Endpoint Protection

View Only

BACK TO LIBRARY

WannaCry: Ransomware attacks show strong links to Lazarus group

28 Recommend

May 22, 2017 06:19 PM

A L Johnson

Tools and infrastructure used in the WannaCry ransomware attacks have strong links to Lazarus, the group that was responsible for the destructive attacks on Sony Pictures and the theft of US$81 million from the Bangladesh Central Bank. Despite the links to Lazarus, the WannaCry attacks do not bear the hallmarks of a nation-state campaign but are more typical of a cybercrime campaign. Our analysis only allows us to attribute these attacks to the Lazarus group. The technical details do not enable us to attribute the motivations of the attacks to a specific nation state or individuals.

Prior to the global outbreak on May 12, an earlier version of WannaCry (Ransom.Wannacry) was used in a small number of targeted attacks in February, March, and April. This earlier version was almost identical to the version used in May 2017, with the only difference the method of propagation. Analysis of these early WannaCry attacks by Symantec's Security Response team revealed substantial commonalities in the tools, techniques, and infrastructure used by the attackers and those seen in previous Lazarus attacks, making it highly likely that Lazarus was behind the spread of WannaCry. These earlier versions of WannaCry used stolen credentials to spread across infected networks, rather than leveraging the leaked Eternal Blue exploit that caused WannaCry to spread quickly across the globe starting on May 12.

Statistics
0 Favorited
0 Views
0 Files
0 Shares
0 Downloads

Summary of links

- Following the first WannaCry attack in February, three pieces of malware linked to Lazarus were discovered on the victim's network: Trojan.Volgmer and two variants of Backdoor.Destover, the disk-wiping tool used in the Sony Pictures attacks.
- Trojan.Alphanc, which was used to spread WannaCry in the March and April attacks, is a modified version of Backdoor.Duuzer, which has previously been linked to Lazarus.
- Trojan.Bravonc used the same IP addresses for command and control as Backdoor.Duuzer and Backdoor.Destover, both of which have been linked to Lazarus.
- Backdoor.Bravonc has similar code obfuscation as WannaCry and Infostealer.Fakepude (which has been linked to Lazarus).
- There is shared code between WannaCry and Backdoor.Contopee, which has previously been linked to Lazarus.

February attack

The first evidence Symantec has seen of WannaCry being used in the wild was February 10, 2017, when a single organization was compromised. Within two minutes of the initial infection, more than 100 computers in the organization were infected.

The attackers left behind several tools on the victim's network that provided substantial evidence into how WannaCry spread. Two files, mks.exe and hptasks.exe (see Appendix C: Indicators of Compromise), were found on one affected computer. The file mks.exe is a variant of Mimikatz (Hacktool.Mimikatz), a password-dumping tool that is widely used in targeted attacks. The latter file, hptasks.exe, was used to then copy and execute WannaCry on other network computers using the passwords stolen by mks.exe.

The spread of WannaCry by hptasks.exe was a two-stage process. In stage one, when run, hptasks can be passed a target list of IP addresses as an argument. When given this command, hptasks reads previously stolen credentials from a file called cg.wry and uses them to connect to every computer in the set of IP address ranges. All connection attempts are logged into the

log.dat file. If a successful connection is made to a remote computer, and there is no file with a .res extension in either the Admin$, or C$\Windows folders, then hptasks.exe will copy the files listed in Table 2 onto the remote computer.

File name	Remote locations	Type
cg.wry	\\%s\Admin$\, \\%s\C$\Windows\ where %s the remote system	Configuration details
r2.wry	\\%s\Admin$\, \\%s\C$\Windows\ where %s the remote system	Message to the user with instructions on how to pay
t1.wry	\\%s\Admin$\, \\%s\C$\Windows\ where %s the remote system	Message to the user, for example "Most of your files are encrypted..."
taskmsgr.exe	\\%s\Admin$\, \\%s\C$\Windows\ where %s the remote system	Application for displaying the messages in t1.wry and t2.wry
taskschs.exe	\\%s\Admin$\, \\%s\C$\Windows\ where %s the remote system	WannaCry encryption application

Table 1. Files copied by hptasks.exe onto target computers

After hptasks.exe executes WannaCry on the remote computer, the second stage begins. hptasks can pass several arguments to the WannaCry installation on the remote computer, including a new set of IP addresses. If WannaCry is run with these IP addresses as arguments, it does not encrypt the files on the local computer. Instead, it connects to the IP addresses passed, accesses the Admin$ and C$ share on those computers using the credentials embedded in the resource section in a file called c.wry, and then remotely encrypts those files.

In addition to hptasks.exe and mks.exe, five other pieces of malware were discovered on a second computer on the victim's network. Three of these tools are linked to Lazarus. Two were variants of Destover (Backdoor.Destover) a tool used in the Sony Pictures attacks. The third was Trojan.Volgmer, malware that has previously been used by Lazarus in attacks against South Korean targets.

March and April attacks

Beginning on March 27, at least five organizations were infected with a new sample of WannaCry. There does not appear to have been a pattern to those targeted, with the organizations spanning a range of sectors and geographies. These attacks revealed further evidence of links between those behind WannaCry and the Lazarus Group.

Two different backdoors were used to deploy WannaCry in these attacks: Trojan.Alphanc and Trojan.Bravonc. Alphanc was used to drop WannaCry onto computers belonging to at least two of the known victims, with a slightly modified version of the malware deployed to each victim.

Alphanc shares a significant amount of code with Backdoor.Duuzer, a sub-family of the Destover wiping tool used in the Sony attacks (see Appendix B: Shared Code). In fact, Symantec investigators believe Alphanc is an evolution of Duuzer. Duuzer has also previously been linked to the activity of Backdoor.Joanap and Trojan.Volgmer, which have both been previously linked to Lazarus.

Symantec researchers were able to establish a detailed timeline of the activity of Alphanc on one of the victim's systems, from the time it got on the system to when WannaCry was deployed.

Timeline of Alphanc activity

Alphanc was deployed on the target computer as armsvc.exe and minutes later copied itself to a new name, javaupdate.exe. The sample executed from this location:

cmd.exe /c "copy c:\Users\Administrator\AppData\armsvc.exe c:\windows\system32\javaupdate.exe > C:\Users\REDACTED\AppData\Local\Temp\NK15DA.tmp" 2>&1

Minutes later, mks.exe, the same credential dumper used in the February WannaCry attacks, was created and executed. There was no activity for three days, until the attackers returned and deployed a version of RAR and created a password-protected archive. Moments later a network scanner called g.exe ran. This performed a DNS lookup for all IP addresses in the IP address range selected by the attackers, probably to determine computers of interest. A two-day gap in activity followed before the attackers returned to profile the local network. Examples of commands used include:

cmd.exe /c "net view > C:\Users\REDACTED\AppData\Local\Temp\NK2301.tmp" 2>&1
cmd.exe /c "net view /domain > C:\Users\REDACTED\AppData\Local\Temp\NK6C42.tmp" 2>&1
cmd.exe /c "time /t > C:\Users\REDACTED\AppData\Local\Temp\NKC74F.tmp" 2>&1

Then, the file taskhcst.exec was created by javaupdate.exe. This was the WannaCry ransomware. The .exec extension is renamed to .exe, as illustrated blow. This was likely a safety check so that the attacker would not mistakenly execute the file prematurely.

cmd.exe /c "ren C:\Windows\taskhcst.exec taskhcst.exe > C:\Users\REDACTED\AppData\Local\Temp\NK833D.tmp" 2>&1

Approximately 45 minutes later, the attacker copied the javaupdate.exe backdoor to a remote computer. A file called bcremote.exe was then also copied to this computer; this was the same tool that was called hptasks.exe in the February attack, and was used to spread WannaCry across the network. The configuration file for this file was then copied, and finally WannaCry itself was copied over:

cmd.exe /c "net use \\REDACTED\ipc$ REDACTED /u:REDACTED > C:\Users\REDACTED\AppData\Local\Temp\NK2E.tmp" 2>&1
cmd.exe /c "copy c:\windows\system32\javaupdate.exe \\REDACTED\c$\windows\javaupdate.exe > C:\Users\REDACTEDAppData\Local\Temp\NK3E49.tmp" 2>&1
cmd.exe /c "copy c:\windows\beremote.exe \\REDACTED\c$\windows\ > C:\Users\REDACTED\AppData\Local\Temp\NK4DD5.tmp" 2>&1
cmd.exe /c "copy c:\windows\c.wry \\REDACTED\c$\windows\ > C:\Users\REDACTED\AppData\Local\Temp\NK7228.tmp" 2>&1
cmd.exe /c "copy c:\windows\taskh.exe \\REDACTED\c$\windows\ > C:\Users\REDACTED\AppData\Local\Temp\NK7DCF.tmp" 2>&1*

The same process took place on a second server on the network, and when the bcremote.exe command was executed, WannaCry was spread across the network.

Trojan.Bravonc

Fewer details are available about the operation of Trojan.Bravonc, but it was used to drop WannaCry onto the computers of at least two other victims, and displays some fairly definitive links to the Lazarus group.

It connects to a command and control (C&C) server at the IP address 87.101.243.252, which is the same IP address used by a sample of Destover, a known Lazarus tool. This IP address was also referenced in Blue Coat's From Seoul To Sony report.

Duuzer has also been observed using this IP address as a C&C server. Bravonc and a variant of Destover also share cryptographic related code (See Appendix B: Shared Code). In addition, Bravonc's method of spreading (over SMB using hardcoded credentials), was the same technique used by Joanap, another Lazarus-linked tool.

May attacks: WannaCry goes global

On May 12, a new version of WannaCry was released which incorporated the leaked "EternalBlue" exploit that used two known vulnerabilities in Windows (CVE-2017-0144 and CVE-2017-0145) to spread the ransomware to unpatched computers on the victim's network and also to other vulnerable computers connected to the internet.

The incorporation of EternalBlue transformed WannaCry from a dangerous threat that could only be used in a limited number of targeted attacks to one of the most virulent strains of malware seen in recent years. It caused widespread disruption, both to organizations infected and to organizations forced to take computers offline for software updates. The discovery and triggering of a kill switch by security blog MalwareTech halted its spread and limited the damage.

The earlier versions of WannaCry and the one used in the May 12 attacks are largely the same, with some minor changes, chiefly the incorporation of the EternalBlue exploit. The passwords used to encrypt the Zip files embedded in the WannaCry dropper are similar across both versions ("wcry@123", "wcry@2016", and "WNcry@2ol7") indicating that the author of both versions is likely the same group.

The small number of Bitcoin wallets used by first version of WannaCry, and its limited spread, indicates that this was not a tool that was shared across cyber crime groups. This provides further evidence that both versions of WannaCry were operated by a single group.

WannaCry links to Lazarus

Aside from commonalities in the tools used to spread WannaCry, there are also a number of links between WannaCry itself and Lazarus. The ransomware shares some code with Backdoor.Contopee, malware that has previously been linked to Lazarus. One variant of Contopee uses a custom SSL implementation, with an identical cipher suite, which is also used by WannaCry. The cipher suite in both samples has the same set of 75 different ciphers to choose from (as opposed to OpenSSL where there are over 300).

In addition, WannaCry uses similar code obfuscation to Infostealer.Fakepude, malware that has previously been linked to Lazarus; and Trojan.Alphanc, malware that was used to spread WannaCry in the March and April attacks and which has been linked to Lazarus (see above).

Fortuitous leak turned WannaCry into global threat

The discovery of a small number of earlier WannaCry attacks has provided compelling evidence of a link to the Lazarus group. These earlier attacks involved significant use of tools, code, and infrastructures previously associated with the Lazarus group, while the means of propagation through backdoors and stolen credentials is consistent with earlier Lazarus attacks. The leak of the EternalBlue exploit was what allowed the attackers to turn WannaCry into a far more potent threat than it would have been had they still been relying on their own tools, since it bypassed many of the steps the attackers previously had to take, removing both the need to steal credentials and copy it from computer to computer.

Thanks to Symantec's Network Protection Research Labs for their contribution to this research.

Appendix A: WannaCry and Lazarus shared network infrastructure

There are a number of crossovers seen in the C&C servers used in the WannaCry campaigns and by other known Lazarus tools. For example, during the attacks against Sony, a malware family called Backdoor.Destover was deployed. Later variants of Backdoor.Destover were seen to use the IP address 87.101.243.252 for command and control. The Trojan.Bravonc sample discovered dropping WannaCry also connects to this IP address. Other shared network infrastructure is listed below:

C&C	Used by	Comments
87.101.243.252	Trojan.Bravonc, Backdoor.Duuzer Backdoor.Destover	
84.92.36.96	Trojan.Alphanc	Also used by a backdoor program which shares an additional C&C with Lazarus-linked Backdoor.Cuprox
184.74.243.67	Trojan.Alphanc	Also seen used by entaskloader.exe which drops a network scanning tool used in March attacks
203.69.210.247	Trojan.Alphanc	
196.45.177.52	Backdoor.Cuprox	Also seen used by a backdoor program dropped by a document called "discussion_QuadrigaCX.doc"

Table 2. Infrastructure shared by WannaCry and other Lazarus tools

Appendix B: Shared Code

Shared network code between Trojan.Alphanc and Backdoor.Duuzer

Trojan.Alphanc and Backdoor.Duuzer use similar code to generate the buffer being sent out after connection to the C&C server is established. This code is part of what could be referred to as a "Fake SSL" handshake. This is similar in concept to the code identified by Google, but different in implementation. Both samples generate a random number, and use that number to lookup a table for additional data to send. That table is identical across both samples. In addition, both samples will prepend the same value, 0x16030100, to the start of the buffer sent to the C&C server.

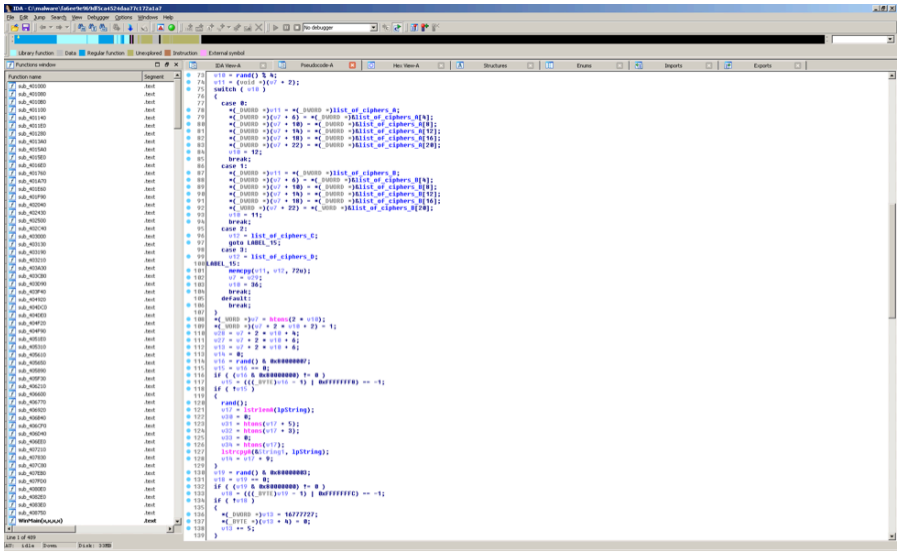

Figure 1. Backdoor.Duuzer sample with the hash fa6ee9e969df5ca4524daa77c172a1a7

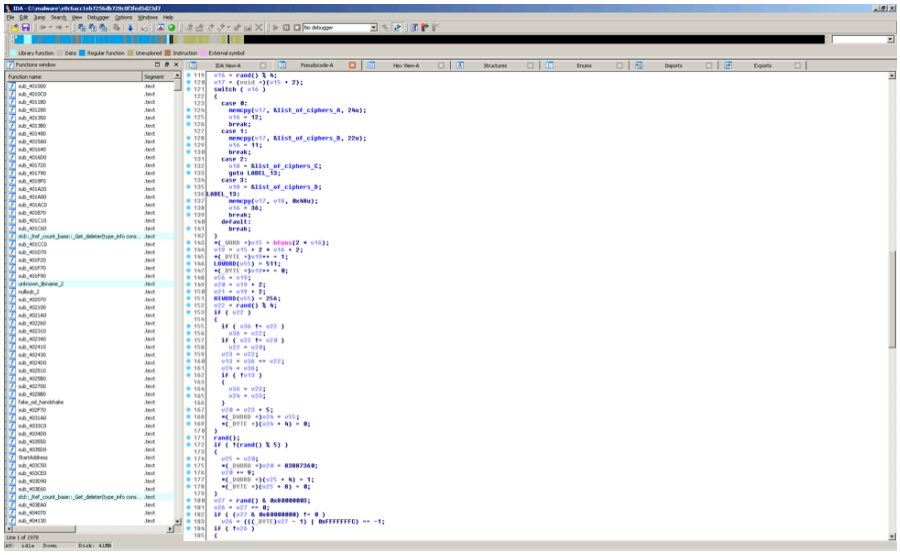

Figure 2. Backdoor Alphanc sample with the hash E8C6ACC1EB7256DB728C0F3FED5D23D7

Common strings between Trojan.Alphanc and Backdoor.Duuzer

The following table demonstrates the common strings between Trojan.Alphanc and Backdoor.Duuzer.

Alphanc 259c82d6db2883dd135c87b0feb44069	Duuzer a7a32b1a01bfc1f3bf769f183eb9fd9e
cm%sx%s"%s %s %s" 2>%s	%sd.e%sc "%s > %s" 2>&1
[system PrOcEss]	[sYsTEM pRocEss]
aAc	aac
ac3	ac3
	amc
aSf	aSf
avi	Avi
cONhosT.exE	cONhOst.exe
Csrss.exe	CsrSs.exe
dllhOst.exe	dllhost.eXe
dWm.exE	dWm.exe
ehrecVr.eXE	ehrecvr.exe
ehsCHed.eXE	ehsched.exe
K3G	K3g
lsass.Exe	Lsass.eXe
lsm.EXe	lsm.exe
m3u	m3u
mid	Mid
midi	miDi
mKv	mkv
mmf	mmf
MOv	MoV
Mp3	mp3
mp4	mp4
mpA	Mpa
mpcmdrun.exe	MpcmdRun.eXE
Mpe	mpE
mpEG	Mpeg
mPg	mpG
msdtc.Exe	mSdtC.exe
Ram	raM
rmvb	rmVb
rundll32.eXE	runDll32.exe
searchindEXeR.eXe	seArcHinDexer.eXE
ServIcEs.exE	serviCes.exE
Skm	skm
smi	smI
smsS.exe	sMss.exe
spOoLsv.eXe	SPooLsv.exe
SpPsvc.exe	sppsVC.exe
sVchost.EXe	svcHosT.exe
sysTEM	SysteM
uSErinit.exe	useriNit.Exe
VoB	vob
wAv	wav
werFaUlt.exE	wErfault.Exe
wIniniT.Exe	winiNit.exe
WinlogOn.exE	WInLOgon.exe
Wma	wma
wmPnetwk.exe	wmpnetwK.exe
wmv	wmv
wudfhost.Exe	wUdFhost.eXe

Figure 3. Common strings between Trojan.Alphanc and Backdoor.Duuzer

Cryptographic number related routines between Backdoor.Bravonc and Backdoor.Destover

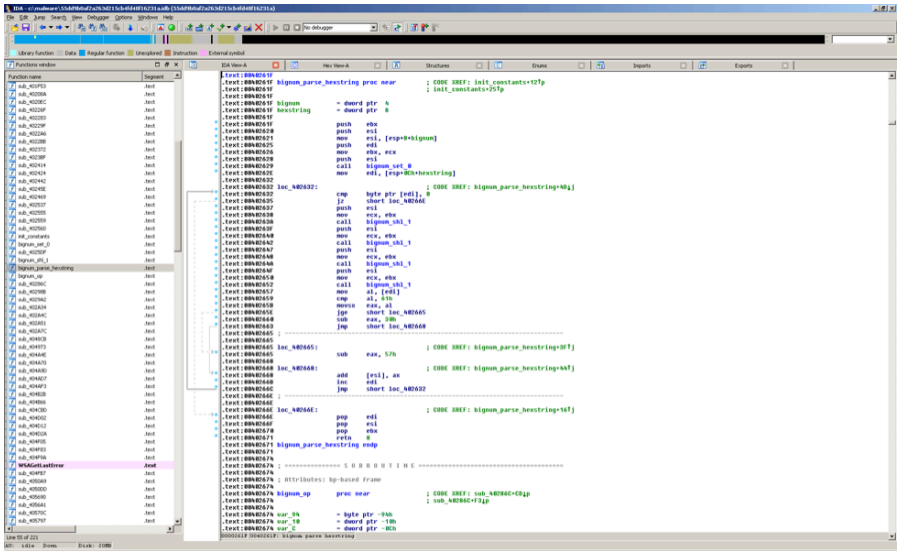

Figure 4. Trojan.Bravonc sample with the hash 55dd9b0af2a263d215cb4fd48f16231a

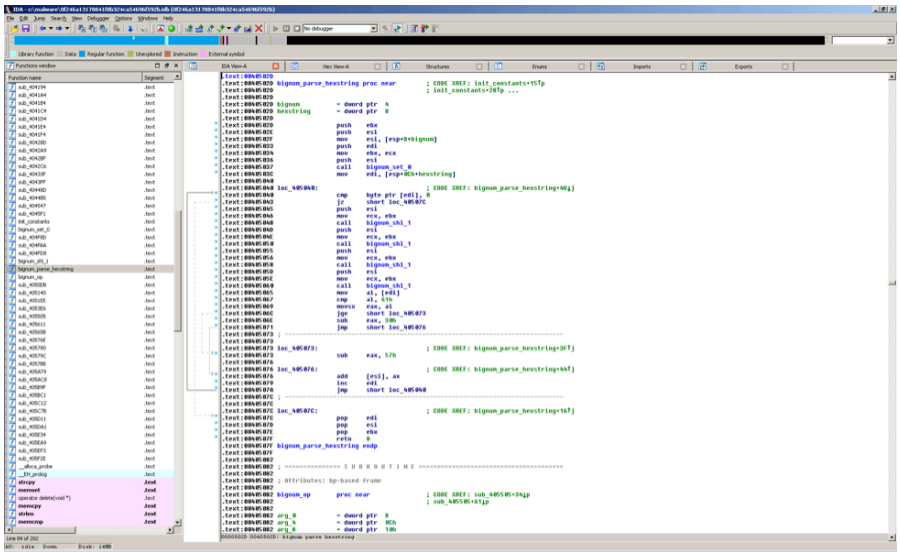

Figure 5. Destover variant with the hash 0f246a13178841f8b324ca54696f592b

Shared function identified by Neel Mehta

On May 15, Google researcher Neel Mehta tweeted the following:

The first hash, 9c7c7149387a1c79679a87dd1ba755bc, is a Ransom.WannaCry variant and ac21c8ad899727137c4b94458d7aa8d8 is a variant of Backdoor.Contopee, a backdoor used in attacks against several banks. The samples referenced in the tweet contain shared code. This shared code is part of a custom SSL implementation, using an identical cipher suite. It could be described as "fake ssl". Each cipher specifies an option for key exchange, authentication, bulk encryption, MAC. The Contopee sample and WannaCry sample have almost identical pieces of code that reference an identical cipher suite. The cipher suite in both samples has the same 75 different ciphers to choose from (as opposed to OpenSSL where there are over 300).

Appendix C: Indicators of Compromise

MD5	SHA256	File nar
21307227ECE129B1E12797ECC2C9B6D9	8A4D2BAA8CF519C7A9B91F414A0A9D8BA2B9E96D21D9E77DA7B34ED849830A36	mks.exe
6F0338AF379659A5155B3D2A4F1A1E92	CA8DC152DC93EC526E505CF2A173A635562FFBF55507E3980F7DC6D508F0F258	hptasks
0489978ffa3b864ede646d0470500336	2A99BCB5D21588E0A43F56AADA4E2F386791E0F757126B2773D943D7CBF47195	ENTASK Creates
a1ffca7ba257b4eca7fe7d1e78bac623	3C86FC0A93299A0D0843C7D7FF1A137A9E799F8F2858D3D30F964E3C12C28C9E	forti.exe javaupd

f27cf59b00dacdd266ad7894a1df0894	92b0f4517fb22535d262a7f17d19f7c21820a011bfe1f72a2ec9fbffbdc7e3e0	creates
a1ffca7ba257b4eca7fe7d1e78bac623	3C86FC0A93299A0D0843C7D7FF1A137A9E799F8F2858D3D30F964E3C12C28C9E	g.exe
511778c279b76cac40d5d695c56db4f5	91146EE63782A2061701DB3229320C161352EE2BC4059CCC3123A33114774D66	svchost
f774c0588da59a944abc78d5910be407	A7EA1852D7E73EF91EFB5EC9E26B4C482CA642D7BC2BDB6F36AB72B2691BA05A	lsasvs.e lsasvs.e
8386379a88a7c9893a62a67ea3073742	7F8166589023CD62AE55A59F5FCA60705090D17562B7F526359A3753EB74EA2F	507931 507931
3bc855bfadfea71a445080ba72b26c1c	043E0D0D8B8CDA56851F5B853F244F677BD1FD50F869075EF7BA1110771F70C2	taskhcs taskhcs
F27CF59B00DACDD266AD7894A1DF089492B0F4517FB22535D262A7F17D19F7C21820A011BFE1F72A2EC9FBFFBDC7E3E0		WannaC armsvc.
E8C6ACC1EB7256DB728C0F3FED5D23D7	524F8F0F8C31A89DF46A77C7A30AF5D2A1DC7525B08BFAFBED98748C3D8A3F1C	javaupd jusched
1D4EC831292B611F1FF8983EBD1DB5D4	41E9D6C3374FD0E78853E945B567F9309446084E05FD013805C70A6A8205CD70	msinj32
D0CE651A344979C8CD11B8019F8E4D7E	436195BD6786BAAE8980BDFED1D7D7DBCCCB7D5085E79EBDCC43E22D8BAE08A8	goyqsv
9A5FA5C5F3915B2297A1C379BE9979F0	9F177A6FB4EA5AF876EF8A0BF954E37544917D9AABA04680A29303F24CA5C72C	exldcm
86759CE27D0FE0B203AAA19D4390A416	AE8E9FF2DC0EC82B6BAE7C4D978E3FEAC93353CB3CD903E15873D31E30749150	oledbg3
FCF3702E52AE32C995A36F7516C662B7	FC079CEFA19378A0F186E3E3BF90BDEA19AB717B61A88BF20A70D357BF1DB6B8	bitssvcs
e117406e3c14ab8e98b27c3697aea0b6	2BA20E39FF90E36086044D02329D43A8F7AE6A7663EB1198B91A95EA556CF563	00bebc

For additional information from Symantec regarding the WannaCry virus, visit our dedicated WannaCry Ransomware page.

Tags and Keywords

Related Entries and Links

No Related Resource entered.