Dec 2012 Dexter - POS Infostealer samples and information

contagiodump.blogspot.com/2012/12/dexter-pos-infostealer-samples-and.html

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
fb46ea9617e0c8ead0e4358da6233f3706cfc6bbbeba86a87aaab28bb0b21241

Additional Files

65f5b1d0fcdaff431eec304a18fb1bd6
7e327be39260fe4bb8923af25a076cd3569df54e0328c7fe5cd7c6a2d3312674

560566573de9df114677881cf4090e79
28a26fe50e2d4e2b541ae083aa0236bd484c7eb3b30cf9b5a7f4d579e77bf438

1f03568616524188425f92afbea3c242
bdbe024a08c9a4e62c5692762aa03b4c1e564b38510cb4b4b1758e371637edb4

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
70feec581cd97454a74a0d7c1d3183d1 (Seculert MD5)
==========
cae3cdaaa1ec224843e1c3efb78505b2e0781d70502bedff5715dc0e9b561785
70feec581cd97454a74a0d7c1d3183d1 (Seculert MD5)

%userprofile%\Application Data\fubqq\fubqq.exe
injected in iexplore.exe

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?):
11e2540739d7fbea1ab8f9aa7a107648.com
7186343a80c6fa32811804d23765cda4.com
e7dce8e4671f8f03a040d08bb08ec07a.com
e7bc2d0fceee1bdfd691a80c783173b4.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
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)
==========
fb46ea9617e0c8ead0e4358da6233f3706cfc6bbbeba86a87aaab28bb0b21241
%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@@YGKPAUHKEY__@@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
ASCI 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**

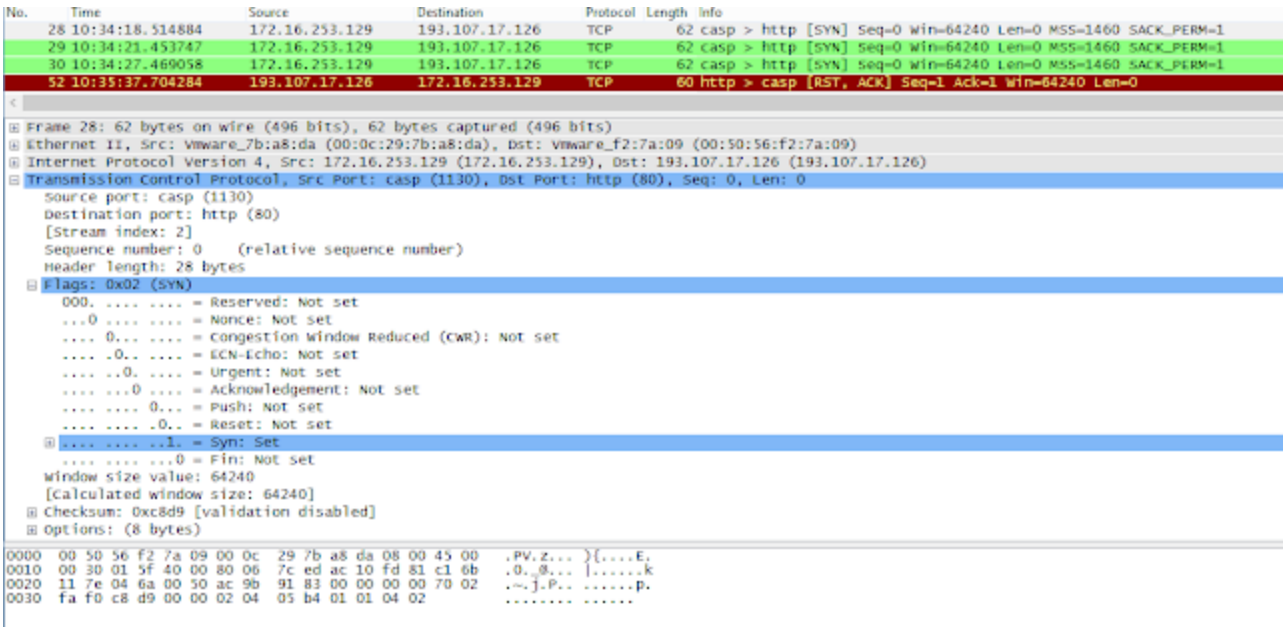
http://193.107.17.126:80/test/gateway.php

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 NOCaddress: Sound & Vision House, Francis Rachel Str. address: Victoria, Mahe, Seychelles remarks: **********

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



6

65F5B1D0FCDAFF431EEC304A18FB1BD6

==========

7e327be39260fe4bb8923af25a076cd3569df54e0328c7fe5cd7c6a2d3312674

65F5B1D0FCDAFF431EEC304A18FB1BD6

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

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

		Frames	Bytes		Frames	Bytes		Frames	Bytes
172.16.253.255	<->	172.16.253.1	30	9000	0	0	30	9000
193.107.17.126	<->	172.16.253.131	9	558	2	120	11	678

pcap and traffic same as above.

ASCI 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\aewtm\aewtm.exe
URL
http://193.107.17.126:80/test/gateway.php

ASCI 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