RAPPORT ESET SUR LES GOUVERNEMENTS :

ciblés mais pas seuls

CYBERSECURITY
EXPERTS ON YOUR SIDE

TABLE DES MATIÈRES

1

GROUPES DE PIRATES, CYBERCRIMINELS ET NÉCESSITÉ D'UNE CYBERSÉCURITÉ RÉSILIENTE POUR LES GOUVERNEMENTS

INTRODUCTION

Même s'il est difficile de faire des prédictions pendant la pandémie, nous pouvons être sûrs que les cyber-risques planant sur les organismes publics continueront d'augmenter, d'évoluer, et de nécessiter une attention et des ressources encore plus importantes pour les atténuer. Comme pour les entreprises, les gouvernements sont confrontés au fait que leurs outils de productivité sont retournés contre leurs intérêts, leur capacité à protéger et fournir des services essentiels, assurer la stabilité économique, et même maintenir la cohésion culturelle et sociétale.

Andy Garth
Government Affairs Lead

Vers le « tout numérique »

Bien entendu, ces risques accrus surviennent à un moment où les organismes publics et les entreprises continuent de naviguer dans les eaux incertaines de la pandémie de COVID-19, ce qui ajoute à un environnement opérationnel déjà complexe pour les responsables de la sécurité et des infrastructures informatiques. Les fonctions des différents organismes gouvernementaux sont certes différentes, mais la tendance générale est à l'expansion de la surface d'attaque. Ce constat est renforcé par l'orientation des organismes publics vers des services numériques si simples et si pratiques que tous ceux qui peuvent les utiliser choisiront de le faire.

Il s'agit notamment du déploiement de systèmes destinés aux citoyens, le passage au Cloud, le recours

accru à des fournisseurs et des prestataires de services tiers, et l'intégration rapide de nombreux utilisateurs en raison de l'adoption de nouveaux modèles opérationnels tels que le télétravail ou le travail hybride. Le rythme de mise en œuvre soutenu de ces éléments ajoute au défi de garantir la résilience des systèmes face aux menaces constantes et évolutives des groupes de pirates et des cybercriminels. Si l'on ajoute à cela la nécessité de rester conforme à la réglementation et de respecter des budgets serrés, il y a certainement de quoi empêcher un RSSI de dormir la nuit.

COVID-19

Les confinements dus au coronavirus et l'augmentation subséquente du nombre de collaborateurs accédant depuis leur domicile aux données des entreprises et des institutions n'ont guère freiné les intérêts des cybercriminels et d'autres acteurs malveillants sponsorisés par des États. En effet, ces deux types de groupes ont mis à profit cette période tumultueuse afin de poursuivre leurs objectifs respectifs, souvent avec une intensité et une persistance accrues. Par exemple, pendant la pandémie, les tentatives d'attaques contre RDP en particulier ont *augmenté* de 768 % entre le premier et le quatrième trimestre 2020.

Les autres menaces détectées par ESET, qui exploitent spécifiquement COVID-19 comme sujet d'intérêt, comportent notamment l'imitation des services gouvernementaux. Par exemple, une *application de suivi de contacts* du « gouvernement canadien ». Pendant les confinements dus à COVID-19, des tentatives d'*hameçonnage via des emails « officiels du gouvernement colombien »* et des attaques de « point d'eau » sur les gouvernements d'Asie du Sud-Est par *OceanLotus*, entre autres, ont ciblé l'interface entre le gouvernement et ses citoyens.

Pendant que les gouvernements luttent pour atténuer les effets de COVID-19 sur la santé, des cyberattaques affectant la prestation de services aux citoyens, volant des données ou compromettant les infrastructures nationales stratégiques, se poursuivent à un rythme effréné. Parmi les plus notables : *le piratage de SolarWinds Orion*, l'*exploitation de Microsoft Exchange*, les attaques sur l'outil de supervision d'infrastructures informatiques *Centreon*, le ciblage délibéré des systèmes de santé en France et en Allemagne, et la multiplication des attaques contre des écoles, des universités et des plateformes d'enseignement.

Au vu des données et des tendances générales, nous nous attendons à ce que les groupes de pirates et les cybercriminels continuent d'affiner leurs tactiques, qui consistent à profiter des préoccupations liées à COVID-19 et cibler des applications largement utilisées. Début 2020, par exemple, les opérateurs du groupe XDSpy *ont diffusé un email* censé provenir des autorités bélarussiennes et prétendant confirmer les premiers cas de coronavirus au Belarus. Il s'agissait en réalité d'une tactique de désinformation relayée sur les réseaux sociaux, comprenant un lien vers un malware.

Cyberespionnage

Les ennemis traditionnels des organismes gouvernementaux sont des acteurs sponsorisés par d'autres États, tentant non seulement de voler des données sensibles, mais cherchant de plus en plus à embarrasser, saper et entraîner des perturbations afin d'assurer leurs propres objectifs politiques et économiques. De tels affrontements entre États se produisent régulièrement dans des zones d'ombre où ils peuvent combattre réciproquement en niant ces activités. Ce cybersport traditionnel s'étend à la sphère économique, avec pour cible prioritaire le pillage de propriété intellectuelle. Dans ce cadre, nous avons constaté un intérêt croissant pour *les développeurs de vaccins* et leurs chaînes d'approvisionnement. Ces activités ont de graves conséquences sur la capacité des gouvernements à protéger les citoyens et leur fournir des services.

Avec des agresseurs cherchant à voler des données ou influencer des événements dans le monde réel, l'ensemble du secteur public, tant au niveau national qu'au niveau local, doit désormais adapter sa posture de sécurité pour contrer en plus les acteurs malveillants sponsorisés par des États, et non plus seulement comme étant la cible de groupes criminels ou de pirates informatiques solitaires. Leurs activités continuent d'augmenter, et pourtant certains organismes estiment ne pas être des

cibles potentielles de ces acteurs. Malheureusement, trop souvent, en raison de l'interconnectivité, les conflits entre États dans une région du globe affectent par inadvertance les systèmes de pays et d'organisations sans rapport avec ces contextes. Devenir un dommage collatéral dans ces batailles croissantes du cyberespace est donc un risque réel.

Gamaredon est un groupe de pirates qui semble parfois agir de manière assez audacieuse, sans faire d'efforts pour se cacher. Son mode opératoire comprend l'utilisation d'injecteurs de modèles ciblant des applications courantes telles que Microsoft Word et Excel, et l'envoi en volume de macros dans le quasi omniprésent Microsoft Outlook pour cibler, par exemple, des individus dans différentes institutions ukrainiennes. En se concentrant sur les outils légitimes utilisés dans les administrations et les entreprises, Gamaredon fait preuve d'une efficacité redoutable pour jauger le contenu d'une machine, comprendre quelles données sensibles sont disponibles, puis se répandre dans le réseau. Nous avons récemment documenté l'évolution du groupe, s'orientant vers le développement de malwares sur mesure.

Grâce à un ensemble d'outils impressionnants, notamment des malwares sans fichier tels qu'un chargeur PowerShell open source personnalisé pour échapper à toute détection, ou *LightNeuron* conçu pour semer la pagaille dans des serveurs Microsoft Exchange désormais trop souvent pris pour cible, le groupe de pirates Turla s'intéresse principalement à des cibles de premier plan : organismes gouvernementaux et entreprises du secteur de la défense. Turla ne se repose cependant pas sur ses lauriers et a créé une nouvelle version de la porte dérobée *Crutch* que nous avons documentée au quatrième trimestre 2020. Elle surveille les disques externes et détourne le stockage dans le Cloud pour ses communications de commande et de contrôle.

Ransomwares : innovation et pression constante

Dans les strates où les acteurs sponsorisés par des États se mêlent aux groupes de pirates de nature plus criminelle, nous pouvons considérer l'évolution vers des attaques ciblées de ransomwares comme étant un indicateur de l'inquiétude croissante des organismes gouvernementaux et des entreprises avec lesquelles ils s'engagent. Par ailleurs, le phénomène de coopération entre plusieurs groupes criminels pour s'introduire dans des systèmes, voler ou chiffrer des données, organiser les paiements et blanchir le produit de la criminalité, est clairement inquiétant.

La collaboration d'ESET en octobre 2020 avec Microsoft, NTT Ltd et plusieurs services de police pour démanteler les botnets Trickbot a révélé un ensemble d'activités complexes, comprenant aussi bien des tentatives de vol d'argent sur des comptes bancaires que l'infection d'entreprises entières avec Trickbot, puis l'utilisation de ce dernier pour exécuter Ryuk et exiger une rançon afin de restituer les systèmes affectés. Il est intéressant de noter que lorsque l'activité de Trickbot a diminué, *l'augmentation des détections dans la télémétrie d'ESET* du botnet *Emotet* a signalé une intensification des activités, y compris du téléchargement de Trickbot.

Cette collaboration a également permis en janvier 2021 de perturber le botnet Emotet, qui est l'un des malwares les plus anciens et les plus répandus. Dirigée par Europol, cette opération à grande échelle a impliqué un certain nombre d'organismes nationaux chargés de l'application de la loi en Europe et en Amérique du Nord.

Avec des enjeux aussi élevés, le personnel de sécurité chargé de défendre la prestation des services et les processus internes est pris entre deux feux, devant rester vigilant à l'égard des acteurs sponsorisés par des États et confronté continuellement aux tactiques, techniques et procédures des groupes de pirates. L'émergence d'une industrie criminelle organisée, qui propose des produits et des services clairs, témoigne de l'innovation et du dynamisme des agresseurs. Ces groupes ont dépassé le stade de l'évaluation des victimes potentielles. Ils cherchent désormais à maximiser leurs gains par la vente de données sur des places de marché criminelles bien établies.

Grâce à leur persistance, ces groupes peuvent souvent passer des semaines voire des mois à l'intérieur des systèmes ciblés, à en effectuer la reconnaissance et récolter des données, avant de *finalement déployer un*

ransomware. Si pour certains, il s'agit d'un moyen de diversifier leurs revenus, pour d'autres, l'objectif est plutôt de saper un gouvernement et les services qu'il supervise. Malgré *de nombreux gouvernements déclarant ouvertement ne pas obtempérer aux demandes de rançons*, il est toujours possible d'en être victime, notamment de techniques d'infection à grande échelle, qui lorsqu'elles sont réussies, sont à la fois dévastatrices et nécessitent beaucoup de ressources pour y remédier.

Les attaques contre les chaînes d'approvisionnement se multiplient rapidement

La perturbation des chaînes d'approvisionnement, qu'elle soit accidentelle ou intentionnelle, est une stratégie qui remonte à l'antiquité, tout comme sa protection ou l'amélioration de sa résilience. La numérisation et les avantages collaboratifs tirés de l'utilisation de fournisseurs tiers ont à leur tour *augmenté le risque d'attaques sur les chaînes d'approvisionnement.*

L'attaque de *DiskCoder.C* (alias NotPetya) en 2017 l'a bien démontré, lorsque le logiciel de comptabilité M.E.Doc, couramment utilisé par un certain nombre d'entreprises régionales et leurs partenaires le long d'une chaîne d'approvisionnement, a été infecté pour perturber les activités des utilisateurs. Que cela ait été prévu ou non, de grandes entreprises internationales ont été victimes de dommages collatéraux. Un grand nombre de ces entreprises, ironiquement, sont impliquées dans la logistique des chaînes d'approvisionnement physique mondiales. Trois ans plus tard, ce n'est plus d'un logiciel de comptabilité infecté donc il s'agit, mais d'une vaste campagne persistante de *piratage de SolarWinds Orion*. L'attaque a touché des milliers d'utilisateurs sur cette plateforme et a ouvert la voie à des activités criminelles à grande échelle.

Les chercheurs d'ESET ont découvert plusieurs autres attaques contre des chaînes d'approvisionnement au cours des derniers mois : le *groupe Lazarus* utilisant des modules complémentaires de sécurité piratés, *Operation Stealthy Trident* attaquant un logiciel de chat pour entreprises spécifique à une région, *Operation SignSight* utilisée pour compromettre une autorité de certification gouvernementale, et *Operation NightScout* piratant un émulateur Android.

Le domicile, le lieu de travail de la nouvelle normalité

Le télétravail et le travail hybride ont considérablement augmenté les risques pour tous les employeurs et donc les administrations publiques. Il est clair que ces arrangements perdureront et continueront d'être une source de préoccupation à mesure qu'une certaine forme de travail hybride permanent deviendra partie intégrante du modèle opérationnel de l'après COVID-19. Du point de vue de la sécurité des systèmes, l'environnement personnel peut ressembler au Far West, avec des « propriétés » et des « avant-postes » plus exposés aux cyberattaques d'un nombre apparemment toujours croissant de cybercriminels de plus en plus sophistiqués qui cherchent à se mêler à l'action.

On estime que *23 % des failles de cybersécurité sont dues à une erreur humaine*. Les agresseurs profitent souvent de l'instinct de cliquer (en quelques millisecondes) sur des liens semblant légitimes. Certaines des plus grandes failles de sécurité ont été provoquées par des professionnels de l'informatique expérimentés, qui auraient dû être plus avisés, notamment en connectant des appareils personnels sur le réseau de l'entreprise, en configurant incorrectement des systèmes dans le Cloud, et par d'autres mauvaises pratiques. Bien entendu, une formation accrue du personnel et le renforcement des processus sont essentiels pour que les comportements requis en matière de sécurité deviennent instinctifs.

Bien que l'on accorde beaucoup d'attention aux attaques de pirates informatiques, le Ponemon Institute a révélé dans son *Rapport mondial de 2020 sur le coût des menaces internes*, que le nombre d'incidents causés par le personnel même des entreprises a augmenté de 47 %, passant de 3 200 en 2018 à 4 716 en 2020. La plupart de ces failles de sécurité de sécurité sont dues à des erreurs humaines, mais certaines sont des attaques internes déclenchées par des *collaborateurs mécontents*. Il peut s'agir de vol de données, de dommages physiques et de suppression de comptes par vengeance, à des fins de profit personnel

ou pour servir les intérêts d'un nouvel employeur, voire d'un autre État. De telles attaques, en particulier celles menées par des personnes disposant de privilèges administrateur, sont plus difficiles à détecter sans un outil de détection et de traitement des incidents ou d'autres solutions de détection avancées gérées par des experts.

Ciblés mais pas seuls

Dans l'environnement de sécurité dynamique actuel, il est plus important que jamais de ne pas surestimer votre cybersécurité. Le cyber-risque continue d'augmenter, et non de diminuer. Des audits réguliers, des tests et des simulations avec des scénarios d'attaque sont de plus en plus essentiels pour vous aider à repousser les attaques et résoudre rapidement les incidents. En raison des compétences des acteurs sponsorisés par des États et des outils dont ils disposent, le risque d'être pris pour cible ou d'être victime de dommages collatéraux nécessite désormais des défenses multicouches complexes, une surveillance active, des ***renseignements actualisés sur les menaces***, et une équipe de sécurité toujours plus qualifiée.

En élargissant votre compréhension des menaces en constante évolution, vous pourrez non seulement mieux protéger vos propres systèmes, mais également mieux informer vos parties prenantes, les entreprises et les citoyens qui se tournent vers les organismes gouvernementaux pour obtenir des conseils. En cette année marquée par de nombreuses perturbations et une grande tristesse, l'une des tendances positives en matière de cybersécurité, tout comme dans la lutte contre le coronavirus, est l'émergence et l'importance d'un partenariat solide entre le gouvernement et le secteur privé pour relever ces défis. ESET s'en félicite, et se réjouit de travailler avec ses partenaires gouvernementaux pour mieux sécuriser le monde numérique.

2

ATTAQUES DES GROUPES DE PIRATES EN EUROPE : UNE MENACE CROISSANTE POUR LES GOUVERNEMENTS

Les attaques spectaculaires menées par les groupes de pirates au cours des six derniers mois sont-elles le signe d'un retour à la normale ou d'une nouvelle tendance dans les attaques contre les chaînes d'approvisionnement ?

Robert Lipovský
Senior Malware Researcher

Au cours des six derniers mois, une série d'attaques notables menées par des groupes de pirates a ciblé des pays du continent européen, de la France à l'Europe de l'Est et aux Balkans, et des gouvernements, des entités militaires et des entreprises privées.

En exemple de telles activités malveillantes découvertes par ESET, une nouvelle version de *Crutch*, une porte dérobée doublée d'un voleur de documents jusqu'alors inconnue, appartenant au groupe de pirates Turla. Les chercheurs d'ESET l'ont trouvée dans le réseau d'un ministère des affaires étrangères d'un pays de l'Union européenne. *Gamaredon*, un groupe de pirates connu pour son ciblage incessant des organisations gouvernementales en Ukraine, et qui a *mis à jour son arsenal de malwares* tout au long de 2020, est une autre découverte d'ESET.

Dans les sections suivantes, nous allons examiner de plus près deux autres exemples : *XDSpy*, un groupe de pirates qui a réussi à rester sous le radar pendant neuf ans, et Sandworm, qui est l'un des groupes de pirates les plus dangereux en activité.

Nous aborderons également le rôle des attaques contre des chaînes d'approvisionnement dans l'arsenal des différents groupes, un sujet qui retient encore plus l'attention que d'habitude depuis que le piratage de SolarWinds a fait la une des actualités internationales.

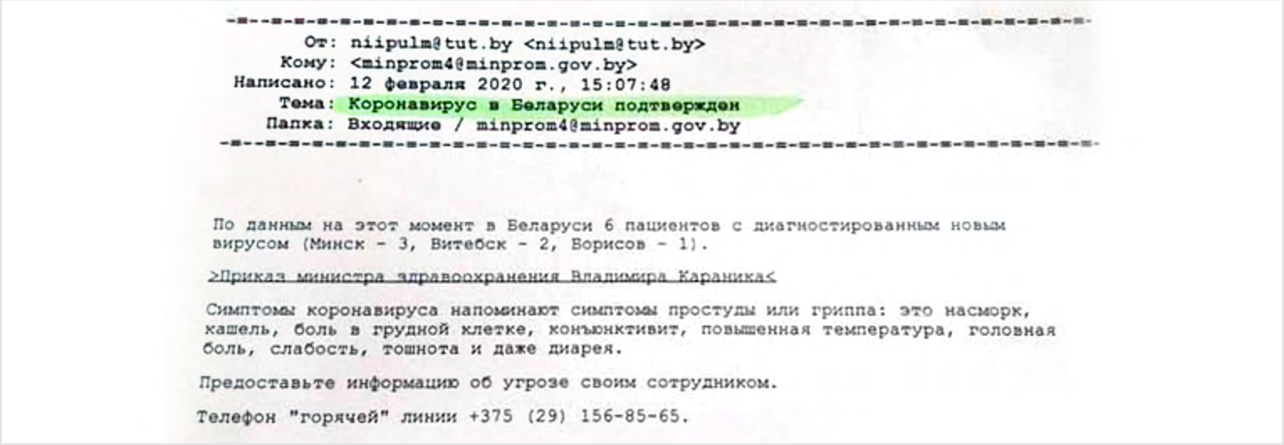
XDSpy – Vol de secrets d'État depuis 2011

La caractéristique la plus intéressante du groupe de pirates XDSpy est probablement qu'il est passé largement inaperçu pendant neuf ans. Ce groupe d'espionnage est actif depuis 2011, et ses activités n'ont jamais été signalées jusqu'à un *avertissement* du CERT biélorusse en février 2020.

Au fil des ans, le groupe a compromis de nombreuses entités gouvernementales, notamment des entités militaires, des ministères des affaires étrangères, et des entreprises privées en Europe de l'Est et dans les Balkans. Selon la télémétrie d'ESET, les cibles de XDSpy sont principalement situées en Biélorussie, en Moldavie, en Russie, en Serbie et en Ukraine.

Les opérateurs de XDSpy utilisent des emails d'hameçonnage pour compromettre leurs cibles. Les emails sont légèrement différents les uns des autres, car certains contiennent une pièce jointe, tandis que d'autres contiennent un lien vers un fichier malveillant. Le premier niveau du fichier malveillant ou de la pièce jointe malveillante est généralement une archive ZIP ou RAR. Fin juin 2020, les opérateurs ont intensifié leur campagne à l'aide d'une vulnérabilité d'Internet Explorer, CVE-2020-0968.

Puis, en septembre 2020, les opérateurs ont utilisé le site officiel du gouvernement russe sur COVID-19, rospotrebnadzor. ru, comme leurre pour télécharger XDDown, le principal composant du malware chargé de récupérer des plugins supplémentaires.



```
От: niipulm@tut.by <niipulm@tut.by>
Кому: <minprom4@minprom.gov.by>
Написано: 12 февраля 2020 г., 15:07:48
Тема: Коронавирус в Беларуси подтвержден
Папка: Входящие / minprom4@minprom.gov.by

По данным на этот момент в Беларуси 6 пациентов с диагностированным новым
вирусом (Минск - 3, Витебск - 2, Борисов - 1).

>Приказ министра здравоохранения Владимира Караника<

Симптомы коронавируса напоминают симптомы простуды или гриппа: это насморк,
кашель, боль в грудной клетке, конъюнктивит, повышенная температура, головная
боль, слабость, тошнота и даже диарея.

Предоставьте информацию об угрозе своим сотрудником.

Телефон "горячей" линии +375 (29) 156-85-65.
```

En termes de fonctionnalité et d'architecture, XDSpy utilise un ensemble d'outils de cyberespionnage typique composé d'un module principal de téléchargement qui récupère des plugins supplémentaires pour effectuer les actions souhaitées. Au cours de nos recherches, nous avons découvert des plugins utilisés pour exfiltrer des fichiers du lecteur principal ou de lecteurs externes, faire des captures d'écran, et extraire des mots de passe enregistrés dans différentes applications telles que des navigateurs web et des programmes de messagerie. L'un des plugins, appelé XDLoc, est utilisé pour énumérer les SSID (noms des points d'accès Wifi) environnants, très probablement pour géolocaliser les machines victimes.

Porte dérobée Exaramel en France : une autre attaque de Sandworm sur une chaîne d'approvisionnement ?

En ce qui concerne le célèbre groupe de pirates Sandworm, la nouvelle la plus importante de ces six derniers mois a été *l'inculpation* par le ministère de la Justice des États-Unis de six officiers du GRU russe pour leur rôle présumé dans les nombreuses attaques du groupe.

Outre l'aspect géopolitique, les défenseurs doivent savoir que, même si les attaques les plus célèbres de Sandworm datent de 2015 (la *première attaque contre le réseau électrique ukrainien*) et 2018 (*Olympic Destroyer*), ce groupe dangereux est toujours très actif en 2021.

En février 2021, l'ANSSI, l'agence nationale de sécurité informatique française, a publié un *rapport* révélant une campagne visant le logiciel de surveillance informatique Centreon, qui a entraîné des intrusions dans plusieurs entreprises françaises. La campagne a duré de 2017 à 2020, et a touché principalement des prestataires informatiques, notamment des hébergeurs web. Deux portes dérobées ont été découvertes sur les systèmes compromis : le webshell P.A.S. et (ce qui est beaucoup plus intéressant) la porte dérobée *Exaramel*.

Exaramel est l'œuvre de Sandworm (plus précisément, un sous-groupe surveillé par ESET, du nom de TeleBots). C'est la preuve qui nous a permis d'attribuer le malware *Industroyer* au même groupe de pirates, en raison de similitudes du code.

En gardant à l'esprit le récent piratage de SolarWinds et le fait que Sandworm a mené des attaques contre des chaînes d'approvisionnement de par le passé (rappelez-vous l'infection de *M.E.Doc* qui a conduit à l'épidémie de NotPetya), le secteur de la cybersécurité s'est immédiatement intéressé aux détails entourant Centreon.

D'après *Centreon*, la faille de sécurité n'était pas le résultat d'une attaque sur une chaîne d'approvisionnement. Au lieu de cela, la campagne a exploité des versions obsolètes de son logiciel de surveillance informatique, et non l'entreprise elle-même.

Le fait qu'il ne s'agissait pas d'une attaque sur une chaîne d'approvisionnement est une constatation positive, car le contraire signifierait une faille de sécurité grave avec des conséquences potentiellement importantes. Un autre fait reste cependant vrai : des entreprises ont utilisé des versions vulnérables du logiciel de surveillance informatique Centreon, et des agresseurs en ont profité pour les compromettre.

Perspectives d'avenir

Les six derniers mois ont montré que les groupes de pirates ont poursuivi normalement leurs activités, qu'il s'agisse de groupes très sophistiqués comme Sandworm que de groupes moins érudits (mais toujours capables de rester sous le radar et d'atteindre leurs objectifs) comme XDSpy, et de tout autre groupe entre les deux.

Les attaques contre des chaînes d'approvisionnement, même si elles ne sont pas toutes aussi spectaculaires que le piratage de SolarWinds (ou d'autres événements, tels que la récente campagne Centreon qui ressemble à une attaque sur une chaîne d'approvisionnement mais n'en est pas), deviennent une tendance majeure. En fait, rien qu'au quatrième trimestre 2020, ESET a découvert probablement autant d'attaques contre des chaînes d'approvisionnement que l'ensemble du secteur n'en a connu annuellement il y a quelques années seulement : le cas de Lazarus détournant le logiciel *WIZVERA VeraPort* utilisé par des sites gouvernementaux et bancaires en Corée du Sud, *Operation StealthyTrident* compromettant le logiciel de chat Able Desktop utilisé par plusieurs agences gouvernementales mongoles, *Operation SignSight* compromettant le logiciel de signature distribué par le gouvernement vietnamien. Plus récemment, au 1er trimestre 2021, ESET a également découvert *Operation NightScout*, une attaque sur une chaîne d'approvisionnement visant les communautés de jeux en ligne.

Compte tenu de la difficulté de détecter et d'empêcher les attaques de la chaîne d'approvisionnement, et de ce que les acteurs malveillants et les cybercriminels ont à y gagner, le nombre de ces attaques ne devrait qu'augmenter dans un avenir proche, tant en Europe que dans le monde entier.

Pour cette raison, gardez à l'esprit les recommandations suivantes pour réduire les risques découlant de chaînes d'approvisionnement logicielles vulnérables :

- Maîtrisez vos logiciels : répertoriez tous les outils open source et propriétaires utilisés dans votre entreprise.
- Restez à l'affût des vulnérabilités connues et appliquez les correctifs dès qu'ils sont disponibles. Même les attaques impliquant des mises à jour infectées ne devraient en aucun cas décourager quiconque de mettre à jour ses logiciels.

- Restez attentif aux failles de sécurité touchant les éditeurs de logiciels tiers.
- Cessez d'utiliser des systèmes, services et protocoles redondants ou obsolètes.
- Évaluez les risques de vos fournisseurs en déterminants leurs processus de sécurité.
- Définissez des exigences de sécurité pour vos fournisseurs de logiciels.
- Demandez des audits réguliers du code et renseignez-vous sur les contrôles de sécurité et les procédures de contrôle des modifications des composants.
- Renseignez-vous sur les tests de pénétration pour identifier les risques potentiels.
- Demandez des contrôles d'accès et une authentification à deux facteurs (2FA) pour protéger les processus et les pipelines de développement de logiciels.
- Utilisez un logiciel de sécurité avec plusieurs couches de protection.

3

SÉCURITÉ INFORMATIQUE ET GOUVERNEMENT : PARALLÈLE AVEC LES ENTREPRISES

Être le RSSI d'une entreprise de cybersécurité, c'est être dans une position unique. Et bien qu'il y ait un avantage inhérent à travailler avec un conseil d'administration qui comprend intrinsèquement les aspects techniques de la sécurité, les entreprises de cybersécurité ne sont pas moins une cible (voire un trophée) pour les cybercriminels. Ce deuxième point, le fait de savoir que nous sommes une cible, est celui où, selon moi, notre expérience se recoupe le plus avec celle des organismes gouvernementaux. Cette notion était une constante au cours de mes 10 années en tant que RSSI chez ESET, et le moteur principal de l'évolution de notre posture de sécurité pour répondre aux besoins de l'environnement en ligne évoluant constamment.

Daniel Chromek
CISO/Section Lead

La réalité de notre statut de cible a également une forte incidence sur la culture de sécurité, la croissance et le modèle commercial de notre entreprise. Les gouvernements sont confrontés à un défi similaire. Ce sont des cibles claires, leurs adversaires ne seront pas facilement éliminés, et l'atténuation des pires symptômes des tactiques et des techniques utilisées dans le paysage des menaces dicte tout, de la politique de sécurité à l'allocation des ressources en passant par la culture et la croissance stratégique.

Les questions sur la façon d'évoluer peuvent avoir une réponse à la fois du point de vue d'ESET et de celui du reste du secteur de la sécurité de l'information. Comme je connais mieux ESET, il est beaucoup plus facile d'aborder le « comment » de ce point de vue. ESET est une entreprise dont l'activité a connu une croissance assez spectaculaire au cours de mon mandat. Nous sommes une communauté soudée dans laquelle de nombreuses activités nécessitent une normalisation et un cadre de gouvernance approprié, afin de rationaliser les processus internes, la communication et l'échange d'informations.

En particulier, la normalisation et la gouvernance chez ESET nous ont aidés à passer de la protection des consommateurs et des PME à une croissance significative dans le segment des grandes entreprises. C'est cette quête qui nous a amené à documenter la sécurité de l'information, à nous conformer à des directives et des règlements distincts, et améliorer nos capacités à répondre aux questions et aux réserves des entreprises clientes lors de la mise en œuvre de solutions de sécurité dans leurs environnements. De manière catégorique, tous les gouvernements sont confrontés à la demande rapide de numérisation de leurs services, d'amélioration des processus internes, et de formalisation des deux par une meilleure gouvernance. Comme dans le cas de l'expérience d'ESET, la formalisation des processus (et de la culture) par la gouvernance reflète la maturité et l'ambition d'atteindre de nouveaux marchés. Dans le cas des gouvernements, il s'agit d'améliorer la croissance, la prestation de services, et la cohésion nationale ou locale.

Implications de la maturation

Bien entendu, les défis liés à la gouvernance ont été relevés bien avant que nous n'atteignions notre niveau de maturité actuel, et avec la croissance de l'entreprise, ils n'ont fait que se complexifier. Ainsi, le déploiement de contrôles de sécurité dans un environnement informatique complexe exige plus de temps et de ressources qu'auparavant. Par conséquent, notre département de sécurité interne s'est considérablement développé et se compose désormais de plusieurs équipes qui se concentrent sur différents aspects de la sécurité.

Il va sans dire que la division de la sécurité interne doit être très bien préparée, car les présentations auprès de la direction peuvent rapidement se transformer en exposés techniques. La dernière fois que nous avons effectué ce type d'exposé, cela concernait le paramètre de score de risque de notre outil de gestion des vulnérabilités et sa formule de calcul, afin que la direction puisse déterminer s'il était approprié de le communiquer. Un débat a notamment eu lieu sur la manière dont la présence d'une exploitation de vulnérabilité dans les kits de malwares peut augmenter le score de risque au-delà des scores CVSS traditionnels. Que ce soit il y a 12 ans lorsque j'ai rejoint les co-fondateurs pour discuter de nos politiques de sécurité ou aujourd'hui, étudier les choses en profondeur reste un phénomène culturel profondément ancré chez ESET.

Bien sûr, même avant que j'assume le rôle de RSSI, nous avions de nombreux collaborateurs très compétents et nous devions trouver un équilibre entre la sécurité et la visibilité, et les craintes de nos collègues d'une surveillance trop omniprésente. Les propriétaires d'ESET étaient conscients du respect de la confidentialité et le restent. Nous avons également compris très tôt l'impact possible sur le moral du personnel. Nous avons donc convenu de configurer la culture d'ESET dès le début comme celle d'une entreprise de sécurité positive, en persuadant tout le monde, y compris la direction, que l'utilisation de tactiques de peur, d'incertitude et de doute ne fonctionne tout simplement pas, et pourrait entraîner la perte du respect des collègues dans toute l'entreprise.

Je soulève cette question parce que nous sommes tous, vous et moi y compris, confrontés à un choix similaire : équilibrer la sécurité et la visibilité avec une autre composante, la confiance. Ce besoin est devenu douloureusement clair en 2020, *l'année qui nous a donné COVID-19* et qui a transporté ESET, et probablement nous tous, vers un avenir de sécurité auquel peu d'entre nous s'attendait. Pour réussir dans le domaine de la sécurité à l'ère covidienne, quelques principes de base doivent être appliqués correctement. Ceux-ci vont au-delà de la confiance et incluent les aspects pratiques de la sécurité que les RSSI doivent garder à l'esprit en 2021. Voici les miens :

1. Adhérez aux principes de base en mode télétravail

« Revenir aux fondamentaux » est toujours un bon conseil en matière de sécurité informatique. Cela s'appliquera également à 2021, lorsque nous passerons, espérons-le, à un monde post-COVID. Les correctifs, les sauvegardes et la protection des postes de travail sont des domaines importants quel que soit l'endroit où les collaborateurs travaillent, que ce soit au bureau ou à domicile. L'expansion et la gestion des comptes VPN du personnel pour un accès plus sécurisé aux plateformes d'une entreprise, ainsi que de nombreuses autres précautions, sont là pour rester. Il peut être utile d'envisager une approche de la sécurité fondée sur le principe Zero Trust ou sur le principe de « faire confiance mais de vérifier » pour aborder les spécificités du télétravail. Gardez-les à l'esprit et cherchez à les optimiser.

2. Développez-vous dans les domaines réglementés

Bien que je ne puisse parler que pour ESET, nous constatons une croissance accélérée des réglementations liées à la sécurité dans le monde entier. Cette tendance devrait s'accentuer de manière exponentielle avec la numérisation déjà rapide, accélérée encore plus par la pandémie de COVID-19. Par exemple, la directive NIS (et la *directive NIS2*) a un impact à la fois sur ESET en tant que fournisseur de cybersécurité et sur de nombreux clients d'ESET, en particulier ceux des secteurs réglementés ou ceux qui fournissent des services directs au gouvernement. Il est donc logique que nous nous engagions ensemble pour créer des approches communes.

Pas plus tard que l'année dernière, au milieu des confinements répétés, ESET et ses produits ont atteint un nouveau degré de conformité réglementaire avec le lancement de nos services ESET PROTECT Cloud. Cela a entraîné des complexités supplémentaires, ESET devant à nouveau se conformer à la directive NIS, et les partenaires d'ESET devant se conformer aux législations locales réglementant l'utilisation de logiciels de sécurité dans le Cloud. Ainsi, même s'il n'est pas très agréable de devoir se conformer à une réglementation unique telle que la directive NIS, c'est une tâche plus simple que de devoir se conformer à de multiples réglementations et normes exigées par les gouvernements, l'industrie et les entreprises clientes.

Pour relever ces défis, une bonne approche consiste à mettre en place un système de gestion de la sécurité de l'information (par exemple, ISO 27001) pour gérer vos processus fondamentaux de sécurité de l'information, puis d'ajouter systématiquement le reste des contrôles de sécurité dont vous avez besoin pour assurer la conformité de votre entreprise. La norme ISO 27001, ainsi que le modèle BSIMM (Build Security In Maturity Model), peuvent aider les entreprises à développer et documenter correctement leur système de gestion de la sécurité et leurs contrôles internes, ce qui est indispensable pour prouver la conformité.

3. Équilibrez les ressources pour prendre en charge différentes initiatives métiers tout en préservant la santé mentale de vos équipes

Je pense que notre secteur se débat avec ce point. Il est probable que le principal problème auquel est confronté tout programme de sécurité mature est sa relation avec de nombreuses activités au sein de l'entreprise. Il est tout simplement difficile d'accorder la priorité aux activités réellement importantes. Les rapports et les mesures ajoutent un autre niveau de complexité. Nous devons suivre les risques, les résultats d'audit et les incidents, recueillir les réactions et les enseignements tirés, identifier les écarts de conformité, etc., même si nous avons parfois l'impression que l'on nous demande de comparer ce qui est incomparable. Les organismes gouvernementaux sont certainement confrontés aux mêmes défis. Ils s'efforcent de trouver un équilibre entre la sécurité des mécanismes internes et les services externes, le tout devant être à la fois conforme et devant fonctionner de manière pratique.

Mais il existe au moins deux façons d'atteindre l'équilibre. La première est la priorité métier. Si les entreprises peuvent identifier leurs priorités, il est alors facile de leur affecter des ressources internes de sécurité. Si, toutefois, les entreprises ne parviennent pas à identifier leurs priorités (que ce soit globalement ou par rapport aux priorités des autres unités commerciales), la clé pour trouver une solution semble être de poser les questions suivantes : Quel est le risque ? Quel est le risque si notre équipe de sécurité ne parvient pas à consacrer des ressources pour prendre en charge l'initiative métier ? Quel est le risque que les constatations d'un audit ne puisse être résolue ? Quel est le risque de… remplissez la suite vous-même ! Le risque peut être utilisé comme une mesure unique pour déterminer la priorité des activités concurrentes.

4. Améliorez la maturité de votre cycle de vie de développement logiciel

Dans le monde de l'entreprise, il est assez courant d'avoir des équipes de développement internes et externes qui développent, personnalisent et maintiennent des systèmes, des produits ou des services essentiels. La perspective d'appliquer un modèle en cascade est un problème qui peut donc se poser en raison de l'utilisation

de plusieurs normes de sécurité dans le cycle de vie du développement logiciel. Cependant, avec le développement et le déploiement agiles rapides devenant une nécessité courante dans le secteur, il n'est tout simplement plus viable d'appliquer une approche en cascade aux activités de DevOps.

L'approche d'ESET consiste à définir les activités de sécurité pour les DevOps, liées à la fois au développement et aux opérations, et engager une discussion patiente avec les équipes de développement sur la manière d'inclure ces activités dans leurs méthodologies et processus de travail. L'objectif : identifier ce qui doit être fourni par les experts internes en sécurité, par opposition aux champions de la sécurité des différentes équipes de développement, et comment automatiser autant que possible.

5. Préparez-vous à faire face à la complexité croissante des attaques

Les *rapports de Verizon sur les fuites de données* de ces dernières années suggèrent clairement que le paysage des menaces s'aggrave. Nous ne savons pas quels types de vulnérabilités seront exploités à l'avenir, quels types d'outils les agresseurs utiliseront, ni quels sont leurs objectifs. Mais ce que nous pouvons faire, c'est nous y préparer : à la fois sur le plan technique par des contrôles multicouches, et sur le plan organisationnel par les moyens, les compétences et la maturité globale des équipes de traitement des incidents.

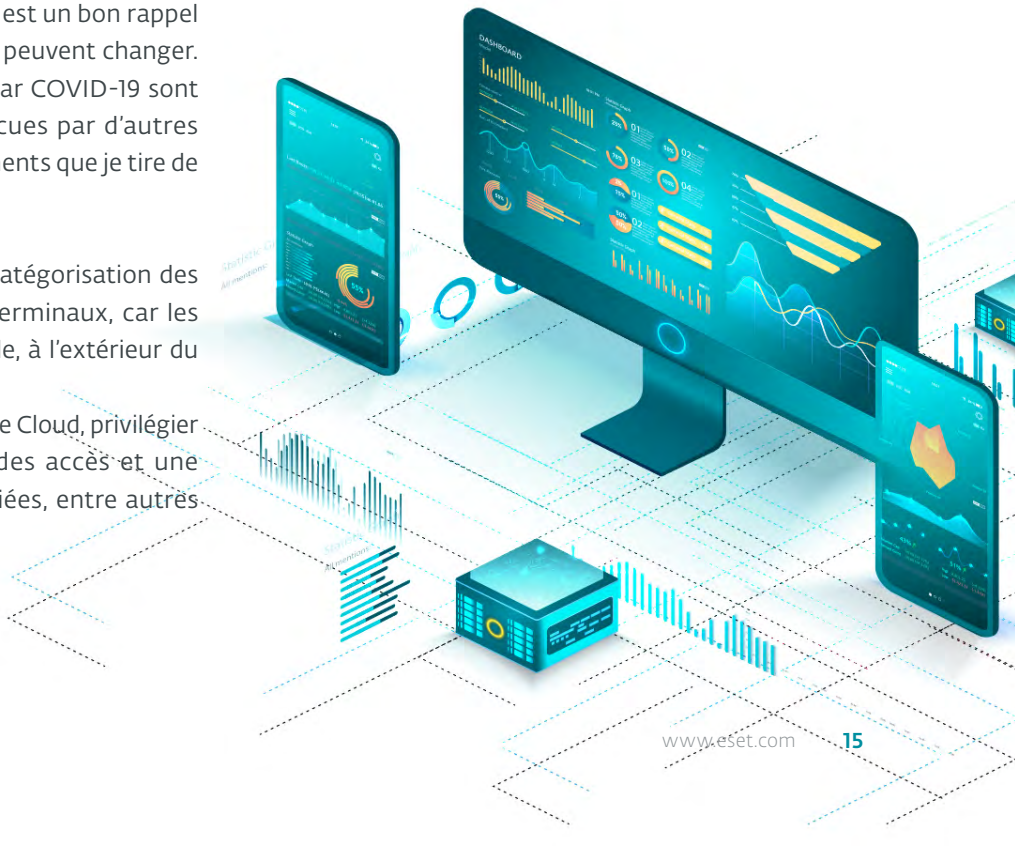
La situation provoquée par COVID-19 est un bon rappel de la rapidité avec laquelle les choses peuvent changer. Les accélérations apportées à ESET par COVID-19 sont probablement similaires à celles vécues par d'autres entreprises. Les principaux enseignements que je tire de cette expérience sont les suivants :

- Mettre davantage l'accent sur la catégorisation des ressources et la visibilité sur les terminaux, car les collaborateurs travaillent à domicile, à l'extérieur du réseau sur site de l'entreprise.
- En cas d'utilisation de services dans le Cloud, privilégier une configuration, une gestion des accès et une allocation des ressources appropriées, entre autres mesures de sécurité du Cloud.

D'après notre propre expérience, nous avons constaté une nette augmentation des attaques, en particulier des attaques dites d'usurpation de messagerie professionnelle (BEC), qui exigent plus d'attention que d'habitude. Nous avons de la chance, car notre portefeuille de solutions comprend un moteur antimalwares robuste, une solution de sandboxing dans le Cloud, *ESET Dynamic Threat Defense*, contre les menaces émergentes, et une solution de détection et de traitement des incidents, *ESET Enterprise Inspector*, qui améliore la visibilité sur les terminaux et renforce nos moyens de traitement des incidents. Nous disposons également d'une solution facile à utiliser de prévention des fuites de données grâce à notre alliance technologique avec Safetica.

Ciblés mais diligent

Oui, nous restons ciblés, mais le fait de disposer d'une base solide, comprenant les éléments mentionnés ci-dessus et une attention particulière à la gouvernance, nous permet de nous concentrer sur des problèmes spécifiques tels que les preuves, ainsi que la collecte et l'intégration de ces résultats dans nos propres produits. C'est là que notre expertise en matière de recherche sur les malwares recoupe le plus clairement le développement de produits. En utilisant ESET Enterprise Inspector en combinaison avec nos technologies de détection, nous pouvons simultanément protéger l'entreprise et faire évoluer constamment nos systèmes, notre culture et nos processus, pour relever les défis du moment.



4

EMISSARYSOLDIER : ACTIVITÉS MALVEILLANTES DU GROUPE LUCKYMOUSE EN 2020

LuckyMouse a compromis des entreprises privées (télécoms, médias et banques) et des réseaux gouvernementaux en Asie centrale et au Moyen-Orient

Matthieu Faou
Malware Researcher

LuckyMouse, également connu sous le nom d'APT27 et d'Emissary Panda, est un groupe de cyberespionnage qui est surtout connu pour son utilisation régulière d'attaques dites de « point d'eau », ou de compromis stratégique du web. Le groupe a infecté non seulement de multiples réseaux gouvernementaux en Asie centrale et au Moyen-Orient, mais également des organisations transnationales telles que l'Organisation de l'aviation civile internationale (OACI).

Dans sa dernière analyse de LuckyMouse, ESET Research a découvert un ensemble d'activités malveillantes qui ont eu lieu en 2020 et dans lesquelles les opérateurs ont principalement utilisé la boîte à outils SysUpdate (alias Soldier). ESET a nommé cet ensemble d'activités EmissarySoldier.

Pour compromettre ses victimes, LuckyMouse utilise généralement des points d'eau, c'est-à-dire des sites web susceptibles d'être consultés par les cibles. Les opérateurs de LuckyMouse analysent également les réseaux de leurs victimes afin de découvrir des serveurs vulnérables connectés à Internet. Bien que le groupe exploite généralement des vulnérabilités déjà connues pour compromettre des serveurs non corrigés, LuckyMouse fait partie des groupes susceptibles d'exploiter les vulnérabilités zero-day de Microsoft Exchange attaquer des serveurs de messagerie.

Une fois que les opérateurs de LuckyMouse ont pris pied sur une machine, ils déploient l'un de leurs modules personnalisés, SysUpdate ou HyperBro. Ces boîtes à outils ont en commun d'utiliser le détournement de l'ordre de recherche des DLL pour déjouer les détections.

LuckyMouse opère une infrastructure réseau assez importante avec des nœuds VPN, des nœuds de transit et des nœuds de commande et de contrôle (C&C). Au cours de la campagne EmissarySoldier, ESET a observé 16 nœuds de relais et de C&C différents.

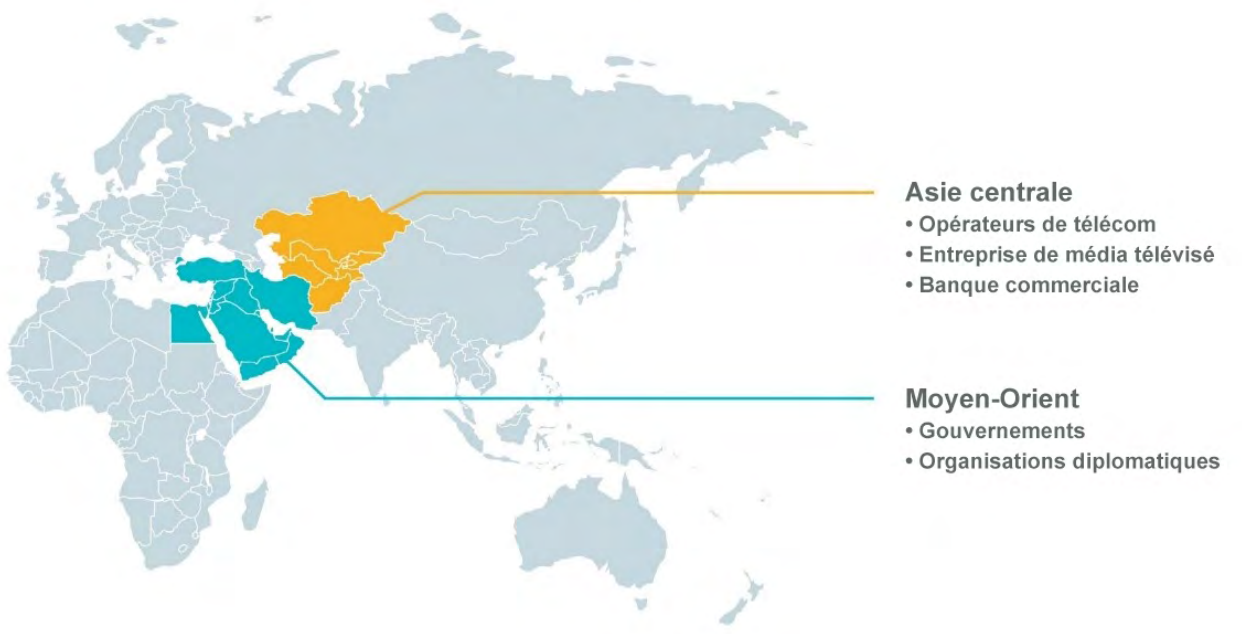
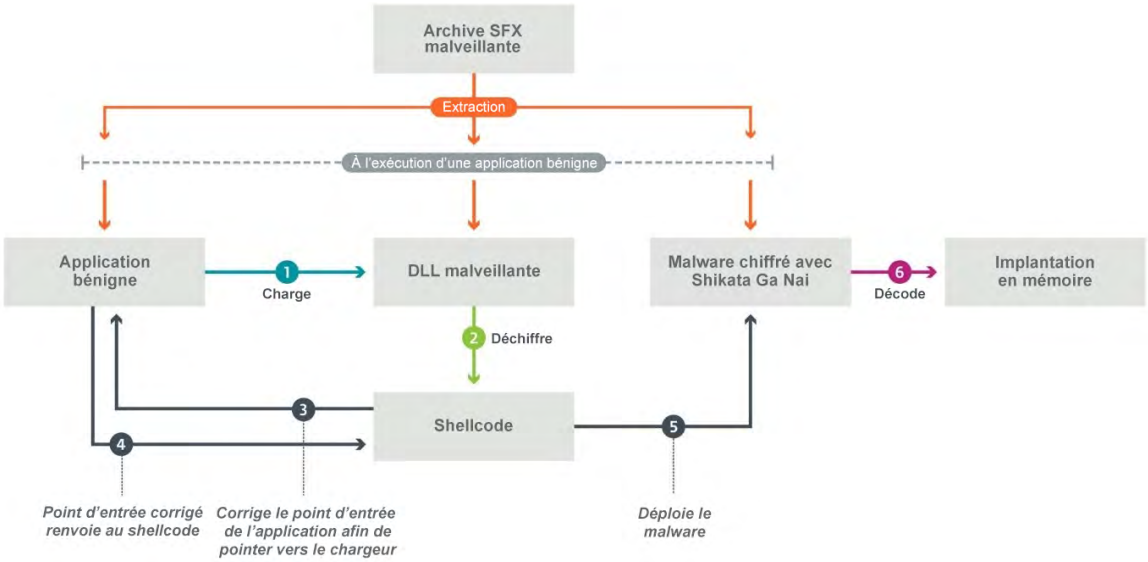


image : Selon la télémétrie d'ESET, LuckyMouse a ciblé les entités suivantes en 2020

Le Moyen-Orient est actuellement un foyer pour de nombreux groupes d'espionnage, et LuckyMouse y a également été très actif. Il est très courant de trouver plusieurs acteurs de menaces sur la même machine ou du moins dans le même réseau. LuckyMouse se concentre principalement sur des entités gouvernementales dans cette région. Les opérateurs essaient probablement d'obtenir des informations sur la situation géopolitique actuelle. Au contraire, la plupart de leurs cibles en Asie centrale sont des entreprises privées (télécom, médias et banques). Cela montre un intérêt stratégique pour la situation économique de la région.

Les chercheurs d'ESET ont également remarqué que certaines des machines compromises hébergeaient Microsoft SharePoint, accessible depuis Internet. En 2019 et 2020, plusieurs vulnérabilités d'exécution de code à distance ont été découvertes dans cette application. Bien qu'ESET n'ait pas la preuve que ces vulnérabilités aient été exploitées, nous avons observé que les composants de LuckyMouse étaient déployés via l'instance des services d'information Internet (IIS) également utilisée par Microsoft SharePoint.

LuckyMouse installe ses modules de manière spécifique, en utilisant un modèle dit « en trident », dans sa boîte à outils SysUpdate. Le modèle en trident comprend une application légitime vulnérable au détournement de DLL, une DLL personnalisée qui charge le malware et un malware en binaire brut chiffré avec Shikata Ga Nai.



Vue d'ensemble du modèle en trident

Comme de nombreux acteurs de menaces motivés par le gain financier, mais également par l'espionnage, LuckyMouse utilise des outils de sécurité offensifs. Même si le groupe utilise principalement des portes dérobées personnalisées, les chercheurs d'ESET ont noté plusieurs autres outils dans certaines intrusions, notamment :

- JuicyPotato, un outil d'escalade de privilèges
- Mimikatz, un outil permettant d'extraire différents secrets de Windows, notamment des mots de passe
- nbtscan, un analyseur NetBIOS

La boîte à outils SysUpdate elle-même, qui était au centre de cette dernière analyse approfondie de l'activité de LuckyMouse, est relativement récente, les premiers échantillons ayant été découverts en 2018. Depuis lors, elle a évolué par étapes successives. Contrairement aux échantillons précédents, ceux utilisés en 2020 présentaient des améliorations majeures et de nouvelles fonctionnalités, notamment la mise en œuvre de plusieurs protocoles de communication de C&C et un remaniement mineur des fonctionnalités déjà implémentées.

Les composants de SysUpdate sont divisés en plusieurs binaires, chacun ayant un objectif opérationnel spécifique. En particulier, les composants du modèle en trident de SysUpdate consistent en une application inoffensive telle que GUP.exe, qui agit comme chargeur initial pour le composant suivant, une DLL, qui à son tour agit comme chargeur pour le composant suivant, le malware de la première étape. Ces trois composants sont installés dans un endroit arbitraire lors de l'accès initial à un système compromis. C'est un schéma qui semble être récurrent dans les activités touchant différentes victimes de différentes régions.

Comme la boîte à outils SysUpdate est hautement modulaire, elle offre à ses opérateurs la possibilité de fournir des fonctionnalités malveillantes à la demande, ainsi que de les retirer à volonté pour limiter leur exposition. C'est précisément pour cette raison que les chercheurs d'ESET n'ont pas pu accéder aux modules malveillants, et ils s'attendent à ce que ce soit un défi récurrent dans l'analyse des campagnes futures utilisant SysUpdate. La meilleure façon de traquer un tel groupe évasif consiste à déployer une solution de détection et de traitement des incidents (EDR) capable d'identifier les événements suspects qui se produisent sur un réseau. LuckyMouse a été de plus en plus actif tout au long de l'année 2020, semblant intégrer progressivement différentes fonctionnalités à la panoplie d'outils de SysUpdate. Cela peut être un indicateur que les opérateurs de LuckyMouse passent progressivement de l'utilisation de HyperBro à SysUpdate.

HyperBro est une boîte à outils beaucoup plus ancienne qui a attiré beaucoup plus d'attention de la part de la communauté de la sécurité au cours des dernières années, et de nombreux éléments indiquent qu'elle a également été adoptée par plusieurs groupes de pirates. À l'opposé, SysUpdate a été peu signalée, très probablement parce qu'elle n'a été déployée que dans un nombre relativement limité de campagnes.

La surveillance de LuckyMouse et des outils utilisés dans ses récentes campagnes reste une priorité. Les chercheurs d'ESET ont fait ce constat lorsqu'ils terminaient leur enquête, au moment même où le groupe exploitait des ***vulnérabilités dans Microsoft Exchange*** pour attaquer des serveurs de messagerie et installer la boîte à outils SysUpdate. Ce point d'intersection constitue un argument de poids pour que les gouvernements et les entreprises renforcent la sécurité des serveurs connectés à Internet, collaborent davantage sur la stratégie de sécurité, renforcent leurs moyens et leur maturité dans l'utilisation des outils d'EDR.

5

HORIZON RÉGLEMENTAIRE : REPÈRES CRITIQUES POUR UNE POSTURE CYBERSÉCURITÉ DANS L'UNION EUROPÉENNE ET AUX ETATS-UNIS

La dépendance de la société à l'égard de la technologie et l'émergence de ceux qui cherchent à en faire mauvais usage ont conduit les gouvernements du monde entier à tenter de plus en plus de réglementer le cyberespace. Ce faisant, les gouvernements s'efforcent de dissuader les acteurs malveillants, que ce soient des organisations criminelles ou qu'ils soient sponsorisés par des États, par des poursuites et des sanctions, de protéger les infrastructures nationales essentielles, les informations personnelles et les ressources de sécurité et de défense, et de renforcer la résilience de la société en veillant à ce que les organismes publics, les entreprises et les autres organisations reconnaissent leurs responsabilités et soient tenus pour responsables. Parallèlement, les gouvernements s'efforcent d'informer les citoyens de l'ampleur des risques liés à la cybersécurité et des mesures d'atténuation nécessaires.

Andy Garth
Government Affairs Lead

Au niveau supranational, les Nations unies tentent d'obtenir un accord sur l'application du droit international à l'activité des États, et de s'appuyer sur 11 normes de comportement responsable dans le cyberespace convenues en 2015. Le RGPD de l'Union européenne est rapidement devenu une référence pour les pays qui cherchent à renforcer la réglementation en matière de confidentialité et de sécurité. L'Union européenne et les États-Unis (sous la nouvelle administration Biden) devraient donner le ton pour une réglementation accrue du cyberespace dans les années à venir.

En l'absence d'une norme ou d'un accord mondial, le paysage réglementaire est plutôt fragmenté. À l'heure actuelle, la réglementation est principalement appliquée au niveau des États et des secteurs. Ce fait, combiné au rythme de l'innovation et aux complexités de la

législation, a laissé la plupart des gouvernements face à des défis de sécurité concrets que beaucoup d'entre eux ont des difficultés à relever.

Compte tenu de l'étendue du cyberespace et des différences entre les approches nationales, les responsables des systèmes d'information et les décideurs devraient garder un œil sur les domaines suivants afin d'identifier les indices essentiels pour une conformité et une posture de sécurité futures.

Union européenne : directive NIS2

En décembre 2020, l'UE a publié le texte préliminaire de la directive NIS2, qui élargit considérablement le nombre d'entités et de secteurs tenus de prendre des mesures renforcées pour améliorer la cybersécurité. Le texte est actuellement au stade de l'examen législatif.

Une fois le texte final adopté, les États membres disposeront de 18 mois pour mettre en œuvre la directive. Les répercussions se feront sentir dans l'UE et au-delà.

La directive NIS2 proposée va :

- Introduire des mesures de surveillance plus strictes.
- Imposer des exigences plus strictes en matière d'application, notamment des régimes de sanctions harmonisés entre les États membres.
- Instaurer un partage d'informations et une coopération en matière de gestion des cybercrises aux niveaux national et européen.
- Mandater la création de stratégies nationales qui garantissent la résilience des entités critiques.
- Obliger la réalisation d'évaluations des risques au niveau national.
- Viser à renforcer la sécurité des chaînes d'approvisionnement.

Une fois adoptée, la directive NIS2 s'appliquera en parallèle des législations sectorielles, telle que la « directive sur la résilience des entités critiques » proposée. Cette directive sectorielle vise à protéger les infrastructures critiques et complétera la directive NIS2 dans la mesure où elle imposera probablement des obligations de gestion des risques de cybersécurité et de notification, d'un effet au moins équivalent à celui des obligations énoncées dans la directive NIS2.

Union européenne : Certification de cybersécurité

La loi de 2019 sur la cybersécurité de l'UE, désormais en vigueur, a accordé un mandat permanent à l'Agence de l'UE pour la cybersécurité (ENISA), avec pour nouveau rôle clé de mettre en place et maintenir un cadre de certification de la cybersécurité. Ce cadre fournira des schémas de certification à l'échelle de l'UE avec un ensemble complet de règles, d'exigences techniques, de normes et de procédures, fournissant aux utilisateurs une assurance basée sur le niveau de conformité aux exigences convenues.

Ces schémas de certification représentent des accords au niveau de l'UE sur l'évaluation des propriétés de sécurité des produits ou services des technologies de l'information et des communications (TIC). En bref, ceux-ci attesteront des produits et des services de TIC en termes de :

- Catégories de produits et de services couverts
- D'exigences en matière de cybersécurité
- De type d'évaluation
- De niveau d'assurance souhaité

L'ENISA et la Commission européenne seront assistées et conseillées par :

- Le Groupe européen de certification en matière de cybersécurité (ECCG)
- Le Groupe de certification des parties prenantes en matière de cybersécurité (SCCG)
- Le Centre de compétence européen en matière de cybersécurité, de technologie et de recherche industrielle (ECCC).

En particulier, l'ECCC devrait devenir le principal instrument d'investissement dans la recherche, la haute technologie et l'innovation en matière de cybersécurité. Cette mission globale alimentera les objectifs suivants :

1. Effectuer les achats de produits et de solutions.
2. Fournir un soutien financier et une assistance technique aux jeunes entreprises et aux PME.
3. Soutenir la recherche et l'innovation grâce à un programme de recherche complet.
4. Créer des normes élevées en matière de cybersécurité, notamment dans le domaine du développement des compétences.
5. Faciliter la coopération entre les sphères civile et de la défense en matière de technologies mixtes (en relation avec le Fonds européen de défense).

Tony Anscombe
Chief Security Evangelist

Réglementation américaine en matière de protection de la confidentialité et évolution des lois sur la cybersécurité

Après la promulgation du RGPD par l'UE en 2018, la mise en œuvre de la réglementation sur la confidentialité des données a également commencé à s'accélérer au niveau des gouvernements des États américains. Les législateurs californiens ont adopté la loi californienne sur la protection de la confidentialité des consommateurs (CCPA) en 2018 et l'ont mise en œuvre en 2020. Fin 2020, la proposition 24 de la Californie a été adoptée, ce qui signifie que la loi californienne sur les droits à la confidentialité (CPRA) entrera en vigueur en 2023. La CPRA apporte des ajouts importants à la CCPA, qui elle-même pourrait être considérée comme étant en deçà du RGPD dans certains domaines, bien qu'elle aille plus loin dans d'autres domaines. Cas ajouts comprennent :

- Le concept de données du ménage en plus des données purement individuelles, comme le souligne le RGPD
- L'extension de la protection des résidents californiens même lorsqu'ils se trouvent hors de l'État, temporairement ou en transit
- Le droit de s'opposer à la vente de données personnelles à des tiers Les entreprises doivent inclure un lien « Ne pas vendre mes informations personnelles » sur les pages d'accueil des sites web. Si des protections similaires existent dans le cadre du RGPD, elles sont moins claires : la personne concernée doit refuser les objectifs marketing et retirer son consentement pour les activités de traitement.

Avec un large consensus sur la nécessité d'une législation fédérale sur la protection de la confidentialité des consommateurs, concrétisé par la loi sur le droit à la confidentialité des consommateurs en ligne (COPRA) en avril 2020, et la reconnaissance apparente par l'administration Biden de la nécessité d'une législation fédérale sur la protection de la confidentialité, nous verrons probablement à une multitude d'initiatives. En effet, la vice-présidente Kamala Harris a de solides antécédents en matière de respect de la confidentialité, comme en témoigne la modification et le renforcement de la loi californienne sur la protection de la confidentialité en ligne (CalOPPA) lorsque Mme Harris était procureure générale de l'État de Californie. Plusieurs membres du gouvernement de l'ère Obama qui ont contribué au projet de loi sur la consommation sont également de retour aux commandes.

Au fur et à mesure que la pandémie se poursuit, les prestataires de soins de santé et les organismes qui ont participé aux campagnes de suivi des contacts, de dépistage et de vaccination, feront l'objet d'une attention particulière. À l'heure actuelle, certains processus de collecte de données à caractère personnel peuvent ne pas faire l'objet d'un examen aussi minutieux en raison de l'urgence et de la nécessité médicale. Il faut toutefois s'attendre à ce que cette latitude soit supprimée et à ce que les exigences en matière de cybersécurité pour ces données soient renforcées et appliquées.

Cela est également vrai au niveau mondial, où l'Internet crée un environnement qui supprime les barrières internationales, étant donné que tout est accessible dans le même Cloud. La législation sur la protection de la confidentialité n'est pas un processus arrêté ; c'est un processus évolutif qui nécessitera probablement des modifications permanentes, surtout si l'on tient compte des nouvelles technologies telles que l'intelligence artificielle, l'Internet des objets et d'autres avancées technologiques. La nécessité de normaliser et d'harmoniser s'est fait sentir au sein des États, et entre pays et continents à travers le monde. Tous les consommateurs devraient bénéficier des mêmes droits en matière de confidentialité des données de la part des entreprises et des organisations, quelle que soit leur localisation. La législation sur la protection de la confidentialité est sans aucun doute un sujet qui restera une priorité pour les législateurs.

Lois sur la cybersécurité aux États-Unis

S'il existe des lois globales sur la cybersécurité aux États-Unis, la législation dépend généralement du secteur d'activité d'une entreprise ou d'une organisation, bien que certaines lois visant des technologies spécifiques peuvent s'appliquer à plusieurs secteurs.

Parmi les principales législations américaines relatives à la cybersécurité, qui s'appliquent à des secteurs :

- Loi sur la portabilité et la responsabilité pour l'assurance maladie (HIPPA)
- Loi Gramm-Leach-Bliley
- Loi Dodd-Frank
- Loi sur l'amélioration de la cybersécurité de l'IdO
- Loi de 2017 sur la protection de la confidentialité des consommateurs, qui oblige les entreprises à sécuriser les informations personnelles et fournir des notifications sur les fuites de données.
- Loi sur le partage des informations de cybersécurité (CISA), qui permet le partage du trafic Internet entre le gouvernement et les entreprises technologiques pour des raisons de cybersécurité.
- Loi fédérale sur la gestion de la sécurité de l'information (FISMA), qui oblige les agences gouvernementales à se doter de politiques, de normes et de directives en matière de sécurité de l'information.

La loi HIPPA est un exemple de législation appliquée à un secteur, qui exige des organismes de soins de santé qu'ils protègent les informations personnelles identifiables contre la fraude et le vol, et qu'ils prennent en compte les limitations de la couverture d'assurance maladie. Dans le secteur financier, les organisations sont tenues de se conformer à la loi Gramm-Leach-Bliley et à la loi Dodd-Frank, qui stipulent qu'une politique doit être mise en place pour protéger les informations contre les menaces de sécurité et les problèmes d'intégrité des données.

En fait, en vertu de la loi Dodd-Frank, le Consumer Financial Protection Bureau a le pouvoir de socialiser de nouvelles règles potentielles. En conséquence, à l'automne 2020, le bureau a publié une notification avancée de proposition de législation qui entraînera probablement des modifications dans un avenir proche des méthodes d'accès aux données autorisées par les consommateurs et du niveau de sécurité des données requis par la loi.

Objets connectés

Enfin, la loi de 2020 sur l'amélioration de la cybersécurité de l'IdO, qui s'applique à tous les secteurs, exige que l'Institut national des normes et de la technologie (NIST) publie des normes et des directives à l'intention des agences fédérales sur l'utilisation appropriée des objets connectés dans les systèmes gouvernementaux.

Ce texte de loi sur l'IdO comporte un calendrier échelonné qui oblige les agences à :

- Se mettre d'accord sur la manière de traiter et de signaler les vulnérabilités des appareils utilisés
- Fixer des exigences minimales en matière de sécurité de l'information pour gérer les risques de cybersécurité
- Examiner et réviser les directives et les normes tous les cinq ans

Le volet final prendra effet en décembre 2022 et interdira l'utilisation d'objets connectés qui ne sont pas conformes aux normes et directives du NIST.

6

ENDPOINT DETECTION AND RESPONSE (EDR) : UNE CONTRE-MESURE FACE AUX MENACES PERSISTANTES

Les grandes entreprises et les institutions gouvernementales, telles que les ministères des affaires étrangères, les ambassades et autres représentants diplomatiques, sont des cibles de choix pour les campagnes d'espionnage. Les pirates ciblent ces institutions de différentes manières pour voler des informations sensibles. La furtivité est un élément essentiel de ces campagnes malveillantes, car rester invisible et éviter d'être détecté dans un réseau cible aussi longtemps que possible est essentiel pour réussir.

La technologie de détection et de traitement des incidents (EDR) peut aider les grandes entreprises à détecter les pirates furtifs en signalant les comportements suspects, en particulier lorsqu'ils utilisent des malwares ou des outils légitimes totalement indétectables. Les solutions d'EDR peuvent générer des alertes lors de l'exécution d'applications peu courantes ou d'outils légitimes connus pour être détournés par les pirates, par exemple des modules du système d'exploitation, ce qui permet aux défenseurs d'enquêter sur les activités suspectes qui se produisent dans leurs réseaux.

Invisimole, un groupe de pirates surveillé par les chercheurs d'ESET depuis quelques années, porte bien son nom, puisqu'il cible des organisations de premier plan à des fins d'espionnage, et déploie différentes stratégies afin d'être difficile à détecter.

Une fois que les opérateurs d'Invisimole ont pris pied dans une organisation, ils mettent généralement en place différentes chaînes de persistance pour garantir un accès en continu. Bien qu'il existe différentes chaînes, elles ont cependant un point commun : Aucun code malveillant n'est présent sur les disques des victimes.

Les opérateurs d'Invisimole détournent des outils légitimes pour charger et déchiffrer en mémoire des outils malveillants utilisés pour leurs activités d'espionnage. L'utilisation de ces outils légitimes rend difficile la détection des anomalies par les technologies standard. Dans ces cas, où la discrétion est le but ultime, les défenseurs qui s'appuient sur une solution EDR correctement configurée peuvent détecter ces activités malveillantes et atténuer correctement les attaques.

7

POINT DE VUE ESET : DÉTECTION ET TRAITEMENT DES INCIDENTS (EDR)

QU'EST-CE QUE LA DÉTECTION ET LE TRAITEMENT DES INCIDENTS ?

Les solutions de détection et de traitement des incidents (EDR) collectent et analysent de grandes quantités de données générées par l'activité des postes de travail. Les comportements suspects déclenchent une alarme qui alerte les professionnels de la sécurité pour qu'ils approfondissent leur enquête et découvrent éventuellement des attaques qui seraient autrement passées inaperçues. ESET a développé ESET Enterprise Inspector (EEI) comme solution d'EDR capable de protéger les terminaux Windows et macOS.

MITRE ATTACK®

ESET Enterprise Inspector s'appuie sur la base de connaissances des tactiques, techniques et procédures adverses de MITRE ATT&CK, qui fournit des informations complètes sur les menaces les plus complexes et les groupes de pirates qui affligent le cyberespace. Avec plus de 20 contributions à la base de connaissances et une participation troisième cycle des *évaluations de MITRE Engenuity ATTACK*, notre solution EDR est éprouvée et mature.

Recherche de menaces

Doté d'un ensemble de règles rigoureusement testées pour détecter les comportements suspects et de fonctionnalités de filtrage avancé pour classer les données en fonction de la popularité des fichiers, de la réputation, de la signature, du comportement et d'autres informations contextuelles, EEI recherche automatiquement et facilement les menaces pour découvrir des attaques ciblées. Comme EEI permet la création de règles personnalisées et d'exclusions de règles, il peut être configuré avec précision pour s'adapter au mieux à un environnement, ou pour réexaminer la base de données des événements avec des configurations personnalisées afin de rechercher des menaces dans un historique.

API publique

ESET Enterprise Inspector dispose d'une API qui permet aux ingénieurs de sécurité d'exporter les détections, permettant ainsi une intégration efficace avec des outils de SIEM, de SOAR, de tickets et autres.

À PROPOS D'ESET

Depuis plus de 30 ans, ESET® développe des logiciels et des services de sécurité informatique de pointe pour protéger les entreprises, les infrastructures critiques et les consommateurs du monde entier contre des menaces digitales de plus en plus sophistiquées. Protection des terminaux et des mobiles, détection et traitement des incidents, chiffrement et authentification multifacteur... les solutions performantes et faciles à utiliser d'ESET protègent et supervisent discrètement 24 heures sur 24, 7 jours sur 7, en mettant à jour les défenses en temps réel pour assurer sans aucune interruption la sécurité des utilisateurs et le bon fonctionnement des entreprises. L'évolution des menaces exige d'une entreprise de sécurité informatique qu'elle évolue également. C'est la cas d'ESET grâce à ses centres de R&D dans le monde entier travaillant à la protection de notre avenir commun. Pour plus d'informations, consultez *www.eset.com/fr/* ou suivez-nous sur *LinkedIn*, *Facebook* et *Twitter*.

Contributeurs d'ESET à la rédaction du rapport :

Rene Holt, ESET PR Writer
James Shepperd, ESET PR Writer
Branislav Ondrasik, ESET Security Research Communications Manager

Contributions supplémentaires de :
Studio créatif de WeLiveSecurity


CYBERSECURITY
EXPERTS ON YOUR SIDE