Capturas con miel

Dr. Daniel Guasch Murillo

Sr. Jordi Enric Martínez Osorio
Sr. David Raya Marcos

UNIVERSITAT POLITÈCNICA DE CATALUNYA
BARCELONATECH
Escola Politècnica Superior d'Enginyeria de Vilanova i la Geltrú

21 de mayo de 2025

§

Escenario de trabajo…

Escenario de trabajo

Equipo de trabajo.

David Raya Marcos
Responsable del Servicio TIC

Jordi Enric Martínez Osorio
Técnico del Servicio TIC

Dr. Daniel Guasch Murillo
Profesor del departamento de Ingeniería Telemática
Miembro de la cátedra INCIBE de ciberseguridad CARISMATICA

Escenario de trabajo

La red UPC presenta una alta complejidad.

Usuarios y Actividad

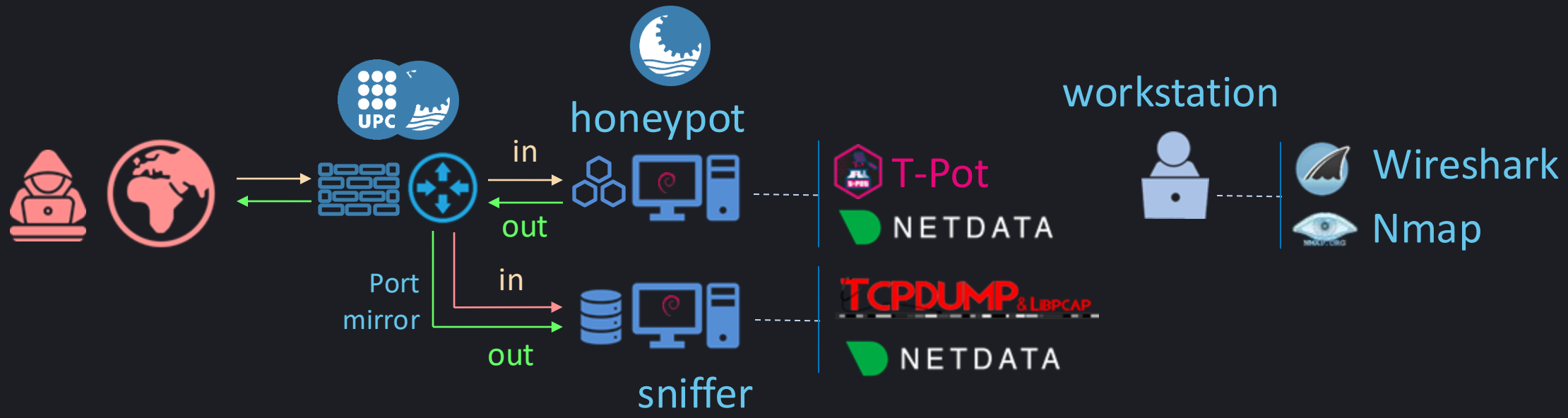
31.327 estudiantes de grado y máster	3.677 personal docente e investigador	2.143 personal téc. de gestión y administración y servicios	67 grados	96 másteres	46 programas de doctorado
18 centros docentes	141 programas de formación permanente	10 patentes el último año	410 M presupuesto 2025	121,6 M ingresos por I+D+i (2024)	91.278 alumni

Direccionamiento

147.83.0.0/16

Escenario de trabajo

Topología del sistema.



Es necesario configurar correctamente los firewalls y routers de las redes UPC

Escenario de trabajo

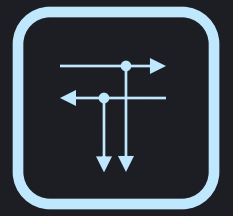
Equipos de trabajo.

honeypot

Análisis de los ataques
Análisis OSIN

Análisis forense del equipo

Routers y firewalls



Port mirror

Firewall rules

Escenario de trabajo

Equipos de trabajo.

sniffer

Captura del tráfico

Análisis forense del equipo

workstation

Análisis del tráfico

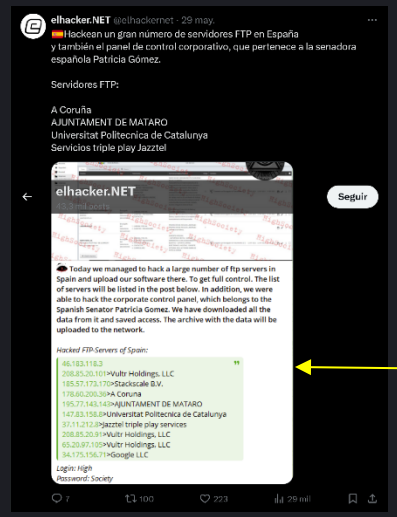
Análisis de red activo

E

Ejemplos…

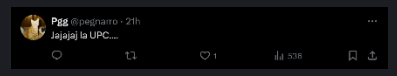
Ejemplo 1. Ataque de intrusión al servicio FTP

En 2024-05-29 se han publicado unos mensajes perturbadores en X ...

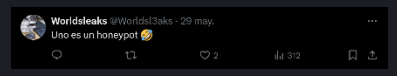


@elhackernet: El Origen...

El servidor de FTP 147.83.158.8 de la UPC ha sido hackeado...



@pegnarro: El oportunista...



@Worldsl3aks: el curioso... “uno es un honeypot!”

https://x.com/elhackernet/status/1795765134465405168?s=46&t=Lu9tDQ9xF8B32ayGabhS1g

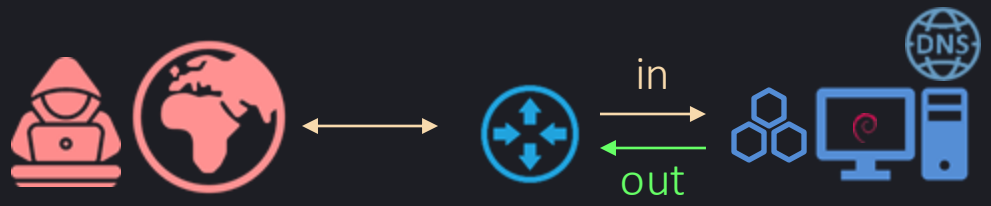
Ejemplo 1. Ataque de intrusión al servicio FTP

Docencia: identificar a los atacantes.

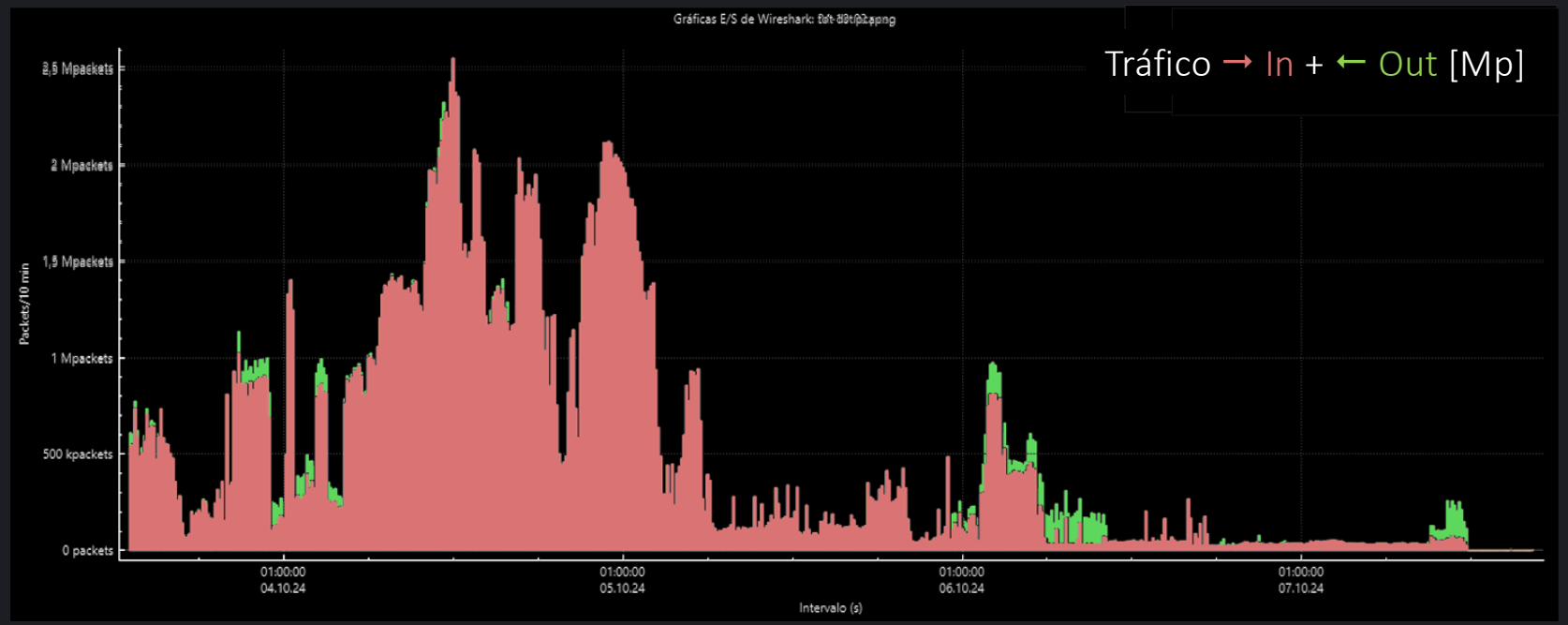
Ejemplo 2. Ataque de DDoS al servicio DNS

El 2024-10-07 se detecta una caída del sistema ...

Intervalo
2024-10-03 14:09:21 h
2024-10-07 17:28:26 h
4 días y 03:19:02 h



Paquetes: 291.064.478 (291 Mp)
Paquetes/s: 814,7
Bytes: 38.860.505.761 (36,2 GB)
Bits/s: 870 k
Tamaño medio paquete: 134 bytes

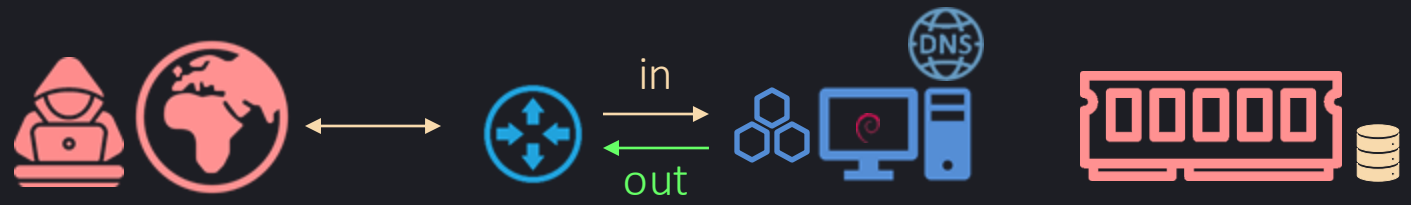


El honeypot quedo expuesto en el ataque anterior y se multiplican los ataques por 100.

Ejemplo 2. Ataque de DDoS al servicio DNS

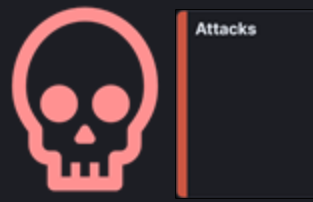
Docencia: ilustrar análisis forense del equipo.

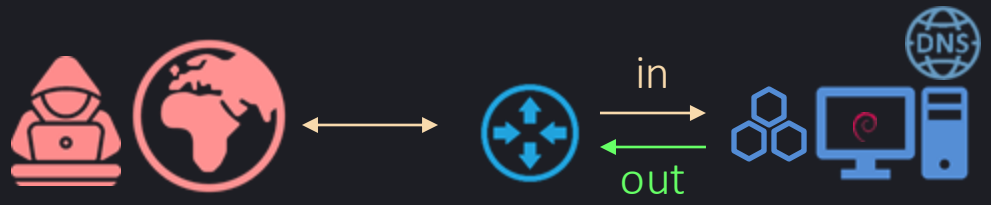
Intervalo
2024-10-03 14:09:21 h
2024-10-07 17:28:26 h
4 días y 03:19:02 h

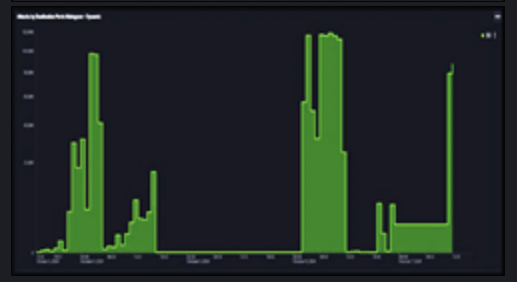


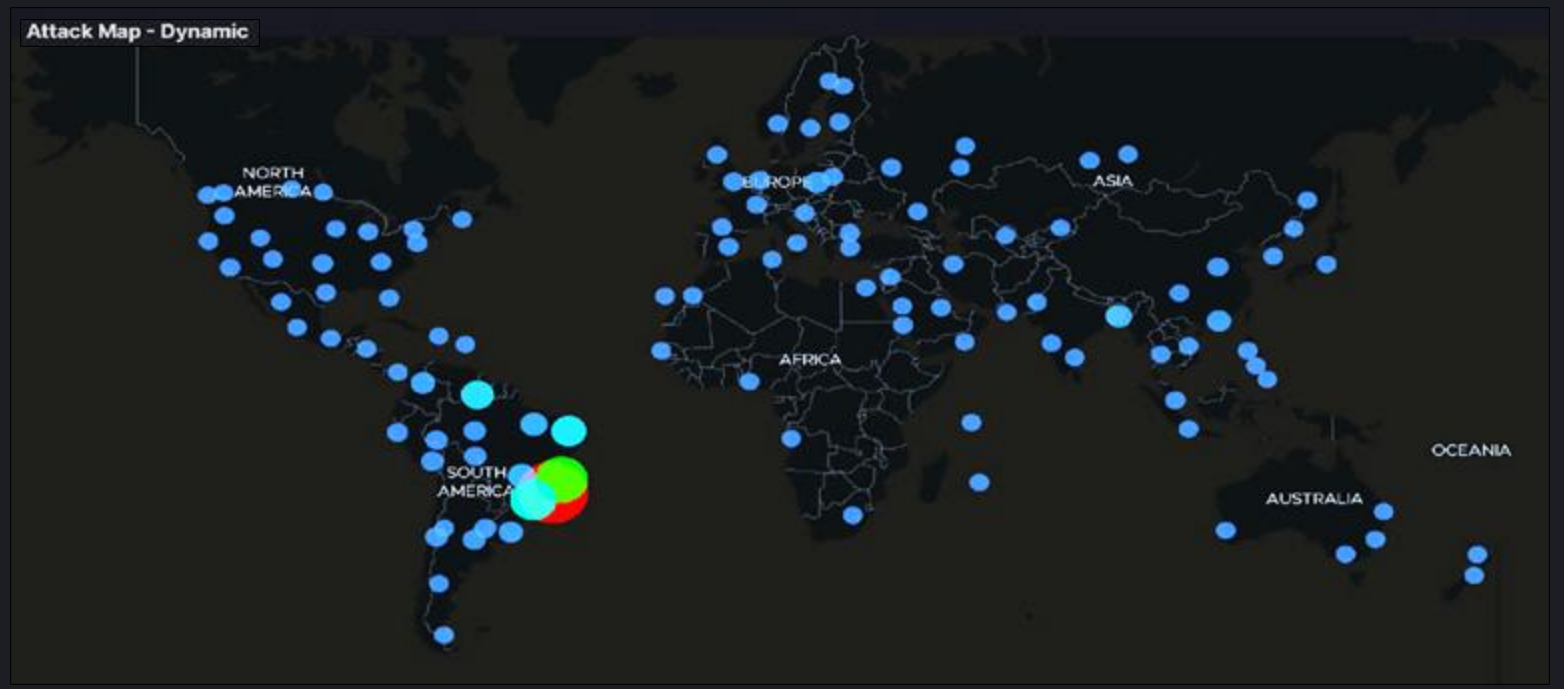
Ejemplo 2. Ataque de DDoS al servicio DNS

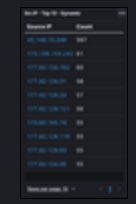
Docencia: identificar el ataque DDoS al DNS.









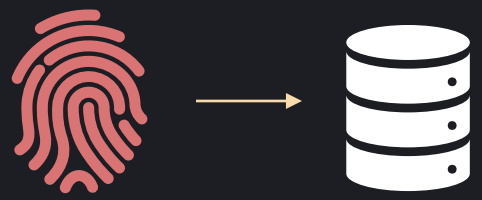


Ejemplo 2. Ataque de DDoS al servicio DNS

Docencia: Proponer contramedidas.

Ejemplo 2. Ataque de DDoS al servicio DNS

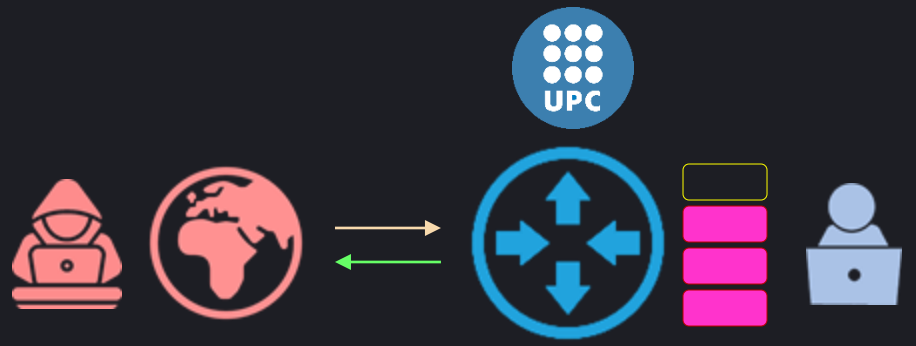
Investigación: identificar perfiles y guardar trazas.



1) Ataque desde 1 IP y 1 puerto.
2) Ataque desde 1 IP y múltiples puertos.
3) Ataque desde 1 red y múltiples puertos.
4) Ataques desde múltiples IP con 1 mismo método.
5) Ataques con ocultación (destino no alcanzable).
6) Ataques con ocultación (TTL, reensamblamiento).

Ejemplo 2. Ataque de DDoS al servicio DNS

Gestión: optimizar la configuración de los equipos.



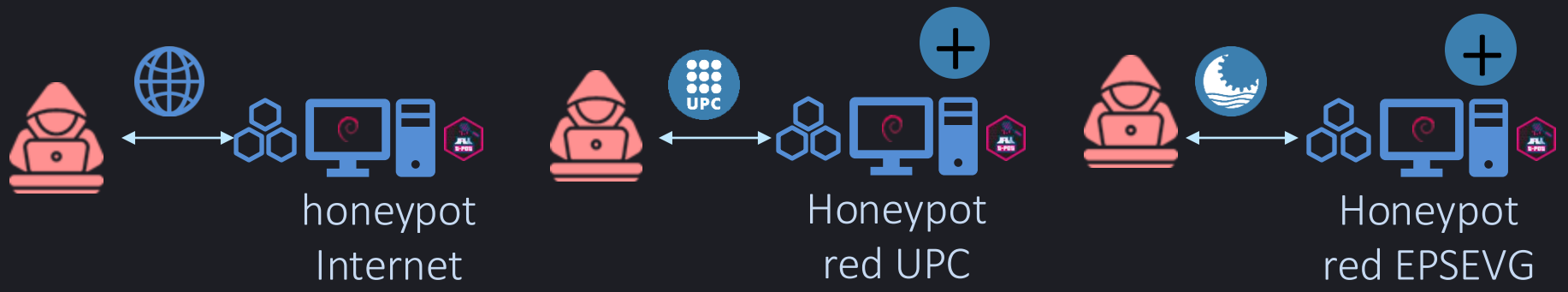
Sesiones UDP activas.

Situación	Problema	Solución
Se alcanzaban 180.000 sesiones UDP simultáneas en el ataque. El router soporta un máximo de 300.000.	Timeout UDP establecido a 180 s (valor por defecto)	Establecer Timeout UDP según recomienda el fabricante: 30 - 40 s

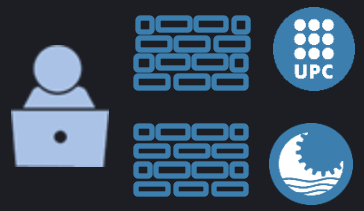
Ejemplo 3. Valoración de amenazas

En 2024-09-23 se investiga el volumen de ataques en las redes UPC…

+ 2 honeypots implementados en máquinas virtuales

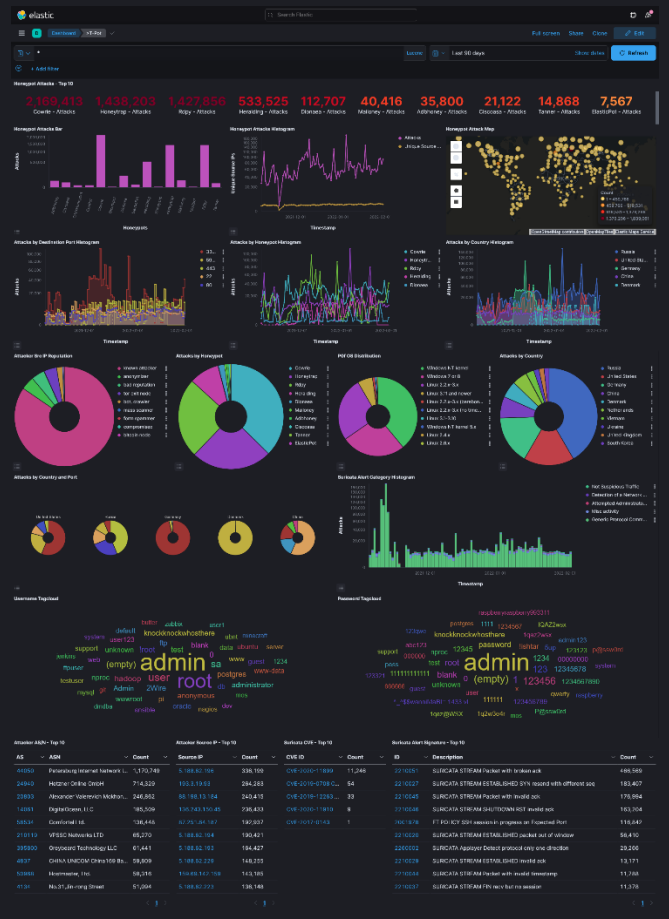


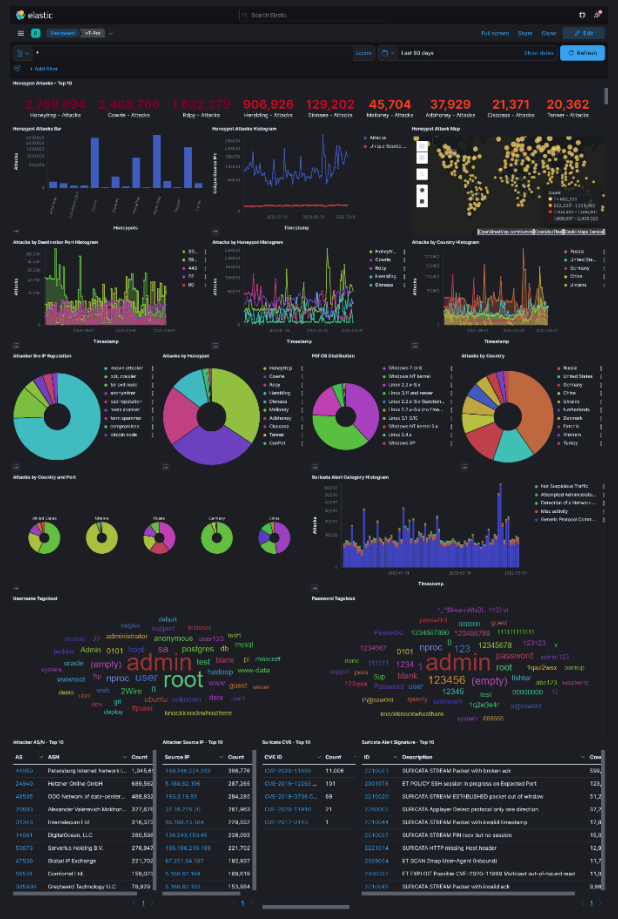
Es necesario actualizar las reglas de los cortafuegos



Ejemplo 4. Contexto mundial

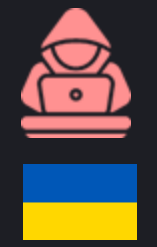
Se comparan medidas del 2022-02-04 y 2022-03-03…





En las estadísticas…

Rusia es el país más activo.



Aparece un país llamado Ucrania.

Ejemplo 4. Contexto mundial

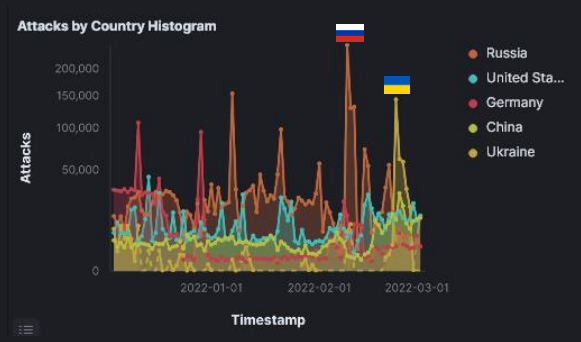
Gestión: Se evidencia el inicio de la guerra entre Rusia y Ucrania del 24 de febrero de 2024.

País

Rusia: 1ª posición

Ucrania: 8ª -> 5ª posición

Ataques (90 días)

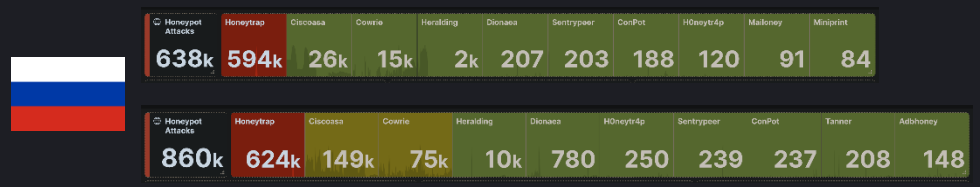


Puertos más atacados

TCP/3389	RDP
TCP/5900	VNC
TCP/443	HTTPS
TCP/22	SSH
TCP/80	HTTP

Actualmente la guerra continúa y se capturan ataques procedentes de ambos países.

Ataques 2025-05-15 (30 y 90 días)



2ª

4ª

10ª

14ª

C

Conclusiones…

Conclusiones

El sistema aporta conocimiento valioso

Docencia

- Aporta casos reales para ilustrar la teoría.
- Incrementa la motivación del estudiantado.

Investigación

- Permite la creación de bancos de trazas.
- Visibiliza tendencias en los ciberataques.

Gestión

- Identifica amenazas en la red.
- Facilita la optimización de los equipos de red.

Conclusiones

Capturas con miel

Más vale un tarro de miel…
…que mil barriles de vodka.

Esta iniciativa se lleva a cabo en el marco de los fondos del Plan de Recuperación, Transformación y Resiliencia, financiado por la Unión Europea (Next Generation), bajo los auspicios de la Cátedra INCIBE de Ciberseguridad CARISMÁTICA.