Ransomware - Threats, Vulnerabilities And Recommendations

Nadeem Shah, Mohammed Farik

Abstract: Attack methodologies transform with the transforming dynamics of technology. Consequently it becomes imperative that individuals and organization implement the highest levels of security within their devices and infrastructure for optimal protection against these rapidly evolving attacks. Ransomware is one such attack that never fails to surprise in terms of its ability to identify vulnerabilities and loopholes in technology. This paper discusses the categories of ransomware, its common attack vectors and provides a threat landscape with the aim to highlight the true potential and destructive nature of such malware based attacks. In this paper we also present the most current ransomware attack that is still a potential threat and also provide recommendations and strategies for prevention and protection against these attacks. A novel solution is also discussed that could be further worked upon in the future by other researchers and vendors of security devices.

Index Terms: Ransomware, WannaCry, WannaCrypt, Malware, Worm, Bitcoin

1 INTRODUCTION

Malware consistently endures to grow as a threat. The rapid development of the Internet of Things (IoT) has contributed equally to this threat by providing a bigger landscape for attacks. Everything we utilize daily in our lives now has the potential to be connected online and collaborate as one, and everything that is connected is vulnerable. Ransomware is a category of malware that spreads like a worm and inhibits or limits users from accessing their system, either by locking the system's screen or by encrypting and locking the users' files unless a ransom is paid [1]. Ransomware usually comprise of indestructible encryption consequently making it impossible to decrypt. Assailants commonly encrypt an organizations critical business data after they have infiltrated its systems, subsequently demanding a monetary payment in digital cash formats such as “bitcoin” [2]. Bitcoin comprises of encryption techniques [3] utilized to regulate the generation of units of currency, whereby fund transfer verification is completed independently of a central bank.

2 CATEGORIES OF RANSOMWARE:

2.1 Encrypting Ransomware

Encrypting Ransomware is ransomware that combines innovative encryption algorithms intended to block access to files requiring a ransom payment for file decryption. Examples of encrypting ransomware are “CryptoLocker”, “Locky”, CryptoWall” [4] with the most recent being “WannaCrypt”.

2.2 Locker Ransomware

Locker Ransomware is a type of malware that locks the target out of the operating system, consequently preventing access to the targets desktop, applications and files [4]. An example of locker ransomware is the “Winlocker”.

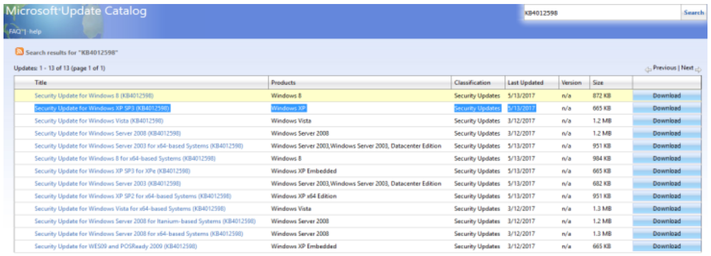
2.3 Ransomware Common Attack Vectors

Malicious Email Attachments: The assailant designs an email pretending to be from a credible source for example Accounts, Human Resources or Information Technology department, and attaches a malicious file in a Microsoft Word or similar document file [5].The recipient trusting the email source opens the attachment and unknowingly downloads the ransomware infecting their system leading to their files being held ransom [5]. A crypto-ransomware named “Locky” infiltrates a victims system through email camouflaged as an invoice with a conforming Microsoft Word document that is embedded with malicious [6] macros. These macros execute malware upon download. Generally macros are disabled by default in Microsoft Word; however enabling macros makes a system vulnerable to potential malicious code. Once a system is infected, the malware Locky searches for directly attached and network attached drives and encrypt files with a “.locky” extension leaving behind a ransom note for file decryption [6]. Malicious Email Links - are URLs (Uniform Resource Locator) in the body of the email and are sent from supposedly trusted sources. Upon clicking these URLs, malicious files are download from the Internet infected the system and holding its files for ransom [5]. The evolutions of malware attacks have simplified its execution consequently making any organization or individual a possible ransomware victim. Exploit Kits - Sophisticated toolkits that exploit vulnerabilities are defined as exploit kits which are executed when a victim visits a compromised website. Malvertisement are malicious code hidden frequently in an advertisement redirecting one to the exploit kit web page in an unobserved fashion [5]. On an unprotected system, a drive-by download of a malicious payload will be executed thus infecting the system and holding its files for ransom. The present most destructive ransomware exploit kit is the “Wanna Cry” or “WannaCrypt” ransomware.

- *Nadeem Shah is currently pursuing masters degree program in Information Technology at The University of Fiji, E-mail: nadeemfiji@gmail.com*
- *Mohammed Farik (Member IEEE) is a Lecturer in Information Technology in the School of Science and Technology at University of Fiji, E-mail: mohammedf@unifiji.ac.fj*

2.4 Destructive Scale of Ransomware

Support for Windows XP terminated on April 8th, 2014 [7] however Microsoft delivered an additional public patch for 16 year old Windows XP operating system to fight 'WannaCrypt' ransomware attacks [8]. This highly unusual step was taken after customers worldwide including England's National Health Service suffered a hit from "WannaCrypt" ransomware [8]. Microsoft patched all of its presently supported systems to fix the flaw back in March, however after the overwhelming effects of the WannaCrypt ransomware, Microsoft released an update available for unsupported systems such as [8] Windows XP, Windows 8 and Windows Server 2003. These critical Microsoft updates "KB4012598" are available at http://www.catalog.update.microsoft.com/Search.aspx?q=KB4012598 [9]. As displayed in the below image, the last update for Windows Service Pack 3 was released on May 13th, 2017. The destructive scale of the WannaCrypt ransomware is truly visible with Microsoft having to release an update for an unsupported 16 year old operating system like Windows Service Pack 3.



Microsoft Update Catalog

FAQ | help

KB4012598 Search

Search results for "KB4012598"

Updates: 1 - 13 of 13 (page 1 of 1)

Previous | Next

Title	Products	Classification	Last Updated	Version	Size	
Security Update for Windows 8 (KB4012598)	Windows 8	Security Updates	5/13/2017	n/a	872 KB	Download
Security Update for Windows XP SP3 (KB4012598)	Windows XP	Security Updates	5/13/2017	n/a	665 KB	Download
Security Update for Windows Vista (KB4012598)	Windows Vista	Security Updates	3/12/2017	n/a	1.2 MB	Download
Security Update for Windows Server 2008 (KB4012598)	Windows Server 2008	Security Updates	3/12/2017	n/a	1.2 MB	Download
Security Update for Windows Server 2003 for x64-based Systems (KB4012598)	Windows Server 2003,Windows Server 2003, Datacenter Edition	Security Updates	5/13/2017	n/a	951 KB	Download
Security Update for Windows 8 for x64-based Systems (KB4012598)	Windows 8	Security Updates	5/13/2017	n/a	984 KB	Download
Security Update for Windows XP SP3 for XPe (KB4012598)	Windows XP Embedded	Security Updates	5/13/2017	n/a	665 KB	Download
Security Update for Windows Server 2003 (KB4012598)	Windows Server 2003,Windows Server 2003, Datacenter Edition	Security Updates	5/13/2017	n/a	682 KB	Download
Security Update for Windows XP SP2 for x64-based Systems (KB4012598)	Windows XP x64 Edition	Security Updates	5/13/2017	n/a	951 KB	Download
Security Update for Windows Vista for x64-based Systems (KB4012598)	Windows Vista	Security Updates	3/12/2017	n/a	1.3 MB	Download
Security Update for Windows Server 2008 for Itanium-based Systems (KB4012598)	Windows Server 2008	Security Updates	3/12/2017	n/a	1.2 MB	Download
Security Update for Windows Server 2008 for x64-based Systems (KB4012598)	Windows Server 2008	Security Updates	3/12/2017	n/a	1.3 MB	Download
Security Update for WES09 and POSReady 2009 (KB4012598)	Windows XP Embedded	Security Updates	3/12/2017	n/a	665 KB	Download

Fig.1. *Microsoft Update Catalog KB4012598 (Microsoft, 2017)*

2.5 Ransomware Payments

After accomplishment of file encryption, ransomware software will usually present a GUI [10] window showing the user that their files have been encrypted and offering them a payment method to recover their files (Microsoft, 2017) with the required decryption key. As discussed earlier, ransomware payment is made with Bitcoin. Additional encryption of genuine AES key with a public key makes it impossible to decrypt files without the private key [10].

3 Ransomware Threat Landscape

Ransomware might not be industry specific; nevertheless it is often connected with the healthcare industry, probably owing to several high-profile healthcare incidents in the recent past [11]. According to the Fortinet Threat Landscape Report Q4 2016, 36% of organizations reporting active botnets during the time frame detected activity related to ransomware [11].

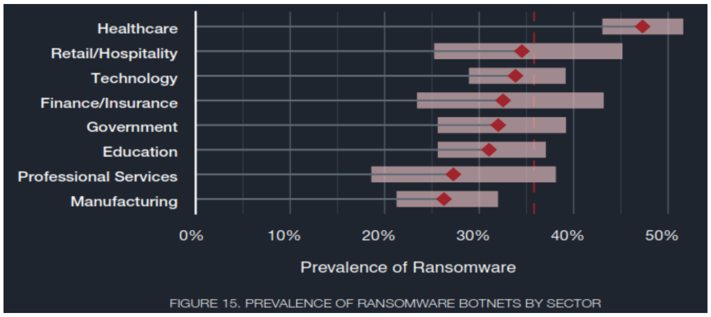


FIGURE 15. PREVALENCE OF RANSOMWARE BOTNETS BY SECTOR

Fig.2. *Occurrence of Ransomware Botnets by Sector according to Fortinet Threat Landscape Report Q4 2016 [11].*

Conferring to the Malwarebytes State of Malware Report 2017, we can see in the Fig.2 below that the dissemination of ransomware amongst January 2016 and November 2016 amplified by 267 percent [12]. This is an unprecedented supremacy of the ransomware threat landscape.

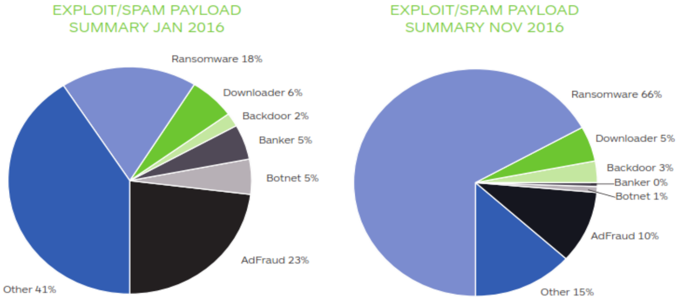


FIG. 3 *Ransomware Payload Summary: January 2016 – November 2016 [12].*

4 Free Ransomware Decryption Tools

Antivirus companies occasionally offer ransomware decryption tools free of cost. AVAST Software, Inc. [13], AVG Technologies [14] and ESET [15] offer decryption tools for selected ransomware such as Alcatraz Locker, Apocalypse, BadBlock, Bart, Crypt888, CrySiS, FindZip, Globe, HiddenTear, Jigsaw, Legion, NoobCrypt, Stampado, SZFLocker and TeslaCrypt. The above mentioned decryption tools have inadequate functionality and are usually not contemporary, consequently taking proactive procedures against ransomware is required for ultimate protection.

5 Future Of Ransomware

Internet of Things incorporates (IoT) thousands of categories of networked devices which offer many services, numerous of which are cloud based consequently IoT [16] threats and responses are closely associated with cloud threats and responses. Botnets are a system of remote computers infected with malicious software. Botnets are small in size, have the capability to hide and execute an immeasurable amount of operations, consequently Botnets could be utilized to distribute ransomware payloads on IoT devices. Malwarebytes foresees variants of ransomware that could transform an infected systems Master Boot Record (MBR), thus depriving a system of its ability to boot into its operating system hence will booting into a lock screen designed by the malware, providing an ultimatum for payment for decryption of files and restoration of access to the primary operating system [12].

6 Recommendations

Our first and most critical recommendation is that organizations quickly patch all their Windows endpoint and server machines with the Microsoft MS17-010 update for protection against the most current ransomware "WannaCrypt" [9] which was detected on May 12, 2017. These critical Microsoft updates "KB4012598" are available at http://www.catalog.update.microsoft.com/Search.aspx?q=KB4012598 and are available for both supported and unsupported operating systems [9]. Spam mail is a common method of ransomware infection. Infection has the potential to spread almost instantaneously the moment a user innocently clicks on a mail infected with ransomware. We strongly recommend that organizations utilize email gateways that provide sandbox protection. A sandbox is an environment created to deceive malware into trusting that it is interrogating external servers even though it is just communicating with a group of fake sandbox IP addresses. In a sandbox, all content is scrupulously scanned comprising of attached URLs. Since testing of these attachments and URLs are done in an environment completely separate of the real network, no harm is done on the real network and only clean data is transferred from the sandbox onto the actual network. Ransomware can potentially encrypt data backup stored on disks; consequently we recommend that organizations utilize backup software that provides end to end encryption with the ability to encrypt data during backup for protection against ransomware. One such solution is the Veeam Availability Suite 9.5 [17] which features AES 256 bit encryption with the ability to secure data during a backup. We also recommend that organizations utilize tape storage to secure data offsite and onsite. Tape backups would help deliver business continuity since anything that is networked can be hacked; consequently data backups transferred to tapes stored off the network would be potentially safe from ransomware attacks and could be utilized to restore business operations post a ransomware attack.

7 Novel Solution

Through research and study of available Ransomware code, we identified that ransomware code will usually try to obtain drive information by issuing the "GetDriveTypeW" command while trying to identify Local, Fixed and Remote drives. We also identified that ransomware code will contain some form of encrypting instructions such as "run_encrypting_thread" which would execute to encrypt all drives connected to an endpoint. Since all Firewalls, Endpoint Protection, Server Protection and Intrusion Detection and Prevention Devices nowadays are able to inspect all 7 layers of the OSI model, we recommend that these devices also be included with mechanisms that are able to pick up programs trying to execute the above mentioned commands and prevent them from executing immediately. These commands are usually hidden within any of the 7 layers of the OSI model whilst communication in in progress, and any devices that has visibility of all 7 layers should be able to inspect, identify and stop any attacks of such nature.

8 Conclusion

Through this research we can conclude that being proactive rather than reactive is the best form of defense against ransomware. Organizational users need to be educated on a regular basis on common security threats and security tactics. Users need to be educated against opening of unsolicited links and attachments in emails since this is a common platform for ransomware attacks. Organizations can further enhance prevention of unsolicited email by implementing secure cloud email security gateways that restrict delivery of suspicious email by sandboxing them in their cloud. This approach provides an additional layer of protection as compared to on premise email security gateways that download all emails onto their physical box and then restrict them. Moreover, we can conclude that all individuals and organizations must prioritize and immediately update their Windows systems with the Microsoft update released for protection against the "WannaCrypt" ransomware. Seeing that Microsoft has unusually released updates for unsupported operating systems is evidence of the scale of the threat caused by the WannaCrypt ransomware.

References

[1]. Deo, S. And M. Farik Information Security - Recent Attacks In Fiji. INTERNATIONAL JOURNAL OF SCIENTIFIC & TECHNOLOGY RESEARCH VOLUME, 2016. 5(12): P. 218-220.

[2]. Guide For Cybersecurity Event Recovery. 2016, NIST.

[3]. Coindesk. What Is Bitcoin? 2015 May 14; Available From: Http://Www.Coindesk.Com/Information/What-Is-Bitcoin/.

[4]. What Is Ransomware And 15 Easy Steps To Keep Your System Protected [Updated]. 2017; Available From: Https://Heimdalsecurity.Com/Blog/What-Is-Ransomware-Protection/.

[5]. Ransomware Common Attack Methods. 2016, Palo Alto Networks, Inc.

[6]. New Crypto-Ransomware Locky Uses Malicious Word Macros. 2016; Available From: Https://Www.Trendmicro.Com/Vinfo/Us/Security/News/Cybercrime-And-Digital-Threats/New-Crypto-Ransomware-Locky-Uses-Word-Macros.

[7]. Support For Windows XP Ended 2014; Available From: Https://Www.Microsoft.Com/En-Us/Windowsforbusiness/End-Of-Xp-Support.

[8]. Microsoft Patches Windows XP To Fight 'Wannacrypt' Attacks. 2017; Available From: Https://Www.Engadget.Com/2017/05/13/Microsoft-Windowsxp-Wannacrypt-Nhs-Patch/.

[9]. Microsoft Update Catalog. 2017; Available From: Http://Www.Catalog.Update.Microsoft.Com/Search.Aspx?Q=KB4012598.

[10]. The Current State Of Ransomware. Https://Www.Sophos.Com, 2015.

[11]. THREAT LANDSCAPE REPORT Q4 2016. 2016, Fortinet Inc.

[12]. State Of Malware Report. 2017, Malwarebytes.

[13]. Free Ransomware Decryption Tools. 2017; Available From: Https://Www.Avast.Com/Ransomware-Decryption-Tools.

[14]. AVG. Free Ransomware Decryption Tools. 2017 [Cited 2017 May 12]; Available From: Http://Www.Avg.Com/Ww-En/Ransomware-Decryption-Tools.

[15]. Download ESET Tools And Utilities. 2017; Available From: Https://Www.Eset.Com/Int/Download-Utilities/.

[16]. Mcafee Labs 2017 Threats Predictions. 2016, Mcafee. Part Of Intel Security.

[17]. End-To-End Encryption. 2017; Available From: Https://Www.Veeam.Com/Backup-Files-Encryption.Html.