Les Ã‰tats-Unis victimes dâ€™une gigantesque opÃ©ration de cyberespionnage

Description

Dans le cyberespace, le gouvernement des Ã‰tats-Unis, premiÃ¨re puissance mondiale et Microsoft, lâ€™une des entreprises amÃ©ricaines les plus rentables de la planÃ¨te ont fait figure de gÃ©ants aux pieds dâ€™argile face Ã lâ€™ampleur de la plus grande opÃ©ration de cyberespionnage dont ils ont Ã©tÃ© victimes pendant prÃ¨s de neuf mois, sans jamais sâ€™en apercevoir.

Lâ€™opÃ©ration aurait dÃ©butÃ© en mars 2020. Elle a Ã©tÃ© dÃ©voilÃ©e par la sociÃ©tÃ© de cybersÃ©curitÃ© FireEye le 13 dÃ©cembre 2020, elle-mÃªme victime de cyberattaques.Â Il sâ€™agit dâ€™uneÂ *Advanced Persistent Threat*, uneÂ Â«Â menace persistante avancÃ©eÂ Â»Â qualifiÃ©e de majeure, selon la typologie propre au secteur de la sÃ©curitÃ© informatique.Â Ce type dâ€™opÃ©ration prend la forme dâ€™un piratage informatique furtif et continu dont lâ€™objectif est de rester inaperÃ§u le plus longtemps possible.Â Selon le Centre gouvernemental de veille, d’alerte et de rÃ©ponse aux attaques informatiques (CERT-FR), responsable de l’alerte franÃ§aise,Â il sâ€™agit plus prÃ©cisÃ©ment dâ€™uneÂ *Â«Â attaque par la chaÃ®ne d’approvisionnementÂ Â»*Â :Â au lieu de sâ€™attaquer directement Ã une grande entreprise ou aux services informatiques dâ€™une administration publique, les pirates visent un acteur secondaire, plus vulnÃ©rable,Â qui fournit des services aux cibles visÃ©es. Le choix des pirates sâ€™est portÃ© sur la sociÃ©tÃ© amÃ©ricaine SolarWinds, ainsi que sur des revendeurs de logiciels cloud de Microsoft.

SolarWinds offre des logiciels professionnels de gestion centralisÃ©e des rÃ©seaux, systÃ¨mes etÂ infrastructuresÂ informatiques Ã quelqueÂ 330 000Â clients dans le monde, parmi lesquels de nombreuses agences fÃ©dÃ©rales amÃ©ricaines, quasiment toutes les sociÃ©tÃ©s du Fortune 500 et les dix premiers opÃ©rateurs de tÃ©lÃ©communications amÃ©ricains.

Les pirates ont rÃ©ussi Ã introduire unÂ *malware*Â (logiciel malveillant) nommÃ©Â Â«Â SunburstÂ Â», quelques lignes de code informatique malveillant compromettant le systÃ¨me de mise Ã jour du logiciel Orion, dÃ©veloppÃ© par SolarWinds et utilisÃ© parÂ 33 000Â clients.Â 18 000Â dâ€™entre eux ont effectuÃ© la mise Ã jour de mars 2020 et, sans le savoir, ont infectÃ© le rÃ©seau que le logiciel Ã©tait censÃ© surveiller. Une fois installÃ© sur un serveur,Â leÂ *malware*Â Sunburst restait inactif pendant 12 Ã 14 jours,Â afin de sâ€™assurer quâ€™il Ã©tait bien passÃ© inaperÃ§u. Puis il envoyait des informations basiques Ã lâ€™attaquantÂ *viaÂ* le domaine avsvmcloud.com afin dâ€™identifier une potenÂtielle victime, puis dÃ©cider si celle-ci mÃ©ritait dâ€™Ãªtre espionnÃ©e plus en dÃ©tails.

Le directeur intÃ©rimaire de l’Agence de cybersÃ©curitÃ© et de sÃ©curitÃ© desÂ infrastructures, Brandon Wales, a affirmÃ© quâ€™*Â«Â environ 30 % des victimes du secteur privÃ© et du gouvernement liÃ©es Ã la campagneÂ*

[dâ€™espionnage]Â *n'avaient aucun lien direct avec SolarWindsÂ Â»*. Lorsquâ€™ils ne sont pas passÃ©s par le logiciel Orion, les pirates ont, selon les enquÃªteurs,Â *Â«Â pÃ©nÃ©trÃ© dans ces systÃ¨mes en exploitantÂ des bogues connus dans les logiciels, en devinant des mots de passe en ligne et en tirant parti d'une variÃ©tÃ© de problÃ¨mes dans la faÃ§on dont le logiciel de Microsoft est configurÃ©Â Â»*.

Ã€ nouveau, lâ€™intrusion nâ€™a pas directement portÃ© sur lâ€™entreprise Microsoft mais sur des revendeurs de logiciels, notamment du logiciel Office 365 de la firme de Redmond. Ces revendeurs de logiciels Microsoft dans le cloud sont chargÃ©s de mettre en place et dâ€™assurer la maintenance des logiciels au sein des entreprises clientes. Comme lâ€™explique un expert en cybersÃ©curitÃ© dans des propos rapportÃ©s par leÂ *New York Times*,Â *Â«Â les entreprises peuvent traquer les attaques de phishing* Â (hameÃ§onnage)*Â et les logiciels malveillants autant qu'elles le souhaitent, mais tant qu'elles feront aveuglÃ©ment confiance aux fournisseurs et aux services de cloud computing comme Microsoft, Salesforce Google's G-Suite, Zoom, Slack, SolarWinds et d'autres â€“ et qu'elles leur donneront un large accÃ¨s au courrier Ã©lectronique des employÃ©s et aux rÃ©seaux d'entreprise â€“, elles ne seront jamais en sÃ©curitÃ©Â Â»*.

En janvier 2021, le nom de domaine avsvmcloud.com utilisÃ© par les pirates a Ã©tÃ© saisi par Microsoft, accompagnÃ© dâ€™une coalition d'entreprises technologiques, afin dâ€™intercepter les requÃªtes provenant de tous les systÃ¨mes sur lesquels la version compromise dâ€™Orion avait Ã©tÃ© installÃ©e. Cette technique informatique, appelÃ©eÂ *Â«Â sinkholingÂ Â»*, donne Ã Microsoft la possibilitÃ© dâ€™avertir toutes les victimes infectÃ©es par lâ€™incident deÂ sÃ©curitÃ©.

Le gouvernement amÃ©ricain semble avoir Ã©tÃ© la principale cible de lâ€™opÃ©ration de cyberespionnage. Parmi les administrations touchÃ©es figurent notamment les dÃ©partements du Commerce, du TrÃ©sor, de l'IntÃ©rieur, de l'Ã‰nergie, de la DÃ©fense, de la SantÃ© et des Services sociaux, ainsi que la National Telecommunications and Information Administration (NTIA). Il a Ã©gaÂ-lement Ã©tÃ© Ã©tabli que les pirates informatiques ont accÃ©dÃ© aux systÃ¨mes de l'Administration nationale de la sÃ©curitÃ© nuclÃ©aire, sous la responsabilitÃ© de laquelle est placÃ© le stock d'armes nuclÃ©aires des Ã‰tats-Unis. Si l'ampleur de l'attaque reste encore inconnue,Â certaines agences gouvernementales amÃ©ricaines parmi les plus importantes sur le plan de la sÃ©curitÃ© nationale du pays ont Ã©tÃ© assurÃ©ment espionnÃ©es en continu pendant prÃ¨s de neuf mois.Â Le niveau de technicitÃ© comme de coordination de lâ€™opÃ©ration incite Ã croire que seule une Ã©quipe de hackers soutenue par un Ã‰tat est en mesure de mener Ã bien une telle opÃ©ration.

Les commanditaires

DÃ¨s dÃ©cembre 2020, Mike Pompeo, alors secrÃ©taire dâ€™Ã‰tat du gouvernement amÃ©ricain, a publiquement accusÃ© la Russie dâ€™avoir menÃ© cette opÃ©ration, malgrÃ© les dÃ©clarations contradictoires de lâ€™ancien locataire de la Maison Blanche accusant de son cÃ´tÃ© la Chine sans plus de preuves. Lâ€™opÃ©ration de cyberespionnage aura donc durÃ© neuf mois sans que, dâ€™une part, les autoritÃ©s amÃ©ricaines sâ€™en aperÃ§oivent et, dâ€™autre part, sans quâ€™elles soient en mesure de

rÃ©agir efficacement. Et pour cause,Â le poste de coordinateur de la cybersÃ©curitÃ© Ã la Maison Blanche a Ã©tÃ© supprimÃ© en 2018 par Donald Trump et le directeur de la Cybersecurity and Infrastructure Security Agency (CISA), le plus haut responÂsable de la cybersÃ©curitÃ© du pays, confirmÃ© par le SÃ©nat, a Ã©tÃ© limogÃ©Â par lâ€™ancien prÃ©sident le 18 novembre 2020. Signe des fortes tensions entre les deux pays, le dÃ©parÂtement dâ€™Ã‰tat amÃ©ricain a fermÃ©, en dÃ©cembre 2020, ses deux derniers consulats en Russie, Ã Vladivostok et Ekaterinbourg, et a conservÃ© lâ€™ambassade de Moscou comme unique relais diplomatique sur place.

Le 5 janvier 2021, le FBI, la direction du renseignement intÃ©rieur, lâ€™agence militaire NSA et lâ€™agence amÃ©ricaine chargÃ©e de la cybersÃ©curitÃ© et de la sÃ©curitÃ© desÂ infrastructures (CISA) ont Ã©galement conclu, dans un communiquÃ© commun, que la Russie Ã©taitÂ *Â«Â probaÂ-blementÂ Â»Â* Ã lâ€™origine de cette opÃ©ration de cyberÂespionnage. Abondant dans le mÃªme sens, lâ€™entreprise de cybersÃ©curitÃ© Kaspersky a dÃ©clarÃ© dÃ©but 2021 que leÂ *malware* Â ressemblait fortement Ã celui baptisÃ© Kazuar qui aurait Ã©tÃ© crÃ©Ã© par Turla, un groupe de pirates repÃ©rÃ© depuis 2008 et reliÃ© au FSB, service de sÃ©curitÃ© fÃ©dÃ©ral russe, selon les informations des services de renseignement estoniens. Pour les spÃ©cialistes de la sÃ©curitÃ© informatique,Â cela fait peu de doute que le pays dirigÃ© par Vladimir Poutine soit Ã lâ€™origine de la plus grande opÃ©ration de cyberespionnage Ã laquelle les Ã‰tats-Unis ont eu Ã faire face.Â Il sâ€™agirait de pirates russes, connus sous le nom dâ€™APT29 ou encore Cozy Bear, appartenant au service de renseignement Ã©tranger de la Russie, le SVR, dÃ©jÃ Ã lâ€™origine du piratage des serveurs de courrier Ã©lectronique du dÃ©partement d’Ã‰tat et de la Maison Blanche pendant l’administration Obama.

Comme Ã son habitude, l’ambassade de Russie Ã Washington a qualifiÃ© ces allÃ©gations comme Ã©tantÂ *Â«Â sans fondementÂ Â»*, tout en dÃ©clarantÂ *viaÂ* son compte Facebook queÂ *Â«Â les attaques dans l’espace d’information contredisentÂ Â»*Â la politique Ã©trangÃ¨re et les intÃ©rÃªts nationaux de la Russie, pays quiÂ *Â«Â ne mÃ¨ne pas d’opÃ©rations offensivesÂ Â»*Â dans le domaine cybernÃ©tique.

Sources :

- Â« Le chasseur de pirates informatiques FireEye piratÃ© Â», Virginie Montet, AFP, 9 dÃ©cembre 2020.
- Â« Russian government hackers are behind a broad espionage campaign that has compromised U.S. agencies, including Treasury and Commerce Â», Ellen Nakashima, Craig Timberg, washingtonpost.com, December 14, 2020.
- Â« Des comptes de messagerie du TrÃ©sor amÃ©ricain visÃ©s par une vaste opÃ©ration de cyberespionnage Â»,Â *Le Monde* avec AFP, 22 dÃ©cembre 2020.
- Â« Russians Are Believed to Have Used Microsoft Resellers in Cyberattacks Â», Nicole Perlroth, nytimes.com, December 24, 2020.
- Â« SolarWinds : Les entreprises amÃ©ricaines Ã la manÅ“uvre pour contenir la menace Â», Catalin Cimpanu, zdnet.fr, 5 janvier 2021.
- Â« Les Ã‰tats-Unis estiment la Russie Â«Â probablementÂ Â» Ã lâ€™origine de la cyberattaque

dont ils ont Ã©tÃ© victimes Â», *Le Monde* avec AFP, 6 janvier 2021.
- Â« Cyberattaques : la lourde facture de l'administration amÃ©ricaine Â», Nicolas Rauline, *Les Echos* , 26 janvier 2021.
- Â« Lâ€™affaire SolarWinds, une des opÃ©rations de cyberespionnage Â«Â les plus sophistiquÃ©es de la dÃ©cennieÂ Â» Â», Martin Untersinger, *Le Monde* – Pixels, 27 janvier 2021.
- Â« Suspected Russian Hack Extends Far Beyond SolarWinds Software, Investigators Say Â», Robert McMillan, Dustin Volz, wsj.com, January 29, 2021.
- Â« SolarWinds : A Hack of Nuclear Proportions Â», Pessin Katz Law, P.A., jduspra.com, February 1, 2021.
- Â« Une sociÃ©tÃ© de cybersÃ©curitÃ© a identifiÃ© trois nouvelles failles dans les produits de SolarWinds Â», Valentin Cimino, siecledigital.fr, 7 fÃ©vrier 2021.
- Â« 2020 United States federal government data breach Â», en.wikipedia.org, retrieved February 15, 2021.

Categorie

1. Ailleurs

date crÃ©Ã©e
1 juillet 2021
Auteur
jacquesandrefines