ANALYSE DU RAPPORT SONICWALL 2021 CYBER THREAT

MACIEL BRUNO

NOVEMBRE 2021

Credits: https://aci.defi-aerospace.org/Dossier-Cybersecurite-et-transport-aerien

DEF'INSEEC DEFINSEEC@GMAIL.COM 0 6 6 6 7 3 7 1 6 5

FACE À DES ATTAQUES PLUS NOCIVES, UNE NOUVELLE CYBERDÉFENSE

2021 a été une année record pour la cybercriminalité. Des entreprises de toutes tailles et de tous les secteurs constatent, à leur dépens, cette augmentation de la cybercriminalité. Une partie de cette augmentation peut être attribuée aux nouvelles techniques de ransomware, à la hausse des prix des crypto-monnaies ou à l'augmentation continue des appareils IoT (l'interconnexion entre internet et objets). Toutefois, un facteur important reste le paysage actuel du travail à distance, avec une informatique distribuée et changeante, qui s'est avérée être un environnement exceptionnellement attrayant pour lancer une grande variété d'attaques, dont beaucoup sont extrêmement compromettantes pour tous les types d'organisations.

LE RANSOMWARE BAT UN NOUVEAU RECORD

Parmi les données collectées par les chercheurs de SonicWall Capture Labs au cours des six premiers mois de 2021, disponibles dans le rapport SonicWall 2021 Cyber Threat, les ransomwares, qui étaient déjà nombreux en 2020, ont connu une considérable augmentation depuis lors. De plus, le nombre de cyberattaques utilisant des ransomwares ont augmenté de 151% au cours du premier semestre de l'année. Les mois d'avril, mai et juin ont été suffisamment dangereux pour atteindre des sommets historiques, et les attaques ne montrent aucun signe de ralentissement. Au 30 juin, SonicWall avait enregistré 304,7 millions d'attaques de ransomware dans le monde, dépassant ainsi les 304,6 millions d'attaques comptabilisées en 2020.

Credits : Parasoft

RTDMI ™ ATTEINT DE NOUVEAUX SOMMETS

La mauvaise nouvelle à laquelle nous devons faire face, c'est que les cyberattaques deviennent de plus en plus efficaces et létales. La bonne nouvelle, c'est que les méthodes de défense s'améliorent également. Tirant parti de l'apprentissage automatique, RTDMI (Real-Time Deep Memory Inpection technology) est devenu très efficace pour identifier les menaces nouvelles et avancées, réalisant à un score parfait (100% de détection des logiciels malveillants) au cours des deux derniers cycles de test de l'ICSA Advanced Threat Defense (ATD). Ce programme, développé par SonicWall, vise à trouver et éliminer les malwares (logiciels malveillants) des ordinateurs abritant des serveurs pour combattre les vols de données. Bien plus performant que ses prédécesseurs du fait de sa technologie unique, RTDMI pourrait bien rééquilibrer le rapport de force entre hackers et grandes entreprises.

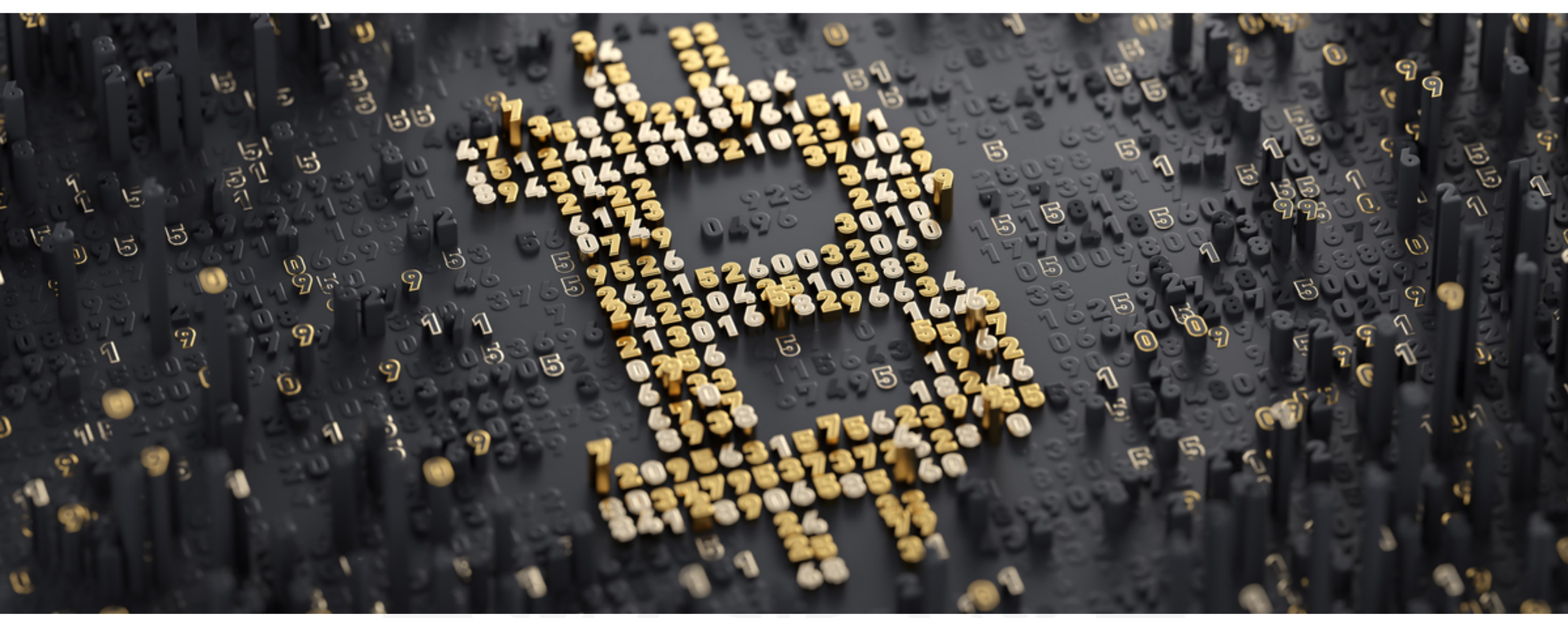
LES ATTAQUES SUR L'IOT AUGMENTENT DE 59%

Avec le nombre d'appareils IoT qui devrait passer de 13,8 milliards aujourd'hui à 30,9 milliards en 2025, et avec des normes de sécurité étonnamment laxistes, les cybercriminels ciblent de plus en plus les attaques sur les appareils connectés. Déjà ancrés dans nos vies quotidiennes, les montres, réveils ou encore maisons connectés sont devenus le nouveau terrain de jeu des pirates informatiques ; faiblement protégé malgré les données qui y transitent, l'Internet of Things est devenu l'enjeu n°1 de la cybersécurité publique. En effet, au premier semestre 2021, SonicWall a enregistré 32,2 millions de tentatives de malware attaquant l'IoT, soit une augmentation de 59 % à ce jour. Ainsi, les entreprises leaders dans les objets connectées mettent sans cesse à jour leur politiques de confidentialité et leurs pare-feu ; pour le moment, cette stratégie n'a pas l'air de fonctionner.

Credits : Geopolitis magazine

LE CRYPTOJACKING CONTINUE D'AUGMENTER

Contre toute attente, le cryptojacking continue également de croître ; au cours des six premiers mois de 2021, SonicWall a découvert 51,1 millions de tentatives de cryptojacking, soit une augmentation de 23 % jusqu'à présent cette année. Les cryptomonnaies, très peu règlementées, sont aussi extrêmement rentables. Plutôt que de voler des sommes déjà existantes, les pirates utilisent les ordinateurs des particuliers pour miner des cryptomonnaies, à l'insu du propriétaire de l'ordinateur, ralentissant les performances de ce dernier. Ce nouveau type de menaces, complètement invisibles, s'inscrit dans la tendance frauduleuse qui entoure l'évolution des cryptomonnaies : très peu règlementées, ces dernières sont le terrain idéal des escrocs et des spéculateurs, qui profitent de la naïveté des utilisateurs pour s'enrichir .



Pour conclure, le rapport SonicWall met en lumière les chiffres effarants de la criminalité informatique, et doit être un outil pour les compagnies et les particuliers qui se pensent à l'abri de toute attaque. Avec la vitesse et l'ampleur des changements affectant le paysage des menaces informatiques, il n'a jamais été aussi important de rester à jour sur les risques d'aujourd'hui et de se préparer à ceux de demain.

Credits : GFI Techtalk, Avast

SOURCES

- https://www.sonicwall.com/2021-cyber-threat-report/
- https://www.cerdant.com/wp-content/uploads/2021/09/2-2021-threat-report-midyear-summary.pdf
- https://cdw-prod.adobecqms.net/content/dam/cdw/on-domain-cdw/brands/sonicwall/sonicwall-2021-cyber-threat-report.pdf

H.E.I.P

AEROSPACE
CYBERSECURITY

DEF'INSEEC

SUIVEZ DEF'INSEEC SUR

DEF'INSEEC DEFINSEEC@GMAIL.COM 06 66 73 71 65