KASPERSKY lab

BE PREPARED FOR RANSOMWARE.

This whitepaper is based on research by Nick Cavalancia of Techvangelism, and Andrey Pozhogin of Kaspersky Lab. It was originally presented in a webcast sponsored by Redmond Magazine.

THE GROWING THREAT OF RANSOMWARE

The goal of ransomware is very simple. Ransomware is designed to take away your access to potentially valuable data stored on your system. Then, it will ask for money in exchange for the release of that information. So, the question is—should you even be worried in the first place? Unfortunately, the answer is yes.

Recently, there have been stories about ransomware in the news. Data shows that, in the past two years alone, the use of ransomware has grown. The mounting threat of ransomware is going to increase. Part of this threat is due to the ease of access to the malware. This whitepaper will discuss the different types of ransomware software, and the types of organizations intent on taking advantage of this threat. It will also cover strategies and tools you can use to combat this growing threat to your business.

THE REALITY OF RANSOMWARE

The first thing to know about ransomware is that it's not being produced by one cyberhacker sitting alone in their basement. There are ransomware businesses with employees, who have healthcare plans and other corporate benefits. The main difference that separates this criminal organization from the average company is that they are in the business of ransomware. Many people assume they'll never be a target. This mindset is dangerous, because to cybercriminals, every unprotected business is a possible target.

It's important to consider that there are many different kinds of malware. Nowadays, there are many ransomware variants that exist. Some ransomware variants are encryption based, some are viral and some are based on PowerShell. Off-the-shelf software can be modified to morph into ransomware. As a result, end users can be threatened by a wide variety of ransomware software. Some of these ransomware forms can be very mature, battle-tested and tactically sophisticated.

Unlike other forms of common hacking, ransomware is not designed to slowly infiltrate an IT system to gain access to sensitive data, such as credit card numbers. That kind of common hacking takes a lot of time and patience. The cybercriminals' strategy for ransomware is different. The goal of ransomware is to get into your system, lock it down and hold it for ransom. It's opportunistic in nature for cybercriminals. Ransomware takes advantage of the vulnerabilities that IT organizations may or may not be trying to address.

THE DANGER OF INACTION

Sometimes, vulnerabilities operate like an unlocked door. A recent data breach investigation report, cited by Nick Cavalancia of Techvangelism, indicated that 99 percent of the attacks obtained access through a vulnerability that had been known for more than a year. This means that a patch was available for a year, but wasn't applied.

User awareness is another area that's often overlooked when users are guarding against ransomware. Users need to know that ransomware attacks are more sophisticated than old-fashioned phishing techniques. It's not as simple as warning users not to click on links in emails from unknown senders. Emails from ransomware companies often look legitimate.

"I'll give you a great example," Cavalancia told a recent audience. "Yesterday, I'm giving a webcast, going to talk about malware. Not 12 minutes before the webcast, I get an email from PayPal Inc. Now I know this is not from PayPal because they never put the Inc. at the end. They don't have to. It's PayPal and that's a marketing name, just PayPal. So, I already know it's going to be a piece of malware or a malicious link to some website trying to download something. The important thing is just 25 minutes earlier I had actually paid someone via PayPal. Then I got this email saying there's something wrong with your account and a transaction, it's going to raise a flag. I don't think those two are related, it's just circumstantial, but if users aren't aware, they are going to fall prey to it."

Other ransomware tactics use names from the user's contact list, so the email appears to be coming from a colleague, business associate, friend or a family member. Ransomware perpetrators can use a simple zip file and an attachment on an innocent looking email to hook end users. End users need to be warned about these email threats. Otherwise, they might not be aware of email threats that can introduce malware into a computer system and lock it down until a ransom is paid.

EVOLVING RANSOMWARE TACTICS

Ransomware is morphing quickly. Cybercriminals use ransomware to encrypt data and demand payment for an encryption key. Newer versions can enter your computer via a false email link and create a master boot record for your hard drive in 15 seconds. Your hard drive is then useless, until you pay for the decryption key.

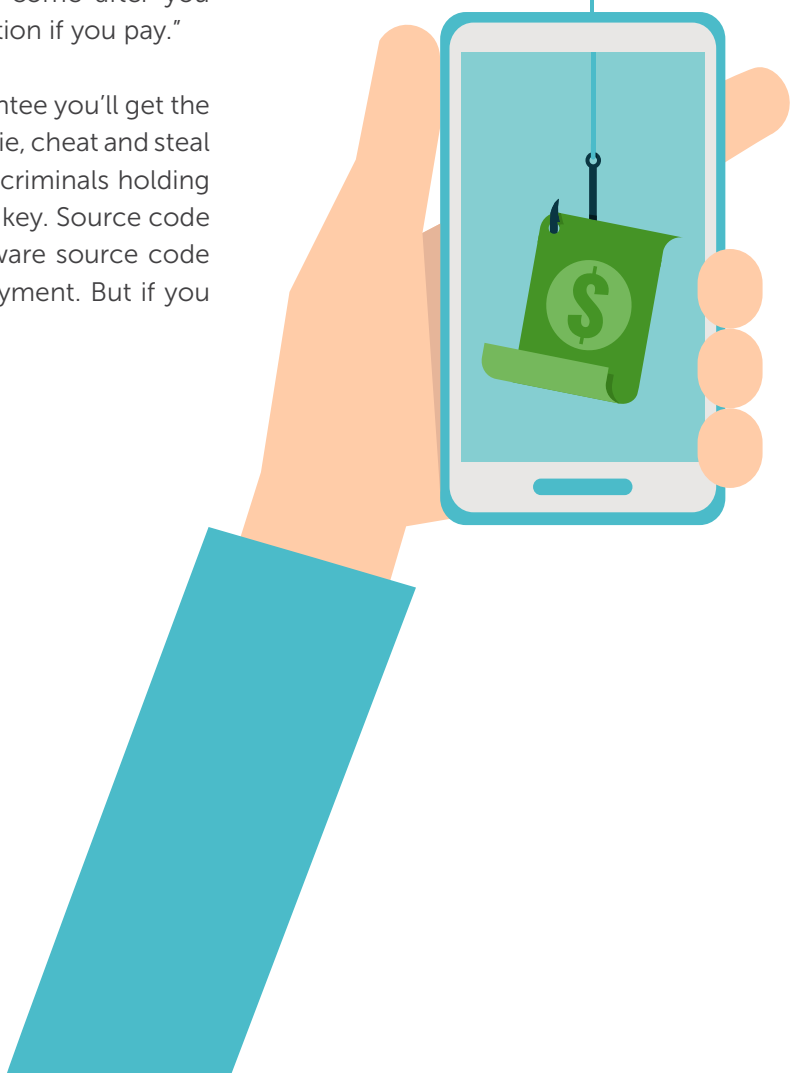
Ransomware is a growing and profitable scheme. It is easier for cybercriminals to encrypt files and hold them for ransom, rather than stealing data. Andrey Pozhogin of Kaspersky Lab estimates that every day there are five to 10 new variances in ransomware. Like normal businesses, ransomware companies put some of their profits into research and development. However, in their case, they produce more and more sinister software. That's the problem that comes with users paying the ransom for their information. Part of the ransom money is going to go into R&D to make more sophisticated ransomware. This sophisticated ransomware may be used against your company or your business partners. By paying the ransom, you are feeding the beast.

Pozhogin is frequently asked the question: to pay or not to pay?

"It's all a personal decision," he answers. "My answer is never pay. Because whatever you pay them will get reinvested to producing better, more sophisticated tools, more advanced tools. And they'll come after you again. You're putting a big target mark on your organization if you pay."

Additionally, when you pay the ransom, there's no guarantee you'll get the decryption key. You are dealing with cybercriminals who lie, cheat and steal for a living. In some cases, Pozhogin warned, the cybercriminals holding your data for ransom may not even have the decryption key. Source code for ransomware gets leaked and groups take the malware source code and repackage it with their information to make the payment. But if you pay, they have no decryption key to give you in return.

"They never had access to that and they will not be able to give you the decryption key," Pozhogin warns, "So, it's not one hundred percent that you will get your key."



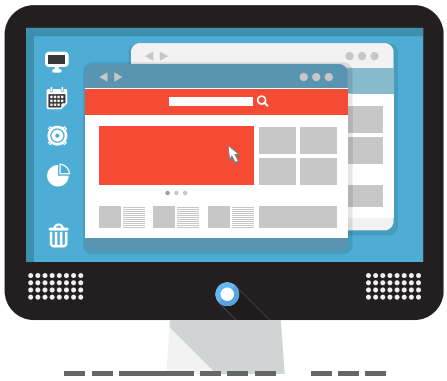
HOW RANSOMWARE SPREADS

Cryptowall is one example of a common ransomware. Cryptowall can enter a computer via a Web browser or through an email. It may look like a common Web advertisement, but when you go to the advertiser's page and click on a link, it can infect the computer. It creates encryption keys that are tied specifically to your machine. The malware navigates your machine, encrypting all your files, one by one, using a unique encryption key for every file.

Even if you work to figure out the encryption, it will only work on one file. The process of decrypting one file at a time would take an enormous amount of time and human resources. Once your system is infected and your information encrypted, it becomes impossible to recover that information. The only way you can get access to all your files is to pay the ransom for the decryption key. Unfortunately, the decryption key is only available from the ransomware company's server.

The only other solution for victims of ransomware encryption is to find a mistake that can be exploited in the perpetrators code. Anti-malware analysts have created software that tries to break into the encryption code. If they find a vulnerability they can exploit, it may open the way to recovering your information. Or, it can at least make it easier and more visible for decryption.

"For some of this malware we have been able to find some vulnerability, so you can get the decryption tool from a security company," Pozhogin said. "But unfortunately that is a very rare case."



BE AWARE OF ADMIN RIGHTS VULNERABILITY

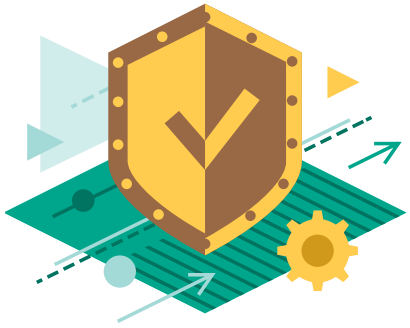
It would be bad enough if one PC in an organization was rendered useless by ransomware. Sophisticated versions of malware can create a map to file servers, so all of an organization's files may be impacted. This is another case where lapses in basic IT security can open the door to perpetrators. The file server may require administrative rights.

However, the problem is that in some companies, too many end users have admin rights. So, if their PC is logged in as an admin when it's hit with ransomware, the file servers are vulnerable. In this case, both backups and shared files may be in jeopardy, Pozhogin said. The ransomware can either delete or encrypt backup files. The latest versions of ransomware also look for shared files that are not on the computer, so it can also encrypt those shared files.

ADDRESSING THE RANSOMWARE THREAT

There is no silver bullet for combating ransomware. Protecting your system requires a multi-pronged approach with layers of security. This approach includes:

- **Secure Backups:** up-to-date and stored where they cannot be accessed from your network.
- **End user awareness:** keep users informed about the threats that may appear in emails or on the Web.
- **Sandboxing:** taking a suspicious attachment, put it in the sandbox, run it, test it and see if there is anything malicious connected through it. If there is, it is quarantined and eliminated from the email message.



KASPERSKY LAB'S 30 LAYERS OF PROTECTION

Kaspersky Lab's security software provides 30 layers of protection against ransomware. For example, the application privilege control can limit which apps can access files. The whitelist might be restricted to standard Microsoft applications. If a ransomware application makes its way into the system, it would have very low privileges. Therefore, if it attempted to encrypt documents, access would be denied.

Kaspersky Lab also offers behavioral analysis as another layer of anti-ransomware security. This software searches for and analyzes the behavior of an application to determine if it is malware. Pozhogin points out that ransomware often looks innocent at a superficial level. Ransomware does things similar to other types of software. It finds, opens, updates and deletes files just like any other program.

Behavioral analysis looks for patterns in the application's operation and will detect if it is damaging the system. It catches the ransomware in the act during the early stages of an attack. The app is then stopped and deleted. The changes it made are rolled back, so the system is restored before serious damage is done.

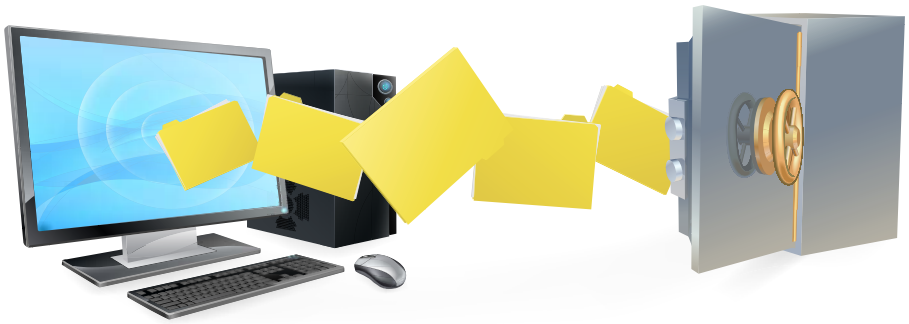
> "The computer is compromised, there is malware on the computer, but it cannot actually do any harm to you, because you took this precaution," Pozhogin explained.

GETTING SERIOUS ABOUT BACKUPS

Up-to-date backups provide insurance against ransomware. However, as malware becomes more sophisticated, IT professionals need to up their game. If backups are done right, the ransomware won't work. The encrypted files can be deleted and replaced by the backup.

The end user has to carefully follow several steps to complete this process. First, you have to think about the access to backup storage from any given entry point in your system. For example, if ransomware gets into a workstation and begins to map a drive, will it find a way to access the server where the backups are stored? It's a complex problem. You have to look at what a given workstation might access. The goal is to prevent the user machines from providing the ransomware with a map to the server where you're storing your backups. Without access to the backups, the cybercriminals will be stopped.

Asked about the importance of backups, Pozhogin says: "Backups are simply a must. There is no excuse for not having a backup. Full period."



DISASTER RECOVERY

A disaster can be as small as an end user inadvertently deleting a file or as large as an earthquake. A ransomware attack falls somewhere in between. One defense you can utilize against ransomware is to have a detailed disaster recovery plan at your disposal. If you have the ability to recover the files being held hostage, you're back in business without paying the ransom.

Creating a plan begins with setting recovery point objectives. This includes how far you want to go; if you want to go back, say, fifteen minutes, then you have to create backups in fifteen-minute increments. That will have an impact on your backup plan.

There's also the recovery time objective. How much time are you going to give yourself to recover to that point? Those two objectives have to be matched. From that point, you need to determine additional objectives, including protecting a given end user's machine. You need to have backups for the workstations in question.

It is important to be selective and thorough in your disaster recovery plan. You may not need to back up all the end users' devices if they are only running applications and not storing data. Then, your disaster recovery plan can focus on the servers with data or backups.

A GROWING THREAT REQUIRES VIGILANCE

Two things are clear when you're preparing to combat ransomware: it is a growing threat that is not going away anytime soon, and there is no silver bullet that can solve the problem completely.

To prevent your organization's data from being held hostage, you will require the multi-layer approach advocated by Kaspersky Lab. It starts with three basic precautions. First and foremost, your organization must have timely backups on a secure server that is isolated from the rest of your system. This way, it cannot be encrypted by ransomware.

Additionally, it's critical for end users to apply security patches as soon as they are available. Finally, all end users need frequent reminders of the dangers lurking in seemingly innocent emails, websites, online advertisements and promotions. End users need to know that one downloaded file could trigger a ransomware attack.

These precautions may be common sense, but they are often overlooked. As a result, it's important for all end users to have multi-layered security software which can detect, block, rollback and alert IT when a ransomware attack attempts to take place.

Kaspersky Lab
500 Unicorn Park, 3rd Floor Woburn, MA 01801 USA
Tel: 866-563-3099 | Email: corporatesales@kaspersky.com
To learn more visit us at: usa.kaspersky.com

KASPERSKY lab
THE POWER OF PROTECTION