Christopher McHugh & Nicholas Jones
SEC-335
Mackenzie Marsocci
1/16/23

<p align="center">Company: **Infinity Ward**</p>

1. **Gather all the interesting info you can about the organization based on its domain names**

   - Owned by Activision publishing company (certificate is issued to Activision)
   - Careers page where we can view active job listings (note careers.infinityward.com has different information in their certificate)
   - Lots of different social media where they post information regarding projects
   - Fortune 100 best companies to work for
   - Previously worked with other companies/non-profits such as MakeAWish, CallofDuty Endowment, and Stackup.org
   - Advertise the perks of working for them which could be helpful for OSINT (access to restaurants, gyms, and more.)
   - They make video games. COD.
   - Personal data collected from customers is encrypted and saved in a safe location
   - They do not claim to be 100% safe and protected
   -

Name Servers	NS1-181.AKAM.NET (has 128,347 domains)
	NS4-66.AKAM.NET (has 128,347 domains)
	NS5-65.AKAM.NET (has 128,347 domains)
	NS7-66.AKAM.NET (has 128,347 domains)

   -

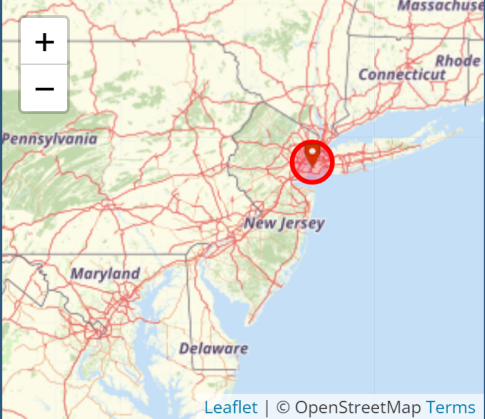 | Test name | Information |
   | --- | --- |
   | Domain NS records | Nameserver records returned by the parent servers are:

ns1-181.akam.net. ['193.108.91.181'] (NO GLUE) [TTL=172800]
ns4-66.akam.net. ['84.53.139.66'] (NO GLUE) [TTL=172800]
ns7-66.akam.net. ['96.7.49.66'] (NO GLUE) [TTL=172800]
ns5-65.akam.net. ['184.85.248.65'] (NO GLUE) [TTL=172800]

l.gtld-servers.net was kind enough to give us that information. |
   | NS records from your nameservers | NS records got from your nameservers listed at the parent NS are:

ns7-66.akam.net ['96.7.49.66'] [TTL=86400]
ns4-66.akam.net ['84.53.139.66'] [TTL=86400]
ns1-181.akam.net ['193.108.91.181'] [TTL=86400]
ns5-65.akam.net ['184.85.248.65'] [TTL=86400] |

   -

- The screenshot above confirmed association between Infinity Ward and Akamai confirming that Akamai is associated with DNS records and IP addresses associated with Infinity Ward.

2. **Gather all the interesting info you can about the organization based on its IP addresses**

InfinityWard Domain IP: 23.221.200.231

IP Details For: 23.221.200.231

Decimal:	400410855
Hostname:	a23-221-200-231.deploy.static.akamaitechnologies.com
ASN:	16625
ISP:	Akamai Technologies Inc.
Services:	Datacenter
Assignment:	Likely Static IP
Country:	United States
State/Region:	New York
City:	New York City
Latitude:	40.712791 (40° 42' 46.05" N)
Longitude:	-74.006065 (74° 0' 21.83" W)

Potential Game Server

- A/The game server IP: 209.170.124.203
- Registrar server: whois.markmonitor.com
- ^Last Updated Date: 2021-09-11T02:32:49Z
- Registrar Abuse Contact Email: abusecomplaints@markmonitor.com
- Domain Status: clientTransferProhibited
- Last update of whois database: 2023-01-17T00:28:42Z
- OS: Apache/2.4.6 (CentOS)

3. **Explore Google Hacking resources:**

    We were able to find that Infinity Ward bought Akamai by using google hacking tools. We did "Infinity Ward" AND "Akamai". This was the one way we were able to find out that there was definitely a relationship between these two companies confirming that some of the IP addresses we found that were associated with Akamai may be related to Infinity Ward.

    The AND functionality with "" aided us on several occasions during our research.

4. **Compile notes for further recon** (what are our next steps)

    Look more into Akamai. This could be potential for getting more insight on Infinity Ward's servers.

    We can also use the employees that work at both Infinity Ward and Akamai for our benefit. Infinity Ward's employees are very active on social media keeping people up to date with new features or changes.

    We could attempt to look into the video games that they created for information but this may be quite difficult and not very beneficial.

    Possible targeted social engineering attack @Registrar Abuse Contact Email: abusecomplaints@markmonitor.com

    Possibly social engineer our way into the company by creating a similar but different email address such as *abusecompliants@markmonitor.com*