Hacktivismo y Ciberguerra

Del clic a la crisis: Protesta y poder en el ciberespacio

Por: David Ramos

IEEE CS ITCR

IEEE COMPUTER SOCIETY
Instituto Tecnológico de Costa Rica
Student Branch Chapter

$whoami

David Ramos Rodriguez (Aka. D0V0)

Digital Forensics Specialist at Lazarus Technology

Coordinador CiberSecUNI
CPTE | CTIA | DFE | eJPT | SC-900 | ISO | SSYB | SFC
Systems Engineering - UNI (⏳)

- 🌎 Advance CTF Ekoparty 2025 - Buenos Aires, Argentina - 2do Puesto
- 🌎 International Cybersecurity Challenge 2024 - Santiago de Chile - 6to Puesto.
- 🌎 **CyberChallenge 2024 OEA - San José, Costa Rica - 2do Puesto.**
- 🌎 CTF Pacifico Seguros Prima AFP - Lima, Perú - 1er Puesto.
- 🌎 International Cybersecurity Challenge 2023 - San Diego, USA - 6to Puesto.
- 🌎 OEA CyberChallenge 2023 - Santiago de Chile - 2do Puesto.
- 🌎 CTF Metared Internacional - Perú 2022 | 2023 | 2024 - 1er Puesto.
- 🧧 Entre otros

Participant in OAS Cybersecurity Program
HackTheBox #Top10 Perú | HTB Ambassador

HACKTHEBOX

<CIBERSEC> UNI

“El hacking descubre la grieta en el sistema; el forense reconstruye la historia que intentaron borrar.”

Contenido

01 Humanidad interconectada
02 Hacktivismo
03 Ciberguerras

Instructor: David Ramos
https://www.linkedin.com/in/david-ramos-rodriguez/

Humanidad interconectada

Tribus digitales, identidad fragmentada y algoritmos sociales

Instructor: David Ramos
https://www.linkedin.com/in/david-ramos-rodriguez/

Las sociedades modernas no solo viven en el mundo, sino también en la red. El ciberespacio se ha convertido en una extensión del tejido social humano.

- Neo-tribus digitales
- Comunidad sin territorio
- Cultura compartida en red

- Identidad múltiple
- El yo en red
- Simulación y vigilancia

Ponente: David Ramos
https://www.linkedin.com/in/david-ramos-rodriguez/

Arquitectura de lo social

La tecnología que usamos configura nuestras relaciones. Los algoritmos seleccionan lo que vemos, deciden con quién interactuamos. Redes como Facebook, X o TikTok no son solo plataformas: son entornos sociales diseñados. Esta arquitectura digital no es neutral: influye en nuestras creencias, emociones y acciones colectivas. Aquí es donde entran fenómenos como el hacktivismo y la ciberguerra.

Cambridge Analytica

Ponente: David Ramos
https://www.linkedin.com/in/david-ramos-rodriguez/

El ciberespacio no es virtual, es real.

Habitamos un nuevo tipo de sociedad.

La conexión transforma lo humano.

Ponente: David Ramos
https://www.linkedin.com/in/david-ramos-rodriguez/

Hacktivismo

Activismo

Ciberactivismo

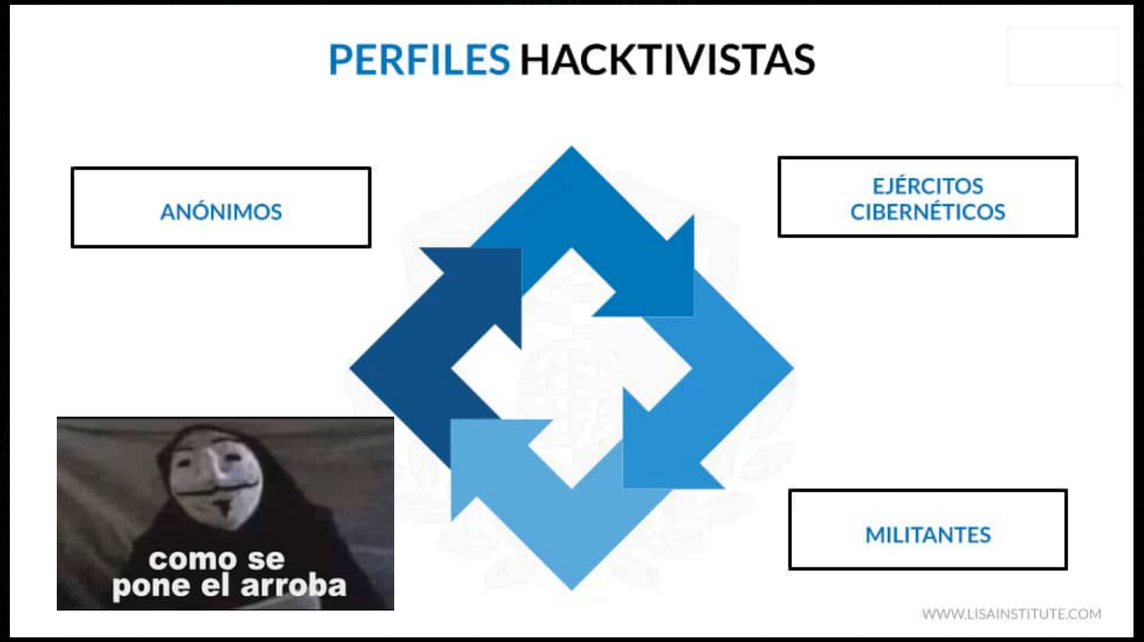
Hactivismo

Hacker + Activismo

Ponente: David Ramos
https://www.linkedin.com/in/david-ramos-rodriguez/

Un hacker se caracteriza por su amplio conocimiento de los sistemas informáticos y por su interés en ampliar las capacidades de éstos. Este conocimiento lleva a los hackers al descubrimiento de técnicas que permiten cambiar las propiedades de los sistemas y explotar su potencialidad.

Un hacktivista es un hacker que usa sus conocimientos informáticos para llevar a cabo acciones en el ciberespacio con una finalidad y una motivación políticas o ideológicas.

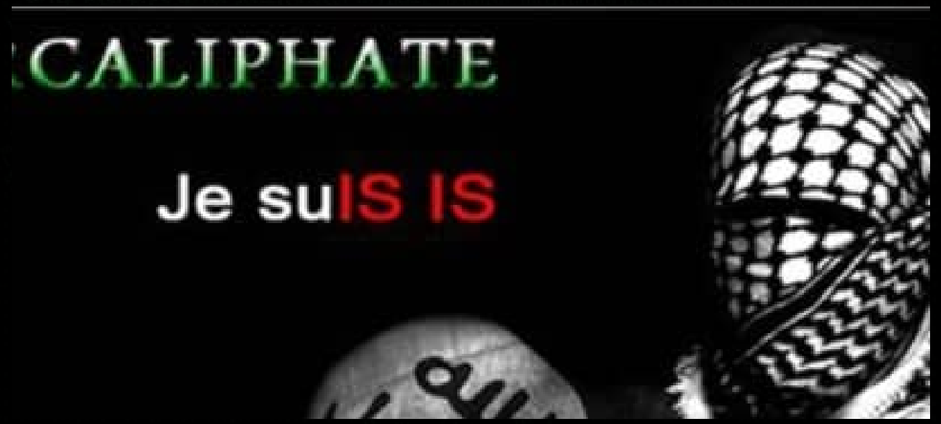


Fuente: LISA INSTITUTE

Ponente: David Ramos
https://www.linkedin.com/in/david-ramos-rodriguez/

Motivaciones principales

- Causas políticas (ej. Palestina, anticorrupción)
- Causas sociales (derechos humanos, antirracismo)
- Motivos religiosos o nacionalistas



Ponente: David Ramos
https://www.linkedin.com/in/david-ramos-rodriguez/

Cronología

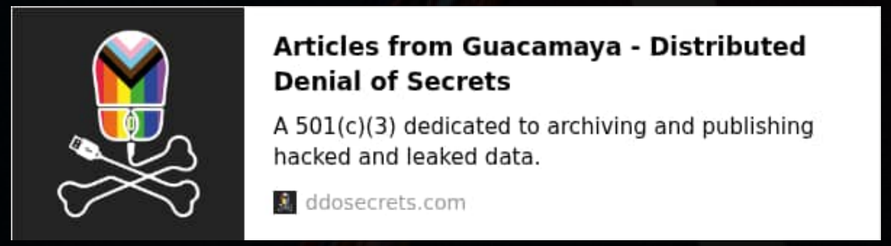
- 1984 – Cult of the Dead Cow (cDc): Defensores del acceso a la información, la privacidad y los derechos digitales.
- 1987 – Critical Art Ensemble (CAE): Arte, ciencia y política. - Resistencia cultural (Control, Poder Tech, Capitalismo).
- 1989 – Worms Against Nuclear Killers (WANK) Infiltración de sistemas de la NASA como protesta contra el lanzamiento del transbordador con material nuclear.
- 1997 – Electronic Disturbance Theater (EDT): Apoyo a movimientos indígenas, derechos humanos, desobediencia civil digital.
- 1999 – Electrohippies Collective (Reino Unido): Ataques DDoS contra cumbres de la Organización Mundial del Comercio.
- 2003 – Anonymous (Internacional): Colectivo descentralizado que surgió en foros como 4chan. DDoS, filtraciones, doxxing.
- 2007 – WikiLeaks (Internacional): Plataforma de filtración de documentos clasificados.
- 2011 – LulzSec (Internacional): Escisión de Anonymous, con un enfoque satírico y disruptivo. (lulz).
- 2014 – Lizard Squad (Internacional): Grupo más orientado al caos. DDoS contra PlayStation Network, Xbox Live, y aerolíneas.

Ponente: David Ramos
https://www.linkedin.com/in/david-ramos-rodriguez/

Cronología

2022 – Guacamaya (Latinoamérica): Colectivo hacktivista con enfoque anticolonial y antimilitarista. Filtraciones masivas a las fuerzas armadas de México, Chile, Colombia, Perú, y otros.

- **Hackeo al Estado Mayor Conjunto de Chile**
- **Hackeo a la Secretaría de la Defensa Nacional de México**
- **Policía Nacional Civil de El Salvador**
- **Comando General de las Fuerzas Militares de Colombia**
- **Fiscalia of Colombia**
- **Fuerza Armada de El Salvador**



Ponente: David Ramos
https://www.linkedin.com/in/david-ramos-rodriguez/

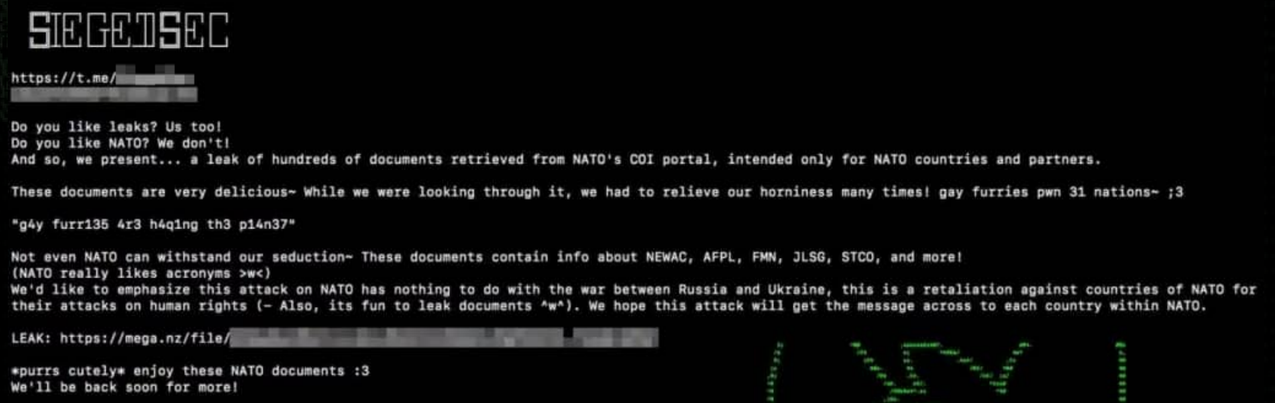
Cronología

- Killnet (Rusia): Colectivo hacktivista prorruso surgido tras la invasión a Ucrania.
- **Anonymous Sudan: Grupo que se presenta como islamista sudanés, pero se sospecha vínculo con operaciones rusas (afiliado a Killnet).**

Ponente: David Ramos
https://www.linkedin.com/in/david-ramos-rodriguez/

Cronología

- SiegedSec: Colectivo satírico y caótico con inclinación progresista. Hacktivismo por los derechos civiles y memes.



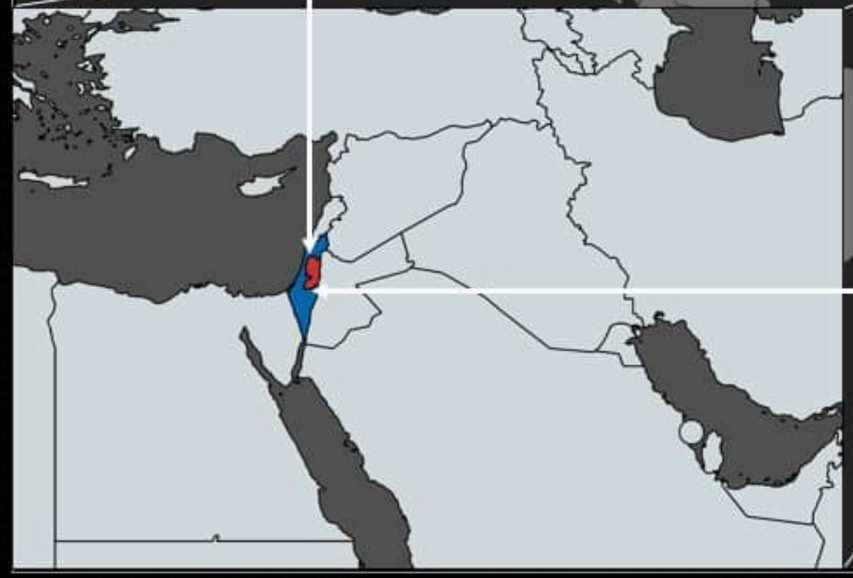
Ponente: David Ramos
https://www.linkedin.com/in/david-ramos-rodriguez/

9 OCT2023 Israel-Palestine CyberTracker – 39 Total Groups

Twitter.com/cyberknow20

Pro-Israel - 4 Groups

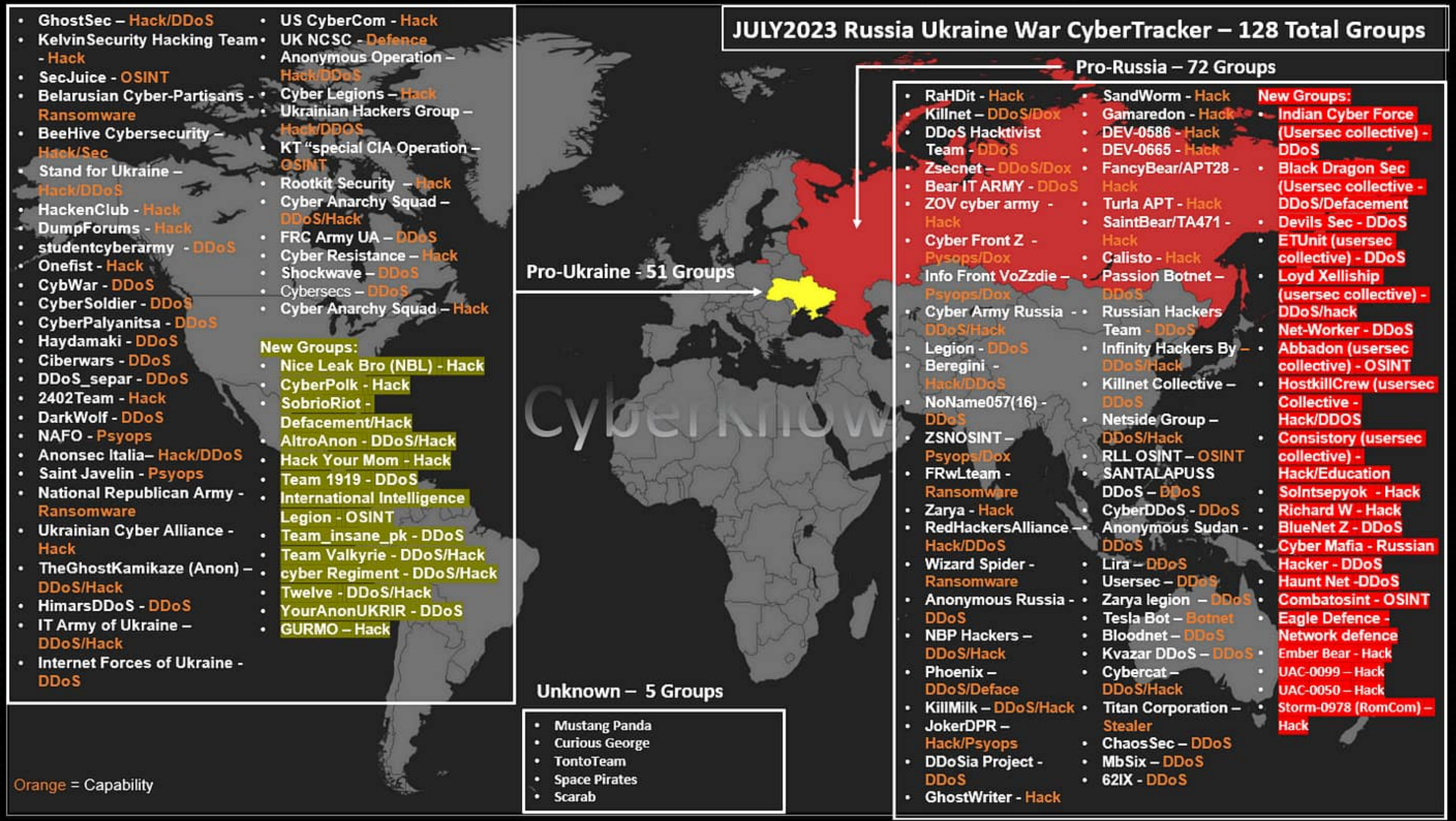
- Team UCC Operations – DDoS
- Garuna Ops – DDoS
- Indian Cyber Force – DDoS
- SilentOne – DDoS



Pro-Palestine – 35 Groups

- Mysterious Team Bangladesh – DDoS
- Team Herox – DDoS
- Ghosts of Palestine – DDoS
- AnonGhost – DDoS
- Blackshieldcrew MY – DDoS
- GhostClan – DDoS
- Anonymous Sudan – DDoS – Pro Russian
- Team_insane_Pakistan – DDoS
- Ganosec team – DDoS
- Team Azrael Angel of Death – DDoS
- Garnesia Team – DDoS
- Moroccan Black Cyber Army – DDoS
- Hacktivism Indonesia – DDoS
- 4 Exploitation – DDoS
- Gb Anon 17 – DDoS
- Team_r70 – DDoS
- Electronic Tigers Unit – DDoS
- YourAnonTl3x – DDoS
- Stucx Team – DDoS
- Hizbullah Cyb3r Team – DDoS
- StarsX Team – DDoS
- Cscrew – DDoS
- SynixCyberCrimeMY – DDoS
- TYG Team – DDoS
- Eagle Cyber Crew – DDoS
- Ghost Clain Malaysia – DDoS
- 1915 Team – DDoS
- Kerala Cyber Xtractors – DDoS
- Killnet – DDoS – Pro Russian
- Panoc team – DDoS
- Sylhet Gang-SG – DDoS
- Muslim Cyber Army – DDoS
- Anonymous Morocco – DDoS
- Pakistani Leet Hackers – DDoS
- Cyber Av3ngers – DDoS

JULY2023 Russia Ukraine War CyberTracker – 128 Total Groups



Pro-Russia – 72 Groups

- RaHDit - Hack
- Killnet – DDoS/Dox
- DDoS Hacktivist Team - DDoS
- Zsecnet – DDoS/Dox
- Bear IT ARMY - DDoS
- ZOV cyber army - Hack
- Cyber Front Z - Psyops/Dox
- Info Front VoZzdie – Psyops/Dox
- Cyber Army Russia - DDoS/Hack
- Legion - DDoS
- Beregini - Hack/DDoS
- NoName057(16) - DDoS
- ZSNOSINT – Psyops/Dox
- FRwLteam - Ransomware
- Zarya - Hack
- RedHackersAlliance – Hack/DDoS
- Wizard Spider - Ransomware
- Anonymous Russia - DDoS
- NBP Hackers – DDoS/Hack
- Phoenix – DDoS/Deface
- KillMilk – DDoS/Hack
- JokerDPR – Hack/Psyops
- DDoSia Project - DDoS
- GhostWriter - Hack
- SandWorm - Hack
- Gamaredon - Hack
- DEV-0586 - Hack
- DEV-0665 - Hack
- FancyBear/APT28 - Hack
- Turla APT - Hack
- SaintBear/TA471 - Hack
- Calisto - Hack
- Passion Botnet – DDoS
- Russian Hackers Team - DDoS
- Infinity Hackers By – DDoS/Hack
- Killnet Collective – DDoS
- Netside Group – DDoS/Hack
- RLL OSINT – OSINT
- SANTALAPUSS DDoS – DDoS
- CyberDDoS - DDoS
- Anonymous Sudan - DDoS
- Lira – DDoS
- Usersec – DDoS
- Zarya legion – DDoS
- Tesla Bot – Botnet
- Bloodnet – DDoS
- Kvazar DDoS – DDoS
- Cybercat – DDoS/Hack
- Titan Corporation – Stealer
- ChaosSec – DDoS
- MbSix – DDoS
- 62IX - DDoS

New Groups:

- Indian Cyber Force (Usersec collective) - DDoS
- Black Dragon Sec (Usersec collective - DDoS/Defacement
- Devils Sec - DDoS
- ETUnit (usersec collective) - DDoS
- Loyd Xelliship (usersec collective) - DDoS/hack
- Net-Worker - DDoS
- Abbadon (usersec collective) - OSINT
- HostkillCrew (usersec Collective - Hack/DDOS
- Consistory (usersec collective) - Hack/Education
- Sointsepyok - Hack
- Richard W - Hack
- BlueNet Z - DDoS
- Cyber Mafia - Russian Hacker - DDoS
- Haunt Net -DDoS
- Combatosint - OSINT
- Eagle Defence - Network defence
- Ember Bear - Hack
- UAC-0099 – Hack
- UAC-0050 – Hack
- Storm-0978 (RomCom) – Hack

Pro-Ukraine - 51 Groups

- GhostSec – Hack/DDoS
- KelvinSecurity Hacking Team - Hack
- SecJuice - OSINT
- Belarusian Cyber-Partisans - Ransomware
- BeeHive Cybersecurity – Hack/Sec
- Stand for Ukraine – Hack/DDoS
- HackenClub - Hack
- DumpForums - Hack
- studentcyberarmy - DDoS
- Onefist - Hack
- CybWar - DDoS
- CyberSoldier - DDoS
- CyberPalyanitsa - DDoS
- Haydamaki - DDoS
- Ciberwars - DDoS
- DDoS_separ - DDoS
- 2402Team - Hack
- DarkWolf - DDoS
- NAFO - Psyops
- Anonsec Italia– Hack/DDoS
- Saint Javelin - Psyops
- National Republican Army - Ransomware
- Ukrainian Cyber Alliance - Hack
- TheGhostKamikaze (Anon) – DDoS/Hack
- HimarsDDoS - DDoS
- IT Army of Ukraine – DDoS/Hack
- Internet Forces of Ukraine - DDoS
- US CyberCom - Hack
- UK NCSC - Defence
- Anonymous Operation – Hack/DDoS
- Cyber Legions – Hack
- Ukrainian Hackers Group – Hack/DDOS
- KT "special CIA Operation – OSINT
- Rootkit Security – Hack
- Cyber Anarchy Squad – DDoS/Hack
- FRC Army UA – DDoS
- Cyber Resistance – Hack
- Shockwave – DDoS
- Cybersecs – DDoS
- Cyber Anarchy Squad – Hack

New Groups:

- Nice Leak Bro (NBL) - Hack
- CyberPolk - Hack
- SobrioRiot - Defacement/Hack
- AltroAnon - DDoS/Hack
- Hack Your Mom - Hack
- Team 1919 - DDoS
- International Intelligence Legion - OSINT
- Team_insane_pk - DDoS
- Team Valkyrie - DDoS/Hack
- cyber Regiment - DDoS/Hack
- Twelve - DDoS/Hack
- YourAnonUKRIR - DDoS
- GURMO – Hack

Unknown – 5 Groups

- Mustang Panda
- Curious George
- TontoTeam
- Space Pirates
- Scarab

Orange = Capability

Hacktivism Coalitions (Jan 2025)

Flavio Queiroz, MSc, CISSP, CISM, CRISC, CCISO
Cyber Threat Intelligence Leader

HydraCorps
High Alert Red Zone
Red Wolf Cyber Team
Keymous+
French Hackers Squad
SECTOR16
TEAM BD CYBER NINJA
New Republic of Coalition
WOLF CYBER ARMY
ANONPIONEERS
NoName
SPIDER-X
Worms Viruses Bd
Z-BL4CK-H4T
BLACK HAT ZOMBIES
CYBER TEAM INDONESIA
Anonymous Guys
INDOHAXSEC
ENTHER ERROR SYSTEM
DXPLOIT
NATION OF SAVIORS
ONE Thousand and ONE
DEFACER KAMPUNG

Main Hub Group

These groups act as central nodes, facilitating alliances and serving as a bridge between different groups.

Hacktivist Coalitions (Apr 2025)

Flavio Queiroz, MSc, CISSP, CISM, CRISC, CCISO
Cyber Threat Intelligence Leader

Main Hub Group

These groups act as central nodes, facilitating alliances and serving as a bridge between different groups.

Dark Storm Team
AL AHAD
ANONPIONEERS
Kal Egy 319
VORTEX
The Anonymous 71
Spider-X
NoName
Electronic Army Special Forces
Golden Falcon
AL-QASSAM CYBER BRIGADES
PalachPro
Captain Error [BD]
ANON SEC
WEBSEC
Vulture
ARAB GHOSTS HACKERS
NATIONS OF SAVIORS
UMMAH LEAGUE
Keymous
SYLHET GANG-SG
HulkSec
Dark Cyber Gang
LulzSec Arabs
ANONYMOUS JORDAN
RABBIT CYBER TEAM
KEDIRISECTEAM

NoName057(16)

While Trudeau spends millions to support Kiev, we continue to work on Canada's internet infrastructure

❌**Virgin Plus is a Canadian provider of postpaid and prepaid wireless voice, text, and data services across Canada (dead on ping)**
check-host.net/check-report/20fe256dkd2a

❌**Virgin Mobile Canada, login portal (dead by ping)**
check-host.net/check-report/20fe2a8ck5ae

❌**Télébec LP — telephone company (dead by ping)**
check-host.net/check-report/20fe2e39k9b9

❌**Télébec LP - Canadian telephone company, authorization portal (dead by ping)**
check-host.net/check-report/20fe3142kd94

❌**Primus Canada — carrier (dead by ping)**
check-host.net/check-report/20fe3383kc6e

❌**Bell MTS Inc - Telecommunications Services in Manitoba**
check-host.net/check-report/20fe362ck85b

Subscribe ➡️ NoName057(16) | DDoSia Project | Reserve | Eng version

🔥 47 👍 17 🤡 5 🤝 2

10.6K 08:25

NoName057(16)

Every decision against Russia is a new minus for Canadian sites. Keep it up, Trudeau!

❌**SaskTel is a Canadian royal telecommunications company**
check-host.net/check-report/20fe37ddkfbb

❌**Authorization on the SaskTel portal**
check-host.net/check-report/20fe3acck5b5

❌**Electronicbox is an Internet service provider for the provinces of Ontario and Quebec**
check-host.net/check-report/20fe4026k282

❌**Authorization on the Electronicbox portal**
check-host.net/check-report/20fe428bkff2

❌**Air Canada Jazz**
check-host.net/check-report/20fe44f6k86c

❌**Air Tindi is a Canadian airline**
check-host.net/check-report/20fe4a8fkd56

Subscribe ➡️ NoName057(16) | DDoSia Project | Reserve | Eng version

⭐ 1 👍 53 🔥 5 🤝 3 🤡 2

10.6K 09:28

NoName057(16) Nov 25

The Australian government has decided to provide Ukraine with 14 military boats worth over $9 million free of charge. As TASS reports, citing Defense Minister Richard Marles, this aid is intended to strengthen maritime security and provide Ukraine with coast guard support.

We looked into Australia to assess their cybersecurity. Result: failure. Rating: unsatisfactory

❌**Australian Centre for International Commercial Arbitration**
check-host.net/check-report/20a59a19kd12

❌**Australian Stainless Steel Development Association**
check-host.net/check-report/20a5a14ck344

❌**IONYX Digital — digital marketing agency**
check-host.net/check-report/20a5a23ck1f0

#OpAu

Subscribe ➡️ NoName057(16) | DDoSia Project | Reserve | Eng version

👍 55 🔥 14 ⚡ 4 ❤️ 3 🤡 3 🤝 3 🤡 1

25.4K edited 08:49

NoName057(16) Nov 27

Australia's cyberspace couldn't handle our visit

❌**Australian Industry and Defence Network (AIDN-NT)**
check-host.net/check-report/20c32d9eka19

❌**Housing Industry Association (HIA)**
check-host.net/check-report/20c345b2kcd6

❌**Northern Territory ICT Industry Association**
check-host.net/check-report/20c330f1kf61

❌**Northern Territory Road Transport Association (NTRTA)**
check-host.net/check-report/20c3316fkff7

❌**Victoria Coroner's Court**
check-host.net/check-report/20c336a0k9e1

❌**BidWrite — tender and proposal management organization**
check-host.net/check-report/20c339d1kc61

❌**Palmerston is a satellite city of Darwin, Australia (dead by ping)**
check-host.net/check-report/20c33d8dk373

❌**Northern Territory is a federal subject of Australia (dead by ping)**
check-host.net/check-report/20c33e15k5ce

❌**Tasmanian Chamber of Commerce and Industry**
check-host.net/check-report/20c34af4kb5a

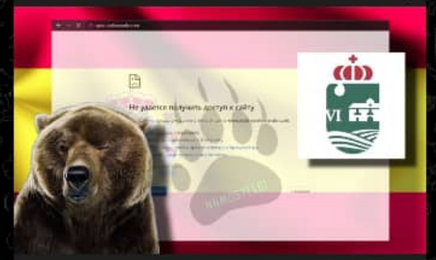
#OpAu

Subscribe ➡️ NoName057(16) | DDoSia Project | Reserve | Eng version

👍 52 🔥 16 🤝 4 🤡 2 ❤️ 1

4495 edited 07:58

NoName057(16) Eng

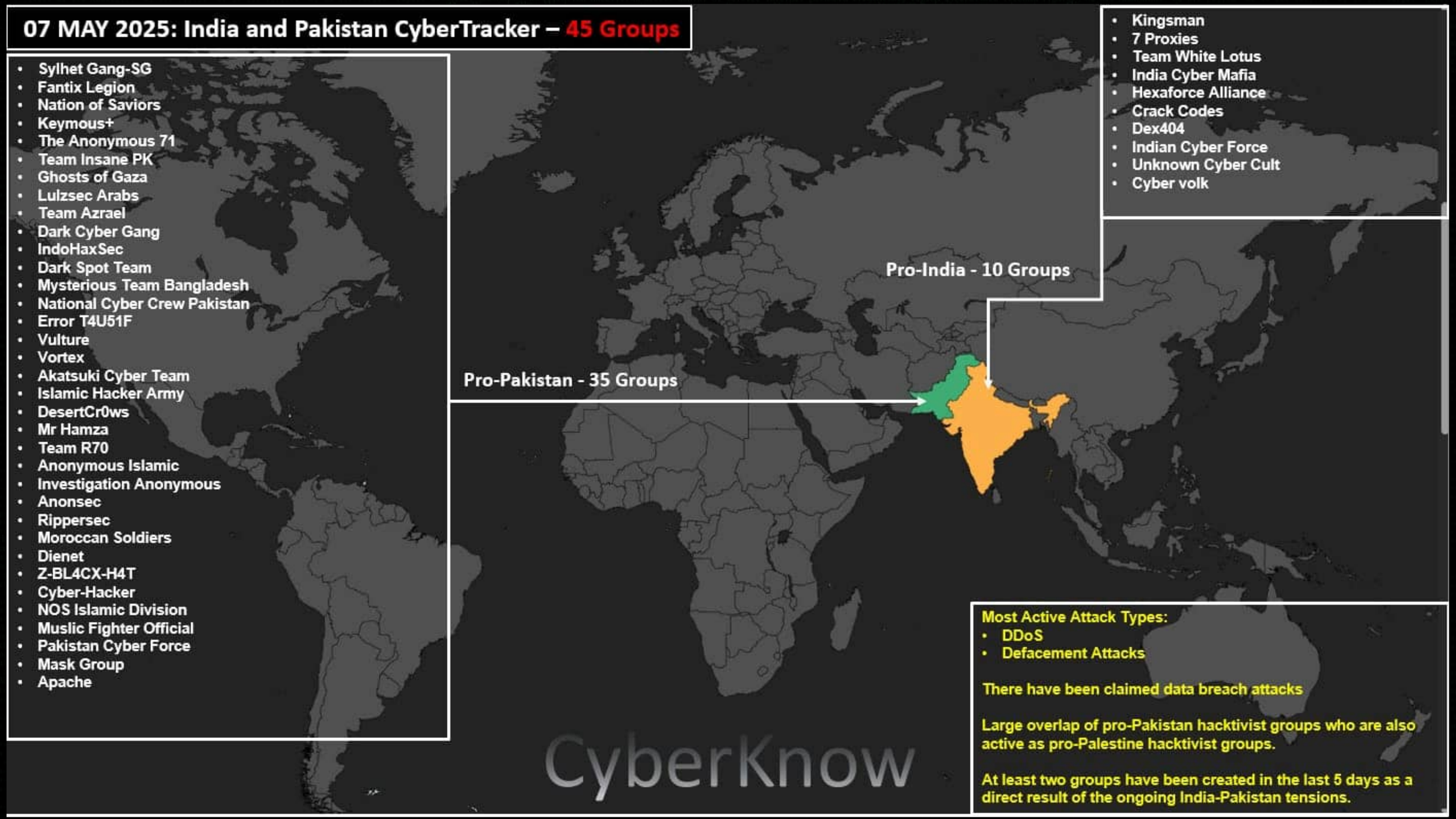


The portal of the city council of the Spanish city of San Fernando de Henares was slammed:

❌https://check-host.net/check-report/10b9f583k766

👉**Subscribe to** NoName057(16)
Join our DDoS-project
⚠️**Subscribe to** reserve channel

07 MAY 2025: India and Pakistan CyberTracker – 45 Groups



- Sylhet Gang-SG
- Fantix Legion
- Nation of Saviors
- Keymous+
- The Anonymous 71
- Team Insane PK
- Ghosts of Gaza
- Lulzsec Arabs
- Team Azrael
- Dark Cyber Gang
- IndoHaxSec
- Dark Spot Team
- Mysterious Team Bangladesh
- National Cyber Crew Pakistan
- Error T4U51F
- Vulture
- Vortex
- Akatsuki Cyber Team
- Islamic Hacker Army
- DesertCr0ws
- Mr Hamza
- Team R70
- Anonymous Islamic
- Investigation Anonymous
- Anonsec
- Rippersec
- Moroccan Soldiers
- Dienet
- Z-BL4CX-H4T
- Cyber-Hacker
- NOS Islamic Division
- Muslic Fighter Official
- Pakistan Cyber Force
- Mask Group
- Apache

- Kingsman
- 7 Proxies
- Team White Lotus
- India Cyber Mafia
- Hexaforce Alliance
- Crack Codes
- Dex404
- Indian Cyber Force
- Unknown Cyber Cult
- Cyber volk

Most Active Attack Types:
- DDoS
- Defacement Attacks

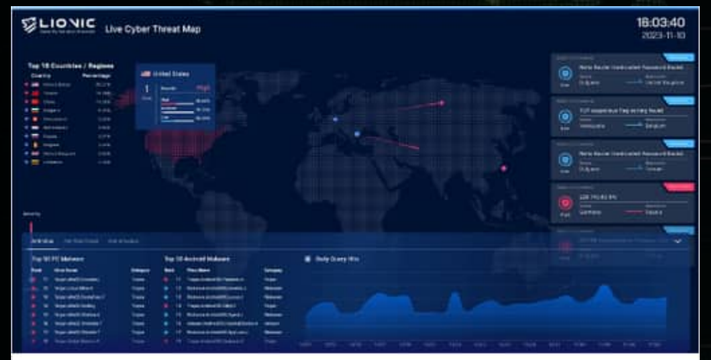
There have been claimed data breach attacks

Large overlap of pro-Pakistan hacktivist groups who are also active as pro-Palestine hacktivist groups.

At least two groups have been created in the last 5 days as a direct result of the ongoing India-Pakistan tensions.

Ciberguerra

El mundo bajo ataque



Cyber Threat Map

The Superior Network Security Solution Provider. We aim to purify and secure your network environment.

lionic.com

Kaspersky Cyberthreat live map

Find out if you're under cyber-attack here #CyberSecurityMap #CyberSecurity

MAP

Outbreak Threat Map

FortiGuard Labs

radware

Live Cyber Threat Map

Radware's Live Threat Map presents near real-time information about cyberattacks as they occur, based on our global threat deception network and cloud systems event information.

Radware

https://securitycenter.sonicwall.com/m/page/worldwide-attacks

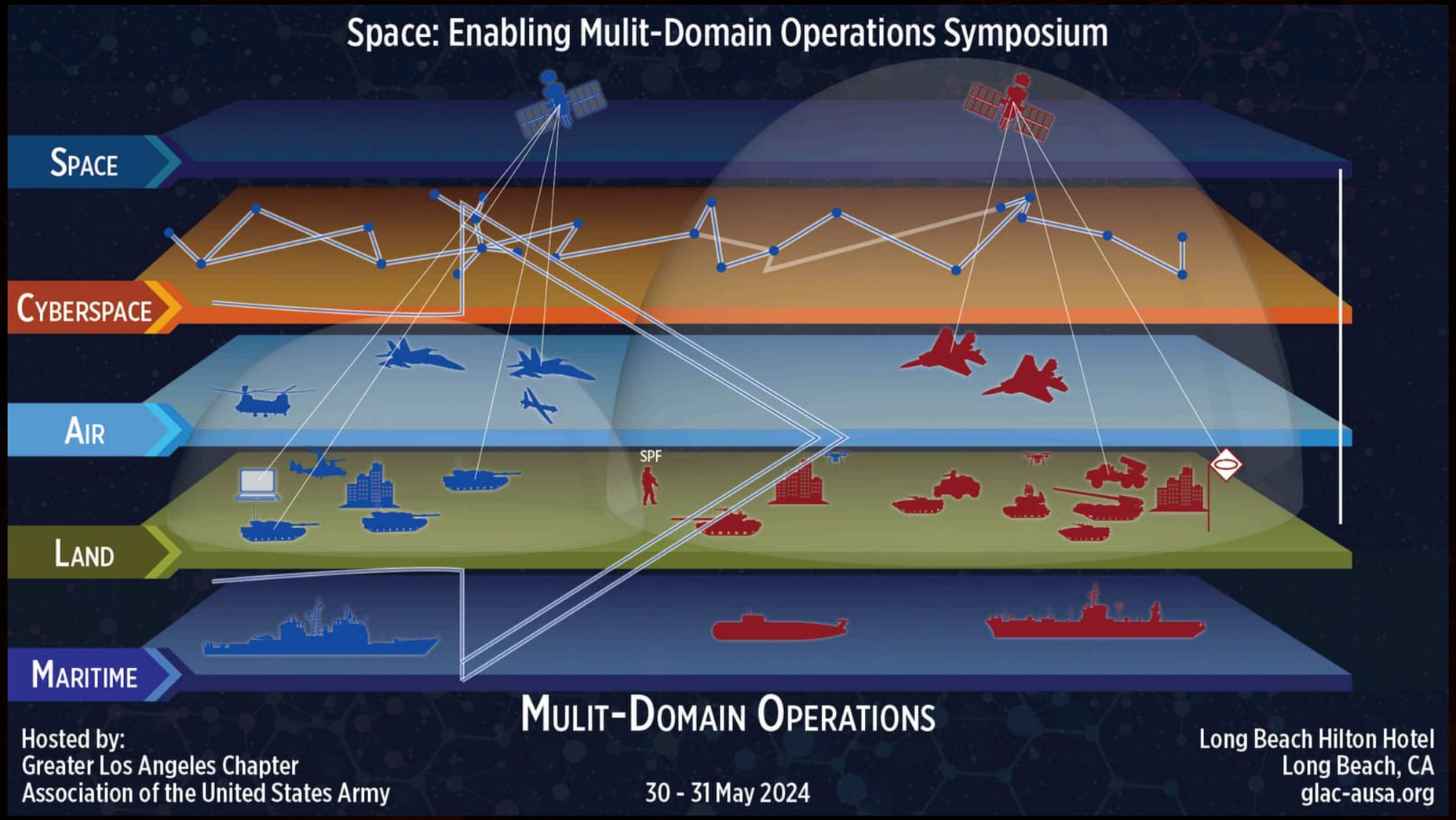
Ponente: David Ramos
https://www.linkedin.com/in/david-ramos-rodriguez/

¿Ciberguerra?

- Conflictos digitales entre Estados
- Buscan dañar infraestructuras o robar inteligencia
- Se libra en el ciberespacio

Ponente: David Ramos
https://www.linkedin.com/in/david-ramos-rodriguez/

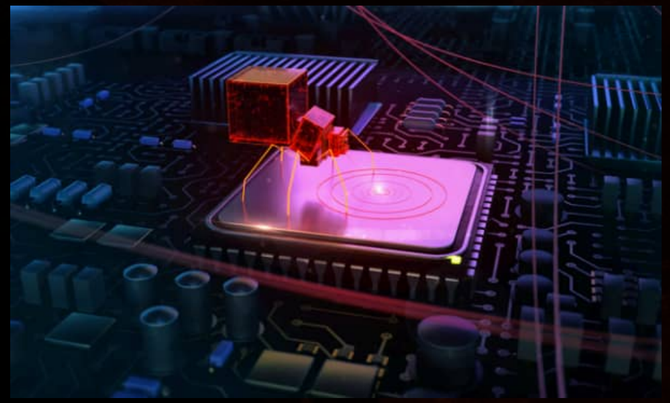
5 dimensiones en la guerra



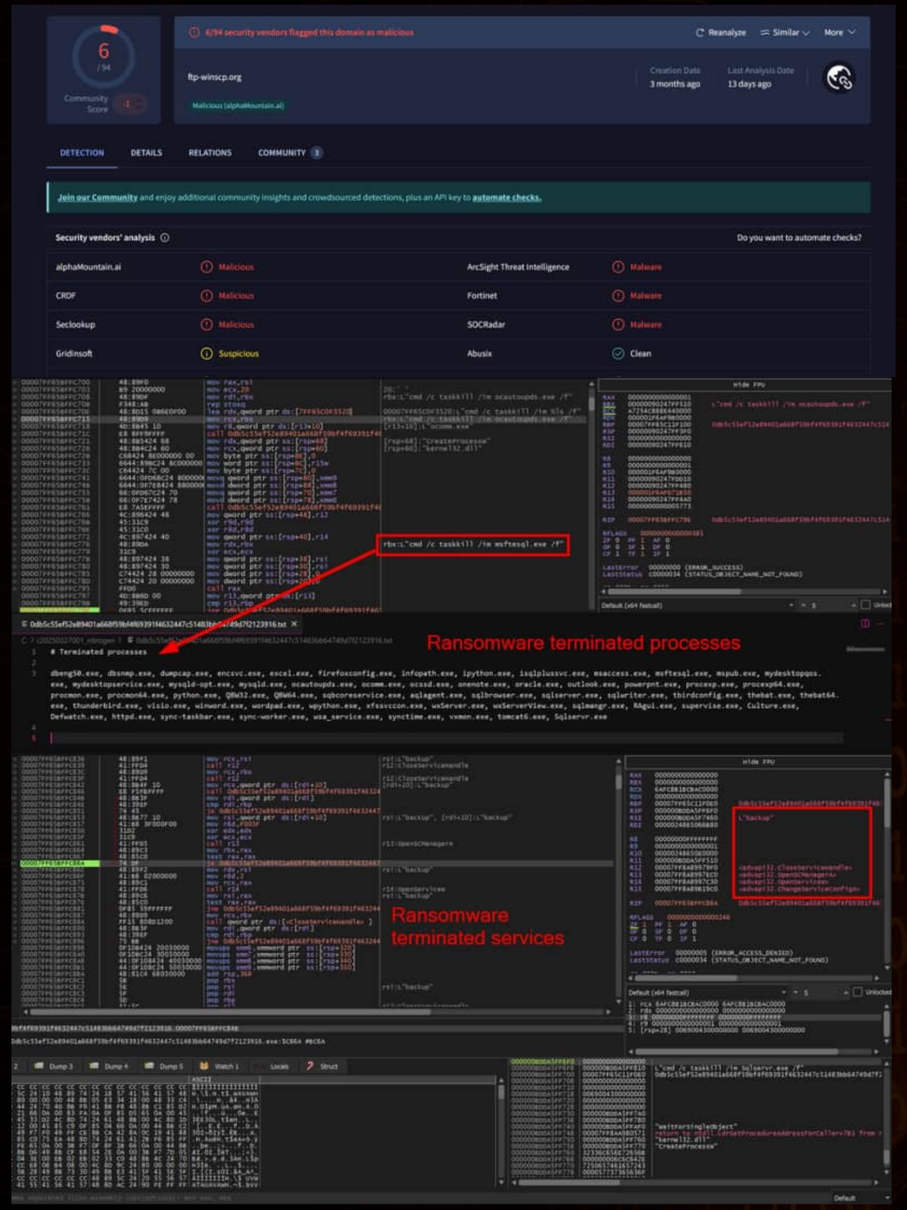
Ponente: David Ramos
https://www.linkedin.com/in/david-ramos-rodriguez/

Tácticas en una ciberguerra

- La infiltración en redes enemigas.
- La recopilación de datos.
- La interferencia de señales inalámbricas.
- Los programas informáticos falsificados y contaminados.
- Los ataques a sistemas enemigos a través de malware.



Ponente: David Ramos
https://www.linkedin.com/in/david-ramos-rodriguez/



urlscan.io Home Search Live API Blog Docs Pricing Login

www.youtube.com

2607:f8b0:4006:806::200e Public Scan

Lookup Go To Rescan

Add Verdict Report

Submitted URL: http://ftp-winscp.org/

Effective URL: https://www.youtube.com/watch?v=dQw4w9WgXcQ

Submission: On February 27 via manual (February 27th 2025, 3:01:46 am UTC) from IN — Scanned from US

Summary | HTTP 211 | Redirects | Links 2 | Behaviour | Indicators | Similar | DOM | Content | API | Verdicts

Summary

This website contacted **20 IPs** in **2 countries** across **9 domains** to perform **211 HTTP transactions**. The main IP is 2607:f8b0:4006:806::200e, located in **United States** and belongs to GOOGLE, US. The main domain is www.youtube.com. The Cisco Umbrella rank of the primary domain is **83**.
TLS certificate: Issued by *WR2* on February 3rd 2025. Valid for: 3 months.

www.youtube.com scanned **10000+ times** on urlscan.io — Show Scans 10000+

urlscan.io Verdict: No classification

Live information

Google Safe Browsing: No classification for *www.youtube.com*
Current DNS A record: 216.58.206.46 (AS15169 - GOOGLE, US)
Domain created: February 15th 2005, 05:13:12 (UTC)
Domain registrar: MarkMonitor, Inc.

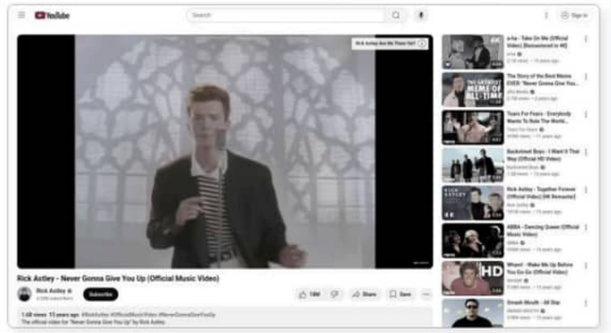
Domain & IP information

IP/ASNs | IP Detail | Domains | Domain Tree | Links | Certs | Frames

	IP Address	AS Autonomous System
1 → 1	23.227.196.13	29802 (HVC-AS)
17	2607:f8b0:4006:806::200e	15169 (GOOGLE)
7	2607:f8b0:4006:821::2016	15169 (GOOGLE)
3	2607:f8b0:4006:809::200a	15169 (GOOGLE)

Screenshot

Live screenshot | Full Image



Page Title

Rick Astley - Never Gonna Give You Up (Official Music Video) - YouTube

Page URL History

Show full URLs

1. http://ftp-winscp.org/ HTTP 307
   https://ftp-winscp.org/ HTTP 302
   https://www.youtube.com/watch?v=dQw4w9WgXcQ Page URL

Page Statistics

211	98 %	45 %	9	18
Requests	HTTPS	IPv6	Domains	Subdomains

20534

Ransomware is predicted to cost the world $57 billion USD annually in 2025

Amenazas

- Espionaje
- Sabotaje
- Propaganda
- Interrupción económica

Ponente: David Ramos
https://www.linkedin.com/in/david-ramos-rodriguez/

APT: los ejércitos invisibles

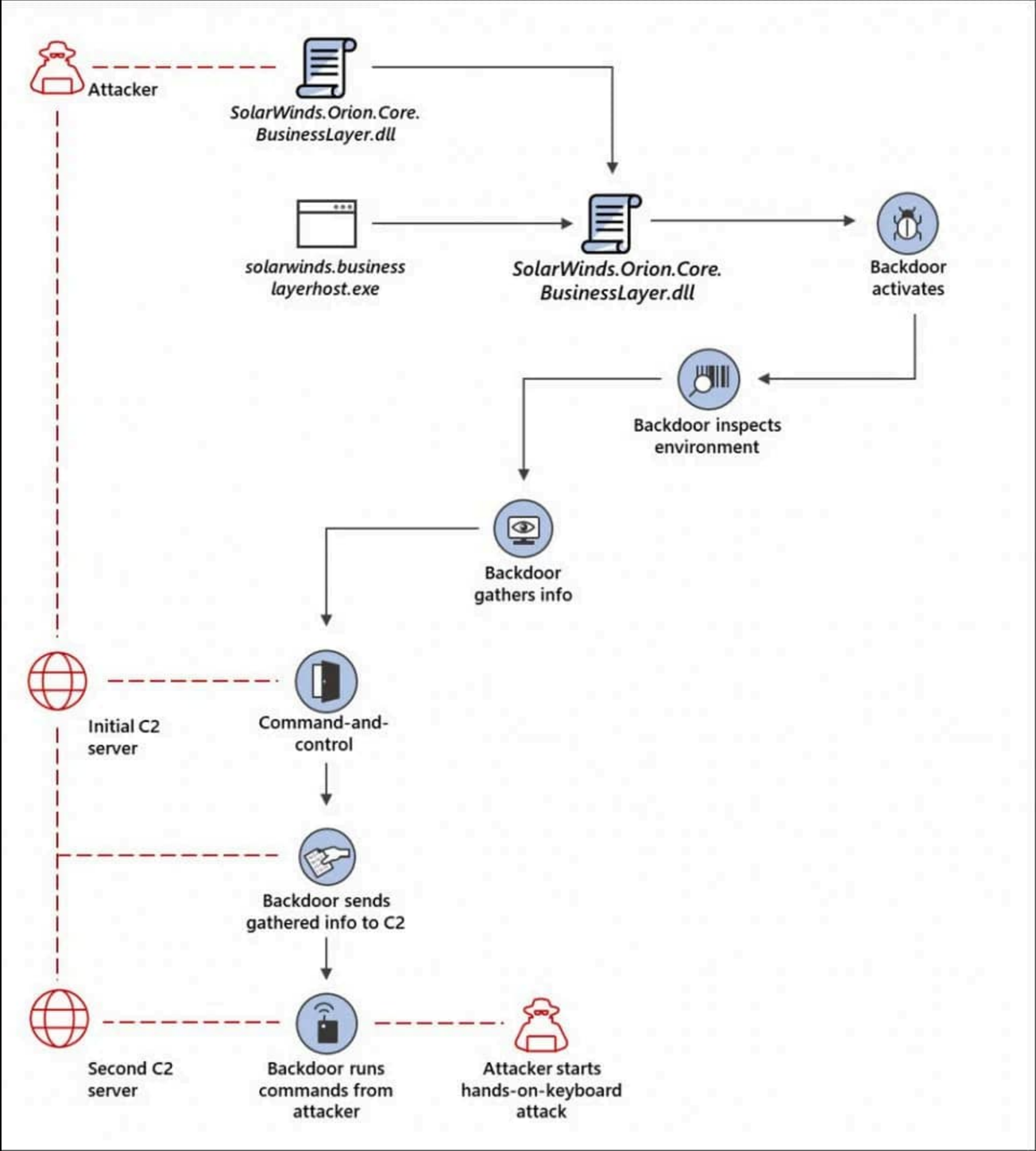
País	APT emblemático
Rusia	Sandworm / APT28
China	APT41
EE. UU.	Equation Group
Irán	Charming Kitten
Corea N.	Lazarus

Ponente: David Ramos
https://www.linkedin.com/in/david-ramos-rodriguez/

Casos - Espionajes

SolarWinds / SunBurst (Rusia-SVR, 2020)

Se infiltró la actualización de un software de gestión usado por 18 000 clientes, incluidas agencias de EE. UU.; los atacantes permanecieron meses copiando correos y documentos confidenciales.

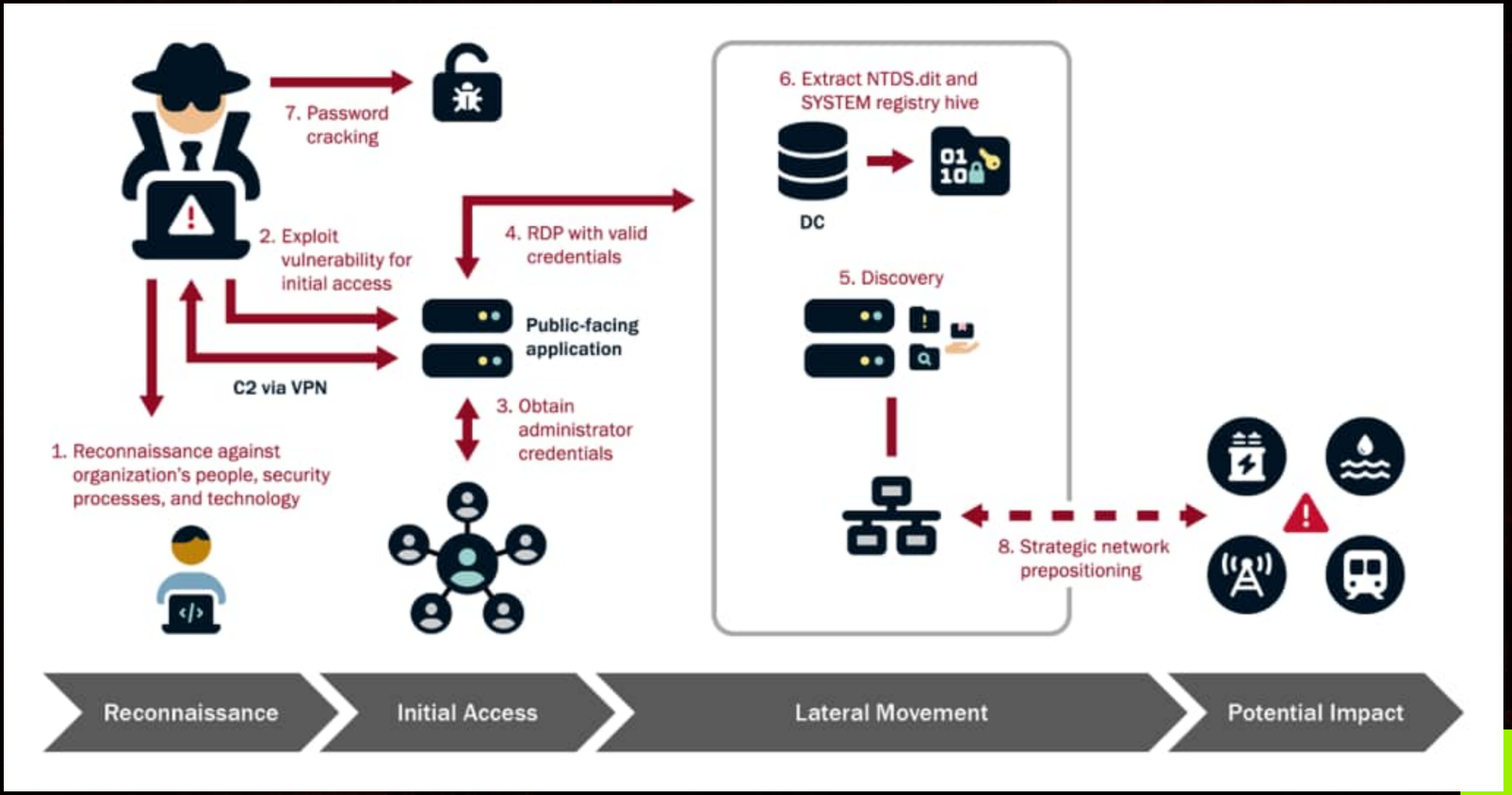


Ponente: David Ramos
https://www.linkedin.com/in/david-ramos-rodriguez/

Casos - Espionajes

Volt Typhoon (China, 2023-24)

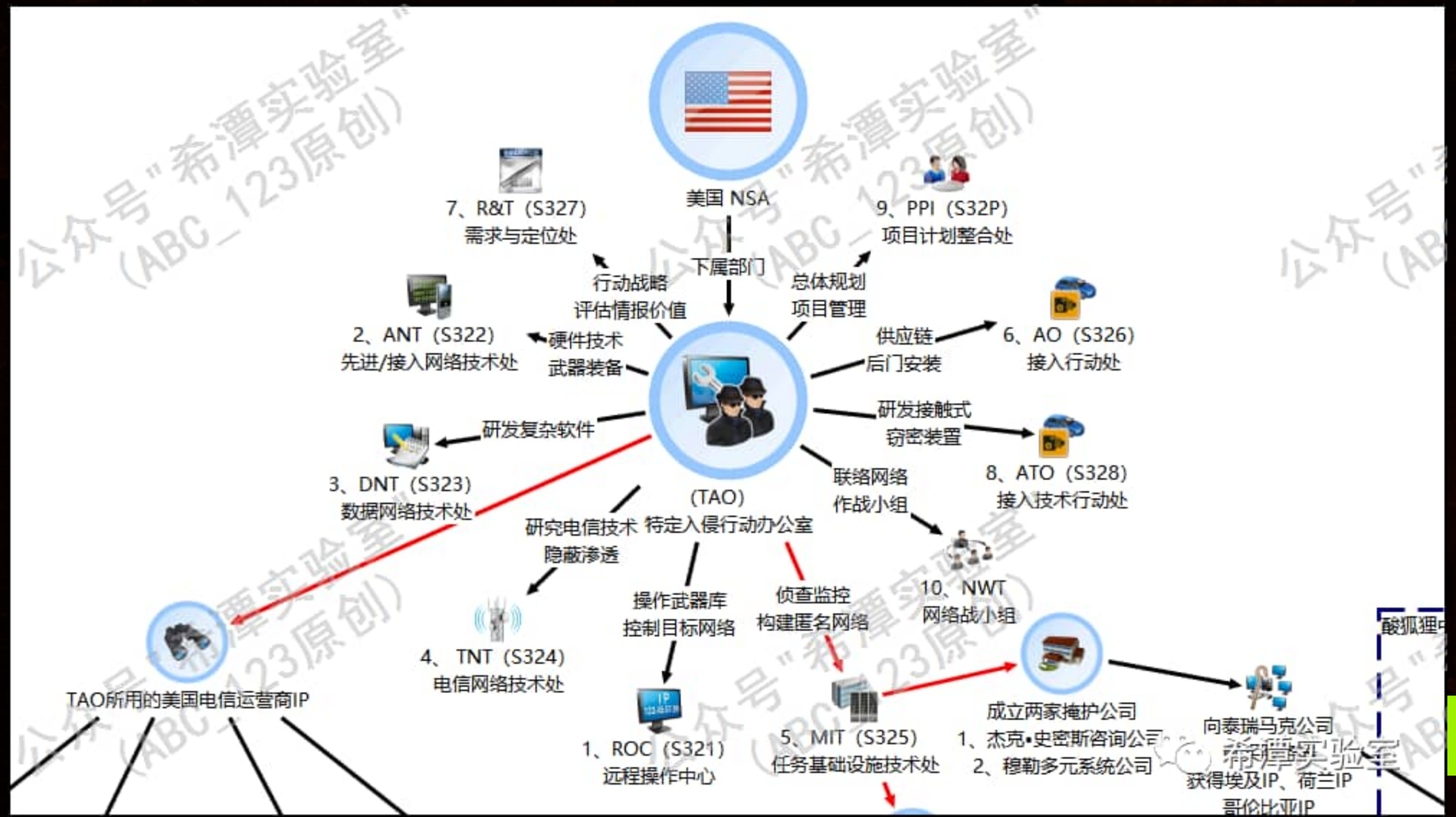
Piratas patrocinados por Pekín se “instalaron” en redes de energía, agua y transporte de EE. UU. y Guam; su objetivo no era espiar datos, sino pre-posicionarse para desconectar infraestructuras en una futura crisis.



Casos - Espionajes

Equation Group / APT-C-40 (EE. UU., revelado 2025)

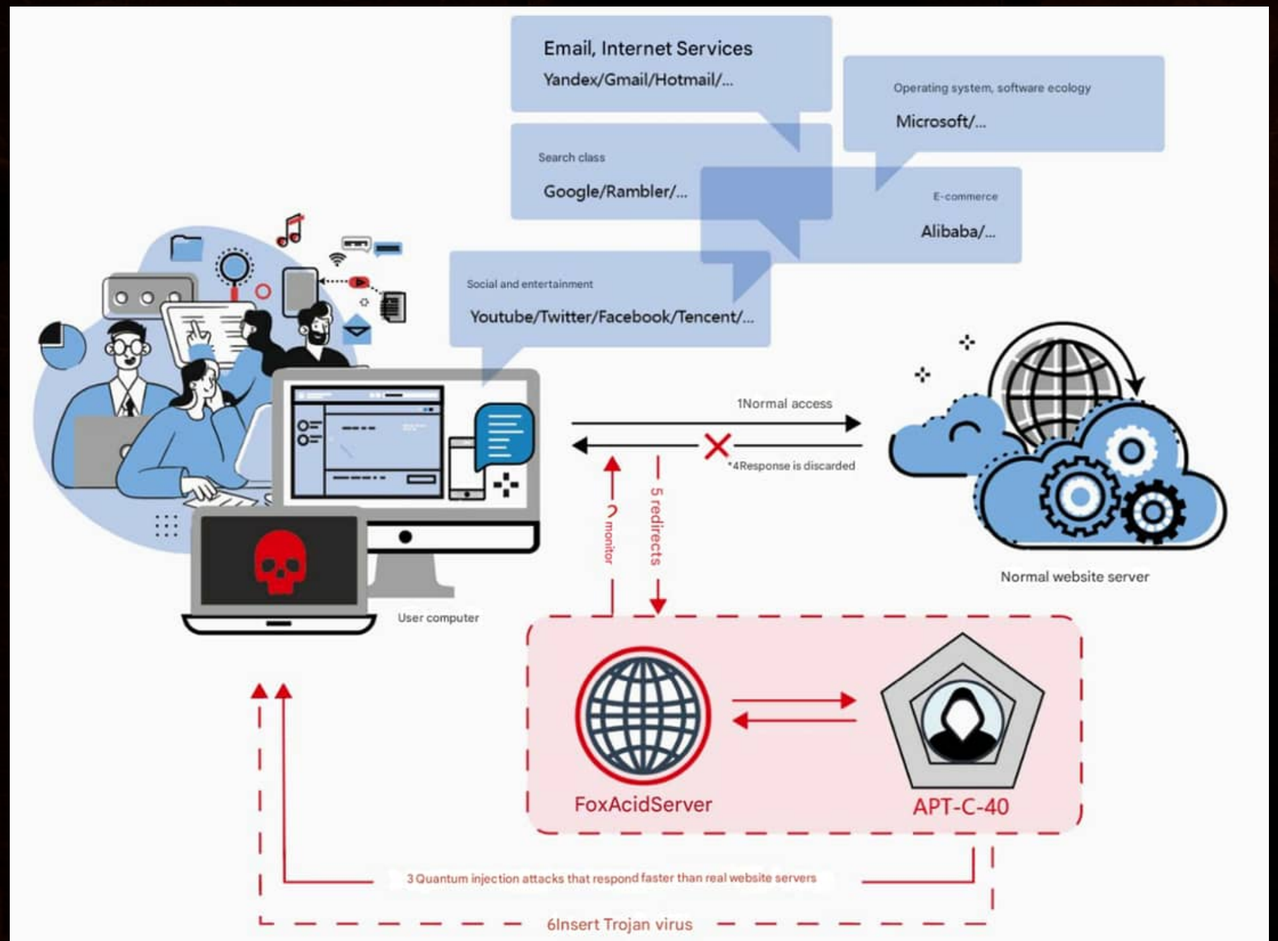
Un informe chino documenta 40+ herramientas de la NSA usadas en universidades e I+D aeroespacial; confirma que todas las potencias mayores emplean operaciones de acceso encubierto a largo plazo.



Casos - Espionajes

Equation Group / APT-C-40 (EE. UU., revelado 2025)

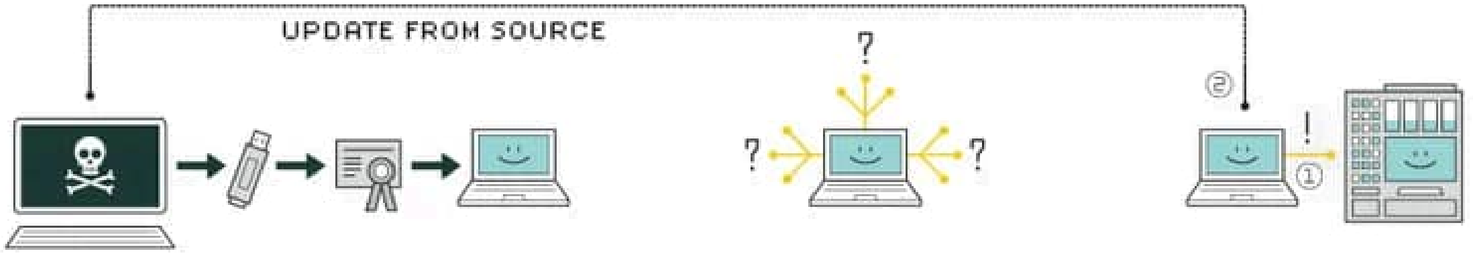
Un informe chino documenta 40+ herramientas de la NSA usadas en universidades e I+D aeroespacial; confirma que todas las potencias mayores emplean operaciones de acceso encubierto a largo plazo.



Sabotaje Stuxnet

(EE. UU.+Israel, 2010)

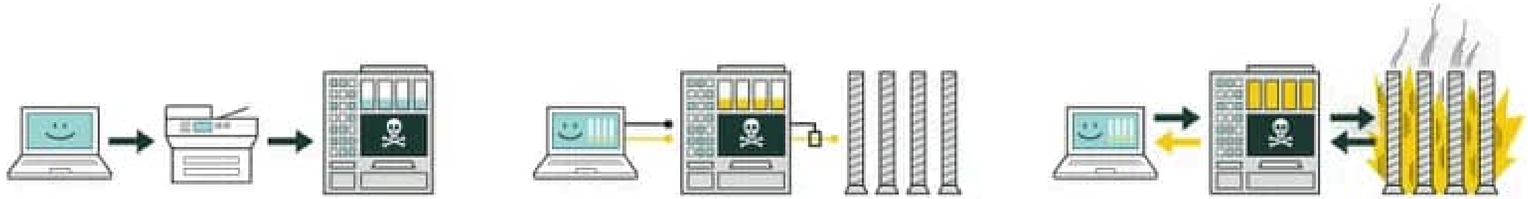
HOW STUXNET WORKED



1. infection
Stuxnet enters a system via a USB stick and proceeds to infect all machines running Microsoft Windows. By brandishing a digital certificate that seems to show that it comes from a reliable company, the worm is able to evade automated-detection systems.

2. search
Stuxnet then checks whether a given machine is part of the targeted industrial control system made by Siemens. Such systems are deployed in Iran to run high-speed centrifuges that help to enrich nuclear fuel.

3. update
If the system isn't a target, Stuxnet does nothing; if it is, the worm attempts to access the Internet and download a more recent version of itself.



4. compromise
The worm then compromises the target system's logic controllers, exploiting "zero day" vulnerabilities-software weaknesses that haven't been identified by security experts.

5. control
In the beginning, Stuxnet spies on the operations of the targeted system. Then it uses the information it has gathered to take control of the centrifuges, making them spin themselves to failure.

6. deceive and destroy
Meanwhile, it provides false feedback to outside controllers, ensuring that they won't know what's going wrong until it's too late to do anything about it.

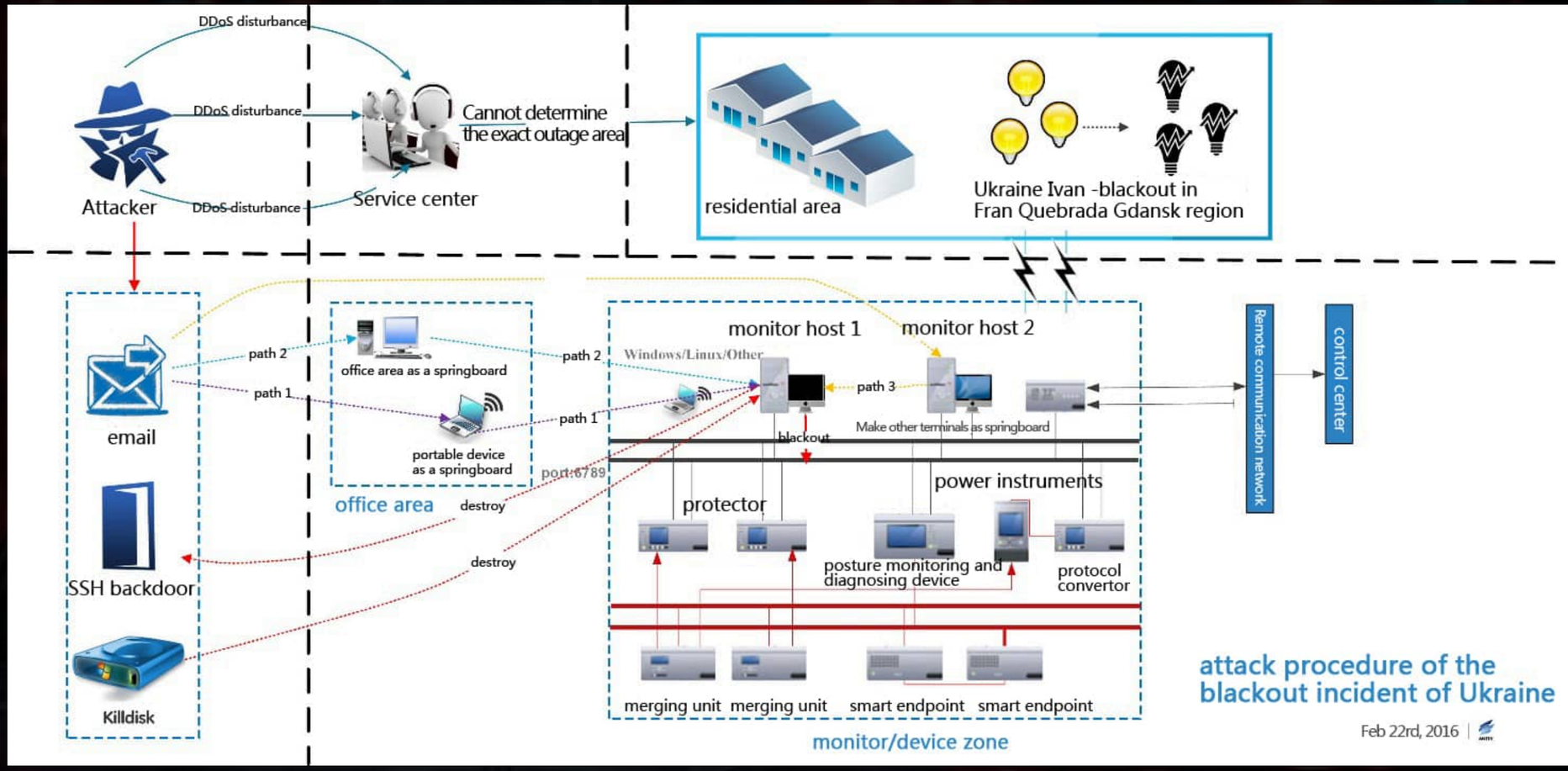
IEEE Spectrum

Ponente: David Ramos
https://www.linkedin.com/in/david-ramos-rodriguez/

Apagón de Ucrania

(Sandworm, Rusia)

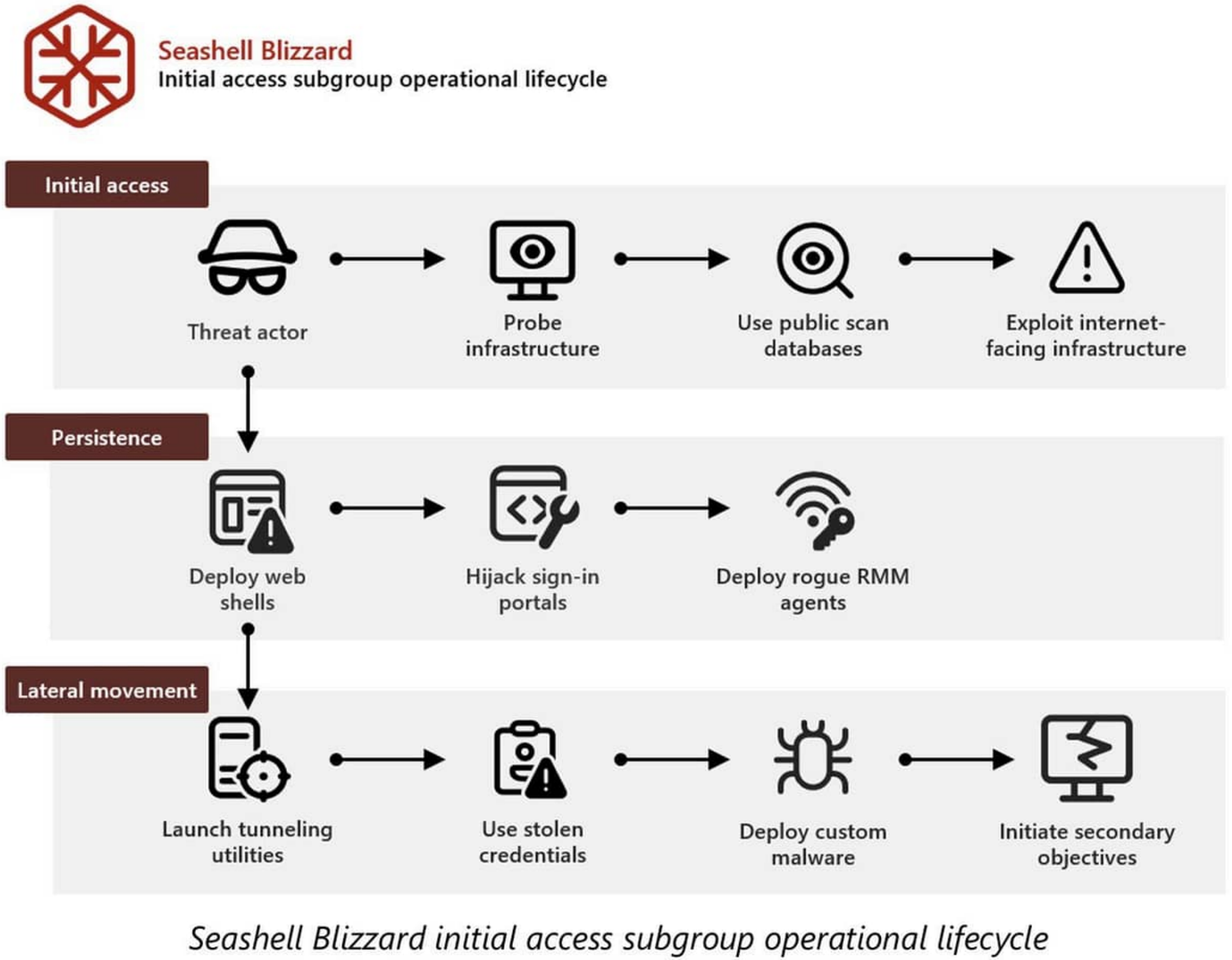
Apagaron 30 subestaciones; 230 000 hogares sin luz 1-6 h



Hack a satélite Viasat / AcidRain (feb-2022): Borrado masivo de módems KA-SAT minutos antes de la invasión a Ucrania; cortó comunicaciones militares y afectó turbinas eólicas en Alemania.

BadPilot

(Sandworm, 2025) Acceso oculto en redes de energía, defensa y transporte de EE. UU./UE; preparado para sabotaje remoto.



Seashell Blizzard initial access subgroup operational lifecycle

Operación Baltic Sentry 2025

La OTAN desplegó la misión Baltic Sentry para proteger cables submarinos tras incidentes de sabotaje en 2024; Bruselas y Washington coordinan ejercicios ‘Locked Shields’ con empresas privadas para blindar redes eléctricas y 5G

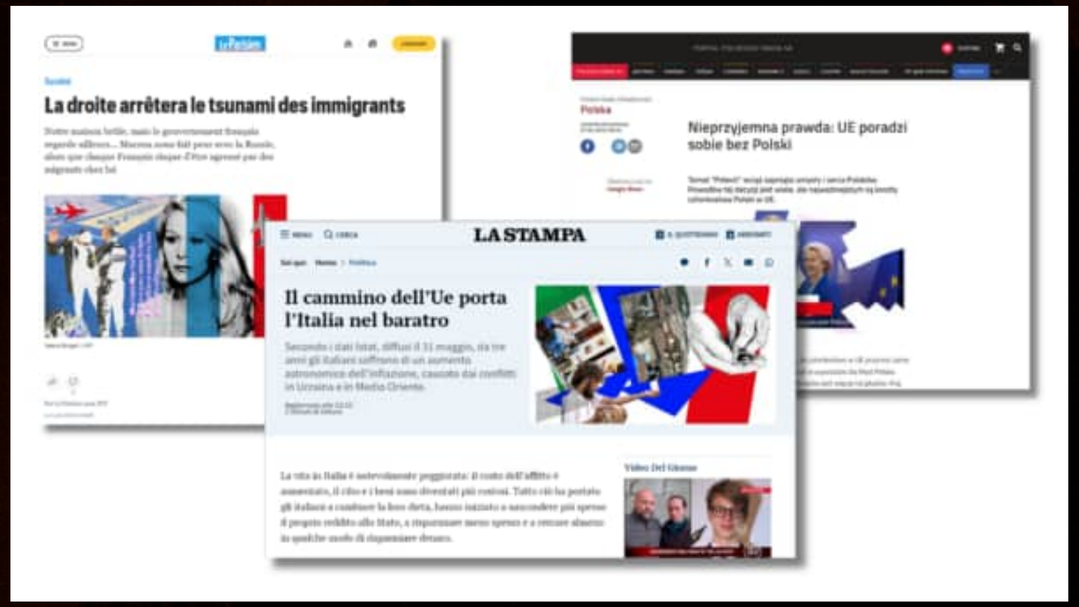
Propaganda

Interferencia rusa en elecciones EE. UU. 2016

La IRA difundió millones de posts falsos y anuncios segmentados; Senado y Mueller detallan la operación.

Campaña Doppelganger – elecciones UE 2024

Réplicas de webs de prensa y deepfakes mancharon la imagen de candidatos; Voice of Europe canalizaba fondos prorrusos.



Ponente: David Ramos
https://www.linkedin.com/in/david-ramos-rodriguez/

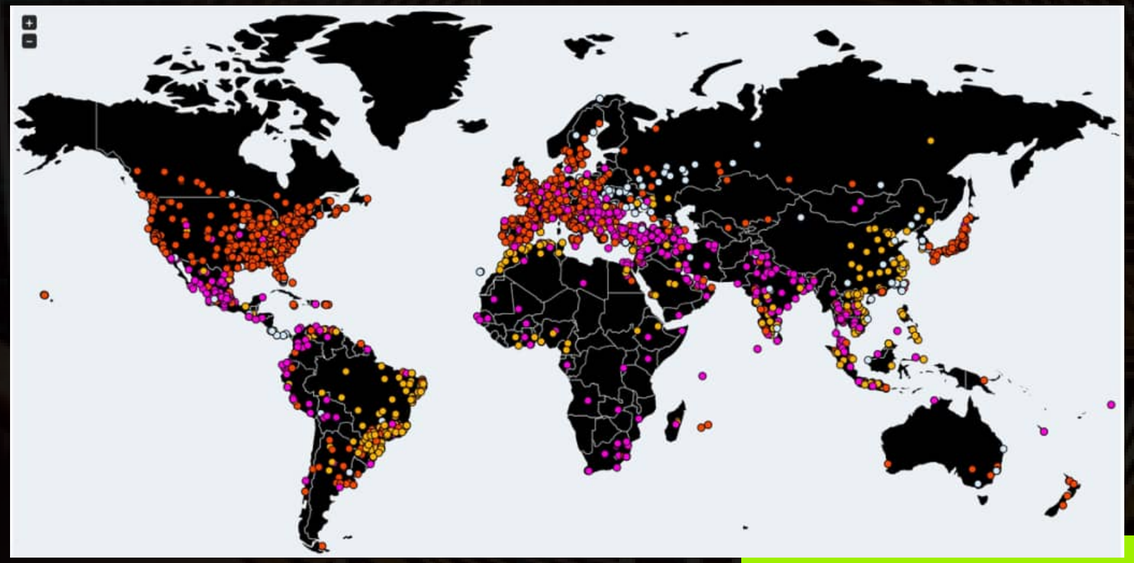
Interrupción económica

Robos de criptomonedas Lazarus (Corea N., 2023-24)

Mayor robo de criptomonedas registrado hasta la fecha, sustrayendo aproximadamente US $1.5 mil millones en Ethereum del exchange Bybit, con sede en Dubái

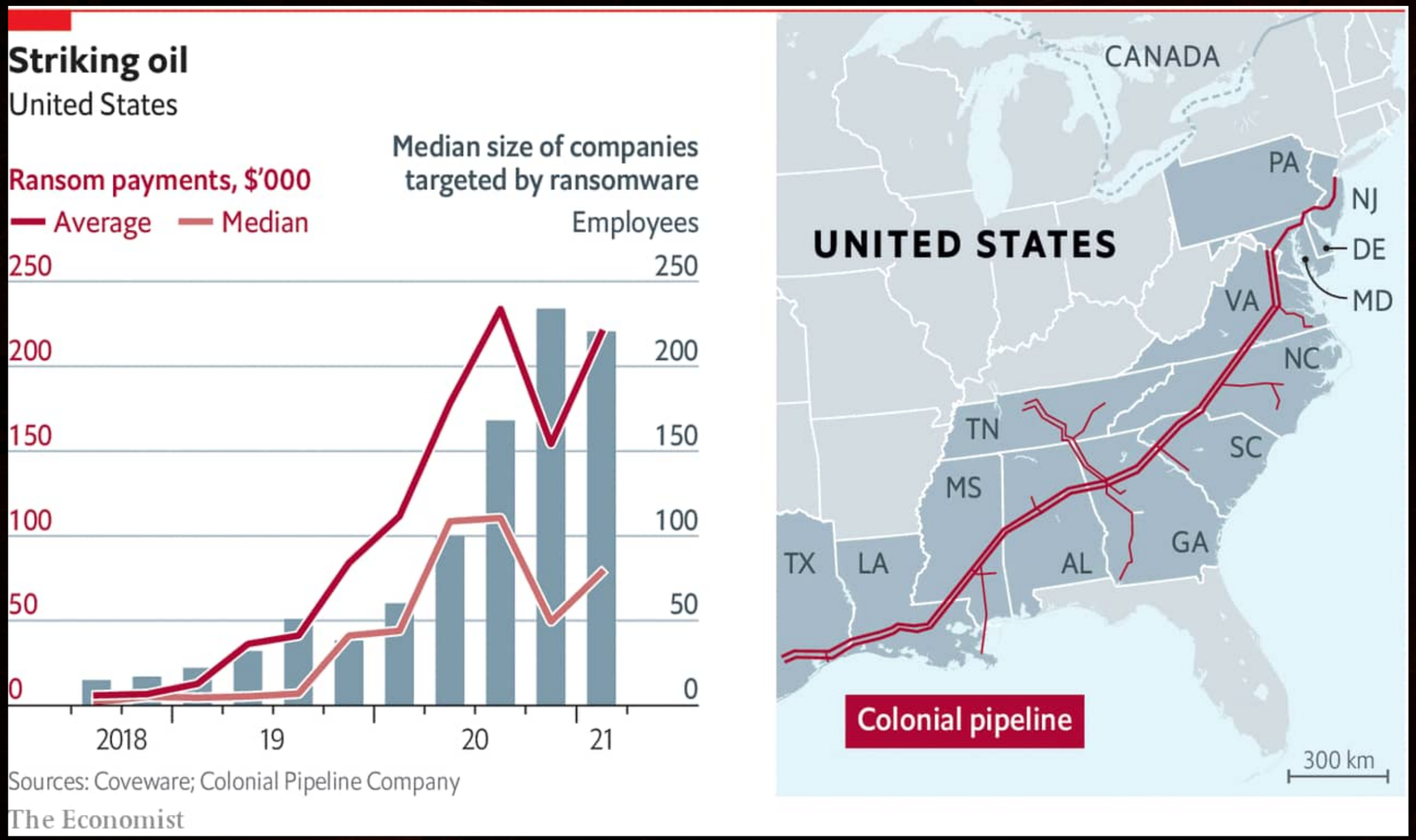
WannaCry (mayo de 2017)

Ataque global de ransomware. Utilizó el exploit EternalBlue, una herramienta de la NSA filtrada por el grupo Shadow Brokers. Infectando en pocas horas más de 300 000 dispositivos en 150 países.



Ponente: David Ramos
https://www.linkedin.com/in/david-ramos-rodriguez/

Colonial Pipeline ransomware attack




Q&A

Muchas Gracias

Datos de contacto:

contact.pastime903@passmail.net

in/david-ramos-rodriguez/