# THE RANSOMWARE THREAT:
## A Guide to Detecting an Attack

## Attacks are Shifting from Individuals to Organisations

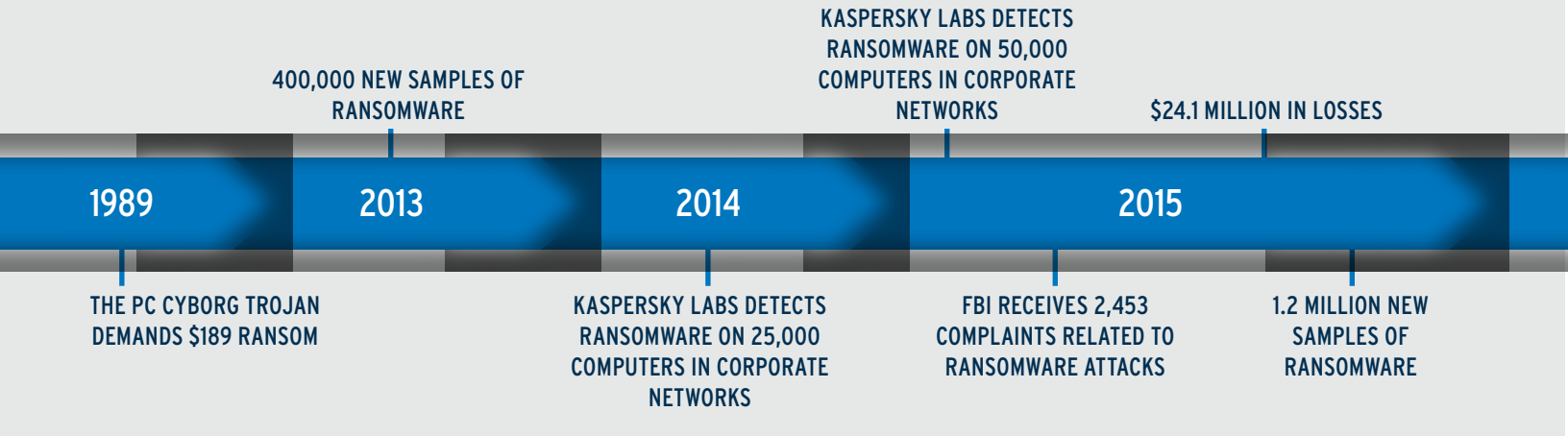
Until recently, most ransomware attacks were simply opportunistic and mostly affected individual users' or small businesses' computers. This has been, and continues to be, a lucrative business for criminals who consider end users to be low-hanging fruit.

But now they have set their sights on larger organisations that have bigger budgets to pay bigger ransom demands. They also have more important files and computer systems that are critical to the organisations' daily operations.

The threat is shifting, according to Ryan Sommers, Manager of Incident Response at LogRhythm. "We are seeing criminals shift their tactics to targeted ransomware attacks. They scope out a specific organization that has deep pockets and is more likely to pay a hefty ransom request in order to minimize the downtime," says Sommers.

Many of the attacks on individuals and small businesses are mass distribution ransomware. The victims are usually targets of opportunity (i.e., these people/businesses were not specifically targeted because of who they were). They most likely acquired the malware through a phishing email, through a drive-by download, or from a compromised website. For example, websites belonging to *The New York Times*, the BBC, AOL and the NFL have all been hijacked by a malicious campaign that attempts to install ransomware on visitors' computers.

On the surface, mass distribution and targeted attacks appear to be similar, but there are underlying technical differences. Mass distribution attacks are typically automated, very fast in their execution — often just 15 minutes from initial infection to a ransom demand being made — and well orchestrated from the attacker's perspective. In contrast, targeted attacks are very similar to an advanced persistent threat (APT); they are usually driven by a person as opposed to an automated system and may take much more time to execute.




[1]Kaspersky Lab, "Kaspersky Security Bulletin 2015"
[2]CNN-Money, http://money.cnn.com/2016/04/15/technology/ransomware-cyber-security/, April 15, 2016
[3]David Common, CBC News, "Ransomware: What You Need to Know," March 11, 2015
[4]Security Magazine, "'Ransomware' Attacks to Grow in 2016," November 23, 2016

## The 5 Phases of a Ransomware Attack

There are distinct phases of a ransomware attack, regardless of whether it's a mass distribution or a targeted attack. "Understanding what happens at each phase, and knowing the indicators of compromise [IOCs] to look for, increases the likelihood of being able to successfully defend against—or at least mitigate the effects of—an attack," says Sommers.

**The phases include:**

1. Exploitation and Infection
2. Delivery and Execution
3. Backup Spoliation
4. File Encryption
5. User Notification and Cleanup

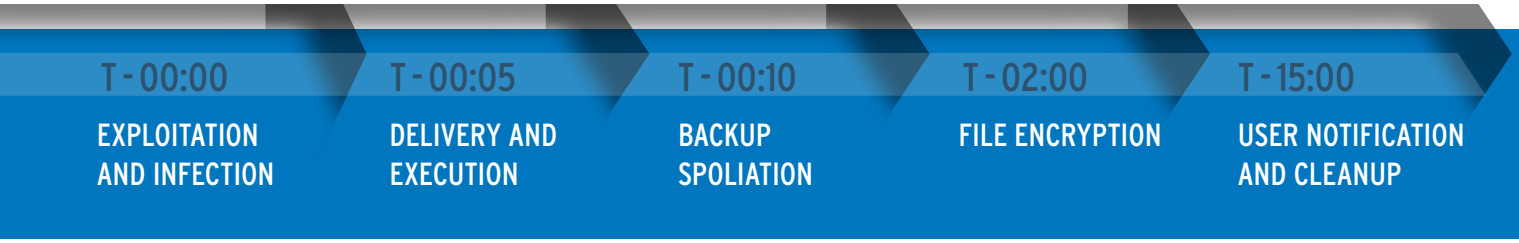



Figure 1: The typical timeline of a mass distribution ransomware attack

We'll make note of where the activity of the phases and the IOCs differ by the type of attack. For instance, one of the distinctions between a mass distribution attack and a targeted attack is how long it takes to fully execute all the steps.

As shown in Figure 1, the timeline of a mass distribution attack is very compressed—often as little as 15 minutes from the exploitation and infection through to the victim receiving the ransom notice. One reason for the shortness of the duration is that the attack is not trying to go beyond the first system it lands on.

In contrast, a targeted attack acts more like an APT; it is looking to inflict as much damage as possible on as wide a footprint as possible. The attackers are trying to affect the entire business rather than an individual user, because they can extort the business and attempt to get a lot more money. Given that targeted attacks are usually operated by a person as opposed to an automated system, the response timeline can be a little less critical than for mass distribution ransomware. Unfortunately this also means the attack can be more difficult to detect.

*Now let's take an in-depth look at the typical phases of an attack.*

## 1 Phase 1: Exploitation and Infection

In order for an attack to be successful, the malicious ransomware file needs to execute on a computer. This is often done through a phishing email or an exploit kit—a type of malicious toolkit used to exploit security holes in software applications for the purpose of spreading malware. These kits target users running insecure or outdated software applications on their computers.

In the case of the CryptoLocker malware, the Angler exploit kit is a preferred method to gain execution. The vulnerabilities favored by the Angler exploit kit are typically found in Adobe Flash and Internet Explorer.

## 2 Phase 2: Delivery and Execution

Following the exploit process, the actual ransomware executable will be delivered to the victim's system. Upon execution, persistence mechanisms will be put in place. Typically, this process takes a few seconds, depending on network latencies.

Unfortunately the executables are most often delivered via an encrypted channel—instead of SSL, a custom encryption layer is added on top of a regular HTTP connection. Because the malware is using a strong encryption, it's difficult to recover the executable from the wire. "Most often, we see the executable files being placed in either the %APPDATA% or %TEMP% folder beneath the user's profile," advises Sommers. "It's good to know this for detection purposes because your organisation can monitor for those events to set up a line of defense."

Most of the Crypto malware will add persistence mechanisms such that if the afflicted machine is rebooted in the middle of the encryption process, the ransomware can pick up where it left off and continue to encrypt the system until it is completed.

## 3 Phase 3: Backup Spoliation

A few seconds after the malware is executed, the ransomware targets the backup files and folders on the system and removes them to prevent restoring from backup. This is unique to ransomware. Other types of crimeware and even APTs don't bother to delete backup files.

Most of the ransomware variants will go out of their way to try and remove any means that the victim has to recover from the attack without paying the ransom. On Windows systems, in both targeted and mass distribution attacks, we often see the vssadmin tool being used to remove the volume shadow copies from the system. For instance, CryptoLocker and Locky will execute a command to delete all of the volume shadow copies from the system. "The good news is that there are event log entries that are created when this happens, so triggerable events can be detected by a SIEM or a host-based product," says Sommers.

Several of the variants, especially in the targeted attacks, will even go so far as to look for folders containing backups and then forcefully remove those files. Even if a program is holding a lock to those files, it will kill the process so it can delete those folders of the backups to make recovery all the more difficult.

## 4 Phase 4: File Encryption

Once the backups are completely removed, the malware will perform a secure key exchange with the command and control (C2) server, establishing those encryption keys that will be used on the local system. Quite often the malware will tag the local system using a unique identifier that will be presented to the user in the instructions at the end. This is also how the C2 server differentiates between the encryption keys used for different victims. Unfortunately most of the variants today use strong encryption such as AES 256, so the victim isn't going to be able to break the encryption on their own.

Not every type of ransomware needs to contact a C2 server to exchange keys. In the case of the SamSam malware, the software application does all encryption locally without reaching out to the internet at all. This is worth noting, because the communication with a C2 server is an IOC that should be monitored, but the absence of this event does not mean that ransomware is not present.

During the file encryption phase, different ransomware variants handle file naming and encryption differently. For instance, CryptoWall version 3 does not encrypt the file name, whereas CryptoWall version 4 randomises the file name and extension. Locky will randomise the file names but add a locky extension to the end. Knowing this, your organisation can sometimes fingerprint the exact ransomware variant based on the file naming convention that it uses.

Depending on network latencies, the amount of documents, and the amount of devices connected, the encryption process can take anywhere from a few minutes to a couple of hours. There have been instances where, on a widely distributed network, the ransomware tries to encrypt files across a wide area network. For a single endpoint device, however, the encryption process is usually done in minutes.

## 5 Phase 5: User Notification and Cleanup

With the backup files removed and the encryption dirty work done, the demand instructions for extortion and payment are presented. Quite often, the victim is given a few days to pay, and after that time the ransom increases.

How the instructions are presented can help you identify which ransomware software has attacked the system. The demand instructions are usually saved onto the hard drive, sometimes in the same folders as the encrypted files. Other times, they are saved to very specific locations on the hard disk. For example, CryptoWall version 3 uses the HELP_DECRYPT file to store the instructions. CryptoWall V4 changed it to HELP-YOUR-FILES. There are a couple different instructions and variations on the theme but you can usually use this guidance to do an internet search and find the exact variant.

Locky takes a different approach in that, not only does it place files on the system, but it also changes the user's wallpaper to contain the instructions for how to decrypt the files. How's that for putting the demand in your face?

Finally, like the Mission Impossible recordings that self destruct, the malware cleans itself off the victimized system so as not to leave behind significant forensic evidence that would help build better defenses against the malware. With the self-removal of the malware code, there should be no lingering malicious files on the systems, and thus no lingering threat, though experts aren't certain of this. "Even though the ransomware removes itself, we recommend you replace rather than simply clean afflicted computers if possible," Sommers advises.

# The 5 Steps of Defense: How to Handle a Ransomware Attack

Now that we understand how ransomware typically works, let's look at what you can do to defend against such an attack. We'll look at the steps in terms of the SANS, NIST and Navy incident handling frameworks; that is, preparation, detection, containment, eradication, and recovery.

1

## Step 1: Preparation

Ransomware attacks are increasing in frequency and seriousness. You need to prepare your organisation for the very real possibility of an attack.

### Patch Aggressively

Because malware often enters systems through known vulnerabilities, the best step you can take to bolster defences is to aggressively patch your systems. This is, of course, one of SANS Institute's Top 20 Critical Security Controls for Effective Cyber Defence: continuous vulnerability assessment and remediation. By eliminating vulnerabilities, the malware may not have a way to get on any of your computers in the first place.

### Create and Protect Your Backups

Ransomware destroys backup files and encrypts regular files, and this puts your organisation in a world of hurt. Therefore, it's imperative to frequently back up all documents to a location that can't be affected by the ransomware (e.g., to offline storage) and then verify that these files can be restored easily if needed. Even network shares or cloud storage may not be entirely safe, as files that have already been encrypted or corrupted by the ransomware could be automatically backed up to the network or the cloud, also corrupting the files in those storage locations.

### Prepare a Response Plan

Your organisation should develop an incident response (IR) plan that is explicitly for a ransomware attack. This step is particularly important to prepare for targeted attacks that can affect broad swaths of your organisation. The IR plan should detail the specific actions people should take as soon as it becomes apparent that an attack is underway. This will help to ensure a prompt response in a situation where time is of the essence to stop or contain a serious situation. Likewise, you should develop a disaster recovery plan specific to this type of attack. "With good planning and a definitive course of action, an attack can have a minimal impact to your organisation," according to Sommers.

### Assign Least Privileges

One critical aspect to defending against ransomware is that of least privilege when it comes to file shares in particular. Many organisations will have one file share accessible to everyone within the company. Certain locations may be read-only or may be inaccessible to certain users, but many organisations operate under a monolithic file share structure. Changing into a least privilege and as-needed basis can limit the damage caused by ransomware infection substantially.

### Connect with Intelligence Sources

Another big step during the preparation phase is to connect with industry intelligence and threat intelligence sources or industry lists specific to crimeware or ransomware and regularly feed those indicators back into detection mechanisms such as intrusion detection systems (IDS).

### Protect Your Endpoints

Your organisation can deploy endpoint protection tools that have the ability to detect and automatically respond to infections in the early stages. Tools such as LogRhythm System Monitor, among others, can be used to detect these infections early and respond to them automatically and quickly so that they don't become big incidents.

### Educate Users

User awareness training is an effective means to teach people to avoid falling victim to phishing email messages that plant malware in the first place. Many attackers rely on social engineering tactics that are growing more and more sophisticated. End users need to know what to expect and what to look for in their messages to avoid infection.

### Buy Insurance

The cost of a ransomware attack can be quite high—not just the cost of the ransom itself, but also the loss of business during the time that files and documents are unavailable. For example, when Hollywood Presbyterian Medical Center experienced its ransomware attack in February 2016, the hospital was crippled. The Radiation Oncology department was shut down, and CT scans and lab work were unavailable. Impacted patients were transferred to other facilities or simply turned away.[8] The inability of the hospital to provide its normal business services for more than a week was financially devastating.

James Carder, LogRhythm CISO and Vice President of LogRhythm Labs, advises organizations to prepare by getting a good cyber insurance policy that explicitly covers losses due to ransomware. "If you have a loss of revenue due to a ransomware infection, you may be able to use your cyber insurance to make a claim to recover that revenue," says Carder "From a pure risk management perspective, getting a really good cyber insurance policy is probably worth its weight in gold in situations like this."

## 2 Step 2: Detection

In the event that your enterprise gets hit with an attack, you can minimize the damage if you can detect the malware early.

### Prime Your Defense Devices

For initial exploitation and infection, a good defense is to get signatures and IOCs into your IDS or other network devices. Use your threat intelligence sources to block or at least alert on the presence of anomalies associated with ransomware in your network traffic. There are numerous signatures for most of the major IDS vendors out there for CryptoWall and Locky traffic. These are usually malware version dependent, and they can change. Therefore, you want to have more defense than just the detection. However, these signatures can be a good source for the most widely distributed tools that enterprises tend to use.

### Screen Email for Malicious Links and Payloads

For the phishing emails that contain or lead users to the ransomware malware, any of your tools that detect malicious attachments or perform attachment scanning to look for executable attachments are your best automated defense against ransomware emails.

### Use Rule Blocks for Executables

Two common areas where the ransomware typically executes from are the %APPDATA% folder and the %TEMP% folder on your system. Looking for any file executing from these locations is a good way to spot ransomware before it has actually had a chance to encrypt files. LogRhythm has developed rules for our tools to monitor for file executions from these folders, as well as to look for file executions from the location and the creation of the instructions.

Similar to the exploitation phase, network rules can also be used to detect the executable delivery and execution, especially for cases like CryptoLocker where there is a very predictable sequence of events to set up the Diffie-Hellman key exchange. You can trigger on those in your IDS to block them. For instance, with CryptoLocker, if you're able to block the key exchange, you could actually avoid having files encrypted because the malware won't progress beyond trying to set up that key.

Backup spoliation is another key area where CryptoLocker can be detected before it has actually had a chance to execute. Specifically, look for that vssadmin command execution. It's very common for this approach to be used, and if you have the tools or the logging in place to highlight when the admin tool is executed, you can take action and perhaps avoid either the laptop or the network shares being encrypted.

[8]Venturebeat, "Next wave of ransomware could demand $millions," March 26, 2016

### Look for Signs of Encryption and Notification

The file encryption phase usually begins with a key exchange that can be detected via network signatures, file naming and registry modifications on the local system. Looking for files with a .locky extension is a good method to try and detect Locky being encrypted on a system. Similarly with CryptoWall, looking for the random filename patterns is another way to detect the ransomware as it is actually running.

Unfortunately it is a little late in the progression of the malware, but if you can detect the user notification files being placed on the system, you can usually at least be alerted to the presence of the encryption even if you weren't able to block it. Quick detection at this stage may help you contain the situation.

## 3 Step 3: Containment

Once the ransomware has already done its dirty work on one device, there are steps you can take to contain it locally so that network files aren't affected.

### Kill the Running Processes and Isolate the Afflicted Endpoint

Having an endpoint protection system that is able to look for the execution and kill the process is usually the best means of containment. However, many enterprises don't have such a solution. For that reason, LogRhythm has developed technologies that block and isolate the local host from the network should we detect, say, a CryptoWall infection. "If LogRhythm detects the ransomware, we can then disable that network connectivity so that if CryptoWall is able to get to the endpoint, it's not able to actually encrypt files on the network," according to Sommers. "At the most, you would just be worried about files on the local system, but you can try to get that system shutdown as quickly as possible so that the least amount of files are encrypted."

In the case of a targeted attack, make sure you have fully scoped the incident, then quickly develop a containment plan. Unlike mass distribution where you are usually dealing with one, two, or maybe a few hosts that are infected, a targeted attack is usually going to affect more systems. Therefore, you must scope the extent of the full attack. You need to kick the attacker off the entire system rather than just playing a game of whack-a-mole and picking them off one system at a time. This is a case where we strongly recommend a system rebuild rather than a cleanup. There can be latent tools the attackers have put in place that you may not catch if you try to clean the system, but if you rebuild, you have a much better chance of starting fresh and completely remediating the attack.

*If LogRhythm detects the ransomware, we can then disable that network connectivity so that if CryptoWall is able to get to the endpoint, it's not able to actually encrypt files on the network," according to Sommers.*

*"At the most, you would just be worried about files on the local system, but you can try to get that system shutdown as quickly as possible so that the least amount of files are encrypted.*

4

## Step 4: Eradication

Once you know you have had a ransomware incident, and it has been contained, you now need to eradicate it from your network.

### Replace, Rebuild or Clean Machines

We usually recommend that machines be replaced rather than cleaned. As with any type of malware, it's difficult to know if residual files are hidden on the system and able to re-infect devices. However, for network locations such as mailboxes or file shares, sometimes it is more relevant to clean those locations, remove the malicious email message from the mailbox, or remove the ransomware instructions from the file share. If you choose to clean rather than replace, continue to monitor for signatures and other IOCs to prevent the attack from re-emerging.

5

## Step 5: Recovery

Follow your disaster recovery plan to get all affected systems up and running again and get back to business as usual.

### Restore from a Clean Backup

For recovery, the number one task is going to be restoring from backup. If you have those good verified backups, any ransomware event can really be made into a non-issue by simply replacing or cleaning your systems and recovering from backups. You may be down for a couple of hours because of the time required to restore from backup, but it shouldn't be a big multi-day issue that you have to deal with.

### Look for the Infection Vector

In most ransomware investigations, you usually want to complete your recovery phase by doing a full investigation into what specific infection vector was used against the system. Was it a phishing email, or was it a web-based attack kit? If it was a web-based attack kit, how did that user get to that webpage?

LogRhythm analysts have seen a number of victims where they were doing nothing more than using Google to search for self-help IT questions. "When the people went to a seemingly harmless response page, they were redirected to strategically compromised websites that then infected them via the Angler exploit kit. Knowing how the ransomware came onto your system can help you better prime your defense systems and direct your detection mechanisms in the future," says Sommers.

*Knowing how the ransomware came onto your system can help you better prime your defence systems and direct your detection mechanisms in the future," says Sommers.*

comtact

PERFORMANCE THROUGH TECHNOLOGY

**Securing the UK's leading organisations 24x7x365 from our UK NOC & SOC**


**Comtact Ltd.** (Head Office)
Clive House
12 - 18 Queen's Road
Weybridge, Surrey KT13 9XB

Tel: 08452 75 75 75
Email: enquiries@comtact.co.uk


**FOLLOW US**

Comtact-Ltd

@comtact_ltd

www.comtact.co.uk