



CIBERINTELIGENCIA, INCIDENTES Y LAS NUEVAS CIBERAMENAZAS



TCOL Francisco MARIN
Mando Conjunto del Ciberespacio (MCCE)
28OCT25



INDICE

- GENERALIDADES
- INTELIGENCIA Y AMBITO CIBERESPACIAL
- AGENTES DE LA AMENAZA



La ciberseguridad se encuentra ahora en la encrucijada entre la seguridad nacional, la innovación tecnológica y la cooperación internacional.

Annual Meeting Global Future Councils and Cybersecurity 2025
World Economic Forum

Particularidades ciberoperaciones

Planeamiento y ejecución difieren respecto a otras en cuanto a los tiempos requeridos

Necesario ejecutar acciones precursoras con antelación.

Proceso de autorización más complejo

Características propias:

- Naturaleza
- Alcance
- Asimetría
- Anonimato

Todo lo anterior implica...

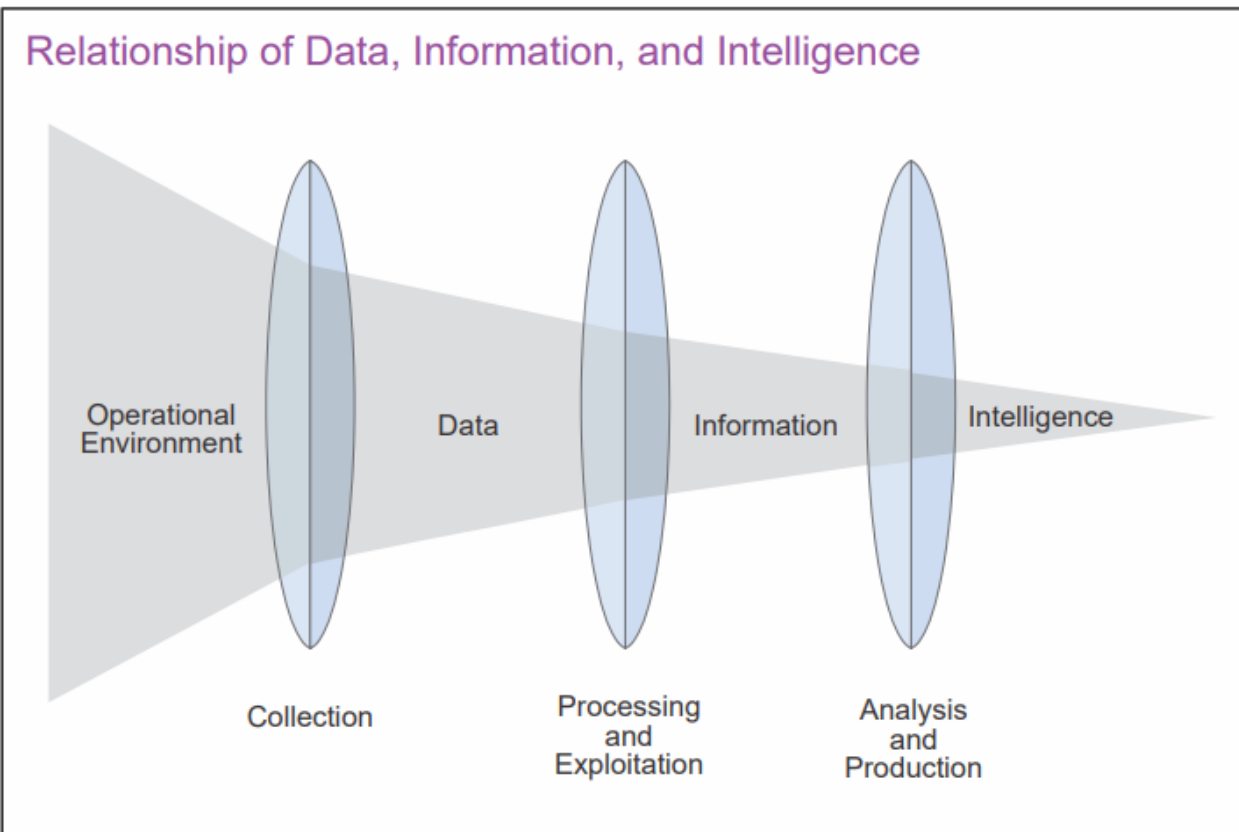
... necesidades particulares de Inteligencia



Capa humana

Capa Lógica

Capa Física



U.S. Joint Chiefs of Staff, Joint Publication 2.0, Joint Intelligence

Generalidades Inteligencia

Datos, Información y, finalmente, Inteligencia

Ciclo de Inteligencia

Niveles

- Estratégico
- Operacional
- Táctico

Inteligencia en o a través del ciberespacio

Ciberinteligencia

NIVELES DE LA CIBERINTELIGENCIA

ESTRATEGICO

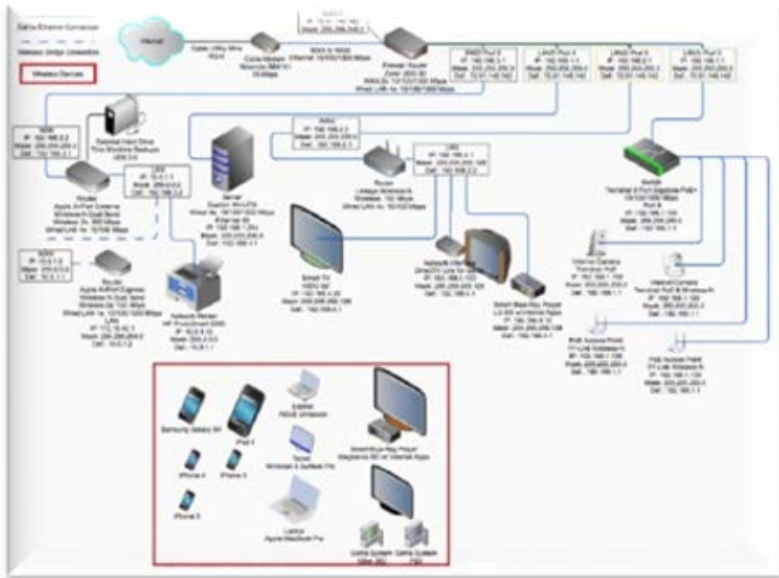
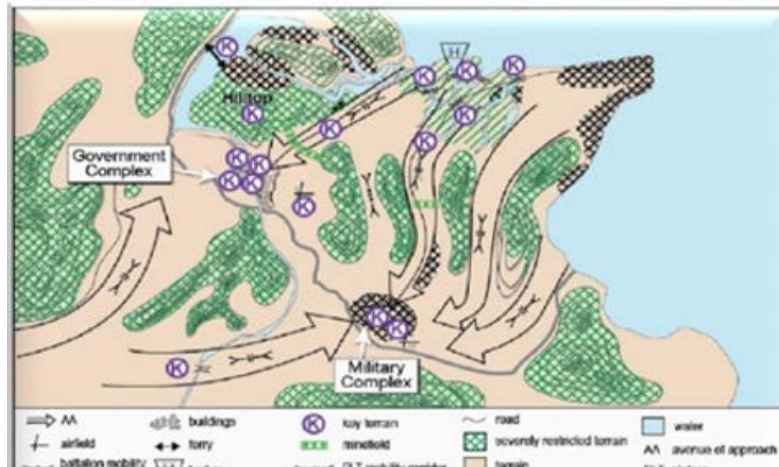
Ofrece una visión amplia, diseñada para informar las decisiones de los dirigentes sobre los riesgos que plantean para su organización las amenazas cibernéticas o físicas.

OPERACIONAL

Más detallada que la anterior, proporciona el «quién, qué, por qué, cuándo y cómo» de las amenazas que afectan a la organización.

TACTICO

Suele consumirse de forma automática, comprende indicadores utilizados para bloquear las comunicaciones sospechosas de ser maliciosas.



MISIONES DE LA CIBERINTELIGENCIA MILITAR

Contribuir al Planeamiento Conjunto

Preparación de Inteligencia del Entorno Operativo aplicada al ciberespacio

Contribuir Cyber Situational Awareness

Definir el sistema de indicadores y alertas en el dominio del ciberespacio



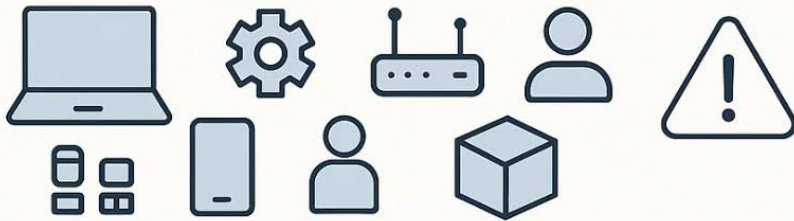
FUENTES DE CIBERINTELIGENCIA

- Análisis de los registros de su propia infraestructura
- Informes del equipo de respuesta a emergencias informáticas (CERT)
- Fuentes abiertas
- *Dark web*
- Informes de amenazas servicios de suscripción comerciales
- Acuerdos de intercambio de información
- Otras disciplinas de inteligencia tradicional

Deben proporcionar datos relevantes de las amenazas específicas para nuestra organización

Proporciona el conocimiento de las brechas y debilidades que un atacante podría explotar (superficie de ataque)

CYBERSECURITY ASSET MANAGEMENT ISSUES



UNKNOWN ASSETS

Risk due to lack of visibility

UNMANAGED ASSETS

Threat due to lack of control

Superficie de ataque

Incremento en los riesgos y exposición a un ritmo nunca visto debido al uso de:

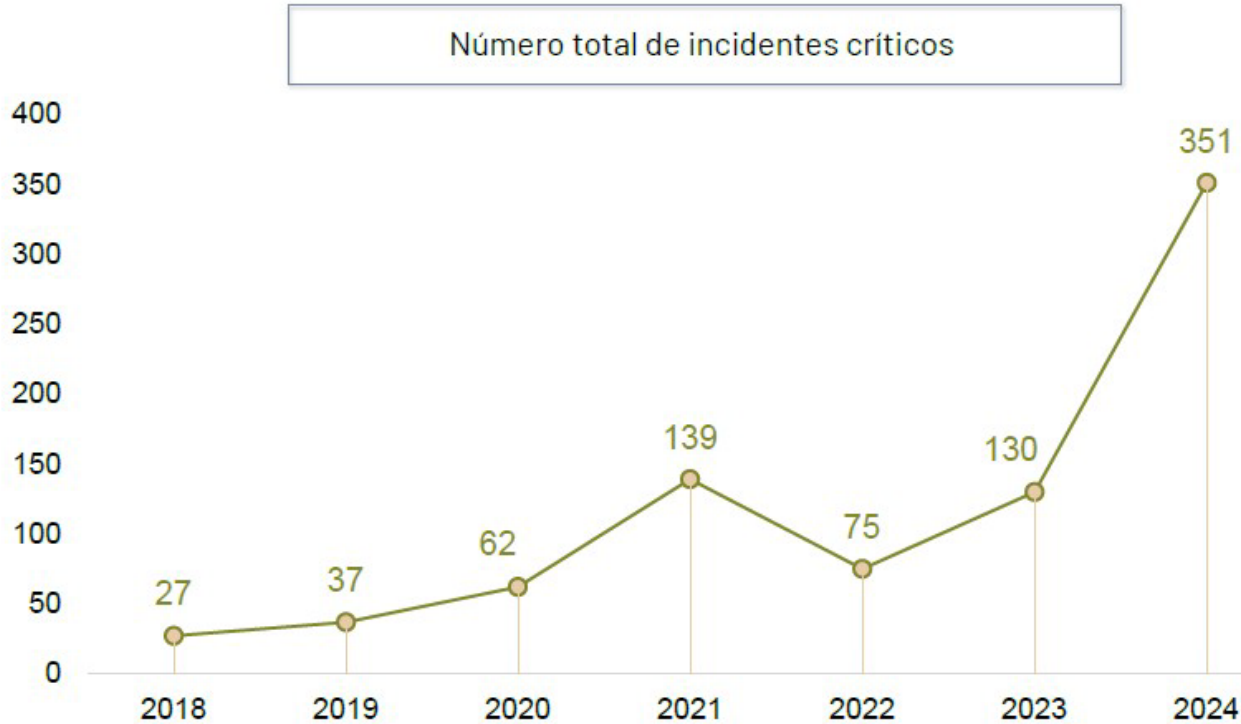
- Servicios basados en la nube
- Sistemas telefonía móvil
- Dispositivos IoT
- Sistemas privados no gestionados (Teletrabajo y "Shadow IT")
- Sistemas conectados desconocidos

La identidad, nuevo perímetro a defender

Ciberincidentes

Evento o conjunto de eventos en el ámbito del ciberespacio que tienen o podrían tener un efecto adverso sobre :

- la disponibilidad, confidencialidad, integridad de la información
- o sobre el funcionamiento del sistema CIS



*Número total de incidentes críticos en el sector público
(Informe Anual CCN-CERT)*

Una de las principales cuestiones es saber quien está detrás de un ciberincidente: la autoría o **atribución**

El problema de la atribución

Las amenazas cibernéticas tradicionales dejan huellas identificables utilizables para la atribución

Los actores del ciberespionaje adoptan técnicas más sofisticadas para cubrir sus huellas

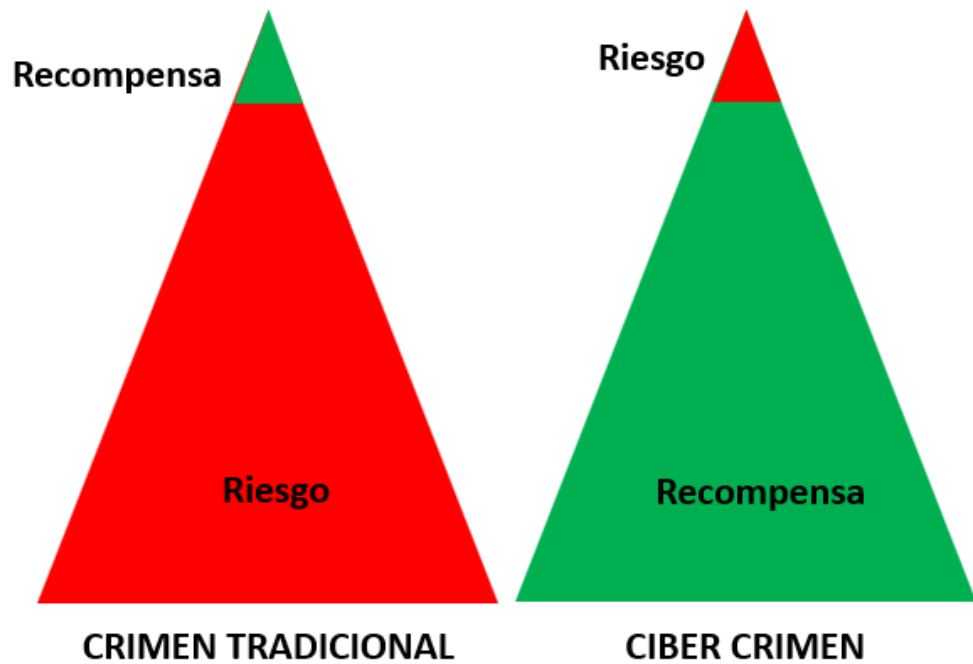
- uso de infraestructuras de terceros comprometidas
- lanzamiento de ataques a través de redes anónimas

Dificulta a expertos y gobiernos rastrear el origen del ataque: importante reto para identificar y responder a incidentes de ciberespionaje, especialmente en el contexto de los marcos jurídicos transfronterizos y la cooperación internacional.

El complejo panorama de agentes de la amenaza permite la utilización de nuevos actores a modo de *proxies*.

AGENTES DE LA AMENAZA

- Ciberdelincuencia
- Hacktivismo
- Actores estatales
- Actores internos
- Nuevos actores (“Posibilitadores”)



Ciberdelincuencia

Uno de los actores más habituales y dinámicos

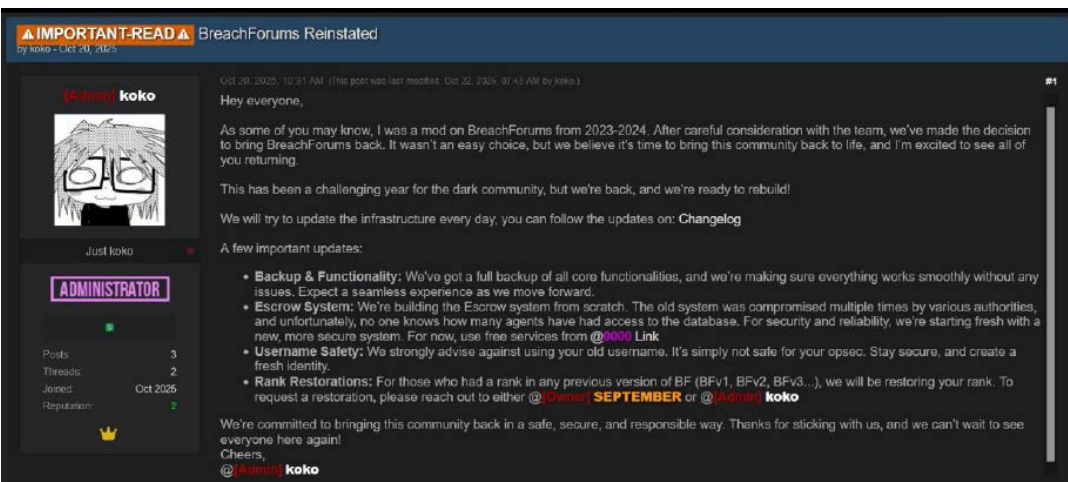
Adaptabilidad a nuevas tecnologías y cambios sociales.

Mejora constante de su cooperación y especialización

Servicios relacionados con el cibercrimen ampliamente disponibles en Internet.

Los proveedores de servicios ilícitos ofrecen diferentes servicios.

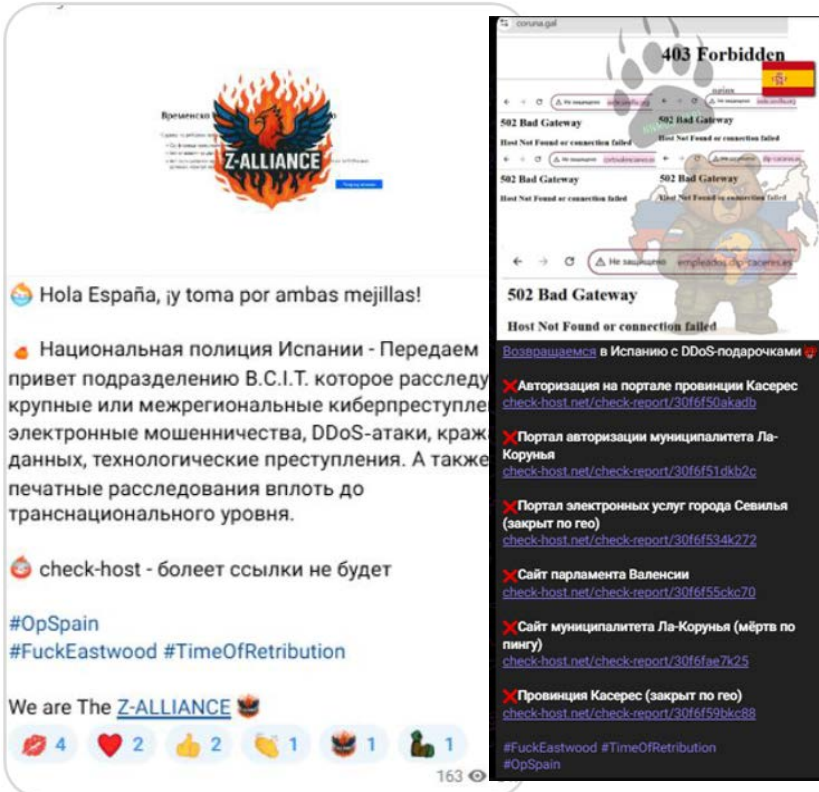
- Initial Access Brokers (IABs)
- Servicios de ofuscación
- Blanqueo de capitales



Hacktivism

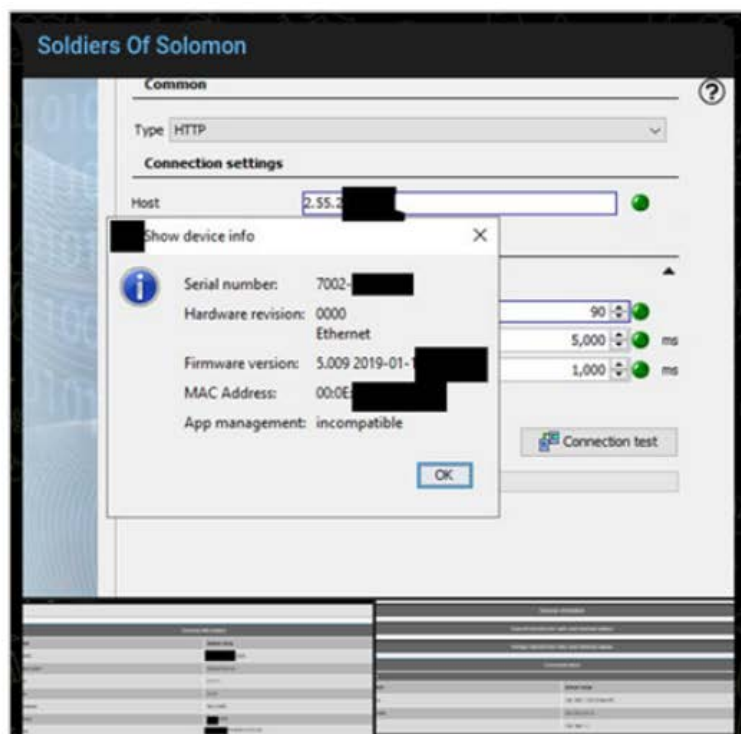
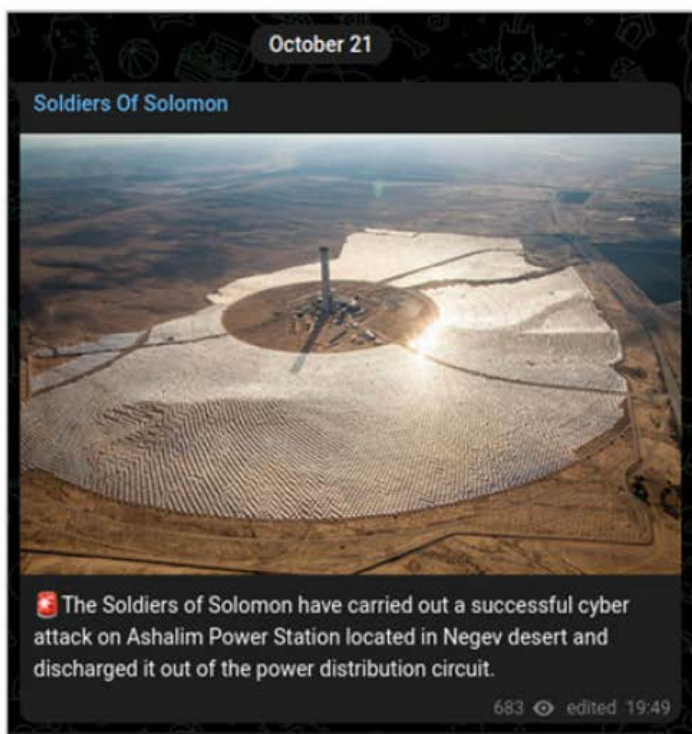
Empleados a modo de *proxies* para efectuar acciones ofensivas en beneficio de los Estados.

- Ataques de denegación de servicio (DDoS)
- Desfiguraciones páginas web (*defacements*)
- Exfiltrar y publicar información de bases de datos (*hack and leak*)
- Capaces de comprometer sistemas OT



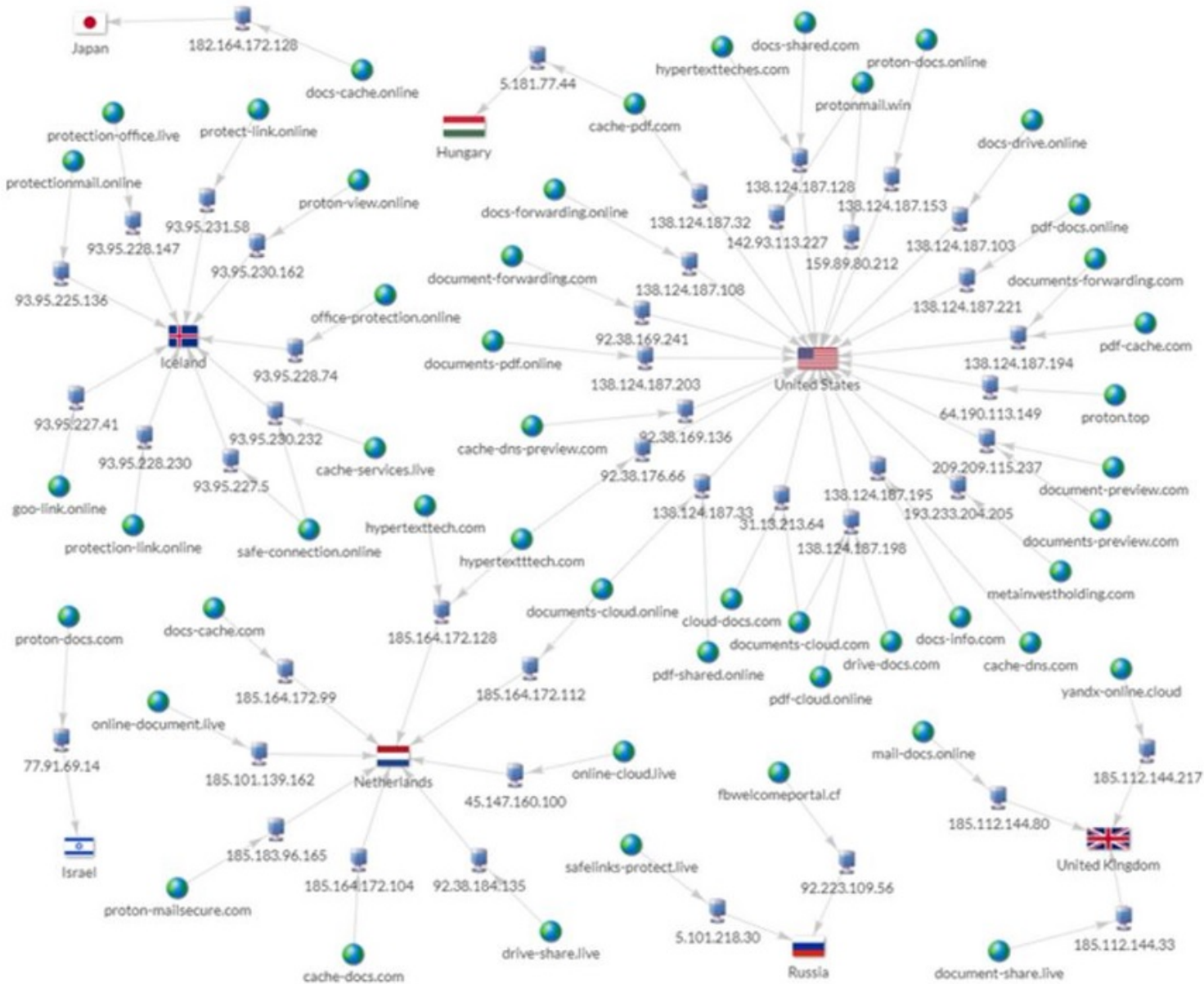


Hacktivism: ejemplo proxies proiraníes conflicto Gaza - Israel

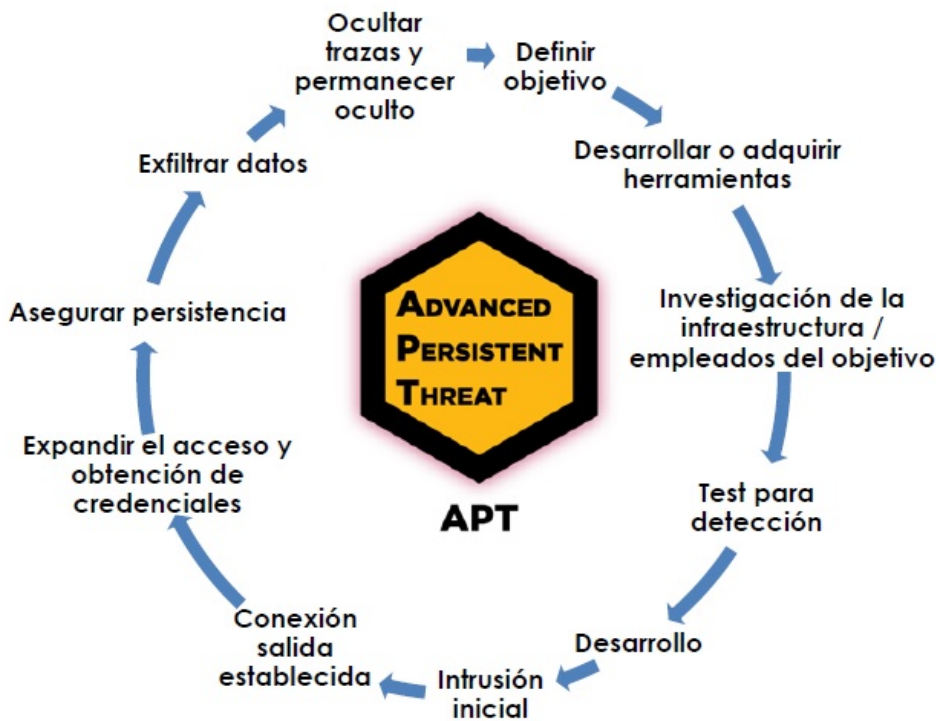




Hacktivismo: ejemplo Grupo Guacamaya



Actores Estado: APTs



Actores Estado: operaciones de espionaje

35% de las campañas han tenido como objetivo organismos gubernamentales

Focos de actividad coincidentes con tensiones geopolíticas:

- Ucrania y Rusia
- Europa (relacionadas con el anterior conflicto)
- Península de Corea (fricciones entre Corea del Sur, Japón y Corea del Norte)
- Subcontinente Indio (India – Pakistán)
- Oriente Medio (conflicto Israel - Hamás en el ámbito ciberespacial)



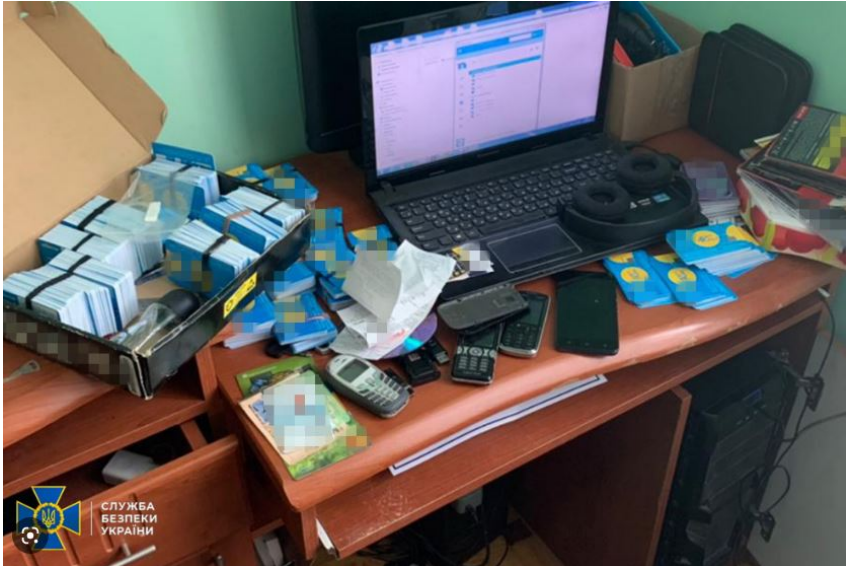
Actores Estado: operaciones de influencia

Empleo de *granjas de trolles* que crean *social bots* ilegítimos

Programas especializados para gestionar dichos perfiles

Generación y gestión de granjas de bots con IA para

- Crear en masa de perfiles creíbles en RRSS
- Difundir contenidos propios de usuarios reales
- Formulación automática de mensajes según perfil



El soldado Manning, condenado a 35 años por las filtraciones a Wikileaks

El uniformado se enfrenta a un máximo de 90 años de cárcel
Antes de la apelación el fallo debe ser aprobado por el responsable del Distrito Militar de Washington



EVA SAIZ

Washington • 22 AGO 2013 • 13:25 CEST



VIDEO: REUTERS LIVE / FOTO: AFP

NEWSLETTERS
Recibe el boletín de Internacional

ESPECIAL PUBLICIDAD

Qué es el omega 3 y por qué no estás consumiendo suficiente

EL PAÍS

ECONOMÍA

MERCADOS MIS AHORROS VIVIENDA MIS DERECHOS FORMACIÓN TITULARES »

Retina CincoDías NEGOCIOS

Arrestado el expleado de HSBC acusado de robar datos secretos

Herve Falciani fue detenido en Barcelona y está a la espera de ser extraditado



AGENCIAS

Ginebra • 24 JUL 2012 • 16:37 CEST

El expleado de HSBC acusado de robar datos de hasta 24.000 cuentas secretas suizas al prestamista británico y entregarlos a la Hacienda francesa ha sido detenido en Barcelona a petición de las autoridades suizas que solicitaban su extradición.

Desde el departamento de Justicia suizo confirmaron la información de medios franceses de que Herve Falciani, exespecialista informático de HSBC y con nacionalidad francesa e italiana, fue detenido en España hace tres semanas: "La representación suiza en Madrid depositó una petición formal de extradición con las autoridades de justicia españolas el 5 de julio", dijo. "Ahora la decisión depende de las autoridades españolas".

NEWSLETTERS
Recibe la mejor información en tu bandeja de entrada

TE PUEDE INTERESAR

Obercrimen. Oberguerra. Obespionaje. Nadie está a salvo en Internet

El talón de Aquiles de los móviles de los soldados israelíes

Hackear a sociedades abiertas



Actores internos

CNN politics

45 CONGRESS SUPREME COURT 2018 KEY RACES PRIMARY RESULTS

f t i s

Possible security gap allowed NSA contractor to shift highly sensitive jobs



By Evan Perez, CNN Justice Correspondent

Updated 2304 GMT (0704 HKT) October 6, 2016



SOURCE: CNN

NSA contractor charged with stealing classified intel 02:10

NEWS & BUZZ

Kavanaugh classmate: Disappointed in blatant lying

Alyssa Milano: Difficult to attend Kavanaugh hearing, but 'felt...'



Nuevos Actores (Posibilitadores)

Alquiler de capacidades: "*espionage-as-a-service*"

Su auge es una de las más alarmantes tendencias en el futuro del ciberespionaje.

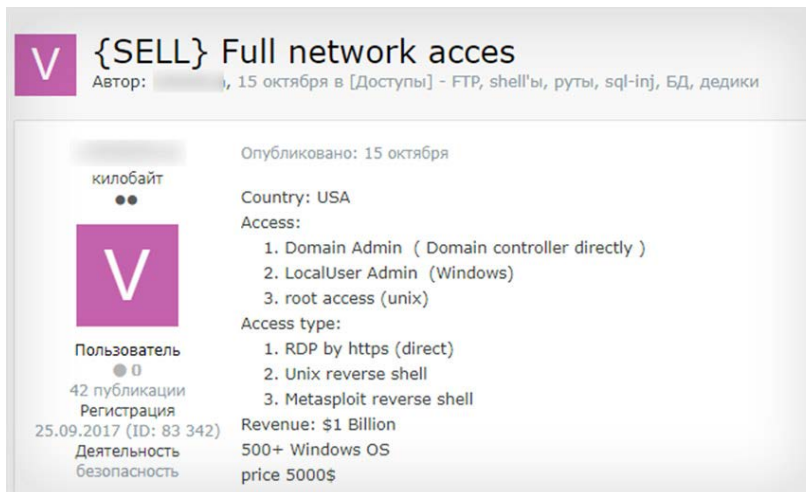
Alquiler de capacidades: "*hackers-for-hire*"

Profesionalización del mercado de la ciberdelincuencia, prestan servicios a grupos de interés estatal

- Ransomware - como - servicio (*RaaS*)
- Botnets
- Venta de malware (*Information stealers*)

Private Sector Offensive Actors (PSOAs)

Entidades comerciales dedicadas a la industria de la cibervigilancia.



La ciberinteligencia tiene como principal objetivo conocer las amenazas específicas para nuestras organizaciones y sistemas

La atribución: el principal problema en un escenario cada vez más complejo

Importancia del intercambio de información para afrontar las nuevas amenazas

- La cooperación y coordinación internacionales son absolutamente críticas a la hora de abordar las ciberamenazas**
- Necesidad de colaboración público-privada**



¿PREGUNTAS?

