MICRO FOCUS

Flash Point Paper

Security

Ransomware: Preventing Hostage Data

Cybercriminals take advantage of a vulnerability in your environment to infest your systems with malware that encrypts your vital business data so it's unusable until you pay them to decrypt it. In some cases, they even steal the data and threaten to release it to your competitors or sell it to the highest bidder.

The WannaCry and NotPetya ransomware attacks have been two of the most devastating incidents in history. WannaCry cost businesses between $4 billion and $8 billion. Losses due to NotPetya were estimated at more than $10 billion. What makes ransomware attacks so dangerously effective is that they are self-propagating. They detect and leverage vulnerabilities in your network and software to gain escalating access to other network devices and data across your environment until the intruder cripples and holds hostage your entire enterprise. As frightening as the prospects of a ransomware attack can be, the reality is that implementing a few simple best practices is typically all that is needed to keep you safe from such attacks.

Prevention Is the Best Defense

Perhaps the biggest irony of most ransomware incidents is that they easily could have been avoided. Ransomware attackers usually exploit well-known vulnerabilities that if victims take known best-practice steps to correct, the attempts to infiltrate their environments will simply fail. Those best practice steps involve keeping all their systems and software patched with all the latest security updates. For example, a month before the WannaCry and NotPetya attacks began to wreak havoc, Microsoft had released a patch to repair the vulnerability that each of those attacks exploited. If the victim

organizations had simply patched their systems, they would have been impregnable to those attacks.

The big question then becomes, why didn't those organizations patch their systems? The answer is that patching every system and piece of software in a timely manner for any mid-size to large environment can be a massively complex undertaking if the organization doesn't have the right tools. The right tools consist of an auto-discovery solution that can detect and inventory every laptop, desktop, and server connected to your network so you know the vulnerability status of everything that might need to be patched. Next, you need a patch management solution that can quickly and automatically update each of those endpoints with the appropriate and most recent security patches. That includes also being able to report back to you the success or failure of

Questions to Ask Yourself About Ransomware

- *How do you prevent ransomware attacks at the moment?*
- *How do you know when users bring unauthorized software or hardware into your work environment?*
- *How often do you have to make decisions about what to patch and what not to patch?*
- *How user-proof is your backup protocol?*
- *How do you store backups? How do you restore it?*

those patch efforts, so you can be certain that every endpoint has been successfully patched and protected.

Instant, Automatic Intrusion Mitigation

What do you do if somehow you still become victim to an attack? First of all, your patch management system needs to continue to automatically scan your environment for potential threats and remediate any that are discovered to further reduce the possibility of an attack ever happening. If a new vulnerability emerges, your patch management system should be able to immediately alert you of any devices or apps that are vulnerable and automatically patch them to block the threat or stop it from propagating if it has already infected your system. Of course, having a strong firewall, application controls, and security policies enforced on each of your endpoints will further increase your ability to block such attacks. And for you to have the visibility you need to ensure you really are vulnerability free, you need centralized management that makes it easy to see the vulnerability and security status of each of your connected endpoints.

Secure Continuous Backups

Even with the protection of automated patching and hardened security policies, you need additional lines of defense to guarantee you never lose your valuable data. That's why the final best practice includes employing secure, continuous backups of all your endpoints. So, even if, in spite of all your protection efforts, cybercriminals somehow still manage to hold your data hostage, you can easily recover using your backups. And don't think that if you get caught without a data backup that you'll be able to get your data back by paying the cybercriminals their ransom. Studies indicate that when ransomware victims have paid a ransom, only 19% of them have actually been able to get their data back.* Sometimes the cybercriminals simply don't release it. Other times the malware they use to encrypt the data corrupts the data so it's not recoverable, whether or not a ransom has been paid.

Simplifying Ransomware Protection

To put you at ease in the face of potential ransomware attacks, Micro Focus offers the solutions that make it simple to employ the best practice steps needed to keep your data and environment safe. Micro Focus® ZENworks® Patch Management automates the process of discovering and monitoring the patch state of all your Windows laptops, desktops, and servers, and makes sure they're always updated with the latest patches. It also makes sure your antivirus and antimalware solutions' definition files stay current to further reduce the risk of infection. It stays on the lookout for exploitable vulnerabilities as they emerge and immediately patches them to prevent infection and network propagation.

To further keep ransomware attacks at bay, Micro Focus ZENworks Endpoint Security Management gives you fine-grained, policy-based control over all your Windows laptops, desktops, and servers, including advanced firewall protection, application controls, wireless security, port controls, and robust storage device controls. Micro Focus Connected MX gives you a cloud-based continuous backup and recovery service with policy-driven protection that makes sure the data on your laptops and desktops can always be recovered, whether it's from an attack, system failure, or natural disaster.

For more information on how Micro Focus can keep your endpoint data safe from ransomware and other threats, visit: **www.microfocus.com/products/zenworks/**.

———————

** CyberEdge Group, "2018 Cyberthreat Defense Report"*

Contact us at:
www.microfocus.com

Like what you read? Share it.