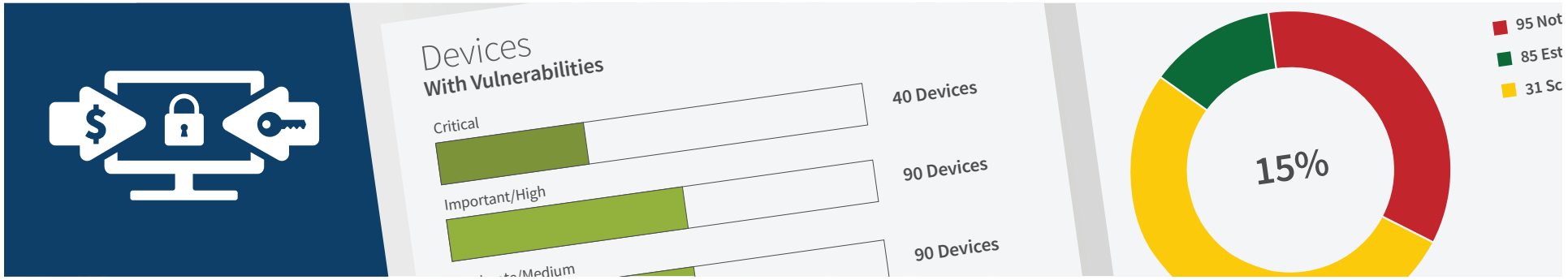
ivanti

9 Steps to Protect Against Ransomware



White Paper

Contents

Introduction

"Just pay the ransom." So said an FBI official during the Cyber Security Summit 2015 in Boston.[1] However, since then, the FBI has published an official document that warns against ransomware and provides a list of best practices on how to fight it. Oh, and the new document specifically says, "The FBI does not support paying a ransom to the adversary."

We now know that most ransomware is spread using phishing or spam emails. Just recently, users in the US House of Representatives fell victim to a ransomware campaign reportedly designed to trick users into opening an attachment sent to their Yahoo Mail accounts. [2]

Increasing end-user education and awareness are always good ideas, but it's important to understand that the "bad guys" are professionals. They use many professional marketing and social engineering tools to improve their abilities to trick users into opening fraudulent emails and attachments. You should therefore assume that even the most educated and aware user may be tricked. In fact, the latest Verizon data breach report found that 23 percent of recipients are opening phishing messages, and 11 percent click on fraudulent attachments.[3] So the odds are against you.

This white paper from Ivanti reviews the FBI's recommendations, and explains nine steps you put in practice to implement them.

Prevention

A “detect and respond” model for ransomware provides little value because once the ransomware is running, it’s too late. That’s why prevention is critical to combatting such malware. The FBI suggests you implement the nine prevention steps or methods below, discussed in more detail in the following pages:

1. Patch the critical operating systems and applications
2. Ensure that antivirus software is up-to-date and that regular scans are scheduled
3. Manage the use of privileged accounts
4. Implement access control that focuses on the data
5. Define, implement, and enforce software rules
6. Disable macros from Microsoft Office files
7. Implement applications whitelisting
8. Restrict users to virtualized or containerized environments
9. Back up critical files frequently

1 Patch the critical operating systems and applications

For most organizations, patching should be the first or second line of defense against any attack. This holds true for ransomware as well.

PATCHING SHOULD BE THE FIRST LINE OF DEFENSE.

DON'T FALL VICTIM TO
RANSOMWARE

ALREADY DISCOVERED

A month ago, a flaw in Adobe Flash was used by the Locky and Cerber ransomware attacks to distribute themselves to victim workstations.[4] You can prevent many such attacks by ensuring that the OS and required third-party applications on each client system are up-to-date. You should also make a special effort to ensure that all critical patches and updates for applications such as Adobe Flash, Java, Web browsers, and Microsoft Office are kept current. What's more, you should prioritize patch and update deployments based on business needs and policies—and you should execute those deployments in ways that don't disrupt user or business operations.

Many organizations fear that comprehensive, timely, and consistent patching is too complex to execute and maintain, or that it may break critical business applications. However, using the latest patch management tools to scan for missing patches and deploy them to workstations or servers is a straightforward task—even in the most complicated environments.

Ivanti has tons of experience delivering complete, flexible, end-to-end patch management solutions. Our experts can demo how you can employ Ivanti solutions efficiently to automate patch management—and to deploy those critical patches with minimal to no disruption to your business or your users.

2 Ensure that antivirus software is up-to-date and that regular scans are scheduled

If patching is your first line of defense, then antivirus (AV) should be the next one. Security researchers know by now that most ransomware attacks cannot be stopped by traditional, signature-based AV solutions. However, you don't want to fall victim to malware threats that are already identified and tagged by your AV vendor.

Ensuring that your virus definition database is always up to date on all your workstations is the most important element of an effective AV strategy. Ivanti security management software can automate this process for you. Our solution can distribute the latest virus definition file to all your endpoints in any size of environment very efficiently bandwidth-wise. Since we support

most AV vendors, our solution will most likely work with your AV vendor. If you choose to use our AV solution, which is based on the Kaspersky Lab antivirus engine, we will also automate scanning and AV management from one console.

3 Manage the use of privileged accounts

Minimizing privileges is an important tactic to protect against many types of malware, including ransomware. For example, a recently discovered ransomware attack called "Petya" requires administrator privileges to run, and will do nothing if the user doesn't grant those privileges. [5]

Removing administrator rights is easy, but balancing privileged access, user productivity, and enterprise security isn't. Thus the need for privilege management solutions.

The Ivanti security team advocates the importance of privilege management, which is one of the reasons why Ivanti acquired Ivanti, providers of a proven solution in this space (among other great tools). Ivanti Privilege Management helps you define policies that limit administrative privileges to those that authorized users need to do their work.

However, one thing to consider when protecting against ransomware is that many ransomware attacks are just executables that users are tricked into running. Once executed, those ransomware instances run inside the current user space, and don't require any administrator privileges to do their damage. An updated version of the Petya ransomware attack (mentioned above) has a fallback mechanism that allows it to encrypt files without the need for administrator privileges.

4 Implement access control that focuses on the data

An effective access control solution can help you protect against ransomware. However, if the solution focuses primarily or exclusively on user access rights, it will likely prove less than effective.

MINIMIZING PRIVILEGES IS AN IMPORTANT TACTIC TO PROTECT AGAINST SPECIFIC TYPES OF RANSOMWARE.

Access control can be highly beneficial for protecting files located in shared drives. That's because some users will likely always have legitimate rights to access and modify at least some files on every shared drive. After all, most of those files are document files created by legitimate users. This means that a ransomware attack that successfully infects the system of a user with legitimate access rights can encrypt and hold hostage all of the files on all connected, shared drives and folders.

Ivanti security solutions offer a different type of access control—one that focuses on the data you want to protect versus the rights of those users. Ivanti software lets you define rules that prevent any program (other than those you specify) to modify critical or sensitive documents or files. For example, a rule that allows only Microsoft Word to modify .doc and .docx files will deny any attempt from successfully installed ransomware to encrypt any such files.

Adding similar rules to protect all Microsoft Office, Adobe PDF, and other frequently used and shared file types provides the best defense against most ransomware attacks. With such rules in place, even if ransomware gets onto a user's system, it won't be able to encrypt protected files. Users will retain access to those files and be able to continue working with minimal to no disruption, and with no need to revert to older, potentially out-of-date backup versions.

(Note that some ransomware attempts to appear as legitimate software and add itself to system startup routines. The Ivanti solution prevents it from doing so.)

Compared to traditional access control, the Ivanti method of focusing on data protection is a more effective defense against ransomware. It relies on understanding the behavior of ransomware, and does not require creation and management of user-specific (and ever-changing) rules. It is therefore also easier to implement and maintain than access control based on user rights management.

RANSOMWARE LEVERAGES MICROSOFT OFFICE MACROS. USE IVANTI SECURITY SUITE TO DISABLE THEM.

5 Define, implement, and enforce software rules

Ivanti software also makes it easy to define, implement, and enforce rules that govern how other software behaves. Rules can restrict the ability of designated software to execute, or to create, modify, or read any file, or files located in specific folders, including the temporary folders used by browsers and other programs. Those rules can be applied globally, or to specific users or groups.

However, before implementing such rules, it is important to consider the user experience degradation such rules can introduce. For example, when installing new or updated software, legitimate users are sometimes required to decompress ("unzip") or execute files directly from their browsers. Users may also rely upon the ability to create or invoke macros to do their jobs. Software restriction rules may block these otherwise legitimate activities.

6 Disable macros from Microsoft Office files

Disabling macros from Office files will block many types of malware, including ransomware. For example, Locky is a relatively new crypto-ransomware that spreads primarily via spam with attachments. It entices users to enable macros in Word documents that download the malware onto machines.

Ivanti Security Suite enables IT administrators to set a policy to disable macros. Deploying this policy to workers that don't require the use of macros will effectively block these types of ransomware from running.

Other considerations

The FBI has issued additional recommendations intended to boost protection of your environment. They are meant to help you defend against multiple types of malware and other attacks, but if used correctly, they will also protect against ransomware.

7 Implement applications whitelisting

This solution effectively eliminates the ability of any ransomware to run, since no ransomware is trusted. It ensures that only known applications designated as trusted can run on any endpoint. The biggest challenges to the success of whitelisting are creating the initial list of trusted applications, and keeping that list accurate, complete, and current.

Ivanti solutions, including Ivanti Application Management, offer multiple options for comprehensive, flexible, effective, straightforward whitelisting. And Ivanti makes it easy to create and maintain your whitelists. For example, the Ivanti solution will "discover" automatically all applications running on "clean" system(s) and will validate application integrity against its own application reputation database. Adding rules to trust applications based on their owners (e.g. authorized admins) and vendors (e.g. Microsoft, Oracle) further reduces the amount of configuration required to create those trusted application lists.

8 Restrict users to virtualized or containerized environments

In most cases, ransomware is distributed as an email attachment. Restricting users to virtualized or containerized environments will ensure that any ransomware that gains access to a user's system will do no harm to the user's primary work environment.

Bufferzone, a Ivanti ONE partner, offers an elegant threat-isolation solution that integrates with Ivanti security solutions. You can find more information about Bufferzone at http://www.Ivanti.com/partners/Ivanti-one/bufferzone/.

9 Back up critical files frequently

The FBI paper recommends using timely, frequent backups of critical files as a business continuity consideration. If done right, backups will save the day if you're attacked by ransomware. However, you won't need to rely on backups alone to combat ransomware if you implement the defenses recommended in this eBook, especially the access control features offered by Ivanti.

PREVENT RANSOMWARE FROM RUNNING IN THE FIRST PLACE

DYNAMICALLY WHITELIST YOUR APPS

ivanti

Ransomware incidents are on the rise. Fight back!

With solutions from Ivanti, you can manage and safeguard any endpoint, protect against threats new and old, and advance toward a new level of protection.

TO SCHEDULE A DEMO OF THE
IVANTI SECURITY SOLUTIONS,
PLEASE CALL OUR TEAM AT (800) 982-2130

References

1. http://www.businessinsider.com/fbi-recommends-paying-ransom-for-infected-computer-2015-10

2. http://www.computerworld.com/article/3068623/security/ransomware-attacks-on-house-of-representatives-gets-yahoo-mail-blocked.html

3. http://www.verizonenterprise.com/verizon-insights-lab/dbir/2016/

4. https://threatpost.com/latest-flash-zero-day-being-used-to-push-ransomware/117248/

5. https://blog.malwarebytes.org/threat-analysis/2016/04/petya-ransomware/.