**Communiqué de presse**

**Les comportements des hackers révélés : le bélier, la nuée et le hérisson**

Sophos identifie des schémas d’attaque, en s’appuyant sur l’étude

Oosterhout, 17 juillet 2019 – **Sophos présente aujourd’hui une nouvelle étude intitulée** [**RDP Exposed: The Threat That’s Already at your Door**](http://www.sophos.com/RDP)**, qui révèle comment les cybercriminels tentent sans relâche d’attaquer les entreprises à l’aide du RDP (Remote Desktop Protocol).**

Le RDP continue d'être une cause d’insomnies pour les administrateurs système. Comme vous le savez peut-être, Sophos signale l’exploitation du RDP par des cybercriminels depuis 2011. D’aileurs, en 2018, nous avons constaté que des groupes de cybercriminels responsables de deux des plus grandes attaques par ransomwares ciblés, Matrix et SamSam, ont presque complètement abandonné toutes les autres méthodes de pénétration des réseaux au profit de la technique utilisant le RDP.

Matt Boddy, spécialiste de la sécurité chez Sophos, et principal chercheur pour ce rapport, a déclaré : *« Récemment, une faille d'exécution de code à distance dans le RDP, surnommée BlueKeep (CVE-2019-0708), a fait la Une de l’actualité. Cette vulnérabilité est si sérieuse qu’elle pourrait être utilisée pour déclencher une épidémie de ransomware, susceptible de se propager dans le monde entier en quelques heures seulement. Cependant, une protection efficace contre les menaces RDP va bien au-delà des systèmes de correctifs contre BlueKeep, qui n'est en réalité que la partie émergée de l'iceberg. En plus de s'occuper de BlueKeep, les responsables informatiques doivent accorder une plus grande attention au RDP. En effet, comme le montre notre étude, les cybercriminels sont déjà en train d'analyser tous les ordinateurs potentiellement vulnérables et exposés au niveau du RDP, 24h/24 et 7j/7, par le biais d’attaques pour deviner les mots de passe ».*

La nouvelle étude RDP de Sophos montre comment les pirates peuvent trouver des appareils avec le RDP activé presque aussitôt après que ces derniers aient fait leur apparition sur Internet. Pour le démontrer, Sophos a déployé 10 honeypots [1] à faible interaction, dispersés géographiquement, pour mesurer et quantifier les risques basés sur le RDP.

Vous trouverez ci-dessous un résumé des recherches et l’analyse de Matt Boddy:

**Les principaux résultats de cette étude montrent que :**

* Les 10 honeypots ont connu une de leur première tentative de connexion RDP après seulement une journée.
* Le Remote Desktop Protocol expose les ordinateurs en 84 secondes seulement.
* Les 10 honeypots RDP ont enregistré un total de 4 298 513 tentatives de connexion infructueuses sur une période de 30 jours. Cela représente une tentative toutes les six secondes.
* En général, le secteur de la cybersécurité estime que les cybercriminels utilisent des sites tels que Shodan pour rechercher des sources RDP ouvertes. Cependant, les recherches de Sophos montrent comment les cybercriminels disposent de leurs propres outils et techniques pour rechercher ces sources RDP ouvertes et ne dépendent plus uniquement de sites tiers pour trouver un accès.

**Les comportements des hackers révélés**

Sophos a identifié des schémas d’attaque, en s’appuyant sur l’étude. Trois profils principaux d'attaque ont été identifiés : *Ram* (le bélier), *Swarm* (la nuée) et *Hedgehog* (le hérisson) :

* **Ram (le bélier)** est une stratégie conçue pour découvrir un mot de passe administrateur. Un exemple tiré de l’étude montre que sur une période de 10 jours, un attaquant a lancé 109 934 tentatives de connexion au honeypot irlandais en utilisant seulement trois noms d’utilisateur pour obtenir un accès.
* **Swarm** **(la nuée)** est une stratégie qui utilise des noms d'utilisateur séquentiels et un nombre fini de mots de passe parmi les plus mauvais. Un exemple présenté dans l’étude a été observé à Paris avec un attaquant utilisant le nom d’utilisateur ABrown neuf fois en 14 minutes, suivi de neuf tentatives avec le nom d’utilisateur BBrown, puis CBrown, suivi de DBrown, etc. Le modèle a été répété avec A.Mohamed, AAli, ASmith et d’autres.
* **Hedgehog** **(le hérisson)** se caractérise par des pics d'activité suivis de périodes d'inactivité plus longues. Un exemple observé au Brésil a vu chaque pic d’activité générée par une adresse IP, durer environ quatre heures et comptabiliser entre 3 369 et 5 199 tentatives afin de deviner les mots de passe.

Matt Boddy explique l’impact de cette exposition au RDP pour les entreprises : « *Actuellement, plus de trois millions d'appareils sont accessibles via le RDP dans le monde entier et constituent désormais un point d'entrée privilégié pour les cybercriminels. Sophos a expliqué comment des cybercriminels déployant des ransomwares ciblés tels que BitPaymer, Ryuk, Matrix et SamSam ont presque complètement abandonné les autres méthodes utilisées pour pénétrer dans une entreprises au profit de simples attaques de mots de passe RDP par force brute. Tous les honeypots ont été découverts en quelques heures, simplement parce qu'ils étaient exposés à Internet via le RDP. La leçon essentielle à tirer de cette étude est de réduire autant que possible l'utilisation du RDP. Il faut aussi garantir que les meilleures pratiques en matière de mots de passe soient appliquées dans l'ensemble de l'entreprise. Ces entreprises doivent agir en conséquence pour mettre en place le bon protocole de sécurité afin de se protéger contre des attaquants impitoyables ».*

###

Le rapport complet est disponible ici : [RDP Exposed: The Threat That’s Already at your Door](http://www.sophos.com/RDP).

Des commentaires sur les résultats sont également disponibles sur Sophos Naked Security dans un article intitulé [RDP Exposed: The Wolves Already at Your Door.](https://nakedsecurity.sophos.com/wolf)

[1] Les honeypots étaient des instances Amazon EC2 utilisant Windows Server 2019 avec une configuration non modifiée et prête à l'emploi qui activait le RDP par défaut. Chaque instance EC2 a été déployée dans un centre de données régional différent et les tentatives de connexion qui ont échoué ont été enregistrées dans une base de données centralisée sur une période de 30 jours, du 18 avril 2019 au 19 mai 2019.

**À propos de Sophos**Sophos est un leader dans la sécurité Next-Generation des systèmes Endpoint et des réseaux. En tant que pionnier en matière de sécurité synchronisée, Sophos développe son offre innovante qui comprend des solutions pour les systèmes Endpoint, les réseaux, le chiffrement, le web, les emails et les mobiles, afin de mieux travailler ensemble. Plus de 100 millions d’utilisateurs dans 150 pays font confiance à Sophos, et considèrent sa gamme complète de produits de sécurité informatique comme la meilleure solution pour se protéger contre les menaces complexes et la perte de données. Les produits Sophos sont disponibles exclusivement via un réseau mondial de plus de 39 000 partenaires enregistrés. Le siège social de Sophos se situe à Oxford (Royaume-Uni), et Sophos a été introduit à la bourse de Londres sous le nom SOPH. Plus d’informations sont disponibles sur [www.sophos.com](http://www.sophos.com).

**Contacts Presse :**Sandra Van Hauwaert, Square Egg, [sandra@square-egg.be](mailto:sandra@square-egg.be), GSM 0497 251816