OSINT: Enhanced Discovery and Profiling

While true;do RM SCOPE.TXT;done / cat resume.txt

Presented by: David DiEnna
Introduction

David DiEnna

• Senior Consultant at Optiv Security
• 5+ years pentesting
• Host security / OSINT
• Video games, Star Wars & MTG
Introduction

Lars Cohenour

• Consultant at Optiv Security
• 6+ years pentesting
• AD / Post-Ex / Exploit Dev
• Video games, technical guitars, long walks on the beach
Agenda

- What this talk covers:
  - Domain profiling techniques
  - People and metadata enumeration
  - Website enumeration

- What this talk doesn’t cover:
  - Forensic investigations
  - Peoplefinder searches
Introduction (cont’d.)

- OSINT should be used on every test
  - Physical threat
  - Public profiling
  - Network perimeters and internals
  - Social Engineering

- Sample Use Cases:
  - sometimes provided scope is inaccurate – validation
  - evasive assessments – you have to find out the scope & validate
THE ONLY PRESCRIPTION IS MORE OSINT
Disclaimer: Tools & Output

- Recommendations for specific toolsets for performing the job
- You can use your favorite toolset if it makes sense for you
- Compare your results to previous tests to look for ways to improve
OSINT
High Level

- IP Discovery
- Subdomain Enum
- Metadata Analysis
- User & Web Enum
OSINT: Passive vs Active

• Passive – you aren’t actively scanning client’s DNS servers
  • Doesn’t violate privacy laws/rules

• Active – intrusive scans, sending traffic to their servers to profile targets
  • You are touching their stuff, can be attributed to your IP (not observing social distancing rules)

• Further reading: The Art of Subdomain Enumeration
  https://appsecco.com/books/subdomain-enumeration/

<table>
<thead>
<tr>
<th>Passive Fingerprinting</th>
<th>Active Fingerprinting</th>
</tr>
</thead>
<tbody>
<tr>
<td>whois</td>
<td>Finding DNS, MX, AAAA, A</td>
</tr>
<tr>
<td>ASN Number</td>
<td>DNS Zone Transfer(s)</td>
</tr>
<tr>
<td>Enumeration with Domain Name</td>
<td>SRV Records</td>
</tr>
<tr>
<td>Publicly available scans of IP Addresses</td>
<td>Port Scanning</td>
</tr>
<tr>
<td>Reverse DNS Lookup using External Websites</td>
<td></td>
</tr>
</tbody>
</table>
OSINT: Operational Awareness

- Home IPs are relatively obscure when doing basic lookups / visiting sites
- Not all OSINT is passive, sometimes you have to touch a host / asset to obtain intel – if you do, use a VPN
- Use At Your Own Risk:
  - IPVanish
  - ProtonVPN
  - NordVPN
- Note: Geolocation of VPN endpoints may be considered an IOC, so use with discretion
  - Applies mainly to non-attributable testing (don’t blow your cover)
- Keep track of the IPs that you are using (cover your ass)
OSINT:
IP Discovery

- IP Discovery
- Subdomain Enum
- Metadata Analysis
- User & Web Enum
Silly Assumptions

• Customer gave you the correct IP scope
• Customer knows how IPv4 networks work
  • Example: provides RFC-1918 restricted ranges in scoping document
• Customer has full knowledge of their environment
• **Make sure the customer owns the IPs**
  - Businesses often lease IPs from a third-party hosting provider
  - Validate that hosting providers are apprised of testing activities (i.e. Rackspace)

• Especially important if you cannot resolve an IP to a hostname and no company branding is tied to the asset (no web services exposed through Shodan, etc)

• Perform some basic lookups to spot check
  - host – IP to DNS name lookup
  - whois 10.10.10.10 or domain.com
  - nslookup – DNS to IP, or reverse lookup
Case Study: optiv.com

**IP Address / Scope**

<table>
<thead>
<tr>
<th>X.X.X.X</th>
<th>X.X.X.X</th>
<th>X.X.X.X</th>
<th>X.X.X.X</th>
<th>....</th>
<th>....</th>
<th>....</th>
<th>....</th>
</tr>
</thead>
</table>

- Client provided IP scope for perimeter pentest
- Client did not provide hostnames for any targets
Whois (ARIN)

- Validate ownership of IP/hostname
- IANA registrant information
- Domain-based lookups
- Can expose DNS server info
Whois-RDAP

- Whois-RDAP covers the globe (all Regional Internet Registry sources)
- Whois-RDAP is HTTP-based
- Responds in JSON, XML
- Can also search by RIR names and ASN #s
- Uses nicinfo RDAP client for CLI

Whois-RWS (common whois) limited to only ARIN networks (US/Canada)

- Whois-RWS is text-based
- Responds in JSON
- Can search by IP, org names and POCs
Advanced Whois Searching

• Pull addtl info from whois:
  • Emails
  • POCs
Nmap Discovery

- By default performs reverse DNS resolution of live IP addresses

- Useful flags:
  - `-R` (DNS resolution for all targets): Always do reverse DNS resolution including for non-live hosts.
  - `-n` (No DNS resolution): Never do reverse DNS resolution. Note, Nmap will still perform forward lookups if supplied a list of hostnames.
  - `--resolve-all` (Scan each address resolved): Scan all addresses that resolve to a hostname. By default Nmap only scans the first resolved address.
OSINT:
Subdomain Enum

- IP Discovery
- Subdomain Enum
- Metadata Analysis
- User & Web Enum
Data sources are everything

• Many tools available to create your subdomain list
  • Crt.sh
  • Sublist3r
  • Discover.sh
  • ViewDNS
  • Google/Bing/Yandex/Duckduckgo
  • And many many more…
<table>
<thead>
<tr>
<th>crt.sh ID</th>
<th>Logged At</th>
<th>Not Before</th>
<th>Not After</th>
<th>Common Name</th>
<th>Matching Identities</th>
<th>Issuer Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>4467876742</td>
<td>2021-05-03</td>
<td>2021-05-03</td>
<td>2022-04-29</td>
<td>servicedesk.optiv.com</td>
<td>servicedesk.optiv.com</td>
<td>C=US, O=Let's Encrypt, CN=CN</td>
</tr>
<tr>
<td>4467868710</td>
<td>2021-05-03</td>
<td>2021-05-03</td>
<td>2022-04-29</td>
<td>servicedesk.optiv.com</td>
<td>servicedesk.optiv.com</td>
<td>C=US, O=Let's Encrypt, CN=CN</td>
</tr>
<tr>
<td>4151422923</td>
<td>2021-04-09</td>
<td>2021-04-06</td>
<td>2022-04-06</td>
<td>remote.optiv.com</td>
<td>remote.optiv.com</td>
<td>C=US, O=DigiCert Inc, CN=GeoTrust TLS DV RSA Mixed SHA256 2020 CA-A</td>
</tr>
<tr>
<td>4365265789</td>
<td>2021-04-06</td>
<td>2021-04-06</td>
<td>2022-04-06</td>
<td>remoteoptiv.com</td>
<td>remoteoptiv.com</td>
<td>C=US, O=DigiCert Inc, CN=GeoTrust TLS DV RSA Mixed SHA256 2020 CA-A</td>
</tr>
<tr>
<td>4152972250</td>
<td>2021-02-26</td>
<td>2021-02-26</td>
<td>2022-01-19</td>
<td>incapsula.com</td>
<td>incapsula.com</td>
<td>C=BE, O=GlobalSign nv-sa, CN=GlobalSign CloudSSL CA - SHA256 2013</td>
</tr>
<tr>
<td>3984203678</td>
<td>2021-01-25</td>
<td>2021-01-25</td>
<td>2022-01-04</td>
<td>imperva.com</td>
<td>imperva.com</td>
<td>C=BE, O=GlobalSign nv-sa, CN=GlobalSign Atlas R3 DV TLS CA</td>
</tr>
<tr>
<td>395193255</td>
<td>2021-01-19</td>
<td>2021-01-19</td>
<td>2022-01-19</td>
<td>incapsula.com</td>
<td>incapsula.com</td>
<td>C=BE, O=GlobalSign nv-sa, CN=GlobalSign CloudSSL CA - SHA256 2020</td>
</tr>
<tr>
<td>3950640250</td>
<td>2021-01-19</td>
<td>2021-01-19</td>
<td>2022-01-19</td>
<td>incapsula.com</td>
<td>incapsula.com</td>
<td>C=BE, O=GlobalSign nv-sa, CN=GlobalSign CloudSSL CA - SHA256 2020</td>
</tr>
<tr>
<td>3950721824</td>
<td>2021-01-19</td>
<td>2021-01-19</td>
<td>2022-01-19</td>
<td>incapsula.com</td>
<td>incapsula.com</td>
<td>C=BE, O=GlobalSign nv-sa, CN=GlobalSign CloudSSL CA - SHA256 2020</td>
</tr>
<tr>
<td>3941032035</td>
<td>2021-01-17</td>
<td>2021-01-17</td>
<td>2022-01-17</td>
<td>experience.optiv.com</td>
<td>experience.optiv.com</td>
<td>C=US, O=Let's Encrypt, CN=CN</td>
</tr>
<tr>
<td>3941023414</td>
<td>2021-01-17</td>
<td>2021-01-17</td>
<td>2022-01-17</td>
<td>experience.optiv.com</td>
<td>experience.optiv.com</td>
<td>C=US, O=Let's Encrypt, CN=CN</td>
</tr>
<tr>
<td>3918557287</td>
<td>2021-01-04</td>
<td>2021-01-04</td>
<td>2022-01-04</td>
<td>imperva.com</td>
<td>imperva.com</td>
<td>C=BE, O=GlobalSign nv-sa, CN=GlobalSign Atlantic R2 DV TLS CA 2020</td>
</tr>
</tbody>
</table>

### Subdomain lookup by certificate transparency logs

Crt.sh provides a powerful tool for subdomain lookup by certificate transparency logs.
Search engine for internet devices

Scans with Zmap Project tools

API available for automated scans
DNSX

Use with caution. You are responsible for your actions. Developers assume no liability and are not responsible.

client.optiv.com
events.optiv.com
guestswifi.optiv.com
optiv.com
map-ext.optiv.com
lab-ein.optiv.com
guestlogin.optiv.com
cdata.optiv.com
securefile.optiv.com
info.optiv.com
remota.optiv.com
dev.optiv.com
jira.optiv.com
autodiscover.wip.optiv.com
lyncdiscover.optiv.com
servicedesk.optiv.com
mobile.wip.optiv.com
acsedi01-dev.wip.optiv.com
acsedi01-wip.optiv.com

OSINT$ subfinder -silent -d optiv.com | dnsx

projectdiscovery.io

Use with caution. You are responsible for your actions. Developers assume no liability and are not responsible.
edp.optiv.com [8.28.83.149]
edp.optiv.com [edp.wip.optiv.com]
cdata.optiv.com [54.183.78.250]
guestlogin.optiv.com [192.168.248.4]
info.optiv.com [192.28.149.240]
events.optiv.com [54.84.134.174]
experience.optiv.com [3.216.251.45]
experience.optiv.com [3.218.135.46]
experience.optiv.com [unbouncesites.com]
jira.optiv.com [45.60.121.175]
jira.optiv.com [efr7buh.x.incapdns.net]
dev.optiv.com [45.60.121.175]
dev.optiv.com [qeqkkn.x.incapdns.net]
client.optiv.com [13.109.132.27]
OSINT$ subfinder -silent -d optiv.com | dnsx -silent -a -resp
events.optiv.com [54.84.134.174]
info.optiv.com [192.28.149.240]
devo.optiv.com [65.60.121.175]
optiv.com [192.230.66.46]
optiv.com [192.230.76.46]
experience.optiv.com [52.52.200.193]
experience.optiv.com [52.53.110.86]
ews.wip.optiv.com [8.38.243.136]
autodiscover.wip.optiv.com [8.28.83.138]
lab.eim.optiv.com [205.235.89.45]
remote.optiv.com [8.28.83.156]
cdata.optiv.com [54.103.78.250]
securefile.optiv.com [54.215.11.185]
securefile-east.optiv.com [107.22.160.149]
edp.optiv.com [8.28.83.149]
ssso.optiv.com [107.154.108.65]
news.optiv.com [8.38.243.136]
autodiscover.optiv.com [8.28.83.138]
mobile.wip.optiv.com [8.28.83.157]
m经营活动iv.com [8.28.83.134]
yl2.younglivingcomms.com
yl3.younglivingcomms.com
bounce2.email.microsoft.com
return1.commscope.com
bounce.buckleyfirm.com
bounce7.nvidia.com
home.shop.ca
e.rumrockroll.com
e.ironman.com
email.jwplayer.com
bounce.monh.com
e-mail.grow.discoverorg.com
e-mail.engage.discoverorg.io
outbound.digital.ge.com
bounce.cs.solorminds.com
em.rumrockroll.com
bounce8.nvidia.com
boloton.mktdns.com
bardenblue.mktdns.com
e1.snag.co
bounce.chicagosharks.com
e-mail.myfico.com
Subfinder

OSINT$ subfinder -silent -d optiv.com -o test_optiv.txt
ddcsvrlrcl01.optiv.com
securefile-east.optiv.com
syslog-ext.optiv.com
sailpoint.optiv.com
syslog.optiv.com
itop.optiv.com
password.penlab.optiv.com
passwordreset.optiv.com
awtr.optiv.com
ddccspes01.optiv.com
outlook.optiv.com
travelform.optiv.com
survey.optiv.com
bucket-pov.optiv.com
kdcsvlyfe03.optiv.com

- Subdomain enum tools vary in their results
- Overlap scans to potentially ID more subdomains
Wordlist Creation - Altdns

- Feed subdomain list into altdns for ultra specific subdomains
- Some subdomains might be specific to org - find key words using cewl or similar

```
OSINT$ altdns -i test_optiv.txt -o altdns_optiv_output -w words.txt -r -s
[*] 500/278889 completed, approx 1:51:21 left
[*] 1000/278889 completed, approx 1:46:31 left
[*] 1500/278889 completed, approx 1:44:47 left
[*] 2000/278889 completed, approx 1:44:08 left
[*] 2500/278889 completed, approx 1:45:01 left
[*] 3000/278889 completed, approx 1:44:13 left
[*] 3500/278889 completed, approx 1:43:35 left
[*] 4000/278889 completed, approx 1:44:01 left
[*] 4500/278889 completed, approx 1:43:35 left
[*] 5000/278889 completed, approx 1:43:19 left
[*] 5500/278889 completed, approx 1:42:43 left
```

```
OSINT$ head -n 50 altdns_optiv_output
2018-lab2.eim.optiv.com
oscedi01.northamerica.optiv.com
singed-ddcsvrcc01.optiv.com
go.5.optiv.com
search-prod.optiv.com
nautilus.ddccscm01pep.optiv.com
cdnkdcscsad01.optiv.com
support20.optiv.com
ews.wip-boards.optiv.com
testing1-jitterbit.optiv.com
ddcsviafe01.mirror.optiv.com
iune.jitterbit.optiv.com
```
CTFR - Enumerate subdomains using CT logs (crt.sh)
DNS Zone Transfers

- Pull a full list of asset names
- Not always effective but sometimes you get lucky
Sublist3r

OSINT$ python3 sublist3r.py -d optiv.com -b -t 50

# Coded By Ahmed Aboul-Ela - @aboul3la

[-] Enumerating subdomains now for optiv.com
[-] Searching now in Baidu..
[-] Searching now in Yahoo..
[-] Searching now in Google..
[-] Searching now in Bing..
[-] Searching now in Ask..
[-] Searching now in Watercraft..
[-] Searching now in DNSdumpster..
[-] Searching now in ThreatCrowd..
[-] Searching now in SSL Certificates..
[-] Searching now in PassiveDNS..
[-] Starting brute force module now using subbrute..
[-] Total Unique Subdomains Found: 185

optiv.com
www.optiv.com
Securemail.optiv.com
access.optiv.com
answerhub.optiv.com
archer.optiv.com
archerdev-optiv.com
archersb-optiv.com
aruba-master-optiv.com
autodiscover-optiv.com
Discover.sh

- Passive Recon
  - ARIN
  - dnsrecon
  - theHarvester
  - Whois
  - recon-ng

- Active Recon
  - traceroute
  - dnsrecon
  - Whatweb
  - recon-ng
ViewDNS.info

<table>
<thead>
<tr>
<th>Domain</th>
<th>Date</th>
<th>Registrar</th>
</tr>
</thead>
<tbody>
<tr>
<td>myoptiv.com</td>
<td>2015-04-17</td>
<td>NETWORK SOLUTIONS, LLC.</td>
</tr>
<tr>
<td>opt-iv.com</td>
<td>2015-04-17</td>
<td>NETWORK SOLUTIONS, LLC.</td>
</tr>
<tr>
<td>optiv-dev.com</td>
<td>2016-01-06</td>
<td>NETWORK SOLUTIONS, LLC.</td>
</tr>
<tr>
<td>optiv.com</td>
<td>1999-10-21</td>
<td>GODADDY.COM, LLC</td>
</tr>
<tr>
<td>optiv.me</td>
<td>2015-04-17</td>
<td>GODADDY.COM, LLC</td>
</tr>
<tr>
<td>optivblogs.com</td>
<td>2015-11-25</td>
<td>NETWORK SOLUTIONS, LLC.</td>
</tr>
<tr>
<td>optivblogs.net</td>
<td>2015-11-25</td>
<td>NETWORK SOLUTIONS, LLC.</td>
</tr>
<tr>
<td>optivblogs.org</td>
<td>2015-11-25</td>
<td>NETWORK SOLUTIONS, LLC.</td>
</tr>
<tr>
<td>optivblogs.us</td>
<td>2015-11-25</td>
<td>NETWORK SOLUTIONS, LLC.</td>
</tr>
<tr>
<td>optivcanada.com</td>
<td>2016-11-30</td>
<td>NETWORK SOLUTIONS, LLC.</td>
</tr>
<tr>
<td>optivclab.info</td>
<td>2015-07-14</td>
<td>GODADDY.COM, LLC</td>
</tr>
<tr>
<td>optivconsulting.biz</td>
<td>2015-04-17</td>
<td>NETWORK SOLUTIONS, LLC.</td>
</tr>
<tr>
<td>optivconsulting.com</td>
<td>2015-04-01</td>
<td>NETWORK SOLUTIONS, LLC.</td>
</tr>
<tr>
<td>optivconsulting.mobi</td>
<td>2015-04-17</td>
<td>NETWORK SOLUTIONS, LLC.</td>
</tr>
<tr>
<td>optivconsulting.net</td>
<td>2015-04-17</td>
<td>NETWORK SOLUTIONS, LLC.</td>
</tr>
<tr>
<td>optivconsulting.org</td>
<td>2015-04-17</td>
<td>NETWORK SOLUTIONS, LLC.</td>
</tr>
<tr>
<td>optivconsulting.us</td>
<td>2015-04-17</td>
<td>NETWORK SOLUTIONS, LLC.</td>
</tr>
</tbody>
</table>

- Reverse Whois lookups
- Identify other domain names the client owns, add to your domain list
- Won’t work if using domain name privacy protection
THIS IS AN AMASS OF QUALITY MEMES

OWASP Amass

- intel
  Collect intelligence on the target in order to determine your starting point

- enum
  Perform enumeration and mapping of your target to determine possible attack avenues

- viz
  Show results in a visual format to assist with analysis and future research

- track
  Compare results across enumerations to see changes in their attack surface
Amass: Intel

```
OSINT$ amass intel -ip --src addr
    204.91.48.0/24
    38.98.181.0/24
    149.5.73.0/24
ASN: 40414 - OPTIVON - Optivon, Inc.
    208.80.237.224/30
    63.131.242.144/29
    208.80.237.0/30
    208.80.238.68/30
    208.80.237.56/29
    63.131.245.48/29
    208.80.237.48/30
```

```
OSINT$ amass intel -org optiv
    248.4.8.28.83.153, 8.38.243.136, 54.183.78.250, 8.28.83.16, 104.
    3.134, 8.28.83.153, 8.28.83.137, 192.230.66.46, 8.28.83.137, 192.2.
    46, 8.38.243.138, 8.28.83.143, 8.28.83.19, 8.28.83.153, 8.38.243.
    149, 8.28.83.16
[Reverse DNS] us-west-1.compute.amazonaws.com 54.183.78.2
[Reverse DNS] us-west-2.compute.amazonaws.com 54.183.78.2
[Reverse DNS] pphosted.com 148.163.158.168
[Reverse DNS] incapdns.net 192.230.66.46
[Reverse DNS] compute-1.amazonaws.com 107.22.160.149
[Reverse DNS] optimss.com 192.131.107.226
[Reverse DNS] gslb.siteforce.com 13.109.132.27
```
## Amass: Enum

### amass enum --src --d optiv.com

<table>
<thead>
<tr>
<th>CertSpotter</th>
<th>ews.wip.optiv.com</th>
</tr>
</thead>
<tbody>
<tr>
<td>HackerTarget</td>
<td>info.optiv.com</td>
</tr>
<tr>
<td>CertSpotter</td>
<td>oscedi01-dev.optiv.com</td>
</tr>
<tr>
<td>CertSpotter</td>
<td>rap-ext.optiv.com</td>
</tr>
<tr>
<td>CertSpotter</td>
<td>securefile-east.optiv.com</td>
</tr>
<tr>
<td>CertSpotter</td>
<td>cdata.optiv.com</td>
</tr>
<tr>
<td>CertSpotter</td>
<td>go.optiv.com</td>
</tr>
<tr>
<td>CertSpotter</td>
<td>oscedi01-dev.wip.optiv.com</td>
</tr>
<tr>
<td>CertSpotter</td>
<td>remote.optiv.com</td>
</tr>
<tr>
<td>CertSpotter</td>
<td>guestlogin.optiv.com</td>
</tr>
<tr>
<td>CertSpotter</td>
<td>securefile.optiv.com</td>
</tr>
<tr>
<td>HackerTarget</td>
<td>media.optiv.com</td>
</tr>
<tr>
<td>SonarSearch</td>
<td>syslog-extend4.optiv.com</td>
</tr>
<tr>
<td>CertSpotter</td>
<td>servicedesk.optiv.com</td>
</tr>
<tr>
<td>CertSpotter</td>
<td>ews.optiv.com</td>
</tr>
<tr>
<td>CertSpotter</td>
<td>mobile.wip.optiv.com</td>
</tr>
<tr>
<td>CertSpotter</td>
<td>autodiscover.wip.optiv.com</td>
</tr>
<tr>
<td>CertSpotter</td>
<td>syslog-extend.wip.optiv.com</td>
</tr>
<tr>
<td>CertSpotter</td>
<td>syslog-extend.optiv.com</td>
</tr>
<tr>
<td>CertSpotter</td>
<td>mail.wip.optiv.com</td>
</tr>
</tbody>
</table>

### amass enum --ip --d optiv.com

<table>
<thead>
<tr>
<th>Guestwifi.optiv.com</th>
<th>1.1.1.1</th>
</tr>
</thead>
<tbody>
<tr>
<td>info.optiv.com</td>
<td>192.28.149.240</td>
</tr>
<tr>
<td>remote.optiv.com</td>
<td>8.28.83.154</td>
</tr>
<tr>
<td>ews.optiv.com</td>
<td>8.38.243.136</td>
</tr>
<tr>
<td>sip.optiv.com</td>
<td>52.112.66.203,2603:1037:0:b::b</td>
</tr>
<tr>
<td>secureaccess.optiv.com</td>
<td>8.28.83.16</td>
</tr>
<tr>
<td>live.optiv.com</td>
<td>52.23.125.165</td>
</tr>
<tr>
<td>ews.wip.optiv.com</td>
<td>8.38.243.136</td>
</tr>
<tr>
<td>mobile.wip.optiv.com</td>
<td>8.28.83.137</td>
</tr>
<tr>
<td>awa.optiv.com</td>
<td>149.126.77.46</td>
</tr>
<tr>
<td>dev.optiv.com</td>
<td>45.60.121.175</td>
</tr>
<tr>
<td>autodeskoptiv.com</td>
<td>192.131.107.226</td>
</tr>
<tr>
<td>autodiscover.optiv.com</td>
<td>8.28.83.138</td>
</tr>
<tr>
<td>events.optiv.com</td>
<td>54.84.134.174</td>
</tr>
<tr>
<td>oscedi01.wip.optiv.com</td>
<td>8.28.83.143</td>
</tr>
<tr>
<td><a href="http://www.optiv.com">www.optiv.com</a></td>
<td>199.83.131.46</td>
</tr>
<tr>
<td>rap-ext.optiv.com</td>
<td>8.28.83.19</td>
</tr>
<tr>
<td>geodns1-extend.optiv.com</td>
<td>8.28.83.130</td>
</tr>
<tr>
<td>lyncdiscover.optiv.com</td>
<td>52.112.64.78,2603:1027::e</td>
</tr>
<tr>
<td>syslog-extend4.optiv.com</td>
<td>8.28.83.153</td>
</tr>
</tbody>
</table>
Amass enum sucked, now what?

```
amass enum --brute --w wordlist --df <list of resolved domains> -json
```
Amass

Results: 42 subdomains

<table>
<thead>
<tr>
<th>ASN</th>
<th>Name</th>
<th>IP Address</th>
<th>Subdomain Name(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>14618</td>
<td>AMZON-AES - Amazon.com, Inc.</td>
<td>107.20.0.0/14</td>
<td>1 Subdomain Name(s)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>54.80.0.0/13</td>
<td>2 Subdomain Name(s)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>52.20.0.0/14</td>
<td>1 Subdomain Name(s)</td>
</tr>
<tr>
<td>16509</td>
<td>AMAZON-02 - Amazon.com, Inc.</td>
<td>54.212.0.0/14</td>
<td>1 Subdomain Name(s)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>54.183.0.0/16</td>
<td>1 Subdomain Name(s)</td>
</tr>
<tr>
<td>13335</td>
<td>CLOUDFLARENET - CloudFlare, Inc.</td>
<td>104.16.0.0/14</td>
<td>5 Subdomain Name(s)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>192.168.0.0/16</td>
<td>1 Subdomain Name(s)</td>
</tr>
<tr>
<td>38726</td>
<td>VTCDIGICOM-AS-VN VTC DIGICOM</td>
<td>8.38.243.0/24</td>
<td>5 Subdomain Name(s)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>8.28.83.0/24</td>
<td>16 Subdomain Name(s)</td>
</tr>
<tr>
<td>15224</td>
<td>OMNITURE - Adobe Systems Inc.</td>
<td>192.28.144.0/20</td>
<td>1 Subdomain Name(s)</td>
</tr>
<tr>
<td>395146</td>
<td>OTVM-AS-01 - Optiv</td>
<td>192.131.107.0/24</td>
<td>1 Subdomain Name(s)</td>
</tr>
<tr>
<td>22843</td>
<td>PROOFPON-ASN-US-EAST - Proofpoint, Inc.</td>
<td>148.163.158.0/23</td>
<td>1 Subdomain Name(s)</td>
</tr>
<tr>
<td>19551</td>
<td>INCAPSULA - Incapsula Inc</td>
<td>45.60.228.0/24</td>
<td>1 Subdomain Name(s)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>45.60.121.0/24</td>
<td>3 Subdomain Name(s)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>192.230.64.0/21</td>
<td>1 Subdomain Name(s)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>107.154.109.0/24</td>
<td>1 Subdomain Name(s)</td>
</tr>
<tr>
<td>14340</td>
<td>SALESFORCE - Salesforce.com, Inc.</td>
<td>13.198.0.0/15</td>
<td>1 Subdomain Name(s)</td>
</tr>
<tr>
<td>8075</td>
<td>MICROSOFT-CORP-MSN-AS-BLOCK - Microsoft Corporation</td>
<td>52.112.0.0/14</td>
<td>2 Subdomain Name(s)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2683:1000::/26</td>
<td>9 Subdomain Name(s)</td>
</tr>
</tbody>
</table>
What is an autonomous system?

The Internet is a network of networks*, and autonomous systems are the big networks that make up the Internet. More specifically, an autonomous system (AS) is a large network or group of networks that has a unified routing policy. Every computer or device that connects to the Internet is connected to an AS.

- Alternate domains
- Subsidiaries
- Wikipedia
ASN Lookup via domain name

```
OSINT$ host optiv.com
optiv.com has address 192.230.74.46
optiv.com has address 192.230.66.46
optiv.com mail is handled by 10 mxa-00046703.gslb.pphosted.com.
optiv.com mail is handled by 10 mxb-00046703.gslb.pphosted.com.
OSINT$
```

![ARIN Lookup Result]

"192.230.66.46"

<table>
<thead>
<tr>
<th>Source Registry</th>
<th>ARIN</th>
</tr>
</thead>
<tbody>
<tr>
<td>Net Range</td>
<td>192.230.64.0 - 192.230.127.255</td>
</tr>
<tr>
<td>CIDR</td>
<td>192.230.64.0/18</td>
</tr>
<tr>
<td>Name</td>
<td>INCAPSULA-NETWORK</td>
</tr>
<tr>
<td>Handle</td>
<td>NET-192-230-64-0-1</td>
</tr>
<tr>
<td>Parent</td>
<td>NET-192-0-0-0-0</td>
</tr>
<tr>
<td>Net Type</td>
<td>DIRECT ASSIGNMENT</td>
</tr>
<tr>
<td>Origin AS</td>
<td>AS19951</td>
</tr>
<tr>
<td>Registration</td>
<td>Wed, 08 May 2013 21:12:25 GMT (Wed May 08 2013 local time)</td>
</tr>
<tr>
<td>Last Changed</td>
<td>Wed, 08 May 2013 21:12:25 GMT (Wed May 08 2013 local time)</td>
</tr>
<tr>
<td>Self</td>
<td><a href="https://rdap.arin.net/registry/ip/192.230.64.0">https://rdap.arin.net/registry/ip/192.230.64.0</a></td>
</tr>
<tr>
<td>Alternate</td>
<td><a href="https://whois.arin.net/rest/net/NET-192-230-64-0-1">https://whois.arin.net/rest/net/NET-192-230-64-0-1</a></td>
</tr>
<tr>
<td>Port 43 Whois</td>
<td>whois.arin.net</td>
</tr>
</tbody>
</table>
ASN Lookup via curl + nmap

- Displays netblocks
Amass ASN Lookup

```
OSINT$ amass intel -asn 19551
incapdns.net
kredit.co.za
experian.co.za
bancopromerica.com
grupopromerica.com
mizuhoglobalcustody.com
lactalisdobrasil.com.br
mhtny.com
andbank.com
promerica.com.sv
defense.gouv.fr
```

- Displays all domains registered under ASN #
- Can be used as a starting point
- Extend wordlist to perform additional subdomain enum
ASN Lookup Tool

No IPQualityScore token found, so disabling in-depth threat analysis and IP reputation lookups. Please visit https://github.com/nitefood/asn#ip-reputation-api-token for instructions on how to enable it.

ASN lookup for 192.230.66.46

192.230.66.46 PTR 192.230.66.46.ip.incapdns.net
ASN 19551 (INCAPSULA, US)
ORG Incapsula Inc
NET 192.230.66.0/24 (INCAPSULA-NETWORK)
ABU abuse@incapsula.com
ROA / UNKNOWN (no ROAs found)
TYP Hosting/DC

• AS Lookup w/ Org name
• AS Path Tracing
• IP geolocation
• IP reputation
• IP type ID (Proxy Host/Mobile)
OSINT: Metadata Analysis

- IP Discovery
- Subdomain Enum
- Metadata Analysis
- User & Web Enum
Pymeta

- CLI-based
- Super fast
- FOCA sux

Note: Use `–dir <FILE_DIR/>` for offline analysis
  - Useful if you’ve already pulled files from other recon
## Pymeta Results

<table>
<thead>
<tr>
<th>Source Link</th>
<th>File Name</th>
<th>File Size</th>
<th>Author</th>
<th>Creator</th>
<th>File Type</th>
</tr>
</thead>
<tbody>
<tr>
<td><a href="https://www.optiv.com">https://www.optiv.com</a> Cloud_Security</td>
<td>337 KiB</td>
<td>n/a</td>
<td>Adobe InDesign CC 13.1 (Macintosh)</td>
<td>PDF</td>
<td></td>
</tr>
<tr>
<td><a href="https://www.optiv.com">https://www.optiv.com</a> Optiv_GDPR</td>
<td>295 KiB</td>
<td>n/a</td>
<td>Adobe InDesign CC 2017 (Macintosh)</td>
<td>PDF</td>
<td></td>
</tr>
<tr>
<td><a href="https://go.optiv.com">https://go.optiv.com</a> Risk_WFH_S</td>
<td>584 KiB</td>
<td>n/a</td>
<td>Adobe InDesign 15.0 (Macintosh)</td>
<td>PDF</td>
<td></td>
</tr>
<tr>
<td><a href="https://go.optiv.com">https://go.optiv.com</a> Risk_RiskAss 2.7 MiB</td>
<td>n/a</td>
<td>Adobe InDesign 15.0 (Macintosh)</td>
<td>PDF</td>
<td></td>
<td></td>
</tr>
<tr>
<td><a href="https://go.optiv.com">https://go.optiv.com</a> BrettWilliam 78 KiB</td>
<td>n/a</td>
<td>Conga PDF Engine 2015.08 A</td>
<td>PDF</td>
<td></td>
<td></td>
</tr>
<tr>
<td><a href="https://www.optiv.com">https://www.optiv.com</a> Optiv%20Brc 1554 KiB</td>
<td>n/a</td>
<td>Adobe InDesign CC 2014 (Macintosh)</td>
<td>PDF</td>
<td></td>
<td></td>
</tr>
<tr>
<td><a href="https://go.optiv.com">https://go.optiv.com</a> Virtual-Optiv 1756 KiB</td>
<td>n/a</td>
<td>n/a</td>
<td>Adobe InDesign CC 13.0 (Macintosh)</td>
<td>PDF</td>
<td></td>
</tr>
<tr>
<td><a href="https://go.optiv.com">https://go.optiv.com</a> Accelerating 612 KiB</td>
<td>n/a</td>
<td>Adobe Illustrator(R) 17.0</td>
<td>PDF</td>
<td></td>
<td></td>
</tr>
<tr>
<td><a href="https://go.optiv.com">https://go.optiv.com</a> Michele_Mu 707 KiB</td>
<td>User</td>
<td>User</td>
<td>PDF</td>
<td></td>
<td></td>
</tr>
<tr>
<td><a href="https://go.optiv.com">https://go.optiv.com</a> KH2019-113 3.8 MiB</td>
<td>n/a</td>
<td>Adobe Illustrator(R) 17.0</td>
<td>PDF</td>
<td></td>
<td></td>
</tr>
<tr>
<td><a href="https://go.optiv.com">https://go.optiv.com</a> Risk_vCISO_2 638 KiB</td>
<td>n/a</td>
<td>Adobe InDesign 15.0 (Macintosh)</td>
<td>PDF</td>
<td></td>
<td></td>
</tr>
<tr>
<td><a href="https://go.optiv.com">https://go.optiv.com</a> LotC-Gate2-2 494 KiB</td>
<td>n/a</td>
<td>Adobe Illustrator CC 2017 (Macintosh)</td>
<td>PDF</td>
<td></td>
<td></td>
</tr>
<tr>
<td><a href="https://go.optiv.com">https://go.optiv.com</a> Justin%20Wi 142 KiB</td>
<td>Ellery Bahn</td>
<td>Ellery Bahn</td>
<td>PDF</td>
<td></td>
<td></td>
</tr>
<tr>
<td><a href="https://go.optiv.com">https://go.optiv.com</a> John-Bock-Bi 481 KiB</td>
<td>n/a</td>
<td>n/a</td>
<td>Adobe InDesign CC 2014 (Macintosh)</td>
<td>PDF</td>
<td></td>
</tr>
<tr>
<td><a href="https://go.optiv.com">https://go.optiv.com</a> General%201 83 KiB</td>
<td>Ellery Bahn</td>
<td>Ellery Bahn</td>
<td>PDF</td>
<td></td>
<td></td>
</tr>
<tr>
<td><a href="https://go.optiv.com">https://go.optiv.com</a> Colleen%20k 136 KiB</td>
<td>Merchant, C Merchant, Colleen</td>
<td>PDF</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><a href="https://go.optiv.com">https://go.optiv.com</a> Speaker%201 80 KiB</td>
<td>Jeanne Bacq Jeanne Bacque</td>
<td>PDF</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><a href="https://go.optiv.com">https://go.optiv.com</a> Speaker%201 78 KiB</td>
<td>Jeanne Bacq Jeanne Bacque</td>
<td>PDF</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><a href="https://go.optiv.com">https://go.optiv.com</a> Cheryl%20M 104 KiB</td>
<td>Martha LeBlanc Martha LeBlanc</td>
<td>PDF</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><a href="https://go.optiv.com">https://go.optiv.com</a> Ralph%20M 109 KiB</td>
<td>Aspen Chumley Aspen Chumley</td>
<td>PDF</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Usernames
- [Usernames](#)

### Tech stack
- [Tech stack](#)
GOCA
Google Dorking

- Filetype
- Intext
- Ext
- Inurl
- Intitle
GoDork

v1.0.1 - @dwisismart0

[ERR] Query: [site:.optiv.com filetype:pdf]
[ERR] Page: 1
[ERR] Engine: Google

[WRN] Use at your own risk! Developers assume no responsibility...
[WRN] If your IP address has been blocked by search engine providers or other reason.

*https://go.optiv.com/rs/696-TJM-901/images/AcceleratingCloudDeployments_Infographic_1.17.pdf
*https://go.optiv.com/rs/696-TJM-901/images/Michele_Mullen-%20Bio.pdf
*https://go.optiv.com/rs/696-TJM-901/images/LEtC-Gate2-WestClubLouneMap.pdf
*https://go.optiv.com/rs/696-TJM-901/images/Justin%20Williams.pdf
*https://go.optiv.com/rs/696-TJM-901/images/Speaker%20Bios%20archer.pdf
OSINT: User & Web Enum

IP Discovery

Subdomain Enum

Metadata Analysis

User & Web Enum
Automated LinkedIn OSINT:

• It's like online speed dating
• (Only 48% less creepy)

THANKS FOR CONNECTING WITH ME ON LINKEDIN

AND THEN MESSAGING ME 5 MINUTES LATER WITH A SALES PITCH.
Why This Matters:

- LinkedIn is a great resource to gather intel about your targets:
  - Usernames
  - Email addresses
  - Job titles
- And use them in almost all of your engagements primarily for:
  - Public Information Profiling
  - Password Guessing
  - Social Engineering

HEY GIRL
LET'S CONNECT FOR LEGITIMATE NETWORKING PURPOSES
Why You Need Friends:

A poorly connected OSINT LinkedIn account yields jack squat when you search for connections.
Don’t Be This Guy (recon-ng with few contacts)
How do you fix this?

- MOAR CONNECTIONS!
DIY OSINT

- OPSEC101
- Little bit creepy
- Need to seed the acct
DIY OSINT Account:

- Gmail account
- Photo of your new other self
- Background summary
- LinkedIn Profile Job Related Skills
- Scented Candles
- Jazz Music
The Secret Sauce:

“People You May Know” Feature - Overview

The “People You May Know” feature on your My Network page suggests LinkedIn members for you to connect with. These recommendations are based on commonalities between you and other LinkedIn members, as well as contacts you’ve imported from your email and mobile address books.

For example, you may have shared connections, have similar profile information and experiences, work at the same company or industry, or may have attended the same school.
Here Be LIONS (and cougars, rawr)
Friends! Yay!
#WINNING (recon-ng + TONS of connections)

* [contact] Jon Dunlop (<blank>) - Sr. Incentive Compensation Analyst at Optiv Inc
* [contact] Matthew Phillips (<blank>) - Cyber Threat Resistance Analyst at Optiv Inc
* [contact] Rebecca Canze (<blank>) - Project Analyst at Optiv Inc
* [contact] Kelly Bukovac (<blank>) - Project Manager at Optiv Inc
* [contact] Ken Liesche ASV (<blank>) - Vulnerability Analyst at Optiv Inc
* [contact] Justin Trejo (<blank>) - Threat Analyst
* [contact] Joshua Coppola (<blank>) - SOC Analyst at Optiv Inc
* [contact] Ateesh Rajak (<blank>) - Information Security Analyst at Optiv Inc
* [contact] Anthony Nguyen (<blank>) - Threat Analyst at Optiv Inc
* [contact] Kyle VanBecelaere (<blank>) - Threat Analyst at Optiv Inc
* [contact] Russell Hite (<blank>) - Threat Analyst at Optiv Inc
* [contact] McKade Ivancic (<blank>) - Malware Analyst at Optiv Security
* [contact] Brian Reed (<blank>) - Senior Threat Analyst at Optiv

```
* 1492 total (1178 new) contacts found.
```
MY NAME IS IÑIGO MONTOYA. YOU KILLED MY FATHER.

I'D LIKE TO ADD YOU TO MY NETWORK ON LINKEDIN.
Zoominfo.com

- Sales/Marketing/Recruiting
- Subscription Based
- Google Indexed (OH YAS)
Public Breach Data Lookup

• You can subscribe to a service but assume your search history is being watched
• Can create privacy issue for customer
• Sensitive data disclosed might be sold to third party
Public Breach Dumps

<table>
<thead>
<tr>
<th>Don’t use Chrome / Google</th>
</tr>
</thead>
<tbody>
<tr>
<td>Brave (lookup other non-tracking browsers) / Duckduckgo</td>
</tr>
<tr>
<td>Reddit / Torrent sites</td>
</tr>
<tr>
<td>Don’t pay for private leaks – download the public sources</td>
</tr>
<tr>
<td>Flat text file typically</td>
</tr>
<tr>
<td>Pay Services (i.e. SpyCloud)</td>
</tr>
</tbody>
</table>
Public Breach Dumps
Public Breach Dumps
Moar Ideas for Breach Data

• Phonebook.cz
Web Enum

- Directory bruteforcing w/ Gobuster
- Website screenshots with Gowitness / Aquatone
- Wayback Machine
- Visit their website
- DNSX + HTTPX
Web Enum Browser Plugin Edition

- Wappalyzer (Firefox/Chrome) – Identify what technologies are in use for a website.
Web Enum Browser Plugin Edition

• Lightbeam (Firefox) – Creates interactive visualizations between third-party sites and visited sites by analyzing tracking cookies.
Web Enum Browser Plugin Edition

- Link Gopher (Firefox) – Extracts all links from web page, then sorts, removes duplicates, and opens results in new tab.
HTTPX

OSINT$ cat test_optiv.txt
pa.optiv.com
syslog-ext4.optiv.com
awoseg.wip.optiv.com
clearpass1.optiv.com
ddcsvlyfe.optiv.com
doclib.optiv.com
kdccarchdevs01.optiv.com
kdccarchdevs02.optiv.com
persona.optiv.com
lab2.eim.optiv.com
media.optiv.com
servicedesk.optiv.com
securemail.optiv.com
ssso.optiv.com
secureaccess.optiv.com
ddcvappm01.optiv.com
kdccspah01.optiv.com

OSINT$ cat test_optiv.txt | httpx

v1.0.5
projectdiscovery.io

Use with caution. You are responsible for your actions.
Developers assume no liability and are not responsible.
https://autodiscover.optiv.com
https://autodiscover.wip.optiv.com
https://edp.optiv.com
https://dev.optiv.com
https://eim.optiv.com
https://events.optiv.com
https://experience.optiv.com
https://go.optiv.com
https://jira.optiv.com
https://lab.eim.optiv.com
https://live.optiv.com
https://lyncdiscover.optiv.com
https://owa.optiv.com
https://optiv.com
https://remote.optiv.com
https://secureaccess.wip.optiv.com
https://secureaccess.optiv.com
https://servicedesk.optiv.com
Aquatone
Wireless Enum (WAT?!)

[Image of a screenshot from a wireless enumeration tool showing a map with Wi-Fi network information]
Wigle.net

- Local BSSID/ESSIDs
- Encryption algos
- WiFi Channel info
OSINT Framework: RiskIQ
OSINT Frameworks: SecurityTrails
Aaaand we’re done
OSINT University

- Twitter - #OSINT
  - follow these fine peeps
  - @namehere111
  - @aprilwright
  - @mtomasini_
  - @k3vk4
  - @xialor78 <--- me
Try it yourself – Free Public Testing Sites
Free Playgrounds

Test Infrastructure

This domain hosts a BIND9 server which exposes several test endpoints used by the Amass build process to identify any issues with domain enumeration during development.

Here are the subdomains currently in use:

- axfr.owasp-amass.com - Used to test zone transfer
- letsencrypt.owasp-amass.com - Used to test passive data sources such as crt.sh
- bruteforce.owasp-amass.com - Used to test the brute-force module
- wildcard.owasp-amass.com - Used to detect wildcards
Sample Testing Domains

Eastlake & Panitz

Best Current Practice

[Page 2]

RFC 2606

Reserved Top Level DNS Names

June 1999

example.com
example.net
example.org

4. IANA Considerations

IANA has agreed to the four top level domain name reservations specified in this document and will reserve them for the uses indicated.
Bonus Round – The “Dark Web”

- WHY?!: org reputation gathering intel
- Requires OPSEC+: TOR browser + VPNs
- Legal issues can arise if not careful
“Web” Terminology

• https://medium.com/@selsecurity/what-is-the-dark-web-259916e9a7eb

• Washington Post Secure Drop: http://vbmwh445k3fs2v4.onion
• Wikileaks Secure Drop: http://suw74isz7wqzpmgu.onion/
• Dark web search engine: https://ahmia.fi/
Deep Web vs Dark Web Searching
Reference Links (what you really came for)

IP Lookups
- https://lookup.icann.org/lookup
- https://www.arin.net/resources/registry/whois/rdap/#using-an-rdap-client
- https://github.com/infosec-au/altdns
- http://he.net/
- https://github.com/nitefood/asn
- https://github.com/projectdiscovery/mapcidr
Subdomain Enum
• https://github.com/projectdiscovery/subfinder
• https://github.com/aboul3la/Sublist3r
• https://securitytrails.com/list/apex_domain/optiv.com
• https://danielmiessler.com/study/amass/
• https://community.riskiq.com/search/optiv.com/subdomains
• https://github.com/nitefood/asn
• https://viewdns.info/asnlookup/?asn=19551
• https://hackertarget.com/as-ip-lookup/
• https://github.com/projectdiscovery/dnsx

Metadata
• https://github.com/dwisiswant0/go-dork
• https://hazanasec.github.io/2021-03-11-Dorking-on-Steriods/
• https://github.com/m8r0wn/pymeta
• https://github.com/gocaio/goca
Metadata
• https://github.com/dwisiswant0/go-dork
• https://hazanasec.github.io/2021-03-11-Dorking-on-Steriods/
• https://github.com/m8r0wn/pymeta
• https://github.com/gocaio/goca

User & Web Enum
• https://github.com/projectdiscovery/httpx
• https://builtwith.com/

Frameworks
• https://community.riskiq.com/login
• https://securitytrails.com/

My OSINT Link Repository
• https://start.me/p/OmGx86/osint
LA FIN
Questions?

- Twitter
  - @xiaolor78
- LinkedIn
  - https://www.linkedin.com/in/david-dienna-4aa39a8/
- Discord
  - LiquidN2#6420