PARIS : Jian – Le cyber-sabre chinois à double tranchant

Au cours des derniers mois, Check Point Research (CPR) s'est concentré sur les récents exploits de Windows Local Privilege Escalation (LPE) attribués à des acteurs chinois.

Faits marquants :

· Un groupe d'attaque chinois (APT31) a cloné et activement utilisé le code de l'outil cyber-offensif d'un groupe d'attaque associé aux Etats Unis (Equation Group) appelé « *EpMe* ».

· Les deux outils d'attaque exploitent une vulnérabilité Windows alors inconnue (CVE-2017-0005), pour élever les privilèges de l'assaillant sur la machine infectée.

· « *Jian* » est la version américaine de l'outil, clonée par APT31 en 2014. Cette version clonée chinoise a été utilisée à son tour depuis 2015 au moins, jusqu'à ce qu'elle soit finalement interceptée et corrigée en mars 2017.

· « *Jian* » a été signalé à Microsoft par l'équipe de réponse aux incidents informatiques de Lockheed Martin, laissant entrevoir une possible attaque contre une cible américaine.

Présentation

Ce LPE est utilisé par les assaillants pour acquérir des droits d'administrateur sur une machine Windows. Au cours de cette enquête, nos chercheurs en logiciels malveillants et en vulnérabilités ont réussi à dévoiler l'histoire et les origines cachées de « Jian », un exploit qui était auparavant attribué au groupe d'attaque chinois APT31 (Zirconium). L'outil d'attaque a été découvert et signalé à Microsoft par l'équipe de réponse aux incidents informatiques de Lockheed

Martin, suggérant une possible attaque contre une cible américaine.

Conclusions

Par souci de concision, nous avons baptisé l'exploitation APT31 « *Jian* ». Au cours de cette enquête, nos chercheurs ont réussi à démêler l'histoire cachée derrière « *Jian* », nom d'un sabre à double tranchant utilisée en Chine. L'exploitation « *Jian* » était auparavant attribuée à APT31 (Zirconium), et nous en avons maintenant découvert les véritables origines.

Nos recherches montrent que CVE-2017-0005, une vulnérabilité de Windows LPE qui a été attribuée à un APT chinois, a été reproduite sur la base d'un exploit de l'Equation Group pour la même vulnérabilité à laquelle l'APT avait accès. « *EpMe* », l'exploit de l'Equation Group pour CVE-2017-0005, est l'un des 4 différents exploits LPE inclus dans le cadre d'attaque DanderSpritz. DanderSpritz est le cadre de post-exploitation de l'Equation Group qui contient une grande variété d'outils pour la persistance, la reconnaissance, le mouvement latéral, le contournement des moteurs antivirus, et plus encore. « *EpMe* » remonte au moins à 2013, soit quatre ans avant qu'on ne réalise qu'APT31 exploitait sa vulnérabilité sur le terrain.

Sur notre blog technique, nous présentons les quatre différents exploits Windows LPE compris dans le cadre DanderSpritz, révélant un code d'exploitation supplémentaire appelé « *EpMo* ». « *EpMo* », l'un des exploits du cadre, n'a jamais été discuté publiquement et la vulnérabilité inconnue qu'il vise a été corrigée par Microsoft en mai 2017 sans qu'aucune annonce ne soit faite. Le patch pourrait potentiellement être associé aux séquelles de la fuite des Shadow Brokers des outils de l'Equation Group. Bien que la vulnérabilité ait été corrigée, nous n'avons pas pu identifier l'identité officielle (CVE-ID) qui lui est associée, et à notre connaissance, c'est la première mention publique de l'existence de cette vulnérabilité supplémentaire de

l’Equation Group.

Chronologie de ce qui avait commencé comme « *EpMe* » (Equation Group) et a finalement été corrigé par Microsoft sous le nom de CVE-2017-0005 (« *Jian* » de APT31)

Synthèse

Nos recherches ont commencé par l’analyse de *« Jian »,* l’exploit chinois (APT31 / Zirconium) de CVE-2017-0005, qui a été signalé par l’équipe de réponse aux incidents informatiques de Lockheed Martin. À notre grande surprise, nous avons découvert que cet exploit APT31 était en fait une version reconstituée d’un exploit de l’Equation Group, baptisé « *EpMe* ». Cela signifie qu’un groupe chinois a utilisé un exploit de l’Equation Group pour potentiellement attaquer des cibles américaines.

Le cas de « *EpMe » / « Jian* » est unique en son genre, car nous avons prouvé que « *Jian »* a été conçu à partir de l’échantillon réel de l’exploit de l’Equation Group. Ayant daté les échantillons d’APT31 à 3 ans avant la fuite du Shadow Broker, nous estimons que les échantillons exploités par l’Equation Group auraient pu être acquis par l’APT chinois de l’une des manières suivantes :

? Capturé lors d’une opération du réseau de l’Equation Group sur une cible chinoise

? Capturé lors d’une opération de l’Equation Group sur un réseau tiers qui était également surveillé par l’APT chinois

? Capturé par l’APT chinois lors d’une attaque sur l’infrastructure de l’Equation Group

A propos de Check Point Software Technologies Ltd.

Check Point Software Technologies Ltd. (www.checkpoint.com) est l’un des principaux fournisseurs de solutions de cybersécurité pour les gouvernements et les entreprises dans

le monde. Ses solutions protègent les clients contre les cyberattaques de 5e génération grâce à un taux de blocage inégalé des logiciels malveillants, des logiciels rançonneurs et autres types d’attaques. Check Point propose Infinity Total Protection avec prévention avancée des menaces de 5e génération, une architecture de sécurité à plusieurs niveaux, qui défend les données des entreprises dans le Cloud, les réseaux et les appareils mobiles. Check Point fournit le système d’administration unifiée de la sécurité le plus complet et le plus intuitif. Check Point protège plus de 100 000 entreprises de toute taille.