Hunt Advanced Attackers on a Budget Less than the GDP of a Small Country

John Strand
Owner
Black Hills Information Security
Problem: Detecting Command and Control is getting hard

- There are a number of backdoors that use a wide variety of different ways to communicate with the bad guys’ Command and Control (C2) servers
  - HTTP Beaconing
  - Social Media
  - DNS
  - QUICK
  - SCTP
- PenTesting firms use these tricks all of the time
- As do the bad guys
- How can we detect these backdoors if the data is encrypted, obfuscated or hidden?
- We can use AI
  - Please.. Don’t stop watching just yet...
Let's think about consistencies.
Let's think about consistencies.
Let's think about consistencies.
Let's think about consistencies.
Let’s talk about setup

- First, you will need to have a system to capture the traffic
- Second, RITA is free and awesome
Why Zeek?

- Speed
- Large user base
- Lots of support
- Consistency
  - Timestamps are key
  - Many devices handle timestamps in different/odd ways
  - Generates required log files
- We are moving away from signature-based detection
- Too many ways to obfuscate
  - Encryption, Encoding, use of third-party services like Google DNS
RITA is free... It is also the source of most of the data we will cover:

https://www.activecountermeasures.com/rita/
VSAgent

```
sec504@slingshot:~$ su -
Password:
root@slingshot:~#
root@slingshot:~# tcpdump -i lo -s0 -A host 10.10.75.1 | grep VIEWSTATE
```

```
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on lo, link-type EN10MB (Ethernet), capture size 262144 bytes
__VIEWSTATE=eyJb21tYW5kcyI6IFtpdCAiYWdlbnQoIiAiMDA6MGM6Mjk6ZTU6NGQ6MDAifQ%3D%3D
<input type="hidden" name="__VIEWSTATE" id="__VIEWSTATE" value="eyJb21tYW5kcyI6IFtpdCAiYWdlbnQoIiAiMDA6MGM6Mjk6ZTU6NGQ6MDAifQ%3D%3D
```

```
__VIEWSTATE=eyJb21tYW5kcyI6IFtpdCAtLCAiYWdlbnQoIiAiMDA6MGM6Mjk6ZTU6NGQ6MDAifQ%3D%3D
```
DNSCat
Housekeeping: Ads

- Ads... Oh my... Ads
- You need to block them
- They bring malware
- They pollute the data
Round Robin Malware Beaconing

- We have been seeing malware that connects to multiple different IP addresses
  - QUIC
  - SCTP
- One giveaway is the datasize
- The IPs may shift, but the dispersion and the data size are still consistent
- Look for an internal system making connections to multiple external systems with the same attributes
What happens when your entire network is connecting to DoD?

- We had a customer who had a large (think thousands) of systems connecting to a DoD IP address on the Internet.
- Very strong and consistent beacon:
  - Datasize
  - Dispersion
  - Interval
- Time to panic?
- Is the NSA hacking them?
- Was it a Vault or ShadowBroker exploit?
- Made no sense at all.....
Quote from a developer...

“Wait... That IP address is odd.. It is the current version of product X.”
Lesson

- Sometimes “beaconing” data is not evil
- Sometimes it is just a mistake
- Trust me, there are lots of mistakes on networks:
  - Syslog from products
  - “Customer experience data”
  - Direct Software updates trying to get to the Internet
- There is a lot of filtering and research when you first do this
- But, it gets easier
- Think Vulnerability Assessments

Did someone say a “Touch of Evil?”
On the topic of blacklisting...

- There are multiple different sources of blacklisted IP/DNS information
- Most of them feed off each other
- Having a hit on a blacklist does not mean the connection is immediately evil
  - Virtual hosting
  - Old entries
- So, simply because a connection is made to an IP address does not mean the system is compromised
What to look for: Numerous hits

<table>
<thead>
<tr>
<th>Engine</th>
<th>Help</th>
</tr>
</thead>
<tbody>
<tr>
<td>MyWOT</td>
<td>More info</td>
</tr>
<tr>
<td>LAPPS Grid Blacklist</td>
<td>More info</td>
</tr>
<tr>
<td>MalwareDomainList</td>
<td>More info</td>
</tr>
<tr>
<td>TalosIntel IPFilter</td>
<td>More info</td>
</tr>
<tr>
<td>AlienVault Reputation</td>
<td>More info</td>
</tr>
</tbody>
</table>
What to look for: Amount of data transferred

- Total Connections: 31833
- Unique Connections: 2
- Bytes Transferred: 123988810
A note on porn
When good sites go bad...
Seems legit..
Spyware is.... Weird

- Not quite ad... Not quite malware...
- Usually used for tracking a user
- All advertisers do this

How do I get rid of revsci.net tracking cookie - Resolved/Inactive ...
https://forum.adaware.com › ... › Resolved/Inactive General Support Issues ▼
Feb 7, 2007 - 2 posts - 2 authors
Also, in Tools > Internet Options > Advanced scroll down to "Security" and make sure that "Empty Temporary Internet Files folder when Browser is closed" is selected - if not, select it, click Apply and Ok
Compromised Servers

```
$ nmap -p 0-65535 13.11.170.149
Nmap scan report for 13.11.170.149
Host is up (0.025s latency).
Not shown: 49132 filtered ports, 16393 closed ports
PORT      STATE    SERVICE
53/tcp    open     domain
80/tcp    open     http
443/tcp   open     https
2082/tcp  open     infowave
2083/tcp  open     radsec
2086/tcp  open     gnunet // GNUNet is a framework for P2P networking
2087/tcp  open     eli // Event logging integration
2095/tcp  open     nbx-ser
2096/tcp  open     nbx-dir
2222/tcp  open     EtherNetIP-1 Typing EtherNetIP-1 to google recommends EthernetIP-1 service exploit
3306/tcp  open     mysql
```
Crypto mining is the new hotness

```
ohn@AlteredCarbon:~$ nmap [IP] 4.81
Starting Nmap 7.60 (https://nmap.org) at 2018-01-22 13:47 MST
Stats: 0:00:13 elapsed; 0 hosts completed (0 up), 1 undergoing Ping Scan
Parallel DNS resolution of 1 host. Timing: About 0.00% done
Nmap scan report for [IP] 174.81
Host is up (0.14s latency).
Not shown: 997 closed ports
PORT       STATE SERVICE
22/tcp      open    ssh
3000/tcp    open    ppp
8080/tcp    open    http-proxy

Nmap done: 1 IP address (1 host up) scanned in 24.74 seconds
ohn@AlteredCarbon:~$`

```
curl http://[IP]:4.81:8080/list
[
{"ip":"[IP], workers":4, power":30}
,
{"ip":"[IP], workers":4, power":30}
,
{"ip":"[IP], workers":4, power":30}
,
{"ip":"[IP], workers":4, power":30}]
```
Online Resource:  IP/URL Void

IP Address Information

<table>
<thead>
<tr>
<th>Analysis Date</th>
<th>2018-02-20 10:09:46</th>
</tr>
</thead>
<tbody>
<tr>
<td>Elapsed Time</td>
<td>2 seconds</td>
</tr>
<tr>
<td>Blacklist Status</td>
<td>BLACKLISTED 4/96</td>
</tr>
<tr>
<td>IP Address</td>
<td>104.27.163.228</td>
</tr>
<tr>
<td>Reverse DNS</td>
<td>Unknown</td>
</tr>
<tr>
<td>ASN</td>
<td>AS13335</td>
</tr>
<tr>
<td>ASN Owner</td>
<td>Cloudflare Inc</td>
</tr>
<tr>
<td>ISP</td>
<td>Cloudflare</td>
</tr>
<tr>
<td>Continent</td>
<td>North America</td>
</tr>
<tr>
<td>Country Code</td>
<td>(US) United States</td>
</tr>
<tr>
<td>Latitude / Longitude</td>
<td>37.751 / -97.822</td>
</tr>
</tbody>
</table>

IP ADDRESS: 104.27.163.228

We have found in our database of already analyzed websites that there are 14 websites hosted in the same web server with IP address 104.27.163.228. Remember that it is not good to have too many websites located in the same web server because if a website gets infected by malware, it can easily affect the online reputation of the IP address and also of all the other websites.

Browse a list of websites hosted in 104.27.163.228 IP address:

<table>
<thead>
<tr>
<th>#</th>
<th>Website</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>prototypo.io</td>
</tr>
<tr>
<td>2</td>
<td>e-glasshouse.com</td>
</tr>
<tr>
<td>3</td>
<td>alphabetawood.com</td>
</tr>
<tr>
<td>4</td>
<td>prayoga.biz</td>
</tr>
<tr>
<td>5</td>
<td>trendo-news.com</td>
</tr>
</tbody>
</table>
**BGP/ASN Ranking**

There are 10401 entries in the list of ASNs with malicious content. The top 100 is printed on this page.

<table>
<thead>
<tr>
<th>ASN</th>
<th>Description</th>
<th>Rank</th>
<th>Source(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>43765</td>
<td>VHOSTER-NET, UA</td>
<td>1.36513671875</td>
<td>BlocklistDeApache, CIArmy, BlocklistDelmap, BlocklistDeMail, BlocklistDeFtp, BlocklistDeSip, RansomwareelpBlockList, DshieldDaily, BlocklistDeStrong, BlocklistDeBots</td>
</tr>
<tr>
<td>265914</td>
<td>TRIUNFO SOLUCOES EM</td>
<td>1.2783203125</td>
<td>DshieldDaily, BlocklistDeSch</td>
</tr>
</tbody>
</table>
Shodan... Not just for pentesters...

The search engine for Buildings

Shodan is the world's first search engine for Internet-connected devices.

Explore the Internet of Things
Use Shodan to discover which of your devices are connected to the Internet, where they are located and who is using them.

Monitor Network Security
Keep track of all the computers on your network that are directly accessible from the Internet. Shodan lets you understand your digital footprint.

See the Big Picture
Websites are just one part of the Internet. There are power plants, Smart TVs, refrigerators and much more that can be found with Shodan!

Get a Competitive Advantage
Who is using your product? Where are they located? Use Shodan to perform empirical market intelligence.
PunkSPIDER is back!

Punk.sh
The new version of PunkSPIDER also with nmap scans

WEB
PORTS
NSE
SERVICES
PRODUCTS
COUNTRIES

Please enter a url or search term...
cats

Advanced search ▼ Remove filters

Found 131 results (0.394 seconds)

blackcatsystems-acars.andro.io as of 2018-02-17

catshogi.andro.io as of 2018-02-17

pupa-realisticpuzzlecats.andro.io as of 2018-02-18

iappsandigames-sleepcatsimulat.andro.io as of 2018-02-17

aaavocats.fr as of 2018-01-26

Sobavocats.fr as of 2018-01-26
Conclusions

- Detecting Command and Control traffic is getting harder and harder
- We released RITA to help detect some of the backdoors we use everyday
- GO GET IT!!!
- There are also a lot of free resources available to research network oddities
- Does require a bit of digging
- Odd != Evil
- Housekeeping is often required!
- Thanks!