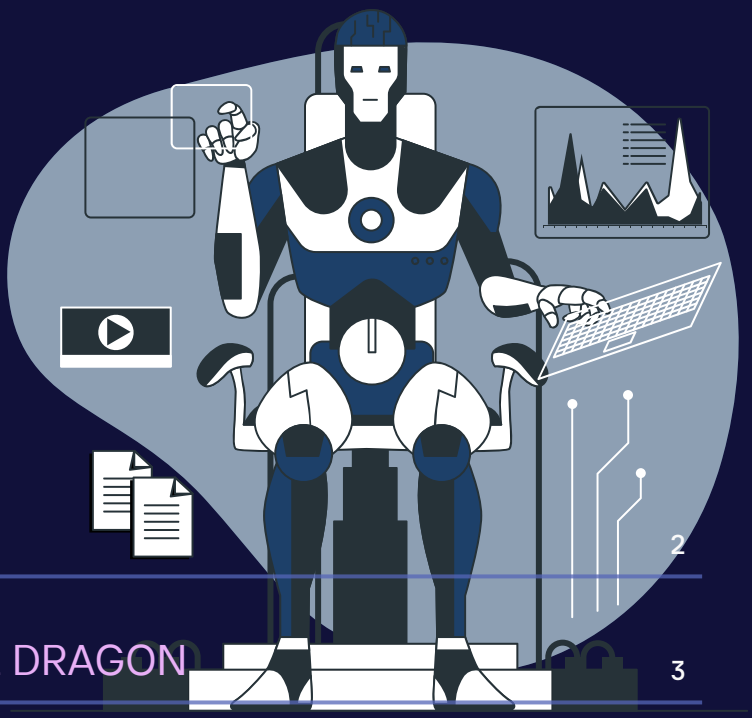
2023

APT 41 : DOUBLE DRAGON

Espions pour le compte du gouvernement chinois le jour, cybercriminels la nuit.

FAIT PAR MAXIME, NESSRINE, KALIFA ET TONY

Sommaire



C'est quoi une APT ?

Une menace persistante avancée (APT) est une cyberattaque ciblée et prolongée au cours de laquelle une personne non autorisée accède au réseau et passe inaperçue pendant une période importante. L'objectif d'une attaque APT est généralement de surveiller l'activité du réseau et de voler des données plutôt que d'endommager le réseau ou l'organisation.

Comment une APT attaque-t-elle ?

Les pirates qui commettent des attaques APT prennent les mesures importantes suivantes pour obtenir un accès permanent au réseau cible :

- Accès au réseau : Pour atteindre la cible, les systèmes cibles APT sont regroupés sur Internet, soit en envoyant un message de phishing ciblé, soit en utilisant une faille de sécurité qui leur permet d'introduire des logiciels malveillants.

- Établir un point d'ancrage : Une fois que l'accès à la cible est établi, les pirates peuvent approfondir leur enquête et commencer à utiliser les logiciels malveillants qu'ils ont installés pour créer des réseaux de portes dérobées et des tunnels qui leur permettent de passer inaperçus. Le comité de parents peut compter sur des techniques malveillantes avancées telles que la réécriture de code pour couvrir leurs traces.

- Propagez l'attaque : Après avoir pénétré dans le réseau cible, les acteurs de l'APT peuvent, entre autres, pirater le mot de passe des privilèges administratifs, ce qui leur permet de mieux contrôler le système et d'accéder à d'autres niveaux.

- Se déplacer dans le système : Après avoir violé les systèmes cibles et obtenu des privilèges administratifs, ils peuvent se déplacer dans le réseau d'entreprise comme ils le souhaitent. En outre, ils peuvent tenter d'accéder à d'autres serveurs ou à d'autres zones protégées du réseau.

- Déployer l'attaque : À ce stade, les pirates centralisent, cryptent et compriment les données pour les filtrer

- Filtrage des données : Les pirates informatiques collectent les données et les transmettent à leur propre système.

- L'accès n'est pas détecté : Les cybercriminels peuvent répéter ce processus pendant longtemps tout en restant invisibles, ou ils peuvent créer une porte dérobée pour accéder au système s'ils le souhaitent.

APT41 : DOUBLE DRAGON

Espions pour le compte du gouvernement chinois le jour, cybercriminels la nuit. C'est la vie que ZHANG Haoran, TAN Dailin, QIAN Chuan, FU Qiang et JIANG Lizhi tous membres de l'APT41.

APT41 aussi connu sous les noms de : DOUBLE DRAGON ; BARIUM; WINNTI; WICKED PANDA; WICKED SPIDER; TG-2633 ; BRONZE ATLAS; `RED KELPIE est un groupe de pirates informatiques chinois connu pour ses opérations de cyberespionnage et de cybercriminalité, ciblant divers secteurs à l'échelle mondiale tels que la santé, les télécommunications et la technologie.

APT41 est actif depuis au moins 2012

Membre du groupe connu a ce jour :

ils sont toujours rechercher

APT41 : Présentation des cibles

Durant toutes ses années apt 41 ont attaqueés 9 principaux secteurs et 14 pays

✸ Les secteurs ciblées :

- les entreprises high-tech
- les media
- les entreprise pharmaceutiques
- Les magasins/supermarché
- Les entreprises de dévéloppement informatique
- Les entreprises de télécom
- Les agences de voyage
- Les écoles
- Les entreprise conceptrice de jeux vidéos

✸ Les pays ciblées :

- États-Unis
- France
- Japan
- L'Inde
- Thailand
- Italie
- Turquie
- Afrique du sud
- Korée du sud
- Singapour
- Angleterre
- Birmanie
- Pays-Bas
- Suisse

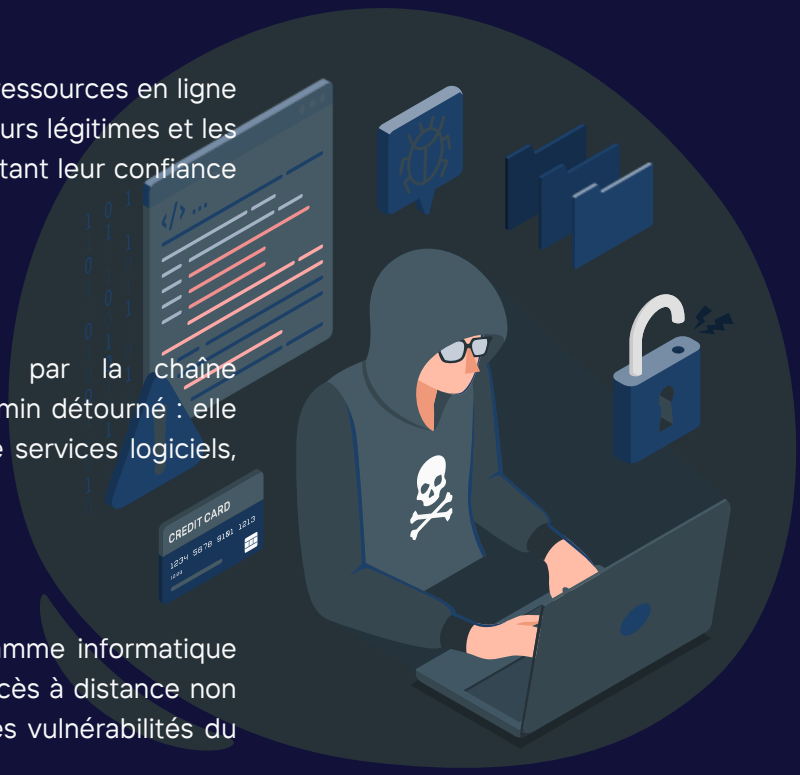
DIFFÉRENT TYPES D'ATTAQUES

Le Spear phishing

- APT41 a été connu pour mener des campagnes de spear-phishing ciblées, où ils envoient des e-mails frauduleux pour tromper les destinataires et les inciter à ouvrir des pièces jointes malveillantes.

Les water holes (point d'eau)

- Les "watering holes" sont des sites web ou des ressources en ligne spécifiquement compromis pour piéger les visiteurs légitimes et les infecter avec des logiciels malveillants, en exploitant leur confiance dans ces sites.



Supply chain attacks

- Comme son nom l'indique, une attaque par la chaîne d'approvisionnement vise sa victime par un chemin détourné : elle infecte un tiers, par exemple, un fournisseur de services logiciels, pour ensuite aller s'en prendre à sa cible finale.

Le blackdoor

- Un backdoor (ou porte dérobée) est un programme informatique malveillant utilisé pour donner aux pirates un accès à distance non autorisé à un ordinateur infecté en exploitant les vulnérabilités du système.

Malware

- Un "malware" (contraction de "malicious software") est un logiciel malveillant conçu pour endommager, infecter ou compromettre un ordinateur, un réseau, ou un appareil électronique, en volant des données, en perturbant des opérations, ou en permettant un accès non autorisé.

commande et contrôle

- L'attaque de "commande et contrôle" est une technique où des acteurs malveillants établissent un contrôle sur des systèmes infectés pour leur donner des instructions, recueillir des données ou les utiliser à des fins malveillantes.

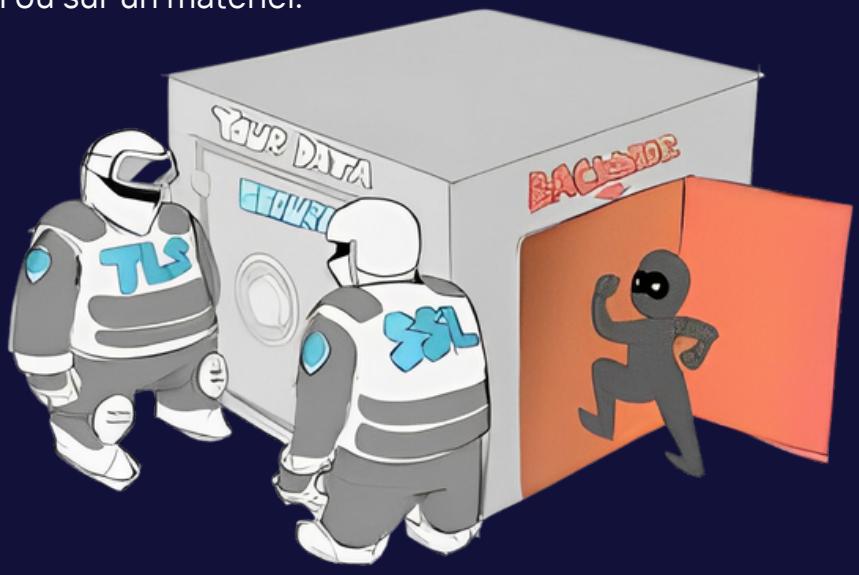
Malware PowerShell

Une attaque ciblée de malware PowerShell par porte dérobée d'APT41 qui contourne les détections et permet aux acteurs malveillants d'exécuter des commandes, de télécharger et de télécharger des fichiers, et de collecter des informations sensibles à partir de systèmes Windows compromis.

✱ Qu'est ce qu'une porte dérobée ?

Le principe de la mise en œuvre d'une « Backdoor » ou porte dérobée correspond à prévoir un accès tenu secret vis-à-vis de l'utilisateur légitime aux données contenues dans un logiciel ou sur un matériel.

source CNIL



✱ Comment fonctionnent les attaques de virus par porte dérobée ?

Une porte dérobée peut être installée légitimement par les développeurs de logiciels et de matériel pour leur permettre d'accéder facilement à leurs applications afin d'exécuter des fonctions telles que la résolution de problèmes logiciels.
Mais dans la plupart des cas, les portes dérobées sont installées par des cybercriminels pour leur permettre d'obtenir un accès illégitime à un appareil, un réseau ou une application logicielle.
Pour que les cybercriminels réussissent à installer un virus de porte dérobée sur votre appareil, ils doivent d'abord trouver un point faible (vulnérabilités du système) ou une application compromise dans votre appareil.

Les vulnérabilités systèmes les plus courantes sont les suivantes

- Logiciels non corrigés
- Ports réseau ouverts
- Mots de passe faibles
- Pare-feu déficien

Les vulnérabilités peuvent également être créées par des logiciels malveillants tels que les chevaux de Troie. Les pirates utilisent les chevaux de Troie présents sur un appareil pour créer des portes dérobées.

Une fois que les cybercriminels se sont introduits dans votre ordinateur par le biais d'une porte dérobée, ils veulent s'assurer qu'ils peuvent facilement y revenir, que ce soit pour voler vos informations, installer un logiciel d'extraction de crypto-monnaie, détourner votre appareil ou saboter votre entreprise.
Les pirates savent qu'il peut être difficile de continuer à pirater un appareil, surtout si la vulnérabilité est corrigée. C'est pourquoi ils installent un code appelé porte dérobée sur l'appareil cible, de sorte que même si la vulnérabilité est corrigée, la porte dérobée reste en place pour leur permettre d'accéder à l'appareil.

✸ Porte dérobée PowerShell d'APT41

La porte dérobée PowerShell d'APT41 est conçue pour fonctionner secrètement et maintenir sa présence sur de longues périodes, souvent utilisée comme charge utile secondaire dans des scénarios d'attaque ciblée.
Après l'installation, la porte dérobée permet à APT41 d'effectuer les activités illicites suivantes sur les systèmes compromis : -

- Exécuter des commandes
- Telecharger des fichiers
- Télécharger des fichiers
- Extraire des données confidentielles

En exploitant cette fonctionnalité, la porte dérobée PowerShell d'APT41 contourne les mesures de sécurité conventionnelles, lui permettant d'infiltrer les systèmes cibles et de récolter des information compromettant

Le spearfishing (Hameconnage ciblé)

Envoyés par milliers, les emails de Phishing permettent aux criminels de se procurer vos données d'accès et mots de passe. La chance que de nombreux utilisateurs ne serait-ce que lisent ces messages falsifiés reste toutefois relativement faible. En revanche, une nouvelle variante d'escroquerie, le spearfishing, procède de manière beaucoup plus ciblée et se solde par de nombreux succès.

Qu'est-ce que le spearfishing ?

L'attaque par hameçonnage ciblé (spearfishing) est par définition une usurpation d'identité d'une personne connu du destinataire pour envoyer un message ciblé a un membre d'une organisation, afin de lui faire ouvrir une pièce jointe malveillante qui permettra d'accéder au réseaux de l'organisation.

source CNIL

Comment fonctionnent les attaques spearfishing ?

les escrocs créent de faux emails, sites Web, voire parfois des SMS en apparence authentique demandant les informations de connexion des utilisateurs. Leur objectif est d'accéder à vos données, d'achats en ligne, de réseaux sociaux ou de mémoires de stockage Cloud. Dans le pire des cas, ils peuvent obtenir vos numéros de cartes bancaires et cartes de crédit. Les criminels savent très bien que de nombreux internautes ne prennent pas la sécurité de leurs mots de passe très au sérieux et utilisent le même pour les services les plus divers et variés. Un simple site Web de phishing leur suffit donc à accumuler d'innombrables données sensibles. Ces informations valent très chères sur le marché noir.
Le spearfishing fonctionne de manière plus ciblée, définit très précisément ses victimes et élabore une tentative d'escroquerie sur mesure, en fonction des personnes sélectionnées. La plupart du temps, ces attaques s'en prennent à des entreprises et organisations.

Outre le vol de coordonnées bancaires, les scénarios d'attaque varient de l'espionnage industriel aux cyberattaques sur des cibles militaires ou sur l'infrastructure d'une région donnée.
En amont, les escrocs espionnent la cible et accumulent les informations leur permettant d'augmenter leur crédibilité. Ils rédigent ensuite un email sur mesure en veillant à le rendre le plus concret possible.
Le spearfishing fonctionne particulièrement bien au sein de larges entreprises internationales, dont les employés ne connaissent pas forcément l'organigramme dans son entier. Les victimes sont ainsi incitées à divulguer des données sensibles ou télécharger des logiciels malveillants.

✷ Comment fonctionnent les attaques spearfishing ?

les escrocs créent de faux emails, sites Web, voire parfois des SMS en apparence authentique demandant les informations de connexion des utilisateurs. Leur objectif est d'accéder à vos données, d'achats en ligne, de réseaux sociaux ou de mémoires de stockage Cloud. Dans le pire des cas, ils peuvent obtenir vos numéros de cartes bancaires et cartes de crédit. Les criminels savent très bien que de nombreux internautes ne prennent pas la sécurité de leurs mots de passe très au sérieux et utilisent le même pour les services les plus divers et variés. Un simple site Web de phishing leur suffit donc à accumuler d'innombrables données sensibles. Ces informations valent très chères sur le marché noir.
Le spearfishing fonctionne de manière plus ciblée, définit très précisément ses victimes et élabore une tentative d'escroquerie sur mesure, en fonction des personnes sélectionnées. La plupart du temps, ces attaques s'en prennent à des entreprises et organisations.

✷ Comment l'Apt 41 utilise t'il le spearfishing

Les e-mails de spear-phishing sont régulièrement utilisés par APT 41 dans le cadre d'attaques de cyberespionnage et d'attaques financières. Le groupe a envoyé de nombreux courriels trompeurs qui tentent de prendre des informations à des cibles de haut niveau après avoir recueilli des données personnelles pour augmenter les chances de succès. Les cibles ont varié, allant de groupes de médias pour des activités d'espionnage à des échanges de bitcoins à des fins financières.
Il s'appuie donc sur des e-mails de spear-phishing qui contiennent des pièces jointes comme HTML (.chm), car pour passer inaperçu, ce malware se terre dans des fichiers d'aide de logiciels Windows, des fichiers en .CHM.

✳ Comment il arrive à extraire des donnée grâce au spear-phishing ?

les escrocs créent de faux emails, sites Web, voire parfois des SMS en apparence authentique demandant les informations de connexion des utilisateurs. Leur objectif est d'accéder à vos données, d'achats en ligne, de réseaux sociaux ou de mémoires de stockage Cloud. Dans le pire des cas, ils peuvent obtenir vos numéros de cartes bancaires et cartes de crédit. Les criminels savent très bien que de nombreux internautes ne prennent pas la sécurité de leurs mots de passe très au sérieux et utilisent le même pour les services les plus divers et variés. Un simple site Web de phishing leur suffit donc à accumuler d'innombrables données sensibles. Ces informations valent très chères sur le marché noir.
Le spearfishing fonctionne de manière plus ciblée, définit très précisément ses victimes et élabore une tentative d'escroquerie sur mesure, en fonction des personnes sélectionnées. La plupart du temps, ces attaques s'en prennent à des entreprises et organisations.

Attaque a plus de 700 millions $

En septembre 2017, Equifax, une agence de déclaration de crédit à la consommation aux États-Unis, qui était considérée comme l'une des trois plus grandes agences de crédit américaines avec Experian et TransUnion, a confirmé avoir été victime d'une violation de données suite à une attaque. Lors de cet incident, les données de près de 147 millions clients américains du groupe avaient été exposées. Les pirates avaient eu accès, de la mi-mai à juillet de la même année, à des informations comme les noms, les adresses, les dates de naissance, les numéros de sécurité sociale et du permis de conduire, autant d'informations qui peuvent servir à une usurpation d'identité. Equifax avait aussi précisé que les cybercriminels étaient parvenus à accéder aux numéros de carte de crédit de 209 000 citoyens américains et avaient mis la main sur plus de 180 000 dossiers de crédits.

Equifax est originellement une société d'évaluation de la cote de crédit. C'est-à-dire de la solvabilité et de la capacité de remboursement d'une personne ou d'une entreprise souhaitant accéder au crédit à la consommation. Cette société dirigée par Richard Smith réalise presque 3 milliards de dollars de chiffre d'affaires annuel (avec 6.664 milliards US$ d'actifs déclarés en 20164).

✸ Mais qui est a l'origine de cette attaque ?

La société Equifax nie toutes implication du groupe APT41. Tandis que les membres du groupe revendique cette attaques et selon eux reconnaitre s'etre fait volées des information par groupe un chinois causerait une grande dégradation de l'image de la société.

✷ L’attaque utilisé a l’encontre de Equifax :

les pirates ont évité d'utiliser certains outils de piratage qui les auraient exposé à l'équipe de sécurité d'Equifax. Cependant, l'un des outils qu'ils utilisent leur a permis de construire des tunnels cachés de « commande et contrôle »

cette attaque s'est faite en quatre étapes

1ere Etape : le pirate installe plusieurs coquilles web, chacune avec une adresse web différente, ce qui a créé plusieurs tunnels cachés. Si l'un était découvert, les autres pourraient continuer à fonctionner . Cette phase d'attaque est connue sous le nom de « commande et contrôle ».

Une attaque "commande et contrôle" consiste à prendre le contrôle à distance d'un système informatique après y avoir introduit des logiciels malveillants, permettant aux pirates de le manipuler à leur guise.

2ieme étape : Une fois à l'intérieur du réseau, les pirates ont le temps de personnaliser les outils de piratage pour exploiter efficacement les logiciels d'Equifax, envoyer des requêtes et analyser des dizaines de bases de données pour déterminer lesquelles contenaient les données les plus précieuses . Cette phase d'attaque est appelée la reconnaissance

3ieme étape : les pirates ont utilisé des outils de tunnellisation spéciaux pour échapper aux pare-feu, analysant et piratant les bases de données l'une après l'autre tout en stockant des données dans les propres systèmes de stockage de l'entreprise : c'est la phase d'attaque connue sous le nom de « mouvement latéral »

4ieme étape : Enfin, pour la dernière phase d'attaque connue sous le nom d' « exfiltration de données », Les pirates ont collecté une mine de données tellement volumineuse qu'il a fallu les diviser en de petits stocks pour éviter le déclenchement des systèmes de détection des anomalies et de prévention des pertes de données .

En conséquence de cette attaque la société devra débourser entre 575 et 700 millions de dollars pour les victimes, les États et les organismes de réglementation américains. L’entreprise a accepté de verser 175 millions de dollars à 48 États, au District de Columbia et à Porto Rico ainsi que 100 millions de dollars au CFPB. Elle devra également constituer un fonds de 300 millions de dollars, extensible jusqu’à 425 millions de dollars, pour fournir aux consommateurs touchés des services de surveillance du crédit et les indemniser

Conclusion

En conclusion, APT41 demeure un acteur majeur et inquiétant dans le paysage du cyberespionnage et de la cybercriminalité. Leur double activité, combinant des opérations d'espionnage à des attaques à motivation financière, rend leur traque et leur neutralisation d'autant plus complexes. Les organisations doivent rester vigilantes, renforcer leurs mesures de sécurité, et collaborer étroitement avec les autorités pour se prémunir contre les menaces persistantes que représente APT41.

Merci !

SOURCES UTILISEES

Office of Information Security
Securing One HHS

CAPS | CENTRE FOR AIR POWER STUDIES
FORUM FOR NATIONAL SECURITY STUDIES

SSRN

DEPARTMENT OF JUSTICE
FEDERAL BUREAU OF INVESTIGATION
FIDELITY BRAVERY INTEGRITY

Digital Guide
IONOS

CNIL.
COMMISSION NATIONALE
INFORMATIQUE & LIBERTÉS

WIKIPÉDIA
L'encyclopédie libre

SOURCES UTILISEES

APT41". Attack.MITRE. https://attack.mitre.org/groups/G0096/
HC3. "APT41 Citrix and ZohoAttacks on Healthcare". HHS. Mar 26, 2020.
https://www.hhs.gov/sites/default/files/apt41-citrix-and-zoho-attacks-on-healthcare.pdf
Kaspersky. "Technical details of MoonBounceImplementation".
https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2022/01/19115831/MoonBounce_technical-details_eng.pdf
•Brown, Rufus. Ta, Van. Bienstock, Douglas. Ackerman, Geoff. Wolfram, John. "Does This Look
Infected? A Summary of APT41 Targeting U.S. State Governments". Mandiant. Mar 8, 2022.
https://www.mandiant.com/resources/blog/apt41-us-state-governments
"MoonBounce: the dark side of UEFI firmware". Kaspersky. Jan 20, 2022.
https://securelist.com/moonbounce-the-dark-side-of-uefi-firmware/105468/
Naraine, Ryan. "Prolific Chinese APT Caught Using 'MoonBounce' UEFI Firmware Implant".
Securityweek. Jan 20, 2022. https://www.securityweek.com/prolific-chinese-apt-caught-using-moonbounce-uefi-firmware-implant