Tracking Unsafe Services that are Hosted by Bots using IP Reputation

Jordan Garzon, Asaf Nadler

Akamai Technologies, Enterprise Security Research

BotConf 2020

About Us

Jordan Garzon

Data Scientist
Akamai Enterprise Security Research

jgarzon@akamai.com

Asaf Nadler

Principal Researcher Lead
Akamai Enterprise Security Research

anadler@akamai.com

Agenda

1 Introduction & System Overview

2 Analysis & Takeaways

Akamai

Introduction

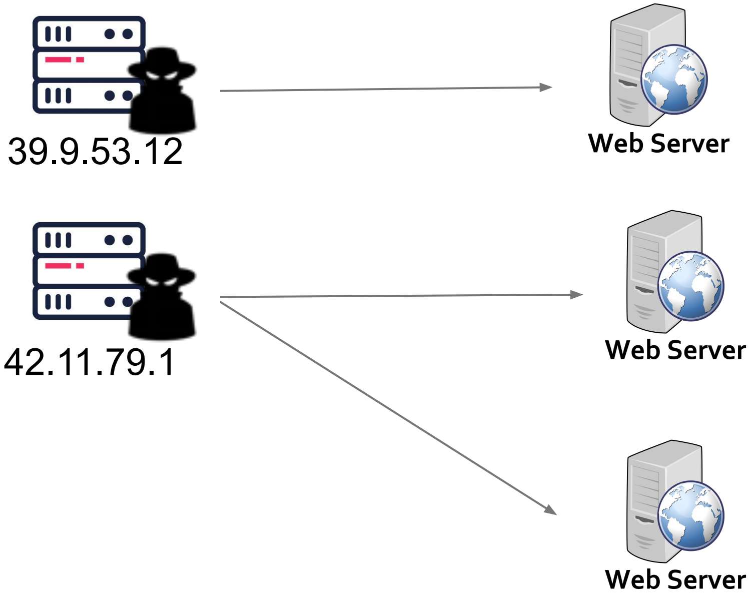
Account Takeover (ATO)

SQL-Injection (SQLi)

Remote File Inclusion (RFI)

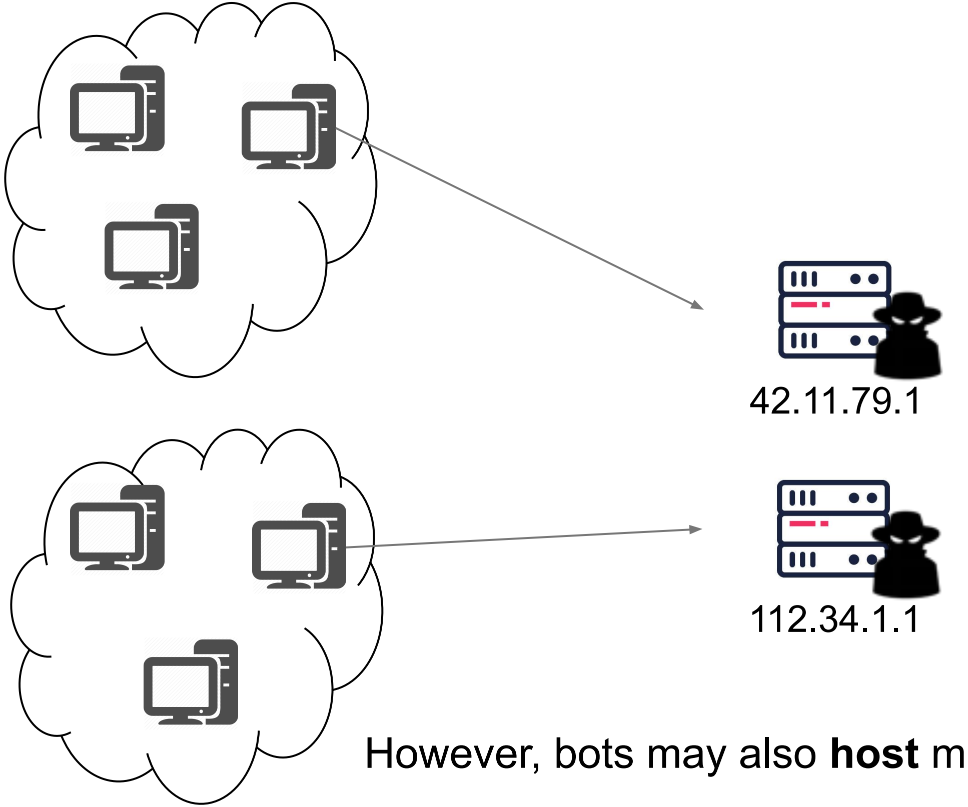
Cross-Site Scripting (XSS)

Distributed Denial-of-Service (DDoS)



Bots are commonly controlled to **deliver** attacks against external services

Introduction



Phishing

Scams and Fraud

Skimmers (Formjacking)

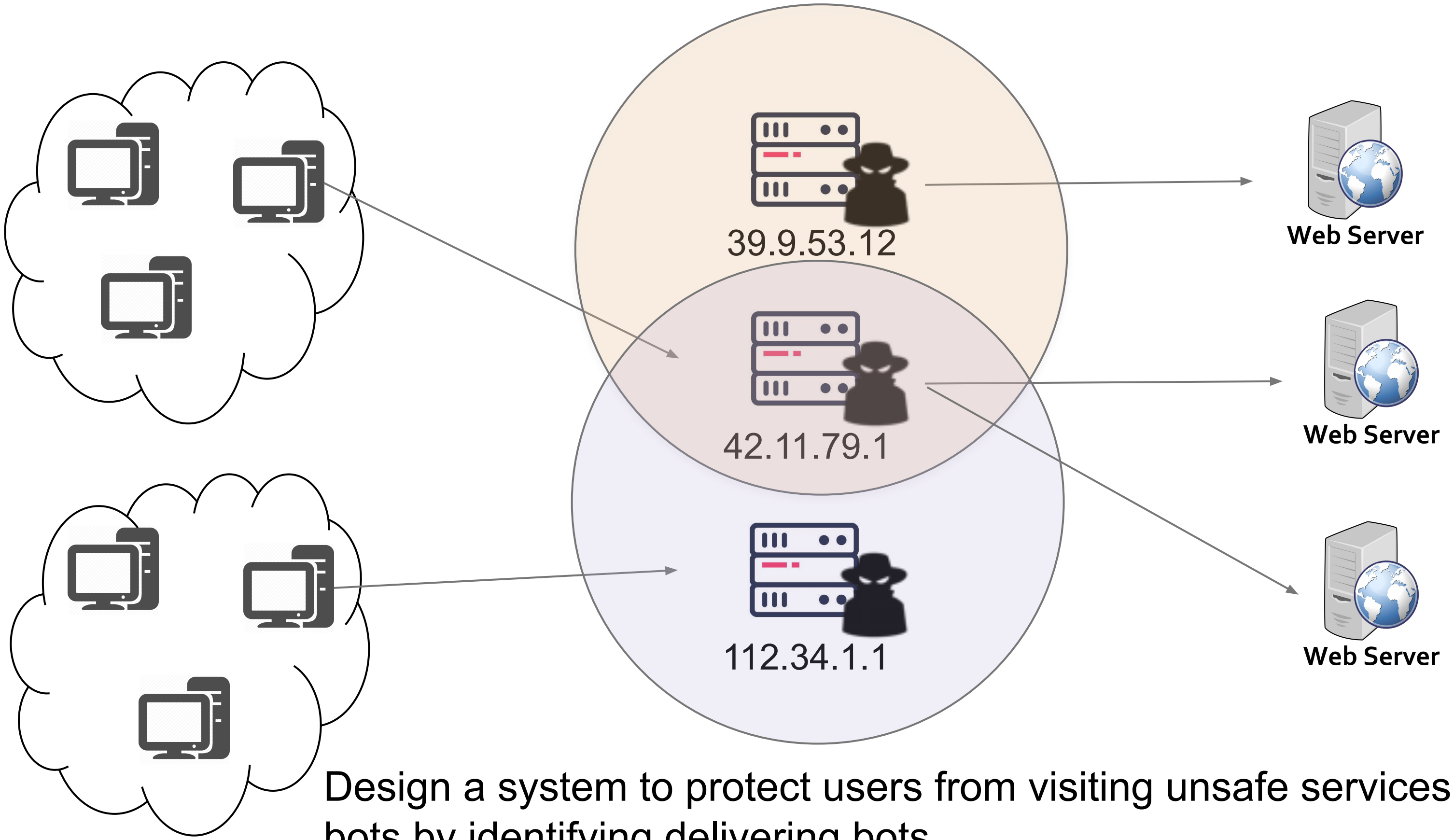
Drive-By Attacks

Callhome Communication

Data Exfiltration

However, bots may also **host** malicious content on behalf of a botmaster

Motivation



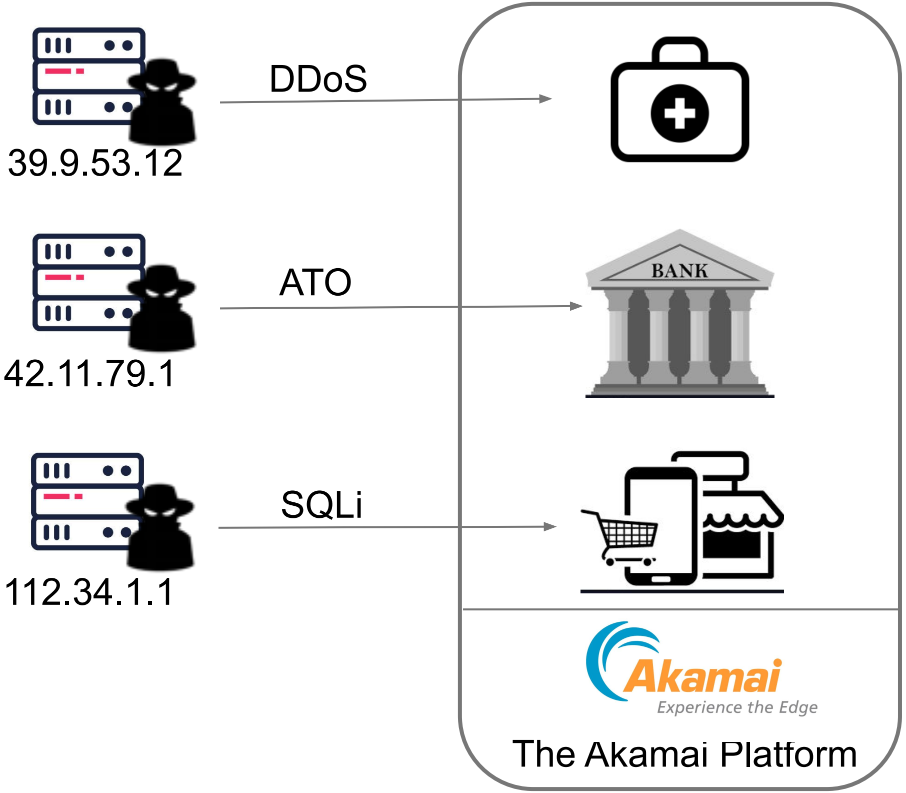
Design a system to protect users from visiting unsafe services hosted on bots by identifying delivering bots

Background: IP Reputation

BANK
Akamai
Experience the Edge

The Akamai Platform

Background: IP Reputation

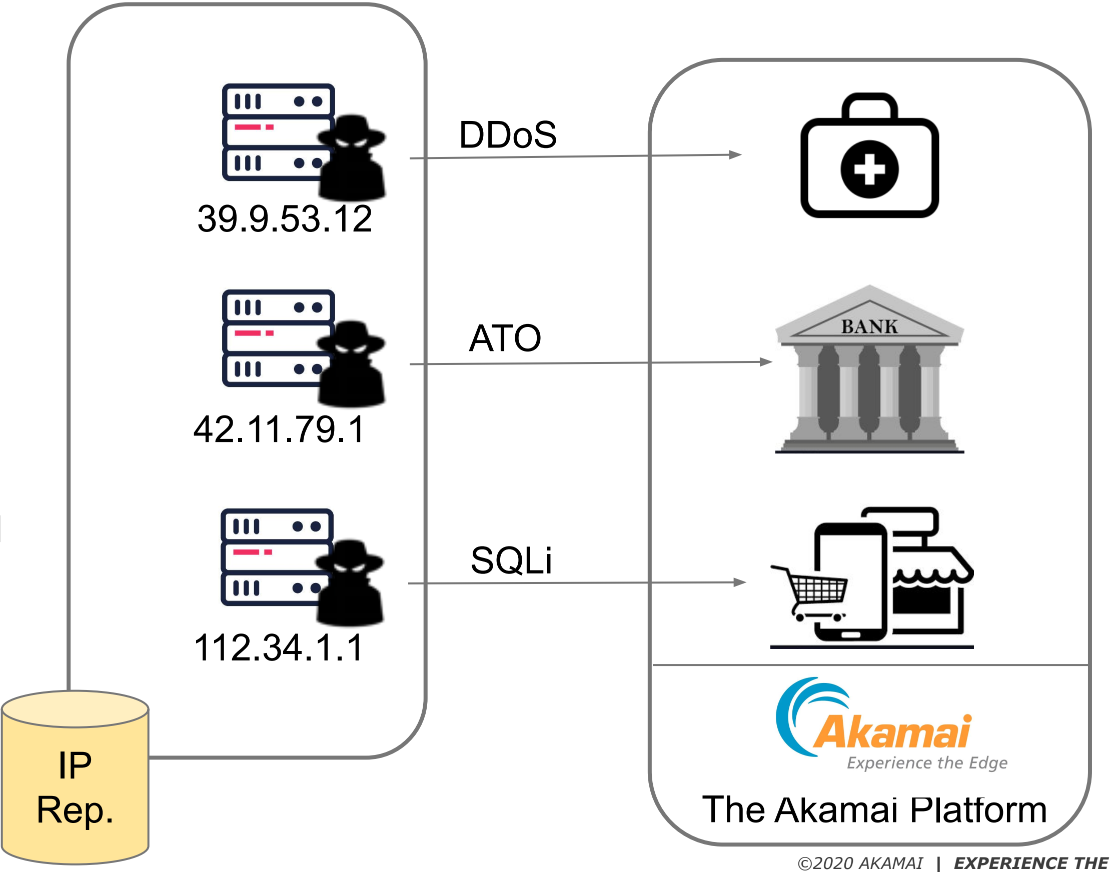


Background: IP Reputation

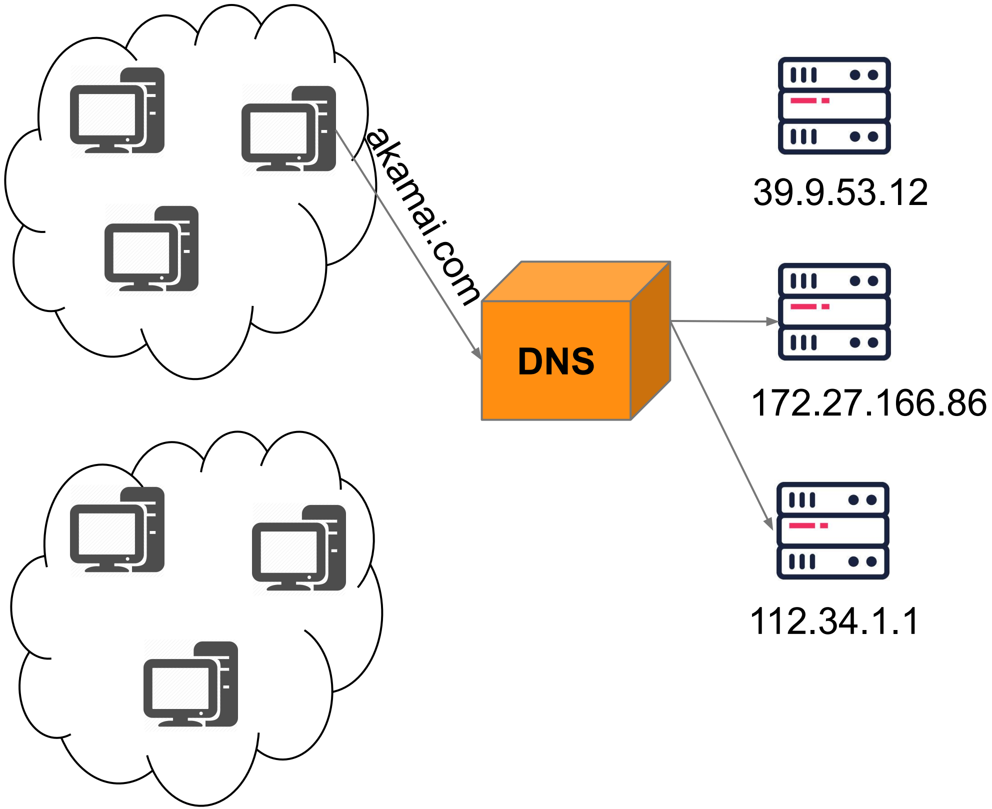
- Akamai CDN hosts 30% of the world's web content, and is accessed by more than 1.3B devices daily

- Akamai Client Reputation (CR) system provides accessing devices with a reputation score

- Devices that carry attacks against websites on the CDN (e.g., D-DoS) receive a low IP reputation score and can be regarded as delivering bots



Background: Domain Name System (DNS)

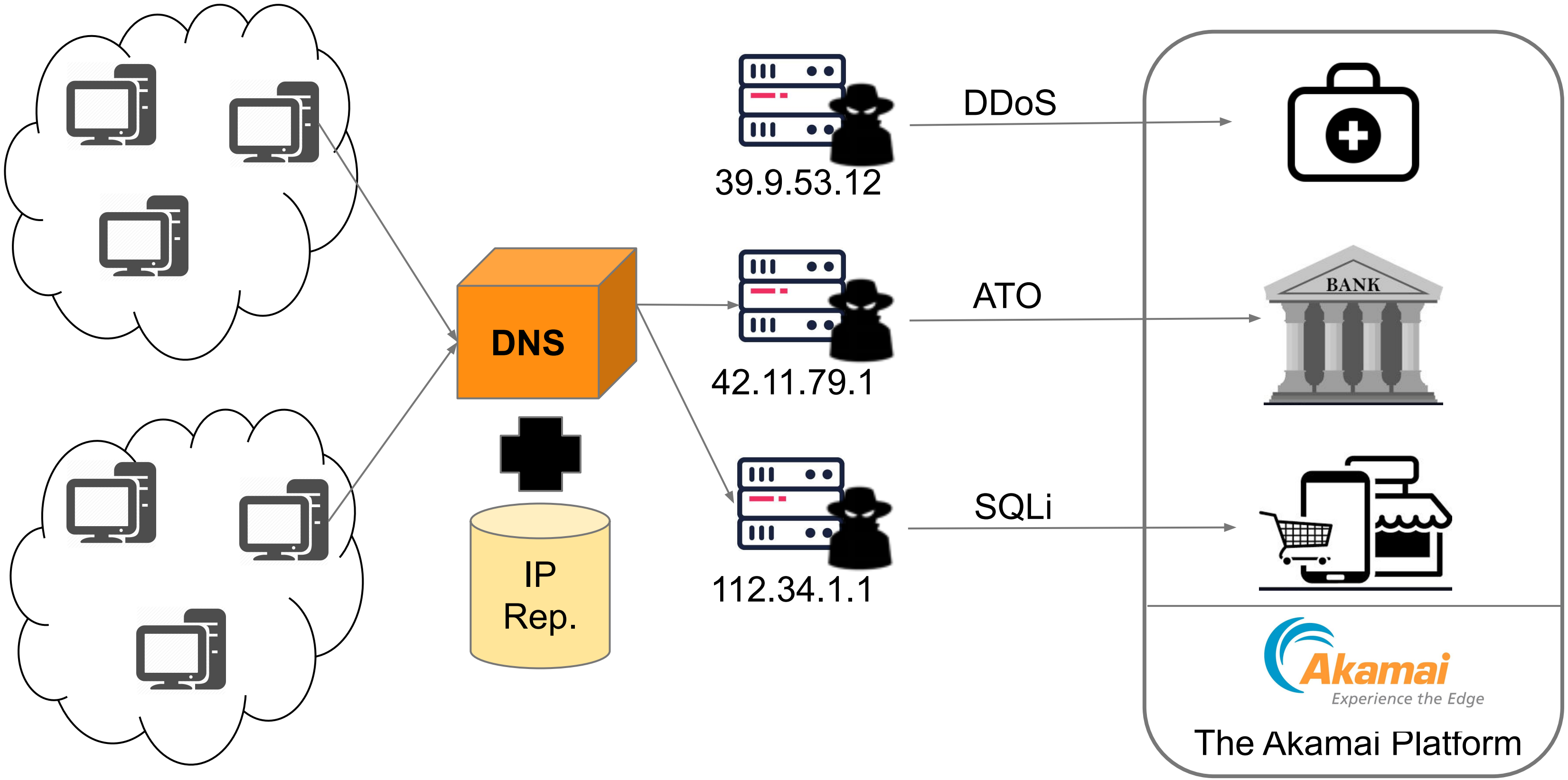


- The DNS protocol to translates human-memorable domain names into Internet-routable IP addresses (e.g., akamai.com to 172.27.166.86)

- Akamai processes >2.2T DNS queries / day

- DNS resolvers can apply security policies on their queries and responses. For instance: don’t translate domain names that resolve to known bots

DNS + IP Reputation to Track Services Hosted on Bots



DNS + IP Reputation to Track Services Hosted on Bots

- The proposed system has two steps

- **Identify IP addresses of bots**: using IP reputation

- **Track services hosted on bots**: in DNS traffic the service (i.e., domain) is hosted on a bot IP, and that IP is not used by any other services for the past 14 days

Analysis & Takeaways

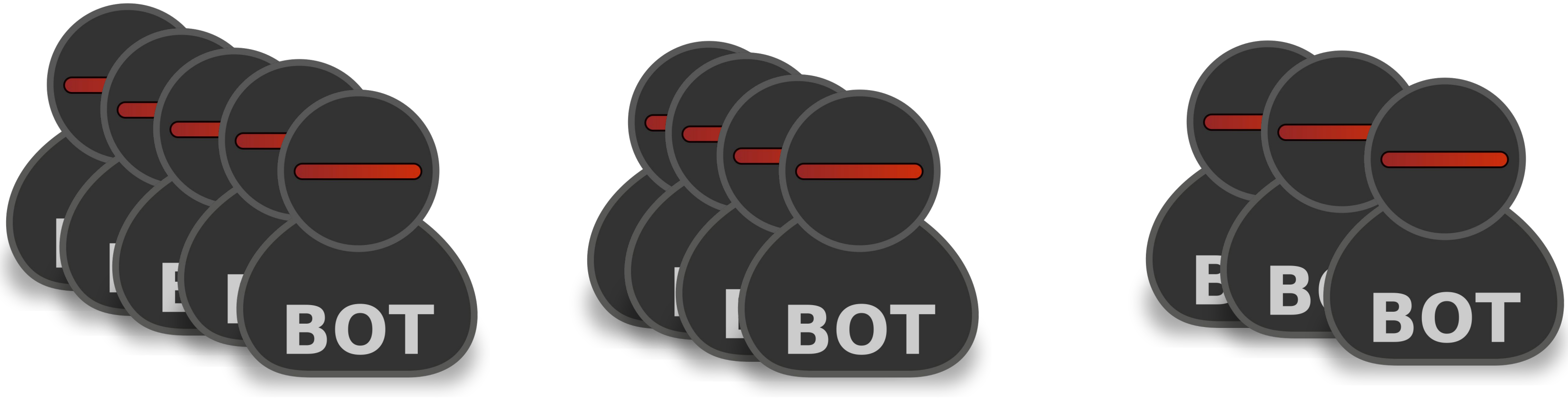
Research Questions for Analysis

- 1. What malicious content is typically hosted on bots ?

- 2. What novel threats are discovered by the system?

Datasets: Bots

- **DS - IP reputation (CDN)**: 737k IP addresses engaged in inbound attacks
  - 721k bots involved in credential abuse and ATO (97.8%)
  - 11k bots involved web attacks such as: SQLi, RFI or XSS attacks (1.5%)
  - 6k bots involved in DDoS attacks (0.7%)



Datasets: Services Hosted on Bots

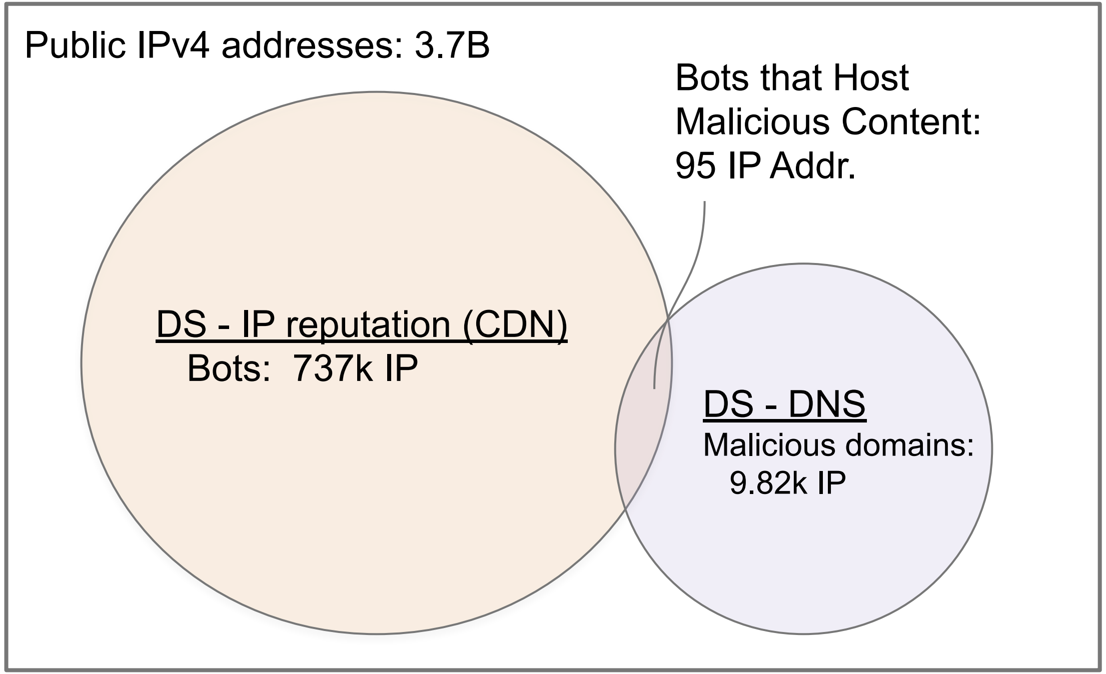
- **Two weeks** of sampled Enterprise DNS traffic with 11B DNS queries / day

- Unique second-level domains: 11.1M (100%)
  - Resolved to a single IP address: 7.87M (70.9%)
  - Resolved IP is unique: 1.66M (14.95%)
  - Identified as outbound attacks: **9.82k (0.1%**)

- **DS - DNS**: **9.82k** domains (100%) with a single and unique IP
  - 4.30k domains that host phishing campaigns (37.97%)
  - 6.26k domains that host malware (55.34 %)
  - 0.76k domains that are used for call home communications (6.69%)

Prevalence of Bots Hosting Malicious Content

~1% of all malicious content (i.e., outbound attacks)
are also involved in inbound attacks (ATO, SQLi, DDOS…)



Public IPv4 addresses: 3.7B

Bots that Host
Malicious Content:
95 IP Addr.

DS - IP reputation (CDN)
Bots: 737k IP

DS - DNS
Malicious domains:
9.82k IP

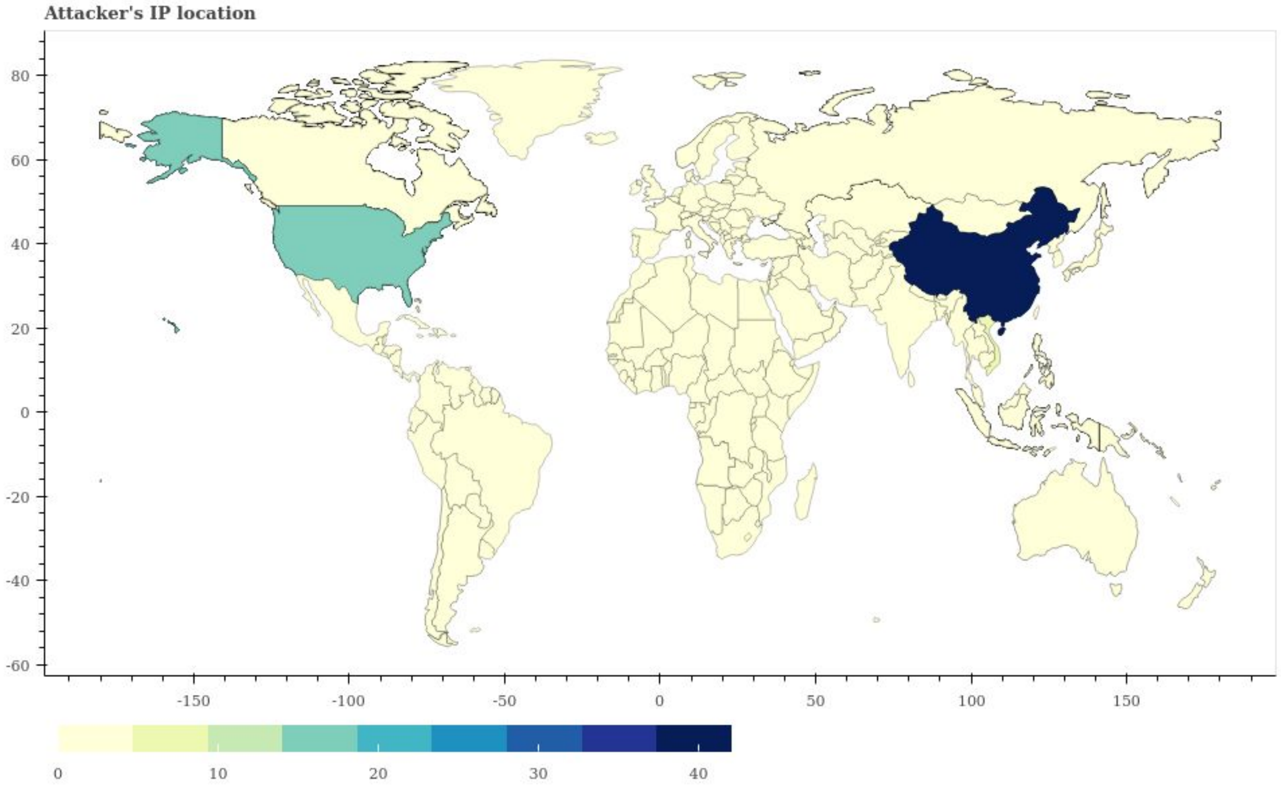
Note:

DS - DNS contains only labelled malicious domain. We can expect a higher correlation than 1%

Prevalence of Bots Hosting Malicious Content

> 61% of inbound/outbound attacks take place from **Asia** and the US

Country	# Machines
China	42 (44.21%)
US	17 (17.89%)
Hong Kong	6 (6.32%)
Vietnam	5 (5.26%)
Singapore	4 (4.21%)
...	...
Total	95 (100%)



The inter-relationships between Bots and Malicious Hosting

>88% of inbound/outbound attacks include a combination of phishing or malware campaigns, with web attacks (SQLi, RFI, LFI, XSS, etc.)

Outbound / Inbound	Web Attack (N=11k)	ATO (N=721k)	DDoS (N=6k)
Phishing-campaigns (N=4.3k)	51	1	0
Malware-hosting (N=6.2k)	33	5	0
C&C Endpoint (N=0.7k)	3	2	0

Detections on Enterprise DNS traffic.

Is it a known issue among the cyber community ?

On a daily basis on Enterprise DNS traffic

- 500 domains blocked **- ~80% not detected by any engine on VT**

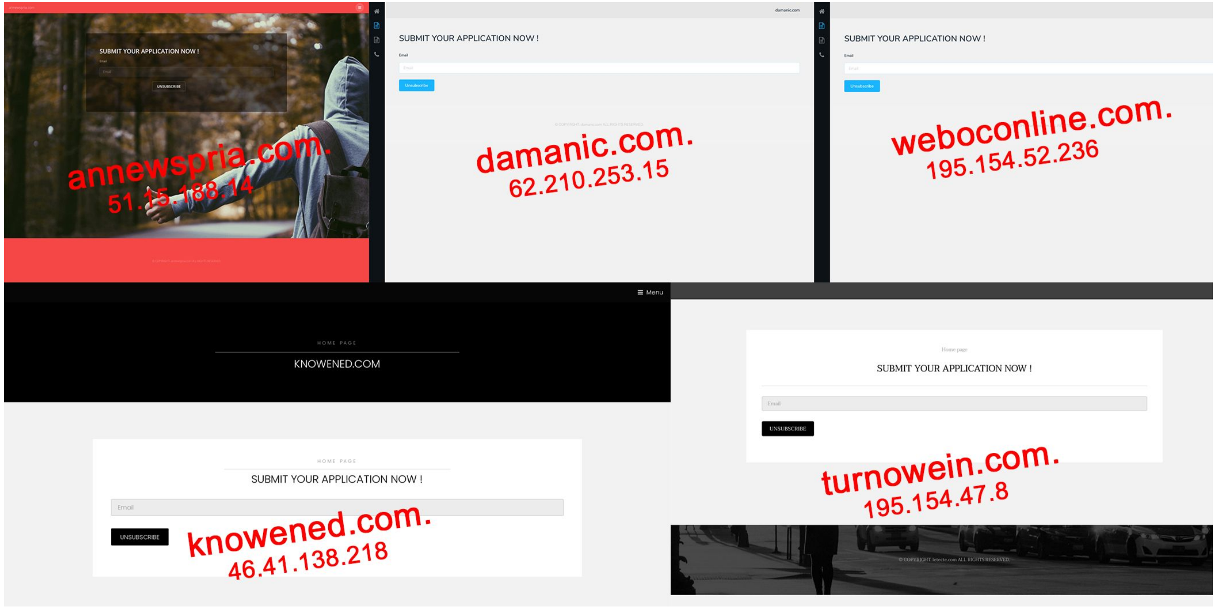
Reminder: By having used very strong filters and high threshold, we can ensure that **those domains are involved in web attacks.**

- 8k domains suspicious

Example: Group of websites under attackers control

October 12th 2020:

- Detection of group of IP issuing ATO attack against a popular French streaming platform
- Some of them get some detections on VT
- Most of them are hosted in France on the same AS
- Websites under attacker's control.



SUBMIT YOUR APPLICATION NOW !

annewspria.com.
51.15.188.14

SUBMIT YOUR APPLICATION NOW !

damanic.com.
62.210.253.15

SUBMIT YOUR APPLICATION NOW !

weboconline.com.
195.154.52.236

KNOWENED.COM

SUBMIT YOUR APPLICATION NOW !

knowened.com.
46.41.138.218

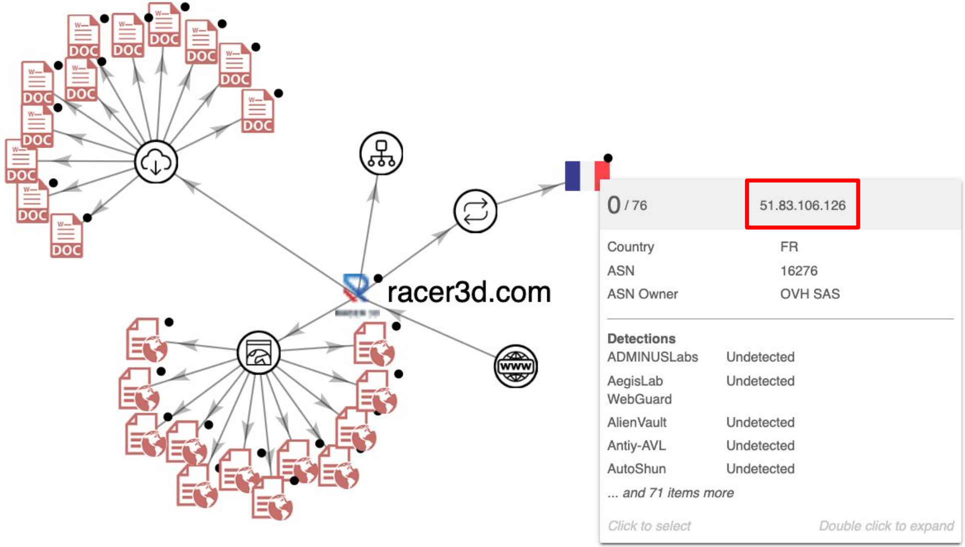
SUBMIT YOUR APPLICATION NOW !

turnowein.com.
195.154.47.8

Would you put your email under the "Submit your application now " ?

We don't recommend it...

Example 2: Classic malicious website



0 / 76	51.83.106.126
Country	FR
ASN	16276
ASN Owner	OVH SAS

Detections	
ADMINUSLabs	Undetected
AegisLab WebGuard	Undetected
AlienVault	Undetected
Antiy-AVL	Undetected
AutoShun	Undetected

... and 71 items more

Click to select *Double click to expand*

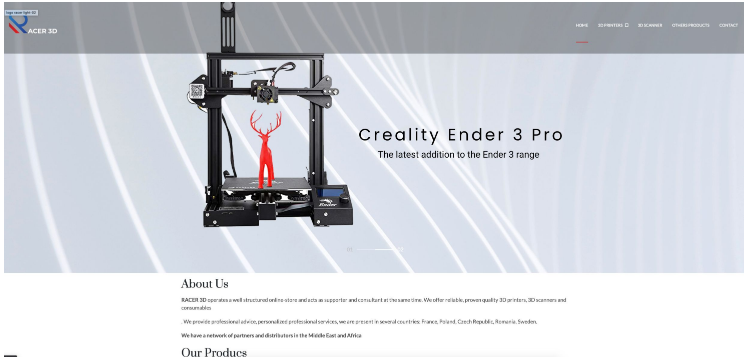
VT graph of racer3d[.]com - November 1st 2020

- 9 detections on VT

EMOTET distributor with .doc files

Started October 30th 2020

- Attacks from 51.83.106.126:
  SQLi, Wordpress vulnerability scans
  on big online retailers ,banks and
  even online pharmacy.
- Our algorithm resolved it to racer3d[.]com
- Domain registered on September 22th 2020



Creality Ender 3 Pro

The latest addition to the Ender 3 range

About Us

RACER 3D operates a well structured online-store and acts as supporter and consultant at the same time. We offer reliable, proven quality 3D printers, 3D scanners and consumables

. We provide professional advice, personalized professional services, we are present in several countries: France, Poland, Czech Republic, Romania, Sweden.

We have a network of partners and distributors in the Middle East and Africa

Our Producs

Home page of racer3d[.]com on November 1st 2020

Conclusions

- More than **1%** malicious websites are involved in web attacks
  - Generally uncommon but exist in specific scenarios
  - Majority appears in non-hosting companies within Asia and US.
  - When looking at phishing or malware-hosting websites, there is a chance that web attacks (SQLi, XSS, LFI…) are issued from the same place

- Protection of users by blocking unsafe web services hosted by bots:
  - > 500 detected domains / day + 8k suspicious domains/day
  - 80% not detected by any AV on VT even though there are definitely linked to malicious activities

Future work

- Convert the suspicious domains to known with metadata (geolocation, AS, website templates, hints from other sources...)

- When it’s possible, convert malicious domains to unique IP to enrich IP reputation

- Release source code/more detailed view the algorithm

Thank you

Q&A