Ransomware Looks to Blackmail Enterprises

- Posted by Patrick Oliver Graf on March 20, 2014 at 9:28am
- View Blog

When most people think of threats to their computer systems and networks, the usual suspects come to mind -- malware and keystroke loggers that are meant to steal passwords to remotely access corporate networks and online accounts. Then, of course, there are the viruses designed simply for the sake of destruction, rendering one's computer little more than an expensive, oversized paperweight.

But perhaps the most dangerous threat of all is one that, while it has been around for a long time, is only now coming into prominence. It's called "ransomware," and if it sounds scary, that's because it is. CryptoLocker is a well-known example circulating today. Ransomware is an accurate moniker, as this breed of malware encrypts the contents of your computer and then its creator offers to provide the decryption key -- for a nominal fee, of course.

Thinking of booting up in safe mode and deleting the ransomware from your computer? That's all well and good, except your files are still encrypted and you still don't have the key to unlock them.

Ransomware Threatens Enterprises on Multiple Levels

Encrypting your most important files isn't the only method that cyber criminals employ, however. They can also place files on your computer that put you in an awkward position. Common practice includes downloading indecent materials on a computer that one uses for work. Employees fearful of losing their jobs for having illicit content found on their devices are that much more likely to pay the "ransom."

And if it works against one employee, cyber criminals have good reason to suspect that others in the same organization will acquiesce, meaning the organization's entire workforce has now become a target. Not to mention the fact that if machines used to access the corporate network are being infiltrated by the likes of CryptoLocker, the next logical step is for the cyber scoundrels to target the company directly, holding critical files on the network for ransom, and likely at a much higher ransom than the individual employees were "invited" to pay. Even more worrisome is that beyond individual files, the network itself could be held for ransom, if a hacker gained the necessary read and write privileges by infiltrating a network administrator's device. Cybercrime goes where the money is, and eventually, all roads lead to the enterprise.

The Link Between Ransomware and BYOD

So why is ransomware gaining so much momentum among cyber criminals? Well, its rise to prominence has paralleled the explosion in popularity of the bring-your-own-device (BYOD) movement. The number of personally owned mobile devices connecting to corporate networks and being granted access to critical files is at an all-time high. It's what you would call a "target-rich environment," where hackers and their ilk have no shortage of potential victims to choose from.

What makes for an even scarier scenario -- as if there wasn't enough already -- is that an individual looking to deploy CryptoLocker or similar machinations doesn't even have to be an expert in encryption algorithms. As a recent CSO article points out, ransomware toolkits can be developed and sold to those willing to pay the price tag. This means that anyone with a few bucks and ill intent, regardless of their hacking know-how, could start targeting people and companies.

Defense in Depth vs. Ransomware

As the threat landscape continues to evolve, enterprises need to adjust their approach to security in kind. Remote access and BYOD have become too ingrained in the working world to disappear now. The top-level talent that every company wants to attract will only sign on the dotted line if they are afforded what were once considered luxuries, but are now simply expected.

The answer is for enterprises to implement a comprehensive, defense in depth information security framework that allows for BYOD and remote access without compromising the corporate network. Because IT staff can't monitor everything employees do on their devices, enterprises should invest in interoperable solutions that can work together to prevent threats like CryptoLocker. The first line of defense would be to require best-of-breed anti-virus and anti-malware solutions on employee devices to protect them against a range of malicious software. Next, those solutions could work in tandem with other network and security solutions such as firewalls blocking access to known CryptoLocker servers, Intrusion Prevention Systems which can block the malware from interacting with the remote command-and-control server and a robust

VPN solution that offers central management capabilities to monitor endpoint devices and ensure anti-virus tools are up-to-date.

With a centrally managed VPN, users with old versions are sent into a digital quarantine zone until their software has been updated, ensuring that every device accessing the corporate network is properly secured. Central management also means that IT administrators can roll out security and remote access policy updates across the whole company than working their way manually through one device at a time.

With a defense-in-depth strategy that includes network and security components working together to prevent and mitigate threats, enterprises will be well on their way to defending against the rapidly expanding threat vector known as ransomware.

Patrick Oliver Graf is General Manager, Americas of remote access security vendor NCP engineering.

This post originally appeared on VPN Haus.

Views: 187

Tags: BYOD, CryptoLocker, VPN, encryption, malware, ransomware, security

Favorite
0 members favorited this

Share Twitter g+1

Like 0

- < Previous Post

Comment

You need to be a member of Innovation Insights to add comments!

Join Innovation Insights

Welcome to
Innovation Insights

Sign Up
or Sign In

Members

-