Proactive Threat Identification Neutralizes Remote Access Trojan Efficacy

By Levi Gundert
Vice President of Threat Intelligence
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) 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.

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. Nation-state campaigns have routinely included payloads like Poison Ivy 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 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 which feature content such as packing/crypting a RAT to evade anti-virus software; demonstrating capabilities with multiple victims; and establishing infrastructure, like dynamic DNS, 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
5 http://www.secularist.com/blog/2014/01/xtreme-rat-strikes-israeli-organizations-again.html
7 http://www.reddit.com/r/hacking/comments/2acwpb/how_to_setup_dark_comet_rat_with_download_and/
8 https://www.youtube.com/watch?v=QmH_ojSZoRU
9 https://www.youtube.com/watch?v=5szzkJxbps
10 https://www.youtube.com/watch?v=fTqccBmzY
11 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 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\(^\text{11}\) was the only available off-the-shelf option (short of writing a custom asynchronous multithreading scanner). The release of Unicorn Scan\(^\text{12}\), and more recent releases of Zmap\(^\text{13}\), and MASSCAN\(^\text{14}\) 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\(^\text{15}\) 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\(^\text{16}\).

---

\(^\text{11}\) https://nmap.org/

\(^\text{12}\) http://sectools.org/tool/unicornscan/

\(^\text{13}\) https://zmap.io/

\(^\text{14}\) https://github.com/robertdavidgraham/masscan

\(^\text{15}\) https://support.microsoft.com/en-us/kb/172983

Proactive Threat Identification Neutralizes Remote Access Trojan Efficacy

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.

17 http://curl.haxx.se/
18 http://www.secdev.org/projects/scapy/
Proactive Threat Identification Neutralizes Remote Access Trojan Efficacy

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\(^\text{19}\). Netresec produced an informative blog in 2014\(^\text{20}\) dissecting Havex’s communication pattern. Noticeably, the Havex response includes the string “havex.”

**Scaling the Methodology**

Shodan\(^\text{21}\), 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.

![Shodan CLI](image)

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\(^\text{22}\). 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](https://www.securityweek.com/attackers-using-havex-rat-against-industrial-control-systems)


\(^{21}\) [https://www.shodan.io/](https://www.shodan.io/)

\(^{22}\) The VirusTotal results can be downloaded from Recorded Future’s GitHub page.
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.

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

<table>
<thead>
<tr>
<th>RAT Controller IP</th>
<th>Document URI</th>
<th>Fragment</th>
</tr>
</thead>
<tbody>
<tr>
<td>37.139.52.43</td>
<td><a href="http://www.facebook.com/406287246141601/posts/536666376437020">http://www.facebook.com/406287246141601/posts/536666376437020</a></td>
<td>Kharkov S1 37.139.52.43 - Germany, 10:09:17 - EVENT :: Moderator sleeperpi (sleeperpi) (38.103.14.232) has entered the room</td>
</tr>
<tr>
<td>38.103.14.232</td>
<td><a href="http://pastebin.com/tGT0nEvT">http://pastebin.com/tGT0nEvT</a></td>
<td>IP Address: 212.83.167.112 (Found from his Skype)</td>
</tr>
<tr>
<td>83.87.20.225</td>
<td><a href="http://pastebin.com/F6KnVR1q">http://pastebin.com/F6KnVR1q</a></td>
<td>Telnet attacked from 212.154.81.158 (<a href="http://t.co/BjAAPAs9u">http://t.co/BjAAPAs9u</a>)</td>
</tr>
<tr>
<td>212.154.81.158</td>
<td><a href="https://twitter.com/atma_es/status/628301520853929985">https://twitter.com/atma_es/status/628301520853929985</a></td>
<td>This code was created on Saturday, March 21st, 2015 at 15:59 UTC from IP 197.2.24.60 (tn)</td>
</tr>
<tr>
<td>197.2.24.60</td>
<td><a href="http://pastebin.com/kLJfgrMD">http://pastebin.com/kLJfgrMD</a></td>
<td>WebApp: SQLi attack from 94.102.51.152 (NL, Noord-Holland - Amsterdam) #netmenaces 1.</td>
</tr>
<tr>
<td>94.102.51.152</td>
<td><a href="https://twitter.com/netmenaces/status/612103433273917440">https://twitter.com/netmenaces/status/612103433273917440</a></td>
<td>Telnet attacked from 212.154.81.158 (<a href="http://t.co/BjAAPAs9u">http://t.co/BjAAPAs9u</a>).</td>
</tr>
<tr>
<td>212.154.81.158</td>
<td><a href="https://twitter.com/atma_es/status/628301520853929985">https://twitter.com/atma_es/status/628301520853929985</a></td>
<td>93.116.43.245.333</td>
</tr>
<tr>
<td>93.116.43.245</td>
<td><a href="https://www.virustotal.com/en/file/">https://www.virustotal.com/en/file/</a></td>
<td>93.116.43.245.333</td>
</tr>
</tbody>
</table>

---

**RAT enrichment IP List**

![RAT enrichment IP List](image_url)
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\(^2\) also returned information for input domains retrieved from Virus Total results for the original RAT controller IP list.

\(^2\) [https://github.com/recordedfuture/ioc-enrichment](https://github.com/recordedfuture/ioc-enrichment)
Proactive Threat Identification Neutralizes Remote Access Trojan Efficacy
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.

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 CryptoSuite26 as “xheemax Hakkinda” and the “About Me” section contains “RAT” and “Cybergate.”

In 2014, Team Cymru’s #totalhash27 also identified xheemax.no-ip.info (204.95.99.109), with corresponding SHA1 hash - 329ed5ef04535f5d11d0e59a361263545d740c6128.

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.

---

26 https://cryptosuite.org/forums/17093xheemax.html
28 https://www.virustotal.com/en/file/3616a88323a25786b8da4064179f8c1f569b678f184ed52003594106674682d/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.
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” service29 designed to “stress test” servers. If the Paste information is correct, this represents an extremely simple case of RAT operator attribution.

## 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**

We arm you with real-time threat intelligence so you can decrease operational risk. With billions of indexed facts, and more added every day, our patented Web Intelligence Engine continuously analyzes the entire Web to give you unmatched insight into emerging threats. Recorded Future helps protect four of the top five companies in the world.