THE JARM'ING ADVENTURES OF A WEAPONIZED OF SECURITY TOOL

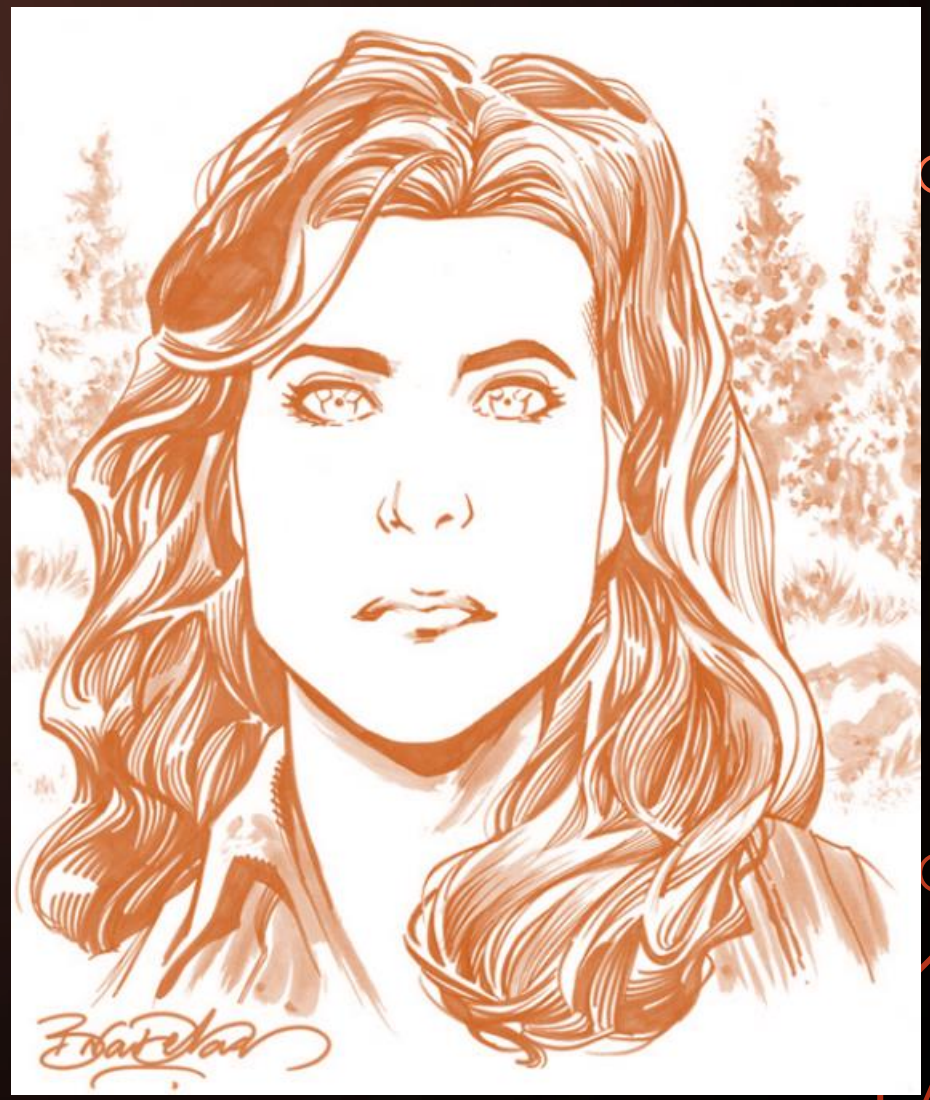
DEFCAMP ROMANIA 2023

CHRIS KUBECKA, CEO HYPASEC

Chris Kubecka @SecEvangelism

PRESENTER

- Critical infrastructure security, ICS cyberwarfare
- Former Roles Head of Aramco Information Protection
- Distinguished Chair of Cyber Middle East Institute
- U.S Air Force Aircrew & Space Command-Command & Control Systems



PRESENTER

How A 10-Year-Old War Dialer Became A Top Cybersecurity Expert

Boeing's poor information security posture threatens passenger safety, national security, researcher says

Extortion and alleged ISIS threats: A Saudi embassy learned the hard way about email security

Ukraine border control hit with wiper cyberattack, slowing refugee crossing

Inside the OSINT Operation to Get Foreign Students Out of Ukraine

A ragtag group of hackers and OSINT professionals is using everything from open flight data to Google Maps to evacuate foreign students from Ukraine.

An American hacker explains how accepting a random LinkedIn request led to the Iranian government hounding her with 'dodgy' job offers for years

QUICK DISCLAIMER

- All research took place in The Netherlands under current ethical hacking guidelines of the country
- **I got bored & went down a rabbit hole**
- Used only FREE level tools, not a spokesperson

JARM & OSINT TOOLS

- Built from JA3S
- Virus Total
- Sales Force Github
- Censys.io
- Available is some other commercial tools

JARM support has been or is being added to:

SecurityTrails

Shodan

BinaryEdge

RiskIQ

Palo Alto Networks

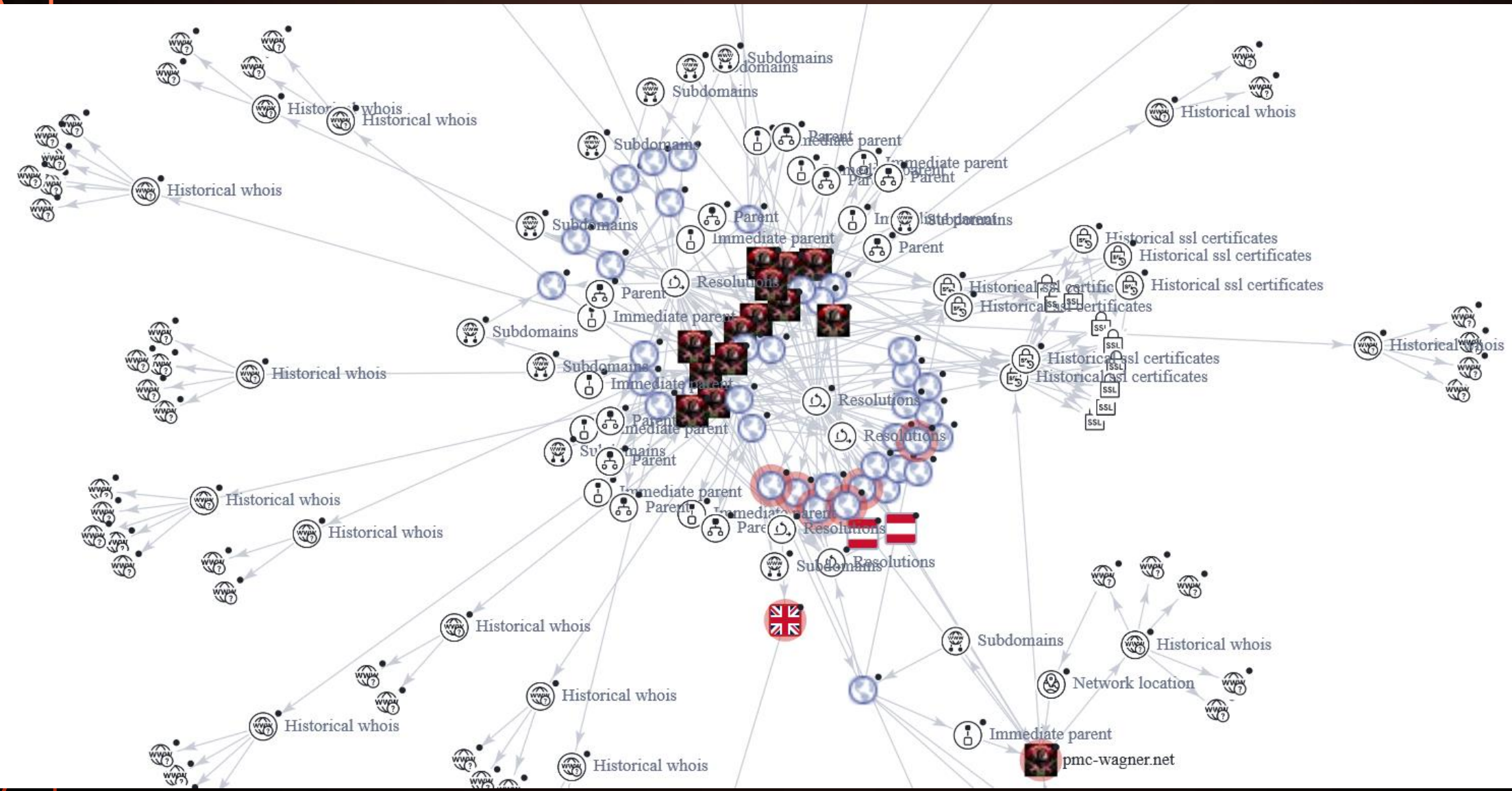
Censys

360

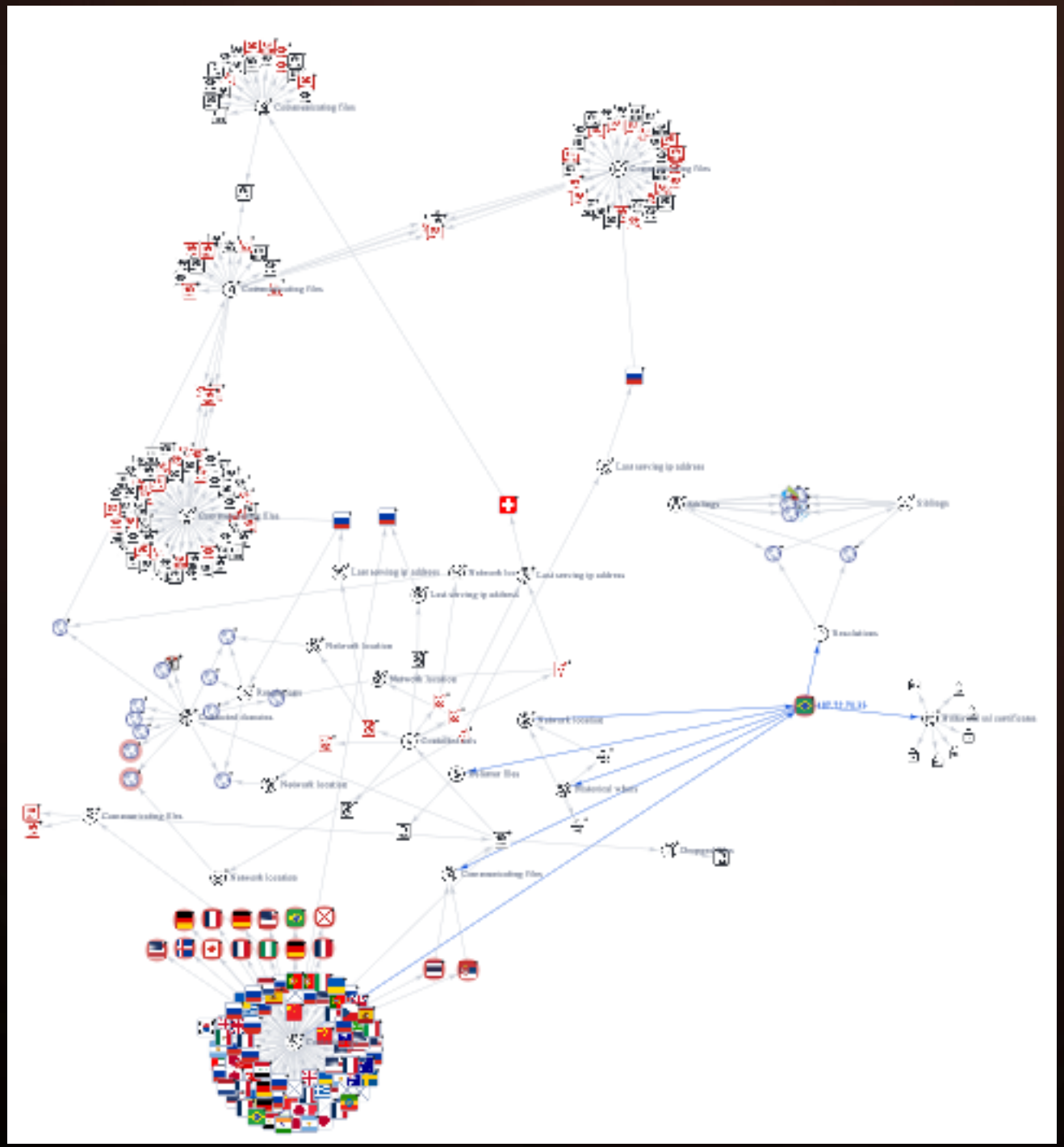
VIRUS TOTAL

- Malware research, safe web, document, URL, malware network, and distribution study
- Graphing
- Link relationships
- Following a Propaganda network starting from Government.ru


VIRUSTOTAL
Analyse suspicious files, domains, IPs and URLs to detect malware and other breaches, automatically share them with the security community.
FILE
URL
SEARCH
Choose file


Historical whois
Historical whois
Historical whois
Subdomains
Subdomains
Subdomains
Parent
Immediate parent
Parent
Immediate parent
Parent
Resolutions
Historical ssl certificates
Historical ssl certificates
Historical ssl certificates
Historical ssl certificates
Historical ssl certificates
Historical whois
Historical whois
Historical whois
Historical whois
Historical whois
Historical whois
Historical whois
Historical whois
Subdomains
Network location
Historical whois
Immediate parent
pmc-wagner.net

Chris Kubecka @SecEvangelism



WHAT IS JARM FINGERPRINTING?

- Fingerprinting tool for TLS servers
- Same TLS configuration same JARM fingerprint
- Asset identification
- Tracking C2 malware & systems

WHY NAUGHTY FOLKS USE IT

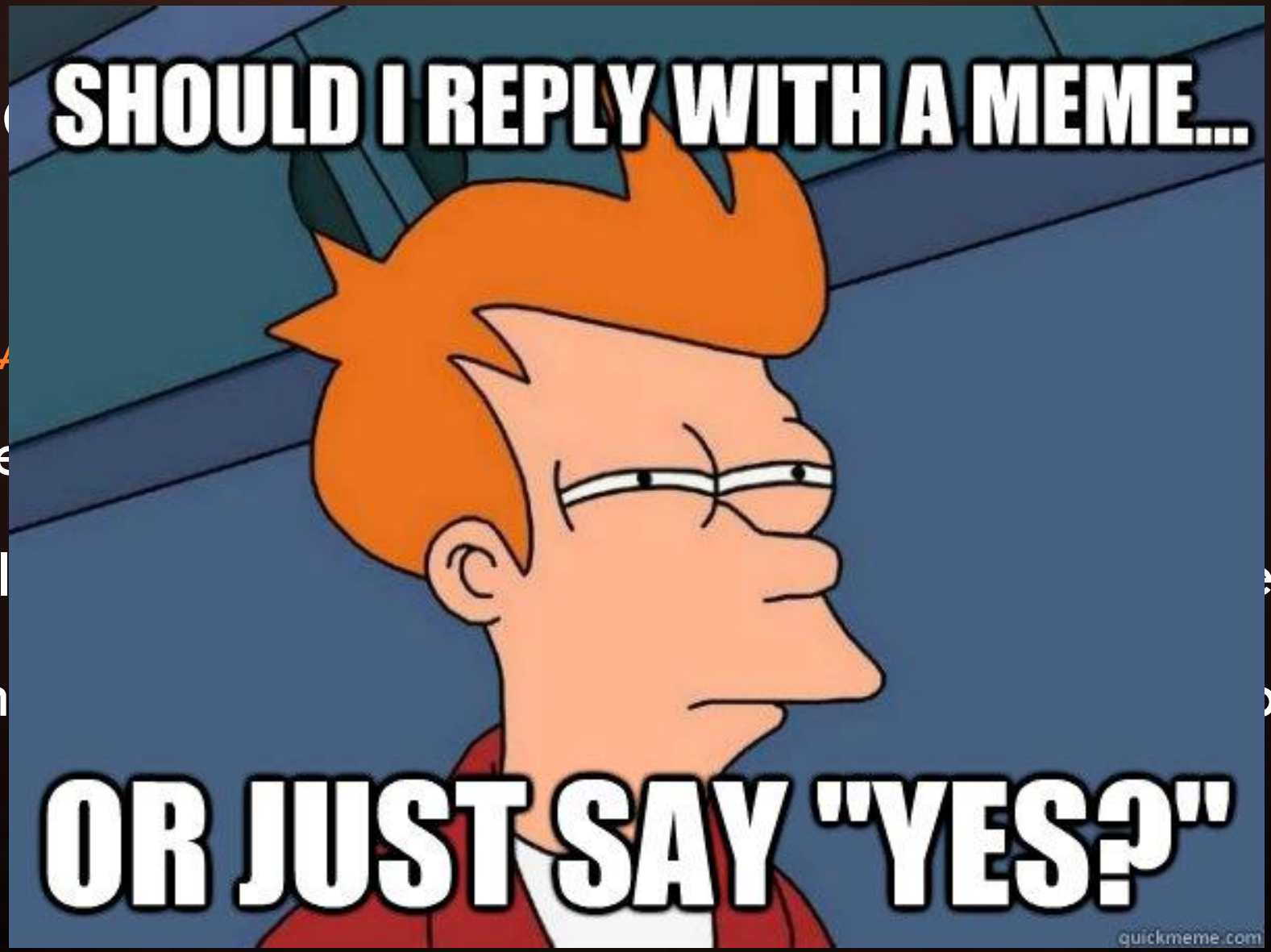
- Attackers are lazy/automate
- Admin lots of systems, duplicate configuration
- Distribution identification
- Tracking systems & control

WHY NICE FOLKS USE IT

- System Administrators are lazy/automate
- Certificates are awesome to pivot off
- Naughty asset identification
- Tracking attackers & spread

SALESF

- https:/
- Require
- Could I ems?
- System os?



SOMETHING LOOKS FAMILIAR

- Familiar, unexpected tool name
- Tested tool previously
- Under export controls from the US
- Point and click to create safe malware for advanced testing

SOMETHING LOOKS FAMILIAR

- JARM Fingerprint malware hunter list late 2022

1	jarm	src_ip	src_port	country	asn	known_c	timestamp
22	2ad2ad16d2ad2ad22c42d42d0000006f254909a73bf62f6b28507e9fb451b5	187.72.70.3	443	BR	16735	SCYTHE	2022-09-27_10:38:29
208	2ad2ad16d2ad2ad22c42d42d0000006f254909a73bf62f6b28507e9fb451b5	20.254.57.1	443	GB	8075	SCYTHE	2022-10-01_09:08:45
502	2ad2ad16d2ad2ad22c42d42d0000006f254909a73bf62f6b28507e9fb451b5	210.0.220.2	443	HK	9304	SCYTHE	2022-10-07_04:04:11
744	2ad2ad16d2ad2ad22c42d42d0000006f254909a73bf62f6b28507e9fb451b5	223.197.18	443	HK	4760	SCYTHE	2022-10-28_04:07:23
240	2ad2ad16d2ad2ad22c42d42d0000006f254909a73bf62f6b28507e9fb451b5	201.221.15	443	CO	22368	SCYTHE	2022-11-03_21:07:44
606	2ad2ad16d2ad2ad22c42d42d0000006f254909a73bf62f6b28507e9fb451b5	201.217.5.1	443	PY	27768	SCYTHE	2022-11-09_05:19:25
412	2ad2ad16d2ad2ad22c42d42d0000006f254909a73bf62f6b28507e9fb451b5	177.229.13	443	MX	13999	SCYTHE	2022-11-22_10:28:41
090	2ad2ad16d2ad2ad22c42d42d0000006f254909a73bf62f6b28507e9fb451b5	201.217.5.1	443	PY	27768	SCYTHE	2022-12-01_01:31:51
8554	2ad2ad16d2ad2ad22c42d42d0000006f254909a73bf62f6b28507e9fb451b5	222.92.117	443	CN	4134	SCYTHE	2023-05-11_14:56:16
9027	2ad2ad16d2ad2ad22c42d42d0000006f254909a73bf62f6b28507e9fb451b5	210.0.220.2	443	HK	9304	SCYTHE	2022-10-02_04:11:51
9080	2ad2ad16d2ad2ad22c42d42d0000006f254909a73bf62f6b28507e9fb451b5	187.72.70.3	443	BR	16735	SCYTHE	2022-10-02_21:44:36
9678	2ad2ad16d2ad2ad22c42d42d0000006f254909a73bf62f6b28507e9fb451b5	187.72.70.3	443	BR	16735	SCYTHE	2022-10-15_18:45:56

CENSYS.IO

- “services.jarm.fingerprint: C2 JARM”
- Or use the Censys ChatGPT search syntax
- Service port 443 – Loads of certificate servers
- Look for duplicates, filter out

C2 JARMS

- “services.jarm.fingerprint: C2 JARM”
- Or use the Censys ChatGPT search syntax
- Service port 443 – Loads of certificate servers
- Look for duplicates, filter out

TOOL C2 RESULTS SUMMARY

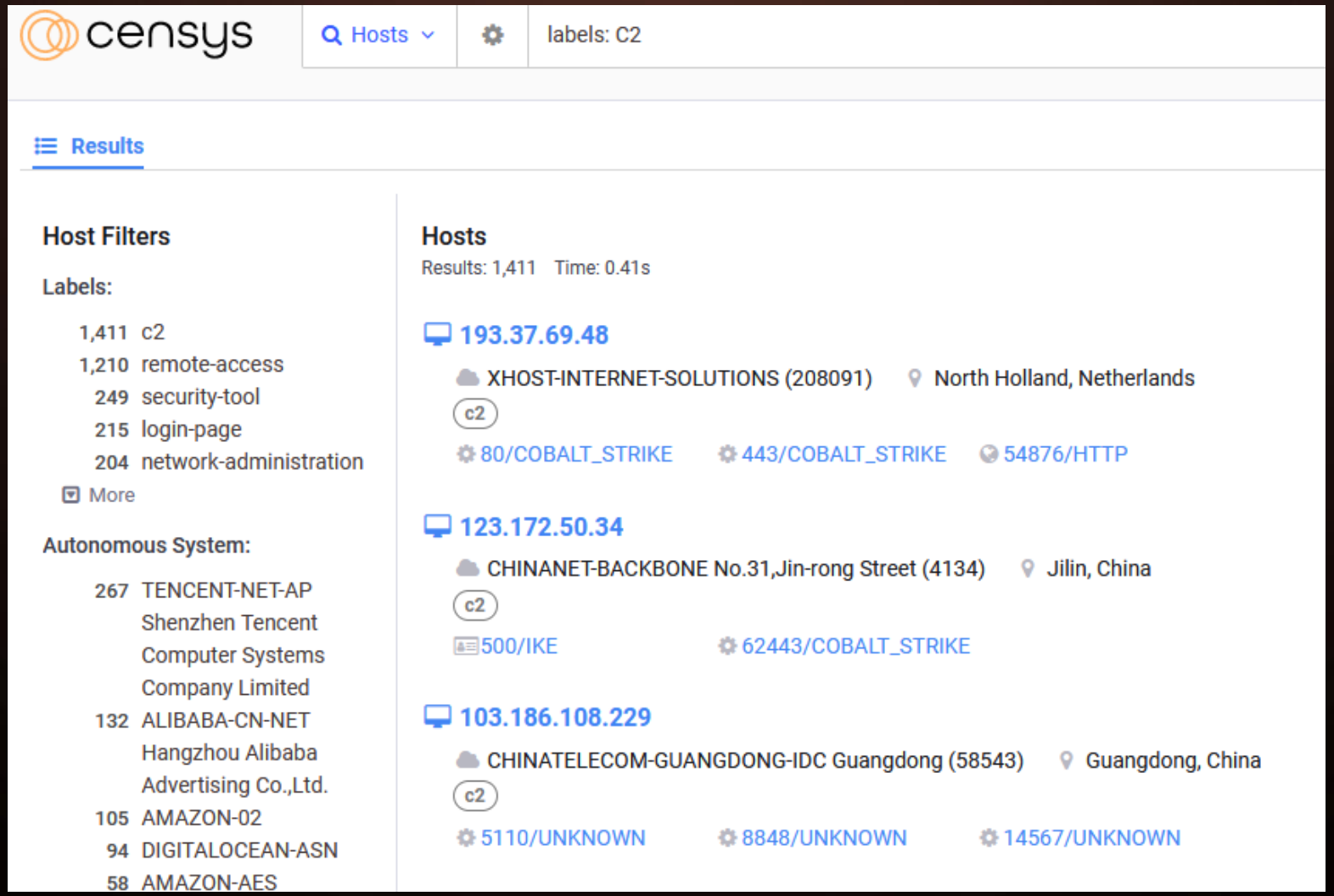
- 40K Remote Access
- 28K File-Sharing
- 26K Database
- 477 IOT
- 12 Scada

- Worldwide
- Many duplicates
- Multi-tennant web hosts
- Hosts listed with multiple tags

TOOL C2 INTERESTING RESULTS

- UK/EU satellite – based precise positioning
- GPS
- Transport
- Construction
- Agriculture
- Cloud
- Widespread
- Lots of exposed systems
- Exploits available

C2 JARMS BY LABELS

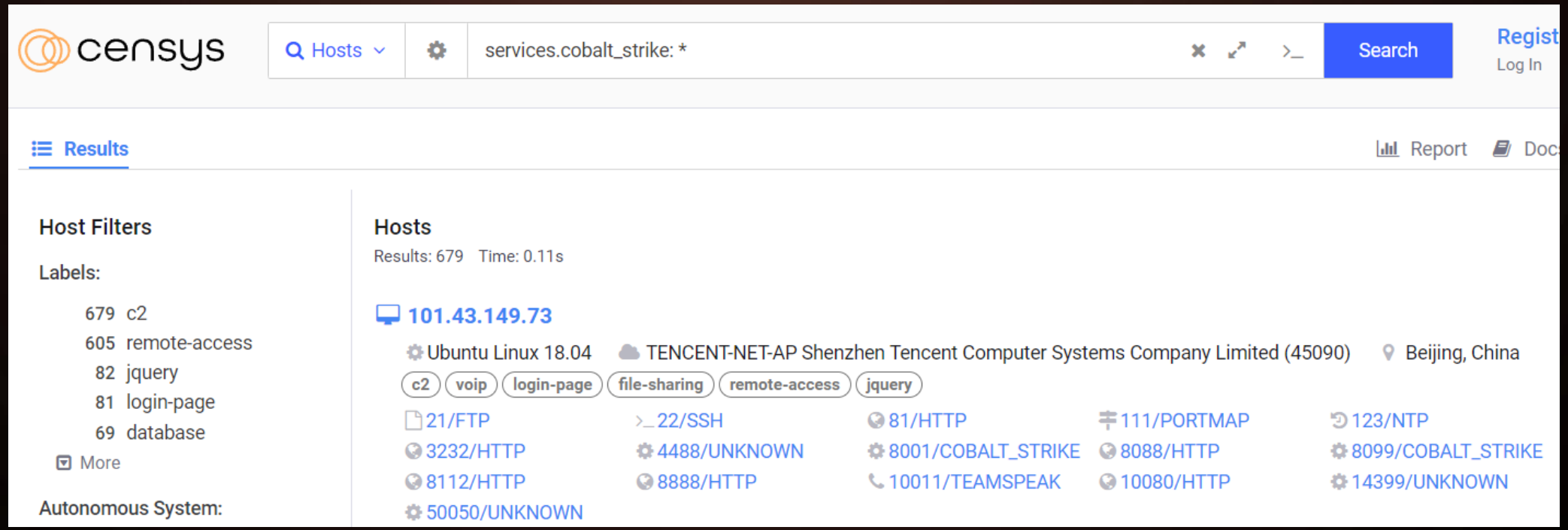


C2 DEMO CERTIFICATE

Certificate

Fingerprint	b662503bdd242f15b22a225ddc0ce72921976cee450a230eb3102f043fb61b40
Subject	C=US, ST=VA, L=Arlington, O=[redacted]E, OU=Engineering, CN=[redacted].test
Issuer	C=US, ST=VA, L=Arlington, O=[redacted]E, OU=Engineering, CN=[redacted].test
Names	[redacted].test

C2 JARMS BY TYPE



C2 JARM LABEL OS REPORT

Report for Hosts

operating_system.product	hosts	
Linux	469	33.24%
linux	391	27.71%
windows	108	7.65%
Windows	84	5.95%
Proxmox	2	0.14%
DSM	1	0.07%
Fireware	1	0.07%
FreeBSD	1	0.07%
Freebox OS	1	0.07%
Linux Kernel	1	0.07%
PIX	1	0.07%
Windows Server 2008 R2	1	0.07%
Windows Server 2012 R2	1	0.07%
Total	**1,411**	**100.0%**

CONCLUSION

- Tool company was unaware
- May the force be with you – Sales Force JARM Github
- Be proactive
- Find naughty things or use for asset tracking
- Make fancy pie charts to show to decision makers

THANK YOU DEFCAMP ROMANIA

- Thanks to everybody with DefCampRO!!!!
- Available for hire
- Hack the World with OSINT & Censys
- Down the Rabbit Hole an OSINT Journey