paloalto NETWORKS

AI in Web and DNS Security

Janos Szurdi

Outline

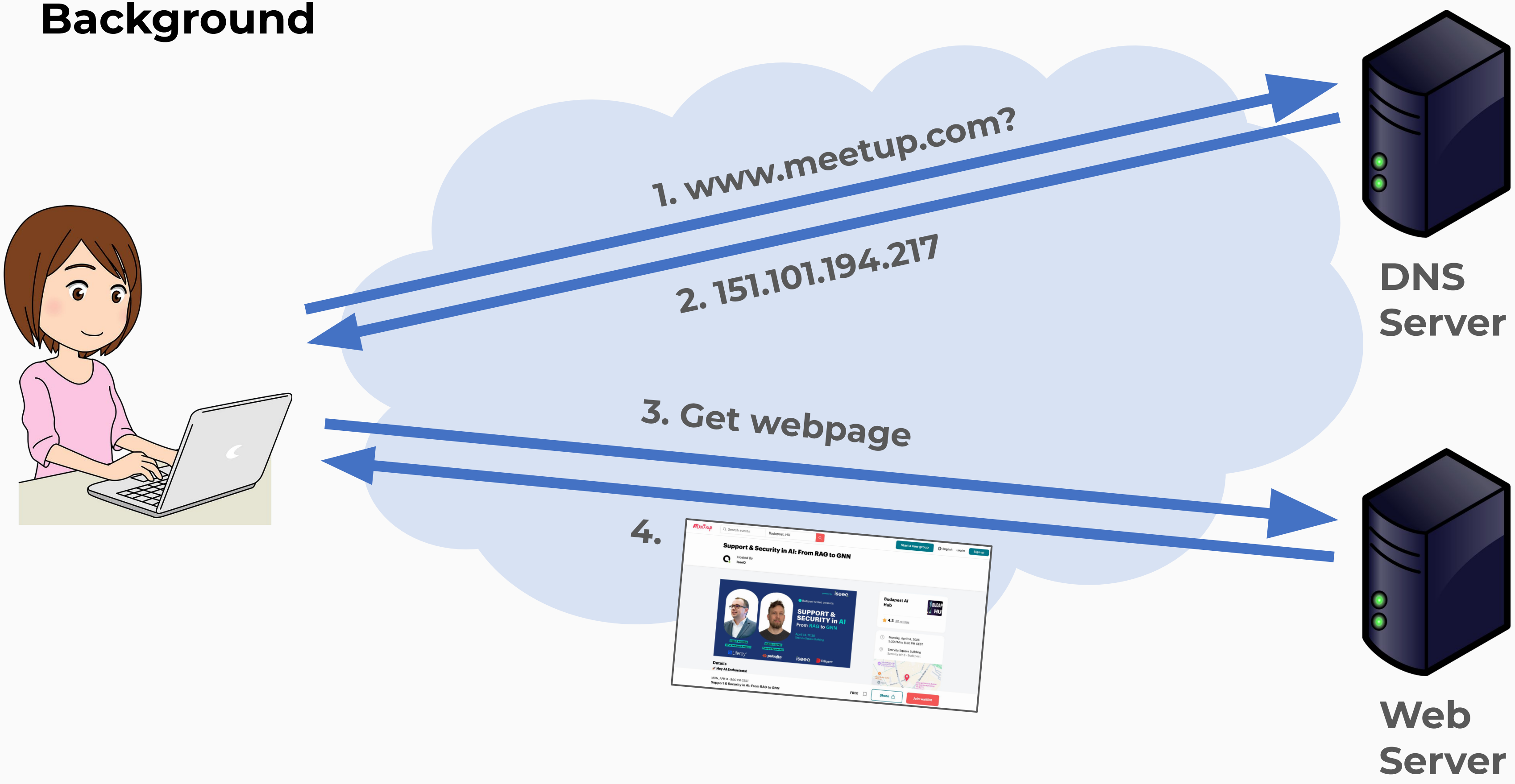
1. Examples of threats we detect using AI

2. Deep Dive 1: knowledge graphs and graph neural networks (GNNs) to proactively find malicious infrastructure

   a. Lead: **Nabeel Mohamed**

3. Deep Dive 2: finding domain hijacking in big datasets

Background



Meetup

Search events

Budapest, HU

Start a new group

English

Log in

Sign up

Support & Security in AI: From RAG to GNN

Hosted By
IseeQ

powered by iseeq

Budapest AI Hub presents:

SUPPORT & SECURITY in AI
From RAG to GNN

April 14, 17:30
Szervita Square Building

ZSOLT BALOGH
VP of Technology & Support

JANOS SZURDI
Principal Researcher

Liferay

paloalto

iseeq

Diligent

Budapest AI Hub

4.3 30 ratings

Monday, April 14, 2025
5:30 PM to 8:30 PM CEST

Szervita Square Building
Szervita tér 8 · Budapest

Details

🚀 Hey AI Enthusiasts!

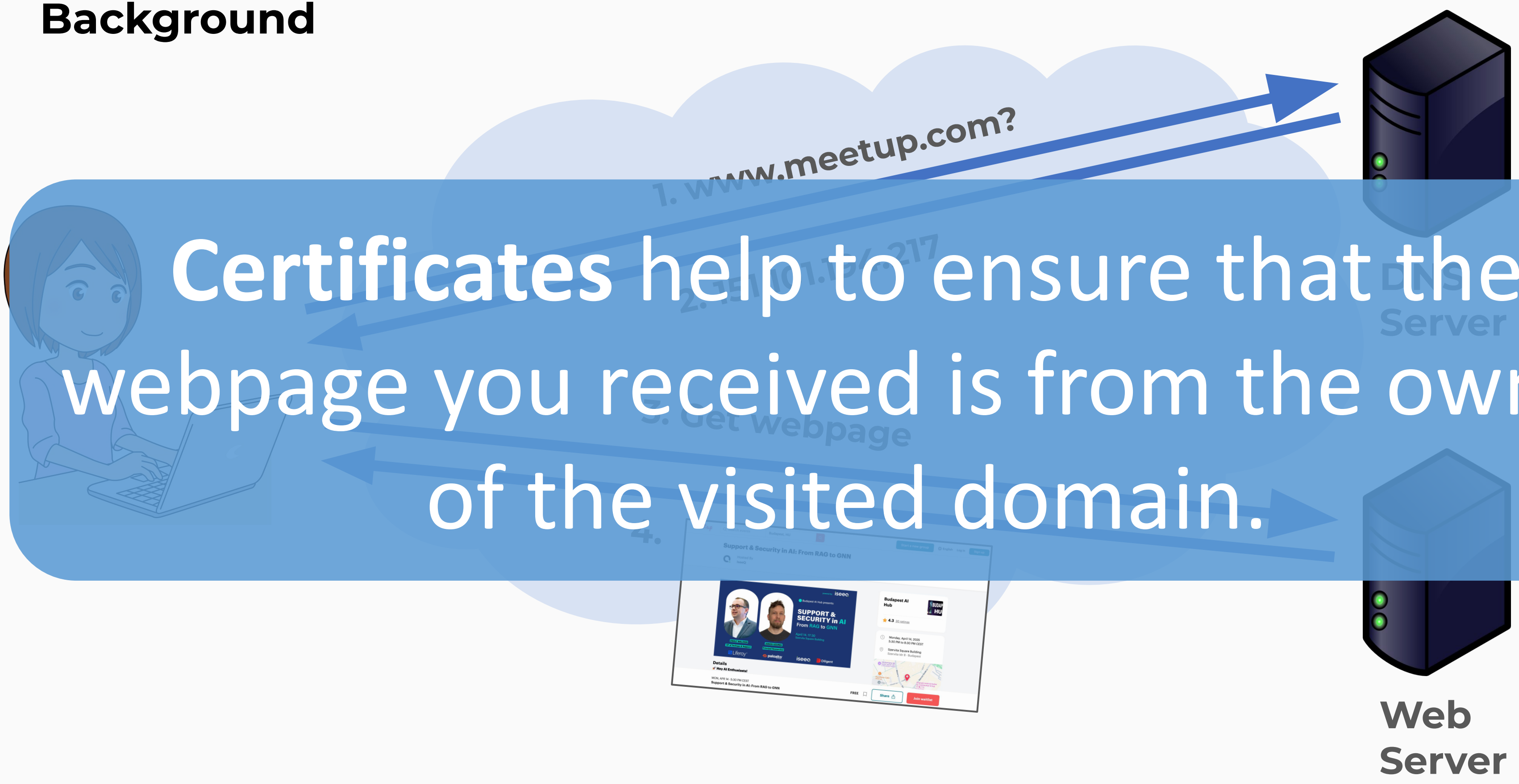
MON, APR 14 · 5:30 PM CEST
Support & Security in AI: From RAG to GNN

FREE

Share

Join waitlist

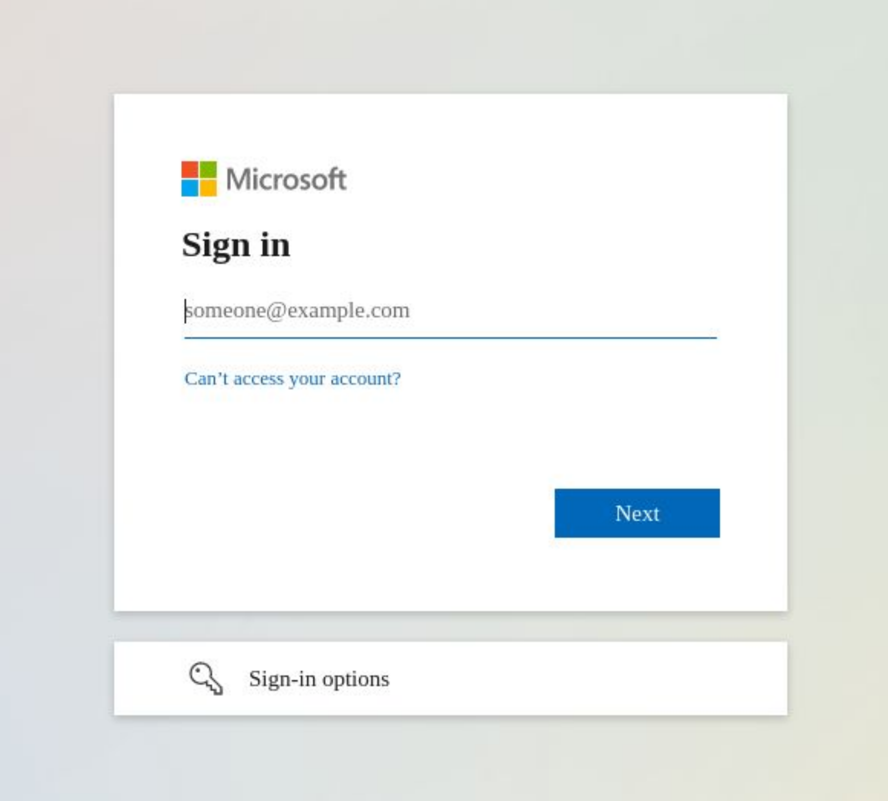
Background



Certificates help to ensure that the webpage you received is from the owner of the visited domain.

Domain Wars

Hijacked Domain Redirecting to a Phishing Page



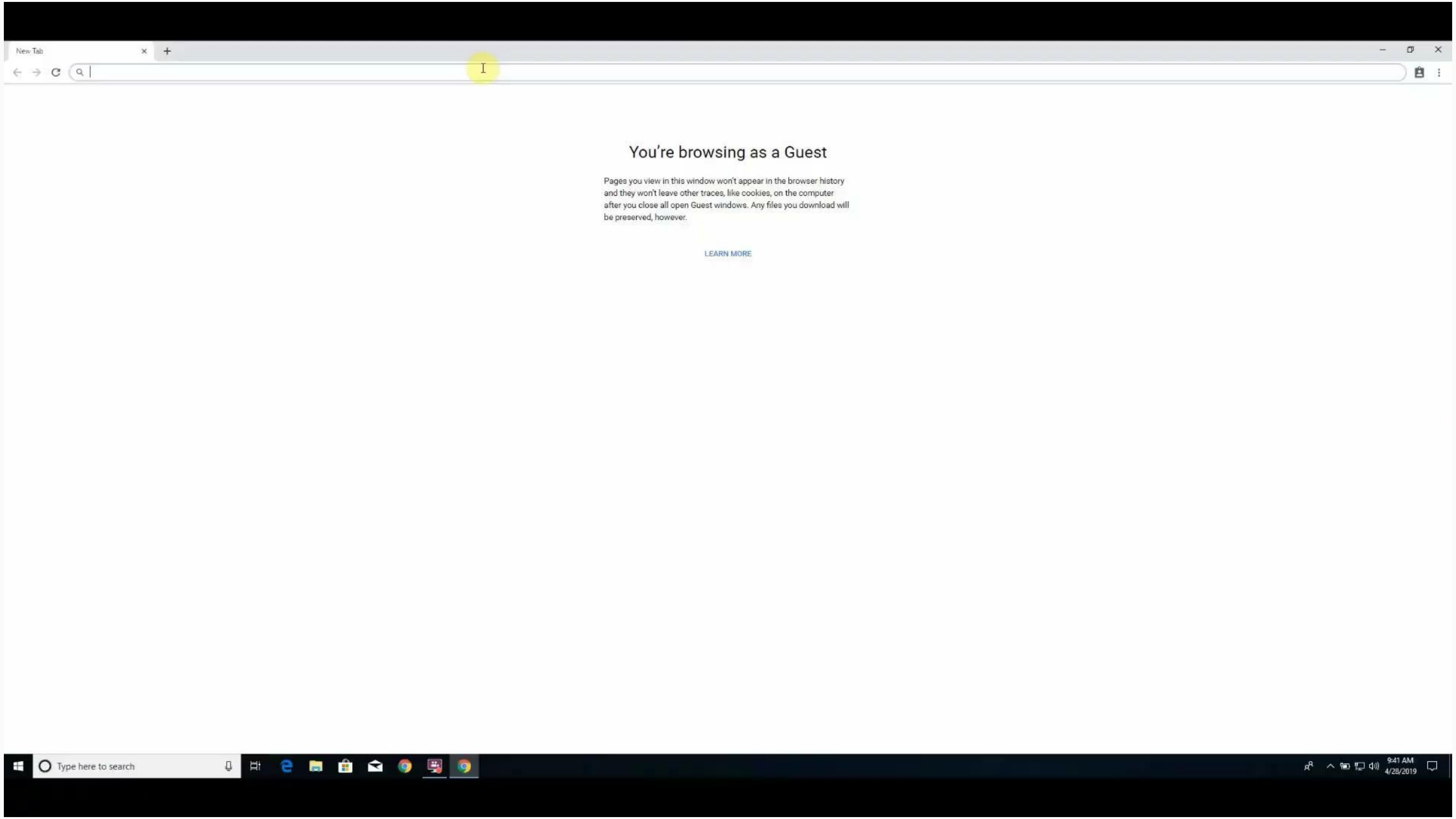
Microsoft

Sign in

someone@example.com

Can’t access your account?

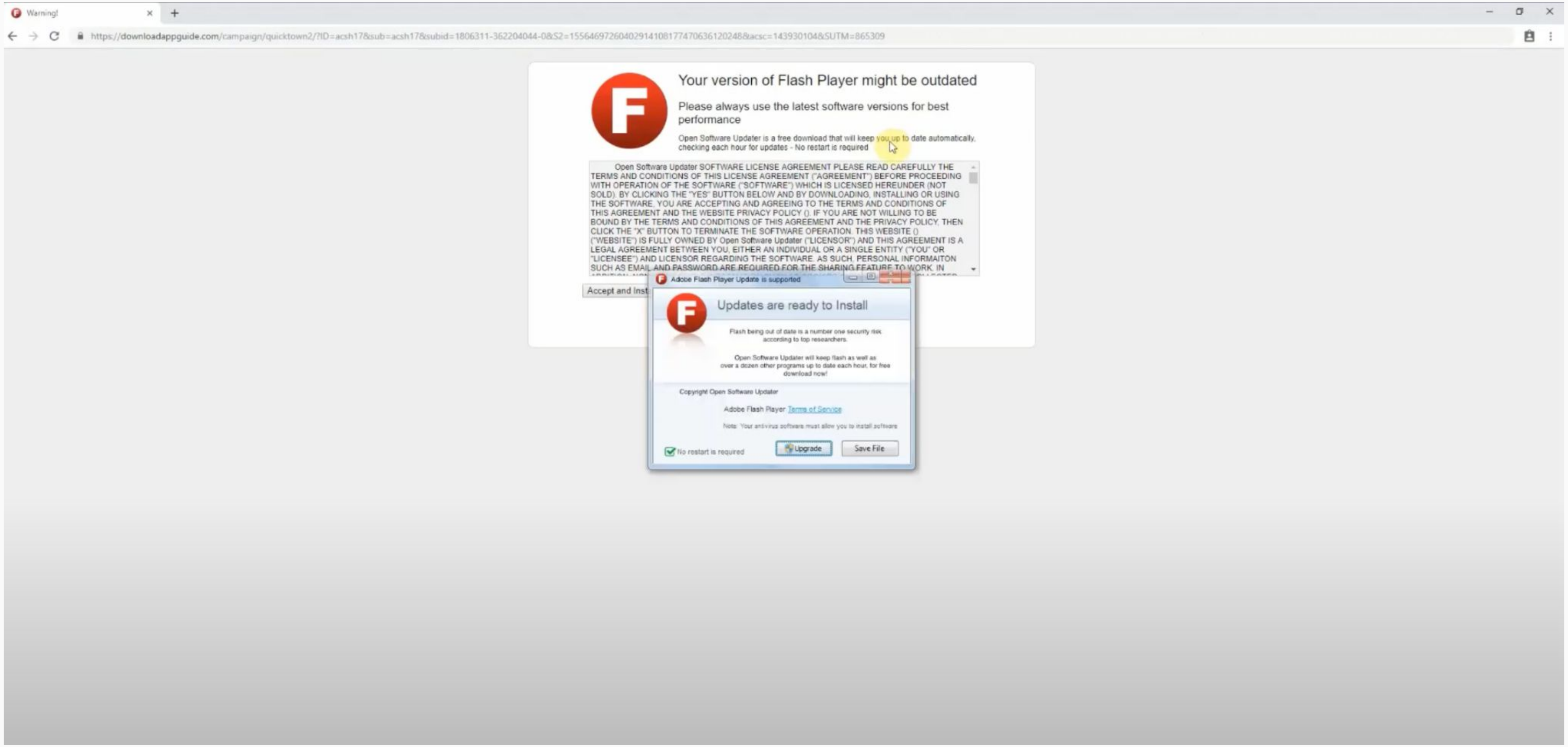
Typosquatting: steampowerTed.com - Malicious Download



You're browsing as a Guest

Pages you view in this window won't appear in the browser history and they won't leave other traces, like cookies, on the computer after you close all open Guest windows. Any files you download will be preserved, however.

Typosquatting: steampowerTed.com - Malicious Download


Warning!
https://downloadappguide.com/campaign/quicktown2/?ID=acsh17&sub=acsh17&subid=1806311-362204044-0&S2=15564697260402914108177470636120248&acsc=143930104&SUTM=865309
Accept and Inst
Adobe Flash Player Update is supported
Upgrade
Save File

Your version of Flash Player might be outdated

Please always use the latest software versions for best performance

Open Software Updater is a free download that will keep you up to date automatically, checking each hour for updates - No restart is required

Open Software Updater SOFTWARE LICENSE AGREEMENT PLEASE READ CAREFULLY THE TERMS AND CONDITIONS OF THIS LICENSE AGREEMENT ("AGREEMENT") BEFORE PROCEEDING WITH OPERATION OF THE SOFTWARE ("SOFTWARE") WHICH IS LICENSED HEREUNDER (NOT SOLD). BY CLICKING THE "YES" BUTTON BELOW AND BY DOWNLOADING, INSTALLING OR USING THE SOFTWARE, YOU ARE ACCEPTING AND AGREEING TO THE TERMS AND CONDITIONS OF THIS AGREEMENT AND THE WEBSITE PRIVACY POLICY (). IF YOU ARE NOT WILLING TO BE BOUND BY THE TERMS AND CONDITIONS OF THIS AGREEMENT AND THE PRIVACY POLICY, THEN CLICK THE "X" BUTTON TO TERMINATE THE SOFTWARE OPERATION. THIS WEBSITE () ("WEBSITE") IS FULLY OWNED BY Open Software Updater ("LICENSOR") AND THIS AGREEMENT IS A LEGAL AGREEMENT BETWEEN YOU, EITHER AN INDIVIDUAL OR A SINGLE ENTITY ("YOU" OR "LICENSEE") AND LICENSOR REGARDING THE SOFTWARE. AS SUCH, PERSONAL INFORMAITON SUCH AS EMAIL AND PASSWORD ARE REQUIRED FOR THE SHARING FEATURE TO WORK. IN

Updates are ready to Install

Flash being out of date is a number one security risk according to top researchers.

Open Software Updater will keep flash as well as over a dozen other programs up to date each hour, for free download now!

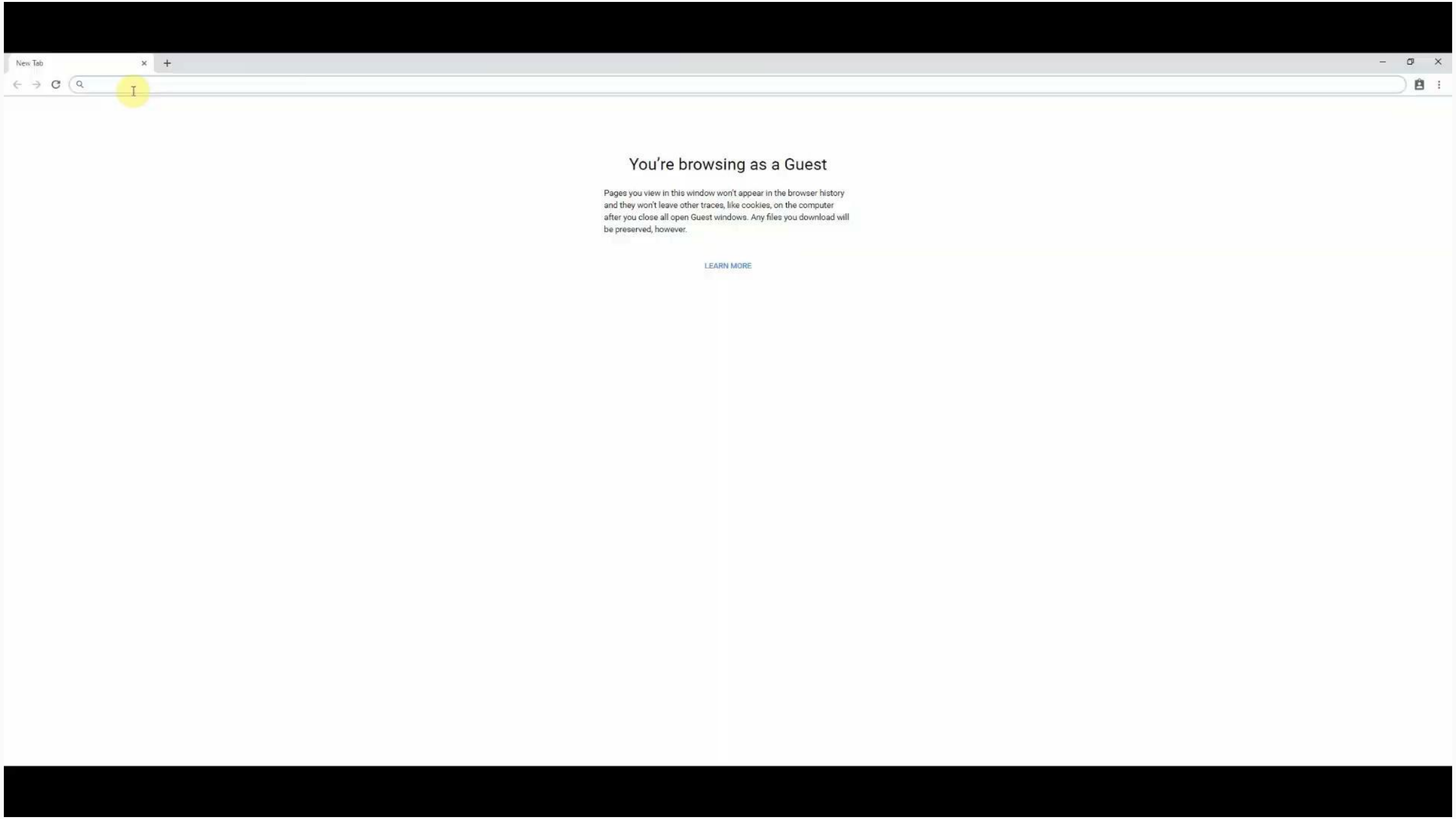
Copyright Open Software Updater

Adobe Flash Player Terms of Service

Note: Your antivirus software must allow you to install software

☑ No restart is required

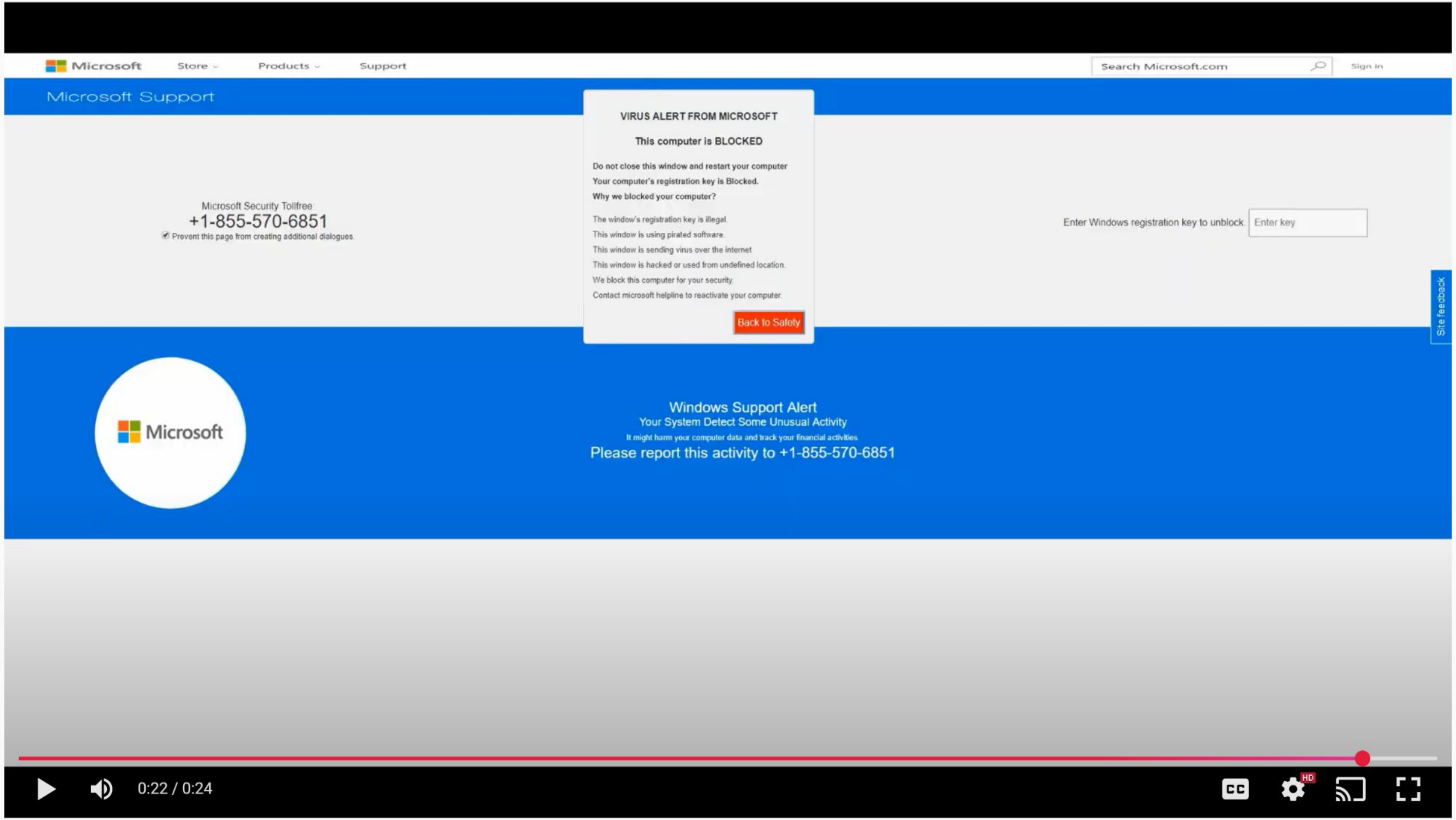
Typosquatting: steampowerTed.com - Scam Page



You're browsing as a Guest

Pages you view in this window won't appear in the browser history and they won't leave other traces, like cookies, on the computer after you close all open Guest windows. Any files you download will be preserved, however.

Typosquatting: steampowerTed.com - Scam Page



Microsoft Security Tollfree:
+1-855-570-6851

☑ Prevent this page from creating additional dialogues.

VIRUS ALERT FROM MICROSOFT

This computer is BLOCKED

Do not close this window and restart your computer
Your computer's registration key is Blocked.
Why we blocked your computer?

The window's registration key is illegal.
This window is using pirated software.
This window is sending virus over the internet
This window is hacked or used from undefined location.
We block this computer for your security.
Contact microsoft helpline to reactivate your computer.

Back to Safety

Enter Windows registration key to unblock: Enter key

Windows Support Alert
Your System Detect Some Unusual Activity
It might harm your computer data and track your financial activities.
Please report this activity to +1-855-570-6851

Dictionary DGA Domains

Customer 1 DNS Requests

azure.bingads.trafficmanager.net
warningscapable.space
google.com
ferrum.network
files.slack.com
resources.xg4ken.com
bbc.co.uk
pendingsuggestaffliction.com
www.youtube.com
physicsseparately.com
announcedvillainvaluable.com
bradstones.ca
sqm.microsoft.com
telex.hu
facebook.com
sdk.privacy-center.org

Customer 2 DNS Requests

api.office.netd
account.bbc.com
waitfree.net
login.windows.net
warningscapable.space
r3.o.lencr.org
autodiscover-s.outlook.com
whetherdirect.net
i.hootsuite.com
e1723.dscd.akamaiedge.net
cdn.onenote.net
fallfree.net
pendingsuggestaffliction.com
verythere.gq
thrashermagazine.com
files.slack.com

Unit 42 Blogs

- **Cybersquatting:** Attackers Mimicking Domains of Major Brands

- Beneath the Surface: Detecting and Blocking **Hidden Malicious Traffic Distribution Systems**

Strategically Aged Domains

Why strategically aged domain matters?

Advanced persistent threats are increasingly **stockpiling domains** with **high reputation** to **evade security vendors** in order to carry out attacks including **phishing** and stealthy **data exfiltration**

Strategically Aged Domains

Domains reserved and left dormant for months or years before use to bypass security vendor reputation checks

Register new domain

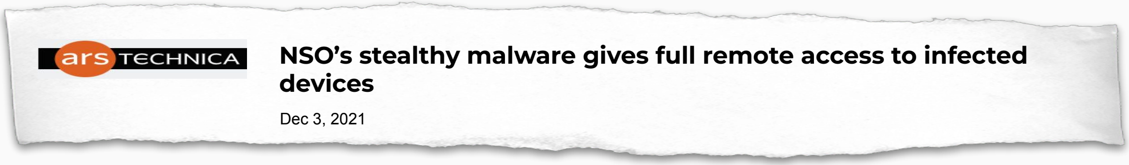
Wait months or years before use

Use aged domain in targeted attack

Every day, **~30K** domains that have been dormant for months or years gain **>10.3 times** more traffic within one day

~22.27% of the domains are malicious or suspicious

Case Study: Pegasus Spyware Campaign

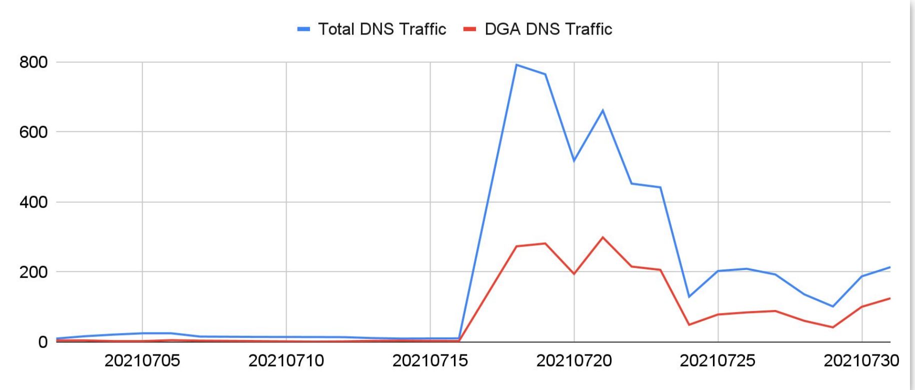


ars TECHNICA

NSO's stealthy malware gives full remote access to infected devices

Dec 3, 2021

- **Two command & control (C2) domains** registered in 2019
- Domains aged for **two years**
- Became active around July 2021 with daily DNS traffic spiking **56x times**
- Use of subdomains generated by **domain generation algorithms (DGA)** to carry C2 traffic



Unit 42 Blogs

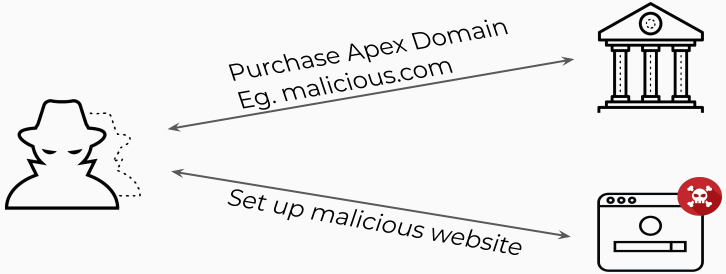
- **Strategically Aged Domain Detection:** Capture APT Attacks With DNS Traffic Trends

- **Toward Ending the Domain Wars:** Early Detection of Malicious Stockpiled Domains

Compromised DNS Zones

Why do attackers use compromised domains?

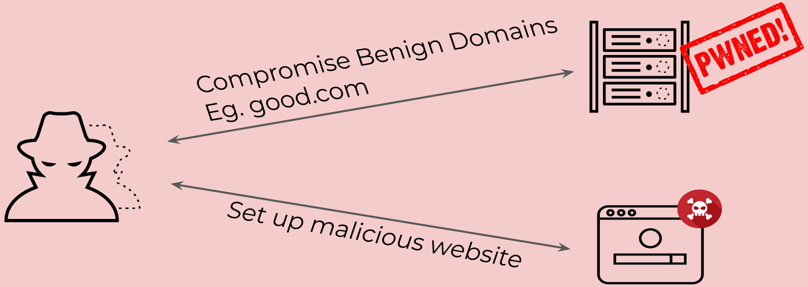
Modus Operandi



Cons:

- Bad domain reputation
- Malicious domain name patterns
- Suspicious traffic behavior

Domain Shadowing



Pros:

- Inherit the reputation of the compromised legitimate domains
- Infinite beguiling subdomain names
- Low cost

Case Study: Microsoft Cred Phishing Campaign

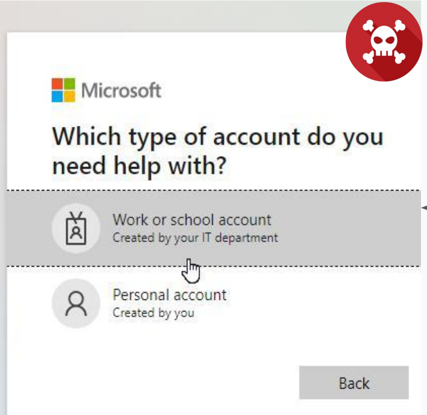
Phishing Email

Initial
Phishing Link

snaitechbumxzzwt.barwonbluff[.]com.au

- **62.204.41.247 (RU)**

Redirect



Microsoft

Which type of account do you need help with?

Work or school account
Created by your IT department

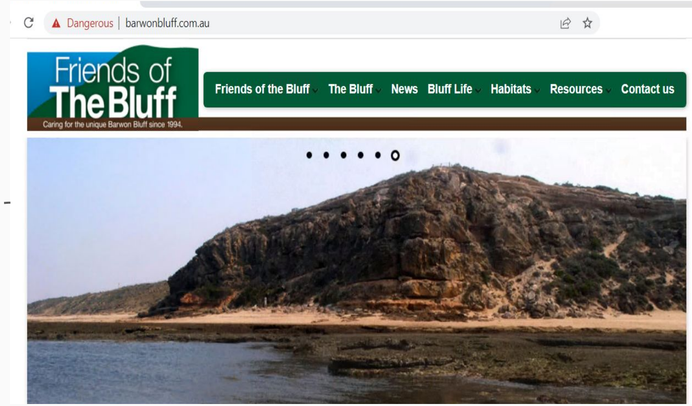
Personal account
Created by you

Back

Landing Page Stealing Microsoft Creds

- *login.elitepackagingblog[.]com*
- **62.204.41.191 (RU)**

Home
Page



barwonbluff[.]com.au

- **27.131.74.5 (AU)**
- Active since 2003, Used to be in Alexa Top list in 2018

IP

62.204.41.0/24

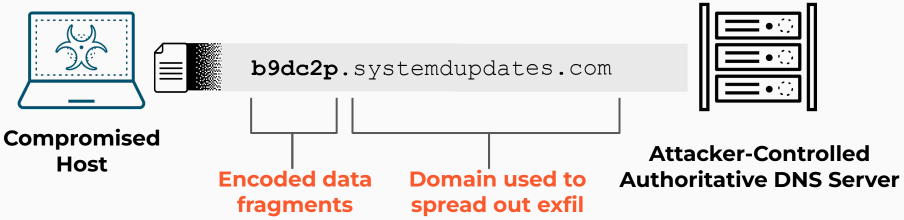
ocwdvmjjj78krus.halont.edu[.]au
carriernhoousvz.brisbanegateway[.]com …

Unit 42 Blogs

- **Domain Shadowing:** A Stealthy Use of DNS Compromise for Cybercrime
- **Automatically Detecting DNS Hijacking in Passive DNS**

DNS Tunneling

Covert Communication over DNS



Compromised Host

`b9dc2p.systemdupdates.com`

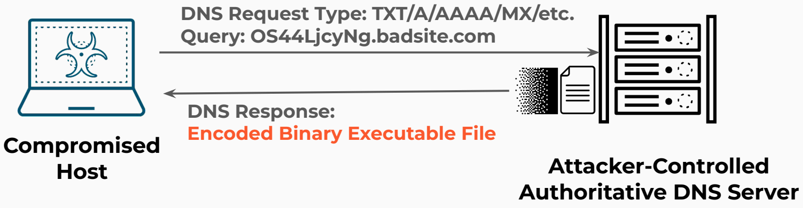
Encoded data fragments

Domain used to spread out exfil

Attacker-Controlled Authoritative DNS Server

DNS Exfiltration

Attackers can leverage DNS to exfiltrate the stolen data



DNS Request Type: TXT/A/AAAA/MX/etc.
Query: OS44LjcyNg.badsite.com

DNS Response:
Encoded Binary Executable File

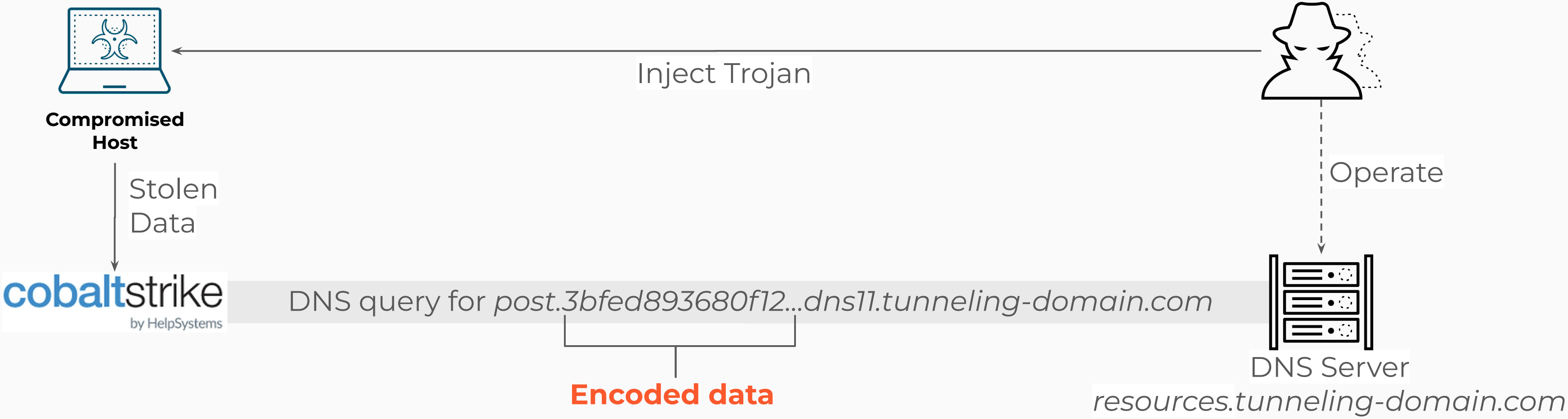
Compromised Host

Attacker-Controlled Authoritative DNS Server

DNS Infiltration

Attackers can leverage DNS to download malicious payload to facilitate next steps

Case Study: Cobalt Strike Exfiltration


Inject Trojan
Compromised Host
Stolen Data
Operate
cobaltstrike by HelpSystems
DNS query for *post.3bfed893680f12...dns11.tunneling-domain.com*
Encoded data
DNS Server
resources.tunneling-domain.com

- Cobalt Strike is a commercial command & control (C2) application. It’s widely used in penetration tests and attacking campaigns.
- The tunneling domain was registered on July 7, 2021 and carried data exfiltration traffic on March 24, 2022.
- DNS Security blocked ~4KB data exfiltration through 112 DNS requests.

Unit 42 Blogs

- Understanding DNS Tunneling Traffic in the Wild

- Leveraging DNS Tunneling for Tracking and Scanning

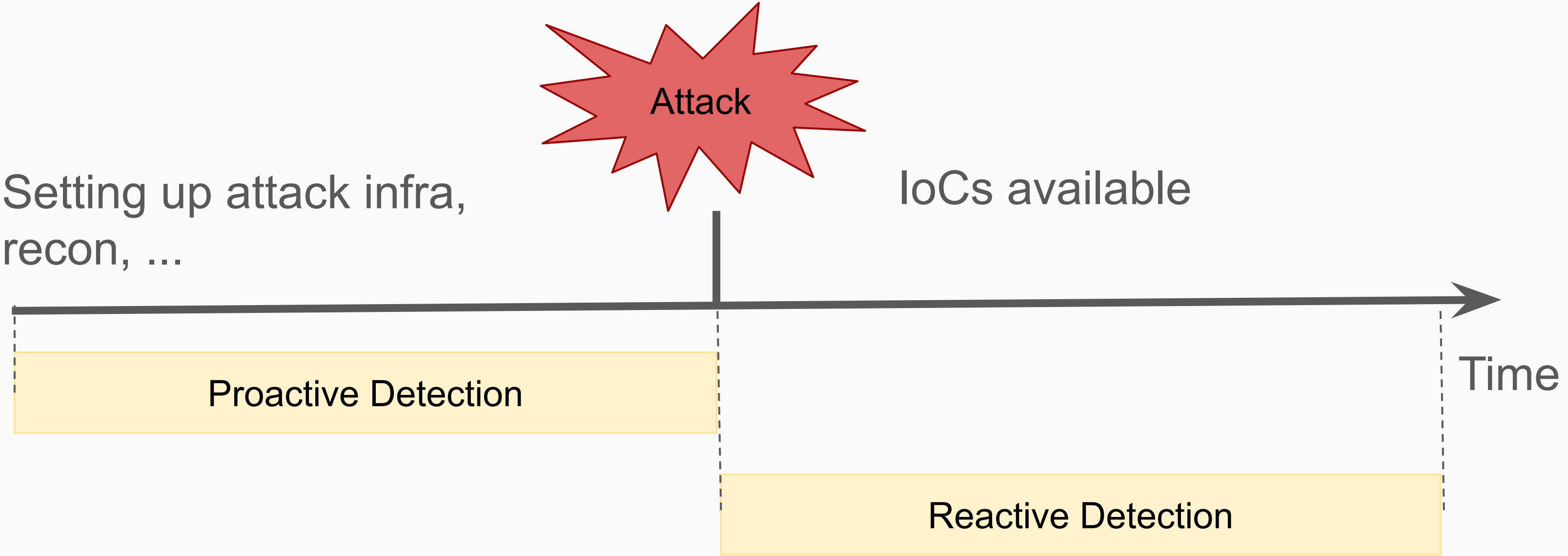
Proactively hunting for low-reputed infrastructure used by large cybercrimes and APTs

Outline

- Motivation with examples
- Methodology
  - Knowledge graph construction
  - Graph AI learner
- Case studies

Introduction

- Reactive: Currently, a lot of attacks are detected ***after*** they are launched
- Proactive: Can we detect attacks ***before*** *they are launched* or ***early*** during the attack?



Observations

Attackers often

- **Rotate** their attack infrastructure (domains, IPs, file hashes, certificates)
- **Automate** hosting related activities
- **Reuse or share** the same attack infrastructure

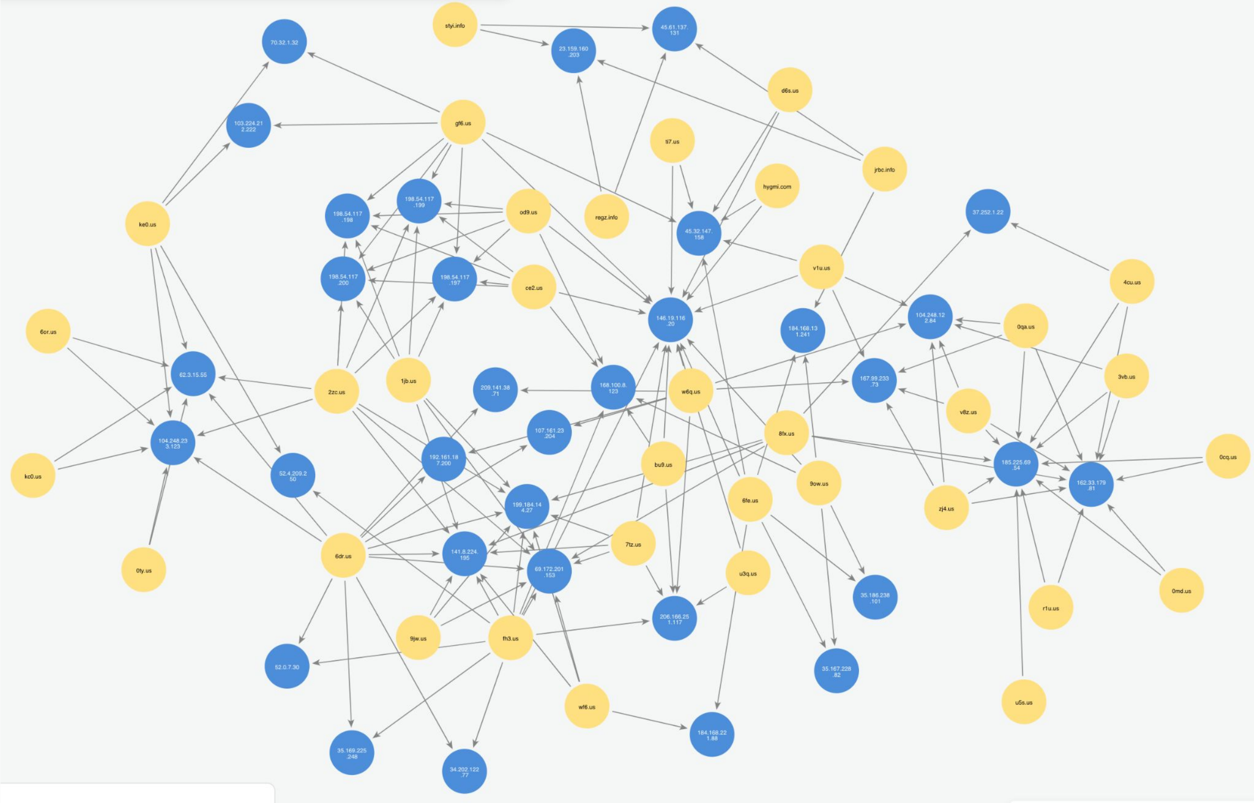
Attackers set up their infrastructure **before** they launch the attack.

Existing analyzers often **detect only parts of** active attack infrastructures.

Pivot on these observations to proactively protect **patient zero** victims.

Example Resource Sharing in the Web

Malicious Domains Share/Rotate Hosting Infrastructure



● Malicious domains

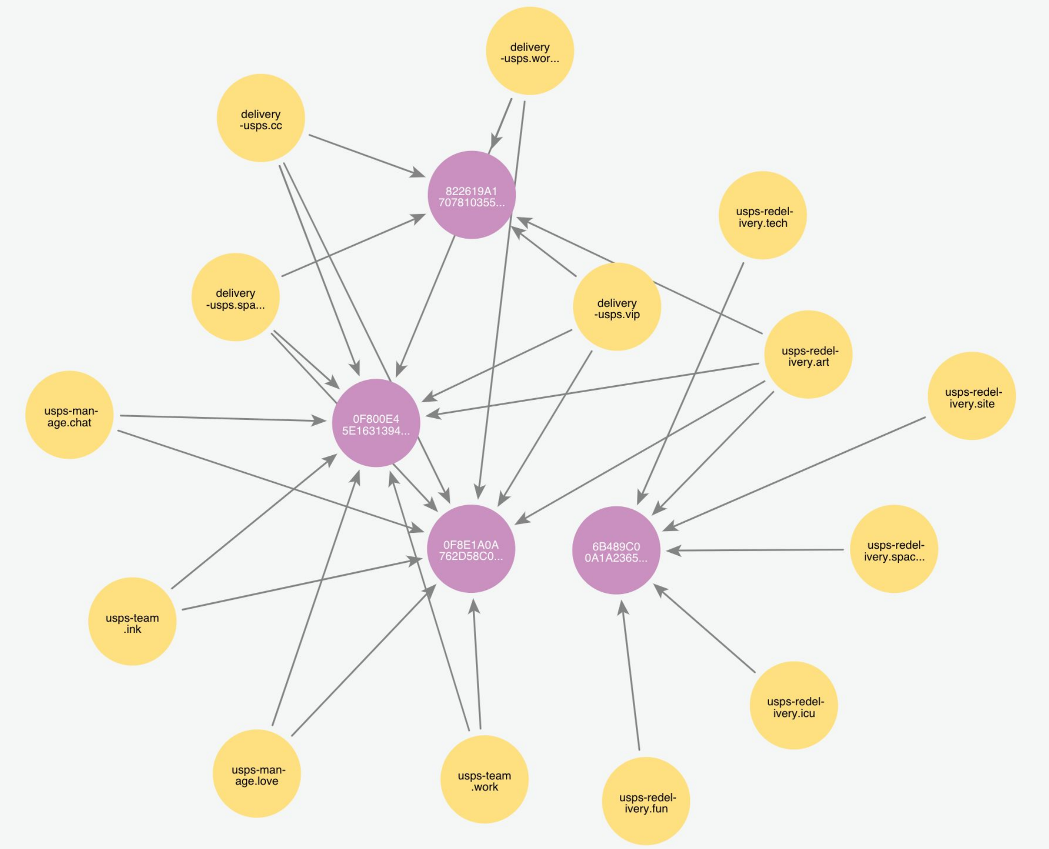
● IP addresses

Top hosting services:

- BL Networks
- AS-CHOOPA
- NameCheap
- Amazon
- Digital Ocean

Prolific Puma malicious link shortening service

Malicious Domains Share TLS Fingerprints

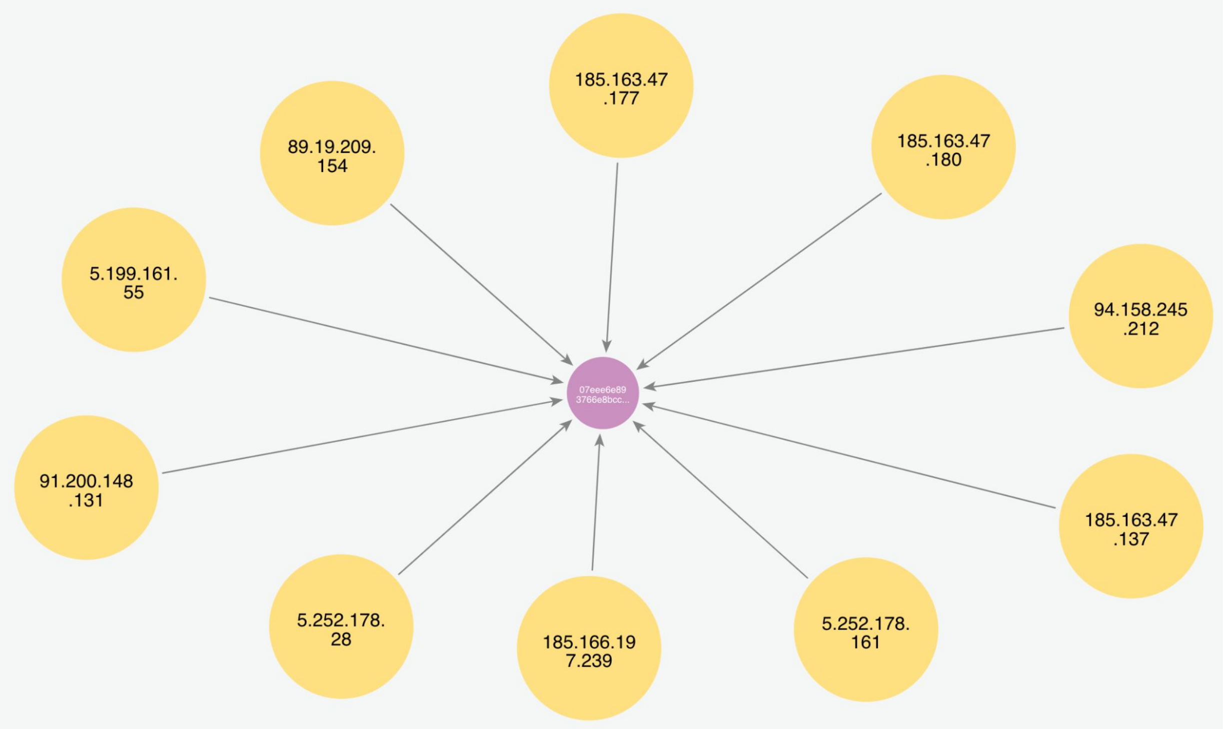


● Malicious domains

● TLS certificate fingerprints

USPS phishing campaign

Multiple IP Addresses Share Same SSH Fingerprint

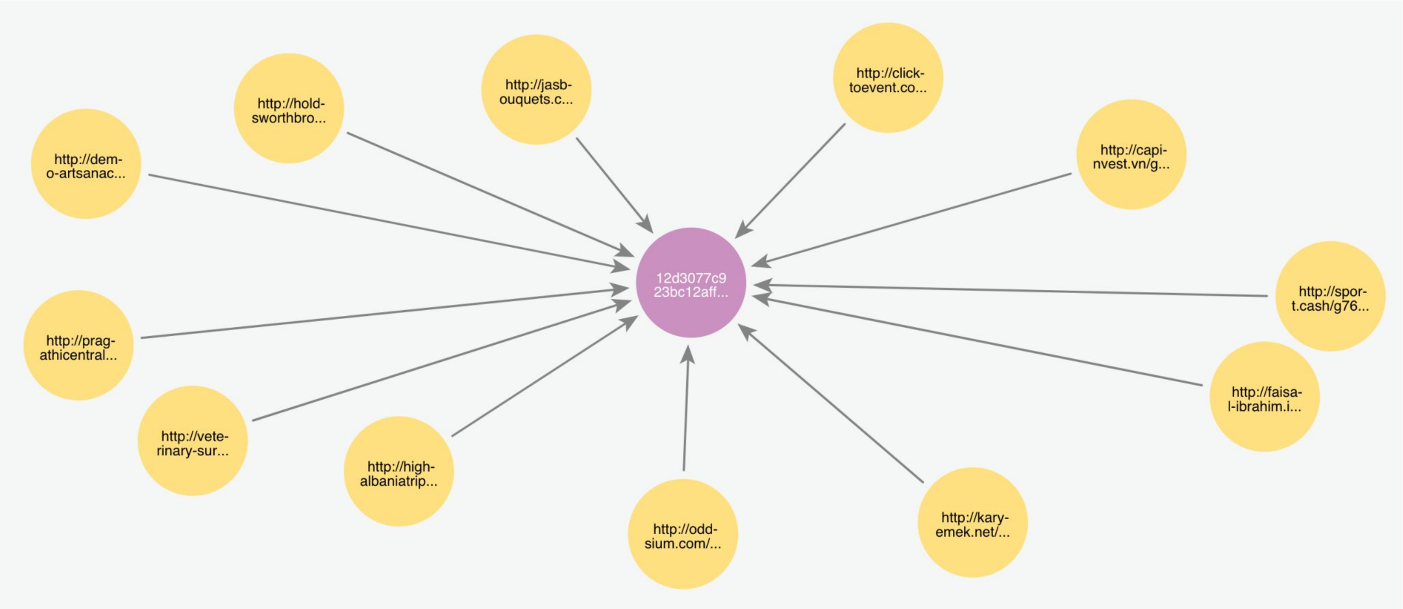


● Malicious IPs

● SSH fingerprint

An active self-signed certificate used by Gamaredon

Multiple Malicious URLs Distribute Same Malware


http://dem-o-artsanac...
http://hold-sworthbro...
http://jasb-ouquets.c...
http://click-toevent.co...
http://capi-nvest.vn/g...
12d3077c9 23bc12aff...
http://spor-t.cash/g76...
http://prag-athicentral...
http://faisa-l-ibrahim.i...
http://vete-rinary-sur...
http://high-albaniatrip...
http://odd-sium.com/...
http://kary-emek.net/...

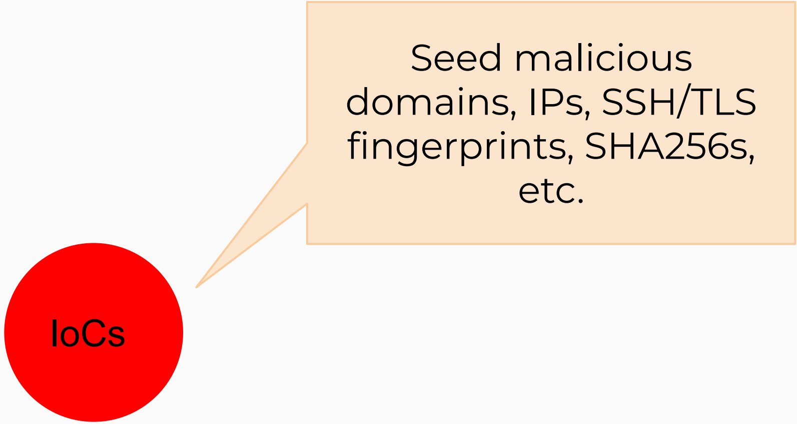
● Malicious URLs

● Malware hash

TeslaCrypt delivery URLs

Our Approach

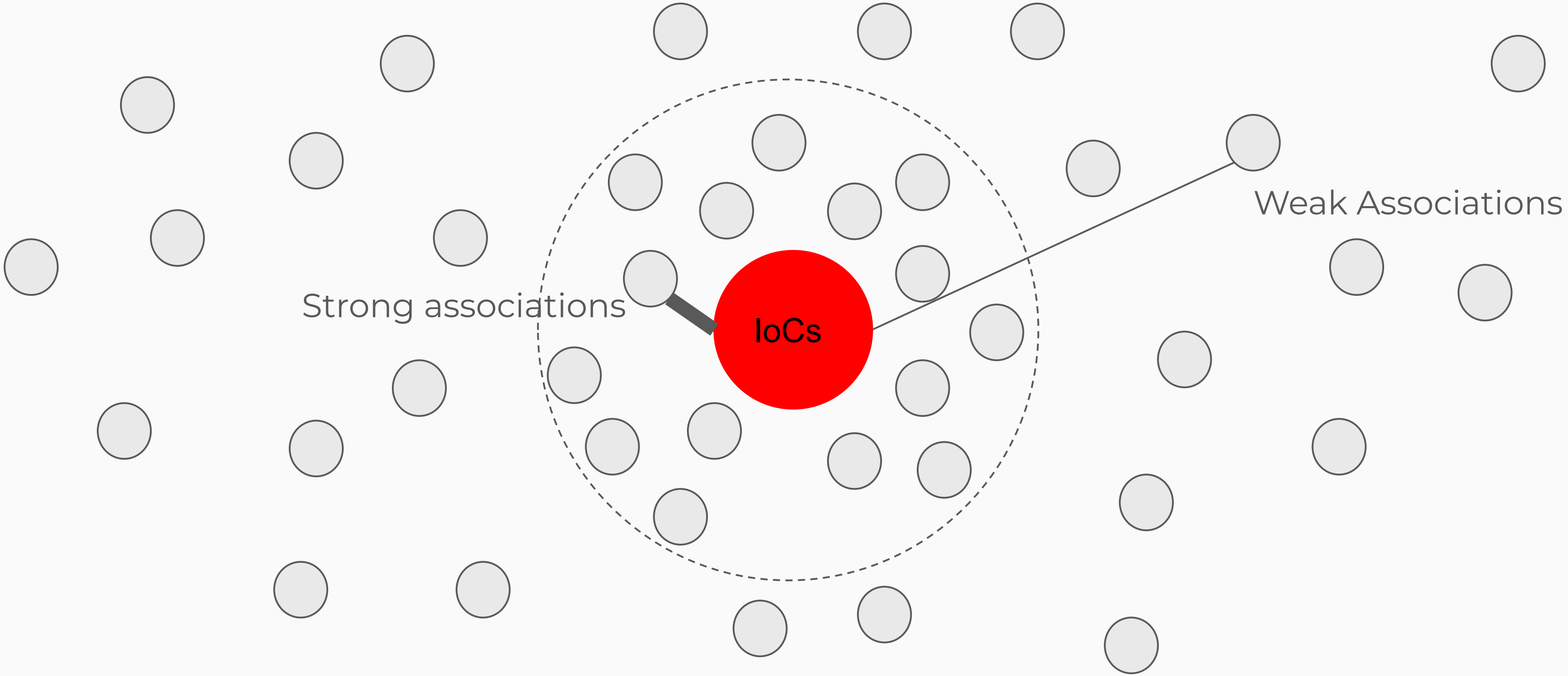
Key Idea: Automated Pivoting + Feature Similarity



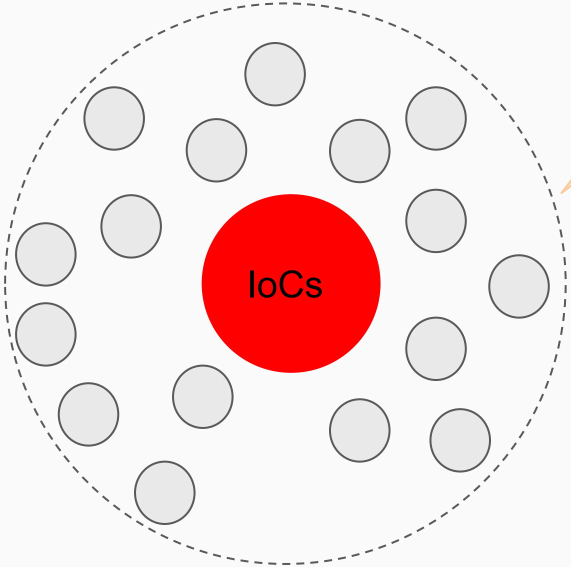
IoCs

Seed malicious domains, IPs, SSH/TLS fingerprints, SHA256s, etc.

Key Idea: Automated Pivoting + Feature Similarity

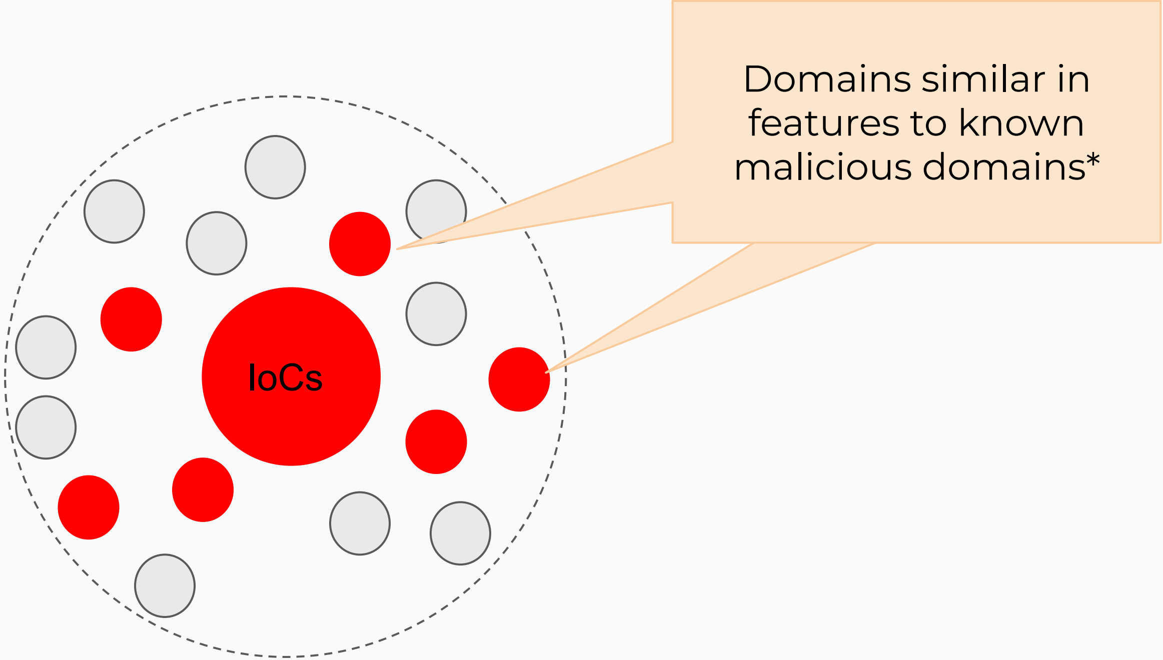


Key Idea: Automated Pivoting + Feature Similarity



High toxicity neighborhood

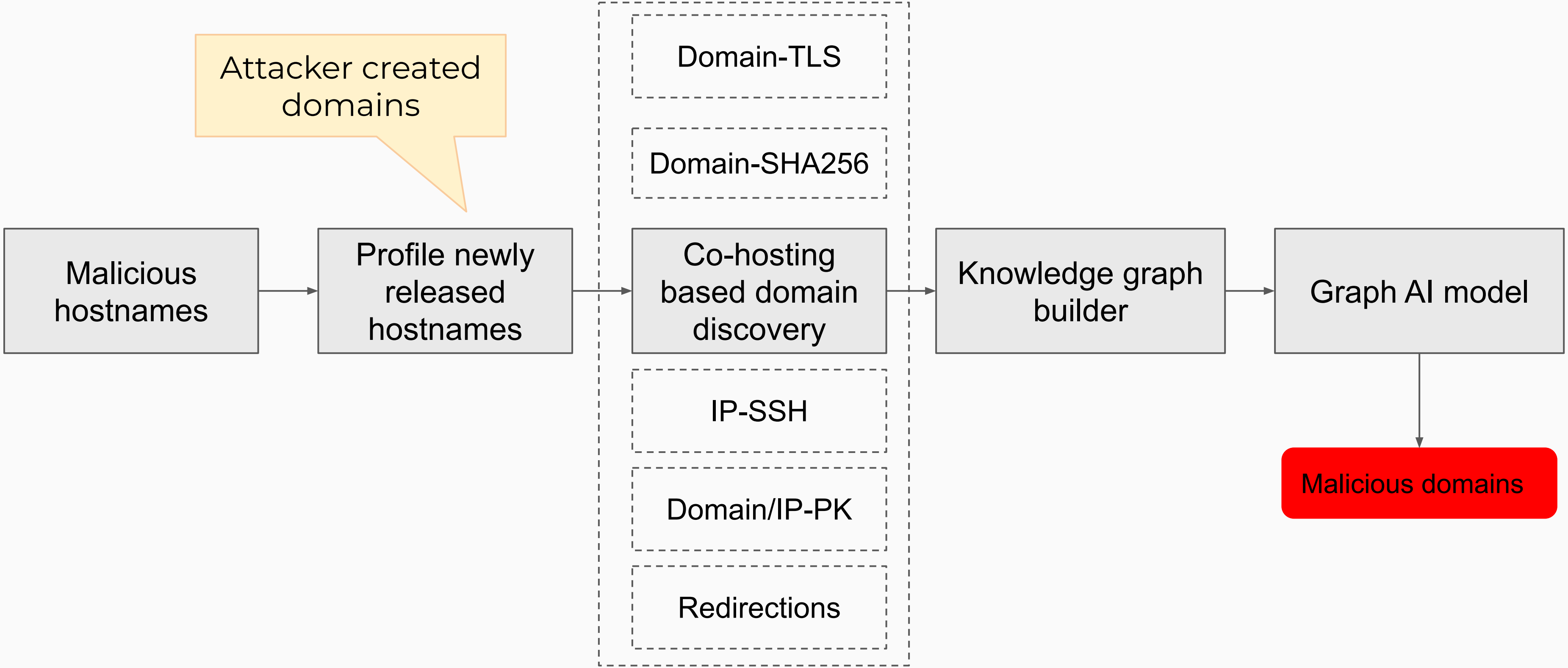
Key Idea: Automated Pivoting + Feature Similarity



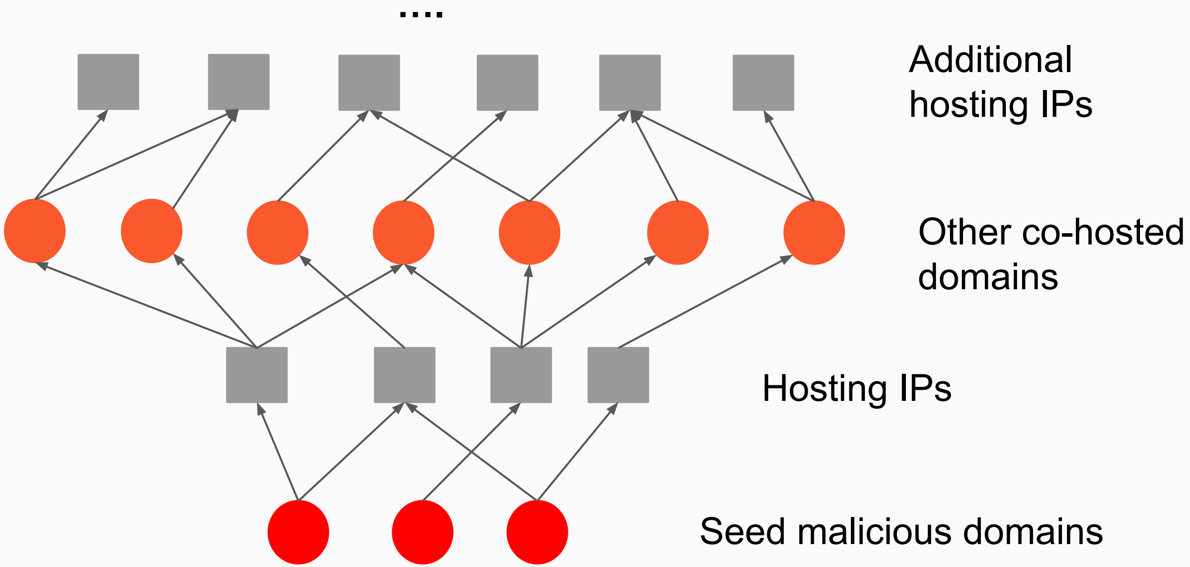
Domains similar in features to known malicious domains*

* Same applies to IPs

Overall Pipeline



Guided Discovery of Domains (Co-Hosting Relationship)



Graph AI-based Detection of Malicious Domains

Graph Schema

- Nodes
  - Domain
  - Subdomain
  - IP
  - File hash
  - TLS/SSH certificate fingerprint
- Edges
  - Domain-Subdomain
  - Domain-IP
  - Domain-FileHash
  - IP-SSH, Domain-TLS

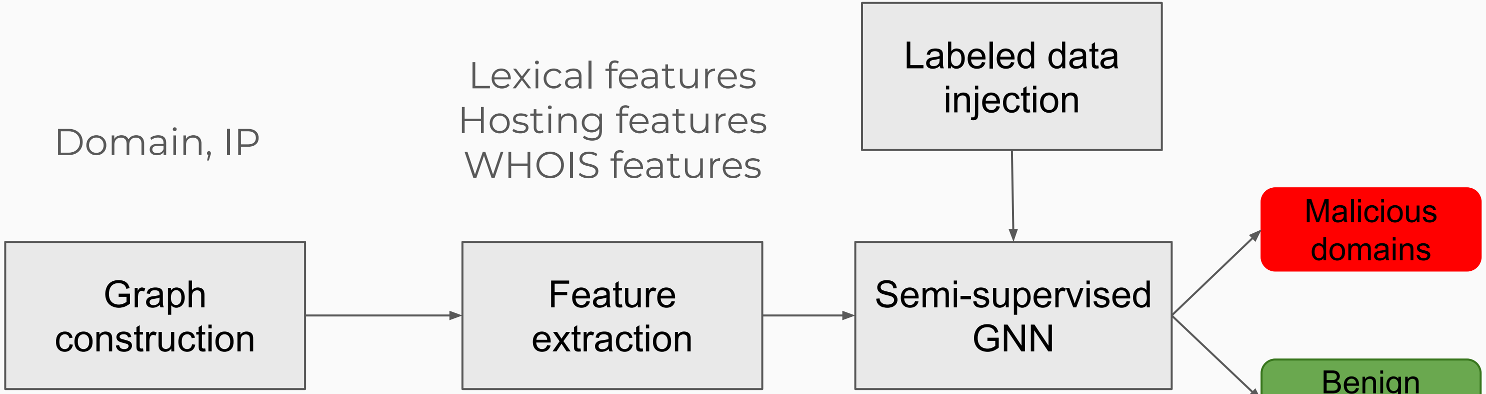
Labeled Data

- Malicious
    - In-house malicious domains
- Benign
    - Tranco top 100K domains
    - In-house benign domains

Features

- **Lexical features** (e.g., # brand/suspicious keywords, # hyphens)
- **Hosting features** (e.g., # IPs, hosting duration)
- **WHOIS features** (e.g., age, days to expiration, privacy)
- **Certificate features** (e.g., type, issuer)
- **IP features** (e.g., # domains, ASN, CC)
- **Content-based features** (e.g., # iframes, webform?)

Training the Graph AI (GNN) Model



(2K from each class)

Domain, IP

Lexical features
Hosting features
WHOIS features

Labeled data injection

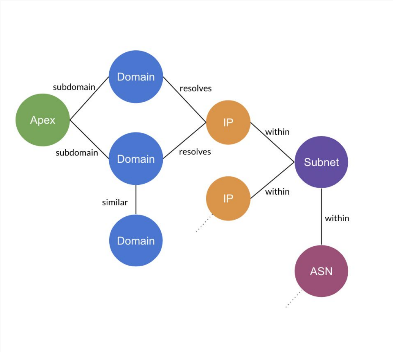
Graph construction

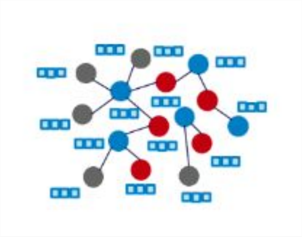
Feature extraction

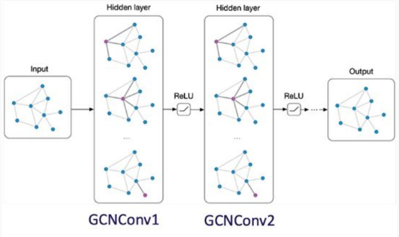
Semi-supervised GNN

Malicious domains

Benign domain







GraphSAGE

Preliminary Results

Model	**Precision***	**Recall***
Local features	81.05	70.10
Shallow embedding (node2vec)	84.07	72.23
Shallow embedding (metapath2vec)	86.22	74.54
Local features + Shallow embedding	89.01	78.32
GNN	**95.20**	**92.30**

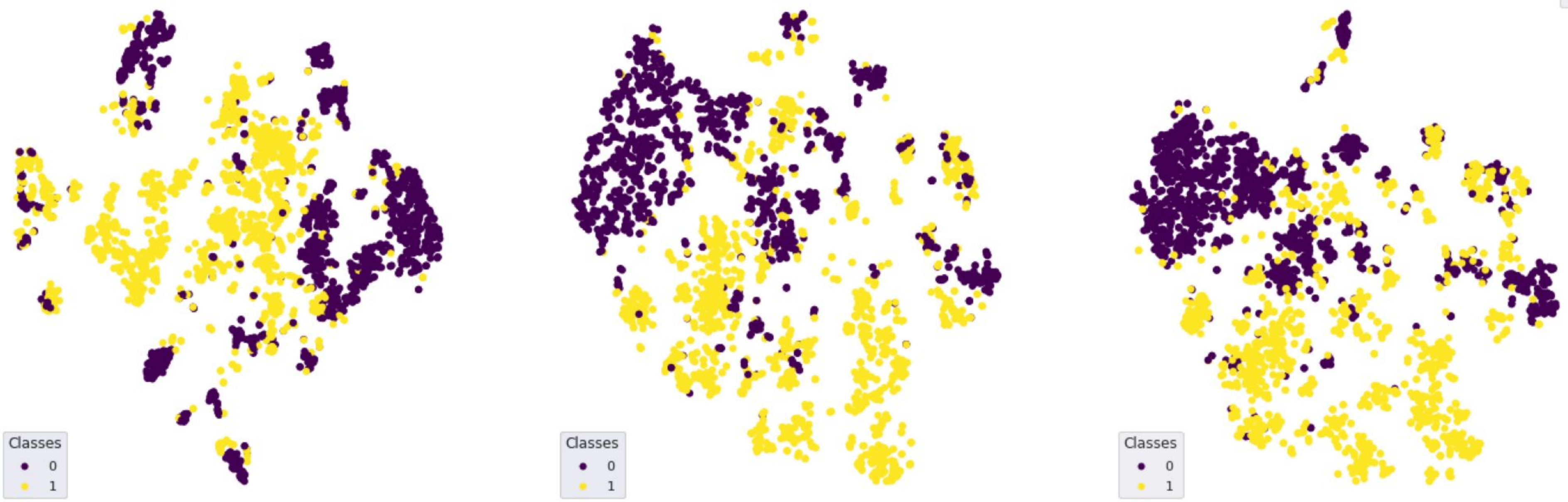
* At 0.5 default cut-off threshold

Metric\Thresh.	**0.50**	**0.98**
Precision	95.2%	99.9%
Recall	92.3%	53.1%

Results - Why it works

● Benign

● Malicious



Week 1

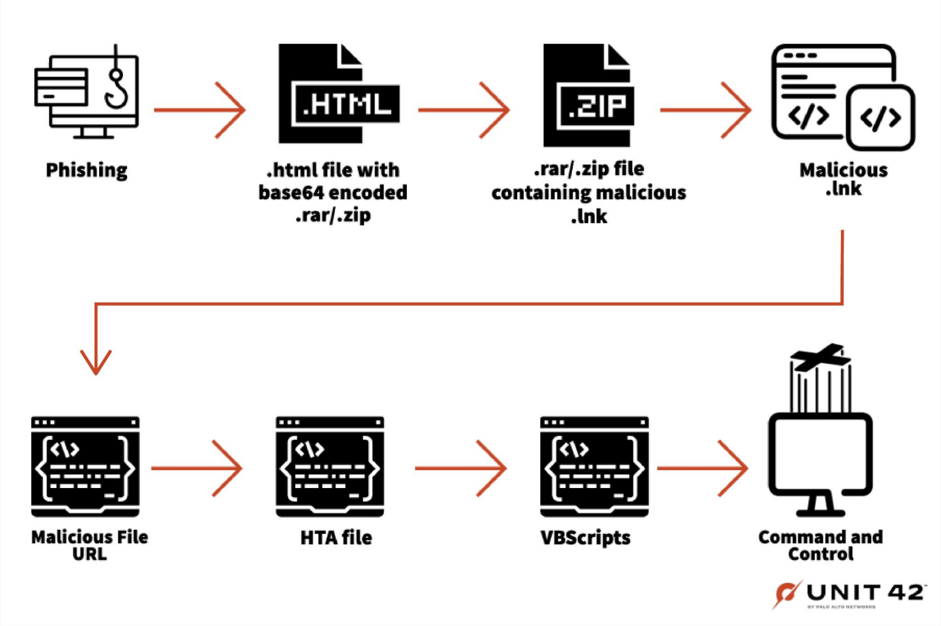
Week 2

Week 3

Case Studies

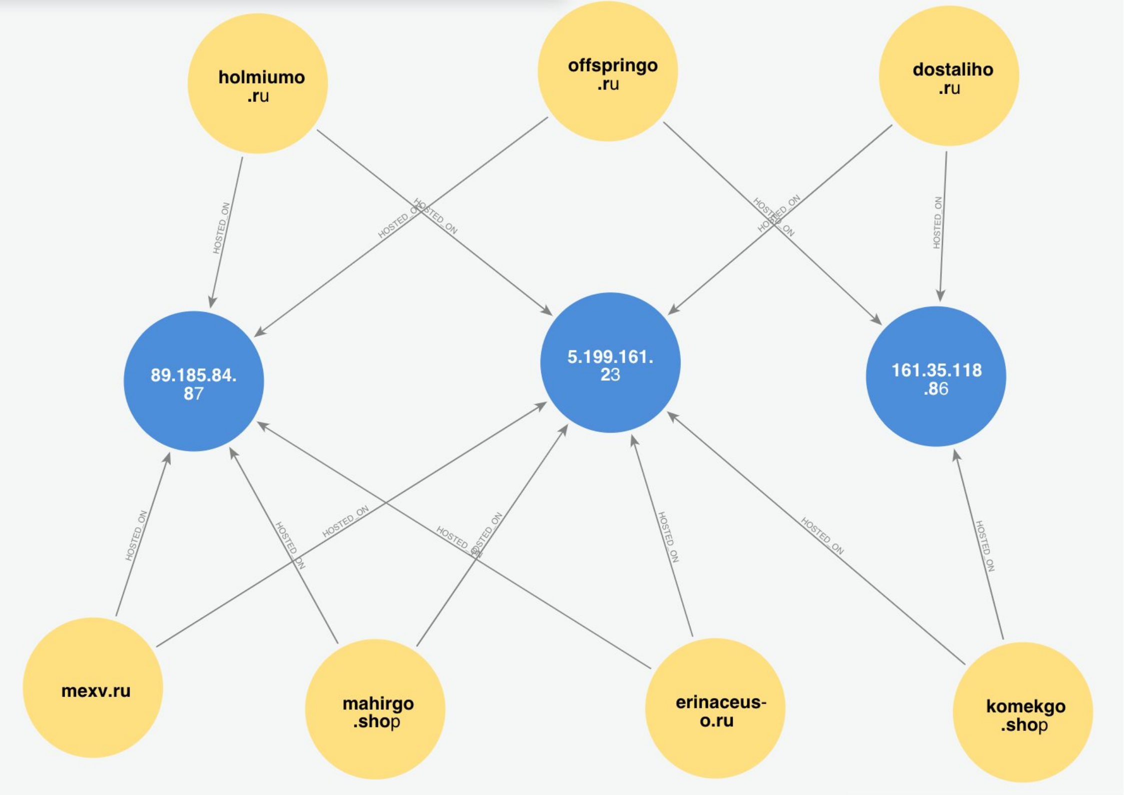
Case Study 1: Gamaredon APT

- A prominent Russian APT group targeting mainly Ukraine
- Operational since 2014
- 100s of seed domains
- ~2500 new malicious domains identified



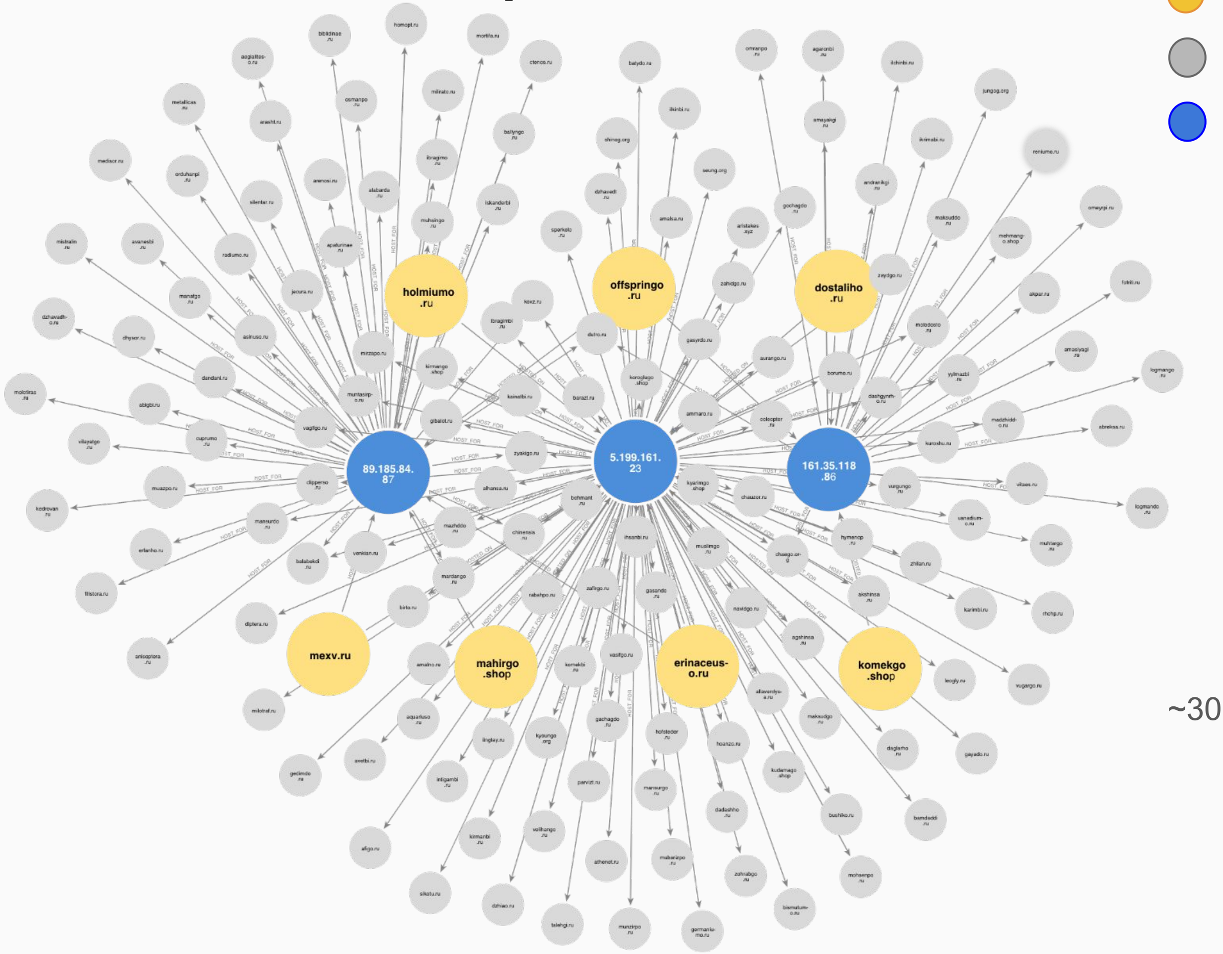
Gamaredon - Seed Domains

- offspringo.ru
- dostaliho.ru
- komekgo.shop
- mexv.ru
- erinaceuso.ru
- mahirgo.shop
- holmiumo.ru



Hosting Infrastructure

Gamaredon - Guided Expansion



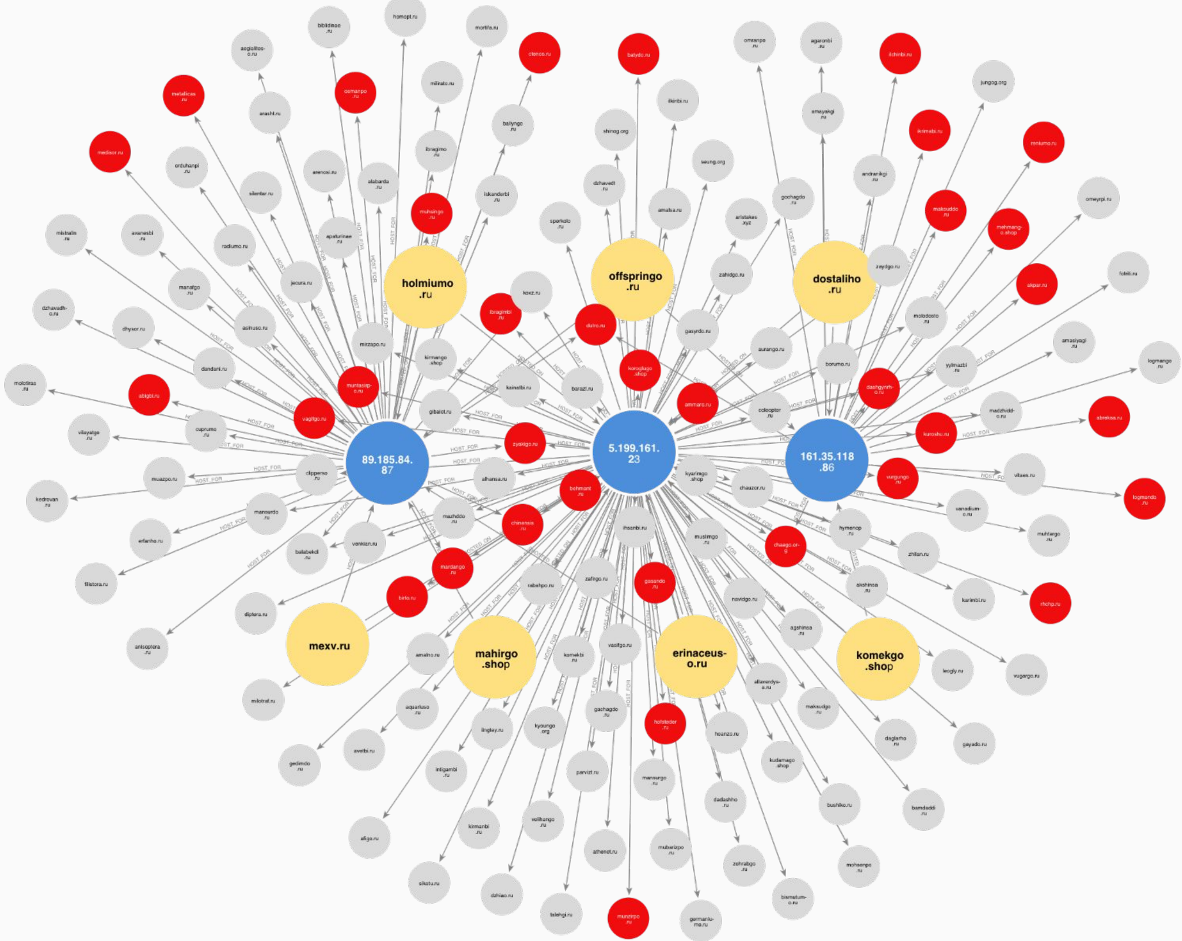
● Seed malicious domains

● Expanded unknown domains

● IP addresses

~300 domains in the neighborhood

Gamaredon - Flagged Malicious Domains



🟡 Seed malicious domains

⚪ Expanded unknown domains

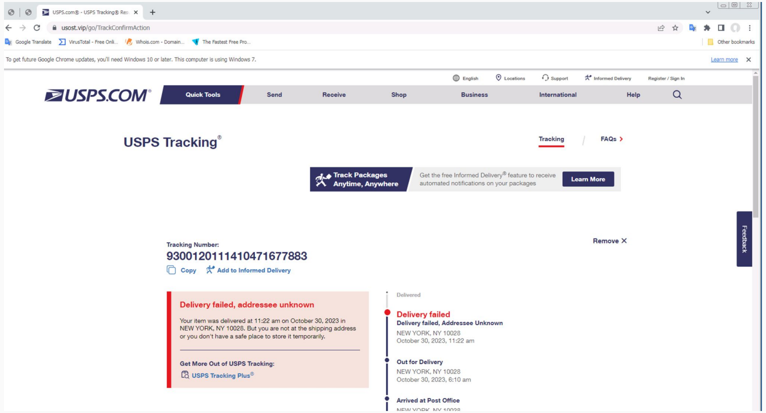
🔵 IP addresses

🔴 Flagged malicious domains

- **40 high-confidence detections**
- Later 34 domains were **flagged later as Malware** by other vendors.

Case Study 2: Postal Phishing Campaign

- A recent campaign targeting USPS and 12 other national postal services around the world.
- Attack vector: Smishing
- Collected ~450 seed domains from this campaign
    - Hosted on ~400 unique IP addresses
- Identified ~5000 additional domains hosted on these ~400 IP addresses in the last 3 months.
    - ~30% of them later flagged malicious by other vendors



To get future Google Chrome updates, you'll need Windows 10 or later. This computer is using Windows 7.

USPS Tracking®

Track Packages Anytime, Anywhere

Get the free Informed Delivery® feature to receive automated notifications on your packages

Tracking Number:
9300120111410471677883

Delivery failed, addressee unknown

Your item was delivered at 11:22 am on October 30, 2023 in NEW YORK, NY 10028. But you are not at the shipping address or you don't have a safe place to store it temporarily.

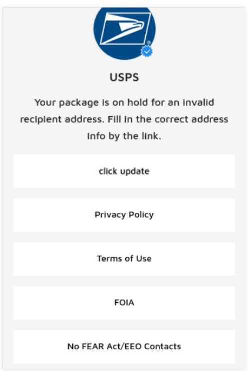
Get More Out of USPS Tracking:

Delivered

Delivery failed
Delivery failed, Addressee Unknown
NEW YORK, NY 10028
October 30, 2023, 11:22 am

Out for Delivery
NEW YORK, NY 10028
October 30, 2023, 6:10 am

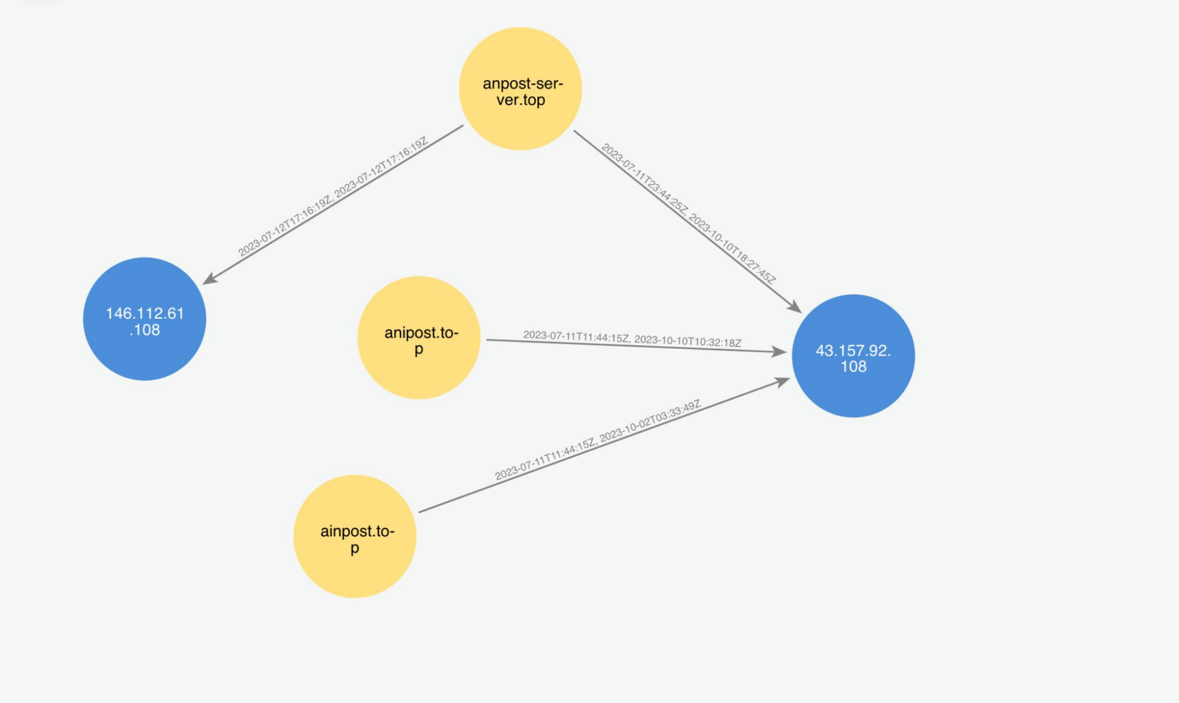
Arrived at Post Office
NEW YORK, NY 10028



USPS

Your package is on hold for an invalid recipient address. Fill in the correct address info by the link.

Postal Phishing Campaign: Seed Domains and Hosting Infrastructure

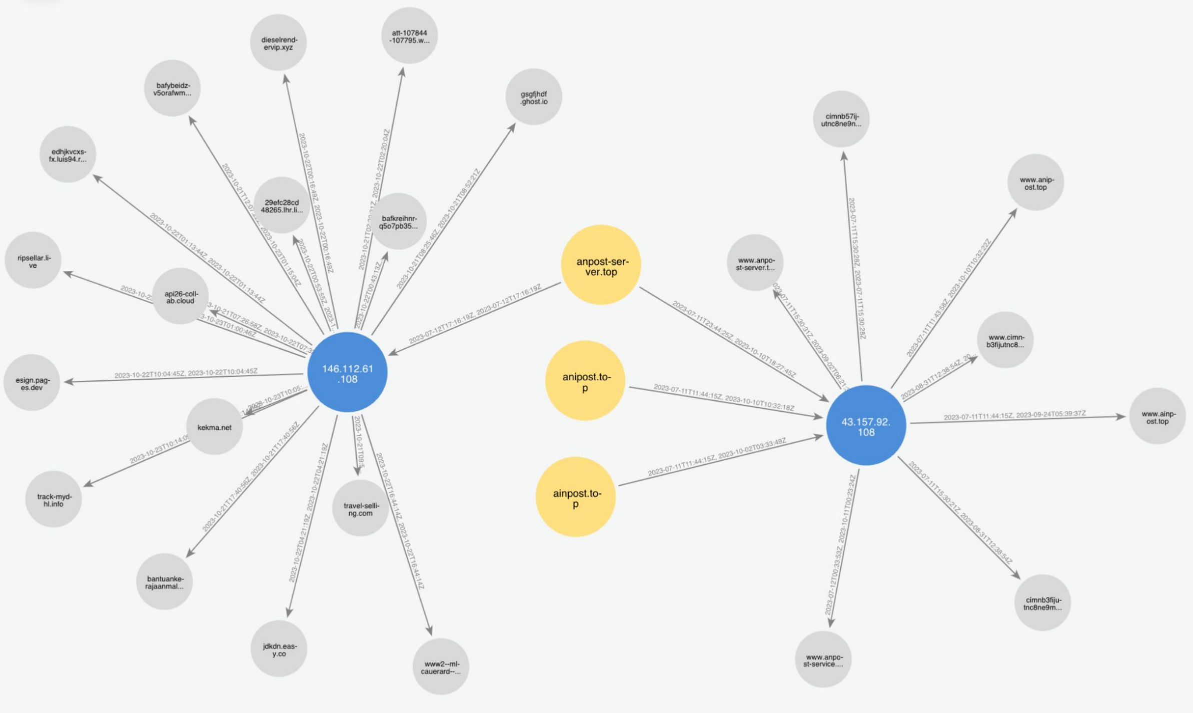

anpost-server.top
2023-07-12T17:16:19Z, 2023-07-12T17:16:19Z
2023-07-11T23:44:25Z, 2023-10-10T18:27:45Z
146.112.61.108
anipost.top
2023-07-11T11:44:15Z, 2023-10-10T10:32:18Z
43.157.92.108
2023-07-11T11:44:15Z, 2023-10-02T03:33:49Z
ainpost.top

● Seed malicious domains

● IP addresses

Hosting infrastructure shared by phishing domains targeting anpost[.]com (Ireland’s national postal service).

Postal Phishing Campaign - Graph Expansion



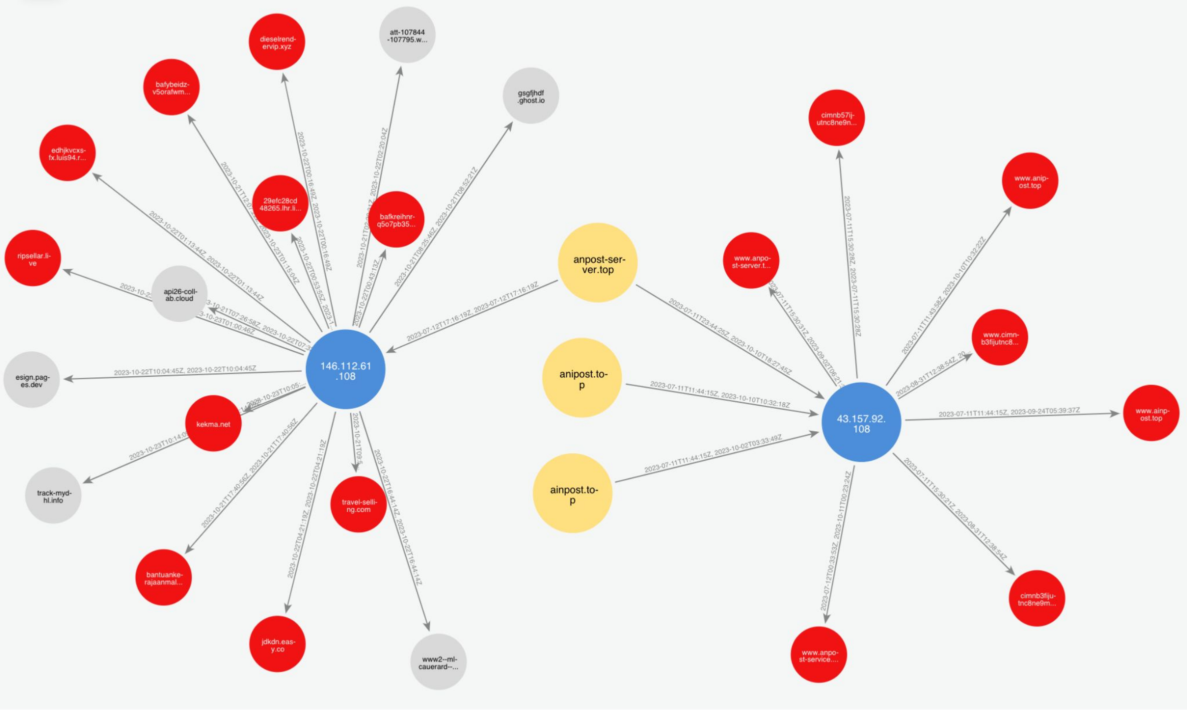
🟡 Seed malicious domains

⚪ Expanded unknown domains

🔵 IP addresses

Graph expansion for the phishing pages targeting An Post (anpost[.]com)

Postal Phishing Campaign - Flagged Malicious Domains


dieselrend-ervip.xyz
att-107844-107795.w...
bafybeidz-v5orafwm...
gsgfjhdf.ghost.io
edhjkvcxs-fx.luis94.r...
29efc28cd48265.lhr.li...
bafkreihnr-q5o7pb35...
ripsellar.li-ve
api26-coll-ab.cloud
anpost-ser-ver.top
146.112.61.108
esign.pag-es.dev
anipost.to-p
kekma.net
track-myd-hl.info
travel-selli-ng.com
ainpost.to-p
bantuanke-rajaanmal...
jdkdn.eas-y.co
www2--ml-cauerard--...
cimnb57ij-utnc8ne9n...
www.anip-ost.top
www.anpo-st-server.t...
www.cimn-b3fijutnc8...
43.157.92.108
www.ainp-ost.top
cimnb3fiju-tnc8ne9m...
www.anpo-st-service....
2023-10-22T00:16:49Z, 2023-10-22T00:16:49Z
2023-10-22T02:20:04Z
2023-10-21T08:25:46Z, 2023-10-21T08:52:21Z
2023-10-22T01:13:44Z, 2023-10-22T01:13:44Z
2023-10-23T01:15:04Z
2023-10-22T00:53:55Z
2023-10-22T00:43:13Z
2023-07-12T17:16:19Z, 2023-07-12T17:16:19Z
2023-10-21T07:26:58Z, 2023-10-22T07:3
2023-10-23T01:00:46Z
2023-10-22T10:04:45Z, 2023-10-22T10:04:45Z
2023-10-23T10:05:...
2023-10-23T10:14:0
2023-10-21T17:40:56Z, 2023-10-21T17:40:56Z
2023-10-22T04:21:19Z, 2023-10-22T04:21:19Z
2023-10-21T09:5...
2023-10-22T16:44:14Z, 2023-10-22T16:44:14Z
2023-07-11T15:30:28Z, 2023-07-11T15:30:28Z
2023-07-11T11:43:58Z, 2023-10-10T10:32:22Z
2023-07-11T23:44:25Z, 2023-10-10T18:27:45Z
2023-07-11T15:30:31Z, 2023-09-02T06:21:...
2023-08-31T12:38:54Z, 20...
2023-07-11T11:44:15Z, 2023-10-10T10:32:18Z
2023-07-11T11:44:15Z, 2023-09-24T05:39:37Z
2023-07-11T11:44:15Z, 2023-10-02T03:33:49Z
2023-07-12T00:33:53Z, 2023-10-11T00:23:24Z
2023-07-11T15:30:21Z, 2023-08-31T12:38:54Z

🟡 Seed malicious domains

⚪ Expanded unknown domains

🔵 IP addresses

🔴 Flagged malicious domains

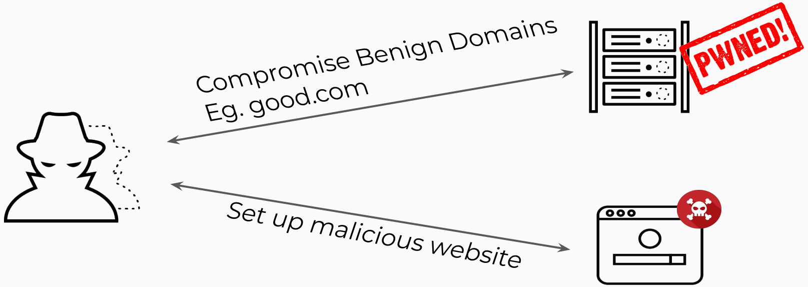
Detecting Domain Hijacking in Passive DNS

Outline

- Introduction
- Methodology
  - Training a machine learning model
  - ML in production
- Case studies

What is Domain Hijacking?

- Attackers compromise a domain name
  - Account takeover at registrar or DNS service provider
  - Compromise registrar or DNS service provider
- Point compromised domain name to attacker server
- Expose users to phishing, MitM attack, drive-by-download sites, etc.



Compromise Benign Domains
Eg. good.com

Set up malicious website

Domain Hijacking of a Large Brazilian Bank

- On Oct. 22, 2016 cybercriminals gained control of all 36 domains of the bank
    - Used Let’s Encrypt to establish certificates
- Pointed all of the bank’s employees and customers to malicious servers
    - Over 5 million customers exposed
    - Phishing sites and malware
- Malware
    - Disabled antimalware software
    - Harvested Credentials
    - Targeted other banks

Challenges

- Hundreds of millions of new DNS records every day
- Only a few domain hijacking records expected
- Hundreds of terabytes of historical data to process
- Very few cases of known hijacking DNS records for training an ML model

Training a Machine Learning Model

- Simulate realistic DNS hijacking attacks
  - Using real DNS data
  - Inject it back to our passive DNS dataset
- Labeled data
  - Positive labels: simulated DNS hijacking records
  - Negative labels: all new records
- Extract 74 features
- Train a machine learning model

Features used

- Comparison of **DNS History** of new IP and old IP addresses
  - Average DNS record age
- **DNS History** of new IP
  - # domains where IP address is new
- Comparison of **geolocation** of new IP and old IP addresses
  - Is country, ISP, ASN new?
- **DNS History** of the compromised domain
  - # IP addresses, # of IP countries
  - # of new record types

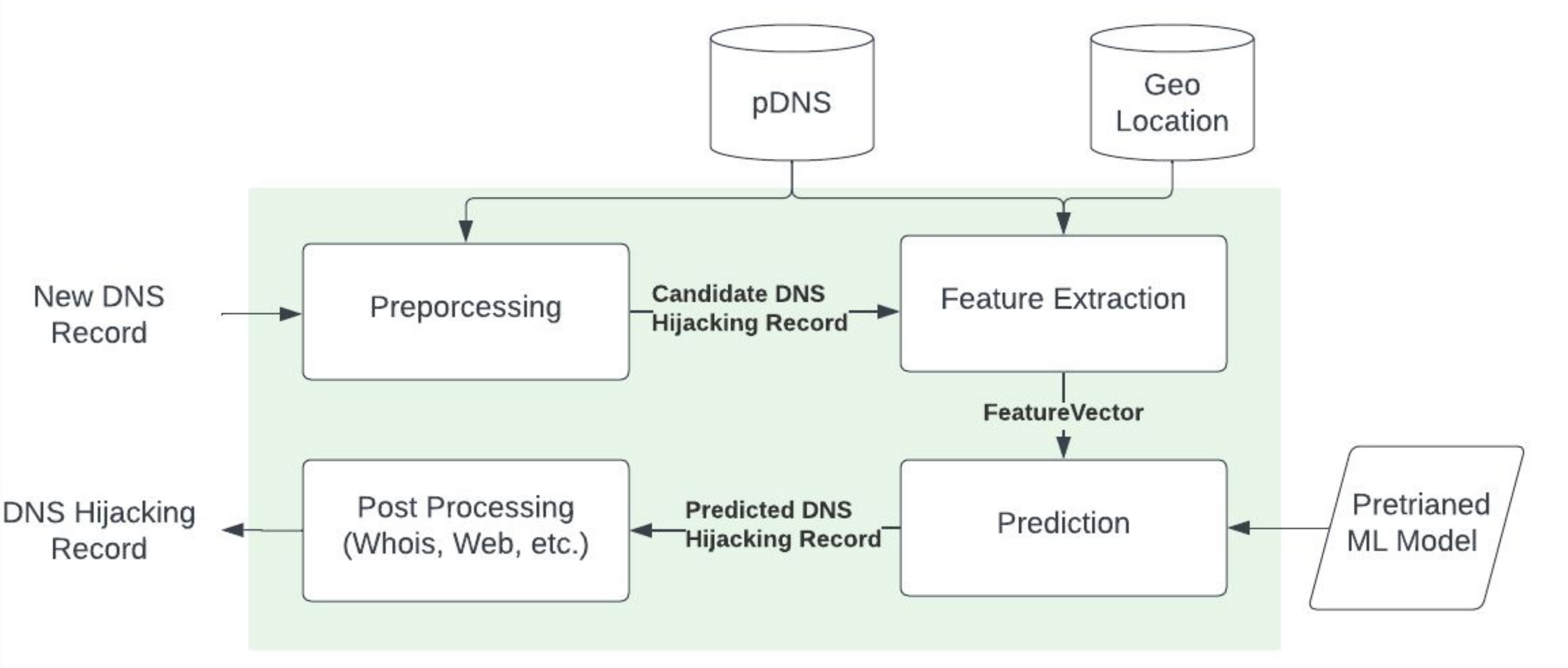
Features used

- Comparison of **DNS History** of new IP and old IP addresses
  - Average DNS record age
- **DNS History** of new IP
  - # domains where IP address is new
- Comparison of **geolocation** of new IP and old IP addresses
  - Is country, ISP, ASN new?
- **DNS History** of the compromised domain
  - # IP addresses, # of IP countries
  - # of new record types

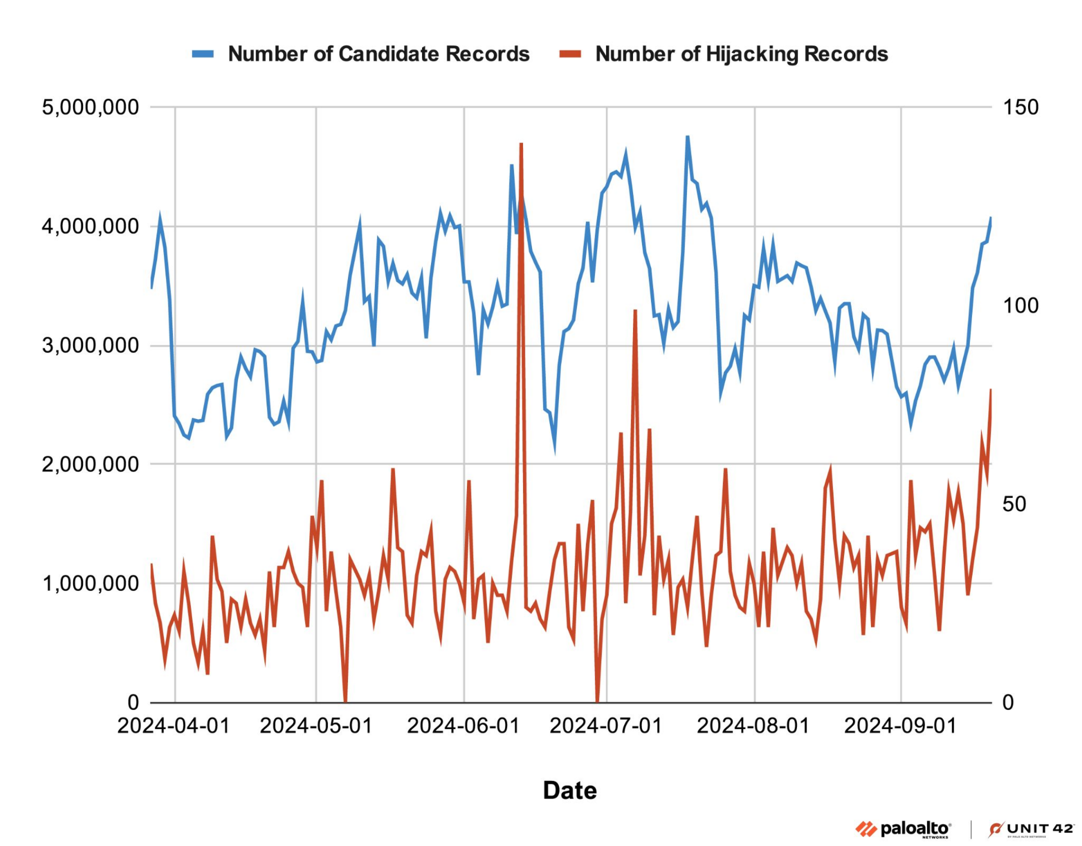
Random forest classifier achieves:

- **Precision: 0.99**
- **Recall: 0.97**

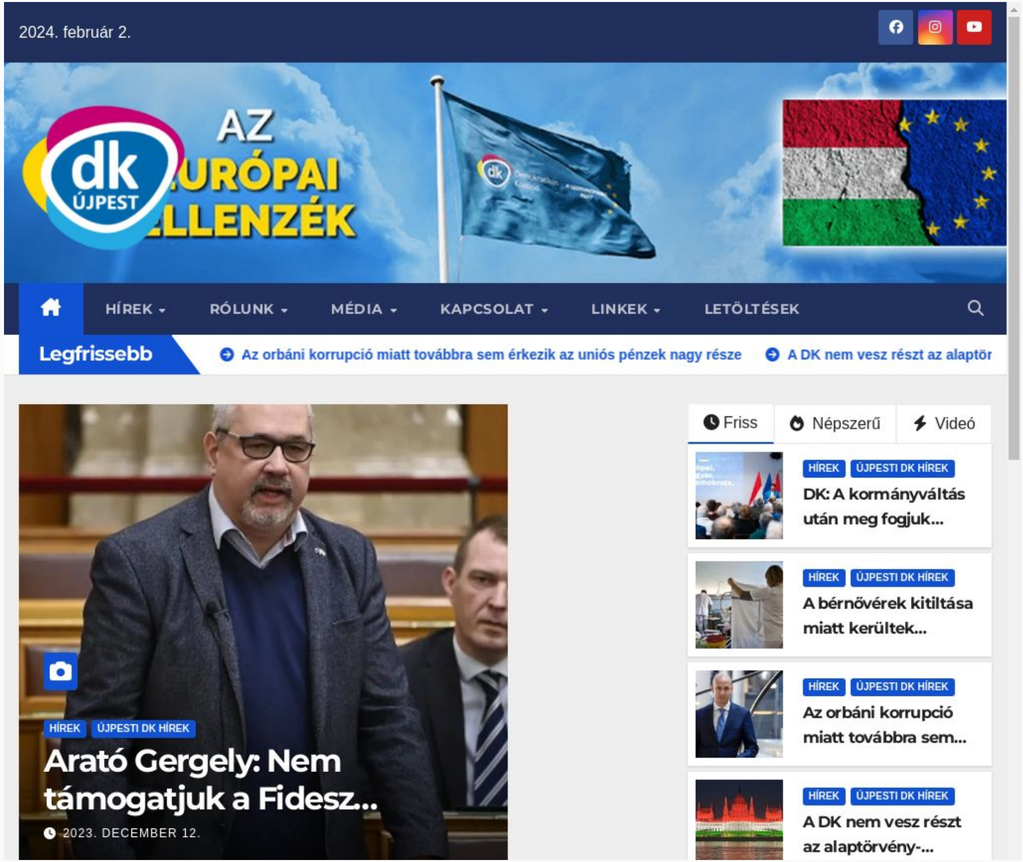
Machine Learning in Production



Numbers in Production



Political party dkujpest[.]hu - original website



2024. február 2.

Legfrissebb

Az orbáni korrupció miatt továbbra sem érkezik az uniós pénzek nagy része

A DK nem vesz részt az alaptör

HÍREK ÚJPESTI DK HÍREK

Arató Gergely: Nem támogatjuk a Fidesz...

2023. DECEMBER 12.

HÍREK ÚJPESTI DK HÍREK

DK: A kormányváltás után meg fogjuk...

HÍREK ÚJPESTI DK HÍREK

A bérnővérek kitiltása miatt kerültek...

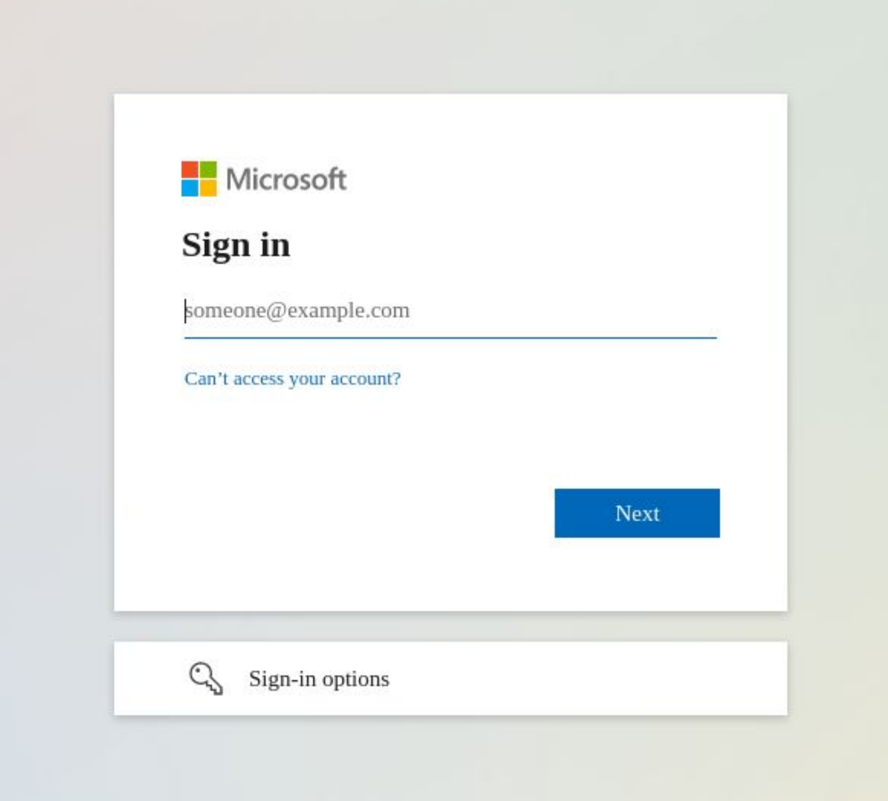
HÍREK ÚJPESTI DK HÍREK

Az orbáni korrupció miatt továbbra sem...

HÍREK ÚJPESTI DK HÍREK

A DK nem vesz részt az alaptörvény-...

Political party dkujpest[.]hu - phishing webpage



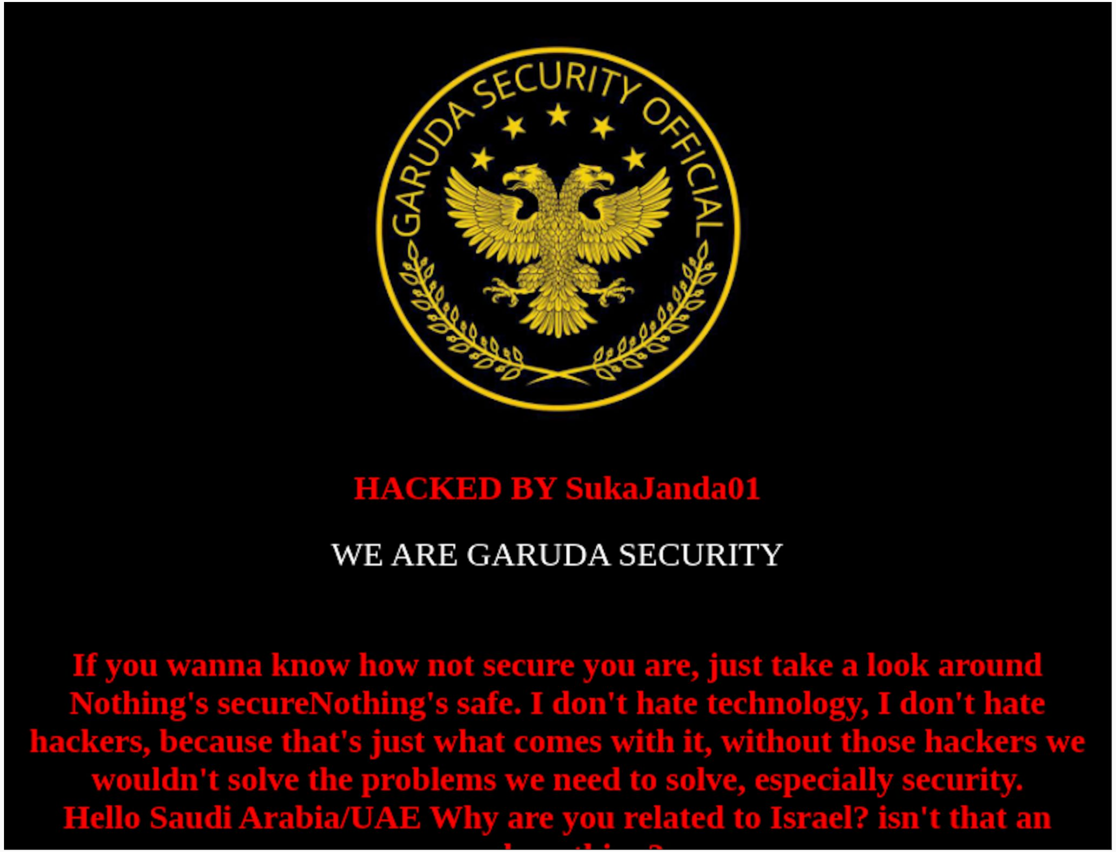
Microsoft

Sign in

someone@example.com

Can’t access your account?

Large U.S. utility management company - defaced webpage

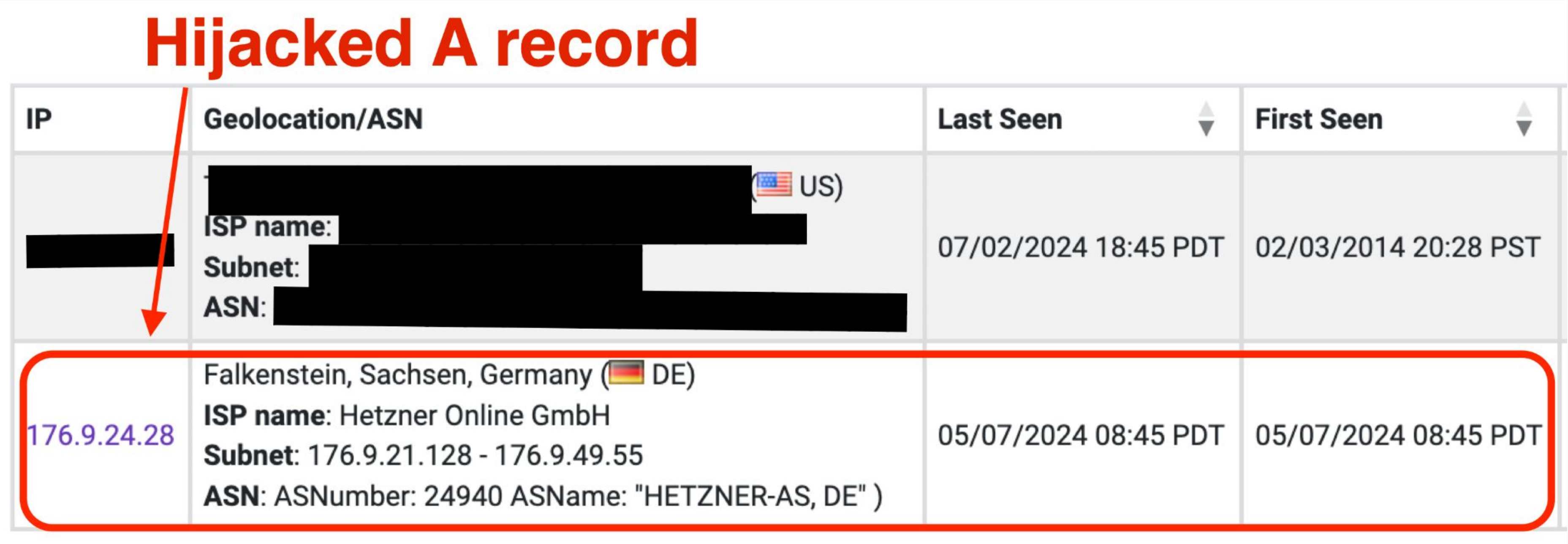


HACKED BY SukaJanda01

WE ARE GARUDA SECURITY

If you wanna know how not secure you are, just take a look around Nothing's secureNothing's safe. I don't hate technology, I don't hate hackers, because that's just what comes with it, without those hackers we wouldn't solve the problems we need to solve, especially security. Hello Saudi Arabia/UAE Why are you related to Israel? isn't that an

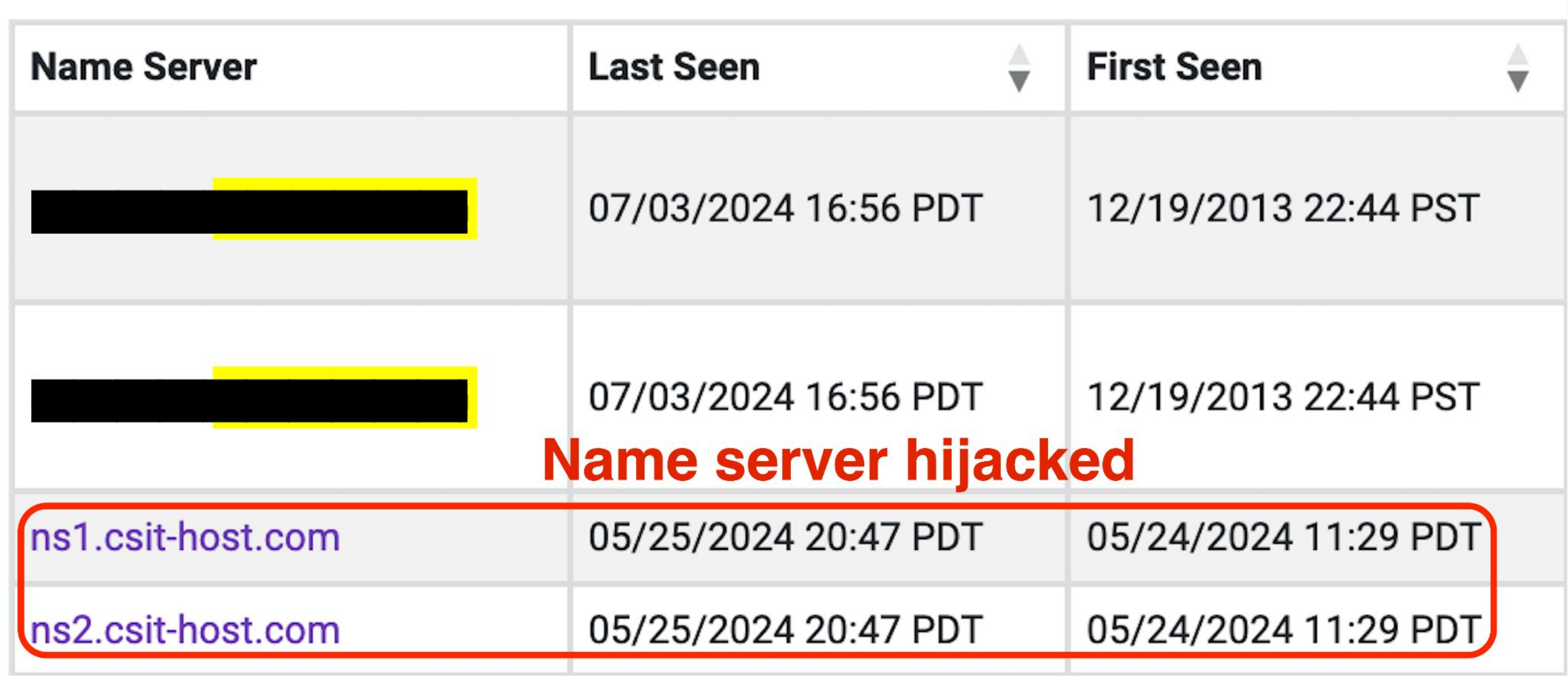
Large U.S. utility management company - hijacked DNS record



Hijacked A record

IP	Geolocation/ASN	Last Seen	First Seen
[redacted]	[redacted] (🇺🇸 US) **ISP name:** [redacted] **Subnet:** [redacted] **ASN:** [redacted]	07/02/2024 18:45 PDT	02/03/2014 20:28 PST
176.9.24.28	Falkenstein, Sachsen, Germany (🇩🇪 DE) **ISP name**: Hetzner Online GmbH **Subnet**: 176.9.21.128 - 176.9.49.55 **ASN**: ASNumber: 24940 ASName: "HETZNER-AS, DE")	05/07/2024 08:45 PDT	05/07/2024 08:45 PDT

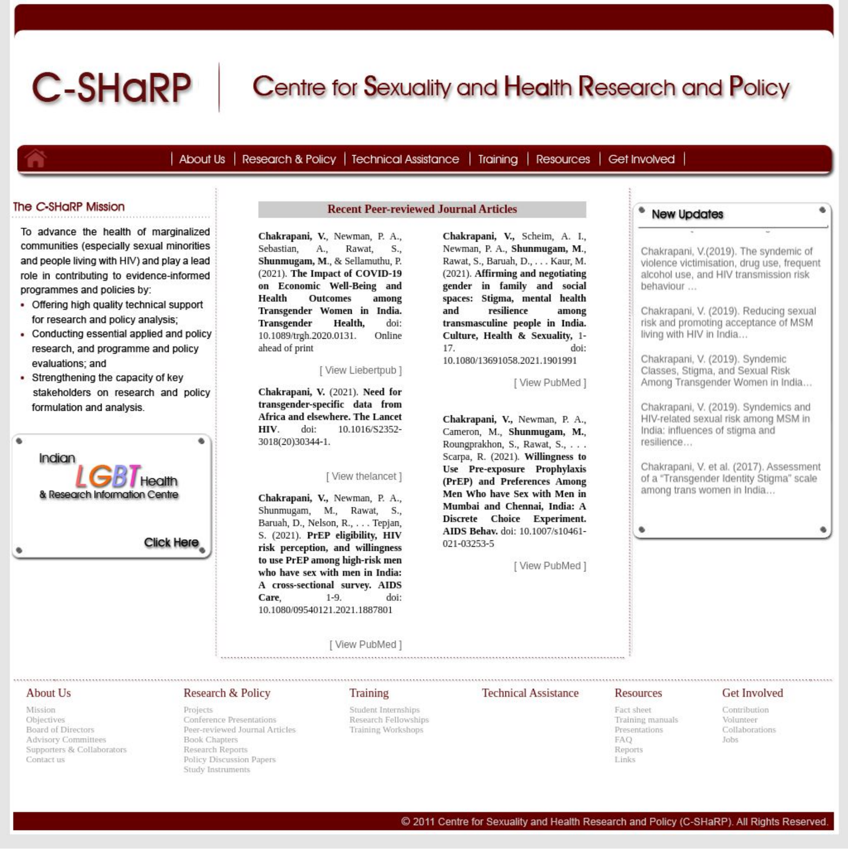
Large internet service provider - hijacked DNS record



Name Server	Last Seen	First Seen
[redacted]	07/03/2024 16:56 PDT	12/19/2013 22:44 PST
[redacted]	07/03/2024 16:56 PDT	12/19/2013 22:44 PST
ns1.csit-host.com	05/25/2024 20:47 PDT	05/24/2024 11:29 PDT
ns2.csit-host.com	05/25/2024 20:47 PDT	05/24/2024 11:29 PDT

Name server hijacked

Research Institution c-sharp[.]in - original website



The C-SHaRP Mission

To advance the health of marginalized communities (especially sexual minorities and people living with HIV) and play a lead role in contributing to evidence-informed programmes and policies by:

- Offering high quality technical support for research and policy analysis;
- Conducting essential applied and policy research, and programme and policy evaluations; and
- Strengthening the capacity of key stakeholders on research and policy formulation and analysis.

Recent Peer-reviewed Journal Articles

Chakrapani, V., Newman, P. A., Sebastian, A., Rawat, S., **Shunmugam, M.**, & Sellamuthu, P. (2021). **The Impact of COVID-19 on Economic Well-Being and Health Outcomes among Transgender Women in India. Transgender Health,** doi: 10.1089/trgh.2020.0131. Online ahead of print

[View Liebertpub]

Chakrapani, V. (2021). **Need for transgender-specific data from Africa and elsewhere. The Lancet HIV**. doi: 10.1016/S2352-3018(20)30344-1.

[View thelancet]

Chakrapani, V., Newman, P. A., Shunmugam, M., Rawat, S., Baruah, D., Nelson, R., . . . Tepjan, S. (2021). **PrEP eligibility, HIV risk perception, and willingness to use PrEP among high-risk men who have sex with men in India: A cross-sectional survey. AIDS Care**, 1-9. doi: 10.1080/09540121.2021.1887801

[View PubMed]

Chakrapani, V., Scheim, A. I., Newman, P. A., **Shunmugam, M.**, Rawat, S., Baruah, D., . . . Kaur, M. (2021). **Affirming and negotiating gender in family and social spaces: Stigma, mental health and resilience among transmasculine people in India. Culture, Health & Sexuality,** 1-17. doi: 10.1080/13691058.2021.1901991

[View PubMed]

Chakrapani, V., Newman, P. A., Cameron, M., **Shunmugam, M.**, Roungprakhon, S., Rawat, S., . . . Scarpa, R. (2021). **Willingness to Use Pre-exposure Prophylaxis (PrEP) and Preferences Among Men Who have Sex with Men in Mumbai and Chennai, India: A Discrete Choice Experiment. AIDS Behav.** doi: 10.1007/s10461-021-03253-5

[View PubMed]

New Updates

Chakrapani, V.(2019). The syndemic of violence victimisation, drug use, frequent alcohol use, and HIV transmission risk behaviour …

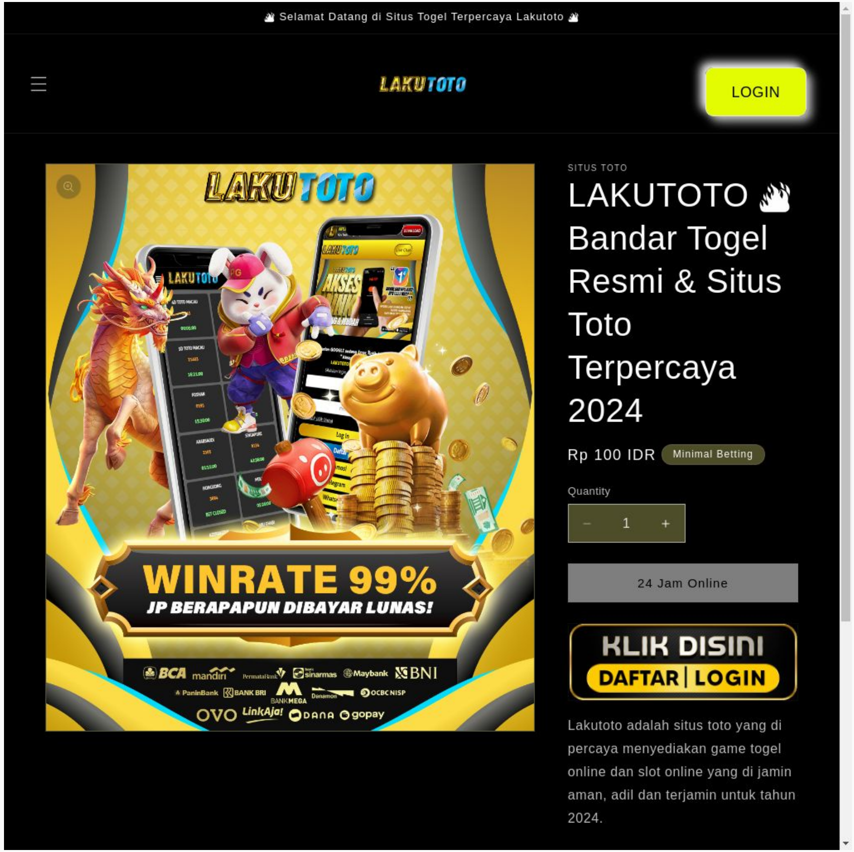
Chakrapani, V. (2019). Reducing sexual risk and promoting acceptance of MSM living with HIV in India…

Chakrapani, V. (2019). Syndemic Classes, Stigma, and Sexual Risk Among Transgender Women in India…

Chakrapani, V. (2019). Syndemics and HIV-related sexual risk among MSM in India: influences of stigma and resilience…

Chakrapani, V. et al. (2017). Assessment of a "Transgender Identity Stigma" scale among trans women in India…

Research Institution c-sharp[.]in - hijacked website



🔥 Selamat Datang di Situs Togel Terpercaya Lakutoto 🔥

LAKUTOTO

LOGIN

SITUS TOTO

LAKUTOTO 🔥 Bandar Togel Resmi & Situs Toto Terpercaya 2024

Rp 100 IDR Minimal Betting

Quantity

− 1 +

24 Jam Online

KLIK DISINI
DAFTAR | LOGIN

Lakutoto adalah situs toto yang di percaya menyediakan game togel online dan slot online yang di jamin aman, adil dan terjamin untuk tahun 2024.

Summary

- We face a **large variety of threats**
- Threat actors **unintentionally leave behind traces** of information
- We can leverage **large datasets** to detect malicious and compromised domains
- **AI is necessary**:
  - Connect the dots in large datasets
  - Proactive detection
  - Solve needle in a haystack problems

Q&A

Janos Szurdi - jszurdi@paloaltonetworks.com

in linkedin.com/in/**szurdi**