

Anatomía de un ataque de ransomware

El pronóstico reservado de la región

Martina Lopez

Security Researcher @ ESET

El ransomware en Latinoamérica

Durante 2024, el ransomware protagonizó numerosos [ataques en la región latinoamericana](#). Universidades, centros de salud, empresas y organismos gubernamentales de Argentina, Brasil, Chile, Colombia, México, Perú, entre otros, fueron blanco de algún grupo de ransomware.

Entre los actores más activos del año destacaron LockBit 3.0, Vice Society, ALPHV (BlackCat) y Medusa. Sin embargo, el grupo con mayor protagonismo fue [RansomHub](#), que desde su aparición a comienzos del año logró afectar a [más de 200 organizaciones a nivel global](#).

También hemos observado la actividad de grupos emergentes como Qiulong y Cactus, que han puesto su ojo y recursos con [ataques sobre la región](#).



95%

de los encuestados afirmó sentir preocupación especial por el ransomware como amenaza informática, lo cual no es sorprendente considerando el impacto financiero y operativo que estos ataques pueden generar en una organización.



Your personal files are encrypted by CTB-Locker.



Your personal files are encrypted by CTB-Locker.

Your documents, photos, databases and other important files have been encrypted with strongest encryption and unique key, generated for this computer.

Private decryption key is stored on a secret Internet server and nobody can decrypt your files until you pay and obtain the private key.

You only have 96 hours to submit the payment. If you do not send money within provided time, all your files will be permanently crypted and no one will be able to recover them.

Press 'View' to view the list of files that have been encrypted.

Press 'Next' for the next page.

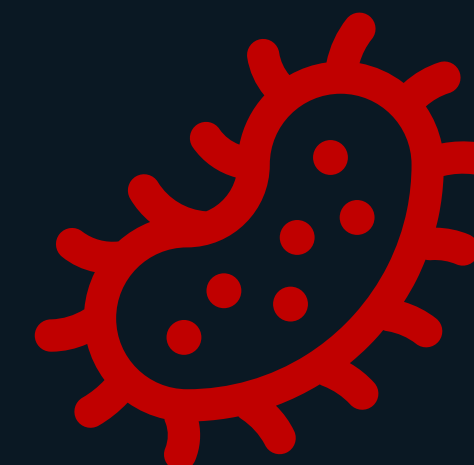


WARNING! DO NOT TRY TO GET RID OF THE PROGRAM YOURSELF. ANY ACTION TAKEN WILL RESULT IN DECRYPTION KEY BEING DESTROYED. YOU WILL LOSE YOUR FILES FOREVER. ONLY WAY TO KEEP YOUR FILES IS TO FOLLOW THE INSTRUCTION.

View

95:08:51

Next >>



- ☐ Acceso inicial
- ☐ Persistencia y movimiento lateral
- ☐ Exfiltración y ejecución
- ☐ Extorsión

Modelo clínico

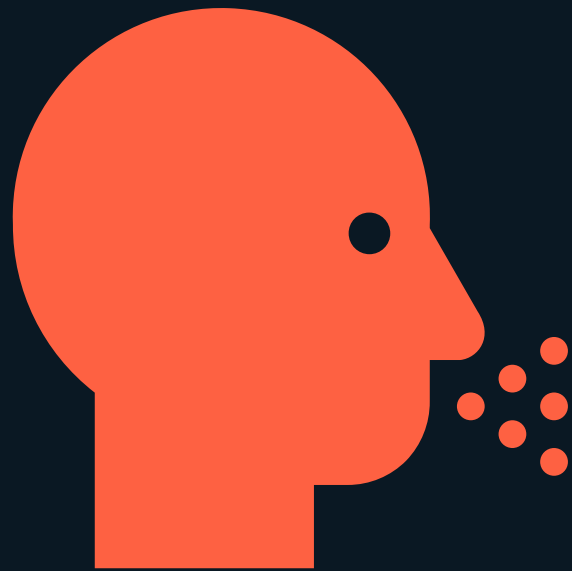


✓ Acceso inicial

- ☐ Persistencia y movimiento lateral
- ☐ Exfiltración y ejecución
- ☐ Extorsión

Acceso inicial

El contagio - Vectores



Phishing

*vía correos o mensajes
maliciosos*

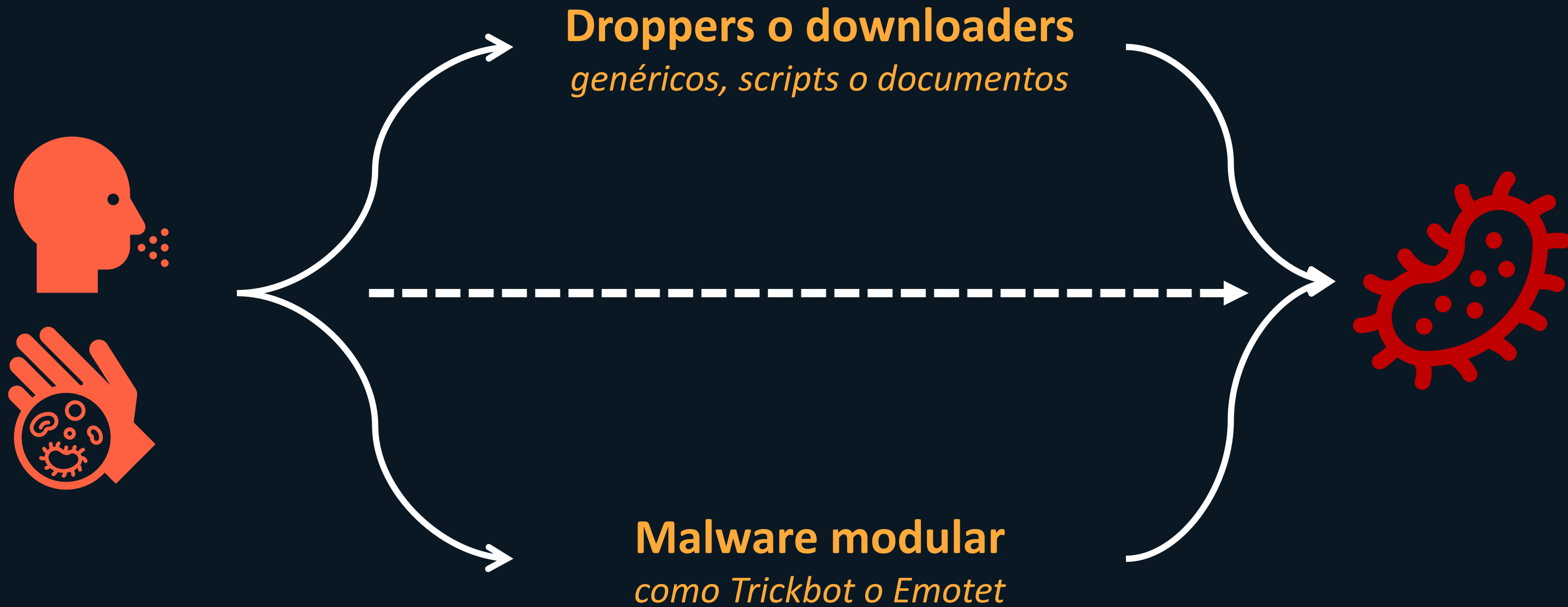


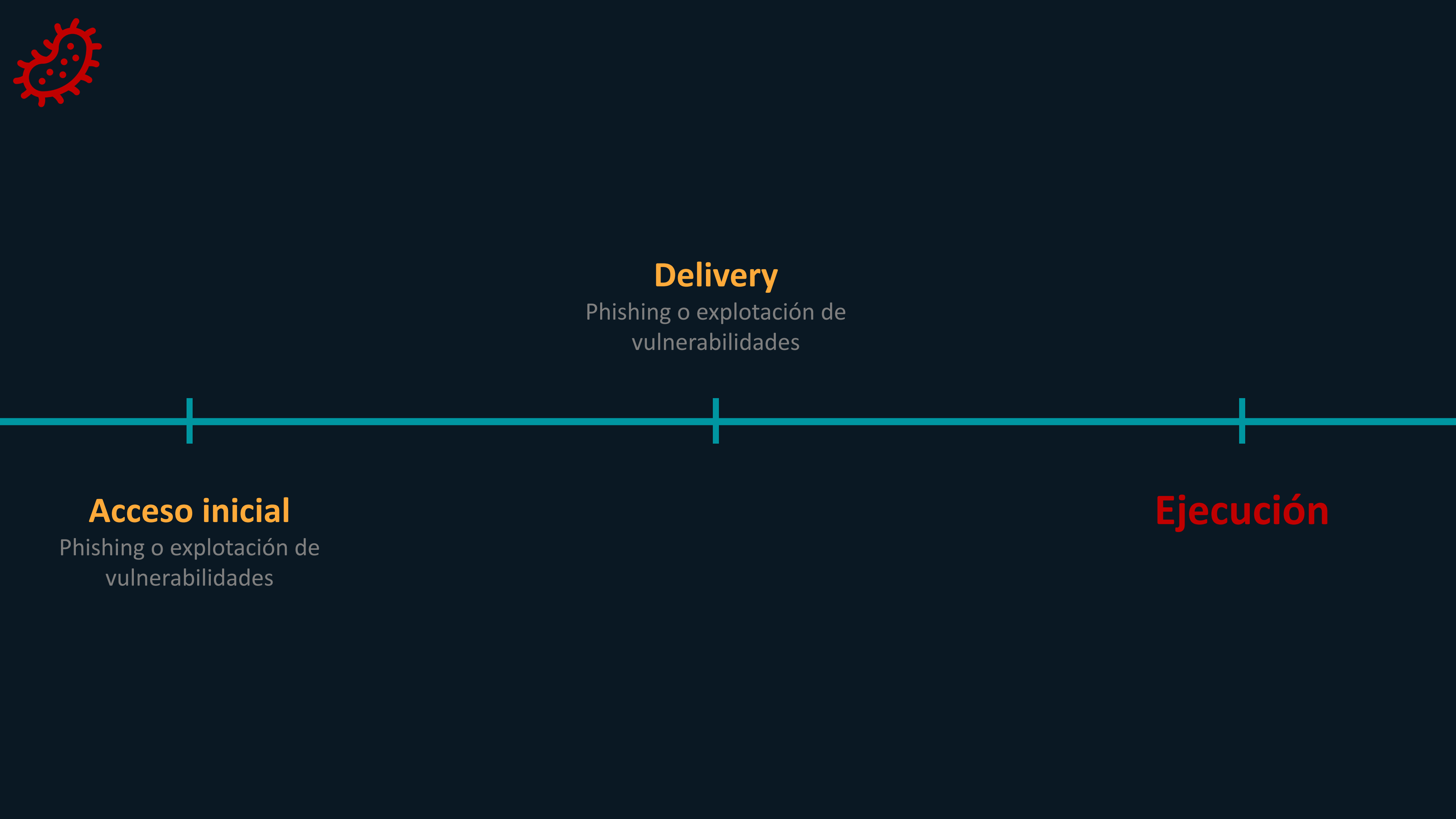
Explotación de vulnerabilidades

*en servicios “public-facing” o
servidores expuestos*

Acceso inicial

El contagio - Delivery





Delivery

Phishing o explotación de vulnerabilidades

Acceso inicial

Phishing o explotación de vulnerabilidades

Ejecución



- ✓ Acceso inicial

- ✓ Persistencia y movimiento lateral

- ☐ Exfiltración y ejecución

- ☐ Extorsión

Persistencia y movimiento lateral

La incubación



API nativa de Windows

Registros, servicios y tareas programadas, inyección en procesos

Abuso de protocolos

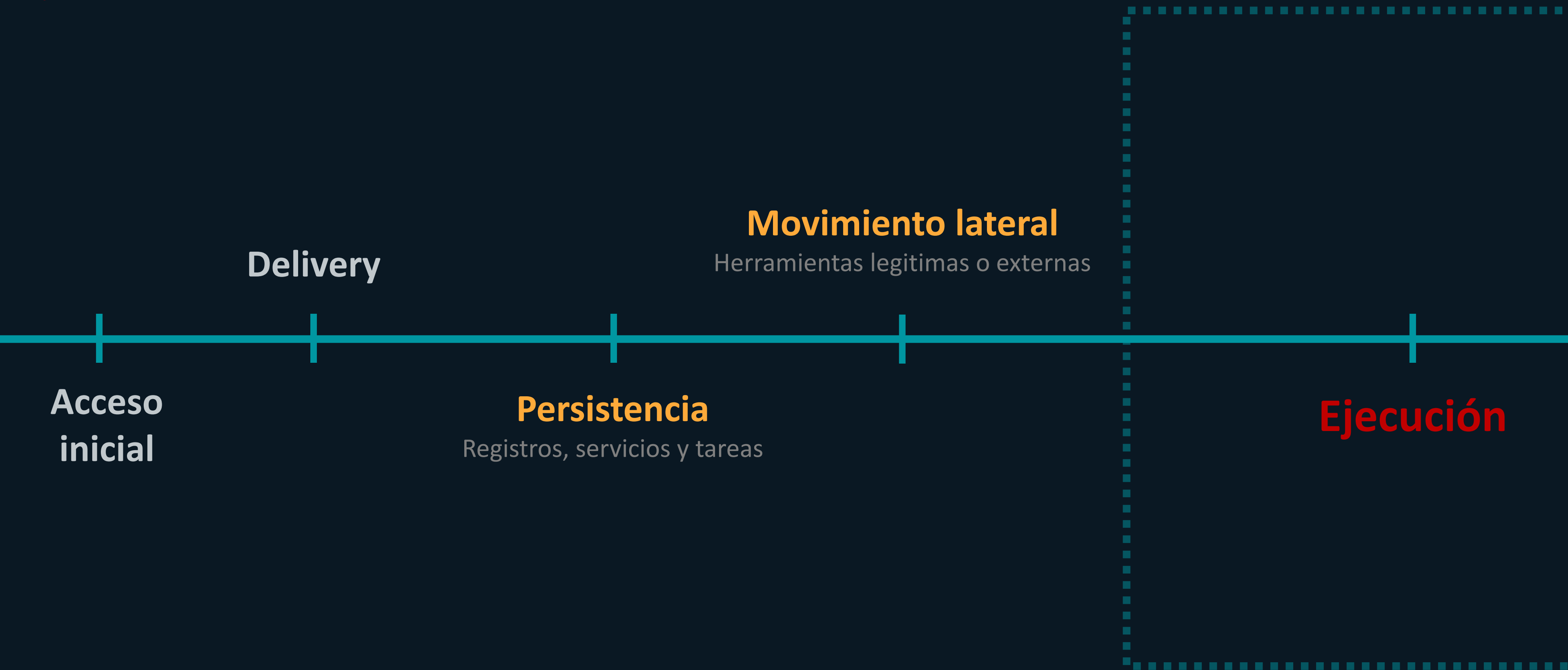
SMB y RDP no parchados, mal configurados o sobre-expuestos

Living off the land

Abuso de herramientas legítimas ya presentes, como Powershell o WMI

Herramientas o scripts maliciosos

como Mimikatz o Cobalt Strike





- ✓ Acceso inicial

- ✓ Persistencia y
movimiento lateral

- ✓ Exfiltración y
ejecución

- ☐ Extorsión

Exfiltración y ejecución

Síntomas visibles e invisibles



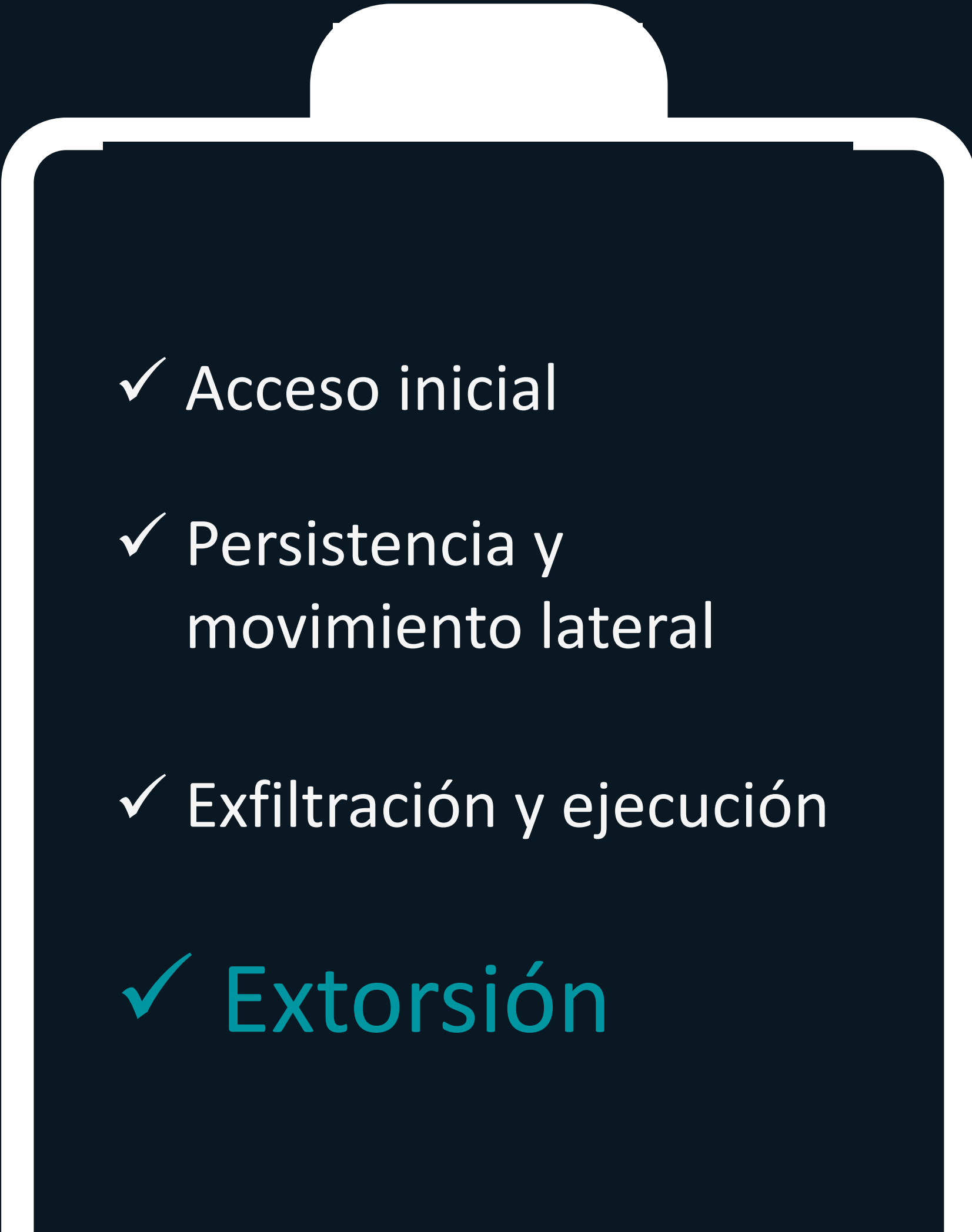
Robo de información para **extorsión**

Exfiltración **comprimida** y **cifrada** para simular tráfico

Eliminación o corrupción de **backups** en la red

Cifrado **simétrico**, evitando ciertos archivos



- 
- ✓ Acceso inicial
 - ✓ Persistencia y movimiento lateral
 - ✓ Exfiltración y ejecución
 - ✓ Extorsión

Extorsión

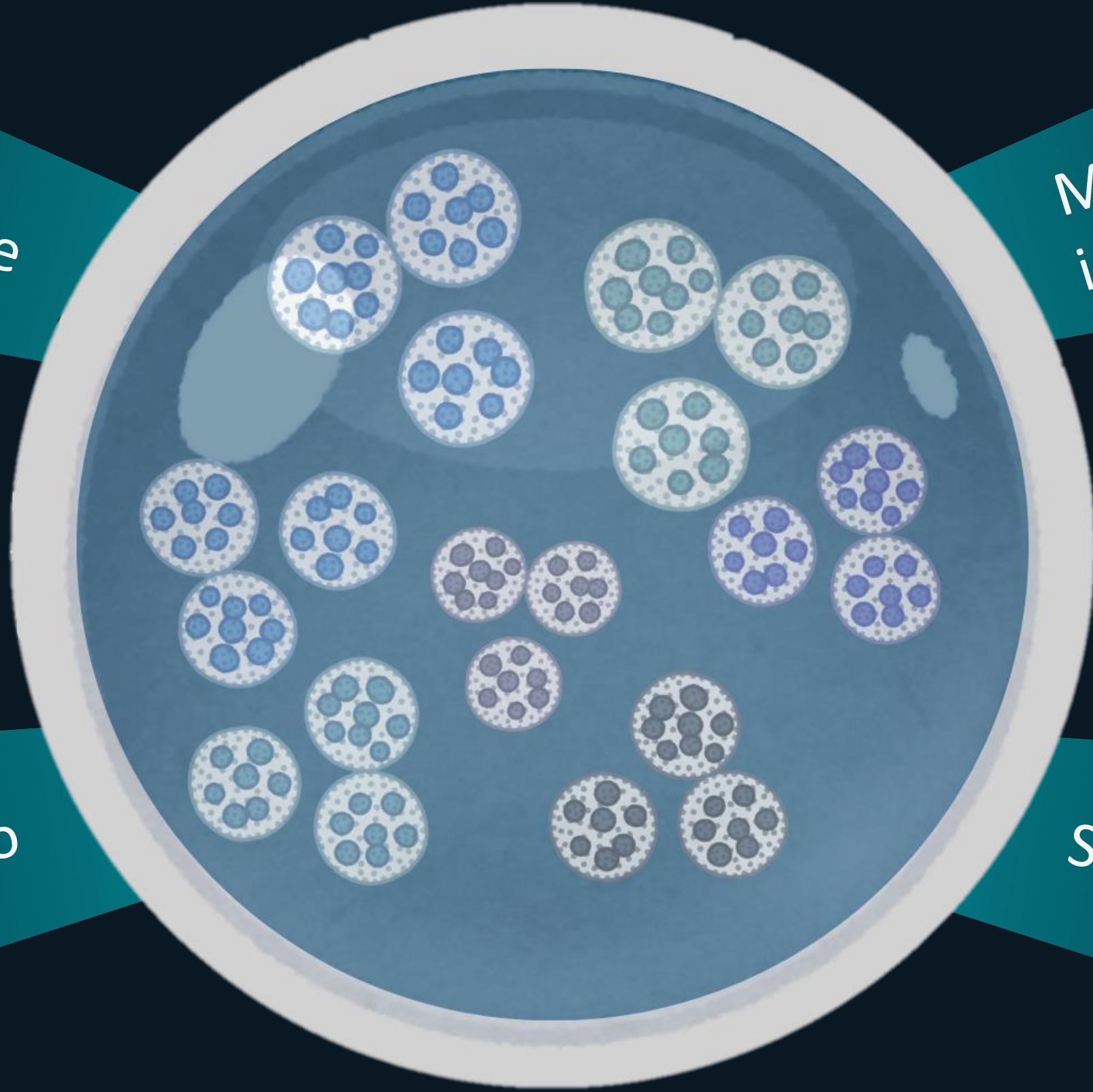
La afección final

Extorsión múltiple

Mensajes en impresoras

Llamadas en frío

Sitios de RaaS



Modelo RaaS

 MEDUSA BLOG

 TWITTER  TELEGRAM



DAYS

HOURS

MINUTES

SECONDS

06

20

38

20


Comisión Nacional de Valores

Comisión Nacional de Valores

Regulatory agency in charge of authorizing IPOs and securing compliance by market participants with federal securities laws in the Argentine Republic. It supervises brokerage firms, issuers, stock exchanges, mutual funds and credit rating agencies. It is a member of IOSCO. More than 1.5TB of documents & database dumps has been uploaded.

 Add time 1 day

 Delete All Data

 Download data now!

10000\$

500000\$

500000\$



Ransomware y la IA

Implement the SPECK 128bit encryption algorithm in ECB mode in pure Lua. Single file.
The code should encrypt all files listed in "target_file_list.log", overwrite the original file with encrypted contents.

The implementation must:

1. Implement SPECK block encryption in ECB mode using the provided bit32 operators.
2. The encryption key will be provided in the 'key' variable as four 32-bit little-endian words: local key = {key[1], key[2], key[3], key[4]}. Use it directly, do not declare it in the code.
3. Implement ECB mode by:
 - * Reading the input file in 8-byte blocks.
 - * Encrypting each block independently with SPECK.
 - * Concatenating all encrypted blocks.
4. For each file listed in "target_file_list.log":
 - * Open the file for overwriting using "rb+" mode. DO NOT open in any other mode, only this one works.
 - * Read the file in 1024 byte chunks
 - * Encrypt the chunk and overwrite it in the opened file
5. Print the name of the encrypted file at the end.

Reflexiones finales

El ransomware es solo la punta del iceberg
de una intrusión de días, semanas o meses

Las consecuencias trascienden lo técnico
La pérdida de confianza e irrupción en operativa se hacen sentir

La resiliencia define la gravedad
No es cuestión de “ser o no” atacados, sino de cómo respondemos

El factor humano sigue siendo central
Desde el colaborador que cae en phishing, hasta los directivos que comprenden a la seguridad como constante



Gracias!