2020 VIRTUAL SYMPOSIUM
AFRICA & ARAB REGIONS | OCTOBER 21-23

AfricaCERT
United in promoting cyber security in Africa

African Union

NCB
National Computer Board

CERT-MU

COVID-19
GESTION DE CRISE CYBER

FIRST™

SMII MONDHER | CYBER SECURITY ANALYST

tunCERT
Tunisian Computer Emergency ResponseTeam

Timeline

1999

Unité de gestion par objectifs

promulgation du cadre réglementaire
Création de l'ANSI

2004

ANSI

2007

FIRST

Adhésion au Forum of Incident Response and Security Teams

2008

CNUCED

Adhésion au réseau des centres d'excellence

2010

Afrique du sud

Assistance à la création du CERT sud africain et accompagnement à l'adhésion au FIRST

2012

HONEYNET Project

Tunisian Chapter

2014

NIGERIA

Assistance à la création du CERT Nigérian et accompagnement à l'adhésion au FIRST

2017

ANSI – ANSSI

Partenariat bilatéral

2018

CERT SECTORIEL

2019

CSIRT.TN

1st Private CERT
FIRST Member

2020

1st Sectoral CERT
FIRST Member

2020

Setting up Health CERT

Crisis and Cyber attack

Le phishing exploite la crise financière américaine

JDN

Christophe Auffray
JDN

Mis à jour le 13/10/08 18:55

L'organisme américain de protection des consommateurs a publié une alerte concernant des attaques de phishing. Celles-ci détournent les faillites et rachats de banque pour abuser les internautes.

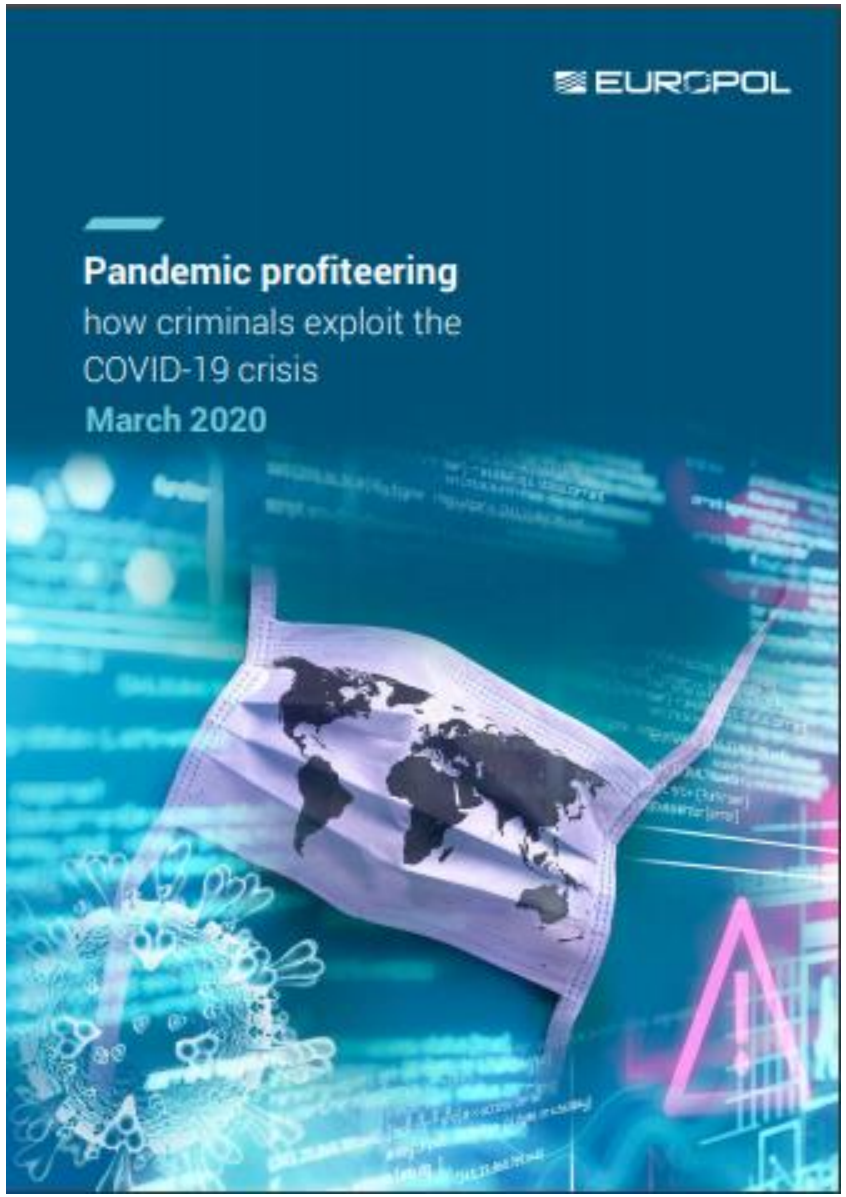
CRISES ET CYBERATTAQUES

Plus de 20 000 sites web français piratés par des hackers : comment se protéger ?

par Régis Rocroy | Fév 28, 2015 | Attaques Web

Suite aux attentats commis à Paris les 7, 8 et 9 janvier 2015 dernier, plus de 20 000 sites web ont été victimes de cyber-attaques menées par des hackers islamistes. Sous la bannière « Opération France », des pirates se présentant comme islamistes ou cyber-djihadistes...

CRISES ET CYBERATTAQUES



« L'impact de la pandémie Covid-19 sur la cybercriminalité a été le plus visible et le plus frappant par rapport à d'autres activités criminelles »

Une situation d'urgence qui obligent les entreprises à …

- **Travailler à distance**
- **Collaborer virtuellement**
- **Protéger les utilisateurs vulnérables**
- **S'adapter rapidement**

Cyber Incident during COVID-19

LES TYPES DES INCIDENTS TRAITÉS

PHISHING

EXTORSION

RANSOMWARE

VALIDATION DES VULNERABILITÉS (FAILLE@ANSI.TN)

TYPOSQUATTAGE

TENTATIVE D'ATTAQUE DEPUIS DEAS @IP TUNISIENNES : FRAUD WATCH & NETCRAFT

LES TYPES DES INCIDENTS TRAITÉS

TYPOSQUATTAGE

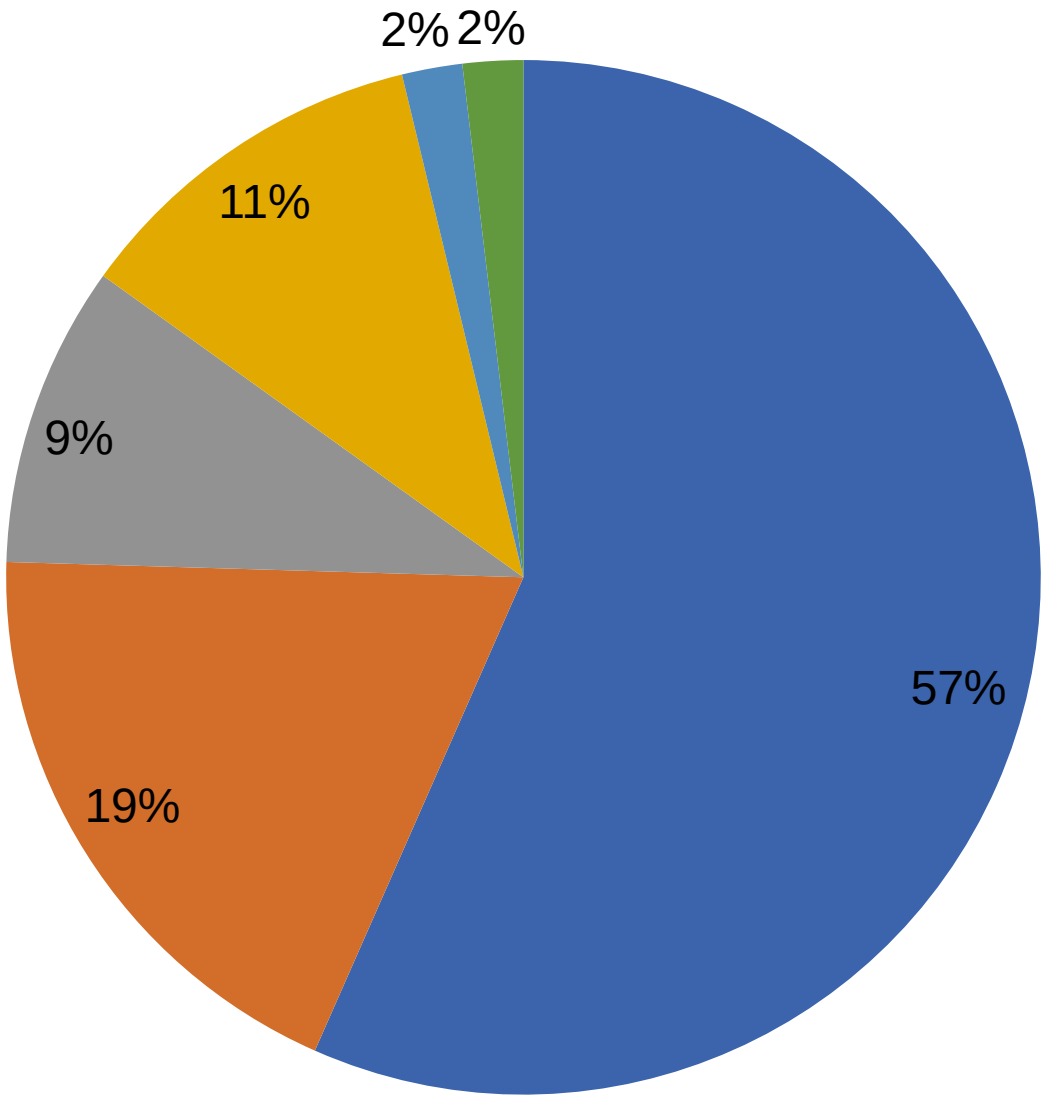
Cette technique est un type de « cybersquattage » dont le principe consiste à acheter des noms de domaine **ressemblant** à des sites connus avec une **faute volontaire**. L'objectif principal consiste à obtenir des visiteurs en se basant sur la possibilité que les internautes fassent une erreur en écrivant l'URL dans la barre d'adresse de leur navigateur.

- ❑ Inverser deux lettres d'un site très connu (exemple: gogole.com).
- ❑ Retirer des lettres (exemple: gogle.com).
- ❑ Faire des doublons volontaires (exemple: gooogle.com).

www.airfrạnce.com: emprunté à l'alphabet vietnamien

Il y a un petit point bien discret sous le « a »

Statistiques



- Phishing
- Extorsion
- Ransomware
- Tentative d’attaque depuis des @ip tunisiennes
- Validation des vulnerabilités (faille@ansi,tn)
- typosquattage

PHISHING

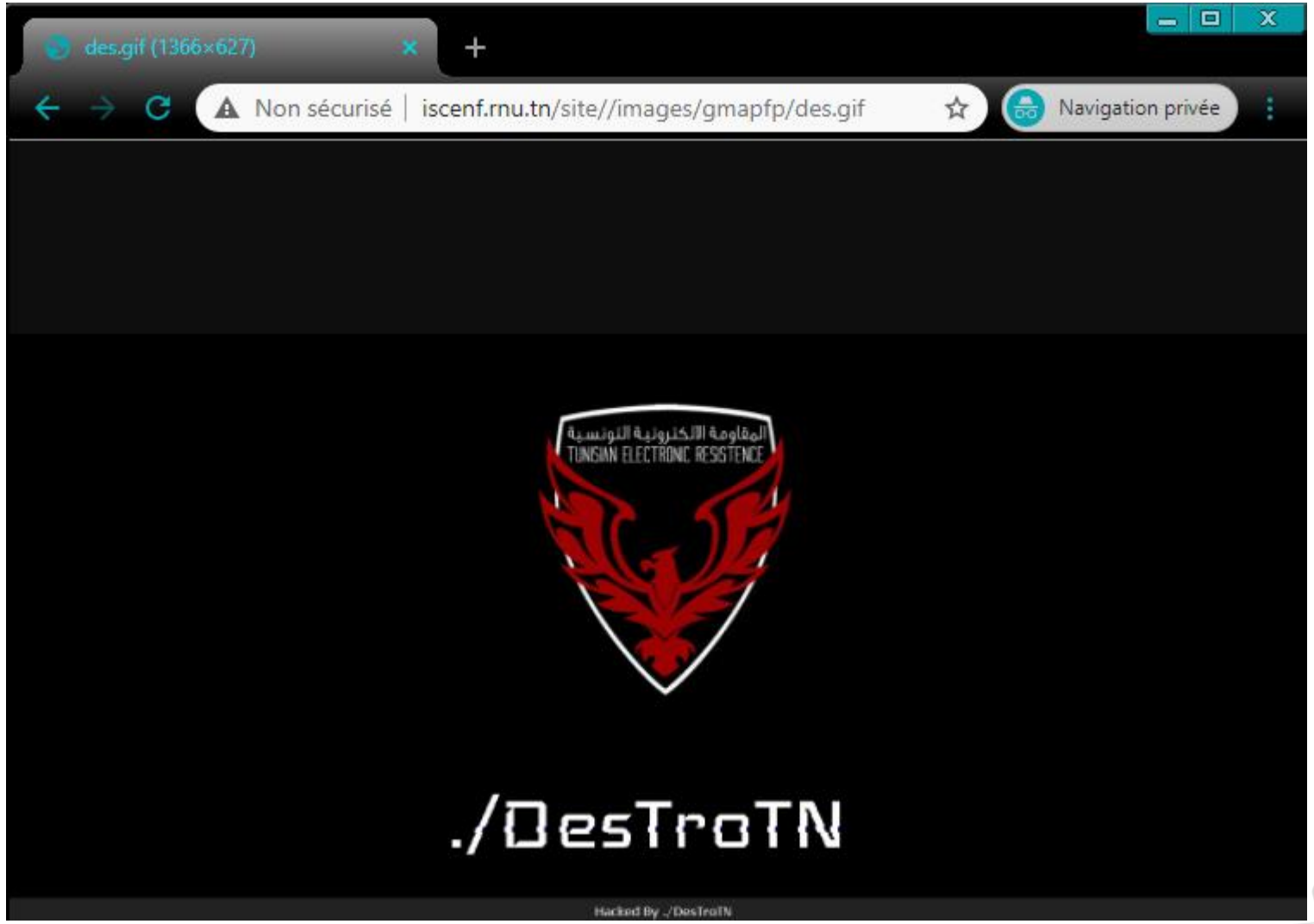

Société Nationale de Distribution des Pétroles AGIL
21 h ·
تعلن الشركة الوطنية لتوزيع البترول عن فتح باب التعيينات في جميع مقار وحقول الشركة المنتشرة .
لجميع المؤهلات ، وللجنسين لشغل الوظائف التالية :
" مهندسي كفاءة - خدمات أمنية - عمالة مواقع - وخدمات مكتبية للأناث "
رجاء القيام بالتسجيل في الأستمارة الإلكترونية بالضغط ع الصورة بالأسفل
وذلك إلتزاما منا بالحرص علي منع التجمعات في هذه الاوقات الصعبة .
بالتوفيق للجميع .
FAKE
ELU PRODUIT
DE L'ANNÉE 2019
5EECD69E03AC3.SITE123.ME
الشركة الوطنية لتوزيع البترول - أهلا بكم في بوابة التقديم لتعينات الشركة الوطنية لتوزيع البترول
235
39 commentaires 120 partages


From: POSTE.TN <Chris.Kennedy@multicraft.com>
Date: Thu, May 7, 2020, 6:22 PM
Subject: POSTE: Dépot 200 DT
To: <[redacted]@gmail.com>
Engagement de la poste Tunisie envers nos clients

FAKE
البريد التونسي
LA POSTE TUNISIENNE
Cher client,
Nous vous informons que vous venez de recevoir un paiment de 200DT de la subvention d'aide sociale.
Vous devez vérifier vos informations afin de pouvoir recevoir le paiment.
Vérifier

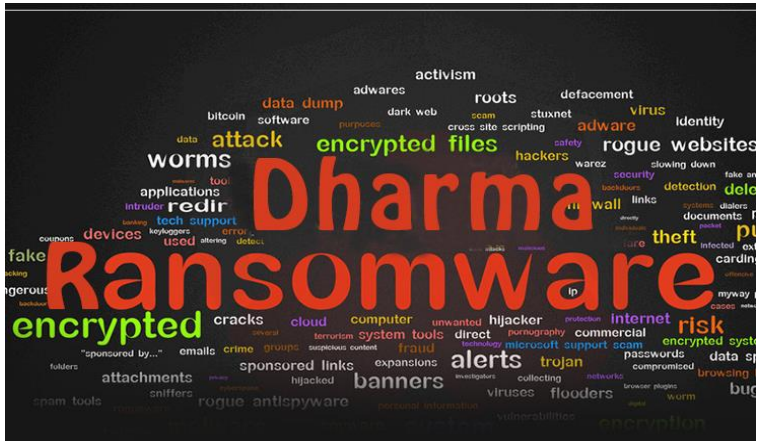
PHISHING

DEFACEMENT


des.gif (1366×627)
Non sécurisé | iscenf.rnu.tn/site//images/gmapfp/des.gif
Navigation privée
المقاومة الالكترونية التونسية
TUNISIAN ELECTRONIC RESISTENCE
./DesTroTN
Hacked By ./DesTroTN

Famille: VoidCrypt
Extension: .void
Décrypteur: NON

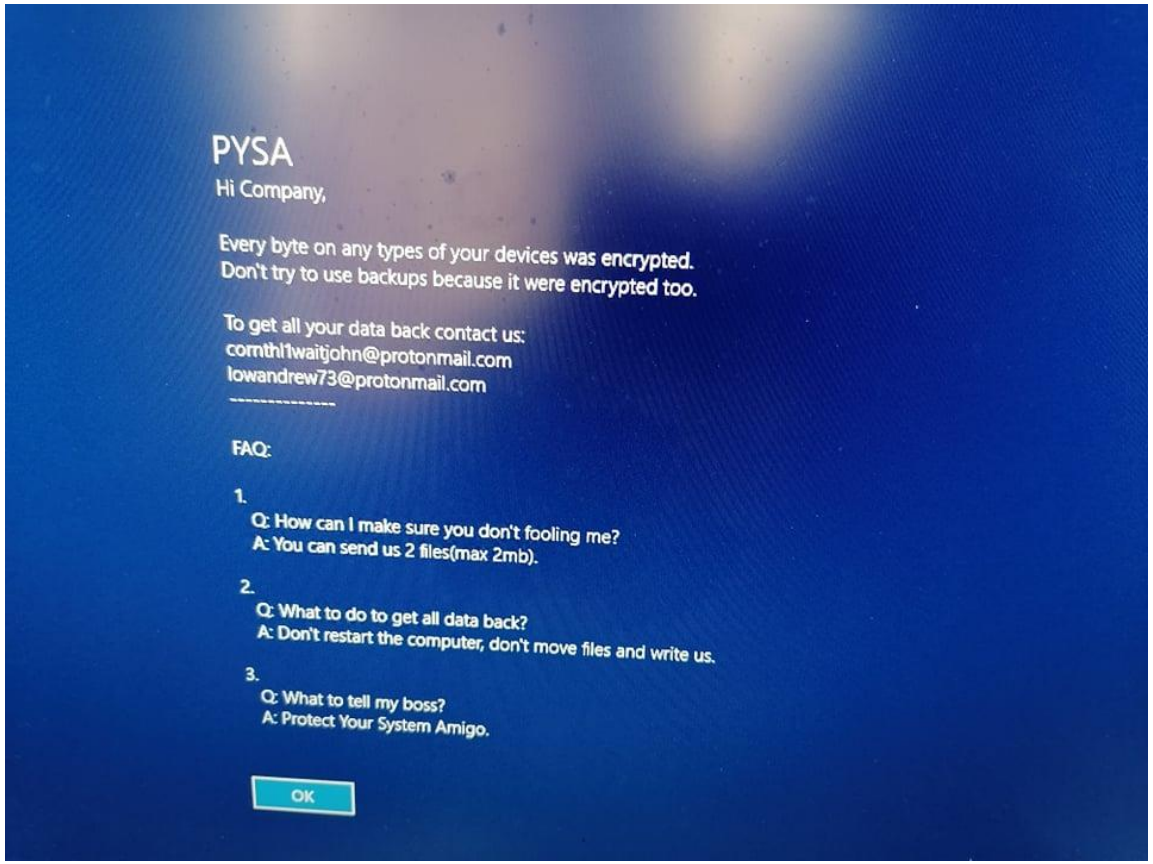
Famille: Mespinoza
Extension:.pysa
Décrypteur: NON

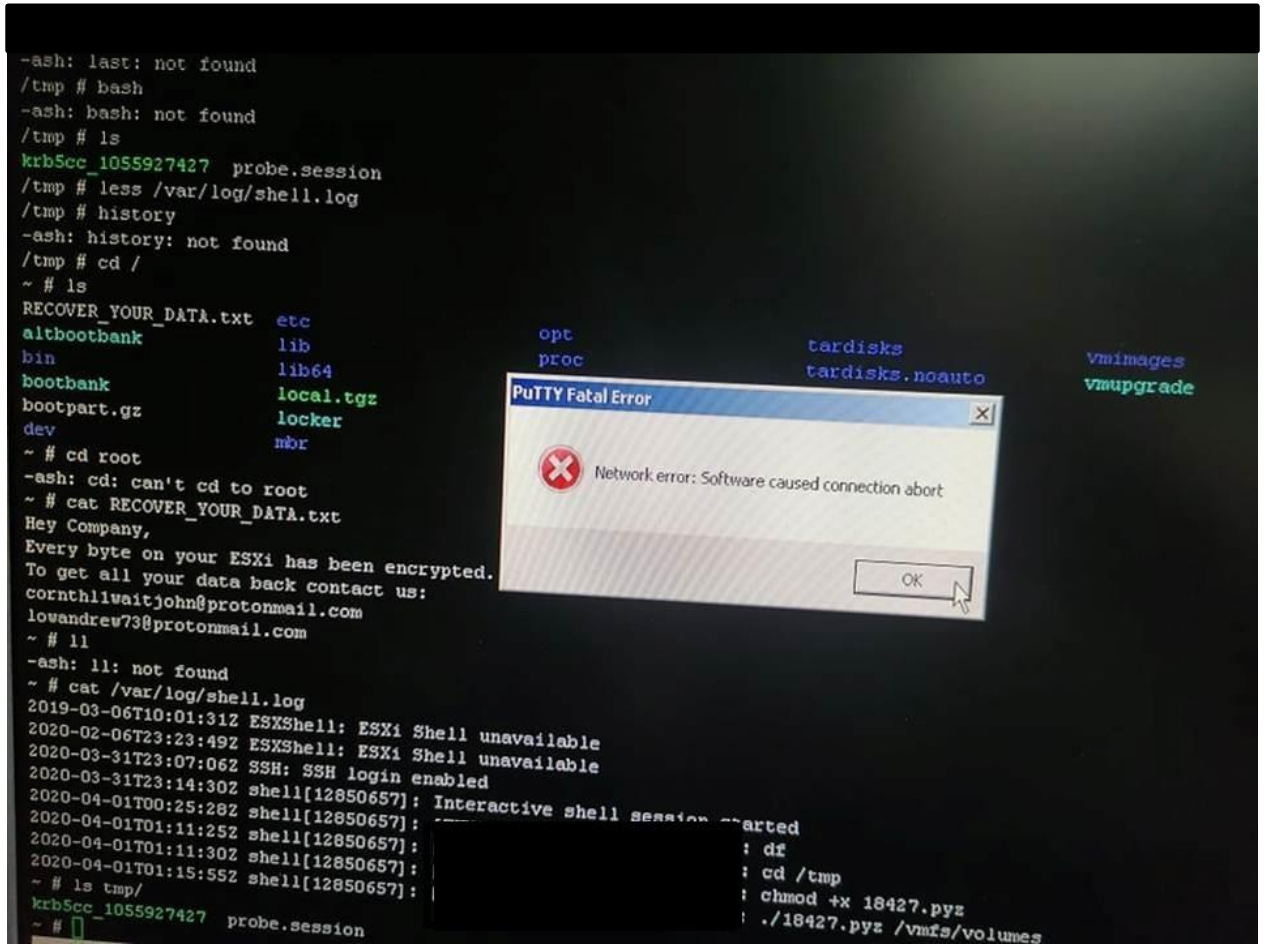


Famille: Dharma
Extension: .ncov
Décrypteur: NON

DJVU
RANSOMWARE

Famille: DJVU
Extension: .opqz
Décrypteur: NON



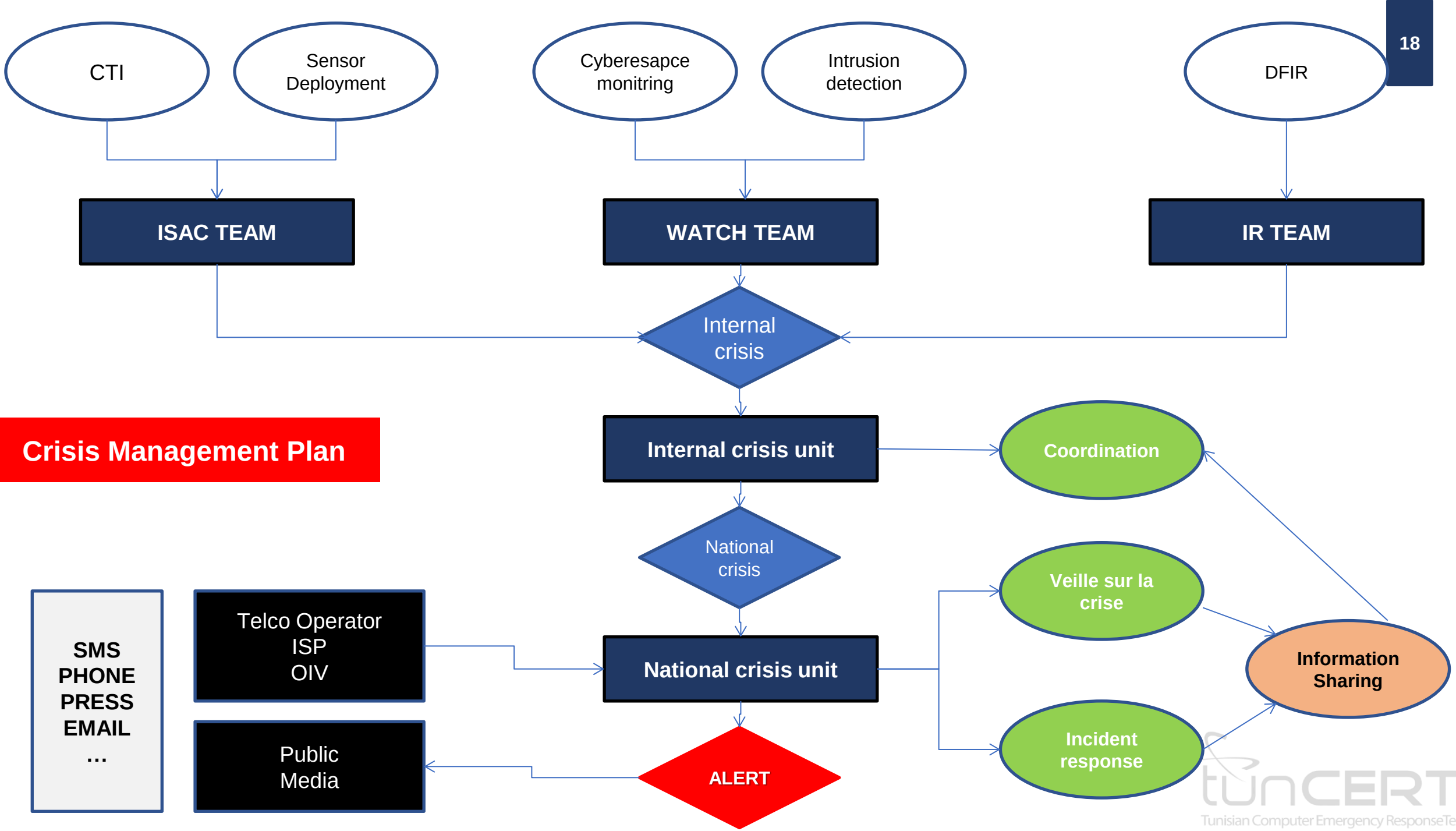


ATTAQUE PAR LE RANSOMWARE MESPINOZA/PYSA

tunCERT
Tunisian Computer Emergency ResponseTeam

Crisis Management Plan

Crisis Management Plan



Crisis Communication during COVID-19

ALERTE


Alerte - Ransomware
"Pysa" descendant du ransomware "Mespinoza"
الوكالة الوطنيّة للسّلامة المعلوماتيّة
Agence Nationale de la Sécurité Informatique
Alerte aux ransomwares
tunCERT
Tunisian Computer Emergency ResponseTeam

ALERTE


الوكالة الوطنية للسلامة المعلوماتية
Agence Nationale de la Sécurité Informatique
Alerte au phishing
tunCERT
Carrefour Tunisia
كارفور
بتمناكم
رمضان مبروك


الوكالة الوطنية للسلامة المعلوماتية
Agence Nationale de la Sécurité Informatique
Alerte aux e-mails de phishing
tunCERT
De : © [redacted] [mailto:[info@hybyhy.live]
Envoyé : vendredi 17 avril 2020 10:44
À : [redacted]
Objet : La boîte aux lettres est bloquée!
(La boîte aux lettres est bloquée!)
ID utilisateur: [redacted]
Courriel de l'utilisateur: [redacted]
Vos e-mails sortants sont désactivés.
Vos e-mails entrants seront également désactivés.
Et votre compte de messagerie sera bientôt fermé.
Arretez ce processus ici
Vous pouvez arrêter cet arrêt ci-dessus,
Si aucune mesure n'est prise pour y mettre fin immédiatement.


الوكالة الوطنية للسلامة المعلوماتية
Agence Nationale de la Sécurité Informatique
SCAM
Alerte aux scams
et au cyber-harcèlement
tunCERT
next Twenty-four hrs, or I will make sure you that you live out of
t I know nearly anything concerning you. Your current fb contact
from previous 184 days.
tage, which brings me to the main motive why I am writing this pa
: porn online sites, my spyware was triggered inside your person
pure play simply by triggering your web cam.
y haha)
I 'm messing around, just reply proof and I will be forwarding t
rKers, boss, parents (I don't know! My software will randomly sele
's eyes again after it" I question that...
way.
negotiable offer.
he listed below address:
hove * from it]
w to acquire bitcoin. Do not waste my valuable time)
let's call it that"). Immediately after that, I will go away and ne
ncerning you. You may very well proceed living your current nor
gain as soon you read this email. I have an special code that will


الوكالة الوطنية للسلامة المعلوماتية
Agence Nationale de la Sécurité Informatique
Alerte aux e-mails de phishing
tunCERT
L'equipe Webmail 'In !®
Cher(e) Membre,
Suite au renouvellement automatique de votre abonnement® le serveur Webmail MG ®! a rencontré certaines erreurs ne permettant pas de répertorier votre adresse. Nous vous informons que vous ne pourrez plus accéder à votre compte, ni utiliser les profils

User Guide

1. Liste des ressources et des formations en ligne gratuites
2. Sélection des outils de visioconférence payants et open source
3. Sélection des solutions de sécurité commerciales gratuites
4. Guide d’utilisateur pour l’installation et la configuration d’outils de télétravail
5. Guide pour la protection de l’identité numérique

Coordination Nationale

TunCERT - Tunisian Computer Emergency Response Team

Cher partenaire,

En plus des circonstances que nous vivons avec la **crise Covid19** et suite aux **dernières attaques massives par ransomwares** qui cribleraient nos **établissements** dans **tous les secteurs**, l'**Agence Nationale de la Sécurité Informatique - ANSI** requiert la **vigilance** et la **coordination** de **nous tous** afin d'avoir ensemble une **meilleure visibilité** et **bien réagir** pour **réduire les impacts d'éventuelles attaques cybernétiques** sur notre **cyberespace national** surtout avec l'usage incrémental de **télétravail**, ...

Pour toute **coordination** suite aux **événements/incidents** de cybersecurité, l'**ANSI** souhaite avoir **votre feedback** et **restera impérativement à votre disposition** au moyen des contacts suivants :

- **Email (s)**: incident@ansi.tn / faille@ansi.tn / ansi@ansi.tn / cert-tcc@ansi.tn;
- **Tel** : 71843200.

Merci d'avance pour votre collaboration patriotique responsable et que DIEU nous protège.

Agence Nationale de la Sécurité Informatique.
Adresse: 49, Av Jean Jaurès, 1000 Tunis.
Tel: 71 843 200 | **Fax**: 71 846 363

Coordination Nationale

ATHENA vous accompagne dans la sécurisation de votre SI

La crise sanitaire due au COVID-19 a bouleversé le fonctionnement de toutes les organisations et a augmenté leur niveau d'exposition aux cyberattaques, notamment, en raison de :

- La mise en place massive et dans l'urgence du télétravail,
- La digitalisation non contrôlée et la mise en place dans l'urgence de services en ligne,
- La focalisation des équipes informatiques sur les opérations d'administration et d'exploitation au détriment des opérations de supervision de la sécurité.

Le secteur financier reste l'un des secteurs les plus ciblés et touchés par les cyberattaques en ce moment. Les institutions financières doivent alors renforcer leur cyber résilience. ATHENA, première et unique entreprise tunisienne certifiée PCI DSS QSA et reconnue en tant que « SWIFT CSP Assessment Provider » et « SWIFT Cyber Security Service Provider » accompagne toutes les organisations dans le renforcement de la résilience de leur infrastructure aux cyberattaques. Quelques exemples de nos services :

- Investigation
- Audit (Audit flash, pentest, audit de conformité, etc.)
- Conformité PCI DSS
- Conformité SWIFT
- Security Opérations Center / Services Managés
- SMSI, PSSI, Analyse de risques
- PCA
- Intégration de solutions de sécurité
- Sensibilisation.

ATHENA
the way to excellence

PCI Security Standards Council
QUALIFIED SECURITY ASSESSOR™

Nos consultants sont bien équipés pour travailler à distance

https://www.athena-experts.com/
contact@athena-experts.com

Coordination Nationale

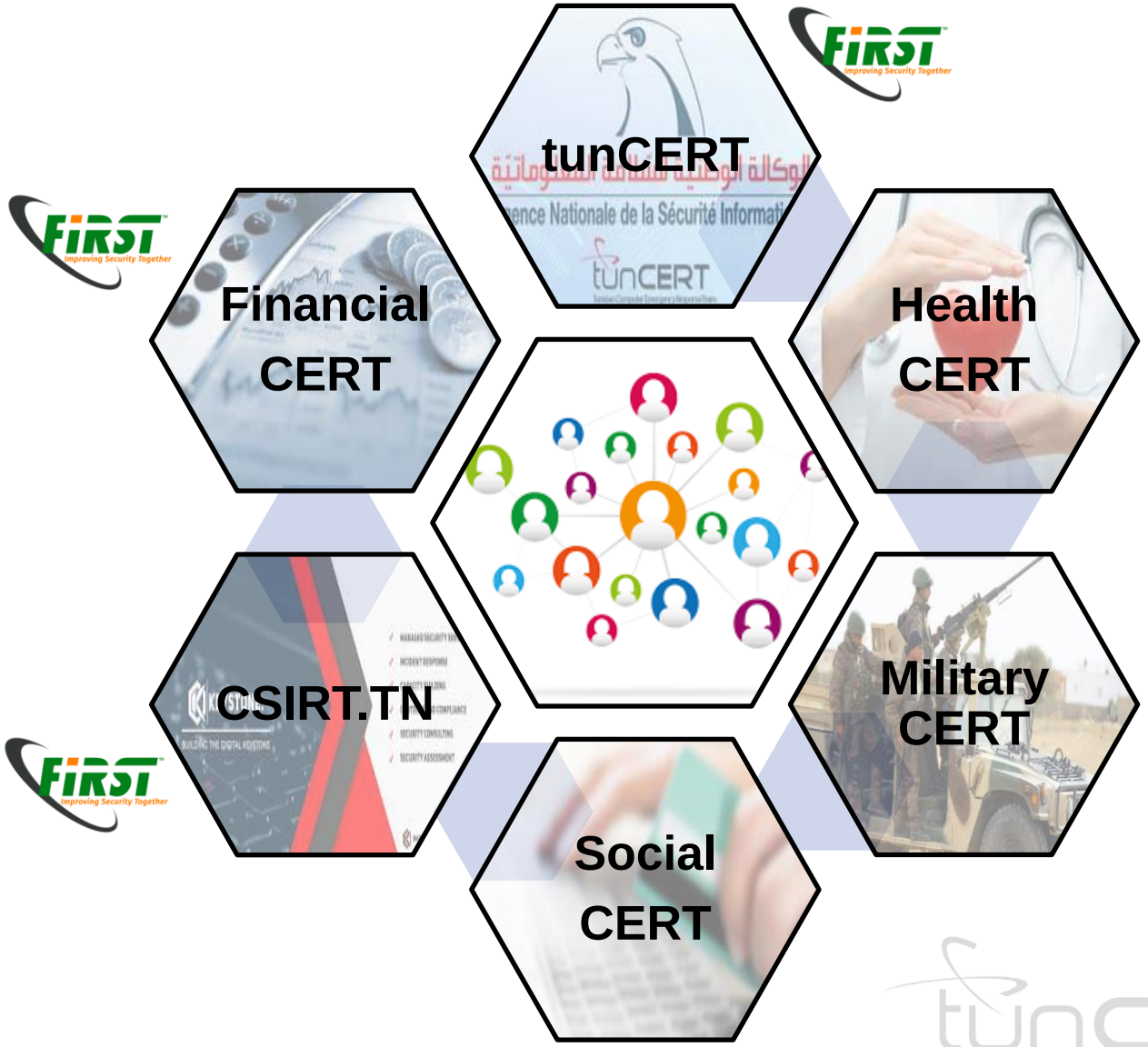
KEYSTONE.

COVID-19: Keystone fournit gratuitement un service enligne de conseil en cybersécurité pour les entreprises tunisiennes qui veulent mettre en œuvre le télétravail.

Comment mettre en œuvre le télétravail en toute sécurité?
Un guide pour les petites entreprises.
https://www.keystone.tn/guide/teletravail.pdf

CERT TN Coalition

- 1 CERT National
- 4 CERT Sectoriel
- 1 CERT Privé



الوكالة الوطنيّة للسّلامة المعلوماتيّة
Agence Nationale de la Sécurité Informatique

tunCERT

Zerologon

CVE-2020-1472

Score CVSS : 10

C'est quoi ?

Vulnérabilité d'élévation de privilèges dans NetLogon.

Par qui ?

Exploitable par quiconque peut établir une connexion TCP avec un serveur Active Directory vulnérable.

Quels risques ?

Usurper l'identité de n'importe quel ordinateur sur un réseau.

Modifier le mot de passe d'un ordinateur sur l'Active Directory

Active Directory

Versions affectées

Windows Server 2008 R2
Windows Server 2012
Windows Server 2012 R2
Windows Server 2016
Windows Server 2019
Windows Server, version 1903
Windows Server, version 1909
Windows Server, version 2004

Recommandations

- Mettre à jour le système, appliquer le correctif publié par Microsoft le 11 août 2020.
- Mettre à jour les signatures de votre firewall / IDS
- Surveiller les journaux d'accès à l'AD
- Bloquer l'accès au serveur AD depuis Internet
- Garder une copie de sauvegarde de votre serveur AD
- Contacter l'ANSI en cas d'incident: incident@ansi.tn

incident@ansi.tn
saher@ansi.tn