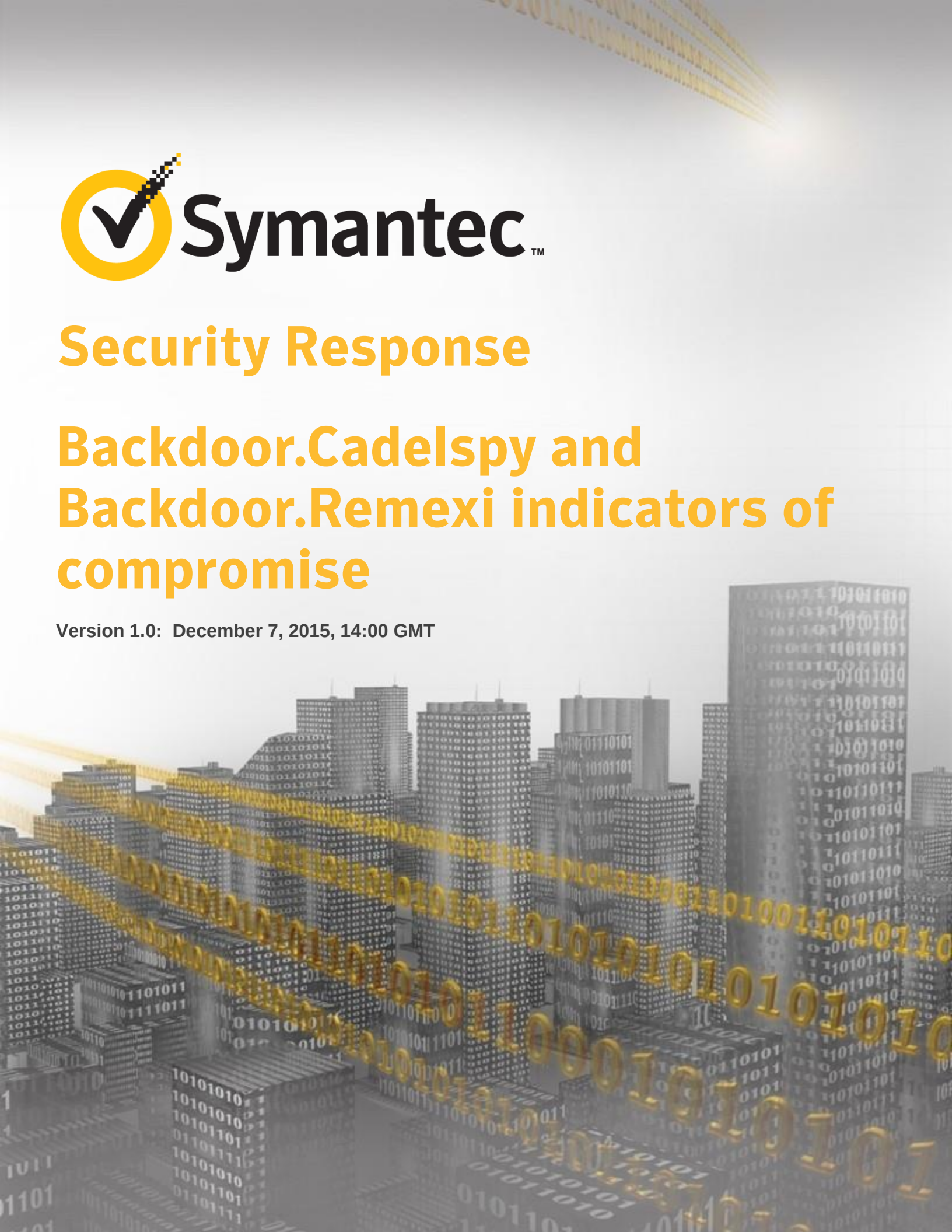

Security Response

Backdoor.Cadelspy and Backdoor.Remexi indicators of compromise

Version 1.0: December 7, 2015, 14:00 GMT

Backdoor.Cadelspy

Dropper

File name	ntinst.exe
MD5	8b9d1fc8e5864a46ba5992f7350d5d89
SHA1	72219ba63f2cb336bc7d2e59e9e527af612e207d
SHA256	c3a14dab06866ce635b45196022a35fe99e1d7ceccf8b378cc807249771e6e42
Size	636,416 bytes
Purpose	Drops all components from its resource section

Table 1. Backdoor.Cadelspy dropper attributes

This is Backdoor.Cadelspy's dropper component. When executed, the dropper extracts other components from its resource section. It drops two of the installer components in the %Temp% folder and the rest in %Temp%\tmp0001. It executes the appropriate installer, depending on whether the computer is a 32- or 64-bit system. The files created by the installer are listed in the following table:

Action	Path	File name	Purpose
create	%Temp%	ldr32_x64.exe	64-bit installer
create	%Temp%	ldr32_x86.exe	32-bit installer
create	%Temp%\tmp001	work.path	Contains encrypted folder path
create	%Temp%\tmp001\x64	2093101001.cfg	Configuration file
create	%Temp%\tmp001\x64	2093101001.rou	Configuration file
create	%Temp%\tmp001\x64	ntsvcst32.dll	64-bit loader of the back door
create	%Temp%\tmp001\x64	ntsvc32.dll	64-bit back door
create	%Temp%\tmp001\x86	2093101001.cfg	Configuration file
create	%Temp%\tmp001\x86	2093101001.rou	Configuration file
create	%Temp%\tmp001\x86	ntsvcst32.dll	32-bit loader of the back door
create	%Temp%\tmp001\x86	ntsvc32.dll	32-bit back door

Table 2. Files created by Backdoor.Cadelspy's installer

Installer

	32-bit installer
File name	ldr32_x86.exe
MD5	6542d5f614ba093a43cd6a3a846d37ff
SHA1	65bb99e15e098166bff04f22805b15810f8fbf71
SHA256	bf24d7f4e40aaa102d8e5b048de82c6ca9ffcc6c07f207ea79d1a4af5ffc9120
Size	75,264 bytes
Purpose	Installs the 32-bit files from the dropper

Table 3. Backdoor.Cadelspy's 32-bit installer attributes

	64-bit installer
File name	ldr32_x64.exe
MD5	269b5a5270b34bf86c60bc793486aab7
SHA1	14a694517ca05165ca09c81c984888923a35f0b0
SHA256	6e8f5c8addab6d875a06bc92e109c0298aede342810eb25e16d292b4fffce535
Size	91,648 bytes
Purpose	Installs the 64-bit files from the dropper

Table 4. Backdoor.Cadelspy's 64-bit installer attributes

This component installs the files from the dropper. It also creates a registry entry to remain persistent on the computer. The installer can be executed with two parameters:

- The first parameter may be the string "true", upon which the installer will terminate the explorer.exe process. Windows will automatically re-launch explorer.exe and load %System%\ntsvc32\ntsvc32.dll
- The second parameter is a file name that needs to be deleted. This may remove the dropper component from the computer after the threat is successfully installed.

When executed, the installer creates the %System%\ntsvc32 folder and moves the appropriate files from the %Temp%\tmp001\[x86 OR x64] folder into it.

On a 32-bit computer, the following files are moved:

Action	Source path	File name	Destination path
move	%Temp%\tmp001\x86	2093101001.cfg	%System%\ntsvc32
move	%Temp%\tmp001\x86	2093101001.rou	%System%\ntsvc32
move	%Temp%\tmp001\x86	ntsvc32.dll	%System%\ntsvc32
move	%Temp%\tmp001\x86	ntsvcst32.dll	%System%\ntsvc32

Table 5. Files moved by 32-bit installer

On a 64-bit computer, the following files are moved:

Action	Source path	File name	Destination path
move	%Temp%\tmp001\x64	2093101001.cfg	%System%\ntsvc32
move	%Temp%\tmp001\x64	2093101001.rou	%System%\ntsvc32
move	%Temp%\tmp001\x64	ntsvc32.dll	%System%\ntsvc32
move	%Temp%\tmp001\x64	ntsvcst32.dll	%System%\ntsvc32

Table 6. Files moved by 64-bit installer

The loader component, %System%\ntsvc32\ntsvc32.dll, decrypts the file %Temp%\tmp0001\work.path, which contains a folder path to create. The remaining files that the dropper created in the %Temp%\tmp0001 folder, with the exception of work.path, are then deleted.

Persistence

The loader component is added to the AppInit_DLLs registry so that it loads when any Windows-based application runs.

Back door

File name	ntsvc32.dll
MD5	200e662384542ccd979d4994dd08163e
SHA1	c5f1bb651f665cc30cf789ce554f2bfc9d91a19f
SHA256	0f7f0283baddacac623b0adcadf4ce146f6e61cc514abb31982299d25cd86400
Size	415,232 bytes
Purpose	Main module containing the back door routine

Table 7. Backdoor.Cadelspy back door attributes

This component is Cadelspy's main back door, which gathers user information, logs keystrokes, captures screenshots and webcam pictures, and performs other functionality. The module also communicates with the command-and-control (C&C) servers. The back door component contains two configuration files:

- 2093101001.cfg (main configuration file)
- 2093101001.rou

The main configuration file contains:

- C&C server information
- Enabled commands
- Applications to monitor

Functionality

The back door component performs the following actions:

- Decrypts the .cfg file to extract the C&C server(s), URI, commands to enable, and other related configuration data
- Decrypts the .rou file to extract settings. If the .rou file is not found, it requests the C&C server to send it one.
- Creates the registry subkeys and values using data extracted from the .rou and .cfg file.
- Creates the %System%\ntinfo32 folder to store all of the gathered data.
- Starts command threads which perform the main functionality of the back door
- The gathered information is saved within .fjr or .rou files in the %System%\ntinfo32 folder. The back door then compresses them as .ecm files. If there is no user activity, the back door compresses the files into a .cab and uploads it to the C&C server.
- Once the files are uploaded, the back door retrieves the C&C server response and saves it in a new .rou file containing commands .

The back door component also retrieves the window names (text) and computer name, and uploads them to /sms.aspx

Note: The input and output during communications are in an XML format (before encryption)

Command and control

The back door component appears to use an open-source HTTP client called Ryeol to communicate with the C&C servers.

During command execution, the following registry entries are examined to determine if the malware is in a active or inactive state:

- HKEY_CURRENT_USER\SOFTWARE\ntsvc32\“PAP” = "CSNPSV"
- HKEY_CURRENT_USER\SOFTWARE\ntsvc32\“PAP” = "CSACTD"

The component also checks to see if there is a valid internet connection to the C&C server using the InternetGetConnectedState API.

The back door attempts to download an update of the main configuration file from the C&C server through the following URL:

- [C&C SERVER ADDRESS]/allusers/2093101001.rou2093101001.txt

If the configuration update is unavailable, the default .rou configuration file is used.

The back door component supports the following commands:

Command	Description
snp	Takes a screenshot and saves it to snp.fjr
wbm	Captures a webcam image and saves it as wbm.fjr. To do this, it calls the WebCamCapture export in \ntsvc32\CamCap.dll
keylog	Logs keystrokes and saves them in the main log file
msc	Captures window titles or text that the mouse clicked. Saves them to msc.fjr
clp	Copies what's in the clipboard and saves it to clp.fjr
RecordSound	Records sound using waveIn APIs
SpoolCommand	Gathers printer information and all of the documents that were sent to be printed. Saves the information to the main log file.
GetMachineInfoCommand	Runs once when the malware is installed. Gathers information about the hard drives and the network, and writes it to the main log file
ExecuteCommand	Executes a given shell command
UploadCommand	Compresses all of the files in the .cab file format. Waits for no user activity (idle time) and then uploads the information

Table 8. Back door’s supported commands

Indicators of compromise

Backdoor.Cadelspy hashes

MD5	SHA256
8b9d1fc8e5864a46ba5992f7350d5d89	c3a14dab06866ce635b45196022a35fe99e1d7ceccf8b378cc807249771e6e42
269b5a5270b34bf86c60bc793486aab7	6e8f5c8addab6d875a06bc92e109c0298aede342810eb25e16d292b4fffce535
6542d5f614ba093a43cd6a3a846d37ff	bf24d7f4e40aaa102d8e5b048de82c6ca9ffcc6c07f207ea79d1a4af5ffc9120
be303010e6ac78c7975c93aa459f2319	36f5744f72674524f56bf286dce7e4b1c93ac2859036513cfdb479daf1c014f1
34b4d84d5e771d2d018d925c6ac40293	82ed6493c494e88e49799c75f6b22c101c1ca3d97ac001b5487610f81d21d961
8d26621cc8e969266985f7000536f557	3db1b57303326b9fea0fbf919ae6113d013e695b2844d645bfe69d3b4bc0ec57
200e662384542ccd979d4994dd08163e	0f7f0283baddacac623b0adcadf4ce146f6e61cc514abb31982299d25cd86400
7beeb3bd4681c17fe93fffcefcd125aa	d6e769121d327a3f00c615459ac04bc4e2149aa17ea29479b86156298834eb62
6d70e287bf472663c1fbb4682d13d74a	fead15c401f0aba8e770b7a85df96852dd1b72ca367c2aef3a0913bca10da0d5
ff521e2a7908745fc951979e03cf0c01	ac187ad5ce438cfbcd58743b2641978c2d9d000d7c30130d2df42c767be08996
f35ad22d762d59672e1977a4d96658af	e2f430fb6f3588cd9cf63a74760e37738c91e7589df41f0bbac9a4e23b745d7e

06291777cc2840a89ce1f8f82db97453	0595979c000ef1aa3a237b0822c0556a64a75edaec8560e37e9214fd57569461
2d8ba12d741fee7edae6454b06f6bc9c	2f0b3cf460b3909f259550a3a09e679d63391847ae45bd44306ddbfc1f53d5ec
15db41840f77723aa7e43460d9d3a5cc	688dbf4cfc00957d2679dc319de0bb80f38e7b5ac4414c1543e135e37c561b8b
05a88017b65754dc66f83c1d37778cc7	247511a37c6e01e1b4acf360003e9e72208c86df614fc711b2b152a4c3fc524f
0069360b20a03728665bd92c4bccf380	c5460b3e2b4dfe9af1c209ecd143c7f847a9092abea86275a071324110f74555
d5601ec9a7d2853b68e639cf9d55b987	8455598c9bbb0a93aa35b083ee8bb83bb01fe27cf02ee7c44052a813cb66767c
5c0d7e787c39d64ef8546c5d2bcdab6d	26f0d3d4eb4d445f4231157198eae01846797ce5ffc624872b0daf90736994e8
0b884517404718397555d5e46255c4bb5	54abd9863f185e7ebd47a3f39f99335532bd55849228a7ed29ffdab8090dc4f6
4387a0855c11ac9b8e8f7593eca32e6e	27f2350d51cb41a4e5330b7cffd87ca89d263278e2a3fb8cbf0d324a4a267223
9aba0581781b7f5f9e57f07716a41f26	6a88964db3e97e8176dd1df4ca69e2bfd92366a5b051d3313fa48aefa4ad288f
e40e83cdf0688e48df2cdb70962a6be2	ebc9d6bcd5f8e738d2ed82b1c232df06b9caf0b33ea8b4b45d7f0bfd8252a97d
dc8fe2004c7cd048bc93c5803c001e3f	2317f2448a689aa3d4802e838ae3dfd772246e6f1eb9e262df4012a221a63825
38f9efa16a3b360c8ad1c872413f8dd9	f8fe5edcdf087368a4aa9e39d583fc80a625209f3297a4db9697d4ade6c8b9ce
5c587530e0d3daca90ca26436e091d08	90bea454ed11dbdfe0d21e097299db4354999b693489cbccc652c11cc1adce22
8a58cb79c33b196036f8d5b960316319	6079c6ff09440faa673be55f0f7f8a613d8654e7d2cb49990db316b0add53063

Table 9. Hashes associated with Backdoor.Cadelspy

Backdoor.Cadelspy Yara signatures

```
rule Cadelle_1
{
  strings:
   $s1 = {
                56 57 8B F8 8B F1 33 C0 3B F0 74 22 39 44 24 0C
                74 18 0F B7 0F 66 3B C8 74 10 66 89 0A 42 42 47
                47 4E FF 4C 24 0C 3B F0 75 E2 3B F0 75 07 4A 4A
                B8 7A 00 07 80 33 C9 5F 66 89 0A 5E C2 04 00
          }

   $s2 = "ntsvc32"
   $s3 = "ntbind32"

    condition:
    $s1 and ($s2 or $s3)
}

rule Cadelle_2
{
  strings:
   $s1  = "[EXECUTE]" wide ascii
   $s2  = "WebCamCapture" wide ascii
   $s3  = "</DAY>" wide ascii
   $s4  = "</DOCUMENT>" wide ascii
   $s5  = "<DOCUMENT>" wide ascii
   $s6  = "<DATETIME>" wide ascii
   $s7  = "Can't open file for reading :" wide ascii
   $s8  = "</DATETIME>" wide ascii
   $s9  = "</USERNAME>" wide ascii
   $s10 = "JpegFile :" wide ascii
   $s12 = "[SCROLL]" wide ascii
   $s13 = "<YEAR>" wide ascii
   $s14 = "CURRENT DATE" wide ascii
```

```
    $s15 = "</YEAR>" wide ascii
    $s16 = "</MONTH>" wide ascii
    $s17 = "<PRINTERNAME>" wide ascii
    $s18 = "</DRIVE>" wide ascii
    $s19 = "<DATATYPE>" wide ascii
    $s20 = "<MACADDRESS>" wide ascii
    $s21 = "FlashMemory" wide ascii

  condition:
  12 of them
}

rule Cadelle_3
{
  strings:
   $s1  = "SOFTWARE\\ntsvc32\\HDD" wide ascii
   $s2  = "SOFTWARE\\ntsvc32\\ROU" wide ascii
    $s3  = "SOFTWARE\\ntsvc32\\HST" wide ascii
    $s4  = "SOFTWARE\\ntsvc32\\FLS" wide ascii
   $s5  = "ntsvc32" wide ascii
   $s6  = ".Win$py." wide ascii
   $s7  = "C:\\users\\" wide ascii
   $s8  = "%system32%" wide ascii
   $s9  = "\\Local Settings\\Temp" wide ascii
   $s10 = "SVWATAUAVAW" wide ascii
   $s11 = "\\AppData\\Local" wide ascii
   $s12 = "\\AppData" wide ascii

    condition:
    6 of them
}

rule Cadelle_4
{
  strings:
   $s1 = "AppInit_DLLs" wide ascii
   $s2 = { 5C 00 62 00 61 00 63 00 6B 00 75 00 70 00 00 }
   $s3 = { 5C 00 75 00 70 00 64 00 61 00 74 00 65 00 00 }
   $s4 = "\\cmd.exe" wide ascii

    condition:
    all of them
}
```

Backdoor.Remexi and Backdoor.Remexi.B

Backdoor.Remexi is a basic back door that lets the attackers open a remote shell and execute commands.

When loaded, the Trojan may log DWORD markers and last-error code values to the following file:

- %Temp%\WIN[RANDOM HEXADECIMAL VALUE].tmp

The following includes two examples of what [RANDOM HEXADECIMAL VALUE] could be:

- 2002010500000000
- 20020205B7000000

In these examples, “20020105” and “20020205” are markers, while the second dwords are last-error code values.

The malware reads arguments from the following registry subkey:

- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\SEA\Parameters\Arguments

For Backdoor.Remexi.B, the service may be called “MAS”.

The first two arguments are the C&C server’s IP address and port number. The remaining two arguments are the working time range. If the current time is not within this range, then the Trojan will fall into sleep mode.

The back door Trojan connects to the C&C server using the IP address and port number that were specified in the registry. The malware then creates a cmd shell. This shell is used to let the attacker send commands to the affected computer .

The threat reads the value of the following registry subkey:

- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\SEA\Parameters\ID

Then, the Trojan may send the ID value to the C&C server and show the ID value for the shell. The shell is open until the "<exit>" is received.The malware can also update the ID and save it to the following registry subkey:

- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\SEA\Parameters\ID

Indicators of compromise

Backdoor.Remexi hashes

MD5	SHA256
19cd900c135a5e9d486735ae3d2c3e97	6c0d1268177ebc1ad7b8f34f04b3d38c74cf4b43e18259677759c0ef91615e24
253e32699d5b9c4cdf8a589ef6309af5	17a73d715333d4af746bf6d180fd129b6334a34599bf299bef48d7e27de95a68
a437c10da3aaa8fe3241c8629c18d21a	6b8a220272382f5481e1900c1c603f67ec9d5fb45ad78bf7788dece1f20dddcd
b457ebbfbaf3d8adcce8bf8b2a7adcea	a8921363b0f3cca72c5487f67230b564598b2c20dcd7ea04807b7b18b78af53a
fd2e29ad73d2e73f16667748f4536c4c	da84353f914c297878e5d5eb55a6905b655410df67b881092008b24faa90bb79

c6acff232a12259d75196a5ba6a233c7	9be5fa0e44b2fe964f292db44236ecf2d790465a9d42fe550dff20faca5a2d52
26afc6ef4315460e7e9e1cd8a3d20700	18CE17849CD25452D98B24987556322DA72E1031D1C8D8680EE9FEC3DFB7CB46

Table 10. Hashes associated with Backdoor.Remexi

Backdoor.Remexi.B hashes

MD5	SHA256
adad23e3ca8057b562fad57a4b1c6137	1E5022576367F6A614AFE0F8963AEDD1F0C7B06502E326C43362A59DDEFD118E
135b226e06a309dad5c4af1e36528f93	de529597194ed2088eb7fc246bcb698dac739c2ac3de8d7b9a5fd0e969f124fa
1fe84feb00e779bcdbece24ddddb38f7	D94B920A5645218D8368C1277E5D2081916E66D815C9C3E150B07ADE02DE970F
2374b9655f6330b07bc3d63df399731e	9f0ac7fa30e86b4015de6f77fe219cced164f317799fdc3faaf35af730a48700
27524accc1559da37deecb583419eb6e	22261e840bfaa43b982ce08a1eb18fd53400dca2a2dc6edebd1398229e5a32ee
2c3ebabc800fd2256dae4a9c363e0f49	f4db775254f4139ec677efa1a633e310189d7ad425a7f5a84fdb6ee4a3c1aa21
894fd325751465d6f48c17106a1a91d1	98a9b2329eefe618daa78b6afed82cebf40cb918ad0aae7a8d7f59af4cb13b41
ac2b52010d43632b2f66573d2550984c	f7e44314521c04626d586e07cbab655ee59a5a0805cccef8311f669c175f5d86

Table 11. Hashes associated with Backdoor.Remexi.B

Backdoor.Remexi C&C domains

- 37atypz123.dns-bind9.com
- 5ppob16.dockerjsbin.com
- 87abfg113.dockerjsbin.com
- 87pqxz159.dockerjsbin.com

Backdoor.Remexi Yara signature

```
rule Remexi
{
   strings:

         $c1   = { 00 3C 65 78 69 74 3E 00 }        /* <exit>  */
          $c2   = { 00 3C 69 64 3E 00 }             /* <id>    */
          $c3   = { 00 3C 72 65 6D 3E 00 }          /* <rem>   */
          $c4   = { 00 3C 63 6C 6F 73 65 3E 00}     /* <close> */
          $c5   = { 00 57 49 4E 00 }                /* WIN     */
          $c6   = { 00 63 6D 64 2E 65 78 65 00 }    /* cmd.exe */
          $c7   = { 00 49 44 00 }                   /* ID      */
          $c8   = { 00 72 65 6D 00 }                /* rem     */

          $d1   = "\\SEA.pdb"
          $d2   = "\\mas.pdb"

          $s1  = "Connecting to the server..."
          $s2  = "cmd.exe /c sc stop sea & sc start sea"
          $s3  = "SYSTEM\\CurrentControlSet\\services\\SEA\\Parameters"
          $s4  = "RecvWrit()-Read_Sock-Failed"
          $s5  = "ReadPipeSendSock()"

   condition:
         (4 of ($c*) and (2 of ($s*) or any of ($d*))) or (5 of ($c*) and
any of ($s*))
}
```

About Symantec

Symantec Corporation (NASDAQ: SYMC) is an information protection expert that helps people, businesses and governments seeking the freedom to unlock the opportunities technology brings -- anytime, anywhere. Founded in April 1982, Symantec, a Fortune 500 company, operating one of the largest global data-intelligence networks, has provided leading security, backup and availability solutions for where vital information is stored, accessed and shared. The company's more than 20,000 employees reside in more than 50 countries. Ninety-nine percent of Fortune 500 companies are Symantec customers. In fiscal 2014, it recorded revenues of $6.7 billion. To learn more go to www.symantec.com or connect with Symantec at: http://www.symantec.com/social/

For specific country offices and contact numbers, please visit our website.

Symantec World Headquarters
350 Ellis St.
Mountain View, CA 94043 USA
+1 (650) 527-8000
1 (800) 721-3934
www.symantec.com