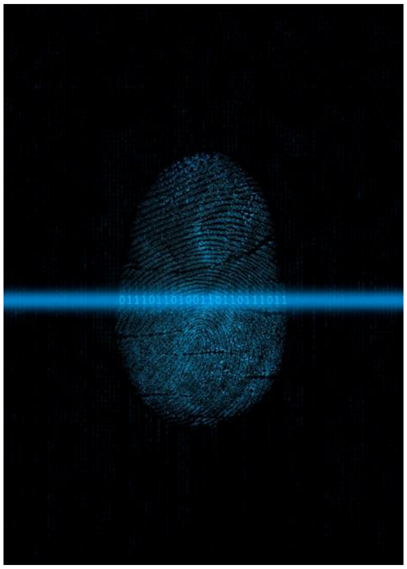
www.pipelinepub.com
Volume 17, Issue 7

Ransomware Explained

By: Mark Hurley



A successful ransomware attack can be devastating to a business. Organizations caught unprepared could be left with the choice between paying a ransom demand and writing off the stolen data entirely.

In our day-to-day cybersecurity practice, we perform a lot of assessments with new and potential clients. Among this wide variety of professional companies, we find very differing understanding of the threat that ransomware poses to their businesses.

There are the ***unknowledgeable optimists*** who believe it will never happen to them. Clearly this is not a recommended stance.

There are also the ***informed optimists*** who believe they have all angles of protection covered. This may or may not be the case. Assumptions can be dangerous.

Finally, there are the ***affected pessimists.*** They have suffered from a ransomware attack, and it may be too late. We receive calls from complete strangers asking how they deal with a ransomware hit. We always ask whether they have a backup and if they carry cyber liability insurance. The silence at the end of the phone can be deafening.

No matter which camp you belong to, it's important to become informed, implement preventative measures and plan for the worst outcomes, so your business can continue to thrive after such an attack.

In this article, we provide key information and some of the measures required to both prepare and recover if your business is affected by a ransomware attack.

What’s ransomware?

Ransomware is a multibillion-dollar criminal enterprise executed by cyber criminals to disrupt access to your systems, business, and personal information. It is a form of malware that encrypts a victim's files. The attacker then demands a ransom from the victim to restore access to the data upon payment.

Once your files are infected, the attackers then demand a ransom (normally in Bitcoin) to liberate access to your data and critical business systems. Ransomware activity is on the rise at an exponential rate. Research suggests that in 2020 a new organization was hit by a ransomware attack every 14 seconds and that ransomware incidence increased 50 percent in Q3 2020 alone.

Adding insult to injury, the cyber criminals are leveraging the Covid crisis to target vulnerable remote workers and infect vulnerable organizations. Cybersecurity Ventures predicts that ransomware damage will exceed $20 billion by 2021.

Ransomware attacks are so effective because they takes many guises. You must be aware of all of them to effectively protect your data and your entire network.

Case Study: The NHS

A famous example of ransomware is the WannaCry attack of May 2017. This was a piece of malware that infected over 230,000 computers across 150 companies within a single day. It encrypted all files it found on a device. Following that, users must pay $300 worth of Bitcoin payments to restore them.

WannaCry mainly affected large organizations, and the National Health Service in the UK was one of highest-profile targets affected. Surprisingly, the attack’s impact was lower than it would have been, due to the fact it was stopped quickly, and it did not target extremely critical infrastructure, like railways or nuclear power plants.However, economic losses from the attack were still in the millions of dollars.

In September 2019, 22 cities in Texas were hit with ransomware. The attackers demanded $2.5 million to restore encrypted files, leading to a federal investigation. These stories are examples of the reality that ransomware attacks are especially prevalent in financial and healthcare organizations. It is estimated that cyber criminals targeted 90 percent of these businesses last year.

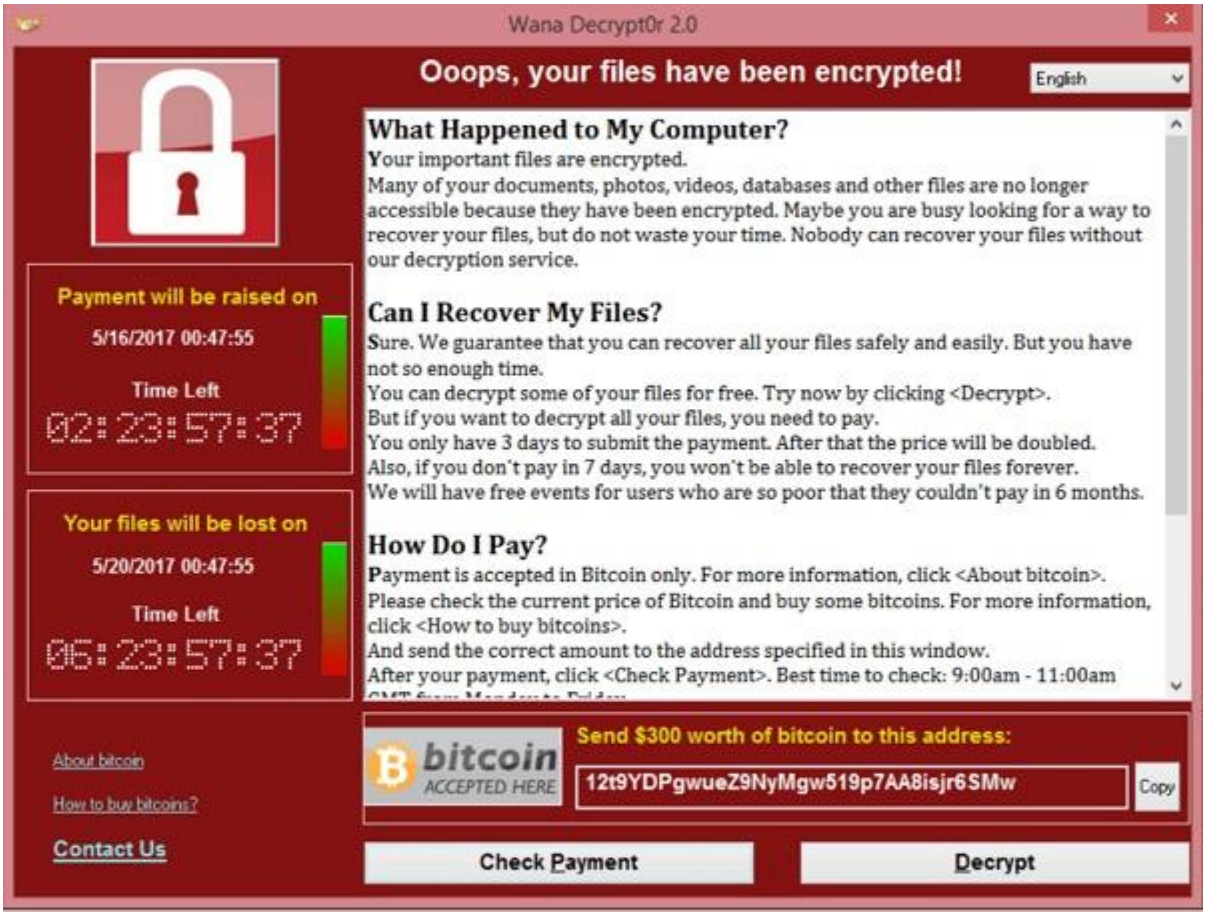
The course of an attack

Ransomware begins with malicious software being downloaded by an unwary person through an infected email or link onto their computer or smart device.

Once ransomware infects an endpoint, it will run freely wherever it has access. In seconds, the malicious software will take over critical processes on the device, then search for files to be encrypted, meaning all the data within them is inaccessible.

The ransomware will then infect any other hard drives, network attached devices and so on, taking out everything in its path—including backups.

This entire process happens extremely quickly. In just a few minutes the device will display a message that looks like this:



Ooops, your files have been encrypted!

What Happened to My Computer?

Your important files are encrypted.

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

Can I Recover My Files?

Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.

You can decrypt some of your files for free. Try now by clicking <Decrypt>.

But if you want to decrypt all your files, you need to pay.

You only have 3 days to submit the payment. After that the price will be doubled.

Also, if you don't pay in 7 days, you won't be able to recover your files forever.

We will have free events for users who are so poor that they couldn't pay in 6 months.

How Do I Pay?

Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.

Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.

And send the correct amount to the address specified in this window.

After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am GMT from Monday to Friday.

Send $300 worth of bitcoin to this address:

12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw

Figure 1: WannaCry Ransomware Attack

This is the message that was displayed to users who were infected with the WannaCry ransomware attack. As you can see, it's a 'cyber blackmail' note. Users are informed that they have been locked out of their files, and they must pay to regain access.

Ransomware risks

The people within your organization are often your biggest security risk. The major issue here is a lack of awareness and staff education about security threats. Many people are unaware of what threats look like, and what they should avoid downloading, leaving you open to risk.

There has been a huge growth in security awareness training platforms. They train users about the risks they face online, at work and at home. Awareness training teaches users what a suspicious email looks like, and the best security practices to follow to stop ransomware, such as ensuring their endpoints are updated with the latest security software. Security awareness training solutions typically also provide phishing simulation technologies.

It may not seem obvious, but identity theft lies at the core of a lot of backdoor ransomware attacks. Hackers use administrative and other accounts to gain a foothold in your core systems. Adding MFA makes the possibility of elevating privileges and giving the attacker the keys to run ransomware without barriers. MFA comes free with most Microsoft 365 packages and more in-depth solutions also exist that extend more granular protection to all devices in the organization.

Continuing the use of end-of-line hardware and software greatly increases your risk. Over time, attackers discover the security vulnerabilities that are widely released by larger corporations. Many organizations rely heavily on older computers or software that are no longer supported, meaning they are open to vulnerabilities. Organizational security policies often overlook hardware or software that is out of date. This greatly increases the organization's risk of falling victim to an attack.

To mitigate risk, keep your operating system and third-party applications patched and up to date to ensure you have fewer vulnerabilities to exploit.

Ransomware attack solutions

One of the most important ways to stop ransomware is to have a strong endpoint security. This is a program that blocks malware from infecting your systems when installed on your endpoint devices (such as phones and computers). Just be sure that ransomware protection is included as many traditional anti-virus products are not equipped to defend against modern ransomware attacks.

As ransomware is commonly delivered through email, email security is key in preventing ransomware. Secure email gateway technologies filter email communications with URL defenses and attachment sandboxing to identify threats and block them from being delivered to users. This stops ransomware from arriving on endpoint devices while blocking users from inadvertently installing malicious programs onto their machines.

DNS web filtering solutions stop users from visiting dangerous websites and downloading malicious files, blocking ransomware that is spread through viruses downloaded from the Internet, including Trojan horse software. DNS filters also block malicious third-party adverts. Isolation technologies completely remove threats from users by isolating browsing activity in secure servers and displaying a safe render to users. Moreover, isolation does not affect the user experience, delivering high security efficacy and seamless browsing.

What to do to minimize downtime

Once a ransomware attack succeeds and your data is compromised, the best protection for your organization is to restore your data quickly and minimize the downtime. The most effective way to protect data is to ensure that it is backed up in multiple places, including in your main storage area, on local disks, and in a cloud continuity service. In the event of a ransomware attack, backing up data means you will be able to mitigate the loss of any encrypted files and regain functionality of systems. Cloud data backup and recovery is a crucial tool in remediating the threat of ransomware attacks.

Reducing the risk and damage of a ransomware attack requires a mix of frameworks, policies, training, and technology. The best companies perform a detailed GAP analysis using a cybersecurity framework such as the NIST CSF in conjunction with security controls such as the CIS 20 controls. This approach leads to better outcomes, period.