threatgeek.com

Turbo Twist: Two 64-bit Derusbi Strains Converge

by Threatgeek • May 2, 2016 • 4 min read • original

To follow up on the March report on the discovery of a 64-bit Linux variant of Derusbi used in the Turbo campaign, this post covers our analysis of two unique Windows variants of the Derusbi PGV_PVID malware. Derusbi has been widely covered and associated with numerous Chinese cyber espionage actors, including the group known as C0d0s0 Team (aka Sunshop Group) and its watering-hole attacks using Forbes[.]com in 2014.

What made these two variants of interest is that, as of April 28, 2016, there are zero (0) antivirus detections of these variants at VirusTotal. On April 29, our team also scanned these variants with two different local antivirus tools running the latest virus signatures and the APT malware was still undetected. Based on compile times in the variants analyzed, it appears that this variant has been around since at least 2013.

Some of the strings in these variants have also been observed in variants of the Bergard APT malware. The Derusbi variants were identified and named by Proofpoint earlier this year.

Our Yara hunting rule that detected these two Derusbi PGV_PVID variants with zero antivirus detections also detected two other variants that are detected by AVs as "Derusbi". One of the Derusbi PGV_PVID samples that we analyzed shares its command-and-control server with a Rekaf sample identified by Proofpoint, **furthering the connection between these families that they established in their post**.

Interestingly, at least one of the domains used here is currently registered with the China-based domain broker we identified in the Turbo campaign report. After doing some pivots involving the IP addresses observed in our analysis, we have a trove of very interesting domains, all listed at the bottom of this report. These domains include ones that might purport to represent prominent U.S. defense contractors, media outlets, etc. It has to be noted that we have not identified malware or a campaign that uses these domains, but in our observation, the purpose of registering these domains would be to launch a targeted campaign against the named organization or others that trust them, such as partners and customers. These techniques were widely observed in 2015, in events involving U.S. OPM, Anthem Healthcare, etc.

These domain pivots have also shown us further connections between these PGV_PVID, Rekaf and Bergard variants of Derusbi. The specific indicators are provided later in this post, but the relationship is illustrated with these tables. The dates on these records is worth noting, since it could potentially indicate campaign periods.

Passive DNS relationship

Domain	**google-dash[.]com**	**office365e[.]com**
Record Type		
Time	first seen 04-09-2016 last seen 04-19-2016	first seen 04-25-2016 last seen 04-29-2016

* Source DomainTools/Farsight DNSDB

Passive DNS relationship from 121.54.168[.]216

Domain	**google-dash[.]com**	**ukoffering[.]com**	**microsoft-cache[.]com**
Record Type			
Time	first seen 01-14-2016 last seen 04-02-2016	first seen 01-29-2016 last seen 02-02-2016	first seen 01-03-2016 last seen 01-23-2016

* Source DomainTools/Farsight DNSDB

In this vein, there's a clear preponderance of popular online services and technologies – variants of Google, Office 365, Virtualbox and VMtools feature in this domain set. It has to be noted that these are technologies that are very popular across a broad set of enterprises and offer a very broad set of opportunities.

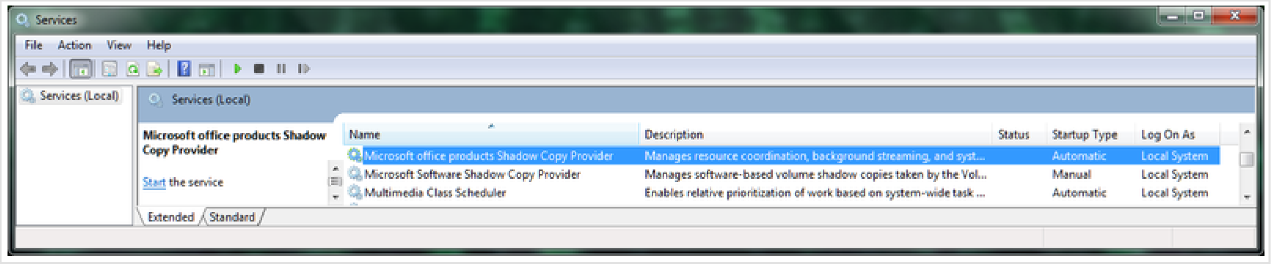
Malware Analysis

All four variants perform an HTTP request that is almost identical, with the exception of the Command & Control server and a small variant in one of the "Referrer" values. Even a 16-digit value in the URL and Cookie was the same. This beacon format and 16-digit value was also observed in the PGV_PVID variants analyzed earlier this year by Proofpoint.

Three of the samples contained the following string of interest: "payload_service_x64.dll".

These PGV_PVID variants were observed encoding some of its configuration, APIs and other strings with a single-byte XOR key. Some of the keys used are: 0x90, 0xEB and 0x57.

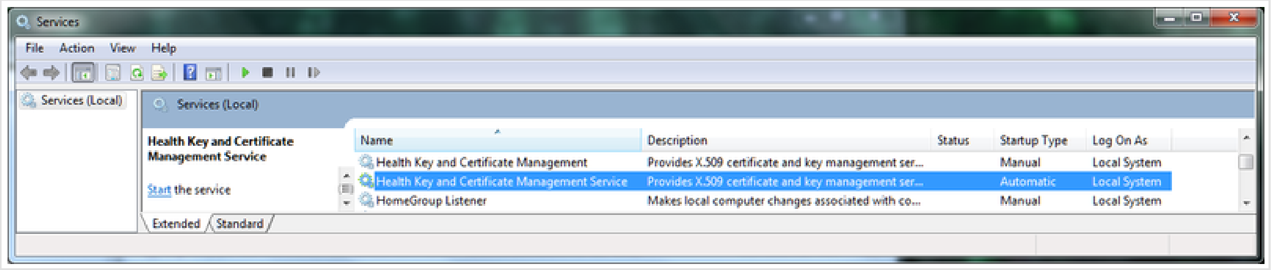
It was also interesting to see how these samples were trying to disguise themselves during entrenchment as valid services in the system to try to confuse incident responders, computer forensics investigators and network administrators. The following screenshots show the Microsoft service management console with the legit and malicious service (malicious service highlighted):



Microsoft office products Shadow Copy Provider

Start the service

Name	Description	Status	Startup Type	Log On As
Microsoft office products Shadow Copy Provider	Manages resource coordination, background streaming, and syst...		Automatic	Local System
Microsoft Software Shadow Copy Provider	Manages software-based volume shadow copies taken by the Vol...		Manual	Local System
Multimedia Class Scheduler	Enables relative prioritization of work based on system-wide task ...		Automatic	Local System



Health Key and Certificate Management Service

Start the service

Name	Description	Status	Startup Type	Log On As
Health Key and Certificate Management	Provides X.509 certificate and key management ser...		Manual	Local System
Health Key and Certificate Management Service	Provides X.509 certificate and key management ser...		Automatic	Local System
HomeGroup Listener	Makes local computer changes associated with co...		Manual	Local System

The following is a list of the malware samples analyzed:

MD5	CnC	AV detections	Compiled Date
3e4fbb9190227848af32dacb17e9fd17	google-dash*[dot]*com	0	12/4/14
b93197e2aa147fe6b70695ae7bb298b0	office365e*[dot]*com	0	12/4/14
4979e819d3ffbea81c7111fb515c1c7	web01.kruul*[dot]*com	22	4/11/13
791295ef196cf8c20913b3cce76af29a	google-dash*[dot]*com	16	12/4/14

Two samples of the network traffic format associated with this threat:

1. b93197e2aa147fe6b70695ae7bb298b0

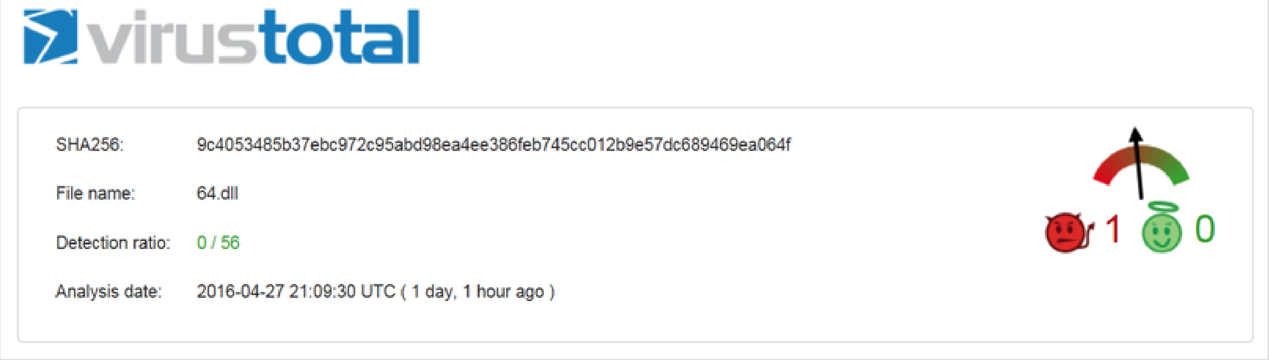
```
GET /pki/nss/init?0220372661170240 HTTP/1.1
Referer: http://www.microsoft.com/
Accept: */*
Accept-Language: en-us
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Win32)
Host: office365e[dot]com:80
Cache-Control: no-cache
Connection: Keep-Alive
Cookie: pgv_pvid=0220372661170240
```

2. 3e4fbb9190227848af32dacb17e9fd17

```
GET /pki/nss/init?0220372661170240 HTTP/1.1
Referer: http://www.google.com/
Accept: */*
Accept-Language: en-us
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Win32)
Host: www.google-dash[dot]com:80
Cache-Control: no-cache
Connection: Keep-Alive
Cookie: pgv_pvid=0220372661170240
```

Antivirus detection for two of the samples:

1. 3e4fbb9190227848af32dacb17e9fd17



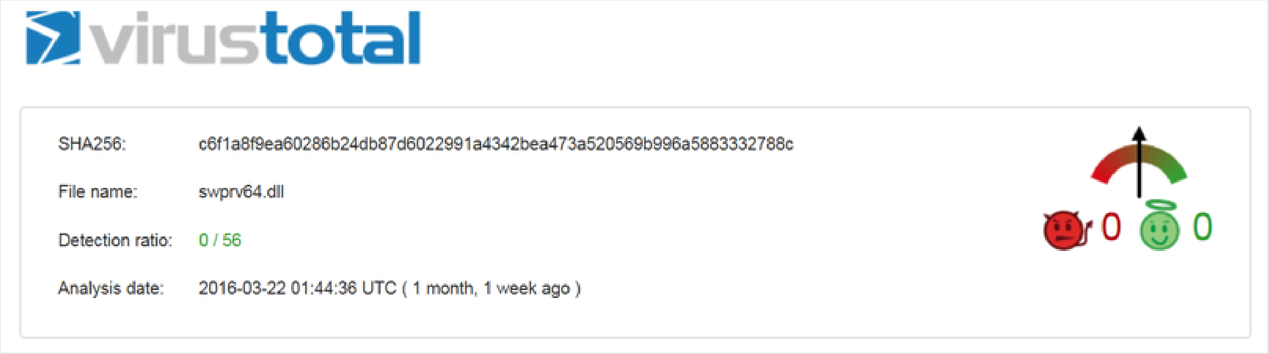
SHA256: 9c4053485b37ebc972c95abd98ea4ee386feb745cc012b9e57dc689469ea064f

File name: 64.dll

Detection ratio: 0 / 56

Analysis date: 2016-04-27 21:09:30 UTC (1 day, 1 hour ago)

2. b93197e2aa147fe6b70695ae7bb298b0



SHA256: c6f1a8f9ea60286b24db87d6022991a4342bea473a520569b996a5883332788c

File name: swprv64.dll

Detection ratio: 0 / 56

Analysis date: 2016-03-22 01:44:36 UTC (1 month, 1 week ago)

Indicators of Compromise

Registry Entrenchment

- HKLM\System\CurrentControlSet\services\hkmservice\Paramet [CWD]\64.dll

- HKLM\System\CurrentControlSet\services\swprvsvc\Parameters\ServiceDll=[CWD]\swprv64.dll
- HKLM\SOFTWARE\Microsoft\Active Setup\Installed Components\{BD5A117E-658C-4b8c-AED3-3D177B36F0A8}\stubpath=C:\Windows\system32\regsvr32.exe /s [CWD]\MSChartCtrl.ocx

Service Information

- Display Name 1: Health Key and Certificate Management Service
- Service Name 1: hkmservice
- Display Name 2: Microsoft office products Shadow Copy Provider
- Service Name 2: swprvsvc

Mutex

- 2-7-26-96EFFFFD-6666-706b-6506-3B6BC6486663-0-7-2
- 1-5-19-85EDC10D-6745-404b-A50D-4BCBC6480873-1-5-19

Command & Control Servers

- google-dash*[dot]*com
- office365e*[dot]*com
- kruul*[dot]*com
- nsa.org*[dot]*cn

URLs

- /projects/security/pki/nss/index.htm?*[16 digits]*
- /developers/menu.php?*[16 digits]*
- /pki/nss/init?*[16 digits]*
- /solutions/company-size/smb/index.htm?*[16 digits]*
- /selfservice/microsites/search.php?*[16 digits]*
- /store/category_groups?*[16 digits]*

Yara detection rule

The following Yara rule was created to detect these samples:

```
rule apt_win32_dll_bergard_pgv_pvid_variant
        meta:
                copyright = “Fidelis Cybersecurity”
        strings:
                $ = ”Accept:”
                $ = ”User-Agent: %s”
                $ = ”Host: %s:%d”
                $ = ”Cache-Control: no-cache”
                $ = ”Connection: Keep-Alive”
                $ = ”Cookie: pgv_pvid=”
                $ = ”Content-Type: application/x-octet-stream”
                $ = ”User-Agent: %s”
                $ = ”Host: %s:%d”
                $ = ”Pragma: no-cache”
                $ = ”Connection: Keep-Alive”
                $ = ”HTTP/1.0”
        condition:
                (uint16(0) == 0x5A4D) and (all of them)
```

Domains identified from pDNS pivots

asixgroupincmeer[.]biz

attrcorp[.]com

smtp.attrcorp[.]com

office365e[.]com

office365e[.]com

usapappers[.]com

e.usapappers[.]com

bee.usapappers[.]com

ftp.usapappers[.]com

sun.usapappers[.]com

wow.usapappers[.]com

shot.usapappers[.]com

email.usapappers[.]com

dijlacultus[.]com

bbs.dijlacultus[.]com

fok.dijlacultus[.]com

back.dijlacultus[.]com

info.dijlacultus[.]com

live.dijlacultus[.]com

mail.dijlacultus[.]com

news.dijlacultus[.]com

serv.dijlacultus[.]com

tele.dijlacultus[.]com

thec.dijlacultus[.]com

zero.dijlacultus[.]com

swiss.dijlacultus[.]com

living.dijlacultus[.]com

mailsrv.dijlacultus[.]com

google-dash[.]com

virtualboxs[.]com

steletracker[.]com

vmtools[.]net

pwc.vmtools[.]net

win.winlogon[.]net

asia.winlogon[.]net

winner.winlogon[.]net

hawkthorn[.]net

strightspunddeals[.]net

northropgruman[.]org

owa.northropgruman[.]org

vpn.northropgruman[.]org

soft.northropgruman[.]org

update.northropgruman[.]org

software.northropgruman[.]org

cegauoqsykgqecqc[.]org

eimqqakugeccgwak[.]org

uogwoigiuweyccsw[.]org

soyy[.]info

haha[.]school

ns1.krimeware[.]com

ns2.krimeware[.]com

tianzhen[.]co

www[.]tianzhen[.]co

monsterlegendsvn[.]biz

www[.]monsterlegendsvn[.]biz

nickytoh[.]com

www[.]nickytoh[.]com

seratjati[.]com

aiselamodefactory[.]com

tasty-and-healthy[.]com

nickytoh[.]net

www[.]nickytoh[.]net

animationmyth[.]net

www[.]animationmyth[.]net

petersenstore[.]org

www[.]petersenstore[.]org

forum.haha[.]school

musicis[.]science

References

-- The Fidelis Threat Research Team

Original URL:
http://www.threatgeek.com/2016/05/turbo-twist-two-64-bit-derusbi-strains-converge.html