



Cyber Security and Data Protection

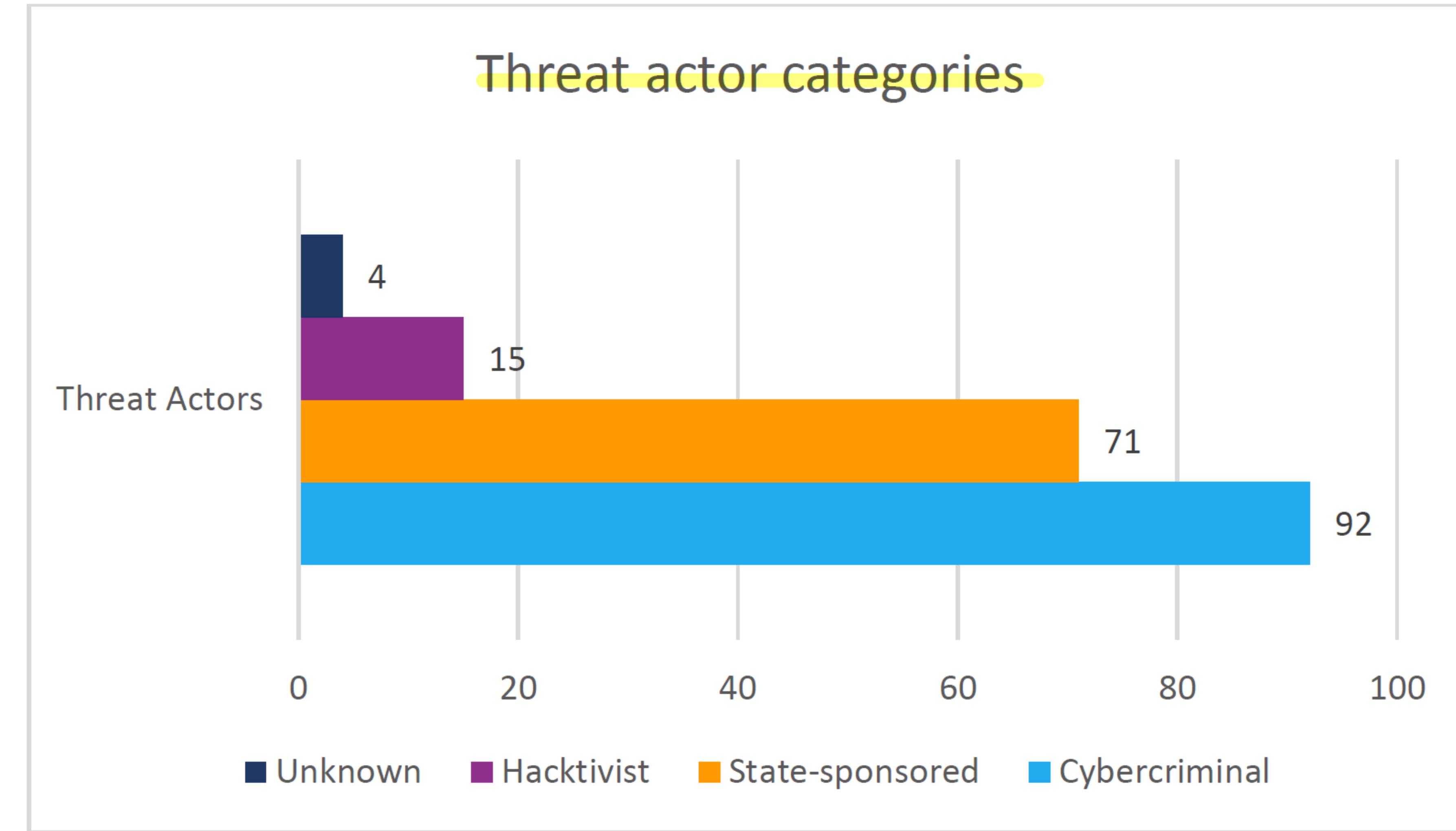
Cyber Threat Actors

Prof.Federica Paci



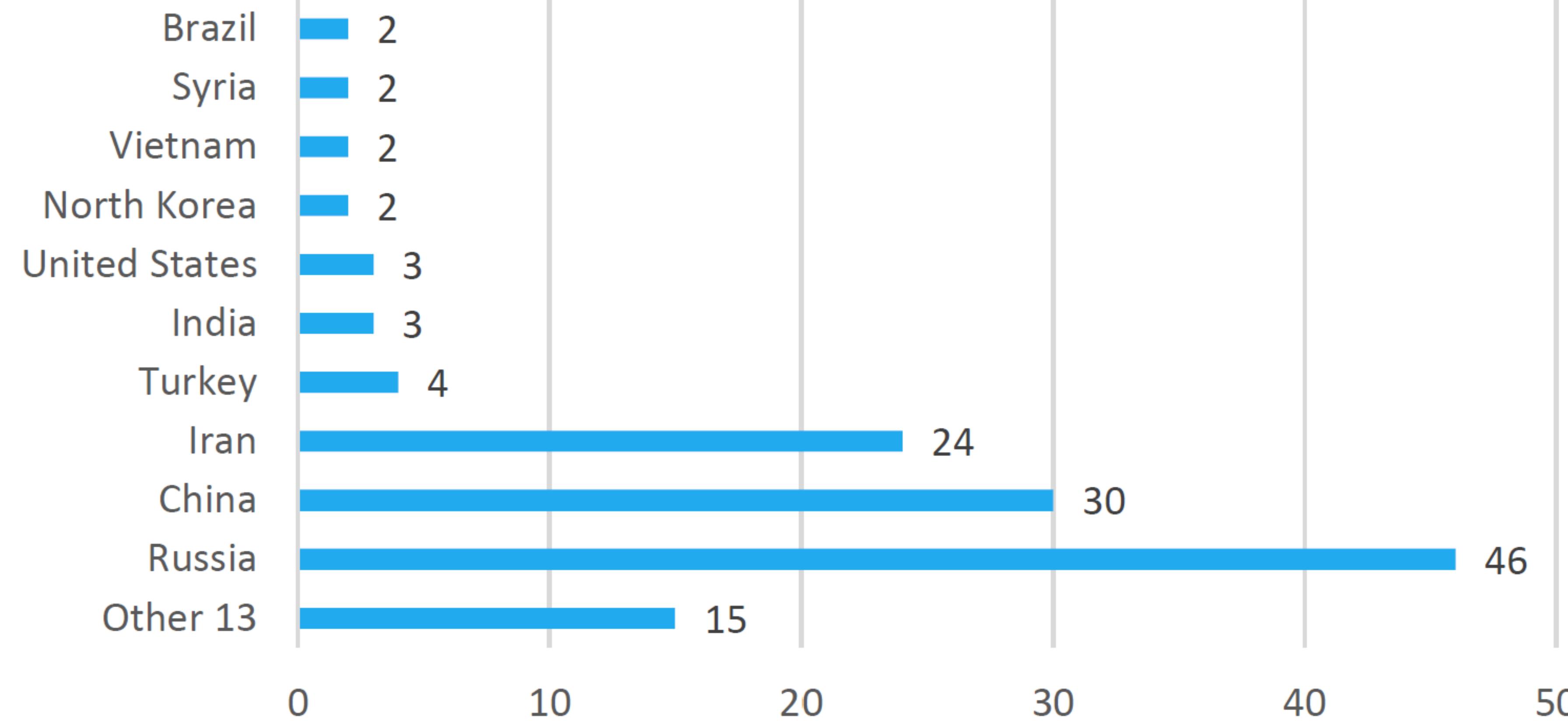
Who is behind the last cyber attacks ?

Threat Actors Categories



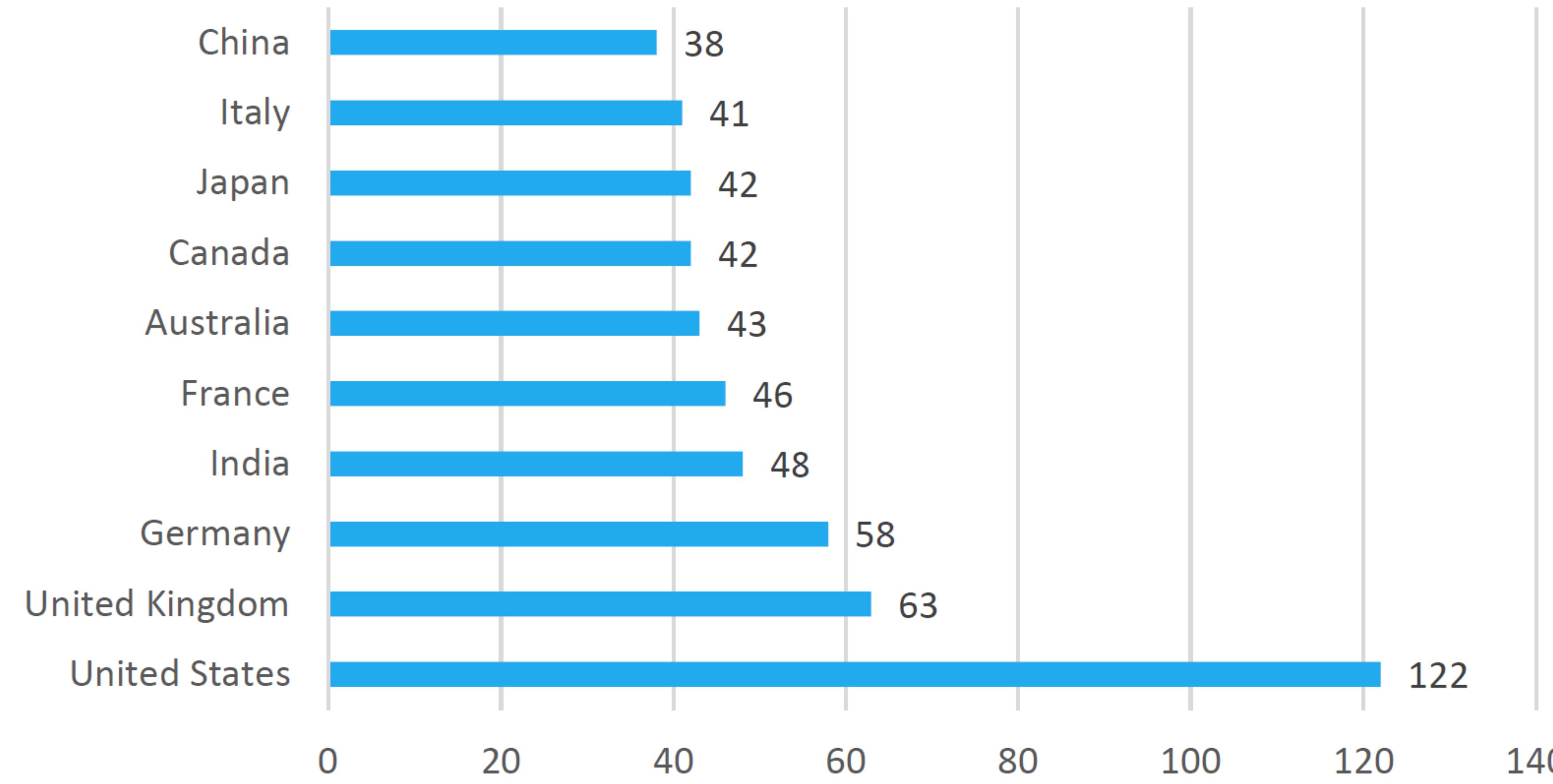
Threat Actors Country of Origin

Threat Actors per country of origin



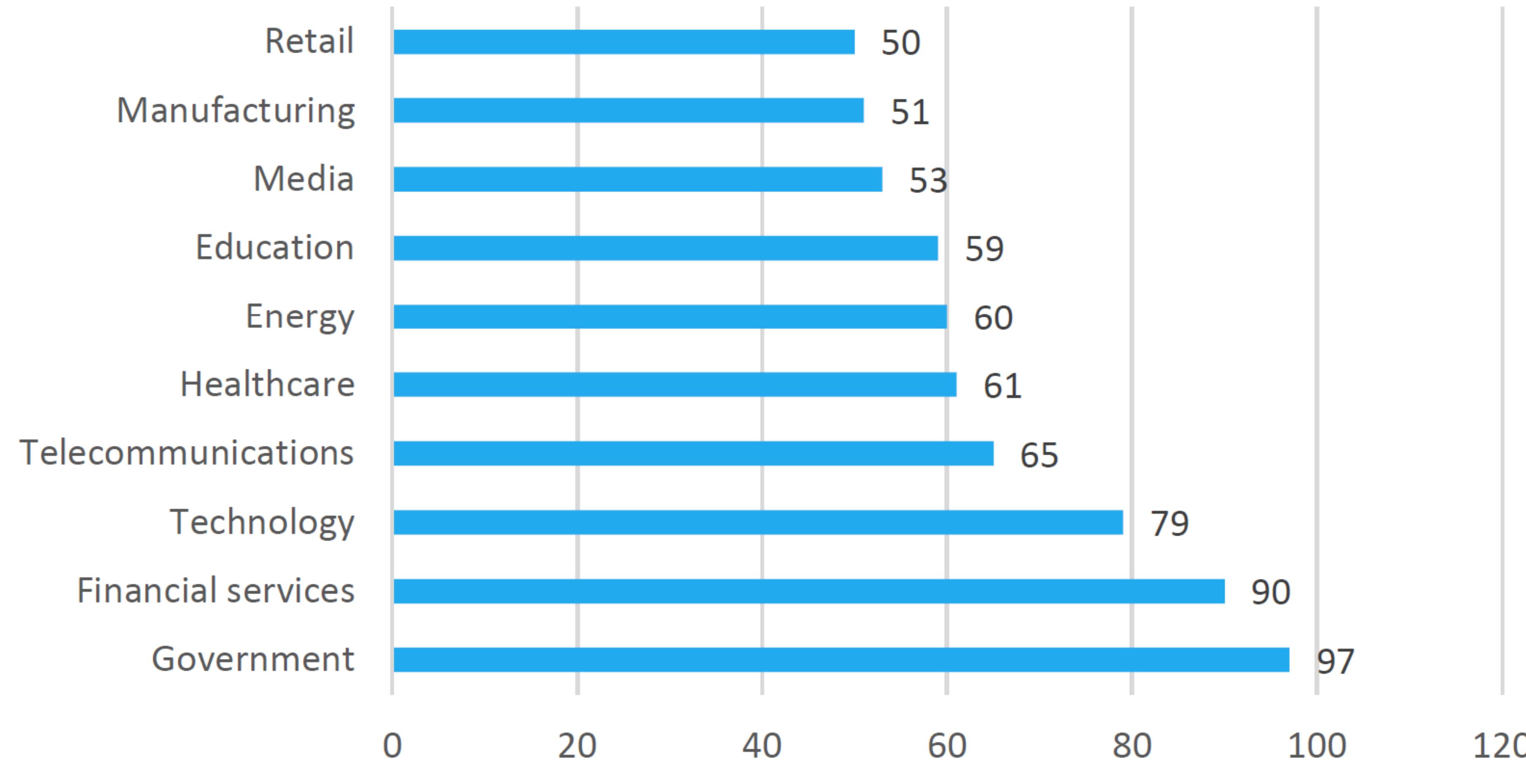
Threat Actors Target Countries

Top 10 targeted countries



Threat Actors – Target Industries

Top 10 targeted industries



Cyber criminals

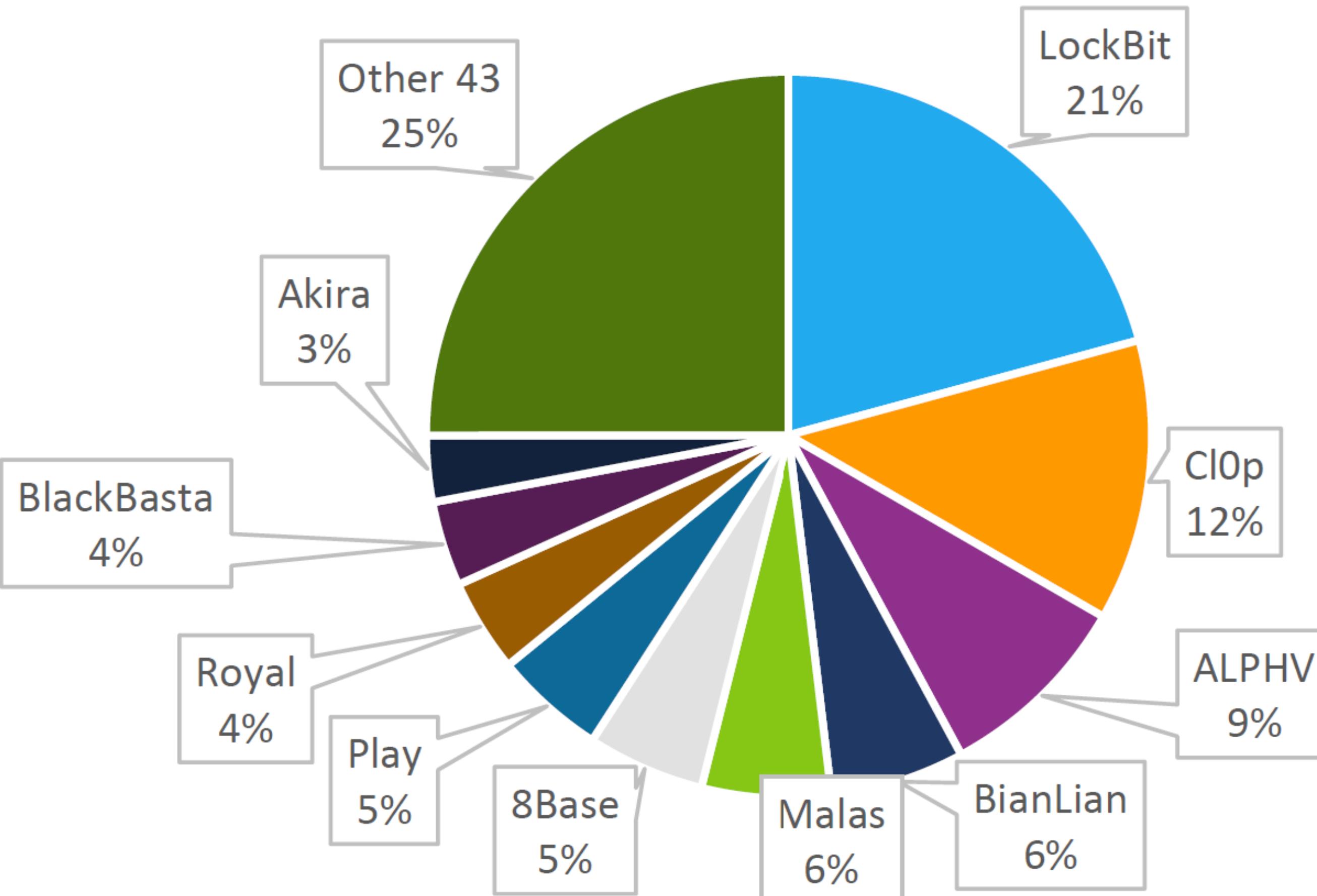
- Interested in illegal profit
- Typical attacks
 - Ransomware
 - Infostealers
 - Proxyjacking

- 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

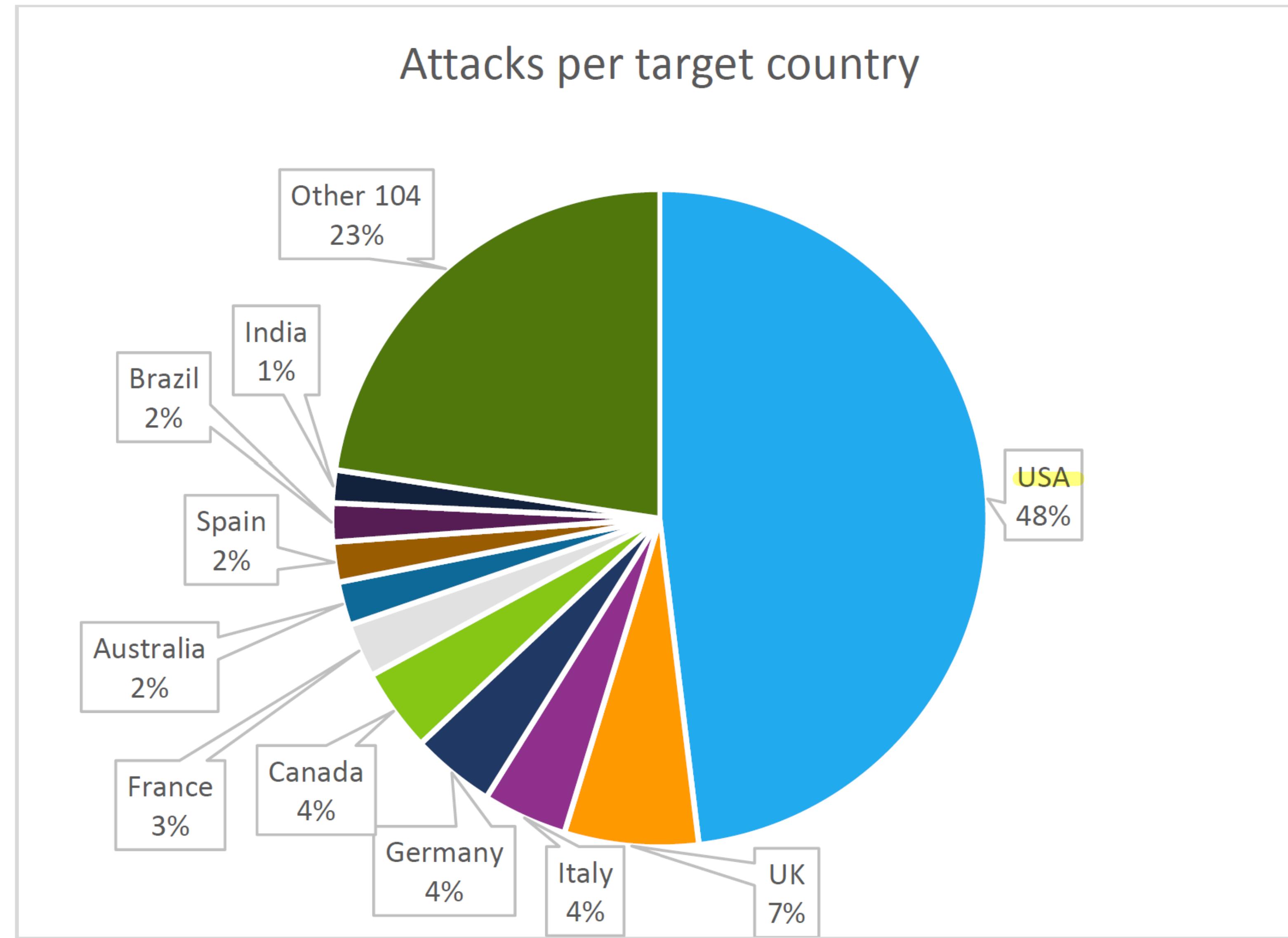


Ransomware Groups

Attacks per group in 2023H1



Ransomware Campaigns' Targets



Info stealers

Raccoon stealer | only serious business

11 September 2022

Channel "ertheryher" created

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)

BLUEFOX STEALER V2 - личный MaaS функционал

distamx · Sep 2, 2022 · bluefox, cookies, mnemonic seed, passwords, stealer, tor, wallets, криптокошельки, сбор seed, стиллер

Sophos X-Ops

ESCROW AVAILABLE IN THIS THREAD!

New deal

The screenshot shows a forum post titled "BLUEFOX STEALER V2 - личный MaaS функционал". The post was made by a user named "distamx" on September 2, 2022. The post includes a user profile with a picture, a "Premium" badge, and statistics: Joined Jun 8, 2019, Messages 120, Reaction score 26, Escrow deals 2, Deposit 0.035. Below the profile, there is a large block of text detailing the stealer's features:

Перенесенная и обновленная из <https://xss.is/threads/60322> standalone версия. Интерфейс был актуализирован, добавлен полезный функционал. Комплексное решение для большого количества трафика и управления логами благодаря системе меток и профилей. Логи на вашем сервере, доступ к ним только у вас.

Нативный x86 исполняемый файл без использования CRT, с запуском .NET в памяти, без зависимости от версии. Вес: 200 KB (~80 KB под UPX). Криптуется как натив. Запуск на Windows 7 - Windows 11 (Windows Server 2008 R2 - Windows Server 2022) x86 x64. Связь с сервером на сокетах через собственный протокол на TCP/IP в зашифрованном виде. Поддерживаются bridge (прокси) сервера для скрытия основного сервера.

Функционал исполняемого файла

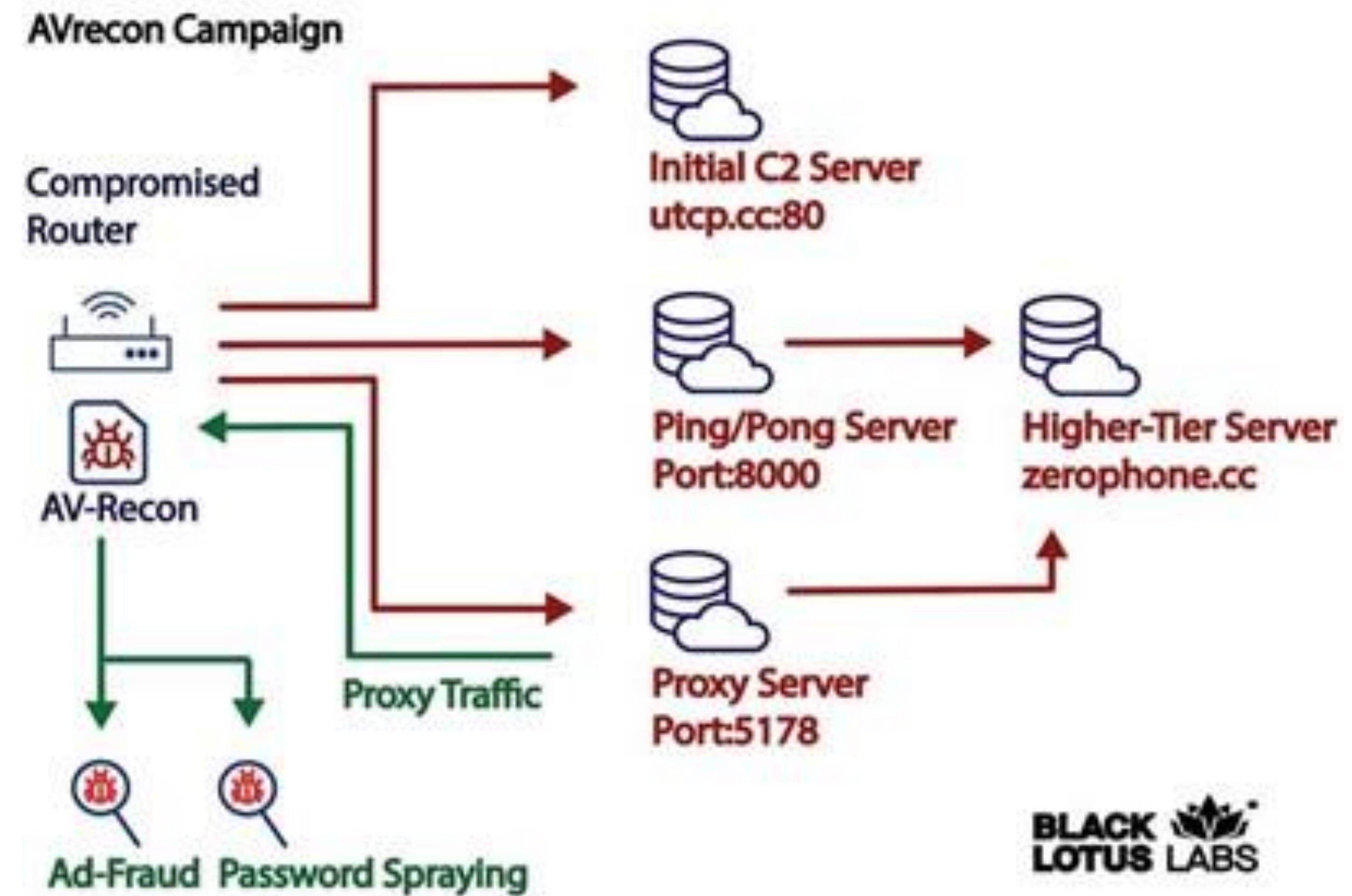
- Сбор паролей, куки, автозаполнений из Chromium (включая 80+ версии, Edge), Firefox-based (включая 74+ версии) через рекурсивный поиск со всех профилей. Расшифровка обоих типов на сервере.
- Сбор парольных расширений и кошельков из браузера: bitwarden, 1Password, robofarm, MetaMask, TronLink, Binance Chain, Yoroi, Coinbase, Jaxx и т.д. со всех профилей.
- Сбор холодных кошельков типа wallet.dat, *.wallet, default_wallet через рекурсивный поиск.
- Сбор холодных кошельков: Ethereum, Electrum, Exodus, Jaxx, frame, Coinomi, Guarda, atomic, Binance, Wasabi, Monero со стандартных путей.
- Сбор данных Pidgin, PSI+/, Thunderbird, FileZilla, Snowflake, Cyberduck, Keepass, NordPass.
- Сбор данных о PC, скриншот рабочего стола сканируется с потерей качества 60% на запускаемой машине.
- Поиск seed фраз BIP39 в файлах с граббера на сервере.
- Добавление путей для софтов в выходной лог (см. скриншоты).
- Настраиваемый граббер файлов через wildcard.
- Настраиваемый лаадер и запуск файлов.

Вся работа с данными происходит в памяти, ничего не подкачивается (dll в том числе), zip собирается на сервере, используется только один файл из %tmp%, удаляется после отправки.



- [!\[\]\(3bf0e820234707dea72b072754f6fe6f_img.jpg\) Free REDLINE Logs 01-02.10.2022](#)
by [shanghaizao](#), ① October 5, 2022, 01:31 AM
- [!\[\]\(7778072f38e36a97832dd8f2ca2e6795_img.jpg\) FREE LOGS \(Pages: 1 2 3 \)](#)
by [jezdicioko](#), ① May 6, 2022, 11:34 PM
- [!\[\]\(db6d4fd1d64d5bb6bbe506bdc56ba5ec_img.jpg\) 1.15M botnet logs from darth-maul.top \(Pages: 1 2 3 4 \)](#)
by [jules](#), ① March 19, 2022, 10:05 AM
- [!\[\]\(2f08b32f6943a6d1a8116d98ce45b74b_img.jpg\) 10GB Stealer logs \(Mixed\) 2022 \(Pages: 1 2 3 4 \)](#)
by [buffbyte](#), ① June 20, 2022, 04:18 PM
- [!\[\]\(7494e1ed795865daeeb04378d257e080_img.jpg\) 875 logs REDLINE 04.10](#)
by [shanghaizao](#), ① Yesterday, 07:48 AM
- [!\[\]\(49a034655720744b57cb1b5b2d92c7d5_img.jpg\) 1535 Fresh logs from redline stealer \(18.09\) \(Pages: 1 2 3 \)](#)
by [Eyes2](#), ① September 18, 2022, 05:20 PM
- [!\[\]\(b0f9c5767051615b0a8a0ee6ccb220ac_img.jpg\) fresh logs from redline stealer](#)
by [jd1zzl3](#), ① October 4, 2022, 12:00 PM
- [!\[\]\(922e20e33ccc2e8248ea6548a7406b6f_img.jpg\) 260 + Netflix Logs Last And Fresh \(Pages: 1 2 \)](#)
by [EvilHacker](#), ① September 30, 2022, 03:34 PM
- [!\[\]\(b6043c19411599f3d5cb6bede9595fda_img.jpg\) BRAZIL LOGS #2 +800 MB \(Pages: 1 2 3 \)](#)
by [HappyMDFK](#), ① September 9, 2022, 12:29 PM
- [!\[\]\(f5c0cbbb0b48b69d65353bb50bba716d_img.jpg\) 750x Valorant Stealer Log \(Pages: 1 2 \)](#)
by [d4rkness0](#), ① September 9, 2022, 07:20 AM

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'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

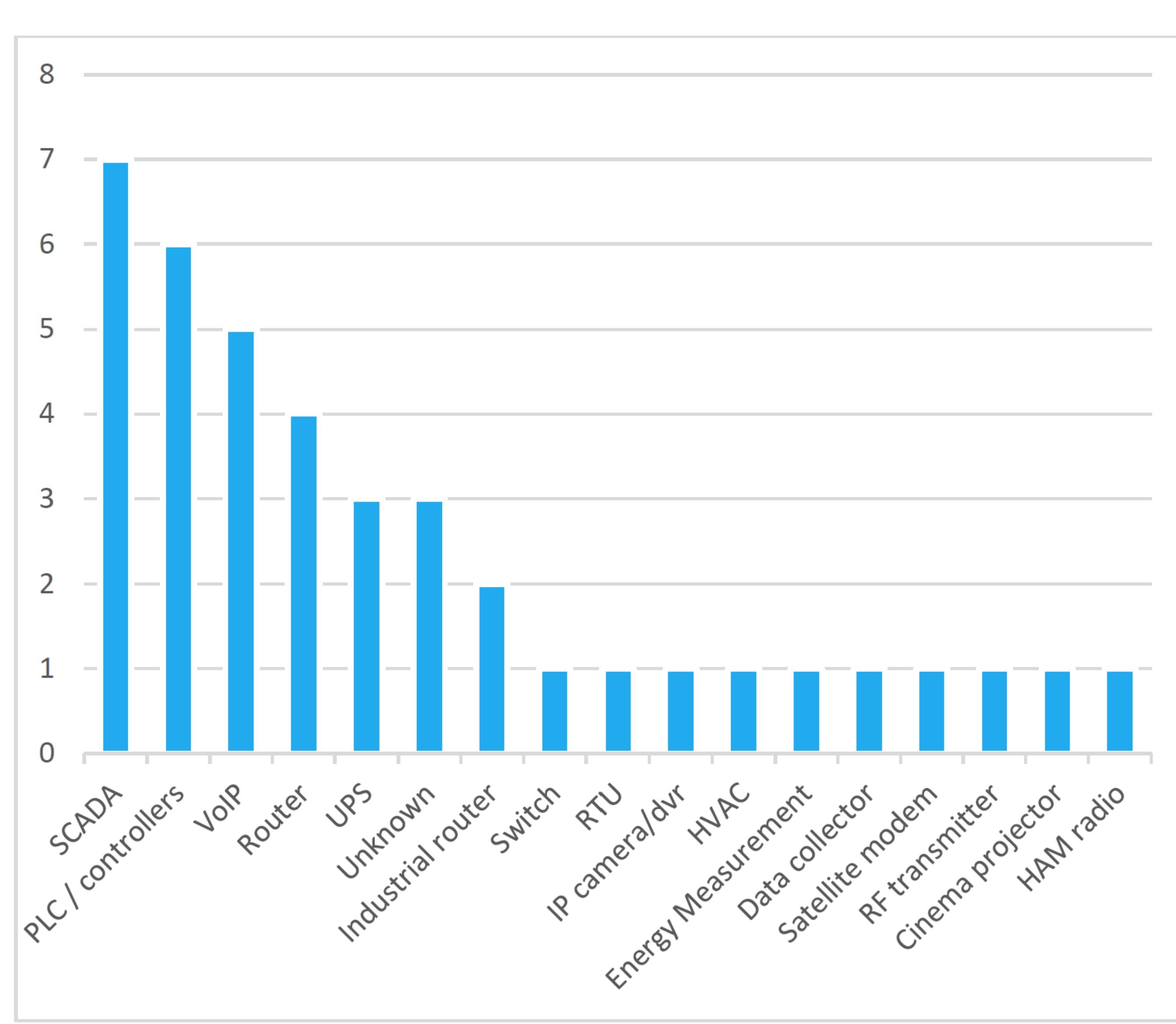


Hacktivists

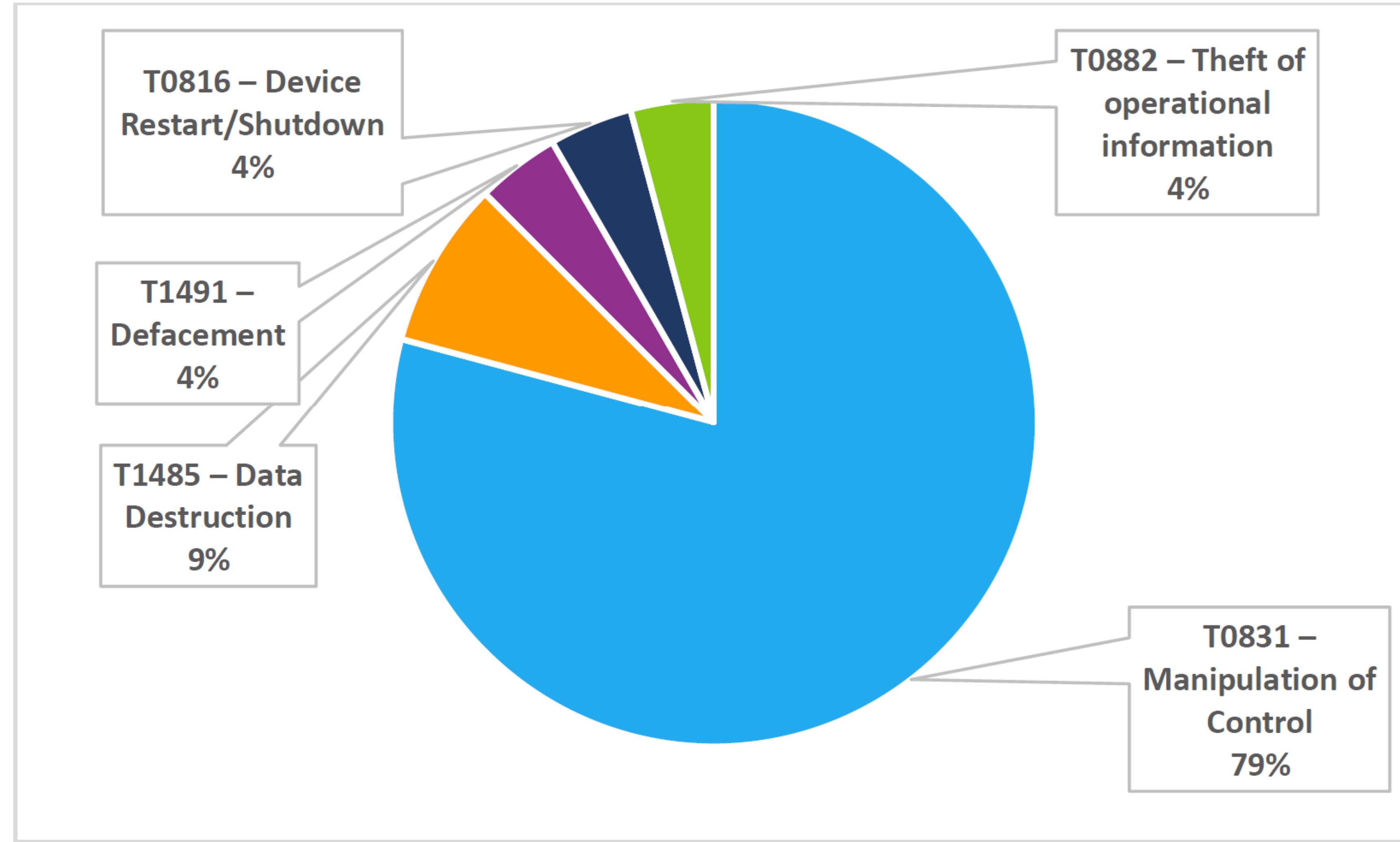
- Motivated by
 - Political views*
 - Cultural/religion belief*
 - National Pride*
 - Terrorist Ideology*
- Typical attacks
 - distributed denials of service (DDoS),
 - data breaches or leaks
 - data wipers
 - distributing propaganda
 - attacks to unmanaged devices



Targeted Unmanaged Devices



Common Techniques



Anonymous



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

Print this Message.pdf - Adobe Acrobat Reader DC (64-bit)

View Sign Window Help

Tools Print this Message... x

Printer HL-1210W series Properties Advanced

Print in grayscale (black and white) Save ink/toner

Scale: 96% 8.5 x 11 Inches

Current Pages 1 - 2

& Handling

Poster Multiple Booklet

Actual size Custom Scale: 100 %

Fit source by PDF page size

Both sides of paper

Portrait Landscape

Forms

Summarize Comments

Print

Page 1 of 2

Printer Document View

Brother HL-1210W series Microsoft Print to PDF (redirected 2)

Unspecified (4) KX (XPS) v4 Driver for U

Document Name Status Owner Pages Size Submitted

Print this Message.pdf Administra... 2 237 KB 7:40:33 PM

Print this Message.pdf Administra... 2 237 KB 7:40:26 PM

Print this Message.pdf Administra... 2 237 KB 7:40:11 PM

Print this Message.pdf Administra... 2 237 KB 7:40:07 PM

Print this Message.pdf Administra... 2 237 KB 7:39:59 PM

Print this Message.pdf Printing Administra... 2 79.6 KB/237 KB 7:39:47 PM

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



Team OneFist

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



This map of Ukraine in the dark
is now available online.



 Let's Chat!

← **GhostSec**
196 posts

F NOT US, THEN WHO ?
F NOT NOW, THEN WHEN ?



Follow

GhostSec
@ghost_s3curity

Official #GhostSec • #HackThePlanet • #GSM #Anonymous • #Oplran
#GhostSecMafia

📍 No Nation 🔗 t.me/GhostSecc 📅 Joined June 2022

26 Following **7,241 Followers**

KillNet

DDOS MAP POLAND

⚡ 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"

|"Každa agresja ze strony polskiej władzy w kierunku Rosji, natychmiast rozpoczęcie cyklu zmasowanego ataku ddos na wszystkie istotne i Państwowe zasoby sieciowe"

196 1 32.8K 19:04



| 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 ↳ Cybersecurity and Infrastructure Agency o altamente sofisticati da parte loro



How do Threat Actors operate?

Attack as a service

Sep 6, 2022

FRESH 400 RDP'S 50%+ VALID RATE (200 RDP's)

Replacement Available Only in 24 Hours Not more

ZoomInfo And other things I Didn't checked I don't have time

Romanians
HDD-drive
Пользователь

Joined: Jun 14, 2022
Messages: 35
Reaction score: 0

200/RDP's
Mix Country / Bulk Selling
99% Administrator Rights
90% NO ANTIVIRUS
Local / Shares / Neighbor PC's
80% Asian Country Korea / China / HK / India . etc
Workgroup
10\$ 1 RDP

start 2 000\$
step \$500
Blits 4 000\$

Garantor will always be accepted here!

Sophos X-Ops

★ Spreading your Virus (installs) ★

ZorosPalace •
Junior
Member
• •

01-28-2022, 02:49 PM

Greetings,

Welcome to our new service. We are spreading your viruses/loggers (.exe) all over the world, including USA, EU, CA, AU, NZ, GB.

The virus will be spread by a webmaster.

You can specify which regions you would like to spread your virus. We can do the following regions:

(prices for 1000 downloads)
-World - 200\$
-Europe - 1500\$
-USA - 2000\$
-CA, AU, NZ, GB - 1200\$

Minimum download volume is 500.
Maximum download volume we can parse is 20.000 (more can be discussed privately)

We will provide the statistics.

Bulk orders receive good discounts.

We do not load these types of viruses: Lockers, Encryptors, Ransomware

Everything as a service

Phi4er

kilobyte
••



Active arbitrage

• 0
27 posts

Joined

06/24/22 (ID: 132361)

Activity
кодинг / coder

Posted June 24 (edited)

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.

SophosX-Ops

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

SophosX-Ops

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.

Compromise network devices for initial access



INTERNET



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



Use of Offensive Security Tools

VirusTotal Enterprise(Downloader)
by mbrk256 - Wednesday September 28, 2022 at 12:40 PM

September 28, 2022, 12:40 PM (This post was last modified: September 28, 2022, 02:31 PM by mbrk256.)

I'm selling software that provides VirusTotal Enterprise with an annual fee of \$10,000.

[You can download any file in virustotal you want using this software.](#)

Using the software is quite simple. You just need the virustotal scan result link.

Usage Video:

[virustotal-enterprise](#)
Powered by dailymotion

Pricing:
\$400 annual license

mbrk256

BreachForums User

MEMBER

Posts: 3
Threads: 1
Joined: Sep 2022
Reputation: 0

Yesterday at 5:58 AM

Brute Ratel C4. The price is \$1500. Latest version - Scandinavian Defense 1.2.9, the latest update.

Working very much with escrow! If you have any doubts you can immediately start an escrow deal!

TOX: 79AFB784C41EBDB7E9123F382290F89EF680AC41C2B79457FD10AB2B6C166825D75A7C6B4EBE

blackedge
CD-диск

Пользователь

Joined: Nov 4, 2020
Messages: 16
Reaction score: 1

Add War Room + admin@localhost:1011

Operator C4 Profiler Server Autosave Disa

Listeners Badgers Creds

Name Host Port SSL

Watchlist

other Metasploit PRO 20220928

nX3 · 02.10.2022

02.10.2022

Trial is not required. Release from Pwn3rzs
[Download](#)

nX3
CD disc

Sophos X-Ops

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 broker di accesso siamo 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>