Automated Attacks at Scale

Understanding “Credential Exploitation”

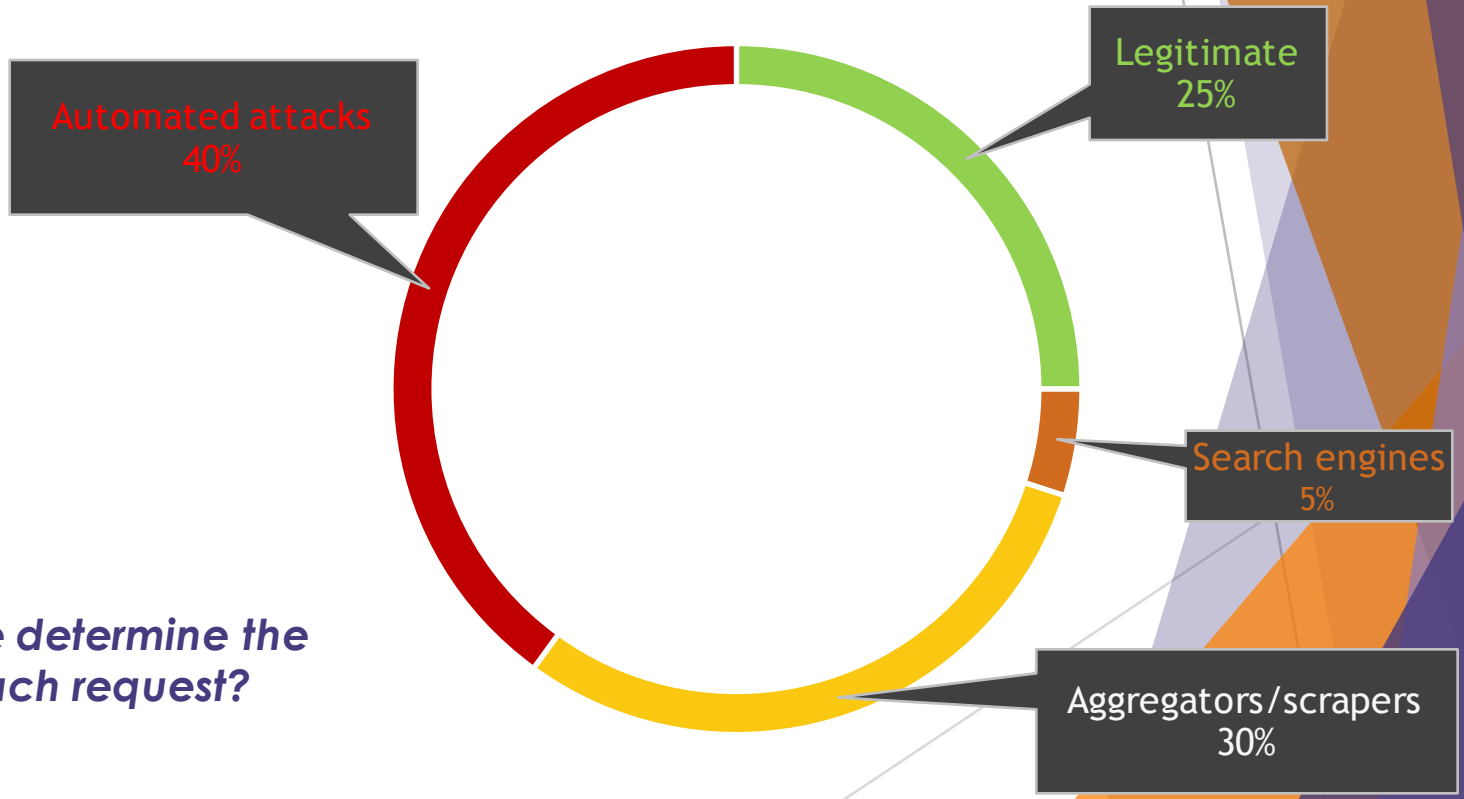
Mayank Dhiman
Principal Security Researcher
mayank@stealthsec.com
@l0pher

Will Glazier
Threat Intelligence Analyst
will@stealthsec.com
@wglazier21

What do we mean by an “Automated Attack”?

Fundamentally a Bot problem

- Attack toolkits available on underground
- Custom scripts
- Attacks on API endpoints



How do we determine the intent of each request?

Attacker's Goals

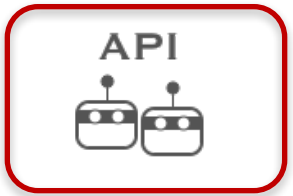
Account Take Over

Fake Account Creation

PII / PHI Theft

Shopping Bots

API Abuse



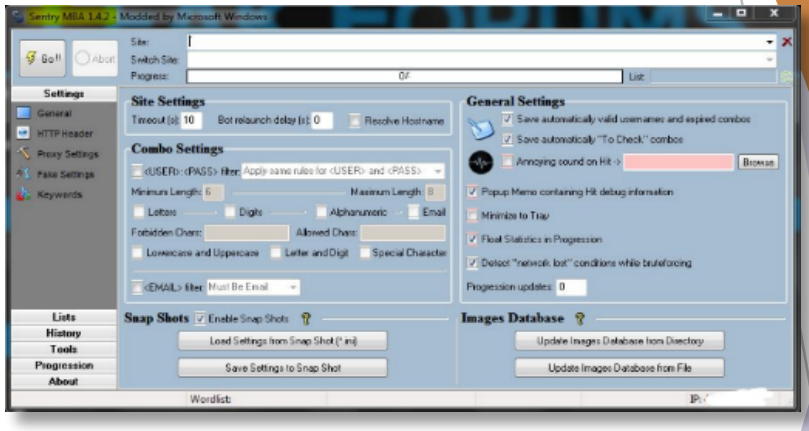
The Attacker’s Perspective

The 5 Pillars of a credential exploitation attack

1) Black Market Attack Tool or Custom tool configured for a target
2) Set of Stolen Credentials
3) Ability to rotate over many IP addresses
4) Compute Power
5) Ability to bypass deployed security solutions

Attack Toolkits & Config Files

- SentryMBA
- Hydra
- PhantomJS
- Medusa
- Curl, Wget
- Ncrack
- Other custom scripts



Understanding Config Files…

- Program instructions for how to login and differentiate between failed and successful logins for that particular target. Writing config files is one of the chief ways to monetize in this criminal ecosystem.
- “Capture” setting – optional setting enables attackers to understand the value of a compromised account without logging back in again.

Quick Facts – Underground Ecosystem

- 1,853 unique target sites on sentry.mba
- 10% of Alexa Top 1000 have config files readily available
- 184 API config files - roughly 10% of targets
- $1.73 – average cost of a config file.
- Top industries targeted – Gaming, Entertainment, E-Commerce

https://goo.gl/AEwhRx

POPULAR TARGET SITES

Popular Streaming, Gaming and Social Networking websites are also attackers' favorite targets.
This may indicate most attackers are script kiddies.

884 Downloads
* Reposted *25* times

335 Downloads

314 Downloads
* Reposted *22* times

290 Downloads
Universal Email Access Checker

289 Downloads
* Reposted *19* times

227 Downloads
* Reposted *41* times

214 Downloads

137 Downloads
* Reposted *14* times

134 Downloads

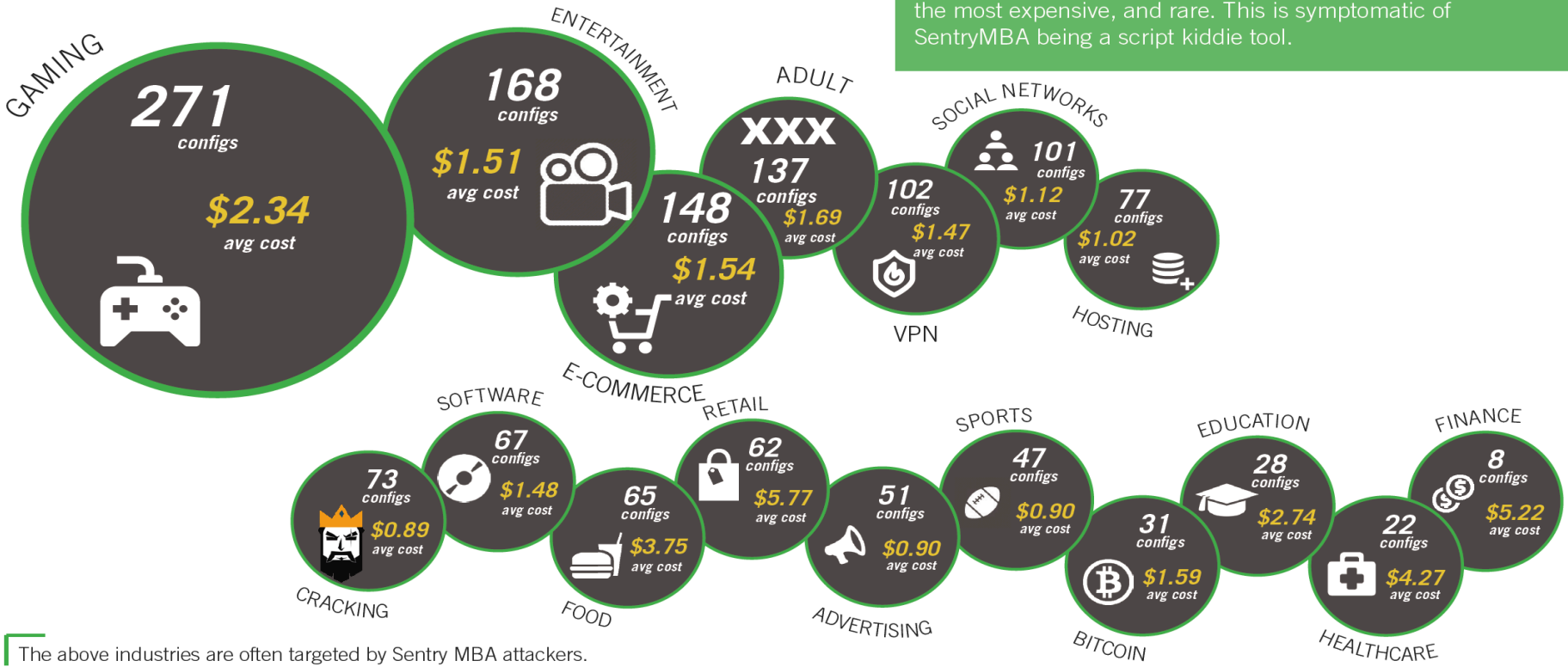
125 Downloads

115 Downloads

80 Downloads

TARGET INDUSTRIES

All major industries are actively under attack. Some face a disproportionate volume of attacks such as Gaming, Entertainment & E-Commerce. Finance and Retail configs are the most expensive, and rare. This is symptomatic of SentryMBA being a script kiddie tool.

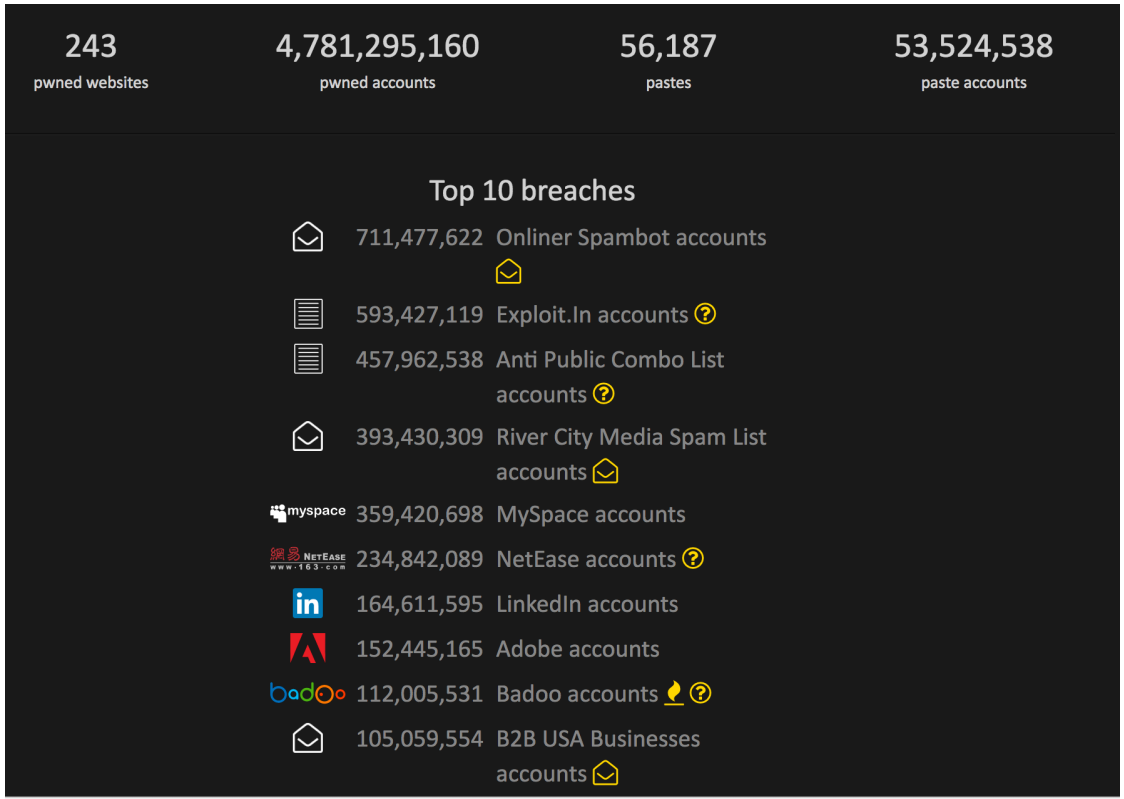


The above industries are often targeted by Sentry MBA attackers. Included is the number and average cost of configs posted per industry.

The 5 Pillars of a credential exploitation attack

1) Black Market Attack Tool or Custom tool configured for a target
2) Set of Stolen Credentials
3) Ability to rotate over many IP addresses
4) Compute Power
5) Ability to bypass deployed security solutions

Stolen Credentials



* https://haveibeenpwned.com/

- Simple Pastebin Crawler – harvests more than 20,000 credentials every day
- Users average 6.5 credentials per 50 websites

* Microsoft Research

Quick aside – How much money can attackers really net?

Social Security number (sold as part of 'Fullz' dossier)	$30
Date of birth	$11
Health insurance credentials	$20
Visa or MasterCard credentials	$4
American Express credentials	$7
Discover credit credentials	$8
Credit card with magnetic stripe or chip data	$12
Bank account number (balance of $70,000 to $150,000)	$300 or less
Full identity 'Kitz'	$1,200 to $1,300

Source: Dell SecureWorks

- Attacker tries 1,000,000 credentials – if each stolen account sells for only $0.25, then a successful login rate of only ***0.1%*** will net $250.00

The 5 Pillars of a credential exploitation attack

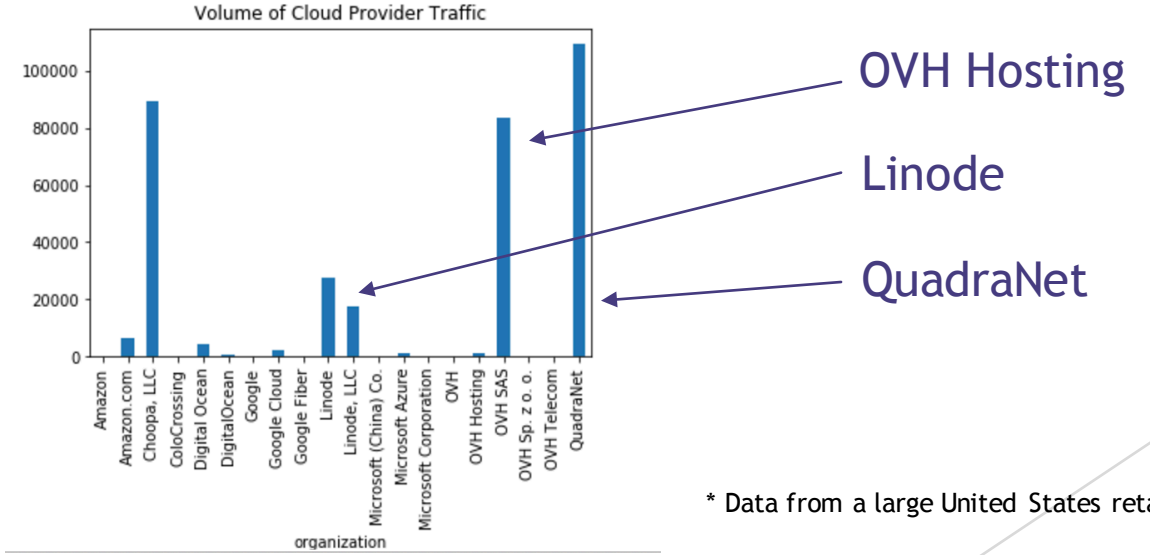
1) Black Market Attack Tool or Custom tool configured for a target
2) Set of Stolen Credentials
3) Ability to rotate over many IP addresses
4) Compute Power
5) Ability to bypass deployed security solutions

IP Rotation & Compute Power

How to gather the necessary infrastructure?

Option 1: Cloud Hosting Providers

- High reputation – AWS & Azure will never get blacklisted
- Virtualization allows easy instance creation programatically

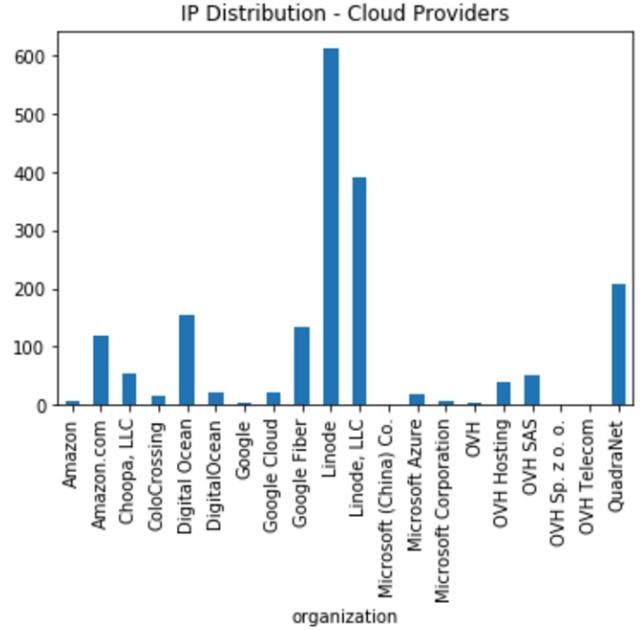


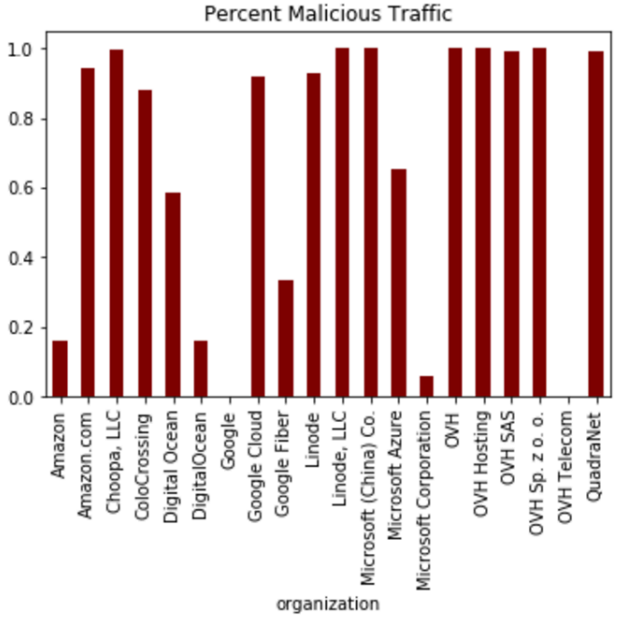
OVH Hosting

Linode

QuadraNet

* Data from a large United States retailer in Sept. 2017

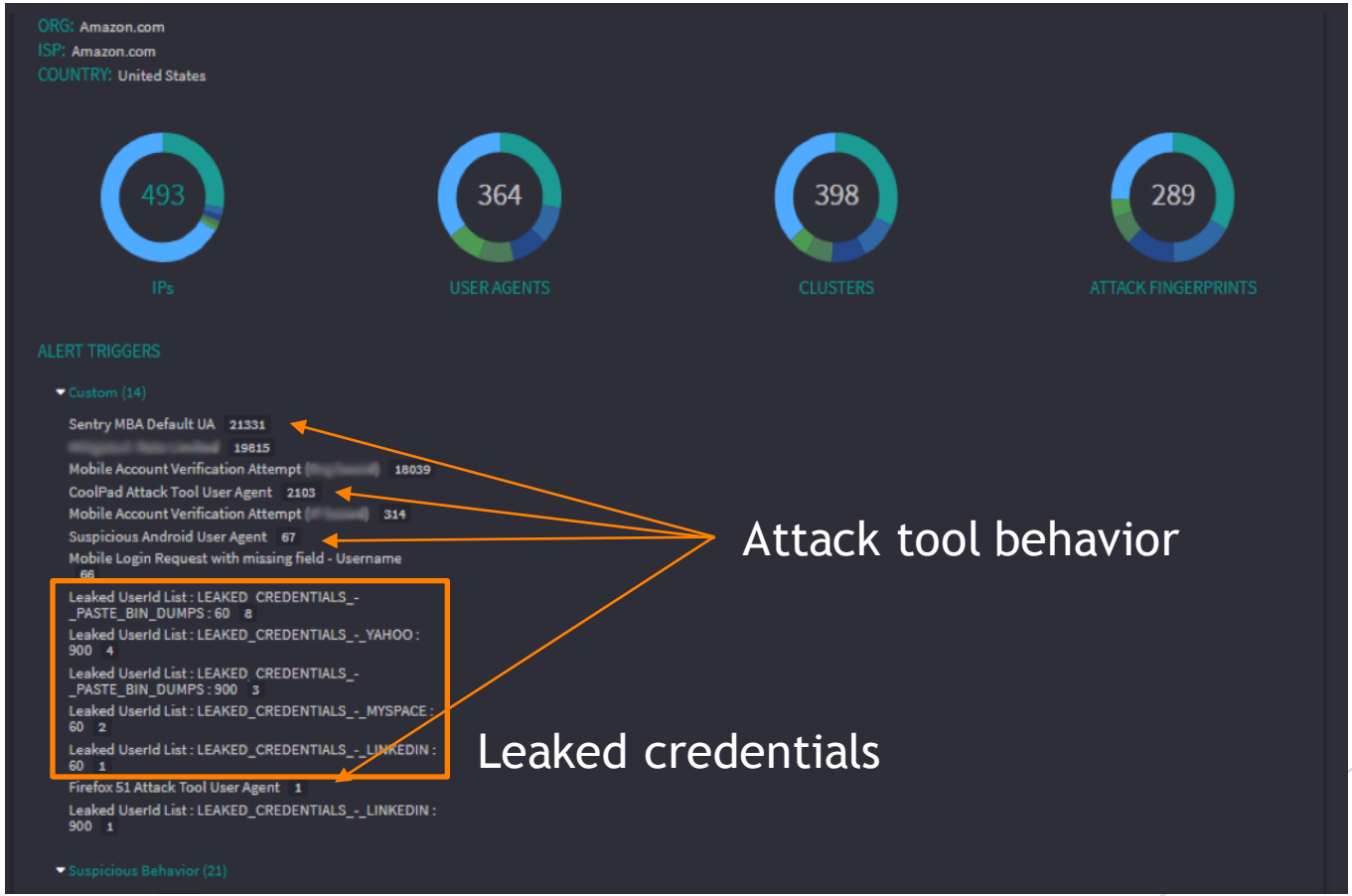




How long do these IP's "stick around" and continue sending malicious traffic before being recycled?

Answer: Surprisingly long…

Example: AWS


ORG: Amazon.com
ISP: Amazon.com
COUNTRY: United States
493
IPs
364
USER AGENTS
398
CLUSTERS
289
ATTACK FINGERPRINTS
ALERT TRIGGERS
Custom (14)
Sentry MBA Default UA 21331
19815
Mobile Account Verification Attempt 18039
CoolPad Attack Tool User Agent 2103
Mobile Account Verification Attempt 314
Suspicious Android User Agent 67
Mobile Login Request with missing field - Username 66
Leaked UserId List : LEAKED_CREDENTIALS_-_PASTE_BIN_DUMPS : 60 8
Leaked UserId List : LEAKED_CREDENTIALS_-_YAHOO : 900 4
Leaked UserId List : LEAKED_CREDENTIALS_-_PASTE_BIN_DUMPS : 900 3
Leaked UserId List : LEAKED_CREDENTIALS_-_MYSPACE : 60 2
Leaked UserId List : LEAKED_CREDENTIALS_-_LINKEDIN : 60 1
Firefox 51 Attack Tool User Agent 1
Leaked UserId List : LEAKED_CREDENTIALS_-_LINKEDIN : 900 1
Suspicious Behavior (21)
Attack tool behavior
Leaked credentials

Option 2: Compromised Devices, IoT Botnets

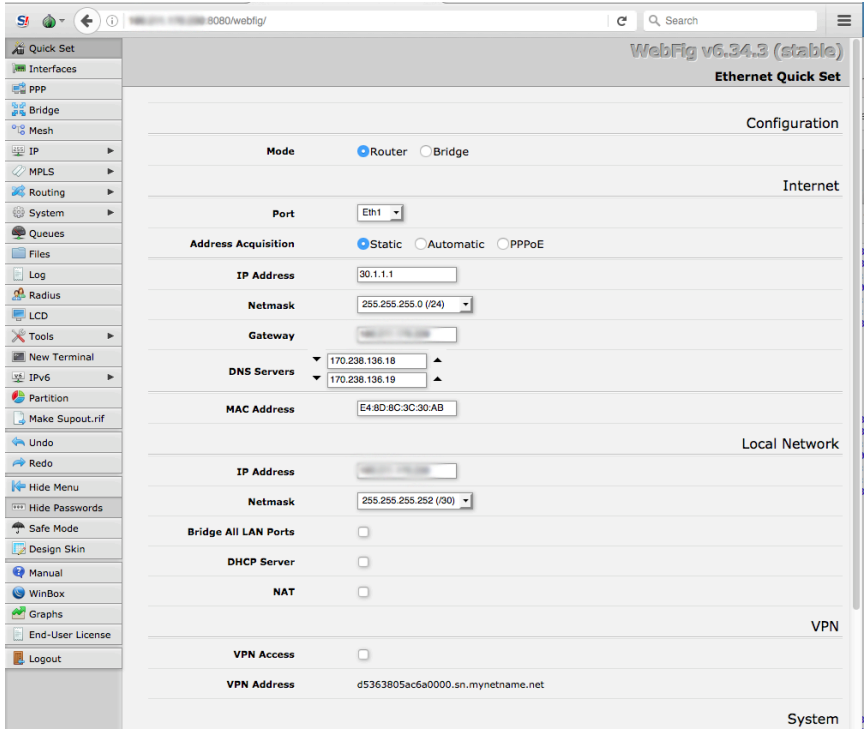
- Easily exploitable routers, old firmware models & default credentials available with a quick google search
- Client side fingerprinting challenges for defenders
- Available for rent in black market

Data Observed December 2016-2017 at large financial institution

- Device Types: 175 open home routers, 10 DVR/camera systems, 10 web servers (incl. Apache Tomcat), 4 webcams, 1 SCADA system

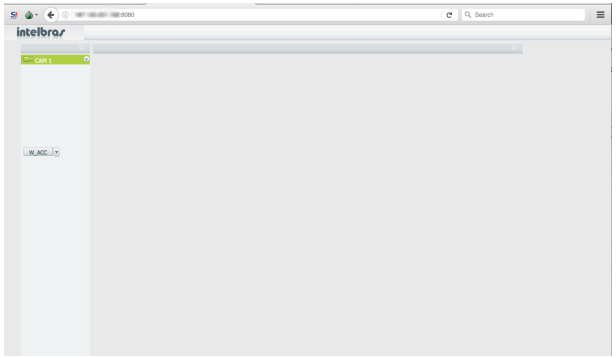
- Common ISPs – Telmex (25%) (Mexico), VDC (Vietnam), Claro Dominican Rebublic, Link Egypt, Telefonica del Peru, TE Data (Egypt), Qubee (Pakistan)

Example – Open routers

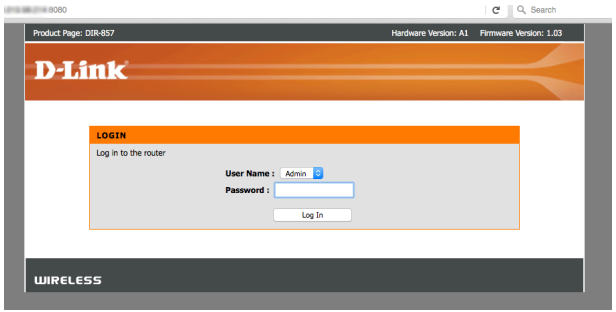


- Admin page open to public on port 8080
- SSH logs showed other attackers trying to brute force login via SSH – "tug-of-war" between attackers.

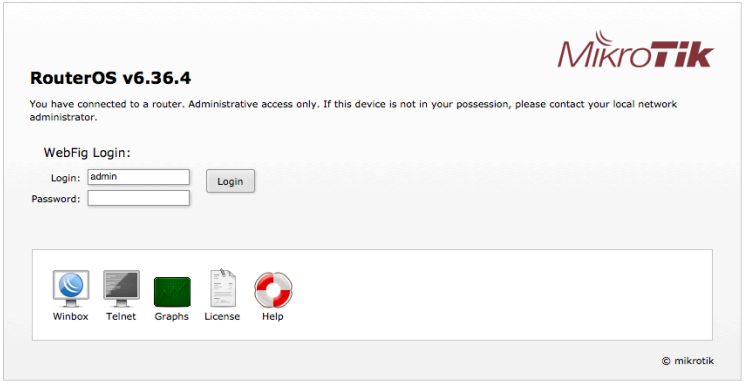
Other device examples:



Intelbras camera system



D-Link, Huawei HG532 and HG8245H, Advantech WebAccess browser-based HMI/SCADA software system (not pictured)



Mikrotic (v6.36.4 and v6.34.3)

Option 3: An Artificially Geo-Distributed Proxy Farm – “The AWS for bad guys”

Levi Strauss

California Gold Rush of 1848
And the creation of Levi’s jeans

Who is this actor and what are some indicators?

Orgs, ISPs, ASNs

ISPs

- Petersburg Internet Network ltd. – 38.7%
- Transit Telecom LLC -- 15.6%
- Atomohost -- 15%
- Link Telecom LLC -- 7.5%
- PP Trusov Ilya Igorevych -- 4.8%

Orgs

- DepoDataCenter -- 25%
- net for depo40.ru -- 25%
- Atomohost -- 11.5%
- Petersburg Internet Network ltd. – 9.5%

ASNs

- 50896
- 29802
- 200557
- 44050, 32181, 44750

```
% Abuse contact for '5.8.44.128 - 5.8.44.255' is 'abuse@pinspb.ru'

inetnum:        5.8.44.128 - 5.8.44.255
netname:        PanamaNet
descr:          Network Panama
country:        PA
admin-c:        TII34-RIPE
tech-c:         TII34-RIPE
status:         ASSIGNED PA
mnt-by:         MNT-DEPO40
created:        2015-01-24T21:22:19Z
last-modified:  2015-01-24T21:22:19Z
source:         RIPE

person:         Trusov Ilya Igorevych
address:        249806, Russia, Kaluga region, Moscow Street 258, office 16
phone:          +79533100064
abuse-mailbox:  abusemail@depo40.ru
nic-hdl:        TII34-RIPE
mnt-by:         MNT-DEPO40
created:        2015-01-24T20:24:14Z
last-modified:  2015-11-20T19:04:51Z
source:         RIPE
```

5.189.200.0/21	DEPO-NET	net for depo40.ru	RU
5.189.200.0/25	CapeTownNet	South Africa Network	ZA
5.189.200.128/25	SeoulNetwork	South Korea Network	SK
5.189.201.0/25	CairoNet	Egypt Cairo Network	EG
5.189.201.128/25	Jakarta Indonesia	Jakarta Indonesia Network	ID
5.189.202.0/25	IslamabadNet	Islamabad Network	PK
5.189.202.128/25	Hanoi Network	Hanoi-Vietnam-Network	VN
5.189.203.0/25	SG-Net	Singapore Network	SG
5.189.203.128/25	Las Vegas Network	Nevada Las Vegas Network	US
5.189.204.0/25	TehranNet	Iran Network	IR
5.189.204.128/25	OgdenNet	Ogden Utah Network	US
5.189.205.0/25	VancouverNetwork	Canada Vancouver Network	CA
5.189.205.128/25	ParisNetwork	France Network	FR
5.189.206.0/25	AlaskaNetwork	Network Alaska US	US
5.189.206.128/25	Helsinki Network	Helsinki Finland Network	FI
5.189.207.0/25	Miami Network	Network Infrastructure to Miam	US
5.189.207.128/25	SwedenNetwork	Sweden Network	SE

More Indicators…

```
organisation:     ORG-TII6-RIPE
org-name:         Trusov Ilya Igorevych
org-type:         LIR
address:          Moscow Street 258, office 16
address:          248021
address:          Kaluga
address:          RUSSIAN FEDERATION
phone:            +79533100064
mnt-ref:          RIPE-NCC-HM-MNT
mnt-ref:          MNT-DEPO40
mnt-by:           RIPE-NCC-HM-MNT
abuse-mailbox:    abusemail@depo40.ru
descr:            Kaluga Data Center Depo
created:          2013-11-08T11,14,03Z
last-modified:    2017-03-29T11,44,15Z
source:           RIPE
e-mail:           iluxa85@inbox.ru
abuse-c:          AC28994-RIPE

person:           Trusov Ilya Igorevych
remarks:          Depo Data Center Kaluga
address:          248021, Russia, Kaluga region, Moscow Street 258, o
phone:            +79533100064
nic-hdl:          TII10-RIPE
e-mail:           noc@depo40.ru
abuse-mailbox:    abusemail@depo40.ru
mnt-by:           MNT-DEPO40
created:          2013-07-19T09,32,30Z
last-modified:    2017-03-26T13,29,22Z
source:           RIPE
```

Lookup Connected Domains Lookup tips

buy.fineproxy.org LOOKUP

Example: 65.55.53.233 or 64.233.161.%

Reverse IP Lookup Results — more than 3 domains hosted on IP address 104.25.240.28

	Domain	View Whois Record	Screenshots
1.	best-proxy.ru		
2.	best-vpn.ru		
3.	fineproxy.org		

IP history results for fineproxy.org.

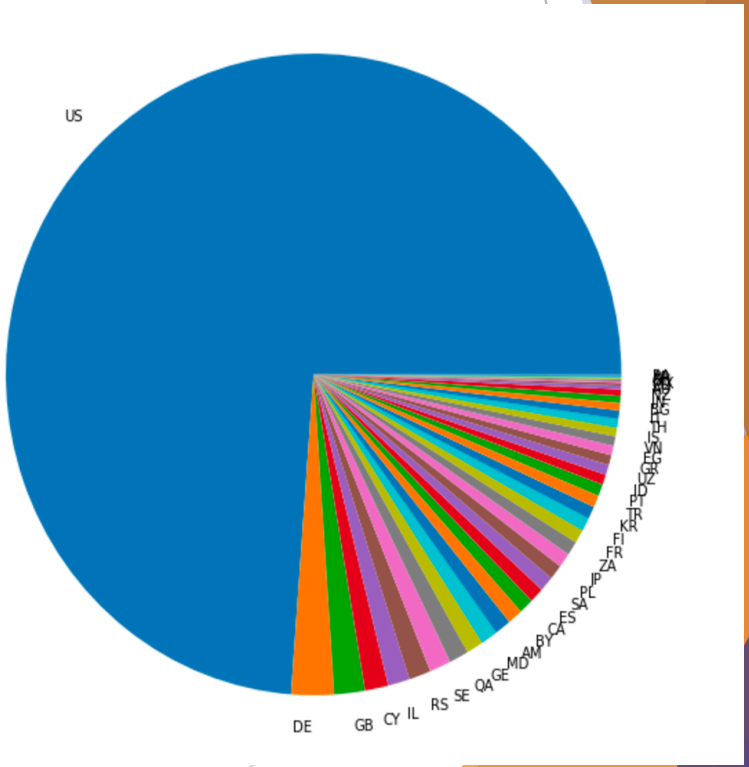
IP Address	Location	IP Address Owner	Last seen on this IP
188.166.44.117	Amsterdam - Netherlands	Digital Ocean, Inc.	2017-10-04
104.25.241.28	United States	Cloudflare, Inc.	2017-08-30
104.25.240.28	United States	Cloudflare, Inc.	2017-08-30
188.166.44.117	Amsterdam - Netherlands	Digital Ocean, Inc.	2017-08-12
104.25.241.28	United States	Cloudflare, Inc.	2017-08-10
104.25.240.28	United States	Cloudflare, Inc.	2017-08-10
104.25.42.16	United States	Cloudflare, Inc.	2016-12-25
198.211.121.105	Amsterdam - Netherlands	DigitalOcean, LLC	2016-12-17

Case Study: Large US Retailer

Attack Statistics

- > 2% of login traffic for over 4 months
- At least 6 unique attack tools used
- 40,000 IP addresses from 61 countries
- Nearly 75% of traffic blending in with US customers
- Thousands of accounts compromised every week

Country Distribution according to MMDB



Was this traffic really coming from the US?

Distributed Traceroute Experiment

RTT from Moscow

MM_City	Max_RTT mean	Max_RTT median	IP count
Albuquerque	69.753600	3.9270	15
Anchorage	602.785067	3.9070	15
Baltimore	4.049400	3.8800	15
Cedar Falls	3.695688	3.7005	16
Dallas	3.818667	3.8140	15
Detroit	356.223118	3.7030	17
Honolulu	5.079800	3.8020	15
Las Vegas	318.735211	3.6900	19
Los Angeles	3.841933	3.8420	15
Miami	203.213533	3.6720	15
None	4.649216	3.8670	51
Ogden	3.766667	3.7300	15
Orlando	3.828545	3.8160	22
Portland	3.900625	3.8340	16
Seattle	3.903438	3.8260	16

RTT from Washington

MM_City	Max_RTT mean	Max_RTT median	IP count
Albuquerque	113.620067	133.8720	15
Anchorage	735.037600	137.0600	15
Baltimore	132.246600	131.7100	15
Cedar Falls	135.660375	134.7540	16
Dallas	136.748600	133.9290	15
Detroit	138.642529	134.1860	17
Honolulu	131.118867	130.6670	15
Las Vegas	455.526316	139.1030	19
Los Angeles	134.830067	133.8160	15
Miami	335.337733	133.4570	15
None	136.346333	135.5950	51
Ogden	136.639333	136.7310	15
Orlando	137.369773	134.7120	22
Portland	133.129375	131.1810	16
Seattle	135.956437	134.1655	16

RTT from Moscow

MM_Country	Max_RTT mean	Max_RTT median	IP count
Argentina	3.705111	3.6865	18
Armenia	4.905533	3.6880	15
Australia	3.690800	3.6910	15
Belarus	4.098400	3.7400	30
Brazil	377.541938	3.7130	16
Bulgaria	3.922000	3.6870	15
Canada	235.931500	3.7685	30
Chile	4.533000	3.7110	15
China	3.924812	3.7580	32
Colombia	180.153412	3.7380	17

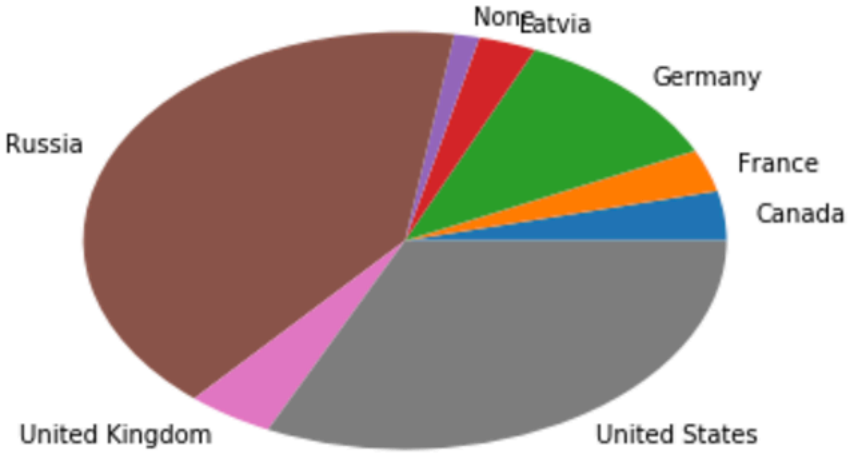
RTT from Washington

MM_Country	Max_RTT mean	Max_RTT median	IP count
Argentina	136.020167	134.8850	18
Armenia	136.280800	134.9330	15
Australia	137.350467	136.7090	15
Belarus	135.353300	134.4010	30
Brazil	511.674937	136.7345	16
Bulgaria	135.216600	134.1660	15
Canada	327.714200	133.7280	30
Chile	137.067067	138.1580	15
China	137.494906	136.5790	32
Colombia	313.156765	136.7450	17

Distributed Traceroute Experiment

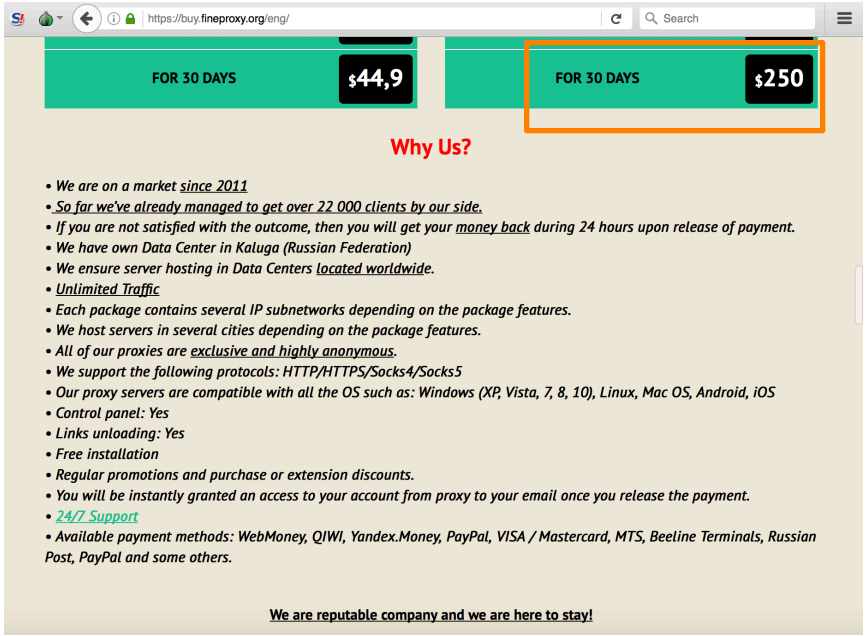
	Chicago	Los Angeles	Moscow
Moscow	143.327ms	213.498ms	—
Tokyo	158.802ms	109.451ms	305.845ms
Washington	35.241ms	62.305ms	136.09ms
Zurich	120.878ms	147.692ms	49.58ms

* https://wondernetwork.com/pings

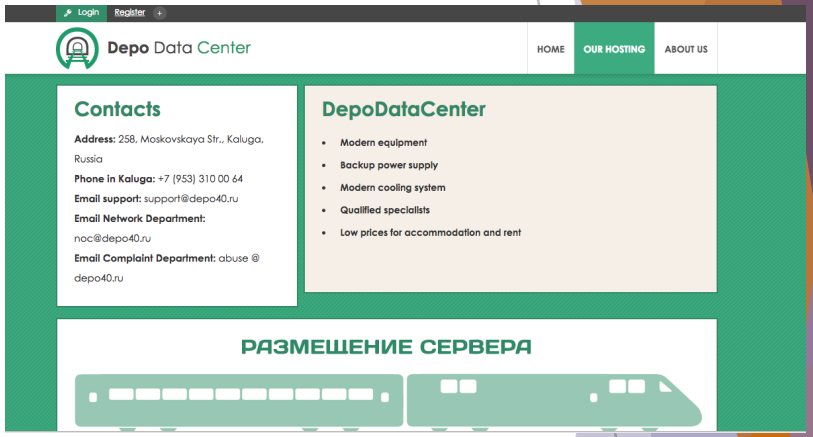


- Country labels according to MMDB for traffic from USA

How do they monetize?



- Remember that "break even" point of $250 with a 0.1% successful login rate? Possible to hit that within 1-3 days.



Defender's Challenge:

How can we detect these attacks in a *proactive* way instead of *reactive* ?

The Defender’s Perspective

The 5 Pillars of Detection for protecting against automated attacks at scale

1) Analysis of HTTP/HTTPS requests and headers to fingerprint attack tools

2) Machine learning models to detect forged browser behavior

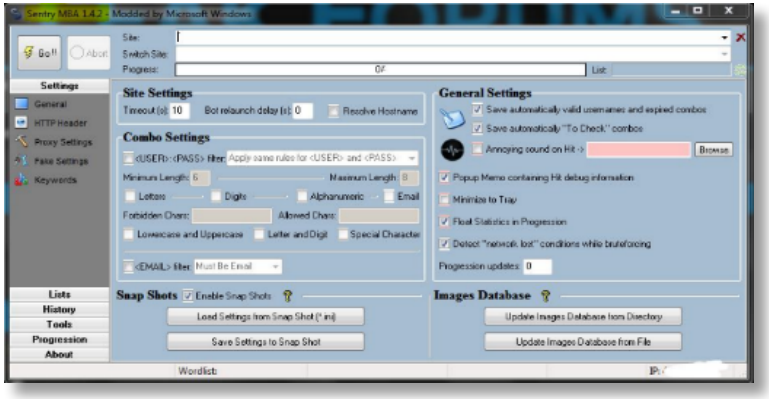
3) Threat intelligence designed to starve attackers of resources (IP addresses, compute power, stolen credentials)

4) Data analytics beyond the individual transaction level – need to detect "recon" behavior & "low and slow" attacks

5) Technology that covers Web, Mobile & API channels – attackers move to wherever there is the least resistance

Case Study: SentryMBA – the "plug & play" attack tool

Pillar 1: HTTP Request Fingerprinting



Default User-Agent Strings

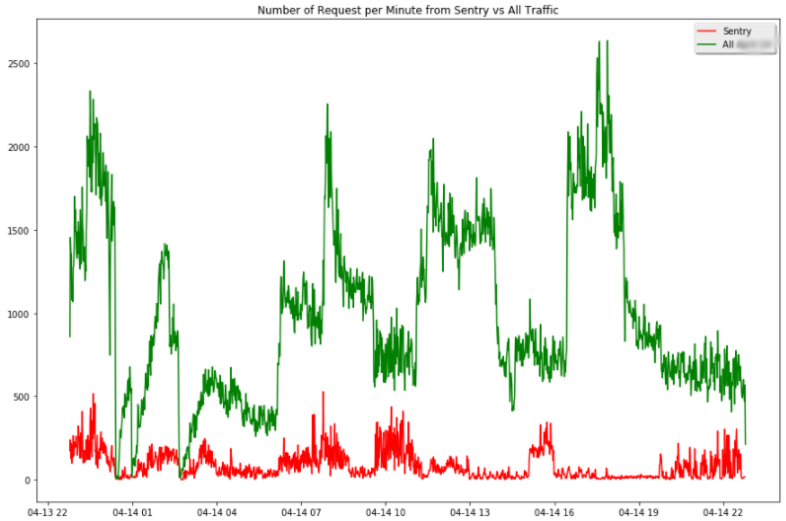
- Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0; .NET CLR 1.1.4322; .NET CLR 2.0.50727; .NET CLR 3.0.4506.2152; .NET CLR 3.5.30729)
- Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; .NET CLR 1.1.4322; .NET CLR 2.0.50727; .NET CLR 3.0.4506.2152; .NET CLR 3.5.30729)
- Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.9.0.11) Gecko/2009060215 Firefox/3.0.11
- Mozilla/5.0 (Windows; U; Windows NT 5.1; en) AppleWebKit/522.11.3 (KHTML,, like Gecko) Version/3.0 Safari/522.11.3
- Opera/9.80 (Windows NT 6.0; U; en) Presto/2.2.0 Version/10.00
- Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1) **Testing UA**

SentryMBA HTTP Fingerprint observations

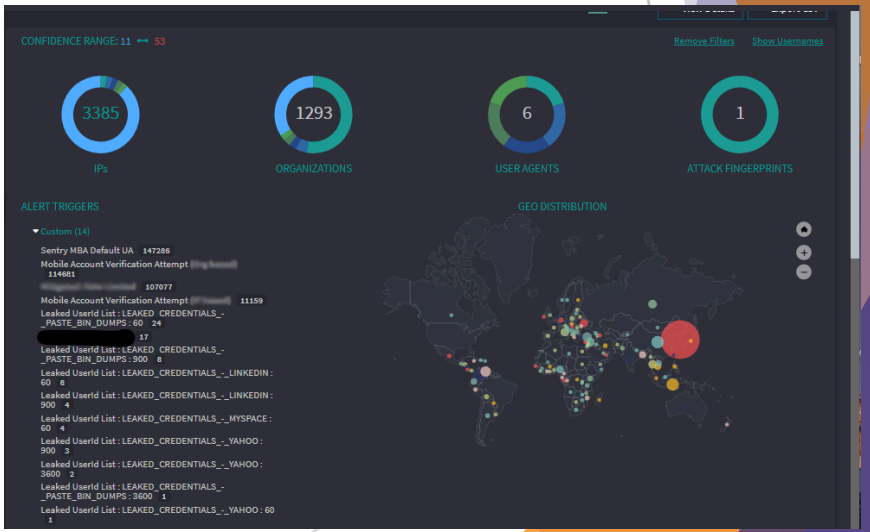
- We analyzed over 1500 config files and found that only 12% changed the request fingerprint
- Often missing referrer, accept-language or accept-encoding

Traffic Patterns

- Both high velocity and low & slow attacks. Suggesting multiple actors using the tool
- Recon activity w/ successful login ratios < .01% and verified credential attacks w/ successful login ratios > 95%



- 150,000 requests from 3,385 IP's and 1,293 Organizations (1 day).
- Leaked credentials from MySpace, Yahoo, LinkedIN, others



The 5 Pillars of Detection for protecting against automated attacks at scale

1) Analysis of HTTP/HTTPS requests and headers to fingerprint attack tools

2) Machine learning models to detect forged browser behavior

3) Threat intelligence designed to starve attackers of resources (IP addresses, compute power, stolen credentials)

4) Data analytics beyond the individual transaction level – need to detect "recon" behavior & "low and slow" attacks

5) Technology that covers Web, Mobile & API channels – attackers move to wherever there is the least resistance

Case Study: Drago & Vlad – "Forged Browser Family"

Pillar 2: Forged Browser detection - ML

Attack Tool "Vlad"

Mozilla/5.0 (Windows NT 10.0; WOW64; rv:40.0) Gecko/20100101 Firefox/40.0

- Impersonating Firefox 40 on Windows 10
- Behaves similar to a command line tool like Wget or Curl

Attack Tool "Drago"

Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/56.0.2924.87 Safari/537.36

- Impersonating Chrome 56 on Windows 8.1
- Doesn't behave like any other browser in Chromium family

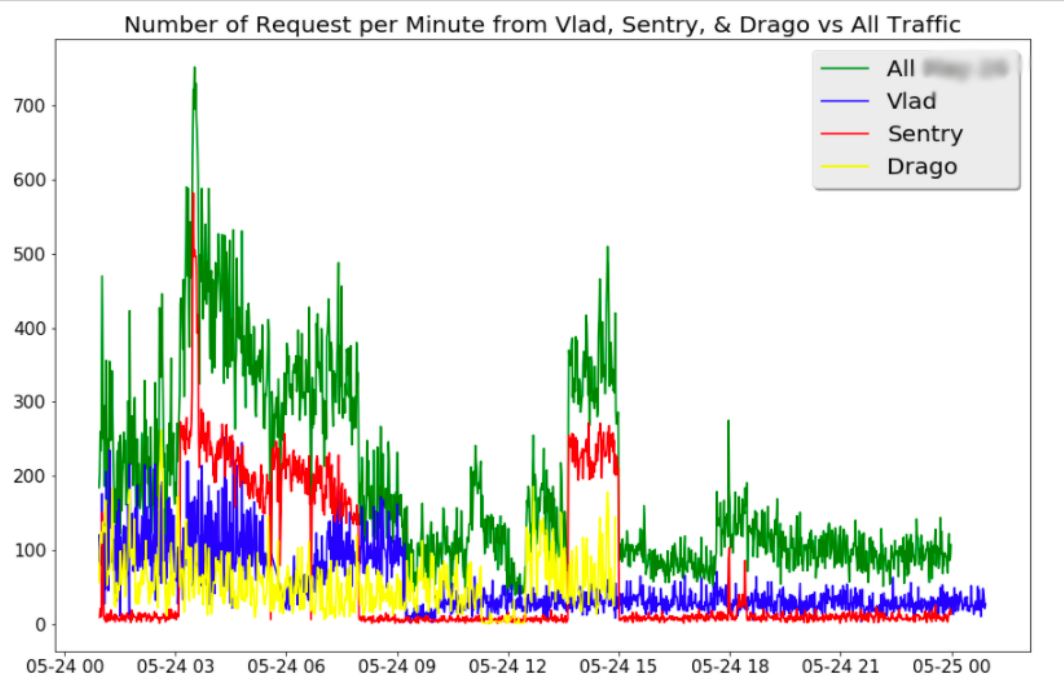
Traffic Patterns

Drago

- More than 3,769 ISPs, 4,160 Organizations and more than 150 countries, with no single ISP/Organization being responsible for more than 3.5% of the tool's traffic.

Vlad

- All traffic claimed to come from the US, yet every request had Accept-language header value equal to "ru-RU"



- Attack tools were responsible for every large spike in traffic, resulting in massive infrastructure overprovisioning.

The 5 Pillars of Detection for protecting against automated attacks at scale

1) Analysis of HTTP/HTTPS requests and headers to fingerprint attack tools

2) Machine learning models to detect forged browser behavior

3) Threat intelligence designed to starve attackers of resources (IP addresses, compute power, stolen credentials)

4) Data analytics beyond the individual transaction level – need to detect "recon" behavior & "low and slow" attacks

5) Technology that covers Web, Mobile & API channels – attackers move to wherever there is the least resistance

Case Study: Leaked Credentials

Pillar 3: Threat Intelligence targeted at resources attackers need

Top Data Breaches Observed per Attack Tool

SentryMBA

23%

19%

17%

- Each username tried appeared in an average of 3.5 breaches

Vlad

32%

25%

22%

- Each username tried appeared in an average of 3.4 breaches

Legitimate Traffic

No Breaches
42%

15%

11%

- Each username tried appeared in an average of 2.6 breaches

The 5 Pillars of Detection for protecting against automated attacks at scale

1) Analysis of HTTP/HTTPS requests and headers to fingerprint attack tools

2) Machine learning models to detect forged browser behavior

3) Threat intelligence designed to starve attackers of resources (IP addresses, compute power, stolen credentials)

4) Technology that covers Web, Mobile & API channels – attackers move to wherever there is the least resistance

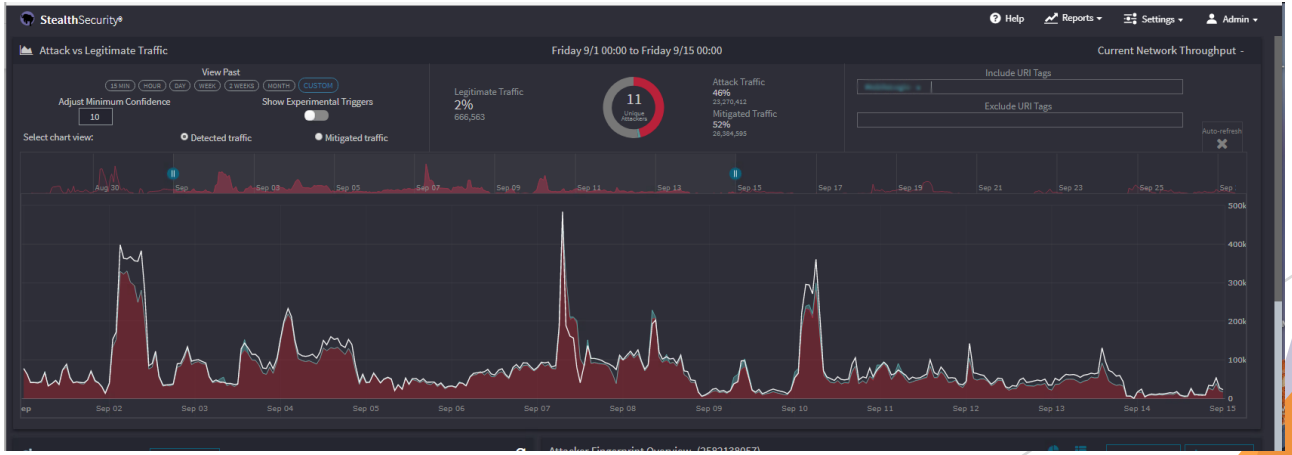
5) Data analytics beyond the individual transaction level – need to detect "recon" behavior & "low and slow" attacks

Case Study: "CoolPad" & Firefox

Pillar 4: Detection and Visibility across Web, Mobile & API

"Coolpad" Attack Tool

- Mozilla/5.0 (Linux; Android 4.4.2; Coolpad 8675 Build/KOT49H) AppleWebKit/537.36 (KHTML, like Gecko) Version/4.0 Chrome/30.0.0.0 Mobile Safari/537.36
- Responsible for 97.2% of traffic to a legacy API login
- A popular Chinese mobile device – which for a US retailer raised a red flag



Firefox 51 Attack Tool

- Mozilla/5.0 (Windows NT 10.0; WOW64; rv:51.0) Gecko/20100101 Firefox/51.0
- Responsible for 40% of web login traffic
- Average of almost exactly 1 login request per unique username for sustained period of time. Legitimate traffic has 1.15-1.3 login requests per unique username.
- Traffic from 210 different countries with accept-language value always "en-US,en;q=0.5,"

Conclusions & Takeaways

- Easy-to-use attack tools have made barriers to entry lower than ever before
- Sensitive data breaches will continue – defenders must pursue this data for preventative measures. Assume all users' info is out there somewhere
- Attackers have a variety of ways to gather the infrastructure they need – cloud hosting providers, botnets-for-rent, compromised machines, etc.
- Researching and fingerprinting the network characteristics of these tools is a very effective first step to detecting these attacks.
- Attackers migrate to the channel with the least friction – defenders need visibility into their API traffic.

Thank you!!!

Will Glazier
will@stealthsec.com
@wglazier21

Mayank Dhiman
mayank@stealthsec.com
@l0pher

www.stealthsec.com