THE RANSOMWARE SURVIVAL HANDBOOK

An IT Manager's Guide to Prevention, Response, and Recovery

Barkly

WHO ARE WE?

Barkly makes more than awesome content. We make endpoint protection software that prevents damage when users click on bad stuff. Our protection works by monitoring system activity and blocking malicious processes from executing. It stops ransomware, zero-day attacks, and other malware that get past antivirus.

LEARN HOW BARKLY WORKS

When they're not building software, our team of malware researchers and security experts like to share their wisdom by writing content.

We hope you find it useful.

Barkly™

HOW RANSOMWARE WORKS

According to a June 2016 survey by Osterman Research, nearly 50 percent of organizations have been hit with ransomware. As infection rates continue to rise, more and more attention and budget is being directed toward finding ways of keeping machines clean and data safe.

To do that, organizations need to understand how ransomware works and what needs to happen in order for an infection to be successful. Let's break down what the infection process looks like, starting with the most common ways ransomware gets delivered and the steps you can take to reduce your risk.

RANSOMWARE DELIVERED VIA EMAIL

Why email?

For cyber criminals, email serves as a direct line straight to the soft, chewy, vulnerable center of your network — your users. By sending emails disguised as legitimate messages the hope for ransomware authors is they can trick users into either opening an infected attachment or clicking a link that takes the user to an infected website.

It's a tactic referred to as phishing (attackers try to catch users by luring them into taking the bait). Unfortunately, it can be highly effective – according to the Verizon 2016 Data Breach Investigation Report, phishing emails have an average open rate of 30% – and research shows ransomware is now the #1 type of malware that phishing delivers[1] (by far).

So we're talking spam emails?

Not exactly. You may still get an obvious mass spam email from a "Nigerian prince" from time to time, but the truth is many of today's phishing emails are surprisingly sophisticated.

[1] http://phishme.com/phishing-ransomware-threats-soared-q1-2016/

For starters, they're more likely to be targeted, with attackers actually taking the time to do a bit of research and craft emails that are personally relevant to their victims. Just a few minutes on LinkedIn can supply an attacker with a name of a business connection or colleague they can reference to make their email much more convincing.

This type of targeted phishing attack is referred to as spear phishing (because the attacker is singling out and going after a specific person or group).

How do phishing emails deliver ransomware?

Two primary ways:

1. Malicious attachments
2. Links to malicious or compromised websites

As of now, simply opening a phishing email isn't enough to get a user infected with ransomware. Attackers still need users to take one additional step in order to get the malicious ransomware code onto their machine – either opening an infectious email attachment or clicking on a link that takes them to an infectious website.

We'll get into how the second option works when we talk about exploit kits. First, let's explore how attackers hide ransomware in attachments.

What types of attachments does ransomware hide in?

The success of ransomware phishing attacks hinges on convincing the victim every aspect of the email is legitimate. An attacker can go to great lengths crafting a customized, relevant message and making it look like it's coming from a sender the victim knows and trusts, but if the attachment looks suspicious that can ruin the chance of the user taking the bait.

To avoid raising suspicion, attackers often hide ransomware in the types of attachments we expect to receive – some of the most common include MS Office docs (Word, Excel, and PowerPoint) and PDFs.

These documents can be disguised as anything from invoices, contracts, regulatory forms, and more.

MS Office docs are a popular choice among ransomware authors because they allow them to leverage macros (bits of code that allow additional functionality) to execute the ransomware without the user's knowledge. The Locky ransomware family originally gained traction and notoriety in early 2016 with its use of malcious macros in Word documents.[2]

If macros aren't enabled, the user won't be able to properly read the document, and they will be asked to enable them. Once macros are enabled that allows code in the document to download and execute the actual ransomware payload.

[2] http://arstechnica.com/security/2016/02/locky-crypto-ransomware-rides in-on-malicious-word-document-macro/

+ SAFETY TIP

If possible, it's a good idea to adjust your users' Microsoft Office default settings to disable macros. That way you can prevent ransomware from exploiting them. Microsoft has a support document that walks you through that process.[3]

More recently, attackers have begun using JavaScript file attachments to deliver ransomware (it's now even more popular than using Word docs[4]). What makes that especially concerning is JavaScript can do anything a regular application can do, without attracting the scrutiny of a .EXE. It's also easy for ransomware authors to disguise JavaScript file extensions so they look like .TXT files or something else innocuous.

How can I prevent ransomware from being delivered via email?

You can't prevent attackers from sending ransomware phishing emails, but you can put security controls in place that a) reduce the risk of users taking the bait, or b) prevent ransomware from successfully executing even if they do.

Email filtering

Actively filtering email attachment types that are potentially dangerous and aren't commonly used or necessary to day-to-day work is certainly a low-effort way for you to lower your risk, but as the example of Locky demonstrates, criminals are becoming increasingly good at sneaking malicious code into file types that will get past most email filtering. For that reason, email filtering is far from a comprehensive solution.

User education

Teaching users how to spot and react to suspicious emails can help transform them from a major liability to a formidable first line of defense. To help, we've put together a **Phishing Field Guide** complete with example phishing emails you can share with users to show them exactly what to watch out for.

User awareness training is a great long-term investment, but it's also an ongoing commitment, and there's no guarantee users are going to be 100% mistake-free 100% of the time. That means you need to have back-up safety nets in place so you're ready for the inevitable when new or even trained users click on something they shouldn't have.

More on what those are in the ***How to stop a ransomware infection*** section.

% QUICK STAT

In a recent survey, 74% of ransomware victims reported they were running email/ content filtering at the time of infection. 100% were running antivirus.

[3] https://support.office.com/en-us/article/Enable-or-disable-macros-in-Office-documents-7b4fdd2e-174f-47e2-9611-9efe4f860b12

[4] https://www.proofpoint.com/sites/default/files/quarterly_threat_summary_apr-jun_2016.pdf

RANSOMWARE DELIVERED VIA EXPLOIT KIT

What's different from ransomware delivery via email?

The biggest difference is, with email, the burden is on the attacker to trick a user into actively downloading and opening a file. By using tools called exploit kits, however, criminals can infect victims who visit a compromised website automatically, without any clicking required.

How do exploit kits work?

Exploit kits allow criminals to upload malicious code to any web page they have access to. That code is designed to exploit specific vulnerabilities in browsers or other software the visitor may be running (ex: an outdated version of Adobe Flash Player). If the vulnerability is present, the exploit kit can leverage it to download ransomware. For a deeper dive, see our blog post Understanding Exploit Kits: How They Work and How to Stop Them.

So avoid sketchy websites and we're good to go?

Sorry, not really. Another way for criminals to boost their infection rates is to compromise ad networks, so even visits to legitimate, mainstream websites can result in a ransomware attack.

That's precisely what happened in March 2016, when malicious ads (malvertising) containing the Angler exploit kit appeared on The New York Times, the BBC, AOL, and the MSN homepage, exposing tens of thousands of visitors.

How can I prevent ransomware from being delivered via compromised websites?

Again, it's all about focusing on the things you can control. You can't stop attackers from creating and using exploit kits, but since they rely on taking advantage of software vulnerabilities, one thing you can do is take precautions to make sure your software is patched and up-to-date.

Patch management

Depending on the size and complexity of your organization, staying on top of, evaluating, and rolling out the latest patches can be a full-time job in and of itself. The good news is, when it comes to successful exploits, the vast majority take advantage of just 10 incredibly popular vulnerabilities.

The following 10 vulnerabilities account for 85% of successful exploits[5] (Verizon 2016 DBIR): CVE-2001-0876, CVE-2011-0877, CVE-2002-0953, CVE-2001-0680, CVE-2012-1054, CVE-2015-0204, CVE-2015-1637, CVE-2003-0818, CVE-2002-0126, CVE-1999-1058

Start out by patching those and you can drastically reduce your risk. From there, you'll want to implement a patch management strategy that ideally involves automation.

Install an ad blocker

Ad blockers can help protect your users from malicious ads (malvertising) that can infect even mainstream, legitimate websites.

HOW RANSOMWARE ENCRYPTS FILES AND SPREADS

Once a ransomware payload is delivered, what happens next?

The precise next steps can vary from ransomware variant to variant, but in general, once ransomware is executed it wastes very little time scanning local and connected drives for files to encrypt. Some variants (such as Locky and DMA Locker) even encrypt unmapped network shares, extending the reach of the infection and making potential damage even more widespread.

Different ransomware variants can also scan for different file types, though many cast their nets wide and can encrypt anything from Office files to multimedia files. It's important to note some ransomware variants like Locky also delete shadow volume copies – live backup snapshots Windows users could otherwise use to restore their files.

? DID YOU KNOW

Ransomware typically only takes a matter of minutes or even seconds to finish encrypting files.

Once the encryption process is complete and the files are rendered inaccessible, the ransomware then creates a ransom note that notifies the user what just happened. Ransom notes are typically .TXT files, but depending on the ransomware, they may also appear on a web page and/or replace the Windows wallpaper, too. The point of the notes is to establish the ransom demand amount, walk the user through how to pay it (typically with Bitcoin), or simply direct them to a web page for further instructions.

Note: Details included in the ransom notices, specifically any URLs that are included, can sometimes provide clues as to the specific type of ransomware you're dealing with (as can any changes the ransomware has made to encrypted file extensions — more on that later).

[5] http://www.verizonenterprise.com/verizon-insights-lab/dbir/2016/

HOW TO STOP A RANSOMWARE INFECTION

In addition to taking precautionary measures to prevent ransomware delivery in the first place, there are several things you can do to render ransomware ineffective even if it does land on a machine. The key is to identify the actions ransomware needs to accomplish in order to successfully complete the infection process — and then stop those actions short.

Do it yourself with policy restrictions

A simple example is disabling MS Office macros to render ransomware that relies on them ineffective.

Another (slightly more complicated) example is using Software Restriction Policies to block executables from running when they're located in specific file locations (ex: the %AppData% and %LocalAppData% folders).

To learn more, visit:
bleepingcomputer.com/virus-removal/locky-ransomware-information-help#prevent

Use Barkly™ to automatically block ransomware attempts for you

The most comprehensive (and also hands-off) approach, however, is to install a solution that actively blocks ransomware behavior and does all the work for you. At the risk of being self-promotional, that's exactly what we've built Barkly to do.

While other solutions and workarounds may be able to help you detect particular strains of ransomware after they've already encrypted a certain number of files, Barkly stops even new, never-seen-before ransomware automatically without a single file being encrypted.

Example of what a ransomware attack looks like with Barkly installed:

Delivery: A user inadvertently triggers the attack by downloading what appears to be a legitimate Firefox update.

Attempted execution: Because the malware hidden in the download was "fileless" the user's antivirus doesn't flag it. Barkly spots a malicious form of process injection being attempted and stops it immediately, so the attack is over before it can even start.

Notification: You get an instant email notification letting you know what happened and which user triggered the attempted attack. The user also gets an immediate pop-up message letting them know a crisis was averted, too. It's a friendly (and effective) way of reminding them to be more careful where they click.

To learn more and see Barkly in action, visit:
barkly.com/how-barklys-endpoint-protection-works

WHAT TO DO IF YOU'VE BEEN INFECTED

In this section, we'll walk you through the steps you should take immediately should you or any of your users become the unfortunate victims of a ransomware attack.

As with any security incident, the important thing is to keep your cool and approach things systematically. That's easier said than done, of course, but having a basic framework for a response plan and practicing it ahead of time can help. Let's walk through what that looks like.

STEP 1: ISOLATE

Disconnect infected machines from the network and lock down shared network drives.

With ransomware, the primary thing you're up against is its speed. Unlike other cyber attacks that prioritize stealth in order to maintain system access and control for long periods of time, ransomware simply prioritizes encrypting as much as possible as fast as it can.

For that reason, depending on how you discovered or were notified of the infection, you may find yourself dealing with just one infected device (consider yourself lucky) or multiple users and machines. Your first step should be isolating any infected machines you're immediately aware of by disconnecting them from the network as well as wifi. Keep in mind, many ransomware variants are able to spread through shared network drives, so you may need to temporarily lock those down and check your file servers, too.

Unfortunately, since ransomware encrypts files so quickly, in many cases the damage on infected devices will already be done. Hope isn't necessarily lost, but don't shift your focus to recovery quite yet.

Determine the full extent of the infection

The majority of ransomware variants make changes to encrypted filenames, often changing all the extensions to something that corresponds with the ransomware name (ex: .zepto or .locky). They also often create README.txt and README.html files with ransom instructions. Looking for these markers can give you an idea as to the extent of the infection and how far it's spread.

It's important to track down any devices with these signs of infection and take them all offline. Missing any single infected device increases the risk of the infection spreading all over again.

STEP 2: INVESTIGATE

Determine what type of ransomware you've been infected with

The reason this is helpful to know is some ransomware variants have been identified as being "fake" – meaning they don't actually encrypt your data effectively. Other variants have been cracked and decryption tools have been made available. Still other variants may not have a good track record of actually delivering a working decryption key even if you decide to try paying the ransom.

New or modified file extensions appended to encrypted files are often one clue as to the particular type of ransomware you're dealing with. Likewise, information included in the ransom screen – specifically, any URLs it points you to for more info or payment steps – can also serve as identifying markers. Researcher Michael Gillespie's website allows you to upload a ransom note and/or a sample encrypted file to learn what type it is.

Lastly, you can try some good old-fashioned googling. Search for the ransom screen messaging, for the extension that has been applied to your locked files, or for some of the symptoms you're experiencing such as encrypted unmapped network shares or encrypted shadow copies. Another great resource to check out for more info on specific ransomware variants is BleepingComputer.com.

+ SAFETY TIP

For a list of possible ransomware types you've been infected with, and to find out whether a decryption tool is available, use our **Ransomware Decryption Tool Finder**

Determine the source and cause of the infection

To understand how the attack started you'll also want to identify "patient zero" – the first person in your organization who got infected. Keep in mind this may not always be the user who reported the incident. In some cases, you may be able to determine patient zero by looking at the properties of one of the infected files and seeing who the owner is listed as. For more on how to identify patient zero, see this thread in Spiceworks.

Again, since most ransomware doesn't wait long to get going once it's on a machine, in many cases you should be able to find out what triggered the attack by finding out what the user was doing shortly before the ransom screen popped up.

Ask users to retrace their steps:

Did they open any new documents?
Click on any attachments or links in an email?
Did they visit any websites they don't normally visit?

Once you determine the cause of the infection it may also be a good idea to share an alert with other users letting them know what to be on the lookout for (ex: phishing emails with fake invoices, etc.).

In the meantime, is there anyone else who needs to know about the ransomware attack right away? If so, now's the time to tell them.

STEP 3: RECOVER

Try to restore your encrypted data

Unfortunately, in most cases, once files are encrypted there's no way of unlocking them without the decryption key. That said, malware researchers are sometimes able to exploit flaws in ransomware encryption methods and develop decryption tools. As mentioned, our **Ransomware Decryption Tool Finder** is an easy way to find out whether a decryption tool is available for the strain of ransomware you've been infected with.

If no decryption tool is available then your only other option is to restore your files from backup. Of course, the only way you can do that is if a viable backup is available. A recent poll of IT pros found that only 42% were able to fully recover their data, even with backups in place.[6]

The top reasons for failed or incomplete backup recoveries were:

1. Backups that weren't regularly monitored or tested didn't work.
2. Local backups or backups connected to a shared drive were also encrypted.
3. There was a loss of data since the last incremental snapshot.

For more tips on how to make your backup strategy ransomware-ready, see our blog post: 3 Better Ways to Use Backup to Recover from Ransomware

Even if you aren't using a dedicated backup provider, you may still be able to recover your data if Microsoft's free volume shadow copy service (VSS) is enabled[7]. Just keep in mind VSS has its limitations, and some ransomware variants are able to encrypt shadow copies, as well.

[6] https://blog.barkly.com/ransomware-prevention-tips-to-avoid-paying-ransom
[7] https://msdn.microsoft.com/en-us/library/windows/desktop/aa384649(v=vs.85).aspx

Decide whether or not you need to pay the ransom

If you can't decrypt or recover your files from backup, you're left with a difficult decision to make. While most authorities don't recommend paying the ransom (and stats indicate very few organizations actually do[8]), ultimately, your decision will have to be based on your situation, not other people's.

Things may come down to how integral access to the encrypted information is to your business. It's a good idea to think about how valuable your data is – are you dealing with law case files, patient health records, customer sales orders, etc. – and make decisions on how you would handle various encryption scenarios ahead of time. That way, you're not forced to make an uninformed decision in the heat of the moment.

Keep in mind, however, once attackers have identified your organization as a successful target the odds of you experiencing repeat attacks are high.

Wipe infected machines to avoid re-infection

The safest way is to nuke the computer and bring it back to factory settings. Then restore from backup.

If you don't have backup you can use, the situation becomes trickier. There are some things you can try in order to salvage some of the files, such as malware-removal tools (Microsoft offers a free one), but you do run the risk of a malicious file getting missed and the infection starting back up all over again.

STEP 4: REINFORCE

Conduct a post-attack retrospective

With the attack contained and any recoverable data restored, business may thankfully be getting back to normal. Now that the immediate crisis is over, however, it's important to take the opportunity to do a full assessment of what happened, how you responded, and any surprises or gaps that were exposed along the way.

Starting with how the ransomware was successfully delivered in the first place, go back and retrace the trajectory of the attack. Try to identify any vulnerabilities that were exploited along the way and specific controls you can put in place to either eliminate or mitigate them.

[8] https://blog.barkly.com/ransomware-prevention-tips-to-avoid-paying-ransom

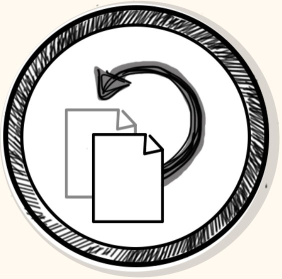
Let's say the attack was launched with a phishing email. What vulnerabilities and gaps in your security allowed the ransomware to be successfully delivered?

For starters, the user who received the email was fooled. Can you invest in awareness training to help users make better educated decisions? Better yet, are there things you can do so damaging user mistakes are harder to make? Can you disable macros in Microsoft Office docs so ransomware authors can't exploit their functionality, for example?

It's also clear if you were running email filtering and antivirus they were both either bypassed or ineffective. Are there adjustments you can make to strengthen them? Are there additional layers of endpoint security you can add that work differently and stop specific types of attacks they don't?

How far did the infection spread? Are there adjustments you can make to user access privileges to limit what infected accounts can reach?

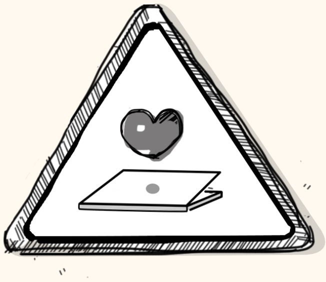
Were you able to wipe machines and adequately recover from backup? Are there any changes to your backup strategy you need to make?



GOOD BACKUP

? DID YOU KNOW

50 percent of ransomware victims experience repeat attacks.



USER TOLERANCE

Unfortunately, suffering one ransomware attack puts you at greater risk for suffering another one. Asking these types of questions will help you probe where your weaknesses are and determine what needs to change to avoid a repeat incident.

In addition, here is a checklist you can use to better prepare for ransomware infections and raise your odds of successfully preventing them in the first place.

RANSOMWARE SLAYER

RANSOMWARE SURVIVAL CHECKLIST

□ Do you have up-to-date antivirus installed on your endpoints?

□ Do you have behavior-based endpoint protection like Barkly installed that can stop attacks antivirus can't?

□ Are you using an automated patch management system? If not, do you have an organized method of discovering, evaluating, and deploying software updates?

□ Have you conducted security awareness training for your users, with an emphasis on identifying potential phishing emails and reporting any suspicious or unusual activity as soon as possible?

□ If possible, have you disabled Microsoft Office macros?

□ Do you understand how an attack can spread through shared network drives?

□ Have you limited user access and privileges to the bare minimum they need to do their jobs?

□ Do you have backups on their own separate network?

□ Do you have an up-to-date inventory of the backup recovery point objective (RPO) and recovery time objective (RTO) for all your workstations and servers?

□ Do you have a schedule for regularly testing your backups?

□ Have you conducted a risk assessment to identify and assign value to your organization's critical data assets?

□ Do you know your cost of downtime? Figuring this out will help you put a dollar amount on keeping your systems up and ransomware-free.

Barkly

ABOUT BARKLY

Barkly™ is a new layer of endpoint protection that prevents damage when users click on bad stuff. Let's face it – ransomware, zero-day attacks, and other sophisticated malware get by antivirus. No matter how diligently you train your users to avoid suspicious emails, websites, and ads, bad clicks still happen. This results in headaches for you and downtime for everyone – but it doesn't have to be that way.

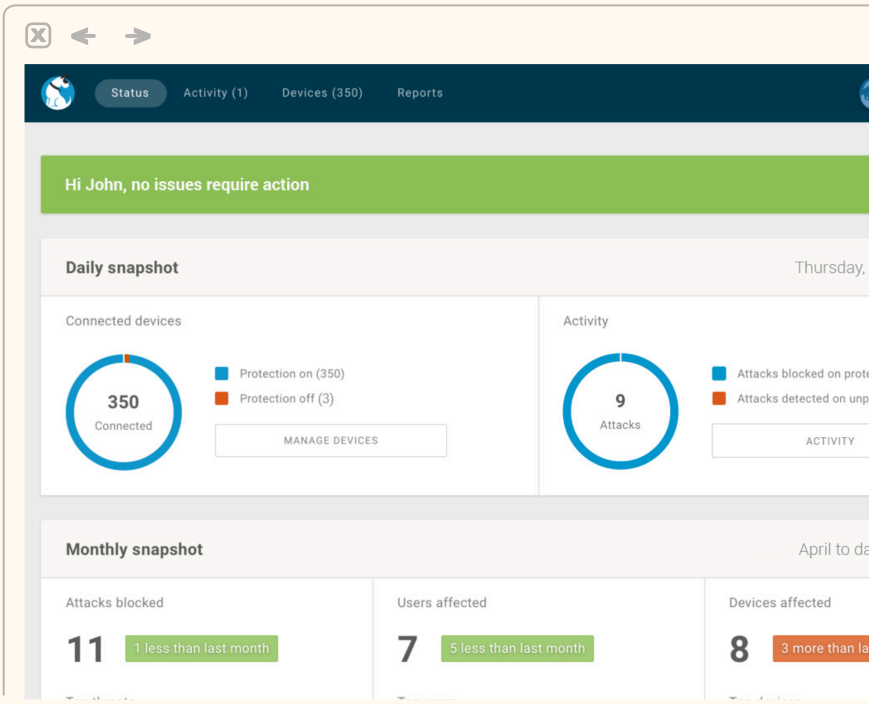
When end user training and antivirus fail, Barkly has your back. Our software monitors activity across the system and blocks malicious processes from executing. We recognize malware based on actions, not appearances, so we can block attacks even if they've never been seen before.

TAKE A TOUR OF BARKLY

Blocks attacks based on behavior
Barkly isn't antivirus, and doesn't look at signatures or scan files. Instead, we recognize malicious behavior, and block it before it can do harm.

Easy to install and manage
It takes just a few minutes to install Barkly on your endpoints. You can manage devices and report on protection 24/7 through Barkly's cloud-based portal.

Low resource utilization
Barkly uses less than 1% of CPU. It's practically invisible to end users. They'll only see Barkly when we block an attack on their device.



Hi John, no issues require action

Daily snapshot
Thursday,

Connected devices
350 Connected
🟦 Protection on (350)
🟥 Protection off (3)

Activity
9 Attacks
🟦 Attacks blocked on prote
🟥 Attacks detected on unp

Monthly snapshot
April to da

Attacks blocked
11 1 less than last month

Users affected
7 5 less than last month

Devices affected
8 3 more than la

LIKE TO LEARN BY DOING?

Jump right into a free 15 day trial and see how Barkly works for you »

Barkly™