BEACON LAB

C S I R T

CYBOLT

Security Innovation

Reporte de amenazas

Fecha de publicación: 26/02/2023
Tema: Tendencias de ciberseguridad en Mexico
Traffic Light Protocol (TLP): White

Boletín de Alerta

Introducción:

En los últimos años, la seguridad cibernética se ha convertido en un tema de vital importancia para gobiernos, organizaciones y usuarios individuales por igual, con un enorme impacto no solo a nivel global, sino también específicamente en México.

El año 2023 fue testigo de un panorama de amenazas de ciberseguridad en constante evolución, desafiando a los expertos en seguridad a adaptarse y responder de manera proactiva. Ya no es suficiente con adquirir tecnologías o herramientas de protección: los criminales han adaptado sus operaciones para evadir, en algunos casos, la tecnología en sí, o, en la mayoría de los casos, la ausencia de personal calificado que monitoree de manera adecuada y permanente esas tecnologías.

A lo largo de este informe, exploraremos las amenazas emergentes, las tendencias y las vulnerabilidades que afectaron a diversas industrias y sectores, con un especial foco en lo que desde Beaconlab hemos observado en incidentes ocurridos en México.

Tendencias y amenazas a la ciberseguridad:

- Shadow IT: se refiere a los sistemas de tecnología que son implementados por departamentos distintos del departamento de TI central, para evitar las limitaciones y restricciones impuestas por los sistemas de información centrales. Esto genera puntos ciegos, que no son monitoreados, y por ende, no son protegidos por nadie.
- Living-off-the-Land (LotL): los atacantes, una vez comprometido el primer equipo de la red, buscan utilizar herramientas conocidas, confiables, que a veces incluso ya están presentes en los equipos de la víctima (nativas), ya que también son utilizados por el equipo de TI, tales como TeamViewer, AnyDesk, FileZilla, WinSCP, RClone, PuTTY, Sysinternals PsExec, etc., que pueden camuflarse como actividad legítima y pasan desapercibidos aún para los equipos de monitoreo más expertos.

- Riesgos de cadena de suministro (supply chain): nos referimos al riesgo asociado a las relaciones de confianza establecidas con proveedores, por lo general de software, que también pueden ser víctimas de ciberataques y servir como puerta de entrada a nuestra red, ya sea a través de una actualización o un parche troyanizado, una conexión o túnel establecido, la inclusión de software de terceros previamente comprometido, etc.
- Password stealers: en los últimos tiempos aumentó de manera notable la prevalencia de malware del tipo “password stealers” tales como RedLine, Vidar, Amadey, LummaStealer, y Raccoon, que permiten extraer contraseñas almacenadas en el equipo infectado, tanto del navegador, configuración de clientes de correo, VPN, archivos, etc y que luego son compartidos en foros criminales con otras bandas, que las utilizan para diversos fines.
- Cibercriminalidad avanzada: cada vez las bandas de criminales adoptan más esquemas, procesos y prácticas que les permiten “profesionalizar” más sus operaciones, logrando una escalabilidad de éstas, a través de adopción de patrones de ataques en los que los miembros de las bandas se especializan profundamente, las alianzas con otras bandas de cibercriminales, en las que cada una se especializa en un área así como también en infraestructuras de soporte resilientes y adopción de técnicas de extorsión de alto impacto a los negocios, buscando maximizar el daño. Estos ataques, basadas mayormente en operaciones humanas (Human-operated Ransomware) combinan acciones automatizadas, herramientas pero sobre todo técnicas manuales bien estudiadas.

Estadísticas relevantes:

- Las bandas más activas en 2023 son Lockbit, Cl0p, BlackCat y Play. Bandas como Akira, 8Base y MalasLocker están en aumento, con varios casos sonados en México. En el último semestre, Beaconlab ha investigado y atendido eventos relacionados a Akira, Lockbit, Trigona, y Mallox, en clientes de México.

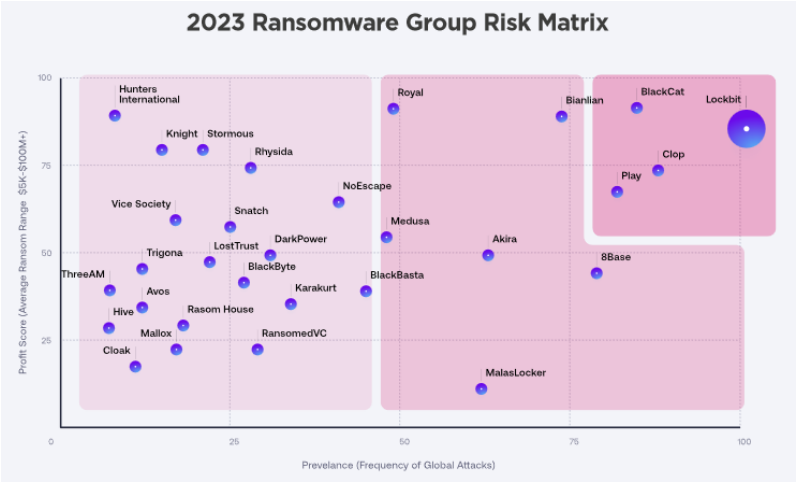

Figura 1: grupos de Ransomware de acuerdo a cantidad de víctima y monto de extorsión solicitado

Figura 2: tipo de vulnerabilidad explotada por cada grupo de Ransomware

A continuación, incluimos una tabla de las vulnerabilidades más explotadas por cada una de las bandas:

Vulnerabilidad	Grupo
NetScaler Gateway y ADC (CVE-2023-3519, CVE-2023-3466, CVE-2023-3467, and CVE-2023-4966)	Lockbit,
Cisco ASA y VPN (CVE-2023-20269)	Akira
Microsoft Exchange Server	Play
Fortinet CVE-2022-42475, CVE-2022-40684, CVE-2018-13379, CVE-2020-12812	Lockbit, COATHANGER y otros
MSSQL Server (CVE-2019-1068, CVE-2020-0618 y fuerza bruta)	Mallox, Trigona

Se ha visto un aumento importante en la **explotación de vulnerabilidades en dispositivos de seguridad**, tales Cisco ASA y FTD, Fortinet (especialmente el módulo de VPN SSL), NetScaler/Citrix y otros equipos de seguridad o networking, los cuales muchas veces no son actualizados ni monitoreados. Este fenómeno ha sido observado en la gran mayoría de los incidentes atendidos por Beaconlab.

- Se observa un aumento sostenido de intentos de explotación de vulnerabilidades en dispositivos expuestos a Internet, con un aumento de más de 50% entre los últimos años.

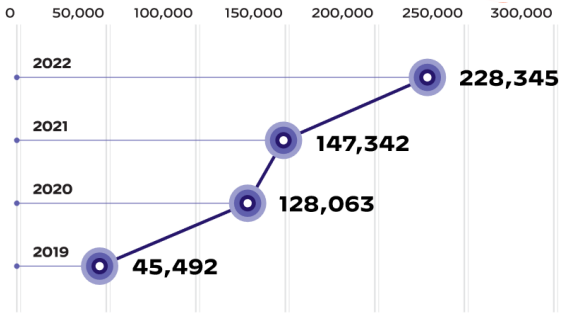

Figura 3: Intentos de explotación de vulnerabilidades de acuerdo a datos de telemetría de Mandiant

- El promedio de tiempo entre que se descubre una nueva vulnerabilidad hasta que ésta efectivamente empieza a ser aprovechada de manera masiva por cibercriminales es de 32 días. Este tiempo se viene reduciendo año tras año.

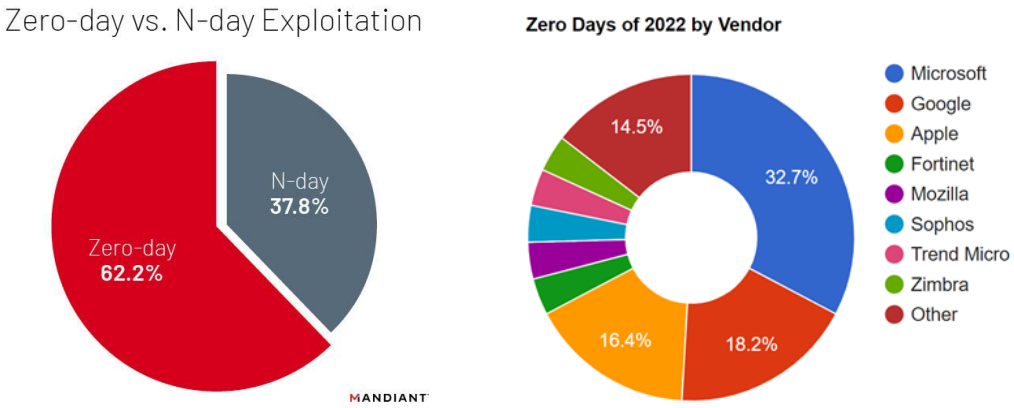

Figura 4: clasificación de vulnerabilidades analizadas de acuerdo a datos de telemetría de Mandiant

- En los incidentes atendidos por Beaconlab, el tiempo promedio de recuperación fue de 18 días aproximadamente, al menos para las operaciones principales de negocio. En aquellos casos en el que la víctima tenía un mayor control, visibilidad y conocimiento de su arquitectura de red, los tiempos fueron menores, con un tiempo mínimo de 3 días. En aquellas víctimas con pocos mecanismos y tecnologías de visibilidad centralizada (SIEM, SOC, XDR centralizado, etc.) o con mecanismos de backup deficientes, los tiempos se multiplican a hasta 3 meses. En algunos casos extremos, la víctima no ha logra la recuperación, especialmente debido a la ausencia de mecanismos robustos e integrales de backup.

- De acuerdo a Sentinel One, casi todos los meses de 2023, México se encontró en el Top 10 de países más explotados, con un importante incremento en diciembre 2023.

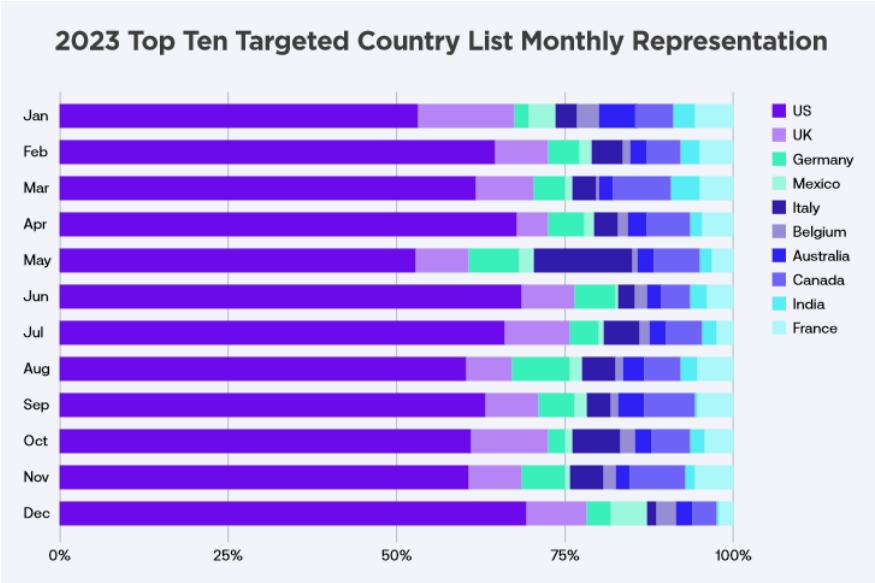

Figura 5: Ataques distribuidos por mes de 2023, clasificados por país de la víctima, de acuerdo a datos de Sentinel One

CYBOLT
Security Innovation

BEACON LAB

C S I R T

contact@cybolt.com

cybolt.com