proofpoint®

THE 2017 RANSOMWARE SURVIVAL GUIDE

What Every Organization Needs to Know
Before, During, After an Attack

EXECUTIVE SUMMARY

Ransomware is an old threat that has come roaring back with a new ferocity. This type of malware—which gets its name from the payment it demands after locking away victims' files— has quickly become one of the top types of cyber attacks.

More than half of companies surveyed in a recent Ponemon Institute poll said they have experienced a ransomware attack. Among that half, victims saw an average of four attacks each. They paid an average of $2,500 per attack.[1] Aside from the ransom itself (assuming victims pay), these attacks can exact a heavy toll: business disruption, remediation costs, and a diminished brand.

Most ransomware spreads through phishing email, though mobile devices and infected websites are also vectors.

Why ransomware is surging

Ransomware has exploded in recent years because of four primary drivers:

- Attackers have many distribution channels, boosting the chances of success
- It's cheaper than ever to build
- If provides more lucrative targets that are highly motivated to pay the ransom
- The ransom is easier to collect, thanks to Bitcoin and other digital currency

Surviving ransomware

Most companies are ill-prepared for a ransomware attack. Although 66% of those surveyed in the Ponemon poll agree that ransomware is "very serious," only 13% said their company can prevent it.[2]

Consider the following a starting point.

Before the attack

The best security strategy is to avoid ransomware altogether. This requires planning and work—before the crisis hits.

Back up and restore

The most important part of any ransomware security strategy is regular data backups. Surprisingly few organizations run backup and restore drills. Both halves are important; restore drills are the only way to know ahead of time whether your backup plan is working.

Update and patch

Keep operating systems, security software and patches up to date for all devices.

Train and educate, beware macros

Employee training and awareness are critical. Your people should know what to do, what not to do, how to avoid ransomware, and how to report it. If employees receives a ransomware demand, they should know to immediately report it to the security team—and never, ever try to pay on their own.

Invest in robust email, mobile and social media security solutions

Even the best user training won't stop all ransomware.

Advanced email security solutions protect against malicious attachments, documents and URLs in emails that lead to ransomware. Also invest in mobile attack protection products to stop malicious mobile applications from compromising your environment.

1 Ponemon Institute. "The Rise of Ransomware." January 2017..
2 Ibid.

During the Attack: Getting Back to Business

While the best ransomware strategy is to avoid it in the first place, this advice means nothing if you're newly infected.

You have short-term problems to resolve, like getting computers, phones and networks back online, and dealing with ransom demands.

Call law enforcement

Ransomware is a crime—theft and extortion are in play. Notifying the proper authorities is a necessary first step.

Disconnect from the network

The second employees see the ransomware demand or notice something is odd, they should disconnect from the network and take the infected machine to the IT department.

Only the IT security team should attempt a reboot, and even that will only work in the event it is fake scareware or rudimentary mobile malware.

Determine scope of problem based on threat intelligence

Your response—including whether to pay the ransom—hinges on several factors:

- The type of attack
- Who in your network is compromised
- What network permissions compromised accounts have

Orchestrate a response

A big part of your response is deciding whether to pay the ransom. The answer is complicated, and may require you to consult law enforcement and your legal counsel. Paying may be unavoidable.

Don't count on free ransomware decryption tools

Most free tools work for only a single strain of ransomware or even a single attack campaign. As attackers update their ransomware, the free tools fall out of date and likely won't work for your ransomware.

Restore from Backup

The only way to completely recover from a ransomware infection is restoring everything from backup. But even with recent backups, paying the ransom might make more financial and operational sense.

After the Attack: Review and Reinforce

We recommend a top-to-bottom security assessment to find threats that may still linger in your environment. Take a hard look at your security tools and procedures—and where they fell short.

Cleanup

Some ransomware contains other threats or backdoor Trojans that can lead to future attacks.

Look closer for hidden threats that you may have overlooked in the chaos.

Post-mortem review

Review your threat preparedness and response. Without figuring out how the ransomware attack got through, you have no way of stopping the next attack.

Assess user awareness

A well-informed employee is your last line of defense. Ensure employees, staff or faculty are up to the task.

Education and training

Develop a curriculum to address employee vulnerability to cyber attack. Create a crisis communications plan in the event of a future attack, and follow-up with drills and penetration testing.

Reinforce your defenses

Today's fast-changing threat landscape requires security solutions that can analyze, identify and block—in real time—the malicious URLs and attachments that serve as ransomware's primary attack vehicles.

Seek out security solutions that can adapt to new and emerging threats and help you respond to them faster.

INTRODUCTION

INTRODUCTION

This first signs of trouble appeared around lunchtime as U.K. healthcare workers tried to log in to hospital computers. They were locked out, and a strange message appeared on the screen.

"Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted," the message said. "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."[3]

The computers were infected with ransomware, a cyber attack that locks away victim's files until they pay a fee to get their data back. The attack left patient records, appointment schedules, internal phone lines, and emails inaccessible. It severed links between computers and medical equipment. It forced medical workers to send emergency patients elsewhere and run the hospital on pen and paper and their personal mobile phones.[4]

"We were told to shut down, take out network cables and unplug the phones," said a worker for the country's National Health System quoted by *The Guardian*, a U.K. newspaper.[5]

The attack, dubbed "WannaCry" by security experts, was spreading. Within hours, more than 40 organizations within the NHS had been infected with the ransomware.[6] Over the next day, it hit tens of thousands of systems of across more than 150 countries, affecting "universities in China, rail systems in Germany, even auto plants in Japan."

For many, WannaCry was a wake-up call about the threat ransomware poses—and how unprepared they are for it. More than half of IT experts surveyed by Ponemon Institute said their organization is not ready to fend off ransomware attacks. And just 38% have a strategy to deal with destructive software.[7]

Consider this guide a starting point. We'll reveal the factors behind ransomware's meteoric rise, what to do if it happens to you, and most important, how to avoid falling victim in the first place.

"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."

WannaCry ransom note

3 Damien Gayle, Alexandra Topping, et al (The Guardian). "NHS seeks to recover from global cyber-attack as security concerns resurface." May 2017.
4 Ibid.
5 Ibid.
6 Nicole Perlroth (The New York Times). "A Cyberattack 'the World Isn't Ready For." June 2017.
7 Ponemon Institute LLC. "2016 State of the Endpoint Report." April 2016.

AN OLD THREAT GETS NEW LIFE

Ransomware is an old threat that has come roaring back in recent months with new variants. It blocks access to a computer system or data, usually by encrypting files with specific extensions (JPG, DOC, PPT, etc.). Files remain out of reach until the victim pays the attacker for an encryption key code to unlock the files. In many cases, the payment demand comes with a deadline. If not met, that ransom can double, or the data can be lost forever and even destroyed.

The real world costs

Nearly 60% of companies surveyed by the Ponemon Institute agreed that a ransomware attack would have "serious financial consequences" for their business.[8]

Aside from the ransom itself (assuming victims pay), these attacks can exact a heavy toll: business disruption, remediation costs, and a diminished brand.

Consider the WannaCry attack. While it didn't net much of a payday for the attackers, the ransomware was highly disruptive. Not having access to critical information and working systems can slow emergency response and jeopardize public safety.

The healthcare sector has been hit especially hard. Infections lock away patient records, slow workflow, and even affect patient monitoring systems. This can make ransomware remediation a matter of life and death.

Exploiting the human factor

Most ransomware spreads through phishing email. These emails trick users into opening a malicious attachment or clicking a malicious URL.

In February 2016, a widely used ransomware strain called Locky infected Methodist Hospital of Kentucky through a targeted email campaign.

After an employee opened what looked like an unpaid invoice, Locky executed and propagated itself through the entire internal network. It locked down workstations and restricted access to the central server. The hospital's choice: restore each workstation from backup or cough up a relatively modest four bitcoins (about $1,600) to unlock the files.

Our researchers had discovered the Locky strain about a month earlier. Locky is primarily distributed through Microsoft Word attachments, often disguised as unpaid invoices. When the document is opened, users are asked to enable macros. If they do, an executable file known as Troj/Ransom-CGXis downloaded from a remote server. It goes on to encrypt sensitive files and ultimately launch Locky.[9]

Once encrypted, a message pops up demanding payment usually with instructions involving the Tor network and bitcoin. Victims can't close nor get around the message. No amount of CTRL+ALT+DEL or rebooting will solve the problem.

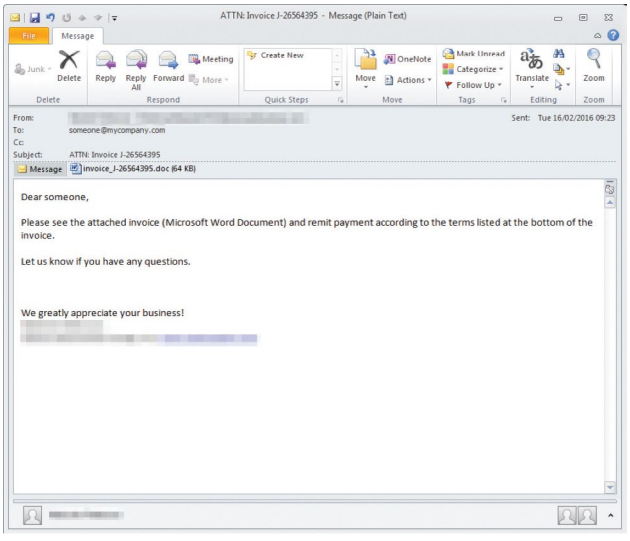
WHERE IT COMES FROM

Ransomware is distributed via three main attack vectors:

- Email
- Mobile devices
- Infected websites/links through social media and malware-infected advertising (malvertising)

By far, emails with malicious attachments or links presents the biggest threat vector, accounting for about 85% of all ransomware we've detected.

These emails look legitimate and can fool unsuspecting employees. Often, the emails will masquerade as official software updates, unpaid invoices, or even a note from the boss targeted to a direct report.



Most ransomware spreads through phishing email like this one.

8 Ponemon Institute. "The Rise of Ransomware." January 2017.
9 Proofpoint. "Dridex Actors Get In the Ransomware Game With 'Locky.'" February 2016.

WHY IT'S SURGING

Ransomware is a decades-old exploit. But it has exploded in recent years because of four primary drivers:

More distribution channels

Cyber criminals can attack thousands of entities simultaneously using a variety of attack vehicles. That means ransomware exploits are succeeding more often.

Conventional email gateways are overwhelmed with threats from all sides:

- Massive botnet-driven email campaigns
- Polymorphic malware that outpaces security vendors' ability to build new signature
- Malicious URLs and malvertising that contain no attachments

Together, these factors give ransomware a better chance of getting through.

Cheaper to build

As in any business, success breeds success. Ransomware authors have honed their craft. And sophisticated tools that would have been feasible for only elite cyber criminals just a few years ago are now widely available. The result is higher success rates and ultimately, economies of scale.

If 4,000 attacks go out in a single day and even 1% of recipients pay a $400 ransom, that's $16,000 revenue for a day's work. Over the course of a year, profits can reach well into the millions.

More lucrative targets

Instead of targeting individuals, cyber criminals are increasingly turning their sights to organizations with sensitive data, thinly stretched IT departments, and a high incentive to quickly settle the matter. Adding fuel to the fire are poor networking configurations common in hospitals, police departments, schools, and other state and local governments.

For these organizations, network downtime is not a viable option. It's no wonder that many make the quick calculation that forking over a ransom is the best business move.

Bitcoin and other digital currencies

Since its debut in 2009, Bitcoin has been a boon to civil libertarians and cyber criminals alike. Payments can't be traced back to sender or recipient, providing an anonymous, friction-free way to transact private commerce.

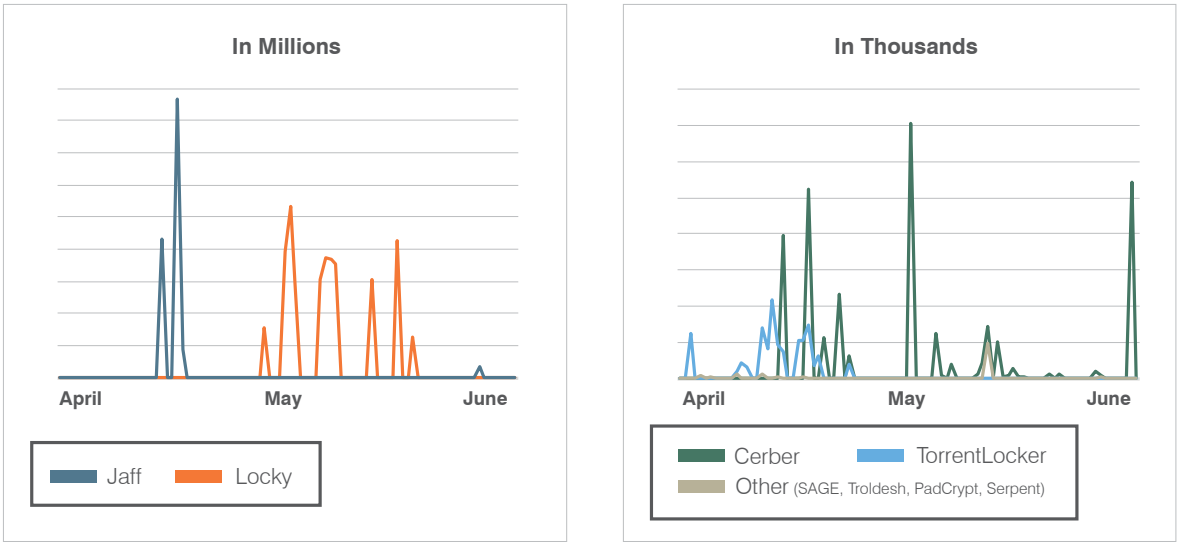
By demanding payment in Bitcoin, cyber criminals get anonymity that makes collecting ransoms far easier than before. Earlier forms of ransomware might require a pre-purchased debit card. While this approach can bypass banks' anti-fraud measures, it's much more cumbersome on both sides of the transaction.

All major variants of ransomware require payment in bitcoin. (See sidebar, page 9.)

Top Malware Payloads by Message Volume

Document attachment campaigns, Q2 2017

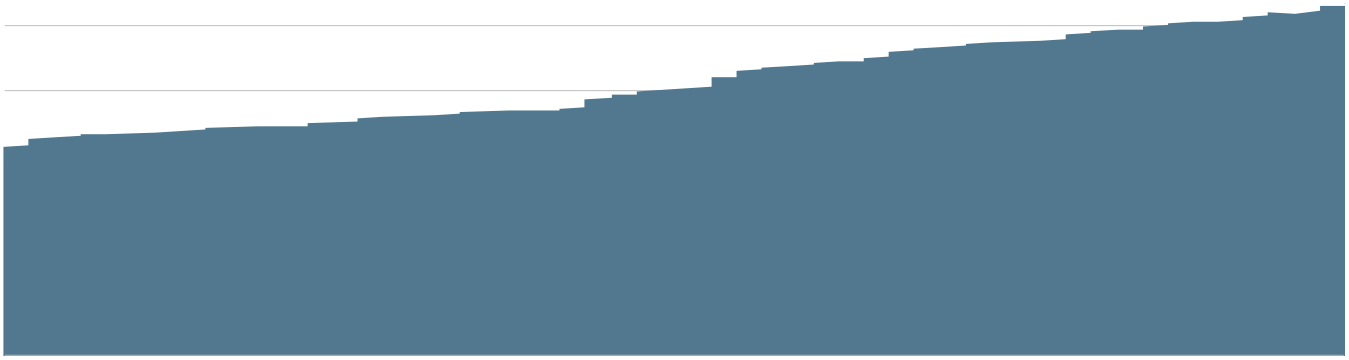
Source: Proofpoint, Inc.



Indexed daily message volume of top ransomware strains, April-June 2017

Cumulative Number of Reported Ransomware Strains, 2017 YTD

Source: Proofpoint, Inc.



December 2015 June 2017

THE BITCOIN MONEY TRAIL

In traditional kidnapping for ransom, the biggest challenge has always been collecting and getting away with the ransom itself. Unfortunately, ransomware cyber criminals have a much easier path.

The most popular form of payment involves untraceable cryptocurrencies, the most well-known of which is Bitcoin. Bitcoin enables person-to-person payment via the internet and does not involve a bank or government. There are 21 million bitcoins in the world. Since its debut in 2008, the currency has seen wild value fluctuations. At the time of this publishing, one bitcoin is worth almost US $600.

A simple way of thinking about cryptocurrencies is to imagine them as the electronic equivalent of a casino chip. The tokens have no intrinsic value in the real world, but users can purchase tokens in their local currency and use them within the establishment—in this case the internet—then trade them in for currency upon exiting.

Similarly, cryptocurrencies can be purchased online using a credit card or bank account, from legitimate sources. In the case of ransomware, victims convert their local currency into “three bitcoins” for example, then send the bitcoins from a bitcoin wallet using the anonymous Bitcoin address provided by the attacker.

The coins don’t always go directly to the attacker. Typically, the tokens will land at a “tumbler,” an electronic service that mixes the bitcoins in with others, then dispenses coins out to the attacker (differently numbered, but the same value minus commission).

Much like money laundering in the physical world, the attackers can end up with untraceable payment. That payment then converts back into their local physical currency by trading in their bitcoins (tokens) for physical cash.

Note that unlike government-backed currency, cryptocurrencies are not widely recognized as money. They are instead regarded as something equivalent to poker chips or gaming tokens. Therefore, the transmission system and tumblers are neither regulated nor considered money laundering—though the effect is arguably the same.

The appeal of Bitcoin is obvious. It gives attackers a hard-to-trace, globally available cyber currency that converts directly to local hard currency, in other words, “unmarked bills.”

Such an approach has clear benefits over the use of stolen credit cards, whose value plummets by the day as financial institutions have become more adept at swiftly shutting down victims’ accounts.

MOBILE RANSOMWARE

Imagine whipping out your phone, but instead of seeing your home screen, it's a warning—seemingly from the FBI—accusing you of viewing illicit images. Your phone has been encrypted and someone is threatening to contact authorities unless a $300 payment is surrendered to make it all go away.

For countless mobile users, this situation is all too real, just one example among hundreds of versions of mobile ransomware.

We have detected three main attack vectors for mobile ransomware.

Android

We have Android-targeted ransomware derives from the same general family as the ransomware variant Cryptolocker. It may masquerade as an Adobe Flash Player update that requires permissions. Or it might piggyback a popular game or "free" app from a rouge app store. (The vast majority of Android ransomware arrives third-party app stores, not the official Google Play store.)

Once launched, the ransomware encrypts the mobile device and requires a timely payment—usually with Bitcoin.

SMS-distributed applications

These are typically porn apps that will take over a device's screen—often with reprehensible images—and demand payment to make it disappear. They are typically spread via text message, but can also be found on social media, often in Twitter or Instagram direct messages.

Unlike most ransomware, the data is generally not encrypted. But for users, the effect is the same—devices are locked up. Getting around this type of threat is possible, but is also highly complicated. Many users opt to just pay the ransom.

iOS browsers

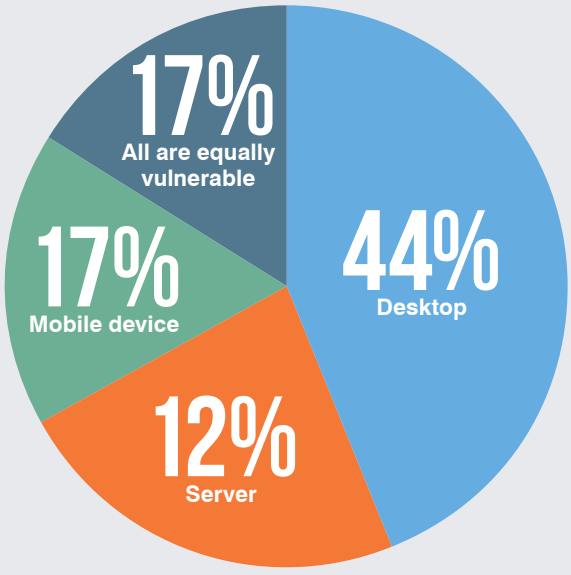
Ransomware targeting iOS devices typically comes in the form of browser-based ransomware. It often warns victims that they've downloaded illegal images or claim that their device is infected. To unlock or "fix" the device, the victim is directed to a site for payment via Bitcoin or pre-purchased debit card.

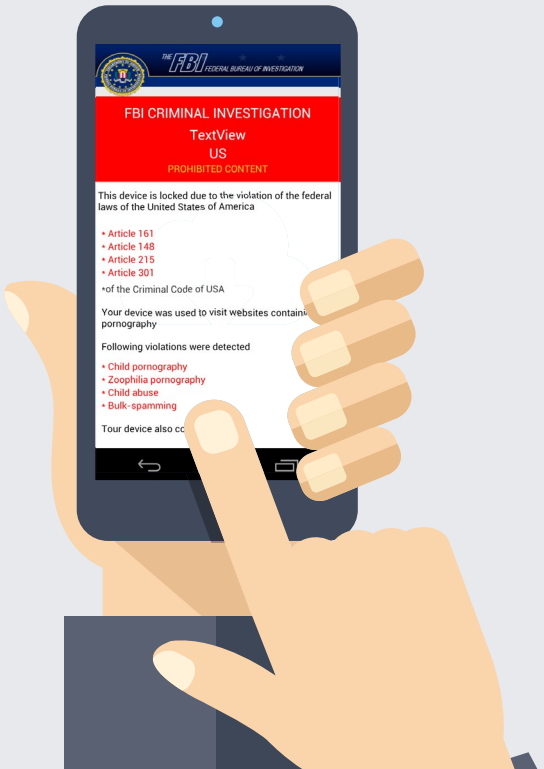
These fraudulent ransomware sites are mostly propagated through adult website malicious ads. The conversion rate of these sites into paying victims is low. But when hundreds of thousands or millions of victims are infected per week, the scheme pays off.

As of this publication, we have not seen broad-based encryption of iOS devices. The majority of these schemes simply lock victims out of their web browsers.

WHICH DEVICES ARE MOST VULNERABLE TO A RANSOMWARE ATTACK?

Source: Ponemon Institute. "The Rise of Ransomware." January 2017.





BEFORE THE ATTACK

PREVENTING RANSOMWARE

The best security strategy is to avoid this extortion altogether. This is well within the power of most companies, but it requires planning and work—before the crisis hits.

Back up and restore

The most important part of any ransomware security strategy is regular data backups. Most companies do this, but surprisingly few run backup and restore drills. Both processes are important; restore drills are the only way to know ahead of time whether your backup plan is working.

You may have some kinks to work through before crisis mode hits. If backups and restore testing are done regularly, a ransomware infection won't have a devastating impact; you'll have a safe, recent restore point.

To repeat: most companies and individuals do backups. But regular testing of a full restore is just as critical.

Update and patch

Ensure operating systems, security software and patches are up to date for all devices. It sounds basic enough, but according to a recent survey, about half of IT professionals admit they struggle to keep up with sheer volume of patches released every month. And respondents reported that updates vary wildly in terms of complexity and release schedule.

Teams also struggle when updating certain applications, like Adobe Flash, that might break other internal functionality that relies on the software. Hackers understand that these and other factors can lead to "patch fatigue," and develop their exploits accordingly.[9]

Train and educate, beware macros

Most ransomware begins with a single well-intentioned employee opening what appears to be a work-related email.

That's why employee training and awareness are critical. Your people should know what to do, what not to do, how to avoid ransomware, and how to report it. If anyone receives a ransomware demand, they should know to immediately report it to the security team—and never, ever try to pay on their own. (Payment may carry serious brand reputation and security ramifications.)

Our research shows that cyber criminals actively exploit human error and curiosity. The recent surge in ransomware emails is part of a larger cybercrime trend—fooling humans into becoming unwitting accomplices in the quest to lock information and demand payment.[10]

These attacks play on the user's lack of awareness and typically require them to open malicious Word document attachments or JavaScript attachments and enable macros. Once users click the "Enable Content" button to turn on macros, the malicious macro downloads ransomware and starts the attack process. One option is to disable macro scripts from office files transmitted over email. But some macros can be useful, and disabling them completely may hinder productivity.

Invest in robust email, mobile and social media security solutions

Even the best user training won't stop all ransomware. Today's phishing email is sophisticated and highly targeted. Attackers carefully research their targets to create email that looks legitimate and preys on human nature to get them to click.

Because most ransomware is transmitted through email, mobile and social media, you need advanced solutions that can stop these threats in real time. According to our research, the volume of ransomware attacks has soared. In the email channel alone, ransomware accounts for nearly 70% of overall malicious messages.[11]

Traditional legacy mail gateways, web filters, and antivirus software should be updated and running on all networks. But they alone cannot counter the ransomware threat. An effective email security solution must go deeper. That means analyzing embedded URLs and attachments to ensure no malicious content breaches the system. Cyber thieves are always one step ahead, and typical email security configurations rely far too heavily on outdated signatures.

Advanced email security solutions protect against malicious attachments, documents and URLs in emails that lead to ransomware. At the same time, invest in mobile attack protection products to stop malicious mobile applications from compromising your environment.

9 Tripwire, Inc. "Tripwire 2016 Patch Management Study." March 2016.
10 Proofpoint. "The Human Factor 2016." February 2016.
11 Proofpoint. "The Human Factor 2016." February 2016.

AS "RANSOMWORMS" GRAB SPOTLIGHT, EMAIL IS STILL KING

High-profile outbreaks of ransomware threats such as WannaCry and Petya—which spread like a computer worm rather than email—have ushered ransomware into the global spotlight. But these so-called "ransomwoms" remain the exception. Most ransomware attacks, like most cyber threats overall, are sent through email.

Consider Jaff, a strain of ransomware that quickly and quietly eclipsed the largest malware campaigns of 2017. By midyear, Jaff was by far the top malware payload by message volume seen in Proofpoint deployments around the globe. It accounted for 72% of ransomware email and nearly half of all malware-laden email overall.

High-volume Jaff campaigns stopped as soon as a decryptor was made available in mid-June. But the attacker behind them switched back to Locky and continued to send another ransomware strain called The Trick. This fast pivot underscores just how easily attackers can adapt to new defenses.

Many other ransomware strains are sent in smaller, more targeted efforts. Cerber, for instance, targets U.S. companies. TorrentLocker is aimed at Europe. And Serpent has affected Belgium and Netherlands.

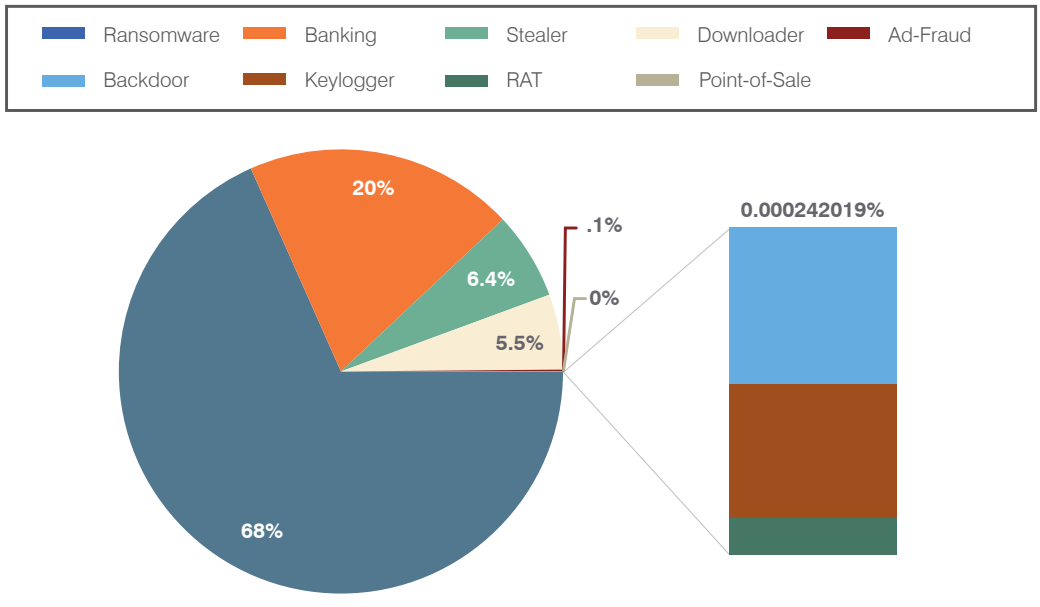
Some ransomware strains, such as the easy-to-customize Philadelphia, even targets specific firms.

WannaCry and Petya remain the exception for another notable reason: they appeared to focus more on wreaking havoc than actually collecting a ransom.

"I'm willing to say with at least moderate confidence that [Petya] was a deliberate, malicious, destructive attack," Nicholas Weaver, a security researcher at the International Computer Science Institute, told journalist Brian Krebs. "Or perhaps a test disguised as ransomware."[12]

For verified ransomware attacks, email is by far the most common source.

Malware by Category, Q1 2017



Comparison of quarterly overall message volume
(Source: Proofpoint)

12 Brian Krebs (Krebs on Security). "'Petya' Ransomware Outbreak Goes Global." June 2017

DURING THE ATTACK

GETTING BACK TO BASICS

You've been hit with ransomware. Now what?

While the best ransomware strategy is to avoid it in the first place, this advice means nothing if you're newly infected. You have short-term problems to resolve, like getting computers, phones and networks back online, and dealing with ransom demands.

But a panicked response won't help—and may make things worse.

Call law enforcement
Ransomware is a crime–theft and extortion are in play. Nobody has the right to seize devices, networks or data, let alone demand a ransom in exchange for it. Notifying the proper authorities is a necessary first step.

Visit your closest field office. Do not be afraid to just pick up your phone and call them. They are there to help you.

Disconnect from the network
The second employees see the ransomware demand or notice something's odd—such as suddenly losing access to their own files—they should disconnect from the network and take the infected machine to the IT department.

We advise against having employees reboot their system. Only the IT security team should attempt a reboot, and even that will only work in the event it is fake scareware or rudimentary mobile malware.

In those cases, what appears to be ransomware is better described as "scareware." It may lock the user's screen with a ransom demand and payment instructions, but the data is not actually encrypted. In those scenarios, a simple CTRL+ALT+DELETE, pulling up Windows' "Task Manager" and closing the browser should fix the problem.

Determine scope of problem using threat intelligence
While all ransomware is bad, some attacks are worse than others. Your response—including whether to paying the ransom—hinges on several factors.

Ask the questions:

- What type of attack is this? Ransomware leaves calling cards, and your response may hinge on who's attacking you and the tools.
- Who in your network is compromised?
- What network permissions do any compromised accounts have?

Your answers should help network administrators scope the problem, devise an action plan and possibly curtail the spread.

Orchestrate a response
Depending on network configuration, containing the spread to a single workstation might be possible.

Best case scenario: a new computer is swapped out for the infected machine and a restore from backup is completed. Worst case: every network machine is infected. This will require a quick cost-benefit calculation that weighs man hours needed to resolve vs. simply paying the ransom.

A big part of your response is deciding whether to pay the ransom. The answer is complicated and may require you to consult law enforcement and your legal counsel. For many victims, paying may be unavoidable (see page 16).

Don't count on free ransomware decryption tools
Some security vendors offer free ransomware decryption programs. In some cases, they can help you retrieve your data without paying the ransom.

But most work for only a single strain of ransomware or even a single attack campaign. As attackers update their ransomware, the free tools fall out of date and likely won't work for your ransomware.

You may get lucky with a free decryption tool, but don't make it part of your incident response plan.

Restore from Backup
The only way to completely recover from a ransomware infection is restoring everything from backup—backups that should be happening every day. This might come last in terms of steps to take once infected, but should be first in terms of prevention.

Even with recent backups, though, paying the ransom might make more financial and operational sense. Restoring backups takes time and effort. Some businesses might not be able to afford the downtime.

TO PAY OR NOT TO PAY: RANSOMWARE'S MORAL DILEMMA

Ransomware is bad enough in itself. But one of its especially loathsome aspects is that it forces victims to make both a Hobson's Choice and a moral one. When you're under the gun of a ransomware threat, you don't often have the luxury of time to carefully weigh the moral nuances of paying up. The attack is here—now.

Up until now, malware exploits have mostly required a straightforward course of action: fraud detection, report filing, and resolution. Ransomware now introduces morality into the equation.

Paying up isn't just a repugnant but necessary evil. It actively funds the attacker that has just broken into your network and stolen your data. It marks you as someone with a vulnerable network and incentive to pay. And it enables the cyber criminal to bankroll future attacks.

But recent attacks highlight an uncomfortable fact: there isn't always a black and white answer on whether to pay.

No organization wants to be extorted, let alone fund criminal rings. Then again, what choice did the hospital have? In some ways, it's the price to pay for having underfunded IT departments running unpatched or outdated software. There are still hospitals in the U.S. running Windows XP. And $17,000 is a relatively small price to pay when lives are on the line.

Even the FBI has advised victims to "just pay the ransom," according to Joseph Bonavolonta, Assistant Special Agent in Charge of the Cyber and Counterintelligence Program in the FBI's Boston office.[13] Still, the agency officially discourages paying. It points out that even you pay, you may not get your data back.[14]

Organizations must to weigh conflicting considerations when choosing the best course of action. These factors can include:

- Time and man-hours getting back online
- Responsibilities to shareholders to keep the business up and running
- Safety of customers and employees
- What criminal activity the payment will potentially fund.

As with most complicated questions, no two organizations will answer them in the same way.

PAYING UP ISN'T JUST A REPUGNANT BUT NECESSARY EVIL. IT ACTIVELY FUNDS THE ATTACKER THAT HAS JUST BROKEN INTO YOUR NETWORK AND STOLEN YOUR DATA.

13 Tess Danielson (Business Insider). "The FBI says you may need to pay up if hackers infect your computer with ransomware." October 2015.
14 FBI. "Ransomware." April 2016.

AFTER THE ATTACK

REVIEW AND REINFORCE

Regardless of the damage caused by ransomware, the attack reveals a security failure resulted in a device or network compromise. Now that things are back to normal, you have an opportunity to learn from the security breach and avoid future attacks.

We recommend a top-to-bottom security assessment, perhaps by an outside services firm, to find threats that may still linger in your environment. Now is also the time to take a hard look at your security tools and procedures—and where they fell short.

Cleanup
Some ransomware contains other threats or backdoor Trojans that can lead to future attacks. That's why wiping every device and restoring from a clean backup is a must. Look closer for hidden threats that you may have overlooked in the chaos.

Post-mortem review
Review your threat preparedness and response. How was the crisis plan executed? Can we improve networking configurations to contain future attacks? Can we implement a more robust email security solution?

Audit current security measures and ask if this is enough to combat today's threats. Turn this into a learning experience—because it very well might happen again. Without figuring out how the ransomware attack got through, you have no way of stopping the next attack.

Assess user awareness
Most strains of ransomware rely on human interaction to deploy payloads. Should current security measures fail and an infected "unpaid invoice" makes it onto the email server, a well-informed employee is the last line of defense between a company, hospital or school staying online or becoming another ransomware statistic. Ensure employees, staff or faculty are up to the task.

It might also be worthwhile to invest in penetration-testing companies, whose mission involves driving employee awareness and improving company security. By replicating real world attacks via spear phishing, social engineering and social media exploits, "pen-testers" can analyze and identify security vulnerabilities ahead of actual attacks.

Education and training
After user awareness is analyzed, develop a curriculum to address employee vulnerability to cyber attacks, including lessons learned from previous encounters. Create a crisis-communications plan in the event of a future attack, and follow-up with drills and penetration testing as outlined above.

Invest in modern defenses
Hackers and other cyber criminals have historically been one step ahead of endpoint security measures and law enforcement professionals.

While most networks are adept at blocking known threats, today's fast-changing threat landscape requires security solutions that can analyze, identify and block—in real time—the malicious URLs and attachments that serve as ransomware's primary attack vehicles.

Seek out security solutions that can adapt to new and emerging threats and help you more quickly respond to them.

CONCLUSION

Ransomware has made an impressive and lucrative comeback. These guidelines can start you on the path of dealing with ransomware before, during and after an actual attack.

Of course, the easiest way to combat ransomware is to stop it at the gates. That requires an advanced threat solution that can detect ransomware delivered via email, mobile devices, and social media.

Robust cybersecurity identifies and kills ransomware before it sets foot in your environment. This includes the ability to analyze email attachments and links in real time, deconstruct threats in a virtual environment, and update policies on the fly. This helps reduce the human factor—the weakest link in most security infrastructures.

To learn more about how you can stop ransomware attacks, visit www.proofpoint.com/targeted-attack-protection.

RANSOMWARE SURVIVAL CHECKLIST

Here's a quick checklist to assess whether you're ready to prevent and manage ransomware threats.

Before: preventing ransomware

- [ ] Back up and restore
- [ ] Update and patch
- [ ] Train and educate users
- [ ] Invest in robust email, mobile and social media security solutions

During: getting back to business

- [ ] Call law enforcement
- [ ] Disconnect from the network
- [ ] Determine scope of problem based on threat intelligence
- [ ] Orchestrate a response
- [ ] Don't count on free ransomware decryption tools
- [ ] Restore from backup

After: review and reinforce

- [ ] Clean up
- [ ] Post-mortem review
- [ ] Assess user awareness
- [ ] Education and training
- [ ] Invest in modern defenses

ABOUT PROOFPOINT

Proofpoint, Inc. (NASDAQ:PFPT), a next-generation cybersecurity company, enables organizations to protect the way their people work today from advanced threats and compliance risks. Proofpoint helps cybersecurity professionals protect their users from the advanced attacks that target them (via email, mobile apps, and social media), protect the critical information people create, and equip their teams with the right intelligence and tools to respond quickly when things go wrong. Leading organizations of all sizes, including over 50 percent of the Fortune 100, rely on Proofpoint solutions, which are built for today's mobile and social-enabled IT environments and leverage both the power of the cloud and a big-data-driven analytics platform to combat modern advanced threats.

©Proofpoint, Inc. Proofpoint is a trademark of Proofpoint, Inc. in the United States and other countries.
All other trademarks contained herein are property of their respective owners.

proofpoint. www.proofpoint.com

R-0004-0816