Parc d'Activités Schweitzer
26 rue du bois Fossé
85300 CHALLANS
Tél. 02 51 49 31 31

espace technologie

FICHE CONSEIL

2022
LA MONTEE EN PUISSANCE DES MALWARES EN TANT QUE SERVICE

❖ Pénétrez dans l'esprit des hackers et leur nouveau modèle d'affaires très lucratif

Imaginez que vous faites partis d'un groupe de hackers de très haut niveau et que vous passez des heures à coder le parfait logiciel malveillant.

Ensuite, vous et votre équipe parvenez à infiltrer quelques entreprises avec un ransomware. Les rançons obtenues seront déjà d'un très bon rapport mais il vous est possible de gagner beaucoup plus.

Maintenant, imaginez que vous puissiez proposer votre logiciel malveillant à d'autres hackers sans grandes qualifications sous forme de service, moyennant rétribution !
Vous voilà dans le monde des malwares en tant que service (MaaS).

Pour comprendre la crise actuelle liée à la démultiplication des attaques, nous devons nous mettre à la place de ces pirates qui travaillent dur pour alimenter leur fonds de commerce.
Tout d'abord, il faut savoir que les logiciels malveillants sont avant tout des logiciels, autrement dit du business. Certains sont géniaux, quoique malintentionnés.

Et le piratage en tant que service ?
C'est juste le niveau de génie supérieur.

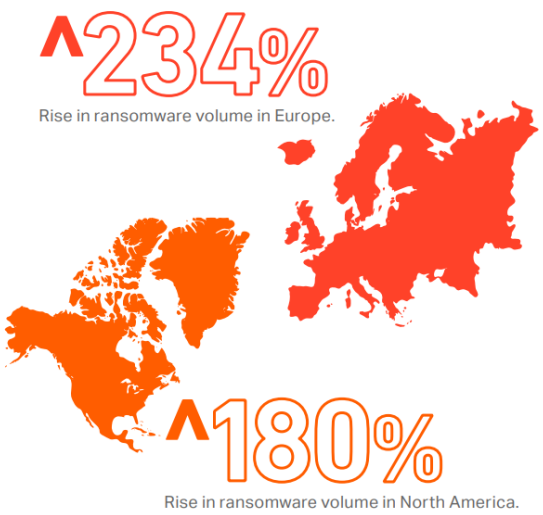
En effet, le nombre de pirates de niveau faible à moyen sont très nombreux mais incapable de créer des Malwares de haut niveau. Par contre, s'ils peuvent se procurer des Malwares de haut niveau moyennant rétribution, le nombre d'attaques de haut niveau est démultiplié. Et tout le monde est gagnant, sauf les victimes !!!

Le mode MAAS est né (Malware As A Service)

❖ La preuve en chiffre

Il y a de quoi être étonné quand les hackers en sont déjà à développer un modèle d'affaires pour faire prospérer leur « industrie », alors que nous sommes encore, pour beaucoup, des novices en matière de cyber sécurité.

Il y a quatre mois, SonicWall a publié sa célèbre mise à jour semestrielle du Rapport SonicWall 2021 sur les cybers menaces, avec des nouvelles alarmantes sur la progression fulgurante des ransomwares et autres attaques malveillantes. Malheureusement, les actualités du troisième trimestre ne sont guère meilleures : l'essor des ransomwares ne ralentit pas.



Cette année 2021 s'avérait déjà être la plus active qu'on ait connue en matière de ransomwares. Selon les données les plus récentes, l'activité continue de grimper et un ralentissement n'est pas en vue. Après un deuxième trimestre marqué par un nombre inédit de 188,9 millions d'attaques de ransomwares, la tendance se poursuit, atteignant un nouveau record de 190,4 millions au troisième trimestre.

Au total, cela fait 495,1 millions d'attaques, soit un bond de 148 % par rapport à 2020, faisant de 2021 l'année la plus coûteuse et la plus dangereuse jamais observée.

❖ MaaS, un modèle d'affaires convaincant

Microsoft 365, Google Workspace, Salesforce et autres sont autant d'éditeurs de logiciels qui proposent leurs produits en tant que service (SaaS). Dans ce modèle d'affaires, les éditeurs se chargent de développer et de maintenir des applications personnalisables qui gèrent toutes sortes de tâches.

Cela constitue une aide précieuse pour les entreprises qui ne possèdent pas de compétences logicielles ou qui n'ont simplement pas envie de développer leurs propres applications. De manière similaire, les hackers expérimentés peuvent proposer leurs malwares en tant que service (MaaS) aux personnes désireuses de gagner de l'argent par le piratage, ce qui nous mène aux « ransomwares en tant que service » (RaaS). MaaS ou RaaS, deux appellations qui décrivent parfaitement les activités exercées par des gangs de hackers bien connus tels que Circus Spider, Conti, DarkSide ou encore REvil.

Ils sont des dizaines d'autres groupes à mettre à disposition leurs compétences à d'autres gangs possédant une expertise et des aptitudes complémentaires dans différents domaines – phishing, ingénierie sociale, outils de chiffrement, analyse des performances de serveurs, récupération de rançons… Tout cela bien sûr en s'entendant sur le partage des revenus générés par leurs activités conjointes.

Le fait que nous puissions parler de modèle d'affaires en dit long sur la gravité de la situation. Dans ce contexte, des apprentis criminels ont soudain l'opportunité de devenir des géants mondiaux de la cybercriminalité et ce, quel que soit leur niveau de compétence. Quiconque ayant une rancune et suffisamment de temps à disposition peut s'en prendre à des agences gouvernementales, à de grands réseaux d'entreprise, voire à des acteurs plus petits, un simple télétravailleur par exemple.

❖ MaaS, une menace clé en main

De fait, on peut vraiment dire que le MaaS est une menace clé en main. Parmi les données les plus récentes de SonicWall sur les menaces se trouve un autre signe de ce que cela pourrait signifier : la hausse de 73 % des variantes uniques de logiciels malveillants.

Grâce à sa technologie brevetée RTDMI™ (Real-Time Deep Memory Inspection), intégrée à son service de sandbox cloud Capture Advanced Threat Protection (ATP), SonicWall a découvert 307 516 variantes de malwares inédites au cours des trois premiers trimestres 2021. Cette découverte préoccupante signifie que les cybercriminels sortent en moyenne 1 126 nouvelles versions de malwares par jour.

L’augmentation du nombre de variantes doublée de l’activité accrue montre que « l’industrie des hackers » a appris à diversifier rapidement les logiciels utilisés pour attaquer réseaux et ordinateurs. Résultat : les entreprises, les gouvernements et les individus vont avoir de plus en plus de mal à se protéger. Les faiblesses en matière de sécurité démontrées par les attaques précédentes, associées à l’augmentation du MaaS/RaaS ont définitivement abouti à des menaces d’une toute nouvelle dimension.

❖ Se familiariser avec le nouveau paysage des menaces

Vu la vitesse à laquelle le paysage des menaces a évolué cette année, les opérateurs de réseaux de toute taille mènent une course contre la montre pour garder le pas sur la crise, en améliorant leur cybersécurité. Une gestion efficace des vulnérabilités doit être au cœur de toute mission allant dans ce sens.

Comment se protéger

Le service Cyber Sécurité d’Espace Technologie piloté par Jérôme, Expert en Cyber Sécurité, est dédié à la protection des S.I. de nos clients.

Nous proposons des solutions de haut niveau adaptées aux risques de nos clients.

Audit Cyber Sécurité
Tests d’intrusion
Capagne test Fishing
Maintenance préventive Cyber
Intervention après sinistre
Formation
Antivirus,
Anti Ramsomwares
Anti Spams
Firewall
NDR : Détection et réponse du réseau basé sur l'intelligence artificielle
Supervision par sonde
Sauvegardes déconnectées