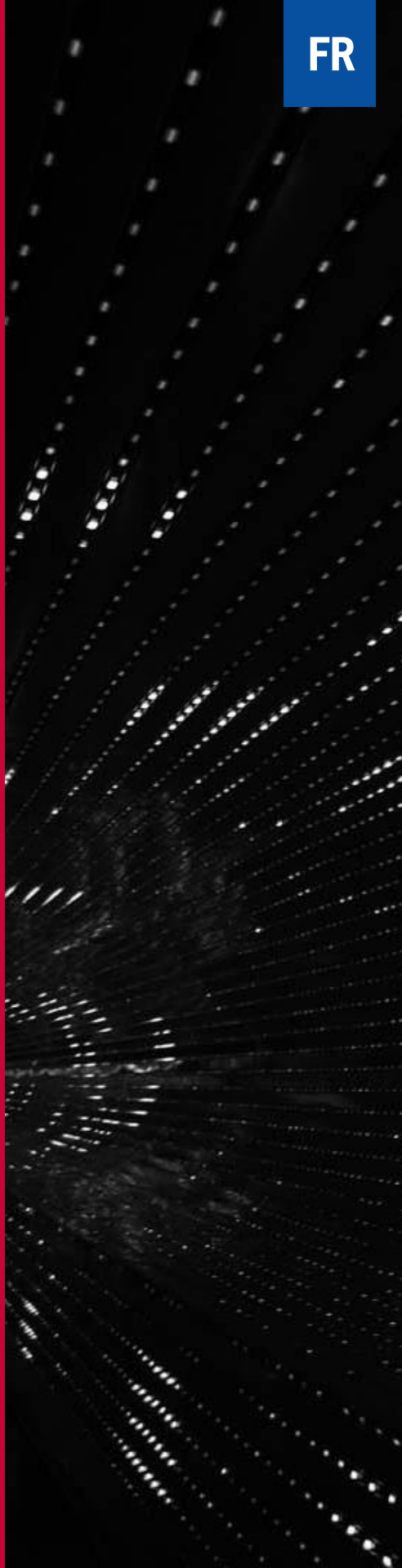
FR

enisa

EUROPEAN
UNION AGENCY
FOR CYBERSECURITY



De janvier 2019 à avril 2020

Les réseaux de machines zombies

Paysage des menaces de l'ENISA

Aperçu

Un réseau de machines zombies (*botnet*) est un réseau d'appareils connectés qui sont infectés par un logiciel malveillant de type robot (*bot*). Ces appareils sont généralement utilisés par des acteurs malveillants pour mener des attaques par déni de service distribué (DDoS - *Distributed Denial of Service*). Fonctionnant en mode poste-à-poste (P2P - *Peer-to-Peer*)[1] ou depuis un centre de commande et de contrôle (C&C)[2], les réseaux de machines zombies sont contrôlés à distance par un acteur malveillant pour garantir une synchronisation du fonctionnement afin d'obtenir un certain résultat.[3]

Les avancées technologiques en matière d'informatique distribuée et d'automatisation ont permis aux acteurs malveillants d'explorer de nouvelles techniques et d'améliorer leurs outils et méthodes d'attaque. Grâce à cela, les réseaux de machines zombies fonctionnent de manière beaucoup plus répartie et automatisée; ils sont disponibles en libre-service et prêts à l'emploi auprès de fournisseurs.

Les robots malveillants, appelés « *bad bots* », sont non seulement en constante évolution, mais les compétences des individus et le niveau de développement de ces robots sont désormais hautement spécialisés dans certaines applications, comme dans les fournisseurs de défense, voire dans les techniques d'évasion.[4] En outre, les réseaux de machines zombies fournissent un vecteur aux cybercriminels pour lancer diverses opérations allant de la fraude bancaire en ligne au rançongiciel (*ransomware*), en passant par le minage de cryptomonnaies et les attaques par déni de service distribué (DDoS).[5]

Conclusions

7,7_millions d'appareils IoT sont connectés à l'internet chaque jour

Parmi ceux-ci, on estime qu'un sur 20 est protégé par un pare-feu ou un outil de sécurité réseau similaire.[6]

57 %_d'augmentation du nombre de variantes de Mirai détectées en 2019

Bien que les variantes de Mirai soient connues pour avoir recours à des techniques d'attaque par force brute pour compromettre principalement les appareils IoT, une augmentation des techniques par force brute (51 %) et des techniques d'exploitation du réseau (87 %) a été observée en 2019.[7]

300 000_notifications du trafic du *botnet* Emotet observées en 2019

Ce chiffre représente plus de 100 000 alertes de victimes supplémentaires par rapport à la même période de 2018. Après avoir comparé le second semestre de 2018 et celui de 2019, les chercheurs ont estimé que le nombre d'échantillons Emotet avait augmenté de 913 %.[7]

60 %_de l'activité des nouveaux *botnets* rivaux est associée au vol d'identifiants[9]

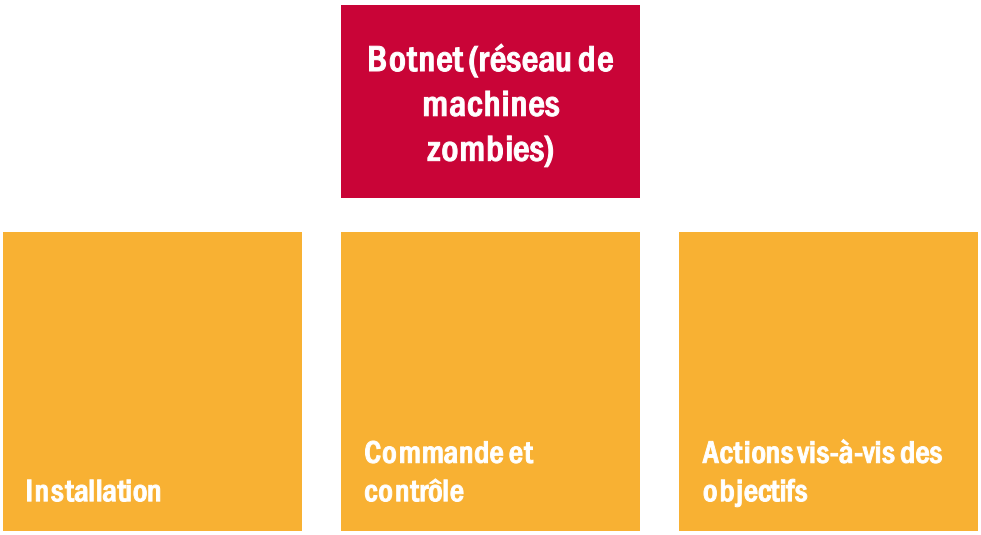
17 602_serveurs C&C de *botnets* pleinement opérationnels découverts en 2019

Augmentation de 71,5 % par rapport à 2018.[5]

Chaîne de frappe

Étape du processus d'attaque

Ampleur de l'objectif



Mis au point par Lockheed Martin, le modèle de Cyber Kill Chain® s'inspire d'un concept militaire lié à la structure d'une attaque. Pour étudier un vecteur d'attaque en particulier, utilisez cette chaîne de frappe schématisée pour représenter chaque étape du processus puis référencer les outils, les techniques et les procédures utilisés par l'attaquant.

EN SAVOIR PLUS

Tendances

_Les bots, c'est beaucoup d'argent

Les bots facilitent le recours à la force brute en incitant les victimes à acheter des articles en édition limitée ou des articles en promotion pour ensuite les revendre à un prix plus élevé. Cette réalité a été mise en évidence grâce à l'analyse d'une offre d'emploi dans laquelle l'annonceur cherchait un développeur de logiciels expérimenté dans le contournement des systèmes de protection et la création de bots avec techniques d'évasion (par ex., moissonnage de données sur le web ou *web scraping*, contournement reCAPTCHA, génération de cookies, etc.); celui-ci était prêt à payer 15 000 dollars (env. 12 750 euros) pour le candidat idéal.[4]

_Le Silexbot briqué

En juin 2019, un chercheur en sécurité[17] a procédé à l'analyse d'un nouvel échantillon de bot mis au point pour perturber les fonctionnalités des appareils IoT non sécurisés. Autrement dit, ce bot était conçu pour utiliser les identifiants de connexion connus/par défaut des appareils IoT et ensuite détruire l'appareil en supprimant les configurations réseau et en ajoutant une règle iptables pour supprimer toutes les connexions. Outre les capacités techniques, le message laissé sur l'échantillon du logiciel malveillant est un point intéressant à souligner. L'acteur malveillant y présente ses excuses pour son acte et justifie ses actions comme un moyen de prévenir l'exploitation massive des appareils IoT non sécurisés visant à créer des réseaux de machines zombies à des fins malveillantes.

Echobot et son vecteur de menace croissant

En juin 2019, un chercheur en sécurité a identifié une version mise à jour d'Echobot. Dans son analyse, le chercheur a découvert un échantillon compilé en x86 conduisant à des vecteurs d'attaque utilisés par cette variante de Mirai dans 26 incidents différents.[10] En août, un autre chercheur en sécurité a constaté une accélération d'Echobot, exploitant 50 vulnérabilités différentes, dont l'«injection de commandes sur HTTP» (CPAI-2016-0658).[25,26] En décembre 2019, une autre équipe a détecté une version améliorée d'Echobot comprenant 71 codes d'exploitation. Les codes d'exploitation récemment ajoutés visaient des vulnérabilités, tant anciennes que nouvelles, et bénéficiaient d'une capacité supplémentaire importante pour cibler les systèmes de contrôle industriel (SCI). Il s'agissait notamment d'entreprises et de dispositifs tels que Mitsubishi, Citrix NetScaler App Delivery Controller, Barracuda Web Application Firewall et les outils d'UEM (*Unified Endpoint Management* ou gestion unifiée des terminaux).[27]

Necurs sur le déclin tandis qu'Emotet se relève

En janvier 2019, on a constaté que Necurs s'était lancé dans une campagne de pourriels (*spams*) de type amateur, laissant penser aux chercheurs que les acteurs malveillants derrière tout cela avaient beaucoup perdu de leurs compétences.[20] À l'inverse, l'activité d'Emotet s'est considérablement accrue depuis septembre 2019, avec une montée en flèche vers fin 2019 marquée par l'injection de binaires compilés uniques représentant un vecteur de distribution et des mécanismes de communication persistants.[7] Une analyse a révélé une forte augmentation de la diffusion d'Emotet par messagerie électronique.[22]

Tendances

_Retadup, le *botnet* à l'origine du minage de Monero est tombé

Aux capacités polymorphes, Retadup était principalement actif comme ver de minage du Monero.[23] Il a infecté des machines fonctionnant sous Windows en Amérique latine. Les capacités de ce bot allaient du minage au déploiement de code personnalisé, en passant par le téléchargement de fichiers sur les machines des victimes (on a également constaté qu'il distribuait le rançongiciel STOP[24]). C'est en mars 2019 qu'un chercheur en sécurité a commencé à surveiller l'activité de Retadup et, ce faisant, a remarqué que le protocole C&C avait été conçu de manière simple. L'équipe a alors identifié une faille dans le protocole qui lui a permis de désinfecter les machines de la victime en prenant le contrôle du serveur C&C. L'infrastructure de cette activité malveillante a été identifiée, elle se trouvait principalement en France. Le *botnet* a été démantelé en collaboration avec la Gendarmerie nationale française et près de 850 000 ordinateurs ont alors été désinfectés.

_Mirai est mort, longue vie à Mirai

C'est peut-être en raison de l'absence de compétences et de caractéristiques du code original que Mirai et ses variantes restent dominants dans les familles de *botnets*; en outre, plus de 20 000 échantillons uniques ont été observés chaque mois au cours du premier semestre 2019. Ces variantes utilisent différentes techniques pour compromettre les dispositifs IoT, allant du forçage brut de mots de passe codés en dur par défaut jusqu'aux codes d'exploitation.[6] Selon deux chercheurs en sécurité, il existe également une grande diversité d'architectures de systèmes ciblées par ces variantes. La figure 1 présente plus de statistiques concernant l'activité d'Emotet.[7,18]

_Le *botnet* poste-à-poste Roboto

L'activité de Roboto, un *botnet* poste-à-poste, a été observée pour la première fois en août 2019 par une équipe de recherche en sécurité. Un fichier ELF suspect a été le premier échantillon saisi. En octobre, l'équipe de recherche a identifié un autre échantillon (fichier ELF) qui s'est avéré être le téléchargeur de l'échantillon précédent. À l'issue d'une analyse plus approfondie, l'équipe de recherche a découvert que le *botnet* Roboto pouvait prendre en charge sept fonctions, à savoir le shell inversé, l'autodésactivation, la collecte d'informations sur les processus et le réseau, la collecte d'informations sur les bots, l'exécution de fichiers spécifiés dans les URL, les attaques par déni de service distribué et les attaques de système d'exploitation. À noter que, selon l'un des chercheurs, l'attaque par déni de service distribué ne semble pas constituer son principal cas d'utilisation. Contrairement à d'autres *botnets*, ce bot se propageait en exploitant la vulnérabilité d'exécution de code à distance dans Webmin (CVE-2019-1507[28]).[11]

_Mozi, un autre *botnet* basé sur la technologie DHT

Baptisé d'après le nom de son fichier de propagation, Mozi a été remarqué par un chercheur en sécurité en septembre 2019 et identifié comme un tout nouveau *botnet* basé sur la technologie DHT (*Distributed Hash Table* ou table de hachage distribuée). Après une première analyse de l'échantillon réalisée par un autre chercheur en sécurité[38], il a été identifié comme Gafgyt, notamment en raison de la réutilisation partielle du code de Gafgyt. Ce *botnet* se propage en utilisant quelques codes d'exploitation et en exploitant la faiblesse de mots de passe Telnet. L'analyse de ses fonctionnalités a révélé qu'il pouvait être en mesure de lancer des attaques par déni de service distribué, de collecter des informations, d'exécuter et de mettre à jour un échantillon/une charge utile à l'aide d'une URL spécifiée et d'exécuter des commandes.[29, 30]

Tendances

Statistiques sur l'activité d'Emotet

Données	Statistiques
Nombre total de systèmes autonomes détectés:	5 430
Nombre total d'adresses IP distinctes détectées:	120 764
Total des pays participants:	193
Nombre total de courriels envoyés:	10 935 346
Nombre total d'URL de distribution:	4 726
Nombre de destinataires distincts ciblés:	8 052 961

Figure 1: Source: Spamhaus[5]

«Les avancées technologiques en matière d'informatique distribuée et d'automatisation ont permis aux acteurs malveillants d'explorer de nouvelles techniques et d'améliorer leurs outils et méthodes d'attaque.»

ETL 2020

Conclusions

_Statistiques et autres chiffres pertinents

Selon un chercheur en sécurité, **7,7 millions d'appareils IoT sont connectés à l'internet chaque jour** et on estime que seul un sur 20 est protégé par un pare-feu ou un outil de sécurité réseau similaire.[6] Cette estimation révèle que les **appareils IoT sont encore vulnérables et susceptibles d'être exploités** par des cybermenaces, à l'image de Mirai.

- Au cours du premier semestre 2019, l'activité des *botnets* et l'hébergement des serveurs C&C ont considérablement augmenté[32], représentant une hausse de 7 % sur l'ensemble des *botnets* détectés et de 1,8 % des serveurs C&C dans le monde. Les services financiers et leurs clients ont été le secteur le plus souvent visé.
- La Thaïlande se classait en tête des pays hébergeant des serveurs C&C, tandis que la Malaisie arrivait en deuxième position, suivie par les Philippines, Singapour et l'Indonésie.
- D'après les recherches d'Interpol, Andromeda a été le *botnet* le plus détecté, bien qu'il ait été démantelé en 2017.[33] Conficker[34] arrivait en deuxième position, suivi de Necurs[35], Sality[36] et Gozi[37].

En 2019, le nombre de variantes de Mirai détectées a augmenté de plus de 57 % par rapport à 2018, comme le montre la figure 2.

Bien que les variantes de Mirai soient connues pour avoir recours à des techniques d'attaque par force brute pour compromettre principalement les appareils IoT, une augmentation des techniques par force brute (51 %) et des techniques d'exploitation du réseau (87 %) a été observée en 2019.

Nombre d'échantillons Mirai

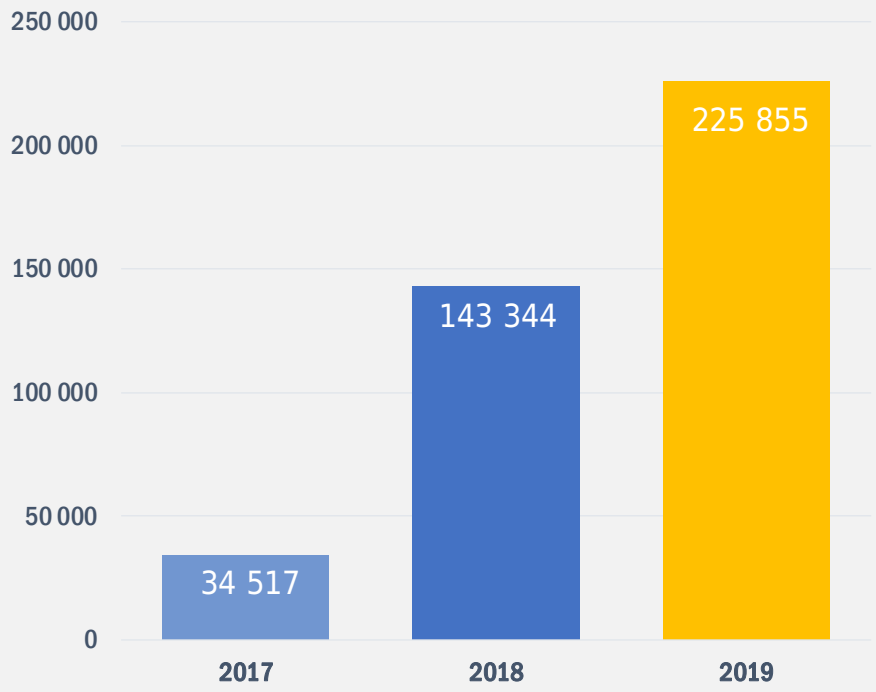


Figure 2 - Source: NETSCOUT[7]

Conclusions

_Statistiques et autres chiffres pertinents

- En 2019, un chercheur en sécurité a constaté près de 300 000 notifications supplémentaires relatives au trafic du *botnet* Emotet et plus de 100 000 alertes de victimes supplémentaires par rapport à la même période de 2018. Selon ce chercheur, il y a eu une augmentation de 913 % du nombre d'échantillons Emotet si l'on compare le second semestre 2018 à celui de 2019.[7,22]
- L'activité des *botnets* poste-à-poste a augmenté depuis que Roboto et Mozi sont devenus actifs.[8]
- Les *botnets* sous Linux ont été responsables de près de 97,4 % des attaques.[8]
- La plus forte proportion de *botnets* a été enregistrée aux États-Unis (58,33 %) au quatrième trimestre 2019. Bien qu'il s'agisse d'une augmentation par rapport au troisième trimestre 2019 (47,55 %), le nombre total de serveurs C&C a presque diminué de moitié. Alors en quatrième position, le Royaume-Uni est passé au deuxième rang avec 14,29 %, tandis que la Chine a conservé sa place avec 9,52 %. La baisse la plus significative des serveurs enregistrés C&C s'est produite aux Pays-Bas (de 45 % à env. 1 %). Pour en savoir plus sur la répartition des serveurs C&C de *botnet* par pays, veuillez consulter la figure 3.[8]
- En 2019, LokiBot est resté en tête de liste des bots de vol d'identifiants avec une augmentation du nombre d'activités C&C de 74 % par rapport à 2018. AZORult se plaçait en deuxième position juste derrière LokiBot.[39]
- 17 602 serveurs C&C de *botnet* étaient en service en 2019, ce qui représente une augmentation de 71,5 % par rapport à 2018.[39]

Répartition des serveurs C&C de *botnet* par pays

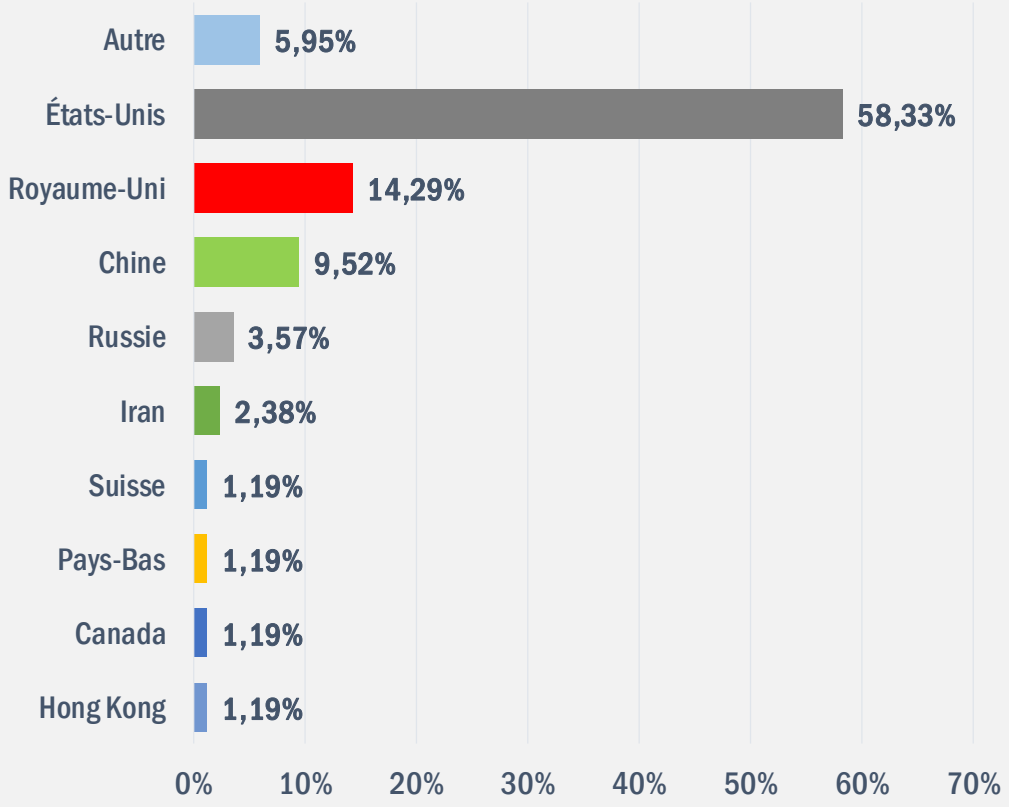


Figure 3 - Source: Kapersky[8]

Vecteurs d'attaque

_ Les attaques de *botnet*

Selon un chercheur en sécurité, en 2019, près de 60 % de l'activité des nouveaux *botnets* rivaux était associée au **vol d'identifiants**. Comme mentionné précédemment, LokiBot est le plus actif dans ce domaine. Outre le vol d'identifiants, **la fraude à la banque en ligne et la fraude financière** sont d'autres domaines où la présence des *botnets* est importante. Emotet et TrickBot sont de bons exemples dans le domaine, avec un modèle actualisé couvrant non seulement la fraude à la banque en ligne, mais également les services de *pay-per-install* (PPI - paiement à l'installation).[9]

En outre, **les chevaux de Troie autorisant un accès à distance** (RAT - *Remote Access Trojans*) ont fait partie des outils les plus utilisés dans les activités C&C des *botnets*. En 2018, la plupart de ces activités étaient associées à Adwind, mais en 2019, son activité s'est réduite et a été remplacée par NanoCore.[5]

Des vecteurs d'attaque spécifiques ont été adoptés en 2019. Les *botnets* utilisent différents vecteurs d'attaque pour atteindre leurs objectifs. Les machines infectées ou réseaux de machines zombies sont créés en exploitant des vulnérabilités communes par force brute et par le biais d'autres techniques d'infection courantes.[10,11,12] Par la suite, le propriétaire du *botnet* (appelé «*botmaster*») est capable de fournir une plateforme pour différents types d'attaques, comme une vaste campagne de pollupostage et de logiciels malveillants, le vol et la réutilisation d'identifiants, le cryptominage et le déni de service distribué.

La **«triple menace»** constitue un autre exemple de vecteur d'attaque utilisé dans une attaque par *botnet*. Dans ce cadre, l'organisation ciblée est d'abord infectée par le logiciel malveillant Emotet. Puis, le logiciel malveillant Emotet diffuse le cheval de Troie TrickBot qui cible et explore les informations sensibles. Si les informations sont trouvées et que l'environnement/réseau ciblé figure sur la liste de l'attaquant, le rançongiciel Ryuk est exécuté.[13]

Nombre de serveurs C&C de *botnet* observés entre 2014 et 2019

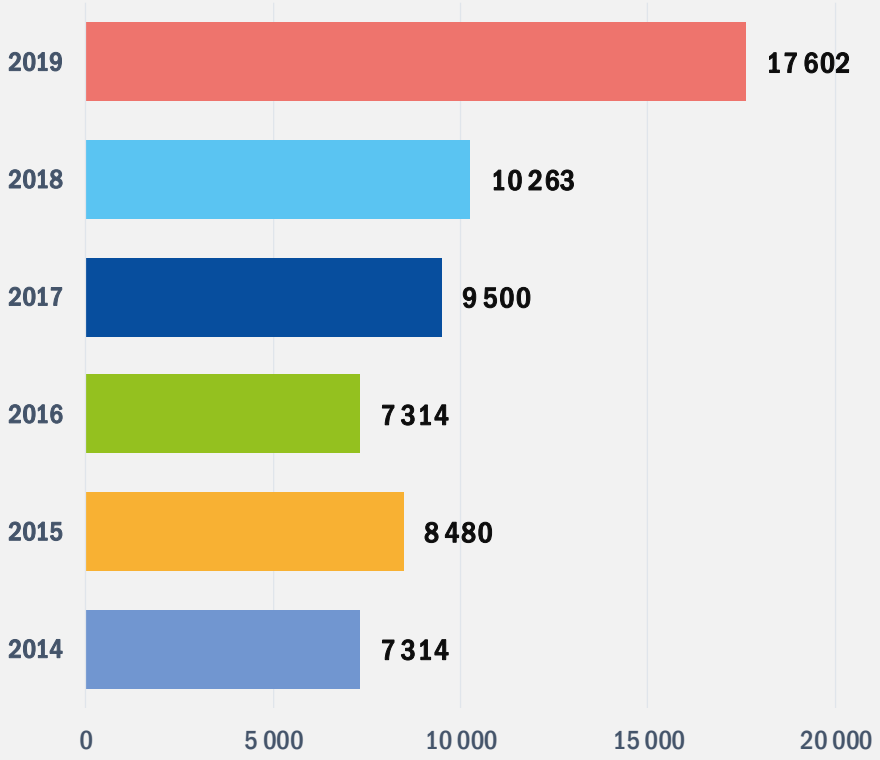


Figure 4 - Source: Spamhaus[5]

Atténuation

_ Actions proposées

La connaissance de l'environnement est l'un des aspects clés d'une défense solide. Elle permet d'identifier les activités malveillantes au sein du trafic en fonction de l'éventuelle base de référence (c.-à-d. les détections comportementales)[14] mesurée par un outil de surveillance du trafic.[4] Une partie importante du trafic des *botnets* étant liée aux attaques par déni de service distribué, les techniques d'atténuation relatives à ces menaces s'appliquent également.

- Déployer un protocole BGP (*Border Gateway Protocol*) ayant la capacité de rechercher des domaines de premier niveau décentralisés pour bloquer les connexions aux adresses IP liées à l'activité C&C du *botnet*.[8]
- Comprendre et catégoriser les vulnérabilités, puis mettre en œuvre de solides correctifs et des procédures de mise à jour.[15,16]
- Restreindre ou bloquer les groupes de minage de cryptomonnaies et surveiller l'environnement pour les utilisateurs requis.[5]
- Déployer des fonctionnalités basées sur des défis pour les sites web requis afin de vérifier l'origine du trafic (par ex., reCAPTCHA).[16]
- Mettre en place de solides stratégies de mot de passe et d'authentification à deux facteurs (A2F) sur les serveurs ou infrastructures accessibles au public afin d'éviter d'être victime d'une exploitation liée à un mot de passe/une authentification faible.[5]
- Déployer et configurer des pare-feu pour le réseau et les applications.

«La sophistication des capacités de menace s'est accrue en 2019; de nombreux adversaires ont désormais recours aux codes d'exploitation, au vol d'identifiants et aux attaques en plusieurs étapes.»

ETL 2020

Références

1. «Peer-to-peer (P2P).» Malwarebytes Labs https://blog.malwarebytes.com/glossary/peer-to-peer/
2. Monnappa K A. «Learning Malware Analysis.» Juin 2018. O'reilly. https://www.oreilly.com/library/view/learning-malware-analysis/9781788392501/17a1735d-9583-4d86-9d1e-8b2735af5168.xhtml
3. «ASEAN Cyberthreat Assessment 2020.» 17 février 2020. Interpol https://www.interpol.int/fr/Actualites-et-evenements/Actualites/2020/Un-rapport-d-INTERPOL-met-en-evidence-les-principales-cybermenaces-en-Asie-du-Sud-Est
4. «State of The Internet Security - DDoS and Application Attacks Report: Volume 5, Issue 1.» 2019. Akamai. https://www.akamai.com/us/en/multimedia/documents/state-of-the-internet/state-of-the-internet-security-ddos-and-application-attacks-2019.pdf
5. «Spamhaus Botnet Threat Report 2019.» 28 janvier 2020. Spamhaus. https://www.spamhaus.org/news/article/793/spamhaus-botnet-threat-report-2019
6. «NETSCOUT Threat Intelligence Report: Powered by ATLAS - Findings from H1 2019.» 2019.
7. «NETSCOUT Threat Intelligence Report - With key findings from the 15th Annual Worldwide Infrastructure Security Report (WISR) - Findings from H2 2019.» 2019. NETSCOUT. https://www.netscout.com/threatreport
8. Oleg Kupreev, Ekaterina Badovskaya, Alexander Gutnikov. «DDoS attacks in Q4 2019.» 13 février 2020. Kaspersky. https://securelist.com/ddos-report-q4-2019/96154/
9. Alina Dettmer. «What is Pay Per Install.?» 26 octobre 2017. Aye Studios. https://www.ayetstudios.com/blog/mobile-advertising/mobile-campaign-types/pay-per-install
10. Larry Cashdollar. «Latest Echobot: 26 Infection Vectors.» 13 juin 2019. Akamai. https://blogs.akamai.com/sitr/2019/06/latest-echobot-26-infection-vectors.html
11. «The awaiting Roboto Botnet.» 20 novembre 2019. Netlab. https://blog.netlab.360.com/the-awaiting-roboto-botnet-en/
12. Asher Davila. «Home & Small Office Wireless Routers Exploited to Attack Gaming Servers.» 31 octobre 2019. Paloalto. https://unit42.paloaltonetworks.com/home-small-office-wireless-routers-exploited-to-attack-gaming-servers/
13. «Triple Threat: Emotet deploys Trickbot to steal data & spread Ryuk.» 2 avril 2019. Cybereason. https://www.cybereason.com/blog/triple-threat-emotet-deploys-trickbot-to-steal-data-spread-ryuk-ransomware
14. «Bots.» Imperva. https://www.imperva.com/learn/application-security/what-are-bots/
15. Rebecca Carter. «Bot Mitigation Best Practices.» 19 octobre 2018. DYN. https://dyn.com/blog/bot-mitigation-best-practices/
16. «What is a Botnet?» Veracode. https://www.veracode.com/security/botnet
17. «SIRT Advisory: Silexbot bricking systems with known default login credentials». 26 juin 2019. Akamai.
18. «Mirai Botnet Continues to Plague IoT Space». 10 septembre 2019. Reversing Labs. https://blog.reversinglabs.com/blog/mirai-botnet-continues-to-plague-iot-space
19. The Shadowserver Foundation. https://www.shadowserver.org/
20. «As Necurs Botnet Falls from Grace, Emotet Rises» 27 janvier 2020. Threat Post. https://threatpost.com/as-necurs-botnet-falls-from-grace-emotet-rises/152236/

21. «Mirai malware, attacks Home Routers». 14 décembre 2016. ENISA. https://www.enisa.europa.eu/publications/info-notes/mirai-malware-attacks-home-routers

22. «Estimating Emotet's size and reach». 12 décembre 2019. SPAMHAUS. https://www.spamhaus.org/news/article/791/estimating-emotets-size-%20-and-reach

23. «Monero-Mining RETADUP Worm Goes Polymorphic, Gets an AutoHotKey Variant». 23 avril 2018. Trend Micro. https://blog.trendmicro.com/trendlabs-security-intelligence/monero-mining-retadup-worm-goes-polymorphic-gets-an-autohotkey-variant/

24. «Meet Stop Ransomware: The Most Active Ransomware Nobody Talks About». 20 septembre 2019. Bleeping Computer. https://www.bleepingcomputer.com/news/security/meet-stop-ransomware-the-most-active-ransomware-nobody-talks-about/

25. «Command Injection Over HTTP». 26 juillet 2016. Check Point. https://www.checkpoint.com/defense/advisories/public/2016/cpai-2016-0658.html/

26. «August 2019's Most Wanted Malware: Echobot Launches Widespread Attack Against IoT Devices». Août 2019. Check Point. https://blog.checkpoint.com/2019/09/12/august-2019s-most-wanted-malware-echobot-launches-widespread-attack-against-iot-devices/

27. «Echobot Malware Now up to 71 Exploits, Targeting SCADA». 18 décembre 2019. F5 Labs. https://www.f5.com/labs/articles/threat-intelligence/echobot-malware-now-up-to-71-exploits--targeting-scada

28. «CVE-2019-15107 Detail». NIST. https://nvd.nist.gov/vuln/detail/CVE-2019-15107

29. «What is a distributed hash table?». EDPresso. https://www.educative.io/edpresso/what-is-a-distributed-hash-table

30. «A Look into the Gafgyt Botnet Trends from the Communication Traffic Log». 23 juillet 2019. https://nsfocusglobal.com/look-gafgyt-botnet-trends-communication-traffic-log/

32. «ASEAN Cyberthreat Assessment 2020, Key Insights From The ASEAN Cybercrime Operations Desk» Interpol, 2020

33. «International team takes down virus-spewing Andromeda botnet». 5 décembre 2017. The Register. https://www.theregister.com/2017/12/05/international_team_takes_down_virusspewing_andromeda_botnet/

34. «The odd, 8-year legacy of the Conficker worm». 21 novembre 2016. WeLiveSecurity. https://www.welivesecurity.com/2016/11/21/odd-8-year-legacy-conficker-worm/

35. «The Necurs Botnet: A Pandora's Box of Malicious Spam». 24 avril 2017. https://securityintelligence.com/the-necurs-botnet-a-pandoras-box-of-malicious-spam/

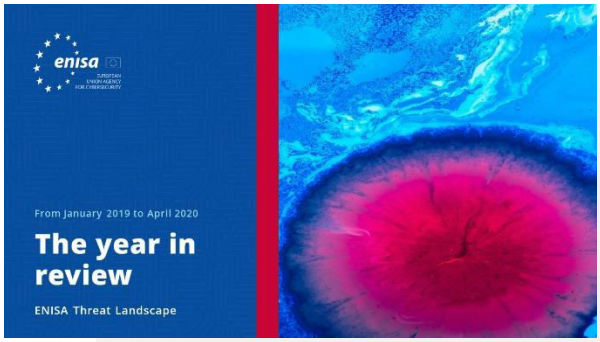
36. «WhitePaper: Sality: Story of a Peer to-Peer Viral Network». 10 juin 2011. Broadcom.

37. «Botnet C&C: Gozi». FortiGuard Labs. https://fortiguard.com/encyclopedia/botnet/7630489

38. Virustototal. https://www.virustotal.com

39. «Spamhaus Botnet Threat Report 2019» 2020. Spamhaus. https://www.spamhaus.org/news/article/793/spamhaus-botnet-threat-report-2019

Documents connexes



Rapport sur le Paysage des menaces de l'ENISA **Bilan de l'année**

Résumé des tendances en matière de cybersécurité observées entre janvier 2019 et avril 2020.

LIRE LE RAPPORT

Rapport sur le Paysage des menaces de l'ENISA
Liste des 15 principales menaces

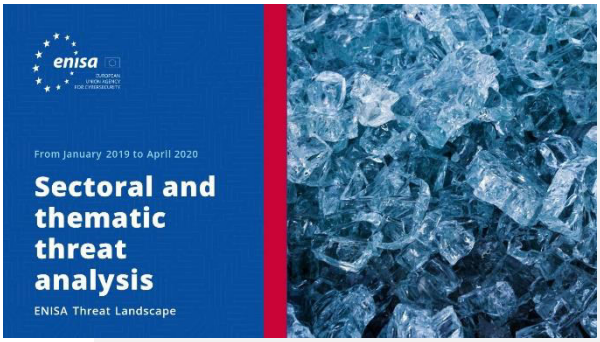
Liste des 15 principales menaces de l'ENISA pour la période comprise entre janvier 2019 et avril 2020.

LIRE LE RAPPORT

Rapport sur le Paysage des menaces de l'ENISA
Thèmes de recherche

Recommandations concernant les thèmes de recherche provenant de divers secteurs de la cybersécurité et du renseignement sur la cybermenace.

LIRE LE RAPPORT



LIRE LE RAPPORT

Rapport sur le Paysage des menaces de l'ENISA **Analyse sectorielle et thématique de la menace**

Analyse contextualisée de la menace entre janvier 2019 et avril 2020.

LIRE LE RAPPORT

Rapport sur le Paysage des menaces de l'ENISA **Tendances émergentes**

Principales tendances en matière de cybersécurité observées entre janvier 2019 et avril 2020.

LIRE LE RAPPORT

Rapport sur le Paysage des menaces de l'ENISA
Aperçu du renseignement sur la cybermenace

L'état actuel du renseignement sur la cybermenace dans l'UE.

À propos

_ L'Agence

L'Agence de l'Union européenne pour la cybersécurité (ENISA) est l'agence de l'Union dont la mission consiste à garantir un niveau élevé commun de cybersécurité dans toute l'Europe. Créée en 2004 et renforcée par le règlement de l'Union européenne sur la cybersécurité, l'ENISA contribue à la politique de l'Union en matière de cybersécurité, améliore la fiabilité des produits, services et processus TIC à l'aide de schémas de certification de cybersécurité, coopère avec les États membres et les organes de l'Union, et aide l'Europe à se préparer aux défis cybernétiques de demain. En partageant les connaissances, en renforçant les capacités et en organisant des initiatives de sensibilisation, l'Agence œuvre de concert avec ses principales parties prenantes pour renforcer la confiance dans l'économie connectée, améliorer la résilience des infrastructures de l'Union et, au bout du compte, maintenir la sécurité numérique de la société européenne et de ses citoyens. Pour plus d'informations sur l'ENISA et ses travaux, consultez le site https://www.enisa.europa.eu/media/enisa-en-francais/.

Contributeurs

Christos Douligeris, Omid Raghimi, Marco Barros Lourenço (ENISA), Louis Marinos (ENISA) et *tous les membres du groupe des parties prenantes CTI de l'ENISA:* Andreas Sfakianakis, Christian Doerr, Jart Armin, Marco Riccardi, Mees Wim, Neil Thaker, Pasquale Stirparo, Paul Samwel, Pierluigi Paganini, Shin Adachi, Stavros Lingris (CERT-UE) et Thomas Hemker.

Éditeurs

Marco Barros Lourenço (ENISA) et Louis Marinos (ENISA).

Contact

Pour toute question sur ce document, veuillez utiliser l'adresse enisa.threat.information@enisa.europa.eu.

Pour les demandes de renseignements des médias concernant le présent document, veuillez utiliser l'adresse press@enisa.europa.eu.

Nous aimerions avoir votre avis sur ce rapport!
Merci de prendre un moment pour remplir le questionnaire. Pour accéder au formulaire, veuillez cliquer ici.

Avis juridique

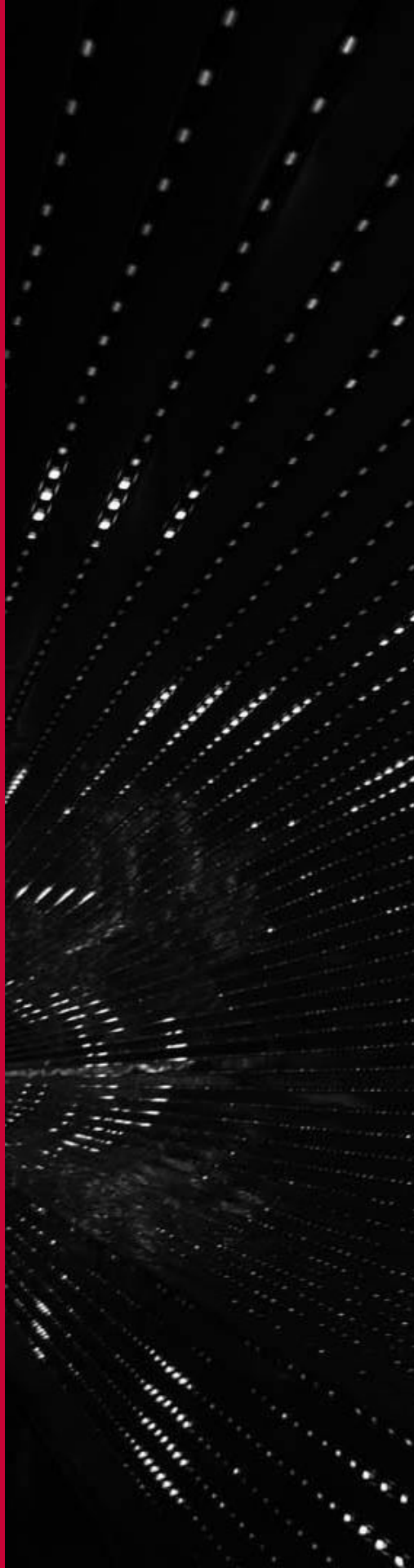
Il convient de noter que, sauf mention contraire, la présente publication représente les points de vue et les interprétations de l'ENISA. Elle ne doit pas être interprétée comme une action légale de l'ENISA ou des organes de l'ENISA à moins d'être adoptée conformément au règlement (UE) nº 526/2013. Elle ne représente pas nécessairement l'état des connaissances et l'ENISA peut l'actualiser périodiquement.

Les sources de tiers sont citées de façon adéquate. L'ENISA n'est pas responsable du contenu des sources externes, notamment des sites web externes, mentionnées dans la présente publication.

La présente publication est uniquement destinée à des fins d'informations. Elle doit être accessible gratuitement. Ni l'ENISA ni aucune personne agissant en son nom n'est responsable de l'utilisation qui pourrait être faite des informations contenues dans la présente publication.

ISBN: 978-92-9204-354-4
DOI: 10.2824/552242

Vasilissis Sofias Str 1, Maroussi 151 24, Attiki, Grèce
Tél.: +30 28 14 40 9711
info@enisa.europa.eu
www.enisa.europa.eu



enisa

EUROPEAN
UNION AGENCY
FOR CYBERSECURITY

https://www.enisa.europa.eu