RANSOMWARE

Comment se protéger ?

SMII Mondher (@smii_mondher)
Cyber Security Analyst | ISAC Team

الوكالة الوطنيّة للسّلامة المعلوماتيّة
Agence Nationale de la Sécurité Informatique

Agence Nationale de la Sécurité Informatique

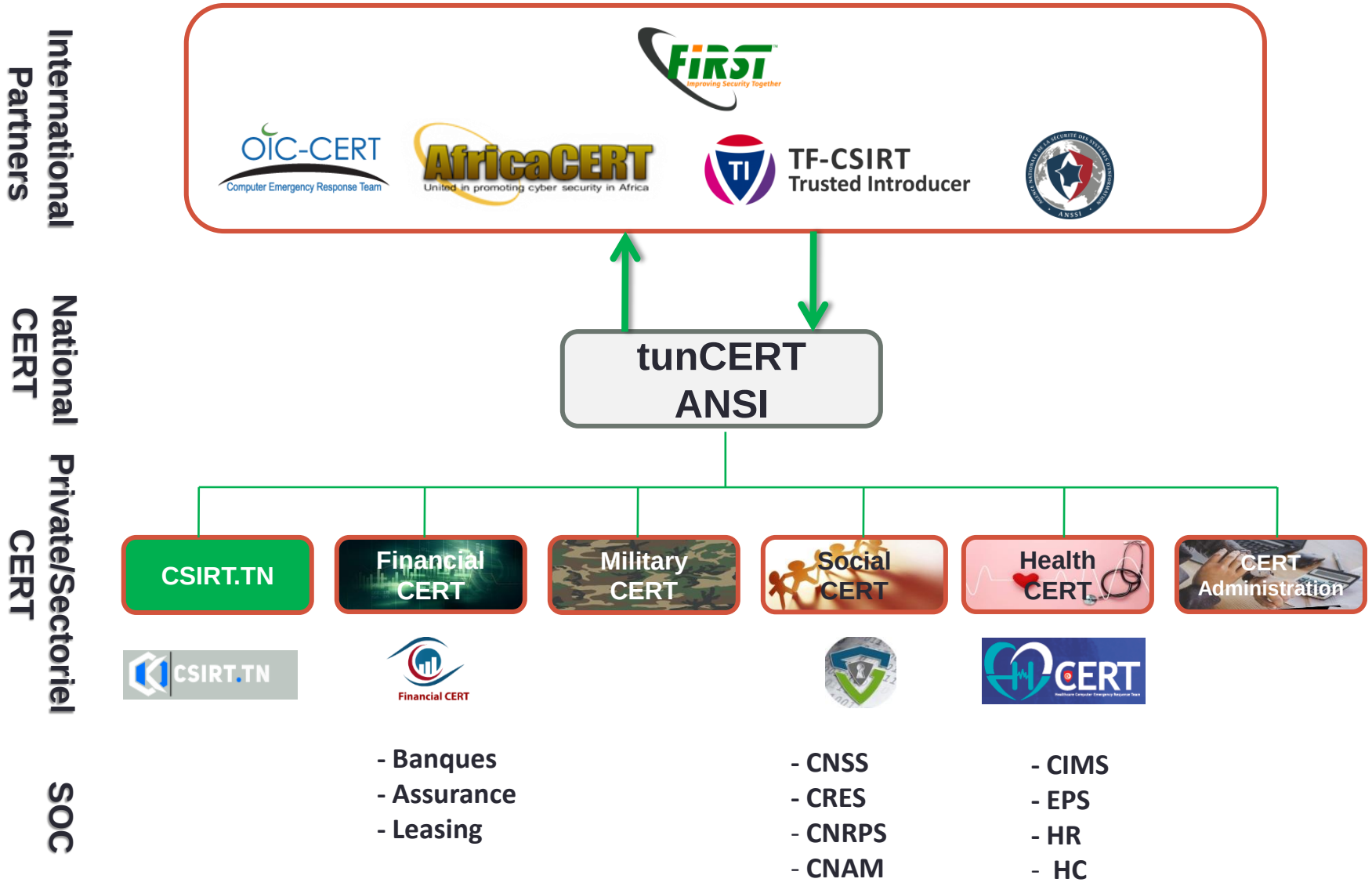
- **Renforcer la sécurité du cyber espace national contre les risques et les menaces cybernétiques.**
- **Renforcer la protection des Systèmes d'informations nationales.**
- **Favoriser le développement d'un cadre juridique et règlementaire adéquat.**
- **Instaurer une culture cybersécurité de haut niveau.**
- **Instaurer un partenariat avec les structures académiques de recherche et le secteur privé.**

Audit	Sensibilisation	Evaluation	ISAC	CSIRT	SOC/A&W

Acteurs cybersécurité

- Opérateurs Télécom (Tunisie Télécom, Orange et Ooredoo)
- Fournisseurs de services Internet (Topnet, Globalnet, Hexabyte, Bee, CCK, CIMS, CIMF, CNTE, IRESA, …)
- Centre National de l'Informatique CNI
- Agence Nationale de la sécurité Informatique
- INPDP
- CERT Sectoriels / privés
- Ministère / End Users …

Vision


International Partners
National CERT
Private/Sectoriel CERT
SOC
FIRST
Improving Security Together
OIC-CERT
Computer Emergency Response Team
AfricaCERT
United in promoting cyber security in Africa
TF-CSIRT
Trusted Introducer
tunCERT
ANSI
CSIRT.TN
Financial CERT
Military CERT
Social CERT
Health CERT
CERT Administration
CSIRT.TN
Financial CERT
CERT
- Banques
- Assurance
- Leasing
- CNSS
- CRES
- CNRPS
- CNAM
- CIMS
- EPS
- HR
- HC

https://ncss.tunisia.gov.tn/

أهداف الإستراتيجيـــــــــــة

تهدف هذه الإستراتيجيّة إلى:

قيادة الفضاء السّيبرني الوطني وإدارته، من خلال تحديد الأطراف المكلّفة بتعزيز العمل المشترك بين كل المتداخلين في المجال ودعم التّنسيق بينها.

التوقّي من التّهديدات السّيبرنية والصّمود، من خلال تعزيز القدرات الوطنيّة ودعم التّوعية وحماية البُنَى التّحتيّة المعلوماتيّة الحيويّة.

دعم الثّقة الرّقمية، من خلال وضع الآليات والإجراءات الضرورية للغرض.

تحقيق الرّيادة في المجال الرّقمي، من خلال تطوير بيئة رقميّة آمنة وتحقيق الأسبقيّة إقليميا ودوليا.

التّعاون الدّولي، من خلال إرساء مقاربة متوازنة بين التعاون الدولي وضمان المصالح العليا للدّولة

الجمهورية التونسية
رئاسة الحكومة
تونس في 05 2020
منشور عدد 24
من السيد رئيس الحكومة
إلى
السيدات والسادة الوزراء وكتاب الدولة والولاة ورؤساء المؤسسات والمنشآت العمومية
الموضوع: حول تدعيم إجراءات السلامة المعلوماتية بالهياكل العمومية.
المراجع: - القانون عدد 5 لسنة 2004 المؤرخ في 3 فيفري 2004 المتعلق بالسلامة المعلوماتية.
- الاستراتيجية الوطنية للأمن السيبرني.
- المنشور عدد 19 لسنة 2007 المؤرخ في 17 أفريل 2007 المتعلق بتدعيم إجراءات السلامة المعلوماتية بالهياكل العمومية.

الجمهورية التونسية
رئاسة الحكومة
تونس في 05 2020
منشور عدد 23
من السيد رئيس الحكومة
إلى
السيدات والسادة الوزراء وكتاب الدولة والولاة ورؤساء المؤسسات والمنشآت العمومية
الموضوع: حول إحكام التصرف في الصفحات والحسابات الرسمية بشبكات التواصل الاجتماعي الراجعة بالنظر للهياكل العمومية.
المراجع: - القانون الأساسي عدد 22 لسنة 2016 المؤرخ في 24 مارس 2016 المتعلق بالحق في النفاذ إلى المعلومة
- القانون عدد 5 لسنة 2004 المؤرخ في 3 فيفري 2004 المتعلق بالسلامة المعلوماتية.

La Présidence du gouvernement tunisien a communiqué deux circulaires relatives aux nouvelles mesures à adopter pour améliorer le niveau de la cybersécurité des SI gouvernementaux et des entreprises publiques.

Circulaire n° 23 - du 05 novembre 2020, relative à la gestion des comptes officiels des entreprises publiques sur les réseaux sociaux.

Circulaire n° 24 - du 05 novembre 2020, relative à l'amélioration et l'optimisation des mesures de sécurité informatique au niveau des entreprises publiques.

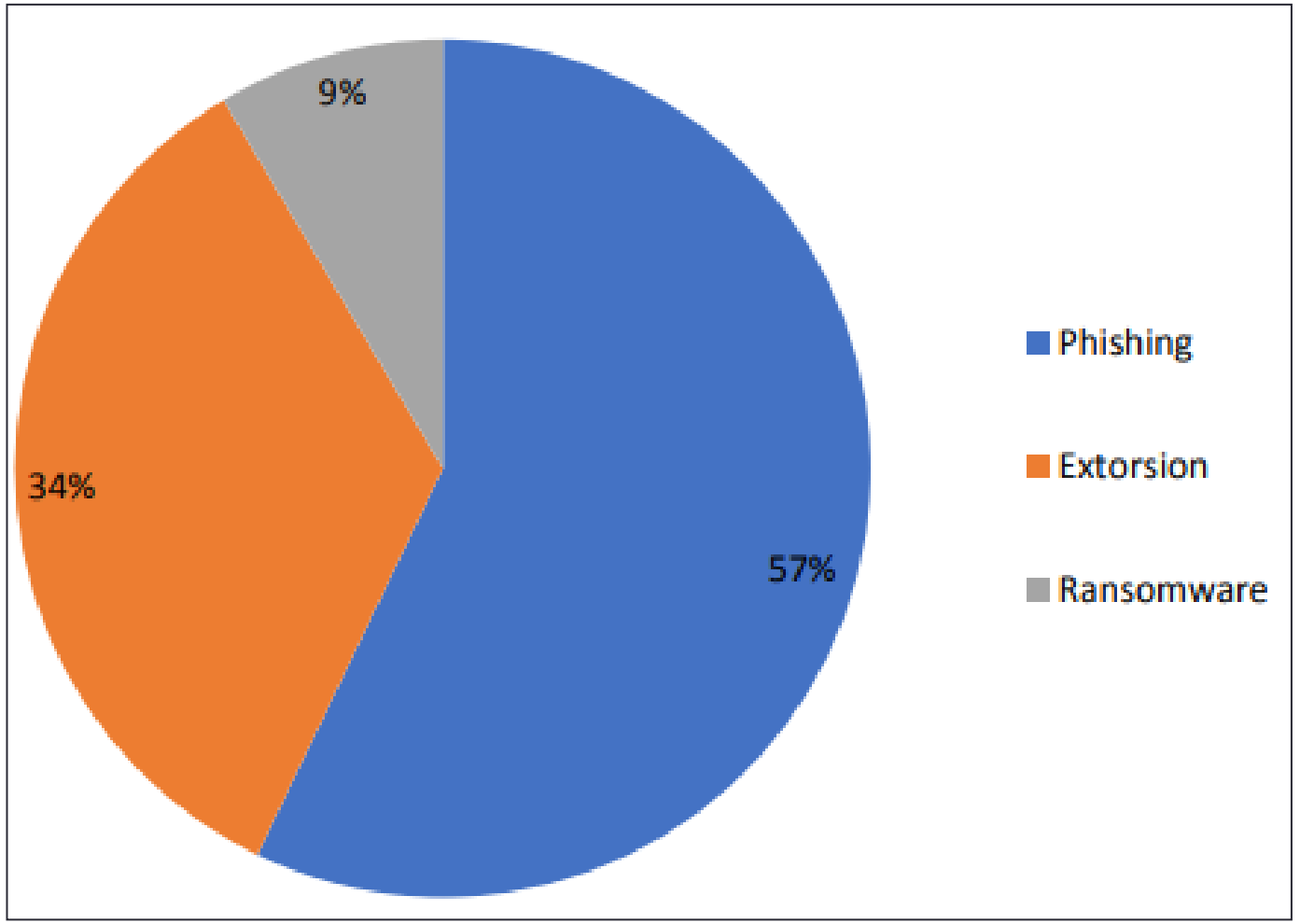
Covid19

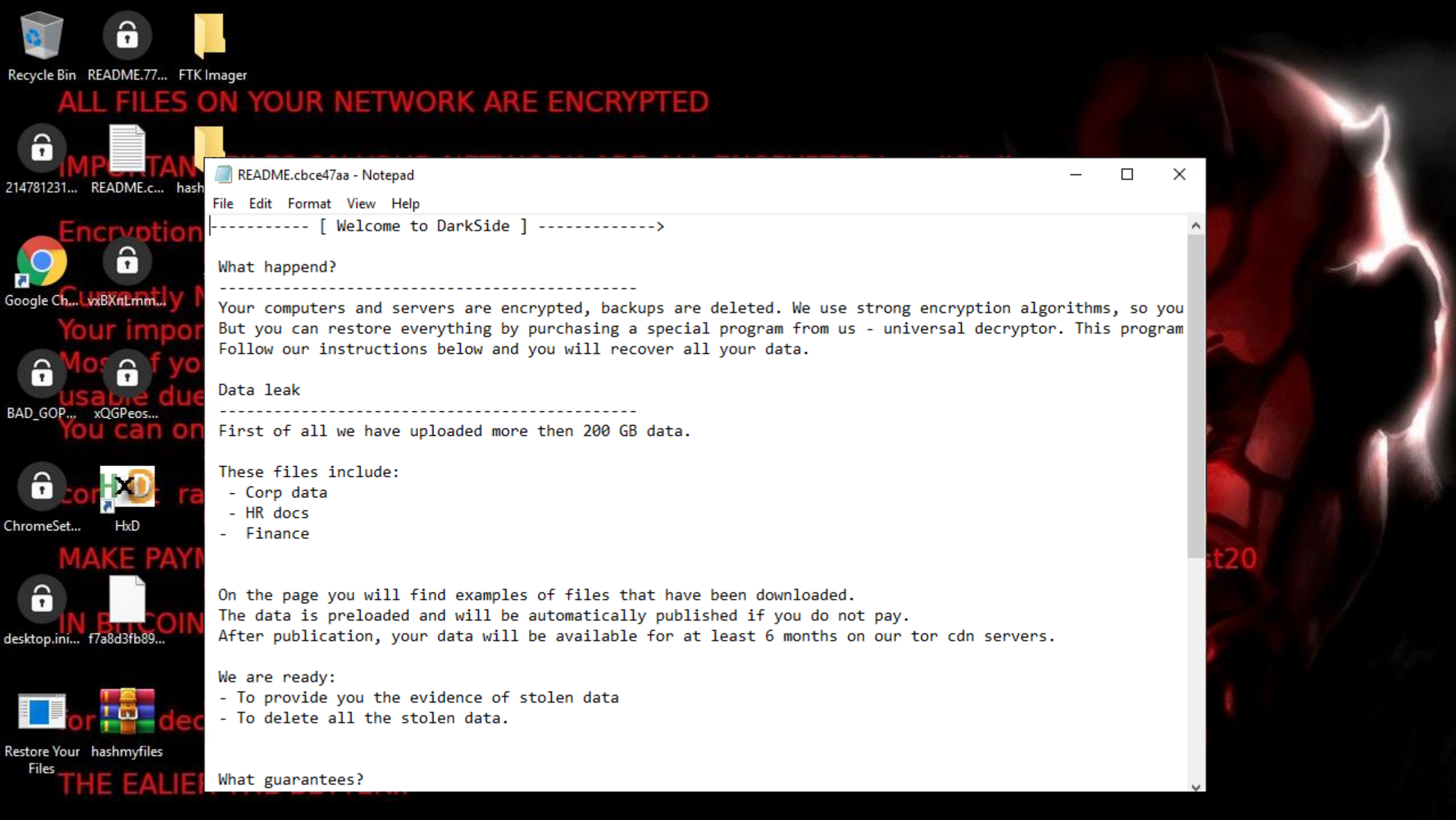
phishing

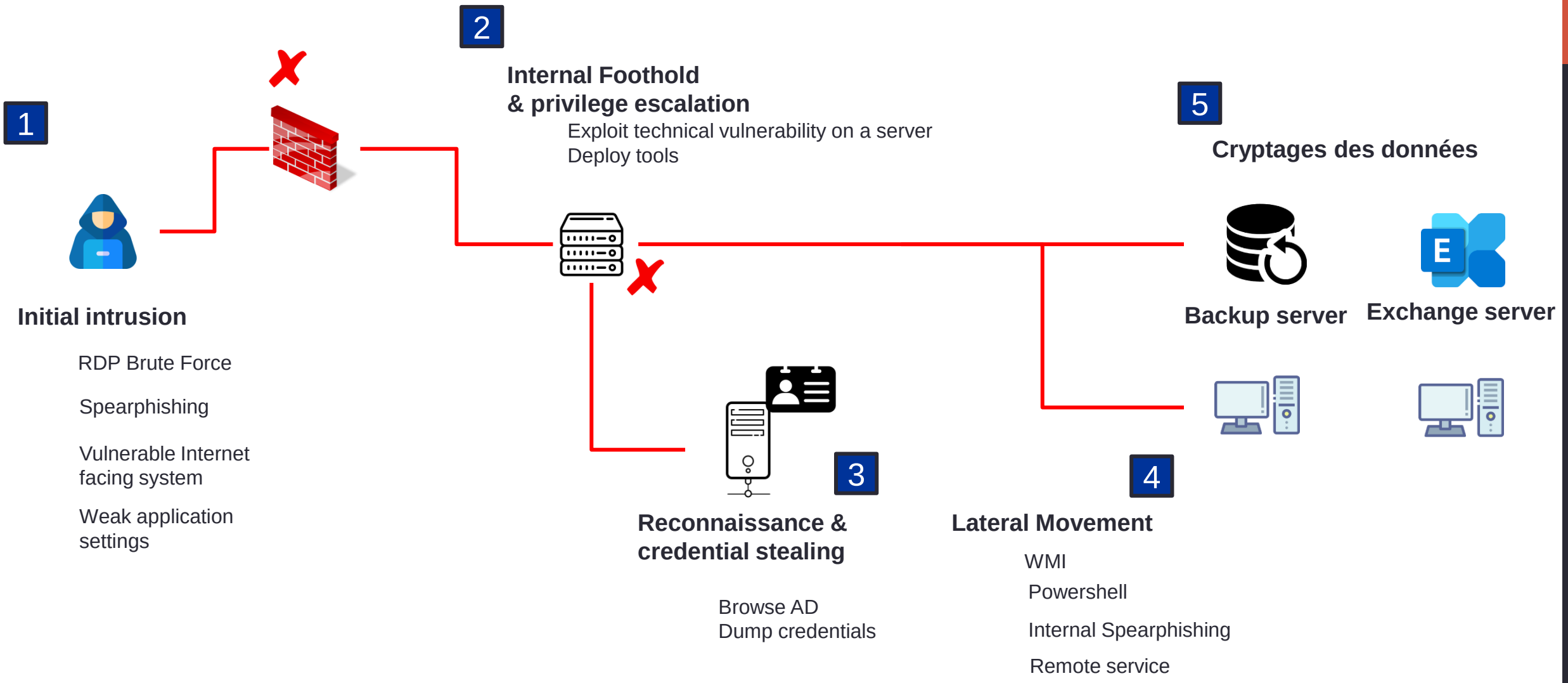
Ransomware

Lien malicieux

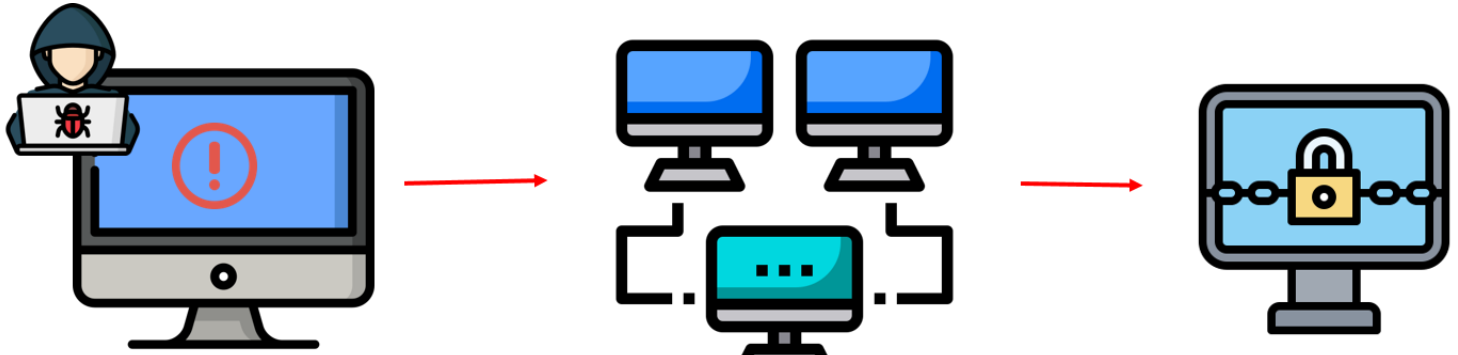
Covid19



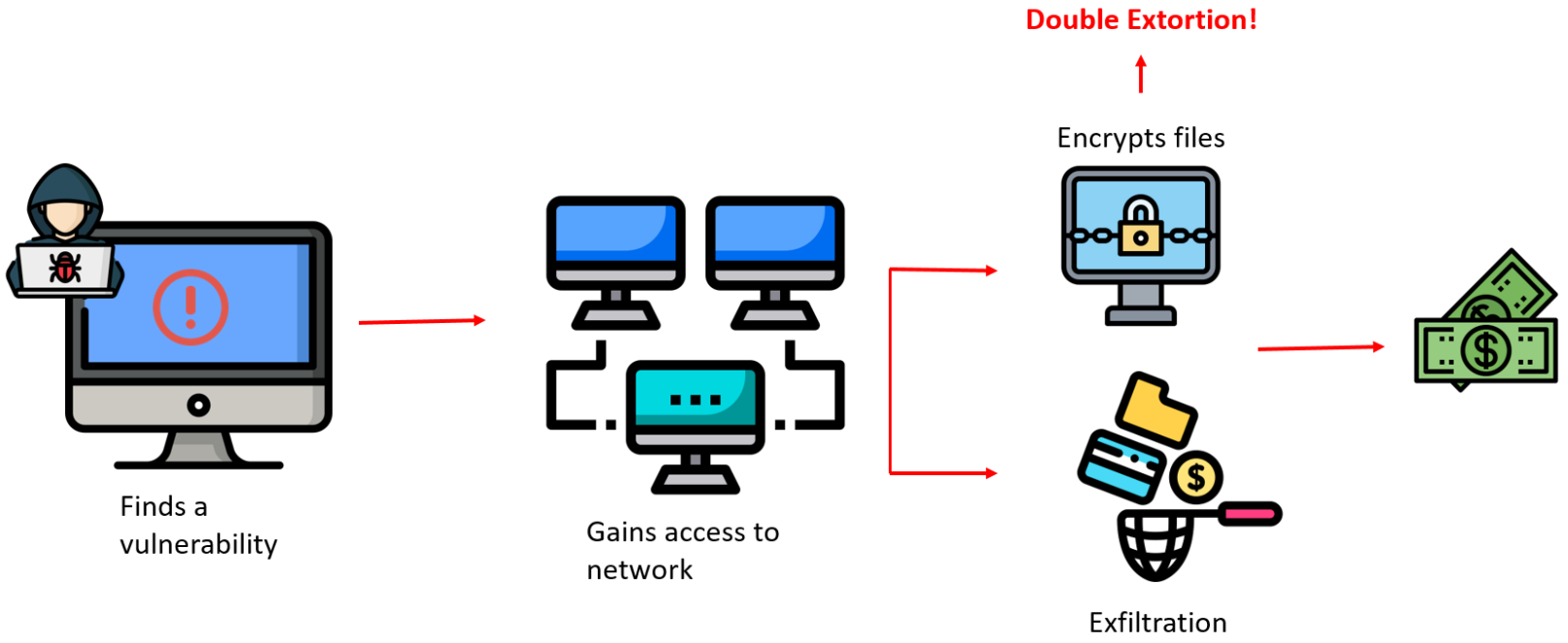

Recycle Bin
README.77...
FTK Imager
ALL FILES ON YOUR NETWORK ARE ENCRYPTED
214781231...
README.c...
hash
Encryption
Google Ch...
vxBXnLmm...
Currently
Your impor
BAD_GOP...
xQGPeos...
You can on
ChromeSet...
HxD
MAKE PAYM
desktop.ini...
f7a8d3fb89...
IN BITCOIN
Restore Your Files
hashmyfiles
THE EALIE
README.cbce47aa - Notepad
File Edit Format View Help
---------- [Welcome to DarkSide] ------------>
What happend?
Your computers and servers are encrypted, backups are deleted. We use strong encryption algorithms, so you
But you can restore everything by purchasing a special program from us - universal decryptor. This program
Follow our instructions below and you will recover all your data.
Data leak
First of all we have uploaded more then 200 GB data.
These files include:
- Corp data
- HR docs
- Finance
On the page you will find examples of files that have been downloaded.
The data is preloaded and will be automatically published if you do not pay.
After publication, your data will be available for at least 6 months on our tor cdn servers.
We are ready:
- To provide you the evidence of stolen data
- To delete all the stolen data.
What guarantees?


1
Initial intrusion
RDP Brute Force
Spearphishing
Vulnerable Internet facing system
Weak application settings
2
Internal Foothold & privilege escalation
Exploit technical vulnerability on a server
Deploy tools
3
Reconnaissance & credential stealing
Browse AD
Dump credentials
4
Lateral Movement
WMI
Powershell
Internal Spearphishing
Remote service
5
Cryptages des données
Backup server
Exchange server

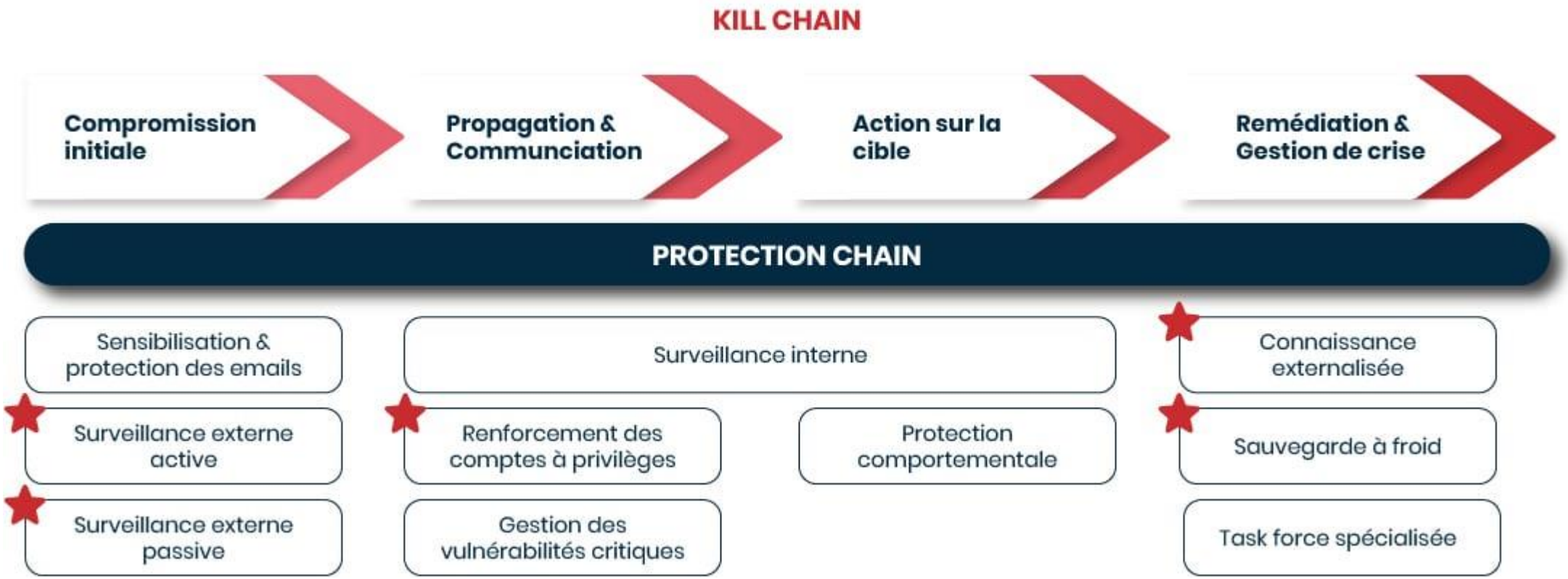
It’s not just encryption anymore, it’s double extortion …



It’s not just encryption anymore, it’s double extortion …



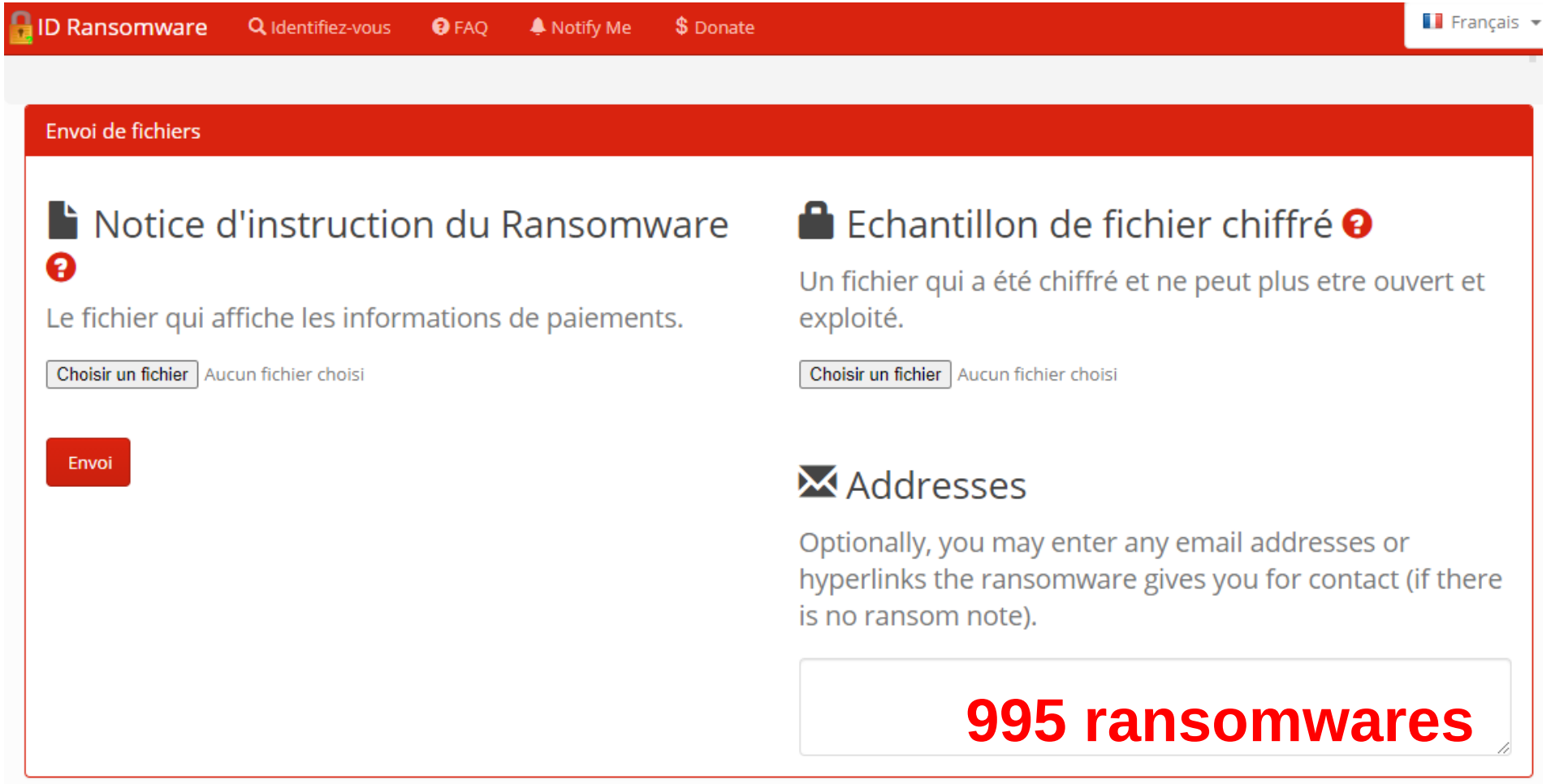
Protection Chain



Bonne pratique

- Sensibilisation des collaborateurs
- Limitation des droits administrateurs sur les postes et dans le réseau
- Utilisation d’une solution de sécurité Endpoint multicouche à administration centralisée
- Filtrage Antispam et antivirus sur la passerelle de messagerie
- Désactivation de l’exécution automatique des macros dans les logiciels de bureautique
- Désactivation du Remote powershell Disable-PSRemoting
- Sauvegardes régulières des données
- Mises à jour régulières des programmes installés et des systèmes d’exploitation des clients du réseau
- Collecte et analyse des journaux windows

ID Ransomware



https://id-ransomware.malwarehunterteam.com/

Knowing is half the battle

GI Joe

Adresse : 49, avenue Jean Jaurès, 1000 Tunis

Tél : 71 846 020 / 71 843 200

Fax : 71 846 363

incident@ansi.tn **saher@ansi.tn** **audit@ansi.tn**

الوكالة الوطنيّة للسّلامة المعلوماتيّة

Agence Nationale de la Sécurité Informatique