proofpoint.

ADAPTED FROM THE 2021 RANSOMWARE SURVIVAL GUIDE

Ransomware Survival Guide: Executive Summary

Ransomware is an old threat that persists as a modern-day problem. This type of malware—which gets its name from the payment it demands after locking away victims' files— is a major issue for any organisation that relies on IT.[1] It's one of today's most disruptive types of cyber attacks, putting victims out of business[2], forcing hospitals to turn away patients,[3] and bringing entire city governments to a standstill.[4]

Despite a sharp decline in the overall volume of ransomware attempts from historical peaks,[5] the number of organisations experiencing ransomware attacks increased by 15% over one year and have more than tripled in frequency over two years, according to the Ponemon Institute.[6]

Aside from the ransom itself (assuming victims pay), these attacks can exact a heavy toll: business disruption, remediation costs and a diminished brand.[7]

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

Why Ransomware is Still Around

Ransomware has persisted because of four primary drivers:

- Ransoms are easier to collect than in other types of fraud, thanks to Bitcoin and other digital currency
- Attackers have many distribution channels—including existing compromises of an environment—boosting the chances of success
- A large pool of targets relies heavily on IT but have weak or outdated cyber defences and poor backup and recovery routines
- Attackers are getting better at targeting and more sophisticated in their tactics

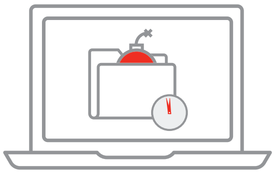
[1] Verizon. "2019 Data Breach Investigations Report."
[2] Jessie Davis *(Health IT Security)*. "Michigan Practice to Shutter after Hackers Delete Patient Files." April 2019.
[3] Lindsey O'Donnell *(Threat Post)*. "Ransomware Attacks Leave U.S. Hospitals Turning Away Patients." October 2019.
[4] Manny Fernandez, David Sanger, Marina Trahan Martinez *(The New York Times)* "Ransomware Attacks Are Testing Resolve of Cities Across America." August 2019.
[5] Proofpoint. "Quarterly Threat Report Q3 2018." October 2018,
[6] Ponemon Institute. "Ninth Annual Cost of Cybercrime Study." 2019.
[7] Ibid.

Surviving Ransomware

Most companies are ill-prepared for a ransomware attack. Although 66% of those surveyed in a Ponemon poll agree that ransomware is "very serious," only 13% said their company can prevent it.[8]

Ransomware compromises systems and data, but the attacks that lead up to it target people. Like most cyber attacks, ransomware usually requires someone to act on the attacker's behalf, such as opening an attachment or clicking a URL. That's why fighting ransomware requires a people-centric approach.

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

One of the most important parts of any ransomware security strategy is regular data backups. Because many ransomware strains target network-connected backups, maintain those backups offsite or in the cloud.

Surprisingly few organisations 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, applications and network hardware patched and up to date.

Train and educate users

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 receive 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 people-centric 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. These solutions also protect against other malware, typically delivered through email, that can install malware in targeted follow-up attacks.

[8] Ponemon Institute. "The Rise of Ransomware." January 2017

During the Attack: Contain the Damage and Get 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—like any form of theft and extortion—is a crime. Notifying the proper authorities is a necessary first step.

Disconnect from the network

The moment 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 run-of-the-mill 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, specifically the ransomware strain used and the attacker behind it
- The presence of earlier malware payloads that may have been used for reconnaissance or loading the ransomware
- Who in your network is compromised
- What network permissions any compromised accounts have

Many ransomware infections are often the result of secondary infections on already compromised networks. That means each of the factors are critical in assessing the scope of the problem and preventing further infections and data loss.

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. In some cases, paying may be unavoidable.

In any case, organisations must proceed thoughtfully. Whenever possible, organisations should have plans—and contingency plans—in place before an attack. And these plans should be tailored to the business. A hospital's response to ransomware on mission-critical patient care systems may be very different than a federal agency's.

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 is delivered through other threats or backdoor Trojans that can lead to future attacks. Often, the victim's environment was already compromised, opening a door for the ransomware.

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

Post-mortem review

Review your threat preparedness, the chain of events that led to the infection, and your 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 defence. Make sure employees, staff and faculty are up to the task. Regular assessments and phishing simulations can help pinpoint who is most vulnerable, and to which email lures and other tactics.

Education and training

Develop a curriculum to address employee vulnerability to cyber attacks. It should be based on real-world attack campaigns and tactics. Create a crisis communications plan in the event of a future attack, and follow-up with drills and penetration testing.

Reinforce your defences

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.

LEARN MORE

For more information, visit **proofpoint.com**.

ABOUT PROOFPOINT

Proofpoint, Inc. (NASDAQ: PFPT) is a leading cybersecurity company that protects organisations' greatest assets and biggest risks: their people. With an integrated suite of cloud-based solutions, Proofpoint helps companies around the world stop targeted threats, safeguard their data, and make their users more resilient against cyber attacks. Leading organisations of all sizes, including more than half of the Fortune 1000, rely on Proofpoint for people-centric security and compliance solutions that mitigate their most critical risks across email, the cloud, social media, and the web. More information is available at **www.proofpoint.com**.

proofpoint.