

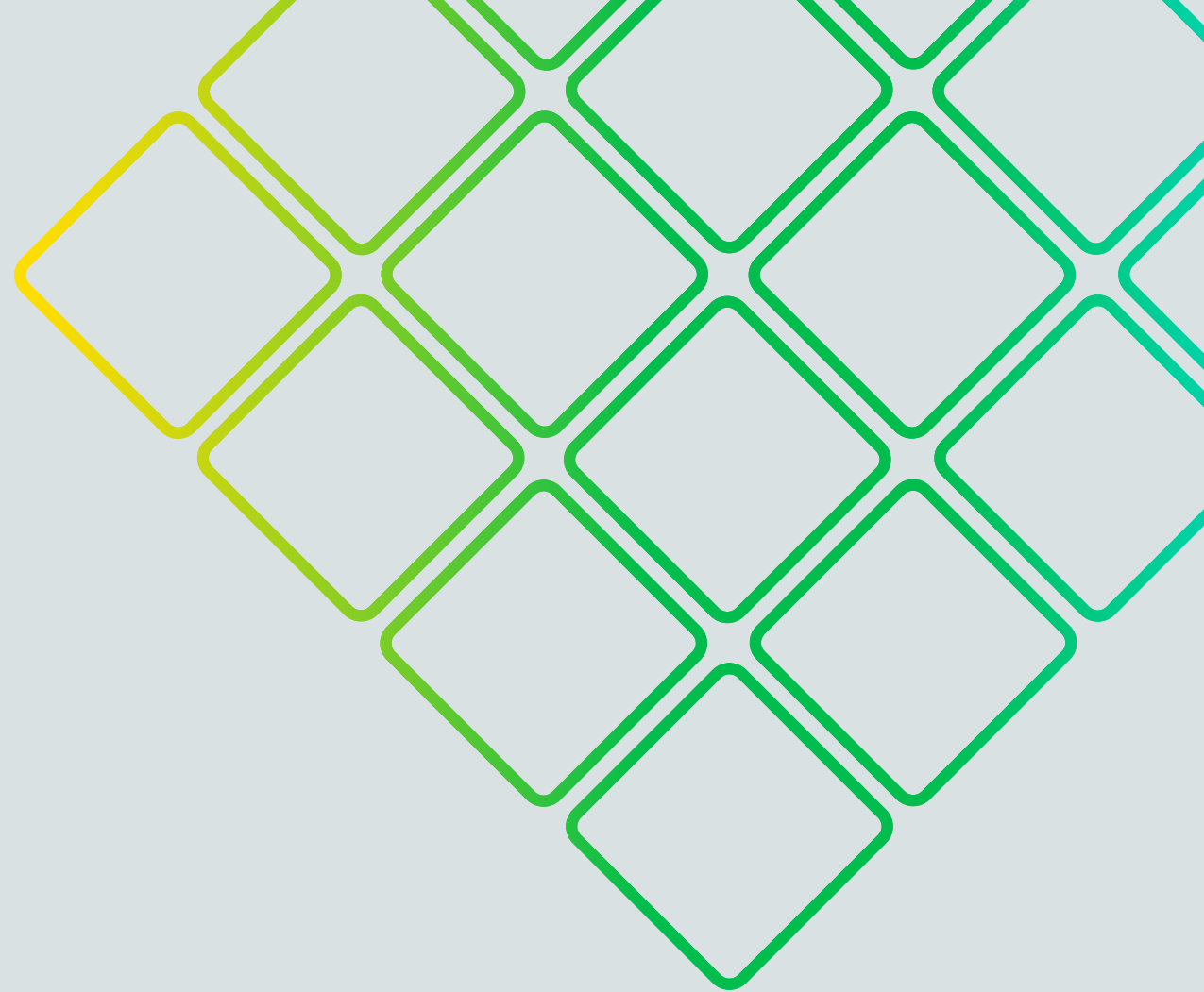


DNS ATT&CK

LOOKALIKE DOMAINS

Cosmin Vilcu
Territory Account Manager
cvilcu@infoblox.com

Jan Rynes
Solution Architect
jrynes@infoblox.com



SECURE DNS LEADING VENDOR

US COMPANY
12,000+ CUSTOMERS

Gartner®

„Infoblox accounting for approximately
50% of the existing installed base”

8000⁺
CUSTOMERS

50%
MARKET
SHARE

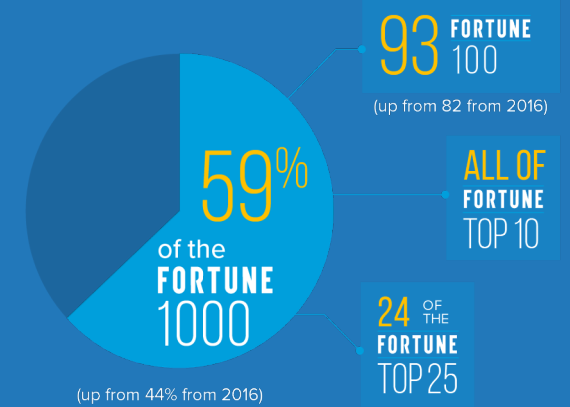
133
COUNTRIES

1000⁺
PARTNERS

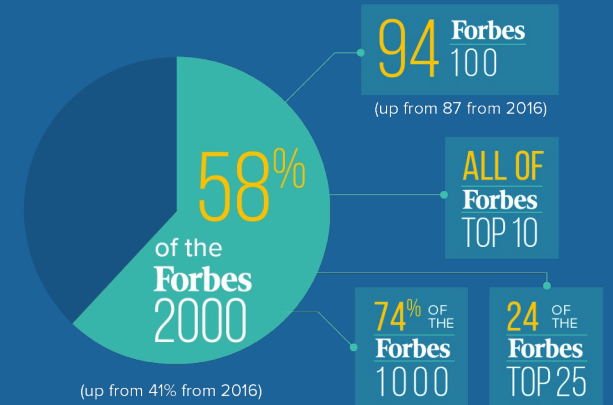
58.4
NPS

95.4
CUSTOMERS SAT.

FORTUNE 1000



Forbes 2000

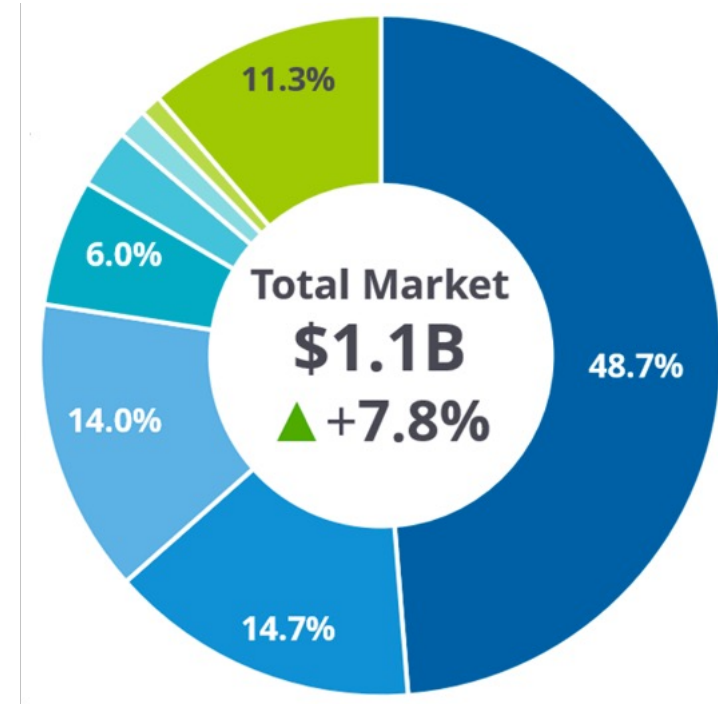


SECURE DDI LEADER

- US COMPANY WITH 20+ YEARS OF EXPERIENCE
- 12,000+ CUSTOMERS
- 93 FROM FORTUNE 100
- 350 FROM FORTUNE 500

Gartner[®]

„Infoblox accounting for approximately 50% of the existing installed base”



IDC
ANALYZE THE FUTURE

Worldwide DDI
Market Shares, 2021

Infoblox

MARKET LEADERS CHOOSE INFOBLOX

Telecom	
Retail	
Manufacturing	
Media and Internet	
Transportation	
Government	
Life Sciences	
Financial Services	
Education	
Energy	
Technology	

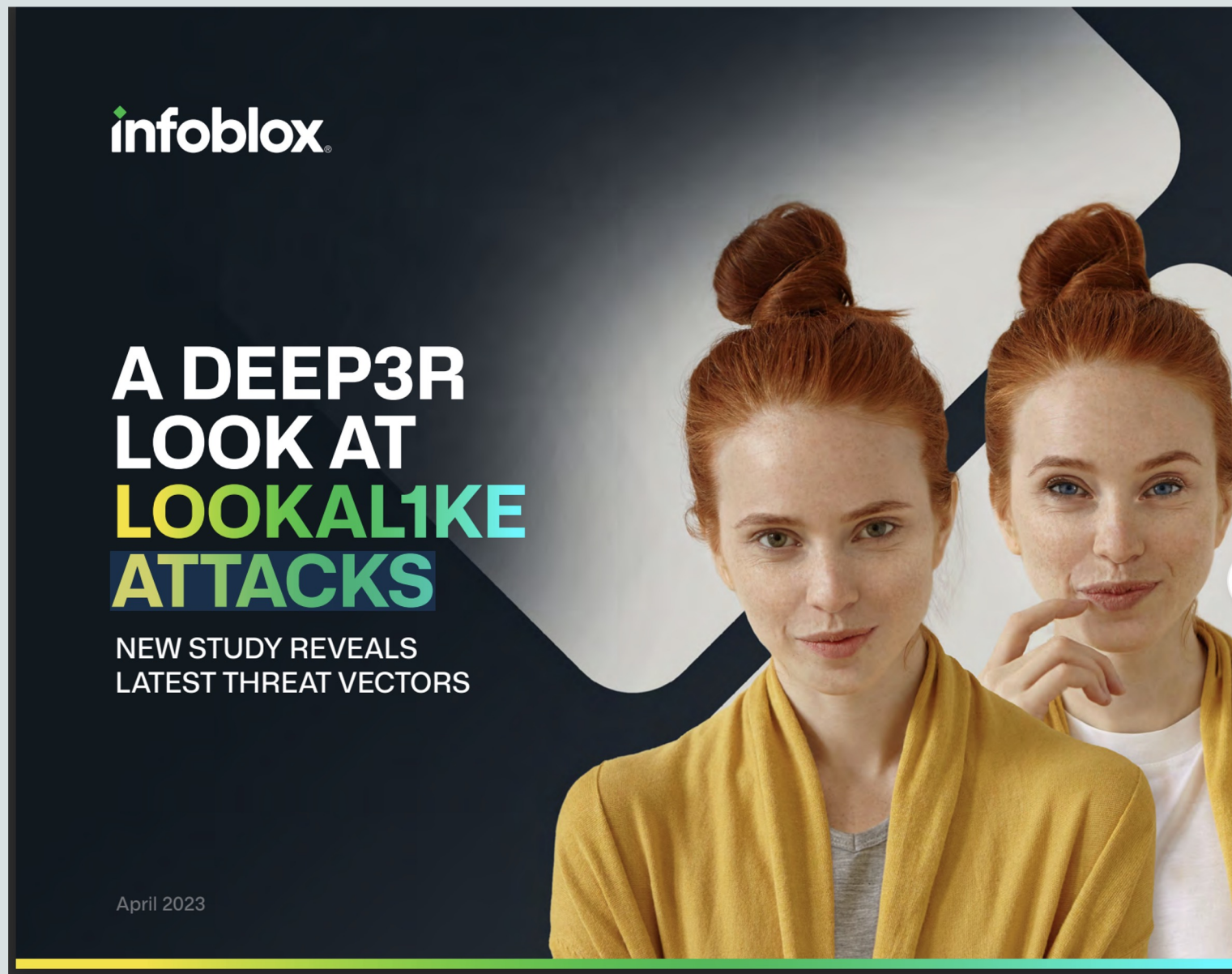
Lookalike Domains

- Visually similar
- Designed to trick human beings

What is similar?

- It depends.

Let's take a look!



infoblox

**A DEEP3R
LOOK AT
LOOKALIKE
ATTACKS**

NEW STUDY REVEALS
LATEST THREAT VECTORS

April 2023

Lookalike Domain Detection

Detects from Newly Observed Domains (NOD), domain names that try to mimic popular domains (Alexa top-100) or strategic domains for phishing (e.g. banks) and spamming.

Detects domains that overlaps and/or have homograph n-grams, e.g. letter 'O' and number '0' are considered homographs. Use distance analysis to detect the likelihood of lookalike attacks

SOA record is analyzed and used for catching false positives.

Detects

- Letter replacement, example g00gle.com, google.com, bankofthevest.com, rn1cr0soft.com



Lookalike domain techniques

TECHNIQUES TO CREATE LOOK-ALIKE DOMAIN NAMES

TLD swap	phishlabs.tech	Omission	phshlabs.com
Subdomains	phish.labs.com	Transposition	phsihlabs.com
Typosquatting	phishlavs.com	Insertion	phishxlabs.com
Hyphenation	phish-labs.com	Homoglyph	phishlaᄁbs.com
Repetition	phishllabs.com	Vowel-swap	phishlebs.com
Replacement	ph1shlabs.com	Addition	phishlabss.com

OFFICIAL



LOOKALIKE



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 [infobloxbenefits\[.\]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	paypał.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

Examples from Romania

14:18

post.youxinc.pub

POȘTA ROMÂNĂ

Total: 2.23 LEI

Metode de plată acceptate:

VISA, Mastercard, AMEX, DISCOVER, JCB

POLITICA DE CONFIDENTIALITATE
PROTECȚIA DATELOR CU CARACTER PERSONAL

Măta

1234

12/34 1234

Plățiți acum

Despre noi

Legislație

Conducere

Organizare și funcționare

f, t, g+, +

40

14:40

parcel-romania.com

POȘTA ROMÂNĂ

RO Cauta in site

POLITICA DE CONFIDENTIALITATE
PROTECȚIA DATELOR CU CARACTER PERSONAL

te un serviciu complet securizat, în conformitate

Track & Trace

CAUTĂ ÎN ROMÂNIA

Un serviciu oferit de Poșta Română

RO215296951HU

Cauta

Vrei sa primești notificare prin email? Click aici!

CHESTIONAR EVALUARE SERVICIUL DE CURIERAT POȘTA ROMÂNĂ

- Poșta Română folosește un cod standard de identificare format din 13 caractere (AB123456789CD)
- Codul de urmărire utilizat de alți operatori poate avea o structură diferită.
- Pentru trimerile postale trimise în străinătate, codul de

f, t, g+, +

< > ↗ 📖 📄

Scam

Scurte instrucțiuni despre cum să începeți să câștigați pe "RomTrading"

- Utilizați link-ul furnizat de Robert Turcescu.
- Alimentați-vă soldul. Depozitul minim pentru a începe programul este de 1200 de lei românești.
- În câteva minute, programul va începe tranzacțiile.
- Retragera banilor se poate face în orice moment. Acesta este creditat în cont în 2-3 ore (în funcție de bancă).
- Până la **9/26/2023** , înregistrarea conturilor va fi gratuită.

```
https://whossoeverfop.top/?_lp=1&_token=uuid_1ef0p0t2ipk2_1ef0p0t2ipk26512a0171b5166.83493319&pixel_id=667248275436131&sub_3=a8400y35rob
```

VIZITAȚI SITE-UL OFICIAL

Scam

Dossier™ Threat Research Portal

Enter a domain, IP Address, Hostname, EMail, URL, or Hash value...

Search

Resources

whossoeverfop.top

Last Active Threat Detection: 09/13/2023 (Active) [Add to Custom List](#) [Generate API Request](#) [Feedback on Results](#) [Export](#)

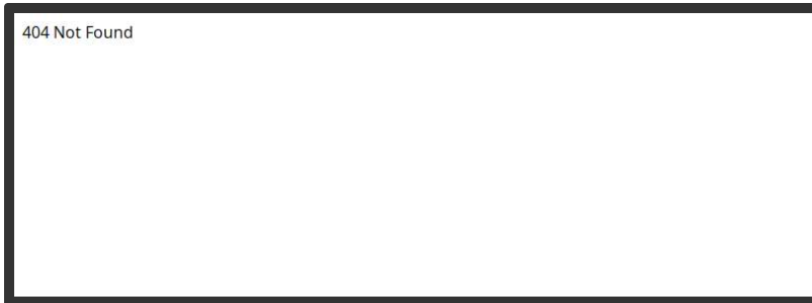
Summary

More Details

- Impacted Devices
- Current DNS
- Related Domains
- Related URLs
- Related IPs
- Related File Samples
- Related Contacts
- Metadata
- Timeline
- Threat Actor
- MITRE ATT&CK™
- WHOIS Record
- Raw Whois

Summary

Domain Screen Image



Full Image

7 DNS Record Count | 0 Domain/Subdomain Count | 0 URL Count | 4 IP Count

Categorizations

Infoblox Info	Virus Total key has not yet been configured for this account
Infoblox TLD Score	High Risk (7)
Infoblox Threat Property	Suspicious_EmergentDomain
Infoblox Nameserver Reputation	Moderate Risk (5)

Registered Owner (WHOIS)

Infoblox Threat Level

Threat Level is designed to help users understand how dangerous an indicator can be, since not all malware behave the same way. The information can be used in combination with other scores from Infoblox.

5.8/10



Infoblox Risk Level

The Risk score represents the likelihood that a user will be exposed to a threat or compromised by interacting with the indicator.

8/10



Infoblox Confidence Level

The Confidence Score provides additional insight into the indicator class and property. It represents our level of trust in the classification and threat of the indicator.

High

Infoblox Threat Intelligence Group Research Notes

Emergent domain recently observed by Infoblox found to have suspicious registration, behavior, or common associations with known threats. Some of the domain's characteristics are: domain created on 2023-09-11. Registered with a highly abused registrar based on the Infoblox registrar reputation score. Using TLD that has high risk of being abused for hosting malicious indicators per Infoblox TLD reputation score.

Active Threat Feeds and Status

Info Low Medium High

Suspicious-noed



Easy money 😊

Dossier™ Threat Research Portal

Enter a domain, IP Address, Hostname, EMail, URL, or Hash value...

hidroelectrica.info

Summary

More Details

Impacted Devices

Current DNS

Related Domains

Related URLs

Related IPs

Related File Samples

Related Contacts

Metadata

Timeline

Threat Actor

MITRE ATT&CK™

WHOIS Record

Raw Whois

Summary

Domain Screen Image



Full Image

13 DNS Record Count	0 Domain/Subdomain Count	0 URL Count	5 IP Count
-------------------------------	------------------------------------	-----------------------	----------------------

Categorizations

Infoblox Nameserver Reputation	Moderate Risk (5)	▼
Infoblox TLD Score	Moderate Risk (6)	▼
Infoblox Web Category	Finance - Other	
Infoblox Threat Property	Phishing_Generic	
Infoblox Info	Virus Total key has not yet been configured for this account	

Link to ad

This ad is from a URL link

Library ID: 1048050422876681

Inactive

6 Oct 2023 - 7 Oct 2023

Platforms

EU transparency

See ad details



Hidroelectrica România
Sponsored

Cumpărând 10 acțiuni ale celei mai profitabile companii Hidroelectrica la prețul de 1200 RON, ai garanția că vei primi plăți de 7 500 RON pe lună! Investițiile în companie sunt acum disponibile pentru toți cei din țară - lăsați o solicitare telefonică managerului companiei și veți putea să vă îmbunătățiți situația financiară.



DEMYQEAGAE.COM

Citește mai mult

Acțiunile reprezintă dreptul de proprietate al unei fracțiuni din capitalul social al unei societăți pe acțiuni, adică atunci când cumpărați o acțiune, obțineți o parte dintr-o...

Learn more

Close

X

Lookalike – partial match



DATUM 14/06/2021

SLEDOVACÍ KÓD BUDE ZASLÁN PO
PROVEDENÍ PLATBY!

CELKOVÁ ČÁSTKA: 53,47 Kč

ZPŮSOB PLATBY :

 Kreditní karta

PLATIT A POKRAČOVAT

ZRUŠIT

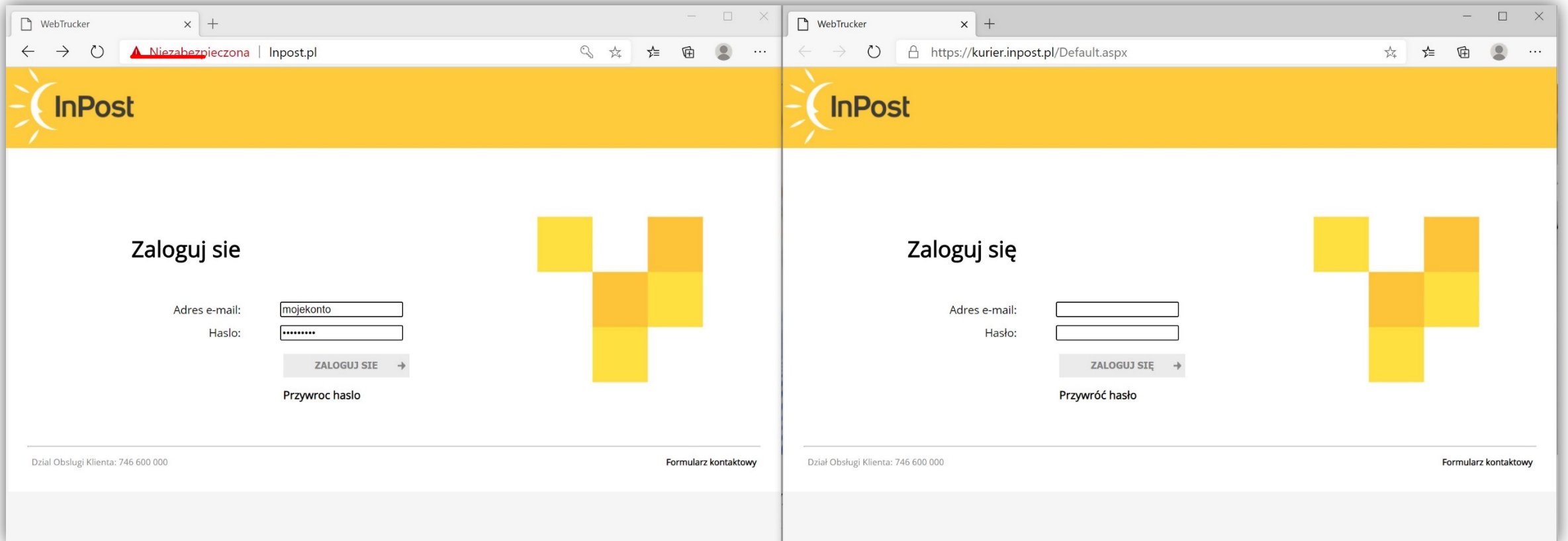
Ceskapostapay[.]com

192[.]64[.]117[.]221 Malicious Activity!

Effective URL: [https://ceskapostapay\[.\]com/payment/Package/Select-payment-method.php?NAME_PATH=track_yy_dl24&SCREEN=identification_contrat_...](https://ceskapostapay[.]com/payment/Package/Select-payment-method.php?NAME_PATH=track_yy_dl24&SCREEN=identification_contrat_...)

WHOIS Record (Created)	2021-06-14T01:40:11+00:00
Policy_NewlyObservedDomains	2021-06-14T01:44:32.000Z
MalwareDownload_Generic	2021-06-15T05:51:33.037Z

Letter replacement: InPost.pl



Fake: `<form method="post" action="hXXp://18.194.99[.]238/post.php"index.html" class="account" name="sign-in" id="form1">`

Original: `<form method="post" action="./Default.aspx?ReturnUrl=%2f" id="form1">`

Lookalike + web advertisement (!)

Google

getin bank

All Maps News Images Videos More Settings Tools

About 4,770,000 results (0.59 seconds)

Ad · www.getin-secure-bank.xyz/ ▾
GETIN | Online Bank | getin-secure-bank.xyz
Konta osobiste, lokaty, kredyty, leasing. Oferta **Getin Banku** ze względu na swą kompleksowość i innowacyjność.

www.getinbank.pl ▾ Translate this page
Getin Bank - Klienci Indywidualni
Konta osobiste, lokaty, kredyty, leasing. Oferta **Getin Banku** ze względu na swą innowacyjność, zainteresuje szczególnie osoby oczekujące ...
You've visited this page 3 times. Last visit: 1/9/20

sgb

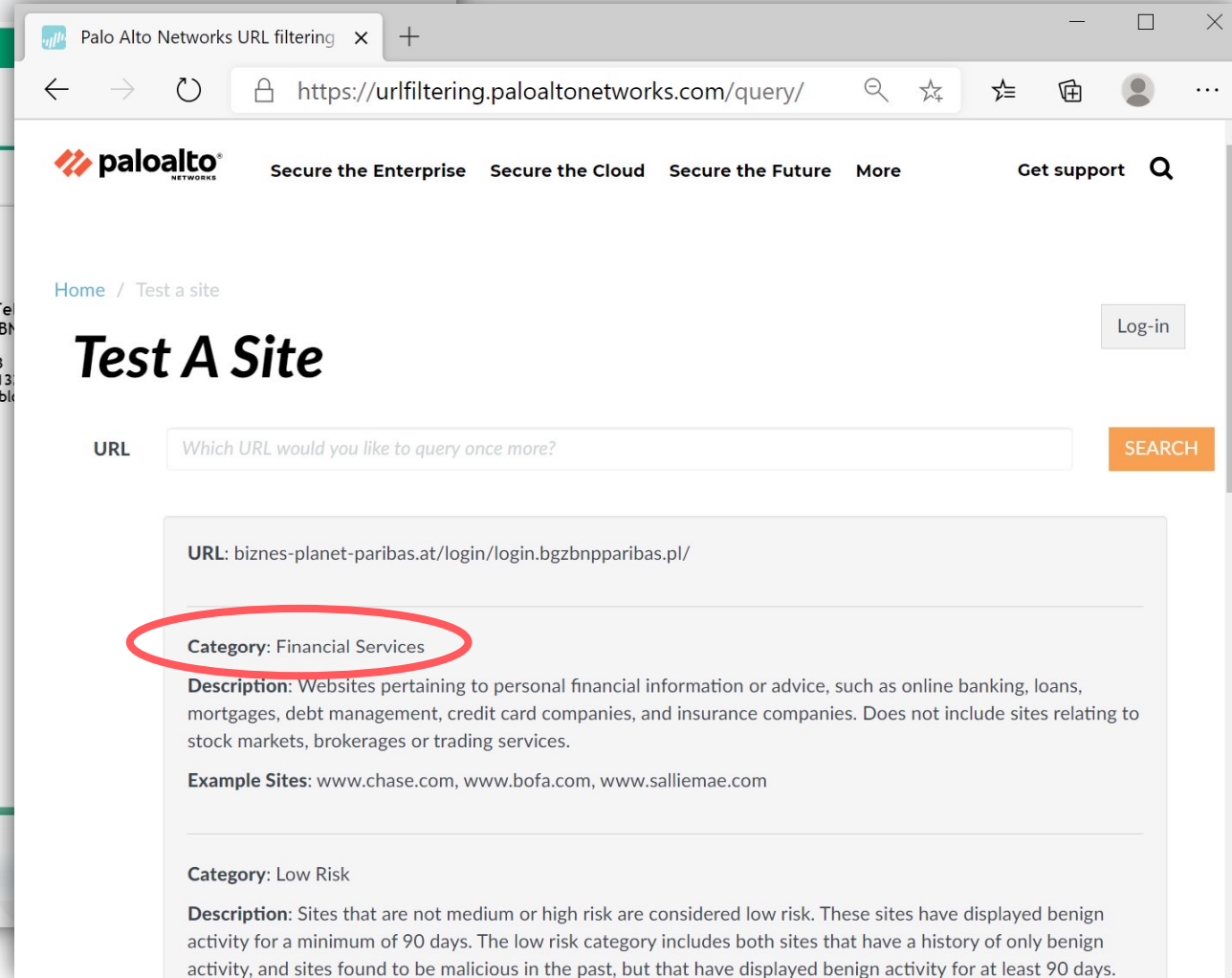
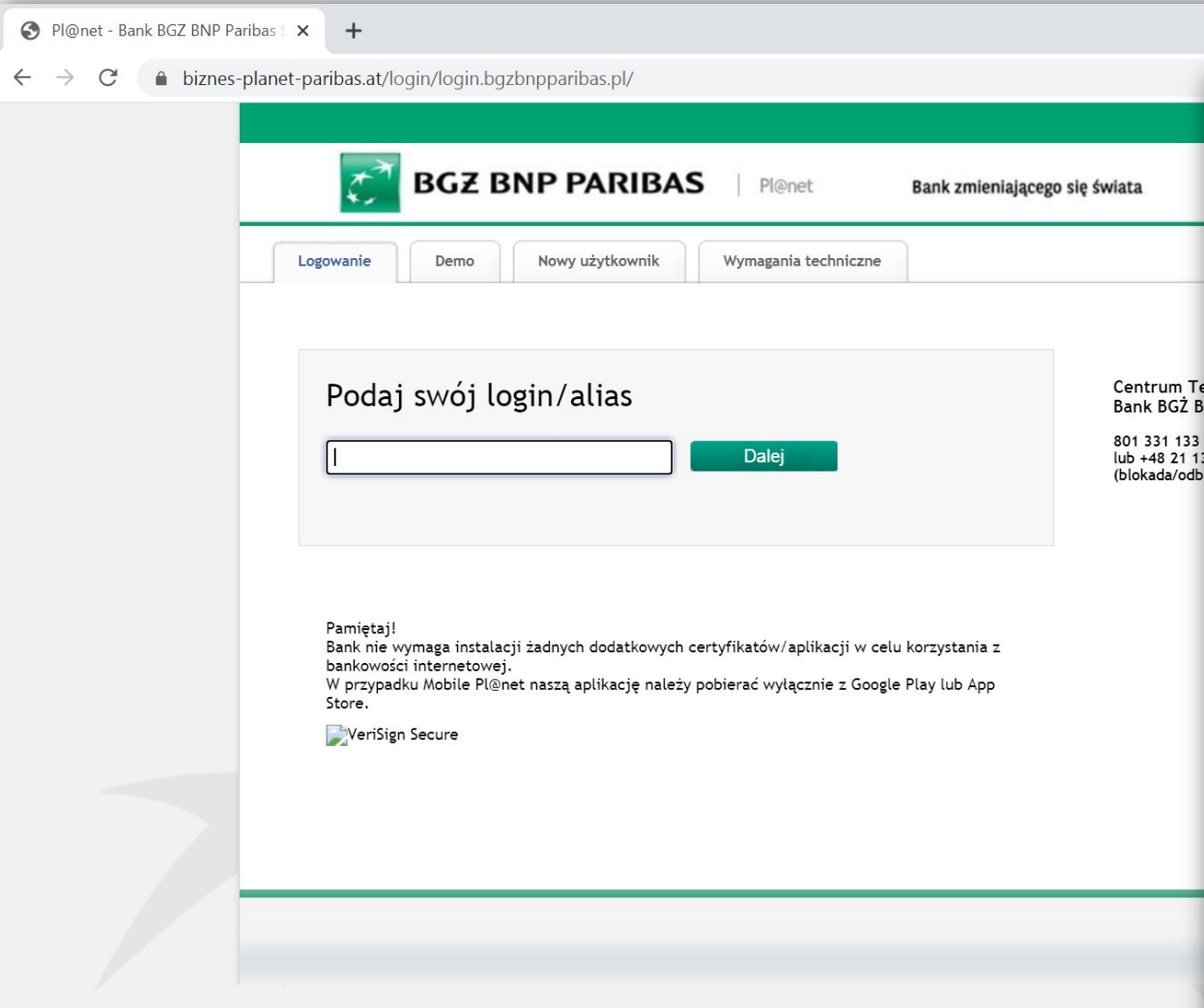
All Images Videos News Maps More Settings Tools

About 22,800,000 results (0.74 seconds)

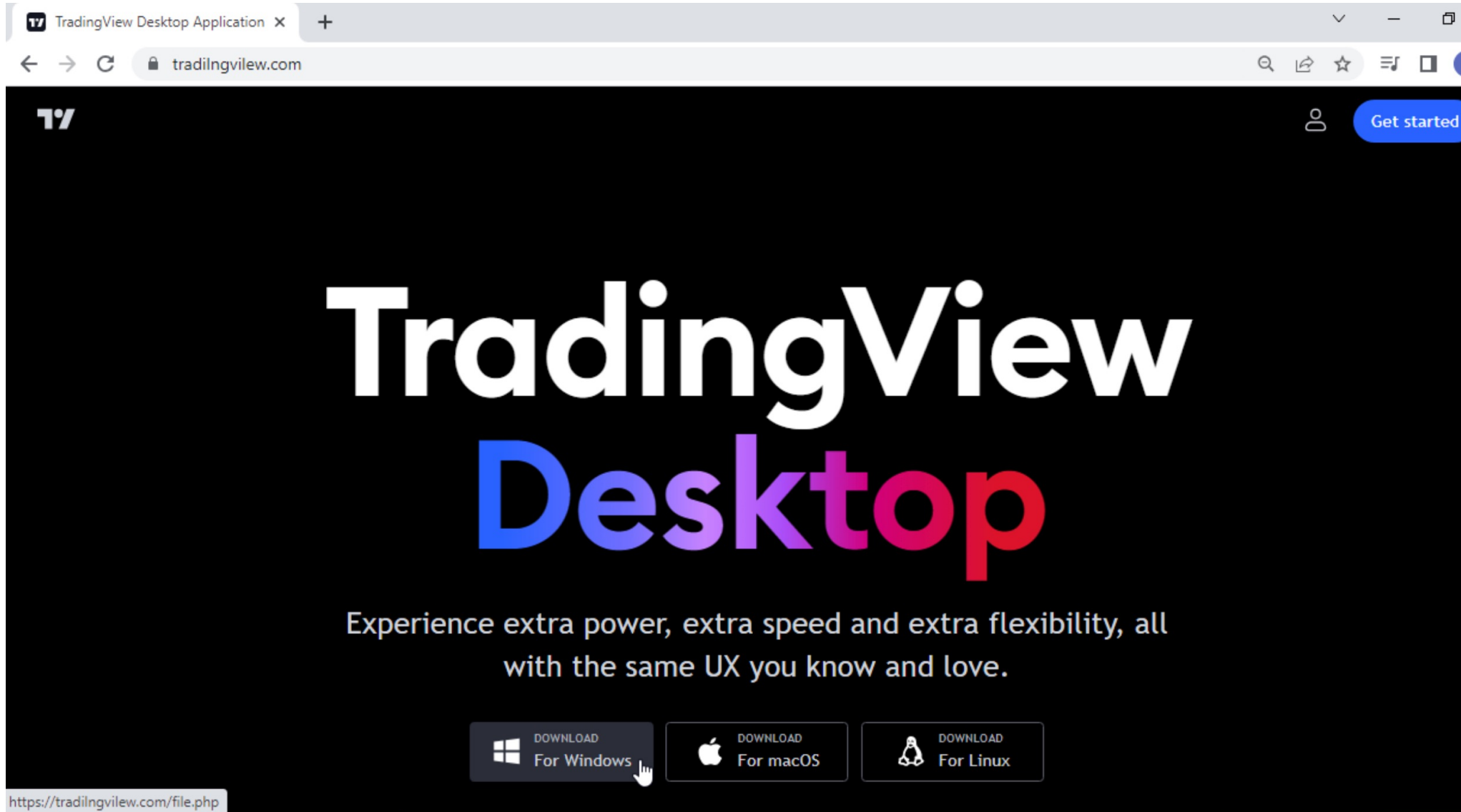
Ad www.sgb.pl/ ▾
SGB.pl - SGB24IBank - SGB24IBiznes
Skorzystaj z nowej elastycznej bankowości internetowej i mobilnej. Dostosuj SGB24IBIZNES do swoich preferencji korzystania z produktów i usług.

<https://sgb-24.at> /secure/c8003551a70f30affdfe82ee8db24265/login/?kw=sgb24&device=c&lp=1

Lookalike + redirect to legitimate page



Letter addition



The image shows a web browser window with the URL `tradingview.com`. The page features the TradingView logo in the top left and a "Get started" button in the top right. The main heading is "TradingView Desktop" in a large, white and colorful font. Below the heading is the text "Experience extra power, extra speed and extra flexibility, all with the same UX you know and love." At the bottom, there are three buttons for downloading the application: "DOWNLOAD For Windows", "DOWNLOAD For macOS", and "DOWNLOAD For Linux". A mouse cursor is pointing at the Windows button. The address bar at the bottom left shows the URL `https://tradingview.com/file.php`.

TradingView Desktop

Experience extra power, extra speed and extra flexibility, all with the same UX you know and love.

DOWNLOAD For Windows

DOWNLOAD For macOS

DOWNLOAD For Linux

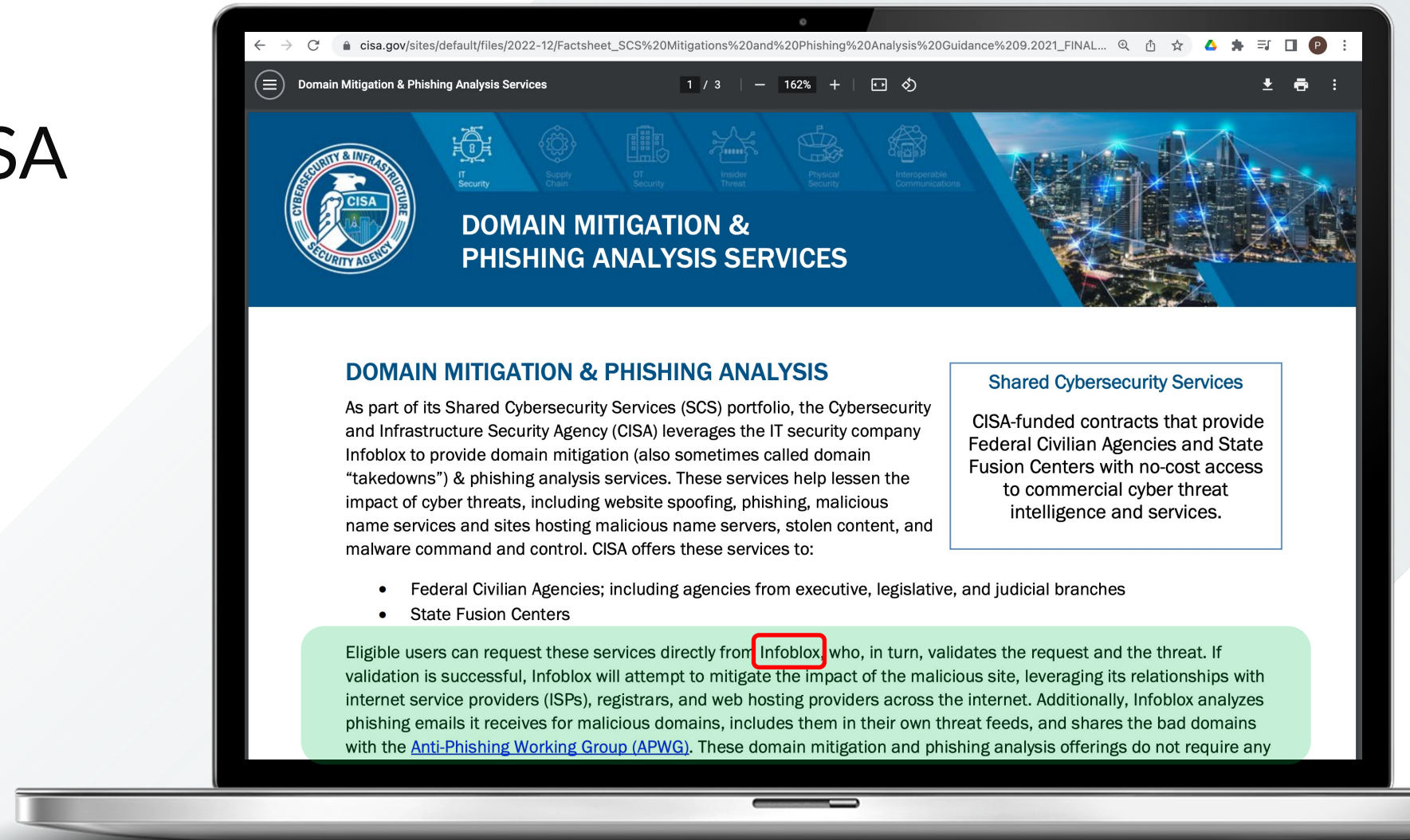
<https://tradingview.com/file.php>

C2 from Steam / Telegram profiles

The image shows two overlapping browser windows. The background window is a Steam profile page for user 'r0chnu' with IP address 'http://128.140.35.86'. The profile picture is a question mark. A tooltip shows 'This user has also played as:' with three entries: 'r0chnu http://128.140.35.86', 'r0chnu http://116.203.166.22', and 'r0chnu http://116.203.15.76'. The status is 'Currently Offline' and there is an 'Inventory' link. A cookie consent banner is at the bottom.

The foreground window is a Telegram channel page for 'rechnungsbetrag' with a blue profile picture containing a white 'R'. The channel has '1 subscriber' and the user 'r0chnu http://167.235.207.108:490|'. A blue button says 'VIEW IN TELEGRAM' and the text 'Preview channel' is below it.

Trusted by CISA

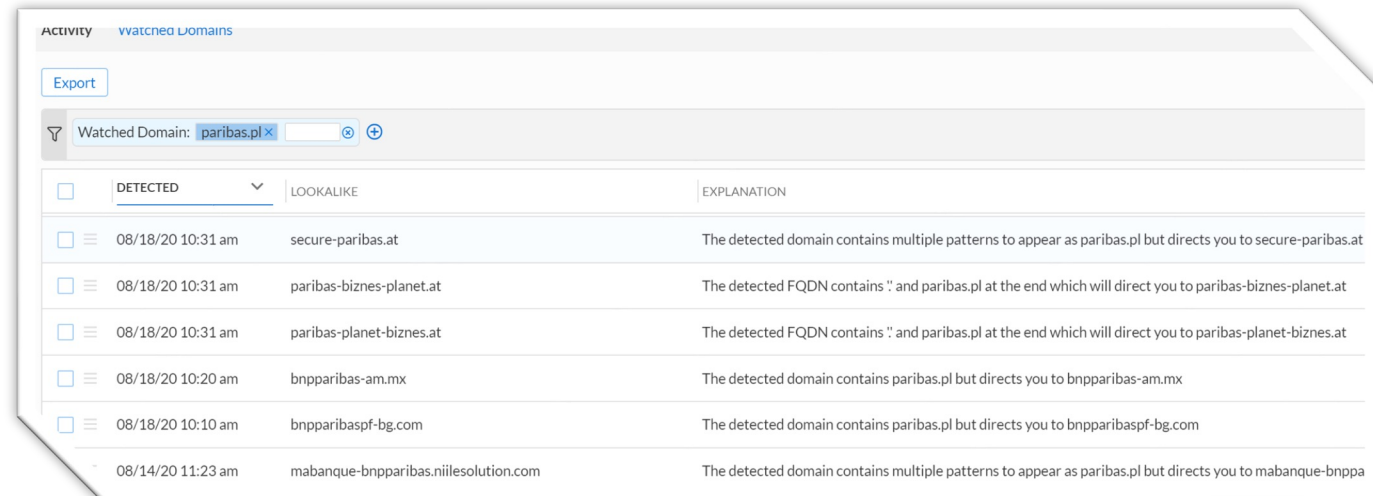


DNS Threat Intelligence



Searching for lookalike domains in TIDE

- `curl -s "https://csp.infoblox.com/tide/api/data/threats/host/daily?target=apple.com&data_format=tsv&field=detected,host&rlimit=20&property=Policy_LookalikeDomains"`
- `apple.bucket.americanexpress[.]com`
- `www.apple.com-login-online.ekdriywyxq65irefusvlhxat1s4jbww97rdamd89d67.coastalcarolinalandmaintenance[.]com`
- `www.apple.com-login-online.hgxxurwzv560nm8tzbkyd9solvn4spw97rdamd89d67.coastalcarolinalandmaintenance[.]com`
- `appleid.apple.com.update.gq.opsgeni[.]us`
- `www.appleid.apple.com-support-account.fvsag[.]com`



The screenshot shows the TIDE interface with the 'Watched Domain' set to 'paribas.pl'. The table below lists several detected lookalike domains with their detection times and explanations.

	DETECTED	LOOKALIKE	EXPLANATION
<input type="checkbox"/>	08/18/20 10:31 am	secure-paribas.at	The detected domain contains multiple patterns to appear as paribas.pl but directs you to secure-paribas.at
<input type="checkbox"/>	08/18/20 10:31 am	paribas-biznes-planet.at	The detected FQDN contains "." and paribas.pl at the end which will direct you to paribas-biznes-planet.at
<input type="checkbox"/>	08/18/20 10:31 am	paribas-planet-biznes.at	The detected FQDN contains "." and paribas.pl at the end which will direct you to paribas-planet-biznes.at
<input type="checkbox"/>	08/18/20 10:20 am	bnpparibas-am.mx	The detected domain contains paribas.pl but directs you to bnpparibas-am.mx
<input type="checkbox"/>	08/18/20 10:10 am	bnpparibaspf-bg.com	The detected domain contains paribas.pl but directs you to bnpparibaspf-bg.com
<input type="checkbox"/>	08/14/20 11:23 am	mabanque-bnpparibas.niilesolution.com	The detected domain contains multiple patterns to appear as paribas.pl but directs you to mabanque-bnppa

Lookalike Domain Detection

- Alphabet change, used in homograph attacks like Beta Bot Trojan:
adoḃe[.]com http://xn--adoc-x34a[.]com/

LOT Polish Airlines rozdaje 2 darmowe bilety z okazji 89. rocznicy. Uzyskaj bezpłatne bilety na: <http://www.lot.com/> .

apple.com (Cyrillic)
apple.com (Latin)

apple.6r

IDN homograph test



Piotr Glaska
Do Piotr Glaska

Action Items

Hi!

Let's see how Outlook displays IDN homographs:

Please log in to:

<http://paypal.com>

<http://paypal.com>

<http://paýpal.com>

<http://päýpäl.co> <http://paypal.com>

<http://paýpal.co> **Kliknij lub naciśnij, aby śledzić link.**

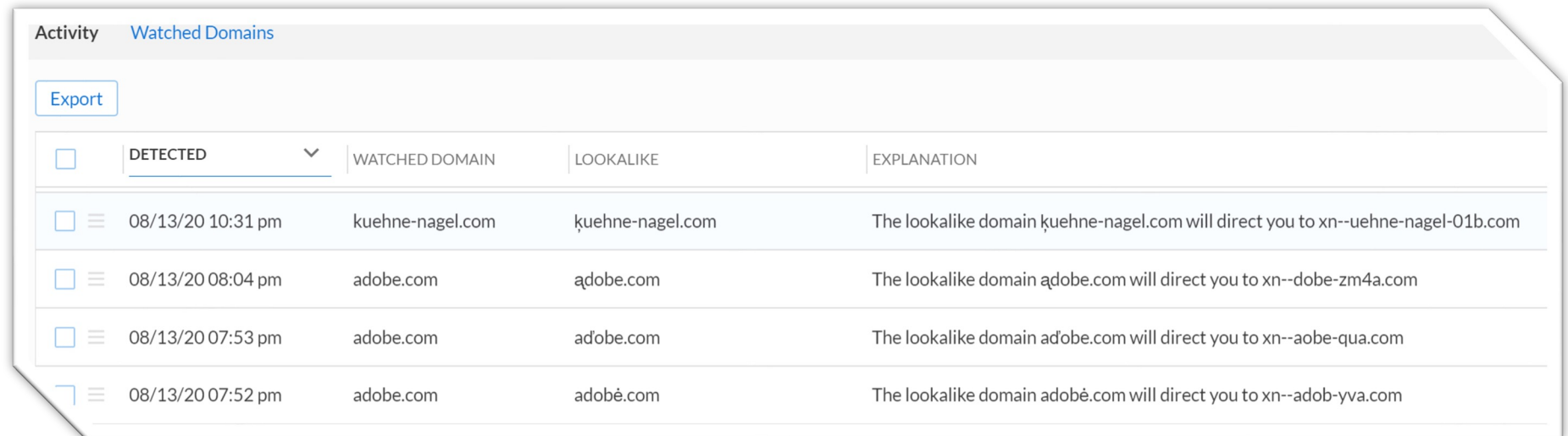
<http://paypal.com>

Searching for IDN homographs in TIDE

- `curl -s "https://platform.activetrust.net:8000/api/data/threats/host?property=Policy_IDNHomograph&target=apple.com&field=host&rlimit=100&data_format=csv"`

[..]

åplè[.]com
æpple[.]com
appé[.]com
äpplé[.]com
ápplë[.]com
apple[.]com
äpplê[.]com
ápplé[.]com
àpple[.]com
apple[.]com



The screenshot shows the 'Watched Domains' section of the TIDE interface. It features a table with columns for 'DETECTED', 'WATCHED DOMAIN', 'LOOKALIKE', and 'EXPLANATION'. An 'Export' button is visible above the table. The table contains four rows of detected lookalike domains for 'adobe.com'.

<input type="checkbox"/>	DETECTED	WATCHED DOMAIN	LOOKALIKE	EXPLANATION
<input type="checkbox"/>	08/13/20 10:31 pm	kuehne-nagel.com	ķuehne-nagel.com	The lookalike domain ķuehne-nagel.com will direct you to xn--uehne-nagel-01b.com
<input type="checkbox"/>	08/13/20 08:04 pm	adobe.com	ądobe.com	The lookalike domain ądobe.com will direct you to xn--dobe-zm4a.com
<input type="checkbox"/>	08/13/20 07:53 pm	adobe.com	ad'obe.com	The lookalike domain ad'obe.com will direct you to xn--aobe-qua.com
<input type="checkbox"/>	08/13/20 07:52 pm	adobe.com	adobè.com	The lookalike domain adobè.com will direct you to xn--adob-yva.com

Dossier™ Threat Research Po...

Enter a domain, IP Address, Hostname, EMail, URL, or H

orlen.in

Last Active Threat Detection:

Summary

More Details

Impacted Devices

Current DNS

Related Domains

Related URLs

Related IPs

Related File Samples

Related Contacts

Discovered on	Expired on	Description
---------------	------------	-------------

	6/13/23	Active Source: Infoblox Property: Suspicious_Lookalike orlen.in
	6/13/23	Active Source: Infoblox Property: Policy_LookalikeDomains orlen.in
	6/14/23	Active Source: Infoblox Property: Phishing_Lookalike orlen.in
	4/21/23	4/28/23 Source: Infoblox Property: Policy_NewlyObservedDomains orlen.in
	4/19/23	4/22/23 Source: FarsightSecurity Property: Policy_NewlyObservedDomains orlen.in

ThreatLab

Test Results

Benign

100%

[Send Us Feedback](#)

RISK

0

0

0

0

paloalto

Products

Home / Test a site

Test A Site

URL

Which URL would you like to test?

URL: orlen.in

Category: Government

Description: Official website

Example Sites: www.orlen.in

Category: Low Risk

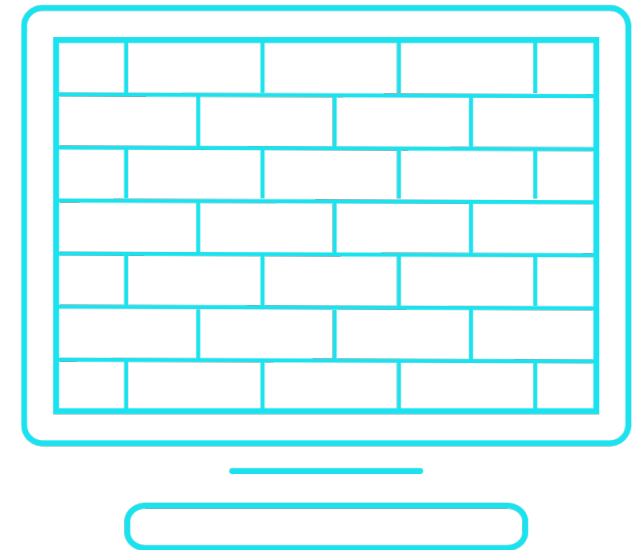
Description: Sites that have been categorized as low risk. The low risk category displays benign activity.

Example Sites: www.orlen.in

[Request Change](#)

Infoblox Secure DNS

- Like a firewall it implements a security policy
- Which has triggers:
 - Queried domain name
 - IP address in response
- And actions:
 - Block (log or don't log)
 - Redirect (log or don't log)
 - Allow (log or don't log)



Suspicious feeds

- Suspicious Lookalikes
- Suspicious NOED (Newly Observed Emergent Domains)
- Suspicious Domains

Domains that have suspicious characteristics typical for malicious domains.

Listed in suspicious feed for 4 months.

June 25th 2023 21:52 CET

The image shows a composite screenshot. On the left is a LinkedIn post from RIFFSEC (233 followers) posted 1 hour ago. The post contains a warning about phishing activity on mBank, mentioning a fake website at `hxxps://00wil[.]ru[.]com/mbn/prelogonAuthentication/logon/mb.php`. On the right is a network monitoring dashboard for the domain `hole.cert.pl`. The dashboard shows a JSON entry for `00wil.ru.com` with a registration date of `2023-06-23T14:15:51`. Below this is a clock showing `Warszawa, 21:52` and a line graph showing query activity over time, with a peak of 10 queries on `06/23/2023 12:00 PM`. The x-axis of the graph ranges from `5/27` to `06/25`.

Post | LinkedIn
linkedin.com/posts/getriffsec_rsalert-mbank-phishing-activity-7078804641781551104-8IW7/

RIFFSEC
233 followers
1h · 🌐

UWAGA #RSalert! Ostrzegamy przed fałszywymi wiadomościami od mBank S.A. i fałszywą stroną bankowości internetowej #mBank

Nie dajcie się nabrać! Adres fałszywej strony:
`hxxps://00wil[.]ru[.]com/mbn/prelogonAuthentication/logon/mb.php`

DW: CSIRT KNF / #phishing #scam #alert
[See translation](#)

05/26/2023 - 06/25/2023
Max. Queries: 20

06/23/2023 12:00 PM
Queries: 10

Warszawa, 21:52
Dzisiaj, +0 GODZ.
Wschód słońca: 04:15
Zachód słońca: 21:01

5/27 05/29 05/31 06/01 06/03 06/05 06/07 06/09 06/11 06/13 06/15 06/17 06/19 06/21 06/23 06/25

00wil.ru.com

6
/ 88

⚠ 6 security vendors flagged this domain as malicious

00wil.ru.com | Registrar: GoDaddy

Community Score

DETECTION | DETAILS | RELATIONS | COMMUNITY

Security vendors' analysis ⓘ

BitDefender	⚠ Phishing	ESET
G-Data	⚠ Phishing	
Kaspersky	⚠ Phishing	
Abusix	✔ Clean	
ADMINUSLabs	✔ Clean	
AlienVault	✔ Clean	
Antiy-AVL	✔ Clean	
benkow.cc	✔ Clean	

Home / Test a site

[Log-in](#)

Test A Site

URL

SEARCH

URL: 00wil.ru.com

Category: Business and Economy

Description: Marketing, management, economics, and sites relating to entrepreneurship or running a business.

Example Sites: www.bothsidesofthetable.com/, www.ogilvy.com, www.geisheker.com/, www.imageworksstudio.com/, www.linearcreative.com/

Additional comments: Includes advertising and marketing firms. Should not include corporate websites as they should be categorized with their technology. Also shipping sites, such as fedex.com and ups.com.

Category: Low Risk

Description: Sites that are not medium or high risk are considered low risk. These sites have displayed benign activity for a minimum of 90 days. The low risk category includes both sites that have a history of only benign activity, and sites found to be malicious in the past, but that have displayed benign activity for at least 90 days.

Example Sites: www.google.com, www.schwab.com, www.amazon.com

[Request Change](#)

00wil.ru.com

Threat	Threat Type
-	-

Content Categories **Security Categories**

Search Engines and Portals
Search Engines (Legacy)

[Dispute Categorization](#)

Risk Score

40

Low Risk

The domain is classified as Low Risk. We found no malicious threats and no suspicious security features.

[▶ SECURITY INDICATORS](#)

Created on 05/16/2023 **Registrant Country/Region** -

Dossier™ Threat Research Po...

Enter a domain, IP Address, Hostname, EMail, URL, or Hash value...

Search

Resources

00wil.ru.com

Last Active Threat Detection: 06/23/2023 (Active)

Add to Custom List

Generate API Request

Feedback on Results

Export

Summary

More Details

Impacted Devices



Current DNS



Related Domains



Related URLs



Related IPs



Related File Samples



Related Contacts



Metadata



• Timeline



Threat Actor



MITRE ATT&CK™



WHOIS Record



5/24/23	Active	Source: Infoblox Property: Suspicious_Generic 00wil.ru.com	Suspicious	Suspicious_Generic	Infoblox	MEDIUM
6/23/23	Active	Source: SURBL Property: UncategorizedThreat_Generic 00wil.ru.com	UncategorizedThreat	UncategorizedThreat_Generic	SURBL	HIGH
6/23/23	Active	Source: Infoblox Property: Phishing_Generic 00wil.ru.com	Phishing	Phishing_Generic	Infoblox	MEDIUM
5/15/24		WHOIS Record (Expires)			WHOIS	INFO
6/25/23		Last Resolved to IP 91.234.99.51			PDNS	INFO
5/23/23	5/30/23	Source: Infoblox Property: Policy_NewlyObservedDomains 00wil.ru.com	Policy	Policy_NewlyObservedDomains	Infoblox	LOW
5/22/23		Last Resolved to IP 5.104.80.223			PDNS	INFO
5/22/23	5/25/23	Source: FarsightSecurity Property: Policy_NewlyObservedDomains 00wil.ru.com	Policy	Policy_NewlyObservedDomains	FarsightSecurity	LOW

00gtk.ru.com



No security vendors flagged this domain as malicious

00gtk.ru.com
ru.com

Community Score

DETECTION DETAILS RELATIONS COMMUNITY

Security vendors' analysis

0xSI_f33d	? Unrated
Acronis	? Unrated
AICC (MONITORAPP)	? Unrated
alphaMountain.ai	? Unrated

Test A Site

URL

Log-in

SEARCH

URL: 00gtk.ru.com

Category: Streaming Media

Description: Sites that stream audio or video content for free and/or purchase.

Example Sites: www.hulu.com, www.youtube.com, www.pandora.com, www.spotify.com, www.grooveshark.com

Additional comments: Includes online radio stations and other streaming music services.

Category: Low Risk

Description: Sites that are not medium or high risk are considered low risk. These sites have displayed benign activity for a minimum of 90 days. The low risk category includes both sites that have a history of only benign activity, and sites found to be malicious in the past, but that have displayed benign activity for at least 90 days.

Example Sites: www.google.com, www.schwab.com, www.amazon.com

[Request Change](#)

00gtk.ru.com

Threat Threat Type

- -

Content Categories

Search Engines and Portals

Search Engines (Legacy)

[Dispute Categorization](#)

00gtk.ru.com

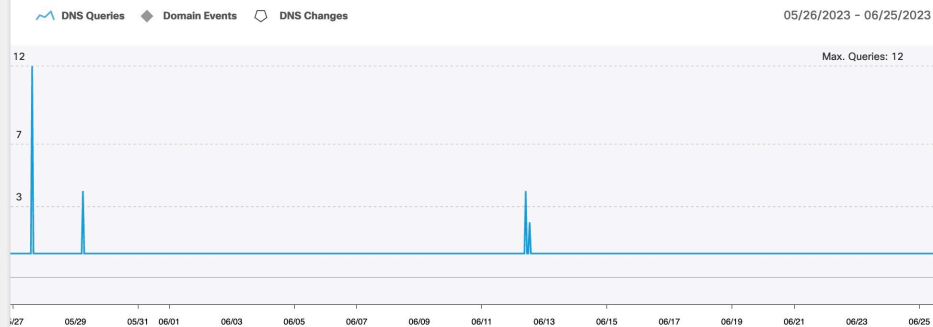
INVESTIGATE

BACK TO TOP

Timeline

DNS Query Volume

Queries Unique Visitors



Risk Score



Medium Risk

The domain is classified as Medium Risk due to a combination of suspect security features.

[SECURITY INDICATORS](#)

Created on Registrant Country/Region

16/2023 -

IP IP Country/Region Prefix ASN Network Owner Description

234.99.51

BZ

91.234.99.0/24

AS213058

PIHL-AS, BZ 86400

[VIEW ALL IP \(1\)](#)

00gtk.ru.com

Last Active Threat Detection: 05/24/2023 (Active)

Add to Custom List

Generate API Request

Feedback on Results

Export

Summary

The timeline shows major events in the domain registration. Watch for changes in ownership. The sources include WHOIS (real records), PDNS (Passive DNS observed from actual traffic), and various feeds such as SURBL who track Domains when they are new.

More Details

- Impacted Devices
- Current DNS
- Related Domains
- Related URLs
- Related IPs
- Related File Samples
- Related Contacts
- Metadata
- Timeline**
- Threat Actor
- MITRE ATT&CK™
- WHOIS Record

5/24/23	Active	Source: Infoblox Property: Suspicious_Generic 00gtk.ru.com	Suspicious	Suspicious_Generic	Infoblox	MEDIUM
5/15/24		WHOIS Record (Expires)			WHOIS	INFO
6/13/23		Last Resolved to IP 91.234.99.51			PDNS	INFO
5/23/23	5/30/23	Source: Infoblox Property: Policy_NewlyObservedDomains 00gtk.ru.com	Policy	Policy_NewlyObservedDomains	Infoblox	LOW
5/22/23		Last Resolved to IP 5.104.80.223			PDNS	INFO
5/22/23	5/25/23	Source: FarsightSecurity Property: Policy_NewlyObservedDomains 00gtk.ru.com	Policy	Policy_NewlyObservedDomains	FarsightSecurity	LOW
5/16/23	5/19/23	Source: SURBL Property: Policy_NewlyObservedDomains 00gtk.ru.com	Policy	Policy_NewlyObservedDomains	SURBL	LOW
5/15/23		WHOIS Record (Created)			WHOIS	INFO

Related Contacts

Metadata

Timeline

Threat Actor

MITRE ATT&CK™

WHOIS Record

Raw Whois

Full Image

4	0	0	2
DNS Record Count	Domain/Subdomain Count	URL Count	IP Count

Categorizations

Infoblox Threat Property	Suspicious_Generic
Infoblox Nameserver Reputa...	Moderate Risk (6)

Hash value... Search Resources

Threat Detection: 05/24/2023 (Active) Add to Custom List Generate API Request Feedback on Results Export

Infoblox Threat Level

Threat Level is designed to help users understand how dangerous an indicator can be, since not all malware behave the same way. The information can be used in combination with other scores from Infoblox.

5.5 /10

Medium

Infoblox Risk Level

The Risk score represents the likelihood that a user will be exposed to a threat or compromised by interacting with the indicator.

4.9 /10

Medium

Infoblox Confidence Level

The Confidence Score provides additional insight into the indicator class and property. It represents our level of trust in the classification and threat of the indicator.

High

Infoblox Threat Intelligence Group Research Notes

Domain is part of a cluster of 15 simultaneously observed, algorithmically generated domains (DGA) with an unknown purpose. The first creation date of domains in the cluster is 2023-05-16. Registered DGA domains are often used for illegal and malicious activity.


Infoblox Threat Feeds

- **Public DoH** - provides a list of known public DNS over HTTPS resolving services. This may be from a browser, a piece of malware, or a user attempting to bypass your organization's DNS policies. This feed contains “canary” domains. We recommend all organizations enable this blocking rule.
- **Country-based** custom feed – all IP addresses located in specified countries
- **Custom feeds** – anything we have in threat intelligence database






Newly Observed Emergent Domains – recently created and newly active domains

Threat Intelligence provider for US Gov

An official website of the United States government [Here's how you know](#) EMAIL US CON Infoblox

 **CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY**

Search [cisa.gov/uscert](#) [Report Cyber Issue](#)

 CYBERSECURITY  INFRASTRUCTURE SECURITY  EMERGENCY COMMUNICATIONS  NATIONAL RISK MANAGEMENT  ABOUT CISA  MEDIA

SHARED CYBERSECURITY SERVICES

Shared Cybersecurity Services (SCS) is a portfolio of Cybersecurity and Infrastructure Security Agency (CISA)-funded contracts that provides federal civilian agencies, state fusion centers, and select information sharing and analysis centers with no-cost access to commercial Cyber Threat Intelligence (CTI) and services.

[Collapse All Sections](#)

Service Scope

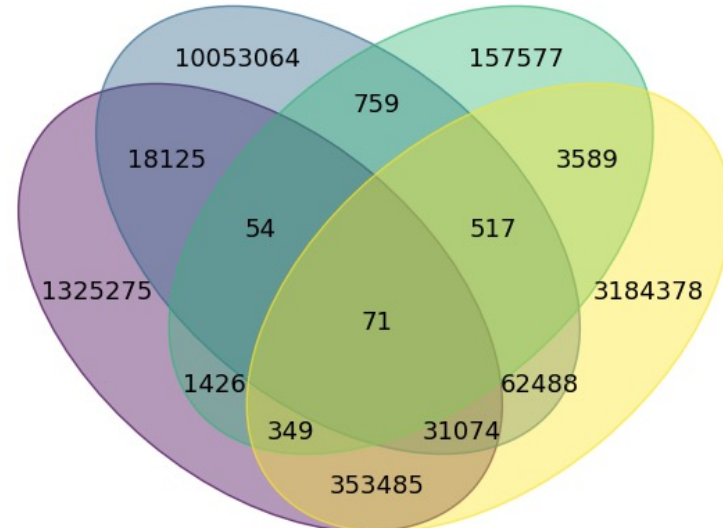
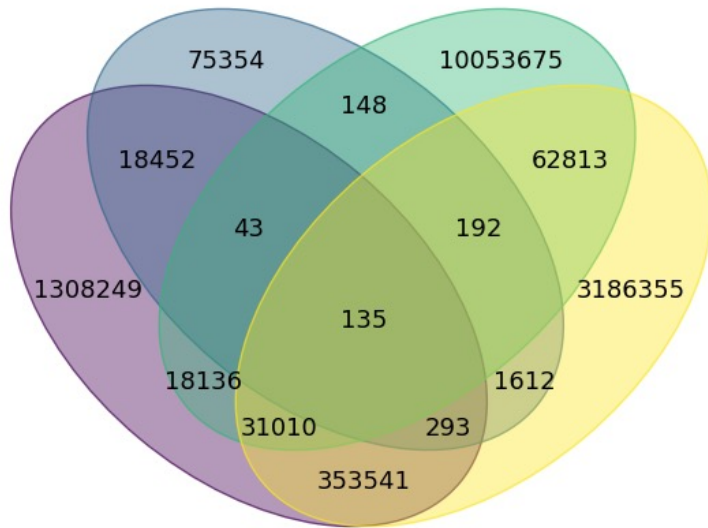
SCS allows users to access, research, and enrich CTI through a commercial enterprise license. Core offerings include access to CTI management platforms (scoutPRIME, [BloxOne Threat Defense](#), and Mandiant Advantage), automated sharing, training and IT Support, and limited analytical support (e.g. Requests for Information [RFIs]).

Service Vendors

CISA currently contracts with three commercial providers, LookingGlass, [Infoblox](#), and Mandiant, to provide CTI and associated services. Each vendor provides a similar set of core offerings that includes access to: CTI platform accounts and training/technical support, Application Programming Interfaces (APIs) that support machine-to-machine threat data connections, and analyst support. In addition, each vendor offers specific capabilities, including Domain Takedowns and Phishing Analysis, tied to their special area of expertise. The SCS portfolio also allows the vendors to share and enrich intelligence, Indicators of Compromise (IOCs), and threat reporting amongst each other, ultimately enhancing the quality of CTI available to SCS users. See our [SCS Mitigations and Phishing Analysis Fact Sheet](#) for more information

Threat feeds overlap between vendors

- 2 graphs due to 5 sources



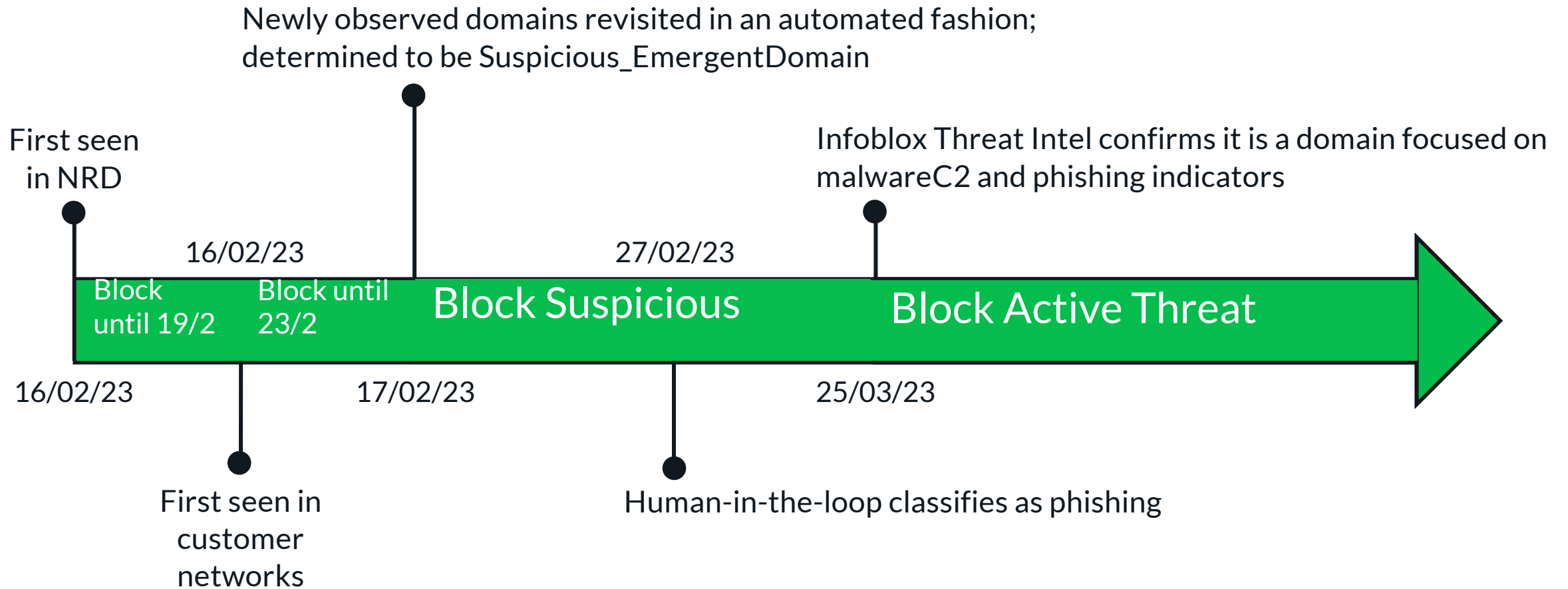
US Dept. Of Homeland Security Feeds

Automated Indicator Sharing (AIS) enables the exchange of threat indicators, among the Federal Government and the private sector.

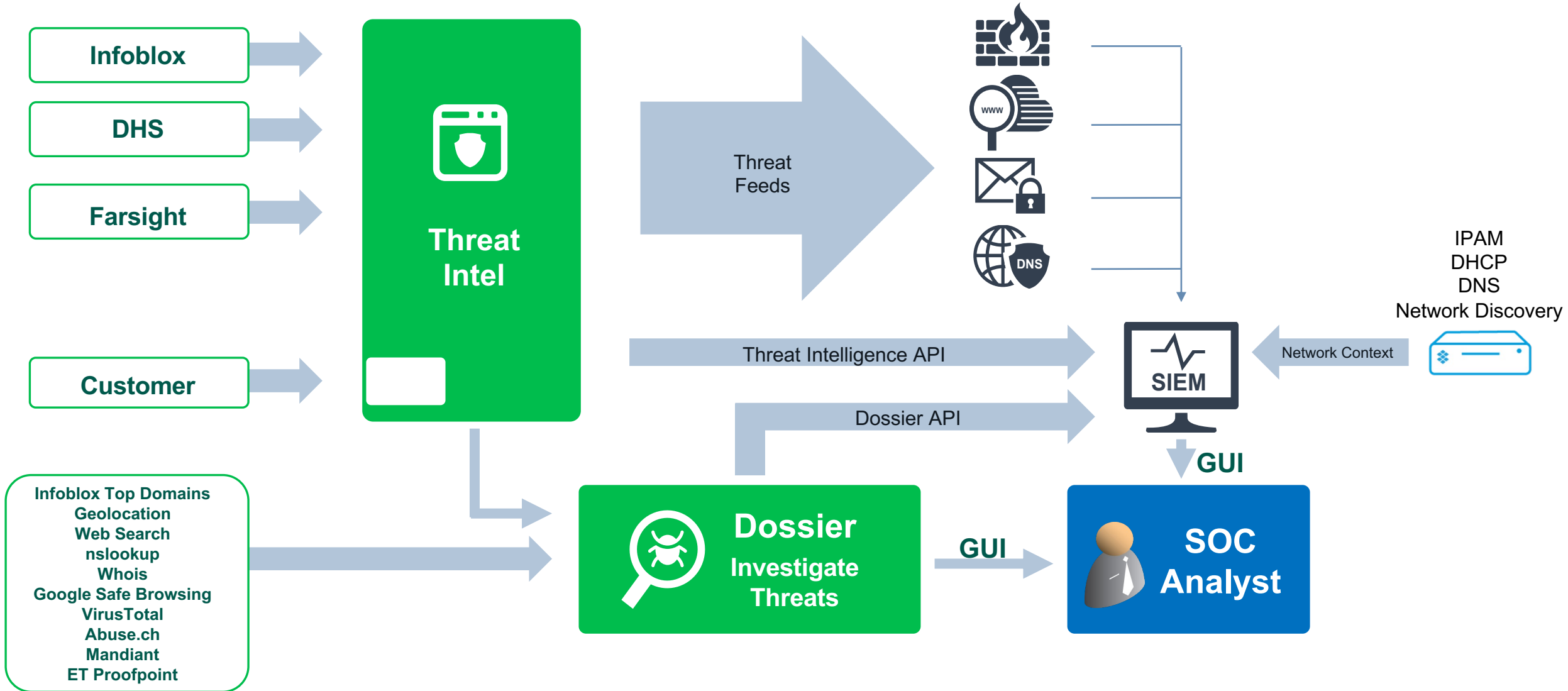
- **Automated Indicator Sharing (AIS)** – Indicators of compromise (Hostnames and IP addresses) shared through Department of Homeland Security with the private sector
- **AIS NCCIC Watchlist** – Indicators contained in this feed appear on the watch list from the National Cybersecurity & Communications Integration Center (NCCIC). These are medium confidence feeds with a higher chance for false positives since they are not verified or validated by DHS or Infoblox.

Domain Lifecycle

Indicator ekisenos-jp[.]top ▶



DNS Threat Intelligence





THANK YOU

JAN RYNES

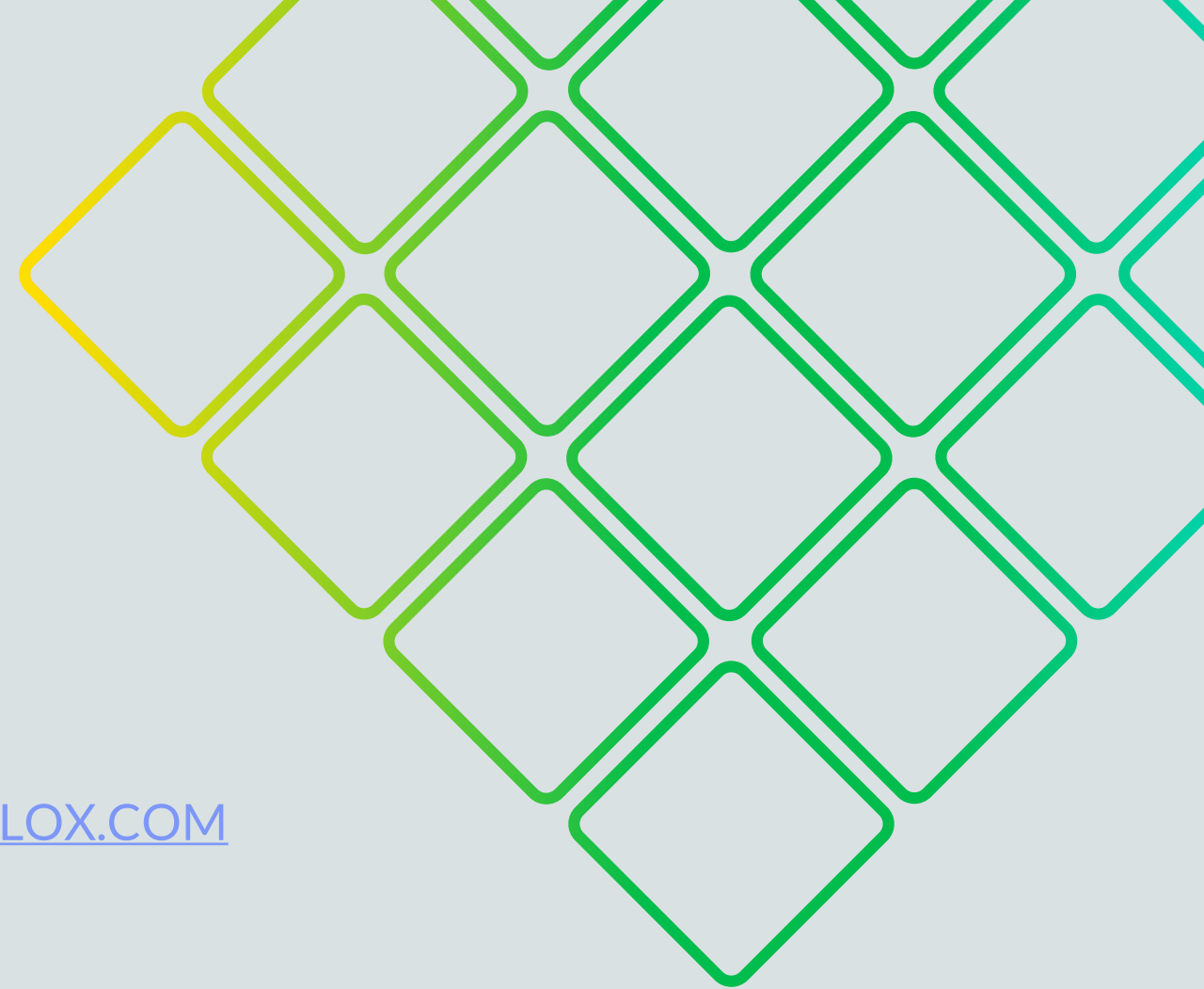
JRYNES@INFOBLOX.COM

+420 731 591 259

COSMIN VILCU

CVILCU@INFOBLOX.COM

+40 764 433 310



SECURITY. IT'S IN OUR DNS.