Synthèse HP Wolf Security Threat Insight Report Q122

Emotet se hisse en tête des logiciels malveillants les plus détectés au premier trimestre 2022

Le dernier rapport Threat Insights de HP Wolf Security révèle une augmentation de 27 % de l'ensemble des menaces détectées, avec notamment une recrudescence des logiciels malveillants basés sur des scripts, de la contrebande HTML (HTML Smuggling) et des réinfections persistantes.

Meudon-sur-Seine, le 24 mai 2022 - L'équipe de recherche sur les cybermenaces HP Wolf Security a identifié, au premier trimestre 2022, une multiplication par 27 des détections du programme malveillant Emotet par rapport au dernier trimestre de 2021, date à laquelle Emotet était réapparu. Cette augmentation résulte des campagnes de spams effectuées, par ce dernier, en début d'année 2022. Le récent rapport mondial HP Wolf Security Threat Insights, qui analyse les cyberattaques en temps réel, indique que Emotet représente désormais la famille de logiciels malveillants la plus fréquemment détectée ce trimestre (9 % de tous les programmes malveillants détectés), et enregistre un bond de 36 places au classement. L'une de ces campagnes de cyberattaques visait notamment des organisations japonaises et consistait à détourner des fils de messagerie. Ils trompaient ainsi les destinataires et infectaient ainsi leur PC à leur insu. Elle a été en grande partie responsable de l'augmentation de 879 % des échantillons de logiciels malveillants de type .XLSM (Microsoft Excel) détectés par rapport au trimestre précédent.

En isolant les menaces qui ont échappé aux outils de détection et sont parvenues jusqu'aux terminaux des utilisateurs, HP Wolf Security parvient à dresser un tableau précis des toutes dernières techniques utilisées par les cybercriminels. Parmi elles, on y retrouve notamment :

- **Les détournements malveillants de documents Microsoft Office gagnent en popularité, tandis que les macros sont délaissés :** Microsoft ayant commencé à désactiver les macros, HP a constaté une augmentation des formats non-Microsoft Office, notamment des fichiers Java Archive (+476 %) et JavaScript (+42 %) malveillants par rapport au trimestre précédent. Les entreprises ont plus de mal à se défendre contre ces attaques, car il est compliqué de détecter ces types de fichiers, ce qui augmente les risques d'infection.

- **Selon les indicateurs, la contrebande HTML est en hausse :** la taille médiane des fichiers HTML est passée de 3 ko à 12 Ko, ce qui laisse penser que le recours à la contrebande HTML s'est accru. Cette technique consiste, pour les cybercriminels, à intégrer du code malveillant directement dans les fichiers HTML afin de contourner les passerelles de messagerie et d'échapper à la détection, avant de se frayer un chemin pour voler des informations financières essentielles. Des campagnes de ce type ont récemment ciblé des banques d'Amérique latine et d'Afrique.
- **Une campagne d'attaques « deux-en-un » à l'origine de plusieurs infections au malware RAT** : HP Wolf Security a observé qu'une attaque via script Visual Basic avait été utilisée pour déclencher une chaîne de frappe, laquelle a entraîné plusieurs infections sur le même appareil, offrant ainsi aux pirates un accès permanent aux systèmes de leurs victimes via des chevaux de Troie VW0rm, NjRAT et AsyncRAT.

« Nos données du premier trimestre révèlent que Emotet enregistre la plus forte activité depuis le démantèlement du groupe au début de l'année 2021, ce qui indique clairement que ses opérateurs se reforment, reconstituent leurs forces et investissent dans la croissance du botnet. Emotet a été décrit par la CISA (agence fédérale américaine pour la cybersécurité et la sécurité des infrastructures) comme l'un des programmes malveillants les plus destructeurs et les plus coûteux à éliminer. Ceux qui l'opèrent collaborent souvent avec des groupes de cyber-extorsion (ransomware), une tendance qui devrait se poursuivre. Leur réapparition est donc une mauvaise nouvelle pour les entreprises comme pour le secteur public », explique Alex Holland, Senior Malware Analyst, HP Wolf Security, HP Inc. *« Emotet continue également de fournir un terreau favorable aux attaques par macros, peut-être dans une sorte de baroud d'honneur avant le blocage de ces dernières par Microsoft en avril, ou simplement parce que les utilisateurs ont toujours des macros activées chez eux et qu'il reste possible de les pousser à cliquer là où il ne faut pas. »*

Les résultats sont tirés de données issues de plusieurs millions d'ordinateurs utilisant HP Wolf Security. HP Wolf Security traque les programmes malveillants en ouvrant les tâches à risque dans des micro-machines virtuelles (ou micro-VM) isolées, afin de protéger l'utilisateur, de comprendre et capturer l'ensemble de la chaîne de la tentative d'infection, atténuant ainsi les menaces qui ont échappé aux autres outils de sécurité. À ce jour, les clients de HP ont cliqué sur plus de 18 milliards de pièces jointes, pages Web et téléchargements sans qu'aucune faille de sécurité ne soit signalée[1]. Ces données fournissent des informations précieuses sur la façon dont les cybercriminels utilisent les logiciels malveillants dans les situations réelles.

Quelques autres enseignements de ce rapport :

- 9 % des cybermenaces n'avaient jamais été observées au moment où elles ont été isolées, et 14 % des e-mails malveillants ont contourné au moins un scanner de passerelle de messagerie.
- Il a fallu aux autres outils de sécurité plus de 3 jours (79 heures) de contrôle de hachages, en moyenne, pour les identifier.

- 45 % des programmes malveillants isolés par HP Wolf Security étaient des formats de fichiers Office.
- Les pirates ont utilisé 545 familles de logiciels malveillants différentes dans leurs tentatives d'infecter des organisations. Emotet, AgentTesla et Nemucod composent le trio de tête.
- Un exploit réalisé via Microsoft Equation Editor (CVE-2017-11882) représente 18 % de tous les échantillons malveillants capturés.
- 69 % des programmes malveillants détectés ont été transmis par e-mail, et 18 % téléchargés sur Internet.
- Les pièces jointes les plus couramment utilisées pour diffuser des programmes malveillants sont les feuilles de calcul (33 %), les fichiers exécutables et scripts (29 %), les archives (22 %), et les documents (11 %).
- Les appâts les plus couramment utilisés dans les attaques par hameçonnage ont été les transactions commerciales (« Commande », « Paiement », « Achat », « Demande » et « Facture », par exemple).

« Ce trimestre, nous avons constaté une augmentation significative de 27 % du volume des cybermenaces détectées par HP Wolf Security. À mesure que les cybercriminels affinent leurs approches en réaction à l'évolution du paysage informatique, le volume et la variété des attaques continuent d'augmenter, et il devient de plus en plus difficile pour les outils conventionnels de détecter ces attaques », commente le Dr Ian Pratt, Global Head of Security for Personal Systems, chez HP. *« Pour faire face à l'augmentation des types de fichiers et des techniques utilisées pour contourner la détection, les entreprises doivent changer de cap et adopter une approche à plusieurs niveaux en matière de sécurité des terminaux. En appliquant le principe du moindre privilège et en isolant les vecteurs d'attaques les plus courants (e-mails, navigateurs ou téléchargements), elles peuvent neutraliser les programmes malveillants diffusés par ces vecteurs. Cela réduit considérablement leur exposition aux cybermenaces. »*

L'équipe de HP Wolf Security discutera du rapport Threat Insights pour le premier trimestre 2022 lors d'un webinaire d'information qui se tiendra le 7 juin à 8 h (heure du Pacifique). Cliquez ici pour en savoir plus.

À propos des données

Ces données ont été recueillies de manière anonyme sur les machines virtuelles des clients de HP Wolf Security entre janvier et mars 2022.

A propos de HP

HP Inc. développe des technologies pour améliorer la vie de chacun, chaque jour, partout dans le monde. Grâce à nos solutions d'impression, nos systèmes personnels et nos services associés, nous créons des expériences d'exception. http://www.hp.fr

À propos de HP Wolf Security

Conçu par le fabricant de PC et imprimantes les plus sécurisés au monde, HP Wolf Security est une offre innovante pour assurer la sécurité des terminaux. Ce portfolio comprend la sécurité intégrée au matériel et des services de sécurité axés sur les terminaux. Il est conçu pour aider les entreprises à protéger les PC, les imprimantes et les personnes contre les cyberprédateurs. HP Wolf Security offre une protection complète et une résilience des terminaux, tant au niveau du matériel que des logiciels et services. Plus d'informations sur hp.com/fr/wolf

HP WOLF SECURITY

[1] Hypothèses fondées sur l'analyse interne par HP des informations fournies par les clients et la base installée.