I am HDRoot! Part 2

By Dmitry Tarakanov

Published: 2015-10-13 · Archived: 2026-04-05 18:11:49 UTC

Some time ago while tracking Winnti group activity we came across a suspicious 64-bit sample. It was a standalone utility with the name HDD Rootkit for planting a bootkit on a computer. Once installed the bootkit infects the operating system with a backdoor at the early booting stage. The principles of this bootkit's work, named HDRoot, have been described in the first part of our article. During our investigation we found several backdoors that the HDRoot bootkit used for infecting operating systems. These backdoors are described in this part of the article.

Backdoors

Since the backdoor installed with the use of HDRoot might be arbitrary, we can't describe what malware is run by HDRoot bootkit in every case where it might be found. But at least we have managed to collect two types of malware that were identified while tracking HDRoot. The first one was extracted manually from the hard drives of victims where HDRoot was detected and who contacted us for the help with combating the infection. Another one was found in a standalone dropper that contained both HDRoot and the installed backdoor.

1st type backdoor

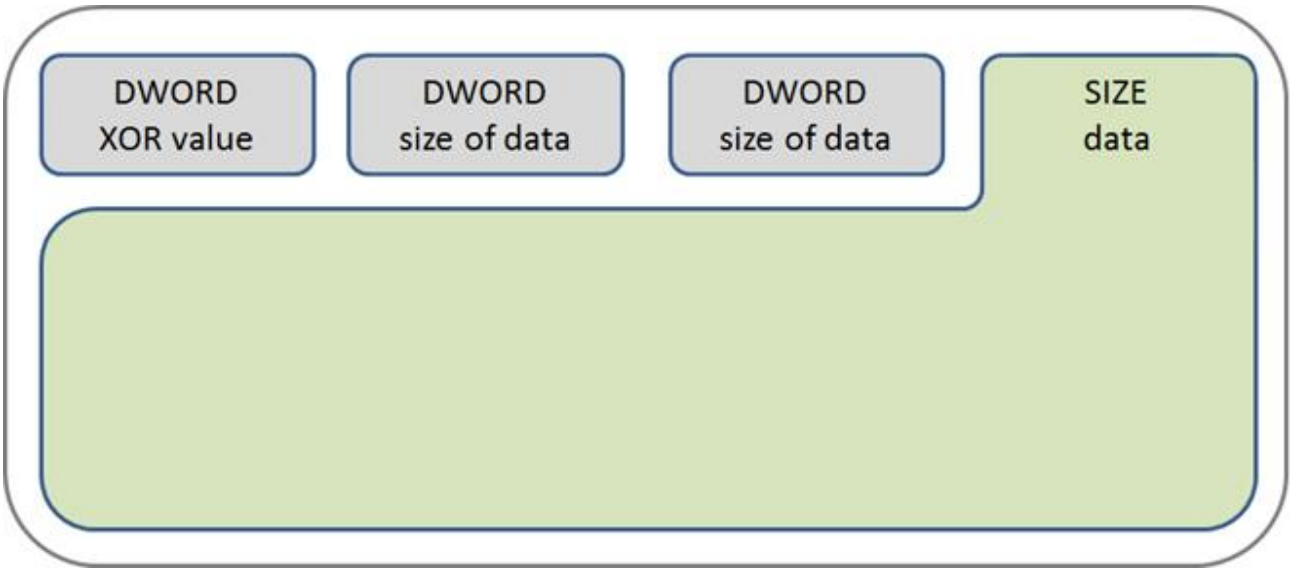
MD5	Size	Linker	Compiled on
C0118C58B6CD012467B3E35F7D7006ED	113'152	10.00	2012-12-19 17:14:21

Property	Value
FileVersion	6.1.7601.17514 (win7sp1_rtm.101119-1850)
FileDescription	ProfSvc
InternalName	ProfSvc
OriginalFilename	ProfSvc.dll
LegalCopyright	© Microsoft Corporation. All rights reserved.
ProductName	Microsoft® Windows® Operating System
CompanyName	Microsoft Corporation

This is the malware family known as server-side Derusbi, which we observed during several Winnti-related incidents. Usually this is a DLL with the internal name *OfficeUt32.dll* and exported functions like:

DllRegisterServer
DllUnregisterServer
ServiceMain
SvchostPushServiceGlobals
WUServiceMain
__crt_debugger_hook

This list of functions can differ slightly from version to version. The main DLL includes other malware components in its body, usually maintained in the XOR-ciphered form:



The structure for maintaining additional modules

The Derusbi samples installed with the use of the HDRoot bootkit contained a Remote Shell module and network driver.

The installation routine is implemented in the exported function "*DllRegisterServer*". When called, this function performs the following actions:

- It copies itself to the folder "*%System32%wbem*", with a name consisting of "*ntfs*" + three random letters, and a "*.mof*" extension, for example "*ntfsqwe.mof*", and sets the year to 2005 in the date attributes of the file.
- It puts a string with its own path to the "*ServiceDll*" value in the registry that associates with the "*iphlpsvc*" or "*wuauserv*" system service depending on Windows version, and saves the original value of "*ServiceDll*" in encrypted form to the "*Security*" parameter of the same registry key. It executes the malware on system startup.
- After the malware service has started, it starts the original system service that was replaced, running the dynamic link library associated with the service specified in the "*Security*" parameter during malware installation.

The malware stores its configuration data in encrypted form in the "*Security*" value of the *HKLMSOFTWAREMicrosoftRpc* registry key. It contains a unique computer identifier, and the signature for

matching incoming C&C server packets.

The malware can either connect to the C&C server directly if it is specified in the settings block in its body or work in listening mode if no C&C server is defined. The samples related to the HDRoot bootkit we found worked in listening mode.

1st type backdoor: the driver

MD5	Size	Linker	Compiled on
C8DAF9821EBC4F1923D6DDB5477A8BBD	37’264	9.00	2012-12-19 17:08:53

Property	Value
FileVersion	6.1.7601.17514 (win7sp1_rtm.101119-1850)
FileDescription	Partition Management Driver
InternalName	partmgr.sys
OriginalFilename	partmgr.sys
LegalCopyright	© Microsoft Corporation. All rights reserved.
ProductName	Microsoft® Windows® Operating System
CompanyName	Microsoft Corporation

(The driver was signed on December 19, 2012 17:11:14 with the stolen certificate of South Korean online gaming company **XL Games**. The certificate was revoked on Jun 21, 2013. Its serial number is: **7b:d5:58:18:c5:97:1b:63:dc:45:cf:57:cb:eb:95:0b**).

The main malware DLL decrypts, drops and runs the rootkit as a file *“%System32%DriversLst_Update.sys”*. The driver at the very beginning of the process removes all registry values created during its launch and the actual driver file. The rootkit conceals malicious network activity from popular network monitoring tools by hooking the *IRP_MJ_DIRECTORY_CONTROL* service routine of *“DeviceTcp”* or *“Drivernsiproxy”* system objects. It also hides the file *“windowssystem32wiarpc.dll”* from user-mode applications by hooking the *IRP_MJ_DIRECTORY_CONTROL* service routine of the file system driver *“FileSystemNtfs”*.

If the malware works in listening mode, the rootkit is also engaged in the communication routines. It sniffs all incoming network packets and searches them for a specially crafted signature. If found, it redirects these packets to the listening socket opened by the main malware module. The main module creates a network socket on a random port on all network interfaces. If the rootkit pushes a network packet that matches the predefined signature, the main malware module will process it. This network packet includes command code and the module ID that has to perform that command. Known versions of the malware recognize five modules with different commands:

Module ID	Supported commands
0x80	Services management: list of services, creating, starting, stopping, deleting services Manage running processes: terminating, retrieving module file name, processes token Registry management
0x81	Execution of arbitrary files or shell commands on infected system
0x82	Traffic redirection via port forwarding: infected host is used as proxy
0x84	Browsing the file system, uploading/downloading files
0x240	Main module control: removing the main module, stopping the main module, downloading and starting DLL from the remote server (this DLL will be saved in *%TEMP%* as *"tmp1.dat"*), starting network proxy

1st type backdoor: remote shell library

MD5	Size	Linker	Compiled on
1C30032DC5435070466B9DC96F466F95	13'360	10.00	2012-12-19 17:12:12

Property	Value
ProductVersion	6.1.2600.1569
ProductName	Microsoft®Windows®Operating System
CompanyName	Microsoft Corporation
FileDescription	Microsoft update
FileVersion	6.1.2600.1569

As was mentioned earlier, besides a network driver there was only one additional module included in the discovered versions of the Dersubi samples related to HDRoot – Remote Shell. The main malware module decrypts, drops and runs it as the file *"%Systemroot%Helpperfc009.dat"*. This is the DLL with the internal name *Office.dll* and one exported function *R32*. The library is run by executing the following command line:

rundll32.exe %Systemroot%Helpperfc009.dat R32 <random_number>

where *<random_number>* is a pre-shared value generated by the main module.

The Remote Shell library creates two named pipes used to communicate with the main module:

pipeusb<random_number>i
pipeusb<random_number>o

The command line from the operator for execution is expected to come through the pipe *pipeusb<random_number>o*. When this command comes a new process is created to execute it in the working directory *%SystemDrive%*. Standard input of the process that has just been created is set to be obtained from the pipe *pipeusb<random_number>o*, while output and *STDERR* are redirected into the parallel pipe *pipeusb<rando_number>i*. This means input to the executing program comes from an operator and the program's output goes back to him, framing an effective backdoor channel.

2nd type backdoor: the dropper

MD5	Size	Linker	Compiled on
755351395AA920BC212DBF1D990809AB	266'240	6.00	2013-11-18 19:23:12

We were able to spot a sample that turned out to be a one-click installer of the backdoor with the use of HDRoot. This is a Win32 executable compiled on 18 November 2013 according to its data stamp in the header. The executable includes resources *"102"* and *"103"* of custom type *"MHM"*. These are the executable of HDRoot installer and the installed backdoor.

The role of the installed backdoor is played by the executable maintained as the resource *"102"* and dropped as the file *%windir%bootmgr.exe*. (Running a few steps forward we have to say that formally it's not a backdoor but a downloader.) The tool "HDD Rootkit" which is the resource *"103"* is dropped as *%windir%hall32.exe*. Then the dropper runs the following command line:

%windir%hall32.exe inst %windir%bootmgr.exe c:

that instructs the HDRoot installer named *hall32.exe* to install the HDRoot bootkit onto the hard drive where disk C: is located with subsequent running of the downloader *bootmgr.exe* on system start-up.

There are other files specified in the dropper's body that it checks for in the file system or which the malware uses in intermediate procedures:

%windir%system32midimapbits.dll
%windir%system32mpeg4c32.dll
%windir%bootmgr.dat

The downloader

MD5	Size	Linker	Compiled on
11E461ED6250B50AFB70FBEE93320131	69'632	6.00	2013-11-18 19:22:30

The downloader *bootmgr.exe* was also compiled on 18 November 2013 like the dropper. According to the list specified in its body, it downloads files by following URLs and runs them:

http://www.gbutterfly.com/bbs/data/boot1.gif
http://www.btdot.com/bbs/data/boot1.gif

http://boot.ncook.net/bbs/data/boot1.gif
http://www.funzone.co.kr/bbs/data/boot1.gif
http://www.srsr.co.kr/bbs2/data/boot1.gif

If anything is available via these URLs, it is dropped onto the disk with one of the following file names and run:

%windir%v3update000.exe
%windir%v3update001.exe
%windir%v3update002.exe

The downloader checks the size of the dropped file and only runs it if it is greater than 20896 bytes.

It turned out that this is a double downloader: it maintains another sample with downloading functionality in its body. The malware drops it with the file name *%windir%svchost.exe* and subsequently runs it with the parameter *"install"*. For some reason, immediately after running the 2nd downloader the malware stops the work of the Internet Connection Sharing service with the command line:

cmd.exe /c net stop sharedaccess

There are other files specified in the downloader's body that it checks for in the file system:

%windir%system32midimapbits.dll
%windir%system32mpeg4c32.dll
%windir%winurl.dat

The 2nd downloader

MD5	Size	Linker	Compiled on
ACC4D57A98256DFAA5E2B7792948AAAE	22'016	6.00	2013-11-18 19:06:32

This malware is able to recognize two parameters: *"install"* and *"remove"*. In the installation branch it creates the auto-starting *"Winlogon"* service with the description *"Provides automatic configuration for the 802.11 adapters"* and adjusted to run its own executable. The *"remove"* parameter obviously leads to the deleting of this service.

While running, the service decrypts the list of URLs included in its body and tries to download the content by addresses formed by appending *"default.gif"* to the URLs from the list. This is a complete decrypted list of URLs:

http://www.netmarble.net/
http://www.nexon.com/
http://www.tistory.com/start/
http://m.ahnlab.com/
http://www.joinsmsn.com/
http://fcst.co.kr/board/data/media/
http://www.hangame.com/
http://www.msn.com/

http://adw.naver.com/
http://www1.designrg.com/
http://www.topani.com/
http://www.nate.com/
http://www.v3lite.com/
http://www1.webschool.or.kr/
http://snsdate.gndot.com/
http://www.srsr.co.kr/bbs2/data/
http://funzone.co.kr/bbs/data/
http://www.moreuc.com/
http://www1.ncook.net/

As you can see, this list includes sites of legitimate and trusted parties and they are unlikely to maintain malware components. Because every site is generally not malicious, some of them were probably compromised, or else the malware would not have been functional.

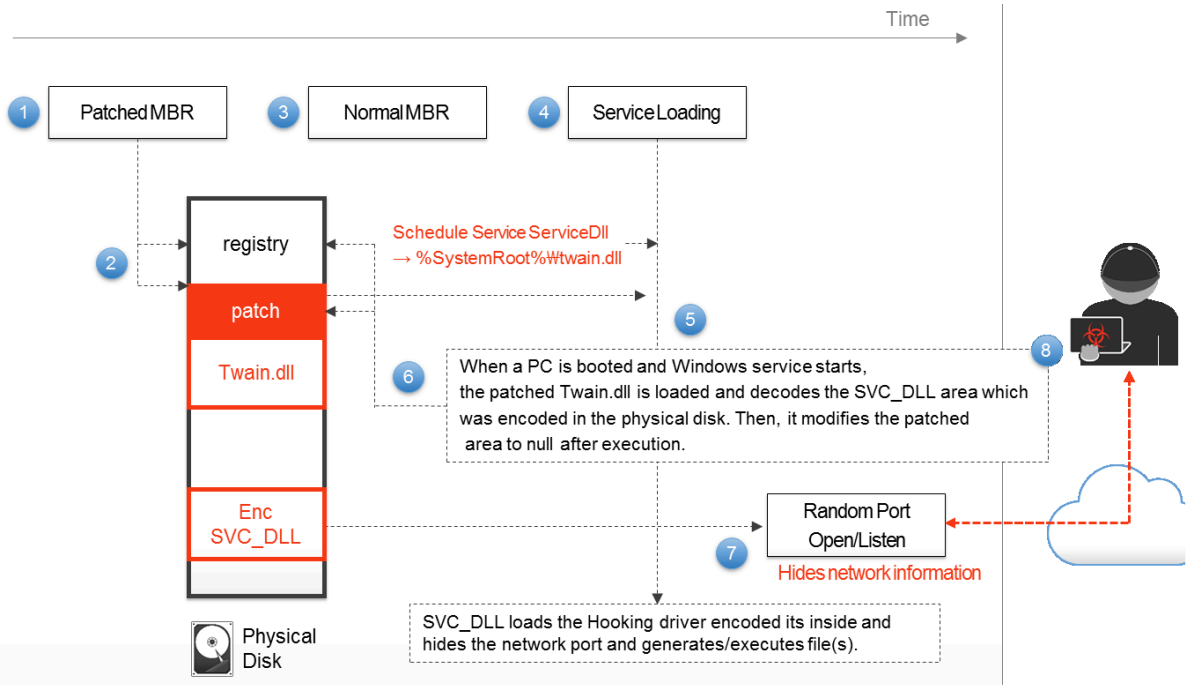
The content is downloaded into the file *%windir%image.jpg*. But this is only an intermediate stage. It should be a text file that is parsed by the malware. The first line of that file should contain only numbers greater than 139; if not, the malware skips processing that content. The second line is for the URL the malware should use to download an executable and the third line specifies the file name for the downloaded executable that is dropped into the file system. After downloading the malware restores 2 bytes "MZ" at the very beginning of the dropped file and runs it.

At the same time as it is downloading, the malware tries to remove specific antivirus software. On finding an uninstall command line in the registry the malware runs it and by manipulating the user interface buttons of the application it tries to remove three AV products: AhnLab's V3 Lite, AhnLab's V3 365 Clinic and ESTsoft's ALYac. Although there is a process for those products only, the malware also includes inactive functions to disable Naver Vaccine and McAfee Security Center. The origin of those vendors clearly suggests that the malware was intended for targets in South Korea.

Since the malware is already quite old we have not been able to download any relevant material from the URLs specified both in the 1st and 2nd downloaders. Servers have been responding with nothing or pages stating the absence of content.

Earlier discovery

We were not actually the first AV company to encounter HDRoot malware face to face. At the end of 2013 South Korean AhnLab issued a comprehensive report on the ETSO Hacking group based on incident response cases their digital forensic team was working on. ETSO malware, according to AhnLab's classification, mostly corresponds to Winnti malware as we detect it. During their analysis AhnLab's engineers discovered infected MBRs that, according to their description (pages 14-15, chapter "2.5 Maintain Network Presence"), sound like the result of an HDRoot bootkit installer at work:



AhnLab's HDRoot scheme of work

Also, we know about incident handlers not necessarily from AV companies that are acquainted with the HDD Rootkit utility. However, when it comes to detection, despite the fact that this dangerous threat is quite old, antivirus products were not that good at detecting it.

Statistics

As expected, HDRoot infections prevail in Winnti's traditional region of primary interest – South East Asia, especially South Korea, according to KSN. But other parts of the world have also been affected and the extent and impact of this threat may be significant.

HDRoot-related malware hits

It's important to point out that the numbers don't represent the nature of the targets. It means that by simply looking at the numbers we can't see what sort of companies were attacked. Hence, the map may present a different story from the reality in terms of probable damage for a particular country.

For example, we were involved in mitigating an HDRoot infection in two major companies in Russia and the UK where the malware was discovered on multiple servers with the use of our products. In both cases, the damage due to infection could be very significant, especially in Russia where many of the company's customers could have been affected. However, on the map Russia is shown as having suffered just a single hit, while the UK has 23 attacked systems.

Although we have not found many malware families installed using HDRoot, and attribute known HDRoot-related activity to Winnti, we continue to assume that this bootkit may be used in multiple APT. We already know about an overlap in Winnti activity and other APT from previous incidents. Taking into account the HDRoot installer's nature as a standalone tool, it's very possible that this bootkit could be in the hands of other threat actors.

We detect HDRoot malware with following verdicts:

Hacktool.Win32.HDRoot
Hacktool.Win64.HDRoot
Rootkit.Win32.HDRoot
Rootkit.Win64.HDRoot
Trojan.Boot.HDRoot

Backdoors and downloaders related to HDRoot bootkit:

Backdoor.Win64.Winnti
Trojan.Win32.Agentb.aemr
Trojan.Win32.Genome.amvgd

Indicators of Compromise

Samples hashes

2c85404fe7d1891fd41fcee4c92ad305
4dc2fc6ad7d9ed9fcf13d914660764cd
8062cbccb2895fb9215b3423cdefa396
c7fee0e094ee43f22882fb141c089cea
d0cb0eb5588eb3b14c9b9a3fa7551c28
a28fe3387ea5352b8c26de6b56ec88f0
2b081914293f415e6c8bc9c2172f7e2a
6ac4db5dcb874da2f61550dc950d08ff
6ae7a087ef4185296c377b4eadf956a4
e171d9e3fcb2eeccdc841cca9ef53fb8
ae7f93325ca8b1965502b18059f6e46a
e07b5de475bbd11aab0719f9b5ba5654
d200f9a9d2b7a44d20c31edb4384e62f
cc7af071098d3c00fdd725457ab00b65
c0118c58b6cd012467b3e35f7d7006ed
c8daf9821ebc4f1923d6ddb5477a8bbd
755351395aa920bc212dbf1d990809ab
11e461ed6250b50afb70fbee93320131
acc4d57a98256dfaa5e2b7792948aaae
1c30032dc5435070466b9dc96f466f95
7d1309ce050f32581b60841f82fc3399
b10908408b153ce9fb34c2f0164b6a85
eb3fbfc79a37441590d9509b085aaaca
3ad35274cf09a24c4ec44d547f1673e7
f6004cfaa6dc53fd5bf32f7069f60e7a
c5d59acb616dc8bac47b0ebd0244f686
e19793ff58c04c2d439707ac65703410
4dc2fc6ad7d9ed9fcf13d914660764cd
8062cbccb2895fb9215b3423cdefa396
c7fee0e094ee43f22882fb141c089cea
d0cb0eb5588eb3b14c9b9a3fa7551c28

Files

%windir%twain.dll
%windir%systemolesvr.dll
%windir%msvidc32.dll
%windir%helpaccess.hlp
%windir%syswow64C_932.NLS
%windir%syswow64C_20949.NLS
%windir%syswow64irclass.dll
%windir%syswow64msvidc32.dll
%windir%syswow64kmddsp.tsp
%windir%tempsvchost.exe
%System32%wbemntfs<3 random chars>.mof
%System32%DriversLst_Update.sys
%Systemroot%Helpperfc009.dat
%windir%bootmgr.exe
%windir%hall32.exe
%windir%system32midimapbits.dll
%windir%system32mpeg4c32.dll
%windir%bootmgr.dat
%windir%v3update000.exe
%windir%v3update001.exe
%windir%v3update002.exe
%windir%svchost.exe
%windir%winurl.dat
%windir%image.jpg
