La Cyber Résistance Ukrainienne

La maitrise du risque numérique et la Gouvernance

Bernard BARBIER

@barbier_bernard

linkedin.com/in/bernard-barbier-52538459

bernard.barbier@bbcyber.fr

Ingénieur de l'École Centrale de Paris 1976,

Master en Physique des Plasmas

Membre de l'académie des technologies

Président de BBCyber SAS

-2014-2018 : CAPGEMINI, responsable de la cybersécurité du groupe, responsable de la cyberdéfense interne pour toutes les entités CAPGEMINI dans le monde. 55 pays, 210 000 personnes

-2006-2013 : Directeur technique à la DGSE (équivalent du directeur de la NSA aux États-Unis), en charge du renseignement technique français : SIGINT, IMINT, Cyber Int, cyber opération et cyberdéfense

-2003-2006 : Directeur du LETI (Minatec Grenoble), l'un des meilleurs laboratoires de recherche au monde, dans le domaine de la nanoélectronique et des nanotechnologies (1500 chercheurs)

-2000-2003 : Directeur des Systèmes d'information du Commissariat à l'Energie Atomique (CEA)

PLAN

- La Cyber Résistance Ukrainienne
- Une situation alarmante, l'espionnage
- Bon Risk Appétit, apprendre à gérer le risque numérique

La stratégie cyberdéfense de l'Entreprise

•La Cyber Résistance Ukrainienne

27 JUIN 2017-NOTPETYA: une surprise stratégique

June 27

— **22.14:** Maersk confirms cyberattack, sets out initial response
— **21.46:** Maersk updates holding statement
— **21.03:** *MeDoc denies responsibility for attacks*
— **19.46**: *Ukraine police confirm accounting software company MeDoc is infected by NotPetya*
— **18.15**: *German email provider Posteo confirms it blocked ransom email address*
— **16.12**: *Kapersky says NotPetya wiper destroys data, affects ~2,000 organisations*
— **14.02**: *Symantec confirms use of Petya ransomware for attacks*
— **14.16:** Maersk updates holding statement
— **13.21**: Maersk publicly confirms IT systems are down
— **11.30**: *Ukraine Central Bank confirms attack on IT systems*
— **04.00**: *Ransomware attack on Ukrainian banks, power companies etc*

Timings are GMT+1

•La Cyber Résistance Ukrainienne

-NOTPETYA: une surprise stratégique

The weapon's target was Ukraine. But its blast radius was the entire world. "It was the equivalent of using a nuclear bomb to achieve a small tactical victory," Bossert says.

The release of NotPetya was an act of cyberwar by almost any definition—one that was likely more explosive than even its creators intended. Within hours of its first appearance, the worm raced beyond Ukraine and out to countless machines around the world, from hospitals in Pennsylvania to a chocolate factory in Tasmania. It crippled multinational companies including Maersk, pharmaceutical giant Merck, FedEx's European subsidiary TNT Express, French construction company Saint-Gobain, food producer Mondelēz, and manufacturer Reckitt Benckiser. In each case, it inflicted nine-figure costs. It even spread back to Russia, striking the state oil company Rosneft.

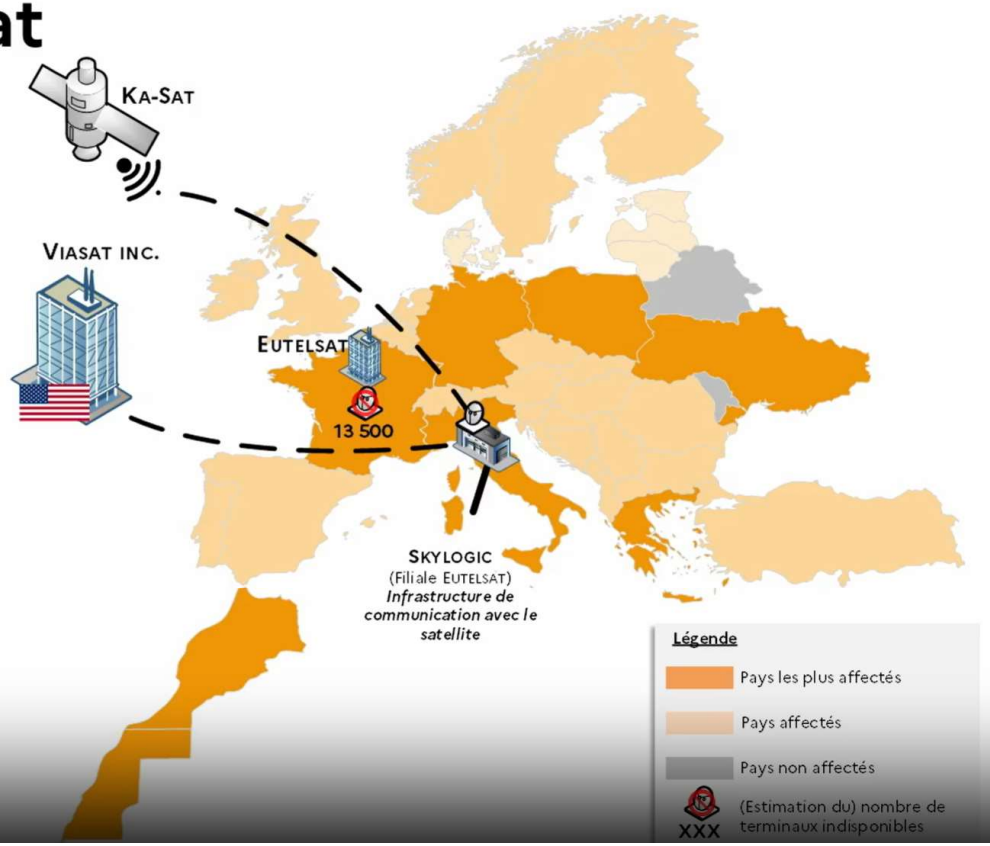
The result was more than $10 billion in total damages, according to a White House assessment confirmed to WIRED by former

La Cyber Résistance Ukrainienne

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

Sabotage : Ka-Sat / Viasat

Février 2022 : l'ANSSI dans l'espace



Impact cyber d'un conflit terrestre

Illustration du « **débordement** » d'une attaque par sabotage

La Cyber Résistance Ukrainienne

Russian Threat Actors Behind the Attacks in Ukraine

Despite the high level and technical sophistication of the cyberattacks, and the Russian Special Services' ability to cover their tracks, several traces remain present after the attacks which leave no doubt of Russia's involvement in the current attacks against Ukraine.

As mentioned in a report released by the Estonian Foreign Intelligence Service and a UK government publication we can clearly draw some connections between the most notorious threat groups involved and Russian special services.

APT29, also known as Cozy Bear or The Dukes to the Russian Foreign Intelligence Service (SVR).

APT28, also known as Fancy Bear or Sofacy was traced to the Main Directorate of the General Staff of the Armed Forces of the Russian Federation (Former GRU) Unit 26165.

SANDWORM, also known as Black Energy, was tied to the Main Directorate of the General Staff of the Armed Forces of the Russian Federation (Former GRU) Unit 74455.

DRAGONFLY, also known as Energetic Bear or Crouching Yeti was identified as the Russian Federal Security Service (FSB) Unit 71330.

GAMAREDON, also known as Primitive Bear or Armageddon, traced to the Russian Federal Security Service (FSB) in November 2021. The Security Service of Ukraine (SSU) successfully identified individuals behind Gamaredon confirming their ties with FSB.

«ARMAGEDON»: REGULAR HACKERS OF THE FSB

Security Service Of Ukraine

leadership of the FSB of the Russian Federation in the Republic of Crimea and the city of Sevastopol

Mykhailiuk Leonid Volodymyrovych (01.01.1970)
the head of Department of FSB of the "Russian Federation in the Republic of Crimea and the city of Sevastopol"

Kundikov Yehor Volodymyrovych (08.05.1978)
Deputy Head of the Counterintelligence Operations Service of the FSB of the "Russian Federation in the Republic of Crimea and the city of Sevastopol"

Nosov Ihor Valeriiovych (15.11.1979)
the Head of the 4th section of Service of counterintelligence operations (SCO) of the Department of FSB of the "Russian Federation across the Republic of Crimea and the city of Sevastopol"

Sklianko Oleksandr Mykolaiovych (05.08.1973)
the deputy chief of the 4th section of SCO of the Department of FSB of the "Russian Federation in the Republic of Crimea and the city of Sevastopol"

SUBORDINATE

ACCOUNTABLE

18th Center of Information Security of the FSB

Chernykh Mykola Serhiiovych (12.10.1978)
head of the unit of the 4th section of SCO of the Department of FSB of the "Russian Federation in the Republic of Crimea and the city of Sevastopol"

Starchenko Anton Oleksandrovych (28.11.1985)
officer of the unit of the 4th direction of SCO of the Department of FSB of the "Russian Federation in the Republic of Crimea and the city of Sevastopol"

Miroshnychenko Oleksandr Valeriiovych (16.09.1984)
officer of the unit of the 4th direction of SCO of the Department of FSB of the "Russian Federation in the Republic of Crimea and the city of Sevastopol"

Sushchenko Oleh Oleksandrovych (12.10.1989)
officer of the unit of the 4th direction of SCO of the Department of FSB of the "Russian Federation in the Republic of Crimea and the city of Sevastopol"

La Cyber Résistance Ukrainienne

- Prior to February 2022, the U.S. government worked closely with Ukrainian government ministries and critical infrastructure sectors to support Ukraine's cyber resilience, including by providing over $40 million in cyber capacity development assistance since 2017. Among these efforts:
  - Beginning in 2020, USAID launched an ambitious $38 million cybersecurity reform program that will work over the next several years to strengthen Ukraine's cybersecurity legal and regulatory environment, build Ukraine's cyber workforce and strengthen course offerings at leading Ukrainian universities, and develop connections between critical infrastructure operators and private sector solution providers. This program has embedded more than 20 technical experts within the Government of Ukraine to bolster Ukraine's cyber response and recovery capabilities, and deployed cybersecurity software and hardware tools to ensure the resilience of critical infrastructure to physical and cyber attacks.
  - DOE has a long-standing relationship with the energy sector in Ukraine, including work with Ukrainian utilities to help enhance their cybersecurity posture. In the leadup to Russia's further invasion of Ukraine, DOE, leveraging the expertise of our National Labs, worked with utilities to focus on potential near-term cybersecurity enhancements, while also continuing our work on long-term resilience efforts.

La Cyber Résistance Ukrainienne

Russia failed to take down Ukrainian computer systems with a massive cyber-attack when it invaded this year, despite many analysts' predictions. The work of a little-known arm of the US military which hunts for adversaries online may be one reason. The BBC was given exclusive access to the cyber-operators involved in these global missions.

In early December last year, a small US military team led by a young major arrived in Ukraine on a reconnaissance trip ahead of a larger deployment. But the major quickly reported that she needed to stay.

"Within a week we had the whole team there ready to go hunting," one of the team recalls.

They had come to detect Russians online and their Ukrainian partners made it clear they needed to start work straight away.

"She looked at the situation and told me the team wouldn't leave," Maj Gen William J Hartman, who heads the US Cyber National Mission Force, told the BBC.

"We almost immediately got the feedback that 'it's different in Ukraine right now'. We didn't redeploy the team, we reinforced the team."

Une situation alarmante,

Des CYBER Corsaires protégés

WANTED BY THE FBI

MAKSIM VIKTOROVICH YAKUBETS

Conspiracy; Conspiracy to Commit Fraud; Wire Fraud; Bank Fraud; Intentional Damage to a Computer

DESCRIPTION

Aliases: Maksim Yakubets, "AQUA"	
Date(s) of Birth Used: May 20, 1987	**Place of Birth:** Ukraine
Hair: Brown	**Eyes:** Brown
Height: Approximately 5'10"	**Weight:** Approximately 170 pounds
Sex: Male	**Race:** White
Citizenship: Russian	

REWARD

The United States Department of State's Transnational Organized Crime Rewards Program is offering a reward of up to $5 million for information leading to the arrest and/or conviction of Maksim Viktorovich

Alleged Russian Hacker Behind $100 Million Evil Corp Indicted

The US is charging Maksim Yakubets over two of the biggest cybertheft campaigns of the last decade, and offers a record reward for information on t case.

Le plus grand cyber-escroc du monde démasqué en tant qu'ancien agent de renseignement russe

Maksim Yakubets, 32 ans, a été nommé le plus grand cybercriminel du monde après avoir dirigé le groupe de cybercriminalité le plus dangereux du monde, Evil Corp

Un pirate informatique russe accusé de tromper des victimes britanniques sur des centaines de millions de livres a été désigné comme le plus grand cybercriminel du monde.

Maksim Yakubets, 32 ans, a éclaboussé un tigre de compagnie et des lionceaux, et possède une Lamborghini personnalisée avec une plaque d'immatriculation qui lit THIEF en russe.

Il est décrit comme intouchable à Moscou, où il se filme régulièrement au volant de «beignets» autour de la police, avec des crissements de pneus, dans l'une de ses flottes de supercars.

Pendant une décennie, le multimillionnaire aurait dirigé le groupe de cybercriminalité le plus nuisible au monde - Evil Corp., qui porte bien son nom. Il a ciblé des milliers de Britanniques et volé leurs économies en piratant leurs coordonnées bancaires.

Yakubets, qui a travaillé pour l'agence de renseignement du FSB russe, vivrait comme un roi, dépensant plus de 250 000 £ lors de son mariage.

CYBER: LES PAYS HOSTILES
IRAN: SHAMOON, CRAMBUS, APT34

En février 2019, les États-Unis ont inculpé quatre ressortissants iraniens pour conspiration avec un ancien agent de renseignements de l'armée de l'air américain qui s'était rendu en Iran en 2013. Le groupe a utilisé les renseignements fournis par l'agent de l'US Air Force pour lancer des attaques de phishing par courrier électronique et par les médias sociaux.

Behzad Mesri, l'un des quatre pirates informatiques, avait déjà été accusé en novembre 2017 d'avoir piraté la chaîne HBO et d'avoir diffusé des épisodes et des scripts inédits de plusieurs séries télévisées, notamment de la série Game of Thrones diffusée sur HBO.

Groupe Mabna

Identifié en mars 2018, ce groupe de pirates informatiques parrainé par l'État iranien a été accusé du piratage des réseaux de 320 universités à travers le monde. Le groupe était également connu sous le nom de Cobalt Dickens ou Silent Librarian dans les rapports de diverses entreprises de cybersécurité, et a poursuivi ses activités de piratage informatique malgré les accusations américaines.

PLAN

- **Une situation alarmante, l'espionnage**

Cyber Espionnage en hausse

Accueil > News > Cybersécurité

L'Anssi pointe du doigt la menace de l'espionnage chinois

Sécurité : *L'agence de cybersécurité française accorde une place importante à la question de l'espionnage dans son rapport annuel, et pointe du doigt l'activité des « modes opératoires réputés chinois » qui représente l'essentiel des attaques majeures identifiées par l'agence.*

Cyber Espionnage en hausse

TECH

Microsoft warns that China hackers attacked U.S. infrastructure

PUBLISHED WED, MAY 24 2023•3:36 PM EDT | UPDATED THU, MAY 25 2023•9:19 AM EDT

Rohan Goswami
@IN/ROHANGOSWAMICNBC/
@ROGOSWAMI

SHARE

KEY POINTS

- Chinese state-sponsored hackers have compromised “critical” cyber infrastructure in a variety of industries, including government and communications organizations, Microsoft said Wednesday.
- The hacking group is code-named “Volt Typhoon,” and has been in operation since 2021.
- Impacted parties have already been notified.

RAPPORT CERT-ANSSI Ciblage permanent des entreprises

Ciblage constant des secteurs industriels stratégiques 2/3

2017-2020 : ciblage des ESN et chaînes d'approvisionnement

Série d'attaques visant **l'écosystème** des cibles finales
Rebond vers les machines des cibles finales *via* les interconnexions
Exfiltration de données industrielles

Retour en force des **MOA liés à la Chine**
Attaquants **discrets, efficaces et préparés**

Nouvelle typologie de **bénéficiaires**
Possibilité de **remédiation complète ?**

Ciblage constant des secteurs industriels stratégiques 3/3

2021- présent : intervention auprès de prestataires de plus en plus petits

Cibles (sous-traitants et prestataires) de **plus petite taille**
Compromissions larges et de longue durée
Bénéficiaires souvent très **mal sécurisés**, très **peu conscients de la menace**

MOA **non observés jusqu'ici** et liés en sources ouvertes à la **Chine**
Recherche d'**informations industrielles stratégiques**

Secteur **structurellement ciblé** : déplacement des attaquants vers le **maillon le plus faible** ?

Ciblage d'équipements embarqués

2011-... : ça va couper !

Ciblage d'**équipements « non-conventionnels »**
Ciblage du **secteur des télécommunications** au sens large

Intérêt constant pour les groupes d'attaquants aux **intérêts stratégiques**

Surface d'attaque large
Expérience de l'ANSSI sur l'investigations numérique sur ce type d'équipements
Création de **relations** avec les opérateurs de télécommunications

Nouvelles formes d'espionnage

Un bourriquot ailé dans ton téléphone !

Compromission de **téléphones individuels** de **personnalités publiques**
Mise en œuvre rapide de capacités de dépistage et investigations

LIO privée : ajout d'un **intermédiaire** entre le commanditaire de l'attaque et la cible, **complique l'imputation d'une compromission**
Code malveillant très sophistiqué : Pegasus

Bon Risk Appétit

apprendre à gérer le risque numérique

Bon Risk appetite: to learn how to manage the digital risk

https://www.capgemini.com/blog/cto-blog/2014/12/technovision-2015-bon-risk-appetit

The *Bon Risk Appétit* design principle is not about eliminating all risks – an impossible task. It is about doing business at an acceptable level of risk. It is also about taking a fresh perspective dealing with risks – a perspective which not only makes the risks acceptable, but also could well turn them into opportunities – a new competitive advantage or even a disruptive business model.

DE LA LIGNE MAGINOT

VERS L'AEROPORT DES DONNEES

•Les éléments clés de la cyber sécurité

NIST FRAMEWORK: THE ZERO TRUST MODEL

CYBERSECURITY STRATEGY: PASS FROM THE FORTRESS TO THE AIRPORT

IDENTIFY

MONITOR

DETECT

REACT

PREVENT

HARDENING
INFRASTRUCTURE

La stratégie cybersécurité de l'Entreprise

•De la SSI classique vers le sécurité 360°

Les fondamentaux

-apprendre à gérer le risque numérique

-séparer clairement les fonctions d'exploitant du numérique (DSI) et de contrôleur du numérique (CISO)

-créer une tour de contrôle du numérique rattachée au PDG

-mettre en place des nouveaux métiers: identifier (Cyber Threat Intelligence)-créer un CERT, détecter et réagir (SOC CSIRT), apprendre à gérer la crise cyber, préparer et tester un plan de reprise d'activité PRA

-contrôler en temps réel la bonne garantie des règles techniques des exigences de sécurité (ISO27xxx, ANSSI, NIST..)

Les fondamentaux

-pour gérer le risque numérique quatre instances sont fondamentales

-la cyber design authority qui est responsable da la qualification de toutes applications de l'entreprise

-le SOC CSIRT: détecter, réagir

- le CERT identifier les risques (internes) et les menaces (externes)

- le maintien en conditions de sécurité: AD, FIREWALL, PATCH, DMZ..

Il faut disposer d'une capacité opérationnelle de défense, expérimentée et entrainée

Deux éléments clés de réussite

Comprendre et réagir très vite

Rester discret

La plupart des entreprises n'ont pas les ressources pour créer une capacité opérationnelle de défense efficace, elles externalisent

Contractualiser la disponibilité immédiate de CYBER SWAT prête à se projeter immédiatement pour conduire la guerre défensive au sein de l'entreprise

Segmenter les réseaux, plan d'occupation des sols, Zero Trust Network

Mettre en place des bastions durcis: tier0 et comptes à privilèges, MFA, IAM

Système de détection et réaction avancée: EDR et SOAR

Chiffrement des données, maitriser les données dans le CLOUD

Former les dirigeants et le salariés (80 des attaques réussies sont d'origine humaine)

Rancongiciels, une situation critique

ANOZR WAY

BAROMÈTRE ANOZR WAY DU RANSOMWARE #4 SEPT 2022

CHIFFRES CLÉS

1,06 milliard d'€
de perte de CA cumulé estimée pour les entreprises françaises victimes du 1er janvier au 31 août 2022

1 attaque
par ransomware est revendiquée **toutes les 3h** en moyenne dans le monde

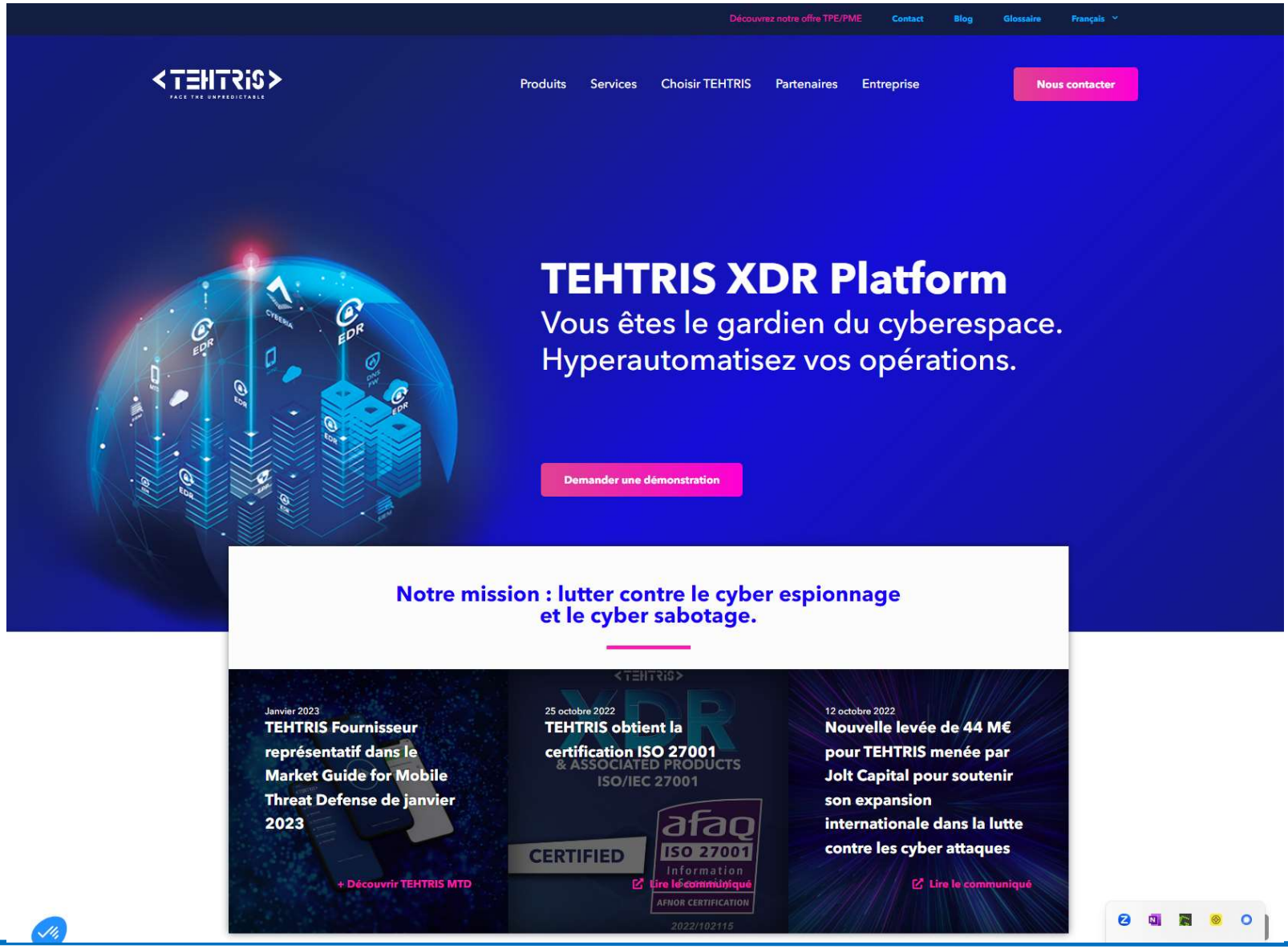
+14%
de hausse des attaques revendiquées envers le secteur public en Europe ces 4 derniers mois
(mai – août 2022)

15
nouvelles franchises de ransomware créées ces 4 derniers mois
(mai – août 2022)

5

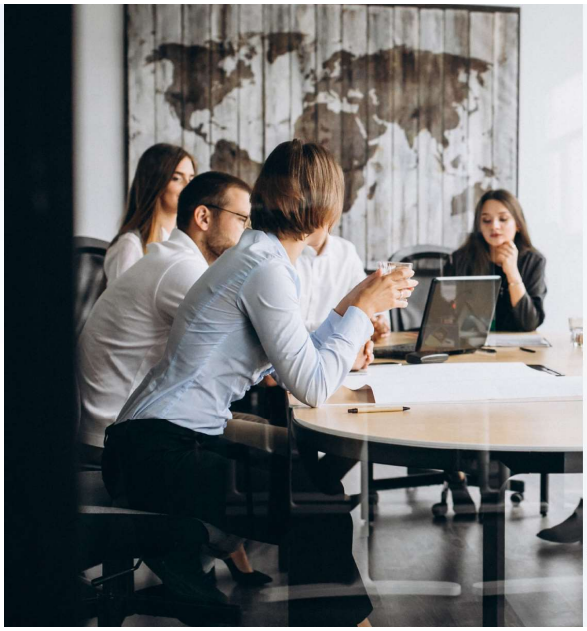
Les éléments clés de la cyber sécurité

Installer un EDR



Les éléments clés de la cyber sécurité

Le facteur HUMAIN (80% des attaques réussies)



https://www.youtube.com/watch?v=BmBp5ICaFsI