OSPREY SECURITY

TECHNICAL ADVISORY

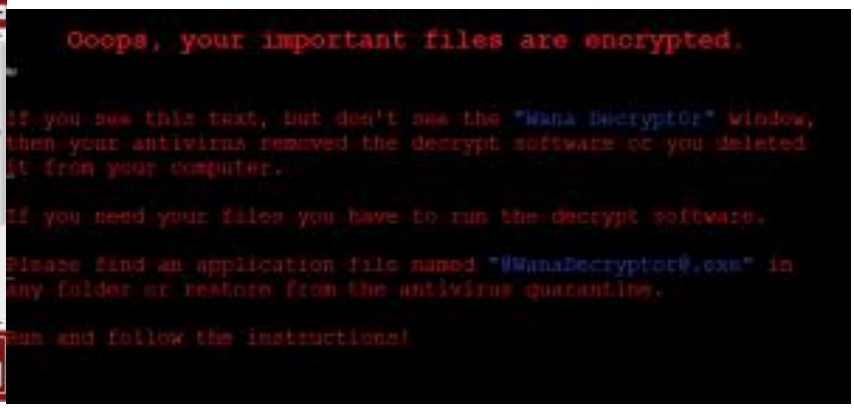
THIS ADVISORY POST IS A DETAILED TECHNICAL OVERVIEW OF THE WANNACRY RANSOMWARE ATTACK AND HOW ENDPOINT INTELLIGENCE PLATFORM CUSTOMERS ARE PROTECTED.

BACKGROUND

On May 12th, 2017, at approximately 7:30am Pacific Time, the Osprey Security Threat Research team was made aware of a large scale cyberattack spreading globally with over 190,000 infections detected in over 150 countries at the time of the publication of this security advisory. This malware has been identified as WannaCry (WCry 2 or WanaCry or WanaCrypt0r 2.0) and is a ransomware type of attack. This attack is the first weaponization of the Shadow Brokers dump of NSA exploits for malicious and criminal purpose, and happened in 28 days since the release of the NSA exploits, resulting in a crippling worldwide cyber attack. The SMB vulnerability from the NSA dump that is utilized is called EternalBlue. If successful, the ransomware installs the DoublePulsar backdoor, and was part of the collection of cyber tools and vulnerabilities amassed and developed by the US National Security Agency. WannaCry represents the first global scale cyberattack through a worm not seen since 2008 (Conficker worm).

SHA256:	32f24601153be0885f11d62e0a8a2f0280a2034fc981d8184180c5d3b1b9e8cf
File name:	lhdfrgui.exe
Detection ratio:	22 / 27
Analysis date:	2017-05-16 03:09:03 UTC (3 hours, 36 minutes ago)

WannaCry falls under the classification of Ransomware or more specifically Crypto ransomware. Organizations infected with WannaCry will encrypt the files and other user data and seeks out a ransom in bitcoins (typically USD $300-$600). The WannaCry ransomware has worm like capabilities and uses a known SMB (Server Message Block) vulnerability in the Microsoft Windows operating system. SMB is a protocol that allows for file-sharing over a company network. Once the initial machine is infected, the malware scans for other vulnerable machines in the network, looking for network shares and removable storage devices. It checks for certain file extensions and encrypts them using strong encryption.



This post is a detailed technical overview of this ransomware attack and details how Osprey Security's Endpoint Intelligence Platform customers are protected from this ransomware threat.

Caution: If you wish to do your own malware analysis, the exploit code is available here: https://github.com/RiskSense-Ops/MS17-010

WannaCry Mitigation

The table below provides a list of mitigation techniques for the WannaCry ransomware attack and native capabilities of the Osprey Security Endpoint Intel platform.

Security Control	Control Summary	Osprey Security Protection
Patch the vulnerability Apply patches for MS17-010 from Microsoft. This also includes patches under KB4012598 for end-of-life Microsoft Windows operating systems.	This patch mitigates the exploits revealed by the NSA Shadow Brokers dump.	Native patch-management module that can scan all your endpoints and automatically deploy patches. In this case, customers can verify the presence of these vulnerabilities and track remediation progress over time against MS17-010.
Contain the spread of the ransomware Disable outdated and legacy protocol SMBv1	The exploit takes advantage of vulnerabilities in the SMB protocol in an organization's network. • A quick way to verify that SMBv1 is disabled is through the Windows registry. • HKLM:\SYSTEM\CurrentControlSet\Services\ • LanmanServer\Parameters\SMB1 for value 0 (which will be disabled, 1 is enabled) • Another option is through Powershell. PS Z:\> Disable-WindowsOptionalFeature -Online -FeatureName smb1protocol	Native configuration management module that can monitor or disable specific ports, protocols, processes, and services. In this case, customers can detect all systems that have SMB port open and block it.

	• Also block incoming SMB traffic over port 445. • Additionally, filter and block NetBIOS port 139 from all externally accessible hosts • Filter RDP port 3389 to prevent WannaCry from infecting other devices within that network	
Monitor and block the WannaCry network indicators of compromise. These are listed in the section below.	• These include blocking outbound traffic on port 9001. • Also includes blocking outgoing requests to IP address on ports 80/443 that do not resolve into a domain. • Also, there should be no rationale for a device on your company network to connect to a TOR node. Block all outbound connections to TOR exit nodes. • Sinkhole the kill-switch domains and redirect the following to a webserver in your control. • hxxp://iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com • hxxp://ifferfsodp9ifjaposdfjhgosurijfaewrwergwea.com	Native network security module that leverages machine learning capabilities to scan for outbound traffic on designated ports. This includes lookups on OSINT and other threat feeds like VirusTotal to block malicious and uncategorized URLs and domains. All outbound access to TOR nodes and .onion sites are blocked.
Advanced deception techniques	WannaCry malware has behavior that avoids infecting the same machine twice. It does this by creating a mutex infection marker on that host.	Native Cyber-deception module that can simulate the infection marker that WannaCry uses to determine that it has already infected that endpoint, thus preventing it from running and in-turn triggering the ransomware from encrypting your endpoint.
Deploy the IOCs	Advanced Indicators of Compromise have been developed including hashes.	Native Malware Analysis module scans through every file in the file system and generates a risk score by using its internal malware analysis sandbox and

		through threat intel feeds.

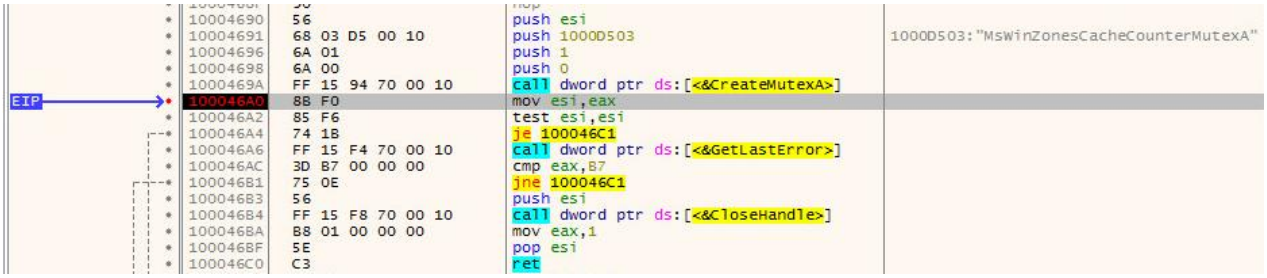


Figure 1: Osprey Security creates fake WannaCry mutex infection markers

WannaCry Detection and Indicators of Compromise

The table below is a quick summary of all the known indicators of compromise for the WannaCry ransomware, how to detect it within your environment, and finally a quick snapshot on how the Osprey Endpoint Intel platform provides security to its customers.

RansomWare Indicator	Malware Technique Summary	Osprey Security Protection
WannaCry Command and Control over the TOR network	The WannaCry ransomware communications are done using the anonymous TOR network	Semi-supervised machine learning models look for variants of TOR gateways and exit nodes and post authorization by the customer, can block outbound network communications to those hosts.
WannaCry ONION sites	The ransomware tries to connect to various .onion sites as part of its infection propagation process	The network security module can listen in, monitor, and when authorized block all outbound network communications to the dark web incl. onion sites.

WannaCry Command & Control TOR Network

The following is the list of TOR gateway nodes that the WannaCry ransomware tries to establish connections to. All Command and Control of the malware post infection is done by utilizing these TOR nodes. Osprey Security recommends that the following IP addresses be blocked for any outbound network communications. Also, monitor for all traffic originating over port 9001. Detect and block access on IP addresses communicating over ports 80/443 and that do not resolve in a domain. The following list below has been sourced from various security partners and leaders incl. McAfee, IBM XForce, Cisco Talos, and Payload Security sandbox.

18.82.1.29:9001
37.187.22.87:9001
38.229.72.16
50.7.151.47:443
50.7.161.218:9001
51.255.41.65:9001
62.138.7.231:9001
62.138.10.60:9001
79.172.193.32
81.30.158.223
82.94.251.227:443
83.162.202.182:9001
83.169.6.12:9001
86.59.21.38:443
89.39.67.33:443
89.45.235.21
94.23.173.93:443
104.131.84.119:443
128.31.0.39:9101
136.243.176.148:443
146.0.32.144:9001
163.172.25.118:22
163.172.129.29:9001
163.172.153.12:9001
163.172.185.132:443
171.25.193.9:80
178.62.173.203:9001
178.254.44.135:9001
185.97.32.18:9001
188.138.33.220
188.166.23.127:443
192.42.115.102:9004
193.22.244.244:443
194.109.206.212:443
195.154.164.243:443

198.199.64.217:443
212.47.232.237
213.61.66.116:9003
213.239.216.222:443

WannaCry ONION Sites

The Onion sites are part of the TOR network and typically constitutes the dark web of the Internet. The WannaCry ransomware tries to connect to various .onion sites which are listed below.

iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea[.]com (sinkholed)
gx7ekbenv2riucmf.onion
57g7spgrzlojinas.onion
Xxlvbrloxvriy2c5.onion
76jdd2ir2embyv47.onion
cwwnhwhlz52maqm7.onion
sqjolphimrr7jqw6.onion

WannaCry File Names

- d5e0e8694ddc0548d8e6b87c83d50f4ab85c1debadb106d6a6a794c3e746f4fa b.wnry
- 055c7760512c98c8d51e4427227fe2a7ea3b34ee63178fe78631fa8aa6d15622 c.wnry
- 402751fa49e0cb68fe052cb3db87b05e71c1d950984d339940cf6b29409f2a7c r.wnry
- e18fdd912dfe5b45776e68d578c3af3547886cf1353d7086c8bee037436dff4b s.wnry
- 4a468603fdcb7a2eb5770705898cf9ef37aade532a7964642ecd705a74794b79 taskdl.exe
- 2ca2d550e603d74dedda03156023135b38da3630cb014e3d00b1263358c5f00d taskse.exe
- 97ebce49b14c46bebc9ec2448d00e1e397123b256e2be9eba5140688e7bc0ae6 t.wnry
- b9c5d4339809e0ad9a00d4d3dd26fdf44a32819a54abf846bb9b560d81391c25 u.wnry

WannaCry Hashes / IOCs

The following is a list of file hashes that are associated with for the WannaCry ransomware. This IOC has been developed working with trusted partners like US CERT team.

Filename	MD5	SHA1	SHA256
qeriuwjhrf	3175E4BA26E1E75E52935009A526002C	5D68E2779E2CCCEE49188363BE6CDDBB0BAC7053	7E369022DA51937781B3EFE6C57F824F05CF43CBD66B4A24367A19488D2939E4

mssecsvc.exe	31DAB68B11824153B4C975399DF0354F	14249E7FB3FB6F4B363C47D5AAE9F46DAB2083C1	9B60C622546DC45CCA64DF935B71C26DCF4886D6FA811944DBC4E23DB9335640
cliconfg.exe	4FEF5E34143E646DBF9907C4374276F5	47A9AD4125B6BD7C55E4E7DA251E23F089407B8F	4A468603FDCB7A2EB5770705898CF9EF37AADE532A7964642ECD705A74794B79
diskpart.exe	509C41EC97BB81B0567B059AA2F50FE8	87420A2791D18DAD3F18BE436045280A4CC16FC4	09A46B3E1BE080745A6D8D88D6B5BD351B1C7586AE0DC94D0C238EE36421CAFA
lhdfrgui.exe	5BEF35496FCBDBE841C82F4D1AB8B7C2	50049556B3406E07347411767D6D01A704B6FEE6	4186675CB6706F9D51167FB0F14CD3F8FCFB0065093F62B10A15F7D9A6C8D982
b9c5d4339809e0ad9a00d4d3dd26fdf44a32819a54abf846bb9b560d81391c25	775A0631FB8229B2AA3D7621427085AD	8286354A6A051704DEC39993AF4E127D317F6974	00FDB4C1C49AEF198F37B8061EB585B8F9A4D5E6C62251441831FE2F6A0A25B7
b9c5.bin	7BF2B57F2A205768755C07F238FB32CC	45356A9DD616ED7161A3B9192E2F318D0AB5AD10	B9C5D4339809E0AD9A00D4D3DD26FDF44A32819A54ABF846BB9B560D81391C25
2584E1521065E45EC3C17767C065429038FC6291C091097EA8B22C8A502C41DD.dat	7F7CCAA16FB15EB1C7399D422F8363E8	BD44D0AB543BF814D93B719C24E90D8DD7111234	2584E1521065E45EC3C17767C065429038FC6291C091097EA8B22C8A502C41DD
waitfor.exe	8495400F199AC77853C53B5A3F278F3E	BE5D6279874DA315E3080B06083757AAD9B32C23	2CA2D550E603D74DEDDA03156023135B38DA3630CB014E3D00B1263358C5F00D
tasksche.exe	84C82835A5D21BBCF75A61706D8AB549	5FF465AFAABCBF0150D1A3AB2C2E74F3A4426467	ED01EBFBC9EB5BBEA545AF4D01BF5F1071661840480439C6E5BABE8E080E41AA
diskpart.exe	86721E64FFBD69AA6944B9672BCABB6D	8897C658C0373BE54EEAC23BBD4264687A141AE1	C365DDAA345CFCAFF3D629505572A484CFF5221933D68E4A52130B8BB7BADAF9
8dd63adb68ef053e044a5a2f46e0d2cd.virus	8DD63ADB68EF053E044A5A2F46E0D2CD	1BC604573CEAB106E5A0E9C419ADE38739228707	201F42080E1C989774D05D5B127A8CD4B4781F1956B78DF7C01112436C89B2C9
Message	B0AD5902366F860F85B892867E5B1E87	A52E025D579BEBAE7C64CB40236B469B3C376024	CA29DE1DC8817868C93E54B09F557FE14E40083C0955294DF5BD91F52BA469C8
kbdlv (3.13)	B675498639429B85AF9D70BE1E8A8782	B8B49A36A52ABCF537FEBCBF2D09497BEE799987D	7108D6793A003695EE8107401CFB17AF305FA82FF6C16B7A5DB45F15E5C9E12D
ransomware07_no_detection.exe	D6114BA5F10AD67A4131AB72531F02DA	A1818054B40EC9E28BEBE518ECC92F4ECEAFFEF4	7C465EA7BCCCF4F94147ADD808F24629644BE11C0BA4823F16E8C19E0090F0FF
mssecsvc.exe	DB349B97C37D22F5EA1D1841E3C89EB4	E889544AFF85FFAF8B0D0DA705105DEE7C97FE26	24D004A104D4D54034DBCFFC2A4B19A11F39008A575AA614EA04703480B1022C
Message	E372D07207B4DA75B3434584CD9F3450	F3839C1CDE9CE18021194573FDF0CAE09A62172F	4B76E54DE0243274F97430B26624C44694FBDE3289ED81A160E0754AB9F56F32
mssecsvc.exe	F107A717F76F4F910AE9CB4DC5290594	51E4307093F8CA8854359C0AC882DDCA427A813C	F8812F1DEB8001F3B7672B6FC85640ECB123BC2304B563728E6235CCBE782D85
taskhcst.eee	F529F4556A5126BBA499C26D67892240	FB18818FC383330B401FC5B332CC63A5BBD4CD30	DFF26A9A44BAA3CE109B8DF41AE0A301D9E4A28AD7BD7721BBB7CCD137BFD696
WCry_WannaCry_ransomware.exe	4DA1F312A214C07143ABEEAFB695D904	B629F072C9241FD2451F1CBCA2290197E72A8F5E	AEE20F9188A5C3954623583C6B0E6623EC90D5CD3FDEC4E1001646E27664002C

localfile~	DB349B97C37D22F5EA1D1841E3C89EB4	E889544AFF85FFAF8B0D0DA705105DEE7C97FE26	24D004A104D4D54034DBCFFC2A4B19A11F39008A575AA614EA04703480B1022C
taskhcst.exe	3BC855BFADFEA71A445080BA72B26C1C	BC978DB3D2DC20B1A305D294A504BB0CEB83F95A	043E0D0D8B8CDA56851F5B853F244F677BD1FD50F869075EF7BA1110771F70C2
findstr	B9B3965D1B218C63CD317AC33EDCB942	02408BB6DC1F3605A7D3F9BAD687A858EC147896	5D26835BE2CF4F08F2BEEFF301C06D05035D0A9EC3AFACC71DFF22813595C0B9
dvdplay	5C7FB0927DB37372DA25F270708103A2	120ED9279D85CBFA56E5B7779FFA7162074F7A29	BE22645C61949AD6A077373A7D6CD85E3FAE44315632F161ADC4C99D5A8E6844
Cmd.Exe	66DDBD108B0C347550F18BB953E1831D	432C1A5353BAB4DBA67EA620EA6C1A3095C5D4FA	F7C7B5E4B051EA5BD0017803F40AF13BED224C4B0FD60B890B6784DF5BD63494
taskhcst.exe1	B6DED2B8FE83BE35341936E34AA433E5	64B8E679727E99A369A2BE3ED800F7B969D43AA8	FC626FE1E0F4D77B34851A8C60CDD11172472DA3B9325BFE288AC8342F6C710A
diskpart.exe	509C41EC97BB81B0567B059AA2F50FE8	87420A2791D18DAD3F18BE436045280A4CC16FC4	09A46B3E1BE080745A6D8D88D6B5BD351B1C7586AE0DC94D0C238EE36421CAFA
WCry_WannaCry_ransomware.exe	4DA1F312A214C07143ABEEAFB695D904	B629F072C9241FD2451F1CBCA2290197E72A8F5E	AEE20F9188A5C3954623583C6B0E6623EC90D5CD3FDEC4E1001646E27664002C
diskpart.exe	86721E64FFBD69AA6944B9672BCABB6D	8897C658C0373BE54EEAC23BBD4264687A141AE1	C365DDAA345CFCAFF3D629505572A484CFF5221933D68E4A52130B8BB7BADAF9

Filename Extensions Encrypted by WannaCry Ransomware

.der, .pfx, .key, .crt, .csr, .p12, .pem, .odt, .sxw, .stw, .3ds,
.max, .3dm, .ods, .sxc, .stc, .dif, .slk, .wb2, .odp, .sxd, .std,
.sxm, .sqlite3, .sqlitedb, .sql, .accdb, .mdb, .dbf, .odb, .mdf,
.ldf, .cpp, .pas, .asm, .cmd, .bat, .vbs, .sch, .jsp, .php, .asp,
.java, .jar, .class, .mp3, .wav, .swf, .fla, .wmv, .mpg, .vob,
.mpeg, .asf, .avi, .mov, .mp4, .mkv, .flv, .wma, .mid, .m3u,
.m4u, .svg, .psd, .tiff, .tif, .raw, .gif, .png, .bmp, .jpg,
.jpeg, .iso, .backup, .zip, .rar, .tgz, .tar, .bak, .ARC, .vmdk,
.vdi, .sldm, .sldx, .sti, .sxi, .dwg, .pdf, .wk1, .wks, .rtf,
.csv, .txt, .msg, .pst, .ppsx, .ppsm, .pps, .pot, .pptm, .pptx,
.ppt, .xltm, .xltx, .xlc, .xlm, .xlt, .xlw, .xlsb, .xlsm,
.xlsx, .xls, .dotm, .dot, .docm, .docx, .doc