Des ransomwares plus extrêmes et pourquoi les attaques se multiplient

Florian Bayard ⁝

Les attaques par ransomware se sont multipliées au cours des derniers mois.
Après une année 2022 très calme, les cybercriminels font un retour en force avec de nouvelles méthodes agressives.

L'an dernier, le nombre d'attaques par ransomware s'est considérablement réduit.
D'après les experts de Chainalysis, une société spécialisée dans la surveillance de la blockchain, **le volume d'offensives a chuté** en même temps que le butin des cybercriminels.
L'an dernier, ceux-ci ont obtenu moins de 500 millions de dollars en exigeant des rançons en cryptomonnaies. Interrogé par Wired, Jackie Burns Koven, responsable du renseignement sur les cybermenaces chez Chainalysis, explique :

> *« Nous avons été très surpris de constater ce déclin.*
> *Ensuite, nous avons parlé à des partenaires externes – des entreprises de réponse aux incidents, des compagnies d'assurance – et ils ont tous dit, oui, nous payons moins, et nous voyons également moins d'attaques »*.

Chainalysis attribue la baisse des attaques à l'essor de nouveaux systèmes de sécurité et d'outils de déchiffrage.
Ceux-ci, mis à disposition par les autorités, a permis à de nombreuses victimes de r**écupérer un accès à leurs données** sans devoir verser une rançon.
La guerre en Ukraine a également affecté les activités de la myriade de gangs basés en Russie.

À lire aussi : Ce nouveau ransomware « Robin des Bois » a une exigence très particulière

Les hackers s'en mettent plein les poches

Malheureusement, les gangs de ransomware se sont remis au travail au cours des six premiers mois de 2023.
En l'espace d'un seul semestre, les pirates ont **extorqué 449,1 millions de dollars**.
Si la tendance se poursuit, le butin annuel des hackers pourrait atteindre les 898,6 millions de dollars, pas loin du record de 2021 (939,9 millions de dollars).
Chainalysis précise qu'il ne s'agit évidemment que d'une estimation.
C'est très compliqué de calculer avec exactitude le total des fonds extorqués par le biais de la blockchain.
Par ailleurs, certaines entreprises préfèrent garder le secret pour éviter de nuire à leur image.

Le constat de Chainalysis corrobore les conclusions de ReliaQuest.
Dès le premier trimestre de l'année, la société a remarqué une recrudescence de l'activité des ransomwares.
Certains gangs ont multiplié les attaques.
C'est le cas de Lockbit, qui est d'ailleurs désormais capable de s'en prendre aux Macs.

De nouvelles tactiques musclées

Malgré les *« déficits budgétaires »* de l'an dernier, les criminels ont développé des *« techniques d'extorsion plus extrêmes »*, souligne Jackie Burns Koven.
Face aux refus de leurs victimes, de plus en plus de pirates se montrent impitoyables et sans merci.
Pour forcer la main de leurs cibles, ils n'hésitent plus à mettre en ligne des données très sensibles et à violer la vie privée de quidams.
Fort d'une série de nouvelles méthodes musclées, les pirates ont multiplié les assauts ces derniers mois pour compenser les piètres résultats de l'année dernière.

Le premier semestre 2023 a également été marqué par l'émergence d'un nouveau gang, baptisé Royal.
Apparu fin 2022, le groupe s'attaque essentiellement aux entreprises américaines.
Citons aussi l'entrée en scène de Rorschach, un mystérieux malware qui s'est rapidement imposé comme le ransomware le plus redoutable au monde.
Il est en effet capable de chiffrer les données d'un ordinateur à la vitesse de l'éclair, encore plus vite que LockBit.

L'explosion des attaques résulte par ailleurs de l'essor des ransomware en tant que service (RaaS).
Ces logiciels malveillants, disponibles par le biais d'un simple abonnement, permettent à n'importe quel apprenti hacker de déployer des ransomwares, sans avoir besoin d'un long apprentissage technique.
Combinés à des méthodes innovantes, ces services ont contribué à la recrudescence des offensives.

Source : Wired

Recherche et mise en page:
Michel Cloutier
CIVBDL
20230715
"C'est ensemble qu'on avance"