infoblox®

LAME DELEGATION

SITTING DUCKS FOR CYBERCRIMINALS

Chance Tudor
Threat Researcher

Infoblox Threat Intel

WHAT IS DOMAIN HIJACKING?

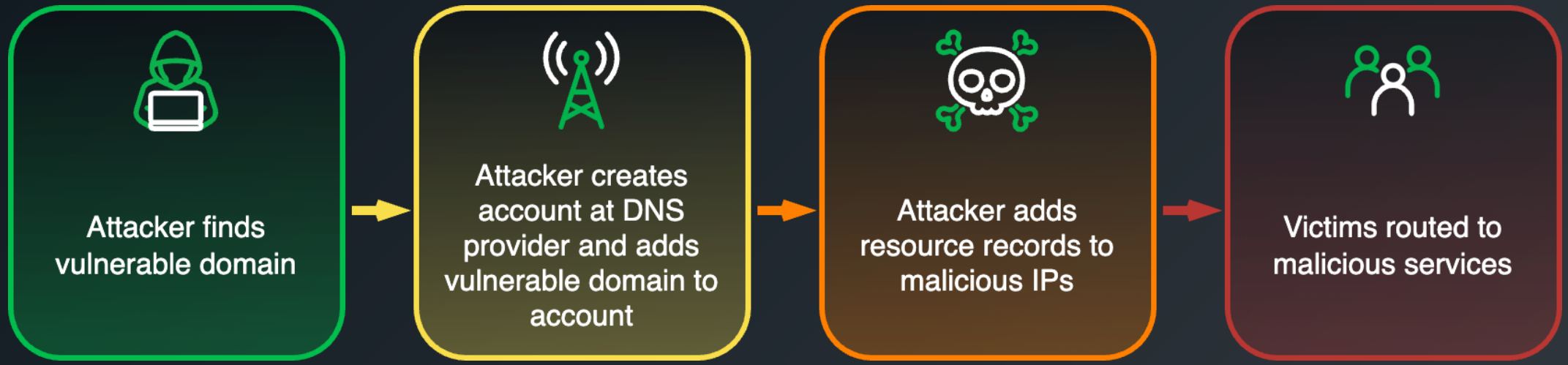
AKA DOMAIN THEFT

- Using unauthorized methods to change the registration of a domain name
- Methods
  - Access at the registrar
  - Access at the name server
  - Access via misconfigurations
- Types
  - Domain shadowing
  - Dangling CNAMEs (and other records)
  - Lame delegation

infoblox.

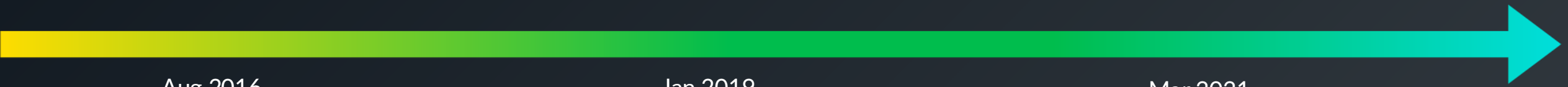
A situation where a DNS server is designated as authoritative for a domain but does not have the proper zone information to answer queries for that domain.

Lame delegation



Sitting Ducks Attack Vector

A HISTORY OF LAME DELEGATION WARNINGS



Aug 2016
"Floating Domains – Taking Over 20K DigitalOcean Domains via a Lax Domain Import System"

- Matt Bryant

Dec 2016
"The Orphaned Internet – Taking Over 120K Domains via a DNS Vulnerability in AWS, Google Cloud, Rackspace and Digital Ocean"

- Matt Bryant

Jan 2019
"Bomb Threat, Sextortion Spammers Abused Weakness at GoDaddy.com"

- Brian Krebs, KrebsOnSecurity

Nov 2020
Notification from Group-IB to Russian authorities

Mar 2021
"The prevalence, persistence, and perils of lame delegations"

- Guatam Akiwate, APNIC

Jun 2024
Sitting Ducks
Infoblox & Eclypsium

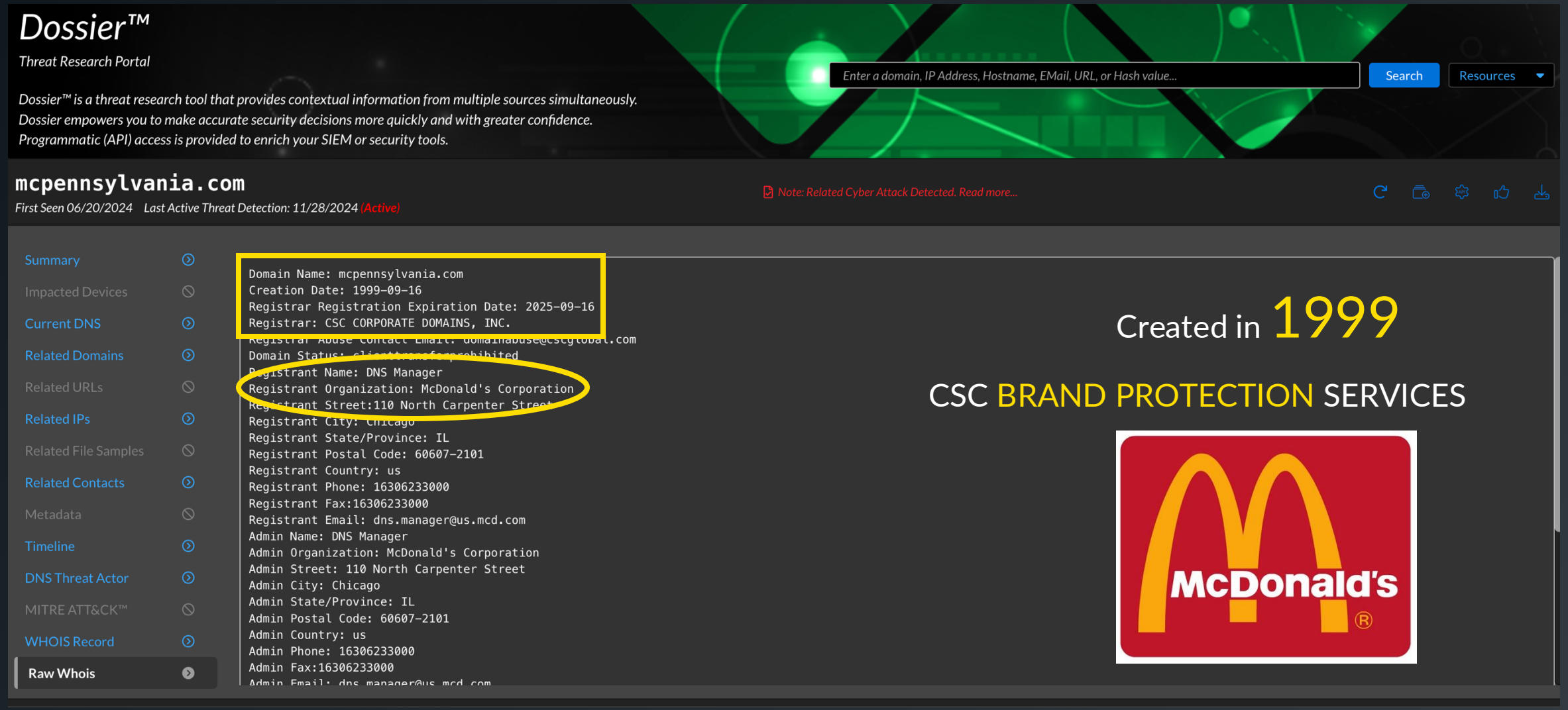
THREAT ACTORS USING SITTING DUCKS

- Over a dozen distinct actors using Sitting Ducks
- Most threat actors have a Russian nexus
- Earliest confirmed hijack is November 2019 by Vacant Viper

VACANT VIPER

- DNS Threat Actor operating 404TDS **(Proofpoint, Feb. 2023)**
  - Uses 404 redirects to deliver malware (DarkGate, AsyncRAT), scams, and phishing
  - Active since Dec 2019, hijacking ~2500 domains/year
  - Abuses DigiCert, DNS Made Easy, and Constellix
  - Targets high-reputation domains; repeated hijacking

MCPENNSYLVANIA[.]COM



Created in 1999

CSC BRAND PROTECTION SERVICES

infoblox

MCPENNSYLVANIA[.]COM

IP Address History

Event Date	Action	Pre-Action IP	Post-Action IP
2005-03-05	New	-none-	24.225.7.105
2007-09-23	Change	24.225.7.105	74.205.90.114
2007-10-21	Not Resolvable	74.205.90.114	-none-
2007-10-21	Not Resolvable	74.205.90.114	-none-
2011-04-10	New	-none-	74.205.90.114
2015-08-04	Change	74.205.90.114	54.235.159.97
2016-02-14	Change	54.235.159.97	52.70.175.181
2016-09-09	Change	52.70.175.181	107.170.2.22
2017-04-23	Change	107.170.2.22	127.0.0.1
2017-07-26	Not Resolvable	127.0.0.1	-none-
2022-10-28	New	-none-	45.136.49.35
2022-11-18	Change	45.136.49.35	157.230.67.179
2023-02-12	Not Resolvable	157.230.67.179	-none-
2023-06-20	New	-none-	34.102.136.181
2023-06-27	Change	34.102.136.181	193.3.19.220
2023-08-26	Not Resolvable	193.3.19.220	-none-
2023-11-13	New	-none-	95.216.35.61
2024-01-10	Change	95.216.35.61	157.230.67.179
2024-04-09	Not Resolvable	157.230.67.179	-none-
2024-12-07	New	-none-	44.208.147.61
2024-12-10	Change	44.208.147.61	40.76.41.180

Name Server History

Event Date	Action	Pre-Action Server	Post-Action Server
2002-04-05	Transfer	Verio.net	Eagleinteractive.net
2003-08-04	Transfer	Eagleinteractive.net	Eaglecable.net
2004-01-01	Transfer	Eaglecable.net	Ruraltel.com
2007-09-17	Transfer	Ruraltel.com	Dnsmadeeasy.com
2024-12-08	Transfer	Dnsmadeeasy.com	Cscdns.net

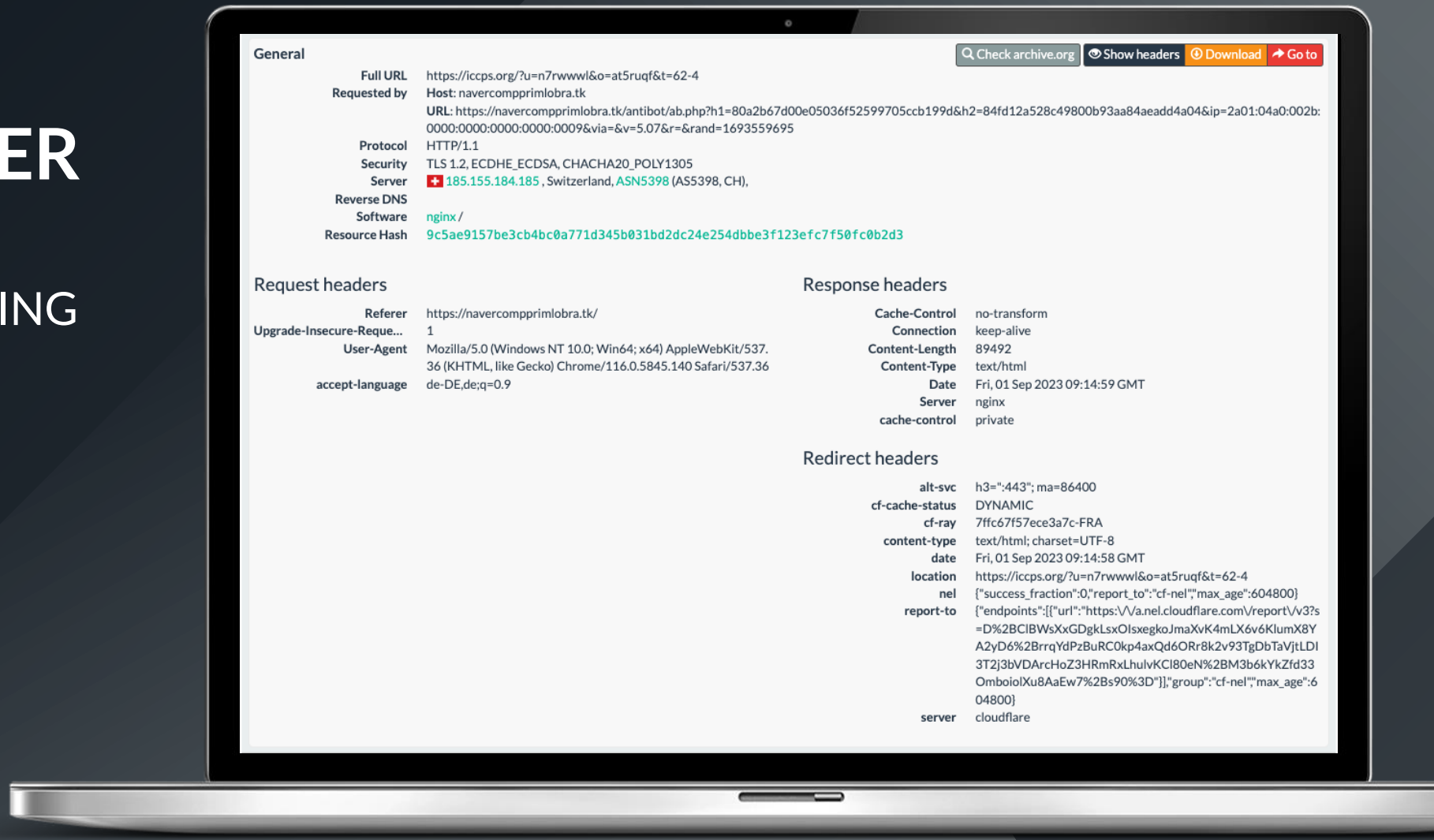
Credit: DomainTools (https://research.domaintools.com/research/hosting-history/?q=mcpennsylvania%5B.%5Dcom)

VEXTRIO VIPER

- DNS Threat Actor operating large criminal enterprise to deliver malware, scams, and illegal content
- Active since at least 2017
- Uses hijacked domains in their TDS similarly to Vacant Viper
  - Hijacks lame domains once delegated to DigiCert/DNS Made Easy (DME), Constellix, and DigitalOcean
- Over 65 known affiliate partners, some of whom also hijack domains via Sitting Ducks
  - ClearFake, SocGholish

VEXTRIO VIPER

ICCPS[.]ORG HIJACKING

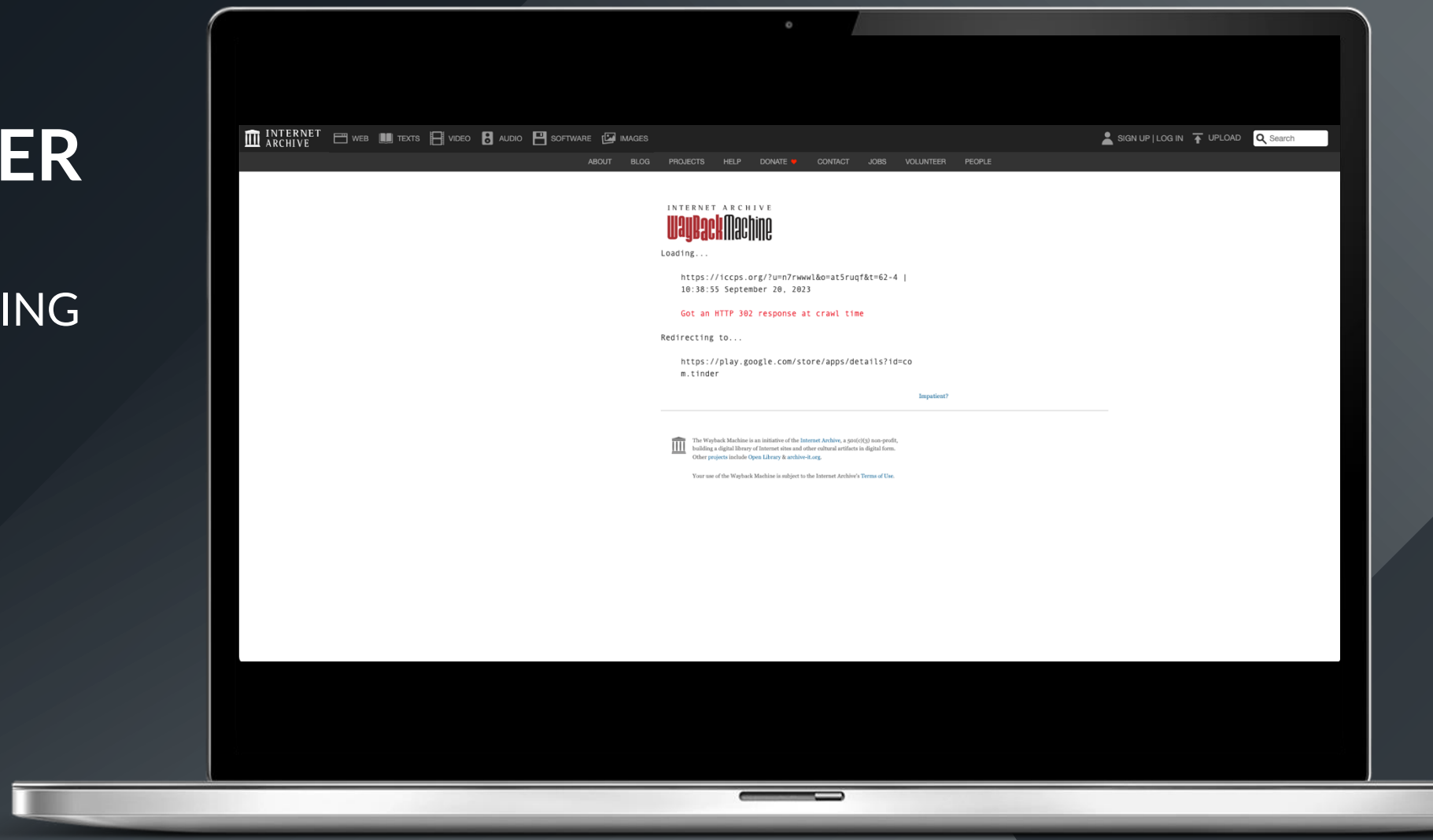


Credit: URLScan (https://urlscan.io/result/e6f9255f-9ce2-4bf7-833e-3d4bc05d65c3/#transactions)

infoblox

VEXTRIO VIPER

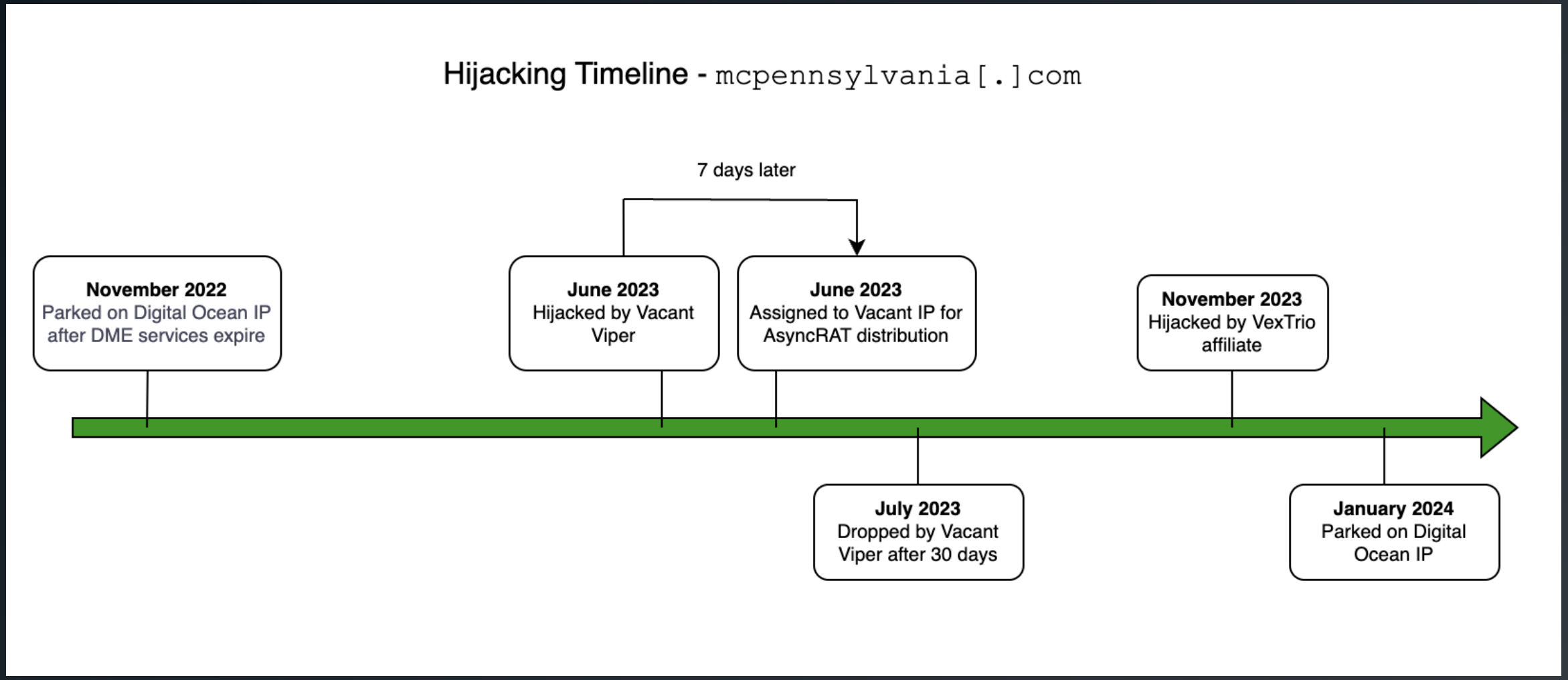
ICCPS[.]ORG HIJACKING



Credit: Internet Archive (https://web.archive.org/web/20250000000000*/https://iccps.org/?u=n7rwwwl&o=at5ruqf&t=62-4)

infoblox

ROTATIONAL HIJACKING



infoblox

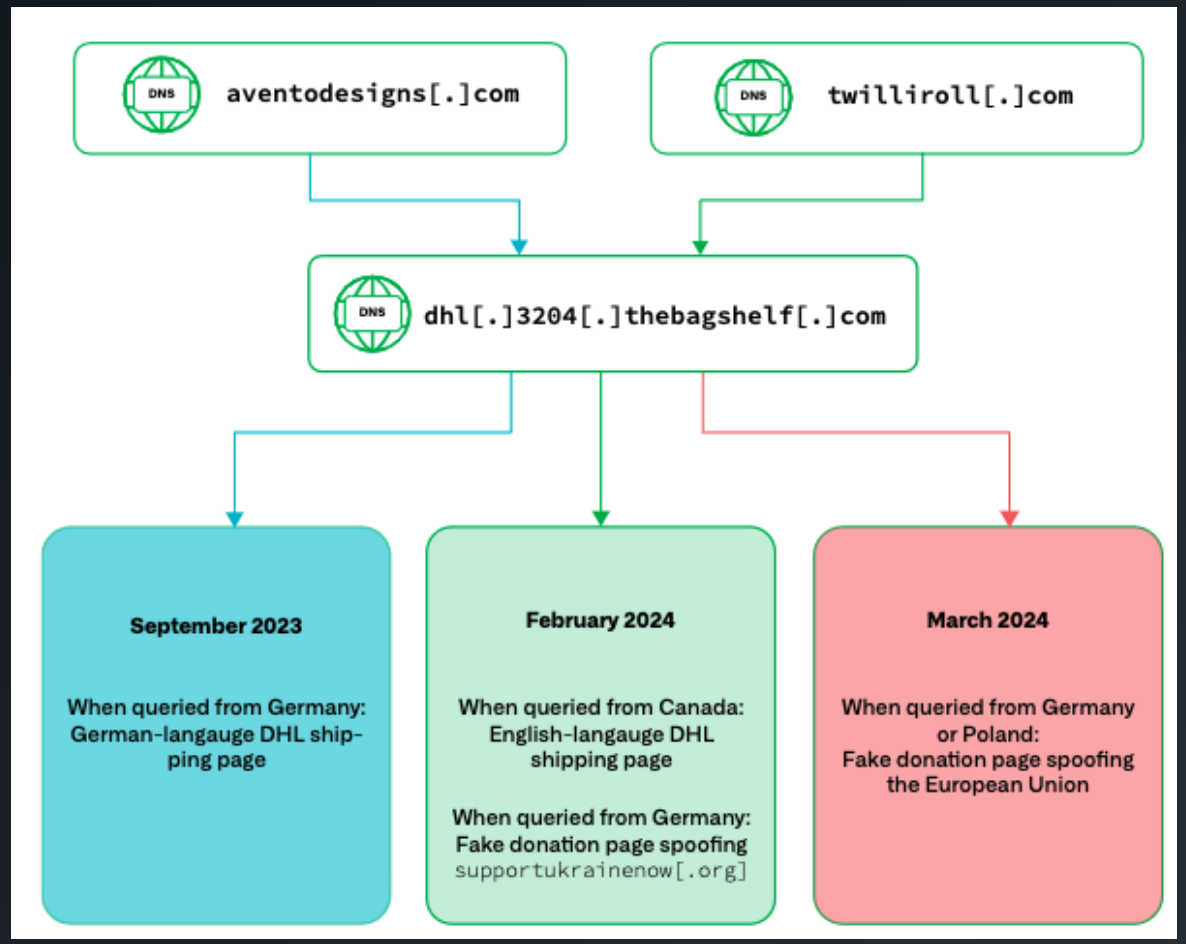
HORRID HAWK

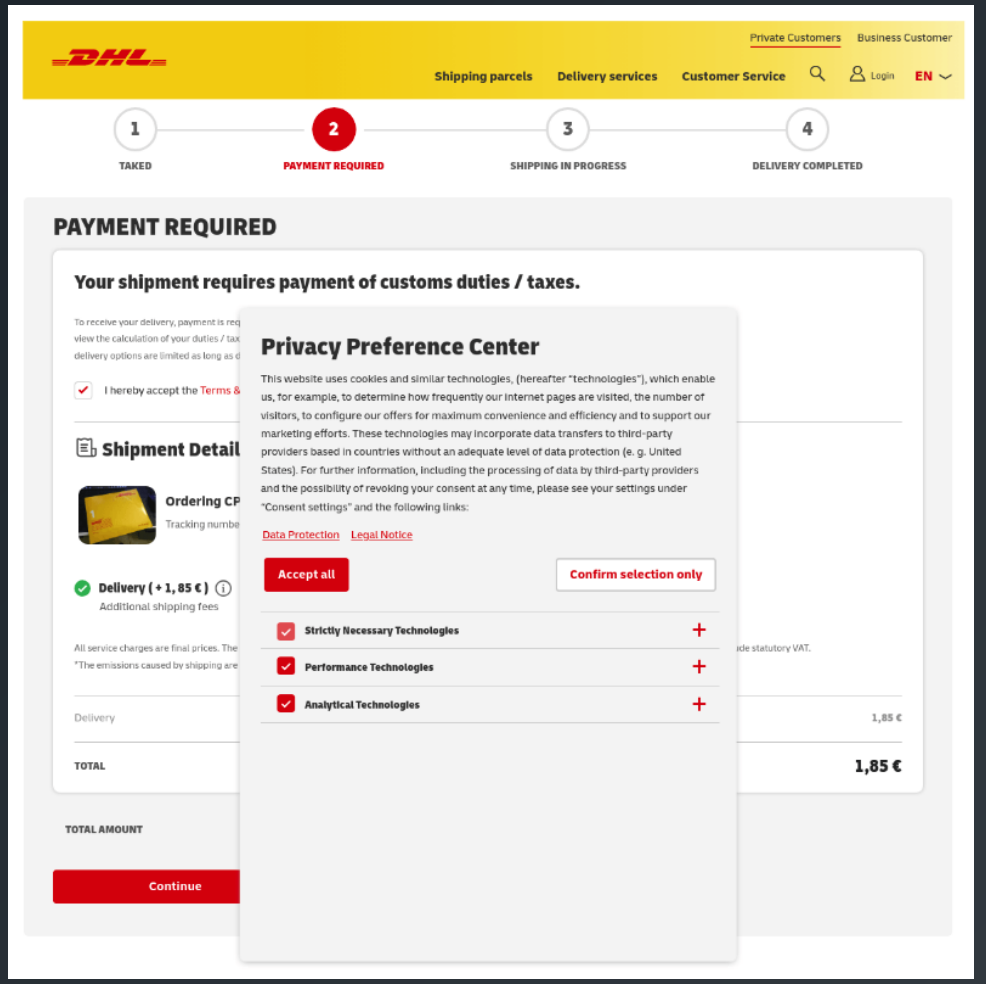
- Conducting large-scale investment fraud scams since February 2023
  - Nearly 5k domains hijacked
- Embeds hijacked domains in Facebook ads targeting users in over 30 languages
- Uses TDS to profile potential victims, filter out security researchers & bots
- Exploiting multiple DNS and web hosting providers
  - Linode, TierraNet, A2 Hosting

HASTY HAWK

- Conducting widespread phishing campaigns since March 2022
  - Spoofs DHL shipping pages and fake Ukrainian donation sites
- Over 200 hijacked domains
  - HawkHost, Maria Hosting, Digital Ocean
  - Reconfigured to host content on Russian IP space

HASTY HAWK





DNS PREDATORS ATTACK: VIPERS AND HAWKS HIJACK SITTING DUCKS DOMAINS (November 2024)

infoblox

PREVENTING LAME DELEGATION HIJACKS

Domain owners should audit and create delegations for all owned zones

- Create zone file config, or
- Change primary and secondary NS to the registrar's or use dummy placeholders

Providers use dynamically assigned NS from a large pool when adding a zone to a DNS provider

- Requires access to registrar to make sure they match

Registrar could test for lame delegations and modify NS records to placeholders

THANK YOU!

Infoblox Threat Intel

www.infoblox.com/threat-intel/

TALK TO US ON MASTODON

infobloxthreatintel@infosec.exchange

GET OUR RESEARCH

infoblox.