Volt Typhoon : en route vers le sabotage ?

Lucien Lagarde

18 juin 2023

Le 24 mai 2023, plusieurs agences étatiques américaines (dont la NSA, la CISA, le FBI), britanniques (NCSC), canadiennes (GCSB) et australiennes (ACSC, ASD) publiaient une Joint Cybersecurity Advisory au sujet d'un mode opératoire des attaquants (MOA) baptisé Volt Typhoon. Cette publication est elle-même accompagnée d'un billet de blog de l'éditeur Microsoft détaillant les tactiques, techniques et procédures (TTPs) de ce MOA.

Actif depuis mi-2021, Volt Typhoon serait associé aux autorités chinoises et se livrerait à des campagnes d'espionnage. La victimologie de ce mode opératoire apparait particulièrement large et en parfaite adéquation avec les centres d'intérêt de Pékin. Elle couvrirait le secteur des télécommunications, des services, des transports, les technologies de l'information, l'éducation, le maritime ainsi que les institutions gouvernementales. Dans son rapport, Microsoft met néanmoins l'emphase sur une campagne de Volt Typhoon qui ciblerait des infrastructures critiques à Guam et ailleurs aux États-Unis. Derrière une formulation prudente, l'éditeur américain suggère que ce MOA pourrait chercher à se prépositionner à des fins de sabotage :« Microsoft assesses with moderate confidence that this Volt Typhoon campaign is pursuing development of capabilities that could disrupt critical communications infrastructure between the United States and Asia region during future crises. »

Ce n'est pas la première que la Chine est accusée de se livrer à des opérations de pré positionnement à des fins de sabotage. En 2021, Recorded Future rapportait ainsi que le mode opératoire RedEcho aurait visé plusieurs infrastructures critiques du réseau électrique indien. Dénuée d'intérêt économique, une telle campagne aurait ainsi eu pour objectif, selon Recorded Future, d'être en mesure de réaliser des coupures de courant. Une hypothèse crédible dès lors que cette opération intervenait dans le contexte de tensions dans certains territoires frontaliers disputés par les deux puissances . Peu discrète, cette campagne aurait alors pu être en réalité un avertissement à destination des autorités indiennes. La Chine aurait cependant continué à cibler le secteur de l'énergie indien en 2022, utilisant notamment des objets connectés compromit comme serveurs de commande et de contrôle (C2) et aurait utilisé à cette même fin l'outil légitime FastReverseProxy.

En avril 2020, un acteur, associé à la Chine par l'éditeur de solution de cybersécurité Cycraft Technology, se serait, quant à lui, livré à des opérations de sabotage d'infrastructures vitales à Taiwan, en marge de l'inauguration du mandat du nouveau Président taiwanais, peu favorable à Pékin . Cette opération de sabotage avait néanmoins été déguisée en attaque par rançongiciel, suggérant une volonté de ses auteurs de brouiller les pistes et d'éviter une attribution trop simple de cette campagne.

Si des précédents existent donc, force est néanmoins de constater que le ciblage d'infra-

structures vitales américaines à des fins de prépositionnement – si avéré - constituerait la confirmation d'une évolution majeure des finalités de la lutte informatique offensive chinoise. En pareille hypothèse, Guam constituerait à n'en pas douter une cible de choix pour Pékin. Ce territoire des États-Unis constitue en effet une pièce maitresse du dispositif militaire américain dans le Pacifique ainsi qu'un nœud de communication majeur. Comme le rapporte le New York Times, Guam serait en particulier au centre de toute réponse américaine en cas d'invasion de Taiwan.

Au-delà de la possible finalité de ses campagnes, ce sont les TTPs de Volt Typhoon qui interpellent. En effet, ce mode opératoire semble chercher à rester discret au maximum. En témoigne par exemple l'utilisation de techniques dites Living off the land, c'est-à-dire l'utilisation d'outils et solutions légitimes déjà présents sur le système d'information compromis, et non de codes malveillants déployés pour l'occasion.

En outre, Volt Typhoon aurait également utilisé des routeurs d'entreprises et de particuliers (SOHO, pour Small Office/Home Office) comme Operation relay boxes (ORBs) afin de communiquer avec son infrastructure d'attaque. Cette technique permet, entre autres, à un attaquant de réduire la probabilité d'être détecté, notamment en utilisant des routeurs situés dans l'aire géographique de sa cible ; tout en rendant la cartographie de son infrastructure d'attaque plus compliquée. L'utilisation d'ORBs semble d'ailleurs une tendance grandissante chez les acteurs associés à la Chine, en témoignent les cas d'APT31 ou de Red Menshen. Cette technique fut d'ailleurs utilisée lors de la campagne précitée ciblant le grid indien, tout comme l'utilisation de l'outil légitime FastReverseProxy. Difficile néanmoins d'en tirer de réelle conclusion en matière d'imputation tant les modes opératoires associés à la Chine sont adeptes du partage de TTPs, d'outil et d'infrastructure.Discret au moment de l'accès initial et dans le choix de son infrastructure, les opérateurs de Volt Typhoon le semblent cependant beaucoup moins dans leurs actions sur les systèmes d'information de leurs victimes. Microsoft rapporte ainsi que :

« Once Volt Typhoon gains access to a target environment, they begin conducting hands-on-keyboard activity via the command line. Some of these commands appear to be exploratory or experimental, as the operators adjust and repeat them multiple times. »

En outre, les commandes exécutées par Volt Typhoon apparaissent particulièrement bruyantes :

Un tel manque de discrétion au moment de la post-exploitation n'est pas rare chez les opérateurs de modes opératoires associés à la Chine. Plusieurs hypothèses, non mutuellement exclusives, peuvent être formulées pour expliquer un tel comportement. Tout d'abord, il est possible que, face à des pénuries de main-d'œuvre, l'accès initial soit réservé aux meilleurs opérateurs. L'attaquant peut, par exemple, considérer (à tort ou à raison) qu'il est plus important d'éviter d'être détecté au moment de la compromission de sa victime, qu'aux étapes suivantes de l'opération. Il est également possible que les opérateurs cherchent à réduire leurs coûts, employant à ce stade des individus moins bien formés, ou tentent simplement d'agir le plus rapidement possible, quitte à être plus bruyants.

Un tel manque de discrétion interroge néanmoins dans le cadre d'une éventuelle opération de prépositionnement. En effet, un attaquant a tout intérêt à voler sous le radar de ses cibles afin de pérenniser son accès et de pouvoir l'utiliser à des fins de sabotage en cas de conflit. Là encore, plusieurs explications sont possibles : s'agissait-il d'envoyer un message à Washington ? Est-ce

réellement une opération de prépositionnement qui est décrite dans ce rapport de Microsoft ?

Plusieurs questions restent ainsi en suspens, et la faible littérature disponible en sources ouvertes sur Volt Typhoon ne permet d'y apporter de réponse pour l'instant.

La menace dans le cyberespace est souvent décrite comme des capacités au service d'une intention et qui exploitent une ou des opportunités. S'il ne fait guère de doute - à l'aune de ces publications sur Volt Typhoon et plus généralement sur la lutte informatique chinoise - que Pékin dispose de capacités suffisamment avancées pour pouvoir se livrer à des opérations de sabotage, et que de nombreuses opportunités sont susceptibles de se présenter à l'avenir ; la question de l'intention des autorités chinoises demeure. Au-delà des attaques cybercriminelles qui sont monnaie courante aujourd'hui et des opérations d'espionnage susceptibles de les viser, les opérateurs d'importance vitale en France et en Europe devront également probablement suivre de près l'évolution de la pratique chinoise en matière de prépositionnement et sabotage.