infoblox®

DNS DR – WHAT THIS CAN HELP WITH?

JAN RYNEŠ

SOLUTIONS ARCHITECT

ALL THE BUZZWORDS

EDR - Endpoint NDR - Network
XDR – all together

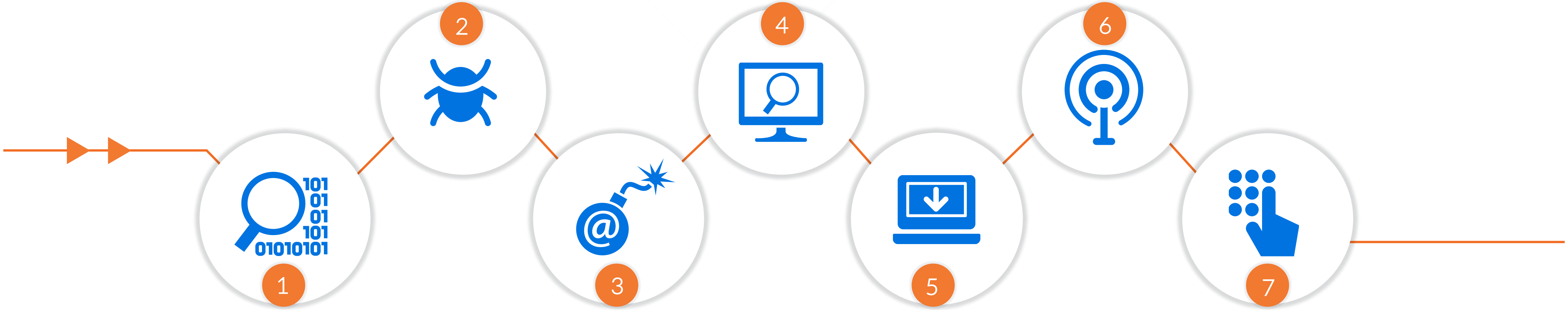
Detection and Response -> Something is happening, and I can see it – and I will respond (automatically?)

DNS DR?

Things that you can see only on DNS level

And what this could be?

HOW WILL APT GROUP/ATTACKER BEHAVE



Reconnaissance

Harvesting email addresses, conference information, etc.

DNS Reconnaissance

Weaponization

Coupling exploit with backdoor into deliverable payload

Delivery

Delivering weaponized bundle to the victim via email, web, USB, etc.

DNS Resolution
DNS Infiltration

Exploitation

Exploiting a vulnerability to execute code on victim's system

DNS Protocol Anomalies
DNS Exploits
DNS Hijacking

Installation

Installing malware on the asset

Command & Control (C2)

Command channel for remote manipulation of victim

DNS Resolution
DNS Callback
DNS Tunneling

Actions on Objectives

With "Hands on Keyboard" access, intruders accomplish their original goal

DNS Tunneling
DNS Exfiltration
DNS DDoS

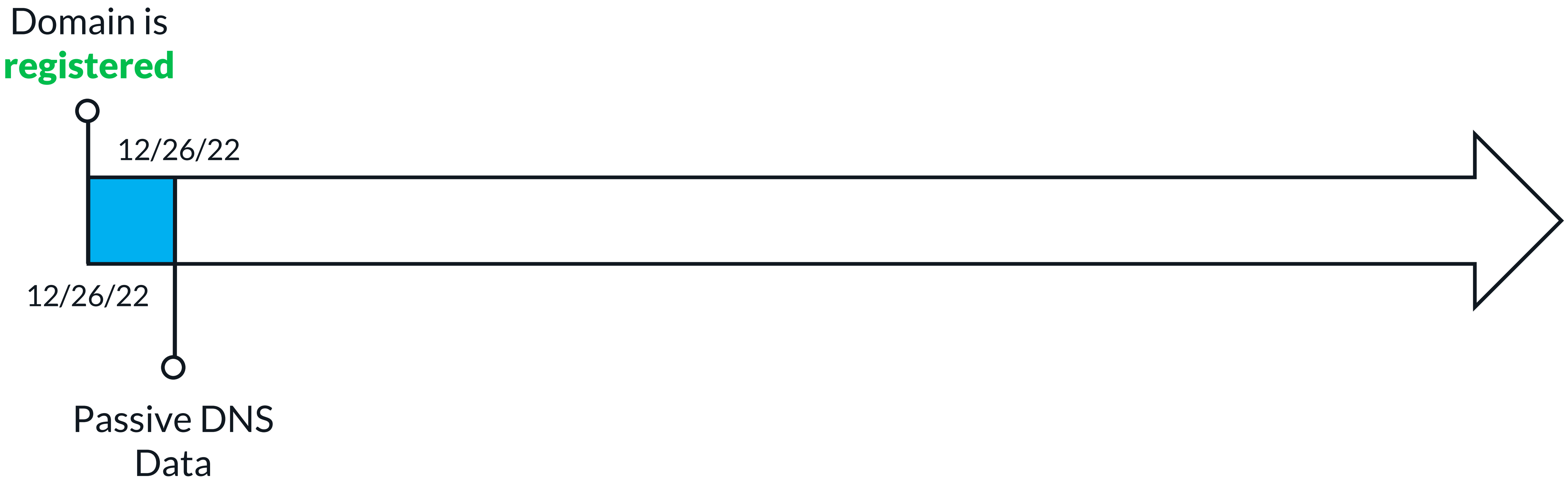
infoblox

TRADITIONAL THREAT INTELLIGENCE

WE NEED TO KNOW WHY TO BLOCK RIGHT?

Domain Lifecycle

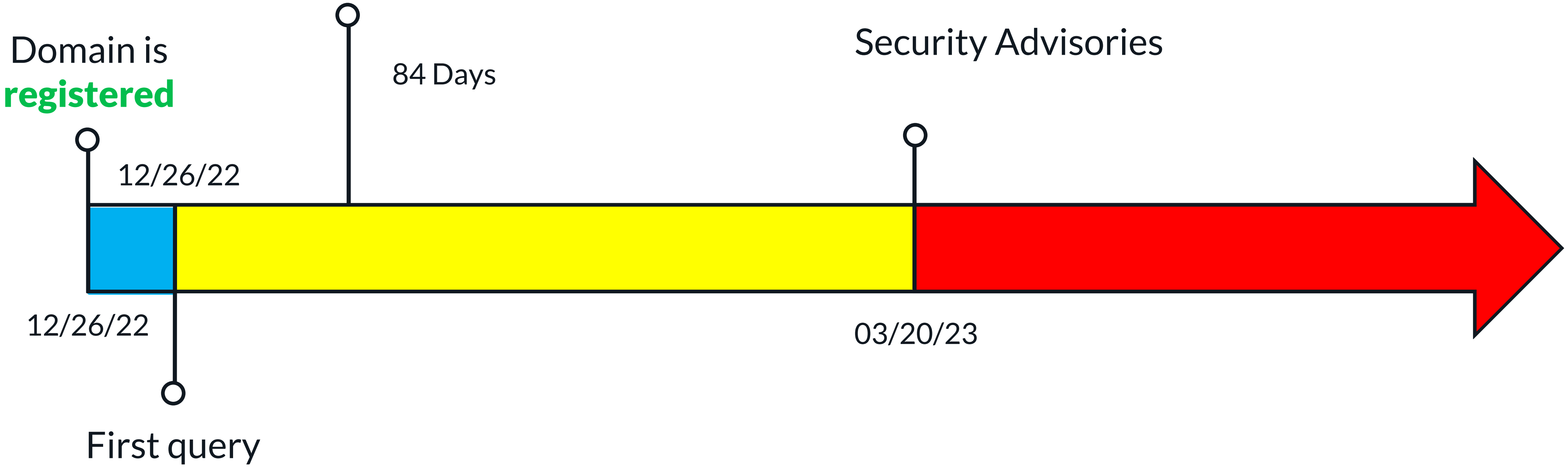
Example IoC: pbxphonenetwork[.]com



Domain Lifecycle

Example IoC: pbxphonenetwork[.]com

Window of Impact (12/26 – 3/20)



NEW APPROACH

SUSPICIOUS DOMAINS

- In order to prepare for attack, even attacker must start somewhere
  - Having domain name as it would be weird to send you mail with, please connect to this IP here
    - Need to either highjack or register domain name.
  - In domain zone you can hide the IP until the last minute
    - You will simply change the IP as needed
  - But the zone need to be hosted somewhere
    - Cloudflare or similar, own name server …

- Such domain can be look-a-like, totally fresh or even strategically aged

Lookalike Domains

- Visually similar
- Designed to trick human beings

What is similar?

- It depends.

Let’s take a look!

infoblox

A DEEP3R LOOK AT LOOKAL1KE ATTACKS

NEW STUDY REVEALS LATEST THREAT VECTORS

April 2023

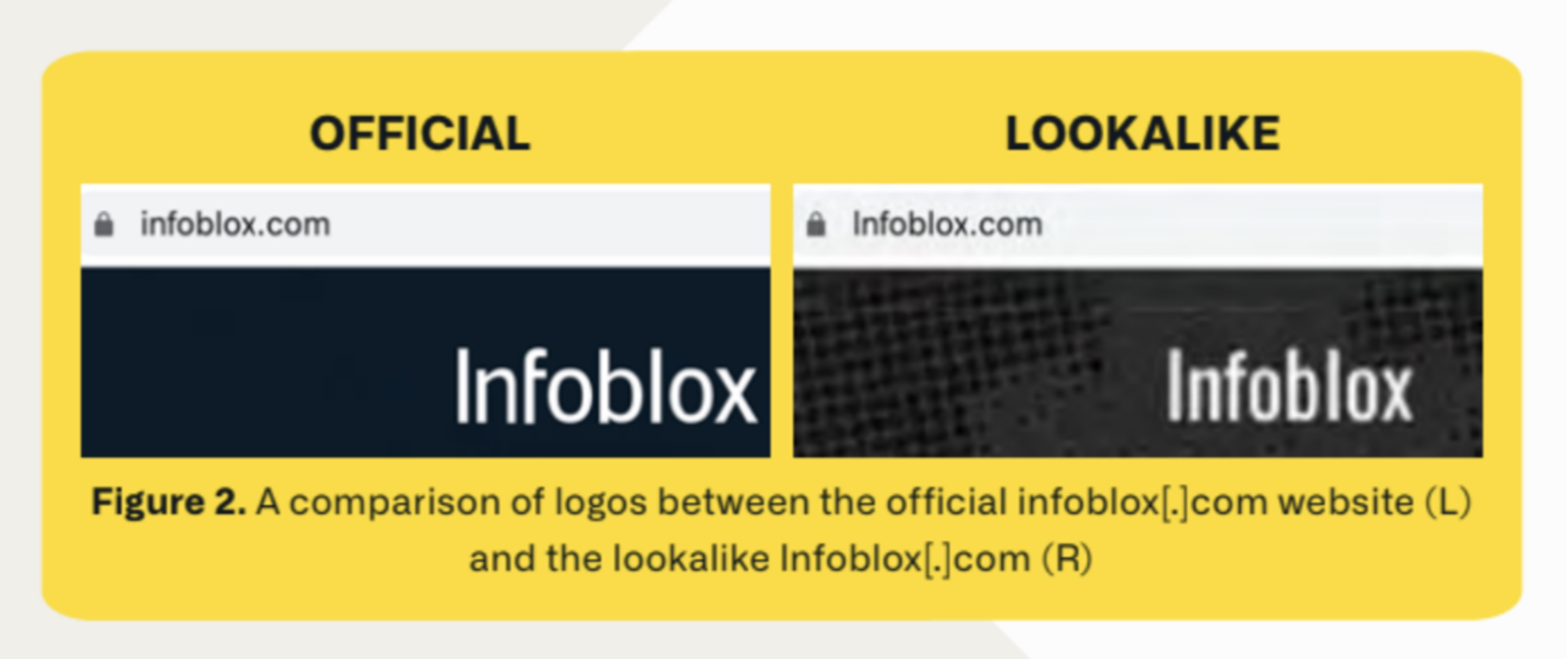
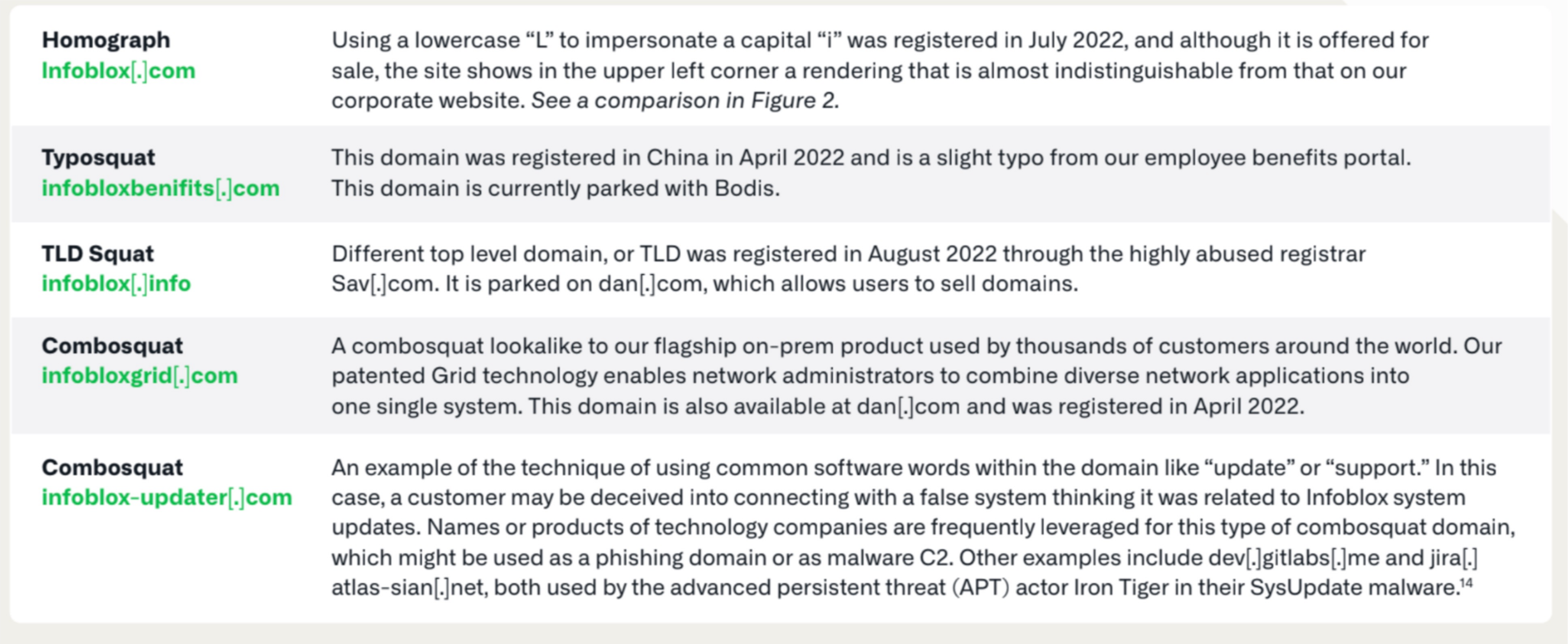


Figure 2. A comparison of logos between the official infoblox[.]com website (L) and the lookalike Infoblox[.]com (R)

Infoblox.com and Infoblox.com- try that at 7 point font!

Everyone is a Target! Example Infoblox.



Homograph Infoblox[.]com	Using a lowercase "L" to impersonate a capital "i" was registered in July 2022, and although it is offered for sale, the site shows in the upper left corner a rendering that is almost indistinguishable from that on our corporate website. *See a comparison in Figure 2.*
Typosquat infobloxbenifits[.]com	This domain was registered in China in April 2022 and is a slight typo from our employee benefits portal. This domain is currently parked with Bodis.
TLD Squat infoblox[.]info	Different top level domain, or TLD was registered in August 2022 through the highly abused registrar Sav[.]com. It is parked on dan[.]com, which allows users to sell domains.
Combosquat infobloxgrid[.]com	A combosquat lookalike to our flagship on-prem product used by thousands of customers around the world. Our patented Grid technology enables network administrators to combine diverse network applications into one single system. This domain is also available at dan[.]com and was registered in April 2022.
Combosquat infoblox-updater[.]com	An example of the technique of using common software words within the domain like "update" or "support." In this case, a customer may be deceived into connecting with a false system thinking it was related to Infoblox system updates. Names or products of technology companies are frequently leveraged for this type of combosquat domain, which might be used as a phishing domain or as malware C2. Other examples include dev[.]gitlabs[.]me and jira[.]atlas-sian[.]net, both used by the advanced persistent threat (APT) actor Iron Tiger in their SysUpdate malware.[14]

Lookalike Domain Detection

paypal.com	**pąypąl.com**	**paypal.com**	Text
xn--pypl-53dc.com	xn--pypl-btac.com	paypal.com	Punycode

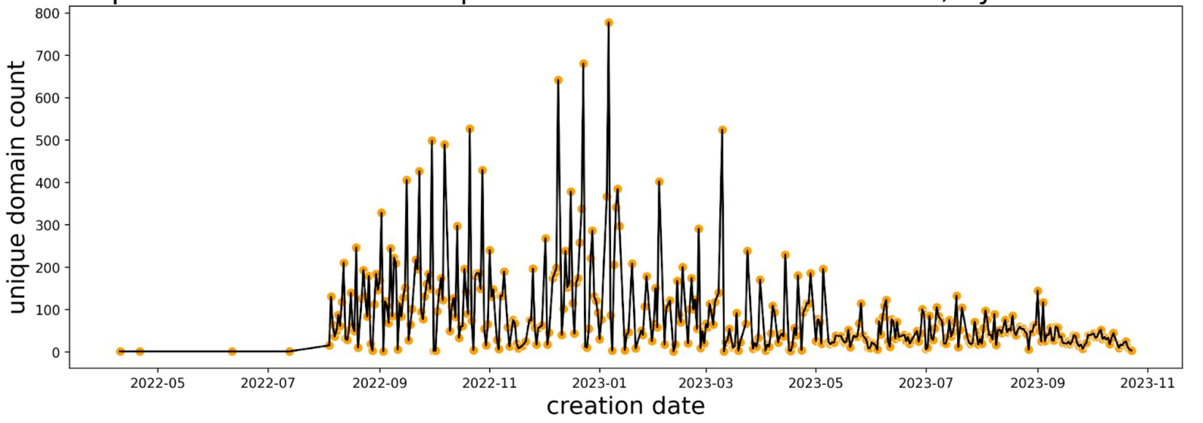
google.com	**google.com**	**google.com**	Text
google.com	xn--ggle-0nda.com	xn--ggle-55da.com	Punycode

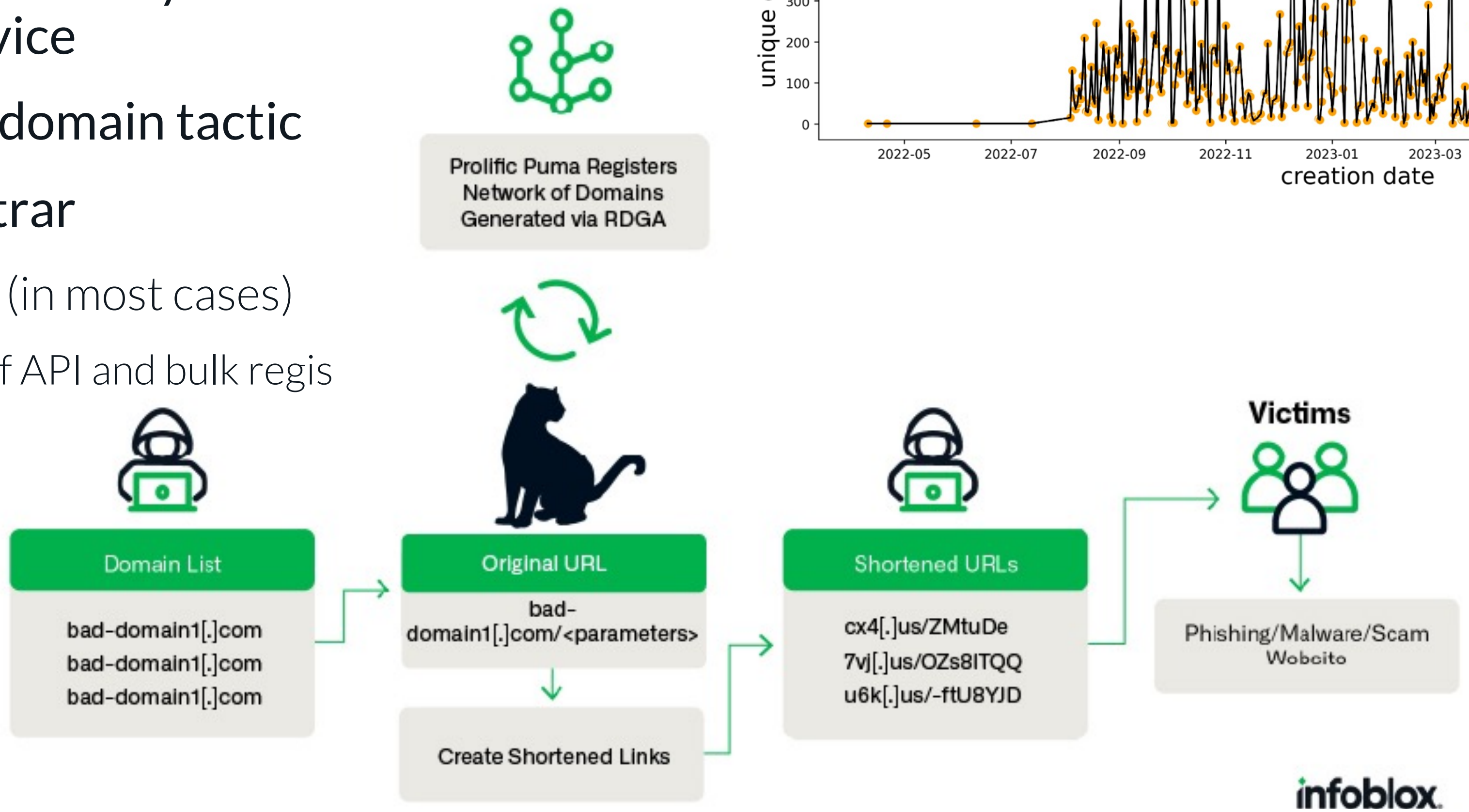
RDGA – Registered Domain Generation Algorithm

Example of “Prolific Puma” threat actor

- Use of ”.us” TLD
- Not attacker directly only as a service
- Use of aging domain tactic
- Use of Registrar
  - NameSilo (in most cases)
    - Use of API and bulk regis

Unique number of domains part of the Prolific Puma network, by creation date





Prolific Puma Registers Network of Domains Generated via RDGA

Domain List

bad-domain1[.]com
bad-domain1[.]com
bad-domain1[.]com

Original URL

bad-domain1[.]com/<parameters>

Create Shortened Links

Shortened URLs

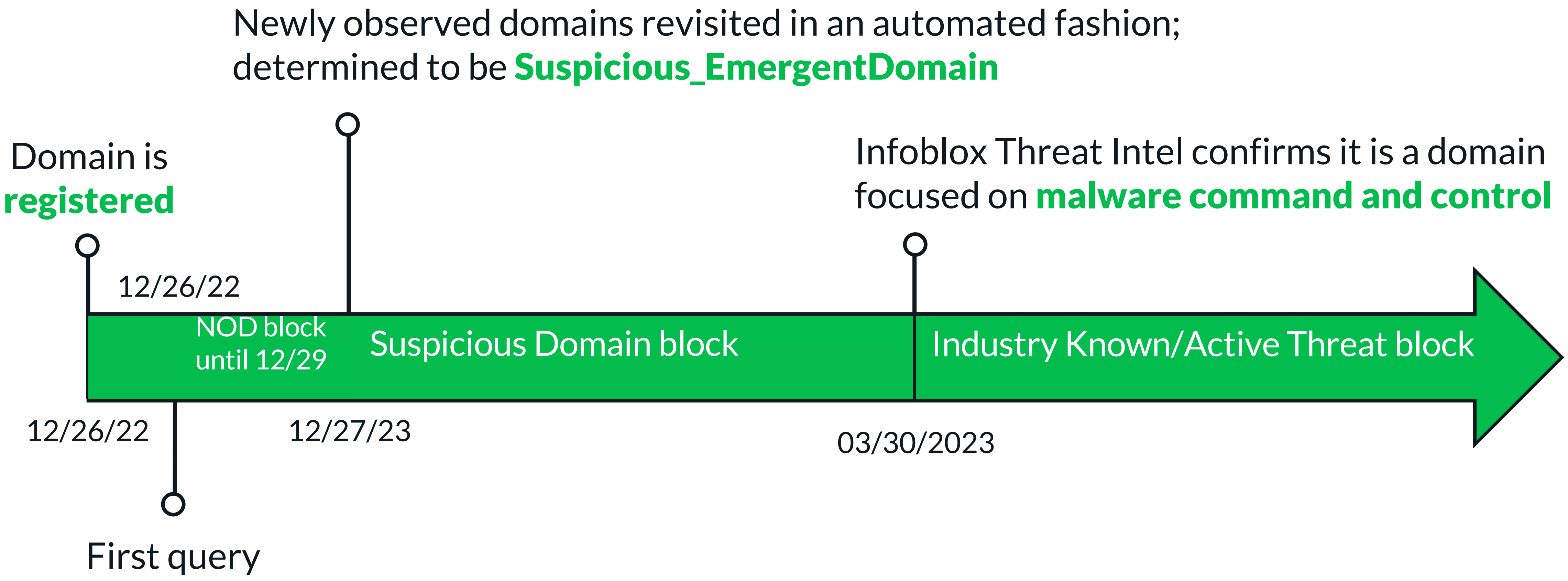
cx4[.]us/ZMtuDe
7vj[.]us/OZs8ITQQ
u6k[.]us/-ftU8YJD

Victims

Phishing/Malware/Scam Website

Domain Lifecycle

Example IoC: pbxphonenetwork[.]com

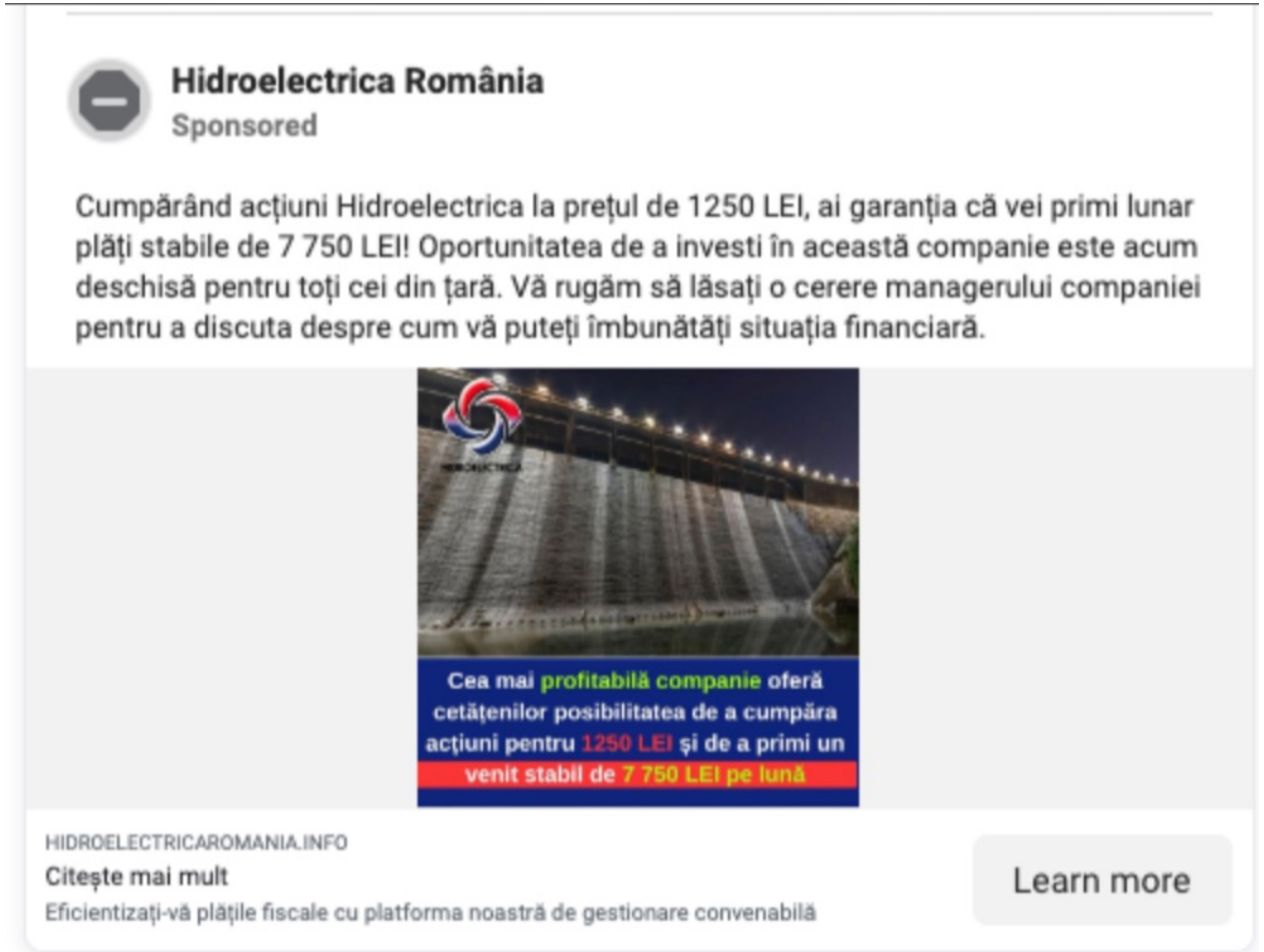


Newly observed domains revisited in an automated fashion; determined to be **Suspicious_EmergentDomain**

Domain is **registered**

Infoblox Threat Intel confirms it is a domain focused on **malware command and control**

First query



Hidroelectrica România

Sponsored

Cumpărând acțiuni Hidroelectrica la prețul de 1250 LEI, ai garanția că vei primi lunar plăți stabile de 7 750 LEI! Oportunitatea de a investi în această companie este acum deschisă pentru toți cei din țară. Vă rugăm să lăsați o cerere managerului companiei pentru a discuta despre cum vă puteți îmbunătăți situația financiară.

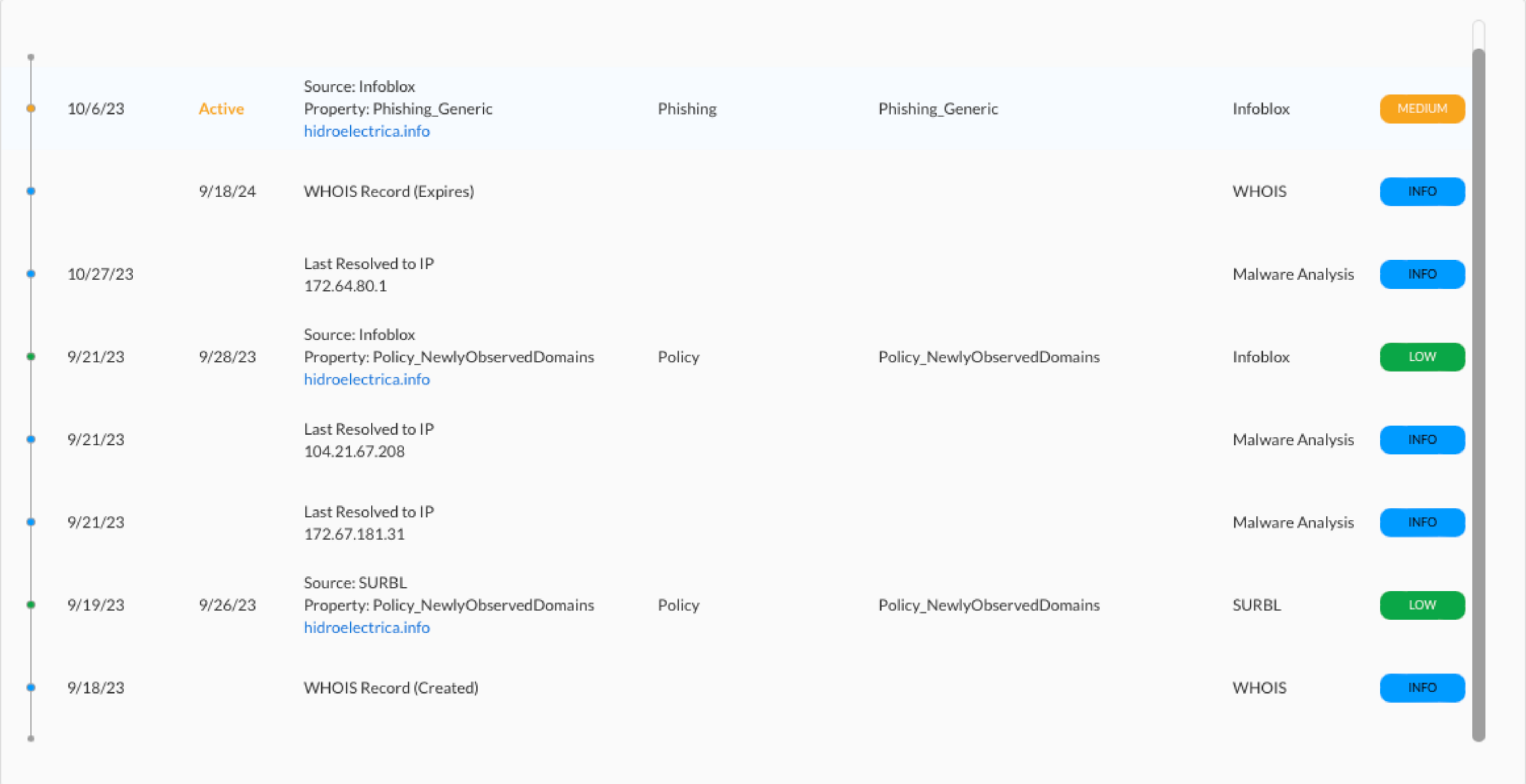
Cea mai profitabilă companie oferă cetățenilor posibilitatea de a cumpăra acțiuni pentru 1250 LEI şi de a primi un venit stabil de 7 750 LEI pe lună

HIDROELECTRICAROMANIA.INFO

Citește mai mult

Eficientizați-vă plățile fiscale cu platforma noastră de gestionare convenabilă

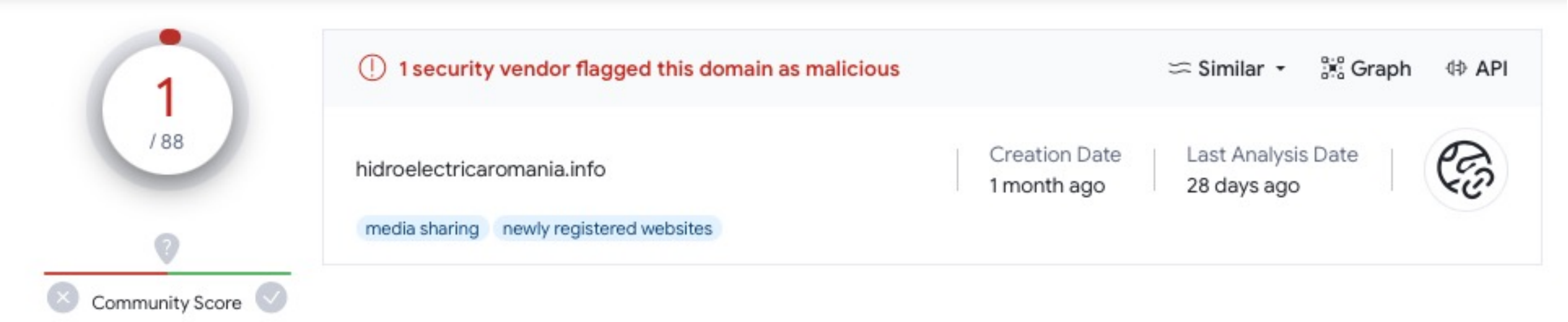
Example of local threat: hidroelectricaromania[.]info



10/6/23	Active	Source: Infoblox Property: Phishing_Generic hidroelectrica.info	Phishing	Phishing_Generic	Infoblox	MEDIUM
	9/18/24	WHOIS Record (Expires)			WHOIS	INFO
10/27/23		Last Resolved to IP 172.64.80.1			Malware Analysis	INFO
9/21/23	9/28/23	Source: Infoblox Property: Policy_NewlyObservedDomains hidroelectrica.info	Policy	Policy_NewlyObservedDomains	Infoblox	LOW
9/21/23		Last Resolved to IP 104.21.67.208			Malware Analysis	INFO
9/21/23		Last Resolved to IP 172.67.181.31			Malware Analysis	INFO
9/19/23	9/26/23	Source: SURBL Property: Policy_NewlyObservedDomains hidroelectrica.info	Policy	Policy_NewlyObservedDomains	SURBL	LOW
9/18/23		WHOIS Record (Created)			WHOIS	INFO

And how about traditional approach?

Lets wait for the threat to be seen!



1 / 88

Community Score

1 security vendor flagged this domain as malicious

hidroelectricaromania.info

Creation Date
1 month ago

Last Analysis Date
28 days ago

media sharing
newly registered websites

ありがとう

köszönjük

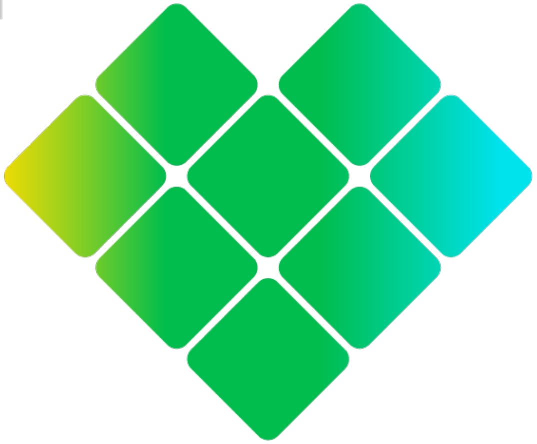
Cảm ơn

धन्यवाद

terima kasih

gracias

고마워요



teşekkür ederim

Σας ευχαριστ

Спасибо

obrigado

grazie

merci

THANK YOU!

谢谢

takk

ขอบคุณ

شكرا

tack

danke

bedankt

kiitos

infoblox