AOÛT 2021

Rapport sur le panorama mondial des menaces

Un rapport semestriel de FortiGuard Labs

TABLE DES MATIÈRES

Synthèse et temps forts

Dans l'univers de la cybersécurité, chaque année semble se caractériser par un élément ou évènement majeur. Et il semblerait bien que 2021 soit "l'année des alertes." Certes, 2020 mériterait également ce sobriquet, et il aura sans doute fallu attendre une année pour que les alertes émises l'an dernier ne se concrétisent sur le terrain. Les six premiers mois de 2021 ont ainsi connu des attaques récurrentes et de grande ampleur qui ont impacté de nombreuses organisations et d'innombrables individus. Nous en avons étudié les conséquences et tenté d'en tirer des leçons qui, nous l'espérons, vous permettront d'anticiper les prochaines risques majeurs à venir.

ProxyLogon sous le feu des attaques

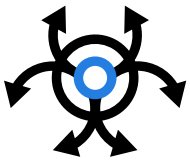
Hafnium, un groupuscule basé en Chine, s'en est pris à des milliers d'organisations en ciblant quatre vulnérabilités de Microsoft Exchange Server, connues conjointement sous l'appellation ProxyLogon, et ce, plusieurs mois avant la disponibilité de patchs. Un exemple suivi par d'autres groupes ayant senti la bonne affaire. Il n'est ainsi guère surprenant que nos capteurs aient identifié une forte croissance des activités liées et nous vous invitons à en savoir plus en consultant notre étude de cas.

La vague des ransomware

La ransomware s'était déjà montré virulent en 2020 et cette tendance n'a guère fléchi, avec un volume multiplié par 10,7 en 12 mois. Le malware est devenu bien plus prévalent et nocif. Les attaques ayant paralysé l'activité d'entreprises comme Colonial Pipeline et JBS semblent être des signes avant-coureurs de la montée en puissance de gangs spécialisés dans le ransomware et qui vont peser davantage sur nos vies au quotidien. Découvrez nos perspectives sur ces tendances et leurs orientations.

L'OT n'évolue plus à l'ombre de l'IT

L'informatique industrielle OT (Operational Technology) n'attire pas le même niveau d'attention que l'IT, mais son interconnexion au monde physique souligne un impact potentiellement important sur nos vies quotidiennes. 2021 nous le rappelle au travers des ransomware et autres attaques ciblant les environnements industriels. Nous analysons les exploits détectés qui ciblent les systèmes de contrôle industriel (ICS) et témoignent que l'OT est bien plus ciblé par les assaillants qu'on ne l'imagine.



Démantèlement d'Emotet et autres succès des forces de l'ordre

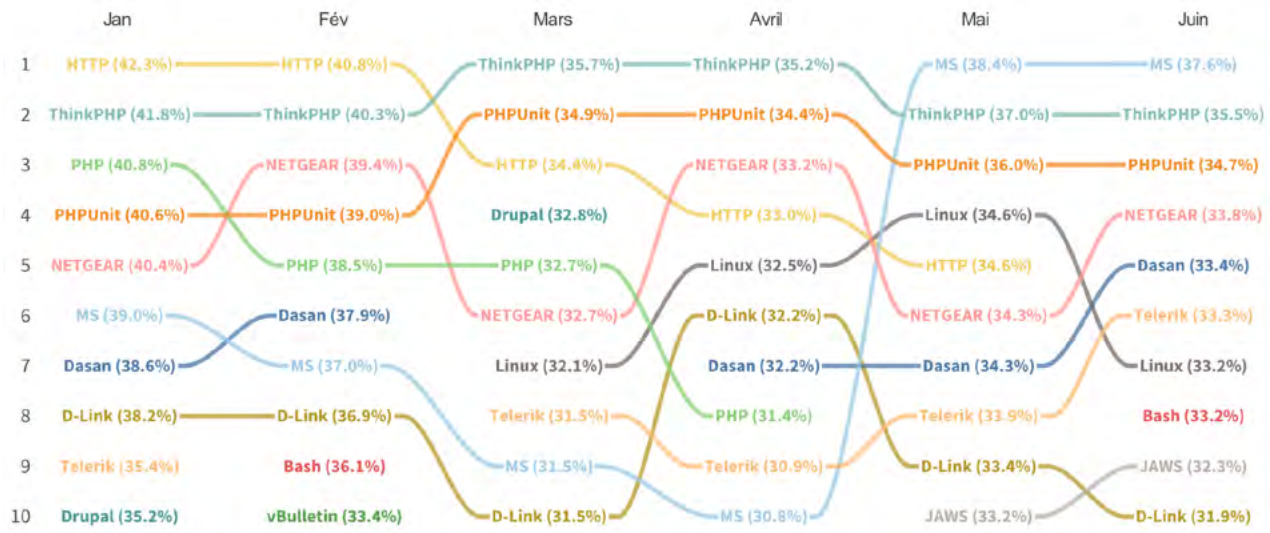
La cybersécurité se joue sur le long terme et seules quelques actions ont un effet immédiat et durable. C'est la raison pour laquelle nous pouvons savourer les petites victoires dans notre combat quotidien. Le démantèlement coordonné d'Emotet, une des opérations les plus prolifiques des dernières années, ainsi que les actions entreprises pour perturber l'activité des ransomware Egregor, NetWalker et Cl0p, constituent des étapes majeures pour les organisations gouvernementales et les forces de l'ordre dans leur lutte contre la cybercriminalité. Nous sommes heureux de contribuer à ces actions que nous vous invitons à découvrir.

Principales menaces sur le premier semestre 2021

Ce rapport reflète les travaux de veille des FortiGuard Labs, basés sur un large panel de capteurs réseau recueillant des milliards d'évènements par jour sur les menaces en environnement de production dans le monde. Selon une étude indépendante,[1] Fortinet dispose du parc de dispositifs de sécurité le plus important du secteur, ce qui concrétise une visibilité de bout en bout sur l'univers des menaces et des perspectives que nous partageons avec vous. Nous démarrons par un examen des menaces les plus prévalentes sur les six premiers mois de 2021.

Détections par IPS

MITRE ATT&CK s'est imposé en tant que framework pertinent pour étudier les tactiques, techniques et procédures (TTP) des attaques. Les trois premiers groupes de TTP dans ATT&CK couvrent la reconnaissance, le développement de ressources et l'accès initial. Ils décrivent comment les assaillants identifient les vulnérabilités, élaborent des infrastructures malveillantes et s'en prennent à leurs cibles. Nos capteurs du système de prévention FortiGuard (IPS), disponibles sur nos pare-feu FortiGate, offrent une excellente visibilité au cœur de ce type d'activité dans le monde, ces capteurs étant souvent positionnés pour être le premier point de contact avec un adversaire qui cherche à identifier des vulnérabilités.



Graphique 1 : prévalence des détections IPS par technologie sur S1 2021

Le graphique 1 présente les technologies le plus souvent ciblées au cours du premier semestre de 2021. De manière générale, les détections IPS reflètent des cibles identifiées depuis déjà quelque temps : serveurs, systèmes de gestion des contenus et objets connectés. Nous y reviendrons plus tard dans cet ouvrage. L'entête de signature HTTP, qui est la cible N°1 en janvier et février, reste une notion vague, mais qui englobe une longue liste d'exploits ciblant les serveurs web. Pour donner quelques exemples concrets, les détections par IPS les plus nombreuses portent sur HTTP.Server.Authorization.Buffer.Overflow et HTTP.URI.Java.Code.Injection, tandis que HTTP.Header.SQL.Injection et HTTP.URI.SQL.injection ont été détectés par le plus grand nombre d'organisations.

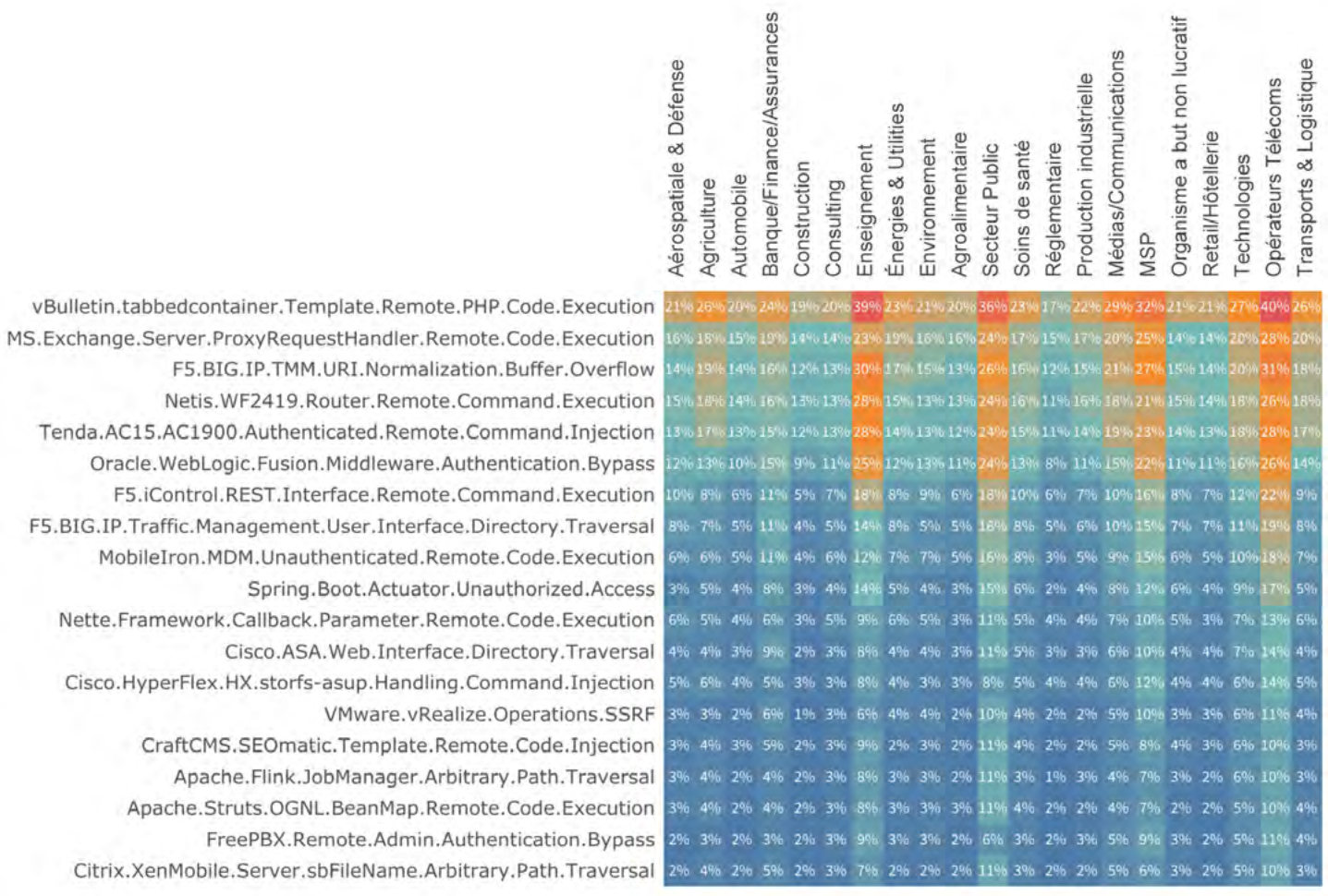
En matière d'exploits ciblant les serveurs web et d'entreprise, Microsoft et Linux sont régulièrement cités dans le graphique 1, ce qui n'est guère surprenant compte tenu de la prévalence de ces plateformes. La signature principale associée à la croissance des détections en environnement Linux depuis mars est liée à une vulnérabilité qui permet à un assaillant de manipuler à distance le kernel des systèmes dans l'optique de les mettre à l'arrêt. Microsoft ressort en première place en mai et juin, le résultat d'une longue liste de signatures. Une des signatures les plus prévalentes est associée à des tentatives d'exploiter une vulnérabilité permettant l'exécution à distance d'un code logiciel dans Microsoft Exchange Server. Nous y reviendrons dans une de nos études de cas.

Les exploits ciblant ThinkPHP, un CMS basé sur PHP, comptent parmi les plus courantes sur les mois étudiés. D'autres CMS (Drupal, vBulletin) et leurs frameworks de développement (PHPUnit) figurent dans le top 10 mensuel. Les CMS sont des cibles privilégiées par des cybercriminels opportunistes. Ces systèmes sont conçus pour simplifier la gestion des contenus web, mais représentent une menace majeure en cas d'intrusion malveillante. Si votre entreprise dispose d'un CMS, il devient essentiel de déployer les patchs nécessaires.

Les détections par IPS les plus courantes portent sur différents exemples de réseaux et de dispositifs IoT particulièrement ciblés, notamment ceux de Netgear, D-Link, Dasan et JAWS. Ces équipements, essentiellement destinés aux petites entreprises ou au grand public, s'inscrivent dans une tendance que nous avions déjà identifiée dans nos prédictions de sécurité pour 2021. La migration vers le travail à distance et à domicile a incité les cybercriminels à se pencher sur les dispositifs présents au sein de ces nouveaux environnements de télétravail. Cette attractivité est liée au fait que ces dispositifs stockent de nombreuses informations à propos des utilisateurs et de leurs activités en ligne, des informations qui permettraient aux assaillants de mener des actions frauduleuses et des campagnes d'ingénierie sociale.

Un autre risque pesant sur la sécurité des entreprises est lié aux attaques potentiellement menées depuis le réseau résidentiel d'un télétravailleur. Il suffit de dénombrer le nombre de dispositifs présents entre un collaborateur travaillant à domicile et les données et applications d'entreprise auxquelles il accède dans le cadre de son travail. De nombreuses possibilités s'offrent ainsi aux assaillants qui parviendraient à pirater ces dispositifs. Et ces assaillants en ont conscience.

Dans leur majorité, les exploits mentionnés dans le graphique 1 ne datent pas d'hier. Il faut en effet un certain temps pour gagner en prévalence. Mais quid des nouveaux exploits ? Pour les prendre en compte, le graphique 2 a modifié l'algorithme



Graphique 2 : prévalence des nouvelles (- de 12 mois) détections IPS sur S1 2021

pour se focaliser sur les nouveaux exploits ayant le vent en poupe et pour lesquels nous avons conçu des signatures IPS au cours de l'année passée. Ce graphique compare également les niveaux de détection entre différents secteurs d'activité.

Nous savons qu'un terme comme IPS.Signature.Naming.Schema est quelque peu abscons, mais il est possible d'en savoir plus sur tout ce qui est présenté dans le graphique 2 dans notre Encyclopédie des menaces. Ce tableau restitue les nouveaux exploits détectés par des entreprises similaires à la vôtre.

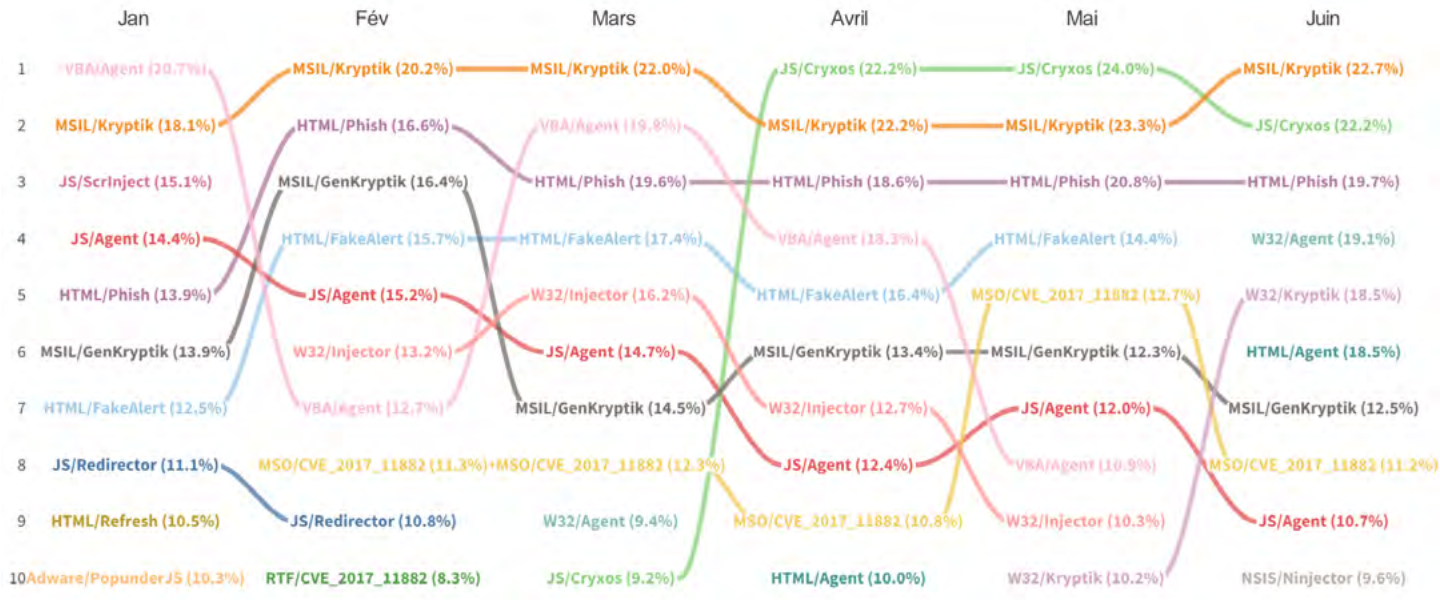
Le graphique 2 indique clairement que certains secteurs subissent un niveau plus élevé d'activité pour les exploits. Les secteurs de l'enseignement, des fournisseurs de services managés de sécurité et des télécommunications sont les plus ciblés, avec une prévalence de deux à trois fois plus importante que pour les autres secteurs d'activité. Les entreprises dans ces secteurs ont tendance à disposer de très nombreux dispositifs et à gérer différentes entités (implantations locales pour les administrations ou clients pour les MSSP/opérateurs). Et certaines d'entre elles, notamment dans le secteur de l'enseignement, contrôlent la sécurité et l'usage de ces dispositifs de manière aléatoire.

Au-delà, les secteurs qui subissent le plus d'exploits (institutions financières, acteurs de la technologie, etc.) sont ceux attendus. La présence du secteur agricole peut étonner. Mais puisque l'agriculture est devenue dépendante de la technologie, ces résultats font du sens. Une ferme moderne, ou tout autre site agricole, est susceptible d'héberger un grand nombre de dispositifs IoT, chacun d'entre eux avec ses propres connexions et vulnérabilités. Autant d'opportunités pour les cybercriminels.

Détections de malware

Les échantillons détectés par nos multiples solutions anti-malware offrent une visibilité sur les techniques populaires utilisées pour s'immiscer au cœur des environnements corporate. Dans le contexte du framework ATT&CK, cette activité est corrélée avec la phase d'Exécution au cours de laquelle les assaillants tentent de déployer et d'exécuter un malware sur les systèmes ciblés.

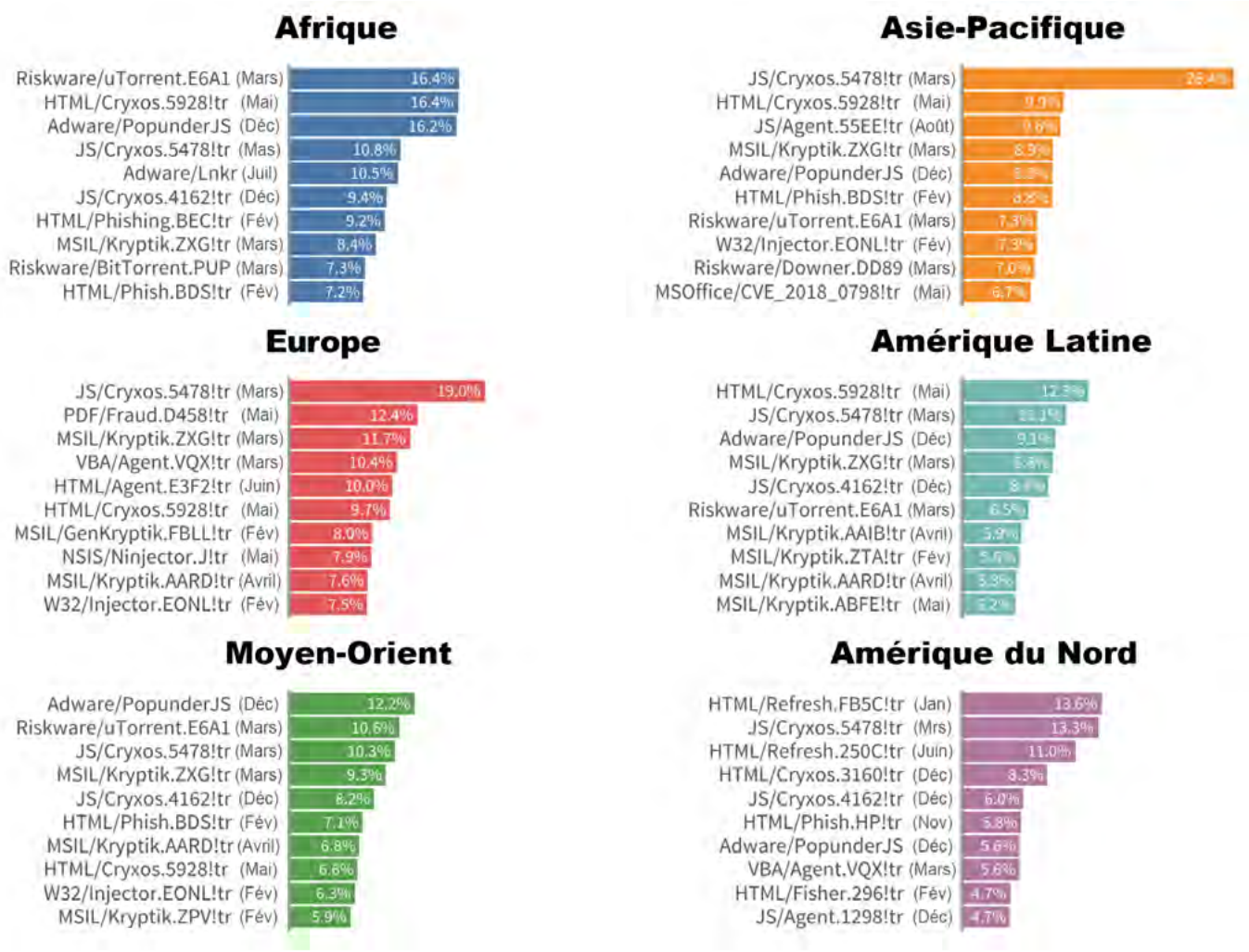
Dans le graphique 3, nous avons choisi de regrouper les malware par famille, plutôt que par variante spécifique. Notre objectif est de regrouper les multiples variantes, à durée de vie courte, pour éviter de rentrer dans le détail et disposer d'une visibilité globale pertinente. Le graphique 4 présente une vue détaillée des nouvelles variantes qui se propagent dans le monde.



Graphique 3 : prévalence des détections de malware par famille sur S1 2021

Du point de vue du critère des attaques, les familles et les variantes présentées dans les deux tableaux peuvent être regroupées selon deux méthodes de distribution : plateformes Microsoft et navigateurs web. Les plateformes Microsoft sont des vecteurs pour des malware de type exécutables pour Windows 32-bit., fichiers malveillants VBA et Office, ou utilisant .NET ou le langage MSIL (Microsoft Intermediate Language). Les malware exploitant les navigateurs web se voient souvent attribuer le préfixe HTML ou Javascript (JS). Ils prennent la forme de campagnes malveillantes associées au phishing et de scripts qui injectent du code et redirigent les utilisateurs vers des sites malveillants. De telles techniques ont récemment gagné en popularité, en réponse au besoin d'informations du grand public durant la pandémie de COVID-19 et de la migration vers le télétravail, en dehors du périmètre protégé par les filtres web corporate.

Le classement des principaux malware détectés selon leur prévalence reflète une recrudescence des techniques d'ingénierie sociale, basé sur du malvertising et du scareware utilisant javascript. De telles techniques sont généralement associées à des notifications prétendument émises par l'équipe de support de Microsoft. Dans un scénario classique, les utilisateurs reçoivent un message (pop-up de navigateur par exemple) qui indique que leur dispositif est infecté ou piraté. L'utilisateur est incité à contacter l'équipe support pour régler le problème moyennant finances ou pour leur accorder un accès distant. De manière générale, plus d'une entreprise sur 4 a détecté des tentatives de malvertising ou de scareware sur le premier semestre 2021.



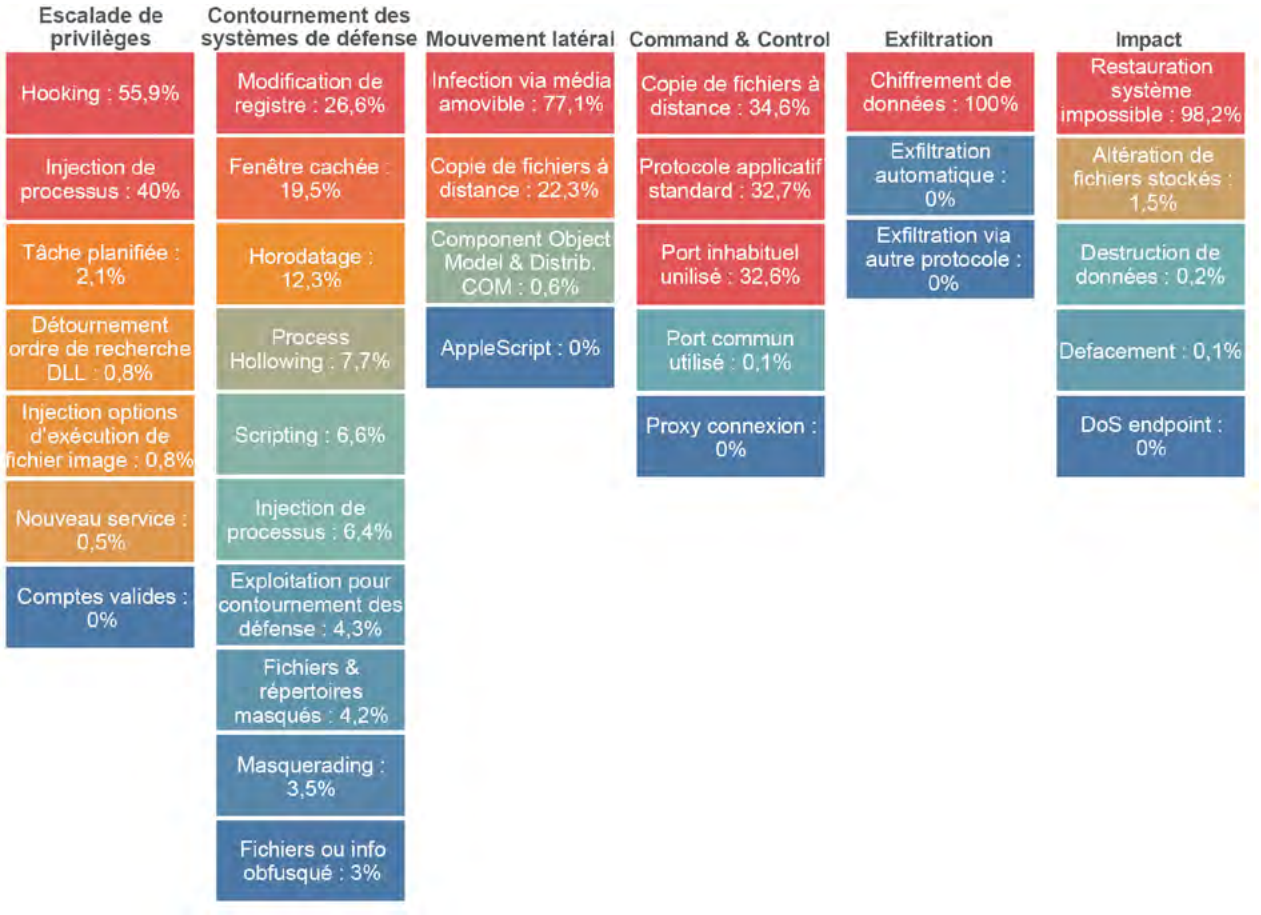
Graphique 4 : prévalence des nouveaux malware (- de 12 mois) par région sur S1 2021

Le malvertising n'est ni une nouvelle tactique, ni la forme de malware la plus dangereuse. Le télétravail a indubitablement contribué à sa montée en puissance. Avec autant de collaborateurs opérant hors du périmètre corporate sécurisé et éloignés des équipes informatiques présentes au bureau, les collaborateurs sont plus isolés que jamais. Ceci est un nouvel exemple de comment les cybercriminels adaptent leurs outils existants à des conditions qui évoluent.

Tactiques, techniques et procédures (TTP) des malware

En identifiant les malware actifs sur les six premiers mois de l'année, nous souhaitions aller plus loin pour étudier leurs fonctionnalités spécifiques. Pour cela, il s'agit d'exécuter chaque malware et d'observer son mode opératoire. C'est ce que nous présentons dans le graphique 5.

Ce graphique 5 illustre les TTP ATT&CK de chaque malware analysé par le service FortiSandbox Cloud. De quoi identifier toutes les exactions que ces malware auraient pu commettre s'ils avaient été exécutés au sein d'un environnement réel. Il s'agit notamment de s'octroyer des privilèges plus élevés, de contourner la ligne de défense en place, de se propager en interne, d'établir des communications command and control, d'exfiltrer des données compromises et de concrétiser l'impact attendu.



Graphique 5 : fréquence relative des TTP de malware, tels qu'observés par Fortinet sur S1 2021

Les pourcentages indiqués dans le tableau sont basés sur la fréquence de chaque technique associée aux tactiques les plus utilisées. Ainsi, 55 % des tentatives d'escalade de privilège utilisent la technique de hooking, 40 % font appel à l'injection de processus, etc. Ainsi, ce sont les tactiques de contournement et d'escalade de privilèges qui sont les plus utilisées. Ces tactiques ne sont pas nouvelles mais certaines d'entre elles exigent d'intervenir au niveau du kernel pour comprendre comment le processus malveillant interagit avec le cœur du système d'exploitation pour requérir des ressources. Il devient essentiel d'inspecter ces interactions pour intercepter les menaces avancées susceptibles de percer la ligne de défense traditionnelle en place. C'est d'ailleurs précisément ce qui s'est passé dans des attaques comme celles autour de ProxyLogon.

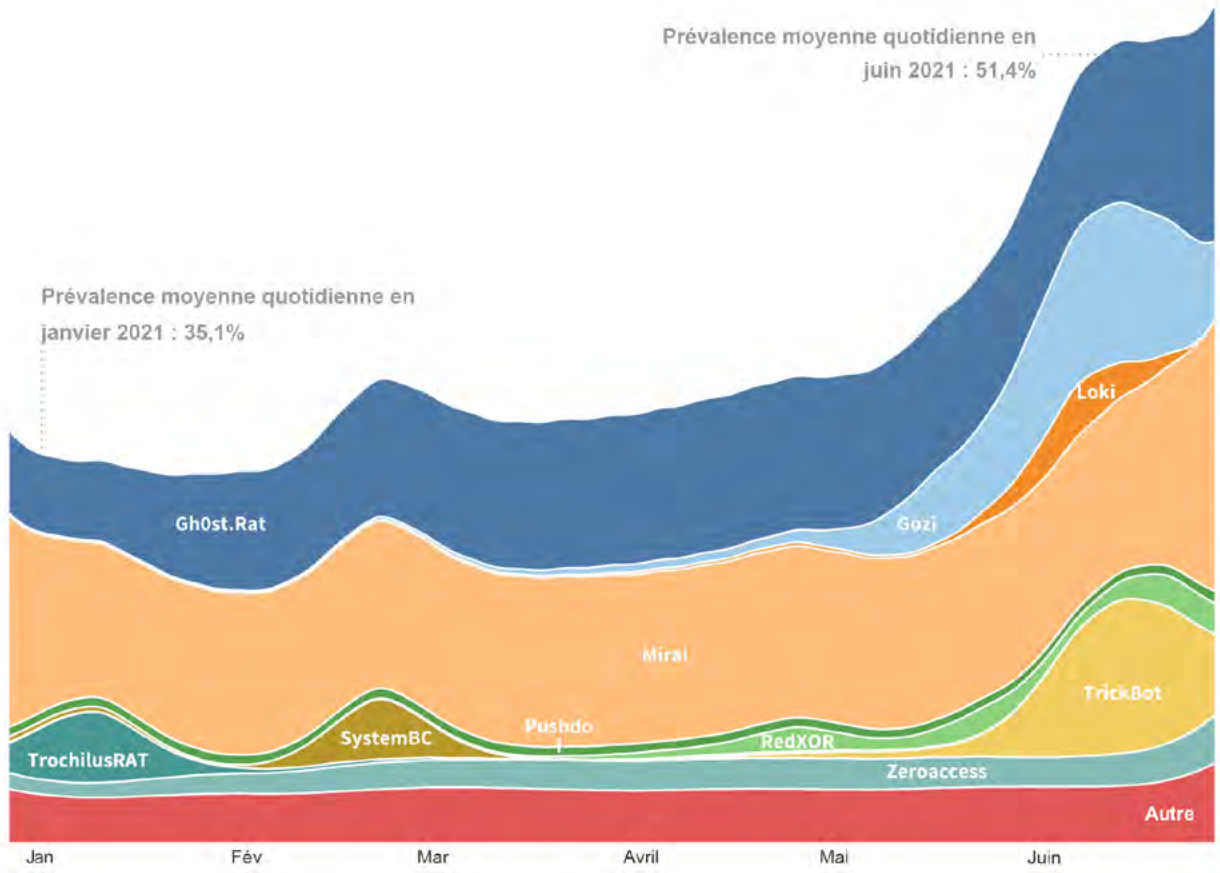
Nous avons ainsi vu des groupes APT tirer parti de vulnérabilités zero-day pour infiltrer les réseaux. Ainsi, identifier un tel processus, avant tout impact sur un système en production, pour ensuite le neutraliser, est essentiel pour interrompre l'exécution des étapes ultérieures de la chaîne de frappe. Ceci est rendu plus simple lorsque vous connaissez les techniques spécifiques les plus courantes chez les cybercriminels. Cette information peut être utilisée pour adapter l'arsenal de défense.

FortiGuard Labs contribue activement au Center for Threat-Informed Defense du framework MITRE, au travers de projets comme le Sightings Ecosystem. Ceci rentre dans le cadre de nos multiples collaborations avec des partenaires du secteur pour vous apporter des renseignements de qualité et améliorer votre sécurité.

Détection de botnets

Alors que l'IPS et les tendances de malware révèlent ce qui se passe en amont d'une compromission, les botnets, de leur côté, offrent une visibilité sur les activités malveillantes post-compromission. Dans un contexte ATT&CK, ceci est associé à des techniques relevant de la tactique Command and Control, lorsque des systèmes infectés communiquent avec des hôtes distants malveillants. Le graphique 6 présente les principaux bots sur le premier semestre 2021.

Dans un premier temps, il s'agit d'interpréter la présence de ces bots. La hauteur des courbes colorées est liée au nombre d'entreprises ayant détecté une activité associée à chaque botnet. Les botnets détectés mais non mentionnés dans le graphique sont répertoriés dans la catégorie « Autres ». On constate que la Loi de Pareto s'applique aux botnets : 80 % de l'activité est liée aux 10 botnets les plus prévalents. C'est la raison pour laquelle le démantèlement des principaux botnets constitue une stratégie efficace contre les cybermenaces. Le démantèlement du botnet Emotet fait l'objet d'une de nos études de cas.



Graphique 6 : prévalence des détections de malware sur S1 2021

Nous constatons également dans le graphique 6 une forte recrudescence d'activité vers la fin du semestre. En début d'année, 35 % des entreprises avaient détecté une activité de botnet. Six mois plus tard, ce chiffre bondit à 51 %. Un tel niveau d'activité, qui est peu commun, mérite une analyse plus fine.

Mirai, le botnet le plus commun, a surperformé Gh0st au début de 2020 et règne en maître depuis. Mirai s'est fait connaître il y a quelques années suite à ses multiples attaques DDoS sur des objets connectés. Depuis lors, ce botnet a intégré de nouvelles armes pour assurer son leadership (exemple 1 et 2). Il est probable que la domination de Mirai soit partiellement liée à des cybercriminels cherchant à exploiter les dispositifs IoT utilisés par des télétravailleurs, ou à proximité d'eux.

Gh0st est également actif sur la période, ce qui est déjà le cas depuis plusieurs années. Ce botnet d'accès distant permet aux assaillants de prendre le total contrôle des systèmes infectés, d'enregistrer les frappes au clavier, de détourner des flux en direct de webcam ou de microphone ou encore de télécharger des fichiers.

Notons également que les autres botnets présentés dans le graphique 6 ne figuraient pas dans le top 10 précédemment. Le regain de prévalence vers la fin du semestre démontre que ces nouveaux arrivants ont contribué à la forte croissance de l'activité des botnets.

Les communications avec le botnet Trochilus ont progressé en début d'année, notamment sur les zones Océanie et Asie du Sud-est. Dans le passé, le cheval de troie Trochilus a été utilisé à escient par des groupuscules chinois d'espionnage lors d'opérations ciblant ces régions (voir graphique 7).

	Afrique	Asie	Europe	Amérique Latine	Moyen-Orient	Amérique du Nord	Océanie
TrickBot	50.0%	41.3%	66.8%	48.6%	40.9%	64.1%	66.4%
Gh0st.Rat	61.8%	61.4%	65.2%	61.4%	56.6%	71.9%	70.5%
TrochilusRAT	41.0%	38.7%	46.4%	42.5%	38.7%	51.5%	54.4%
Necurs	6.2%	4.0%	2.5%	2.9%	4.1%	3.8%	3.8%
Sality	12.9%	13.7%	3.0%	6.2%	18.2%	3.1%	3.3%
RedXOR	11.6%	12.3%	10.8%	20.5%	11.1%	7.9%	8.6%
Nymaim	0.4%	5.7%	0.3%	0.1%	0.1%	0.2%	0.4%

Graphique 7 : prévalence of botnets présentant des variations régionales importantes sur S1 2021.

SystemBC, en troisième position en février (graphique 6), est un cheval de troie utilisé par plusieurs campagnes de ransomware. Sa popularité s'explique par la présence d'une backdoor persistante avec chiffrement TLS et par la possibilité d'établir des communications Command & Control. Les assaillants ont repensé leur stratégie, en s'éloignant des attaques menées par email, et en y substituant la revente "d'accès initiaux" piratés dans le cadre de leurs exactions. SystemBC s'inscrit dans cette tendance.

Le regain d'activité de TrickBot vers la fin du semestre, comme le souligne le graphique 6, est en grande partie responsable de la forte progression des botnets en juin. TrickBot a émergé sur la scène de la cybercriminalité en tant que cheval de troie bancaire. Depuis, il s'est transformé en un toolkit sophistiqué, modulaire et séquencé qui contribue à de nombreuses activités illicites. Le CISA (Cybersecurity & Infrastructure Security Agency) a émis une alerte en mai indiquant une montée en puissance des campagnes de spear phishing utilisant TrickBot. Rappel que les cybercriminels ne sont pas toujours impunis, le développeur à l'origine de TrickBot a été inculpé de plusieurs chefs d'accusation en juin.

Loki a également connu une forte progression de son activité en juin (graphique 6). Fin 2020, le CISA émettait une alerte sur la progression de ce malware. Nous ne disposons pas d'informations concernant des campagnes nouvelles ou spécifiques à l'origine de cette progression, mais nous suivons plus que jamais de près ce malware. Pour connaître ce qui attire le plus notre attention, nous vous avons préparé des études de cas sur les six premiers mois de l'année.

Cas d'école

ProxyLogon sous le feu des attaques

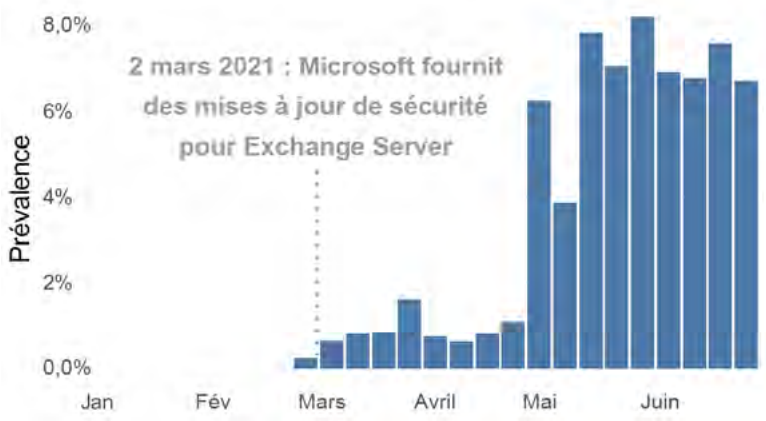
Quatre vulnérabilités de Microsoft Exchange Server ont constitué une préoccupation majeure au premier semestre 2021, compte tenu du nombre de systèmes impactés et de l'exploitation active de ces défauts par les assaillants en amont de la disponibilité des patchs de Microsoft le 2 mars. Ces vulnérabilités, nommées ProxyLogon, ont constitué une réelle menace pour les entreprises disposant de serveurs Exchange directement connectés à Internet et acceptant des connexions externes n'étant pas de confiance. Certains éditeurs ont ainsi identifié que plus de 30 % des incidents détectés au printemps 2021 étaient liés aux vulnérabilités des serveurs Exchange.

Les vulnérabilités identifiées étaient les suivantes : CVE-2021-26855, une problématique SSRF (Server-Side Request Forgery) pouvant permettre un contournement de l'authentification, CVE-2021-26857, une vulnérabilité basée sur une faiblesse de la désérialisation permettant une escalade de privilèges, ainsi que CVE-2021-26858 et CVE-2021-27065, deux vulnérabilités d'écriture de fichier arbitraire après authentification. Lorsque associées, ces 4 vulnérabilités permettent à des assaillants d'exécuter un code malveillant à distance sur des serveurs Exchange pour y déployer des backdoors.

'Hafnium', un groupuscule chinois spécialisé dans les menaces APT (advanced persistent threat) s'en est pris à plus de 30 000 entreprises américaines en exploitant les vulnérabilités de Microsoft, avant leur correction par des patchs officiels. Les premiers exploits ont été identifiées en janvier, soit deux mois avant la disponibilité du patch. Des think thanks, des entreprises du secteur de la défense, des cabinets juridiques, des ONG et des acteurs de la recherche sur les maladies infectieuses ont ainsi été ciblés sur le sol américain. Suite à la divulgation de ces vulnérabilités par Microsoft, d'autres groupes cybercriminels liés à un état et des hackers opportunistes ont commencé à les exploiter. Parmi les assaillants, notons le chinois Barium (ou APT 41), un organisme malveillant déjà identifié par Fortinet comme l'auteur de piratages de chaînes collaboratives ou d'attaques sur des éditeurs de logiciel.

Ces attaques ont donné lieu à des alertes urgentes de la part du CISA, de Microsoft et de nombreux acteurs de la sécurité. La menace était si préoccupante qu'en avril, le FBI a mené une opération sans précédent pour supprimer les webshells malveillants installés par les assaillants sur des centaines de serveurs Exchange aux États-Unis.

Fortinet a traqué ces cybercriminels qui utilisaient différents outils de malware contre ces vulnérabilités, parmi lesquels le coin miner Lemon Duck, le ransomware BlackKingdom, le botnet Prometei, ainsi que 'China Chopper', un webshell léger qui existe depuis au moins 2012 et capable d'établir un accès backdoor sur un système compromis. Les détections IPS de Fortinet liées aux vulnérabilités Exchange Server (voir graphique 8) témoignent que les assaillants ont exploité ces vulnérabilités dans le monde entier, mais principalement en Europe. La Turquie, les États-Unis et l'Italie seraient les trois pays les plus ciblés. Nous avons constaté un niveau particulièrement élevé d'activité liée à CVE-2021-26855, la vulnérabilité SSRF qui a donné aux assaillants un accès initial à des serveurs Exchange vulnérables.

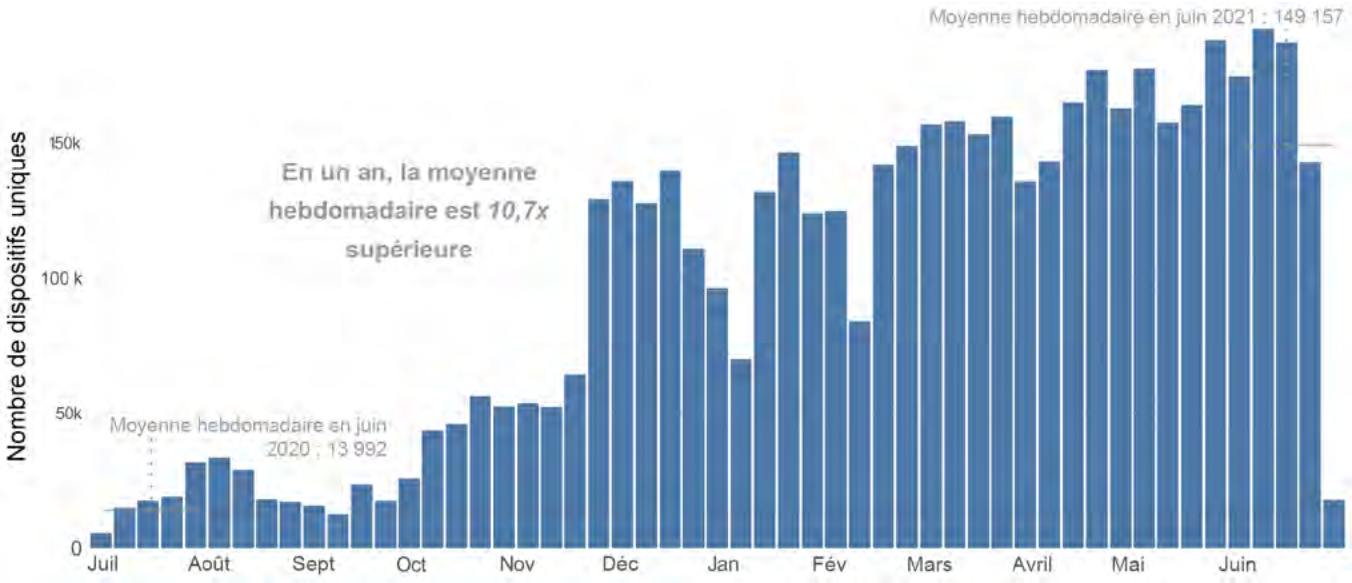


Graphique 8 : exploits des vulnérabilités ProxyLogon d'Exchange Server sur S1 2021.

Pour les équipes de sécurité, ces attaques sont un rappel que les vulnérabilités des technologies utilisées à grande échelle (spécialement l'email) continuent à attirer les cybercriminels. Dans le cas présent, les vulnérabilités ont été exploitées initialement à des fins de cyber-espionnage, par un groupuscule soutenu par un état. Mais après disponibilité des patchs, les assaillants ont utilisé ces vulnérabilités pour mener d'autres types d'attaque, soulignant ainsi à nouveau le besoin d'installer rapidement les patchs et de disposer d'une sécurité en profondeur.

La vague des ransomware

Le ransomware a continué à lourdement peser sur les entreprises dans le monde lors du premier semestre 2021. Nous n'avons cependant pas constaté de progression fulgurante des attaques comme sur le second semestre 2020. Pour autant, le niveau d'activité des ransomware est resté élevé tout au long de l'année. L'activité moyenne hebdomadaire du ransomware en juin 2021 était 10,7 fois plus élevée qu'une année auparavant (graphique 9). De plus, contrairement à l'idée reçue, le ransomware représente une menace pour de nombreux secteurs d'activité, et pas seulement les soins de santé, le service public ou l'enseignement (graphique 10).

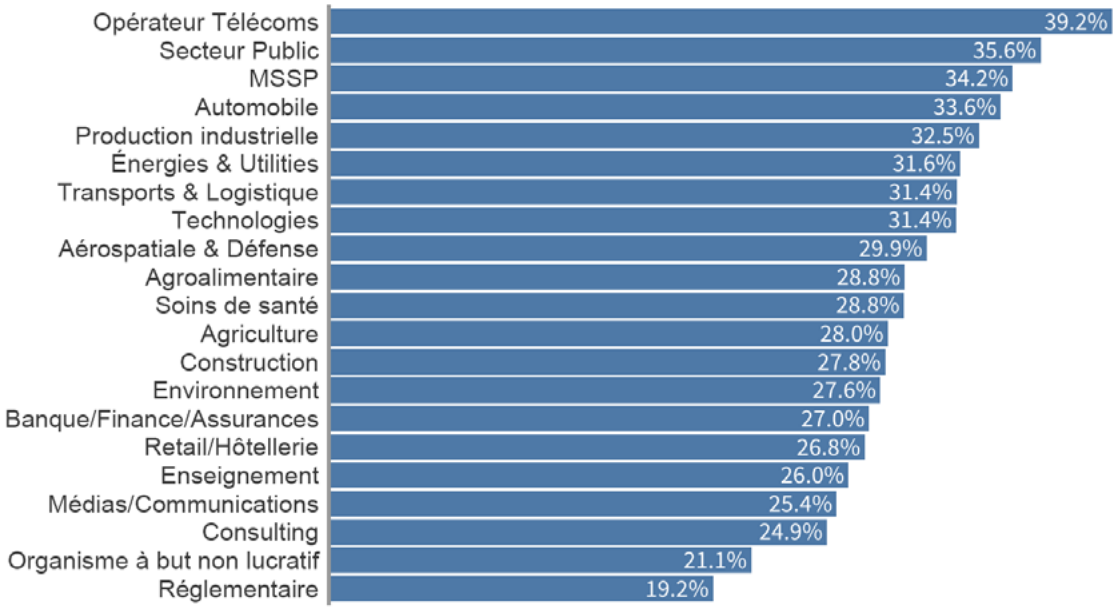


Graphique 9 : croissance des détections de ransomware sur les 12 derniers mois (07/20 - 06/21)

Notons que les réseaux OT et des secteurs d'importance vitale ont été la cible d'attaques cette année. À l'image de celle en mai sur Colonial Pipeline qui a très fortement perturbé la fourniture de carburant sur une grande partie de la côte est des États-Unis. Colonial Pipeline a réglé la somme de $4,4 millions à DarkSide, l'opérateur russe à l'origine de l'attaque, pour pouvoir reprendre la main sur ses pipelines. Une autre attaque, également en mai, a ciblé JBS, géant mondial de la transformation de la viande, avec de fortes perturbations dans la distribution de viande sur les États-Unis. JBS a réglé $11 millions aux assaillants pour résoudre cette problématique.

Ces deux incidents majeurs ont fait du ransomware une préoccupation majeure et d'intérêt national aux États-Unis. Ils ont incité le département de la justice américaine à se pencher sur l'intérêt d'attribuer à de telles attaques le même niveau de priorité qu'à des attaques terroristes. La préoccupation engendrée par ces attaques au plus haut niveau du gouvernement américain a sans doute incité certains opérateurs de ransomware (DarkSide, Avaddon et Ziggy) à annoncer la fin de leurs activités.

En janvier, Fortinet a identifié une nouvelle variante de ransomware, DarkWorld. Ce malware, codé en .NET, présente 10 menaces par chiffrement et utilise l'algorithme de chiffrement(AES) Rijndael pour verrouiller les fichiers des victimes. L'essentiel de l'activité associée à ce ransomware provient d'Inde, suivi de la Colombie, de la France, du Chili et des États-Unis.



Graphique 10 : prévalence des détections de malware par secteur d'activité sur S1 2021.

Le graphique 10 témoigne que le ransomware menace tous les secteurs d'activités. Cependant, ce sont les acteurs des télécommunications qui ont été les plus impactés, suivi par les administrations, les fournisseurs de services managés, l'automobile et le secteur industriel. La prévalence de ce ransomware dans les domaine de l'enseignement et des soins de santé (généralement considérés comme étant des cibles majeures) est moindre comparé aux autres secteurs. Le principal enseignement de ces observations est que le ransomware constitue un danger clair et omniprésent, quel que soit le secteur d'activité ou la taille des entreprises ciblées.

L'OT n'évolue plus à l'ombre de l'IT

L'informatique industrielle (OT pour Operational Technology) n'attire pas le même niveau d'attention que l'IT, mais son interconnexion au monde physique indique un impact potentiellement important sur nos vies quotidiennes. Jusqu'à récemment, les réseaux OT étaient cloisonnés et leur cybersécurité n'était donc pas une priorité. Les exploits sur les systèmes SCADA et ICS étaient considérés comme une part négligeable des attaques ciblées. Reste à savoir si cette perception reste d'actualité face aux menaces modernes. Pour cela, venons-en au fait.

Le graphique 11 répertorie les détections IPS selon leur prévalence et leur volume. Les points gris représentent le spectre de prévalence et de volume des attaques sur l'IT (cf. graphique 1 pour des exemples de technologies de la zone droite supérieure), tandis que les points rouges sont liés aux systèmes OT. Si les exploits IT sont clairement plus nombreux et affichent une prévalence et des volumes plus importants, le volume relativement important d'exploit OT peut en surprendre plus d'un. Ainsi, nous ne pouvons que remettre en cause la perception que les exploits ICS ne constituent qu'une niche dans l'univers des cybermenaces.

Ce changement de perspective est essentiel, compte tenu des nouvelles exigences des entreprises et d'infrastructures OT vieillissantes. La frontière traditionnelle entre OT et IT s'estompe, ce qui favorise la convergence de ces réseaux. Vous pouvez vous familiariser avec les solutions qui rendent une infrastructure de sécurité plus flexible dans notre publication Industry Perspective dédiée aux tendances au sein des environnements industriels.

Graphique 11 : prévalence et volume des exploits ciblant l'OT (rouge) et l'IT (gris) sur H1 2021.

Le positionnement de certains systèmes ICS dans le graphique 11 est cohérent avec nos observations sur un graphique similaire datant d'un an. Ceci révèle un intérêt continu de la part des cybercriminels pour identifier des vulnérabilités OT et inclure ces vulnérabilités au sein de différents outils d'exploit. Il en résulte un coût financier moindre pour l'attaque, tandis que les novices sont aussi capables que les groupes APT d'identifier vos systèmes OT vulnérables.

Au cours du premier semestre de l'année, on note une prévalence et un volume renforcé des exploits ciblant les systèmes WindRiver VxWorks. VxWorks est le système d'exploitation temps réel le plus couru dans le monde et présente donc une surface d'attaque particulièrement large. Cet OS a toujours présenté de nombreuses vulnérabilités, comme celles identifiées par Rapid7 en 2010 le plus récent "Urgent/11" divulgué par Armis Labs en 2019.

Armis a publié une mise à jour sur Urgent/11 à la mi-décembre 2020, indiquant que 97 % des dispositifs OT impactés par URGENT/11 n'avaient pas été patchés. Cette alerte n'est sans doute pas passée inaperçue chez les assaillants, ce qui a donné lieu à une plus forte activité de reconnaissance pour identifier ces vulnérabilités. Cette théorie est validée par le fait qu'une des détections les plus prévalentes porte sur des tentatives de scan pour déterminer la version de VxWorks. Ce scan n'est pas vraiment une menace en lui-même, mais il tente sans doute d'identifier d'autres vulnérabilités connues dans le stack TCP/IP de VxVorks, avec un risque d'exécution de malware à distance.

Les exploits OT sont plus communs qu'on ne le pense, ce qui indique un regain d'intérêt de la part des assaillants. Le meilleur moyen de protéger les systèmes de contrôle industriel consiste à identifier et à restaurer les vulnérabilités, avant toute attaque potentielle. Pour y parvenir, FortiGuard Labs se mobilise pour identifier et divulguer les vulnérabilités zero-day des infrastructures ICS. Ainsi, sur ce seul semestre, nous avons notifié quatorze d'entre elles à Schneider Electric.

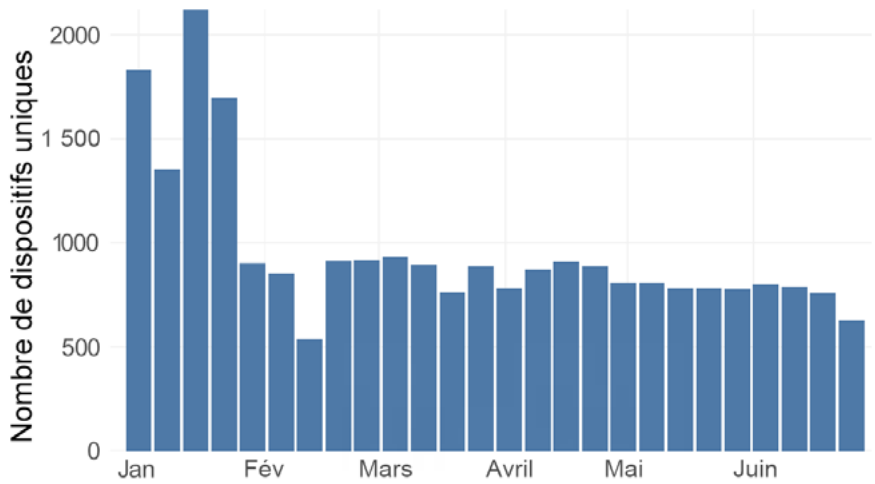
Démantelement d'Emotet et autres succès des forces de l'ordre

En janvier, les forces de l'ordre de différents pays (États-Unis, Pays-Bas, Royaume-Uni et Allemagne) ont réussi à démanteler le botnet Emotet, à l'issue d'opérations coordonnées visant à neutraliser l'un des malware les plus prolifiques sur ces récentes années. Cette opération a permis de mettre à l'arrêt de manière simultanée des centaines de serveurs dans le monde qui étaient utilisés à des fins de communication command-and-control. D'autre part, le trafic des systèmes infectés a été redirigé vers une infrastructure contrôlée par les forces de l'ordre.

Emonet était utilisé à grande échelle pour acheminer différents malware, dont des outils de détournement d'information, des chevaux de troie et des ransomware. Ce botnet était notamment utilisé par les opérateurs des ransomware Ryuk et Qakbot et du cheval de Troie bancaire Trickbot. Ainsi, le démantèlement d'Emotet a marqué un coup d'arrêt pour les cybercriminels tentant de distribuer leur malware.

D'autres opérations collaboratives ont également eu lieu dans différents pays, ce qui a mis un terme à plusieurs opérations cybercriminelles sur le premier semestre 2021 (ransomware Egregor, NetWalker et Cl0p notamment). Ces succès constituent une étape majeure pour les gouvernements et forces de l'ordre dans leur lutte face aux cybercriminels. Les forces de l'ordre se sont senties encouragées par les sanctions infligées à différents groupes APT financés par des états, suite à des attaques comme celles sur SolarWinds, Colonial Pipeline et JBS. Un autre signe encourageant suite à l'attaque sur Colonial Pipeline est la mise à l'arrêt volontaire de groupuscules cybercriminels comme DarkSide, Avaddon et Ziggy, ainsi que le refus de certains forums underground de traiter avec le ransomware. Il en résulte que certains groupes de cybercriminels se révèlent plus préoccupés par les actions des forces de l'ordre.

Cependant, aussi louables que soient ces succès, les actions des forces de l'ordre et les mises à l'arrêt volontaires ont des résultats généralement temporaires. Les données de Fortinet témoignent d'un ralentissement de l'activité suite au démantèlement d'Emotet, mais pas d'une éradication des menaces (voir graphique 12). L'activité associée à TrickBot et Ryuk, si elle s'est comprimée, s'est néanmoins poursuivie après l'arrêt d' Emotet. D'autres éditeurs indiquent un déclin temporaire dans le nombre de malware détectés suite à la cessation d'Emotet, suivi d'un retour graduel à la normale : les assaillants ont donc su utiliser d'autres outils pour véhiculer leur malware.



Graphique 12 : détections de communications Emotet sur S1 2021.

Ces données prouvent à nouveau à quel point il est difficile d'éradiquer les cybermenaces et rappellent aux entreprises qu'elles ne doivent pas baisser leur garde, même face aux succès des forces de l'ordre. Ces réussites sont évidemment essentielles, mais se débarrasser des cybercriminels implique des efforts sur le long terme. Nous contribuons à ces efforts au travers de ce rapport de sécurité qui, nous l'espérons, vous aidera à mieux anticiper les mois à venir.

Savez-vous que...

Fortinet est membre fondateur du Centre for Cybersecurity (C4C) du Forum économique mondial, une plateforme indépendante qui favorise le dialogue et la collaboration entre la communauté mondiale de la cybersécurité, les acteurs du service public et les entreprises. L'initiative Partnership Against Cybercrime fait parti de la plateforme C4C Platform. Dans ce contexte, Fortiguard Labs pilote un projet de cartographie de l'écosystème cybercriminel, de ses relations et de ses opérations, afin de mieux cibler les efforts visant à perturber cet écosystème.

Ceux qui souhaitent mieux comprendre comment renchérir les coûts et les risques pour les cybercriminels sont invités à consulter ce rapport que nous avons co-rédigé. Il se penche sur l'amélioration des capacités globales pour les opérations de démantèlement et la lutte contre la cybercriminalité.

[1] IDC Worldwide Security Appliance Tracker avril 2020 (sur la base des unités annuelles d'appliances de pare-feu, UTM et VPN vendues)

décembre 3, 2021 4:14 PM

1221850-0-0-FR