

Les États-Unis victimes d'une gigantesque opération de cyberespionnage

Description

Dans le cyberspace, le gouvernement des États-Unis, première puissance mondiale et Microsoft, l'une des entreprises américaines les plus rentables de la planète ont fait figure de géants aux pieds d'argile face à l'ampleur de la plus grande opération de cyberespionnage dont ils ont été victimes pendant près de neuf mois, sans jamais s'en apercevoir.

L'opération aurait débuté en mars 2020. Elle a été dévoilée par la société de cybersécurité FireEye le 13 décembre 2020, elle-même victime de cyberattaques. Il s'agit d'une *Advanced Persistent Threat*, une « menace persistante avancée » qualifiée de majeure, selon la typologie propre au secteur de la sécurité informatique. Ce type d'opération prend la forme d'un piratage informatique furtif et continu dont l'objectif est de rester inaperçu le plus longtemps possible. Selon le Centre gouvernemental de veille, d'alerte et de réponse aux attaques informatiques (CERT-FR), responsable de l'alerte française, il s'agit plus précisément d'une « *attaque par la chaîne d'approvisionnement* » : au lieu de s'attaquer directement à une grande entreprise ou aux services informatiques d'une administration publique, les pirates visent un acteur secondaire, plus vulnérable, qui fournit des services aux cibles visées. Le choix des pirates s'est porté sur la société américaine SolarWinds, ainsi que sur des revendeurs de logiciels cloud de Microsoft.

SolarWinds offre des logiciels professionnels de gestion centralisée des réseaux, systèmes et infrastructures informatiques à quelque 330 000 clients dans le monde, parmi lesquels de nombreuses agences fédérales américaines, quasiment toutes les sociétés du Fortune 500 et les dix premiers opérateurs de télécommunications américains.

Les pirates ont réussi à introduire un *malware* (logiciel malveillant) nommé « Sunburst », quelques lignes de code informatique malveillant compromettant le système de mise à jour du logiciel Orion, développé par SolarWinds et utilisé par 33 000 clients. 18 000 d'entre eux ont effectué la mise à jour de mars 2020 et, sans le savoir, ont infecté le réseau que le logiciel était censé surveiller. Une fois installé sur un serveur, le *malware* Sunburst restait inactif pendant 12 à 14 jours, afin de s'assurer qu'il était bien passé inaperçu. Puis il envoyait des informations basiques à l'attaquant *via* le domaine avsvmcloud.com afin d'identifier une potentielle victime, puis décider si celle-ci méritait d'être espionnée plus en détails.

Le directeur intérimaire de l'Agence de cybersécurité et de sécurité des infrastructures, Brandon Wales, a affirmé qu'« *environ 30 % des victimes du secteur privé et du gouvernement liées à la campagne [d'espionnage] n'avaient aucun lien direct avec SolarWinds* ». Lorsqu'ils ne sont pas passés par le logiciel Orion, les pirates ont, selon les enquêteurs, « *pénétré dans ces systèmes en exploitant des bogues connus dans les logiciels, en devinant des mots de passe en ligne et en tirant parti d'une variété de problèmes dans la façon dont le logiciel de Microsoft est configuré* »

À nouveau, l'intrusion n'a pas directement porté sur l'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 chargés de mettre en place et d'assurer la maintenance des logiciels au sein des entreprises clientes. Comme l'explique un expert en cybersécurité dans des propos rapportés par le *New York Times*, « *les entreprises peuvent traquer les attaques de phishing (hameçonnage) et les logiciels malveillants autant qu'elles le souhaitent, mais tant qu'elles feront aveuglément confiance aux fournisseurs et aux services de cloud computing comme Microsoft, Salesforce Google's G-Suite, Zoom, Slack, SolarWinds et d'autres – et qu'elles leur donneront un large accès au courrier électronique des employés et aux réseaux d'entreprise –, elles ne seront jamais en sécurité* ».

En janvier 2021, le nom de domaine avsvmcloud.com utilisé par les pirates a été saisi par Microsoft, accompagné d'une coalition d'entreprises technologiques, afin d'intercepter les requêtes provenant de tous les systèmes sur lesquels la version compromise d'Orion avait été installée. Cette technique informatique, appelée « *sinkholing* », donne à Microsoft la possibilité d'avertir toutes les victimes infectées par l'incident de sécurité.

Le gouvernement américain semble avoir été la principale cible de l'opération de cyberespionnage. Parmi les administrations touchées figurent notamment les départements du Commerce, du Trésor, de l'Intérieur, de l'Énergie, de la Défense, de la Santé et des Services sociaux, ainsi que la National Telecommunications and Information Administration (NTIA). Il a également été établi que les pirates informatiques ont accédé aux systèmes de l'Administration nationale de la sécurité nucléaire, sous la responsabilité de laquelle est placé le stock d'armes nucléaires des États-Unis. Si l'ampleur de l'attaque reste encore inconnue, certaines agences gouvernementales américaines parmi les plus importantes sur le plan de la sécurité nationale du pays ont été assurément espionnées en continu pendant près de neuf mois. Le niveau de technicité comme de coordination de l'opération incite à croire que seule une équipe de hackers soutenue par un État est en mesure de mener à bien une telle opération.

Les commanditaires

Dès décembre 2020, Mike Pompeo, alors secrétaire d'État du gouvernement américain, a publiquement accusé la Russie d'avoir mené cette opération, malgré les déclarations contradictoires de l'ancien locataire de la Maison Blanche accusant de son côté la Chine sans plus de preuves. L'opération de cyberespionnage aura donc duré neuf mois sans que, d'une part, les autorités américaines s'en aperçoivent et, d'autre part, sans qu'elles soient en mesure de réagir efficacement. Et pour cause, le poste de coordinateur de la cybersécurité à la Maison Blanche a été supprimé en 2018 par Donald Trump et le directeur de la Cybersecurity and Infrastructure Security Agency (CISA), le plus haut responsable de la cybersécurité du pays, confirmé par le Sénat, a été limogé par l'ancien président le 18 novembre 2020. Signe des fortes tensions entre les deux pays, le département d'État américain a fermé, en décembre 2020, ses deux derniers consulats en Russie, à Vladivostok et Ekaterinbourg, et a conservé l'ambassade de Moscou comme unique

relais diplomatique sur place.

Le 5 janvier 2021, le FBI, la direction du renseignement intérieur, l'agence militaire NSA et l'agence américaine chargée de la cybersécurité et de la sécurité des infrastructures (CISA) ont également conclu, dans un communiqué commun, que la Russie était « *probablement* » à l'origine de cette opération de cyber-espionnage. Abondant dans le même sens, l'entreprise de cybersécurité Kaspersky a déclaré début 2021 que le *malware* ressemblait fortement à celui baptisé Kazuar qui aurait été créé par Turla, un groupe de pirates repéré depuis 2008 et relié au FSB, service de sécurité fédéral russe, selon les informations des services de renseignement estoniens. Pour les spécialistes de la sécurité informatique, cela fait peu de doute que le pays dirigé par Vladimir Poutine soit à l'origine de la plus grande opération de cyberespionnage à laquelle les États-Unis ont eu à faire face. Il s'agirait de pirates russes, connus sous le nom d'APT29 ou encore Cozy Bear, appartenant au service de renseignement étranger de la Russie, le SVR, déjà à l'origine du piratage des serveurs de courrier électronique du département d'État et de la Maison Blanche pendant l'administration Obama.

Comme à son habitude, l'ambassade de Russie à Washington a qualifié ces allégations comme étant « *sans fondement* », tout en déclarant *via* son compte Facebook que « *les attaques dans l'espace d'information contredisent* » la politique étrangère et les intérêts nationaux de la Russie, pays qui « *ne mène pas d'opérations offensives* » dans le domaine cybernétique.

Sources :

- « Le chasseur de pirates informatiques FireEye piraté », Virginie Montet, AFP, 9 décembre 2020.
- « Russian government hackers are behind a broad espionage campaign that has compromised U.S. agencies, including Treasury and Commerce », Ellen Nakashima, Craig Timberg, *washingtonpost.com*, December 14, 2020.
- « Des comptes de messagerie du Trésor américain visés par une vaste opération de cyberespionnage », *Le Monde* avec AFP, 22 décembre 2020.
- « Russians Are Believed to Have Used Microsoft Resellers in Cyberattacks », Nicole Perlroth, *nytimes.com*, December 24, 2020.
- « SolarWinds : Les entreprises américaines à la manœuvre pour contenir la menace », Catalin Cimpanu, *zdnnet.fr*, 5 janvier 2021.
- « Les États-Unis estiment la Russie « probablement » à l'origine de la cyberattaque dont ils ont été victimes », *Le Monde* avec AFP, 6 janvier 2021.
- « Cyberattaques : la lourde facture de l'administration américaine », Nicolas Rauline, *Les Echos*, 26 janvier 2021.
- « L'affaire SolarWinds, une des opérations de cyberespionnage « les plus sophistiquées de la décennie » », Martin Untersinger, *Le Monde – Pixels*, 27 janvier 2021.
- « Suspected Russian Hack Extends Far Beyond SolarWinds Software, Investigators Say », Robert McMillan, Dustin Volz, *wsj.com*, January 29, 2021.
- « SolarWinds : A Hack of Nuclear Proportions », Pessin Katz Law, P.A., *jduspra.com*, February 1, 2021.

-
- « Une société de cybersécurité a identifié trois nouvelles failles dans les produits de SolarWinds », Valentin Cimino, siecledigital.fr, 7 février 2021.
 - « 2020 United States federal government data breach », en.wikipedia.org, retrieved February 15, 2021.

Categorie

1. Ailleurs

date créée

1 juillet 2021

Auteur

jacquesandrefines