THALES

COVID-19

CYBER THREAT ASSESSMENT

24/03/2020

Version – 01

CYBER THREAT INTELLIGENCE ASSESSMENT

COVID-19
UN PUISSANT FACTEUR CRISOGENE

RÉSUMÉ

L'aggravation de la crise COVID-19 en Europe, qui est devenue le nouvel épicentre de l'épidémie, implique une augmentation du nombre d'acteurs de la menace utilisant des leurres liés à cette actualité pour compromettre leurs victimes.

Un changement dans cette dynamique doit notamment être pris en compte par les institutions et organisations critiques.

Alors que les acteurs profitant de l'actualité pour mener leurs attaques étaient initialement des cybercriminels, on constate que de plus en plus de groupes parrainés par des états (*Advanced Persistent Threat*) utilisent ce thème pour mener leurs campagnes d'espionnage.
Un autre phénomène à suivre est le nombre croissant d'applications mobiles Android utilisées pour compromettre largement les populations.

Globalement il apparait aujourd'hui, suivant plusieurs sources, que 50% des noms de domaines créés depuis Décembre et liés au thème du COVID-19 ou Coronavirus peuvent amener à l'injection de logiciels malveillants (infographies présentées en 1.6).

TYPE D'ACTEUR DE LA MENACE IDENTIFIÉS

- ✓ GROUPES SOUPÇONNÉS D'ÊTRE SPONSORISÉS PAR DES ETATS
- ✓ CYBERCRIMINELS

MOTIVATION

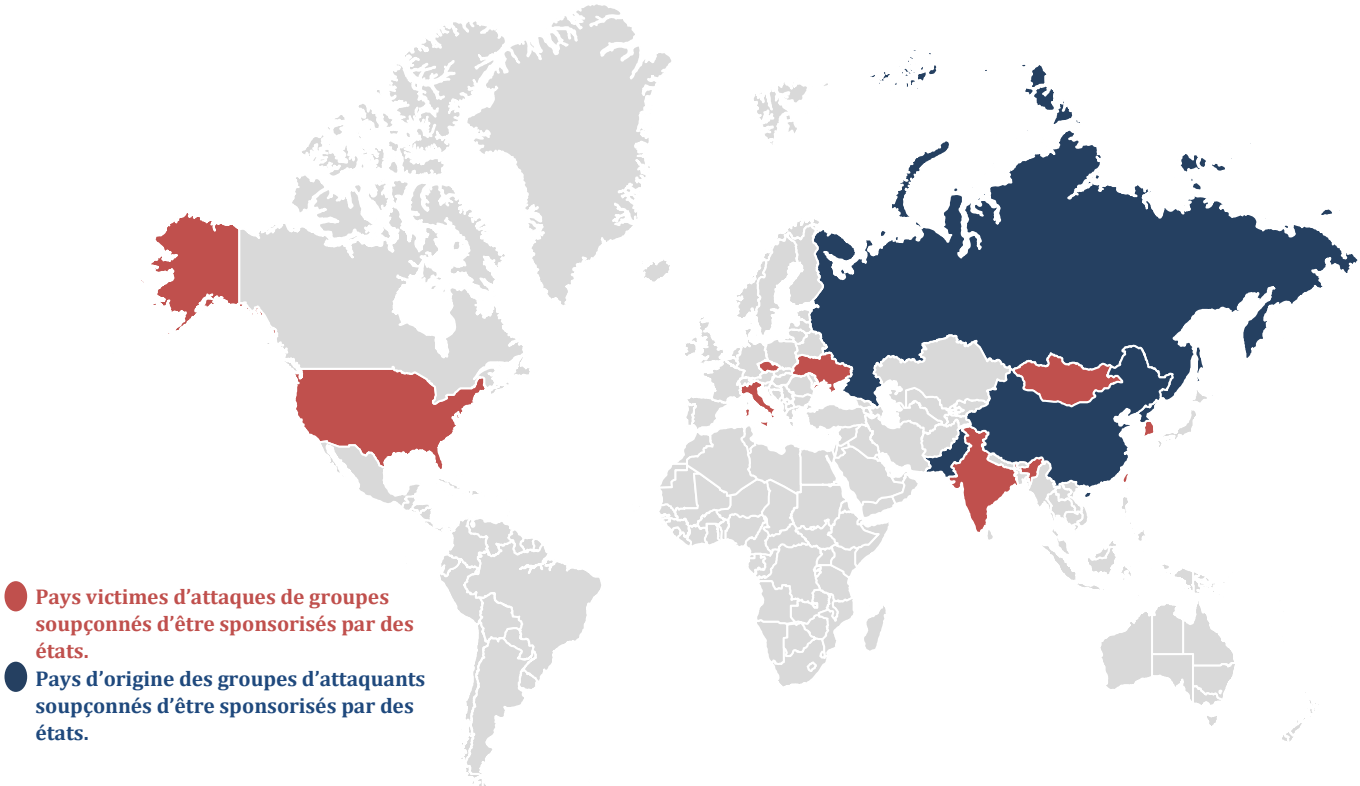
- ✓ GAINS FINANCIERS
- ✓ ESPIONAGE

TABLE DES MATIÈRES

1.1 AVIS CTI

Comme le nombre d'acteurs de la menace utilisant des leurres et des applications corrompus liés au COVID-19 augmente rapidement, une prudence particulière doit être observée. Ces campagnes d'attaques profitent d'un phénomène de stupéfaction collective qui a pour effet de poser des œillères sur les yeux du plus grand nombre.

Il semble que l'écosystème de la menace cyber suive la propagation géographique du COVID-19 avec des attaques d'abord en Asie, puis en Europe de l'Est et maintenant en Europe de l'Ouest. Le territoire français présente donc un risque d'attaques accru.



Pays pris pour cible par des attaquants aux mode opératoire centré sur la thématique du CORONAVIRUS.

Notre attention, sursollicitée par la crise du COVID-19, peut nous pousser à agir sans considérations pour notre sécurité immédiate, notamment cyber.

La crainte nous pousse à rechercher le plus d'informations possible pour bâtir une sensation de maîtrise individuelle d'un phénomène qui nous échappe. Or cet élan nous rend beaucoup plus vulnérable aux fausses nouvelles.

Cette vulnérabilité doit être prise en compte, intégrée et acceptée par les institutions, les organisations et les individus. Seule cette première étape permet de moduler son comportement comme recommandé ci-après.

Selon les déclarations de certains groupes d'attaquants, les hôpitaux devraient être épargnés. Des groupes de grands cybercriminels notamment ceux opérants les ransomwares MAZE et DOPPELPAYMER ont affirmé qu'aucun hôpital ne serait pris pour cible dans le cadre de cette campagne mondiale. Néanmoins, ces déclarations ne doivent en aucun cas amener à relâcher sa vigilance puisque des attaques ont été constatées notamment contre les Hôpitaux de Paris.

1.2 ACTEURS ACTIFS DE LA MENACE

Les acteurs de la menace identifiés à ce jour comme utilisant la crise COVID-19 dans le cadre de leurs campagnes d'attaque sont les suivants :

✓ **Vicious Panda (origine chinoise présumée)** : Check Point Research a découvert une nouvelle campagne contre le secteur public mongol, qui profite de l'actuelle alerte au coronavirus, afin de livrer à la cible un implant de logiciel malveillant jusqu'alors inconnu.

Original

МОНГОЛ УЛСААС БНХАУ-Д СУУГАА ЭЛЧИН САЙДЫН ЯАМ

ШУУРХАЙ МЭДЭЭ

2020 оны 1 дүгээр сарын 22-ны өдөр — №ШМ072004 — Бээжин хот

Шинэ коронавирусын халдварын тархалтын тухай

БНХАУ-ын Төрийн зөвлөлийн Хэвлэл мэдээллийн албанаас өнөөдрийн 10.00 цагт хийсэн хэвлэлийн бага хурлын үеэр Хятад улсад шинэ коронавирусын халдварт хатгалгаагаар өвчилсөн 440 хүн байгаа бөгөөд 9 нас барсан тохиолдол байгааг мэдээлсэн.

Хятадын Үндэсний эрүүл мэндийн хорооноос гаргасан статистик мэдээллээр өнөөдрийн байдлаар Хятад улсын өмнөд болон зүүн өмнөд хэсгийн 14 муж, хот мөн АНУ, Япон, Өмнөд Солонгос, Австрали (тус бүр 1), Сингапур (7), Тайланд (2) зэрэг улсад тархсан байна. Вирусын тархалтын эрчүүдэн байгаа бөгөөд дээрх 440 өвчтөний оймын хүрээний нийт 2197 хүнд танцалт хийж, 765 хүний халдварүүйг тогтоож, 1394 хүнийг үргэлжлүүлэн хянаж байна.

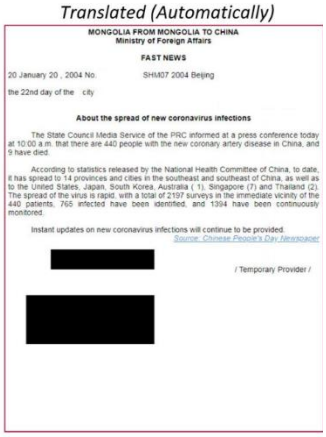
Шинэ коронавирусын халдварын талаарх шуурхай мэдээллийг үргэлжлүүлэн хүргэж болно.

Эх сурвалж: Хятадын Ардын вөрийн сонин цахим мэдээ

БОЛОВСРУУЛСАН: [redacted]

[redacted]

Translated (Automatically)



MONGOLIA FROM MONGOLIA TO CHINA
Ministry of Foreign Affairs

FAST NEWS

20 January 20 , 2004 No: SHM07 2004 Beijing

the 22nd day of the city

About the spread of new coronavirus infections

The State Council Media Service of the PRC informed at a press conference today at 10:00 a.m. that there are 440 people with the new coronary artery disease in China, and 9 have died.

According to statistics released by the National Health Committee of China, to date, it has spread to 14 provinces and cities in the southeast and southeast of China, as well as to the United States, Japan, South Korea, Australia (1), Singapore (7) and Thailand (2). The spread of the virus is rapid, with a total of 2197 surveys in the immediate vicinity of the 440 patients, 765 infected have been identified, and 1394 have been continuously monitored.

Instant updates on new coronavirus infections will continue to be provided.

Source: Chinese People's Day Newspaper

[redacted]

/ Temporary Provider /

[redacted]

Original

ГАДААД ХАРИЛЦААНЫ ЯАМ
БАРИМТ БИЧИГИЙН ТӨСӨЛД САНАЛ АВАХ ХҮҮДАС

Нягтлэн хэр: [redacted]
Боловсруулсан ажилтны нэр: [redacted]
Боловсруулсан огноо: 2020.01.02
Баримт бичгийн төрөл: Сайдын албан тоотын төсөл
Төөч утга, тарүу: Санал хүргүүлэх тухай

№	Албан тушаалын нэр	Гарын үсэг, огноо
1	[redacted]	
2		
3		

[redacted]

Санал хүргүүлэх тухай

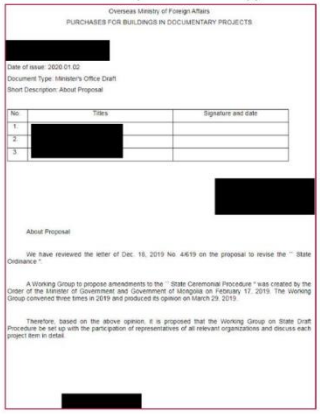
"Терөйн ёслолын журам"-ын шинэчлэн боловсруулах санал авах тухай 2019 оны 12 дугаар сарын 10-ны өдрийн 4/619 тоот албан бичгээрэй танилцуулав.

Монгол Улсын сайд, Засгийн газрын Хэрэг эрхлэх газрын дарын 2019 оны 2 дугаар сарын 22-ны өдрийн 17 дугаар тушаалаар "Терөйн ёслолын журам"-д өөрчлөлт оруулах санал боловсруулан Ахлын хэсгийг байгуулсан билээ. Ахлын хэсэг 2019 оны нүүлэн удаа хуралдаж, 2019 оны 3 дугаар сарын 29-ний өдөр санал дүгнэлтээ боловсруулж гаргасан болно.

Иймд дээр санал дүгнэлтийн дагуу "Терөйн ёслолын журам"-ын төслийг боловсруулах Ахлын хэсгийн хойлогдох бүх байгуулагын төлөөлийг оролцуулан байгуулж, төслийн эцэй эцэст бүрийг нарийвчлан хэлэлцэх боловсруулах санаатай байна.

[redacted]

Translated (Automatically)



Overseas Ministry of Foreign Affairs
PURCHASES FOR BUILDINGS IN DOCUMENTARY PROJECTS

[redacted]

Date of issue: 2020.01.02
Document Type: Minister's Office Draft
Short Description: About Proposal

No.	Titles	Signature and date
1	[redacted]	
2		
3		

[redacted]

About Proposal

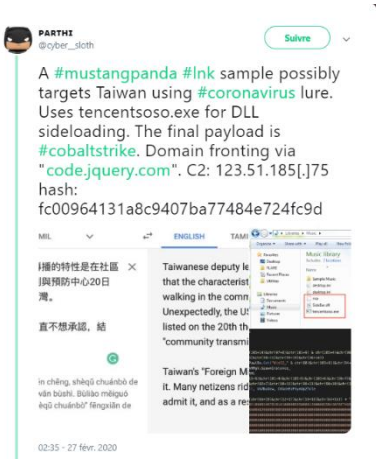
We have reviewed the letter of Dec. 18, 2019 No. 4/619 on the proposal to revise the " State Ordinance ".

A Working Group to propose amendments to the " State Ceremonial Procedure " was created by the Order of the Minister of Government and Government of Mongolia on February, 17, 2019. The Working Group convened three times in 2019 and produced its opinion on March 29, 2019.

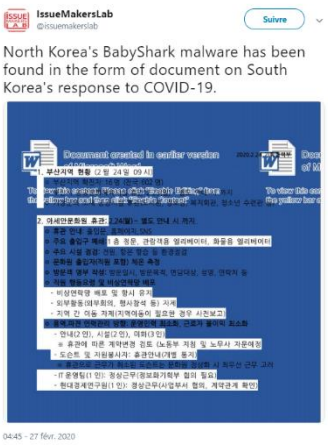
Therefore, based on the above opinion, it is proposed that the Working Group on State Draft Procedure be set up with the participation of representatives of all relevant organizations and discuss each project item in detail.

Un examen plus approfondi de cette campagne permet de la relier à d'autres opérations qui ont été menées par le même groupe anonyme, datant d'au moins 2016. Au fil des ans, ces opérations ont ciblé différents secteurs dans de nombreux pays, comme l'Ukraine, la Russie et la Biélorussie.

✓ **Mustang panda (origine chinoise présumée) :** Mustang Panda est un adversaire basé en Chine qui a démontré sa capacité à assimiler rapidement de nouveaux outils et tactiques dans ses opérations. Dans le cadre de la crise du COVID-19 il est parvenu à utiliser de nouveaux leurres pour prendre Taïwan pour cible.

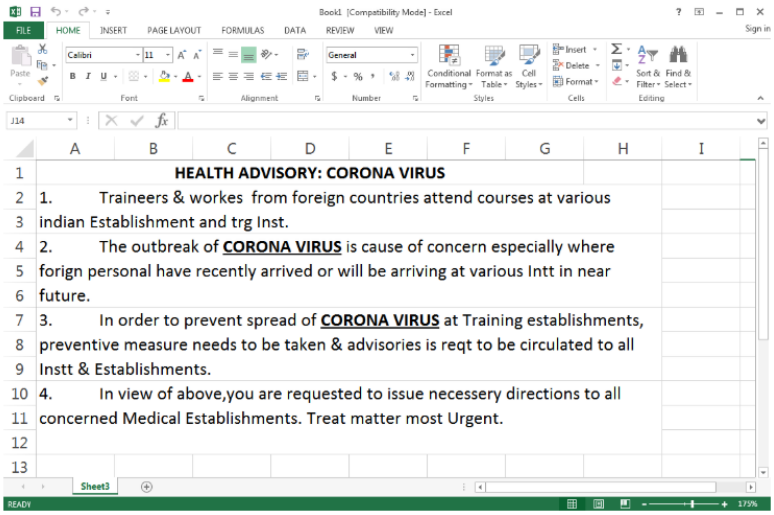


✓ **Kimsuky (origine suspectée : Corée du Nord) :** ATK72 (Kimsuky) a été identifié pour la première fois en 2013 par Kaspersky. Depuis 2013, le groupe Kimsuky poursuit une campagne de cyber-attaque contre des organisations gouvernementales et des agences liées à la défense en Corée du Sud ainsi que contre des institutions et des entreprises liées à l'engagement de la Corée du Sud avec la Corée du Nord. Cet acteur menaçant cible les groupes de réflexion, l'industrie, les exploitants d'énergie nucléaire et le ministère de l'Unification sud-coréens à des fins d'espionnage. Cet acteur semble faire partie de l'unité chargée de l'espionnage en Corée du Sud.



Selon un tweet partagé par la société de cybersécurité sud-coréenne IssueMakersLab, un groupe de pirates informatiques nord-coréens a également caché des logiciels malveillants à l'intérieur de documents détaillant la réponse de la Corée du Sud à l'épidémie de COVID-19.

Ces documents, qui auraient été envoyés à des responsables sud-coréens, ont été piégés avec BabyShark, une souche de malware utilisée auparavant par Kimsuky.



- ✓ **APT36 (origine pakistanaise suspectée) :** APT36 s'appuie principalement sur du spearphishing et les attaques par watering hole pour infecter ses victimes. Le courriel de phishing est soit un document macro malveillant, soit un fichier rtf exploitant des vulnérabilités, tel que CVE-2017-0199. Dans l'attaque sur le thème des coronavirus, APT36 a utilisé un courriel phishing avec un lien vers un document malveillant se faisant passer pour le gouvernement indien (email.gov.in.maildrive[.]email/?att=1579160420).

- ✓ **Groupe Hades (lié à l'APT28 et d'origine russe présumée)** : Le premier groupe de piratage parrainé par l'État à utiliser un leurre à coronavirus a été le groupe Hades, dont on pense qu'il opère depuis la Russie, et qui est lié à APT28 (Fancy Bear), l'un des groupes qui a également piraté le DNC en 2016.

  Selon la société de cybersécurité QiAnXin, les pirates informatiques de Hades ont mené une campagne à la mi-février en cachant un cheval de Troie C# dans des documents appâts contenant les dernières nouvelles concernant COVID-19.

  Les documents ont été envoyés à des cibles en Ukraine, déguisés en courriels provenant du Centre de santé publique du ministère de la Santé ukrainien.

  Les courriels ciblés semblent avoir fait partie d'une campagne de désinformation plus vaste qui a touché l'ensemble du pays, sur différents fronts.

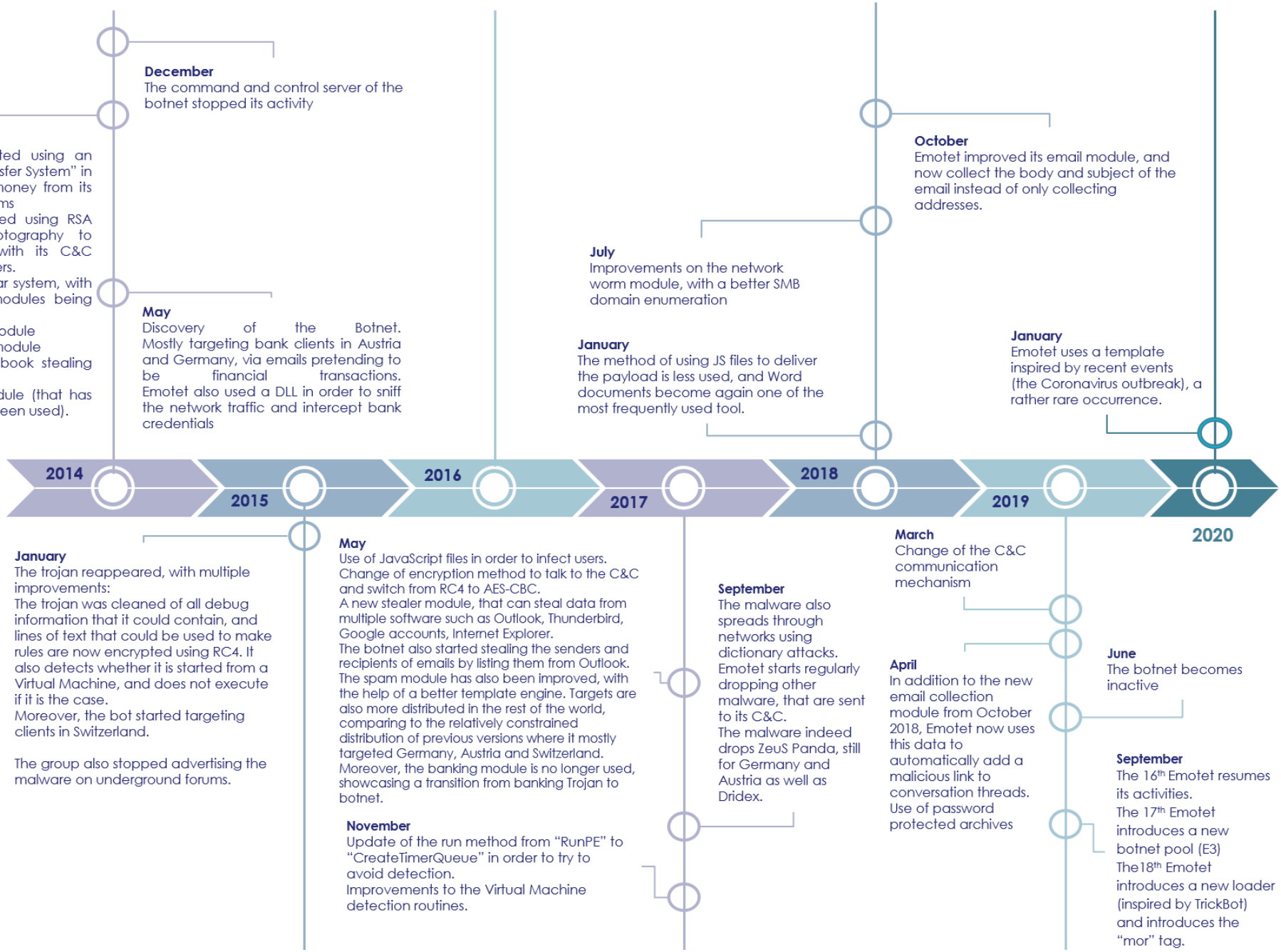
  Tout d'abord, au moment même où Hadès visait ses cibles, une vague de courriers électroniques non sollicités sur le thème des coronavirus a frappé le pays. Deuxièmement, la campagne de courriels a été suivie d'une avalanche de messages sur les médias sociaux prétendant que la maladie COVID-19 était arrivée dans le pays.

Selon un reportage de BuzzFeed News, l'un de ces courriels est devenu viral, et soutenu par la vague d'alarmisme sur les médias sociaux, a provoqué une panique générale et de violentes émeutes dans certaines parties du pays.

BuzzFeed News a rapporté que dans certaines villes ukrainiennes, les habitants ont bloqué les hôpitaux de peur que leurs enfants ne soient infectés par des évacués infectés par des coronavirus venant de la région orientale de l'Ukraine déchirée par la guerre.

Dans cette panique générale, quelques courriels contenant des logiciels malveillants avaient beaucoup plus de chances de passer inaperçus et d'atteindre leurs cibles, dont la plupart étaient très probablement intéressées par les événements actuels qui se déroulaient dans le pays.

- ✓ **TA542 ou Emotet :** Emotet est un téléchargeur très efficace exploité depuis 2014 par ATK104 (alias TA542), un acteur de la menace financière. Ce malware a été remarqué par les excellentes capacités OPSEC de ses auteurs. Il s'appuie sur une infrastructure de commandement et de contrôle résiliente et est conçu pour être difficile à détecter avec des règles de détection statiques. Il a été observé en train de diffuser des logiciels malveillants provenant d'autres acteurs de la menace, ce qui implique qu'être infecté par Emotet signifie être potentiellement infecté par tout autre acteur utilisant ses services.



Timeline présentant les différentes évolutions d'Emotet.

- ✓ **Les acteurs utilisant le malware LokiBot :** Loki, ou "LokiBot" (pour ne pas le confondre avec Loki RAT), est un voleur d'informations vendu sur les forums clandestins. Ce logiciel malveillant recueille des informations à partir de la machine, notamment :
  - Les références de :
    - Navigateurs
    - Plates-formes de jeu
    - Outils de transfert de fichiers
    - Boîtes aux lettres
    - Gestionnaires de mots de passe
  - Portefeuilles en monnaie cryptée
  - Captures d'écran
  - Coups clés
  - Cookies et autres informations du navigateur

  Ces données sont ensuite exfiltrées via des requêtes HTTP POST.

- ✓ **Acteurs utilisant le malware Trickbot :** TrickBot est un logiciel espion de type cheval de Troie qui a été principalement utilisé pour cibler les sites bancaires aux États-Unis, au Canada, au Royaume-Uni, en Allemagne, en Australie, en Autriche, en Irlande, à Londres, en Suisse et en Écosse. TrickBot est apparu dans la nature en septembre 2016 et semble être le successeur de Dyre. TrickBot est développé dans le langage de programmation C++. Trickbot a souvent été abandonné par Emotet.

  Trickbot est apparu à l'automne 2016 et a été initialement décrit comme le successeur de Dyreza, un voleur de titres de compétences. Trickbot est un malware modulaire avec des fonctions supplémentaires comme un spammeur de courrier électronique. Sa fonction la plus notable est le mouvement latéral. En juillet 2017, Trickbot a ajouté un module de propagation de vers basé sur SMB, mais n'avait pas encore inclus un exploit.

  Depuis 2018, nous avons observé qu'Emotet avait abandonné le malware Trickbot. Nous sommes convaincus que ces logiciels malveillants proviennent d'auteurs différents, mais ils semblent être liés et collaborer.

  En 2020, l'auteur continue à améliorer le malware Trickbot, en ajoutant, par exemple, de nouvelles techniques de contournement de l'UAC de Windows 10.

  Dans le cadre des attaques utilisant la thématique du COVID-19 avec Trickbot, l'Italie est particulièrement prise pour cible.

- ✓ **L'hôpital universitaire de Brno (le plus grand laboratoire tchèque pour les tests VIDOC-19) a également été visé par un attaquant inconnu.**

- ✓ **Le Department of Health and Human Services américain a également été victime d'une cyber-attaque liée au contexte du COVID-19.**

1.3 LES APPLICATIONS ANDROID

Certains attaquants ont remarqué que les populations, en plus de suivre les médias traditionnels, utilisent des applications mobiles pour suivre la propagation du virus dans le monde entier. Ils ont donc créé des applications corrompues pour atteindre de nouvelles victimes :

- ✓ **CovidLock** : Application mobile de suivi du coronavirus qui contient un logiciel de rançon,
- ✓ Version reconditionnée du cheval de Troie bancaire **Cerberus Android**,
- ✓ **Covid Android Ransomware**, (qui peut être déverrouillé avec le code "4865083501")

1.4 RAMSOMWARES UTILISANT LE COVID-19 COMME LEURRE

- ✓ **Azorult** : Azorult est un cheval de Troie qui est utilisé pour voler des informations à des hôtes compromis. Il a été vendu en ligne sur des forums de cybercriminalité russophones pour environ 100 dollars.

  Azorult a été observé dans la nature dès 2016. Son auteur a officiellement cessé de le développer en décembre 2018, mais le malware est encore largement utilisé de nos jours dans diverses campagnes en raison des différentes copies qui ont fui.

  Comme Azorult était commercialisable, il n'est pas surprenant qu'il ait été largué à l'aide d'une grande variété de compte-gouttes et de kits d'exploitation.

  Aujourd'hui Azorult utilise une fausse carte géographique de suivi de l'évolution de la pandémie corrompue pour infecter ses victimes.

- ✓ **SpyNote RAT** : SpyNote RAT (Remote Access Trojan) est une famille d'applications Android malveillantes. L'outil de construction SpyNote RAT peut être utilisé pour développer des applications malveillantes avec les fonctionnalités du logiciel malveillant.

- ✓ **Formbook** : Formbook est un voleur d'informations, qui est apparu pour la première fois en février 2016. Il est vendu en ligne par "ng-Coder", pour environ 30$ par semaine, aux côtés de son panel. L'auteur fournit également un hébergement pour ses logiciels malveillants.

  Il dispose de capacités d'enregistrement de touches, peut récupérer des informations d'identification à partir de plusieurs sources, mais l'une de ses caractéristiques est le vol de données de formulaires directement à partir du navigateur, d'où le nom "Formbook". Pour ce faire, il utilise la méthode "WININET.DLL" et surtout la méthode "HttpSendRequest".

  Il est possible pour l'opérateur de télécharger et d'exécuter un logiciel malveillant supplémentaire sur l'ordinateur de la victime.

- ✓ **BlackWater** : BlackWater est un cheval de Troie d'accès à distance qui utilise les utilisateurs de CloudFlare pour ses communications C&C. Il est probablement utilisé pour que l'infrastructure ne soit pas facilement bloquée.

Il utilise JSON afin d'obtenir des commandes qui doivent être exécutées.

À des fins de leurre, ce logiciel malveillant ouvre un document Word lorsqu'il est lancé.

Ce logiciel malveillant est probablement encore en cours de développement et continuera peut-être à évoluer.

- ✓ **Cerberus** : Cerberus est un cheval de Troie bancaire Android signalé pour la première fois par ThreatFabric en juin 2019 et qui pourrait être actif depuis au moins 2017. Le malware est en vente sur un forum de piratage russe appelé xss [...] où les acteurs derrière son développement vendent des licences pour le service entre 4 000 et 12 000 dollars. Ce nouveau malware-as-a-service a peut-être comblé le vide pour les acteurs qui ont besoin de services de location de malware Android comme Anubis et Red Alert qui ont cessé d'exister.

  Les analystes de ThreatFabric soulignent que le logiciel malveillant s'active lorsque les victimes se déplacent, déclenchant l'accéléromètre à l'intérieur de l'appareil. Cerberus reste en sommeil jusqu'à ce que le podomètre (qui mesure le nombre de pas) atteigne un certain nombre de pas. Il modifie également le leurre en fonction du nom du paquet Android, en saisissant les coordonnées bancaires ou les références postales.

1.5 RECOMMANDATIONS

RECOMMANDATIONS

Agence Nationale de Sécurité Des Systèmes D'information

✓ **Suivre les recommandations de l'ANSSI dans son Bulletin d'actualité CERTFR-2020-ACT-002 relatives à la situation actuelle de confinement et au télétravail[1] :**

1. Important de n'exposer sous aucun prétexte sur Internet les interfaces web de serveurs Microsoft Exchange qui ne sont pas au dernier niveau de correctif,
2. Ne pas donner un accès à vos serveurs de partage de fichiers via le protocole SMB,
3. Si vous exposez ou devez impérativement exposer de nouveaux services sur Internet, mettez-les à jour au plus vite avec les derniers correctifs de sécurité et activez les mécanismes de journalisation. Dans la mesure du possible, activez l'authentification double facteur,
4. Appliquer les correctifs de sécurité rapidement, notamment sur les équipements et logiciels exposés sur Internet (solution VPN, solution de bureau distant, solution de messagerie, etc.),
5. Effectuer des sauvegardes hors ligne pour vos systèmes critiques,
6. Utiliser une solution d'accès de type VPN (Virtual Private Network, réseau privé virtuel) propre à l'entreprise, idéalement IPsec ou TLS à défaut, pour ne pas exposer les applications directement sur Internet,
7. Mettre en œuvre des mécanismes d'authentification à double facteur pour limiter les risques d'usurpation d'identité (VPN et applications accessibles) ;
8. Consulter régulièrement les journaux d'accès aux solutions exposées sur Internet pour détecter des comportements suspects.
9. Consulter impérativement le guide du nomadisme de l'ANSSI (disponible ici : https://www.ssi.gouv.fr/uploads/2018/10/guide_nomadisme_anssi_pa_054_v1.pdf)

[1] https://www.cert.ssi.gouv.fr/actualite/CERTFR-2020-ACT-002/

Thales
Recommandations Addionnelles

✓ **Privilégier les canaux de confiance pour s'informer.**

En ce qui concerne l'obligation de surveiller les informations sur un sujet aussi sensible, nous vous conseillons de ne vous informer que par des canaux de confiance (.gouv.fr, médias nationaux, etc.).

Si vous souhaitez suivre l'évolution de l'épidémie utilisez uniquement la carte de l'Université Johns Hopkins (États-Unis)[2]

✓ **Restreindre le nombre de canaux et se prémunir contre le sensationnalisme.**

Ne pas multiplier les canaux d'informations et prendre ses distances par rapport au sensationnalisme de certains supports.

✓ **Fact-checker les informations jugées peu vraisemblables.**

Outre l'augmentation du nombre d'attaques, ce type de sujet est propice à la multiplication des campagnes de fausses nouvelles. Pour éviter cela, les conseils donnés ci-dessus sont également valables. Croiser les informations jugées peu vraisemblable entre plusieurs canaux de confiance permet de réduire l'incertitude.

✓ **Alerter ses collaborateurs en télétravail sur la base des recommandations de l'ANSSI.**

En période de confinement les institutions et organisations ont opté en grande majorité pour le télétravail afin d'éviter les contaminations. Néanmoins le changement de mode de travail ne doit pas amener les collaborateurs à changer leurs habitudes. Bien au contraire, à la lumière des événements détaillés ici, il est conseillé de rappeler les bonnes pratiques à observer largement dans son organisation.

✓ **Face aux campagnes des grands attaquants, privilégier le renseignement cyber.**

Certains attaquants mentionnés plus avant comme les APT sont extrêmement performants. Suivre leurs mouvements à l'aune des campagnes en cours apparaît indispensable à l'échelle des institutions et organisations. Les équipes spécialisées dans le renseignement d'intérêt cyber connaissent bien ces groupes, savent comment ils opèrent et qu'elles sont leurs motivations. S'approvisionner en analyse régulièrement permet d'adopter une position proactive face à ces attaquants.

✓ **Coupler des outils de détection au renseignement cyber pour protéger ses systèmes.**

L'emploi d'outils de type IDS (*Intrusion Detection Systems*) enrichies avec les informations délivrer par le renseignement cyber permet de détecter les attaques de l'ensemble des groupes présentés dans cette analyse au moment de leurs attaques et ainsi de réduire significativement le préjudice potentiel.

[2] https://gisanddata.maps.arcgis.com/apps/opsdashboard/index.html#/bda7594740fd40299423467b48e9ecf6

1.6 INFOGRAPHIES

Timeline des attaques utilisant le COVID-19 comme leurre pour atteindre leurs victimes.

February 1, 2020 – Crooks commence à exploiter le Coronavirus comme appât pour diffuser des logiciels malveillants

Les chercheurs en sécurité mettent en garde contre les campagnes visant à diffuser des logiciels malveillants qui exploitent l'attention des médias sur le COVID-19.

February 25, 2020 – Corée du Sud de la propagation des personnes infectées par le virus Corona 19

Eset Security a trouvé un code malveillant déguisé en programme d'enquête "Corona 19 real time status" et a demandé l'attention du public.

February 26 – La nouvelle cyber-campagne s'appuie sur l'infodémie COVID-19

Des chercheurs du Cybaze Yoroi ont repéré une nouvelle campagne exploitant l'intérêt de l'évolution de COVID-19 pour diffuser des logiciels malveillants

March 6 – TrickBot vise l'Italie en utilisant de faux courriels de l'OMS sur le coronavirus comme appât

Crooks continuent à exploiter l'attention sur l'épidémie de COVID-19, les opérateurs de TrickBot ciblent les utilisateurs italiens.

March 8 – Une nouvelle campagne anti-pourriel sur le thème des coronavirus diffuse le logiciel malveillant FromBook

Les experts ont découvert une nouvelle campagne sur le thème de COVID-19 qui distribue un téléchargeur de logiciels malveillants qui fournit le cheval de Troie l'infostealer FormBook.

March 12 – Azorult diffusé au moyen d'une carte sur le coronavirus compromise

Alors que l'OMS déclare que l'épidémie de COVID-19 est une pandémie, les escrocs tentent d'exploiter la situation pour rentabiliser leurs efforts.

March 13 – Des pirates informatiques parrainés par des états lancent des attaques sur le thème des coronavirus

Les pirates informatiques soutenus par l'État utilisent maintenant des leurres à base de coronavirus pour infecter leurs cibles.

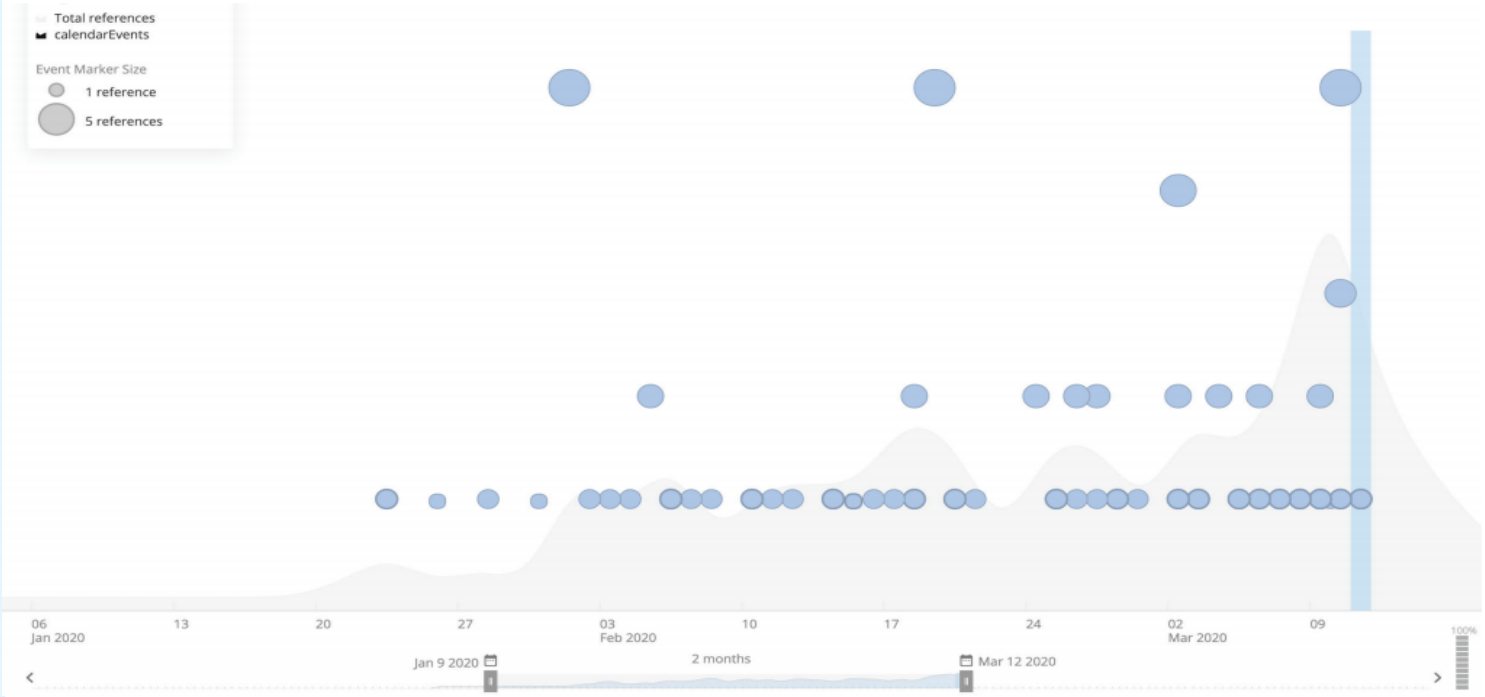
March 15 – BlackWater, un logiciel malveillant qui utilise les "Cloudflare Workers" pour la communication C2

Crooks continue d'abuser de l'intérêt porté à l'épidémie de Coronavirus, maintenant que les experts ont trouvé une nouvelle porte dérobée appelée BlackWater qui prétend fournir des informations sur COVID-19.

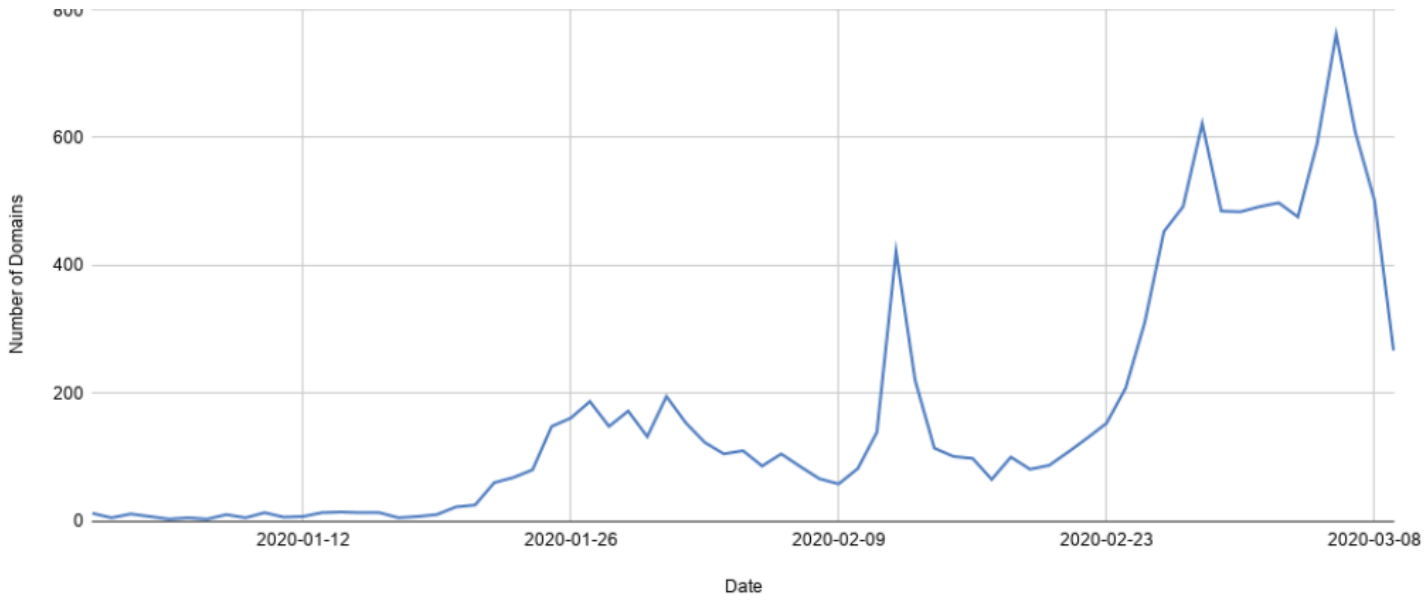
March, 15 - Acient Tortoise utilise le thème du COVID-19 pour lancer des attaques de type BEC

Un gang de cybercriminalité axé sur le Business Email Compromise (BEC) a commencé à utiliser des e-mails frauduleux sur le thème de COVID-19 dans ses attaques.

Évolution du nombre de cyberattaques reliées à l'exploitation de l'actualité sur le COVID-19.



Évolution du nombre de noms de domaines liés au COVID-19 créés depuis Décembre. Check Point, souligne que 50% des noms de domaine liés au terme coronavirus sont susceptibles de provoquer l'intrusion de logiciels malveillants.



[3] https://www.recordedfuture.com/coronavirus-panic-exploit/

1.7 REFERENCES

- ✓ https://securityaffairs.co/wordpress/99744/hacking/us-health-and-human-services.html
- ✓ https://research.checkpoint.com/2020/vicious-panda-the-covid-campaign/
- ✓ http://feedproxy.google.com/~r/eset/blog/~3/D-6mwELGotQ/
- ✓ https://securityaffairs.co/wordpress/99682/cyber-warfare-2/coronavirus-themed-attacks.html
- ✓ https://blog.malwarebytes.com/threat-analysis/2020/03/apt36-jumps-on-the-coronavirus-bandwagon-delivers-crimson-rat/
- ✓ https://www.recordedfuture.com/coronavirus-panic-exploit/
- ✓ https://twitter.com/WebSecurityIT/status/1238877553642831872
- ✓ https://twitter.com/1ZRR4H/status/1239751485312970753
- ✓ https://twitter.com/LukasStefanko/status/1239826056103825408
- ✓ https://korii.slate.fr/tech/hackers-covid-19-coronavirus-cartes-emails-diffusion-virus-malwares-cheval-de-troie
- ✓ https://www.cert.ssi.gouv.fr/actualite/CERTFR-2020-ACT-002/
- ✓ https://www.cert.ssi.gouv.fr/actualite/CERTFR-2020-ACT-001/
- ✓ https://www.ssi.gouv.fr/uploads/2018/10/guide_nomadisme_anssi_pa_054_v1.pdf
- ✓ https://www.lci.fr/police/coronavirus-les-hopitaux-de-paris-aphp-victimes-d-une-cyberattaque-deni-de-service-de-hackers-2148857.html