Ransomware Infection to Encryption in Three Seconds

REPORTED RANSOMWARE ATTACKS

- 433 percent increase in 2016 ransomware attacks
- Fivefold increase in the course of one year
- $24 million dollars in victim costs in 2015

Sources: Arctic Wolf Networks, Kaspersky Labs, and FBI Internet Crime Complaint Center

Ransomware: The Digital Plague

Ransomware is a type of malware that encrypts the files on machines and demands a ransom from the user in exchange for the encryption key to make the files accessible. Ransomware is a booming business for cybercriminals, and right now it's quite lucrative! In 2016 ransomware struck in a major way, with victims like MedStar, Hollywood Presbyterian Medical Center and Michigan Utility BWL just to name a few. It's clear that organizations of all kinds, from hospitals to large corporations to government entities have fallen victim to ransomware schemes, but small businesses in particular are even more at risk.

Arctic Wolf Networks has seen a 433 percent increase in ransomware attacks this year among our SMB customers – and other leading security experts are reporting dramatic increases as well. Kaspersky Labs reported that ransomware attacks have increased fivefold in the course of one year, going from 131,111 infection attempts in 2014-2015 to 718,536 in 2015-2016. Further, the FBI's Internet Crime Complaint Center reported that a total of 2,453 ransomware complaints were received in 2015, costing victims more than $24 million dollars. The numbers show that ransomware is on the rise, and businesses should be paying attention.

Any cyber hack presents a threat to an organization, but ransomware does so by making it impossible to conduct business. Without access to servers, devices and files, an organization is crippled, losing money with every minute that passes. The impact extends beyond a one-time financial loss since a ransomware incident is highly disruptive and can damage a company's relationship with its customers.

From Infection to Encryption

Like most malware, the majority of ransomware enters the organization through email. User error creates an entry point: an unsuspecting employee opens an email that looks legitimate, clicks on a suggested link, and inadvertently installs the malware onto the system. But, what makes ransomware so unique, so dangerous, are the actions it takes once installed on the system. Unlike malware that lies dormant and often undetected for a while before stealthily combing through and encrypting files, ransomware takes action as quickly as possible.

Timeline (in Seconds)	Activity
0:00.0	User clicks on phishing email
0:01.0	User unknowingly downloads ransomware
0:01.5	Ransomware unpacks and executes
0:02.0	Ransomware downloads encryption keys
0:02.5	Scans computer to identify all attached drives
0:03.0	File encryption begins
Encryption Completed	User gets ransom notification

Within just a few seconds, the ransomware unpacks and executes itself and then reaches out to a command and control server to retrieve a key, which it will use to encrypt the files. It is only a matter of seconds from infection to encryption. Then it becomes a race against time.

Unlike other malware, ransomware typically does not spread to other computers on its own. It is designed to "infect and encrypt" quickly, creating as many incidents as possible before being shut down. However, infections do commonly spread when a user forwards an email with a malware attachment to others within their own organization. Since the recipient recognizes the sender, they often open it, click on the infected attachment and infect the new computer. The above timeline then starts all over again.

Ransomware for Sale

Ransomware has become a business, and has evolved to the point where anybody can purchase a ransomware kit and begin extorting money. Malware expert Lawrence Abrams discovered a site on the Dark Web called Hall of Ransomware that is selling infections and unlocking services. The site sells the Locky ransomware for $3,000 and Goliath for $2,100, a next generation ransomware created to make carrying out an attack easier for beginner hackers. Features include the ability to download the contents of the infected computer and the ability to lock or unlock a computer with a single click.

There are a number of sites like the Hall of Ransomware, and they continue to multiply. Some even offer a commission-based pricing structure that give criminals the ransomware for free, but require them to pay a percentage of the ransom. Ransomware is quickly starting to resemble an industry of independent software vendors, and the number of attacks and variants will only get worse.

Ransomware Detection and Remediation

Stopping ransomware is nearly impossible, so the best defense today is rapid detection, response and remediation. You only have three seconds from the time of infection to save your business-critical data. The ransomware aims to encrypt as much as possible, making restoring efforts such a daunting task that organizations will opt to make the ransom payment in exchange for the data. Once a threat is detected, the best course of immediate action is to turn off your computer to limit the number of files the ransomware has time to encrypt.

Aside from the last resort action of paying the ransom, the only option an organization has once they've been hit by ransomware is to wipe the machine of all programs and files in order to start fresh. For this reason, having a trusted and tested backup and disaster recovery plan in place is the most critical component of successfully recovering from a ransomware attack. Without a proper backup and disaster recovery strategy, businesses will be left with no option but to pay the ransom.

Whenever possible, it is advised NOT to pay the ransom, but to wipe hard drives clean. From there, businesses can re-install base operating systems like Windows and Linux, and begin recovery from the latest backup of files.

There are, however, several dangers with this approach including:

- The victimized organization suffers monetary loss
- The organization is ultimately funding organized cybercrime
- There is no guarantee that the files or data will be returned once a ransom is paid
- Even if all access and files are returned to an organization, using files that have been encrypted/altered by a cybercriminal is risky in itself

Best Practices and Protection

Below is a series of everyday best practices that organizations should embrace including:

- **Backup your data/files.** Perform system backups regularly and often to ensure any data held ransom can be recovered internally.
- **Carefully monitor your network**. It is possible to detect when ransomware dispatches if you're carefully monitoring your network. When that initiation is quickly detected, disabling the workstation immediately can take recovery time from 24 hours to as little as 5 minutes.
- **Regularly train all of your users.** User error is the key to ransomware's success, so educating users on the basics of security such as not opening emails from unknown senders and downloading attachments is key. You can also train your users on how to spot security threat warnings, and how to deal with them properly.
- **Keep your perimeter defenses up to date.** A sound security strategy comes down to discipline. Most organizations make investments in antivirus or email scanning systems, but if these are not updated regularly to ensure the latest signatures and patches are in place, they become less effective at blocking and flagging suspicious activity.

Ransomware is a digital plague that is costing businesses billions of dollars every year. All indicators point to a continued increase in the number of ransomware attacks, particularly at SMBs. While there is no foolproof vaccine to this plague, rapid detection, response and remediation can greatly reduce the damage it brings.

ARCTIC WOLF

Arctic Wolf Networks, Inc. / 111 West Evelyn Ave., Suite 115, Sunnyvale, CA 94086 / T 1.888.272.8429 / www.arcticwolf.com