INDICATORS OF COMPROMISE FOR WANNACRY

Yara Signatures for Wannacry:

```
rule Wanna_Cry_Ransomware_Generic {

        meta:

                description = "Detects WannaCry Ransomware on Disk and in Virtual
        Page"

                author = "US-CERT Code Analysis Team"

                reference = "not set"

                date = "2017/05/12"

        hash0 = "4DA1F312A214C07143ABEEAFB695D904"

        strings:

                $s0 = {410044004D0049004E0024}

                $s1 = "WannaDecryptor"

                $s2 = "WANNACRY"

                $s3 = "Microsoft Enhanced RSA and AES Cryptographic"

                $s4 = "PKS"

                $s5 = "StartTask"

                $s6 = "wcry@123"

                $s7 = {2F6600002F72}

                $s8 = "unzip 0.15 Copyrigh"

                $s9 = "Global\\WINDOWS_TASKOSHT_MUTEX"

                $s10 = "Global\\WINDOWS_TASKCST_MUTEX"

                $s11 =
        {7461736B736368652E6578650000000054617361274000000742E776
        E7279000069636163}
```

```
        $s12 = {6C73202E202F6772616E742045766572796F6E653A46202F54202F43202F51006174747269622202B68}

        $s13 = "WNcry@2ol7"

        $s14 = "wcry@123"

        $s15 = "Global\\MsWinZonesCacheCounterMutexA"

    condition:

        $s0 and $s1 and $s2 and $s3 or $s4 and $s5 and $s6 and $s7 or $s8 and $s9 and $s10 or $s11 and $s12 or $s13 or $s14 or $s15

}

/*The following Yara ruleset is under the GNU-GPLv2 license (http://www.gnu.org/licenses/gpl-2.0.html) and open to any user or organization, as long as you use it under this license.*/

rule MS17_010_WanaCry_worm {

    meta:

        description = "Worm exploiting MS17-010 and dropping WannaCry Ransomware"

        author = "Felipe Molina (@felmoltor)"

        reference = "https://www.exploit-db.com/exploits/41987/"

        date = "2017/05/12"

    strings:

        $ms17010_str1="PC NETWORK PROGRAM 1.0"

        $ms17010_str2="LANMAN1.0"

        $ms17010_str3="Windows for Workgroups 3.1a"

        $ms17010_str4="__TREEID__PLACEHOLDER__"

        $ms17010_str5="__USERID__PLACEHOLDER__"
```

```
        $wannacry_payload_substr1 = "h6agLCqPqVyXi2VSQ8O6Yb9ijBX54j"

        $wannacry_payload_substr2 = "h54WfF9cGigWFEx92bzmOd0UOaZlM"

        $wannacry_payload_substr3 = "tpGFEoLOU6+5I78Toh/nHs/RAP"

    condition:

        all of them

}
```

IP Addresses and Domains

IPv4 197(.)231.221.211

IPv4 128(.)31.0.39

IPv4 149(.)202.160.69

IPv4 46(.)101.166.19

IPv4 91(.)121.65.179

URL hxxp://www(.)btcfrog(.)com/qr/bitcoinpng(.)php?address

URL hxxp://www(.)rentasyventas(.)com/incluir/rk/imagenes(.)html

URL hxxp://www(.)rentasyventas(.)com/incluir/rk/imagenes(.)html?retencion=081525418

URL hxxp://gx7ekbenv2riucmf(.)onion

URL hxxp://57g7spgrzlojinas(.)onion

URL hxxp://xxlvbrloxvriy2c5(.)onion

URL hxxp://76jdd2ir2embyv47(.)onion

URL hxxp://cwwnhwhlz52maqm7(.)onion

URL hxxp://197.231.221(.)211 Port:9001

URL hxxp://128.31.0(.)39 Port:9191

URL hxxp://149.202.160(.)69 Port:9001

URL hxxp://46.101.166(.)19 Port:9090

URL hxxp://91.121.65(.)179 Port:9001

Hashes

Hash-MD5	5a89aac6c8259abbba2fa2ad3fcefc6e
Hash-MD5	05da32043b1e3a147de634c550f1954d
Hash-MD5	8e97637474ab77441ae5add3f3325753
Hash-MD5	c9ede1054fef33720f9fa97f5e8abe49
Hash-MD5	f9cee5e75b7f1298aece9145ea80a1d2
Hash-MD5	638f9235d038a0a001d5ea7f5c5dc4ae
Hash-MD5	80a2af99fd990567869e9cf4039edf73
Hash-MD5	c39ed6f52aaa31ae0301c591802da24b
Hash-MD5	db349b97c37d22f5ea1d1841e3c89eb4
Hash-MD5	f9992dfb56a9c6c20eb727e6a26b0172
Hash-MD5	46d140a0eb13582852b5f778bb20cf0e
Hash-MD5	5bef35496fcbdbe841c82f4d1ab8b7c2
Hash-MD5	3c6375f586a49fc12a4de9328174f0c1
Hash-MD5	246c2781b88f58bc6b0da24ec71dd028
Hash-MD5	b7f7ad4970506e8547e0f493c80ba441
Hash-MD5	2b4e8612d9f8cdcf520a8b2e42779ffa
Hash-MD5	c61256583c6569ac13a136bfd440ca09
Hash-MD5	31dab68b11824153b4c975399df0354f
Hash-MD5	54a116ff80df6e6031059fc3036464df
Hash-MD5	d6114ba5f10ad67a4131ab72531f02da
Hash-MD5	05a00c320754934782ec5dec1d5c0476
Hash-MD5	f107a717f76f4f910ae9cb4dc5290594
Hash-MD5	7f7ccaa16fb15eb1c7399d422f8363e8
Hash-MD5	84c82835a5d21bbcf75a61706d8ab549
Hash-MD5	bec0b7aff4b107edd5b9276721137651
Hash-MD5	86721e64ffbd69aa6944b9672bcabb6d

Hash-MD5	509c41ec97bb81b0567b059aa2f50fe8
Hash-MD5	8db349b97c37d22f5ea1d1841e3c89eb
Hash-SHA1	6fbb0aabe992b3bda8a9b1ecd68ea13b668f232e
Hash-SHA256	0a73291ab5607aef7db23863cf8e72f55bcb3c273bb47f00edf011515aeb5894
Hash-SHA256	21ed253b796f63b9e95b4e426a82303dfac5bf8062bfe669995bde2208b360fd
Hash-SHA256	228780c8cff9044b2e48f0e92163bd78cc6df37839fe70a54ed631d3b6d826d5
Hash-SHA256	2372862afaa8e8720bc46f93cb27a9b12646a7cbc952cc732b8f5df7aebb2450
Hash-SHA256	2ca2d550e603d74dedda03156023135b38da3630cb014e3d00b1263358c5f00d
Hash-SHA256	3ecc7b1ee872b45b534c9132c72d3523d2a1576ffd5763fd3c23afa79cf1f5f9
Hash-SHA256	43d1ef55c9d33472a5532de5bbe814fefa5205297653201c30fdc91b8f21a0ed
Hash-SHA256	49fa2e0131340da29c564d25779c0cafb550da549fae65880a6b22d45ea2067f
Hash-SHA256	4a468603fdcb7a2eb5770705898cf9ef37aade532a7964642ecd705a74794b79
Hash-SHA256	616e60f031b6e7c4f99c216d120e8b38763b3fafd9ac4387ed0533b15df23420
Hash-SHA256	66334f10cb494b2d58219fa6d1c683f2dbcfc1fb0af9d1e75d49a67e5d057fc5
Hash-SHA256	8b52f88f50a6a254280a0023cf4dc289bd82c441e648613c0c2bb9a618223604
Hash-SHA256	8c3a91694ae0fc87074db6b3e684c586e801f4faed459587dcc6274e006422a4
Hash-SHA256	aae9536875784fe6e55357900519f97fee0a56d6780860779a36f06765243d56
Hash-SHA256	b9c5d4339809e0ad9a00d4d3dd26fdf44a32819a54abf846bb9b560d81391c25
Hash-SHA256	ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa

Hash-SHA256	f7c7b5e4b051ea5bd0017803f40af13bed224c4b0fd60b890b6784df5bd63494
Hash-SHA256	09a46b3e1be080745a6d8d88d6b5bd351b1c7586ae0dc94d0c238ee36421cafa
Hash-SHA256	149601e15002f78866ab73033eb8577f11bd489a4cea87b10c52a70fdf78d9ff
Hash-SHA256	190d9c3e071a38cb26211bfffeb6c4bb88bd74c6bf99db9bb1f084c6a7e1df4e
Hash-SHA256	24d004a104d4d54034dbcffc2a4b19a11f39008a575aa614ea04703480b1022c
Hash-SHA256	2584e1521065e45ec3c17767c065429038fc6291c091097ea8b22c8a502c41dd
Hash-SHA256	4186675cb6706f9d51167fb0f14cd3f8fcfb0065093f62b10a15f7d9a6c8d982
Hash-SHA256	593bbcc8f34047da9960b8456094c0eaf69caaf16f1626b813484207df8bd8af
Hash-SHA256	5ad4efd90dcde01d26cc6f32f7ce3ce0b4d4951d4b94a19aa097341aff2acaec
Hash-SHA256	7c465ea7bcccf4f94147add808f24629644be11c0ba4823f16e8c19e0090f0ff
Hash-SHA256	9b60c622546dc45cca64df935b71c26dcf4886d6fa811944dbc4e23db9335640
Hash-SHA256	9fb39f162c1e1eb55fbf38e670d5e329d84542d3dfcdc341a99f5d07c4b50977
Hash-SHA256	b47e281bfbeeb0758f8c625bed5c5a0d27ee8e0065ceeadd76b0010d226206f0
Hash-SHA256	b66db13d17ae8bcaf586180e3dcd1e2e0a084b6bc987ac829bbff18c3be7f8b4
Hash-SHA256	c365ddaa345cfcaff3d629505572a484cff5221933d68e4a52130b8bb7badaf9
Hash-SHA256	d8a9879a99ac7b12e63e6bcae7f965fbf1b63d892a8649ab1d6b08ce711f7127
Hash-SHA256	f8812f1deb8001f3b7672b6fc85640ecb123bc2304b563728e6235ccbe782d85
Hash-SHA256	11d0f63c06263f50b972287b4bbd1abe0089bc993f73d75768b6b41e3d6f6d49

Hash-SHA256	16493ecc4c4bc5746acbe96bd8af001f733114070d694db76ea7b5a0de7ad0ab
Hash-SHA256	6bf1839a7e72a92a2bb18fbedf1873e4892b00ea4b122e48ae80fac5048db1a7
Hash-SHA256	b3c39aeb14425f137b5bd0fd7654f1d6a45c0e8518ef7e209ad63d8dc6d0bac7
Hash-SHA256	e14f1a655d54254d06d51cd23a2fa57b6ffdf371cf6b828ee483b1b1d6d21079
Hash-SHA256	e8450dd6f908b23c9cbd6011fe3d940b24c0420a208d6924e2d920f92c894a96

Sandbox Analysis Reports

https://www.virustotal.com/en/file/dff26a9a44baa3c...
https://www.virustotal.com/en/file/201f42080e1c989...
https://www.virustotal.com/en/file/ed01ebfbc9eb5bb...
https://www.virustotal.com/en/file/c365ddaa345cfca...
https://www.virustotal.com/en/file/4a468603fdcb7a2...
https://www.hybrid-analysis.com/sample/57c12d8573d2f3883a8a0ba14e3eec02ac1c61dee6b675b6c0d16e221c3777f4?environmentId=100
https://www.hybrid-analysis.com/sample/ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa?environmentId=100
https://www.hybrid-analysis.com/sample/b9c5d4339809e0ad9a00d4d3dd26fdf44a32819a54abf846bb9b560d81391c25?environmentId=100

SNORT IDS Rules

alert smb $HOME_NET any -> any any (msg:"ET EXPLOIT Possible ETERNALBLUE MS17-010 Echo Response"; flow:from_server,established; content:"|00 00 00 31 ff|SMB|2b 00 00 00 00 98 07 c0|"; depth:16; fast_pattern; content:"|4a 6c 4a 6d 49 68 43 6c 42 73 72 00|"; distance:0; flowbits:isset,ETPRO.ETERNALBLUE; classtype:trojan-activity; sid:2024218; rev:1;)

alert smb $HOME_NET any -> any any (msg:"ET EXPLOIT Possible ETERNALBLUE MS17-010 Echo Response"; flow:from_server,established; content:"|00 00 00 31 ff|SMB|2b 00 00 00 00 98 07 c0|"; depth:16; fast_pattern; content:"|4a 6c 4a 6d 49 68 43 6c 42 73 72 00|"; distance:0; flowbits:isset,ETPRO.ETERNALBLUE; metadata: former_category EXPLOIT; classtype:trojan-activity; sid:2024218; rev:1;)

alert smb $HOME_NET any -> any any (msg:"ET EXPLOIT Possible ETERNALBLUE MS17-010 Echo Response"; flow:from_server,established; content:"|00 00 00 31 ff|SMB|2b 00 00 00 00 98 07 c0|"; depth:16; fast_pattern; content:"|4a 6c 4a 6d 49 68 43 6c 42 73 72 00|"; distance:0; flowbits:isset,ETPRO.ETERNALBLUE; classtype:trojan-activity; sid:2024218; rev:1;)