Comprendre et prévenir les attaques RDP, en hausse depuis le début de l'épidémie

Malgré sa simplicité de mise en oeuvre, ce type d'accès à distance s'accompagne d'une exposition importante et de vulnérabilités aux cyber-attaques, particulièrement celles liées aux ransomwares.

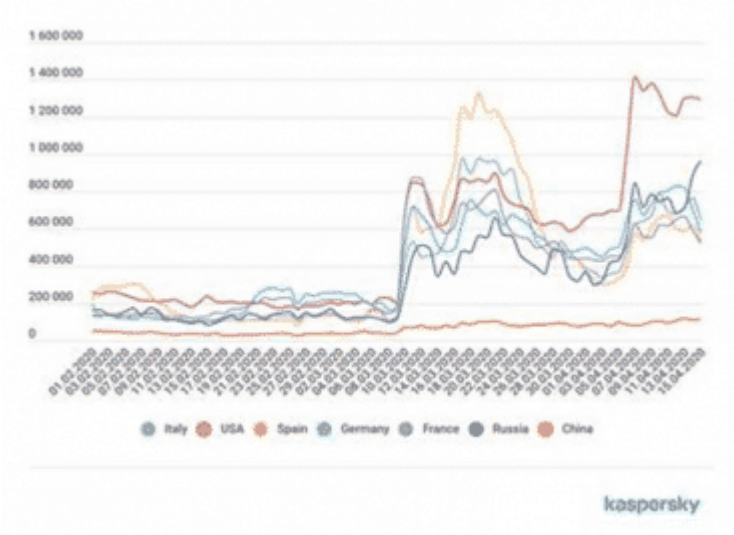
Pour s'en prémunir, il est important de comprendre le déroulement d'une attaque utilisant ce vecteur. Quelques exemples dans l'actualité récente l'illustrent assez bien et méritent d'être explorés. Une fois cette compréhension acquise, il est possible de mettre en place des mécanismes de protection et d'atténuation pour limiter l'exposition.

Les attaques liées à ce protocole sont en augmentation

Les ports Remote Desktop Protocol, principalement le port 3389, sont fréquemment exposés sur Internet.

Un des moyens les plus simples de sécuriser les accès de type RDP est de ne pas les exposer publiquement, mais de forcer les utilisateurs à passer au travers d'une connexion VPN et des stratégies d'authentification multi facteurs.

Cependant, la mise en place de solutions de travail à distance au début de la pandémie, souvent dans la précipitation, n'a laissé que peu de temps pour l'ajout de toutes les couches de sécurité nécessaires. Une étude récente de McAfee[1] a révélé que le nombre de ports RDP exposés sur Internet a grimpé en flèche, passant de trois millions en janvier 2020 à quatre millions et demi en mars ! Une autre étude menée par Kaspersky[2] a dénombré 145 000 attaques de force brute sur des ports RDP le 8 mars 2020 et 872 000 de ces mêmes attaques le 11 mars uniquement en France.



Atlas VPN indique que les attaques sur RDP ont explosé avec plus de 148 millions d'entre elles menées pendant le confinement dans le monde entier.

Anatomie d'une attaque RDP

Concrètement, voici la chaîne d'événements qui composent une attaque RDP :

Reconnaissance : Tout d'abord, les attaquants scannent et identifient des ports RDP exposés sur Internet. Leurs cibles sont également les ports ouverts dont les vulnérabilités n'ont pas été corrigées, ce qui leur confère un avantage dans la phase d'exploitation.

Intrusion : le cyber criminel utilise le « password spraying », une attaque par force brute (dont le nombre a été multiplié par 6 en France au début de la pandémie) ou une tentative de phishing pour pénétrer dans le réseau. Il est à noter que les attaquants peuvent également détourner des sessions RDP légitimes.

Exploitation : Une fois les systèmes pénétrés, les attaquants peuvent exploiter de très graves vulnérabilités non corrigées qui permettent d'installer des vers et d'exécuter du code à distance (deux facultés très recherchées pour construire une attaque ransomware).C'est à ce stade que sont déployés les ransomwares tels que MAZE lorsque c'est l'objectif poursuivi par les attaquants.

Augmentation des privilèges : lors de récents incidents liés au ransomware MAZE, les enquêteurs de FireEye ont découvert que les cybercriminels utilisent des attaques RDP comme moyen d'entrer, de prendre pied pour infecter plus d'hôtes et même d'exfiltrer des données avant d'activer le ransomware.

Les attaques de ransomware sont, en effet, de plus en plus liées à des vols de données. Les cybercriminels menacent les entreprises de divulguer publiquement ces données en plus des pratiques habituelles des chantage au chiffrement (cf. BlackBaud Mai 2020).

Mouvement latéral : En s'appuyant sur l'escalade des privilèges, les criminels augmentent leur emprise en compromettant d'autres systèmes grâce aux mouvements latéraux rendus possibles par le RDP. Ils peuvent se connecter à des ressources qui ne sont pas exposées publiquement. Ils installent ensuite des outils tels que BEACON Cobalt Strike.

Obfuscation / Dissimulation : Après l'exfiltration de données, les attaquants cherchent à brouiller les pistes afin d'atténuer les risques d'être détectés ou identifiés. Pour cela, le plus simple est

souvent de tout crypter. Là encore, l'utilisation de MAZE intervient souvent. Si l'organisation criminelle souhaite totalement dissimuler son intrusion afin de pouvoir la répéter (dans un objectif de recherche d'informations spécifiques comme de l'espionnage industriel), elle cherchera plutôt à purger les différents logs natifs des systèmes corrompus.

Déni de service : conséquence de l'opération d'obfuscation, l'exécution d'un ransomware sur un serveur RDP non patché ou sur une machine présentant une vulnérabilité aux vers peut entraîner des perturbations conséquentes et une situation de déni de service pour les utilisateurs et les systèmes légitimes.

Atténuation et suppression

Si elles peuvent paraître implacables, les attaques RDP ne sont pourtant pas une fatalité. Quelques bonnes pratiques peuvent largement contribuer à l'atténuation du risque. Il existe aussi des techniques de récupération qui limitent leur impact sur le fonctionnement de l'entreprise et qui ont fait leurs preuves.

- Bloquer les accès RDP aux ressources non indispensables via la protection périmétrique (Firewall) est évidemment la première étape évidente.
- S'assurer que les accès RDP sont désactivés sur les machines qui n'en ont pas besoin (les stations de travail notamment) via GPO. Des outils de gestion des GPO permettent de simplifier ces démarches.
- Utilisez RDP conjointement avec un VPN et une solution d'authentification multi facteurs via un serveur d'entrée qui se trouve en zone sécurisée sur le réseau d'entreprise.
- Collecter et sécuriser les informations de connexion, y compris les connexions à distance, avec une solution adaptée.
- Verrouiller les comptes dont les tentatives de connexion ont échoué en trop grand nombre (paramétrable via GPO).
- Identifier les adresses IP à l'origine d'échecs de tentatives de connexion multiples et les bloquer dans le Firewall Windows des systèmes. Cette opération peut être automatisée avec des solutions spécifiques.
- Réduire le nombre d'administrateurs locaux, les rendre uniques et identifiables ; limiter le nombre d'utilisateurs qui peuvent se connecter à l'aide de RDP.
- Mettre en place un plan de sauvegarde et de récupération en cas de sinistre pour vos fichiers et votre Active Directory (d'autant plus que beaucoup de ces attaques visent les serveurs Windows). Ici aussi, des solutions logicielles professionnelles peuvent aider.

Le dernier point est essentiel pour avoir une couverture complète. Même en déployant toutes les mesures de protection existantes, une attaque peut aboutir. Il vous faudra alors avoir une stratégie de récupération et de reprise efficace afin de limiter l'impact sur les opérations de l'organisation que vous défendez.

L'utilisation d'un système d'accès disant autre que RDP n'est pas une solution. Kaspersky a en effet identifié 37 vulnérabilités non corrigées dans les implémentations VNC fin 2019[3].

[1] https://www.kaspersky.com/blog/vnc-vulnerabilities/31462/

[2] https://securelist.com/remote-spring-the-rise-of-rdp-bruteforce-attacks/96820/
[3] https://www.kaspersky.com/blog/vnc-vulnerabilities/31462/