aDvens

Security for the greater good

Renseignement sur les menaces
Bulletin du mois d'août 2022

2022-09-01 | **TLP:CLEAR** | CERT aDvens - CTI

Sommaire

1. Synthèse

Ce mois-ci, l'agence américaine CISA a publié *vingt-trois CVE* dans son catalogue de vulnérabilités actuellement exploitées.

La version 2.0 de la norme **TLP** est effective depuis cet été. Cette norme régit le partage de l'information dans le domaine de la cybersécurité.

Une recrudescence d'emploi du **Vishing** et du **SMiShing**, techniques d'ingénieries sociales, a été constaté. L'analyse de la cyberattaque dont à fait l'objet CISCO, en mai dernier, en est un parfait exemple.

Mi-août, une nouvelle campagne d'attaque utilisant le cheval de Troie **Agent Tesla** a ciblé des entreprises européennes et sud africaines. Une présentation de cet outil et de ses modes opératoires sont présentées dans ce bulletin.

Les systèmes industriels sont des systèmes d'information fréquemment ciblés car peu protégés. Comme le démontre le scénario d'attaque baptisée **Evil PLC**.

Au cours de ce second semestre, sur fond de tensions géopolitiques, de nouvelles cyberattaques présumées d'origines chinoises ont fait l'objet de condamnation de plusieurs pays auprès de la communauté internationale.

2. CVE

Pour mener leurs politiques de maintien en condition de sécurité de leurs infrastructures, les RSSI se basent, entre autres, sur les publications des CVE et des notes CVSS associés pour évaluer les risques et mettre à jour leurs environnements. Toutefois, les prioriser peut paraître complexe.

Le modèle *EPSS* peut les accompagner dans cette démarche en leur apportant une évaluation complémentaire.

L'**E**xploitation **P**rediction **S**coring **S**ystem fournit une métrique sur la probabilité d'exploitation d'une vulnérabilité. Ce modèle fera l'objet d'un article dans le prochain bulletin mensuel.

Les cinq CVE, ci-après, sont présentées en raison d'une forte probabilité d'exploitation massive sur les produits *Zimbra*, *muhttpd*, *Arris*, *CISCO* et *Chrome*.

Certaines d'entre elles ont fait l'objet de bulletins d'alerte par le CISA.

2.1. CVE-2022-37042 et CVE-2022-27925

Figure 1. CVE-2022-37042

Figure 2. CVE-2022-27925

Ces deux vulnérabilités affectent les serveurs de messagerie Zimbra et plus spécifiquement le composant **Zimbra Collection Suite (ZCS)** pour les versions 8.8.15 et 9.0.0.

Ces vulnérabilités ont été exploitées, conjointement, lors de campagnes d'attaques ciblant des organisations privées et gouvernementales. Comme le confirme des chercheurs de chez Volexity dans leur article du 10 août, avec la compromission de plus de 1000 instances ZCS.

Les failles portent toutes deux sur une routine de vérification de fichier dans la fonction *mboximport*. Elles permettent à un attaquant de charger un fichier dans un dossier (directory traversal) et d'exécuter du code arbitraire sur le système.

L'emploi simultané de ces deux failles permet à un attaquant d'installer un web shell.

Recommandations

Pour se prémunir de ces deux vulnérabilités, l'éditeur a publié des mises à jour dont le patch 33 pour la version 8.8.15 et le patch 26 pour la 9.0.0.

2.2. CVE-2022-31793

Une vulnérabilité a été détectée sur un composant du serveur web *muhttpd*, embarqué dans certains équipements réseaux du constructeur Arris. Ce serveur web permet de mener des actions d'administration.

Cette faille permet à un attaquant de lire arbitrairement des fichiers en ajoutant au début de sa requête un caractère spécifique.

Les versions du serveur muhttpd antérieures à 1.1.7 sont impactées et concernent les produits ci-dessous :

- NVG443
- NVG599
- NVG589
- NVG510
- BGW210
- BGW320

Recommandations

Il est recommandé d'installer la version 1.1.7. Si cette mise à jour ne peut pas être déployée, il est recommandé d'arrêter le serveur web.

2.3. CVE-2022-20866

Une vulnérabilité sur la gestion des clés RSA affecte certaines versions des produits Cisco Adaptive Security Appliance (ASA) et Cisco Firepower Threat Defense (FTD). Cette faille permet à un attaquant non authentifié, et à distance, de retrouver des clés privés RSA.

Cette vulnérabilité est provoquée par une erreur logique lors de l'enregistrement de la clé en mémoire sur la plateforme. Une attaque de type *side-channel* permettrait de récupérer les clés privées, de facto, déchiffrer les communications.

Produits impactés

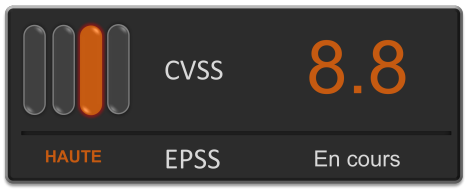
- ASA 5506-X with FirePOWER Services
- ASA 5506H-X with FirePOWER Services
- ASA 5506W-X with FirePOWER Services
- ASA 5508-X with FirePOWER Services
- ASA 5516-X with FirePOWER Services
- Firepower 1000 Series Next-Generation Firewall
- Firepower 2100 Series Security Appliances
- Firepower 4100 Series Security Appliances
- Firepower 9300 Series Security Appliances
- Secure Firewall 3100

A noter que les versions 9.16.1 et supérieures sont impactées pour CISCO ASA ainsi que les versions ultérieures 7.0.0 (incluse) pour FTD.

Recommandations

CISCO met à disposition dans son bulletin de sécurité des indicateurs de compromission pour détecter d'éventuelle exploitation.

2.4. CVE-2022-2856



Si une note EPSS est en cours d'attribution, cette vulnérabilité mérite d'être prise en compte dans une politique de mises à jour de son parc.

Cette zéro-day affectant Google Chrome, est due à une vérification insuffisante de données rentrées par les utilisateurs dans Web intents.

Web Intents est une interface de programmation d'application de Google Chrome qui peut être utilisée pour lancer des applications à partir de pages web et communiquer des informations à ces applications.

Un attaquant peut exploiter cette faille en forgeant un site web afin d'exécuter du code arbitraire sur le poste de la victime.

Cette vulnérabilité a été ajoutée sur le site du CISA comme une vulnérabilité **activement exploitée**.

Recommandations

Google encourage de mettre à jour Chrome vers la version 104.0.5112.101 ou une version supérieure.

3. Mise à jour du Traffic Light Protocol version 2 (TLPv2)

3.1. Présentation

TLP est une norme largement utilisée pour l'échange d'informations liées à la cybersécurité dans les communautés de la réponse aux incidents, de la criminalistique numérique et du renseignement sur les cybermenaces. Il a été initialement créé en 1999.

En 2015, FIRST a joué un rôle de premier plan dans l'unification et la normalisation du TLP.

Le « Forum of Incident Response and Security Teams » (FIRST) a récemment publié la version 2 du Protocole TLP (Traffic Light Protocol) qui fait « autorité à partir d'août 2022 », dépréciant la version 1 précédente.

TLP utilise un code couleur pour :

- Donner une indication sur la sensibilité des informations liées à la cybersécurité
- Spécifiez les restrictions de partage associées à ces informations.

La communauté cybersécurité l'utilise comme norme de facto pour l'échange d'informations avec leurs pairs, leurs partenaires et leurs mandataires.

TLP n'est pas un système de classification, et n'est pas juridiquement contraignant; son utilisation est basée sur la confiance.

3.2. Définitions des termes

Communauté :

Une communauté est un groupe qui partage des objectifs communs, des pratiques et des relations de confiance informelles. Une communauté peut être aussi large que tous les acteurs de la cybersécurité dans un pays (ou dans un secteur ou une région).

Organisation :

Une organisation est un groupe qui partage une affiliation commune par adhésion formelle, liée par des politiques communes définies par l'organisation. Une organisation peut être aussi large qu'une entreprise ou un groupe.

Client :

Les clients sont les personnes ou entités qui reçoivent des services de cybersécurité d'une organisation.

3.3. Charte graphique

Dans un email le TLP doit être placé :

- Au début de l'objet de l'email (ex : [TLP:RED])
- Au tout début du corps de l'email
- Le texte ne doit pas contenir d'espace, être en MAJUSCULE de la couleur du TLP, surligné de noir et d'une taille de 12 minimum.

Dans un document le TLP doit être placé :

- Dans l'entête et pied de page
- Le texte ne doit pas contenir d'espace, être en MAJUSCULE de la couleur du TLP, surligné de noir et d'une taille de 12 minimum.

3.4. Règles de partage de l'information

TLP:RED

La source

Utiliser lorsqu'il est nécessaire de restreindre l'information à un certain nombre de personnes ayant le besoin d'en connaître.

Le destinataire

Restreint au seul besoin d'en connaître des destinataires individuels uniquement (limité aux participants de la conférence, limité aux destinataires de l'email…).

TLP:AMBER+STRICT

La source

Utiliser lorsqu'il est nécessaire de limiter la diffusion aux personnes d'une organisation ayant le besoin d'en connaître.

Le destinataire

Partage limité, les destinataires ne peuvent partager l'information qu'aux personnes ayant le besoin d'en connaître au sein de leur organisation uniquement.

TLP:AMBER

La source

Utiliser lorsqu'il est nécessaire de limiter la diffusion aux personnes d'une organisation et les clients de cette organisation, uniquement s'ils nécessitent le besoin d'en connaître.

Le destinataire

Partage limité, les destinataires peuvent partager des informations qu'avec les membres de leur propre organisation et ses clients, mais uniquement en cas de besoin d'en connaître.

TLP:GREEN

La source

Utiliser lorsqu'il est nécessaire de limiter la diffusion au sein de leur communauté au sens large.

Le destinataire

Partage limité, les destinataires ne peuvent partager l'information qu'avec des pairs et des organisations partenaires au sein de leur communauté, mais pas via des canaux accessibles au public.

TLP:CLEAR

La source

Utiliser lorsqu'il est nécessaire de diffuser l'information sans restriction.

Le destinataire

Les destinataires peuvent partager l'information dans le monde entier et sans restriction.

4. Le Vishing et le SMiShing

4.1. Introduction

Dans la continuité de l'article concernant l'ingénierie sociale du précédent bulletin, une analyse a été effectuée sur les différentes méthodes du **Vishing** et du **SMiShing**. Ces deux techniques consistent à mener des campagnes d'hameçonnage à l'encontre de personnels d'une entreprise ciblée, via un échange vocal (Vishing) ou SMS (SMiShing). Le rapport « State of the Phish 2022» de la Société ProofPoint démontre une nette augmentation du Vishing et du SMiShing au niveau mondial. Les statistiques de ce rapport se basent sur un questionnaire rempli par 600 entreprises situées sur tous les continents.

Selon ce rapport, en 2021, 69% de ces entreprises ont été victimes de Vishing contre 54% en 2020 et 74% ont été victimes de SMiShing contre 61%. Compte tenu de la méfiance des internautes face au phishing, ces attaques sont en **constante augmentation**.

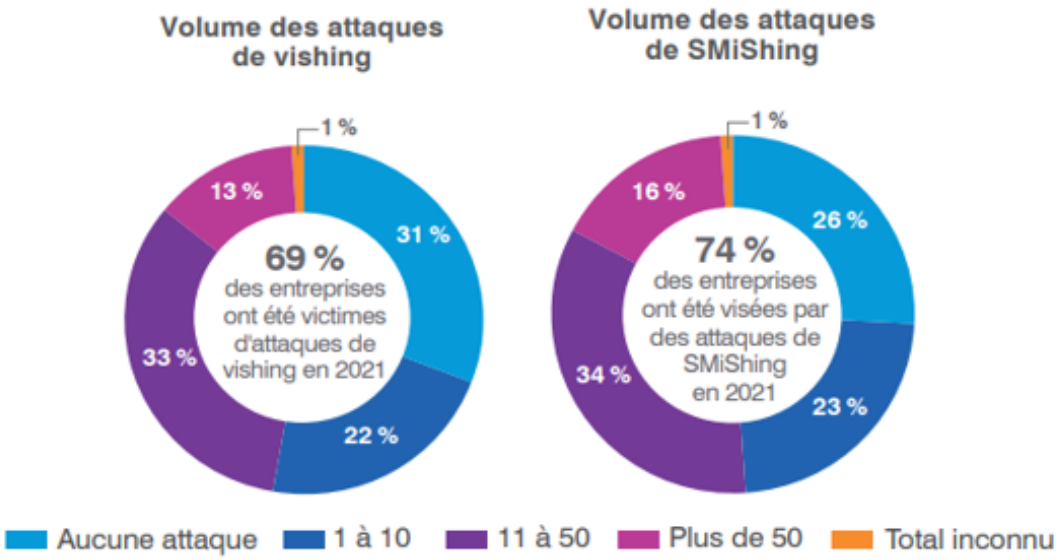


Figure 3. Statistique de Vishing et Smishing

4.2. Une entreprise victime

Au mois de mai 2022, l'entreprise Cisco a été victime d'une attaque informatique. Celle-ci soupçonne le groupe de *Ransomware Yanluowang* de l'avoir perpétrée. Dans son rapport sur l'incident, l'entreprise mentionne qu'« Au cours de l'enquête, il a été déterminé que les informations d'identification d'un employé de Cisco avaient été compromises après qu'un attaquant avait pris le contrôle d'un compte Google personnel où les informations d'identification enregistrées dans le navigateur de la victime étaient synchronisées »

« L'attaquant a mené une série d'attaques de phishing vocale sophistiquées sous le couvert de diverses organisations de confiance tentant de convaincre la victime d'accepter les notifications et les demandes d'authentification multi-facteurs (MFA) initiées par l'attaquant. L'attaquant a finalement réussi à obtenir une acceptation push MFA, lui

accordant l'accès au VPN dans le contexte de l'utilisateur ciblé. »

Le vecteur initial de l'attaque a donc été la récupération d'information d'identification de compte grâce une attaque de type Vishing cumulé à du SMiShing.

4.3. Définitions

4.3.1. Le Vishing

Vishing est l'abréviation de "Vocal phishing". Cette technique consiste à manipuler les victimes par téléphone pour les inciter à divulguer des informations sensibles. Dans cette définition du Vishing, l'attaquant tente de s'emparer des données de la victime et de les utiliser à son profit.

Les attaques les plus courantes sont :

- Offres de prêt ou d'investissement non sollicitées.

Les attaquants utilisent l'ingénierie sociale en forçant les victimes en leur offrant d'investir dans un projet ou d'obtenir un prêt. Étant donné que ces types de transactions financières impliquent souvent la divulgation d'informations financières personnelles, si l'attaquant peut convaincre la victime que son offre est légitime, la cible peut n'avoir aucun problème à divulguer des informations sensibles.

- Arnaque à l'assurance-maladie ou à la sécurité sociale.

Les attaquants utilisent l'état de santé de la victime comme levier. Cela pourrait impliquer une promesse de les inscrire à une offre gratuite, à des programmes de test de médicaments, d'obtenir un remboursement ou de recevoir un chèque, uniquement après avoir fourni ses données personnelles comme son numéro d'Assuré Social.

- Compte bancaire ou de carte de crédit compromis.

Si un attaquant peut obtenir les informations sur le compte bancaire ou la carte de crédit d'une victime, il peut accéder à ses fonds. Les numéros d'acheminement des comptes bancaires peuvent être facilement trouvés en ligne. Avec la combinaison des informations de routage d'une banque et du numéro de compte personnel de la victime, l'attaquant peut potentiellement retirer ou transférer des fonds de son compte vers le sien.

- Escroquerie fiscale.

Avec une escroquerie fiscale usurpant le Service des Impôts, l'attaquant profite du fait que la personne peut en avoir peur s'il y a un défaut de paiement des impôts par exemple. L'attaquant peut alors proposer une solution au problème, si la cible accepte de divulguer ses données personnelles.

4.3.2. Le SMiShing

SMiShing est l'abréviation de « SMS phishing ». Ce phishing est appelé ainsi lorsque l'attaquant utilise un SMS convaincant pour inciter les destinataires ciblés à cliquer sur un lien et à envoyer à l'attaquant des informations privées ou à télécharger des programmes malveillants sur un smartphone. L'ingénierie sociale est utilisée en combinaison avec le SMiShing. L'attaquant peut appeler l'utilisateur pour lui demander des informations privées avant d'envoyer un SMS. Les informations les plus couramment volées sont les suivantes :

- Informations d'identification d'un compte (compte VPN, compte Amazon…),
- Informations privées pouvant être utilisées dans le cadre d'un vol d'identité (numéro d'assuré social, numéro de carte d'identité…),
- Données financières pouvant être revendues sur le marché noir ou pour la fraude en ligne.(numéro de compte bancaire, numéro de carte de crédit…).

4.4. Recommandations

Dans son rapport cité plus haut, ProofPoint fait aussi état de la méconnaissance de ces menaces et des termes utilisés.

Il est important de sensibiliser au maximum les utilisateurs afin de limiter les attaques et leurs conséquences. Les recommandations face au Vishing et au SMiShing sont les suivantes :

Identifier ces attaques

- Un sentiment par la victime d'une urgence grave est développé,
- Des informations personnelles sont demandées,
- Des doutes sur l'identité réelle de l'interlocuteur apparaissent.

Se protéger de ces attaques

- Ne pas répondre à des numéros inconnus (appel vocal ou SMS),
- Ne pas appuyer sur tous les boutons du téléphone,
- Redemander et vérifier l'identité de l'interlocuteur et son numéro de téléphone,
- En cas de doute, raccrocher le téléphone ou supprimer le SMS

5. AGENT TESLA

5.1. Cheval de Troie Agent Tesla

5.1.1. Présentation

Agent Tesla est un logiciel malveillant de type **RAT** (*Remote Access Trojan*) développé par *Mustafa can Ozaydin* et découvert au cours de l'année 2014.

Il s'agit d'un cheval de Troie conçu pour le vol de données sensibles (identifiants et mots de passe) contenues sur le poste de la victime.

Il est commercialisé sous différentes licences, chacune d'entre elles proposent des options supplémentaires selon le prix. Par exemple, la licence « gold » propose du chiffrement pour les communications et une capture améliorée des frappes de clavier.

Agent Tesla est aussi défini par les experts en tant que **MaaS** (*Malware-as-a-Service*) puisqu'il peut être utilisé pour déployer d'autres logiciels malveillants. Le vecteur d'infection le plus utilisé est l'hameçonnage via des courriels malveillants et le partage de fichiers sur Discord. Lorsque la souche virale infecte le poste, celle-ci tente d'établir sa persistance en ajoutant une clé de registre sur le système puis commence la collecte d'information. Agent Tesla installe le navigateur TOR et l'utilise pour communiquer les informations volées vers un serveur C2.

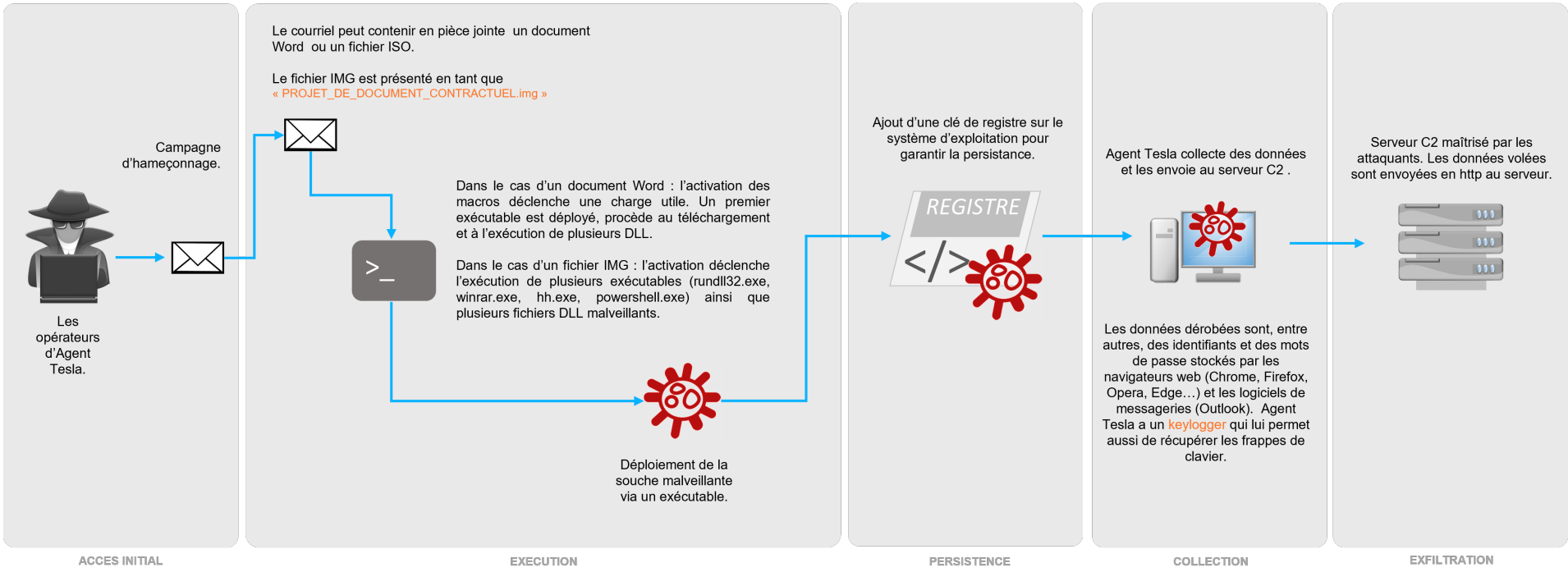
5.1.2. CVE exploitées

Plusieurs observations ont révélé l'exploitation de deux vulnérabilités par les attaquants.

CVE-2017-11882 et **CVE-2017-8570** : Ces deux vulnérabilités affectent Office de Microsoft. L'exploitation, réalisée localement et sans aucun privilège, permet à un attaquant d'exécuter de code arbitraire sur le système de la victime. IBM X-Force précise qu'une interaction de l'utilisateur est nécessaire, en effet l'attaquant doit inciter l'utilisateur à ouvrir un contenue spécifiquement forgé. De plus, il est aussi précisé que l'exécution du code arbitraire est réalisée avec le niveau de privilège de l'utilisateur lors de l'ouverture du contenue.

5.1.3. Techniques, tactiques et procédures

Le schéma d'attaque ci-dessous présente les principales étapes d'une cyberattaque menée par les attaquants au cours de l'année 2022. C'est l'hameçonnage qui est essentiellement utilisé pour réaliser un accès initial.



5.1.4. Matrice Mitre ATT&CK

TA0001 : Initial Access	TA0002 : Execution	TA0003 : Persistence	TA0004 : Privilege Escalation	TA0005 : Defence Evasion	TA0006 : Credential Access	TA0007 : Discovery	T10009 : Collection	TA0011 : Command and Control	TA0010 : Exfiltration
T1566.001 : Hameçonnage avec pièce jointe	T1203 : Exploitation pour une exécution client	T1547.001 : Démarrage, clé registre	T1087.001 : Découverte des comptes, comptes locaux	T1140 : Désobscurcir du code ou de l'information	T1555.003 : Identifiants issues des stockages de mots de passes, navigateurs Web	T1087.001 : Découverte des comptes, comptes locaux	T1071.003 : Protocole couche application, protocole mails	T1555.003 : Identifiants issues des stockages de mots de passes, navigateurs Web	T1048.003 : Exfiltration via protocole alternatif, exfiltration via un protocole non-chiffré et non-C2
T1190 : Exploitation de vulnérabilités	T1053.005 : Tâche planifiée, tâche planifiée	T1053.005 : Tâche planifiée, tâche planifiée	T1057 : Découverte des processus	T1564.001 : Dissimulation d'artéfact, fichier et dossiers dissimulés	T1506.001 : Capture de données, keylogger	T1057 : Découverte des processus	T1071.001 : Protocole couche application, protocole Web	T1506.001 : Capture de données, keylogger	
	T1204.002 : Exécution utilisateur, fichier malveillant		T1082 : Découverte système d'information	T1564.003 : Dissimulation d'artéfact, Dissimulation Windows	T1552.001 : Identifiants non sécurisés, identifiants dans des fichiers	T1082 : Découverte système d'information	T1105 : Outil d'intégration transfert	T1552.001 : Identifiants non sécurisés, identifiants dans des fichiers	
	T1047 : Instrumentation management Windows		T1016 : Découverte de la configuration du réseau du système	T1562.001 : Compromission de la défense, désactivation ou modification d 'outils	T1552.002 : Identifiants non sécurisés, identifiants dans les registres	T1016 : Découverte de la configuration du réseau du système	T1562.001 : Compromission de la défense, désactivation ou modification d 'outils	T1552.002 : Identifiants non sécurisés, identifiants dans les v	

TA0001 : Initial Access	TA0002 : Execution	TA0003 : Persistence	TA0004 : Privilege Escalation	TA0005 : Defence Evasion	TA0006 : Credential Access	TA0007 : Discovery	T10009 : Collection	TA0011 : Command and Control	TA0010 : Exfiltration
				T1112 : Modification registre		T1033 : Découverte propriétaire du système	T1112 : Modification registre		
				T1055.012 : Injection dans des processus de type «Hollowing »		T1124 : Découverte temps du système	T1055.012 : Injection dans des processus de type « Hollowing »		
				T1218.009 : Exécution proxy de binaire système, Regsvcs / Regasm		T1497 : Evasion de la virtualisation et de l'analyse bac à sable	T1218.009 : Exécution proxy de binaire système, Regsvcs /Regasm		
				T1497 : Evasion de la virtualisation et de l'analyse bac à sable			T1497 : Evasion de la virtualisation et de l'analyse bac à sable		

6. EVIL-PLC

6.1. Etude d'une nouvelle offensive

6.1.1. Le PLC en tant que prédateur

Les experts Team82 de la société Claroty ont réussi à détourner le fonctionnement d'un PLC, automate programmable industriel, afin d'établir un accès initial aux postes de travail qui y sont connectés. De plus, l'exploitation a aussi permis aux chercheurs de s'introduire dans les réseaux OT (Operative Technology) appartenant à différentes entreprises.

Baptisée « Evil-PLC » par les chercheurs, cette nouvelle offensive peut être réalisée à l'encontre des entreprises telles que Rockwell Automation, Schneider Electric, GE, B&R, XINJE, OVARRO, et Emerson.

Un exemple de cyberattaque menée par Team82 a été le déploiement et l'exécution d'un rançongiciel sur de multiples postes de travail destinés à la supervision des PLC.

« Using a Controller as Predator Rather than Prey »

Selon les chercheurs, cette cyberattaque est considérée comme nouvelle puisque le PLC est ici utilisé comme « prédateur (arme) » et non comme une « proie (cible) »

« The goal is not the PLC, such as it was, with the notorious Stuxnet that stealthily changed PLC logic to cause physical damage. Instead, we want to use the PLC as a pivot point to attack and gain deeper access to the OT network. »

Contrairement au célèbre logiciel malveillant Stuxnet, dont l'objectif était de permettre la compromission d'infrastructure critique en ciblant les PLC. Evil-PLC s'appuie sur les PLC comme un moyen de pivot pour permettre la réalisation de cyberattaque et l'intrusion dans le réseau OT.

6.1.2. Trois scénarios possibles

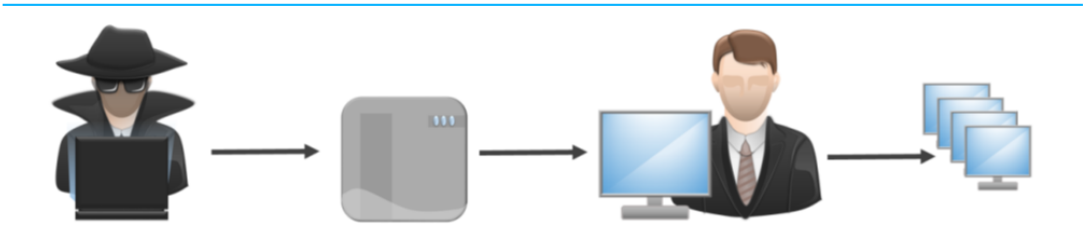
Les chercheurs ont identifié **trois** scénarios possibles.

Cyberattaque pour obtenir l'accès initial

Un attaquant pourrait utiliser un PLC pour établir un accès initial sur le ou les postes de travail connectés, et de pivoter vers d'autres réseaux, notamment le réseau OT de l'entreprise. Il s'agit ici du scénario malveillant où Evil-PLC est utilisé par des cybercriminels à l'encontre des entreprises.

Les principales étapes sont les suivantes :

1. Dans un premier temps, l'attaquant fait de la reconnaissance, il cherche des PLC qui sont exposés à Internet. Pour cela, il peut utiliser le moteur de recherche Censys.
2. L'attaquant utilise un logiciel légitime d'ingénierie pour se connecter au PLC.
3. L'attaquant modifie la configuration du PLC afin de provoquer volontairement une erreur. Le but étant d'attirer un ingénieur à venir vérifier la configuration.
4. Un ingénieur remarque l'erreur et télécharge la configuration du PLC pour réaliser un diagnostic.
5. La configuration téléchargée sur le poste de travail vulnérable contient une charge utile : celle-ci infecte le poste de travail de l'ingénieur et permet à l'attaquant d 'avoir un accès au système.
6. L'attaquant peut porter un impact sur le poste de travail en y déployant un rançongiciel ou il peut réaliser du mouvement latéral et tenter de pénétrer dans le réseau OT.



L'attaquant identifie un PLC exposé à Internet. L'attaquant réalise une attaque Evil-PLC et infecte le PLC avec une configuration malveillante.	PLC infecté. Une erreur est volontairement générée par l'attaquant pour attirer un ingénieur à réaliser un diagnostic.	Un ingénieur remarque le signalement d'une erreur sur le PLC infecté. Il télécharge la configuration du PLC : celle-ci contient une charge utile qui infecte son poste de travail vulnérable. L'attaquant à accès au poste et à tous les PLC connectés.	L'attaquant peut aussi tenter de pénétrer le réseau OT de l'entreprise.

Cyberattaque « Traveling Integrators and contractors »

Un attaquant pourrait utiliser Evil-PLC à l'encontre d'entreprises tierces afin d'établir un accès vers d'autres organisations dans le monde. Il s'agit ici du second scénario malveillant où Evil-PLC est utilisé par des cybercriminels à l'encontre des entreprises. Les principales étapes sont les suivantes :

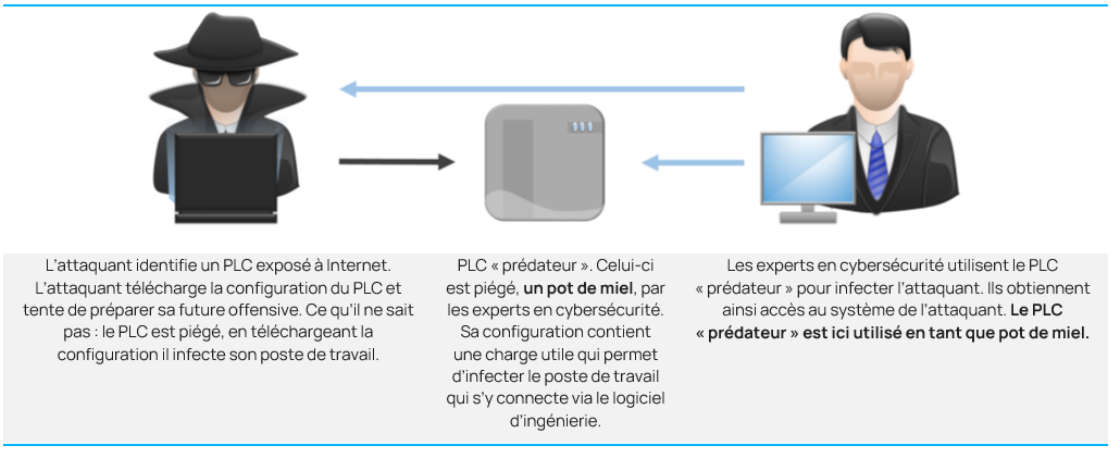
1. Dans un premier temps, l'attaquant fait de la reconnaissance, il cherche des PLC qui sont exposés à Internet. Pour cela, il peut utiliser le moteur de recherche Censys.
2. L'attaquant utilise un logiciel légitime d'ingénierie pour se connecter au PLC.
3. L'attaquant modifie la configuration du PLC afin de provoquer volontairement une erreur. Le but étant d'attirer un ingénieur à venir vérifier la configuration.
4. Un ingénieur remarque l'erreur et télécharge la configuration du PLC pour réaliser un diagnostic.
5. La configuration téléchargée sur le poste de travail vulnérable contient une charge utile : celle-ci infecte le poste de travail de l'ingénieur et permet à l'attaquant d'avoir un accès initial au système. Le poste de travail infecté de l'ingénieur est celui de l'entreprise tierce qui supervise le PLC d'un client A.
6. L'attaquant, ayant accès au poste de travail de l'entreprise tierce, est désormais dans la possibilité d'utiliser ce poste comme un pivot pour infecter divers PLC appartenant à d'autres clients. Depuis sa première infection de PLC du client A, l'attaquant peut ainsi atteindre les PLC des clients B, C, D…

L'attaquant identifie un PLC exposé à Internet. L'attaquant réalise une attaque Evil-PLC et infecte le PLC avec une configuration malveillante.	PLC infecté du **client A**. Une erreur est volontairement générée par l'attaquant pour attirer un ingénieur à réaliser un diagnostic.	Un ingénieur remarque le signalement d'une erreur sur le PLC infecté. Il télécharge la configuration du PLC : celle-ci contient une charge utile qui infecte son poste de travail vulnérable. L'attaquant a accès au poste de travail de l'entreprise tierce et à tous les PLC des clients que l'entreprise supervise.	L'attaquant peut ainsi accéder à tous les PLC des différents clients (**client B, C, D…**) de l'entreprise tierce.

Cybersécurité : « Honeypot »

Selon Team82, des experts en cybersécurité pourraient établir un piège, un pot de miel, afin d'attirer des pirates informatiques et tenter un accès initial dans leurs systèmes. Il s'agit ici du scénario bienveillant où Evil-PLC est utilisé par des experts à l'encontre des cybercriminels. Les principales étapes sont les suivantes :

1. Dans un premier temps, les experts en cybersécurité forgent une configuration spécifiquement conçue pour infecter un poste de travail qui se connecte via un logiciel d'ingénierie au PLC. Le PLC est un « prédateur (arme) » volontairement exposé à Internet.
2. L'attaquant utilise un logiciel légitime d'ingénierie pour se connecter au PLC.
3. L'attaquant télécharge la configuration du PLC « prédateur » pour préparer son offensive. Sans le savoir, l'attaquant infecte son poste de travail lorsque cette configuration est récupérée par son logiciel d'ingénierie.
4. Les experts en cybersécurité ont désormais accès au système de l'attaquant.



L'attaquant identifie un PLC exposé à Internet. L'attaquant télécharge la configuration du PLC et tente de préparer sa future offensive. Ce qu'il ne sait pas : le PLC est piégé, en téléchargeant la configuration il infecte son poste de travail.

PLC « prédateur ». Celui-ci est piégé, **un pot de miel**, par les experts en cybersécurité. Sa configuration contient une charge utile qui permet d'infecter le poste de travail qui s'y connecte via le logiciel d'ingénierie.

Les experts en cybersécurité utilisent le PLC « prédateur » pour infecter l'attaquant. Ils obtiennent ainsi accès au système de l'attaquant. **Le PLC « prédateur » est ici utilisé en tant que pot de miel.**

6.1.3. Solutions d'atténuations

L'étude réalisée par Team82 fait ressortir les éléments suivants pour atténuer le risque de cyberattaque :

- **Segmentation** et **hygiène informatique**. Afin de réduire la surface d'attaque, il est recommandé de segmenter le réseau et de limiter le nombre de postes de travail ayant accès au PLC.
- **Authentification**. En plus de réduire le nombre de poste de travail ayant accès au PLC, il est essentiel d'implémenter une authentification afin de s'assurer de la légitimité de la demande d'accès.
- **Infrastructure à clé publique**. Les experts de la Team82 recommandent le recours à une infrastructure à clé publique (PKI) pour sécuriser les communications entre les PLC, les postes de travail et les serveurs. La PKI permet de délivrer des certificats numériques, ceux-ci sont utilisés pour des opérations cryptographiques, notamment le chiffrement des données et les signatures numériques. Ces opérations cryptographiques ont essentiellement pour finalité de garantir la confidentialité, l'authentification, et l'intégrité des données.
- **Surveillance**. Lors d'une offensive de type Evil-PLC, les attaquants doivent télécharger et traiter des données. Une surveillance du réseau et des téléchargements est recommandée pour signaler toutes activités suspectes.
- **Mise à jour**. Il est conseillé d'être vigilant et attentif aux correctifs concernant les vulnérabilités découvertes lors de récentes études. Une entreprise qui applique les mises à jour de ces logiciels réduit considérablement le risque de subir une cyberattaque.

6.1.4. STUXNET et EVIL-PLC, un contraste ludique

STUXNET	EVIL-PLC
	
Le PLC est la cible, il est infecté par un logiciel malveillant dont le but est de compromettre l'infrastructure critique (Stuxnet ciblait les centrifugeuses iraniennes d'enrichissement d'uranium).	Le PLC est utilisé comme une arme pour établir un accès initial sur un ou plusieurs postes de travail connectés. Il peut aussi porter atteinte à l'intégrité du terminal (rançongiciel), ou servir de pivot pour s'introduire dans le réseau OT.
Le PLC est la « proie », selon les chercheurs de Team82	**Le PLC est le « prédateur », selon les chercheurs de Team82**

7. Activités des APT chinoises sur ce premier semestre 2022

En 2021 les Etats-Unis alertent la communauté internationale sur les activités cybercriminelles et d'espionnage menées par des groupes d'attaquants avancés (APT) affiliés à la République Populaire de Chine.

Cette année, sur fond de tensions géopolitiques, leurs activités demeurent intenses et leurs modes opératoires, évolutifs dès leur détection. Leurs attaques visent les secteurs d'intérêts privés (technologique, industrie, énergie) et gouvernementaux (défense, sécurité) sur les différents continents.

Le 20 juillet, le ministère des affaires étrangères belge condamne dans un communiqué, les campagnes d'attaques perpétrées par les groupes chinois **APT27**, **APT30**, **APT31** et **SOFTCELL** contre leurs ministères de l'intérieur et de la défense.

Cet article s'attarde sur deux faits marquants, sur ce premier semestre, liés à des menaces chinoises.

7.1. Activités d'espionnage à l'encontre de pays de l'Europe de l'Est

L'éditeur de sécurité Kaspersky découvre en début d'année, plusieurs campagnes de cyber espionnage opérées par le groupe **TA428**, à l'encontre d'entreprises militaro-industrielles et d'entités gouvernementales de certains pays de l'Europe de l'Est (Biélorussie, Russie, Ukraine et Afghanistan).

Cette attribution a pu se faire, au vu des outils et du modus operandi employés.

Ces attaques ont débuté, sans surprise, par des campagnes d'hameçonnage, ciblant des employés occupant des postes stratégiques au sein des entités visées. Le courriel embarque un document Word légitime provenant d'une entreprise militaro-industrielle. Ce document office a été modifié par l'attaquant pour exploiter la vulnérabilité CVE-2017-11882, permettant l'exécution de code à distance.

A l'ouverture du fichier malveillant, aucune activation de macro n'est demandée, et la porte dérobée PortDoor est installée.

Ce maliciel collecte des informations sur le poste compromis et déploie un autre implant de la même famille, nccTrojan.

Lors de ses tentatives de latéralisation sur le réseau de la victime, les portes dérobées DNSep et Cotx sont déployées via la technique de *"DLL Hijacking"* sur les nouveaux postes compromis. En outre, l'attaquant emploie le « process hollowing » pour éviter toute détection, en injectant leurs codes en mémoire dans des processus légitimes. Dllhost.exe pour Cotx et Powercfg.exe pour DNSep.

La porte dérobée Logtu sera déployée sur le même mode opératoire que celui de Cotx et DNSep.

Lors de leurs investigations, Kaspersky a découvert une nouvelle porte dérobée, nommée CotSam en raison des similitudes avec Cotx.

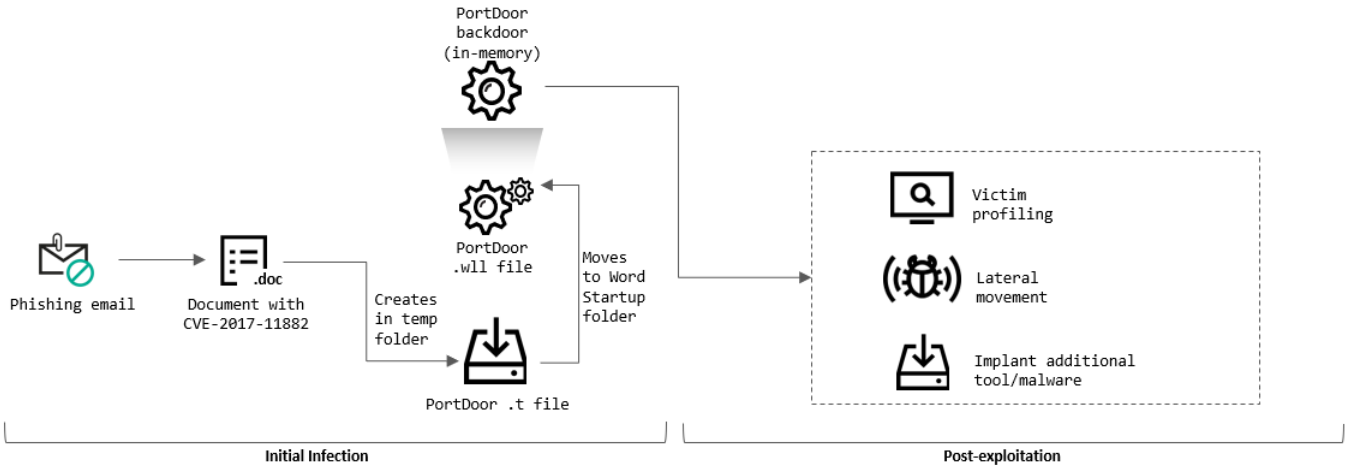


Figure 4. Modus operandi de l'attaque I Source : Kaspersky

L'emploi de ces six portes dérobées dans une même campagne d'attaque, démontre la volonté de l'attaquant de préserver son accès sur le réseau de la victime, en cas de détection.

Dès lors que le contrôleur de domaine est compromis, l'attaquant extrait les empreintes des mots de passes et vérifie les relations avec d'autres domaines au sein de l'entreprise.

Après avoir collecté les informations sensibles, ces dernières sont compressées et chiffrées avant d'être archivées dans des fichiers ZIP, protégés par un mot de passe, pour être exfiltrées. Les archives sont envoyées à un premier serveur Command & Control (C2), localisé n'importe où dans le monde, puis transférées vers un second serveur situé en Chine.

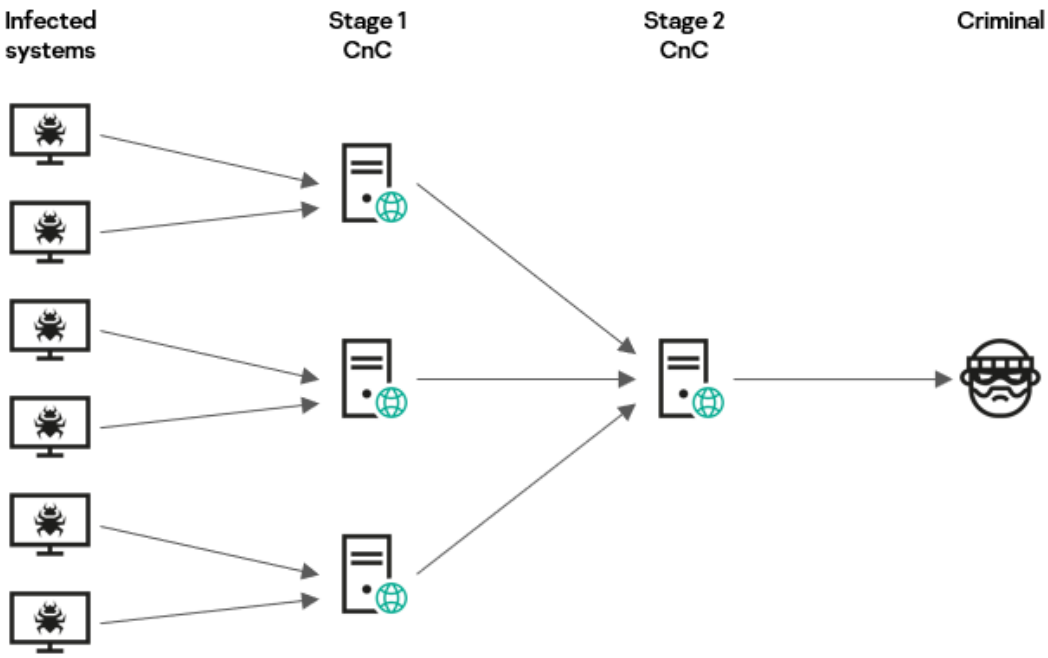


Figure 5. Processus d'exfiltration des données I Source : Kaspersky

L'éditeur Kaspersky met à disposition des indicateurs de compromission concernant cette campagne.

7.2. Exploitation massive de vulnérabilités connues d'équipement réseau

Le 07 juin, l'agence américaine *CyberSecurity & Infrastructure Securiy Agency* (CISA) alerte dans son bulletin AA22-158A, sur l'exploitation de vulnérabilités connues impactant des équipements réseau ; équipements utilisés dans le cadre privé (NAS) et professionnel (routeurs).

Ces failles ont été exploitées lors de campagnes d'attaques ciblant des entreprises de télécommunications par des APT chinois.

Vendor	CVE	Vulnerability Type
Cisco	CVE-2018-0171	Remote Code Execution
	CVE-2019-15271	RCE
	CVE-2019-1652	RCE
Citrix	CVE-2019-19781	RCE
DrayTek	CVE-2020-8515	RCE
D-Link	CVE-2019-16920	RCE
Fortinet	CVE-2018-13382	Authentication Bypass
MikroTik	CVE-2018-14847	Authentication Bypass
Netgear	CVE-2017-6862	RCE
Pulse	CVE-2019-11510	Authentication Bypass
	CVE-2021-22893	RCE
QNAP	CVE-2019-7192	Privilege Elevation
	CVE-2019-7193	Remote Inject
	CVE-2019-7194	XML Routing Detour Attack
	CVE-2019-7195	XML Routing Detour Attack
Zyxel	CVE-2020-29583	Authentication Bypass

Figure 6. Tableau listant les CVE exploitées contre les équipements réseaux I Source : CISA

Les attaquants procèdent au préalable à une phase de reconnaissance via des outils disponibles en source ouverte, comme RouterSploit et RouterScan pour identifier les marques et modèles vulnérables.

Après avoir pénétré le réseau du fournisseur de télécommunication, l'attaquant tente de compromettre le serveur Remote Authentication Dial Dans User Service (RADIUS), en charge des accès aux équipements. L'attaquant exporte sa base de données contenant l'ensemble des mots de passes des utilisateurs et des comptes d'administration.

Sur la base de ces informations, l'attaquant accède avec des comptes légitimes aux éléments actifs du réseau de l'entreprise, via le protocole SSH.

Ce processus est automatisé lorsque le réseau de la victime est conséquent, afin d'industrialiser la sauvegarde et l'exfiltration des configurations des routeurs.

Pour mener ses activités d'espionnage, l'attaquant modifie les configurations des éléments actifs pour effectuer des copies de flux réseaux (mise en place de port mirroring) et initier des tunnels de communication vers un serveur extérieur, pour l'exfiltration.

A l'issu, pour effacer toute trace d'activité et éviter toute détection, les journaux d'activités des routeurs et serveurs sont modifiés ou tout simplement effacés.

Pour limiter sa surface d'attaque, il est recommandé de :

- Mettre à jour ses équipements ou des contremesures si cela n'est pas possible.
- Segmenter son infrastructure réseau.
- Désactiver les services, ports et protocoles non utilisés.
- Activer la double authentification (MFA)pour les utilisateurs et les administrateurs.
- Mettre en œuvre la double authentification lors des connexions Virtual Private Network (VPN) ou à minima emploi de mots de passe complexes.
- Avoir une politique de mots de passes au sein de l'entreprise
- Activer, paramétrer et surveiller les journaux d'activités de ses équipements
- Avoir une politique de sauvegardes et les tester régulièrement

8. Références

CVE

CVE-2022-27925 et CVE-2022-37042

- https://wiki.zimbra.com/wiki/Zimbra_Releases/9.0.0/P26
- https://wiki.zimbra.com/wiki/Zimbra_Releases/8.8.15/P33

CVE-2022-31793

- https://derekabdine.com/blog/2022-arris-advisory
- https://blog.malwarebytes.com/exploits-and-vulnerabilities/2022/08/millions-of-arris-routers-are-vulnerable-to-path-traversal-attacks/

CVE-2022-20866

- https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-rsa-key-leak-Ms7UEfZz

CVE-2022-2856

- https://chromereleases.googleblog.com/2022/08/

Mise à jour du Traffic Light Protocol version 2 (TLPv2)

- https://www.first.org/tlp/
- https://cert.europa.eu/blog/tlp-version-2-primer

Le Vishing et le SMiShing

- https://www.proofpoint.com/sites/default/files/threat-reports/pfpt-fr-tr-state-of-the-phish-2022.pdf
- https://blog.talosintelligence.com/2022/08/recent-cyber-attack.html
- https://www.gendarmerie.interieur.gouv.fr/nos-conseils/pour-les-particuliers/me-proteger-sur-internet/le-vishing#

AGENT TESLA

- https://nvd.nist.gov/vuln/detail/CVE-2017-11882
- https://nvd.nist.gov/vuln/detail/CVE-2017-8570
- https://www.gatewatcher.com/malware-analysis-agent-tesla
- https://blogs.quickheal.com/coronavirus-themed-campaign-delivers-agent-tesla-malware/

EVIL-PLC

- https://thehackernews.com/2022/08/new-evil-plc-attack-weaponizes-plcs-to.html
- https://claroty.com/team82/blog/evil-plc-attack-using-a-controller-as-predator-rather-than-prey
- https://thehackernews.com/2022/08/new-evil-plc-attack-weaponizes-plcs-to.html
- https://www.lemondeinformatique.fr/actualites/lire-une-attaque-retourne-les-plc-industriels-contre-leur-systeme-de-gestion-87710.html

Activités des APT chinoises sur ce premier semestre 2022

- https://ics-cert.kaspersky.com/publications/reports/2022/08/08/targeted-attack-on-industrial-enterprises-and-public-institutions/
- https://www.spiceworks.com/it-security/threat-reports/news/chinese-ta428-cyber-espionage-campaign/
- https://ics-cert.kaspersky.com/publications/reports/2022/08/08/targeted-attack-on-industrial-enterprises-and-public-institutions/
- https://www.cisa.gov/uscert/ncas/alerts/aa22-158a