DearCry : un ransomware spécial serveurs Exchange ?

Attraper un *ransomware* ? Sur les serveurs Exchange exposés à la faille ProxyLogon, le risque n'est plus seulement théorique. Et il a un nom : DearCry.

Le 9 mars, des échantillons avaient commencé à remonter vers les principales plates-formes d'analyse des menaces. À un volume relativement faible, mais en provenance d'au moins trois continents.

> *Currently seen victim companies from the following countries: Canada, Denmark, United States, Australia, Austria.*
> *First victim seen on March 9, at around noon.*
> *Can't tell for now how they got in, but anyhow, patching is important people! https://t.co/40vp5v2n8N*
>
> *— MalwareHunterTeam (@malwrhunterteam) March 11, 2021*

Depuis lors, Microsoft a confirmé avoir détecté – et bloqué – DearCry. Pour lui, il ne s'agit pas simplement d'un ransomware, mais de toute une famille. Trois souches (1, 2, 3) semblent en l'occurrence se détacher.

> *Microsoft Defender customers utilizing automatic updates do not need to take additional action to receive these protections. On-premises Exchange Server customers should prioritize the security updates outlined here: https://t.co/DL1XWnitYO*
>
> *— Microsoft Security Intelligence (@MsftSecIntel) March 12, 2021*

DearCry donne, notamment au niveau de son mécanisme de chiffrement, l'impression d'avoir été codé à la va-vite. Le nom qu'on lui a donné fait référence à la chaîne de caractères « DEARCRY! » ajoutée au début de chacun des fichiers qu'il chiffre. L'extension qu'il utilise (.CRYPT) est un classique dans cet univers. La note de rançon aussi, même si elle contient un hash différent pour chaque victime. Certains l'ont trouvée en plusieurs exemplaires : Bureau, dossiers Images et Téléchargements… L'un des utilisateurs qui témoignent dans ce sens précise qu'on lui a demandé 1/3 de bitcoin (soit environ 16 000 €).

DearCry : l'effet PoC ?

D'après ESET, au moins une dizaine de groupes cybercriminels ont exploité tout ou partie des failles qui touchent les serveurs Exchange. Au moins quatre paraissent en avoir eu connaissance avant leur révélation.

Voilà dix jours que les correctifs sont disponibles. Mais les serveurs vulnérables se compteraient encore par dizaines de milliers. Or, l'exploitation de ProxyLogon y est désormais facilitée par l'existence de démonstrations techniques et de PoC. Microsoft a décidé, au nom de la sécurité, de supprimer l'un d'entre eux, hébergé sur sa plate-forme GitHub. L'initiative n'a pas été du goût de tous.

> *Yep. If the policy from the start was no PoC/metasploit/etc – that would suck, but it's their service. Instead they said OK, and now that its become the standard for security pros to share code, they have elected themselves the arbiters of what is « responsible ». How convenient.*
>
> *— Tavis Ormandy (@taviso) March 11, 2021*

Le PoC n'a pas disparu de la circulation. Il reste accessible sur des plates-formes concurrentes. Il n'est pas pleinement fonctionnel, mais quelques adaptations suffisent à en faire un outil d'exécution de code à distance.

> *Hafnium Exchange RCE Exploit*
> *I've confirmed there is a public PoC floating around for the full RCE exploit chain. It's has a couple bugs but with some fixes I was able to get shell on my test box.*
>
> *— MalwareTech (@MalwareTechBlog) March 10, 2021*

Illustration principale © vege – Fotolia