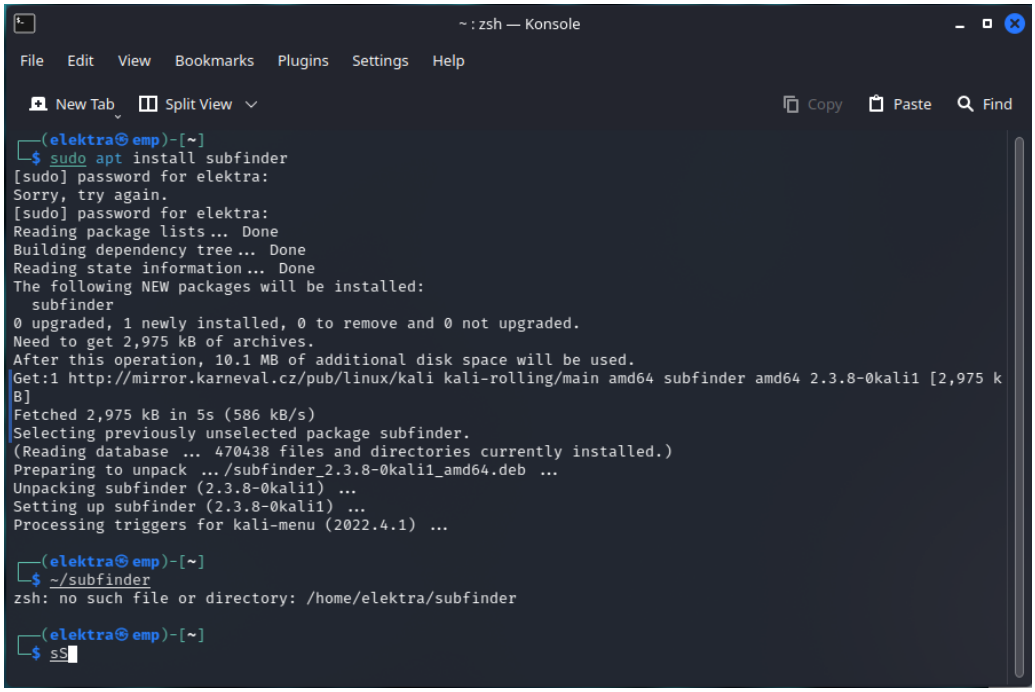
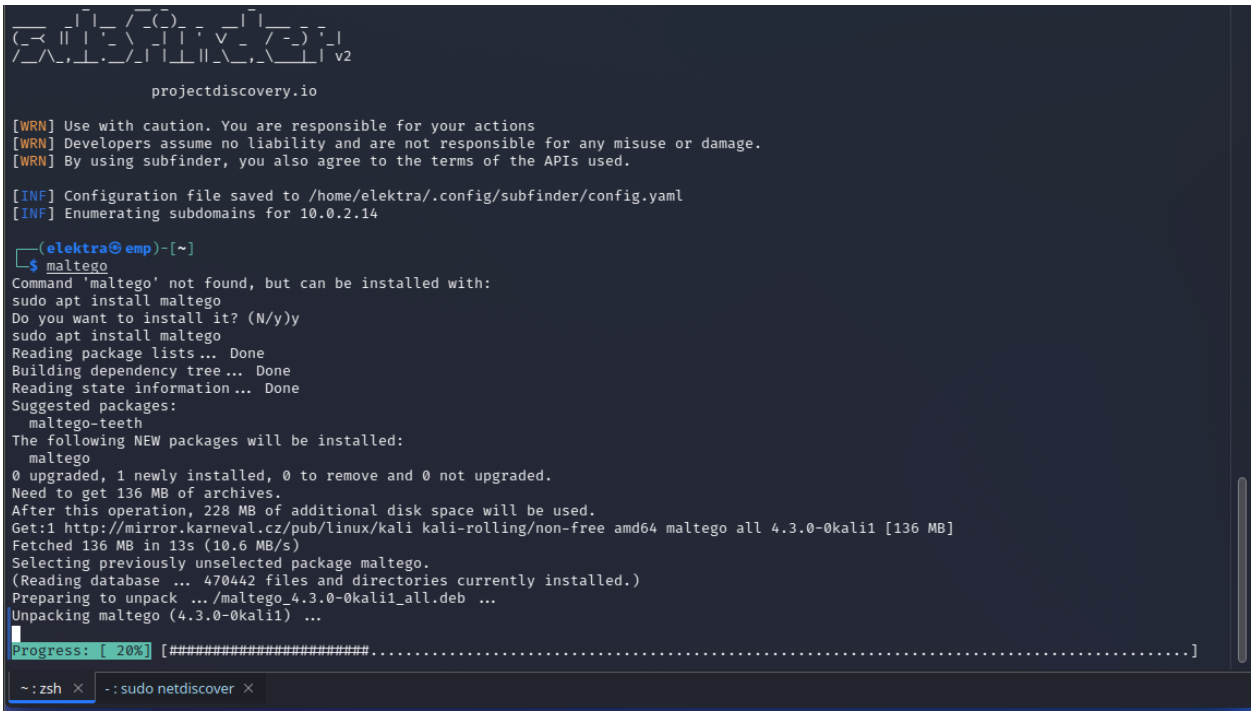
Subfinder Install

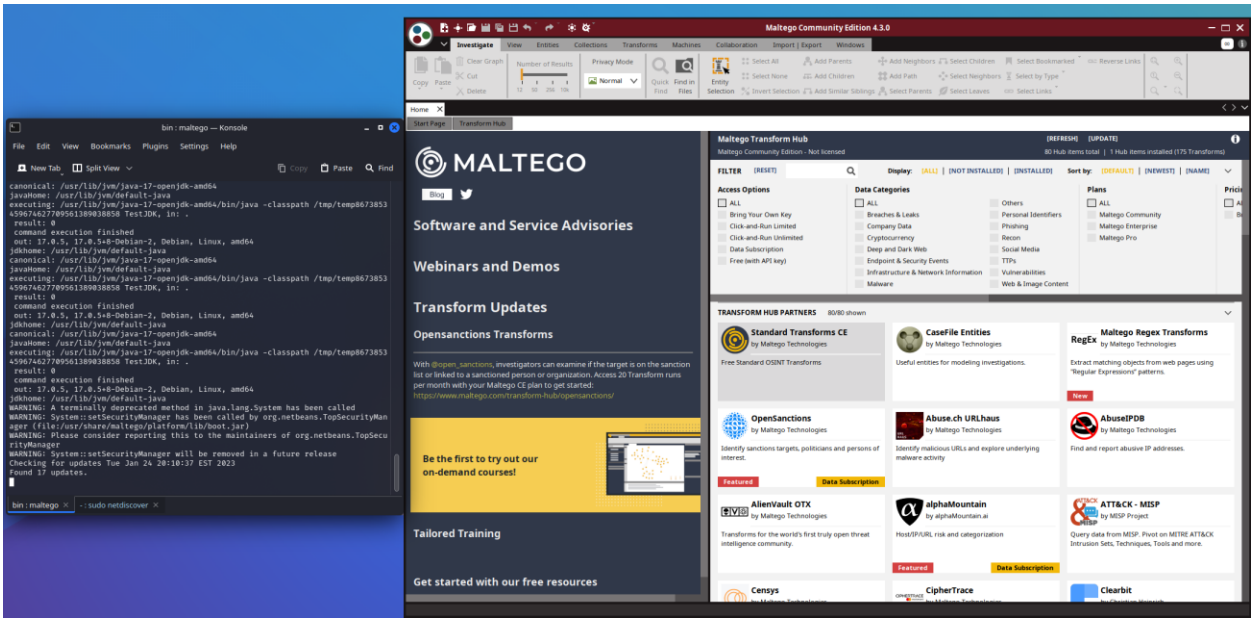


Installing subfinder to traverse the domains

Maltego Install

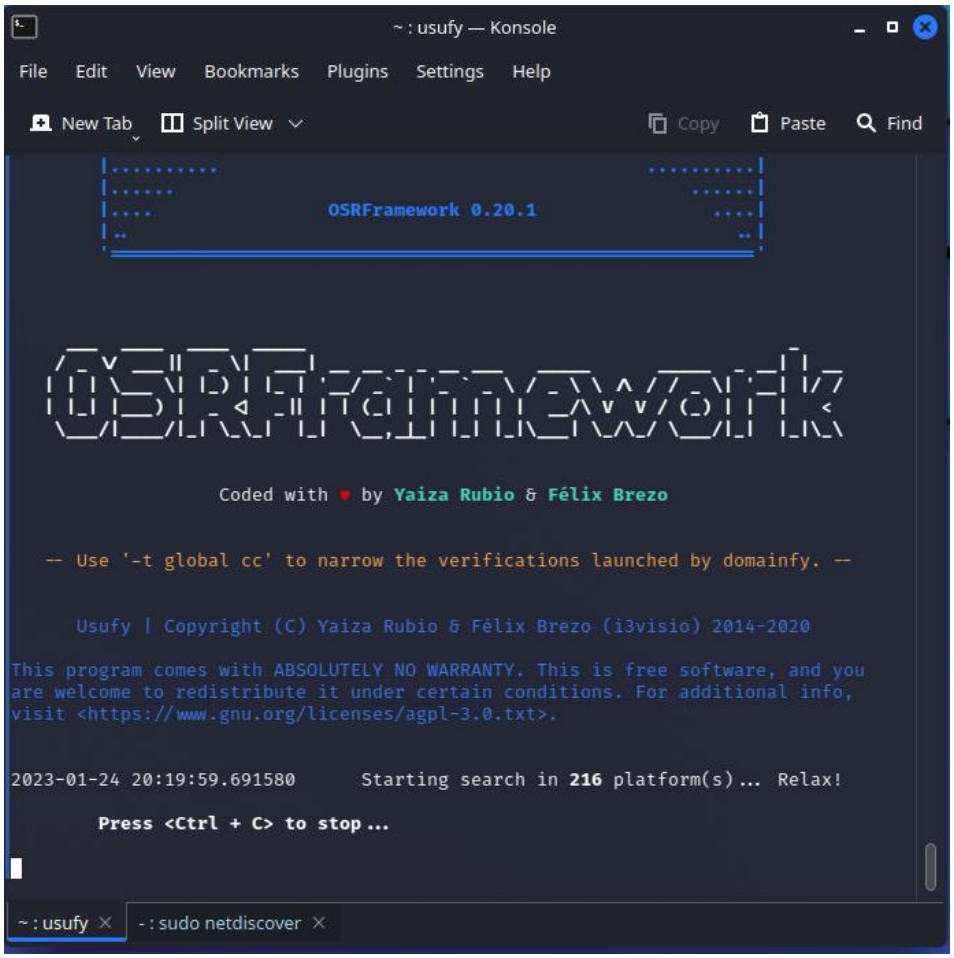


Installing Maltego

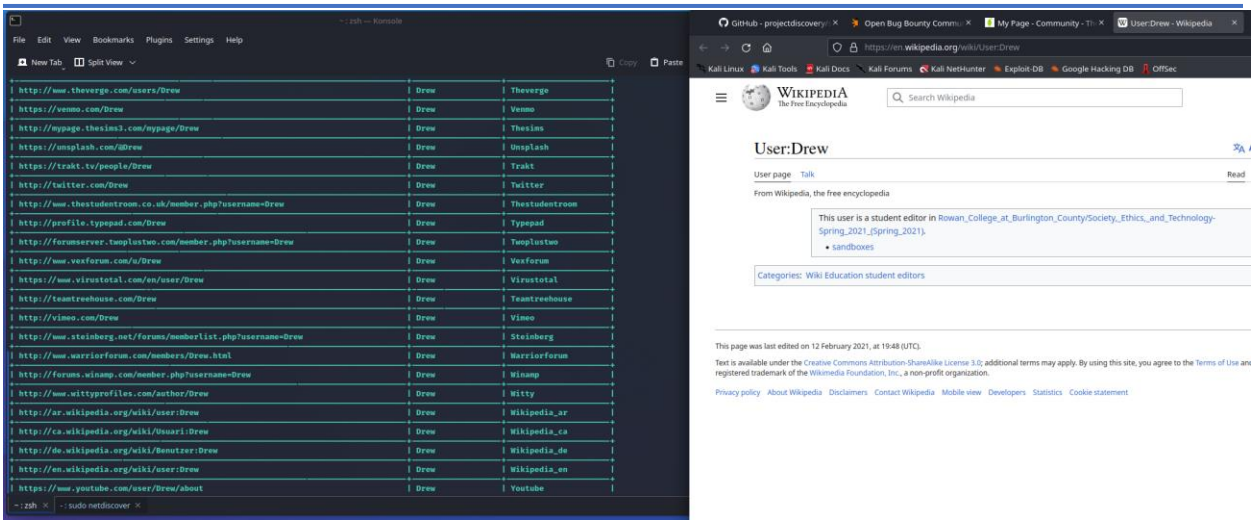


Successful install and registration of Maltego.

OSRFramework



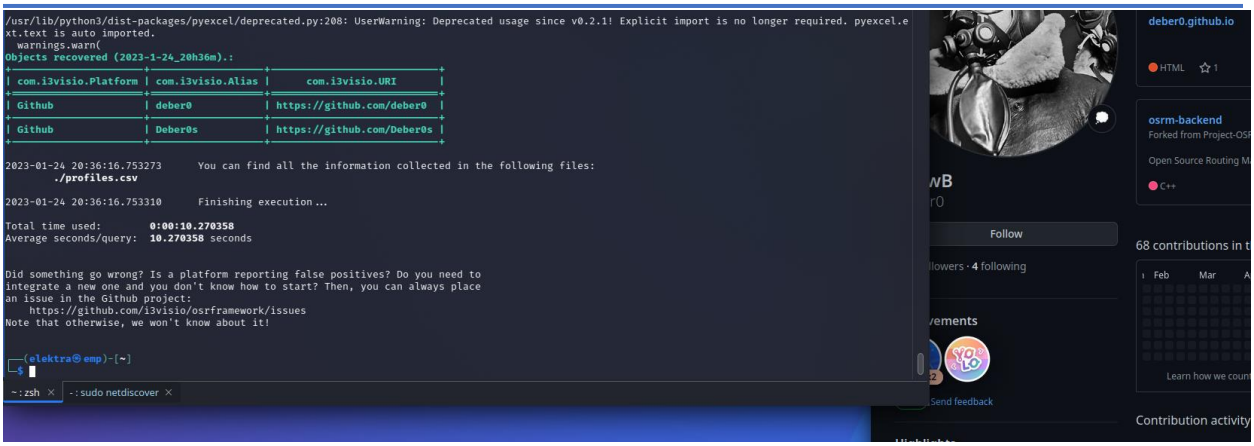
Sending `usufy -n cyberhia,` prompted me to install OSRFramework as that is not a tool that came default with Kali. After install, the following pictures show a brief overview of the tools



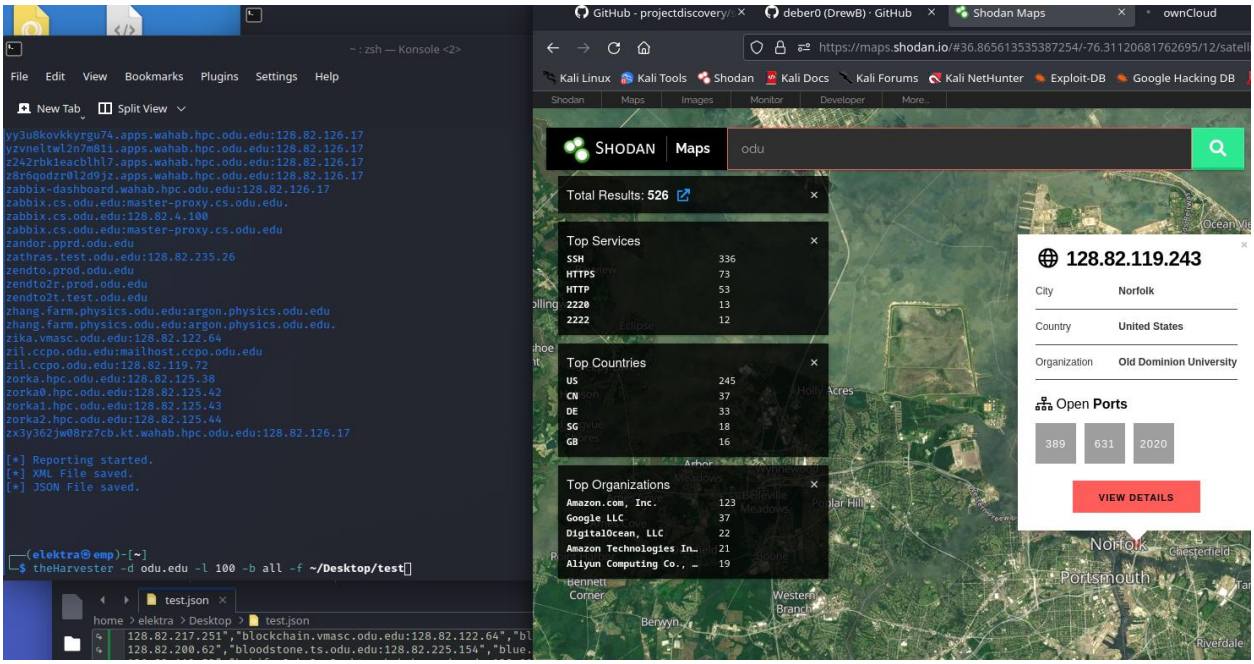
http://www.theverge.com/users/Drew	Drew	Theverge
https://venmo.com/Drew	Drew	Venmo
http://mypage.thesims3.com/mypage/Drew	Drew	Thesims
https://unsplash.com/@Drew	Drew	Unsplash
https://trakt.tv/people/Drew	Drew	Trakt
http://twitter.com/Drew	Drew	Twitter
http://www.thestudentroom.co.uk/member.php?username=Drew	Drew	Thestudentroom
http://profile.typepad.com/Drew	Drew	Typepad
http://forumserver.twoplustwo.com/member.php?username=Drew	Drew	Twoplustwo
http://www.vexforum.com/u/Drew	Drew	Vexforum
https://www.virustotal.com/en/user/Drew	Drew	Virustotal
http://teamtreehouse.com/Drew	Drew	Teamtreehouse
http://vimeo.com/Drew	Drew	Vimeo
http://www.steinberg.net/forums/memberlist.php?username=Drew	Drew	Steinberg
http://www.warriorforum.com/members/Drew.html	Drew	Warriorforum
http://forums.winamp.com/member.php?username=Drew	Drew	Winamp
http://www.wittyprofiles.com/author/Drew	Drew	Witty
http://ar.wikipedia.org/wiki/user:Drew	Drew	Wikipedia_ar
http://ca.wikipedia.org/wiki/Usuari:Drew	Drew	Wikipedia_ca
http://de.wikipedia.org/wiki/Benutzer:Drew	Drew	Wikipedia_de
http://en.wikipedia.org/wiki/user:Drew	Drew	Wikipedia_en
https://www.youtube.com/user/Drew/about	Drew	Youtube

http://www.spoj.com/users/Brown	Brown	Spoj
http://www.v7n.com/forums/members/Brown.html	Brown	V7n
https://tippin.me/@Brown	Brown	tippin_me
https://trakt.tv/people/Brown	Brown	Trakt
http://teamtreehouse.com/Brown	Brown	Teamtreehouse
http://mypage.thesims3.com/mypage/Brown	Brown	Thesims
https://venmo.com/Brown	Brown	Venmo
https://unsplash.com/@Brown	Brown	Unsplash
http://www.thestudentroom.co.uk/member.php?username=Brown	Brown	Thestudentroom
http://profile.typepad.com/Brown	Brown	Typepad
http://forumserver.twoplustwo.com/member.php?username=Brown	Brown	Twoplustwo
https://www.virustotal.com/en/user/Brown	Brown	Virustotal
http://vimeo.com/Brown	Brown	Vimeo
https://vk.com/Brown	Brown	Vk
http://www.warriorforum.com/members/Brown.html	Brown	Warriorforum
http://twitter.com/Brown	Brown	Twitter
http://ar.wikipedia.org/wiki/user:Brown	Brown	Wikipedia_ar
http://www.steinberg.net/forums/memberlist.php?username=Brown	Brown	Steinberg
http://ca.wikipedia.org/wiki/Usuari:Brown	Brown	Wikipedia_ca
http://forums.winamp.com/member.php?username=Brown	Brown	Winamp
http://www.wittyprofiles.com/author/Brown	Brown	Witty
https://www.youtube.com/user/Brown/about	Brown	Youtube

`usufy -n Drew Brown` returns searches for the results of username ‘Drew’ and ‘Brown’ various websites had both names attributed to accounts. None of which were mine.

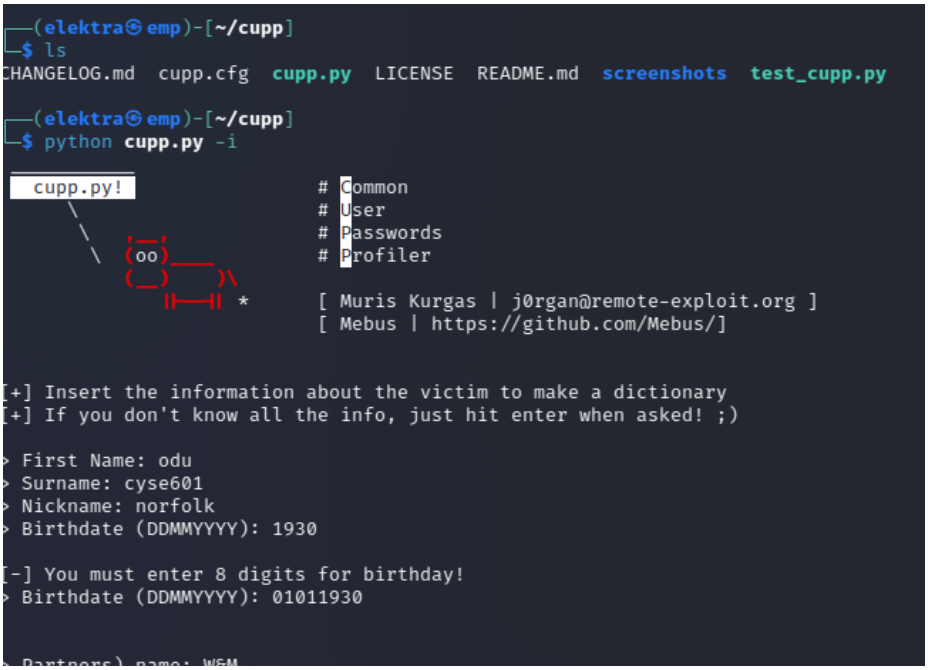


With searchfy, `searchfy -q "deber0"`, my github repo was found.

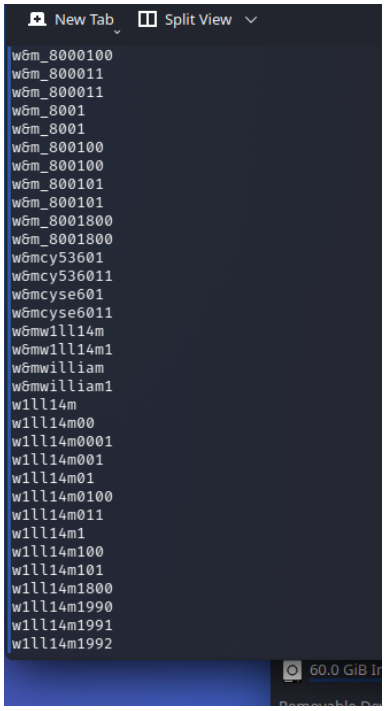


The Harvester tool is installed by default. Ran `theHarvester -d odu.edu -l 100 -b all -f ~/Desktop/test`. Also ran a shodan search for odu and found an LDAP server.

Installing Cupp – Wordlist generator

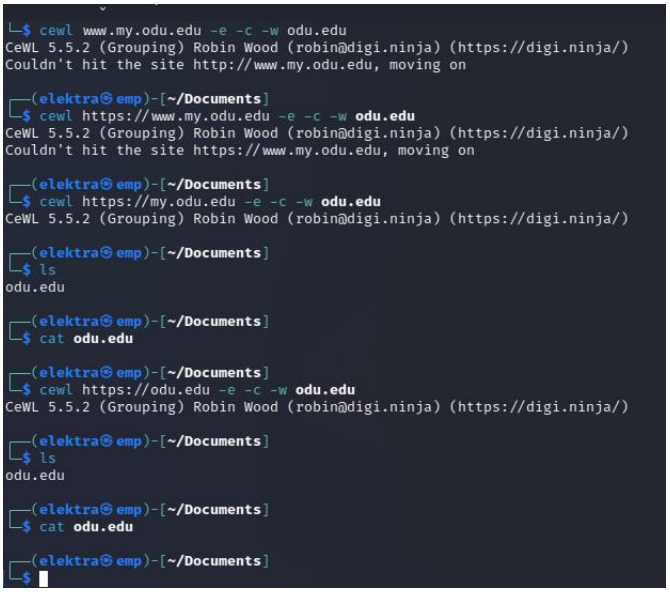


Installing cupp wordlist tool and generating an odu.txt wordlist based on various artifacts of data.

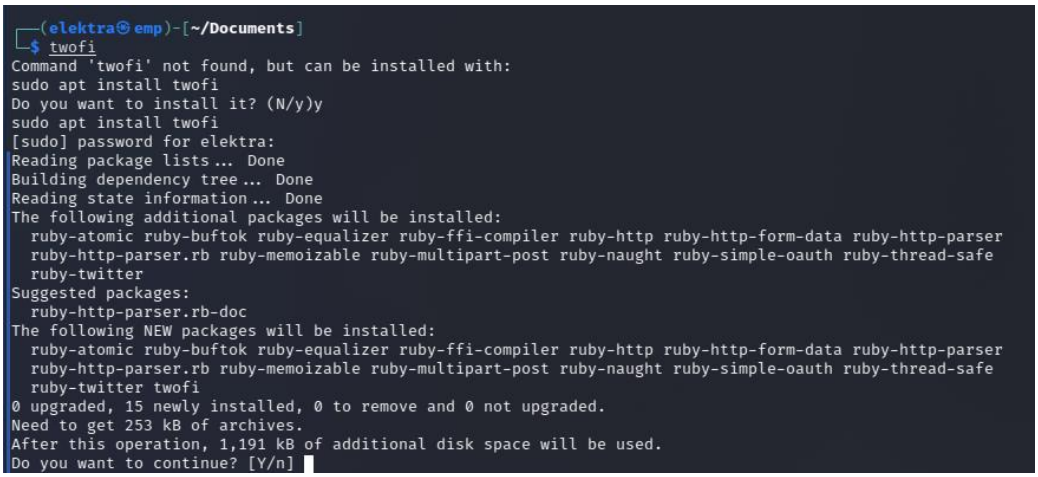


The cupp wordlist creation tool is quite nifty.

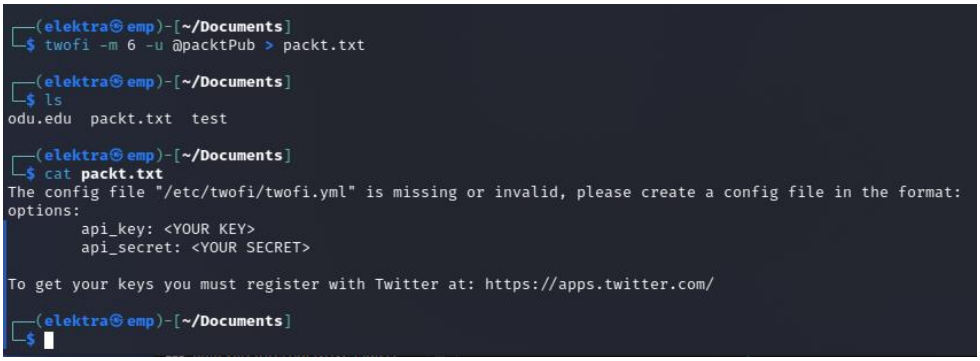
Installing CeWL and twofi



Using CeWL to scrape https://my.odu.edu to generate a wordlist. It was not successful however.



Install twofi to prepare for Twitter engagement. Regarding API keys for interaction with twitter, there seems to be some kind of issue with registration.

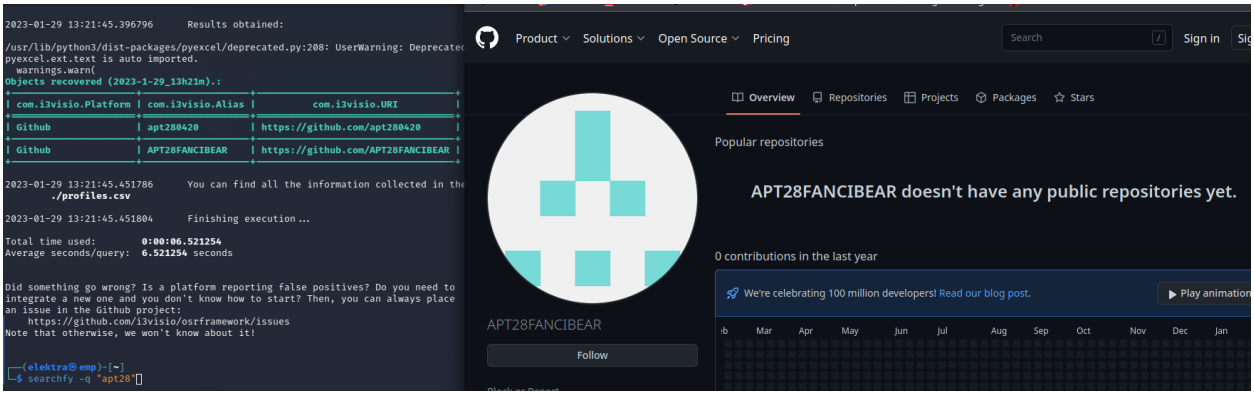


Fancy Bear Passive Recon OSINT

Fancy bear is a state actor Russian-backed advanced persistent threat cyber espionage group. Various organizations refer to this group as different names: APT28 by Mandiant, Pawn Storm, Sofacy Group by Kaspersky, Sednit, Tsar Team by FireEye, Strontium by Microsoft. Security firms and and the United States Special Counsel have identified Fancy bear to be sponsored by the Russian government. Additionally, the United States have identified the group as GRU Unit 26165.

GRU is a soviet era Russian Intelligence unit which is still used as a common reference to the now Main Directorate of the General Staff of the Armed Forces of the Russian Federation previously known as Main Intelligence Directorate.

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



Running `searchfy -q "apt28"` returns interesting private repo GitHub results which could easily be an innocuous user but could just as easily be the group of interest hiding in plainsight.

Fancy Bear Current Affairs

The Russian-Ukraine war seems to be the main focus of Fancy Bear efforts. Fancy Bear is known to commonly target government, military, and security organizations. It is believed that APT28 is the group responsible for the 2016 United States presidential election meddling. They are also believed to be responsible for the cyber attacks on German Parliament, Norweigian Parliament, the White House, NATO, the Democratic National Committee, Organization for Security Co-operation in Europe and the election campaign of French presidential candidate Emmanuel Macron.

https://killingthebear.jorgetesta.tech/campaigns/russia-ukraine-war

APT28 Tools

X-Tunnel

X-Tunnel is a network tunneling tool for network traversal and pivoting. This creates a secured SSL tunnel to APT28 controlled command and control servers. This enables the threat actor to use a variety of standard networking tools and protocols to connect to victim internal services.

Indicators of Compromise (IoCs) for X-Tunnel

The subsequent table below are a list of IP addresses and domains associated with X-Tunnel communications.

IP Address	Domain
23.163.0.59	Picturecrawling.com
86.105.1.123	
185.86.149.218	
185.145.182.80	
89.37.226.106	
94.177.12.238	

Hashes

The following table are MD5 hashes of X-Tunnel files which have been intercepted. The file hashings have been collected and logged to properly identify malware file signatures that relate to X-Tunnel infections.

Filename	Hash
Gpu.dll	8dbe37dfb0d498f96fb7f1e09e9e5c8f
Incstnt.exe	5086989639aed17227b8d6b041ef3163

X-Agent

This tool is also known as CHOPSTICK. This is a second stage modular remote access trojan (RAT). It is capable of running on most devices: Windows, iOS, and Unix-based operating systems. X-Agent is deployed against victims of APT28 by using key logging and file extraction techniques. Second-stage malware is used as a follow on means of establishing system persistence to monitor victim organizations. This mean this specific piece has first stage infections such as CORESHELL and GAMEFISH. This malware is used in conjunction with X-Tunnel to securely funnel gathered X-Agent data. It is also used in conjunction with CompuTrace/Lojack. It is stated X-Agent uses SSL/TLS encryption channel which I believe is a result of X-Tunnel.

Indicators of Compromise (IoCs) for X-Agent

The following IP addresses and domain names have been found to be used with X-Agent Command and Control Servers to monitor and effect victim organization operations.

IP Address	Domain
139.5.177.205	malaytravelgroup.com
80.255.6.15	worldimagebucket.com
89.34.111.107	fundseats.com
86.106.131.229	globaltechengineers.org
139.5.177.206	
185.181.102.203	beststreammusic.com
185.181.102.204	thepiratecinemaclub.org
169.239.129.31	coindmarket.com
213.252.247.112	creekcounty.net
185.86.148.15	
89.45.67.110	virtsvc.com
185.86.150.205	
193.37.255.10	moderntips.org
195.12.50.171	daysheduler.org
51.38.128.110	escochart.com
185.144.83.124	loungecinemaclub.com
185.216.35.10	genericnetworkaddress.com
185.94.192.122	bulgariatripholidays.com
185.216.35.7	georgia-travel.org
103.253.41.124	bbcweather.org
185.189.112.195	politicweekend.com
185.230.124.246	truefashionnews.com
87.120.254.106	protonhardstorage.com
77.81.98.122	moldtravelgroup.com
89.34.111.132	iboxmit.com
46.21.147.55	brownvelocity.org
103.208.86.57	pointtk.com
185.128.24.104	narrowpass.net
145.239.67.8	powernoderesources.com
185.210.219.250	
86.105.9.174	topcinemaclub.com
89.34.111.107	fundseats.com

Hashes

The following table are SHA-1 hashes of X-Agent files which have been collected by security agencies. The file hashings have been collected and logged to properly identify malware file signatures that relate to X-Agent infections.

Notice the common email communication tool msoutlook and outlook to be spoofed by the threat actors to pose as an innocuous background process. T

Filename	Hash
chost.exe	46e2957e699fae6de1a212dd98ba4e2bb969497d
msoutlook.dll	c53930772beb2779d932655d6c3de5548810af3d
Samp_(16).file	fa695e88c87843ca0ba9fc04b176899ff90e9ac5
outlook.dll	046a8adc2ef0f68107e96babc59f41b6f0a57803

CompuTrace/Lojack

This is a unique tool in that the CompuTrace/Lojack is a legitimate piece of software. This is a highly commercialized asset tracking tool that was advertised across the 90's and early 00's. In the event of a lost or stolen laptop device, the software can remotely connect to the device and destroy the device or completely lock the thief from using the device. APT28 has stolen and modified the source code to establish persistence on victim's machine operations.

Indicators of Compromise (IoCs) for CompuTrace/Lojack

The following IP addresses have been connected and attributed to a Command and Control server associated with APT28 and the CompuTrace/Lojack malware tool.

IP Addresses
185.86.151.2
46.21.147.76
46.21.147.71
162.208.10.66
185.86.151.104
185.86.149.116
86.106.131.54
185.181.102.201
179.43.158.20
85.204.124.77
185.86.148.184
185.183.107.40
185.94.191.65
94.177.12.150
54.37.104.106
93.113.131.103
169.239.129.121
169.239.128.133

Hashes

The following file and accompanying SHA-1 hash is attributed to file signature related to a CompuTrace/Lojack file.

Filename	Hash
dcbfd12321fa7c4fa9a72486ced578fdc00dcee79e6d95aa481791f044a55.dll	d70db6a6d660aae58ccfc688a2890391fd873bfb

Concluding Notes

Each of the above tools are used to penetrate target networks and follow-on efforts are used to establish and maintain persistence. The tools are used to hook into systems drivers to access local accounts and the Lightweight Directory Access Protocol (LDAP) which is a directory service protocol used to run directly over the TCP/IP stack via ports TCP and UDP ports 389 whereas LDAPS (over SSL) uses port 636. LDAP is a directory interface employed by businesses to maintain IT infrastructure for email and user account authorizations. The LDAP service tree are critical interfaces for client-server authentication interactions. Use case industry examples include: Docker, Kubernetes, Jenkins, Linux Samba servers, OpenVPN.

All the above tool overviews have deeper details in the National Cyber Security Centre's APT28 Advisory which outline Snort rules that can be used to detect all the included tools within the advisory.

Sources

National Cyber Security Centre – Indicators of Compromise for Malware used by APT28

https://www.waterisac.org/system/files/articles/NCSC_APT28_Advisory.pdf

X-Tunnel - Mitre

https://attack.mitre.org/software/S0117/

X-Agent for Android – Mitre

https://attack.mitre.org/software/S0314/

X-AgentOSX

https://attack.mitre.org/software/S0161/

Explanation of LDAP server

https://thecyphere.com/blog/what-is-ldap-server/

Various Advanced Persistent Threat Actors Compilation – Killing the Bear

https://killingthebear.jorgetesta.tech/