International Journal of Commerce and Management Research
ISSN: 2455-1627, Impact Factor: RJIF 5.22
www.managejournal.com
Volume 3; Issue 6; June 2017; Page No. 41-43

A conceptual study on Ransomware: The effects and preventions

Nayana KS, Shwetha C, Arunakumari K

Assistant Professor, Department of Commerce, St. Claret College, Bengaluru, Karnataka, India

Abstract
The study on ransomware was carried out after its rampant outbreak in the third week of May 2017. Understanding the facts behind ransomware is important so that it can help in preparing and protecting against it. The study is based on newspaper articles, journals, website information about the possible effects of ransomware attack and its prevention techniques.

Keywords: ransomware, bitcoins, wannacry

Introduction

Ransomware is a type of malicious software that blocks access to the victim's data or threatens to publish or delete it until a certain ransom is paid. The victim of such ransomware attack may not even be sure if his data will be restored to him or deleted. Simple ransomware may lock the system in a way which is not difficult for a knowledgeable person to reverse. More advanced malware uses a technique called cryptoviral extortion, in which it encrypts the victim's files, making them inaccessible, and demands a ransom payment to decrypt them. WannaCry (also known as Wana Decryptor or WCry) first emerged in Europe and appears to have hit Russia the hardest. The malware targeted government buildings, banks and railroads in Russia, prompting a stern response from government officials. India being among the 99 countries affected by a global cyber-attack that took down, among others, health services in the UK, a telecom network in Spain. Investigations have recognized WannaCry as the culprit and explosion of this ransomware, in a significant number of cases, appears to have been through a route that most of us tend to overlook - use of expired/pirated software. WannaCry exploited vulnerability in a commonly used operating system to spread. This can pose a significant risk to businesses and individuals in India, considering the rampant use of expired and/or pirated software.

Bitcoin is a digital currency created in 2009. It follows the ideas set out in a white paper by the mysterious Satoshi Nakamoto, whose true identity has yet to be verified. Bitcoin offers the promise of lower transaction fees than traditional online payment mechanisms and is operated by a decentralized authority, unlike government-issued currencies.

History of ransom ware

The first ransomware virus was unleashed in 1989 — pre-dating the Internet and email as we know it — and distributed on floppy disk by the post office.

The culprit was Joseph L. Popp, an American evolutionary biologist with a Ph.D. from Harvard. The 20,000 disks Popp sent out to health researchers around the world that year masqueraded as a survey designed to test one's risk of contracting AIDS. But after a fixed number of reboots, the virus locked the computer. Users were instructed to turn on their printers, from which a ransom note soon emerged, demanding a $189 "licensing fee" in exchange for a decryption key. Ransomware has been the most pervasive cyber threat since 2005. According to publicly available information, Ransomware infections have outnumbered data breaches 7694 to 6013 over the past eleven years. Over the years, there have been 2 distinct varieties of ransomware which remain consistent crypto and locker based. Crypto ransomware variants that actually encrypt file and folders hard drivers etc., whereas locker ransomware only locks users out of their devices, most often seen with android based ransomware.

Objective of the study

- To understand the effects of unauthorised programmes used in all sizes of business
- To know the preventive measures to avoid being affected by malwares for business and individuals
- To know the impact of Ransomware in India

Possible effects of ransomware

Ransomware not only targets home users; businesses can also become infected with ransomware, leading to negative consequences, which includes:

- Temporary or permanent loss of sensitive or proprietary information,
- Disturbance to regular operations,
- Financial losses incurred to restore the important data, and
- Probable harm to an organization's status.

Paying the ransom does not guarantee the encrypted files will be released; it only guarantees that the malicious actors receive the victim's money, and in some cases, their banking information. In addition, decrypting files does not mean the malware infection itself has been removed.

How Ransomware has affected India

According to the BSA Global Software Survey 2016, about 58% of software in India is pirated and/or unlicensed. The world average, in comparison, is about 39%. Among organizations, it was found that globally about 25% of software used was unlicensed and this included heavily regulated industries like Banking and Securities.

Interestingly, the survey report also found that at least a fourth of employees surveyed admitted to installing external software on work computers including two or more unauthorized

programs. This practice is fairly common among small and medium enterprises in India that do not have strong information security policies nor conduct periodic checks on the prevalence of unlicensed software.

In the past, it has been estimated that at least 65% of victims of all targeted cybercrime attacks, including ransomware, have been small and medium organizations. It is, therefore, possible that a large proportion of WannaCry attack victims were likely to be small and medium enterprises.

Most Ransomware encrypt specific file types on an impacted system and a ransom is demanded for the victim to regain access to these files. In some instances, built-in algorithms identify files created most recently and in others files accessed most frequently. WannaCry is different because it moves across a network without human intervention, and which perhaps is the reason for the 'epidemic' like environment it has created.

Prior to WannaCry, there have been several cases of Ransomware attacks in India in recent times. Many have gone unreported and in several cases the "ransom" up to over 50 bitcoins has been paid. (Ransom is usually asked for in bitcoins due to various reasons.) The results have been mixed, where in some instances, individuals have got access to their encrypted files and in others the files continue to remain encrypted despite ransom payment.

In some cases we have observed other malware being injected into the victims' systems, escaping detection as the victims focus energies on addressing the Ransomware issue.

A number of individuals, smaller businesses and perhaps some larger organizations in India continue to use versions of the affected operating system that are no longer supported by the publisher. As a result any inherent vulnerability that was undiscovered or unaddressed at the time support was discontinued by the publisher may continue to exist. Inadequate IT support can also result in critical updates not being applied.

This is further complicated by people using pirated versions of antivirus software, where virus definitions are not updated and hence, spyware and other forms of malware attacks go undetected.

The result Loss of confidential data, increased exposure to further cyber-attacks, and increased cost of battling a ransomware attack. The BSA Global software survey report 2016 indicates that it costs an organization $11 million to remediate a successful cyber-attack. In India, cyber-attack remediation cases have impacted organizations to the extent of a couple of hundred crores rupees.

Prevention Methods

- Organizations should address infrastructural issues. If any business can benefit from use of technology, then it is important that cyber security is built into the infrastructure, as the cost of addressing a breach can end up being more expensive than investing in the right mechanisms to create a line of defence. This includes purchasing and installing genuine operating systems and office applications, mechanisms to track release, and application of security updates and internet security software. In addition, based on business context, measures such as spam filters, firewalls etc. can also be deployed.
- Employees and other individuals need to be more aware of the dangers that lurk in cyberspace-that no stranger in another country is going to pay you a million dollars, attachments in emails that are. exe, .zip or .scr should generally not be clicked on without checking with the sender, and that one should be wary of emails from unknown addresses whether or not they have attachments or links.
- Caution should also be exercised while clicking on web links, especially those embedded in emails. Risky sites, including most pornography websites, should be avoided as many are replete with hidden malware. A structured awareness program that can periodically educate employees on these dangers can benefit organizations in the long run.
- It is critical for businesses of all sizes to have a plan around backing up information residing on computer systems. While large organizations tend to invest in automated backing up mechanisms, small organizations could do something simpler such as backup on external hard drives periodically.
- Refrain from opening attachments that look suspicious. Not only does this apply to messages sent by unfamiliar people but also to senders who you believe are your acquaintances. Phishing emails may masquerade as notifications from a delivery service, an e-commerce resource, a law enforcement agency, or a banking institution.
- Patch and keep your operating system, antivirus, browsers, Adobe Flash Player, Java, and other software up-to-date.
- Keep the Windows Firewall turned on and properly configured at all times. Enhance protection more by setting up additional Firewall protection. There are security suites out there that accommodate several Firewalls in their feature set, which can become a great addition to the stock defense against a trespass.
- Switch off unused wireless connections, such as Bluetooth or infrared ports. There are cases when Bluetooth get exploited for stealthily compromising the machine.
- Block known-malicious Tor IP addresses. Tor gateways are the primary means for ransomware threats to communicate with their C&C servers. Therefore, blocking those may impede the critical malicious processes from getting through.

Conclusion

Since ransomware is definitely today's number one cyber danger due to the damage it causes and the prevalence factor, the countermeasures above are a must. Otherwise, most important files could be completely lost. The key recommendation, though, is the one about backups – offline or in the cloud. In this scenario, the recovery consists of removing the ransom Trojan and transferring data from the backup storage.

Currently, dealing with the consequences of ransomware isn't very promising from the file decryption perspective. That is why thwarting the virus attack can save a pretty penny and guarantee peace of mind.

References

1. http://economictimes.indiatimes.com/articleshow/58787536.cms?utm_source=contentofinterest&utm_medium=text&utm_campaign=cppst

2. http://economictimes.indiatimes.com/articleshow/58666596.cms?utm_source=contentofinterest&utm_medium=text&utm_campaign=cppst
3. https://www.tripwire.com/state-of-security/security-data-protection/cyber-security/22-ransomware-prevention-tips/
4. Bitcoin http://www.investopedia.com/terms/b/bitcoin.asp#ixzz4iRiOrMdS
5. Mehmood, Shafqat (3 May 2016). "Enterprise Survival Guide for Ransomware Attacks". *SANS Information Security Training | Cyber Certifications | Research*. sans.org. Retrieved 3 May 2016.
6. http://www.rollingstone.com/culture/news/wannacry-what-you-need-to-know-about-global-ransomware-attack-w482268