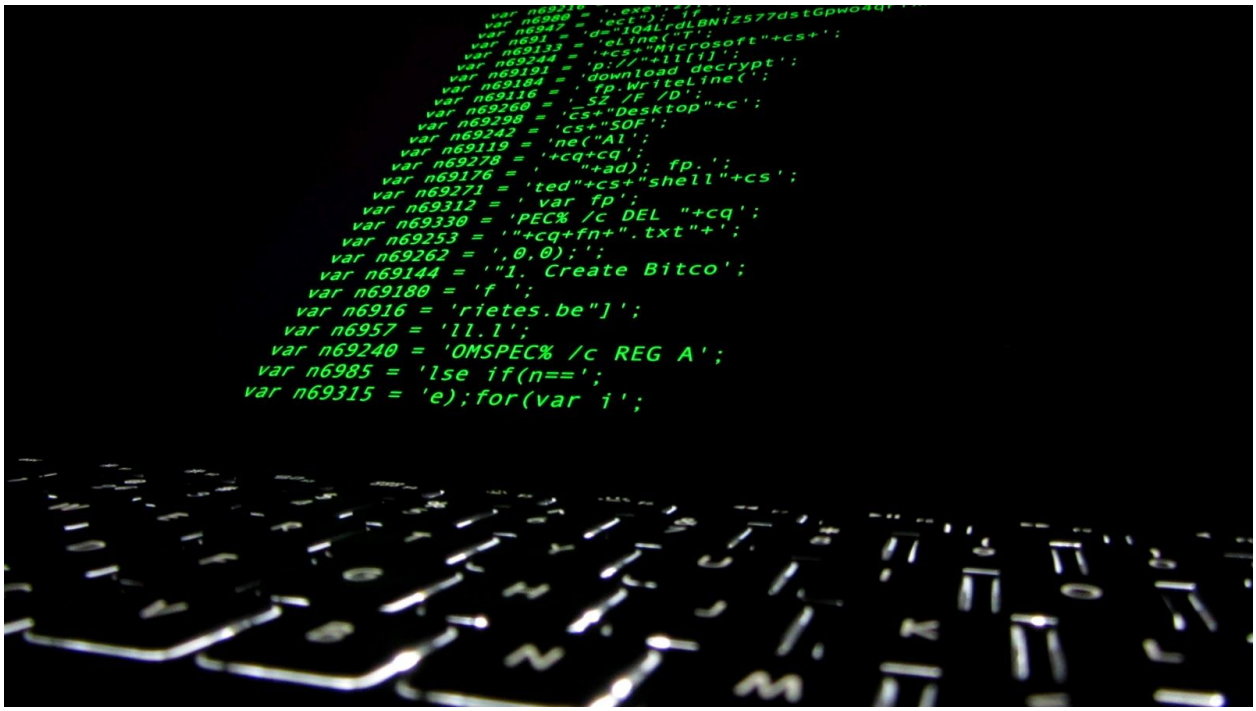
Ransomware is Here!

What you can do about it?



Overview

Over the last few years, ransomware has emerged as one of the most devastating and costly attacks in the hacker arsenal. Cyber thieves are increasingly using this form of attack to target individuals, corporate entities and public sector organizations alike by holding your system or files for ransom. Unlike other forms of cyber theft that often involve stolen financial or healthcare information, ransomware cuts out the middleman. In cases where an attacker steals health or financial documents, they must sell them on to third parties to make money. As far as ransomware is concerned, the money comes directly from the victim.

Ransomware is a quickly growing threat vector. According to the FBI's Internet Crime Complaint center (IC3), infected users made complaints about ransomware 2,453 times in 2015—nearly double the figure for 2014. What's more, these figures most likely represent only the tip of the iceberg, as many users pay their ransom without making a report to the authorities. A recent survey conducted by a Cyber Security Research Center at the University of Kent found that over 40% of those infected with CryptoLocker actually agreed to pay the ransom demanded, which is a big incentive for hackers to target more systems.

What is ransomware?

Ransomware is a type of malware that infects a computer and takes control of either the core operating system using lockout mechanisms or possession of data files by encrypting them. The program then asks the user to make a “ransom” payment to the malicious individual or organization in order to remove the locks and restore the user’s endpoint or files.

Less sophisticated malware simply locks the user out of the system, preventing them from logging in and accessing programs and data on their device. More advanced forms of ransomware will target specific data files such as sensitive documents, spreadsheets, PDF files, pictures and videos. These files are encrypted with advanced cryptographic techniques so that they become inaccessible for use. This more advanced mechanism may also traverse network shares and hold hostage data files that are present on shared drives and online file storage/sharing services.

The malware will also use very long encryption keys making it virtually impossible for the user to circumvent the extortion demands. In either case, once infected, a computer or the data files cannot be used without the decryption key. In many cases, even when the ransom has been paid the ransomware will remain, lying dormant on the hard drive which makes this threat even more concerning.

Ransomware examples

Reveton

This malware did not encrypt files, but rather blocked internet access with a fake law enforcement warning demanding payment to restore access. Reveton falsely warned victims that their computers had been identified by the FBI or Department of Justice as being associated with child pornography websites and other illegal online activity.

Cryptowall/Crowti

This is a recent. CryptoLocker variant in this family, and Cryptowall first appeared in 2014. This variant employed more sophisticated attack methods and techniques to hide itself from traditional antivirus software. Cryptowall also attempts to delete shadow copies of files eliminating a common method of lost data recovery and thus making it even more damaging and resistant.

CryptoLocker

This malware has surfaced in many different variations, and is one of the most recognizable examples of this ransomware attack. CryptoLocker was first reported in late 2013 and was one of the first to employ the encryption/ransom technique. Originally, it also claimed to only allow 72 hours before the decryption key was permanently deleted.

To decrypt the files and allow the victim to recover from an attack, these tools require payment using either cash cards or BitCoin. The threat actors mostly operate out of TOR websites in an effort to obfuscate their identities. Payments typically range from $200 to $500, although it is not uncommon for the extortion scheme to run into tens of thousands of dollars per victim. Once paid, a decryption key may be sent which is used to recover the locked system or files – although, as can be expected in a criminal enterprise, this is not guaranteed.

What can you do if you're infected?

Ransomware follows an attack pattern that consists of 5 steps. In most cases, these steps take less than a few seconds to execute. Even the most benign activities can result in the endpoint becoming a victim of ransomware, and your personal and/or business critical files becoming hostage to extortion.

1. Alert law officials.

They probably won’t be able to help, but like any ransom activity, they should be informed.

2. Isolate the infected machine.

It's important that the system is taken offline, as they essentially own your machine now and can use it to gain access to other systems on the network.

3. Don't pay the ransom.

As with any form of ransom, you are not guaranteed to get your data back, and you're just encouraging attackers to keep up their lucrative game. In addition, if you pay and actually get your keys once, you may be the target of a repeat (and potentially more costly) ransom attack in the future.

4. Remediate.

Run ***endpoint security software**** to discover and remove the ransomware software. If it cannot detect the threat, wipe your machine.

5. Restore.

Restore your files with the most recent backup.

What can OC IT Solutions do for you?

*we have recently partnered with the leading endpoint security software provider in the United States. Through our strategic partnership and use of our volume purchasing power, we are able to provide enterprise grade endpoint security without enterprise prices. Our clients enjoy the peace of mind that their systems are equipped with the tools necessary to not only monitor and block cyber attacks but to remedy and recover from them in the event of a malware or ransomware infection.

Protection against ransomware is based on advanced **artificial intelligence and predictive real-time execution inspection/prevention.** With advance recovery tools, the software allows victims can recover from a ransomware infection on any platform such as windows, Mac OS X and mobile OSs (Android and iOS mobile devices) as well as Windows and Linux servers.

Contact us:
https://ocitsolutions.com
(949) 556-3636