techniques, ransomware will likely gain access to and encrypt more valuable data and hold it ransom for larger sums of Bitcoin.

As ransomware attacks continue to grow in popularity and in profitability for attackers, new variants and crypto families will likely continue to be developed at an increasingly rapid pace. The rate at which new variants are released makes it difficult for individuals and organizations to stay ahead of the attacker. For example, it's challenging for antivirus vendors and organizations to maintain and effectively enforce a blacklist to block known threats when new, unknown threats are released into the wild every day.

Defense tactics

There are many steps that organizations can take to mitigate the risk of ransomware causing significant damage.

Backup frequently – In the case that ransomware infiltrates a network, an organization can avoid paying the ransom if it's able to restore from the latest backup.

Patch systems regularly – Ransomware has been known to abuse vulnerabilities for which patches exist. Staying up-to-date with patching systems can help avoid this risk.

Train end-users – Ransomware infiltrates the network through spam and phishing. Educating end users on best practices for endpoint security can reduce the chance that ransomware will get in.

Continuously monitor activities – Oversight of network activities is critical for security teams to identify if and when a potentially damaging activity takes place (such as a malicious application executing).

Enforce endpoint security – The combination of privilege management and application control, including the ability to greylist applications, enables organizations to effectively mitigate the risk of malware attacks.

- **Remove local administrator rights –** Some ransomware requires administrator rights to execute, so removing local administrator rights can greatly reduce the attack surface.
- **Control and monitor applications –** In addition to whitelisting and blacklisting, greylisting helps mitigate the risk of ransomware by enabling unknown application to execute but restricting their access to files.

6 http://money.cnn.com/2016/04/15/technology/ransomware-cyber-security/

Mitigate the risk of ransomware with CyberArk® Privileged Account Security

CyberArk Privileged Account Security can enable organizations to mitigate the risk of ransomware with a combination of privilege management and application control. The CyberArk Labs team tested this approach against 23,000 samples of ransomware and found that, "it was 99.97 percent effective in preventing file encryption in cases when the infected user had local administrator rights, and it was 100 percent effective in preventing file encryption in cases when the user did not have local administrator rights."

By removing local administrative privileges from business users, organizations can reduce the attack surface while still allowing trusted applications requiring local administrator privileges to run. If ransomware, an untrusted application, were able to compromise an endpoint, but it required administrator rights to execute, it would not be able to successfully encrypt files.

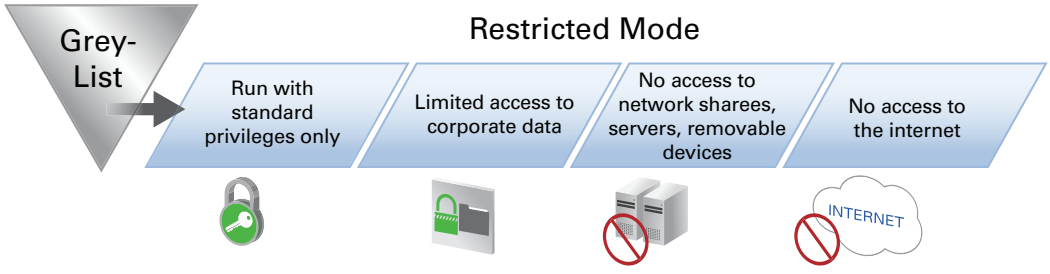
Along with privilege management, organizations should control and monitor applications in order to mitigate the risk of ransomware attacks. CyberArk Viewfinity takes a unique approach to help organizations protect themselves from ransomware. Instead of focusing security on the perimeter and attempting to stop all variants of ransomware and malware from entering the network, the CyberArk solution applies a layer of security on the inside of the network.

With CyberArk Viewfinity, applications fall into one of the following three categories:

Trusted applications	Malicious applications	Unknown applications
Known good applications can be whitelisted to enable them to seamlessly run.	Known malicious applications can be blacklisted to block them from executing.	Unknown applications can be greylisted to enable them to run in Restricted Mode to limit their access.

Greylisting is a key security measure employed to mitigate the impact of ransomware attacks. One reason ransomware is so successful is because attackers are creating new variants every day. These new variants inevitably fall into the "unknown application" bucket. With greylisting, CyberArk Viewfinity can enable these new ransomware variants to execute in Restricted Mode.

Restricted Mode is a customizable feature that enables administrators to limit the access of an unknown application to reduce risk of damage. For example, policies can be created to block applications from reaching the internet and accessing corporate network drives. In addition, policies can be created to restrict access to local drives and specific file types. To protect against ransomware, administrators can block unknown applications from accessing all Microsoft Word documents. A policy such as this would block any unknown application or ransomware from accessing and encrypting all Microsoft Word documents.



The Restricted Mode feature is designed to not only protect endpoints, but also enable end users to be productive. In many cases, unknown applications are not malicious. Enabling end users to swiftly execute unknown applications, even in Restricted Mode, helps keep business productivity high and end users happy.

Summary

Ransomware attacks are unfortunately a growing trend and their rise in popularity isn't slowing down anytime soon. As attackers shift from targeting individuals to targeting organizations, they're generating larger profits from ransomware attacks. Organizations must secure their environments to protect themselves from ransomware attacks. The CyberArk Privileged Account Security Solution offers a unique approach to help organizations mitigate the risk of ransomware attacks by using a combination of privilege management and application control.