kaspersky

Lettre d'actualités
Kaspersky

Juin 2020

Edito

Ce premier semestre 2020 a naturellement été marqué par la crise du coronavirus, dans la sphère physique comme dans le cyberespace. Certaines attaques visant des organisations de santé ont marqué les esprits, tandis que les campagnes d'hameçonnage dans un contexte de recours massif au télétravail ont gagné en visibilité. La plateforme Cybermalveillance.gouv.fr, à laquelle Kaspersky participe, a d'ailleurs montré tout son intérêt au cours des dernières semaines pour informer et conseiller les internautes français. Pour autant, nous n'avons pas identifié de hausse massive des cyberattaques en conséquence du contexte sanitaire actuel : Pierre Delcher, chercheur expérimenté en sécurité que nous sommes heureux d'accueillir depuis quelques mois au sein du GReAT, propose une analyse à froid dans cette newsletter. Cette édition est également l'occasion de revenir sur plusieurs tendances de cybersécurité dont le développement d'un nouveau phénomène inquiétant en matière de violences domestique : les stalkerwares. Sur ces différents sujets, nous nous réjouissons de travailler de concert avec des partenaires français et étrangers. En cette période profondément disruptive, nous en sommes plus que jamais convaincus : la cyber-immunité ne pourra être atteinte qu'à travers une approche multilatérale et un travail de confiance impliquant tous les acteurs de la cybersécurité.

Tanguy de Coatpont
Directeur général
de Kaspersky France,
Afrique du Nord, de l'Ouest
et Afrique centrale

Initiative de Transparence et Capacity building : les prochaines étapes

L'Initiative Mondiale de Transparence (GTI) de Kaspersky va de l'avant. Le transfert des données des utilisateurs européens à Zurich, l'ouverture de centres de transparence pour permettre l'examen du code source, la confirmation des pratiques d'ingénierie fiables grâce à l'audit indépendant SOC 2 et, enfin et surtout, la certification ISO27001 des services de données de Kaspersky sont autant d'étapes qui ont fait de la GTI une initiative unique pour accroître la transparence et la confiance dans la cybersécurité.
Kaspersky élargit aujourd'hui son initiative en lançant d'autres programmes, parmi lesquels :

Cyber Capacity Building Program

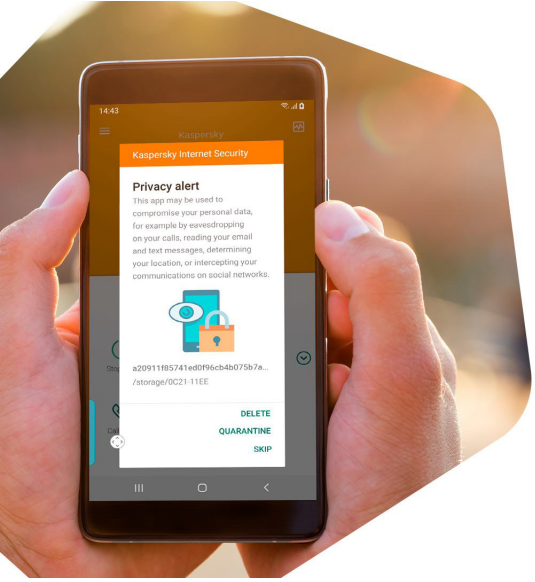
un programme de formation dédié à l'évaluation de la sécurité des produits pour aider les entreprises, les organisations gouvernementales et académiques à développer des compétences pour évaluer la cyber-résistance de leur chaîne d'approvisionnement. Dans le cadre des chaînes d'approvisionnement mondiales et/ou des infrastructures critiques, différents composants de l'infrastructure informatique peuvent être compromis, ce qui nuit à la sécurité publique ainsi qu'au bien-être économique et social. Il existe pourtant des moyens permettant d'évaluer et de garantir la sécurité et l'intégrité de ces éléments. La formation, gratuite et pouvant être suivie à distance, offrira une introduction à l'évaluation de la sécurité des produits et à la modélisation des menaces, ainsi qu'à l'examen du code source et à la gestion des vulnérabilités. Pour y participer, cliquez ici.

Accès virtuel à nos Centres de Transparence.

Dans un contexte mondial de distanciation sociale, les services clés ne peuvent plus être limités par un accès physique. Pour cela, nous lançons l'accès à distance aux services des Centres de transparence, en proposant une option d'évaluation "blue-piste" - la meilleure option pour se familiariser à la fois avec les pratiques d'ingénierie de l'entreprise et la manière dont Kaspersky assure la protection des données. Demandez une visite guidée ici.

Principes éthiques pour la divulgation responsable des vulnérabilités,

qui expliquent comment nous travaillons avec les chercheurs et la communauté de la sécurité pour mieux gérer la sécurité des produits. Ces principes, inspirés de notre expérience et des lignes directrices établies par FIRST, visent à améliorer la transparence et l'efficacité de la gestion des vulnérabilités et à atténuer les dommages et les risques pour les utilisateurs. Découvrez nos principes ici.



Violences conjugales : les stalkerwares, une cybermenace en croissance

Stalkerwares » ou « spousewares » : derrière ces termes barbares, sans traduction encore largement reconnue dans la langue française, se cache une menace récente mais en plein développement. Il s'agit de logiciels de pistage permettant de suivre la vie privée d'une personne en accédant à ses informations personnelles : contacts, journal d'appels, photos, vidéos, SMS voire la localisation. Ils peuvent être achetés en toute légalité et installés par une personne ayant accès à votre téléphone physiquement, ou se cacher derrière le téléchargement d'un programme anodin. La menace vient du fait que les victimes n'ont pas donné leur consentement : la surveillance se fait à leur insu. Et si cet espionnage s'effectue en ligne, les conséquences sont bien souvent réelles pour les victimes, ces logiciels pouvant être utilisés par des individus au comportement abusif, comme dans le cas de violences domestiques ou de harcèlement.

Suite à une prise de conscience de l'ampleur croissante du phénomène, Kaspersky et 9 organisations partenaires issus de différents pays – Avira, l'Electronic Frontier Foundation, le Réseau européen pour le travail avec les auteurs de violences conjugales (WWP EN), DATA CyberDefense, Malwarebytes, le Réseau national de lutte contre les violences conjugales (NNEDV), NortonLifeLock, Operation: Safe Escape et WEISSER RING – ont lancé en novembre 2019 la « **Coalition contre les stalkerwares** » (www.stopstalkerware.org).

COALITION AGAINST STALKERWARE

Les membres fondateurs, acteurs de la cybersécurité et organismes à but non lucratif, ont d'abord développé une définition standard de ce type de logiciels espions et sont parvenus à un consensus sur les critères de détection, de manière à permettre au secteur de la sécurité informatique d'agir concrètement contre cette menace. La Coalition se donne désormais plusieurs objectifs :

- améliorer la détection et l'atténuation des stalkerwares,
- accroître les capacités techniques des victimes et des organisations de lutte contre les violences conjugales,
- faire progresser l'information et la sensibilisation du public.

32%
Hausse du nombre d'utilisateurs de solutions Kaspersky confrontés à des stalkerwares en 2019, le nombre d'attaques ayant doublé au cours du second semestre[1]

Un phénomène mondial

La Russie, le Brésil, l'Inde et les États-Unis sont les pays les plus touchés dans le monde. En Europe, l'Allemagne, l'Italie et la France arrivent en tête

70 %
de femmes ayant été victimes de harcèlement électronique ont également subi au moins une forme de violence physique et/ou sexuelle de la part d'un partenaire intime, selon une étude de l'European Institute for Gender Equality

En raison de l'importance sociétale du sujet, de l'apparition régulière de nouvelles formes de cybermenaces, mais aussi de la complexité de la problématique en situation réelle (en cas de détection du logiciel espion, sa suppression par la victime peut mener à des violences physiques), la Coalition contre les stalkerwares appelle à une coopération toujours plus élargie. **En France** le Centre Hubertine Auclert, déjà actif sur ces sujets, a rejoint en mai 2020 la Coalition. Kaspersky collabore également avec d'autres entités comme la Délégation ministérielle aux industries de sécurité et à la lutte contre les cybermenaces (DMISC) du Ministère de l'Intérieur pour délivrer des formations techniques aux acteurs engagés dans la lutte contre les violences conjugales.

« Selon l'étude sur les cyberviolences conjugales[2] menée en 2018 par le Centre Hubertine Auclert, en France, 21% des victimes ont fait l'expérience de l'utilisation de logiciels espions par un partenaire abusif, tandis que 69% des victimes ont le sentiment que leurs informations personnelles sur leur smartphone ont été consultées par leur partenaire sans leur consentement. Les stalkerwares sont une source majeure de danger et de détresse pour les victimes. La Coalition est une excellente occasion de réunir l'expertise du secteur de la sécurité informatique et des ONG spécialisées dans la lutte contre les violences contre les femmes : cette synergie au niveau international sera fructueuse pour créer ensemble les meilleures solutions pour la protéger les victimes »

Clémence Pajot, Directrice du Centre Hubertine Auclert.

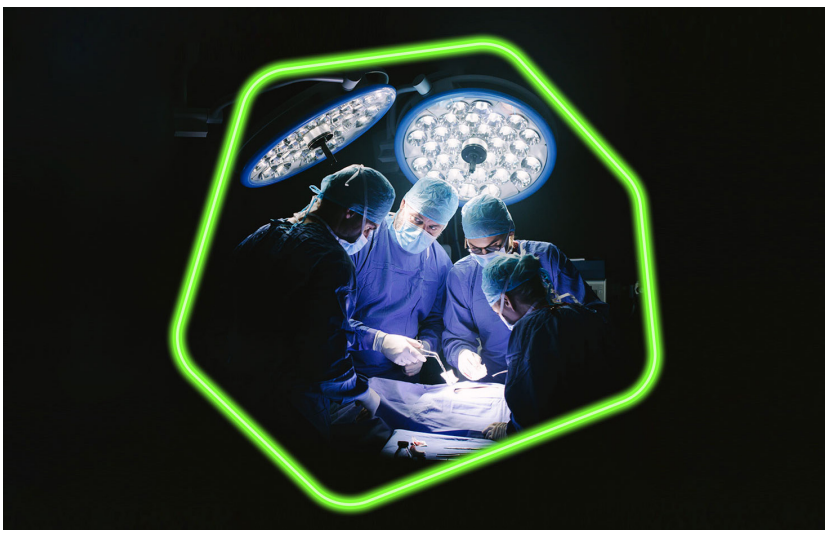
Le Centre a pour mission de promouvoir l'égalité et lutter contre les violences faites aux femmes en Ile-de-France

1 https://securelist.com/the-state-of-stalkerware-in-2019/93634/
2 https://www.centre-hubertine-auclert.fr/outil/rapport-cyberviolences-conjugales-2018

Crise du COVID-19 : quel impact sur la cybersécurité des organisations et des particuliers ?

3 questions à Pierre Delcher, chercheur senior en sécurité informatique au sein de la Global Research & Analysis Team (GReAT) de Kaspersky , expert en threat intelligence.

A-t-on constaté une hausse des cyberattaques à l'occasion du confinement ?
Le confinement est rapidement devenu le terrain d'une course aux chiffres cyber, donnés sans recul, sur fond de placement de produit. En mai, un éditeur constatait « une augmentation de plus de 30 000% des attaques ». D'où proviendraient les capacités humaines permettant une telle augmentation, alors même que le monde entier se confine, et que les activités sont dégradées ? A capacités égales, cela signifierait que les attaquants sont volontairement au ralenti d'habitude ? Non, les moyens qui permettent des attaques informatiques n'ont pas été décuplés, et les motivations qui les soutiennent sont stables. Nos données pour l'ensemble des clients en France attestent qu'il n'y a pas eu d'augmentation globale du nombre de détections de codes malveillants entre la période Janvier-Mai 2020, et la même période en 2019. C'est la même tendance à l'échelle mondiale. En revanche, l'attention autour du sujet COVID-19 a bien été exploitée pour mener des attaques informatiques : l'apparition de ce thème a notamment progressé de 43% dans les tentatives de hameçonnage entre janvier et mars. Les cybercriminels ont aussi proposé des applications de visioconférence piégées, de fausses attestations, notifications d'échecs de livraison de colis, ou encore de faux licenciements par email. Nos produits ont par ailleurs relevé une hausse de 25% des détections de menaces ayant Internet pour origine, entre janvier et avril 2020. Nous pourrions être tentés de justifier ce phénomène par une augmentation du nombre d'attaques exploitant ces vecteurs. Cependant, une augmentation du nombre de détections peut aussi être la simple conséquence d'un usage numérique plus important pendant le confinement, et ne signifie pas forcément qu'il y a eu plus d'attaques, ni qu'elles ont mieux réussi.



2000 hôpitaux bénéficient d'une protection gratuite pendant la pandémie

En solidarité dans la lutte contre le COVID-19, Kaspersky a proposé gratuitement des licences complètes de 6 mois aux établissements de santé publics et privés souhaitant renforcer leur sécurité. Plus de 2000 hôpitaux et organismes de soins à travers le monde ont bénéficié de cette offre ainsi que d'un support prioritaire.

La situation a provoqué un recours massif au télétravail. Quelles leçons tirer de cette période d'expérimentation à grande échelle ?

Des ressources de télétravail (VPN, plateformes collaboratives ou de visioconférence, ordinateurs portables, etc.) ont dû rapidement être exposées ou distribuées en dehors des périmètres de maîtrise habituels. Dans la précipitation, les mesures de sécurité ont pu être négligées. Pourtant, une atteinte à la disponibilité de ces ressources (dénis de services réseau ou rançongiciels, par exemple) désorganiserait profondément toute activité dans cette situation déjà perturbée. Les outils informatiques sont essentiels à toute organisation, et supportent un enjeu de survie dans une telle crise. Les responsables d'organisations doivent dès lors accepter de consacrer des moyens et efforts de sécurité à la hauteur des enjeux, avant qu'une crise survienne : dans le cas d'une situation exceptionnelle, j'aime autant être sûr que je n'aurais pas à affronter l'imprévu sur du papier, sans collaborateurs, avec une catastrophe informatique comme handicap. La seconde leçon, c'est que les moyens numériques modernes de travail ont vocation à être collaboratifs et distribués par construction – tant mieux ; mais que leur exploitation sûre en télétravail impose d'adopter le paradigme de défense en profondeur. Trop souvent, le dispositif de sécurité repose encore sur un périmètre borné et maîtrisé (celui de l'entreprise, de son réseau et de ses locaux), qui protège du « reste ». Il faut considérer que toute ressource informatique (notamment données et postes de travail) peut être exposée individuellement, partout, et doit donc être protégée indépendamment. Cela impose notamment de pouvoir assurer le maintien en conditions de sécurité du poste de travail à distance. De nombreuses autres leçons peuvent être tirées, mais je choisis ce dernier point de vigilance : diverses solutions commercialisées sous appellation cloud peuvent apparaitre comme la réponse à tous les défis numériques soulignés par cette crise. Elles doivent faire l'objet d'au moins autant d'efforts de sécurité que les solutions historiques. Elles introduisent en plus une dépendance tierce difficile à pallier, qui peut devenir une vulnérabilité majeure en cas de crise, ainsi que des difficultés supplémentaires de maîtrise des données. Le recours à de telles solutions peut en outre inviter à réduire encore ses capacités IT propres, qui sont pourtant essentielles à la gestion de situations exceptionnelles.

A défaut d'une augmentation du nombre de cyberattaques, a-t-on constaté une évolution dans ce domaine en période de pandémie ?

Dès janvier, des campagnes ciblées de messages malveillants ont visé des organisations gouvernementales en Asie ou en Europe. La plupart des documents malveillants que nous avons découverts dans ce cadre présentaient des statistiques de propagation du virus, ainsi que des comptes rendus de réunions internationales. Les techniques d'intrusion exploitées par ces acteurs n'ont toutefois pas changé pendant la pandémie. D'autres acteurs avancés ont publié des applications mobiles malveillantes, sous couvert d'outil de de suivi des infections, parfois en usurpant les outils nationaux officiels, comme « Aarogya Setu » en Inde. Nous avons aussi constaté que des organisations du secteur de la santé, y compris internationales, avaient été particulièrement ciblées en début d'année. Ces dernières l'ont probablement été à des fins de renseignement sur la gestion de crise sanitaire, pour anticiper des politiques internationales. L'intrusion informatique étant désormais une composante assumée de nombreux dispositifs de renseignement, et le coronavirus un sujet principal de préoccupation, c'était prévisible. Nous avons aussi identifié quelques cas d'attaques ciblées par rançongiciel, ayant exploité des vulnérabilités connues affectant des passerelles d'accès VPN. Il est possible que ces dispositifs aient été particulièrement ciblés pendant la pandémie, parce que les attaquants ont souhaité profiter de leur exposition précipitée, et parce que que les cibles affectées sont sûrement plus susceptibles de payer une rançon en situation de crise. Enfin, nous avons aussi observé une augmentation significative (80%) du nombre de tentatives de dénis de services réseau au 1er trimestre 2020, par rapport au même trimestre 2019. Ces tentatives visaient principalement des ressources éducatives et publiques, comme l'APHP.

En somme il faut retenir qu'aucune situation de crise ne justifie une trêve pour les attaquants, et qu'au contraire, tout évènement provoquant l'attention sera exploité. Pour réduire l'incertitude et ne pas subir de sur-incident, il n'y a pas d'autre choix que d'adopter en permanence une posture de défense en profondeur pour ses ressources informatiques, voire de préparer des mesures de continuité d'activité prévoyant l'indisponibilité de ces dernières.

Sécuriser le vote électronique pour accompagner le développement de la démocratie en ligne

Les élections en ligne ont des avantages évidents : elles permettent à l'organisateur de réduire les coûts et à l'utilisateur de gagner du temps en évitant les files d'attente ou les embouteillages. Néanmoins, le vote par internet nécessite des investissements importants pour être mis en œuvre dans de bonnes conditions et en toute sécurité. Il a donc souvent été difficile de justifier la nécessité d'introduire cette option.

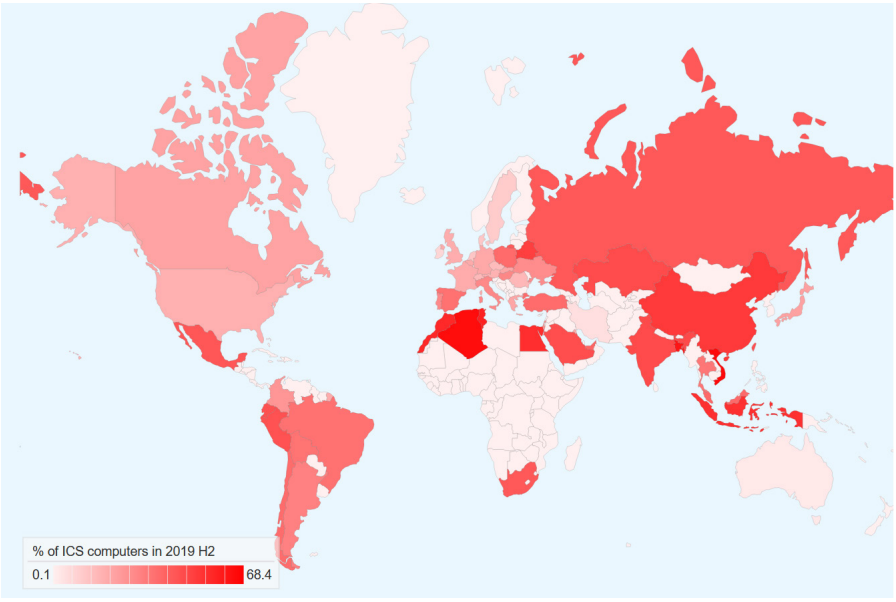
L'exigence actuelle de distanciation sociale rend toutefois la société plus numérique. On constate un intérêt accru pour le vote électronique au sein des collectivités territoriales – qui l'expérimentent déjà à travers les budgets participatifs – mais aussi et surtout pour les conseils d'administration et assemblées générales d'entreprises, associations, syndicats et partis politiques. Nous sommes convaincus que cette tendance va s'accélérer, et que les mesures d'auto-isolement au niveau mondial changeront l'attitude envers le vote à distance.

Kaspersky participe à cette transition en proposant sa nouvelle plateforme de vote à distance axée sur la cybersécurité. Le projet Polys (www.polys.me) consiste en un système clé en main de vote en ligne basé sur la technologie blockchain et, point important, une architecture décentralisée sur plusieurs nœuds qui peuvent être stockés auprès d'un tiers de confiance sur le cloud ou on-premise, sur l'infrastructure de l'initiateur du scrutin. Dernière innovation : des machines à voter et des urnes physiques sécurisées et connectées à la blockchain ! La mission est claire : assurer l'intégrité et l'inviolabilité du vote électronique.

Cybersécurité des systèmes industriels : deux fois plus de vulnérabilités identifiées en 2019

Les nouvelles recherches du CERT ICS de Kaspersky sur les menaces affectant les systèmes de contrôle industriel (ICS) mettent en évidence 103 nouvelles vulnérabilités en 2019 susceptibles d'être exploitées par des cyberattaques – un chiffre ayant presque doublé par rapport aux 61 signalées en 2018. 33 d'entre elles n'étaient toujours pas corrigées par les fabricants à la fin du premier trimestre 2020.

Or la menace est réelle : e**n 2019 des objets malveillants ont été bloqués sur près d'un système ICS sur deux (46,4%)** participant au Kaspersky Security Network, que ce soient des logiciels d'automatisation, des systèmes de contrôle industriel ou d'Internet des objets (IoT). Il est intéressant de noter que les menaces génériques visent également les systèmes industriels spécialisés: des ransomwares (Wannacry – toujours lui – GandCrab…) ont été bloqués sur 1% des systèmes ICS protégés par Kaspersky, représentant ainsi la menace plus potentiellement dévastatrice, particulièrement en Asie du Sud-Est et en Europe du Nord.



Geographical distribution of attacks* on industrial automation systems, H2 2019

* percentage of ICS computers on which malicious objects were blocked

Les secteurs de l'énergie et de l'extraction pétrolière sont parmi les plus touchés dans le monde : 36.6% des systèmes ICS du secteur « Power & Energy » ont été visés par une attaque, et 36.3% pour le secteur « Oil & Gas ». D'autres infrastructures critiques et services essentiels comme le traitement des eaux, la santé ou l'agroalimentaire arrivent par ailleurs en tête en matière de détection de vulnérabilités. Des tendances, malheureusement peu surprenantes, qui confirment l'importance de réaliser des audits de sécurité réguliers et une veille active (*threat intelligence*) pour se protéger des cybercriminels traditionnels comme des menaces persistantes avancées.

En savoir plus : https://ics-cert.kaspersky.com/

Kaspersky France, Afrique du Nord, de l'Ouest et Afrique centrale - 2 rue Joseph Monier - 92500 Rueil-Malmaison

@Kasperskyfrance @kasperskylabfrance Kaspersky France and North, West & Central Africa

kaspersky