WHITEPAPER

Redmond MAGAZINE

BUILDING DEFENSES AGAINST RANSOMWARE

Organizations and individual users at risk for WannaCry and other ransomware attacks need endpoint protection to assure that their systems will not be hijacked and held for ransom. By Peter Varhol

Computer ransomware is a fact of life today. Ransomware is malware that locks a user from gaining access to applications or data. Usually the malware will put up a screen telling the user they cannot continue using the computer, and provide them with a phone number or other communications technique to pay a monetary ransom. Often it claims that a government has detected illegal activity on the computer, giving this attack a veneer of supposed legitimacy.

Alternatively, ransomware malware may also encrypt the contents of a computer's hard disk. With modern encryption algorithms almost completely unbreakable, this attack is a foolproof way of ensuring that the user cannot recover any data from the system. Without continuous and automatic backups, data can be permanently lost.

Usually the malware comes in through social engineering, a seemingly legitimate email, or an open network port. It can take over a running system, or block access once the system is rebooted.

RANSOMWARE IS **VERY DIFFICULT** FOR INDIVIDUAL USERS AND ORGANIZATIONS **TO DELETE** FROM A COMPUTER.

Ransomware is very difficult for individual users and organizations to delete from a computer. It requires identifying how the malware infected the system, and in a very detailed way identify and remove every trace of that malware. It can take many hours simply to diagnose and repair a single computer, even if the IT professional has the requisite knowledge.

While the **WannaCry** attack and similar attacks have brought this type of problem out into the open, ransomware has existed for years, albeit sporadically. Users have battled against it, but have more often paid a fee to get continued access to their computers.

WannaCry changed the dynamic of ransomware attacks, resulting in a large-scale assault that rendered tens of thousands of computers unable to function. Without the key, decryption was out of the question. As a result,

Nicescene / Shutterstock.com

organizations and individual computer users are more aware of the effects of such malware, although they don't know how to effectively combat it.

As of today, despite popular news reports to the contrary, there is no effective "kill switch" for ransomware. Because different ransomware uses different techniques to block access, there is no single universal way to easily disable it on multiple computers. Often it requires manually editing the Windows Registry or other configuration files in very specific and detailed ways.

AS OF TODAY, DESPITE POPULAR NEWS REPORTS TO THE CONTRARY, THERE IS **NO EFFECTIVE "KILL SWITCH"** FOR RANSOMWARE.

THE RIGHT RESPONSE

Today, most major anti-malware vendors accept that ransomware is a very real threat to individuals and organizations, but typically address it only through detection and removal. Because there are a wide variety of ways to inject ransomware into a system, this approach has had only limited success at removing ransomware from traditional PCs.

Further, there are few anti-malware packages available for other computing endpoints, such as tablets, phones, and various types of medical, office and industrial equipment. Attacks against manufacturing facilities and military targets with Stuxnet in 2010 demonstrated these types of systems are vulnerable. In fact, these systems are even more vulnerable, because they are rarely built and updated with cyber security in mind.

These limitations of traditional detection and removal systems mean that organizations have to look in another direction for protection from ransomware.

WHAT RANSOMWARE MEANS TO ORGANIZATIONS

Ransomware costs organizations in two significant ways. First, it denies access to the organization's applications and data. People simply can't work if their systems are displaying a ransomware screen. The loss of productivity and the loss of data, even if temporary, can be staggering.

Further, it generally costs the organization money in paying the ransom. While the sums may not be large per computer, they can add up to a significant amount once all systems, both desktop and mobile, are factored in.

But that's not the only cost. The cost of lost business and lost productivity must also be factored in. If workers cannot use their computers, the loss of productivity is severe. In many cases, it's simply not

possible to conduct any business activities. In extreme cases, it could cause the business to fail completely unless the ransom is paid. Even if there is a backup and recovery plan in place, it could take days to get all computers and devices back online and functioning properly.

Once ransomware is installed on a computing endpoint, getting it off is a matter of detailed technical forensics, if it can be done at all, or simply paying the ransom. The ransom is usually sent to an anonymous account that can't be readily traced back to the attackers, and there is little or no chance of the ransom being returned or recovered.

HOW TO COMBAT RANSOMWARE

The ransomware problem typically manifests itself on the computing endpoints. These are the end user systems, whether computers, tablets, or phones, interacting directly with the human user. By disabling these systems, attackers have a high level of confidence that they are disrupting the work of the organization.

Ransomware can also influence server systems. For those organizations running services from the cloud, it is vital to work with the cloud provider to understand its roles and responsibilities in protecting server instances, and to work with it to minimize risk. For onsite servers, the organization assumes responsibility for their protection.

There are three approaches to preventing ransomware in the first place. The first is to be aware of the problem, and to watch for signs of malware on systems. This might be called social engineering, or education, in that users are taught to recognize attempts to gain access to their systems, whether from human contact, phishing attempts, or removable hard drives.

While social engineering is an important part of ensuring safe user interaction with endpoint devices, it is by no means the end of the story. Even the most vigilant computer user isn't always able to recognize when malware is entering a computing endpoint and infecting the system. It is useful in that it keeps end users aware and engaged in protecting their individual endpoints, but is limited in identifying and protecting against ransomware.

The second approach is detection and removal. Organizations and individuals need malware detection and elimination software that is constantly updated and backstopped by researchers and engineers with a deep understanding of the cyber threats in today's world. This requires vendor and independent organizations that are active in malware research and ways to distribute that research and actionable advice across a broad and worldwide community.

Detection and removal also play a role in protection from ransomware. While it is

very difficult to remove ransomware from a system once it is activated, detecting ransomware on a network or system, and eliminating it before it can do damage, still makes sense. Systems for which anti-malware is available should have it installed, with ongoing and up to date virus definitions enabled.

STANDARDIZED CONFIGURATION AND PATCHING

Possibly the most important method of prevention is using a standard system configuration where appropriate, and making sure that configuration is up to date through monitoring and patching. While not a very sexy activity, managing system configuration is the only ongoing activity organizations can engage in that has a positive impact on attacks such as ransomware.

Most attacks are the result of out of date system configurations. Operating system and application vendors are usually conscientious in keeping their software up to date with the latest security information. However, computer users and even system administrators vary in the attention they pay to ongoing updates and patches. Even if the IT team is receiving, testing, and deploying patches, in many cases it is in a haphazard manner necessitated by distributed offices and employees, offline employees, and multiple and disparate endpoints.

A new operating system, or a new application, is out of date by the time it's delivered, even if every effort has been made to make sure it is free of defects and security issues. New security flaws are discovered daily, and attackers attempt to exploit many of them for profit, fame, or other purposes.

POSSIBLY THE MOST IMPORTANT METHOD OF PREVENTION IS **USING A STANDARD SYSTEM CONFIGURATION** WHERE APPROPRIATE.

Vendors and custom development/DevOps teams typically continue work after an application is delivered, repairing security holes and other defects. These repairs are delivered in the form of periodic patches; for example, Microsoft has "Patch Tuesday," typically the second Tuesday of every month, to release patches created in the previous 30 days. High-priority patches and other fixes are often delivered out of cycle.

These patches can have major implications. Several of Microsoft's "patches" over the last several years have in effect installed new versions of the Windows operating system. These major patches can break critical software and make documented support procedures

obsolete. Organizational IT teams have to assess patches as they receive them, in order to understand the scope and implications of applying them to various configurations.

PATCHING SYSTEMS HAS BECOME **FAR MORE COMPLEX** IN THE ERA OF SERVERS, DESKTOPS, LAPTOPS, TABLETS, PHONES, AND HEADLESS DEVICES.

Because patches and updates are available for Windows and Mac PCs, tablets, phones, and other devices, this becomes a complex issue. Guessing which devices should be patched is not a realistic option.

THE TECHNICAL AND ADMINISTRATIVE BURDENS OF PATCHING

Each of these is significant time and effort burdens for system managers and system and network administrators. Training end users is both ongoing and time-consuming, with no guarantee that the training will be effective. Still, it is necessary to keep up with end user communications in order to make sure all available resources are working on the problem.

Patching systems has become far more complex in the era of servers, desktops, laptops, tablets, phones, and headless devices. Patches will arrive at different times, for Windows, MacOS, Android, iOS, Linux, or other operating systems. There is typically no set schedule for application patches, so those could arrive at unexpected times.

It's up to the organization to determine who gets patches, fixes, and upgrades, and when. Typically organizations test patches on their defined system configurations prior to releasing them. Often, depending on the system configuration, network access, and purpose of the system, they make the decision to patch or not to patch, to update or not to update.

Once they do, it can be a logistical and administrative nightmare without an effective way of distributing and tracking updates. If you are deploying patches to Android 6 but not Android 5 devices, for example, you have to track what the update does and what devices receive it. This type of selective patching/update gives the IT team a high level of control based on the system configuration, applications installed, purpose of system, and type of system. Products such as baramundi Management Suite can enable IT teams to easily customize patches and updates by type of system and version of software, automate the process and reduce the chance or error.

Without an automated tracking solution, there is a high probability that an organization will lose track of matching patches to endpoint device, leaving unpatched or inappropriately patched systems open to attack. Further, patching systems and

applications without regard to compatibility could result in lost application functionality or lost data.

Selective automated patching gives IT teams the flexibility to determine what computing endpoints should be patched, and what the implications are for those that are not. It also provides a record of what systems have been patched and updated, and to what level. Having this flexibility enables the IT team to immediately determine the risk of any endpoint getting infected.

With the baramundi Unified Endpoint Management Suite you can automate many of these endpoint management best practices. In short, the baramundi Management Suite is a unified endpoint management solution that helps organizations automate routine IT tasks such as security patching, compliance and system configuration management as well as assist in software and OS installs. The baramundi Management Suite modules will help IT teams implement security standards and provide inventory data across all applications within the entire organization, reducing the amount of errors and saving time with automation.

CONCLUSIONS

Organizations should never be faced with the crises of ransomware. Proper preparation ahead of time will serve to protect in most cases. Here is what organizations should do.

1. Train your employees to recognize the human and technical characteristics of attacks and to report any activity that seems out of the ordinary. The endpoint users are the first line of defense.

2. Use anti-malware software and keep the malware definitions up to date.

3. Use standard system configurations where possible, and create and execute a comprehensive patch/update strategy for those systems. Take all endpoints—computers, operating systems, tablets, phones, and other computing devices—under management.

Organizations have to practice a multi-prong approach to protection, including training, patching, and malware protection and removal. No approach works by itself; users need to practice all three. While there is no guarantee that an organization will not be hit with a WannaCry or similar ransomware attack, taking these steps will provide protection against the vast majority of attacks.

For more information
https://www.baramundi.com/us/

Peter Varhol is a technical evangelist. He has more than 20 years of experience writing technical articles, blog posts, and papers on technical practices and products. He has graduate degrees in computer science, mathematics, and psychology, and experience as an evangelist, product manager, software developer and tester, and technology journalist.