



TEAM CYMRU

Infrastructure Tracking and Visualization of Modern Threat Actors



Matthew Hall

Senior Security Engineer at Team Cymru





Cybersecurity



cybersecurity

/ˈsaɪbəseɪ,kjʊərəti/

noun

the state of being protected against the criminal or unauthorized use of electronic data, or the measures taken to achieve this.

Identify risk

- Created by yourself / org / supply chain / acquisition, ect.
 - Operational/Process
 - Software/firmware
- Created by adversaries

Industry Trends

“It takes a village”

- Most orgs build CTI capability by marrying internal systems/signal with strategic insight/data they cannot feasibly generate themselves.
- Most mature CTI programs I've interacted with find 2-4 key sources of external cti/signal/capability to help them understand/operationalize their end goals.

Disclaimer

- I'm not here to promote any product/vendor
- I believe in winning.
- The findings and insight I'll present today were done with the data and capabilities I have access to.

Intro to IcedID



IcedID

IcedID (also known as BokBot) started life in early 2017 as a banking trojan that later evolved to include dropper malware capabilities. These capabilities enable IcedID to download and deploy additional malware like Cobalt Strike, with recent infections leading to Quantum ransomware.

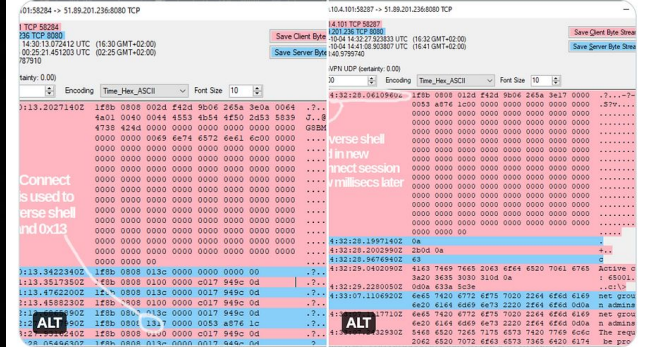


Infected Victim (bot) traffic over TCP/8080

NETRESEC
@netresec

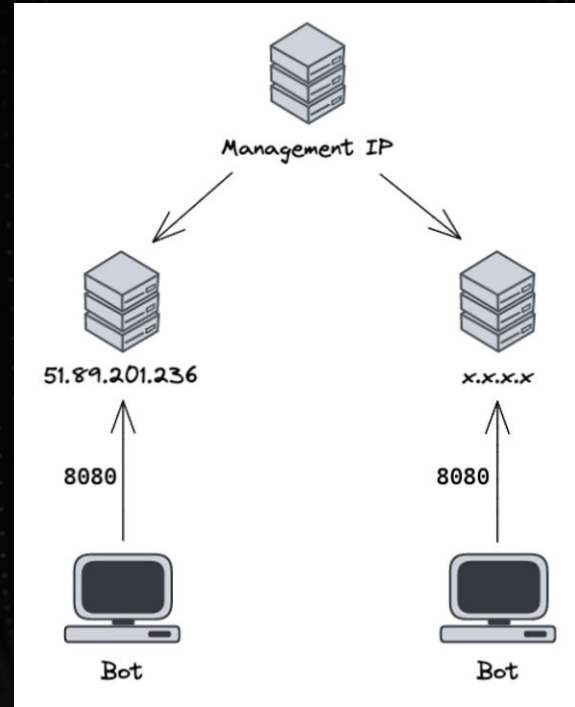
Replying to @malware_traffic and @Unit42_Intel

That's the IcedID BackConnect protocol. It's the same protocol as in your 2022-06-28 TA578 run, but it's using an auth value of Ox08088b1f this time. Apparently the BackConnect command Ox13 launches a reverse shell, haven't seen that before. Thanks for sharing!

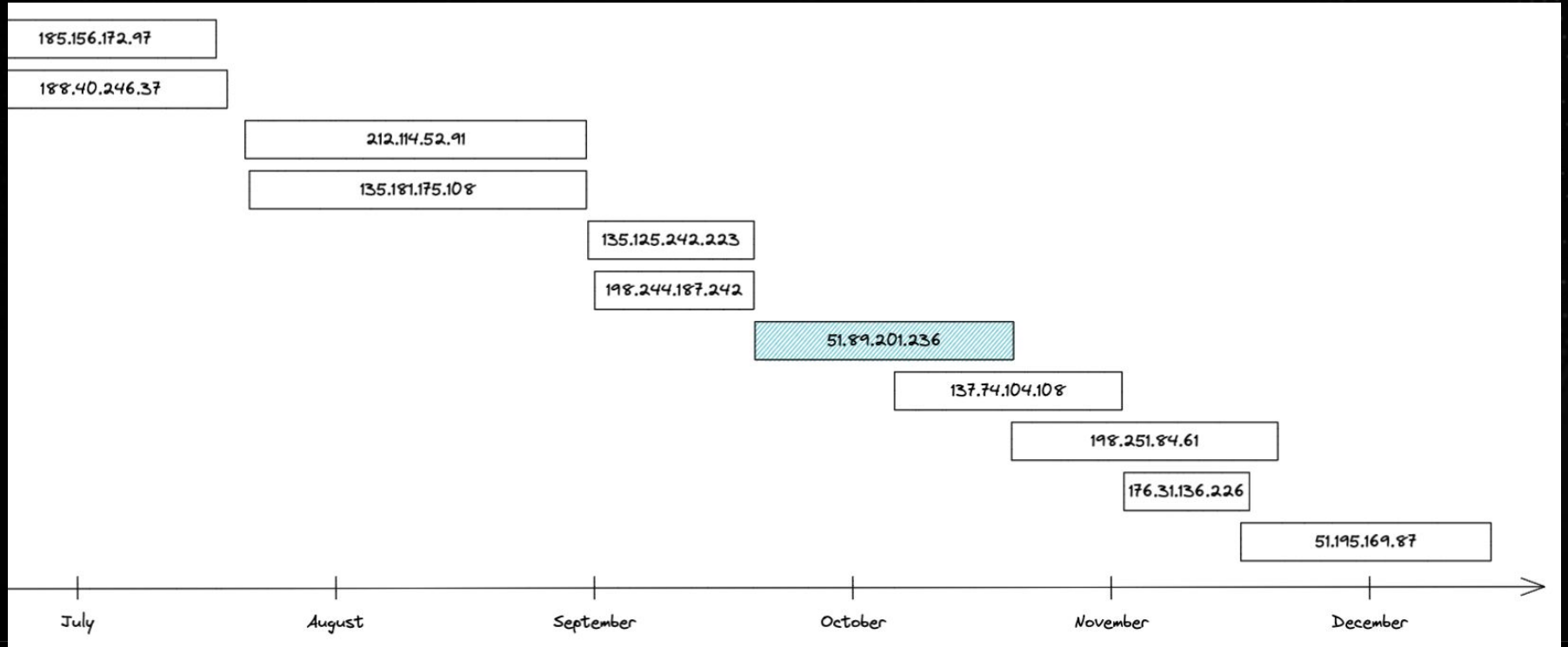


The screenshot shows a network traffic analysis tool interface. On the left, there's a list of connections. One connection is highlighted in red with a pink box and a pink arrow pointing to it. The pink box contains the text: "Connect is used to reverse shell and Ox13". The main window shows a detailed view of a TCP connection. The destination IP is 110.4.101.58287 and the destination port is 8080. The connection is established at 14:30:51. The data section shows a series of hex bytes, with a red box highlighting the command: "reverse shell\nin new\ninject session\n!m!secs kstkr".

11:18 AM · Oct 6, 2022



C2 Lifecycle through 2022



Start with a C2





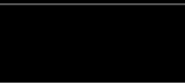
Threat Research Team

Bonjour #IcedID #BackConnect!

We've spotted a new C2 server being set up on:

5.196.196.252 (🇫🇷)

Expect to see this IP in infection chains in the coming days / hours.



cc @netresec

2:30 AM · Jan 24, 2023 · **16.7K** Views

Open Ports/Services of C2

6 (TCP)	8082 (us-cli)	-	-
6 (TCP)	8086 (d-s-n)	-	-
6 (TCP)	22 (ssh)	ssh	SSH-2.0-OpenSSH_8.4p1 Debian-5+deb11u1 less
6 (TCP)	80 (http)	title	Apache2 Debian Default Page: It works less
6 (TCP)	8083 (us-srv)	vnc	RFB 003.008 auth=[VNC-chap] less
6 (TCP)	80 (http)	http.server	nginx/1.18.0
6 (TCP)	80 (http)	http	HTTP/1.1 200 OK Server: nginx/1.18.0 Date: Sat, 28 Jan 2023 1



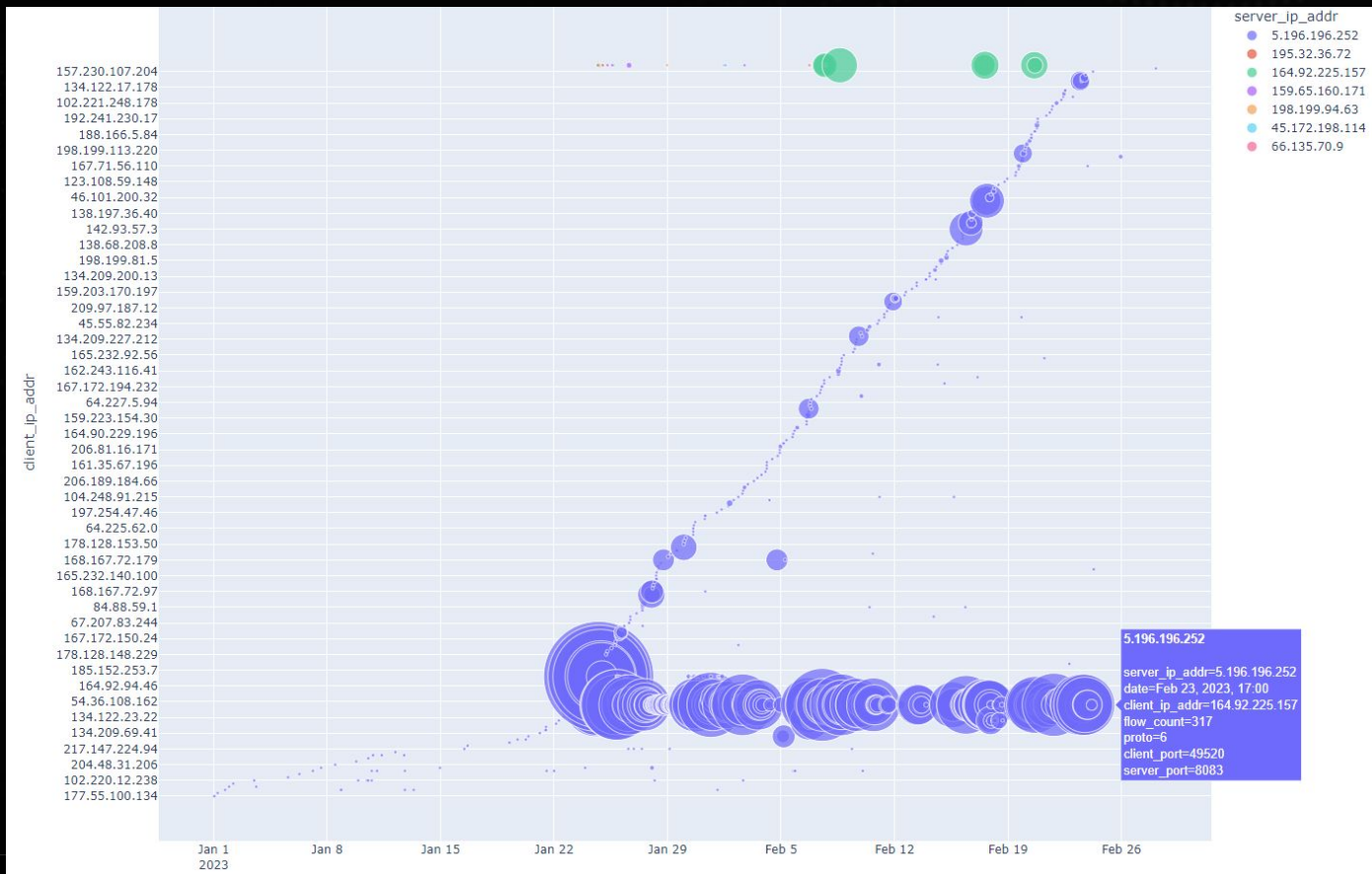
Network Comms to/from C2

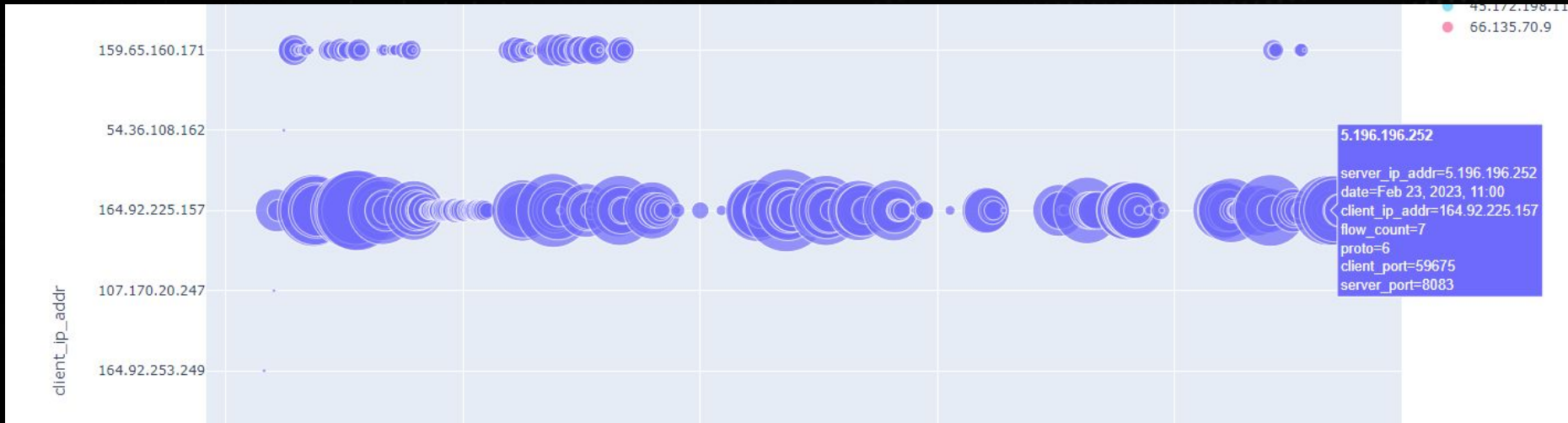
Flow Initiators

...

Protocol	LikelyAction	client_cc	client_ip	ClientPortRange	ClientPortCount	server_port	server_ip	server_cc	ACK_FINISHs	RSTs	SYN_ONLYs	ACK_ONLYs	FlowCount	AvgFlowRate	Duration
TCP	?	US	164.92.225.157	49281-61148	555	8083	5.196.196.252	FR	c:0 s:0	c:0 s:0	c:0 s:0	c:1155 s:17749	26149	34.4/hr	31.7 days
TCP	Beacon	IT	195.32.36.72	50694-63540	2827	8080	5.196.196.252	FR	c:5 s:6	c:0 s:0	c:9 s:0	c:1417 s:2238	4380	23.0/hr	7.9 days
TCP	?	US	159.65.160.171	38990-65529	1658	8082	5.196.196.252	FR	c:29 s:21	c:4 s:3	c:38 s:0	c:496 s:998	2160	3.0/hr	30.1 days
TCP	Beacon	US	66.135.70.9	49766-65477	530	8080	5.196.196.252	FR	c:0 s:1	c:0 s:0	c:0 s:0	c:0 s:493	548	0.8/hr	27.4 days

Network Comms of C2

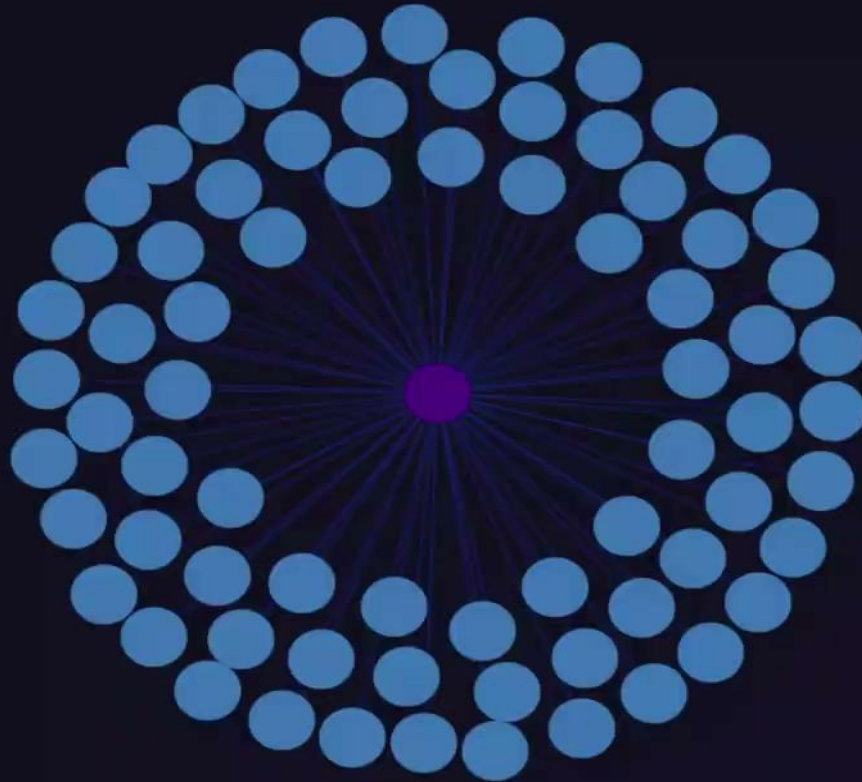




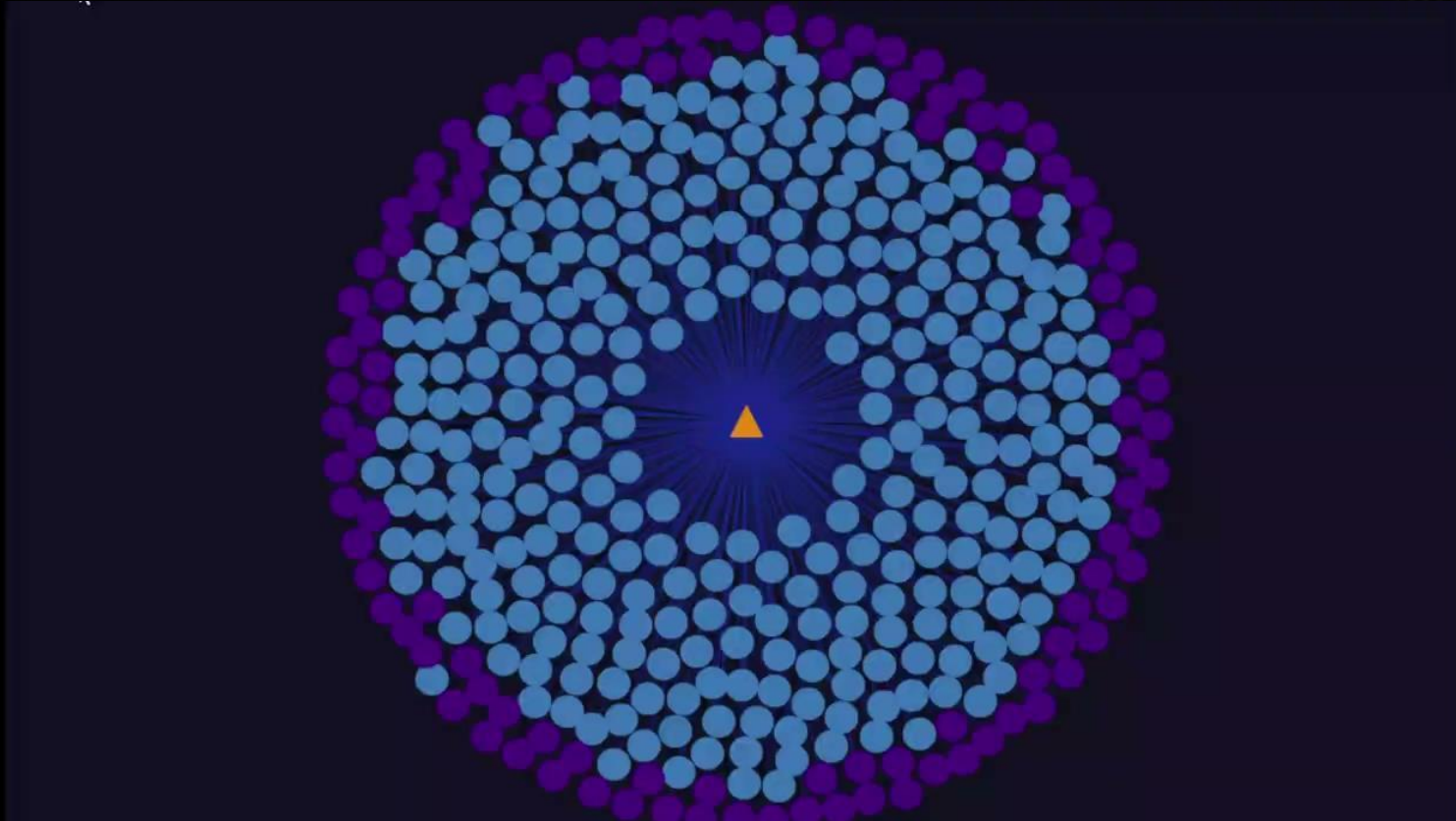
A Unique Approach



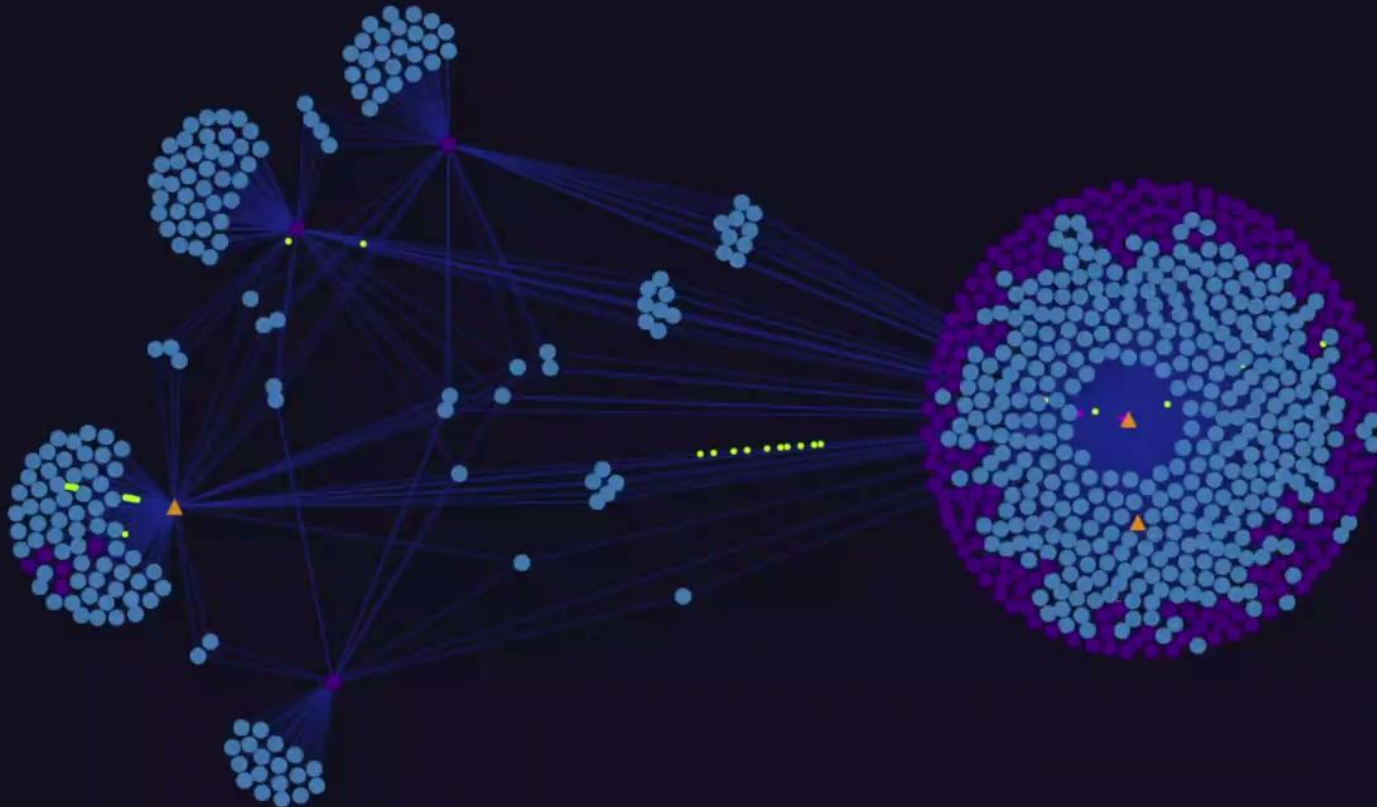
C2 Visual Analysis



Mgmt Host Visual Analysis



T1-T3 Visual Analysis



Key Findings and Takeaways

- IcedID utilized T2 inf for much longer than T1 (c2s)
- Revolving Actor IPs all based in Moldova, while initially lasting 24-48 hours, increased to 3-5 on avg. over 2023
- Unique approaches to visualizing inf. interaction lead to new understandings about port/service usage, as well as primary/secondary nature of C2s through time.

Questions?

Further Reading

<https://www.team-cymru.com/post/inside-the-icedid-backconnect-protocol>

<https://www.team-cymru.com/post/a-visualizza-into-recent-icedid-campaigns>

<https://www.team-cymru.com/post/inside-the-icedid-backconnect-protocol-part-2>

