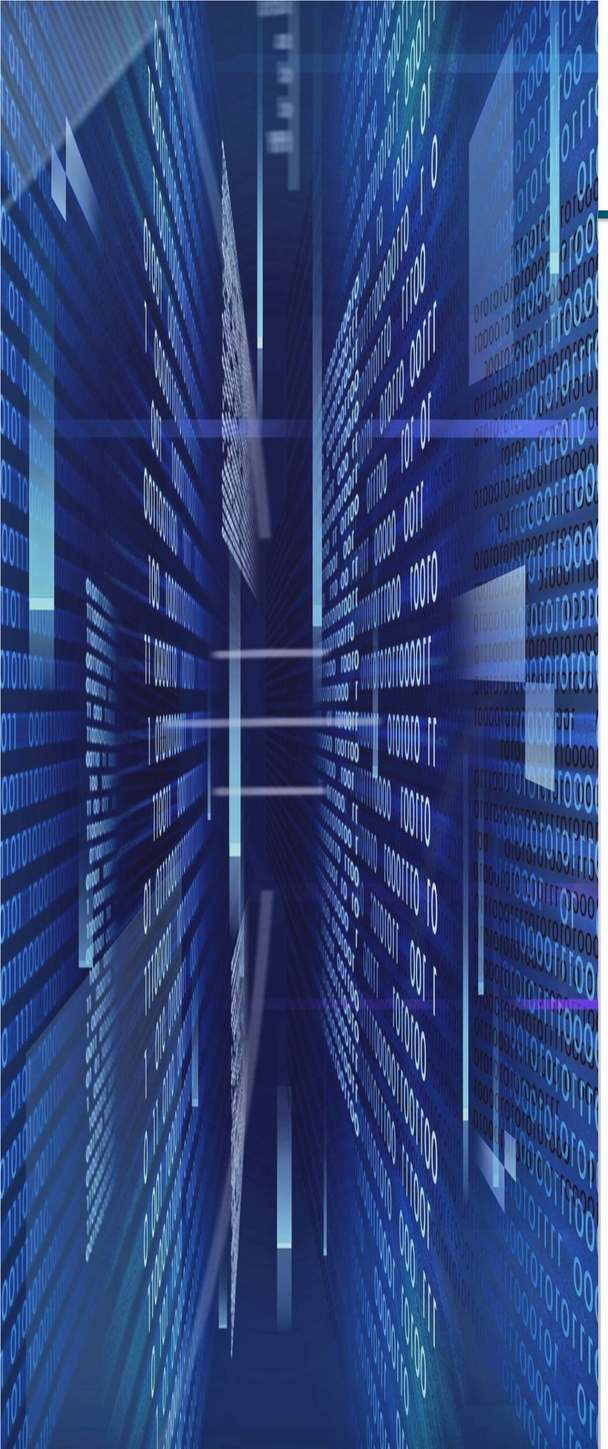


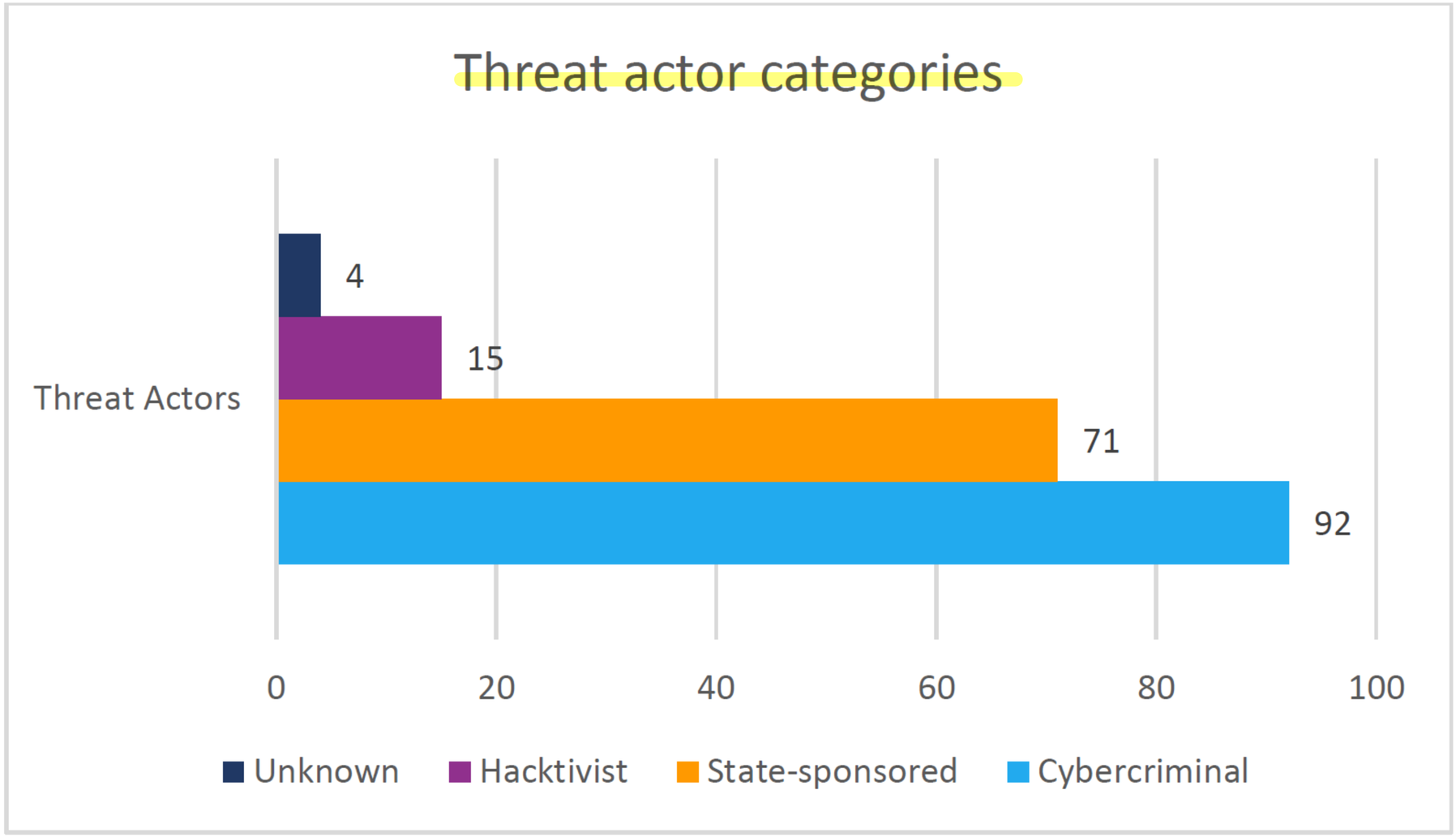
Cyber Security and Data Protection

Cyber Threat Actors

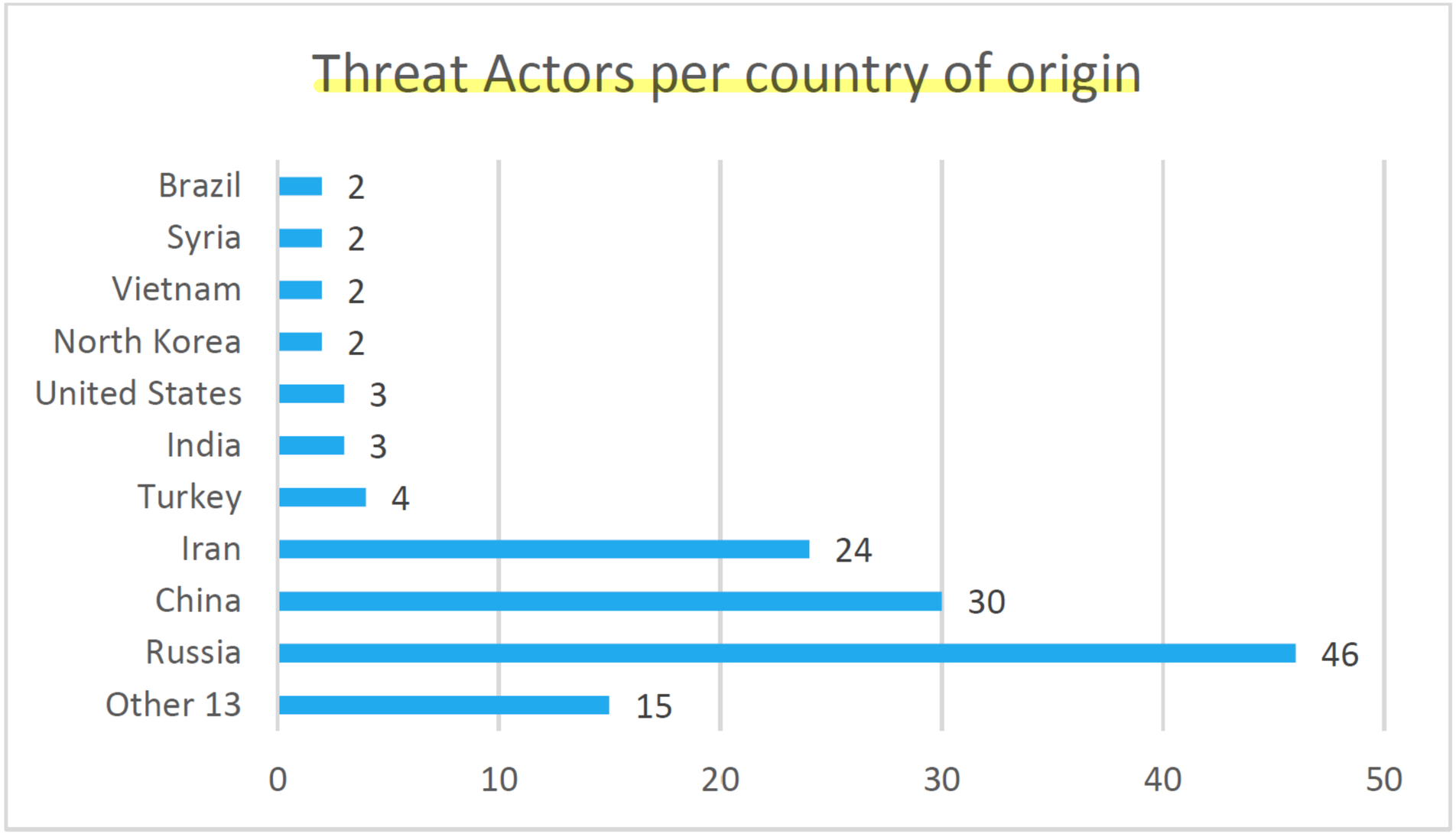
Prof.Federica Paci

Who is behind the last cyber attacks ?

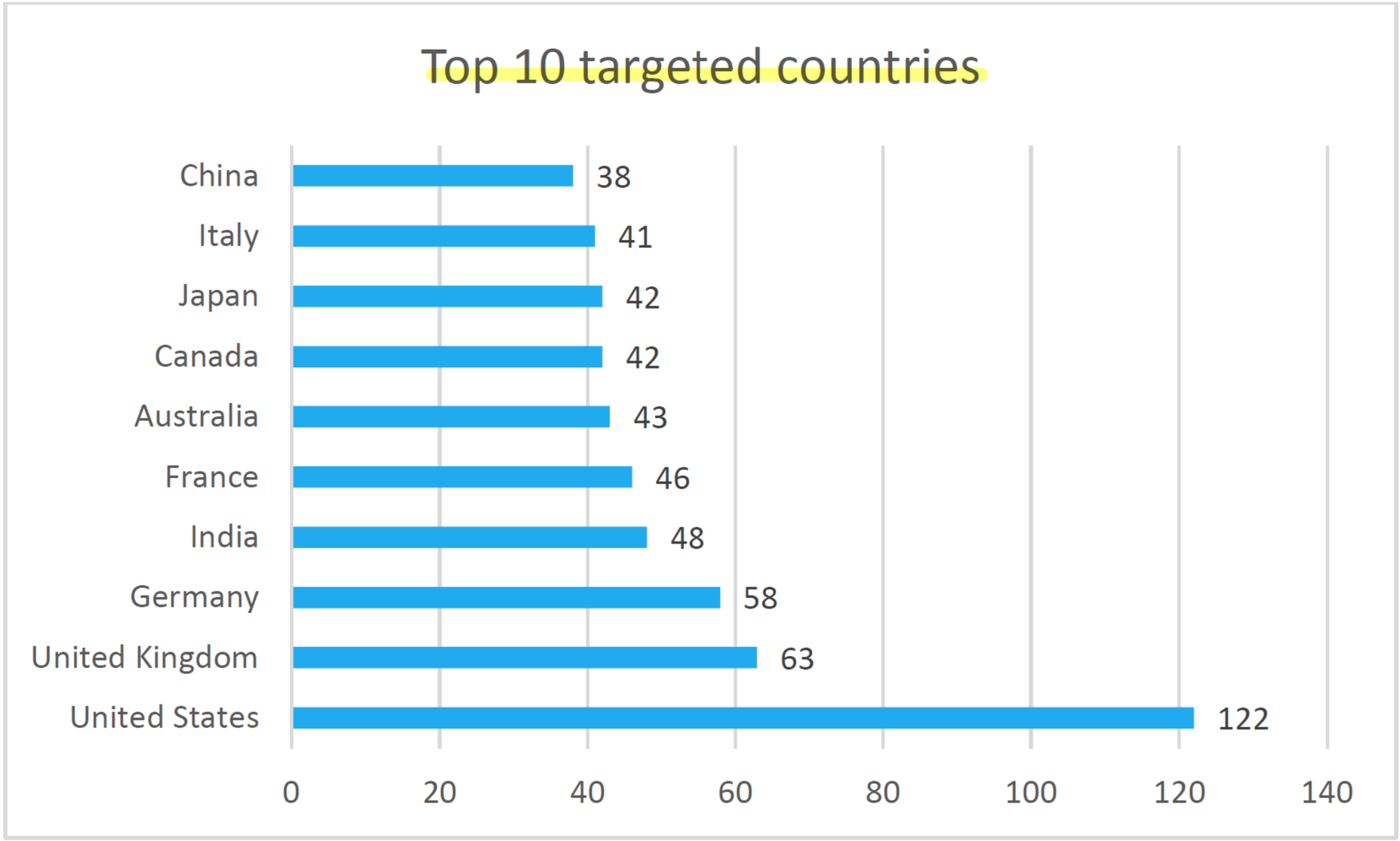
Threat Actors Categories



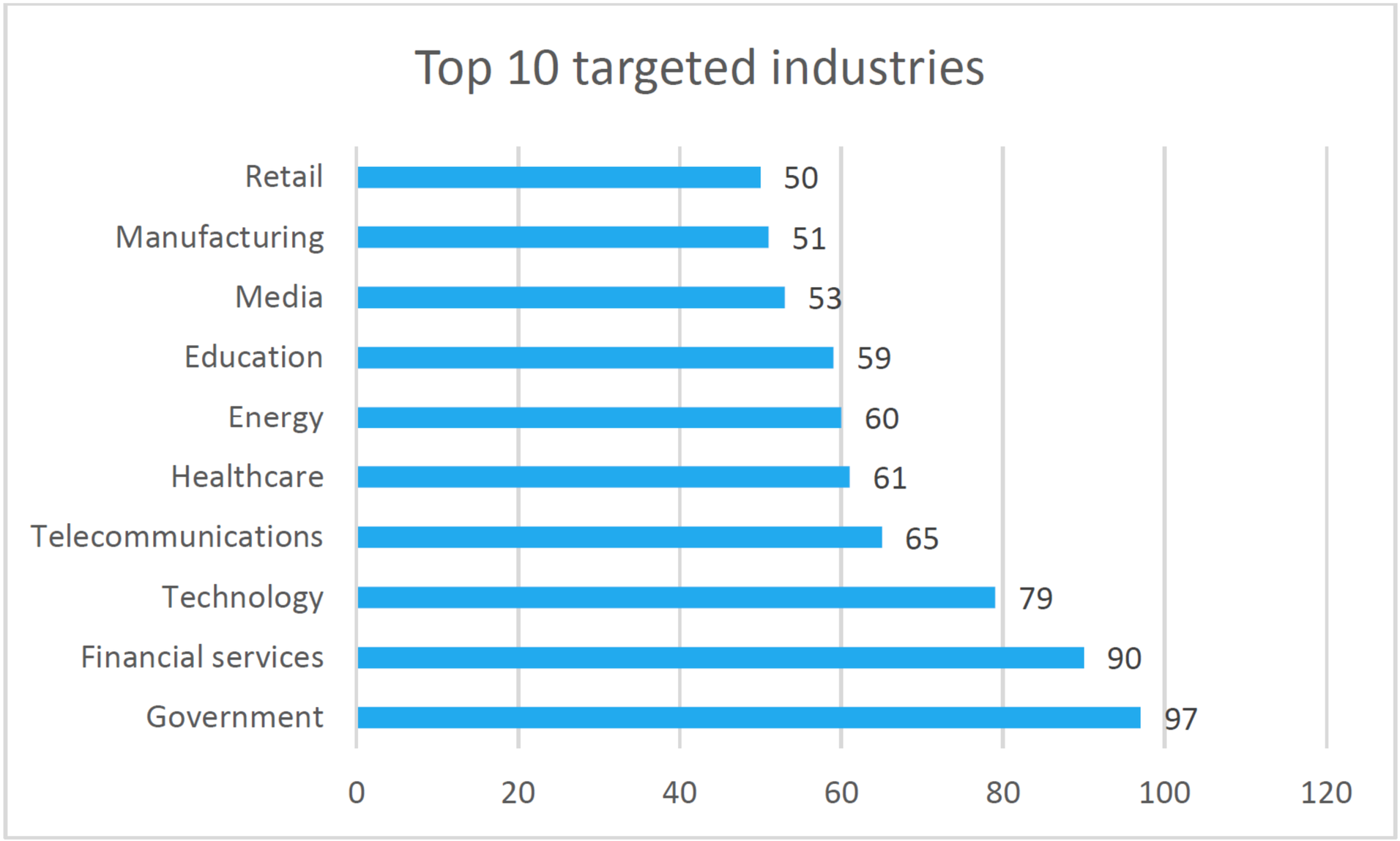
Threat Actors Country of Origin



Threat Actors Target Countries



Threat Actors – Target Industries

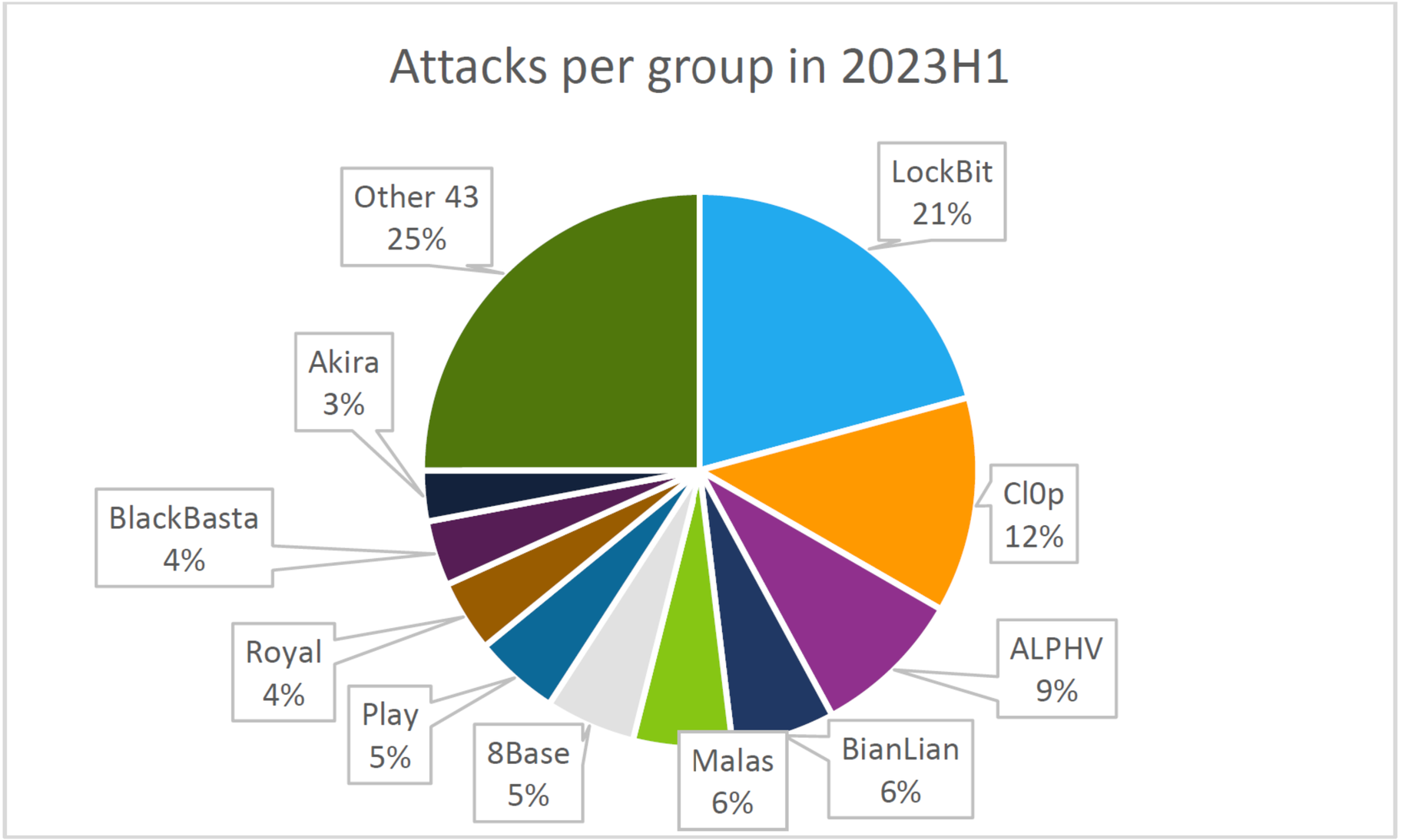


Cyber criminals

- Interested in illegal profit
- Typical attacks
  - Ransomware
  - Infostealers
  - Proxyjacking

- Scoperta la loro preferenza per effettuare brute forcing delle credenziali sulle porte TCP: 21 (FTP), 80 (HTTP), 443 (HTTPS) and 22 (SSH)
- Vengono analizzati i gruppi telegram associati ai gruppi criminali per confermare la prevalenza di attacchi DDoS e mostrare il loro punto di vista sugli attacchi effettuati

Ransomware Groups



Ransomware Campaigns' Targets

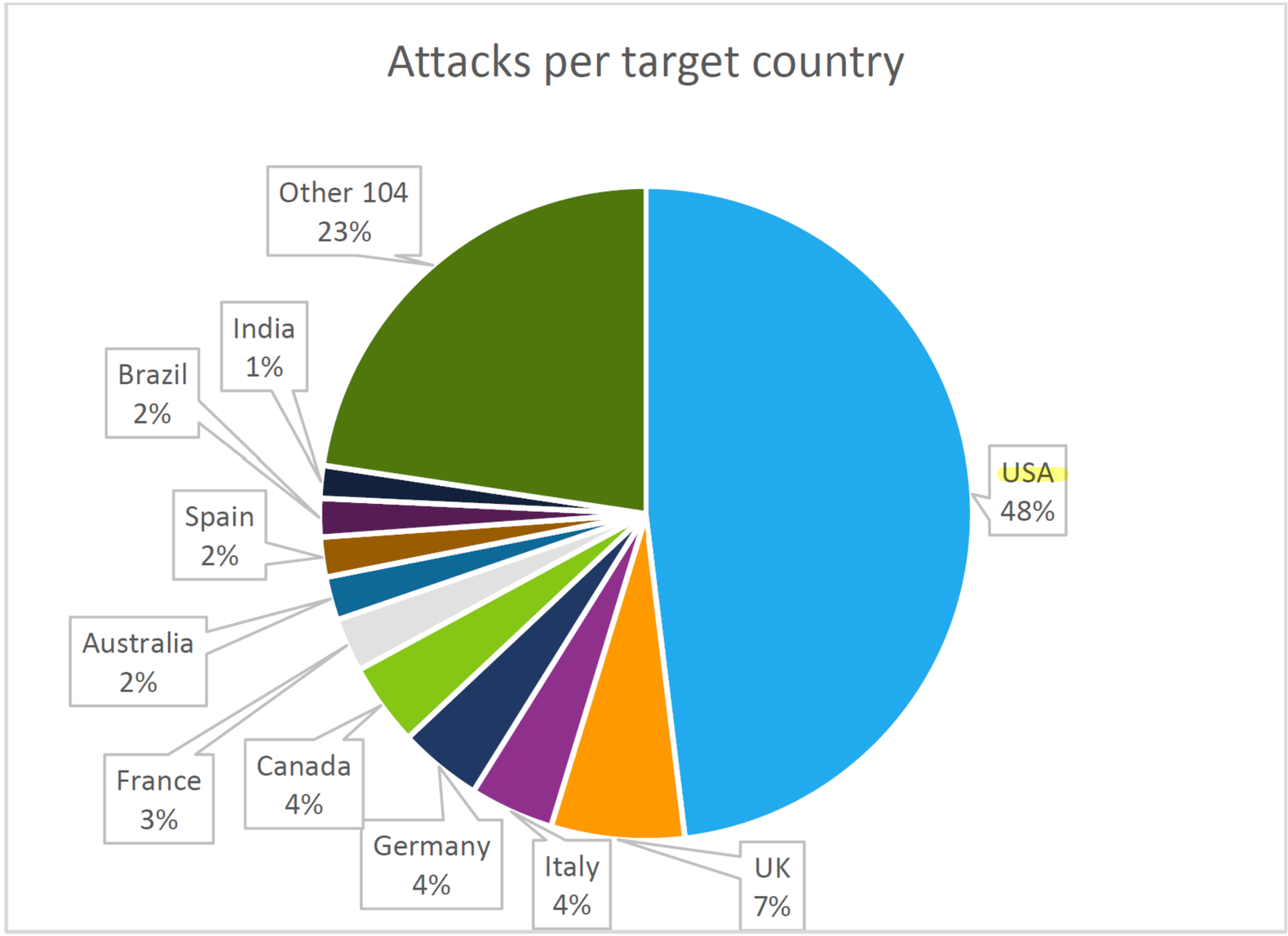


Figure 12 – Ransomware attacks per target country

Infostealers

Raccoon stealer | only serious business

11 September 2022

Channel "ertheryher" created

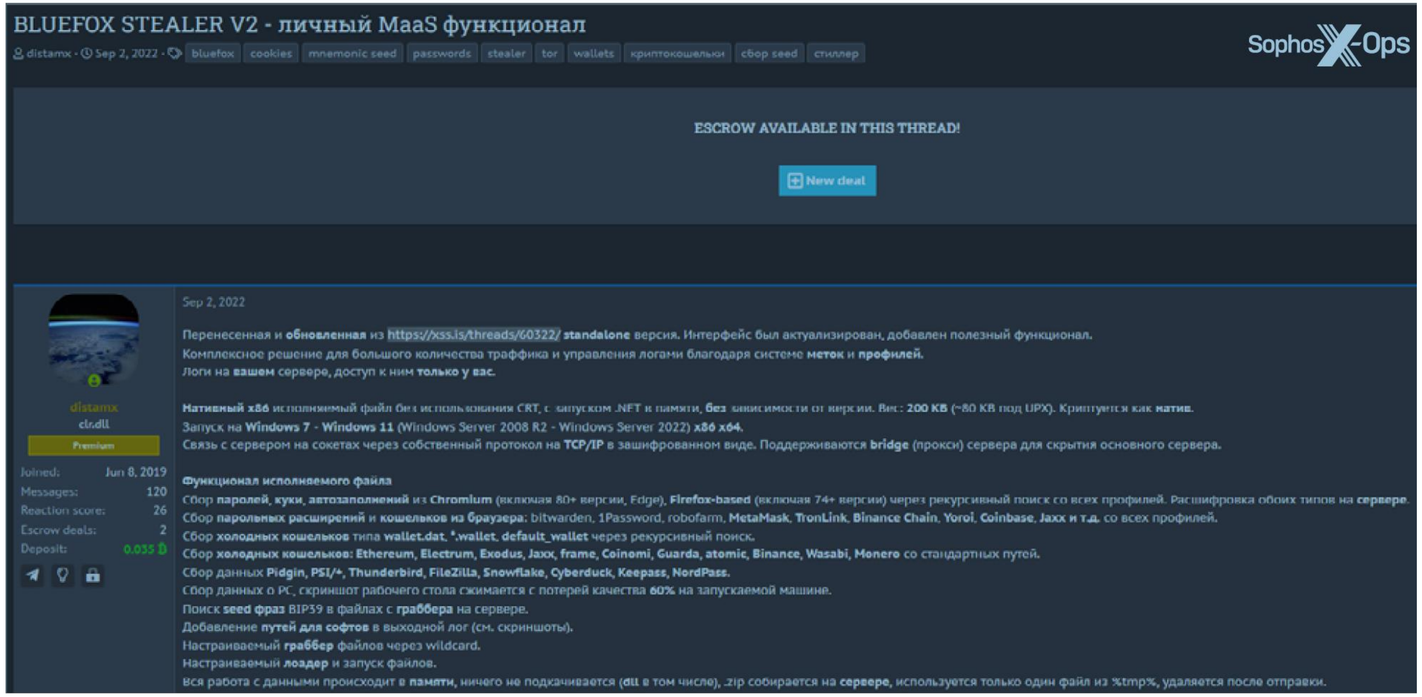
R **Raccoon stealer | only serious business** 03:27

Dear customers,
We are pleased to inform you that the development of a new version of the stiller has come to an end
We have completely rewritten each module of the stiller, completely rewritten the stiller itself (soft part) from scratch

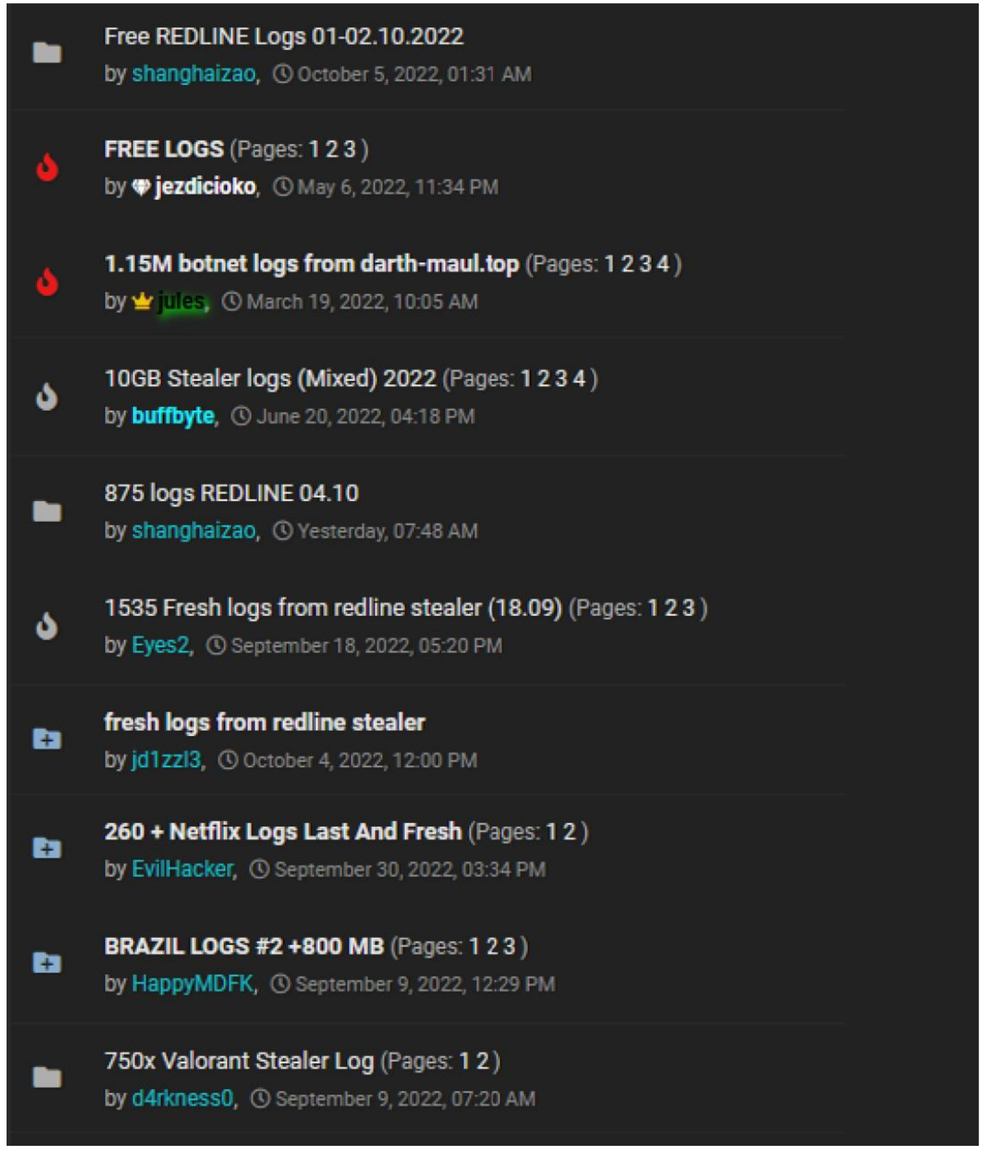
• We have changed the product model and now you will need to register pads through which go build connection, and through the same pads, your logs are downloaded. So, detectors will never intersect with other clients, and installing such a gasket will take you no more than 5 minutes of time. Nobody will interfere with each other.

• A 5 Gbit/S channel (5 times more than the nearest competitor) allows us to register multiple pads for clients, and separate clients into groups, and the load will not overlap

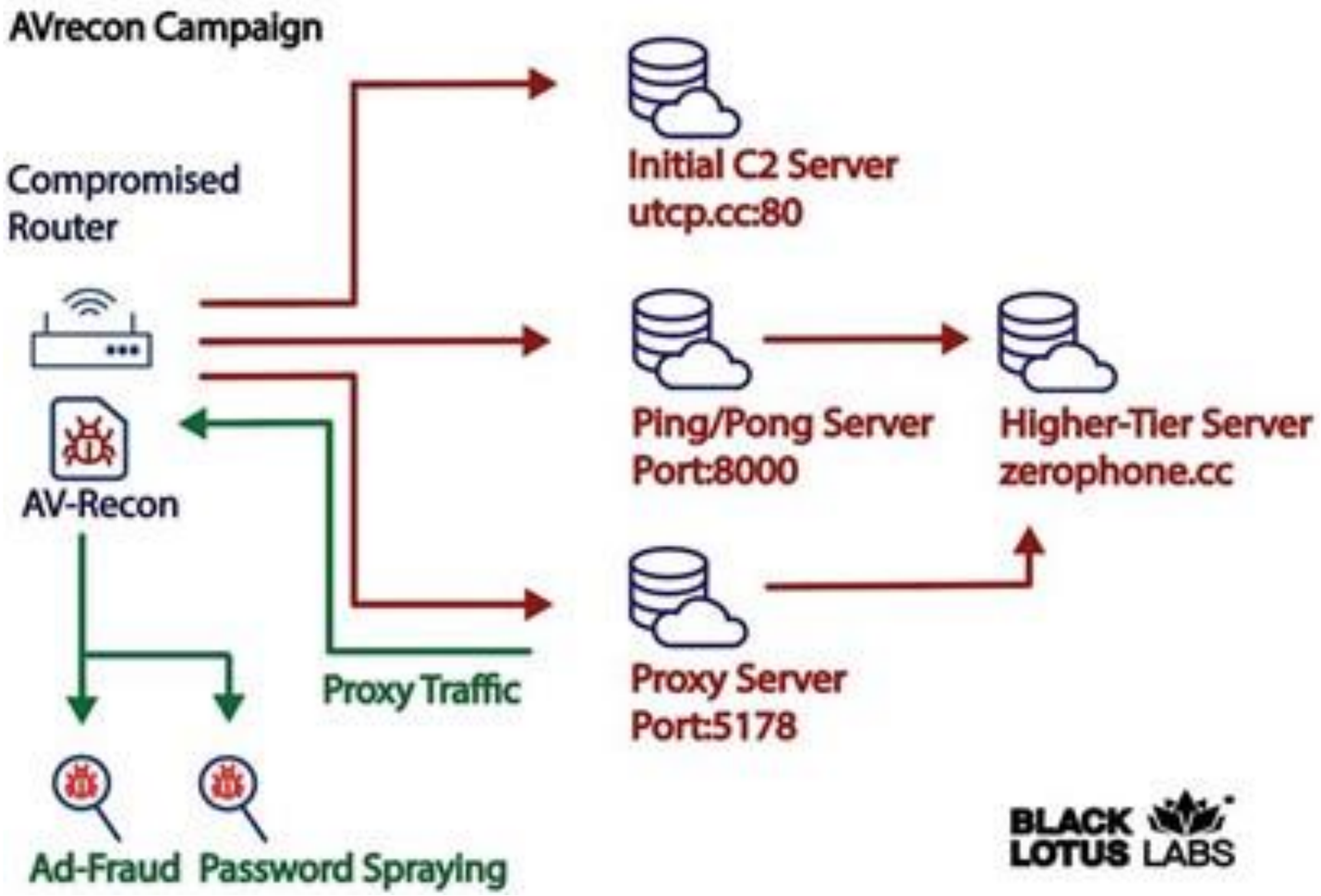
• MULTIDOWNLOAD:**Uploading logs is now ~10 times faster** (before the logs were collected from different servers, so you had to wait a long time, now the archive is collected locally on one server and you are given a link, again the link will lead to YOUR server)



Infostealers



Proxyjacking: Avrecon



Nation States

- Interested in
  - *high quality intelligence*
  - *espionage*
  - *sabotage activities*
  - *subversion e.g political election*
- Typical attacks
  - Attacks to Critical Infrastructures
  - Wipers
  - DDoS

Russian- State Sponsored Activities

US, UK warn of govt hackers using custom malware on Cisco routers

By **Lawrence Abrams**

April 18, 2023 05:42 PM 1

China – Sponsored Activities

China's Volt Typhoon APT Burrows Deeper Into US Critical Infrastructure

US officials are concerned that the Beijing-directed cyberattacks could be a precursor to military disruption and broader destructive attacks on citizens and businesses.

Nate Nelson
Contributing Writer, Dark Reading

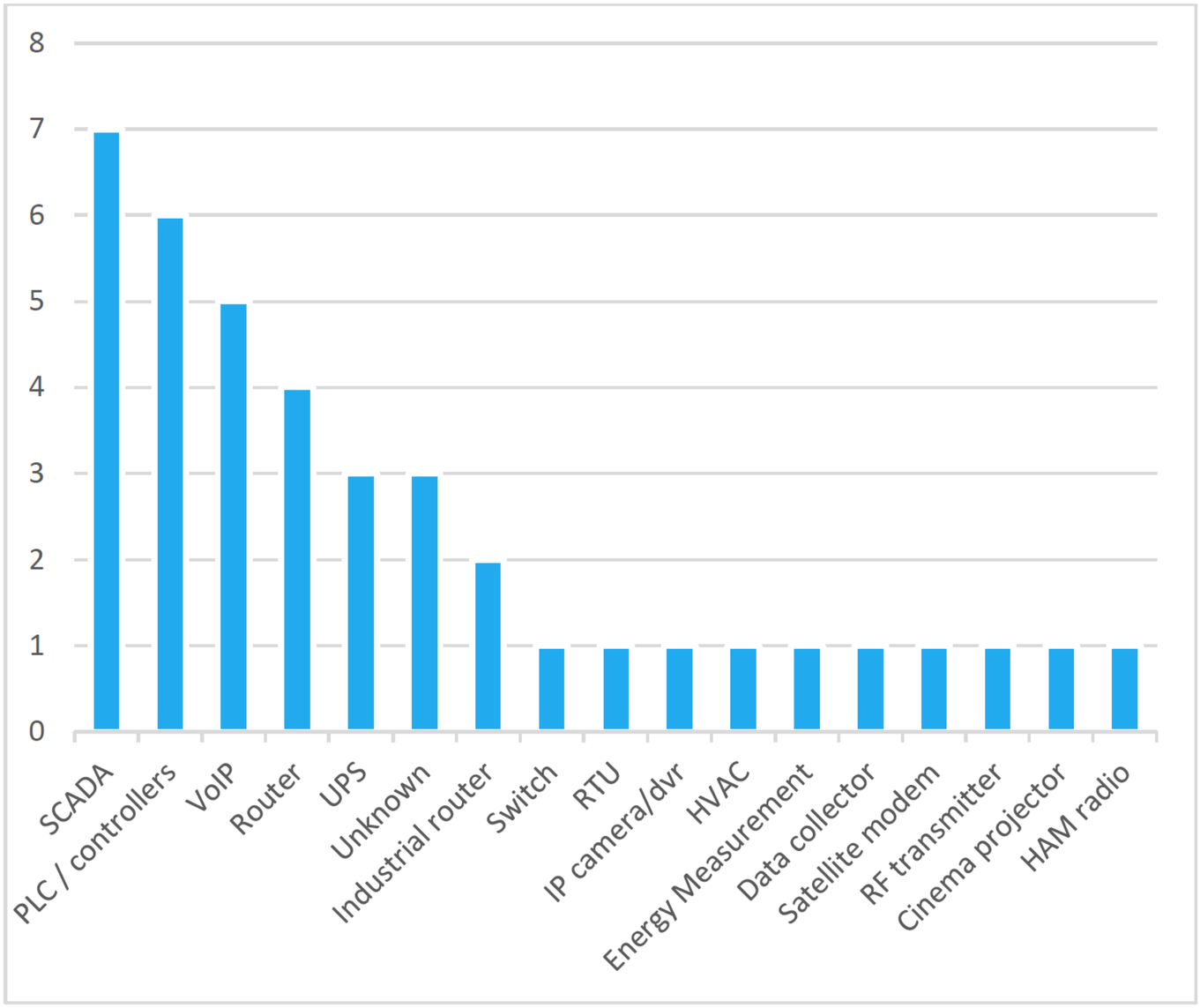
July 31, 2023

Hacktivists

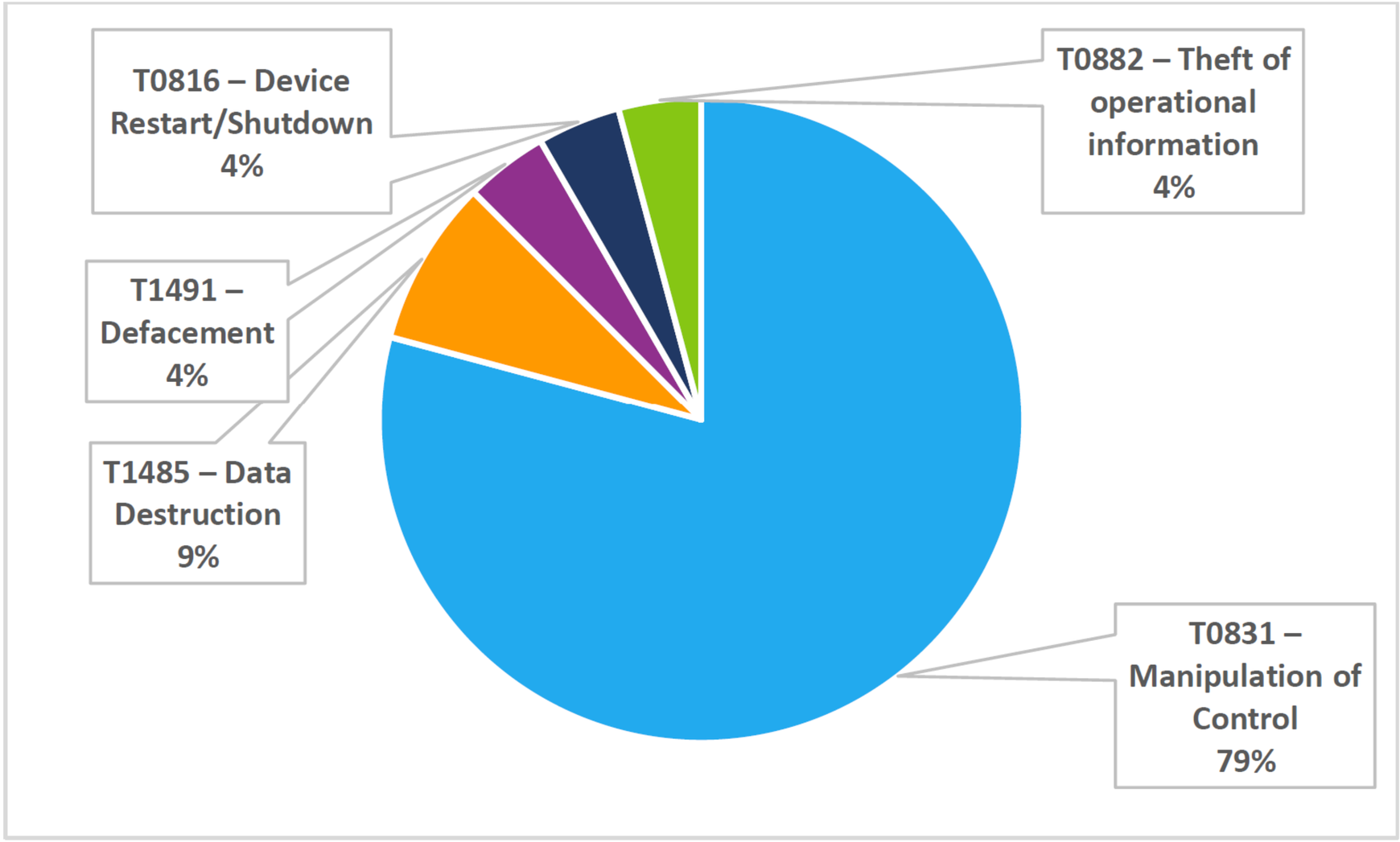
- Motivated by
  - *Political views*
  - *Cultural/religion belief*
  - *National Pride*
  - *Terrorist Ideology*

- Typical attacks
  - distributed denials of service (DDoS),
  - data breaches or leaks
  - data wipers
  - distributing propaganda
  - attacks to unmanaged devices

Targeted Unmanaged Devices



Common Techniques



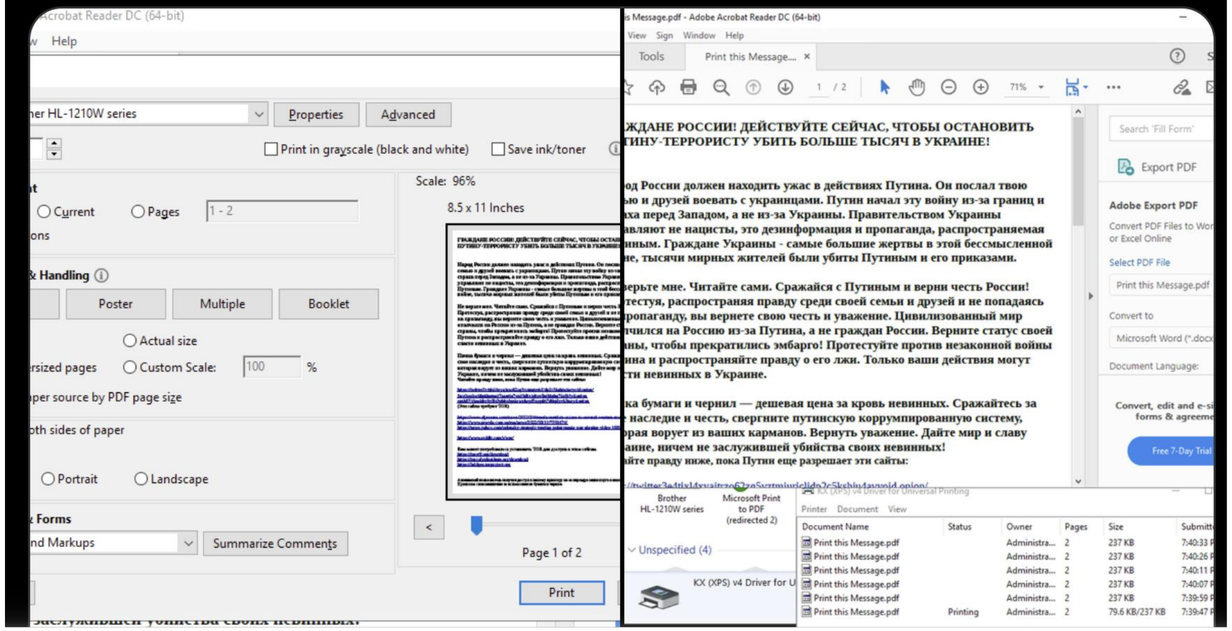
Anonymous

Anonymous 🍀
@DepaixPorteur

We are #Anonymous

We have been printing anti-propoganda and tor installation instructions to printers all over #Russia for 2 hours, and printed 100,000+ copies so far. 15 people working on this op as we speak.

#OpRussia #OpUkraine #ASS #ASSHAT #OpRedScare #AnonOps



← **Post**

Anonymous ✔
@YourAnonNews

"Behind Enemy Lines" Russian camera dump brought to you by #Anonymous
behindenemylines.live

2:53 AM · Mar 17, 2022

967 Reposts **99** Quotes **6,071** Likes **154** Bookmarks

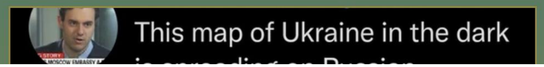
OneFist

Home | Our Operations | Support OneFist | About Us | Online Store

Search...

Team OneFist

Welcome to Team OneFist, Defenders of Ukraine in Cyberspace, Practioners of Cyber Security and Open-Source Intelligence (OSINT) for the people of Ukraine



Let's Chat!

Ghostsec


GhostSec
196 posts
F NOT US, THEN WHO ?
F NOT NOW, THEN WHEN ?
GHOSTSEC
Follow
GhostSec
@ghost_s3curity
Official #GhostSec • #HackThePlanet • #GSM #Anonymous • #OpIran
#GhostSecMafia
No Nation
t.me/GhostSecc
Joined June 2022
26 Following
7,241 Followers

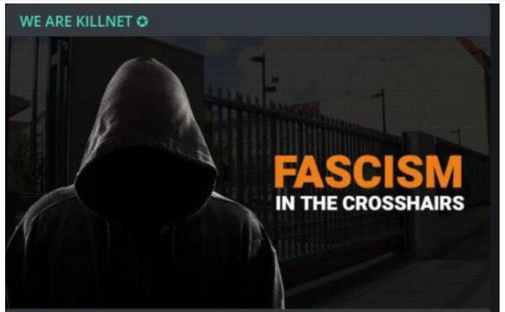
KillNet

⚡ Будущее Польских DNS

❗ "Любая агрессия от Польской власти в сторону России, незамедлительно запустит цикл массированной ddos атаки на все жизненно важные и государственные сетевые ресурсы"

❗ "Każda agresja ze strony polskiej władzy w kierunku Rosji, natychmiast rozpocznie cykl zmasowanego ataku ddos na wszystkie istotne i Państwowe zasoby sieciowe"

❤ 196 👍 1 👁 32.8K 19:04



⚠ Атака остановлена спустя 5 часов

⚡ Атака на официальный сайт министерства обороны Германии
❌ https://www.bmvg.de/de
🔹 https://check-host.net/check-report/8de0a5ck799

🤠 Гитлер Капут...

⚡ Attack on the official website of the German Ministry of Defense.

Hello German politicians, I want to remind you of the recent surrender of your country. Don't do stupid things. Ukraine has no chance as much as all of your Europe!
For the meeting...

⚠ Атака остановлена спустя 5 часов

❤ 1013 👁 40.2K edited 20:24

❗ it is temporarily impossible to purchase a ticket, we apologize to Joe Biden....

⚡ This action is not terror, but a hint that the United States government is not the master of millions of lives in Europe ...
☝ When the supply of weapons to Ukraine stops, attacks on the information structure of your country will instantly stop!
- America, no one is afraid of you...

⚠ АТАКА СТОП СПУСТЯ 17 ЧАСОВ ⚠

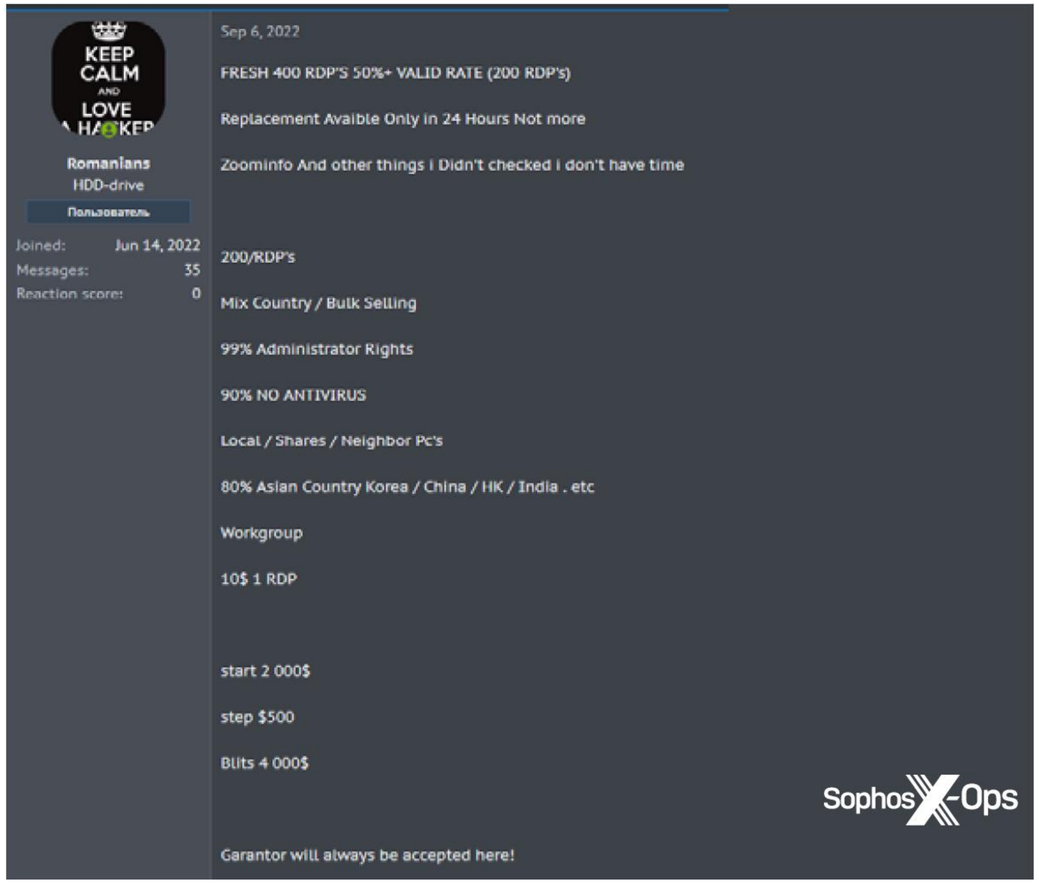
❤ 929 👁 74.6K edited 00:40

Killnet è un gruppo attivista coinvolto nella guerra russo-ucraina. Ci sono più di 100 gruppi che conducono attacchi informatici in questo contesto, principalmente DDoS e violazioni di dati. Killnet, situato in Russia, è uno dei gruppi più attivi, impegnato in attacchi DDoS e infrastrutture critiche occidentali e diffusione di propaganda tramite Telegram. Il gruppo è stato incluso in avvisi di sicurezza e rapporti di organizzazioni come CISA. Non ci sono prove dell'utilizzo di strumenti personalizzati o altamente sofisticati da parte loro

↳ Cybersecurity and Infrastructure Agency

How do Threat Actors operate?

Attack as a service



Everything as a service

Phi4er
kilobyte
●●

Active arbitrage
0
27 posts
Joined
06/24/22 (ID: 132361)
Activity
кодинг / coder

Posted June 24 (edited)

Sophos X-Ops

Every Phisher Dream

Hello,
We offer our services for every phisher that want to success his campaigns. We decided to help you in creation and maintenance for your projects/campaigns with our long experience in phishing.

- We can create/clone any page
- Live panel can be done for the page
- Customizing the live panel for any feature needed
- Anti-bot system that protects the page for days and even weeks new

We can help you hosting your page on our personal servers with anti-bot and auto domain changer with extra fees. Just relax and see your campaigns running successfully,

Why us?

- Client's satisfaction is our priority
- Online 24/7 hours on TG
- We deliver your project/page ASAP
- Edits are done and delivered immediately
- Any features you dream of can be implemented in your page

Our mission?
Simply we are created to help in carrying out your fishing projects in a professional way.

Helium
Malware Services
●●●

Paid registration
3
68 posts
Joined
08/16/21 (ID: 119109)
Activity
вирусология / malware

Posted 16 hours ago (edited)

Our WD crypting service is one of a kind. You won't have to go through the hassle of finding a reputable crypting service any longer.
With our exclusive .bat encryption - your executable (.exe) will be transformed into a small, 6-25 kb batch (.bat) file.
This ensures the best results for manual file distribution.

Using a .bat file has many advantages over the classic .exe file.

- **Guaranteed WD Bypass**
- **Bypass ChromAlert & SmartScreen** (bypasses SmartScreen with non-passworded .zip or .rar file)
- Easy to run and your file will stay undetected for much longer than with a classic .exe
- No need for an EV Signing Certificate compared to regular .exe files

Features:

- Adds a **Windows Defender exclusion** for your file when ran on a computer - this way you won't lose connection.
- Loads your executable from an external host straight to the computer when the .bat file is executed.
- Your file will receive a ripped signature for further anti-detection.

Sophos X-Ops

Compromise network devices for initial access

Shodan, Censys and Kamerka are used to discover **exposed devices** in the targeted countries

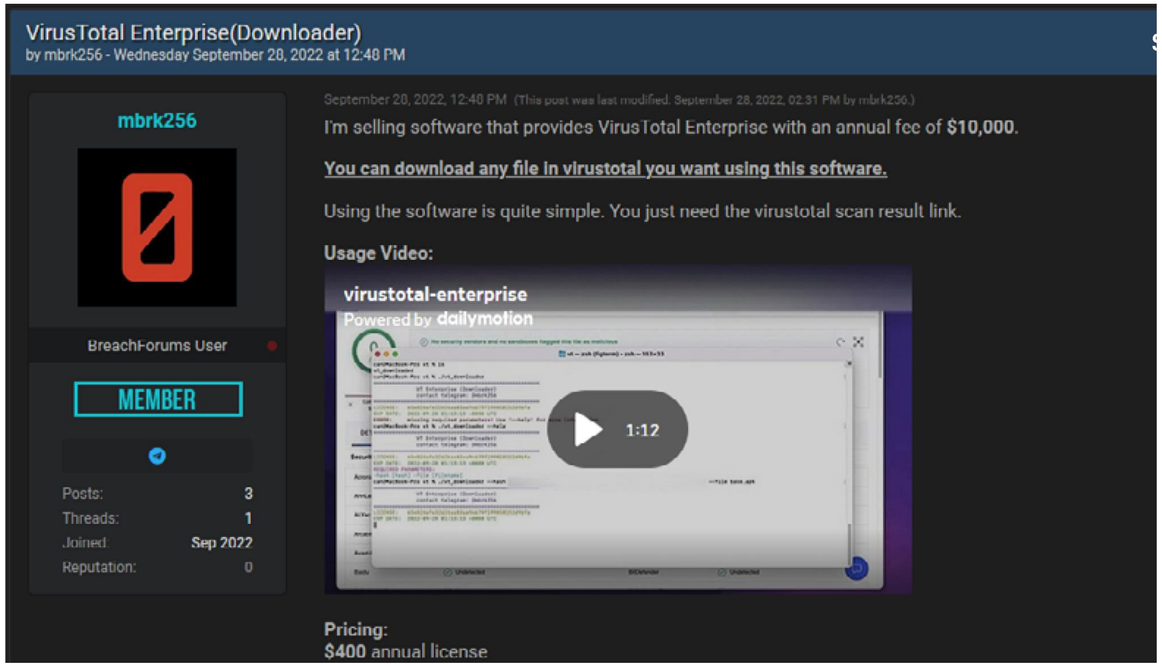
Routers and IP cameras are often compromised via either **default** or weak **credentials**.

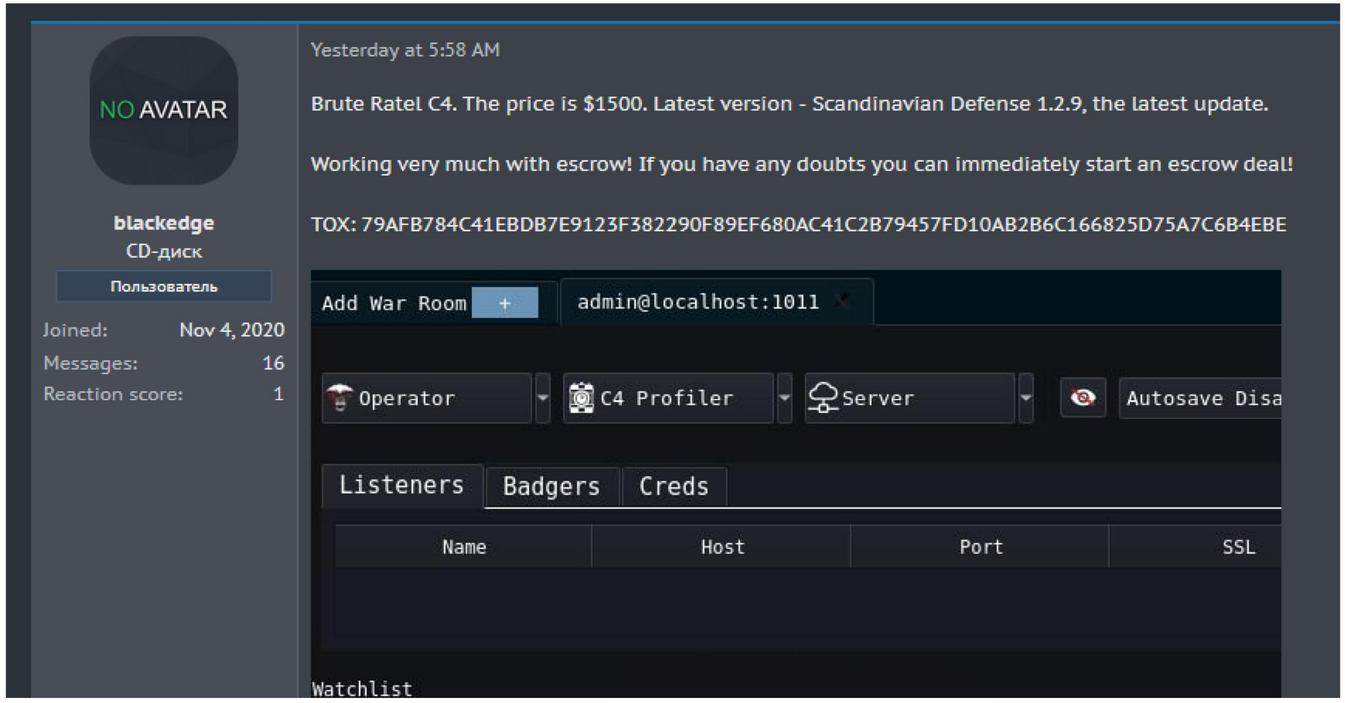
Known vulnerabilities are being used to gain access to exposed routers.

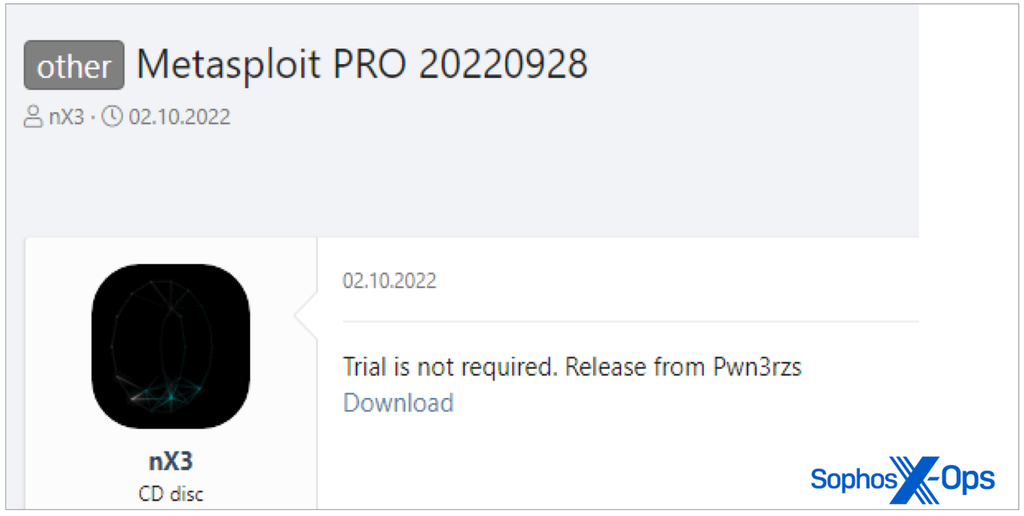
Threat Actors develop **custom tools** or reuse **out-of-the-box pen tools** for data collection and attack execution

FORESCOUT RESEARCH

Use of Offensive Security Tools







Use of Living Off The Land Binaries

LOLBin	Percentage of raw detections	Notes
cmd	92.26%	Default command interpreter
powershell	1.79%	More advanced command-line and scripting shell
certutil	1.09%	Command-line program installed as part of Certificate Services
mshta	1.01%	Microsoft HTML Application Host, allows execution of .HTA (HTML Application)
bitsadmit	0.95%	Background Intelligent Transfer Service, used as part of Windows Update to transfer files
wscript	0.93%	Windows Scripting Host supporting JScript and VBScript execution
bcdedit	0.83%	Command-line tool for managing Boot Configuration Data
rundll32	0.52%	Used to load and run 32-bit dynamic-link libraries (DLLs)
nltest	0.39%	Tool that provides diagnostic information
procdump	0.21%	Command-line application that provides information on system processes

I mercati criminali come Genesis consentono a cybercriminali principianti di acquisire malware e servizi di distribuzione di malware, nonché di vendere credenziali rubate e altri dati in grandi quantità. I booker di accesso stanno sempre più vedendo exploit di software vulnerabile e credenziali ad altre organizzazioni criminali

Questa industrializzazione del ransomware ha permesso ai criminali e ai malware affiliati al ransomware di evolversi in operazioni professionali specializzate nell' exploit. Questi gruppi professionali si specializzano nell'ottenere (o acquistare) accesso per qualsiasi per qualsiasi settore motivato disposto a pagare.

References

- Forescout Research - 2023H1 Threat Review: Vulnerabilities, Threat Actors and Malware – https://www.forescout.com/resources/2023h1-threat-review/
- Forescout Research - The Increasing Threat Posed by Hacktivist Attacks: An Analysis of Targeted Organizations, Devices and TTPs - https://www.forescout.com/resources/threat-report-the-increasing-threat-posed-by-hacktivist-attacks/
- Forescout Research – KillNet Analysis of Attacks from a Prominent Pro- Russian Hacktivist Group - https://www.forescout.com/blog/killnet-analysis-of-attacks-from-a-prominent-pro-russian-hacktivist-group/
- Sophos 2023 Threat Report - Maturing criminal marketplaces present new challenges to defenders : https://www.sophos.com/en-us/content/security-threat-report