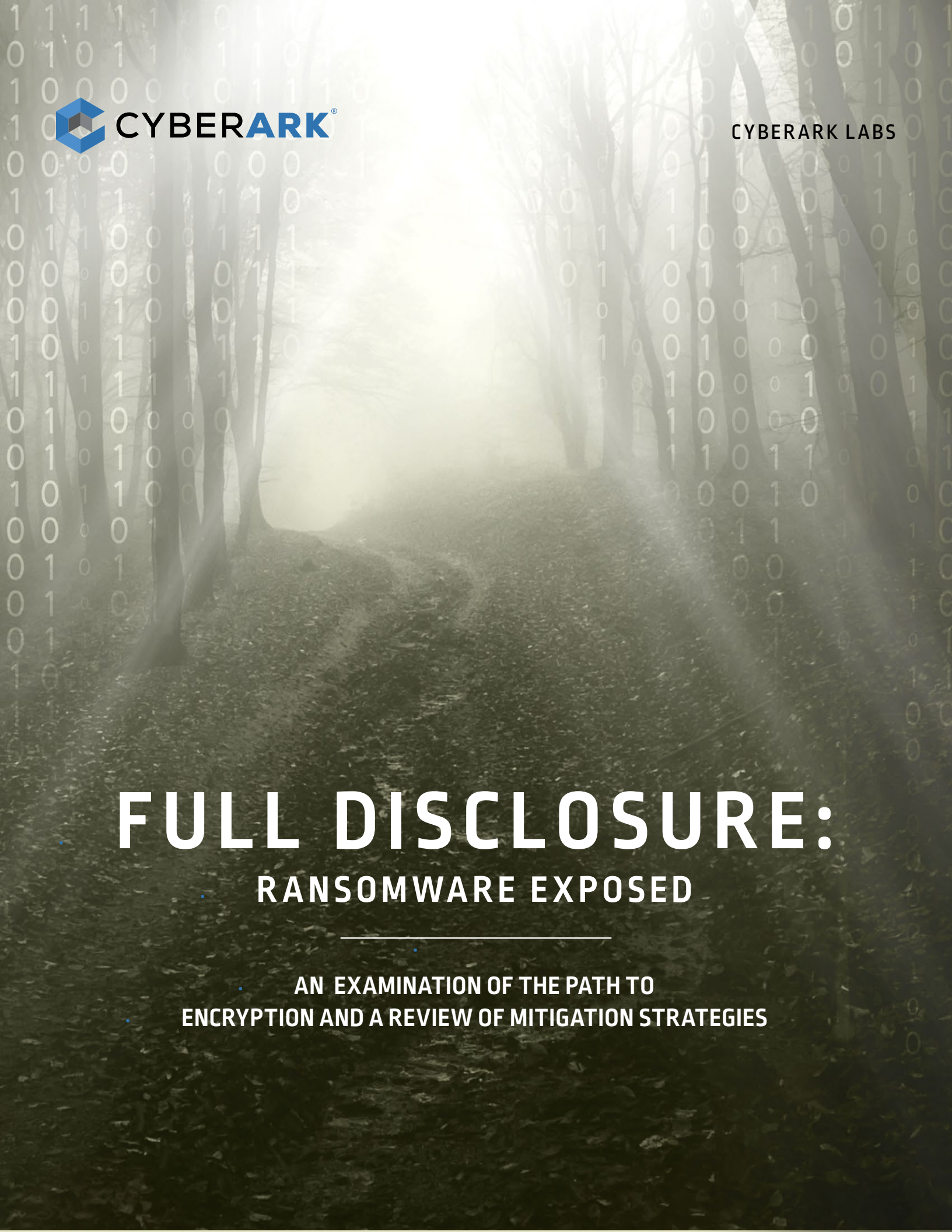

CYBERARK

CYBERARK LABS

FULL DISCLOSURE:

RANSOMWARE EXPOSED

AN EXAMINATION OF THE PATH TO
ENCRYPTION AND A REVIEW OF MITIGATION STRATEGIES

Introduction

Ransomware is one of today's most pervasive and dangerous cyberthreats. The latest ransomware attacks can quickly spread throughout a company, impairing user productivity and disrupting business for hours or even days. The 2017 WannaCry attack infected over 300,000 computers in over 150 countries, wreaking havoc on organizations like Britain's National Health Service (NHS), which was forced to close critical healthcare facilities, cancel surgeries and turn away patients for several days. Research firm Cybersecurity Ventures predicts that the annual global cost of ransomware to businesses will top $20 billion in 2021.[1]

Ransomware has become a preferred means of extortion by opportunistic attackers for two key reasons. First, many organizations fail to practice good hygiene when it comes to backup and recovery. Backups may be few and far between, meaning that once data on endpoints and servers is encrypted and held for ransom, organizations are forced to choose between losing important data forever or forking over Bitcoin to – hopefully – get their data back. Second, many organizations rely on traditional anti-virus solutions, which are often not effective in blocking ransomware. These solutions work by maintaining an inventory of known malware and blocking future executions of that malware. Because ransomware files slightly morph with each new version, and new versions are created by the minute, traditional anti-virus solutions have little realistic chance of preventing an infection.

This paper documents research conducted by CyberArk Labs to investigate ransomware and learn which potential mitigation strategies could be most effective. One of the key findings was that when local administrator rights were removed and application control policies were in place, 100 percent of ransomware samples were prevented from encrypting files.

Contents

Introduction....2
Creating a Real-Life Ransomware Lab....2
Analyzing the path to encryption....3
Reviewing Commonalities Across Ransomware Families....5
Assessing Mitigation Strategies....6
Recommendations....7
Summary....7

The true cost of a ransomware attack is much more than just the ransom payment. Ransomware attacks can impede business, damage a company's reputation and impact the bottom line. FedEx attributed a $300 million loss in earnings to the 2017 NotPetya ransomware attack.[2]

Creating a Real-Life Ransomware Lab

To conduct this research, CyberArk needed real-world samples of ransomware and a realistic lab environment in which the ransomware could be tested. The CyberArk Labs team, an in-house team that was launched to develop innovative information security solutions to combat emerging threats and compliance challenges, built a dedicated lab with real, physical machines and real files so that the ransomware could execute and spread just as it would inside a victim organization. To date, the team has tested over 3 million samples of ransomware, and they are currently testing new samples each day. These samples represent ransomware from dozens of different malware families, with the greatest number of samples coming from Cryptolocker, Petya and Locky, which are the most common and notorious families of ransomware.

Given the number of individual strands of ransomware, these 3 million+ samples represent a small subset of all ransomware. However, given the polymorphic nature of ransomware, this sample is highly representative of ransomware as a whole. Though each new individual piece of ransomware is slightly different from a previous version, all versions share common infection and execution methods. They simply have different file hashes to help evade detection.

[1] Cybersecurity Ventures, 2020
[2] https://www.reuters.com/article/us-fedex-results/cyber-attack-hurricane-weigh-on-fedex-quarterly-profit-idUSKCN1BU2RG

The goal of this research was to analyze the behavior of the tested ransomware samples to determine which strategies could be most effective in mitigating the damage caused by these attacks. As such, the team considered the benefits and challenges of the below strategies:

- Allow listing applications
- Block listing applications
- Greylisting applications
- Least privilege
- Backup and recovery

Analyzing the path to encryption

Before assessing potential mitigation strategies, the research team first sought to understand how ransomware typically behaves. Figure 1 shows the typical workflow that the majority of ransomware samples followed once it began executing. One interesting observation was that even though the various ransomware families had similar workflows, different families had different "triggers," or actions that prompted the ransomware to execute. Some families began executing immediately, some waited for an Internet connection, some waited for the mouse pointer to move and others waited for a Microsoft Office application to run.

Exposed: 4 Ransomware Families

Maze Ransomware – Part of a new trend in ransomware, samples that leak the user's files rather than just encrypt them. Attackers will threaten to publish the data if the ransom is not paid.

Coronavirus Ransomware – A ransomware that rode the wave of covid19 infections. It was delivered alongside a credential stealer (KPOT).

Snake Ransomware – An enterprise targeting ransomware written in Golang and obfuscated. After infecting a machine, Snake will commence usual ransomware behaviour, such as deleting shadow copies and backups from the system and encrypting user files. What makes it noteworthy is that it kills all processes on the system that are related to the industrial control systems and SCADA in order to be able to encrypt its files.

Snatch Ransomware – A unique ransomware that can disable many security products by performing its malicious activities running in safe mode.

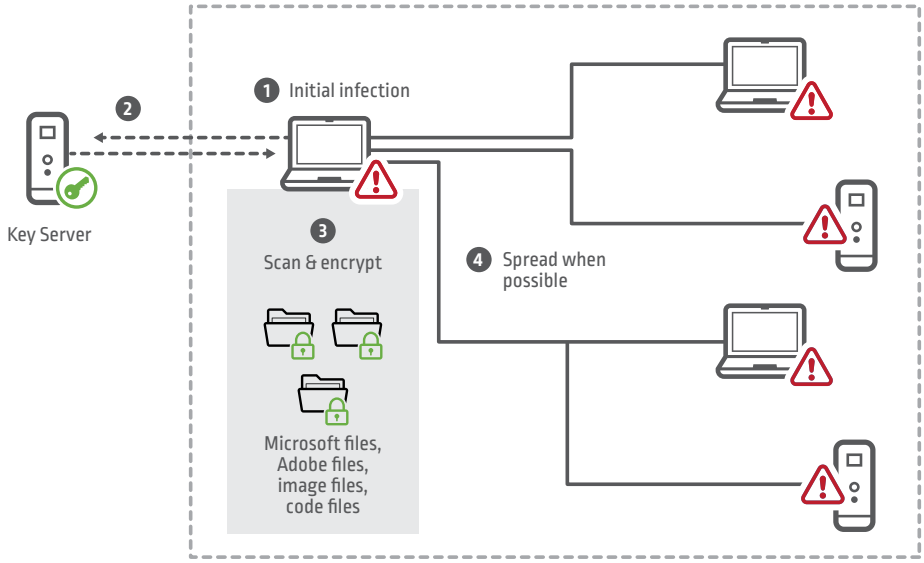

Figure 1: Ransomware Flow

Once the ransomware was triggered to execute, 90 percent of the samples analyzed first attempted to communicate back to an attacker-managed key server, which held the unique public key used to encrypt files on the machine. In 20 percent of all cases, if the connection could not be established, the ransomware would fail. Yet, a full 70 percent of ransomware samples were able to execute using a default public key, even if a unique key could not be retrieved from the key server. Notably, this approach can be less effective for the attacker, as a victim can potentially use a single default decryption key that has already been purchased to decrypt all files that were encrypted using the same key. The remaining 10 percent of samples included the unique public key within the ransomware file itself, thus eliminating the need for an outside connection. Based on this observation, the research team noted that if organizations could limit the ransomware's ability to establish an outside connection, organizations could typically either prevent the ransomware from executing or force the attackers to use a default key, thus minimizing the financial impact of the attack.

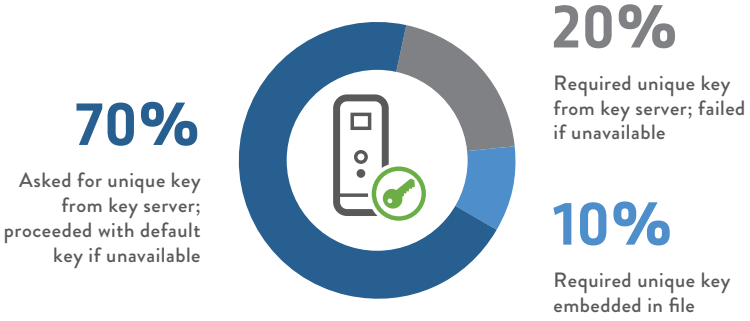

Figure 2: Percent of ransomware that was reliant upon a unique encryption key

Next, the ransomware began to scan the infected machines to locate specific files types. The ransomware samples searched for several file types and extensions, including the following:

- Microsoft Office files: .doc, .docx, .xls, .xlsx, .ppt, .pptx
- Adobe files: .pdf, .ai, .psd, .indd, .ps, .eps
- Image files: .jpeg, .png, .gif, .bmp, .tiff, .pcx, .emf, .rle, .dib
- Code files: .c, .h, .cpp, .py, .vb

Upon locating the files, the ransomware began the encryption process. Some families of ransomware methodically scanned for files, directory by directory, and encrypted them immediately upon discovery. In these cases, the entire encryption-to-notification process took just seconds to minutes. Others operated more stealthily to evade detection. Samples within these families first generated a list of all files to encrypt, and then randomly began the encryption process to stay under the radar of endpoint threat detection solutions.

While the ransomware was busy encrypting files, it simultaneously also tried to maximize the number of impacted machines. To do this, the ransomware searched the infected machine for connected drives, endpoints and servers and spread as much as possible to maximize the number of systems held for ransom. This was typically done in two ways. First, most of the ransomware samples were able to locate shared drives and network drives accessible from infected endpoints. If the user account had access to these drives, so did the ransomware. Second, the ransomware samples often scanned for connected machines and attempted to reuse user credentials to access these machines. If the login was successful, the ransomware was able to spread, thus increasing the total number of infected machines and driving up the recovery cost for the victim.

Once the encryption process was complete and the ransomware had begun its attempt to spread through the network, users were presented with a ransom notice similar to that in Figure 4. To receive the key needed to decrypt the impacted files, users were required to submit payment – the ransom – to the attackers. Payment was typically demanded in Bitcoin, and for Bitcoin novices, some attackers went so far as to set up "help desks" to help victims purchase Bitcoin and complete the funds transfer.

Figure 3: Ransomware notice presented to users infected by CTB-Locker.

Reviewing Commonalities Across Ransomware Families

While the samples within different families of ransomware had slightly different characteristics, they all had three things in common:

- They were easily able to infect machines
- Once the infection occurred, the vast majority of files were encrypted successfully
- The ransomware files themselves could easily be removed

Infection

One of the major takeaways was that traditional anti-virus software was often not effective in stopping the ransomware. This was the case because traditional anti-virus software relies on known block-lists, meaning that a specific piece of malware must already be known (ie: must have already infected at least one machine) to be added to a block-list. Due to the polymorphic nature of most families of ransomware, no two samples were exactly the same. Instead, with each new target victim, the attackers will rapidly create a new, slightly morphed, piece of malware to stay ahead of block-listing technologies and evade detection.

This ease of infection led the research team to conclude that even though the use of anti-virus is good security hygiene, it's not effective against polymorphic malware. To prevent ransomware from infecting machines, organizations must take a more proactive approach to endpoint and server security, such as restricting or blocking certain applications.

Encryption

A second major takeaway is that while many strains of modern malware require local administrator rights to properly execute, not all ransomware strains require these rights.

This led the research team to conclude that while organizations should remove local administrator rights, they should also proactively control applications to prevent file encryption. Specifically, the CyberArk Labs team demonstrated that when read, write and modify file privileges were denied from unknown applications and local administrator rights were also removed, file encryption caused by ransomware was prevented in 100 percent of the cases.

Removal

Unlike some strains of sophisticated malware that can be difficult to locate and remove, the ransomware samples analyzed were easy to locate and remove once they were detected. This means that victim organizations who proactively backup files can dramatically reduce the impact of ransomware and avoid having to make a choice between paying a costly ransom or losing data forever. Instead, once the files are encrypted, victim organizations can locate the ransomware files on infected machines, remove them from the system and then restore the affected files from backup.

As a result, proactive backup of files on endpoints and servers can help mitigate damage caused by ransomware. Frequent backups of valuable files can make it much easier to recover from ransomware attacks and lessen the impact of damage caused by this strain of malware.

Assessing Mitigation Strategies

Before selecting one or more techniques to mitigate the risks associated with ransomware, organizations should consider the benefits and challenges of each option. This section describes the mitigation strategies assessed and tested by the CyberArk Labs team and pros and cons of each.

Research demonstrated that restricting applications coupled with the removal of local administrator rights was 100 percent effective in preventing ransomware from encrypting files.

Allow Listing Applications

By nature, allow listing applications is 100 percent effective in blocking ransomware, as it blocks all applications that are not explicitly trusted from penetrating the environment. While this mitigation strategy is highly effective in preventing ransomware attacks, it is extremely difficult to do well in practice. To effectively allow list applications, IT teams must know exactly what applications and versions are needed by each user and system in the organization, and each individual application version must be explicitly allow listed by the IT team. Allow listing can be an optimal approach for servers, which are typically static, but on dynamic user endpoints, which often require a wide variety of business applications, this approach can bring user productivity to a halt.

Block Listing Applications

By block listing applications, organizations can prevent known malware (ie: malware that has already infected at least one machine) from executing in their environment. While this is helpful in detecting and blocking older versions of opportunistic malware, it is highly ineffective in protecting against ransomware. Thousands of new ransomware samples are released into the wild each day, and traditional application blocks simply cannot keep up.[3] As a result, the research team determined that even though blocking applications is a general best practice, it is not effective in detecting or preventing ransomware.

Greylisting Applications

By greylisting applications, organizations can prevent known, blocked malware from executing in their environments as well as limit the permissions available to all applications that are not explicitly trusted. This approach offers more flexibility than allow listing applications and can be used to prevent unknown applications from doing things such as accessing the Internet and reading, writing or modifying files. Even better, by restricting read, write, and modify file permissions, the ransomware was unable to gain the permissions needed to access and encrypt files. When the CyberArk Labs team tested this approach with the ransomware samples, it was 99.97 percent effective in preventing file encryption in cases when the infected user had local administrator rights, and it was 100 percent effective in preventing file encryption in cases when the user did not have local administrator rights.

Least privilege

This step is not just simply good hygiene; it is also included as one of Microsoft's "Ten Immutable Laws of Security." Interestingly, while the removal of local administrator rights alone is often effective in preventing damage from most modern malware, the CyberArk Labs team noted that this step alone was only effective in preventing damage from 10 percent of the ransomware samples analyzed. Based on this observation, the CyberArk Labs team reiterated the importance of both removing local administrator rights and controlling applications. Notably, before entirely removing local administrator privileges from users, organizations should assess their environment to understand potential productivity challenges that may result from this move. Some legitimate business applications and tasks require administrator privileges to function properly, and the immediate removal of these permissions without exception policies for needed tasks, could potentially halt business productivity.

[3] http://www.businessinsider.com/fighting-ransomware-with-antivirus-2016-1

Backup and recovery

Data backup should be a part of any organization's disaster recovery strategy, and automated backup helps to ensure that backup files are comprehensive and up-to-date. File backup cannot prevent ransomware attacks, but it can significantly lessen the damage caused by these attacks. Instead of paying a ransom to retrieve encrypted data, organizations can simply restore impacted files from the most recent backup. Organizations should consider the cost of backup and storage against the costs of data loss, remediation and recovery, and prioritize files or assets to backup based on the organization's unique risk tolerance and budget.

Recommendations

Based on the research conducted in the CyberArk Lab, the team recommends that organizations apply the following mitigation techniques to mitigate risks associated with ransomware without negatively impacting business productivity.

- Restrict applications on user endpoints to prevent unknown applications, such as new ransomware instances, from accessing the Internet and gaining the read, write and modify permissions needed to encrypt files.
- Allow certain applications on servers to maximize the security of these assets.
- Remove local administrator rights from standard user accounts to reduce the attack surface.
- Automatically elevate account privileges for specific authorized tasks to keep users productive without providing unnecessary privileges.
- Use anti-virus tools to protect against common and known malware.
- Frequently and automatically backup data from endpoints and servers to allow for effective disaster recovery.

For the best results, CyberArk Labs recommends that organizations assess their environments to locate all endpoints and servers that contain sensitive or valuable files. After allowing applications on static servers, organizations should determine what files types on endpoints contain the most important information (ex: .xlsx, .pptx, .pdf, etc). Such an assessment can help organizations understand what file types are most valuable, which in turn can help organizations create effective greylisting policies to protect these file types from unknown applications.

Summary

After analyzing and testing more than 3 million samples of ransomware, CyberArk Labs has demonstrated that an alternative approach to proactive security can be effective in protecting against ransomware and can thus dramatically minimize the impact of this type of attack.

In addition to removing administrator rights from standard user accounts and regularly backing up data, which are both considered standard IT best practices, organizations should also consider application control on endpoints. Organizations can prevent unknown applications, which are neither explicitly trusted nor blocked, from accessing the Internet and gaining read, write and modify permissions on defined file types. This enables organizations to focus on protecting access to the target of malicious applications – the files – instead of solely relying on the ability to detect polymorphic malware, which is incredibly difficult to do in practice. When tested in the CyberArk Lab, the combination of application restricting and the removal of local administrator rights proved to be 100 percent effective in preventing ransomware from gaining the permissions necessary to access protected file types and complete the encryption process.