Threat Profiling: Leveraging Threat Intelligence to Enhance Cyber Defense

Tina Ellis[1], Emma Lancaster[2], Dave Stone[3]

[1] Columbia Basin College, Pasco, WA 99301
[2] Pacific Northwest National Laboratory, Richland, WA 99354
[3] Pacific Northwest National Laboratory, Richland, WA 99354

Abstract

Advanced Persistent Threats (APTs) are highly skilled adversaries, typically nation-state sponsored, that will stop at nothing to carry out their objectives. As Pacific Northwest National Laboratory (PNNL) explores its mission to transform the world through discovery and innovation, it becomes a target for adversary groups, like APTs, who want nothing more than to undermine this global mission. The characteristics of threat groups vary depending on their tactics, techniques, and procedures (TTPs), and their overarching goals. MITRE ATT&CK® is a globally accessible resource that keeps an in-depth knowledge base of cyber threat intelligence, which includes malicious behaviors threat groups and APTs have used at various stages of real-world cyberattacks [1]. The purpose of this project is to demonstrate how publicly available information (PAI) and cyber threat intelligence (CTI) can be analyzed to identify the top threat groups most likely to target PNNL systems. Using PAI, I developed a threat profile on PNNL with classifications of the threat groups who pose the greatest risk. I worked with my team to aggregate the CTI and found the top 5 threat groups who pose the greatest threat to PNNL. Mapping the TTPs observed by these threat groups to other sources of CTI, I identified the TTPs, software, and living off the land binaries (LOLbins) used by these adversaries. The results of this project reveal a common pool of TTPs, software, and LOLbins that all 5 threat groups use. Future work is needed to determine whether PNNL systems are vulnerable to the attacks revealed in this analysis. The structural principles uncovered in this report reveal the opportunity for organizations, such as PNNL, to realize how threat intelligence can be used to strengthen security guidelines and their overall security posture.

Introduction

As Pacific Northwest National Laboratory (PNNL) explores its mission to transform the world through discovery and innovation, it becomes a target for adversary groups who want nothing more than to undermine this global mission. Advancements made in technology and science provide the ideal bait for adversary groups who seek to infiltrate, steal, corrupt, and even disrupt the critical research being done here. Recent cyber-attacks directed at the U.S. government and energy sectors (e.g., SolarWinds [5], the Colonial Pipeline [6]), illustrate the need to name and understand the adversaries behind these cyber-enabled operations. The purpose of this project is to demonstrate how publicly available information (PAI) and cyber threat intelligence (CTI) guide us to a deeper understanding of the threat groups most likely to target PNNL systems, and how this information can be used to improve cyber awareness and defense.

The first phase of this project consists of data collection. Three sets of data were collected:

- PAI on PNNL: public facing information revealed that it is well known that PNNL is a government funded research laboratory. The classification of adversaries most likely to target PNNL systems include those known for espionage, actors acting on behalf of their government, or financially motivated.
- Threat group intelligence: data collected from the MITRE ATT&CK® knowledge base, focused on only espionage minded threats who target U.S. government, energy, or research laboratories.
- Government press releases: advisories from the White House, and the Cybersecurity & Infrastructure Security Agency (CISA), supplied up to date knowledge of threat group activity and overall risk status [2].

Phase two of the project consisted of data analysis, aggregation, and classification. Data analysis of over 60 cyber threat groups resulted in the classification of 5 high risk threat groups. Data aggregation of TTPs, and software, led to the classification of the top TTPs and software used by these threat groups. The resulting data classifications also revealed new goals to find and map the living off the land binaries (LOLbins) used by our top 5 threat groups. The results of this project reveal a common pool of TTPs, software, and LOLbins that all 5 threat groups utilize. Future work is needed to determine whether PNNL systems are vulnerable to the attacks revealed in this analysis.

Future work may include mapping technologies used at PNNL with the findings included in this analysis, analysis of the LOLBins techniques gathered for better understanding of how these tools can be abused, and the best way to mitigate the threats presented from these types of attacks.

Progress

Phase 1 Data Collection

PAI on PNNL
I developed a profile on PNNL using Publicly Available Information (PAI) from sources such as

affiliated websites, job descriptions, and social media profiles. PNNL’s online footprint helped me to understand how an adversary would see this organization. As a government funded research laboratory, I realized that adversaries would typically include those known for espionage. Espionage minded adversaries typically include threat groups acting on behalf of their government, or threat groups financially motivated to infiltrate, steal, and sell proprietary information.

Threat Groups

The MITRE ATT&CK® framework is a globally accessible resource that keeps an in-depth knowledge base of malicious behaviors threat groups have used at various stages of real-world cyberattacks [1]. I used this knowledgebase to collect cyber threat intelligence (CTI) on 63 different threat groups who focus on espionage attacks against U.S. government facilities, energy sector, think tanks, and/or research laboratories.

Press Releases

I collected data from recent U.S. press releases, alerts, and reports. More specifically, data published by the White House, and the Cybersecurity & Infrastructure Security Agency (CISA) supplied insight of current political conditions, recent threat group activity, and overall risk statuses of top priority threat groups [2].

Phase 2 Data Analysis, Aggregation, and Classification

Top 5 Threat Groups

The classification process began with mapping the CTI collected from the MITRE ATT&CK® knowledge base, with the data gathered from U.S. press releases, alerts, and reports. I assigned each threat group with a risk score within three respective categories:

a. known to target U.S. government facilities, energy sectors, think tanks, or research laboratories
b. had recent CISA alerts and High-Risk statuses
c. thought to be currently active

In April of 2022, CISA issued an alert on Russian State-Sponsored and Criminal Cyber Threats to Critical Infrastructure, naming Dragonfly, APT29, Turla, and APT28 as High Alert threat groups, [2]. Among the 63 espionage focused threat groups I analyzed, these 4 stood out as posing the greatest risk to PNNL. Ultimately, a total of 5 high alert threat groups were selected for this study:

1. **Dragonfly** is a Russian Federal Security Service (FSB) affiliated threat group. Common names for Dragonfly include Crouching Yeti, Berserk Bear, and Energetic Bear. They cast a wide net and appear to be in active reconnaissance mode, gathering sensitive data wherever possible. They have targeted State, Local, Tribal, and Territorial (SLTT) government networks in the United States, infiltrated American electric infrastructure, and is suspectedly behind, or affiliated with, the SolarWinds attack that resulted in a massive data breach in both private and public sectors.

2. **APT29** aka Cozy Bear, is an Advanced Persistent Threat group with ties to the Russian Foreign Intelligence Service (SVR). Recent activity from this group proves that they are still actively targeting United States networks. APT29 makes the top five list because of their focus on United States research institutions, government facilities, and think tanks.
3. **Turla** aka Venomous Bear, is known by several different names including Belugasturgeon, Group 88, Iron Hunter, Krypton, Moonlight Maze, Snake, Waterbug, and WhiteBear. I included this Russian aligned cyber threat group in our top five, because their focus on government facilities and research organizations.
4. **APT28** aka Fancy Bear, has been given many names including: Group 74, Iron Twilight, PawnStorm, Sednit, Snakemackerel, Sofacy, Strontium, Swallowtail, TG-4127, Threat Group-4127, Tsar Team, Electrum, Iron Viking, Quedagh, the Sandworm Team, Telebots, and Voodoo Bear. APT28 is affiliated with Russia's GRU Main Special Service Center (GTsSS), and is believed to be, or affiliated with, the Sandworm Team, who is responsible for the 2015 and 2016 Ukrainian electrical sector and the 2017 NotPetya attacks. APT28 is included in our top 5 for their espionage centered attacks on government organizations, research institutions, a United States nuclear facility, and critical infrastructure-related organizations related to the energy sector.
5. **Operation Wocao** aka APT20, makes the top five list because of their focus on government facilities, energy, and technology sectors. Not a lot is known about this hidden threat group, but a recent Fox-It report suggests that this adversary has been working with the Chinese government to target western networks [3].

Tactics, Techniques, and Procedures

One way to analyze the characteristics of a threat group is by examining their tactics, techniques, and procedures. Using the CTI gathered from the MITRE ATT&CK® knowledge base, I consolidated the TTPs used by the top 5 threat groups into an Excel spreadsheet. I worked with my team to import this data into Splunk then queried that data to identify TTP IDs being leveraged most by the top 5 threat groups (Table 1). See ***(Figure 1)*** for a full list of TTPs.

ID	MITRE Technique Name	Actor
T1021	Remote Services	APT28, APT29, Dragonfly, Operation Wocao, Turla
T1087	Account Discovery, Cloud Account, Domain Account	APT29, Dragonfly, Operation Wocao, Turla
T1110	Brute Force, Password Cracking, Password Guessing, Password Spraying	APT28, APT29, Dragonfly, Turla
T1547	Boot or Logon Autostart Execution	APT28, APT29, Dragonfly, Turla
T1566	Phishing	APT28, APT29, Dragonfly, Turla

Table 1. Threat Actor Techniques

Software

Using the CTI gathered from the MITRE ATT&CK® knowledge base, I consolidated the software used by top 5 threat groups into an Excel spreadsheet. Utilizing the same process demonstrated in Table 1, I worked with my team to import the data into Splunk and ran a query that prioritized which software programs are used the most among the top 5 threat groups (Table 2). See ***(Figure 2)*** for the full software list associated with the primary threat groups.

ID	Software Name	Actor
S0002	Mimikatz	APT28, APT29, Dragonfly, Operation Wocao, Turla
S0039	Net	APT28, APT29, Dragonfly, Turla
S0029	PsExec	APT29, Dragonfly, Turla
S0057	Tasklist	APT29, Turla
S0075	Reg	Dragonfly, Turla
S0096	Systeminfo	APT29, Turla

Table 2. Threat Actor Software

Living Off the Land Binaries

Once the top TTPs and Software were identified, our team realized a new objective. We hypothesized that we could map the top TTP data collection to the corresponding Living Off the Land Binaries (LOLBins) a threat group may use during an attack. LOLBins are the native system binaries and preinstalled tools that come with an Operating System. Threat actors have found ways to use these non-malicious binaries to bypass detection and perform malicious activities. Living Off the Land Binaries and Scripts (LOLBAS) is a knowledge base project that works to document the binary, scripts, and libraries that can be used for Living Off the Land attacks [4]. Using the LOLBAS knowledge base, I mapped and documented the LOLBins associated with the top TTPs (Table 3).

ID	Binary	Type	Function
T1003	adplus.exe	OtherMSBinaries	Dump
T1003	Comsvcs.dll	Libraries	Dump
T1003	Diskshadow.exe	Binaries	Dump, Execute
T1003	Dump64.exe	OtherMSBinaries	Dump
T1003	Esentutl.exe	Binaries	Copy, Alternate data streams, Download
T1003	ntdsutil.exe	OtherMSBinaries	Dump
T1003	rdrleakdiag.exe	Binaries	Dump
T1003	Reg.exe	Binaries	Alternate data streams, Credentials
T1003	Rpcping.exe	Binaries	Credentials
T1003	Sqldumper.exe	OtherMSBinaries	Dump
T1003	Tttracer.exe	Binaries	Dump, Execute
T1021	n/a		
T1027	Certutil.exe	Binaries	Download, Alternate data streams, Encode, Decode
T1059	Cmd.exe	Binaries	Alternate data streams
T1059	Fsi.exe	OtherMSBinaries	AWL bypass

T1059	FsiAnyCpu.exe	OtherMSBinaries	AWL bypass
T1070	Update.exe	OtherMSBinaries	Download, AWL bypass, Execute
T1078	Cmdkey.exe	Binaries	Credentials
T1087	n/a		
T1090	n/a		

Table 3. Living Off the Land Binaries

Future Work

More work is needed to decide if the data collected in this process is beneficial to PNNL's security posture. Future work may include:

- Data mapping the technologies used at PNNL with the data findings included in this analysis
- Analysis of the LOLBin techniques gathered for better understanding of how these tools can be abused
- Developing detections for and mitigations against the threats presented from these types of attacks

Impact on Laboratory or National Missions

This project contributes to PNNL's mission by helping to protect the confidentiality, integrity, and availability (CIA) of the research conducted at this lab. By identifying the top actors most likely to target PNNL, and promoting cyber awareness, we can detour threats that could have a national impact.

This project was supported and funded in part by the U.S. Department of Energy, Office of Science, Office of Workforce Development for Teachers and Scientists (WDTS) under the Community College Internships Program (CCI).

Conclusions

By mapping and analyzing cyber threat intelligence, I found the top five threat groups most likely to target PNNL. Comparing the Software and TTPs used by these threat groups revealed the most common tools and techniques deployed by these adversaries. Further analysis of these techniques revealed the binaries these threat groups exploit for malicious purposes. While more work is needed to determine the impact of these findings on PNNL's security posture, the purpose of this project was realized in the successful demonstration of how publicly available information and cyber threat intelligence can be used to improve awareness of the threat groups most likely to target PNNL data.

References

1. MITRE ATT&CK®, "Groups." Groups | MITRE ATT&CK®, n.d.. https://attack.mitre.org/groups/.
2. "Alert (AA22-110A) Russian State-Sponsored and Criminal Cyber Threats to Critical Infrastructure." *CISA*, April 2022. https://www.cisa.gov/uscert/ncas/alerts/aa22-110a.
3. Dantzig, Maarten van, and Erik Schamper. "Operation Wocao Shining a Light on One of China's Hidden Hacking Groups." Fox, December 19, 2019. https://www.fox-it.com/media/kadlze5c/201912_report_operation_wocao.pdf
4. LOLBAS, l. LOLBAS, n.d.. https://lolbas-project.github.io/.
5. The White House, "Fact Sheet: Imposing Costs for Harmful Foreign Activities by the Russian Government." The White House. The United States Government, April 15, 2021. https://www.whitehouse.gov/briefing-room/statements-releases/2021/04/15/fact-sheet-imposing-costs-for-harmful-foreign-activities-by-the-russian-government/.
6. Jones, David. "How the Colonial Pipeline Attack Instilled Urgency in Cybersecurity." Cybersecurity Dive, May 17, 2022. https://www.cybersecuritydive.com/news/post-colonial-pipeline-attack/623859/.

Acknowledgements

I would like to thank the Cyber Security Operations Center (CSOC) team for helping me learn and grow in my knowledge of cyber defense. I would also like to thank my mentor, Emma Lancaster, for all her advice and guidance throughout this project and my time here at PNNL, and Dave Stone for his insight and leadership over this project.

Participants

Name	Role
Tina Ellis (CCI Intern)	Project lead. Collected and analyzed data. Project report and paper author.
Emma Lancaster (PNNL Mentor)	Helped guide the report and paper. Answered my questions about cyber threat intelligence sources, data collection and analysis techniques. Troubleshoot challenges, and reviewed project report paper.
Dave Stone (PNNL)	High level leadership. Presented the project idea, objectives, and goals. Helped with Splunk data aggregation.

Appendix

Figure 1

Full list of Techniques, Tactics, and Procedures used by our top 5 threat groups, Table 1.

ID	Name	Actor	Count
T1059	Command and Scripting Interpreter, PowerShell, Python, Windows Command Shell	APT28, APT29, Dragonfly, Operation Wocao, Turla	19
T1078	Cloud Accounts, Domain Accounts, Local Accounts, Valid Accounts	APT28, APT29, Dragonfly, Operation Wocao, Turla	11
T1070	File Deletion, Indicator Removal on Host, Timestomp	APT28, APT29, Dragonfly, Operation Wocao	10
T1090	Internal Proxy, Multi-hop Proxy, Proxy	APT28, APT29, Operation Wocao, Turla	10
T1003	LSASS Memory, NTDS, OS Credential Dumping	APT28, APT29, Dragonfly, Operation Wocao	9
T1027	Binary Padding, HTML Smuggling, Indicator Removal from Tools, Obfuscated Files or Information, Software Packing	APT28, APT29, Operation Wocao, Turla	9
T1021	Remote Services	APT28, APT29, Dragonfly, Operation Wocao, Turla	7
T1087	Account Discovery, Cloud Account, Domain Account	APT29, Dragonfly, Operation Wocao, Turla	7
T1110	Brute Force, Password Cracking, Password Guessing, Password Spraying	APT28, APT29, Dragonfly, Turla	7
T1547	Boot or Logon Autostart Execution	APT28, APT29, Dragonfly, Turla	7
T1566	Phishing	APT28, APT29, Dragonfly, Turla	7
T1583	Acquire Infrastructure	APT28, APT29, Dragonfly, Turla	7
T1036	Masquerade Task or Service, Masquerading, Match Legitimate Name or Location	APT28, APT29, Dragonfly	6
T1069	Domain Groups, Permission Groups Discovery	APT29, Dragonfly, Operation Wocao, Turla	6
T1071	Application Layer Protocol	APT28, APT29, Dragonfly, Turla	6
T1098	Account Manipulation	APT28, APT29, Dragonfly	6
T1204	User Execution	APT28, APT29, Dragonfly, Turla	6
T1550	Application Access Token, Pass the Ticket, Use Alternate Authentication Material, Web Session Cookie	APT28, APT29	6
T1560	Archive Collected Data, Archive via Utility	APT28, APT29, Dragonfly, Operation Wocao, Turla	6
T1562	Impair Defenses	APT29, Dragonfly, Operation Wocao, Turla	6

T1005	Data from Local System	APT28, APT29, Dragonfly, Operation Wocao, Turla	5
T1016	Internet Connection Discovery, System Network Configuration Discovery	APT29, Dragonfly, Operation Wocao, Turla	5
T1074	Data Staged	APT28, APT29, Dragonfly, Operation Wocao	5
T1083	File and Directory Discovery	APT28, APT29, Dragonfly, Operation Wocao, Turla	5
T1105	Ingress Tool Transfer	APT28, APT29, Dragonfly, Operation Wocao, Turla	5
T1213	Code Repositories, Data from Information Repositories, Sharepoint	APT28, APT29, Turla	5
T1546	Event Triggered Execution	APT28, APT29, Turla	5
T1584	Compromise Infrastructure	APT29, Dragonfly, Turla	5
T1588	Obtain Capabilities	APT28, APT29, Dragonfly, Turla	5
T1018	Remote System Discovery	APT29, Dragonfly, Operation Wocao, Turla	4
T1057	Process Discovery	APT28, APT29, Operation Wocao, Turla	4
T1102	Bidirectional Communication, Web Service	APT28, APT29, Turla	4
T1133	External Remote Services	APT28, APT29, Dragonfly, Operation Wocao	4
T1190	Exploit Public-Facing Application	APT28, APT29, Dragonfly, Operation Wocao	4
T1505	Server Software Component	APT28, APT29, Dragonfly, Operation Wocao	4
T1555	Credentials from Password Stores, Credentials from Web Browsers	APT29, Operation Wocao, Turla	4
T1598	Phishing for Information, Spearphishing Link	APT28, Dragonfly	4
T1001	Data Obfuscation	APT28, APT29, Operation Wocao	3
T1012	Query Registry	Dragonfly, Operation Wocao, Turla	3
T1053	Scheduled Task/Job	APT29, Dragonfly, Operation Wocao	3
T1055	Dynamic-link Library Injection, Process Injection	Operation Wocao, Turla	3
T1068	Exploitation for Privilege Escalation	APT28, APT29, Turla	3
T1082	System Information Discovery	APT29, Operation Wocao, Turla	3
T1112	Modify Registry	Dragonfly, Operation Wocao, Turla	3
T1114	Email Collection	APT28, APT29, Dragonfly	3
T1120	Peripheral Device Discovery	APT28, Operation Wocao, Turla	3
T1140	Deobfuscate/Decode Files or Information	APT28, APT29, Turla	3
T1189	Drive-by Compromise	APT28, Dragonfly, Turla	3
T1203	Exploitation for Client Execution	APT28, APT29, Dragonfly	3
T1218	System Binary Proxy Execution	APT28, APT29	3

T1518	Security Software Discovery, Software Discovery	Operation Wocao, Turla	3
T1553	Subvert Trust Controls	APT29, Turla	3
T1564	Hide Artifacts	APT28, Dragonfly	3
T1573	Encrypted Channel	APT28, APT29, Operation Wocao	3
T1587	Develop Capabilities	APT29, Turla	3
T1595	Active Scanning	APT28, APT29, Dragonfly	3
T1007	System Service Discovery	Operation Wocao, Turla	2
T1025	Data from Removable Media	APT28, Turla	2
T1033	System Owner/User Discovery	Dragonfly, Operation Wocao	2
T1047	Windows Management Instrumentation	APT29, Operation Wocao	2
T1048	Exfiltration Over Alternative Protocol	APT28, APT29	2
T1049	System Network Connections Discovery	Operation Wocao, Turla	2
T1056	Input Capture	APT28, Operation Wocao	2
T1095	Non-Application Layer Protocol	APT29, Operation Wocao	2
T1106	Native API	Operation Wocao, Turla	2
T1113	Screen Capture	APT28, Dragonfly	2
T1119	Automated Collection	APT28, Operation Wocao	2
T1124	System Time Discovery	Operation Wocao, Turla	2
T1134	Access Token Manipulation	APT28, Turla	2
T1135	Network Share Discovery	Dragonfly, Operation Wocao	2
T1136	Create Account	APT29, Dragonfly	2
T1195	Supply Chain Compromise	APT29, Dragonfly	2
T1199	Trusted Relationship	APT28, APT29	2
T1210	Exploitation of Remote Services	APT28, Dragonfly	2
T1221	Template Injection	APT28, Dragonfly	2
T1552	Unsecured Credentials	APT29, Operation Wocao	2
T1558	Steal or Forge Kerberos Tickets	APT29, Operation Wocao	2
T1567	Exfiltration Over Web Service	APT28, Turla	2
T1570	Lateral Tool Transfer	Operation Wocao, Turla	2
T1586	Compromise Accounts	APT28, APT29	2
T1589	Gather Victim Identity Information	APT28, APT29	2
T1606	Forge Web Credentials	APT29	2
T0817	Drive-by Compromise	Dragonfly	1
T0862	Supply Chain Compromise	Dragonfly	1

T1014	Rootkit	APT28	1
T1030	Data Transfer Size Limits	APT28	1
T1037	Boot or Logon Initialization Scripts	APT28	1
T1039	Data from Network Shared Drive	APT28	1
T1040	Network Sniffing	APT28	1
T1041	Exfiltration Over C2 Channel	Operation Wocao	1
T1046	Network Service Discovery	Operation Wocao	1
T1091	Replication Through Removable Media	APT28	1
T1092	Communication Through Removable Media	APT28	1
T1111	Multi-Factor Authentication Interception	Operation Wocao	1
T1115	Clipboard Data	Operation Wocao	1
T1137	Office Application Startup	APT28	1
T1187	Forced Authentication	Dragonfly	1
T1201	Password Policy Discovery	Turla	1
T1211	Exploitation for Defense Evasion	APT28	1
T1482	Domain Trust Discovery	APT29	1
T1484	Domain Policy Modification	APT29	1
T1498	Network Denial of Service	APT28	1
T1528	Steal Application Access Token	APT28	1
T1539	Steal Web Session Cookie	APT29	1
T1542	Pre-OS Boot	APT28	1
T1548	Abuse Elevation Control Mechanism	APT29	1
T1559	Inter-Process Communication	APT28	1
T1568	Dynamic Resolution	APT29	1
T1569	System Services	Operation Wocao	1
T1591	Gather Victim Org Information	Dragonfly	1
T1608	Stage Capabilities	Dragonfly	1
T1615	Group Policy Discovery	Turla	1
T1621	Multi-Factor Authentication Request Generation	APT29	1

Figure 2

Full list of Software used by the top 5 threat groups from Table 2.

ID	Software Name	Actor	Count
S0002	Mimikatz	APT28, APT29, Dragonfly, Operation Wocao, Turla	5
S0039	Net	APT28, APT29, Dragonfly, Turla	4
S0029	PsExec	APT29, Dragonfly, Turla	3
S0057	Tasklist	APT29, Turla	2
S0075	Reg	Dragonfly, Turla	2
S0096	Systeminfo	APT29, Turla	2
S0104	netstat	Operation Wocao, Turla	2
S0160	certutil	APT28, Turla	2
S0183	Tor	APT28, APT29	2
S0357	Impacket	Dragonfly, Operation Wocao	2
S0521	BloodHound	APT29, Operation Wocao	2
S0022	Uroburos	Turla	1
S0023	CHOPSTICK	APT28	1
S0037	HAMMERTOSS	APT29	1
S0044	JHUHUGIT	APT28	1
S0045	ADVSTORESHELL	APT28	1
S0046	CozyCar	APT29	1
S0048	PinchDuke	APT29	1
S0049	GeminiDuke	APT29	1
S0050	CosmicDuke	APT29	1
S0051	MiniDuke	APT29	1
S0052	OnionDuke	APT29	1
S0053	SeaDuke	APT29	1
S0054	CloudDuke	APT29	1
S0091	Epic	Turla	1
S0093	Backdoor.Oldrea	Dragonfly	1
S0094	Trojan.Karagany	Dragonfly	1
S0099	Arp	Turla	1
S0100	ipconfig	APT29	1
S0102	nbtstat	Turla	1
S0105	dsquery	Operation Wocao	1
S0108	netsh	Dragonfly	1

S0117	XTunnel	APT28	1
S0126	ComRAT	Turla	1
S0134	Downdelph	APT28	1
S0135	HIDEDRV	APT28	1
S0136	USBStealer	APT28	1
S0137	CORESHELL	APT28	1
S0138	OLDBAIT	APT28	1
S0139	PowerDuke	APT29	1
S0150	POSHSPY	APT29	1
S0154	Cobalt Strike	APT29	1
S0161	XAgentOSX	APT28	1
S0162	Komplex	APT28	1
S0168	Gazer	Turla	1
S0174	Responder	APT28	1
S0175	meek	APT29	1
S0191	Winexe	APT28	1
S0193	Forfiles	APT28	1
S0194	PowerSploit	Operation Wocao	1
S0195	SDelete	APT29	1
S0243	DealersChoice	APT28	1
S0250	Koadic	APT28	1
S0251	Zebrocy	APT28	1
S0256	Mosquito	Turla	1
S0265	Kazuar	Turla	1
S0314	X-Agent for Android	APT28	1
S0335	Carbon	Turla	1
S0351	Cannon	APT28	1
S0363	Empire	Turla	1
S0393	PowerStallion	Turla	1
S0395	LightNeuron	Turla	1
S0397	LoJax	APT28	1
S0410	Fysbis	APT28	1
S0488	CrackMapExec	Dragonfly	1
S0500	MCMD	Dragonfly	1
S0502	Drovorub	APT28	1
S0511	RegDuke	APT29	1

S0512	FatDuke	APT29	1
S0513	LiteDuke	APT29	1
S0514	WellMess	APT29	1
S0515	WellMail	APT29	1
S0516	SoreFang	APT29	1
S0518	PolyglotDuke	APT29	1
S0537	HyperStack	Turla	1
S0538	Crutch	Turla	1
S0552	AdFind	APT29	1
S0559	SUNBURST	APT29	1
S0560	TEARDROP	APT29	1
S0562	SUNSPOT	APT29	1
S0565	Raindrop	APT29	1
S0581	IronNetInjector	Turla	1
S0587	Penquin	Turla	1
S0588	GoldMax	APT29	1
S0589	Sibot	APT29	1
S0590	NBTscan	Turla	1
S0597	GoldFinder	APT29	1
S0633	Sliver	APT29	1
S0634	EnvyScout	APT29	1
S0635	BoomBox	APT29	1
S0636	VaporRage	APT29	1
S0637	NativeZone	APT29	1
S0645	Wevtutil	APT28	1
S0661	FoggyWeb	APT29	1
S0668	TinyTurla	Turla	1
S0677	AADInternals	APT29	1
S0682	TrailBlazer	APT29	1
S0684	ROADTools	APT29	1