
Look at this Graph

About Us

Scott

Likes: Frosted tips

Dislikes: Stone Sour, ATT&CK Technique T1486, long drives

Supriya

Likes: Nickelback

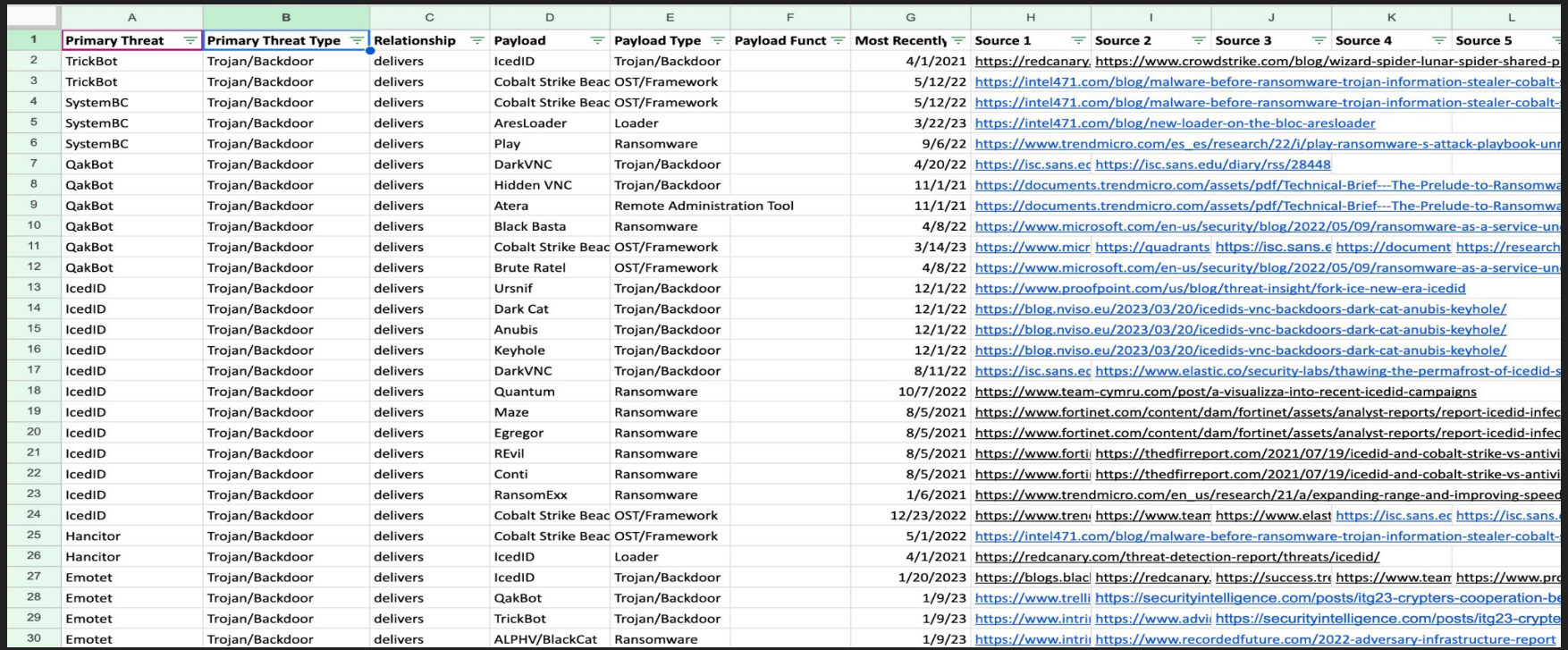
Dislikes: Long walks on the beach, ATT&CK Technique T1622, and the sound of the cooking vent

You might be wondering why we gathered you all here…

Some facts:

- We do not claim to be experts in cyber crime
- We sought to identify common TTPs (and malware) to drive prioritization for (enterprise) defenders
- All the data we're presenting is skewed based on public reporting and OSINT. You all likely have access to better data, therefore we hope you get to take some of our work and iterate on it 🤘

#TransformationFriday



	A	B	C	D	E	F	G	H	I	J	K	L
1	Primary Threat	Primary Threat Type	Relationship	Payload	Payload Type	Payload Funct	Most Recently	Source 1	Source 2	Source 3	Source 4	Source 5
2	TrickBot	Trojan/Backdoor	delivers	IcedID	Trojan/Backdoor		4/1/2021	https://redcanary.	https://www.crowdstrike.com/blog/wizard-spider-lunar-spider-shared-p			
3	TrickBot	Trojan/Backdoor	delivers	Cobalt Strike Beac	OST/Framework		5/12/22	https://intel471.com/blog/malware-before-ransomware-trojan-information-stealer-cobalt-				
4	SystemBC	Trojan/Backdoor	delivers	Cobalt Strike Beac	OST/Framework		5/12/22	https://intel471.com/blog/malware-before-ransomware-trojan-information-stealer-cobalt-				
5	SystemBC	Trojan/Backdoor	delivers	AresLoader	Loader		3/22/23	https://intel471.com/blog/new-loader-on-the-bloc-aresloader				
6	SystemBC	Trojan/Backdoor	delivers	Play	Ransomware		9/6/22	https://www.trendmicro.com/es_es/research/22/i/play-ransomware-s-attack-playbook-unr				
7	QakBot	Trojan/Backdoor	delivers	DarkVNC	Trojan/Backdoor		4/20/22	https://isc.sans.ec	https://isc.sans.edu/diary/rss/28448			
8	QakBot	Trojan/Backdoor	delivers	Hidden VNC	Trojan/Backdoor		11/1/21	https://documents.trendmicro.com/assets/pdf/Technical-Brief---The-Prelude-to-Ransomwa				
9	QakBot	Trojan/Backdoor	delivers	Atera	Remote Administration Tool		11/1/21	https://documents.trendmicro.com/assets/pdf/Technical-Brief---The-Prelude-to-Ransomwa				
10	QakBot	Trojan/Backdoor	delivers	Black Basta	Ransomware		4/8/22	https://www.microsoft.com/en-us/security/blog/2022/05/09/ransomware-as-a-service-un				
11	QakBot	Trojan/Backdoor	delivers	Cobalt Strike Beac	OST/Framework		3/14/23	https://www.micr	https://quadrants	https://isc.sans.e	https://document	https://research
12	QakBot	Trojan/Backdoor	delivers	Brute Ratel	OST/Framework		4/8/22	https://www.microsoft.com/en-us/security/blog/2022/05/09/ransomware-as-a-service-un				
13	IcedID	Trojan/Backdoor	delivers	Ursnif	Trojan/Backdoor		12/1/22	https://www.proofpoint.com/us/blog/threat-insight/fork-ice-new-era-icedid				
14	IcedID	Trojan/Backdoor	delivers	Dark Cat	Trojan/Backdoor		12/1/22	https://blog.nviso.eu/2023/03/20/icedids-vnc-backdoors-dark-cat-anubis-keyhole/				
15	IcedID	Trojan/Backdoor	delivers	Anubis	Trojan/Backdoor		12/1/22	https://blog.nviso.eu/2023/03/20/icedids-vnc-backdoors-dark-cat-anubis-keyhole/				
16	IcedID	Trojan/Backdoor	delivers	Keyhole	Trojan/Backdoor		12/1/22	https://blog.nviso.eu/2023/03/20/icedids-vnc-backdoors-dark-cat-anubis-keyhole/				
17	IcedID	Trojan/Backdoor	delivers	DarkVNC	Trojan/Backdoor		8/11/22	https://isc.sans.ec	https://www.elastic.co/security-labs/thawing-the-permafrost-of-icedid-s			
18	IcedID	Trojan/Backdoor	delivers	Quantum	Ransomware		10/7/2022	https://www.team-cymru.com/post/a-visualizza-into-recent-icedid-campaigns				
19	IcedID	Trojan/Backdoor	delivers	Maze	Ransomware		8/5/2021	https://www.fortinet.com/content/dam/fortinet/assets/analyst-reports/report-icedid-infec				
20	IcedID	Trojan/Backdoor	delivers	Egregor	Ransomware		8/5/2021	https://www.fortinet.com/content/dam/fortinet/assets/analyst-reports/report-icedid-infec				
21	IcedID	Trojan/Backdoor	delivers	REvil	Ransomware		8/5/2021	https://www.forti	https://thedfirreport.com/2021/07/19/icedid-and-cobalt-strike-vs-antivi			
22	IcedID	Trojan/Backdoor	delivers	Conti	Ransomware		8/5/2021	https://www.forti	https://thedfirreport.com/2021/07/19/icedid-and-cobalt-strike-vs-antivi			
23	IcedID	Trojan/Backdoor	delivers	RansomExx	Ransomware		1/6/2021	https://www.trendmicro.com/en_us/research/21/a/expanding-range-and-improving-speed				
24	IcedID	Trojan/Backdoor	delivers	Cobalt Strike Beac	OST/Framework		12/23/2022	https://www.tren	https://www.team	https://www.elast	https://isc.sans.ec	https://isc.sans.e
25	Hancitor	Trojan/Backdoor	delivers	Cobalt Strike Beac	OST/Framework		5/1/2022	https://intel471.com/blog/malware-before-ransomware-trojan-information-stealer-cobalt-				
26	Hancitor	Trojan/Backdoor	delivers	IcedID	Loader		4/1/2021	https://redcanary.com/threat-detection-report/threats/icedid/				
27	Emotet	Trojan/Backdoor	delivers	IcedID	Trojan/Backdoor		1/20/2023	https://blogs.blac	https://redcanary.	https://success.tre	https://www.team	https://www.pro
28	Emotet	Trojan/Backdoor	delivers	QakBot	Trojan/Backdoor		1/9/23	https://www.trelli	https://securityintelligence.com/posts/itg23-crypters-cooperation-be			
29	Emotet	Trojan/Backdoor	delivers	TrickBot	Trojan/Backdoor		1/9/23	https://www.intri	https://www.advi	https://securityintelligence.com/posts/itg23-crypte		
30	Emotet	Trojan/Backdoor	delivers	ALPHV/BlackCat	Ransomware		1/9/23	https://www.intri	https://www.recordedfuture.com/2022-adversary-infrastructure-report			

Primary Subjects

*Disclaimer: We chose not to highlight offensive security technologies or frameworks here (i.e. Cobalt Strike, Sliver, etc.) purely based on scope of this talk

QakBot

IcedID

SocGholish

Gootloader

Bumblebee

Emotet

Trickbot

Truebot

SystemBC

PrivateLoader

Look at this Graph's Summary Metrics

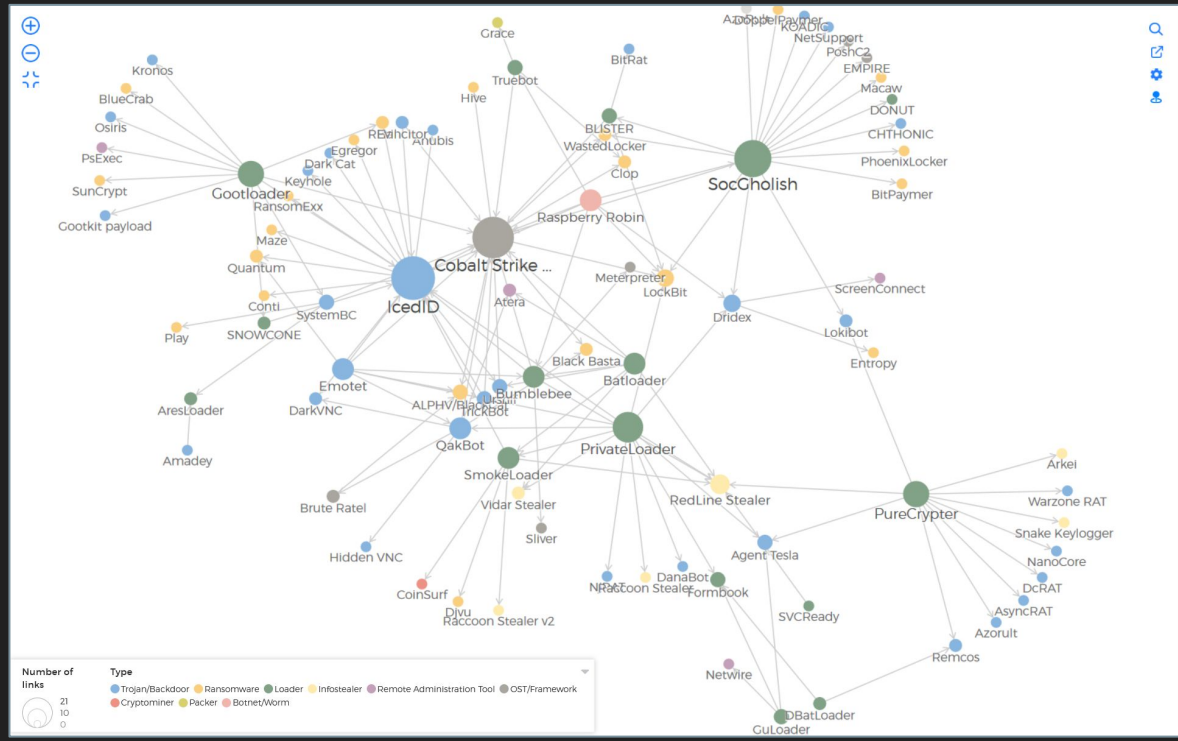
87 Nodes, 133 Edges (links)

Based on 73 public sources, estimated observation dates mainly 2022-23

23 "Primary Threats" (mainly Trojans & Loaders)

78 payloads/later-stage malware families:

- Trojan/Backdoor (46), Ransomware (25), OST/Framework (20), Loader (16), Infostealer (12), Remote Administration Tool (5), Packer (1), Cryptominer (1)



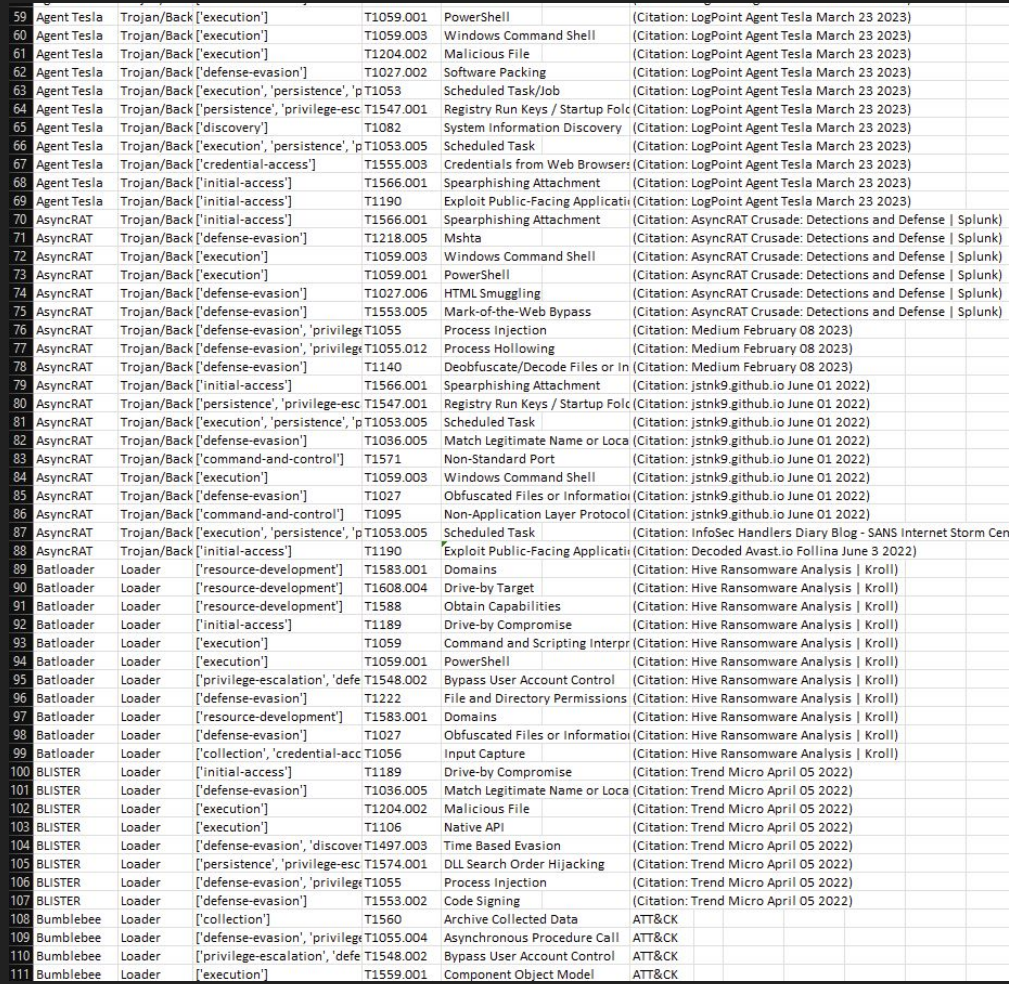
Interact with & download the data:
https://onodo.org/visualizations/235067/

TTP Analysis

We surfaced ATT&CK (Sub-Techniques) for the 28 Primary Threats

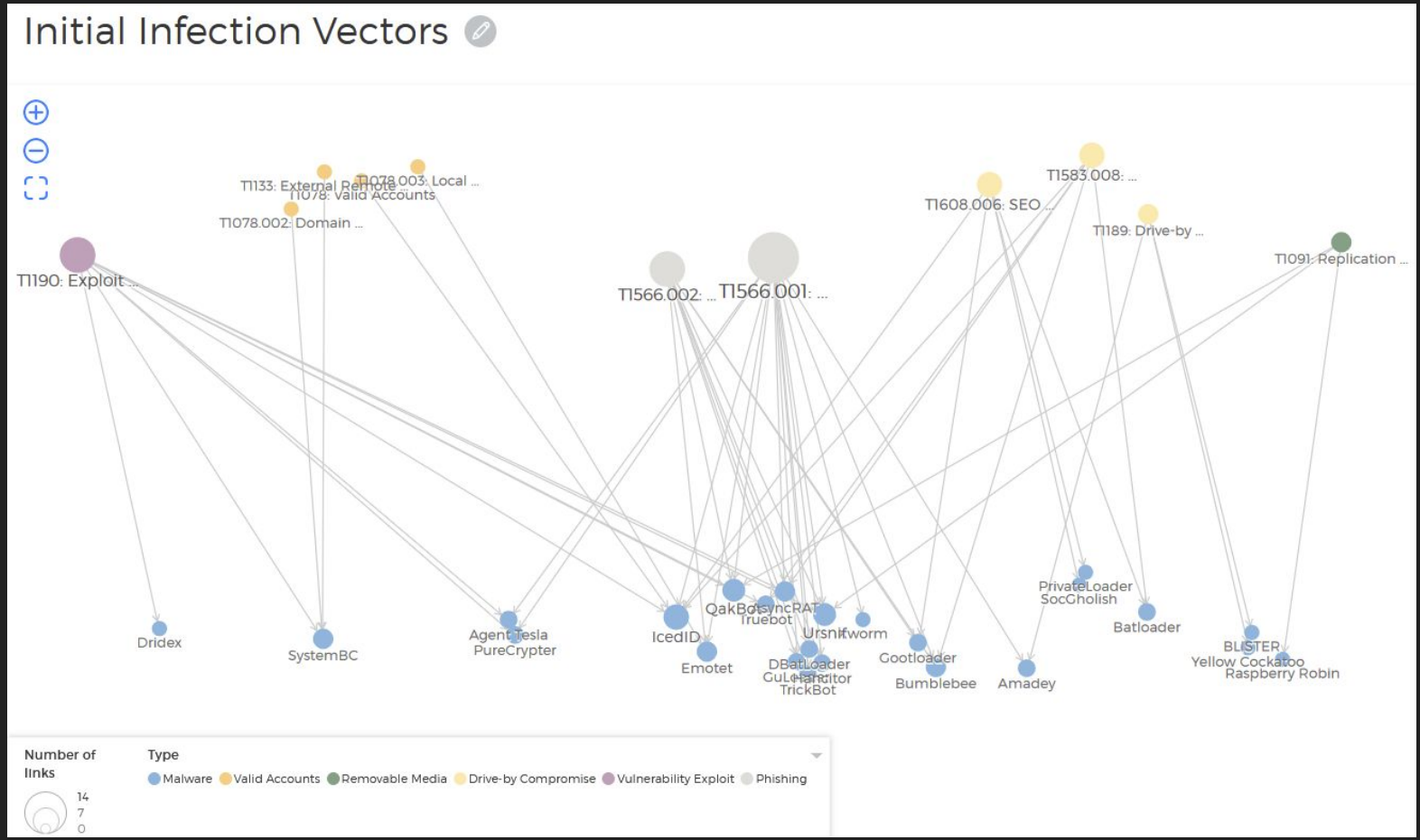
- Derived from 100+ public sources (mapping FTW)
- 14 newly tracked threats, 5 updated ones

760 technique references across **189 discrete techniques** (33% of the entire ATT&CK knowledge base)



59	Agent Tesla	Trojan/Back	['execution']	T1059.001	PowerShell	(Citation: LogPoint Agent Tesla March 23 2023)
60	Agent Tesla	Trojan/Back	['execution']	T1059.003	Windows Command Shell	(Citation: LogPoint Agent Tesla March 23 2023)
61	Agent Tesla	Trojan/Back	['execution']	T1204.002	Malicious File	(Citation: LogPoint Agent Tesla March 23 2023)
62	Agent Tesla	Trojan/Back	['defense-evasion']	T1027.002	Software Packing	(Citation: LogPoint Agent Tesla March 23 2023)
63	Agent Tesla	Trojan/Back	['execution', 'persistence', 'p	T1053	Scheduled Task/Job	(Citation: LogPoint Agent Tesla March 23 2023)
64	Agent Tesla	Trojan/Back	['persistence', 'privilege-esc	T1547.001	Registry Run Keys / Startup Fol	(Citation: LogPoint Agent Tesla March 23 2023)
65	Agent Tesla	Trojan/Back	['discovery']	T1082	System Information Discovery	(Citation: LogPoint Agent Tesla March 23 2023)
66	Agent Tesla	Trojan/Back	['execution', 'persistence', 'p	T1053.005	Scheduled Task	(Citation: LogPoint Agent Tesla March 23 2023)
67	Agent Tesla	Trojan/Back	['credential-access']	T1555.003	Credentials from Web Browsers	(Citation: LogPoint Agent Tesla March 23 2023)
68	Agent Tesla	Trojan/Back	['initial-access']	T1566.001	Spearphishing Attachment	(Citation: LogPoint Agent Tesla March 23 2023)
69	Agent Tesla	Trojan/Back	['initial-access']	T1190	Exploit Public-Facing Applicati	(Citation: LogPoint Agent Tesla March 23 2023)
70	AsyncRAT	Trojan/Back	['initial-access']	T1566.001	Spearphishing Attachment	(Citation: AsyncRAT Crusade: Detections and Defense | Splunk)
71	AsyncRAT	Trojan/Back	['defense-evasion']	T1218.005	Mshta	(Citation: AsyncRAT Crusade: Detections and Defense | Splunk)
72	AsyncRAT	Trojan/Back	['execution']	T1059.003	Windows Command Shell	(Citation: AsyncRAT Crusade: Detections and Defense | Splunk)
73	AsyncRAT	Trojan/Back	['execution']	T1059.001	PowerShell	(Citation: AsyncRAT Crusade: Detections and Defense | Splunk)
74	AsyncRAT	Trojan/Back	['defense-evasion']	T1027.006	HTML Smuggling	(Citation: AsyncRAT Crusade: Detections and Defense | Splunk)
75	AsyncRAT	Trojan/Back	['defense-evasion']	T1553.005	Mark-of-the-Web Bypass	(Citation: AsyncRAT Crusade: Detections and Defense | Splunk)
76	AsyncRAT	Trojan/Back	['defense-evasion', 'privilege	T1055	Process Injection	(Citation: Medium February 08 2023)
77	AsyncRAT	Trojan/Back	['defense-evasion', 'privilege	T1055.012	Process Hollowing	(Citation: Medium February 08 2023)
78	AsyncRAT	Trojan/Back	['defense-evasion']	T1140	Deobfuscate/Decode Files or In	(Citation: Medium February 08 2023)
79	AsyncRAT	Trojan/Back	['initial-access']	T1566.001	Spearphishing Attachment	(Citation: jstnk9.github.io June 01 2022)
80	AsyncRAT	Trojan/Back	['persistence', 'privilege-esc	T1547.001	Registry Run Keys / Startup Fol	(Citation: jstnk9.github.io June 01 2022)
81	AsyncRAT	Trojan/Back	['execution', 'persistence', 'p	T1053.005	Scheduled Task	(Citation: jstnk9.github.io June 01 2022)
82	AsyncRAT	Trojan/Back	['defense-evasion']	T1036.005	Match Legitimate Name or Loca	(Citation: jstnk9.github.io June 01 2022)
83	AsyncRAT	Trojan/Back	['command-and-control']	T1571	Non-Standard Port	(Citation: jstnk9.github.io June 01 2022)
84	AsyncRAT	Trojan/Back	['execution']	T1059.003	Windows Command Shell	(Citation: jstnk9.github.io June 01 2022)
85	AsyncRAT	Trojan/Back	['defense-evasion']	T1027	Obfuscated Files or Informatio	(Citation: jstnk9.github.io June 01 2022)
86	AsyncRAT	Trojan/Back	['command-and-control']	T1095	Non-Application Layer Protocol	(Citation: jstnk9.github.io June 01 2022)
87	AsyncRAT	Trojan/Back	['execution', 'persistence', 'p	T1053.005	Scheduled Task	(Citation: InfoSec Handlers Diary Blog - SANS Internet Storm Cen
88	AsyncRAT	Trojan/Back	['initial-access']	T1190	Exploit Public-Facing Applicati	(Citation: Decoded Avast.io Follina June 3 2022)
89	Batloader	Loader	['resource-development']	T1583.001	Domains	(Citation: Hive Ransomware Analysis | Kroll)
90	Batloader	Loader	['resource-development']	T1608.004	Drive-by Target	(Citation: Hive Ransomware Analysis | Kroll)
91	Batloader	Loader	['resource-development']	T1588	Obtain Capabilities	(Citation: Hive Ransomware Analysis | Kroll)
92	Batloader	Loader	['initial-access']	T1189	Drive-by Compromise	(Citation: Hive Ransomware Analysis | Kroll)
93	Batloader	Loader	['execution']	T1059	Command and Scripting Interpr	(Citation: Hive Ransomware Analysis | Kroll)
94	Batloader	Loader	['execution']	T1059.001	PowerShell	(Citation: Hive Ransomware Analysis | Kroll)
95	Batloader	Loader	['privilege-escalation', 'defe	T1548.002	Bypass User Account Control	(Citation: Hive Ransomware Analysis | Kroll)
96	Batloader	Loader	['defense-evasion']	T1222	File and Directory Permissions	(Citation: Hive Ransomware Analysis | Kroll)
97	Batloader	Loader	['resource-development']	T1583.001	Domains	(Citation: Hive Ransomware Analysis | Kroll)
98	Batloader	Loader	['defense-evasion']	T1027	Obfuscated Files or Informatio	(Citation: Hive Ransomware Analysis | Kroll)
99	Batloader	Loader	['collection', 'credential-acc	T1056	Input Capture	(Citation: Hive Ransomware Analysis | Kroll)
100	BLISTER	Loader	['initial-access']	T1189	Drive-by Compromise	(Citation: Trend Micro April 05 2022)
101	BLISTER	Loader	['defense-evasion']	T1036.005	Match Legitimate Name or Loca	(Citation: Trend Micro April 05 2022)
102	BLISTER	Loader	['execution']	T1204.002	Malicious File	(Citation: Trend Micro April 05 2022)
103	BLISTER	Loader	['execution']	T1106	Native API	(Citation: Trend Micro April 05 2022)
104	BLISTER	Loader	['defense-evasion', 'discover	T1497.003	Time Based Evasion	(Citation: Trend Micro April 05 2022)
105	BLISTER	Loader	['persistence', 'privilege-esc	T1574.001	DLL Search Order Hijacking	(Citation: Trend Micro April 05 2022)
106	BLISTER	Loader	['defense-evasion', 'privilege	T1055	Process Injection	(Citation: Trend Micro April 05 2022)
107	BLISTER	Loader	['defense-evasion']	T1553.002	Code Signing	(Citation: Trend Micro April 05 2022)
108	Bumblebee	Loader	['collection']	T1560	Archive Collected Data	ATT&CK
109	Bumblebee	Loader	['defense-evasion', 'privilege	T1055.004	Asynchronous Procedure Call	ATT&CK
110	Bumblebee	Loader	['privilege-escalation', 'defe	T1548.002	Bypass User Account Control	ATT&CK
111	Bumblebee	Loader	['execution']	T1559.001	Component Object Model	ATT&CK

Look at this Other Graph



Technique Overlap & Trends

Initial Infection Vector	***Trend***	***Associated Threats***
Phishing (T1566.001/2)	Continually shifting download/execution chains “Not phishing”	88%
Drive-by Compromise (T1189)	Malvertising (T1583.008 - New!) SEO Poisoning (T1608.006)	50%
Vulnerability Exploit (T1190)	Some new, some old	39%
Credentials? (T1078)	Ew	17%
Removable Media (T1091)	Yup, still a thing	13%

Technique Overlap & Trends

Execution chains

- *Frequent evolution: Macro blocking → MOTW Bypass*

Discovery methods

- *System checks on top, domain checks popular (HVTs)*

Defense evasion

- *Silver linings (SOC) playbook?*

Outlier techniques

- *Hidden gems*

Mitigations, Detections, and Response

Distance from Impact (“Boom”) — *Defender Control*

Ad customer controls

Email security controls

Workforce awareness & training

Workforce awareness & training

Execution detections

Patching

Discovery detections

Defense evasion, lateral movement, ingress detections

Impact techniques

IR

- Defenders can further prioritize detection development based on factors including:
  - Centrality of links, technique overlap
- Research community: *Call to action!*


Thank
You!!