CYBER-i
Powered By AGC

AGC
Accelerating Business

AGC Networks – Ransomware Threat Advisory

Date: May 14, 2017

AGC Networks – Ransomware Threat Advisory

Malware Summary:

As per the latest update, a huge number of global organisations across a range of sectors in about 104 countries have reported they have been affected by a ransomware attack. India was among the countries worst affected by the Wannacry attack. The attack also includes infections that have disabled more than a dozen hospitals in UK, Spain's largest telecom company, universities in Italy, some Fedx computers and countries including Russia & China.

The malware named "Wannadecryptor" or "Wannacry" or "WCRY" is using vulnerability in Microsoft Windows to encrypt data either on servers or PCs. The objective of the malware is to hold data either on servers or workstations at ransom under the threat of deletion, if required payment in bitcoin is not made.

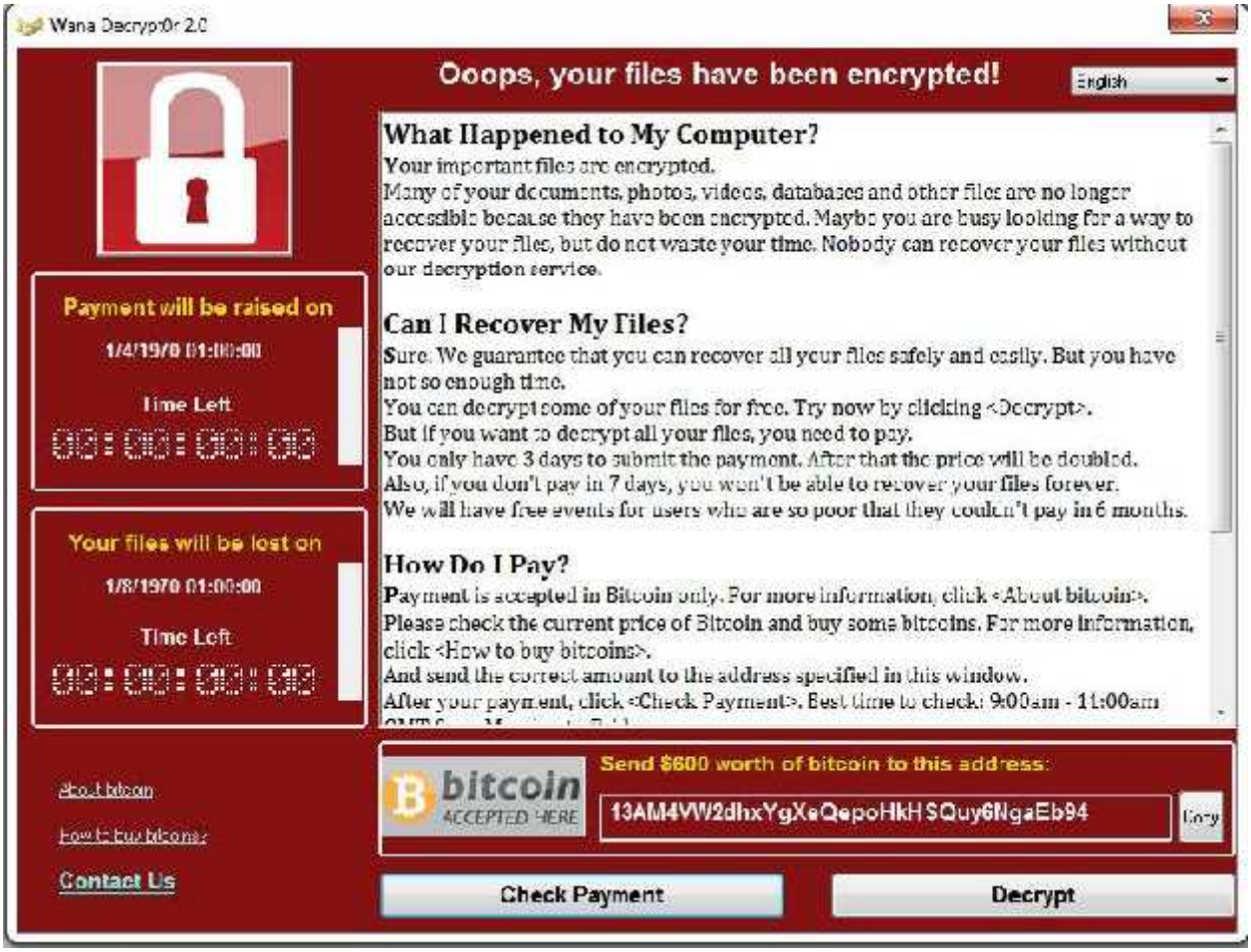
The self-scanning nature of this very aggressive virus enables it to spread widely, one infected asses can threaten entire enterprise.

Impact:

Major Disruption of Service/Operations, Degradation of Service, Financial Loss, Data Loss

WannaCryencrypts files with the following extensions, appending .WCRY to the end of the file name:

The file extensions that the malware is targeting contain certain clusters of formats including:
•Commonly used office file extensions (.ppt, .doc, .docx, .xlsx, .sxi).
•Less common and nation-specific office formats (.sxw, .odt, .hwp).
•Archives, media files (.zip, .rar, .tar, .bz2, .mp4, .mkv)
•Emails and email databases (.eml, .msg, .ost, .pst, .edb).
•Database files (.sql, .accdb, .mdb, .dbf, .odb, .myd).
•Developers' sourcecodeand project files (.php, .java, .cpp, .pas, .asm).
•Encryption keys and certificates (.key, .pfx, .pem, .p12, .csr, .gpg, .aes).
•Graphic designers, artists and photographers files (.vsd, .odg, .raw, .nef, .svg, .psd).
•Virtual machine files (.vmx, .vmdk, .vdi).The WannaCrydropper drops multiple "user manuals" on different languages:*Bulgarian, Chinese (simplified), Chinese (traditional), Croatian, Czech, Danish, Dutch, English, Filipino, Finnish, French, German, Greek, Indonesian, Italian, Japanese, Korean, Latvian, Norwegian, Polish, Portuguese, Romanian, Russian, Slovak, Spanish, Swedish, Turkish, Vietnamese*



Symantec and Norton customers:

Ransom.CryptXXX; Trojan.Gen.8!Cloud; Trojan.Gen.2; Ransom.Wannacry
Intrusion Prevention System Identifications.
21179 (OS Attack: Microsoft Windows SMB Remote Code Execution 3)
23737 (Attack: ShellcodeDownload Activity)
30018 (OS Attack: MSRPC Remote Management Interface Bind)
23624 (OS Attack: Microsoft Windows SMB Remote Code Execution 2)
23862 (OS Attack: Microsoft Windows SMB Remote Code Execution)
30010 (OS Attack: Microsoft Windows SMB RCE CVE-2017-0144)
22534 (System Infected: Malicious Payload Activity 9)
23875 (OS Attack: Microsoft SMB MS17-010 Disclosure Attempt)
29064 (System Infected: Ransom.Ransom32 Activity)
Symantec Security Response has released the certified SEP AV & IPS definitions which cover the WannaCryRansomware.
AV: 5/12/2017 rev. 9IPS: 5/12/2017 rev.11 As cautionary note, considering Liveupdateschedule is less frequent, I would suggest to manually initiate Liveupdateon the SEPM to download the definition. Although Symantec Blog link I shared earlier mentions this, but please note apart from updating the SEP signatures to the latest, please also apply the Microsoft Patches immediately. Primarily patches related to Microsoft Windows SMB. Organizations should also ensure that they have the latest Windows security updates installed, in particular MS17-010 to prevent spreading

McAfee Observations:

By using command-line commands, the Volume Shadow copies and backups are removed:
Cmd/c vssadmindelete shadows /all /quiet & wmicshadowcopydelete & bcdedit/set {default} bootstatuspolicyignoreallfailures& bcdedit/set {default} recovery enabled no & wbadmindelete catalog -quiet
File-size of the ransomwareis 3.4 MB (3514368 bytes)
Authors called the ransomware"WANNACRY" –string hardcoded in samples.
McAfee NSP coverage for WannaCryRansomware:Existing signatures:
0x43c0b800-NETBIOS-SS: Windows SMBv1 identical MID and FID type confusion vulnerability (CVE-2017-0143)
0x43c0b400-NETBIOS-SS: Windows SMB Remote Code Execution Vulnerability (CVE-2017-0144)
0x43c0b500-NETBIOS-SS: Windows SMB Remote Code Execution Vulnerability (CVE-2017-0145)
0x43c0b300-NETBIOS-SS: Microsoft Windows SMB Out of bound Write Vulnerability (CVE-2017-0146)
0x43c0b900-NETBIOS-SS: Windows SMBv1 information disclosure vulnerability (CVE-2017-0147)

Immediate Pre-cautionary Measures Recommended:

- **Microsoft Patch Management:**
  - Verify the March-17 deployment patches (MS17-010, MS17-012) to address CVE-2017-0143 vulnerability
  - Disable SMBv1 and blocking TCP 445, TCP 139, and UDP 137-138 ports at the network level.
  - Patch the Windows XP / Windows 2003 Server with Microsoft latest released patches.

- **End Point Protection:**
  - Block a series of hash values on immediate basis.
  - Block specific list of file types with execution path needs to avoid malware penetration on the endpoints.
  - Please refer the details as mentioned separately under Technical details

- **Email Security Gateway:**
  - Block a specific list of attachments on immediate basis to prevent malware infected email attachments.
  - Please refer the details as mentioned separately under Technical details

- **Web Security Gateway:**
  - Block a series of URL, Domains, and Hostnames that are most vulnerable.
  - Block the "Miscellaneous" category websites temporarily for all users (Any urgent requirement to access genuine site that may be falling under Miscellaneous category can be allowed post verification)
  - Please refer the details as mentioned separately under Technical details

- **Perimeter Security – Next Gen Firewalls**
  - Block the specific list of IPV4 addresses and Domains to prevent malware at the perimeter level.
  - Please refer the details as mentioned separately under Technical details

- **Anti-APT / Sandboxing Solution**
  - All signatures should be updated, verify the logs to trace the possible infection.
  - Keep the Anti-APT / Sandboxing solution in the IN-Line mode of the Email Security Gateway / Mail Servers with quarantine policies on suspected emails and attachments.

- **SIEM**
  - Monitor the logs diligently and verify the IOCs (Indicators of Compromise) that are detected in last 10 days logs.

Technical Details / IOCs

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
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

File Types & Execution Path

- @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

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
URL	http://146.0.32.144:9001
	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

Additional IP Addresses & URLs with ports to be blocked

62.138.10.60:9001
82.94.251.227:443
213.239.216.222:443
51.255.41.65:9001
86.59.21.38:443
198.199.64.217:443
83.169.6.12:9001
192.42.115.102:9004
104.131.84.119:443
178.254.44.135:9001
163.172.25.118:22

- 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
- iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea[.]com (sinkholed)
- Rphjmrpwmfv6v2e[.]onion

- Gx7ekbenv2riucmf[.]onion
- 57g7spgrzlojinas[.]onion
- xxlvbrloxvriy2c5[.]onion
- 76jdd2ir2embyv47[.]onion
- cwwnhwhlz52maqm7[.]onion

Precautions to Remember:

•#ISC threat level raised to Yellow as #WannaCryransom ware hit the internet .. please do follow to avoid getting infected Apply MS17-010 patches ASAP.

•Ensure all critical systems are fully backed upCheckfirewall ports 445/137-139 and 3389,

•Block inbound, Disable SMB v1.

•New ransomwarevariants appear on a regular basis. Always keep your security software up to date to protect yourself against them.

•Keep your operating system and other software updated. Software updates will frequently include patches for newly discovered security vulnerabilities that could be exploited by ransomwareattackers.

•Email is one of the main infection methods. Be wary of unexpected emailsespecially if they contain links and/or attachments.

•Be extremely wary of any Microsoft Office email attachment that advises you to enable macros to view its content. Unless you are absolutely sure that this is a genuine email from a trusted source, do not enable macros and instead immediately delete the email.

•Backing up important data is the single most effective way of combating ransomwareinfection. Attackers have leverage over their victims by encrypting valuable files and leaving them inaccessible. If the victim has backup copies, they can restore their files once the infection has been cleaned up. However organizations should ensure that back-ups are appropriately protected or stored off-line so that attackers can't delete them.

Disclaimer

- The Threat Report with specific advisories are for information purpose only. We recommend you to act upon these advisories in post conducting risk analysis in your specific environment.
- These advisories should be acted upon at your own discretion.
-