FLINT.

2020-056

20/03/2020

SEKOIA THREAT INTELLIGENCE **FLASH** REPORT

RAPPORT SPÉCIAL

Pandémie COVID-19 : mieux appréhender les cybermenaces exploitant le thème du coronavirus

Statut :
EN COURS

Risque :
ÉLEVÉ

Objectifs :
ESPIONNAGE
GAIN FINANCIER

SECTEURS CONCERNÉS : **TOUS**

ZONES GÉOGRAPHIQUES TOUCHÉES : **MONDE**

TLP
WHITE

Synthèse

Comme à l'occasion de chaque événement majeur ou crise internationale, des groupes d'attaquants informatiques cherchent à tirer profit de la baisse de vigilance et de la peur pour lancer leurs attaques. De nombreux groupes ont lancé des campagnes utilisant le thème du COVID-19 depuis janvier 2020. Néanmoins, avec l'expansion récente de la pandémie en Europe, le nombre de ces campagnes de distribution de logiciels malveillants a considérablement augmenté.

Le recours massif aux technologies et appareils connectés dû aux mesures de confinement et au travail à distance risque d'intensifier significativement encore cette menace (cf. FLINT.2020-053).

Ce rapport vise à fournir une meilleure compréhension de la cybermenace née avec la propagation du COVID-19. C'est en étudiant et analysant la menace pour mieux la connaître que nous serons mieux préparés à y faire face.

Analyse

La menace cyber autour du COVID-19 semble principalement concerner le phishing et les arnaques d'ingénierie sociale. Comme cela a été mis en évidence par Proofpoint, les envois de spam et de malware utilisent aujourd'hui majoritairement la thématique du COVID-19.

De nombreux acteurs et logiciels malveillants exploitent cette technique. Les attaques utilisent des courriels contenant des pièces jointes ou des liens, ainsi que de faux sites Web prétendant offrir des recommandations sanitaires et des mises à jour sur la crise, pour diffuser des codes malveillants. Par exemple, un faux courriel de l'Organisation mondiale de la Santé a incité la victime à cliquer sur un lien pour accéder aux "5 conseils pour échapper au coronavirus". Un autre appât observé était une fausse carte de suivi de la pandémie utilisée comme vecteur d'attaque.

Les hôpitaux tels que l'hôpital universitaire de Brno en République tchèque représentent une cible de choix pour les assaillants. En effet, cet hôpital est l'un des plus grands laboratoires d'analyses du COVID-19.

Nos analystes ont identifié 2 types de menaces :

- ## Activités cybercriminelles

Trickbot
Une campagne du trojan bancaire Trickbot a ciblé spécifiquement des adresses e-mail italiennes. L'e-mail de phishing est livré avec un document Word qui prétend contenir des conseils sur des moyens pour prévenir les infections. La pièce jointe intègre un script Visual Basic pour Applications (VBA) malveillant qui déploie une nouvelle variante de Trickbot sur la machine de la victime.

Le corps de l'e-mail est adapté au contexte géographique : il est rédigé dans un italien correct et contient des détails relatifs à l'Italie.

Lokibot
Une campagne distincte de phishing exploitant le thème du coronavirus prétend provenir d'une société de livraison qui fournit de nouvelles informations sur l'impact du virus sur ses opérations. Le but de cette communication est en fait de propager le malware Lokibot.

L'e-mail a pour objet «Coronavirus Customer Advisory Issue» et contient ce qui semble être une pièce jointe au format PDF, mais il s'agit en réalité d'un fichier exécutable.

Emotet, NanoCore et Azorult
Les chercheurs de Proofpoint ont également identifié un certain nombre de campagnes de piratage sur le thème du coronavirus qui installent des logiciels malveillants, notamment Emotet, NanoCore et Azorult sur la machine de leurs victimes. Ces campagnes fournissent aux attaquants un moyen de dérober des données personnelles et leur fournissent un accès via une porte dérobée aux réseaux d'entreprise.

Le cheval de Troie Android Cerberus
Ce récent trojan bancaire pour Android est fourni via de fausses applications Coronavirus hébergées sur des domaines nouvellement enregistrés (et non sur le Google Play Store).

Kpot infostealer & CoronaVirus ransomware
Un faux site internet prétendant promouvoir WiseCleaner distribue en fait un downloader pour l'infostealer Kpot. Kpot vole des cookies et des identifiants de connexion utilisés par de nombreuses applications. Le downloader chiffre les fichiers sur les systèmes et affiche une demande de rançon en utilisant le thème du Coronavirus. Ce malware est également susceptible de verrouiller Windows.

BlackWater
BlackWater est un nouveau malware qui utilise un canal de C&C original : il détourne les Workers Cloudflare. BlackWater a été distribué sous la forme d'un fichier EXE (avec une double extension .docx.exe) contenu dans une archive RAR. Une fois que l'utilisateur a exécuté le fichier malveillant, un document leurre est chargé et le logiciel malveillant est installé sur l'ordinateur de la victime. Les fonctionnalités du malware n'ont pas encore été analysées.

TA505
Ce groupe cybercriminel envoie des fichiers XLS piégés (COVID-19-FAQ.xls) depuis le 10 mars. Une compromission réalisée par un malware de cet acteur pourrait conduire à une attaque ciblée utilisant le rançongiciel Clop.

Bien que les cybercriminels soient les principales menaces utilisant le coronavirus pour leurre, des acteurs étatiques ont également exploité l'épidémie de COVID-19 comme appât.

- ## Activités liées à des Etats

Pakistan
Le groupe APT-36, qui opèrerait à partir du Pakistan, a utilisé un document prétendant offrir des conseils sur la santé comme leurre pour diffuser Crimson RAT, un malware qui permet d'exfiltrer des données.

Russie
Le premier groupe d'attaquants étatique à utiliser le coronavirus comme leurre semble être le groupe Hadès, censé opérer à partir de la Russie et lié à APT28 (Fancy Bear).

Des documents malveillants ont été envoyés à des cibles en Ukraine, sous la forme de courriels usurpant l'identité du Centre de santé publique du ministère de la Santé Ukrainien.

Corée du Nord
Un groupe nord-coréen a envoyé des logiciels malveillants via des documents piégés détaillant la réponse de la Corée du Sud à l'épidémie de COVID-19.

Les documents - qui auraient été envoyés à des responsables sud-coréens - déployaient BabyShark, un malware précédemment utilisé par le groupe d'attaquants nord-coréen Kimsuky.

Chine
Le groupe Mustang Panda a diffusé des e-mails contenant une archive RAR présentée comme un message du Premier ministre vietnamien sur l'épidémie de coronavirus. L'attaquant a installé un cheval de Troie sur les ordinateurs des utilisateurs qui ont téléchargé et décompressé le fichier.

Un autre groupe associé à la Chine, nommé Vicious Panda, a ciblé des organisations gouvernementales mongoles avec des documents affirmant détenir des informations sur la prévalence de nouvelles infections à coronavirus.

Un groupe associé à la nébuleuse Winnti a envoyé un document malveillant exploitant le thème de l'épidémie du coronavirus au Kirghizistan pour déployer le malware Winnti.

Iran
Le ministère iranien de la Santé a conseillé à sa population de télécharger une application spécifique créée par le gouvernement et fournissant des explications sur les symptômes du COVID-19. L'application était en réalité un logiciel espion visant à recueillir l'emplacement de son utilisateur permettant de déterminer où et quand les citoyens iraniens se déplacent.

SEKOIA a également observé le groupe iranien connu sous le nom de MuddyWater utiliser le thème du coronavirus pour ses messages de spear-phishing.

Recommandations

- **Suiver les conseils des organismes officiels afin de vous protéger contre la propagation de fausses informations liées au COVID-19**
- **Soyez attentif aux communications non sollicitées contenant des messages alarmistes et / ou pouvant se faire passer pour des institutions officielles de santé et de sécurité.**
- **Sensibiliser aux attaques de phishing et à la fraude au président (Business Email Compromise)**
- **S'assurer que les systèmes d'exploitation et les logiciels sont à jour**
- **Pratiquer le principe de moindre privilège**
- **Utiliser l'authentification multi-facteurs lorsque cela est possible**
- **Désactiver les macros**
- **Surveiller les points potentiels d'exfiltration de données**
- **Placez sur liste noire tous les indicateurs associés à ces menaces spécifiques**

Détails techniques & IoC

RiskIQ produit une liste de nouveaux indicateurs observés en lien avec le thème du coronavirus (contient vraisemblablement aussi des sites légitimes)
https://covid-public-domains.s3-us-west-1.amazonaws.com/README

Un serveur MISP dédié à partager des indicateurs de compromission liées à des menaces COVID-19 (si vous souhaitez un accès, il suffit de demander sur Twitter par DM au compte @MISPProject)
https://covid-19.iglocska.eu/

Flux d'hostnames trouvés dans les logs de Certificate Transparency liés au COVID-19
https://1984.sh/covid19-domains-feed.txt

Tous les IoC des diverses campagnes et logiciels malveillants exploitant le thème dy COVID-19 sont disponibles dans l'Intelligence Center, notre base de renseignement sur les cybermenaces, qui inclut un feed CTI.

SEKOIA.IO, notre plateforme SaaS de détection et réponse aux incidents de sécurité bénéficie d'indicateurs et de CTI pour permettre la détection en temps réel des menaces sur le thème du coronavirus.

CONFIANCE

HAUTE

SOURCES

- FLINT. 2020-031 - Malicious campaigns using Coronavirus as bait
- FLINT 2020-047 - The data-stealing FormBook malware use Coronavirus as bait
- FLINT 2020-051 - Cloudflare Worker leveraged by BlackWater malware for Command & Control
- [Recorded Future] Capitalizing on Coronavirus Panic, Threat Actors Target Victims Worldwide
- [ZDNet] State-sponsored hackers are now using coronavirus lures to infect their targets
- [F-Secure] Coronavirus email attacks evolving as outbreak spreads
- [Threatpost] APT36 Taps Coronavirus as 'Golden Opportunity' to Spread Crimson RAT
- [BleepingComputer] BlackWater Malware Abuses Cloudflare Workers for C2 Communication
- [ZDNet] Czech hospital hit by cyberattack while in the midst of a COVID-19 outbreak
- [Cyberscoop] Cybercriminals, nation-states increasingly tailoring coronavirus spearphishing campaigns
- [Threatpost] Coronavirus-Themed APT Attack Spreads Malware
- [ZDNet] State-sponsored hackers are now using coronavirus lures to infect their targets
- [ProofPoint] Coronavirus Threat Landscape Update
- [Lukas Stefanko] Android – Coronavirus – related malware tracker
- [ProofPoint] Coronavirus Threat Landscape Update
- [Lukas Stefanko] Android – Coronavirus – related malware tracker