Sept 21 Greedy Shylock - financial malware

contagiodump.blogspot.com/2011/09/sept-21-greedy-shylock-financial.html

Not one, my lord.
Besides, it should appear, that if he had
The present money to discharge the Jew,
He would not take it. Never did I know
A creature, that did bear the shape of man,
So keen and greedy to confound a man:
(The Merchant of Venice W. Shakespeare Act 3, Scene 2)

On September 7, 2011 (2011-09-13T06:44:39+0000), Trusteer announced they are investigating new financial malware they called Shylock that "uses unique mechanisms not found in other financial malware toolkits, including: an improved method for injecting code into additional browser processes to take control of the victim's computer; a better evasion

technique to prevent malware scanners from detecting its presence; a sophisticated watchdog service that allows it to resist removal attempts and restore operations"

Trusteer called the malware Shylock for Shakespeare quotes in the properties of the file.

publisher....: He is ready at the door
copyright....: (c) 2009
product.....: He is
description..: So keen and greedy to confound a man
or
publisher....: To take a tedious leave thus
copyright....: (c) 2008
product.....: To take
description..: Exeunt GRATIANO and LORENZO

or
publisher....: And so riveted with faith unto
copyright....: (c) 2009
product.....: And so
description..: And be a day before our husbands home

or
publisher....: Therefore he hates me
copyright....: (c) 2009
product.....: Therefore he
description..: Thou almost makest me waver in my faith
or
publisher....: Which makes me think that this
copyright....: (c) 2009
product.....: Which makes
description..: price of hogs if we grow all to be porkeaters we
or
publisher....: I humbly do desire your grace
copyright....: (c) 2009
product.....: I humbly
description..: The dearest friend to me the kindest man

and so on

Read more about greedy Shylock from Merchant of Venice here. Read more about Shylock malware below

Exploit information and analysis links

- New Trusteer Cybercrime Prevention Architecture Adds Browser Exploit Removal and Fraudster Machine Fingerprinting to Arsenal - Trusteer
- Signature and Traffic - ET TROJAN Shylock Module Server Response Emerging sigs
- http://www.threatexpert.com/report.aspx?md5=4fda5e7e8e682870e993f97ad26ba6b2
- Debugging Injected Code with IDA Pro by malwareninja
- Shylock via volatility

The file is digitally signed by an invalid digital certificate - the CN may vary

> 00 df 44 1a bc fc 5b 32 fa
> CN = Astothyfriendsforwhendidfriendshiptake
> Thursday, August 18, 2011 7:08:46 PM
> Wednesday, May 14, 2014 7:08:46 PM

ANTONIOI am as like to call thee so again,To spit on thee again, to spurn thee too.If thou wilt lend this money, lend it notAs to thy friends; for when did friendship takeA breed for barren metal of his friend?But lend it rather to thine enemy,Who, if he break, thou mayst with better faceExact the penalty. *(The Merchant of Venice W. Shakespeare Act 1, Scene 2)*

```
sigcheck:
publisher....: He is ready at the door
copyright....: (c) 2009
product......: He is
description..: So keen and greedy to confound a man
original name: He.exe
internal name: He.exe
file version.: 5.1.4.153 (win7_rtm.090713-1255)
comments.....: n/a
signers......: -
signing date.: -
verified.....: Unsigned
```

General File Information

MD5:
4fda5e7e8e682870e993f97ad26ba6b2
bae400baf6760a1646cd44e348eea0f7
742cfd2be5d44fa072802bd4b031e818
1fd7cf2405ae599c1a91fe75912d18ff
d74f5f045c4b0f1d61746ded3a2a152e
fe17c2cddffd731ee6a34457121c6b20
a8ff900f5f3134a1f04d9217ab2d5dd0
715fb3cef70458b857bd55a0259a1265 - unconfirmed - see this related
5571be9c7b0d2e950bada71e72984e7a
72ace5e603bb4a5e2d8ef4434dc31417
9a8657a61daeafd7053017103ab53cd6
File Type: exe

Download

Email me if you need the password

Automated Scans

Original scan:
http://www.virustotal.com/file-scan/report.html?id=4c71d1e15287d7a90b0526c23dbe21400a65fe683eb75e88368696f1aa24ac21-1314121053
File name:
d1b17c351bafc899ba14c84e09b5cc258a2195bf
2011-08-23 17:37:33 (UTC)
Result:4 /44 (9.1%)
Comodo 9847 2011.08.23 TrojWare.Win32.Trojan.Agent.Gen
Kaspersky 9.0.0.837 2011.08.23 UDS:DangerousObject.Multi.Generic
Symantec 20111.2.0.82 2011.08.23 Suspicious.Cloud.5
MD5 : 4fda5e7e8e682870e993f97ad26ba6b2

Scan dated today:
4FDA5E7E8E682870E993F97AD26BA6B2
Submission date:2011-09-21 20:29:18 (UTC)
Current status: Result:29 /43 (67.4%)
http://www.virustotal.com/file-scan/report.html?id=4c71d1e15287d7a90b0526c23dbe21400a65fe683eb75e88368696f1aa24ac21-1316636958
AhnLab-V3 2011.09.21.02 2011.09.21 Win-Trojan/Caphaw.371800
AntiVir 7.11.15.3 2011.09.21 TR/Agent.hvbv
Avast 4.8.1351.0 2011.09.18 Win32:Malware-gen
Avast5 5.0.677.0 2011.09.18 Win32:Malware-gen
AVG 10.0.0.1190 2011.09.21 Agent3.AETB
BitDefender 7.2 2011.09.21 Gen:Variant.Kazy.35924
CAT-QuickHeal 11.00 2011.09.21 Trojan.Agent.hvbv
Comodo 10196 2011.09.21 TrojWare.Win32.Trojan.Agent.Gen
Emsisoft 5.1.0.11 2011.09.21 Backdoor.Win32.Caphaw!IK

F-Secure 9.0.16440.0 2011.09.21 Gen:Variant.Kazy.35924
Fortinet 4.3.370.0 2011.09.21 W32/Agent.TDB!tr
GData 22 2011.09.21 Gen:Variant.Kazy.35924
Ikarus T3.1.1.107.0 2011.09.21 Backdoor.Win32.Caphaw
Kaspersky 9.0.0.837 2011.09.21 Trojan.Win32.Agent.hvbv
McAfee 5.400.0.1158 2011.09.21 Artemis!4FDA5E7E8E68
McAfee-GW-Edition 2010.1D 2011.09.21 Artemis!4FDA5E7E8E68
Microsoft 1.7604 2011.09.21 Backdoor:Win32/Caphaw.A
NOD32 6483 2011.09.21 a variant of Win32/Kryptik.SHX
Norman 6.07.11 2011.09.21 W32/Suspicious_Gen2.QKYDE
nProtect 2011-09-21.02 2011.09.21 Gen:Variant.Kazy.35924
Panda 10.0.3.5 2011.09.21 Generic Trojan
PCTools 8.0.0.5 2011.09.21 Trojan.Gen
Sophos 4.69.0 2011.09.21 Troj/Agent-TDB
TheHacker 6.7.0.1.304 2011.09.21 Trojan/Agent.hvbv
TrendMicro 9.500.0.1008 2011.09.21 TROJ_GEN.R4FC2IH
TrendMicro-HouseCall 9.500.0.1008 2011.09.21 TROJ_GEN.R4FC2IH
VBA32 3.12.16.4 2011.09.21 Trojan.Agent.hvbv
VIPRE 10545 2011.09.21 Trojan.Win32.Generic!BT
VirusBuster 14.0.225.0 2011.09.21 Trojan.Agent!WmW5mI7QqD8
MD5 : 4fda5e7e8e682870e993f97ad26ba6b2

Traffic information from http://article.gmane.org/gmane.comp.security.ids.snort.emerging-sigs/12975/match=shylock

```
HTTP/1.1 200 OK
Server: nginx
Date: Sun, 21 Aug 2011 23:48:10 GMT
Content-Type: text/plain; charset=UTF-8
Content-Length: 39
Connection: keep-alive
Keep-Alive: timeout=20
X-Powered-By: PHP/5.2.17
Cache-Control: max-age=0
Expires: Sun, 21 Aug 2011 23:47:40 GMT

###ERROR_SRC###yes###ERROR_SRC_END###
-----

hxxp://nw-serv[.]cc/client.html
hxxp://m-sservices[.]at/client.html
hxxp://webhelper[.]at/client.html
hxxp://globstorage[.]at/client.html
hxxp://additional-group[.]at/client.html

nw-serv.cc                          91.223.180.66
m-sservices.at                      92.60.177.233
webhelper.at                        92.60.177.235
globstorage.at                      92.60.177.230
additional-group.at                 93.190.45.75

91.223.180.66    "56485 | UA | ripencc | 2011-03-02 | THEHOST-AS FOP
Sedinkin Olexandr Valeriyovuch"
92.60.177.233    "15772 | UA | ripencc | 2000-10-10 | WNET LLC W Net Ukraine"
92.60.177.235    "15772 | UA | ripencc | 2000-10-10 | WNET LLC W Net Ukraine"
92.60.177.230    "15772 | UA | ripencc | 2000-10-10 | WNET LLC W Net Ukraine"
93.190.45.75     "6849 | UA | ripencc | 1996-11-29 | UKRTELNET JSC UKRTELECOM,"
```