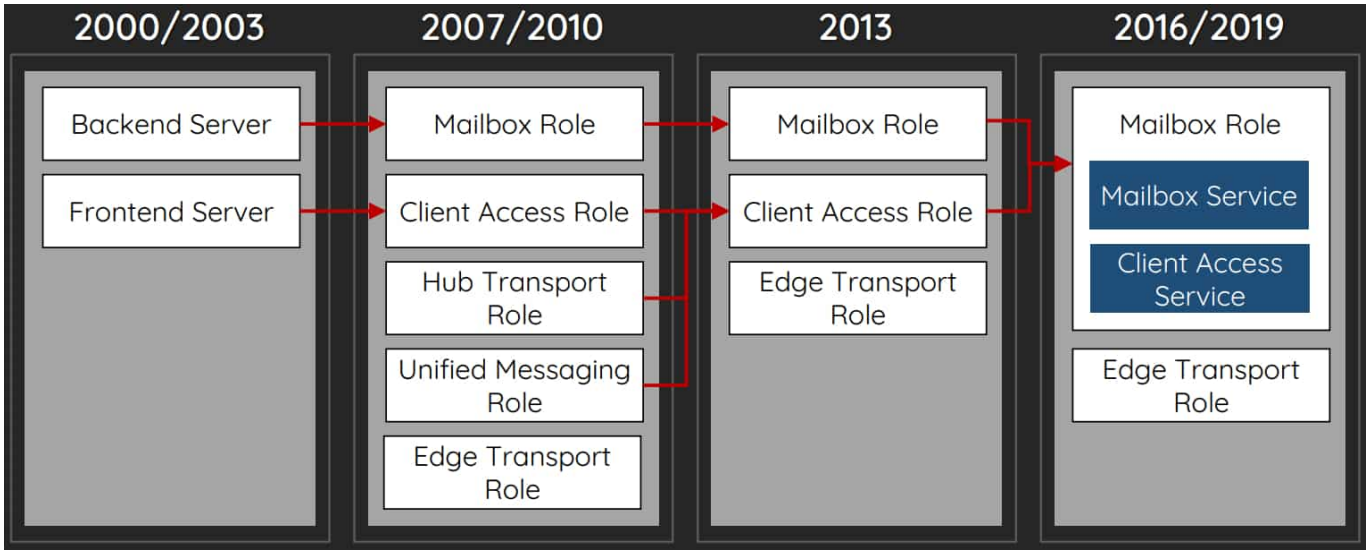
Exchange : une forêt de failles derrière ProxyLogon

Pirater Exchange ? Pour ça, il y a les services d'accès client (CAS). Aujourd'hui intégrés aux serveurs de boîte aux lettres, ils jouent en particulier le rôle de proxy pour les connexions internes et externes. C'est sur eux que se fonde la faille dite ProxyLogon. Microsoft l'avait corrigée début mars. Le chercheur qui lui en avait signalé l'existence quelques semaines en amont ne s'est pas arrêté là. Toujours en s'appuyant sur les CAS, il a déniché d'autres vulnérabilités, regroupées sous les bannières **ProxyOracle** et **ProxyShell**. On en a eu des démos ce mois-ci à la Black Hat USA, puis à la DEFCON. Le tout accompagné d'une série de posts.

Report Time	Name	CVE	Patch Time	Reported by
Jan 05, 2021	ProxyLogon	CVE-2021-26855	Mar 02, 2021	Orange Tsai, Volexity and MSTIC
Jan 05, 2021	ProxyLogon	CVE-2021-27065	Mar 02, 2021	Orange Tsai, Volexity and MSTIC
Jan 17, 2021	ProxyOracle	CVE-2021-31196	Jul 13, 2021	Orange Tsai
Jan 17, 2021	ProxyOracle	CVE-2021-31195	May 11, 2021	Orange Tsai
Apr 02, 2021	ProxyShell (Pwn2Own Bug)	CVE-2021-34473	Apr 13, 2021	Orange Tsai (Working with ZDI)
Apr 02, 2021	ProxyShell (Pwn2Own Bug)	CVE-2021-34523	Apr 13, 2021	Orange Tsai (Working with ZDI)
Apr 02, 2021	ProxyShell (Pwn2Own Bug)	CVE-2021-31207	May 11, 2021	Orange Tsai (Working with ZDI)

Il fut un temps, les CAS étaient un composant indépendant dans Exchange. Leur positionnement a évolué, d'édition en édition du logiciel, à mesure que Microsoft en révisait l'architecture. La démarche a induit, au nom de la compatibilité, des compromis… qui ont ouvert les failles en question.



Par « ProxyLogon », le chercheur entend deux failles. La principale (CVE-2021-26855) permet de

contourner l'authentification en envoyant, via Outlook Web Access, des requêtes HTTP arbitraires ers des ressources statiques. Elle ouvre la voie à l'exploitation de la seconde faille (CVE-2021-27065). Laquelle a notamment entraîné, dans la pratique, l'injection de *webshells*. On a trouvé trace d'un groupe cybercriminel exploitant, aux mêmes fins, deux autres vulnérabilités, dont l'une permettant une élévation de privilèges.

Exchange : le filon des CAS

Quelques jours après s'être vu signaler l'existence de ProxyLogon, Microsoft avait été averti du vecteur d'attaque ProxyOracle. Là aussi, il combine deux failles, patchées respectivement en mai et en juillet. Dans les grandes lignes, elles permettent de récupérer des mots de passe en clair, en exploitant un défaut dans la synchronisation des identités au niveau des CAS. Comme avec ProxyLogon, cela tient en partie à un cookie.

Au printemps, ce fut le tour de ProxyShell. Avec trois failles, colmatées entre avril et mai. Et la même conséquence que ProxyLogon : injection de code à distance au travers du port 443. Mais des moyens différents ; entre autres, une élévation de privilèges sur le *back-end* PowerShell (CVE-2021-34523). Il a en outre fallu contourner des protections ajoutées à Defender après l'épisode ProxyLogon.

Illustration principale © Patrick Hermans – Adobe Stock