THREAT INTELLIGENCE REPORT

Proactive Threat Identification Neutralizes Remote Access Trojan Efficacy

By Levi Gundert

Vice President of Threat Intelligence

Recorded Future

Recorded Future

THREAT INTELLIGENCE REPORT

Proactive Threat Identification Neutralizes Remote Access Trojan Efficacy

By Levi Gundert

Executive's Business Case

Continuously incorporating known remote access trojan (RAT) controller locations into operational defense workflow and detection technologies is useful, and automating correlation with internal telemetry will identify potential infections, but the deeper value to the business, that reduces risk, is to understand the adversary behind each RAT instance.

Adversary attribution is difficult, but worthwhile, since motivation informs methodology. Exploring an attacker's capabilities and infrastructure becomes an ancillary benefit. One of the best ways to achieve consistent attribution results is to develop original attribution methodologies. An example of one such methodology – proactive Internet services enumeration – and the applied results for Trojans like njRAT and Dark Comet are detailed in this report.

Background

A remote access trojan (RAT)[1] is a feature-rich controller/server software suite that facilitates surreptitious (as its name suggests) and unauthorized access to a victim's computer. RATs are generally leveraged by adversaries with malicious intent to record local victim audio, video, keystrokes (in addition to exfiltrating files), and more[2].

The full spectrum of threat actors – especially criminals and nation-state agents – continue to leverage commodity RATs even after the original author has been apprehended[3]. Nation-state campaigns have routinely included payloads like Poison Ivy[4] and close derivatives because they are easy to configure, highly re-usable, and the RAT remains an effective tool against anti-virus software. This is especially true of dictatorial regimes that use RATs to hunt for the identity and location of political dissidents[5] within their own borders.

Criminals use RATs because the technical barriers to entry are low and the knowledge required to effectively operate a RAT can be quickly acquired from free Internet tutorials[6] which feature content such as packing/crypting[7] a RAT to evade anti-virus software; demonstrating capabilities with multiple victims[8]; and establishing infrastructure[9], like dynamic DNS (DDNS)[10], to support a long-term operation.

[1] A remote access tool (RAT) is legitimately used by system administrators. In this report's context, RAT is used to refer only to Trojans that are used for malicious purpose

[2] http://www.washingtonpost.com/news/morning-mix/wp/2014/05/20/5-scary-things-about-blackshades-malware/

[3] http://www.darkreading.com/over-90-arrested-in-global-fbi-crackdown-on-blackshades-rat/d/d-id/1252912

[4] http://www.crn.com/news/security/240160369/poison-ivy-attack-toolkit-with-ties-to-china-linked-to-other-hacking-groups.htm

[5] http://www.seculert.com/blog/2014/01/xtreme-rat-strikes-israeli-organizations-again.html
http://www.darkreading.com/over-90-arrested-in-global-fbi-crackdown-on-blackshades-rat/d/d-id/1252912

[6] http://www.reddit.com/r/hacking/comments/2acwpb/how_to_setup_dark_comet_rat_with_download_and/

[7] https://www.youtube.com/watch?v=QmH_ojSZoRU

[8] https://www.youtube.com/watch?v=5szajA_Xbps

[9] https://www.youtube.com/watch?v=fltTqccBmzY

[10] https://www.youtube.com/watch?v=tXVGLb96WHU

In a bit of a reversal from traditional botnet nomenclature, a commodity RAT file (executable) is typically labeled as the "server" when it is installed on a victim host (through any number of "spreading" mechanisms), and the client (control panel) "or controller" resides on the RAT operator's computer.

Historically, the security community has generally relied upon passive malware collection methodologies to identify RAT families and campaigns. Sources include customer telemetry, honeypots, and malware processing and aggregation services like VirusTotal. While these are useful resources, using them makes it is difficult to quickly and proactively identify all live instances of a particular RAT campaign. Additionally, the derivative insight that businesses rely on is largely reactive and only as good as the sources collecting the malware.

Today, threat intelligence teams continue to depend on the bulk processing of malware samples for derivative indicators of compromise (IOCs) that support new rules in defensive technologies. This approach, while partially effective, relies on large amounts of computing and Internet resources to process the tens (to hundreds) of thousands of daily malware samples collected by security vendors. The problem is that even anti-virus companies encounter challenges processing the vast amount of daily samples.

The solution is proactive and iterative large scale Internet enumeration (scanning), which allows businesses to identify hosts matching specific RAT signatures, and those hosts may lead to quick and direct operator attribution.

This scanning approach reveals a high number of RAT operator locations that were previously unknown to primary malware resources – VirusTotal and #totalhash. Additionally, many of the RAT controllers are located on residential ISP (Internet Service Provider) subnets, potentially indicating the RAT operator's physical location.

Originating Intelligence

Internet scanning was largely impractical when Nmap[11] was the only available off-the-shelf option (short of writing a custom asynchronous multithreading scanner). The release of Unicorn Scan[12], and more recent releases of Zmap[13], and MASSCAN[14] respectively, enabled the enumeration of the full IPv4 address space in a relatively short amount of time – minutes – from a single connected device. In addition to open port discovery, these tools return daemon banner information that is highly useful for identifying RAT controllers. Port scanning tools are often used to identify and count specific services available to the public Internet, and using these same tools to identify and profile RATs is advantageous both for law enforcement and operational defenders.

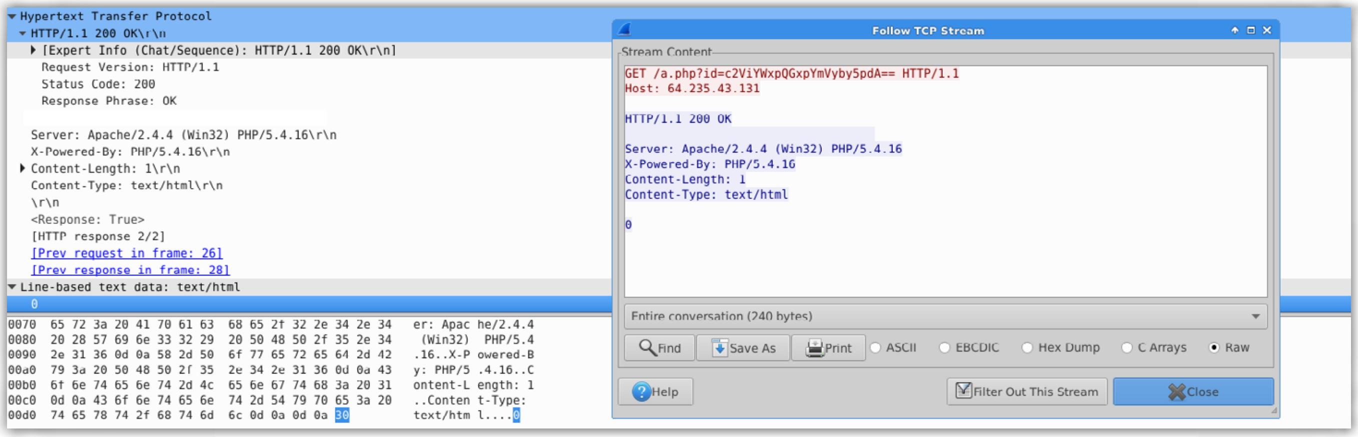
RATs return specific responses (strings) when a proper request is presented on the RAT controller's listener port. Specific signatures are withheld in this report to avoid adding a chapter to the threat actor playbook, but it is a straightforward process to profile a RAT family. In some cases, even a basic TCP three-way handshake[15] is sufficient to elicit a RAT controller response. The unique response is a fingerprint indicating that a RAT controller (control panel) is running on the computer in question. Therefore RAT controllers and their operators are inherently vulnerable because they are often operating openly on the Internet and they generate unique response strings when properly interrogated.

To profile a specific RAT family, samples and/or full packet captures (PCAP) must be obtained. Fortunately, there are numerous security researchers that publicly and generously share malicious code (malware) generated network packet captures[16].

[11] https://nmap.org/
[12] http://sectools.org/tool/unicornscan/
[13] https://zmap.io/
[14] https://github.com/robertdavidgraham/masscan
[15] https://support.microsoft.com/en-us/kb/172983
[16] http://contagiodump.blogspot.com/2013/04/collection-of-pcap-files-from-malware.html

Analysis of RAT controller responses within these packet captures leads to digital fingerprints that can be subsequently used in tandem with an Internet scanner to identify live instances of RAT controllers, and in some cases the RAT operator's home IP address and approximate geographic location.

For example, one version of a ubiquitous RAT returns a "0" subsequent to an HTTP GET method.



```
▾ Hypertext Transfer Protocol
  ▾ HTTP/1.1 200 OK\r\n
    ▸ [Expert Info (Chat/Sequence): HTTP/1.1 200 OK\r\n]
      Request Version: HTTP/1.1
      Status Code: 200
      Response Phrase: OK

    Server: Apache/2.4.4 (Win32) PHP/5.4.16\r\n
    X-Powered-By: PHP/5.4.16\r\n
  ▸ Content-Length: 1\r\n
    Content-Type: text/html\r\n
    \r\n
    <Response: True>
    [HTTP response 2/2]
    [Prev request in frame: 26]
    [Prev response in frame: 28]
▾ Line-based text data: text/html
    0
```

```
0070  65 72 3a 20 41 70 61 63  68 65 2f 32 2e 34 2e 34   er: Apac he/2.4.4
0080  20 28 57 69 6e 33 32 29  20 50 48 50 2f 35 2e 34    (Win32)  PHP/5.4
0090  2e 31 36 0d 0a 58 2d 50  6f 77 65 72 65 64 2d 42   .16..X-P owered-B
00a0  79 3a 20 50 48 50 2f 35  2e 34 2e 31 36 0d 0a 43   y: PHP/5 .4.16..C
00b0  6f 6e 74 65 6e 74 2d 4c  65 6e 67 74 68 3a 20 31   ontent-L ength: 1
00c0  0d 0a 43 6f 6e 74 65 6e  74 2d 54 79 70 65 3a 20   ..Conten t-Type: 
00d0  74 65 78 74 2f 68 74 6d  6c 0d 0a 0d 0a 30         text/htm l....0
```

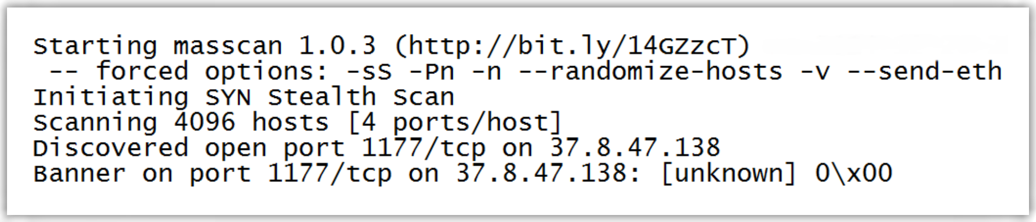
Stream Content

```
GET /a.php?id=c2ViYWxpQGxpYmVyby5pdA== HTTP/1.1
Host: 64.235.43.131

HTTP/1.1 200 OK

Server: Apache/2.4.4 (Win32) PHP/5.4.16
X-Powered-By: PHP/5.4.16
Content-Length: 1
Content-Type: text/html

0
```

Entire conversation (240 bytes)

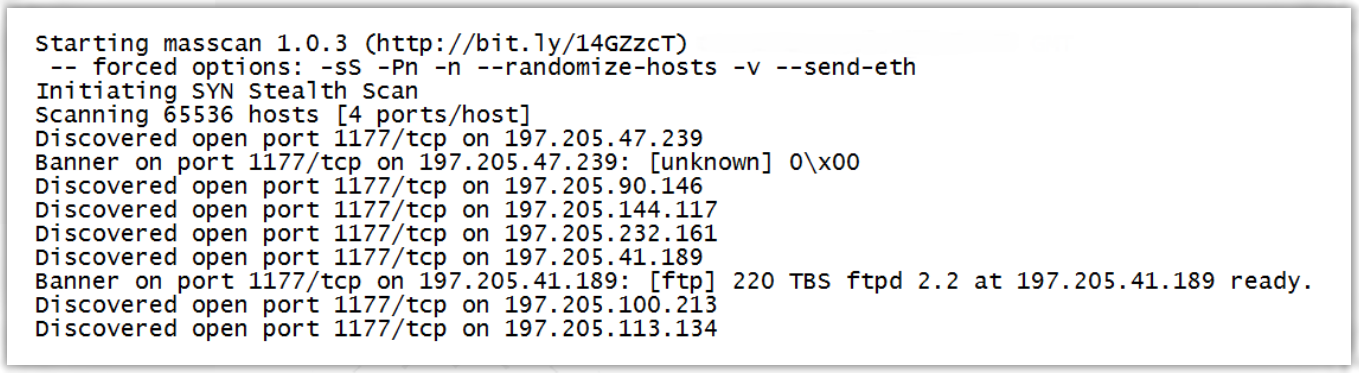
○ ASCII ○ EBCDIC ○ Hex Dump ○ C Arrays ● Raw

Enumeration of a /20 subnet in Palestine with MASSCAN reveals a signature match with a specific host on port 1177.



```
Starting masscan 1.0.3 (http://bit.ly/14GZzcT)
 -- forced options: -sS -Pn -n --randomize-hosts -v --send-eth
Initiating SYN Stealth Scan
Scanning 4096 hosts [4 ports/host]
Discovered open port 1177/tcp on 37.8.47.138
Banner on port 1177/tcp on 37.8.47.138: [unknown] 0\x00
```

Similarly, a scan of a /16 residential subnet in Algeria reveals multiple hosts listening on port 1177, but only one – 197.205.47.239 – that matches the above signature.



```
Starting masscan 1.0.3 (http://bit.ly/14GZzcT)
 -- forced options: -sS -Pn -n --randomize-hosts -v --send-eth
Initiating SYN Stealth Scan
Scanning 65536 hosts [4 ports/host]
Discovered open port 1177/tcp on 197.205.47.239
Banner on port 1177/tcp on 197.205.47.239: [unknown] 0\x00
Discovered open port 1177/tcp on 197.205.90.146
Discovered open port 1177/tcp on 197.205.144.117
Discovered open port 1177/tcp on 197.205.232.161
Discovered open port 1177/tcp on 197.205.41.189
Banner on port 1177/tcp on 197.205.41.189: [ftp] 220 TBS ftpd 2.2 at 197.205.41.189 ready.
Discovered open port 1177/tcp on 197.205.100.213
Discovered open port 1177/tcp on 197.205.113.134
```

Positive matches can be further confirmed via Curl[17] or Python Scapy[18] to identify potential false positives.

[17] http://curl.haxx.se/

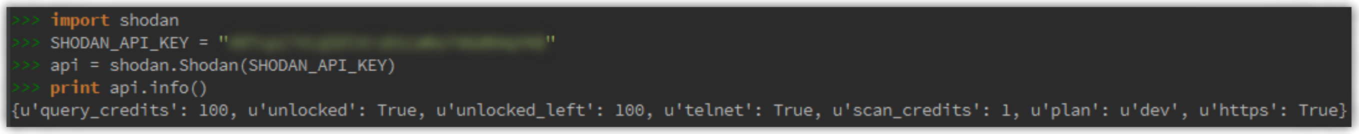
[18] http://www.secdev.org/projects/scapy/

Potentially there are additional legitimate daemons that may also return a "0," thus complete certainty about a positive RAT verdict in this case is absent. Rather, this is one example of RAT profiling with a fairly unique RAT controller response string.

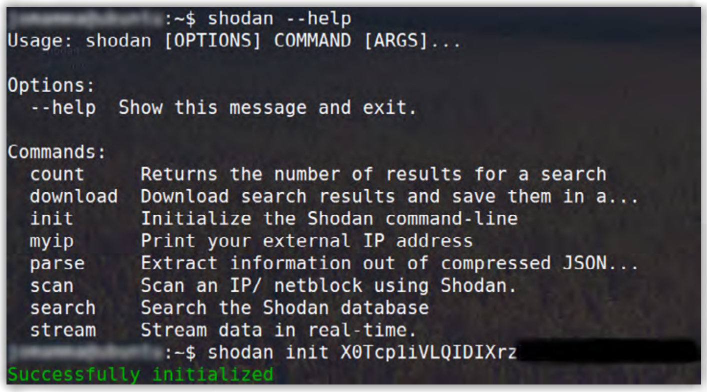
Another example is Havex RAT[19]. Netresec produced an informative blog in 2014[20] dissecting Havex's communication pattern. Noticeably, the Havex response includes the string "havex."

Scaling the Methodology

Shodan[21], the search engine for Internet services, created and currently maintained by John Matherly - is incorporated to scale RAT identification efforts. Shodan contains multiple benefits when compared to traditional scanning tools, including un-attributable tasking, continuous scanning without building and maintaining infrastructure, and Shodan contains hundreds of additional signatures for popular ports and services. Shodan's Web application and command line interface (CLI) are both easy to use, and Shodan results include all available port information for any given host.



```
>>> import shodan
>>> SHODAN_API_KEY = "[redacted]"
>>> api = shodan.Shodan(SHODAN_API_KEY)
>>> print api.info()
{u'query_credits': 100, u'unlocked': True, u'unlocked_left': 100, u'telnet': True, u'scan_credits': 1, u'plan': u'dev', u'https': True}
```

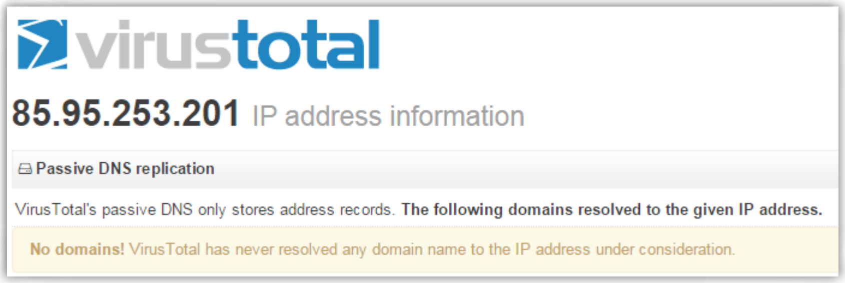


```
[redacted]:~$ shodan --help
Usage: shodan [OPTIONS] COMMAND [ARGS]...

Options:
  --help  Show this message and exit.

Commands:
  count     Returns the number of results for a search
  download  Download search results and save them in a...
  init      Initialize the Shodan command-line
  myip      Print your external IP address
  parse     Extract information out of compressed JSON...
  scan      Scan an IP/ netblock using Shodan.
  search    Search the Shodan database
  stream    Stream data in real-time.
[redacted]:~$ shodan init X0Tcp1iVLQIDIXrz[redacted]
Successfully initialized
```

Shodan's signatures also include RATs, specifically Black Shades, Dark Comet, njRAT, XtremeRAT, Poison Ivy, and Net Bus. Thus Shodan is a valuable and useful originating intelligence source for identifying live RAT controllers. While the number of results varies, Shodan typically identifies between 400 and 600 individual RAT controllers on any given day. The results from September 18, 2015, can be downloaded from Recorded Future's GitHub page.

A week's worth of consolidated and unique RAT controller IP addresses from early July 2015 totaled 633. The week following, VirusTotal returned derivative malware results for 153 of the 633 IP addresses or a 24% positive correlation rate[22]. Consequently, this originating methodology applied with Shodan identifies RAT controller instances often before the malware sample is submitted to VirusTotal, making it useful as a unique threat source.

[19] https://www.securityweek.com/attackers-using-havex-rat-against-industrial-control-systems
[20] http://www.netresec.com/?page=Blog&month=2014-11&post=Observing-the-Havex-RAT
[21] https://www.shodan.io/
[22] The VirusTotal results can be downloaded from Recorded Future's GitHub page.



85.95.253.201 IP address information

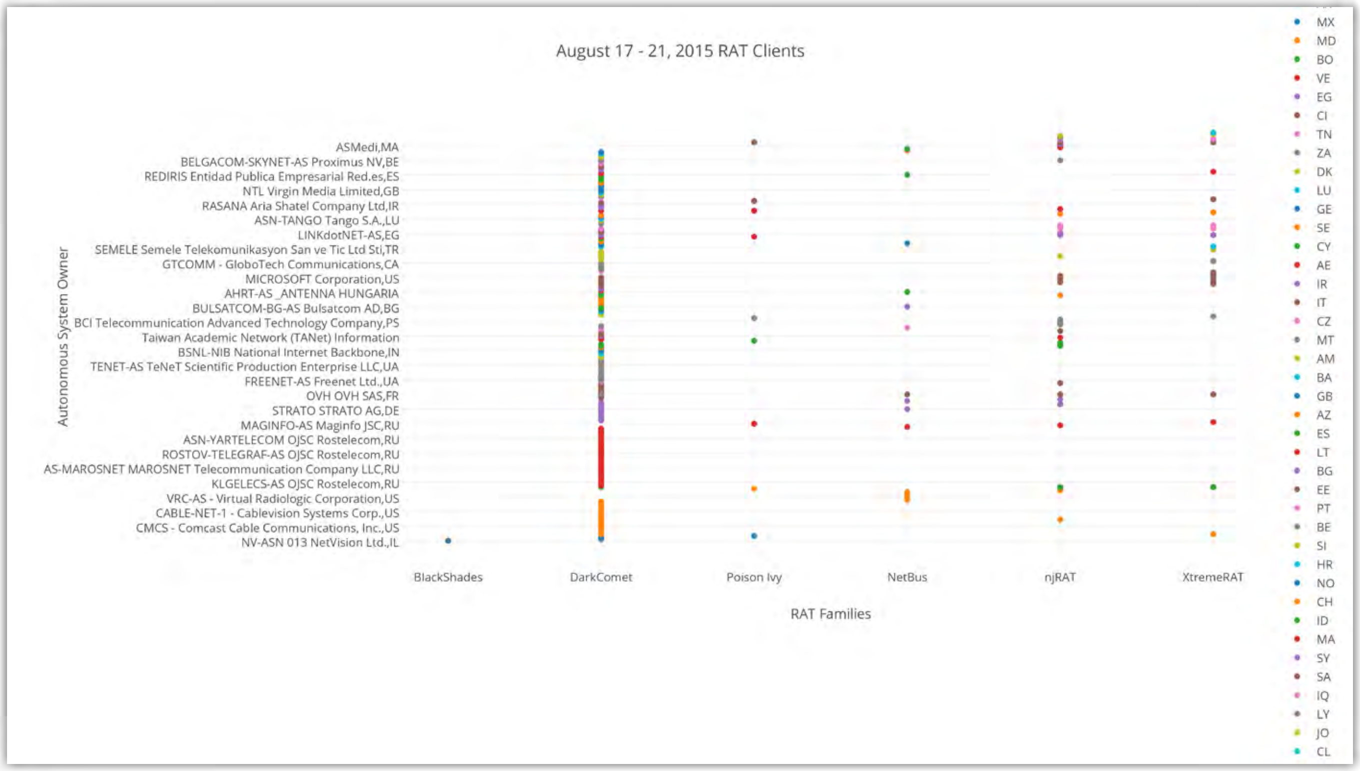
Passive DNS replication

VirusTotal's passive DNS only stores address records. **The following domains resolved to the given IP address.**

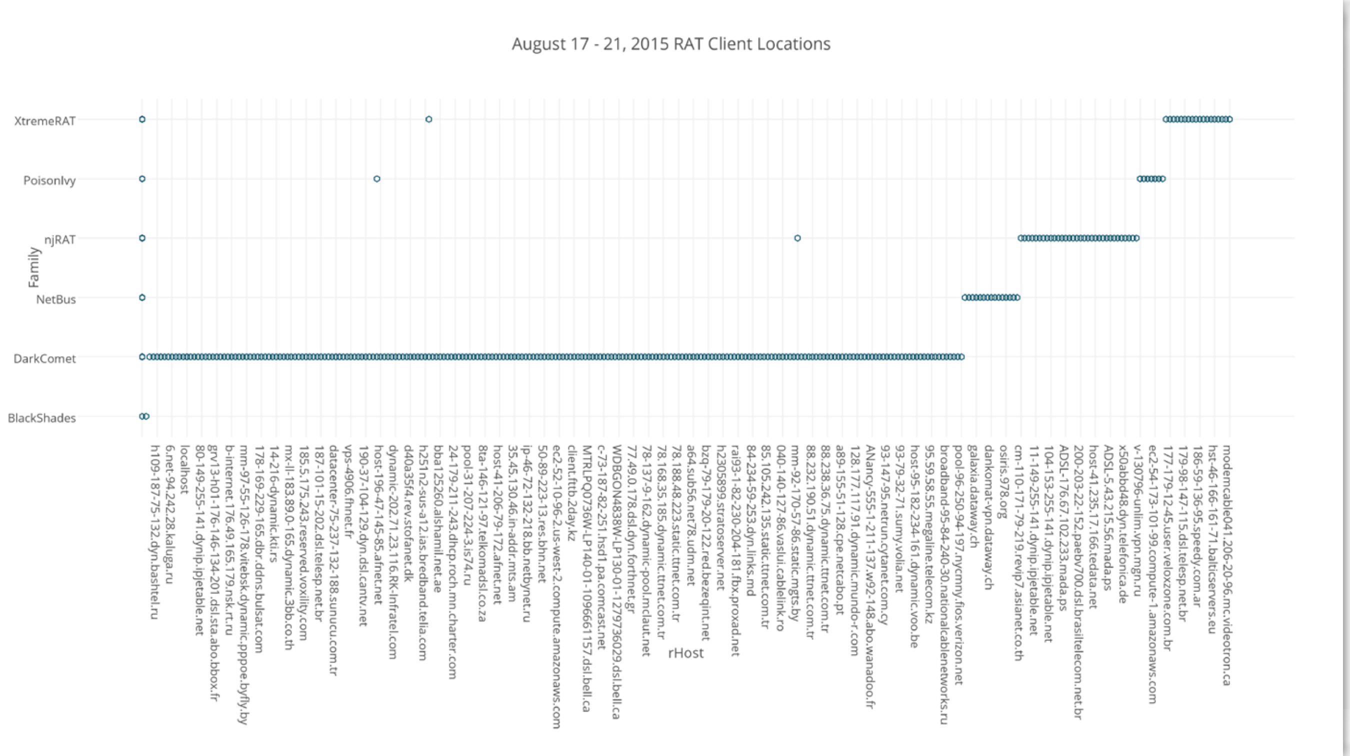
No domains! VirusTotal has never resolved any domain name to the IP address under consideration.

Further, many of the RAT IP addresses are located on residential (and dynamically allocated) networks. RAT operators often run the RAT control panel from home because proxies introduce latency which degrades performance, especially when the RAT operator is interested in collecting live video feeds from a victim's camera ("webcam"). In those countries where the unauthorized access of a computer is a crime, law enforcement need only send a subpoena (or equivalent) to the respective Internet Service Provider to identify the likely RAT operator's identity and residential location.

Between August 17-21, 2015 Shodan RAT results were collected and a list of 471 unique RAT controller locations were identified[23].



[23] https://github.com/recordedfuture/ioc-enrichment



Using the results from July and August 2105, the RAT controller locations were further enriched to understand individual instances, the corresponding RAT operators, and their respective motivations.

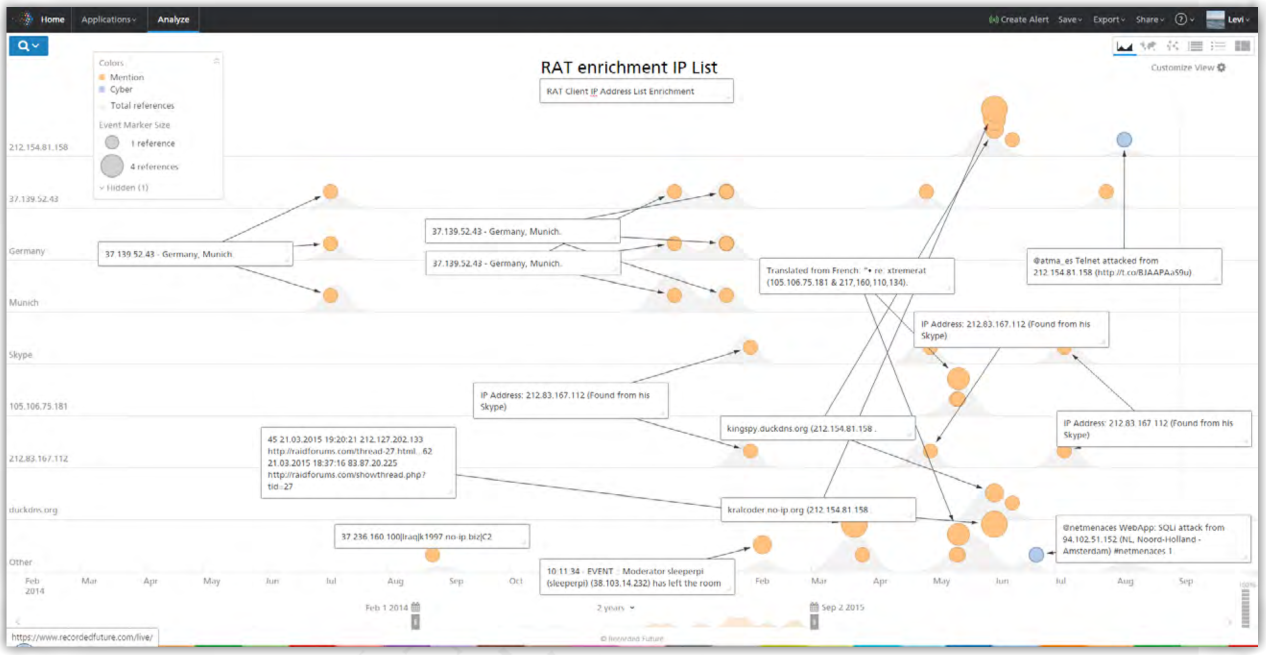
Enriching Intelligence

As previously mentioned, VirusTotal further confirms and enriches the RAT controller results with associated malware metadata. Additional valuable enrichment sources that are programmatically available include Team Cymru and Recorded Future.

Recorded Future's API offers valuable open source verdict confirmation and data enrichment. The Python API script used to produce the full Recorded Future results for the consolidated list of RAT IP addresses is located on Recorded Future's GitHub page.

A sampling of Record Future results from the consolidated list of Shodan's RAT controller IP addresses in early July include:

RAT Controller IP	Document URI	Fragment
105.106.75.181	http://forum.malekal.com/xtremerat-campagne-mails-francais-credit-mutuel-t51664.html#p397641	• Re: xtremerat (105.106.75.181).
37.139.52.43	http://www.facebook.com/406287246141601/posts/536666376437020	Kharkov S1 37.139.52.43 - Germany, 10:09:17 - EVENT :: Moderator sleeperpi (sleeperpi) (38.103.14.232) has entered the room
38.103.14.232	http://pastebin.com/tGT0nEvT	IP Address: 212.83.167.112 (Found from his Skype)
212.83.167.112	http://pastebin.com/cU4WX0hs	37.236.160.100|Iraq|k1997.no-ip.biz|C2
37.236.160.100	http://pastebin.com/2kGEjivz	83.87.20.225 http://raidforums.com/showthread.php?tid=27
83.87.20.225	http://pastebin.com/F6KnVR1q	Telnet attacked from 212.154.81.158 (http://t.co/BJAAPAaS9u)
212.154.81.158	https://twitter.com/atma_es/status/628301520853929985	This code was created on Saturday, March 21st, 2015 at 15:59 UTC from IP 197.2.24.60 (tn)
197.2.24.60	http://pastebin.com/xLTfgmrD	WebApp: SQLi attack from 94.102.51.152 (NL, Noord-Holland - Amsterdam) #netmenaces 1.
94.102.51.152	https://twitter.com/netmenaces/status/612103433273917440	
212.154.81.158	https://twitter.com/atma_es/status/628301520853929985	Telnet attacked from 212.154.81.158 (http://t.co/BJAAPAaS9u).
93.116.43.245	https://www.virustotal.com/en/file/	93.116.43.245:3333 .



RAT enrichment IP List

RAT Client IP Address List Enrichment

37 139 52.43 - Germany, Munich

37.139.52.43 - Germany, Munich.

37.139.52.43 - Germany, Munich.

Translated from French: "• re: xtremerat (105.106.75.181 & 217,160,110,134).

@atma_es Telnet attacked from 212.154.81.158 (http://t.co/BJAAPAaS9u)

IP Address: 212.83.167.112 (Found from his Skype)

IP Address: 212.83.167.112 (Found from his Skype)

45 21.03.2015 19:20:21 212.127.202.133 http://raidforums.com/thread-27.html...62 21.03.2015 18:37:16 83.87.20.225 http://raidforums.com/showthread.php?tid=27

kingspy.duckdns.org (212.154.81.158 .

IP Address: 212.83.167.112 (Found from his Skype)

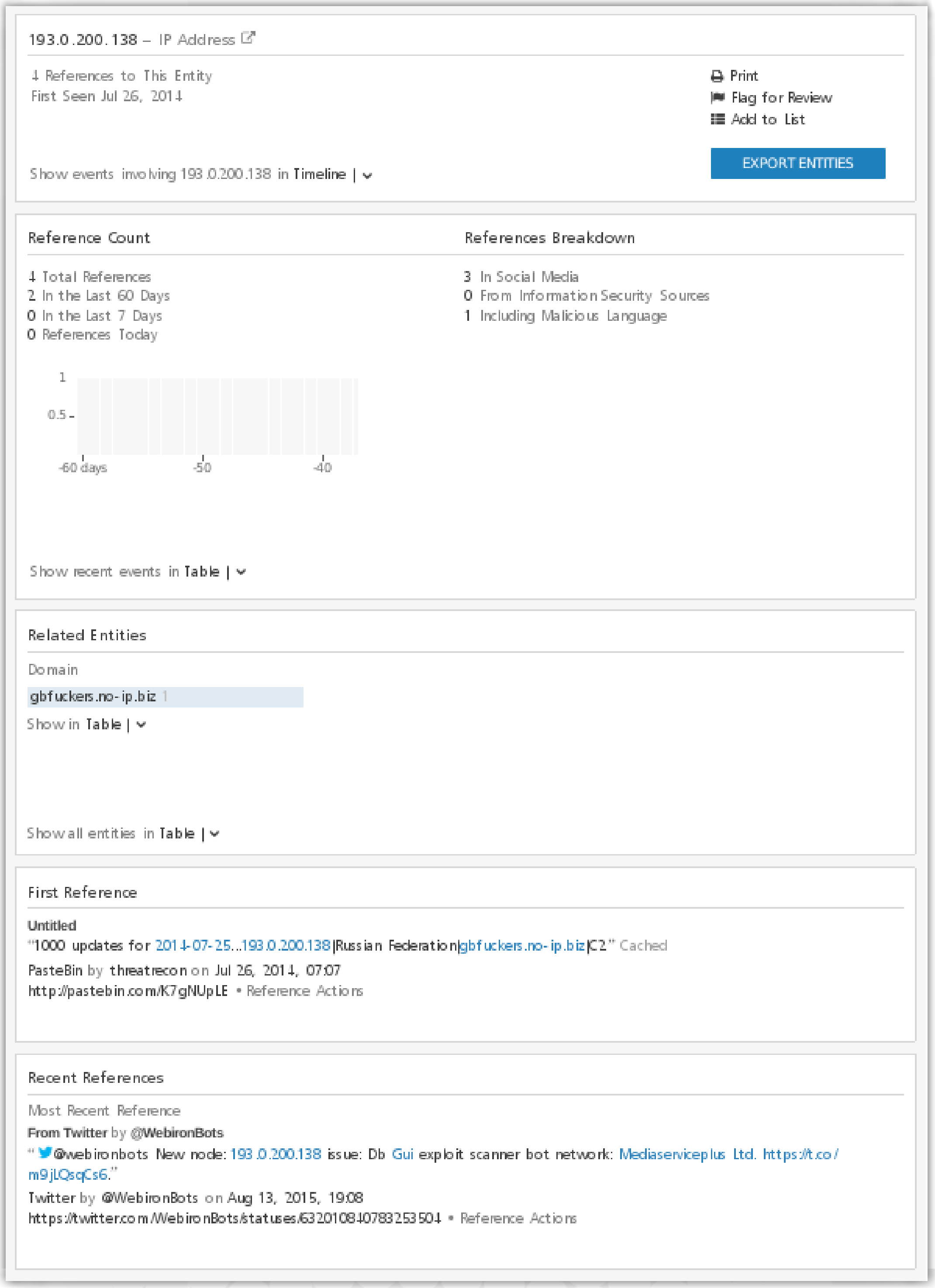
kralcoder.no-ip.org (212.154.81.158

37 236 160 100|Iraq|k1997 no-ip.biz|C2

@netmenaces WebApp: SQLi attack from 94.102.51.152 (NL, Noord-Holland - Amsterdam) #netmenaces 1

10:11:34 - EVENT :: Moderator sleeperpi (sleeperpi) (38.103.14.232) has left the room

To enrich the list of RAT controller locations from August 17-21, 2015, the list of IP addresses was submitted to Recorded Future and Virus Total. The Recorded Future IOC enrichment script returned "entity cards" (for relevant IP addresses) that summarized available information. The enrichment script[24] also returned information for input domains retrieved from Virus Total results for the original RAT controller IP list.



193.0.200.138 – IP Address

4 References to This Entity
First Seen Jul 26, 2014

Show events involving 193.0.200.138 in Timeline |

Reference Count

4 Total References
2 In the Last 60 Days
0 In the Last 7 Days
0 References Today

Show recent events in Table |

References Breakdown

3 In Social Media
0 From Information Security Sources
1 Including Malicious Language

Related Entities

Domain
gbfuckers.no-ip.biz 1

Show in Table |

Show all entities in Table |

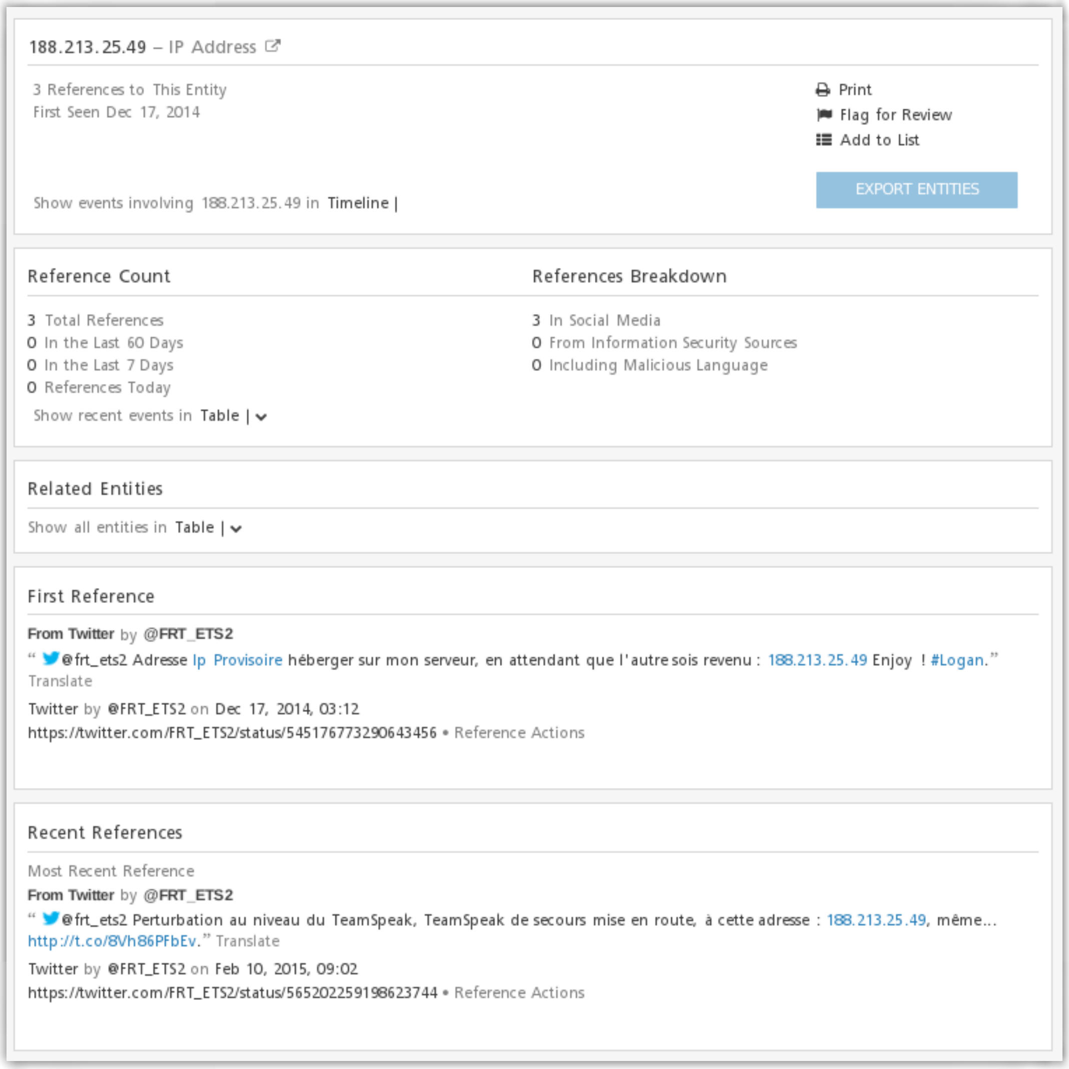
First Reference

Untitled
"1000 updates for 2014-07-25...193.0.200.138|Russian Federation|gbfuckers.no-ip.biz|C2" Cached
PasteBin by threatrecon on Jul 26, 2014, 07:07
http://pastebin.com/K7gNUpLE • Reference Actions

Recent References

Most Recent Reference
From Twitter by @WebironBots
"@webironbots New node: 193.0.200.138 issue: Db Gui exploit scanner bot network: Mediaserviceplus Ltd. https://t.co/m9jLQsqCs6."
Twitter by @WebironBots on Aug 13, 2015, 19:08
https://twitter.com/WebironBots/statuses/632010840783253504 • Reference Actions

[24] https://github.com/recordedfuture/ioc-enrichment



188.213.25.49 – IP Address

3 References to This Entity
First Seen Dec 17, 2014

Show events involving 188.213.25.49 in Timeline |

Reference Count

3 Total References
0 In the Last 60 Days
0 In the Last 7 Days
0 References Today

Show recent events in Table |

References Breakdown

3 In Social Media
0 From Information Security Sources
0 Including Malicious Language

Related Entities

Show all entities in Table |

First Reference

From Twitter by **@FRT_ETS2**

“ @frt_ets2 Adresse Ip Provisoire héberger sur mon serveur, en attendant que l'autre sois revenu : 188.213.25.49 Enjoy ! #Logan.” Translate

Twitter by @FRT_ETS2 on Dec 17, 2014, 03:12
https://twitter.com/FRT_ETS2/status/545176773290643456 • Reference Actions

Recent References

Most Recent Reference

From Twitter by **@FRT_ETS2**

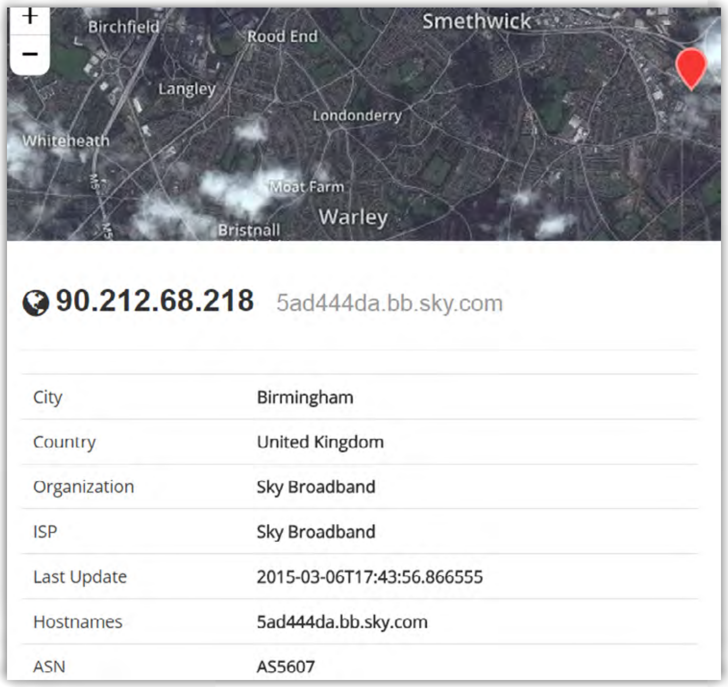
“ @frt_ets2 Perturbation au niveau du TeamSpeak, TeamSpeak de secours mise en route, à cette adresse : 188.213.25.49, même... http://t.co/8Vh86PFbEv.” Translate

Twitter by @FRT_ETS2 on Feb 10, 2015, 09:02
https://twitter.com/FRT_ETS2/status/565202259198623744 • Reference Actions

Proactive RAT Operator Attribution

Example 1 – VirusTotal

Earlier this year Shodan identified a Dark Comet controller running on 90.212.68.218 (Sky Broadband) in the United Kingdom.



90.212.68.218 5ad444da.bb.sky.com

City	Birmingham
Country	United Kingdom
Organization	Sky Broadband
ISP	Sky Broadband
Last Update	2015-03-06T17:43:56.866555
Hostnames	5ad444da.bb.sky.com
ASN	AS5607

Quick IP address enrichment included VirusTotal's associated malware sample with filename, "DeathBotnet!.exe" and domain – yobrohasan[.]ddns.net. "Yobrohasan" is a distinct string that leads to a cached image on the now defunct snog.com of an individual using the moniker "yobrohasan."

It's impossible to fully attribute this particular Dark Comet instance to the above individual, as the RAT operator may have purposefully chosen the "yobrohasan" sub-domain in an attempt at a disinformation campaign, or perhaps the subdomain was chosen due to dislike for the aforementioned individual, or the subdomain choice may have been a coincidence. As previously mentioned, attribution is difficult, and this example serves as a good reminder for the remainder of this report.

Example 2 – Team Cymru

In July 2015, Team Cymru observed a high port UDP session between a njRAT controller IP address – 5.28.184.242 (Ramat Gan Hot Internet, Israel) and a host at 196.36.153.134 (Internet Solutions, South Africa).

In addition to identifying njRAT on port 1177, Shodan further identified UPnP running on port 1900 and HTTP services running on port 80 and 8080 ("WWW-Authenticate: Basic realm="NETGEAR DGN2200v2BEZEQ") respectively, potentially indicating that the 5.28.184.242 host is also acting as a proxy.

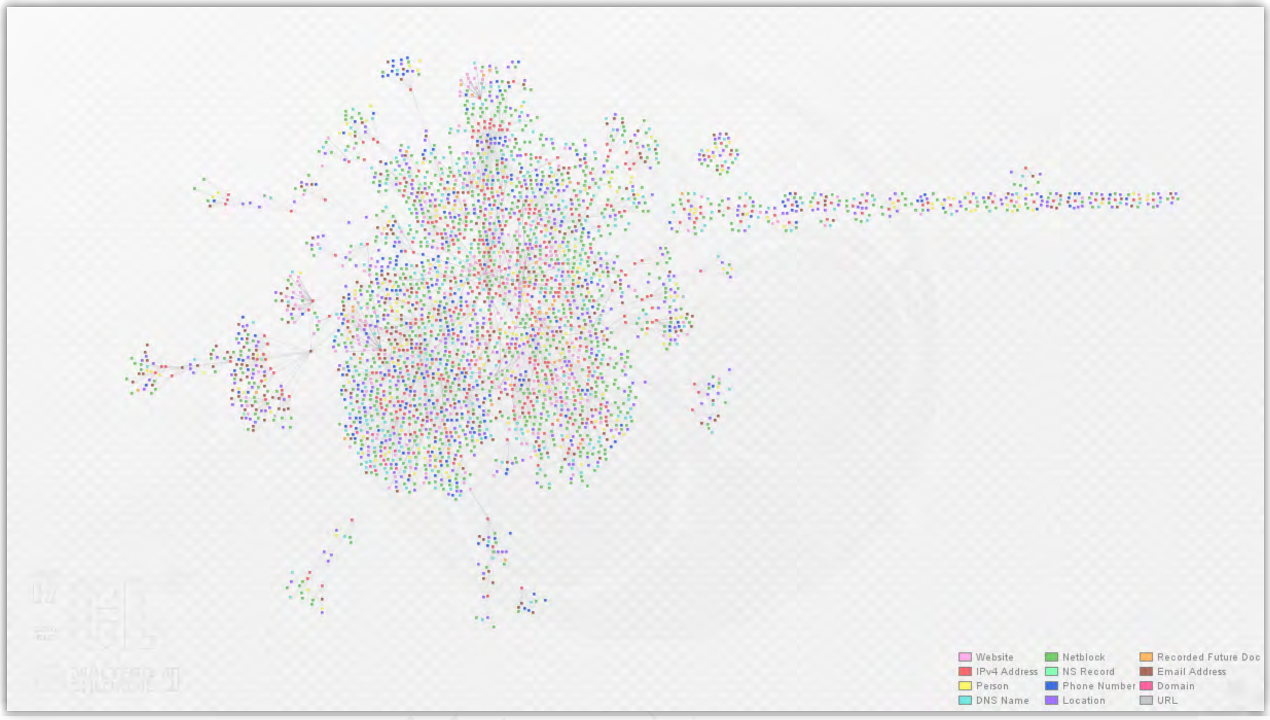
In June, 2015, Team Cymru identified a DNS A record for xheemax.x64.me resolving to 5.28.184.242. The subdomain "xheemax" is a unique string used to produce a new domain from the DDNS service x64.me. The domain currently resolves to 149.78.239.193 (PSINet, Israel).

The online moniker "xheemax" appears in multiple forums beginning in 2011 when the actor asks for assistance in "disabling the small light on the laptop webcam."[25] A profile is also maintained on CryptoSuite[26] as "xheemax Hakkinda" and the "About Me" section contains "RAT" and "Cybergate."

In 2014, Team Cymru's #totalhash[27] also identified xheemax.no-ip.info (204.95.99.109), with corresponding SHA1 hash - 329ed5ef04535f5d11d0e59a361263545d740c61[28].

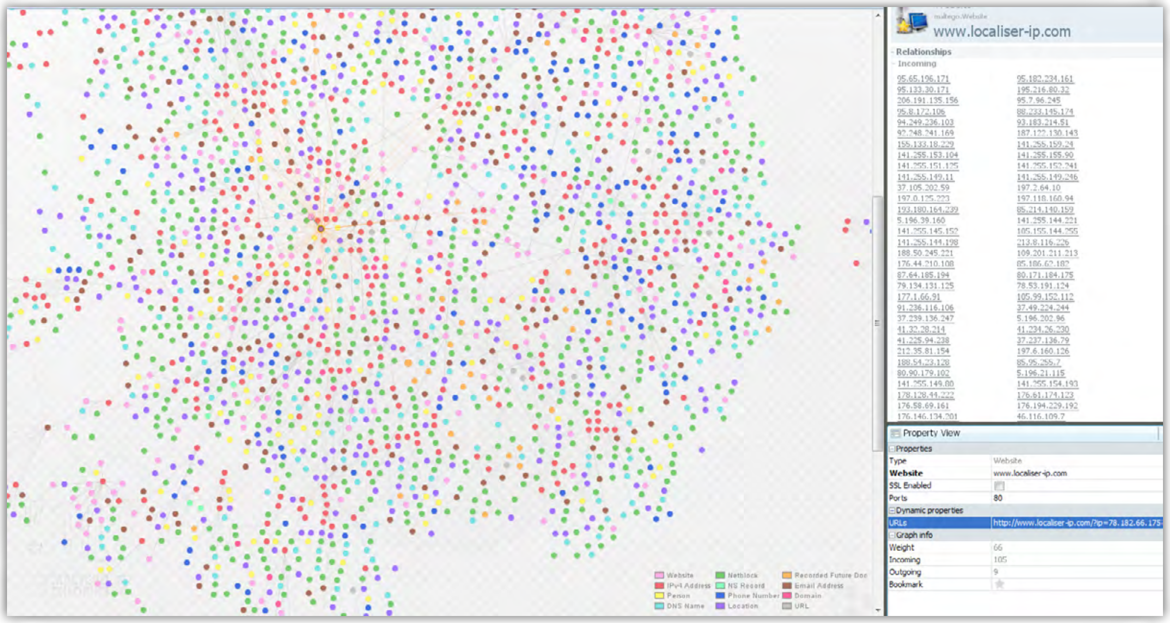
Example 3 – Maltego

Importing the RAT controller IP addresses – from Shodan results for August 17-21, 2015 – into Maltego reveals an enormous amount of commonality.



[25] https://fuckav.ru/archive/index.php/t-8112.html
[26] https://cryptosuite.org/forums/17093xheemax.html
[27] https://totalhash.cymru.com/network/dnsrr:xheemax.no-ip.info
[28] https://www.virustotal.com/en/file/3616af88323a25786b8da40641798fc1569b678f84ed6520035941066724682d/analysis/

The nodes with the highest number of links are related to IP address location checking. The native Maltego transforms specifically correlate over 50 RAT controller IP addresses with websites that include localiser-ip[.]com and iplocationtools[.]com. Multiple historic lists containing the IP addresses in question were also identified on pastebin[.]com.



maltego.Website
www.localiser-ip.com

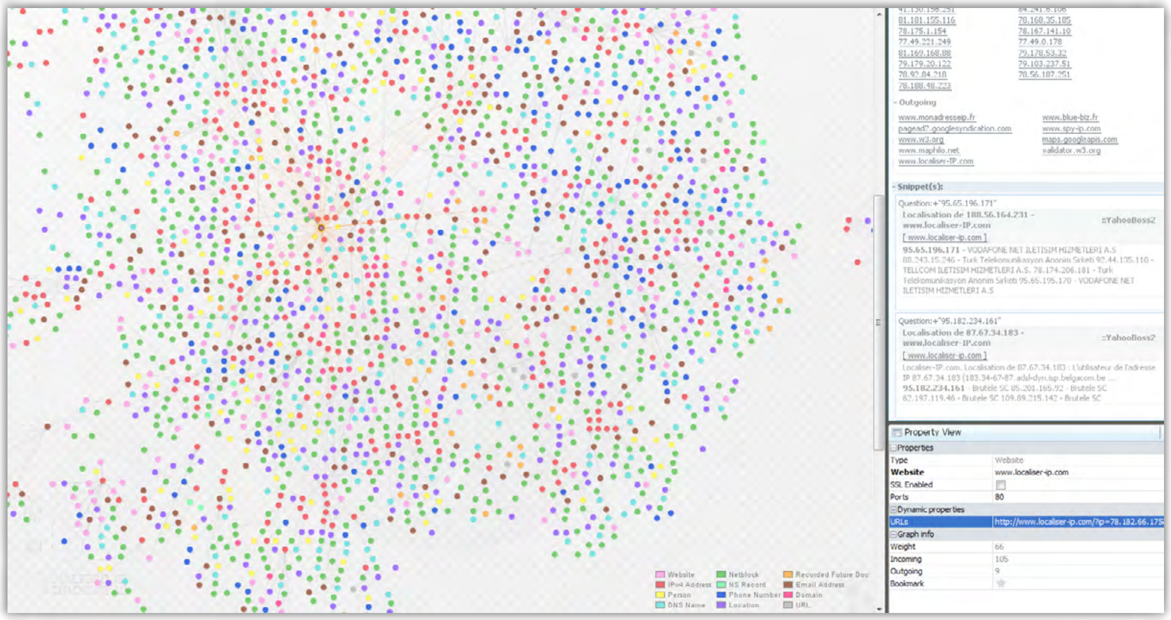
- Relationships
- Incoming

95.65.196.171
95.133.30.171
206.191.135.156
95.8.172.106
94.249.236.103
92.248.241.169
155.133.18.229
141.255.153.104
141.255.151.125
141.255.149.11
37.105.202.59
197.0.125.223
193.180.164.239
5.196.39.160
141.255.145.152
141.255.144.198
188.50.245.221
176.44.210.108
87.64.185.194
79.134.131.125
177.1.66.91
91.236.116.106
37.239.136.247
41.32.28.214
41.225.94.238
212.35.81.154
188.54.23.128
80.90.179.102
141.255.149.80
178.128.44.222
176.58.69.161
176.146.134.201

95.182.234.161
195.216.80.32
95.7.96.245
88.233.145.174
93.183.214.51
187.122.130.143
141.255.159.24
141.255.155.90
141.255.152.241
141.255.149.246
197.2.64.10
197.118.160.94
85.214.140.159
141.255.144.221
105.155.144.255
213.8.116.226
109.201.211.213
85.186.62.182
80.171.184.175
78.53.191.124
105.99.152.112
37.49.224.244
5.196.202.96
41.234.26.230
37.237.136.79
197.6.160.126
85.95.255.7
5.196.21.115
141.255.154.193
176.61.174.123
176.194.229.192
46.116.109.7

Property View

Properties	
Type	Website
Website	www.localiser-ip.com
SSL Enabled	□
Ports	80
Dynamic properties	
URLs	http://www.localiser-ip.com/?ip=78.182.66.175
Graph info	
Weight	66
Incoming	105
Outgoing	9
Bookmark	☆



41.130.158.251
81.181.155.116
78.175.1.154
77.49.221.249
81.169.168.88
79.179.20.122
78.92.84.218
78.188.48.223

84.241.6.108
78.168.35.185
78.167.141.10
77.49.0.178
79.178.53.32
79.103.237.51
78.56.187.251

- Outgoing

www.monadresseip.fr
pagead2.googlesyndication.com
www.w3.org
www.maphilo.net
www.localiser-IP.com

www.blue-biz.fr
www.spy-ip.com
maps.googleapis.com
validator.w3.org

- Snippet(s):

Question:+"95.65.196.171"

Localisation de 188.56.164.231 - www.localiser-IP.com ::YahooBoss2

[www.localiser-ip.com]

95.65.196.171 - VODAFONE NET ILETISIM HIZMETLERI A.S 88.243.15.246 - Turk Telekomunikasyon Anonim Sirketi 92.44.135.110 - TELLCOM ILETISIM HIZMETLERI A.S. 78.174.206.181 - Turk Telekomunikasyon Anonim Sirketi 95.65.195.170 - VODAFONE NET ILETISIM HIZMETLERI A.S

Question:+"95.182.234.161"

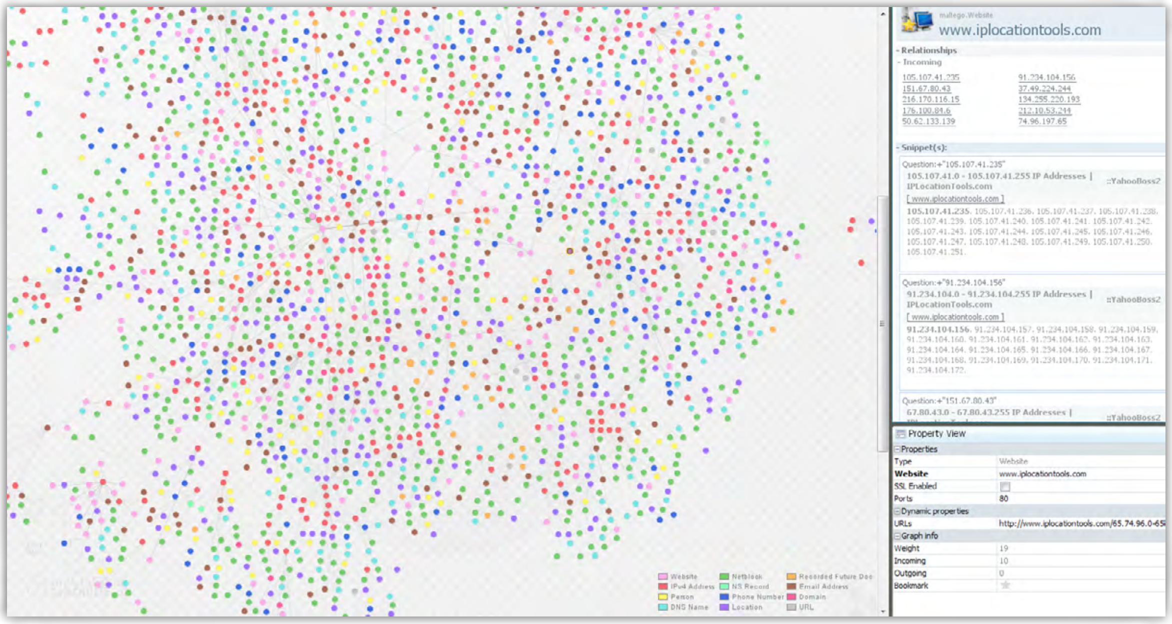
Localisation de 87.67.34.183 - www.localiser-IP.com ::YahooBoss2

[www.localiser-ip.com]

Localiser-IP.com. Localisation de 87.67.34.183 : L'utilisateur de l'adresse IP 87.67.34.183 (183.34-67-87.adsl-dyn.isp.belgacom.be ... **95.182.234.161** - Brutele SC 85.201.165.92 - Brutele SC 62.197.119.46 - Brutele SC 109.89.215.142 - Brutele SC

Property View

Properties	
Type	Website
Website	www.localiser-ip.com
SSL Enabled	□
Ports	80
Dynamic properties	
URLs	http://www.localiser-ip.com/?ip=78.182.66.175
Graph info	
Weight	66
Incoming	105
Outgoing	9
Bookmark	☆



maltego.Website
www.iplocationtools.com

- Relationships
- Incoming

```
105.107.41.235      91.234.104.156
151.67.80.43        37.49.224.244
216.170.116.15      134.255.220.193
176.100.84.6        212.10.53.244
50.62.133.139       74.96.197.65
```

- Snippet(s):

Question:+"105.107.41.235"
105.107.41.0 - 105.107.41.255 IP Addresses | IPLocationTools.com ::YahooBoss2
[www.iplocationtools.com]
105.107.41.235. 105.107.41.236. 105.107.41.237. 105.107.41.238. 105.107.41.239. 105.107.41.240. 105.107.41.241. 105.107.41.242. 105.107.41.243. 105.107.41.244. 105.107.41.245. 105.107.41.246. 105.107.41.247. 105.107.41.248. 105.107.41.249. 105.107.41.250. 105.107.41.251.

Question:+"91.234.104.156"
91.234.104.0 - 91.234.104.255 IP Addresses | IPLocationTools.com ::YahooBoss2
[www.iplocationtools.com]
91.234.104.156. 91.234.104.157. 91.234.104.158. 91.234.104.159. 91.234.104.160. 91.234.104.161. 91.234.104.162. 91.234.104.163. 91.234.104.164. 91.234.104.165. 91.234.104.166. 91.234.104.167. 91.234.104.168. 91.234.104.169. 91.234.104.170. 91.234.104.171. 91.234.104.172.

Question:+"151.67.80.43"
67.80.43.0 - 67.80.43.255 IP Addresses | ::YahooBoss2

Property View

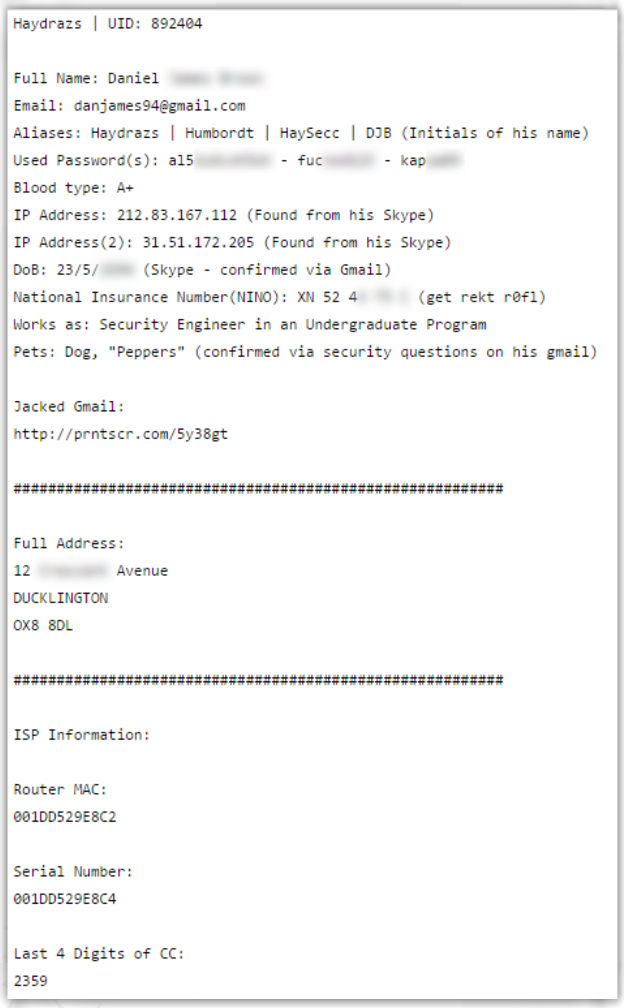
Properties	
Type	Website
Website	www.iplocationtools.com
SSL Enabled	□
Ports	80
Dynamic properties	
URLs	http://www.iplocationtools.com/65.74.96.0-65
Graph info	
Weight	19
Incoming	10
Outgoing	0
Bookmark	☆

Visualization of large data sets enables the identification of "choke points" – through commonality – comprised of (in this case) adversary resources and/or tactics that can be identified and addressed by operational defenders to increase defensive technology efficacy.

Example 4 – Recorded Future

Recorded Future matched a RAT controller IP address to a Pastebin reference – http://pastebin.com/cU4WX0hs – alleging the IP address owner is "Daniel". The Paste author proceeds to list Daniel's personally identifiable information (PII) including date of birth, email, and physical address near Oxford, UK.

The paste author further alleges that "Daniel" works for powerstresser[.]com – an ethically dubious "booter" service[29] designed to "stress test" servers. If the Paste information is correct, this represents an extremely simple case of RAT operator attribution.



```
Haydrazs | UID: 892404


Full Name: Daniel [redacted]
Email: danjames94@gmail.com
Aliases: Haydrazs | Humbordt | HaySecc | DJB (Initials of his name)
Used Password(s): al5[redacted] - fuc[redacted] - kap[redacted]
Blood type: A+
IP Address: 212.83.167.112 (Found from his Skype)
IP Address(2): 31.51.172.205 (Found from his Skype)
DoB: 23/5/[redacted] (Skype - confirmed via Gmail)
National Insurance Number(NINO): XN 52 4[redacted] (get rekt r0fl)
Works as: Security Engineer in an Undergraduate Program
Pets: Dog, "Peppers" (confirmed via security questions on his gmail)

Jacked Gmail:
http://prntscr.com/5y38gt

##########################################################

Full Address:
12 [redacted] Avenue
DUCKLINGTON
OX8 8DL

##########################################################

ISP Information:

Router MAC:
001DD529E8C2

Serial Number:
001DD529E8C4

Last 4 Digits of CC:
2359
```

[29] http://www.eweek.com/security/how-do-booters-work-inside-a-ddos-for-hire-attack

Conclusion

Original, focused, and scalable intelligence methodologies are useful for law enforcement and for defending the enterprise, as demonstrated here. Identifying RAT controller locations and operators before their respective RAT spreading campaigns begin reduces malware processing resources.

Threat data enrichment sources such as Recorded Future increase attribution knowledge, in this case around RAT operators, which lead to enhanced understanding of motivations and derivative tools, techniques, and procedures.

Proactive and repeatable Internet enumeration for known RAT signatures is a viable methodology for producing an operational feed of malicious observables, and more importantly, also presenting further strategic opportunities to identify and understand the adversary.

RAT operators are inherently vulnerable because they are often operating openly on the Internet and the RATs they buy or download generate unique response strings when properly interrogated. The vulnerability extends further because the RAT service listening on a specified port is an easy remote entry point to the attacker's computer.

Special thanks to Shodan founder John Matherly for his support of this research.

Indicators of Compromise (IOC)

All IOCs referenced in this report are located in the Recorded Future GitHub repository.

About Recorded Future