Addressing Ransomware Attacks

First, what exactly are ransomware attacks and what's the motivation behind them? Motivation seems easy enough to decipher – it's monetary greed. In every instance I'd read about, there's always some monetary demand to decipher their sites, generally in BitCoin payments (the preferred currency of cybercriminals everywhere).

One definition is, "Ransomware is a subset of malware in which the data on a victim's computer is locked, typically by encryption, and payment is demanded before the ransomed data is decrypted and access returned to the victim."

The most common source of ransomware attacks

Malicious email attachments are high on our list as a common source of ransomware attacks, followed by software applications (and external storage devices) that have been infected, and what we see more often than not – websites that have been compromised. RDP (remote desktop protocol) is also used simply because it doesn't rely on user interaction.

Can't log into your site?

In some instances, cybercriminals use a lockscreen variant whereby they alter their victim's logins.

Has your data been kidnapped?

Here your data files are encrypted, not necessarily only to the infected device, but to other network devices that are connected.

Early attacks could be reverse engineered, but …

You guessed it. While early attacks could be reverse engineered relatively easily, cybercriminals have developed enhanced versions that utilize exceptionally strong public key encryption.

Previous versions of ransomware attacks

When discussing public key encryption, one of the earliest versions of ransomware that used this was a Trojan horse by the name of Cryptolocker. As usual, the attackers demanded payment via bitcoin, and at the time, because of the RSA cryptology used, this was highly effective malware. Fortunately, the encryption keys for this variant were discovered leading to the development of an online tool that facilitated recovery, effectively defanging the malware.

Ransomwares attacks

A recent attack, defined as WannaCry was disseminated in the Spring of 2017 that infected over 250,000 systems around the world. This malware utilized asymmetric encryption, making recovery difficult. Why? Using this variant, victims faced increasingly difficult recovery paths attempting to discover the private and undistributed key that was necessary for decryption.

Once again, payments via bitcoin were demanded, simply because they couldn’t be traced to the recipients. The net estimated damage from this attack alone may have exceeded $1 billion dollars.

Does paying ransomware demands guarantee you’ll get your files back?

Unfortunately, paying ransomware demands does NOT guarantee that you’ll get your files back. Approximately 20 percent of firms or organizations that pay these fees do NOT get their

data back.

The average amount of ransom demanded currently exceeds $1000

The estimated percentage of business executives that actually paid these demands ranges from 3 to 70 percent, so those aren’t exactly rocket science numbers, although across the board, fewer percentages of US companies tend to pay.

Are internet of things (IoT) vulnerable to ransomware attacks?

Unfortunately, yes, IoT is vulnerable, so it’s imperative that you take precautions. We’re talking about smart thermostats, refrigerators and security systems, as well as many other devices.

Who actually uses ransomware?

Unbelievably, ransomware kits on currently available on the dark web for less money than you might imagine. And you don’t have to be a computer geek to purchase and implement an attack. In some scenarios, the seller of the ransomware malware actually collects the ransomware payments, takes their percentage of the loot and distributes the remaining amount to the purchaser.

How would you know you were attacked?

Of course, there are the more obvious signs of attack like receiving a pop up message telling you that you’ve been attacked. Of course, the approach these cybercriminals take to extort digital currency for their misdeeds vary. Some victims are given deadlines to pay and some are simply threatened by promising to expose confidential information or data.

The key to minimizing ransomware attacks is prevention

First and foremost, backup your data in multiple locations, online and offline remotely and don’t click on suspicious attachments in emails, especially from strangers.

Brought to you by ProlimeHost

We've been in the web hosting industry for over a decade, helping hundreds of clients succeed in what they do best and that's running their business. We specialize in Virtual Private Servers (VPS) and dedicated servers, with data centers in Los Angeles, Denver & Singapore.

VPS Services: Lightning Fast SSD Virtual Servers

Our Virtual Private Servers all feature high performance Xeon processors and SSD storage in a RAID10 configuration to optimize your server's performance, which dramatically enhances visitor experiences on your site.

That speed is backed by unparalleled 24/7 support, featuring both outstanding response AND resolution times to maximize your uptime.

Now is the time to join the ProlimeHost virtual private server revolution.

Dedicated Servers: Backed by a 99.9% SLA network uptime guarantee

We only use enterprise-class hardware in our dedicated servers and offer a four (4) hour hardware replacement. Throw in IPMI for remote management, support for public and private networks, free operating system (OS) re-installs, and SATA, SAS & SSD (including NVMe) storage. Call +1 877 477 9454 or email us at Sales@ProlimeHost.com. We're here to help.