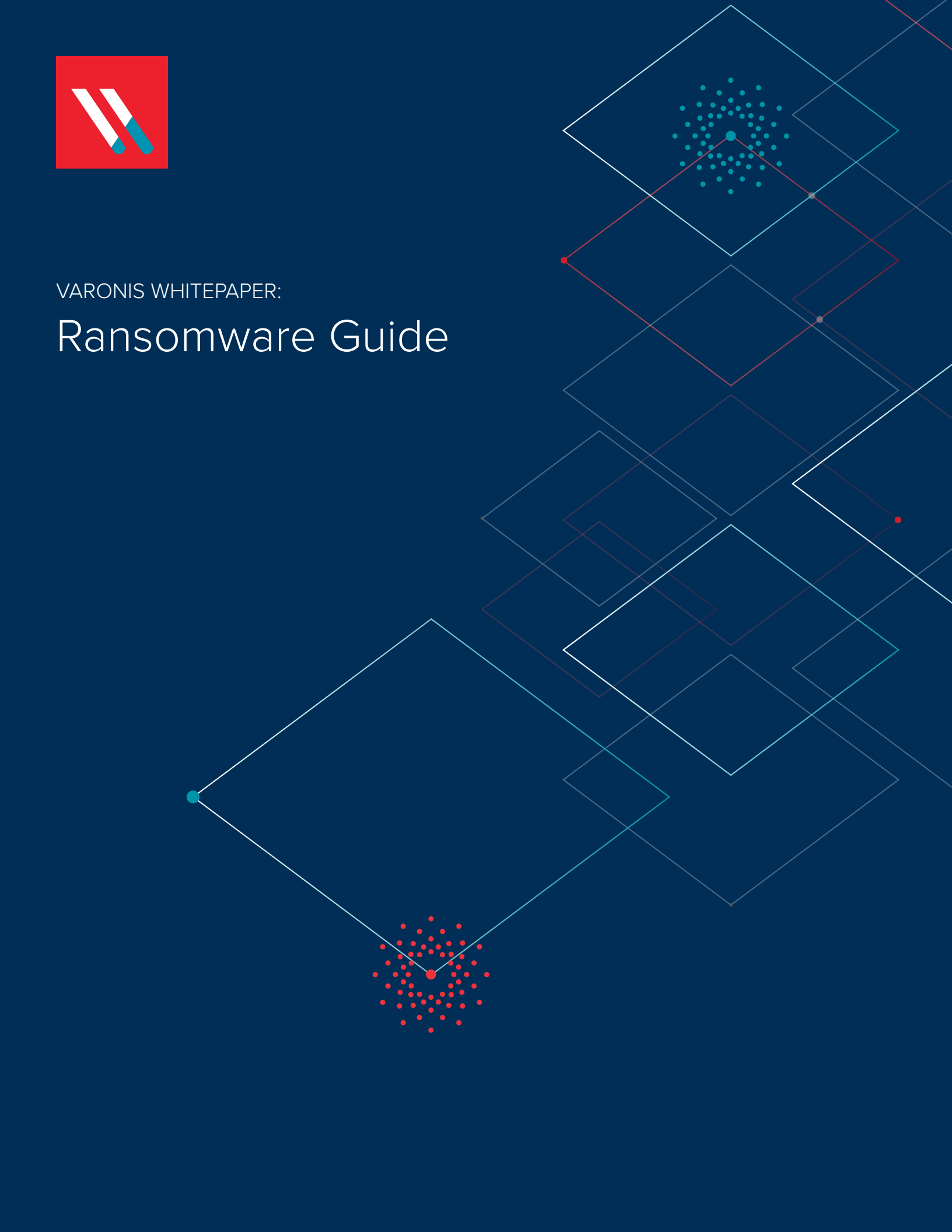


VARONIS WHITEPAPER:

Ransomware Guide

Contents

Ransomware Guide

Overview

Ransomware – malware that encrypts a victim's data, extorting a ransom to be paid within a short time frame or risk losing all his files – has been around for quite some time. In 1989 the first known ransomware, dubbed the AIDS Trojan, infected 20,000 floppy diskettes –remember those? The diskettes supposedly contained AIDS information on the virus, and were handed out during a conference. Upon loading the DOS-based software from the disk, the program counted the number of times the computer was rebooted. Once it reached 90, it would hide the directories, encrypt the names of the files and requested $189.00 to decrypt the files.

Ransomware has since evolved from its early sneaker-net roots, leveraging the Internet and email to spread to different computers. However, it still follows a predictable script, not all that different from the original AIDS Trojan. After entering our networks via a phishing attack, files get encrypted, and the user sees a notification with instructions on how to submit bitcoins in order to decrypt files.

Unfortunately, ransomware attackers have seen how lucrative ransom payments can be. With each attack worth hundreds to thousands of dollars or more, they've become even more ambitious with the amount they're demanding, and how they're demanding it.

How's this for ambition: some attackers, even after you've paid them the ransom, only partially unlock the files in an effort to demand even more from vulnerable businesses. In one case, a hacker even demanded a ransom as high as one million dollars.

They're also pushing the boundaries to see how quickly they're able to extort from unprepared individuals and organizations. Recently, we were introduced to a different attack vector with WannaCry. Instead of a phishing attack, attackers used the NSA's ETERNALBLUE exploit, allowing it to spread peer-to-peer within an organization, impacting vulnerable Windows machines – laptops, desktops, tablets, and servers.

The result? WannaCry was the fastest and largest ransomware attack we've seen so far.

By experimenting with how an attack is released, how much to extort, the intensity and velocity in which they spread harm, hackers advance their knowledge base, changing how they develop new strains as well their attack vector.

However, what hasn't changed is that it is still possible to detect and prevent a zero-day ransomware attack – that's according to a Northeastern University's ransomware research paper. In *Cutting the Gordian Knot: A Look Under the Hood of Ransomware Attacks*, this research team analyzed 1,359 ransomware samples between 2006 and 2014, and found that a *"close examination on the file system activities of multiple ransomware samples suggests that by... protecting Master File Table (MFT) in the NTFS file system, it is possible to detect and prevent a significant number of zero-day ransomware attacks."*[1]

In this guide, we'll help you better understand the role that bitcoin plays in ransomware, various types of ransomware, attack vectors, and cover a few mitigation methods.

What Bitcoin Has to Do with Ransomware

Bitcoin is often associated with ransomware because attackers typically request payments to be submitted in that form of currency. But what exactly is bitcoin?

Bitcoin is digital currency that lets you anonymously buy goods and services. You can send bitcoins digitally using a mobile phone app or computer. It's as easy as swiping a credit card.

Bitcoins are stored in a digital wallet, which resides in the cloud or on a user's computer. It's similar to a bank account, but they're not insured by the FDIC. Also, bitcoins aren't tied to any country, subject to regulation, and there are no credit card fees.

Each bitcoin transaction is on a public log. Names of buyers and sellers are anonymous - only their wallet IDs are revealed. And it allows buyers or sellers do business without easily tracing it back to them. As a result, it's become a popular choice for cybercriminals to choose bitcoin as a form of payment. To evade identification, many bitcoin addresses used by cybercriminals have no more than 6 transactions.[2]

To make a bitcoin payment, victims are often alerted to download anonymous browsers, such as Tor2web or Torproject, in order to visit a URL hosted on anonymous servers. Tor (The Onion Router) makes it difficult to trace the location of the server or the identity of its operators.

Should You Pay?

The short answer is: it depends.

But some say, Yes

At a Cybersecurity Summit, Joseph Bonavolonta, the Assistant Special Agent in charge of the FBI's CYBER and Counterintelligence Program said, *"To be honest, we often advise people just to pay the ransom."*

He explained, *"The success of the ransomware ends up benefitting victims: because so many people pay, the malware authors are less inclined to wring excess profit out of any single victim, keeping ransoms low. And most ransomware scammers are good to their word. You do get your access back."*

If you pay, the FBI stated that most ransomware payments are typically between $200 and $10,000.[3]

But there have been instances where the payment has been much higher. In 2014, the City of Detroit's files were encrypted and the attackers demanded a ransom of 2,000 bitcoins, worth about $800,000.[4] Luckily, the ransom was not paid because the database wasn't used or needed.

There might be times when you're faced with other considerations. The Tennessee Dickson County Sheriff's Office paid $622.00 in bitcoin to hackers who encrypted the department's criminal case files, making them inaccessible to investigators.[5] Detective Jeff McCliss said, *"It really came down to a choice between losing all of that data - and being unable to provide the vital services that that data would've assisted us in providing the community versus spending 600-and-some-odd dollars to retrieve the data."* The department was lucky; it got back access to its files.[6]

Thou Shall Not Pay

Some security experts disagree with Mr. Bonavolonta's remarks and urge you not to pay the ransom because there's no guarantee that even after you pay the ransom, your files will return to its original state. Moreover, paying perpetuates an ongoing problem, making you a target for more malware.

In 2016 it was reported that a Kansas hospital hit with ransomware paid the ransom in hopes of getting back to business as soon as possible, but the payment only *partially* decrypted their files. Instead, the cybercriminals demanded *more* money to decrypt the rest. As a result, the hospital refused to pay a second ransom because it was no longer *"a wise maneuver or strategy."*

Worse, if you get infected with a defective strain such as Power Worm you won't get your files back regardless what you do. Even with the intent of paying the ransom and hopes of recovering your encrypted files, this attack will inevitably destroy the victim's data.

The Department of Homeland Security has also advised victims not to negotiate with hackers. Conflicting advice has prompted a debate about whether the FBI is encouraging behavior that will lead to more hacking.

In a *Wall Street Journal interview*, FBI spokeswoman Kristen Setera declined to say if FBI officials recommend paying a ransom to hackers, as Mr. Bonavolonta stated.[7]

Why you should work with law enforcement

John Carlin, former Assistant Attorney General for the U.S. Department of Justice's National Security Division acknowledged in a recent podcast that there remains confusion at the FBI on whether or not you should pay.

He confirmed that the FBI officially does not encourage paying a ransom. However, similar to a kidnapping case, that doesn't mean that if you go to law enforcement, that they're going to recommend you not to pay.

But one thing is for certain. If you do go to law enforcement, they will be able provide a few insights that you wouldn't otherwise know.

First, law enforcement can provide you with valuable information. Carlin advised *"If it's a group they've been monitoring, they can tell you...whether they've seen that group attack other actors before, and if they have, whether if you pay they're likely to go away or not. Because some groups just take your money and continue."*

Secondly, he also identified a major benefit to working with law enforcement – you'll be hedging against the risk of inadvertently paying off a terrorist when you pay the ransom. He advised, *"You can end up violating certain laws when it comes to the Office of Foreign Assets Control by paying a terrorist or another group that's designated as a bad actor. But more importantly, you do not want to be in a situation where it becomes clear later that you paid off a terrorist."*

But before you pay, find out if there's a decryption tool

Finally, if you are faced with managing a ransomware attack, go online to see if a decryption tool exists. If you're able to find the keys, there's no need to pay. Sometimes, when the police and security experts investigate cybercriminal activity, they can potentially obtain decryption keys from malicious servers and share them online, like for CoinVault, TeslaCrypt, or the popular CryptoLocker.

Keep in mind, whether or not you pay the ransom, the cumulative cost of a ransomware attack is typically greater than the ransom. The cost to the brand, loss of productivity, legal fees, etc all accrue once the attack vector is triggered.

Perhaps another way that might help you decide is to understand the type of ransomware you're dealing with.

Major Ransomware Types

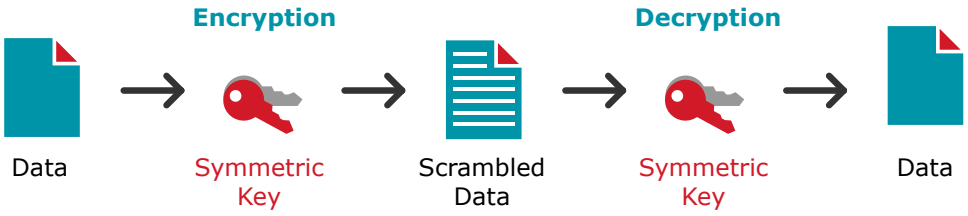
In *Cutting the Gordian Knot: A Look Under the Hood of Ransomware Attacks*, researchers identified three major types: encryption, deletion, and locking.

Encryption

CryptoLocker and CryptoWall have a reputation for being strong encryption ransomware. Encryption is the process of applying an algorithm (also known as ciphers) to data so it is unintelligible to anyone. And to decrypt the data, you'll need keys. There are two types: symmetric and public.

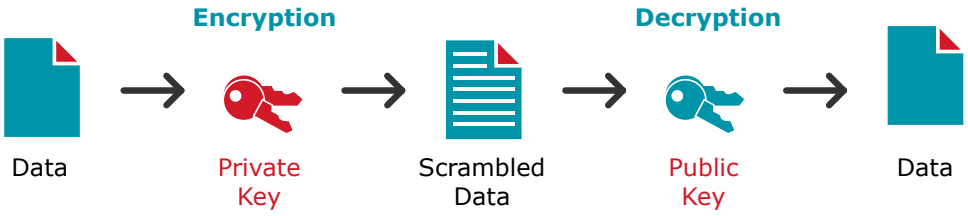
Symmetric Keys

Advanced Encryption Standard (AES), Rivest Cipher 4 (RC4), and Data Standard Encryption Standard (DES) are examples of a symmetric-key algorithm. With symmetric, the same key is used for both encryption and decryption. It's only effective when the symmetric key is kept secret by the two parties involved.



Public Keys (Asymmetrical Key)

Rivest, Shamir, & Aldeman use two different keys in their famous RSA algorithm. A public key that everyone has access to, and a private key that is controlled by the person who you wish to communicate with.



Strength of an Encryption

To understand the strength of the encryption, you have to look at both the type of encryption being used –whether symmetric or public/asymmetric - and the key length.

Two important facts: the longer the key, the stronger the encryption, and key length is measured in bits.

Breaking an Encryption

For a symmetric algorithm, you'll need a couple of hours of computer time for something like a 20-bit key or years for a 128-bit key (2128 = 340282366920938463463374607431 768211456 possible keys of 128-bits)

For a public key algorithm, a key length of 32-bits would only require 232 combinations. Even a 512-bit can be easily broken (within a few months), but 2,048-bit is far harder.

Comparing public and symmetric keys can be confusing. Here's a rough benchmark: a 350-bit RSA key is roughly considered the same strength to 40-bit RC4, and 512-bit AES.

The wonky reasons for these differences in key-breaking speeds has to do with the fact that in RSA, you have to factor a number—don't ask!

Ransomware Encryptions

The first ransomware variants used a symmetric-key algorithm and eventually upgraded to public-keys. Today, more advanced ransomware use a combination of symmetric and public.

Most cybercriminals probably wouldn't use a public key to encrypt large file system because it is much slower than a symmetric key encryption. And taking too long to encrypt files could thwart the ransomware operation before the encryption process is fully completed.

So a better idea is to use symmetric techniques to quickly encode the file data, and asymmetric to encode the key. In CryptoLocker, for example, AES (symmetric) was used for file encryption, and RSA (public) for AES key encryption.

Another blend you might see in the near future is elliptical curve cryptography (ECC) and RSA. ECC is described as the next generation of public key, in which you can create faster, smaller, and more efficient cryptographic keys. Some researchers say that ECC can yield a level of security with a 164-bit key that other systems require a 1,024-bit key to achieve.[8]

Deletion

With deletion, attackers threaten and warn: any of your attempts to decrypt files would only result in an "irrevocable loss of your data."[9] Or if you don't pay, the files get deleted. Popular examples of deletion include Gpcode and FileCoder.

Typically, when we delete something we wipe it off the disk. But in analyzing all the samples, the researchers learned that lots of data remained on disk because attackers were lazy, often choosing the easiest path. However, they're also very clever. The researchers found that while the NTFS Master File Table indicated that files were deleted, the files were actually still on disk, so recovery is potentially possible.

Locking

With locking, attackers create a new login screen or html page that makes it appear as though a law enforcement agency has taken over the computer. They display a warning pertaining to laws such as copyrighted materials or child pornography. Or they might disable other components, typically keyboard shortcuts. Examples include: Winlock and Urausy. It's a nuisance, but the data is usually still there.

Attack Vectors

You can bet that new types of ransomware are constantly being developed, including attack vectors that aren't like the usual garden variety, such as malvertising, ransomworm, and peer-to-peer file transfer programs.

As I was once reminded by a security pro, attacks don't need to be complicated. It can be something as simple as a link in an email or an email attachment and that's what most ransomware strains rely on to get in your network. Therefore curious individuals who can't resist clicking on links or opening attachments would benefit from security awareness training.

Let's not forget the devastating effects of WannaCry, so make sure your software is up-to-date so that your security updates are also up-to-date!

We're also seeing more instances of Ransomware-as-a-Service, where hackers sell their malware to other cybercriminals, increasing the frequency and reach of ransomware. Ransomware authors can enlist anyone to sign up and everyone would earn a percentage of the profits. To combat this problem, organizations might benefit from a few mitigation strategies, which we'll cover later.

What to Do After You've Been Infected

Most people don't realize they've been infected until your screen displays a ransom note, notifying that your files have been encrypted. If you discover that your computer has been infected, shutdown your computer or disconnect from the network.

If you've decided against paying the ransom, scan your computer with an anti-virus or anti-malware program and let it remove everything. You can potentially use PowerShell or other tools to identify encrypted files, but with a new ransomware variant popping up every week, there isn't a one size fits all identification and decryption tool. What most experts recommend is to restore from a backup.

One caveat is that backups aren't 100% fail safe. Some ransomware strains will either encrypt your backups or worse, hide in your backups so that after you restore files they will attack again.

However, if you decide to pay the ransom, you have our sympathy! We empathize and understand what a pain it must have been and hope that once you pay, all your files get decrypted. Don't forget to scan your computer with an anti-virus or anti-malware program and let it remove everything. Also review the mitigation methods below!

Mitigation Methods

Monitor File System Activity

After looking at 1,359 ransomware samples, the Northeastern University researchers learned that it is possible to stop a large number of ransomware attacks, even those using deletion and encryption capabilities.

Significant changes occur in the file system (i.e., large number of deletions in the log) when the system is under attack. By closely monitoring the file system logs and configuring your monitoring solution to trigger an alert when this behavior is observed, you can detect the creation, encryption, or deletion of files.

User Behavior Analytics or Signature-Based?

Some IT pros have turned to endpoint security solutions in the hope that it will detect and stop crypto-malware. However, the industry is catching on to the fact that, as one observer put it, *"signature-based antivirus software that most organizations still rely on to defend them can't cope with modern attacks."*

A recent CIO article described the drawback best:

"... while a signature-based approach reduces the performance hit to the systems on which it runs, it also means somebody has to be the sacrificial sheep. Somebody has to get infected by a piece of malware so that it can be identified, analyzed and other folks protected against it. And in the meantime the malefactors can create new malware that signature-based defenses can't defend against."

Bottom line: endpoint security solutions can't block unknown ransomware variants by, for example, blacklisting connections to a current (but outdated) list of C&C servers. They're also bound to a device/user/process, and so don't provide any anti-heuristics or debugging techniques.

Instead, User Behavior Analytics (UBA) has become an essential go-to ransomware prevention measure. It's also been known to detect zero-day ransomware attacks as well.

Defending the inside from legitimate users is just not part of the equation for perimeter-based security, and hackers are easily able to go around the perimeter and get inside. They entered through legitimate public ports (email, web, login) and then gain access as users.

Once in, cybercriminals have become clever at implementing a ransomware attack that isn't spotted by anti-virus software.

In fact, to an IT admin who is just monitoring their system activity, the attackers appear as just another user.

And that's why you need UBA!

UBA really excels at handling the unknown. In the background, the UBA engine can baseline each user's normal activity, and then spot variances and report in real time – in whatever form they reveal themselves. For instance, an IT admin can configure a rule to, say, spot thousands of *"file modify"* actions in a short time windows.

UBA takes a cross-system approach, too. I.e., it can notice abnormal file behavior combined with weird email actions combined with weird login behavior (from AD). We should mention that: the best UBA benefits from having the most context. Think of UBA as File System Monitoring 2.0 - and keep in mind that the best UBA benefits from having the most context.

Create Honeypots

Cybercriminal may avoid encrypting all files and start by encrypting recently accessed files. Create a decoy by creating fake files and folders and monitor regularly.

This is also a good method for organizations that don't have an automated solution to monitor file access activity. That also means you might be forced to enable file system native auditing. However, it unfortunately taxes your monitored systems. Instead, prioritize sensitive areas and set up a file share honeypot.

A file share honeypot is an accessible file share that contains files that look normal or valuable, but in reality are fake. As no legitimate user activity should be associated with a honeypot file share, any activity observed should be scrutinized carefully. If you're stuck with manual methods, you'll need to enable native auditing to record access activity, and create a script to alert you when events are written to the security event log (e.g. using dumpel.exe).

Least Privilege Model

Another approach is to control access to data and work towards achieving a least privilege model. Your goal is to reduce exposure quickly by removing unnecessary global access groups from access control lists. Groups such as *"Everyone," "Authenticated Users,"* and *"Domain Users"* when used on data containers (like folders and SharePoint sites) can expose entire hierarchies to all users in a company. In addition to being easy targets for theft or misuse, these exposed data sets are very likely to be damaged in a malware attack. On file servers, these folders are known as "open shares"—where both file system and sharing permissions are accessible via a global access group.

Additional Resources

How Varonis solutions can help you prevent ransomware!

Introduction to Ransomware Video Course

3 Ways Varonis Helps You Fight Ransomware

Varonis works across the whole organization. It works with our infrastructure, our Active Directory, it works on all the hardware and software we have. It's allowed us to see what goes on – and see what's out there.

We were able to detect and disable a ransomware infection within 10 minutes of an attack.

- Wade Sendall | Vice President of IT

The Boston Globe

About Varonis

Varonis is a leading provider of software solutions that protect data from insider threats and cyberattacks. Varonis empowers enterprises to stop ransomware in its tracks, discover where sensitive data is overexposed, prioritize vulnerable and stale data, and lock it down without interrupting business. Varonis builds context around the content of data and activity; automates threat detection with predictive threat models built on advanced analytics, user behavior, and machine learning; and monitors critical assets for suspicious activity, including unusual access to sensitive data, abnormal user behavior and file activity to protect against potential exploitation.

All Varonis products are free to try for 30 days.

Our systems engineering team will get you up and running in no time.

Fast and hassle free

Our dedicated engineer will do all the heavy-lifting for you: setup, configuration, and analysis - with concrete steps to improve your data security.

Fix real security issues

We'll help you fix real production security issues and build a risk report based on your data.

Non-intrusive

We won't slow you or your system down. We can monitor millions of events per day without impacting performance.

Live Demo

Set up Varonis in your own environment and see how to stop ransomware and protect your data.

info.varonis.com/demo

Data Risk Assessment

Get your risk profile, discover where you're vulnerable, and fix real security issues.

info.varonis.com/start

Footnotes

[1] http://seclab.ccs.neu.edu/static/publications/dimva2015ransomware.pdf

[2] http://seclab.ccs.neu.edu/static/publications/dimva2015ransomware.pdf

[3] https://www.ic3.gov/media/2015/150623.aspx

[4] http://www.detroitnews.com/story/news/politics/michigan/2014/11/17/north-american-international-cyber-summit/19162001/

[5] http://www.nbcnews.com/nightly-news/security-experts-you-should-never-payransomware-hackers-n299511

[6] http://www.nbcnews.com/nightly-news/security-experts-you-should-never-pay-ransomware-hackers-n299511

[7] https://www.wsj.com/articles/paying-ransoms-to-hackers-stirs-debate-1447106376%0D

[8] http://searchsecurity.techtarget.com/definition/elliptical-curve-cryptography

[9] http://www.anti-spyware-101.com/remove-filecoder-ransomware