Society For Cyberabad Security Council

PRESS RELEASE

What is Ransomware?

Ransomware is a malicious software that encrypts the files and locks device, such as a computer, tablet or smartphone and then demands a ransom to unlock it. Recently, a dangerous ransomware named 'Wannacry'/ Wanna cryptoz2 has been affecting the computers worldwide creating the biggest ransomware attack the world has ever seen. This has affected computers in India also along with 80 countries abroad.

What is WannaCry / Wanna cryptoz2 Ransomware?

WannaCry ransomware attacks windows based machines. It also goes by the name WannaCrypt, WannaCry, WanaCrypt0r, WCrypt, WCRY.It leverages SMB exploit in Windows machines called EternalBlue to attack and inject the malware. All versions of windows before Windows 10 are vulneable to this attack if not patched for MS-17-010. After a system is affected, it encrypts the files and shows a pop up with a countdown and instructions on how to pay the 300$ in bitcoins to decrypt and get back the original files. If the ransom is not paid in 3 days, the ransom amount increases to 600$ and threatens the user to wipe off all the data.. It also installs DOUBLEPULSAR backdoor in the machine.

Bit Coin :- Bitcoin is a digital currency created in 2009. Bitcoin offers the promise of lower transaction fees, a traditional online payment mechanisms and is operated by a decentralized authority, unlike government-issued currencies. There are no physical bitcoins, only balances kept on a public ledger in the cloud, that – along with all Bitcoin transactions – is verified by a massive amount of computing power. Bitcoins are not issued or backed by any banks or governments, nor are individual bitcoins valuable as a commodity.The public key (comparable to a bank account number) serves as the address which is published to the world and to which others may send bitcoins. The private key (comparable to an ATM PIN is meant to be a guarded secret, and only used to authorize Bitcoin transmissions. One bitcoin costs around 1693 US$, converted to Indian Rupees of Rs. 1,10,972. This is a virtual currently and as the entire transaction takes place in encrypted environment, very difficult to trace the ac details where the money has been transferred etc

How it spreads?

It uses EternalBlue MS17-010 to propagate. The ransomware spreads by clicking on links and downloading malicious files over internet and email. It is also capable of automatically spreding itself in a network by means of a vulneability in Windows SMB. It scans the network for specific ports, searches for the vulneability and then exploits it to inject the malware in the new machine and thus it spreads widely across the network. People use Cyber crawling techniques to figure out the most popular websites and try to inject these viruses. Lets assume that one organization has 20 networked computers, if one of the user gets this virus, immediately rest of the users on the network too gets affected.

More than 200,000 victims in over 150 countries fell victim to ransomware called WannaCrypt, also known as WannaCry and Wcry. It affected businesses, governments, and individuals across the globe, particularly those using Windows XP and other unsupported Microsoft operating systems. Healthcare organisations across the UK had systems knocked offline by the ransomware attack, with patient appointments cancelled and NHS England declaring the cyberattack as a 'major incident'. It has affected Health care records, educational institutions etc world wide.

Society For Cyberabad Security Council

What can you do to prevent infection?

- ✓ Microsoft has released a Windows security patch MS17-010 for Winodws machines. This needs to be applied immediately and urgently.
- ✓ Remove Windows NT4, Windows 2000 and Windows XP-2003 from production environments.
- ✓ Block ports 139, 445 and 3389 in firewall.
- ✓ Avoid clicking on links or opening attachments or emails from people you don't know or companies you don't do business with.
- ✓ SMB is enabled by default on Windows. Disable smb service on the machine by going to Settings > uncheck the settings > OK
- ✓ Make sure your software is up-to-date.
- ✓ Have a pop-up blocker running on your web browser.
- ✓ Regularly backup your files.
- ✓ Install a good antivirus and a good anti ransomware product for better security
- ✓ Do not open any attachments with 'tasksche.exe' file
- ✓ Please do not open unsecured websites and open websites which are secured like /https

- Below is a consolidated list that we need to block on you firewall/antivirus

IPs

16.0.5.10:135
16.0.5.10:49
10.132.0.38:80
1.127.169.36:445
1.34.170.174:445
74.192.131.209:445
72.251.38.86:445
154.52.114.185:445
52.119.18.119:445
203.232.172.210:445
95.133.114.179:445
111.21.235.164:445
199.168.188.178:445
102.51.52.149:445
183.221.171.193:445
92.131.160.60:445
139.200.111.109:445
158.7.250.29:445
81.189.128.43:445
143.71.213.16:445
71.191.195.91:445
34.132.112.54:445
189.191.100.197:445
117.85.163.204:445
165.137.211.151:445
3.193.1.89:445
173.41.236.121:445

217.62.147.116:445
16.124.247.16:445
187.248.193.14:445
42.51.104.34:445
76.222.191.53:445
197.231.221.221:9001
128.31.0.39:9191
149.202.160.69:9001
46.101.166.19:9090
91.121.65.179:9001
2.3.69.209:9001
146.0.32.144:9001
50.7.161.218:9001
217.79.179.177:9001
213.61.66.116:9003
212.47.232.237:9001
81.30.158.223:9001
79.172.193.32:443
38.229.72.16:443

Domains:

• iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea[.]com
• Rphjmrpwmfv6v2e[dot]onion
• Gx7ekbenv2riucmf[dot]onion
• 57g7spgrzlojinas[dot]onion
• xxlvbrloxvriy2c5[dot]onion
• 76jdd2ir2embyv47[dot]onion
• cwwnhwhlz52maqm7[dot]onion

File Names:

• @Please_Read_Me@.txt
• @WanaDecryptor@.exe
• @WanaDecryptor@.exe.lnk
• Please Read Me!.txt (Older variant)
• C:\WINDOWS\tasksche.exe
• C:\WINDOWS\qeriuwjhrf
• 131181494299235.bat
• 176641494574290.bat
• 217201494590800.bat
• [0-9]{15}.bat #regex
• !WannaDecryptor!.exe.lnk
• 00000000.pky • 00000000.eky
• 00000000.res
• C:\WINDOWS\system32\taskdl.exe