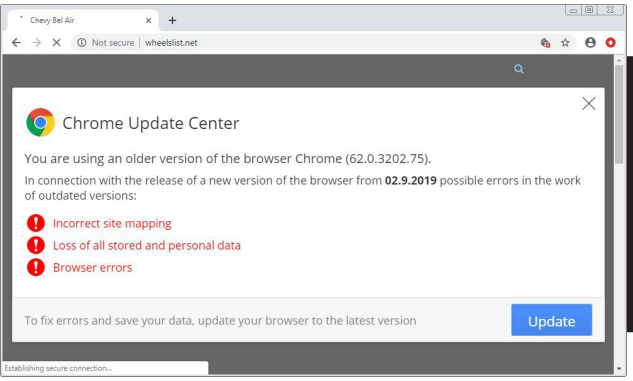
SEKOIA THREAT INTELLIGENCE WEEKLY REPORT

TLP WHITE



EVIL CORP EN MODE DÉCONFINÉ ?

En décembre 2019, Maksim Yakubets et Igor Turashev, deux des leaders du groupe cybercriminel Evil Corp, étaient mis en accusation par la justice américaine et ont fait leur entrée dans le trombinoscope du FBI des Most Wanted cybercriminels. Comme cela se passe aux Etats-Unis, une prime de 5 millions de dollars est offerte à qui permettra l'arrestation de M. Yakubets, suspecté d'être le cerveau du gang.

Evil Corp est l'un des groupes cybercriminels les plus actifs de ces dix dernières années. On lui doit des fraudes financières dont les pertes sont estimées à plusieurs centaines de millions de dollars, perpétrées à l'aide du malware bancaire ZeuS, et des botnets Bugat, Cridex et Dridex. Depuis quelques années, Evil Corp s'est aussi diversifié dans les rançongiciels. Après avoir distribué Locky à l'aide de Dridex, Evil Corp s'est affranchi de cette dépendance et a développé le ransomware BitPaymer.

La publication des avis de recherche et des actes d'accusation en décembre 2019 avaient pour principal objectif de calmer les velléités des membres du groupe. Ceux-ci étant à ce jour hors d'atteinte des forces de police, la Justice américaine espérait envoyer un message suffisamment fort et faire comprendre à ces cybercriminels qu'il était temps de siffler la fin du jeu.

Nous avions consacré à ces mises en accusation un article dans le WE|INT n°23 du 6 décembre 2019, article que nous concluions ainsi : "Reste à savoir si cette cyber-épée de Damoclès les dissuadera de persévérer dans le cybercrime ou calmera leurs ardeurs.".

La réponse n'a pas tardé à être apportée.

La Research and Intelligence Fusion Team de NCC Group a publié une analyse d'un nouveau rançongiciel détecté en mai 2020, appelé WastedLocker, nom basé sur l'extension .wasted utilisé par ce malware pour marquer les fichiers chiffrés par celui-ci. Selon NCC Group, l'analyse de WastedLocker et du modus operandi de ces opérateurs met en évidence des

⊙⊙⊙

EVIL CORP EN MODE DÉCONFINÉ ?

similitudes avec BitPaymer. La RIFT n'y voit pas de simples coïncidences mais le signe que le groupe Evil Corp est de retour et de nouveau actif.

Plusieurs dizaines d'entreprises aux Etats-Unis auraient été ciblées par une campagne visant à distribuer WastedLocker, avec une nette préférence pour les entreprises disposant des ressources financières suffisantes pour verser de fortes rançons. Selon Symantec, qui suit les activités du groupe, 8 entreprises présentes dans le classement Fortune 500 feraient partie des victimes ou des cibles identifiées en mai.

WastedLocker est distribué après la compromission d'ordinateurs à l'aide d'attaques de type "drive-by download". Pour cela, le framework malveillant SocGholish, également connu sous le nom FakeUpdates, est déployé sur des pages de sites légitimes compromis. Symantec en a identifié 150. Il est probable que certains de ces sites utilisent une version obsolète de Joomla dont une vulnérabilité est exploitée pour installer SocGholish.

Lorsqu'une victime navigue sur l'une de ces pages, une fausse alerte de mise à jour du navigateur Chrome s'affiche et une archive Zip contenant du code Javascript est téléchargée. Lors de l'exécution des scripts JS malveillants, la machine cible fait l'objet d'un profilage à l'aide des commandes natives whoami, net user et net group dont les sorties conditionnent la suite des opérations. Si la machine est jugée prometteuse, des scripts PowerShell supplémentaires sont exécutés pour collecter de plus amples renseignements sur la cible.

Si la machine est jugée digne d'intérêt à l'issue de ces deux phases de reconnaissance et de prise d'empreinte, Cobalt Strike est utilisé pour exécuter deux charges utiles en PowerShell dont une contient un injecteur de code développé en .Net extrait du framework Open Source Donut dont l'utilisation est en théorie destinée aux équipes Red Team mais dont l'usage est détourné à des fins malveillantes (comme de nombreux autres outils, d'ailleurs). Un autre outil utilisé pour des simulations d'intrusions, PowerView, est également utilisé durant la phase de compromission de l'attaque, notamment pour recherche dans Active Directory les serveurs Windows et des machine sous Windows 7.

WMI, ProcDump et PSExec sont utilisés pour les mouvements latéraux et le vol d'identifiants. Seul Mimikatz manque à l'appel de ces outils bien connus des administrateurs Windows et des attaquants.

WastedLocker, qui constitue la charge finale de l'attaque, chiffre les fichiers, arrête certains services notamment liés à des logiciels de sécurité et efface les Shadow Copies. Le rançongiciel s'attaque aux fichiers contenus sur les disques locaux, les supports amovibles, les lecteurs partagés et les points de montage distants.

Contrairement à de nombreux autres ransomware, les opérateurs de WastedLocker ne semblent pas intéressés par le vol et la publication de données volées à leurs victimes. Les rançons demandées seraient cependant assez conséquentes. Fox-IT donne une fourchette allant de 500 000 à quelques millions de dollars avec un montant de 10 millions de dollars pour la plus grosse rançon demandée à une victime de WastedLocker.

Références

https://research.nccgroup.com/2020/06/23/wastedlocker-a-new-ransomware-variant-developed-by-the-evil-corp-group/

https://www.zdnet.com/article/new-wastedlocker-ransomware-demands-payments-of-millions-of-usd/

https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/wastedlocker-ransomware-us

https://www.bleepingcomputer.com/news/security/new-wastedlocker-ransomware-distributed-via-fake-program-updates/

L'ACTUALITÉ CYBER DE LA SEMAINE SÉLECTIONNÉE PAR SEKOIA

[ZDNET] CONDAMNATION DU BOTMASTER KENNETH SCHUCHMAN

Kenneth Schuchman, connu sous le sobriquet Nexus Zeta, est l'auteur de plusieurs botnets utilisés pour des attaques en déni de service distribué dont les botnets Satori, Okiru, Masuta, et Fbot/Tsunami.

Le jeune homme de 22 ans de Vancouver, Washington, a été condamné à 13 mois de prison pour avoir créé et exploité plusieurs réseaux de zombies DDoS composés de routeurs domestiques et d'autres dispositifs de mise en réseau et d'Internet des objets (IoT).

Le ministère américain de la justice a déclaré que Kenneth Currin Schuchman louait des botnets pour lancer des attaques DDoS. Ses réseaux de zombies auraient infecté des centaines de milliers d'appareils avec des logiciels malveillants.

Les responsables américains ont déclaré que Schuchman avait deux complices, identifiés seulement comme Vamp et Drake, qui ont également contribué au code et aux fonctionnalités des réseaux de zombies.

https://www.zdnet.com/article/ddos-botnet-coder-gets-13-months-in-prison/

[TRUSTWAVE] GOLDENSPY : UN CHEVAL DE TROIE INTÉGRÉ À UN LOGICIEL COMPTABLE CHINOIS

Les chercheurs de Trustwave SpiderLabs ont découvert une nouvelle famille de malware appelée GoldenSpy, intégrée dans un logiciel de paiement de taxes dont l'utilisation est obligatoire pour les entreprises opérant en Chine.

Deux sociétés britanniques et un établissement financier ayant récemment ouvert des filiales en Chine ont été informées par leur banque respective de l'obligation d'installer un logiciel édité par la société Golden Tax Department of Aisino Corporation.

Trustwave a analysé ce logiciel et a découvert qu'il contenait un cheval de Troie, que ce dernier s'exécute avec les privilèges SYSTEM et qu'il n'était pas désinstallé même après la désinstallation du logiciel légitime.

https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/the-golden-tax-department-and-the-emergence-of-goldenspy-malware/

[PALO ALTO NETWORKS] DES ORGANISATIONS RUSSES VICTIMES DU MALWARE ACIDBOX

L'équipe Unit42 de Palo Alto Networks a identifié un malware appelé AcidBox, qui a été utilisé contre deux organisations russes en 2017.

AcidBox exploite des vulnérabilités de la solution de virtualisation VirtualBox qui ont été exploitées dans des attaques passées par le groupe russophone Turla qui serait affilié au FSB, le service de renseignement intérieur russe. Le groupe d'acteurs à l'origine des attaques de 2017 serait toutefois différent et n'a pas été identifié.

https://unit42.paloaltonetworks.com/acidbox-rare-malware/

L'ACTUALITÉ CYBER DE LA SEMAINE SÉLECTIONNÉE PAR SEKOIA

[ARS TECHNICA] DÉTOURNEMENT DU SERVICE GOOGLE ANALYTICS POUR VOLER DES DONNÉES DE PAIEMENT

Des fraudeurs utilisent Google Analytics pour camoufler les données volées à l'aide de skimmers installés sur sites de e-commerce compromis.

Les fraudeurs enregistrent pour cela des domaines dont le nom ressemble à celui de services légitimes et en particulier ceux utilisés par Google pour son service Analytics. Dans certains cas cependant, des attaques de ce type utilisaient parfois le service légitime.

Dans ce dernier cas, les attaquants ont injecté un code malveillant dans les sites, qui ont recueilli toutes les données saisies par les utilisateurs, puis les ont envoyées via Analytics. En conséquence, les attaquants pouvaient accéder aux données volées dans leur compte Google Analytics.

https://arstechnica.com/information-technology/2020/06/google-analytics-trick-allows-crooks-to-hide-card-skimming/
https://securelist.com/web-skimming-with-google-analytics/97414/

[BLEEPING COMPUTER] MICROSOFT PUBLIE DES RECOMMANDATIONS CONTRE LES ATTAQUES CIBLANT LES SERVEURS EXCHANGE

L'équipe ATP Defender de Microsoft a publié des recommandations pour sécuriser les serveurs Exchange. Ces recommandations sont basés sur l'analyse de plusieurs campagnes étudiées par les chercheurs de Microsoft début avril.

Les chercheurs de Microsoft ont isolé deux scenarii d'attaque contre les serveurs Exchange. Le premier scénario, le plus courant, utilise l'ingénierie sociale ou les attaques de type «drive-by» ciblant les points d'extrémité, afin de voler des identifiants. Les attaquants exploitent ces identifiants pour leurs mouvements latéraux jusqu'à ce qu'ils accèdent à un serveur Exchange.

Dans le second scénario, les attaquants exploitent une vulnérabilité affectant le composant IIS (Internet Information Service) d'un serveur Exchange et permettant une exécution de code à distance, en profitant de serveurs mal configurés afin obtenir des privilèges système.

https://www.bleepingcomputer.com/news/security/microsoft-attackers-increasingly-exploit-exchange-servers/
https://www.microsoft.com/security/blog/2020/06/24/defending-exchange-servers-under-attack/

ACTUALITÉS DES ATTAQUES PAR RANÇONGICIELS

MAZE
Le groupe Maze affirme avoir compromis l'entreprise d'électronique sud-coréenne LG Electronics. Des fichiers appartenant à la société ont été publiés sur le site de Maze.

Le groupe Maze a publié un communiqué sur son site le 22 juin, pour démontrer l'intérêt qu'il y a à payer les rançons. Dans son "étude", Maze met en perspective les pertes financières encourues par ses victimes, en pénalités, en frais d'avocat et en coût de restauration des actifs numériques détruits, par rapport au montant de la rançon. Maze estime le coût moyen d'une attaque entre 50 et 60 millions de dollars, somme pouvant atteindre 250 à 300 millions de dollars pour de grandes entreprises. Les cas des entreprises ST Engineering, MaxLinear, Conduent et M.J. Brunner illustrent cette démonstration.

DopplePaymer
Le groupe DoppelPaymer a diffusé les données volées après la compromission de la ville de Charleville-Mézières.

Clop
Le conglomérat indien Indiabulls Group, qui détient des actifs dans les secteurs de l'habitat, du prêt au consommateur et de la pharmacie, a été victime du rançongiciel Clop.

Hackbit
Les chercheurs de Proofpoint ont analysé une campagne du rançongiciel Hackbit menée contre des entreprises allemandes, autrichiennes et suisses. Hackbit serait une variante du rançongiciel Thanos. Le malware est diffusé à l'aide de pièces-jointes contenant des fichiers Excel malveillants.

Sodinokibi
Sodinokibi aurait ciblé les points de vente électroniques dans des attaques récentes dans le but de maximiser ses gains en volant des données de paiement et en demandant une rançon pour le déchiffrement des fichiers de ses victimes.

Divers
Les chercheurs de la société ESET ont analysé CryCryptor, un ransomware ciblant les utilisateurs d'appareils sous Android. Ce malware est présenté comme une application de traçage de la Covid-19. Les chercheurs d'ESET ont mis au point et mis à disposition un déchiffreur pour ce malware.

ConnectWise, une société de services informatiques aux entreprises a été victime d'une attaque par rançongiciel. Les attaquants ont exploité une vulnérabilité dans le logiciel ConnectWise Automate utilisé pour la surveillance et l'administration à distance des réseaux de l'entreprise et de ses clients. Cette attaque pourrait impacter les 20 000 entreprises clients de ConnectWise.

https://www.zdnet.fr/actualites/charleville-mezieres-le-groupe-doppelpaymer-diffuse-les-donnees-volees-39905603.htm
https://www.bleepingcomputer.com/news/security/indiabulls-group-hit-by-clop-ransomware-gets-24h-leak-deadline/
https://www.cybersecurity-insiders.com/ransomware-attack-on-connectwise/
https://www.proofpoint.com/us/blog/threat-insight/hakbit-ransomware-campaign-against-germany-austria-switzerland
https://www.zdnet.com/article/this-ransomware-has-learned-a-new-trick-scanning-for-point-of-sales-devices/
https://www.welivesecurity.com/2020/06/24/new-ransomware-uses-covid19-tracing-guise-target-canada-eset-decryptor/

INTELLIGENCE-DRIVEN CYBERSECURITY

POUR SIGNALER UN INCIDENT

Si vous êtes victime d'une attaque, si vous avez un doute ou si vous désirez revenir et investiguer sur un incident de sécurité, prenez contact avec le CERT SEKOIA.

cert@sekoia.fr
+33 (0) 805 692 142

SEKOIA accompagne les premières sociétés du CAC40 dans la mise en place de leurs CERTs internes.

Depuis 2013 SEKOIA active son CERT inter-entreprises et offre ses services à des OIV et autres acteurs du CAC40 et du SBF120.

LA THREAT INTELLIGENCE, PIERRE ANGULAIRE DE LA LUTTE INFORMATIQUE DEFENSIVE

SEKOIA dispose d'une offre complète en matière de Cyber Threat Intelligence :

- **conseil & accompagnement**,
- **formation**,
- **veille et rapport sur les cybermenaces** :

BR INT. SEKOIA THREAT INTELLIGENCE **BRIEFING REPORT**

FL INT. SEKOIA THREAT INTELLIGENCE **FLASH REPORT**

SP INT. SEKOIA THREAT INTELLIGENCE **SPECIAL REPORT**

- **base & feed de renseignements cyber :**
  SEKOIA.IO **INTELLIGENCE CENTER**

A PROPOS DE SEKOIA

Pure player et acteur français majeur de la cybersécurité, SEKOIA accompagne au quotidien grands comptes, institutions et entreprises innovantes pour les conseiller sur leur stratégie, les préparer et leur offrir support et assistance dans l'exercice de leurs métiers comme dans les phases les plus critiques d'exposition aux menaces.

Découvrez une structure, un modèle et une stratégie innovante dans le secteur de la cybersécurité.

SEKOIA

SEKOIA — PARIS
18-20,
Place de la Madeleine,
75008 Paris

SEKOIA — RENNES
1137A
Avenue des Champs Blancs
35510 CESSON-SÉVIGNÉ
—
Tél. +33 1 44 43 54 13
—