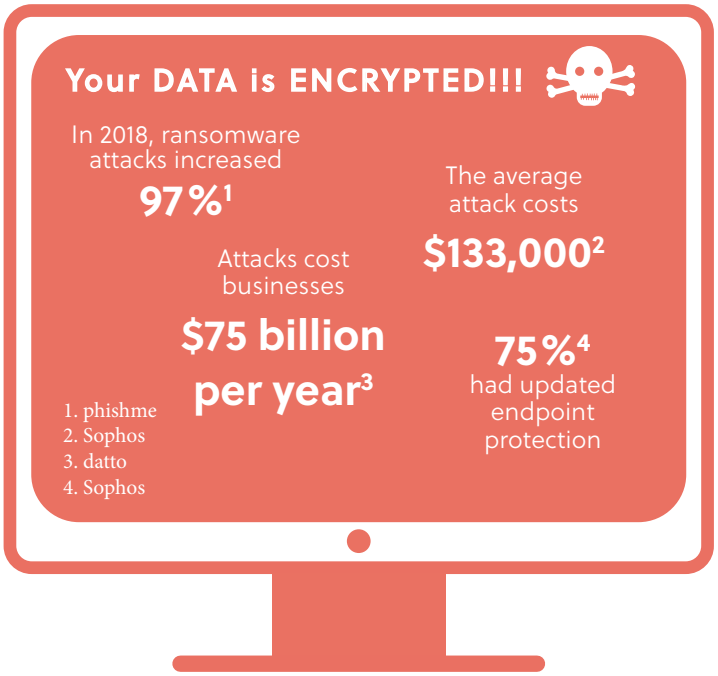
Ransomware: Pay Up & No Byte Gets Hurt

We Value Your Security | Vol. 1 No. 2

The suspense and drama of hijacking, hostage-taking and ransoms has captured the imagination of countless audiences for generations. But if you are looking at a red screen that has sent you scrambling to research "encryption," buy Bitcoins, or try to hack your own device, chances are the excitement of being a part of your own hi-tech swashbuckling, hostage-taking adventure has escaped you. You are the victim of a ransomware attack and the people responsible are betting that you are willing to pay for your cameo to end.

Ransomware attacks are just one way cybercriminals will try to profit from gaining access to protected information. PFM's approach to safety and security stretches well beyond financial guidance and asset management, which is why we believe bringing awareness to cyber attacks, like ransomware, is essential to the stewardship of public funds. In this article we will discuss why ransomware is a threat to public agencies and what you can do to be prepared.

Ransomware is on the March



What is Ransomware?

Ransomware is a type of malicious software designed to make files and systems inaccessible to the rightful owner in order to demand a price, or "ransom," for restoring access. It can take advantage of the myriad of ways hackers gain illicit access of computing devices.

COMMON TYPES OF ATTACKS

- **Phishing Attacks:** An email using social engineering techniques to influence a user to click a link or run a program. We covered these attacks in detail in a previous article (*When You Just Aren't Yourself: Combating Social Engineering Attacks*).
- **Trojan Horses:** Viruses that are embedded or disguised within innocuous programs or even seemingly necessary software that an unwitting user runs on their machine.
- **Worms:** A self-replicating program that moves through computer networks. Unlike the methods above, a worm does not depend on tricking users – all this form of ransomware needs is a device to access an infected network.
- **Hacking Weak Passwords:** Described as using "brute force attacks," this type of hacking uses a program to try common passwords until one works. This approach may seem like a fool's errand, however, it is actually simply a numbers game. Careless or simple passwords and poor network security features can turn an impossibility into an inevitability.

- **Networking Vulnerabilities:** Some of the biggest, most newsworthy attacks have been launched through vulnerabilities identified by hackers related to missing operating system patches, outdated software releases, misconfigured firewalls, and the use of default passwords.

Unlike other types of malicious attacks (spyware, phishing, etc.), ransomware will make itself known. Usually, there is a pop-up informing the user that their data has been taken hostage. There may be a countdown clock, a description of how the data has been made inaccessible and what the user may need to do to get it back.

Invariably, there is a price requested and instructions for how to pay it. The most frequent demand is for Bitcoin or some other cryptocurrency. However, gift cards, premium-rate SMS or long distance telephone fees have also been reported. Some programs even employ negotiating tactics, such as offering some non-essential files back as a goodwill gesture, or using a tiered pricing structure based on how long it takes to pay the ransom. Ransomware attacks also often involve taking control of data and system resources used by public sector entities to deliver essential services (e.g. healthcare, law enforcement, utilities, etc.), which increases the likelihood of a ransom getting paid.

Ransomware can take control of your device in many different ways. Some of the most common are listed below:

- A Blocker is a program that inhibits your ability to use the infected device. It could be a browser window that cannot be closed through the usual means, a fake software update window that demands action, a fake message from a law enforcement agency or a program that floods the screen with unwanted images.
- Encryption is a technology that scrambles data to protect it from being read by anyone except those with the "key." The key is usually a random string of alphanumeric characters. Some forms of encryption can be reversed, but not without significant time and cost that is often beyond the value of the data. For this reason, blockers often claim encryption even if the data is not actually encrypted.
- Leakware is a form of ransomware that threatens to release sensitive information publicly instead of inhibiting access.

How Big of a Problem Is This Really?

According to industry experts, the damages caused by ransomware attacks have increased. This is partly due to hackers getting better at targeting institutions and organizations directly, especially those that have the resources to pay larger ransoms. In other words, your personal computer is less likely to be targeted or taken "hostage," but your work files could be a prized objective for cybercriminals.

It is also important to note that the damages of a ransomware attack go well beyond the actual ransom – in fact paying the ransom could only be the beginning. A ransomware attack can cost an organization millions in lost productivity and reputational damages. Not to mention the time and resources it could take to get the affected system(s) in working order again.

One reported attack on a large municipality was estimated to cost close to $17 million. That price tag may make it seem like a necessity to pay a few thousand in Bitcoin and move on. However, according to an industry research survey,[1] paying the ransom only resulted in the stolen files being returned 26% of the time. Another source suggests the number is closer to 40%, but it underscores the point that there are often no easy answers to ransomware attacks once they have succeeded in locking users out.

Guidelines for Protecting Against Ransomware

In the previous article, we focused on phishing and social engineering attacks because these types of attacks commonly carry ransomware as their payload. The good news is that there are ways to help prevent these kind of attacks.

1 betanews.com

SPAM FILTERS

Spam filters can stop almost all of these emails, especially if they carry suspicious attachments, links, etc. Unfortunately, it only takes one email to get through to cause significant damage. Therefore, end-users must be vigilant as well, understanding the risks associated with clicking on unknown links and downloading attachments. It is important for everyone to understand the current cyber risks that exist and their role in helping to avoid potential breaches, and to protect against cyber threats like ransomware. Nowadays, it is more likely you will need to use your cyber safety training than fire safety or medical emergency training.

ANTIVIRUS SOFTWARE

Antivirus software also plays an important role in protecting against ransomware, since it is a type of malware. While antivirus software may not prevent the next big breach, if kept up-to-date, it can be good way to protect against more well-known forms of malware. To keep antivirus software and signatures up-to-date, it is recommended that regular computer scans be conducted.

"Nowadays, it is more likely you will need to use your cyber safety training than fire safety or medical emergency training."

VIGILANCE

Vigilance applies to information technology processes and professionals as well. Some of the largest ransomware attacks took place after the weakness in a common operating system was already identified and a security patch was made available. The most notable example of this is recent: the WannaCry ransomware worm wrought an estimated $4 billion in damages by exploiting a loophole that was patched weeks before the worm became widespread. All organizations should have a routine process for distributing and installing critical security patches. They should also have trained security professionals who understand the vulnerabilities of their system and can take proactive steps to mitigate the risks.

BACK-UP SYSTEM

Since the threat is directly related to data, one of the chief ways to mitigate ransomware risk is to design a back-up system that is largely independent from the regular network that users operate on a daily basis. The separation is needed to ensure that a ransomware attack doesn't infect the back-up as well. Installing a back-up system will not prevent a cybersecurity threat, but it is a process that can make an attack less damaging, especially if ransomware is identified quickly.

Conclusion

Ransomware attacks have become a major feature of the cyber threat landscape for institutions of all sizes. Like phishing and social engineering attacks, it is no longer a question of whether or even when, but rather of how many attacks institutions will be exposed to on a daily basis. While the most sophisticated attacks may require equally sophisticated prevention measures, the majority can be avoided with widely available technology, a well-thought-out institutional approach to networks and data protection, and end-user education.