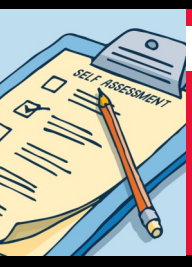
SAHER Magazine

Agence Nationale de la Sécurité Informatique

N°8
Oct. 2019

Clubs et Associations

Présentation de la communauté cybersécurité en Tunisie



Auto-évaluation

Évaluez le niveau de maturité de votre sécurité SI

Vote électronique

Retours d'expériences à travers le monde

الوكالة الوطنيّة للسّلامة المعلوماتيّة
Agence Nationale de la Sécurité Informatique

Séminaire TAIEX sur la protection des systèmes d'information d'importance vitale

L'intégration des TICs dans les processus métiers apporte des opportunités multiples pour le citoyen, l'économie et le gouvernement, en termes d'efficacité, de transparence et de bonne gouvernance, notamment pour les services qui touchent directement la vie du citoyen (télécoms, énergie, santé, transport, etc…). La forte dépendance de ces services des TICs fait que toute perturbation peut impacter la vie du citoyen et peut déstabiliser la société, l'économie.

C'est dans ce contexte qu'un séminaire a été organisé et financé par l'instrument d'assistance technique et d'échange d'informations de la commission européenne (TAIEX) en coopération avec l'Agence Nationale de la Sécurité Informatique (ANSI) sur «La résilience des infrastructures d'information d'importance vitale» à l'hôtel Golden Tulip El Mechtel les 25 et 26 septembre 2019. Ce séminaire s'inscrit dans le cadre de la mise en place d'un plan national pour la Cyber défense issu des travaux du Conseil de la Sécurité Nationale.

Cet événement était une occasion, pour les décideurs des organismes fournisseurs des services d'importance vitale et pour les responsables qui interviennent directement sur les infrastructures d'information d'importance vitale, de prendre conscience des risques qui menacent la pérennité de ces services et d'échanger autour des bonnes pratiques internationales (Italie, France, Croatie, Estonie, République tchèque, Lituanie) pour une protection adéquate afin d'assurer la résilience de leurs services.

© 2019 ANSI - tunCERT

8-10 Octobre 2019

GFCE : Annual Meeting 2019

Participation de l'Agence Nationale de la Sécurité Informatique dans le "GFCE : Annual Meeting 2019" qui a eu lieu à Addis-Abeba, Ethiopie.

L'objectif de cette édition est de renforcer un écosystème de coopération internationale en matière des capacités informatiques. La réunion vise à aller plus loin dans la mise en oeuvre de la CCB (Cyber Capacity Building), et portera sur les éléments suivants:

- Workshops globaux (organisés par les groupes de travail)
- Lancement de la nouvelle version du portail CCB
- Introduction de la Fondation GFCE et du Fond GFCE avec la banque mondiale
- Présentation du mécanisme de centre d'échange
- Discussion sur les développements du GFCE, tels que la gouvernance du programme de recherche GFCE et CCB.

9 Octobre 2019

Commission d'études de l'UIT-D

Participation de l'Agence Nationale de la Sécurité Informatique à la réunion des rapporteurs de la commission d'études de l'UIT-D qui a eu lieu à Genève, en Octobre 2019.

L'ANSI a participé activement à cette réunion durant laquelle la version 4 du questionnaire relatif à l'indice global de la cybersécurité (GCI) a été discuté.

© 2019 ANSI - tunCERT

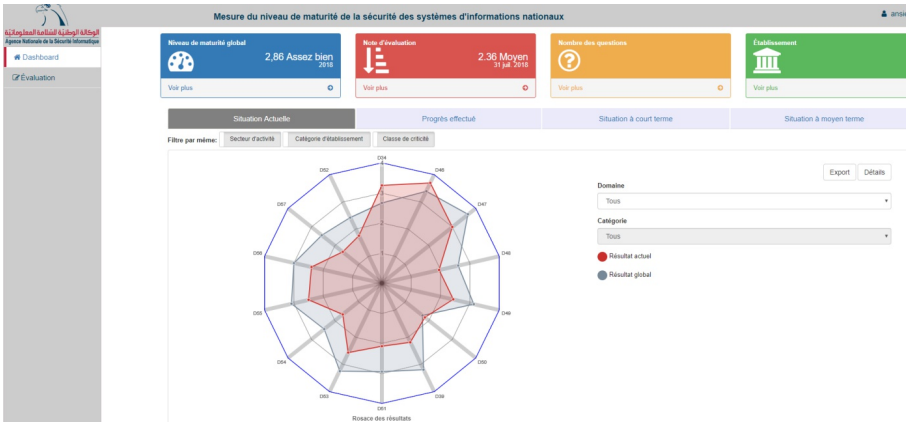
Auto-Evaluation du niveau de maturité de la sécurité du système d'information

On vous pose souvent la question « Est-ce que votre système d'information dispose des mesures de sécurité nécessaires pour faire face aux menaces de cybersécurité ? »
Vous avez besoin de justifier des investissements dans les projets de sécurité des systèmes d'information ?
Vous avez besoin d'évaluer le niveau de sécurité du système d'information actuel avant d'amorcer un projet de conformité par rapport aux standards et aux normes de bonnes pratiques ?

Le service d'Auto-Evaluation du niveau de maturité de la sécurité du système d'information permet de mesurer l'état actuel de la gestion de la sécurité du système d'information, d'évaluer sa maturité par rapport aux bonnes pratiques de la norme ISO 27002 et propose des recommandations adaptées à la réalité de l'organisme en fonction des réponses au questionnaire.
En outre, l'outil d'auto-évaluation est un outil pratique qui permet d'amorcer le projet de mise en place de Système de Management de la Sécurité de l'Information selon la norme ISO 27001 à travers une étude "GAP ANALYSIS".

Qui peut utiliser ce service ?
Le service « Auto-Evaluation du niveau de maturité de la sécurité du système d'information » est utilisé par un représentant de l'organisme souvent le Responsable de la Sécurité des Systèmes d'Information RSSI.
Toutefois, le RSSI peut faire appel aux structures spécialisées de son organisme pour répondre à des questions spécifiques du questionnaire (exemple : Responsable des ressources humaines sur les questions qui concernent le recrutement, le responsable de sécurité physique sur les contrôles de sécurité sur le bâtiment et le data-center, le responsable juridique sur le cadre réglementaire applicable sur l'organisme en relation avec la sécurité de l'information, etc).

Comment utiliser ce service ?
Le représentant de l'organisme désirant faire une auto-évaluation de la sécurité de son système d'information envoie une demande par email à audit@ansi.tn en fournissant les informations relatives à son organisme.
Les services de l'ANSI répondent à la requête par la création d'un compte utilisateur et envoient les paramètres d'accès par mail au concerné.
Le représentant de l'organisme se connecte à travers son compte utilisateur, et crée un nouveau projet d'évaluation.
Le représentant de l'organisme répond aux questions répertoriées par domaine (Chapitres de la norme ISO 27002).
Une fois le représentant de l'organisme répond à l'ensemble des questions du questionnaire, il valide ses réponses. Il est toutefois possible de réaliser l'évaluation sur plusieurs fois.



Les fonctionalités offertes par ce service
L'état de maturité de l'organisme est désormais disponible sous forme de note et de graphiques mais il est aussi possible de :
• Consulter le progrès effectué par rapport à l'évaluation précédente;
• Voir le niveau de maturité lorsque son organisme aura réalisé les actions de sécurité programmé pour le court terme (Situation à court terme) ou lorsque son organisme aura réalisé les actions de sécurité programmé pour le court terme et le moyen terme (Situation à moyen terme);
• Se comparer par rapport à d'autres organismes du même secteur d'activité, de la même catégorie ou de la même classe de criticité.

Comment accéder à ce service ?
Vous pouvez accéder à ce service via ce lien : https://mmsi.ansi.tn

© 2019 ANSI - tunCERT

Clubs de cybersécurité en Tunisie

Les clubs de cybersécurité jouent un rôle très important dans la promotion de la culture sécurité dans le milieu universitaire.

En Tunisie, on compte un dizaine de clubs spécialisé dans la sécurité informatique. Dans cet article, on va présenter quelques-uns.

.....

CSC Iset Jendouba : Cyber Security Club
Page facebook : https://www.facebook.com/ISET-Jendouba-Cyber-Security-Club-1022713044456112/

Le Cyber Security Club de ISET Jendouba a été créé en 2015 par un groupe d'étudiants passionnés par la cybersécurité et encouragés par des enseignants notamment M. Riadh Bouslimi, M. Mokhtar Sellami (ISET Jendouba) et M. Fadhel GHAJATI (ANSI)
Leur premier événement était en avril 2016 en partenariat avec l'ANSI et dont les thèmes sont la cyber threat intelligence, la gestion opérationnelle de la sécurité de l'information et l'audit de la sécurité des SI.

Notre deuxième événement a eu lieu en avril 2017 en partenariat avec l'ANSI et s'est focalisé sur les ransomwares et les techniques de chiffrement.
Le troisième événement était un workshop sur la programmation sécurisée des applications.
Le club envisage cette année de mener une compétition entre les étudiants dans un thème innovant autour des applications mobiles sécurisées.

.....

IEEE Cyber Security Unit ENIS
Page facebook : https://www.facebook.com/IEECSEC/

IEEE Cyber Security Unit ENIS a été fondé en décembre 2017. Le club vise à former les étudiants sur la sécurité informatique, les sensibiliser sur les risques digitaux ainsi que l'apprentissage des méthodes pour y faire face et mieux fortifier la sécurité de n'importe quelle base de données ainsi que les informations personnelles.

Même si le club est récent, il est parvenu à réussir plusieurs évènements, sur le plan humanitaire ainsi que le plan éducatif. Le premier événement a été organisé le 18 Mars 2018 : "I-PROTECT", suivi par "I-PROTECT V2.0" sa deuxième version.
Il est aussi parvenu à réaliser l'évènement "SECURIDAY", au sein de l'ENIS le 10 Novembre 2018, un événement sous forme de Workshop réalisé par l'association ISACA qui a accueilli 150 participants entre étudiants, professionnelles et enseignants.

Les événements ne se sont pas seulement consacrés au côté éducatif mais aussi bien sur le plan humanitaire en consacrant des sessions de Workshop pour les collégiens en leur sensibilisent sur les dangers trouvés de nos jours sur le net ainsi que les réseaux sociaux, cette manifestation était nommée "Secure The Future" faite le 1er Février 2019 au Collège Pilote Sfax.

Le club vise toujours à améliorer de plus les connaissances des nouvelles générations et à les familiariser avec domaine de la cybersécurité.

.....

Club Cyber Trace
Page facebook : https://www.facebook.com/CyberTraceClub/

CyberTrace est un club créé en 2017 par des étudiants passionnés par la sécurité informatique à l'ISSAT Sousse.

Son objectif ultime est de répandre la culture de sécurité informatique au sein des members du club et de partager les connaissances entre les experts et les nouveaux adhérents. Ils s'adresse aux étudiants ayant la curiosité et la volonté d'apprendre.
Un petit historique de nos exploits :
- Le club a été classé 36/1050 et 1er en Tunisie lors du EasyCTF
- En 2018, à l'échelle nationale, le club a décroché le 3ème prix pendant le Securiday organisé par Securinets à l'INSAT, ainsi que le 2ème prix lors des Hackfest au SUP'Com. Il a eu aussi la 5ème place lors du Hackzone à l'ENSI.

© 2019 ANSI - tunCERT

Securinets

La première association nationale de la Sécurité Informatique en Tunisie

Etant débutée comme un club à l'INSAT fondé par des étudiants, Securinets est devenue la première association tunisienne à baser l'intégralité de ses activités autour de la Sécurité Informatique.

Un peu d'histoire

En 2003, 4 étudiants qui sont Ahmed Amine BEN SOUAYAH, Nihel BEN YOUSSEF, Elyès GHANMI et Samy MABROUK ont eu l'idée de fonder un club qui vise à sensibiliser les gens, spécifiquement les étudiants, aux dangers liés aux attaques informatiques. Etant donné que la sécurité informatique était un sujet très peu abordé à cette époque, le club a commencé à attirer l'attention du public jusqu'à acquérir un succès spectaculaire à l'INSAT mais surtout dans d'autres universités.

Aujourd'hui, Securinets est une association qui compte plus de 1500 membres répartis dans 10 universités en Tunisie.

Les évènements principaux de l'association

Securinets organise chaque année deux évènements marquants.

1- National Cyber Security Congress

National Cyber Security Congress est un évènement présenté pour la première fois en 2019. Organisé pendant 3 jours dans un hôtel à Monastir, plus de 250 membres ont participé au NCSC. L'événement a été constitué d'une variété de workshops, de conférences et de challenges assurés par des experts du domaine ainsi que des anciens membres de Securinets.

Le congrès ne se contentait pas aux formations techniques mais a aussi accordé de l'attention aux formations soft skills (communication, PNL..) assurées dans une ambiance conviviale.

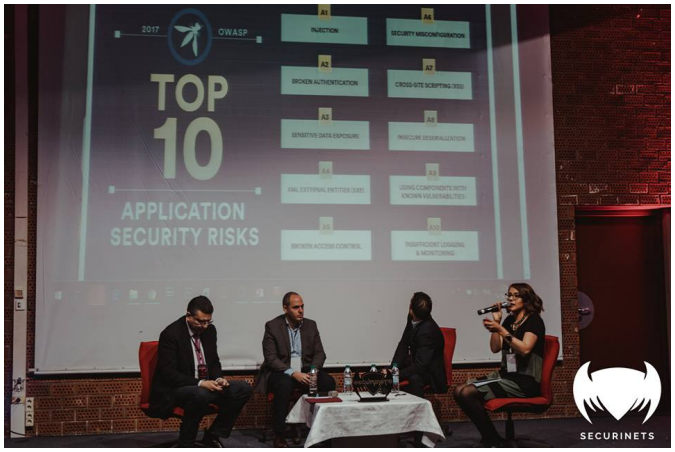
Pour sa première édition, cet évènement a eu l'attention des partenaires professionnels ainsi que des média audio-visuels publiques et privés.

© 2019 ANSI - tunCERT

2- Securiday

Securiday est l'évènement le plus ancien et le plus marquant dans l'histoire de Securinets. Faisant référence à « la journée nationale de la sécurité informatique », Securiday est une journée agrée par le ministère de l'éducation supérieure et la recherche scientifique. Depuis 2006, Securiday fut un rendez-vous annuel incontournable pour les membres de l'association, une journée qui porte chaque année sur un nouveau thème dont le choix est basé sur les dernières actualités de la sécurité informatique.

Etant donné que la sécurité est un domaine qui touche tous les utilisateurs des nouvelles technologies, le cible de la journée ne se contente pas aux mais aussi au grand public qui n'a pas forcément assez de connaissance dans la sécurité



informatique. L'association essaie de vulgariser quelques notions basiques du domaine afin qu'elles soient saisies par tout le monde.

Les axes de la journée

1- Conférences

Chaque année, l'INSAT accueille des grands experts dans le domaine de la sécurité informatique à l'auditorium de l'INSAT pour présenter des conférences liés au thème de la journée. Ayant une capacité de plus de 600 places à l'auditorium, ces conférences sont souvent très utiles aux étudiants puisqu'elles leur permettent d'être très à jour dans le domaine de la sécurité informatique mais aussi de profiter de l'expérience de ces experts afin de s'initier à la vie professionnelle.

© 2019 ANSI - tunCERT

2- Ateliers techniques

Durant Securiday, le grand Hall de l'INSAT est une opportunité aux étudiants ayant travaillé sur des projets liés à la sécurité d'exposer ces projets au grand public, mais surtout aux représentants d'entreprises qui se présentent chaque année dans ce rendez-vous afin de repérer les futurs profils à recruter.

3- Axe junior

L'association Securinets a pensé également aux enfants et aux adolescents puisque ceux-ci sont toujours les cibles les plus privilégiées de toute sorte de menaces. Pour ce fait, l'association a organisé un axe dont le but principal est de sensibiliser les plus jeunes aux dangers qu'ils peuvent rencontrer en ligne. Cet axe est assuré par une équipe d'étudiants bien formés techniquement qui organisent des formations hebdomadaires dans des écoles ou collèges privés. Les projets réalisés par les jeunes seront exposés durant le Securiday dans le hall de l'INSAT.

Les axes techniques

A part les deux évènements majeurs de l'association, Securinets accorde beaucoup d'importance à la formation technique de ses membres. Pour ce fait, Securinets profite toujours du large réseau d'anciens de l'association pour solidifier les compétences pratiques des adhérents à travers des formations presque hebdomadaires.

- Les ateliers techniques : En plus des formations assurées par les anciens membres Securinets, l'association dispose d'une équipe technique bien compétente qui d'intéresse à fournir de nouvelles compétences pratiques à ses membres afin de former les futurs experts en technique. Chaque semestre, 5 ateliers sont organisés de sorte que chaque atelier dispose d'un thème et d'un objectif spécifique réalisé tout le long du semestre de manière hebdomadaire. A la fin de chaque semestre, ces projets seront exposés durant un des deux évènements principaux.

- CTF : On ne peut pas parler de sécurité informatique sans faire référence au challenge le plus connu dans le domaine, Capture The Flag ou tout simplement CTF. Le CTF est un jeu consistant à exploiter des vulnérabilités affectant des logiciels de manière à s'introduire sur des ordinateurs pour récupérer les drapeaux « flags », preuves de l'intrusion. Tout le long de l'année, Securinets organise souvent des compétitions CTF afin de familiariser ses membres avec ce fameux jeu et leur permettre ainsi de gagner plein de cadeaux.

Le CTF le plus marquant de l'histoire de Securinets était le Quals2019, dans lequel plus de 700 équipes de partout dans le monde ont participé. Seules les 10 premières équipes ont été invitées pour participer au CTF final durant SecuriDay 2019.

© 2019 ANSI - tunCERT

Vote électronique: retours d'expérience à travers le monde

Le vote électronique est un système de vote dématérialisé, à comptage automatisé des scrutins, à l'aide de systèmes informatiques. Les principaux buts de ce procédé est d'accélérer, en premier lieu, le processus de traitement des suffrages exprimés, et de permetttre, en second lieu, aux électeurs de voter à distance, chose qui pose encore des problèmes de vérification du vote.

Il existe de multiples formes du vote électronique : vote par boîtier, par internet, machine à voter, stylo numérique, dépouillement automatisé, etc. Les fonctionnalités, les technologies et les cas d'usage de ces dispositifs diffèrent.
Le vote électronique est instauré afin d'accélérer le dépouillement des bulletins de vote, de réduire le coût de paiement du personnel chargé de compter les votes manuellement, il peut aussi améliorer l'accessibilité pour les électeurs à mobilité réduite et augmenter ainsi le taux de participation.
Dans cet article nous allons relater les expériences de quelques pays dans ce domaine.

Belgique
Le vote électronique a été expérimenté pour la première fois en Belgique en 1991. Il consiste en un tableau électronique muni de nombreux boutons, un en face de chaque candidat. Ce système a été abandonné la même année pour d'autres systèmes comme la carte magnétique en 1994, le comptage par lecture optique en 1999, en 2003 un système de ticketing a été ajouté à la lecture optique. Il consiste à voter avec une carte magnétique mais le choix de l'électeur est imprimé sur un ticket, derrière une vitre et, après validation, le ticket tombe dans une urne présente à côté de l'isoloir. Le comptage des tickets permet de vérifier le fonctionnement des machines à voter et de vérifier la volonté de l'électeur tel qu'il l'a validée.
Le 14 octobre 2012, un nouveau système est testé, cette fois les noms des partis et candidats pour lesquels l'électeur vote est imprimé sur un papier qu'il faudra plier en deux de manière à ne laisser apparaître qu'un code barre, qui sera lu optiquement au moment où l'on glisse ce papier dans l'urne. Grâce à ce système l'essentiel est assuré, à savoir qu'à tout moment l'électeur peut vérifier son vote et qu'un recomptage manuel des votes est possible autant qu'on le souhaite pour effectuer les vérifications.

France
La première utilisation d'une machine à voter fut introduite en 1969, grace à un système entièrement mécanique. Ces machines furent très vite abandonnées en raison des pannes importantes et de la non diminution des fraudes.

Il faudra attendre jusqu'aux élections présidentielles de 2002, où l'expérience du vote électronique à été renouvelée et testée dans 3 villes de France en parallèle du vote traditionnel. En 2003 le vote par internet à été introduit pour les français résidents aux Etats-Unis.

Brésil
Le Brésil a lancé en 1996 la mise en place de systèmes de vote électronique. Cette année-là, 32% des votes furent émis à travers les urnes électroniques. Lors du scrutin du 6 octobre 2002, 100% des électeurs ont utilisé le vote électronique. Un système informatisé identifiait chaque candidat par un numéro et une photographie, et dont les données, à la clôture du scrutin, étaient transmises, sans possibilité d'interférence, via un réseau privé aux instances électorales régionales. Grâce à ce système, utilisant 414 000 « urnes électroniques », il a suffit de 24 heures pour connaître les résultats de l'ensemble du territoire national.

Estonie
l'Estonie a adopté le vote par Internet pour la première fois en 2005 et depuis le succès est croissant a tel point que depuis 2012 ils peuvent voter via leurs smartphone.

Pays-Bas
Les Pays-Bas ont choisi d'abondonner définitivement le vote electronique en 2008 et de revenir au vote traditionnel. Cette décision fut prise suite à la démontration faite par un groupe de citoyens néerlandais de la facilité de détournement des votes suite au sabotages des logiciels des ordinateurs. Le taux de vote électronique atteignait en ces temps là les 90%.

© 2019 ANSI - tunCERT

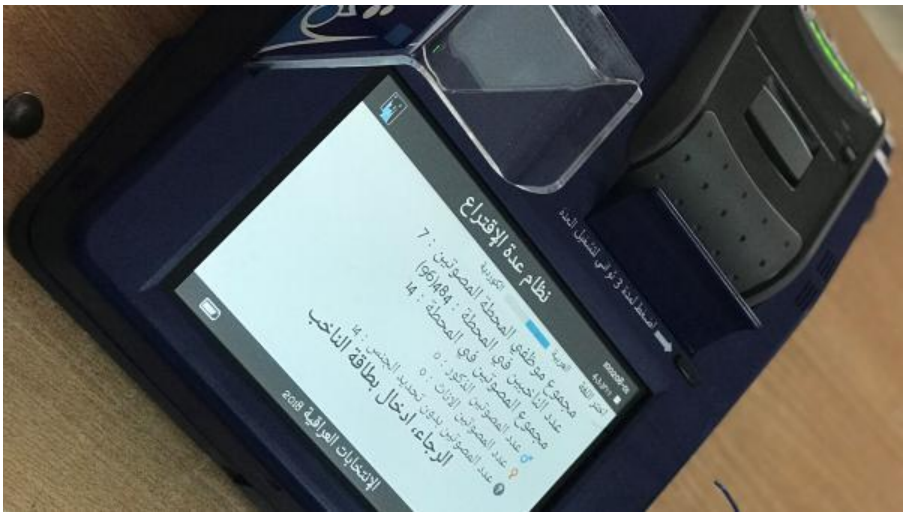
Les exigences du vote électronique

Les dispositifs qui permettent de voter en ligne ou au moyen de machine électronique doivent concilier impératifs de sécurité et enjeu démocratique; en effet, pour qu'un vote électronique soit valable, il doit répondre aux exigences suivantes:

• Unicité : chaque électeur ne peut voter qu'une seule fois par scrutin ;
• Confidentialité : les électeurs expriment leur vote à l'abri du regard d'autrui et sont protégés des pressions ;
• Anonymat : il est impossible de relier un bulletin de vote à l'électeur qui l'a choisi ;
• Transparence : toutes les étapes du processus de vote peuvent être contrôlées par les scrutateurs ;
• Sincérité : le décompte des bulletins permet de proclamer le gagnant choisi par l'ensemble des suffrages qui ont été exprimés.

Néanmoins, de nombreuses contraintes réglementaires et techniques existent.
En effet, le plus grand problème du vote électonique est la transparence qui est une notion assez complexe dans ce contexte ; il s'agit de l'ensemble des règles et des mesures organisationnelles qui permettent le constat d'éventuelles atteintes à la sincérité d'une élection ou au secret du vote (bourrage d'urnes, substitution de bulletins, pressions, achats de votes, etc.). La transparence électorale est donc un fondement essentiel de la confiance des électeurs et de la légitimité des élus. Mais puisque cette procédure est totalement dématérialisée, le vote électronique est devenu totalement opaque car toutes les expressions de vote, sans aucune exception, sont transformées plusieurs fois et que ces transformations ne sont pas observées. Des traitements de données modifiant les choix des électeurs (par erreur ou par fraude) pourraient intervenir et changer l'issue d'une élection sans qu'aucune preuve ne puisse être apportée à un juge électoral.

Cette perte de transparence inhérente à l'informatisation s'est accompagnée de l'apparition de nouvelles problématiques jusqu'alors absentes du domaine électoral : la sécurité et la vérifiabilité.
La fiabilité est la capacité d'un système à fonctionner sans erreur et sans tomber en panne: lenteur, panne, non présentation de candidats, absence de bouton de vote, établissement de résultats erronés.



la sûreté est l'ensemble des moyens matériels, humains, organisationnels visant à éviter ou à contrer toute attaque malveillante. Cette attaque peut être d'origine interne (membre du bureau de vote, personnel d'une entreprise de vote électronique) ou externe (personne non impliquée dans l'organisation du vote).
La promesse d'une sécurité parfaite ne peut donc compenser la disparition de la transparence.

Critiques

Plus les systèmes de votes deviennent complexes, plus les alternatives de fraudes deviennent possibles.
La principale critique faite par les experts en sécurité contre le vote electronique est la non possibilité de vérifier les votes. En effet, la plupart des machines de vote ne permettent pas de vérifier les votes, comme par exemple le cas en Belgique en 2003 où le décompte des voix exprimées a dépassé de 4 096 le nombre d'inscrits dans la circonscription.

C'est pour cette raison que les machines DRE (Direct-Recording Electronic) doivent avoir des traces d'audit papier vérifiables par l'électeur et que les logiciels utilisés sur les ordinateurs DRE doivent être soumis à des examens publics pour garantir la précision du système de vote. Des bulletins de vote vérifiables sont nécessaires car les ordinateurs peuvent mal fonctionner ou être compromises.

De nombreuses insécurités ont aussi été trouvées dans les machines à voter commerciales, telles que l'utilisation d'un mot de passe d'administration par défaut. Des cas de machines faisant des erreurs imprévisibles et incohérentes ont également été rapportés. Et, il y a un risque que les résultats des machines à voter commerciales soient modifiés par la société fournissant la machine. Il n'y a aucune garantie que les résultats sont collectés et rapportés avec précision.

En outre, le vote électronique a été critiqué pour sa mise en place inutile et coûteuse. Alors que des pays comme l'Inde continuent à utiliser le vote électronique, plusieurs pays ont annulé leurs systèmes de vote électronique ou décidé de ne pas les déployer à grande échelle, notamment les Pays-Bas, l'Irlande, l'Allemagne et le Royaume-Uni en raison de problèmes de fiabilité des MVE.

Mais le principal problème reste la confiance. Les électeurs craignent que leur vote ne soit modifié par un virus sur leur PC ou la machine de vote, ou lors de la transmission aux serveurs gouvernementaux.

Sources:

https://fr.wikipedia.org/wiki/Vote_%C3%A9lectronique
https://journals.openedition.org/terminal/4190
https://www.civiciti.info/fr/7-avantages-du-vote-electronique/
https://www.techtalks.fr/vote-electronique-comment-concilier-securite-et-democratie/
https://www.cairn.info/revue-le-genre-humain-2011-2-page-41.htm?contenu=resume#

© 2019 ANSI - tunCERT

«Nodersok», nouveau malware sans fichier, cible les PC Windows et les transforme en proxy zombie

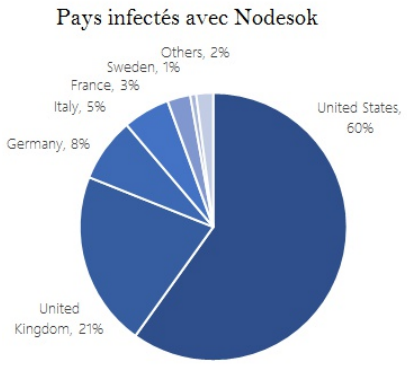
Connu sous le nom de "Nodersok" ou parfois "Divergent", Microsoft et Cisco Talos semblent avoir mis le doigt sur un nouveau malware. Ce dernier est distribué via des publicités malveillantes en ligne et infecte les utilisateurs via une attaque de téléchargement furtif (drive-by download).

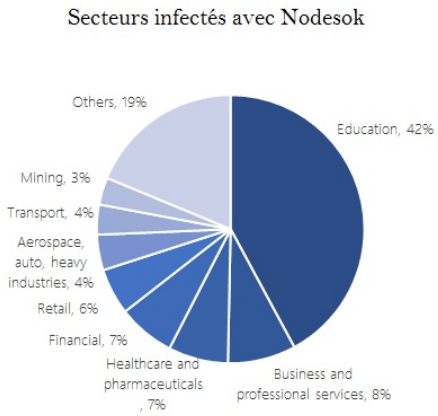
Vue d'ensemble de l'attaque

Nodersok a déjà infecté des milliers de machines, la plupart des cibles étant situées aux États-Unis et en Europe. La majorité des cibles sont des utilisateurs d'internet à domicile, mais environ 3% des infections se produisent dans des organisations tels que l'éducation, la santé, et la finance.

Le processus d'infection

L'infection commence quand les publicités malveillantes déposent un fichier de type "HTML application"

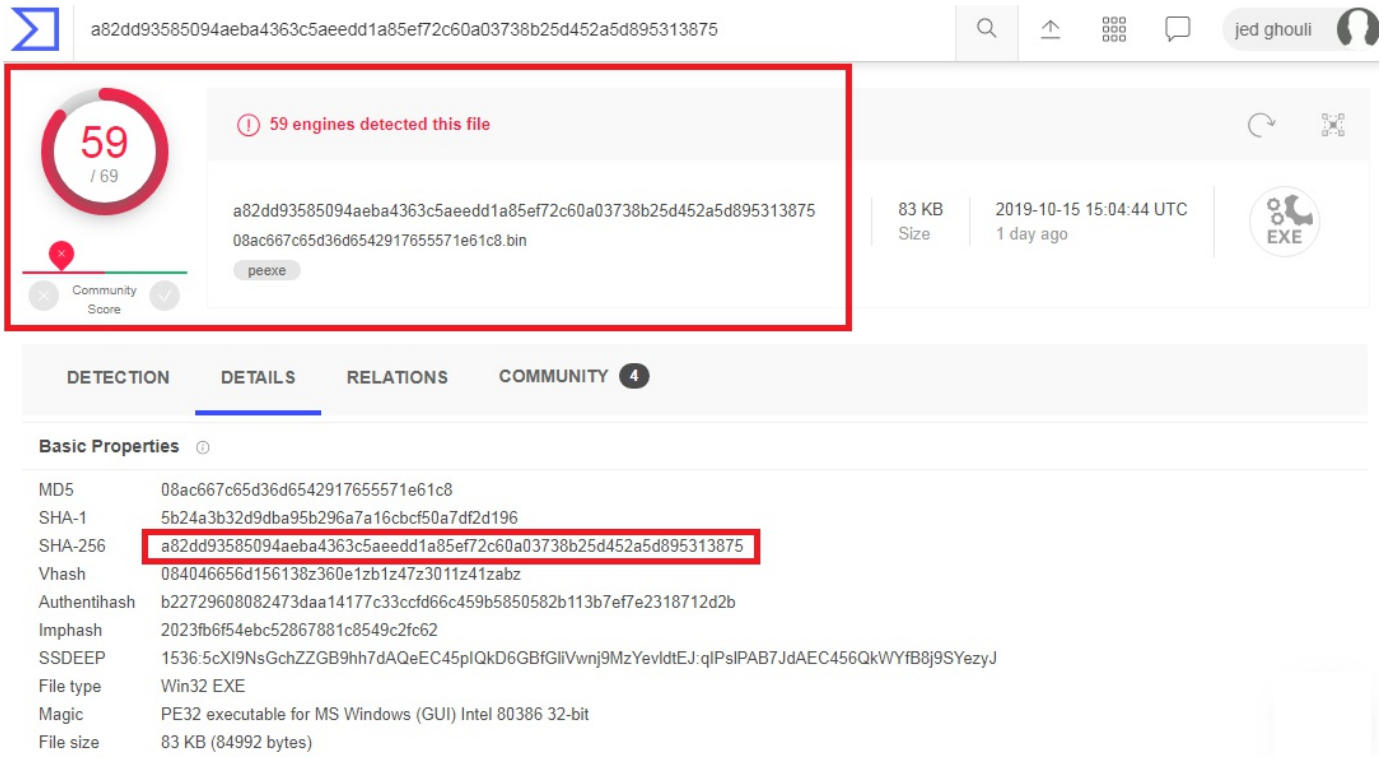




(Player1566444384.hta), puis attire les utilisateurs à cliquer sur une fausse annonce, qui pointe vers le fichier HTA.

Ce dernier va lancer une série d'événements sous JavaScript qui va à son tour exécuter une commande PowerShell. Celle-ci va créer automatiquement des proxys et exécuter plusieurs outils malveillants, dont un capable de désactiver Windows Defender.

• Scripts PowerShell : Tente de désactiver l'antivirus Windows Defender et la mise à jour Windows.



© 2019 ANSI - tunCERT

• Shellcode Binaire : Tente d'élever les privilèges en utilisant l'interface COM.

• Node.exe : l'implémentation Windows de la populaire framework Node.js, elle a une signature digitale valide et exécute du JavaScript malveillant pour opérer dans le contexte d'un processus.

• WinDivert (Windows Packet Divert): Une utilité qui permet de capturer et de manipuler des paquets de réseau que les malware utilisent pour filtrer et modifier certains paquets sortant.

Le moteur de proxy basé sur Node.js a deux principaux objectifs :

1. connecter le système infecté vers un serveur command-and-control distant, contrôlé par le pirate

2. recevoir des requêtes HTTP en retour.

Une fois que le serveur démarre, le client démarre aussi et se connecte à celui-ci. En réponse, le serveur envoie une requête HTTP (utilisant le protocole "Socks4A") au client. La requête est un simple HTTP GET. Le client envoie la requête HTTP au site Web cible et renvoie la réponse HTTP (200 OK) et la page HTML fait un retour au serveur. Ce test montre qu'il est possible d'utiliser ce malware en tant que proxy.

Supprimer Nodersok

Pour supprimer Nodersok de votre ordinateur, nous vous recommandons d'effectuer les étapes suivantes:

1. Démarrer l'ordinateur en mode sans échec

2. Cliquer les boutons Windows+r et taper « regedit »

3. Nettoyer les registres généralement ciblés des machines Windows qui sont les suivantes:

• HKEY_LOCAL_MACHINE Software Microsoft Windows CurrentVersion Run

• HKEY_CURRENT_USER Software Microsoft Windows CurrentVersion Run

• HKEY_LOCAL_MACHINE Software Microsoft Windows CurrentVersion RunOnce

• HKEY_CURRENT_USER Software Microsoft Windows CurrentVersion RunOnce

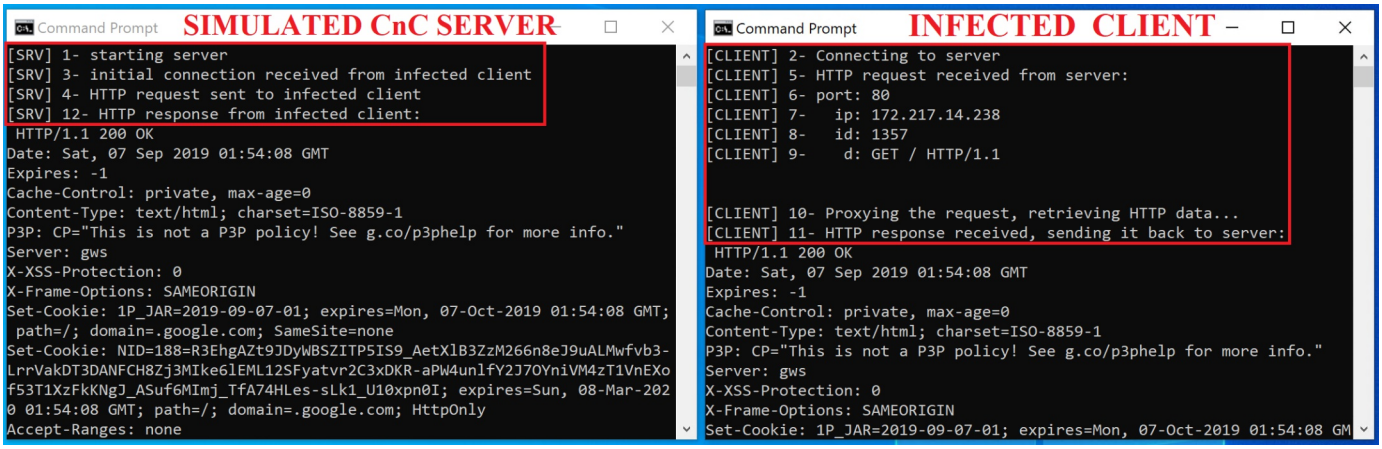
Recommandations

• Bloquez tous les IoCs basés sur les URL et IP au niveau du pare-feu, des IDS, des passerelles Web, des routeurs ou autres périphériques basés sur un périmètre.

• Assurez-vous que le logiciel antivirus et les fichiers associés sont à jour.

Source

https://blog.talosintelligence.com/2019/09/divergent-analysis.html



© 2019 ANSI - tunCERT

Attention au malware SMOMINRU et ses nouvelles variantes.

Récemment, des propagations massives ont été signalées sur le net et causées par le botnet « SMOMINRU » et ses nouvelles variantes. En effet, ce malware cible les systèmes Windows vulnérables via l'outil d'exploitation « EternalBlue » sur divers services, notamment MS-SQL, RDP, Telnet, SMB, RCP, etc.

Dans sa phase de post-infection, SMOMINRU collecte les informations de la machine infectée (CPU, processus, mémoire, etc), vole les informations d'identification de la victime par le moyen d'un outil nommé Mimikatz, installe un module de cheval de Troie et de cryptomining et se propage à l'intérieur du réseau. En outre, Smominru a réussi d'infecter plus que 90 000 machines dans le monde avec un taux d'infection de 4 700 machines par jour.

Pour se protéger face à cette menace, nous vous conseillons d'être vigilant et de suivre les mesures préventives suivantes:

- Scanner périodiquement votre réseau afin de déterminer les vulnérabilités existantes puis procéder à les corriger en installant les patchs correctifs depuis les sources officielles.
- Désactiver immédiatement tous les services que vous n'avez pas besoin.
- S'assurer de la robustesse des mots de passe des comptes utilisateurs et administrateurs dans vos systèmes et aussi vos équipements réseaux.
- Appliquer des règles de filtrage rigoureuses pour sécuriser l'administration de vos serveurs à distance.

Source
https://tuncert.ansi.tn/publish/content/news.asp?idn=154

Les vulnérabilités signalées par tunCERT durant le mois de Septembre

Référence	Date découverte	Titre
tunCERT/Vuln.2019-337	30/09/2019	PHP
tunCERT/Vuln.2019-336	27/09/2019	Produits Apple
tunCERT/Vuln.2019-335	26/09/2019	Produits VMware
tunCERT/Vuln.2019-334	26/09/2019	Joomla !
tunCERT/Vuln.2019-333	26/09/2019	Systèmes Cisco IOS et IOS XE
tunCERT/Vuln.2019-332	25/09/2019	Adobe ColdFusion
tunCERT/Vuln.2019-331	24/09/2019	Windows Defender
tunCERT/Vuln.2019-330	24/09/2019	Internet Explorer
tunCERT/Vuln.2019-329	23/09/2019	Systèmes Linux Red Hat
tunCERT/Vuln.2019-328	23/09/2019	F5 BIG-IP
tunCERT/Vuln.2019-327	20/09/2019	Produits VMware
tunCERT/Vuln.2019-326	20/09/2019	Mozilla Firefox
tunCERT/Vuln.2019-324	19/09/2019	Google Chrome
tunCERT/Vuln.2019-323	18/09/2019	Pilote des cartes graphiques AMD Radeon RX 550
tunCERT/Vuln.2019-322	18/09/2019	Produits VMware
tunCERT/Vuln.2019-321	17/09/2019	Moodle
tunCERT/Vuln.2019-320	13/09/2019	Systèmes Linux Red Hat
tunCERT/Vuln.2019-316	11/09/2019	Adobe Flash Player
tunCERT/Vuln.2019-315	11/09/2019	Google Chrome
tunCERT/Vuln.2019-314	11/09/2019	Microsoft: Outils de développement
tunCERT/Vuln.2019-313	11/09/2019	Noyau des systèmes Microsoft Windows
tunCERT/Vuln.2019-312	11/09/2019	Microsoft Office
tunCERT/Vuln.2019-311	11/09/2019	Microsoft Edge
tunCERT/Vuln.2019-310	11/09/2019	Internet Explorer
tunCERT/Vuln.2019-309	06/09/2019	Serveur de messagerie Exim
tunCERT/Vuln.2019-308	06/09/2019	WordPress
tunCERT/Vuln.2019-307	05/09/2019	Cisco Industrial Network Director
tunCERT/Vuln.2019-306	05/09/2019	Mozilla Firefox
tunCERT/Vuln.2019-305	05/09/2019	Cisco Webex Teams
tunCERT/Vuln.2019-304	04/09/2019	Google Android
tunCERT/Vuln.2019-303	04/09/2019	Samba sous Unix / Linux
tunCERT/Vuln.2019-302	03/09/2019	Systèmes Linux Ubuntu

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

© 2019 ANSI - tunCERT

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