“WannaCry” Ransomware – Infecting Computer’s

1. Executive Summary

Security researchers found a ransomware called “WannaCry” or “Wanna Decryptor” is a type of ransomware which spreads from machine to machine silently and remains invisible to users until it unveils itself, Which then warns users that all their files have been encrypted with a key known only to the attacker and that they will be locked out until they pay to an anonymous party using the cryptocurrency Bitcoin.

2. Introduction

Wana Decrypt0r triggered security alerts for ETERNALBLUE, an alleged NSA exploit. ETERNALBLUE works by exploiting a vulnerability in the SMBv1 protocol to get a foothold on vulnerable machines connected online. Microsoft patched the flaw in **MS17-010**, released in March, but that doesn't mean all Windows PC owners have applied the security update.

3. Infection Vector and Analysis

Researchers found that WannaCry attack is based on an attack developed by the NSA, codenamed ETERNALBLUE. Once a computer is infected, the ransomware typically contacts a central server for the information it needs to activate, and then begins encrypting files on the infected computer with that information. Once all the files are encrypted, it posts a message asking for payment to decrypt the files – and threatens to destroy the information if it doesn’t get paid.

Figure 1: Wanna Cry Warning Window

Spreading channel:

Like all ransomware the WannaCry also spreads through Word documents, PDFs and other files normally sent via email.

The malware is delivered as a Trojan through a loaded hyperlink that can be accidentally opened by a victim through an email, advert on a webpage or a Dropbox link. Once it has been activated, the program spreads through the computer and locks all the files with the same encryption used for instant messages.

Once the files have been encrypted it deletes the originals and delivers a ransom note in the form of a readme file, and this malware modifies files in the **/Windows and /windows/system32** directories and enumerates other users on the network to infect. Both of these actions require administrative privileges.

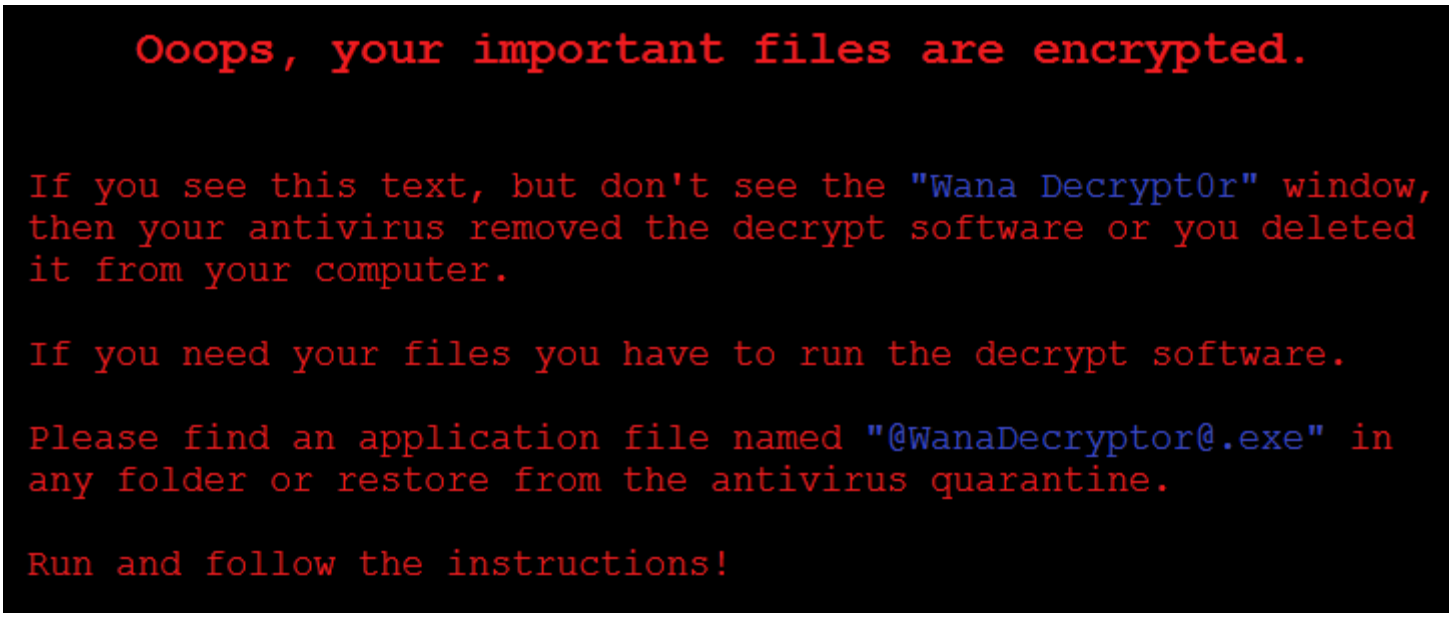

Figure 2: Wanna Cry Warning Window

4. Indicator of Compromise (IoCs)

IOC's are mentioned below:

TYPE	INDICATOR
FileHash-SHA256	09a46b3e1be080745a6d8d88d6b5bd351b1c7586ae0dc94d0c238ee36421cafa
	11d0f63c06263f50b972287b4bbd1abe0089bc993f73d75768b6b41e3d6f6d49
	149601e15002f78866ab73033eb8577f11bd489a4cea87b10c52a70fdf78d9ff
	16493ecc4c4bc5746acbe96bd8af001f733114070d694db76ea7b5a0de7ad0ab
	190d9c3e071a38cb26211bfffeb6c4bb88bd74c6bf99db9bb1f084c6a7e1df4e
	24d004a104d4d54034dbcffc2a4b19a11f39008a575aa614ea04703480b1022c
	2584e1521065e45ec3c17767c065429038fc6291c091097ea8b22c8a502c41dd
	4186675cb6706f9d51167fb0f14cd3f8fcfb0065093f62b10a15f7d9a6c8d982
	593bbcc8f34047da9960b8456094c0eaf69caaf16f1626b813484207df8bd8af
	5ad4efd90dcde01d26cc6f32f7ce3ce0b4d4951d4b94a19aa097341aff2acaec
	6bf1839a7e72a92a2bb18fbedf1873e4892b00ea4b122e48ae80fac5048db1a7
	7c465ea7bcccf4f94147add808f24629644be11c0ba4823f16e8c19e0090f0ff
	9fb39f162c1e1eb55fbf38e670d5e329d84542d3dfcdc341a99f5d07c4b50977
	b3c39aeb14425f137b5bd0fd7654f1d6a45c0e8518ef7e209ad63d8dc6d0bac7
	b47e281bfbeeb0758f8c625bed5c5a0d27ee8e0065ceeadd76b0010d226206f0
	b66db13d17ae8bcaf586180e3dcd1e2e0a084b6bc987ac829bbff18c3be7f8b4
	c365ddaa345cfcaff3d629505572a484cff5221933d68e4a52130b8bb7badaf9
	d8a9879a99ac7b12e63e6bcae7f965fbf1b63d892a8649ab1d6b08ce711f7127
	e14f1a655d54254d06d51cd23a2fa57b6ffdf371cf6b828ee483b1b1d6d21079
	e8450dd6f908b23c9cbd6011fe3d940b24c0420a208d6924e2d920f92c894a96
	ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa
	f01644082db3fa50ba9f4773f11f062ab785c9db02a3a3cfe022cc69763f631d

	f8812f1deb8001f3b7672b6fc85640ecb123bc2304b563728e6235ccbe782d85
	9b60c622546dc45cca64df935b71c26dcf4886d6fa811944dbc4e23db9335640
	2ca2d550e603d74dedda03156023135b38da3630cb014e3d00b1263358c5f00d
	4a468603fdcb7a2eb5770705898cf9ef37aade532a7964642ecd705a74794b79
	7a828afd2abf153d840938090d498072b7e507c7021e4cdd8c6baf727cafc545
	a897345b68191fd36f8cefb52e6a77acb2367432abb648b9ae0a9d708406de5b
	b43b234012b8233b3df6adb7c0a3b2b13cc2354dd6de27e092873bf58af2693c
	b9c5d4339809e0ad9a00d4d3dd26fdf44a32819a54abf846bb9b560d81391c25
	c73633e55a1d66af88a3dc2d46e7d47e0a47ce0bab0930a70b97b003adafc9af
	f5cbff5c100866dd744dcbb68ee65e711f86c257dfcc41790a8f63759220881e
FileHash-MD5	666c806b76568adb5a6c3d34c434820e
	d41d8cd98f00b204e9800998ecf8427e
	a8d30fd8ffd02886818a89ebdd8e7502
	05a00c320754934782ec5dec1d5c0476
	26b205ffe4adaadbb442442cae653bdd
	29365f675b69ffa0ec17ad00649ce026
	46d140a0eb13582852b5f778bb20cf0e
	4fef5e34143e646dbf9907c4374276f5
	509c41ec97bb81b0567b059aa2f50fe8
	5ad5075d8d66cd7c05899d8044fdab65
	5bef35496fcbdbe841c82f4d1ab8b7c2
	775a0631fb8229b2aa3d7621427085ad
	7bf2b57f2a205768755c07f238fb32cc
	7f7ccaa16fb15eb1c7399d422f8363e8
	835fff032c51075c0c27946f6ebd64a3
	83e5a812a371e0790066c6fb038f0d26
	8495400f199ac77853c53b5a3f278f3e
	84c82835a5d21bbcf75a61706d8ab549
	86721e64ffbd69aa6944b9672bcabb6d
	f107a717f76f4f910ae9cb4dc5290594
	8dd63adb68ef053e044a5a2f46e0d2cd
	b0ad5902366f860f85b892867e5b1e87
	d6114ba5f10ad67a4131ab72531f02da
	db349b97c37d22f5ea1d1841e3c89eb4
	e372d07207b4da75b3434584cd9f3450
	f529f4556a5126bba499c26d67892240
	f9992dfb56a9c6c20eb727e6a26b0172
	f9cee5e75b7f1298aece9145ea80a1d2
IPv4	146.0.32.144
	188.166.23.127
	193.23.244.244
	2.3.69.209
	50.7.161.218
	74.125.104.145
	http://146.0.32.144:9001

URL	http://188.166.23.127:443
	http://193.23.244.244:443
	http://2.3.69.209:9001
	http://50.7.161.218:9001
Mutex	Global\MsWinZonesCacheCounterMutexA0
	MsWinZonesCacheCounterMutexA
	RasPbFile
domain	gx7ekbenv2riucmf.onion
	sqjolphimrr7jqw6.onion
	xxlvbrloxvriy2c5.onion
	cwwnhwhlz52maqm7.onion
	76jdd2ir2embyv47.onion
	57g7spgrzlojinas.onion
hostname	r12.sn-h0j7sn7s.gvt1.com
	www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com
FileHash-SHA1	e889544aff85ffaf8b0d0da705105dee7c97fe26
	87420a2791d18dad3f18be436045280a4cc16fc4
	51e4307093f8ca8854359c0ac882ddca427a813c
	45356a9dd616ed7161a3b9192e2f318d0ab5ad10
	6faeaf98d0eaf6671d74bc8e468bddc8ed1e0597
	bd44d0ab543bf814d93b719c24e90d8dd7111234
FilePath	C:\WINDOWS\system32\msg
	C:\Windows\mssecsvc.exe
	C:\WINDOWS\tasksche.exe
CVE	CVE-2017-0144

5. Mitigation

These are following mitigation to avoid these kind of attacks,

1. **Backup Regularly:** To always have a tight grip on all your important files and documents, keep a good backup routine in place that makes their copies to an external storage device that is not always connected to your PC.
2. **Keep your Antivirus software up-to-date:** Virus definitions have already been updated to protect against this latest threat.
3. Update latest patches of windows. (**MS17-010** is a patch for ETERNALBLUE vulnerability.)
4. **Keep your system Up-to-date:** First of all, if you are using supported, but older versions of Windows operating system, keep your system up to date, or simply upgrade your system to Windows 10.
5. **Using Unsupported Windows OS?** If you are using unsupported versions of Windows, including Windows XP, Vista, Server 2003 or 2008, apply below emergency patch released by Microsoft
http://www.catalog.update.microsoft.com/Search.aspx?q=KB4012598

6. **Enable Firewall:** Enable firewall, and if it is already there, modify your firewall configurations to block access to SMB ports over the network or the Internet. The protocol operates on TCP ports 137, 139, and 445, and over UDP ports 137 and 138.
7. **Beware of Phishing:** Always be suspicious of uninvited documents sent an email and never click on links inside those documents unless verifying the source.
8. **Disable SMB:** Follow steps given below as described by Microsoft to disable Server Message Block (SMB). https://support.microsoft.com/en-in/help/2696547/how-to-enable-and-disable-smbv1,-smbv2,-and-smbv3-in-windows-vista,-windows-server-2008,-windows-7,-windows-server-2008-r2,-windows-8,-and-windows-server-2012.

6. Reference URL's

https://www.bleepingcomputer.com/news/security/wana-decrypt0r-ransomware-using- nsa-exploit-leaked-by-shadow-brokers-is-on-a-rampage/
https://theintercept.com/2017/05/12/the-nsas-lost-digital-weapon-is-helping- hijack-computers-around-the-world/
https://www.theguardian.com/technology/2017/may/12/nhs-ransomware-cyber-attack- what-is-wanacrypt0r-20
https://otx.alienvault.com/pulse/5915db384da2585b4feaf2f6/

Disclaimer:-

1. These advisories are for information purpose only. We recommend you to act upon these advisories at your own discretion after conducting risk analysis in your specific environment.

2. These advisories are time sensitive in nature and may be over ridden is subsequent updates from our side as new information is received on the threats.