©ISTOCKPHOTO.COM/ZAPP2PHOTO

Making sense of the ransomware mess (and planning a sensible path forward)

Nolen Scaife, Patrick Traynor, and Kevin Butler

©ISTOCKPHOTO.COM/LEREMY

It started out as a seemingly isolated event. Reports early during the morning of 12 May 2017 talked about an unknown piece of ransomware attacking systems within the British National Health System (NHS) hospital network. Well over 50,000 NHS systems were infected, forcing affected hospitals to divert patients to other facilities. As hours passed, however, it became clear that this event was not isolated, and systems spanning more than 150 countries quickly succumbed to what would come to be known as WannaCry (which is known by multiple names including WanaCry, WannaCrypt, and WannaCrypt0r, among others.)

Health care was not the only major industry impacted. As the attack continued, WannaCry also disrupted railways (e.g., Deutsche Bahn), the automotive industry (e.g., Renault and Honda), couriers (e.g., FedEx), natural gas providers (e.g., Iberdrola), banks (e.g., BBVA), and virtually every other industry. The WannaCry outbreak took advantage of an exploit stolen from the U.S. National Security Agency, a vulnerability that had an available patch for months prior (and multiple graduate courses in computer science and law could easily be built around this point alone). Major news outlets covered unpatched systems as the leading reason for this outbreak, and while this was a significant cause, the payload could have been any other kind of malware.

The real takeaway from WannaCry is that once the ransomware had reached these systems, it successfully encrypted their data, despite having some of the best-trained security staff and being protected by a wealth of traditional antivirus tools. Moreover, in the months since, we have seen at least two other significant ransomware attacks. How is this possible?

Ransomware is easy to make

The rapid spread of WannaCry stems from its ability to exploit a vulnerability in Microsoft Windows: one that allows unauthenticated remote

Digital Object Identifier 10.1109/MPOT.2017.2737201
Date of publication: 10 November 2017

code execution. Coupled with unpatched systems and Internet-exposed services, the malware simply needs to scan for vulnerable public hosts, exploit the service, and deploy itself. Once installed, WannaCry encrypts the victim's files, attempts to extort a payment for recovery, and finds additional hosts to infect.

As complicated as that may appear, WannaCry is not substantially different from other kinds of ransomware. If you ignore its ability to self-replicate (most ransomware does not do this), WannaCry is your standard, run-of-the-mill ransomware. Ransomware needs to accomplish only three things to convince a victim to pay:

1) read original data
2) encrypt/write encrypted data
3) wipe original data.

Unsuccessfully performing any of these three tasks puts the attack at risk. Without reading the original data, the best the attacker can hope for is to destroy data, leaving little incentive to pay. Likewise, poor implementation of encryption or unsuccessfully wiping all unencrypted copies leaves victims with the opportunity to recover their data without payment. With the advent of easy-to-use cryptographic application programming interfaces (APIs), almost anyone with access to a computer can write ransomware.

This has led to a wide range of qualities of ransomware. In our study, "CryptoLock (and Drop It): Stopping Ransomware Attacks on User Data," which was published at the 2016 IEEE International Conference on Distributed Computing Systems, we found substantial variety in how various samples of ransomware encrypt files. These strategies range from traditional depth-first searches to a variant that encrypts the victim's files in size-ascending order. While all samples we saw attacked common office documents (e.g., pdf, doc, xls), some naively also encrypt program files (e.g., exe, dll), which can cause the victim's system to behave abnormally or even prevent them from paying the ransom.

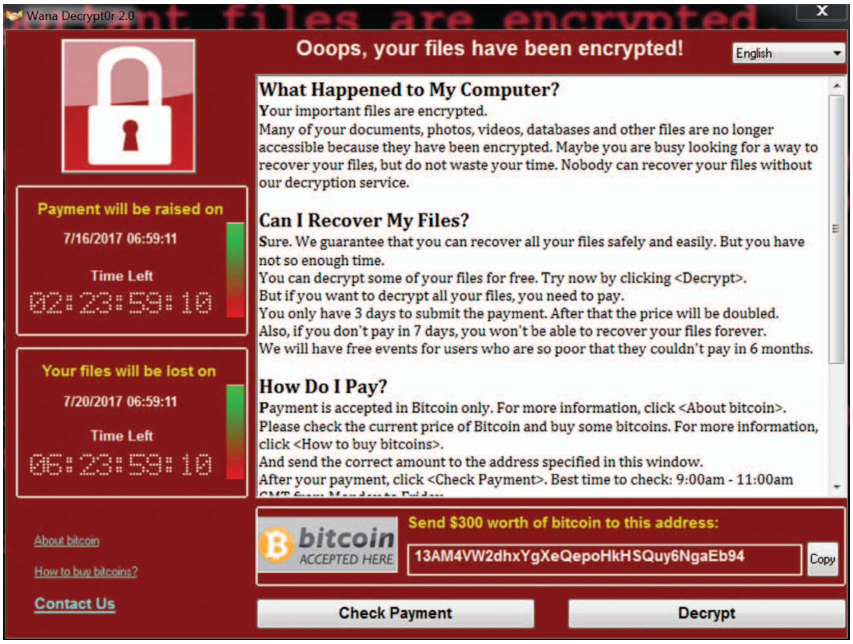
Of course, this is merely one simple behavior of the malware, and ransomware does not need to be perfect to be effective. If it is good enough to convince a victim to pay, the attack is successful. Fortunately, not all ransomware uses cryptography correctly. While we cannot cover every nuance of cryptographic errors and API misuse, in some cases the security community can exploit poorly written ransomware to provide recovery options (called "decryptors") to victims. One can easily see the pervasiveness of "bad" ransomware via the number of decryptors available. These tools require time to build and deploy, and many victims will be unaware of their existence. A far better option would be to stop ransomware before it starts, a task antivirus technology has been trying to solve for years. Why, then, does this problem continue to be pervasive?

Antivirus software is an incomplete solution

To understand why ransomware is so difficult to detect, it is necessary to explore how traditional antivirus detection works. Generally, antivirus products intercept reads and writes to files, scanning the files for known indicators of malware. Signatures range from full file hashes (e.g., SHA-256) to specific patterns and positions of bytes. These signatures are delivered in the form of frequent antivirus updates.

Signatures form the basis for why antivirus software is ineffective at detecting new variants of malware: it simply lacks a signature for the variant. Vendors attempt to compensate for this by creating generic or family signatures that detect more general aspects of the malware, but a malware writer needs only to slightly modify the code to evade detection. When malware goes undetected, a person must analyze the sample, creating a lead time between when a malware sample and when a signature is released. This was an effective model for generic malware for many years, as the shelf life for a given sample might be months or years. This is not the case with ransomware; the malware only needs to execute successfully once to create an opportunity to extort a victim. Removing the malware later will not decrypt the files.

Antivirus technologies are also ineffective against the rise of "fileless malware" that does not exist on the disk. The simplicity of ransomware means that it can be deployed completely in-memory. While this could happen via an exploited program on the system, ransomware can (and has) been implemented in scripting languages. One such family of ransomware, PoshCoder, is written in PowerShell. Though impractical as it may seem, such a script can be



Ooops, your files have been encrypted!

What Happened to My Computer?
Your important files are encrypted.
Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?
Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.
You can decrypt some of your files for free. Try now by clicking <Decrypt>.
But if you want to decrypt all your files, you need to pay.
You only have 3 days to submit the payment. After that the price will be doubled.
Also, if you don't pay in 7 days, you won't be able to recover your files forever.
We will have free events for users who are so poor that they couldn't pay in 6 months.

How Do I Pay?
Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.
Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.
And send the correct amount to the address specified in this window.
After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am

Send $300 worth of bitcoin to this address:
13AM4VW2dhxYgXeQepoHkHSQuy6NgaEb94

A screenshot of the WannaCry ransom demand.

loaded onto a USB keyboard emulator (e.g., a USB rubber ducky) and automatically "typed" quickly into a victim host. Such malware becomes far more difficult to detect since it may exist entirely inside a legitimate program. As a result, even "block-and-ask" strategies may confuse a victim into allowing the ransomware to run.

Even traditional administrative wisdom such as account-based access controls fails to defend against ransomware. Ransomware does not require administrative permissions to encrypt a victim's files; after all, it is accessing the victim's files under the context of the victim. While access controls can prevent collateral damage (e.g., inaccessible network file shares), when a victim opens a maliciously-crafted document, the malware gains access to everything the document reader can access. In most cases, this is everything the user can access.

If signatures are failing to detect ransomware (as they have in the attacks mentioned previously), then what remains is to detect it by its behavior. As we discussed, ransomware needs to read and write the victim's data to encrypt it. The encrypted file looks nothing like the original, but because the ransomware is already running, traditional antivirus software makes no further attempt to stop the attack. Many antivirus products can detect the text files containing the ransom message, but this is a trailing indicator of infection.

Our research has shown that monitoring user data is effective in detecting ransomware, since it must access the data to succeed. Furthermore, the encrypted data look completely dissimilar to the original data. Through fast detection while the victim's data are changing, the ransomware can be stopped and the data recovered. With no further incentive to pay the ransom, the attack fails.

Backups are not a panacea

One seemingly obvious solution is to maintain backups of data. Data backup systems are now decades old and can be relatively inexpensive. Ransomware attacks continue despite the understanding that backups are a major part of a healthy environment. How can this be the case?

While some organizations overlook backups entirely, others treat backups as a "set-and-forget" task—once started, administrators move to other tasks and do not perform maintenance on the process. A key part of the backup process is to continually verify that the backups contain the correct data and restore them correctly. Procedural errors such as leaving the backup online can allow the ransomware to encrypt the backups. If the backup cannot replace the encrypted data, the attackers are successful. Moreover, backups often fail to protect every device with critical information in an organization (e.g., laptops).

Recently, a South Korean web hosting company paid a US$1 million ransom to recover its systems and bring customers' sites back online. Again, although backups may have mitigated the need to pay the ransom, we should also consider the business decision of restoring from backup as opposed to paying the attackers. Restoration can be slow, and due to its fixed-point-in-time nature, may result in data loss. Depending on what was encrypted, this could mean restoring from backup (itself a multiday process), reapplying code patches or database changes, and performing quality assurance checks before bringing a system back online. For applications with complex clustering, this process may be significantly longer. For those with transactional backends (e.g., order fulfillment), restoring from backup might result in the failure of millions of dollars in sales as systems are rolled back hours or days.

Conversely, paying the ransom is no guarantee that the key will be provided or that data recovery might be successful. The Kansas Heart Hospital paid a ransom in 2016, and the attackers immediately demanded a second ransom. Victims of the recent NotPetya "ransomware" campaign later found that the malware simply erased the files but was disguised as ransomware, and no recovery was possible (despite displaying a ransom demand). Despite the risk, the attackers may hold the only mechanism able to quickly restore an entire business to the most recent point in time.

The decision a business must make is more complicated than whether or not to restore from backup. For backups to starve the ransomware economy, they must have a lower cost than attempting to pay the ransom. Today, that cost varies from case to case, so backups are not going to be a panacea for ransomware in the foreseeable future.

Creating a sensible path forward

WannaCry exposed millions of machines to ransomware. However, the most disappointing part of this story has been its continued spread. Despite international news coverage, many administrators who were initially not impacted by this ransomware seemed to have made no significant changes to the security footing of their systems.

In many ways, ransomware is a perfect storm: the rise of pseudo-anonymous cryptocurrency hides the identity of the attackers; privacy-enhancing hidden services resist attempts to find their servers; the accessibility of strong cryptographic APIs allow even rudimentary programmers to create ransomware; the same strong cryptography prevents file recovery; the attack is simple enough that it can be written a seemingly infinite number of ways to bypass antivirus; and the attack targets what users care most about on their computers: their data. The notion of data-centric security is not new. Ransomware highlights the need to place stronger security controls on the data (in conjunction with controls near the data). Operating systems and programs can be reinstalled, but data are irreplaceable.

In both industry and academia, we have long considered the user's data to be merely the output of some program's execution. We have focused on the program, its contents, and its behavior—in effect, what it is and what it does. To protect against the rising threat of ransomware, we need to shift our focus to protecting data and identifying suspicious interactions with it. We believe that there is no reason to focus on the problem of what ransomware is. Any program can be or become ransomware. Systems like CryptoDrop demonstrate how data protection techniques can be implemented to detect and stop ransomware. With a stronger focus on data, we can potentially save individuals and businesses untold amounts of time and money.

Read more about it

- CryptoDrop. (2017). We Stop Ransomware. [Online]. Available: http://www.westopransomware.com
- No More Ransome! (2017). [Online]. Available: https://www.nomoreransom.org/decryption-tools.html
- L. Constantin. (2017). Hard-to-detect fileless attacks target banks, other organizations. [Online]. Available: http://www.computerworld.com/article/3167589/security/hard-to-detect-fileless-attacks-target-banks-other-organizations.html
- S. Morgan. (2015). Cybersecurity alert: Backup your files to thwart a ransomware attack. [Online]. Available: https://www.forbes.com/sites/stevemorgan/2015/11/12/cybersecurity-alert-backup-your-files-to-thwart-a-ransomware-attack-on-your-laptop-and-pc/#524c55d72097
- Catalan Company (2017). South Korean web hosting provider pays $1 million in ransomware demand. [Online]. Available: https://www.bleepingcomputer.com/news/security/south-korean-web-hosting-provider-pays-1-million-in-ransomware-demand/
- M. Smith. (2016). Kansas Heart Hospital hit with ransomware; Attackers demand two ransoms. [Online]. Available: http://www.csoonline.com/article/3073495/security/kansas-heart-hospital-hit-with-ransomware-paid-but-attackers-demanded-2nd-ransom.html
- I. Arghire. (2017). Destructive wiper disguised as ransomware. [Online]. Available: http://www.securityweek.com/notpetya-destructive-wiper-disguised-ransomware

About the authors

Nolen Scaife (scaife@ufl.edu) earned his B.S. degree from the University of Massachusetts Lowell and his M.S. degree from the Georgia Institute of Technology. He is a doctoral researcher at the University of Florida focused on computer security. He is the chief technology officer of CryptoDrop and has over ten years of industry security experience.

Patrick Traynor (traynor@ufl.edu) is an associate professor and John and Mary Lou Dasburg Preeminent Chair in Engineering at the University of Florida, where he codirects the Florida Institute for Cybersecurity Research. He is the chief executive officer of CryptoDrop and a Senior Member of the IEEE.

Kevin Butler (butler@ufl.edu) is an associate professor in the Department of Computer and Information Science and Engineering at the University of Florida. He is the chief operating officer of CryptoDrop. His expertise spans systems and security.