Microsoft

Cybersécurité et secteur public, des défis aux solutions

Bart Asnot
National Security Officer
Microsoft

BELGIQUE

La Chancellerie du Premier ministre visée par une cyberattaque : les pirates ont tenté de voler des données personnelles

Les urgences du CHU Saint-Pierre à nouveau accessibles après une cyberattaque

L'hôpital Saint-Pierre, dans le centre de Bruxelles, a dû provisoirement fermer ses urgences samedi et dévier la ligne 112 vers d'autres institutions en raison d'une cyberattaque, a indiqué l'établissement de soins dans un communiqué.

"Si vous jetez une **grenouille dans une casserole d'eau bouillante**, elle en **sortira tout de suite**.
Mais si vous **mettez cette grenouille dans une casserole d'eau tiède** et que vous la **réchauffez lentement**, la grenouille ne comprendra que trop tard ce qui se passe : **c'est la grenouille bouillie**.
Il s'agit simplement de travailler par petits degrés."

ACCUEIL • SOCIÉTÉ • RÉGIONS • WALLONIE

Cyberattaque au CHR Sambre et Meuse: 22 jours plus tard, «l'impact de cette crise est toujours très important»

Aucun contact n'a été établi avec les hackers et qu'aucune demande de rançon n'a été reçue. L'accent est mis sur «la reconstruction de l'infrastructure informatique».

Charleroi: le plus gros CPAS wallon mis hors ligne suite à une cyberattaque, les services fermés ce mardi

Depuis lundi matin, toute l'informatique du CPAS de Charleroi a été mise à l'arrêt après une cyberattaque. Certains services seront fermés ce mardi.

Didier Albin

Publié le 21-08-2023 à 19h03

Enregistrer

Cyber attacks Belgium in 2022

Microsoft Digital Defense Report 2023

January

Jan 10
Ranst
Game retailer

Jan 24
Verviers
City administration

Jan 24
Belgium
Network operator

Jan 26
Tielt
Hospital

Jan 30
Gent
Port terminal

February

Feb
Antwerp
Crematoria

March

Mar 21
Belgium
Universities

April

Apr 08
Kortrijk
University of appli...

April
Turnhout
Coffee, coffee mach...

April
Herentals
Hospital

May

May 14
Bastogne
Hospitals

May 23
Liège
University

May 23
Liège
Hospital

May 24
Brussels
Technology

July

July
Brussels
Government

Jul 20
Maldegem
Social welfare

August

Aug 01
Olen
Home furnishin

August
Oosterhout
Dental practices

Aug 10
Brussels
Chancellery

September

Sep 05
Mouscron
Social service

Sep
Zwijndrecht
Police

Sep 22
Geraardsbergen
City government

October

Oct 23
Wevelgem
Nursing home

November

Nov 18
Liège
Hospitals

Nov 25
Brussels
Automobile club

December

Dec 06
Antwerp
City government

Dec 12
Diest
Municipality

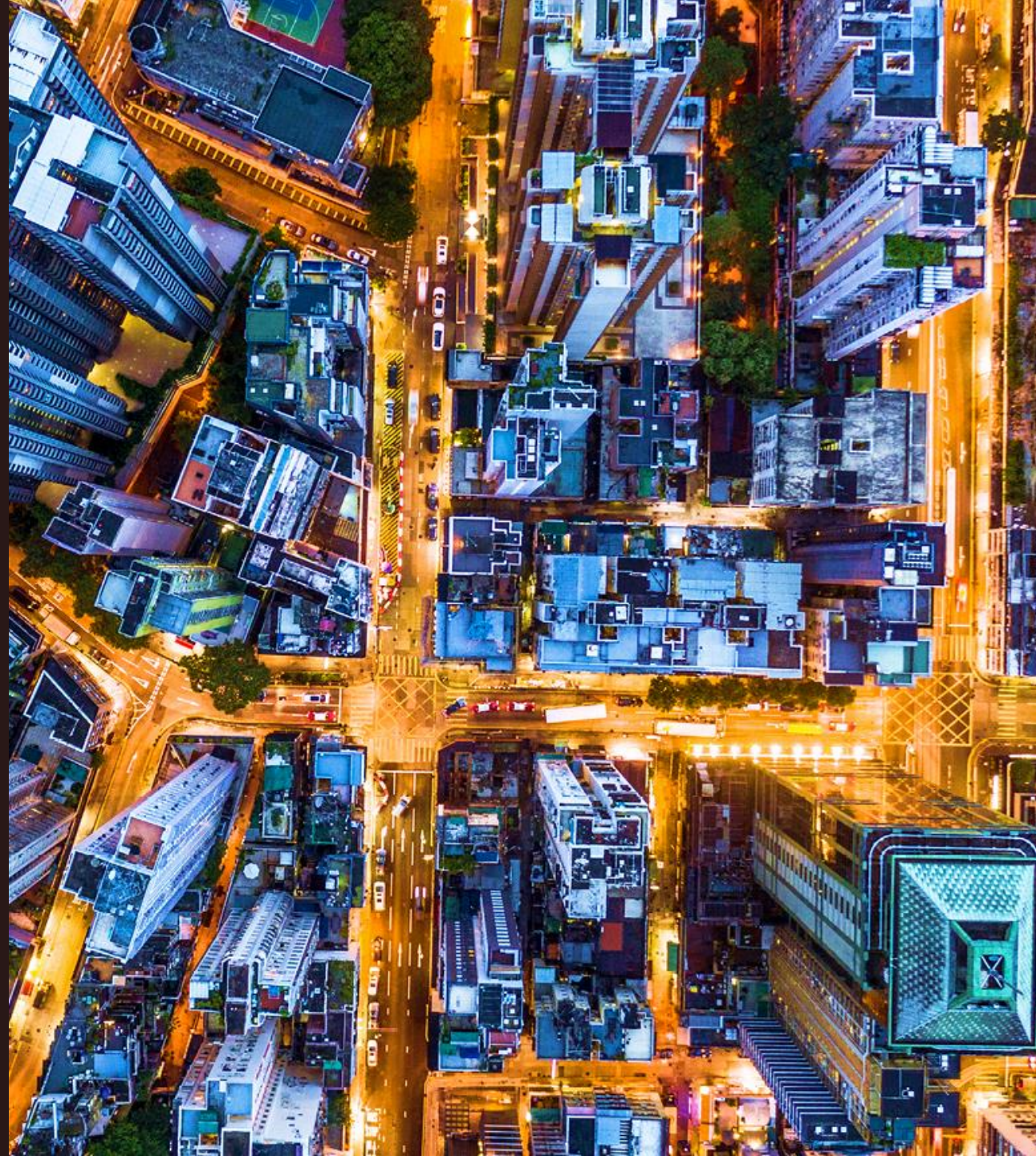
Dec
Staden
Vehicles

Assurer notre Cybersecurity ensemble

> “Les défenseurs sont amenés à innover et à collaborer plus étroitement que jamais.”

L'état de la cybercriminalité

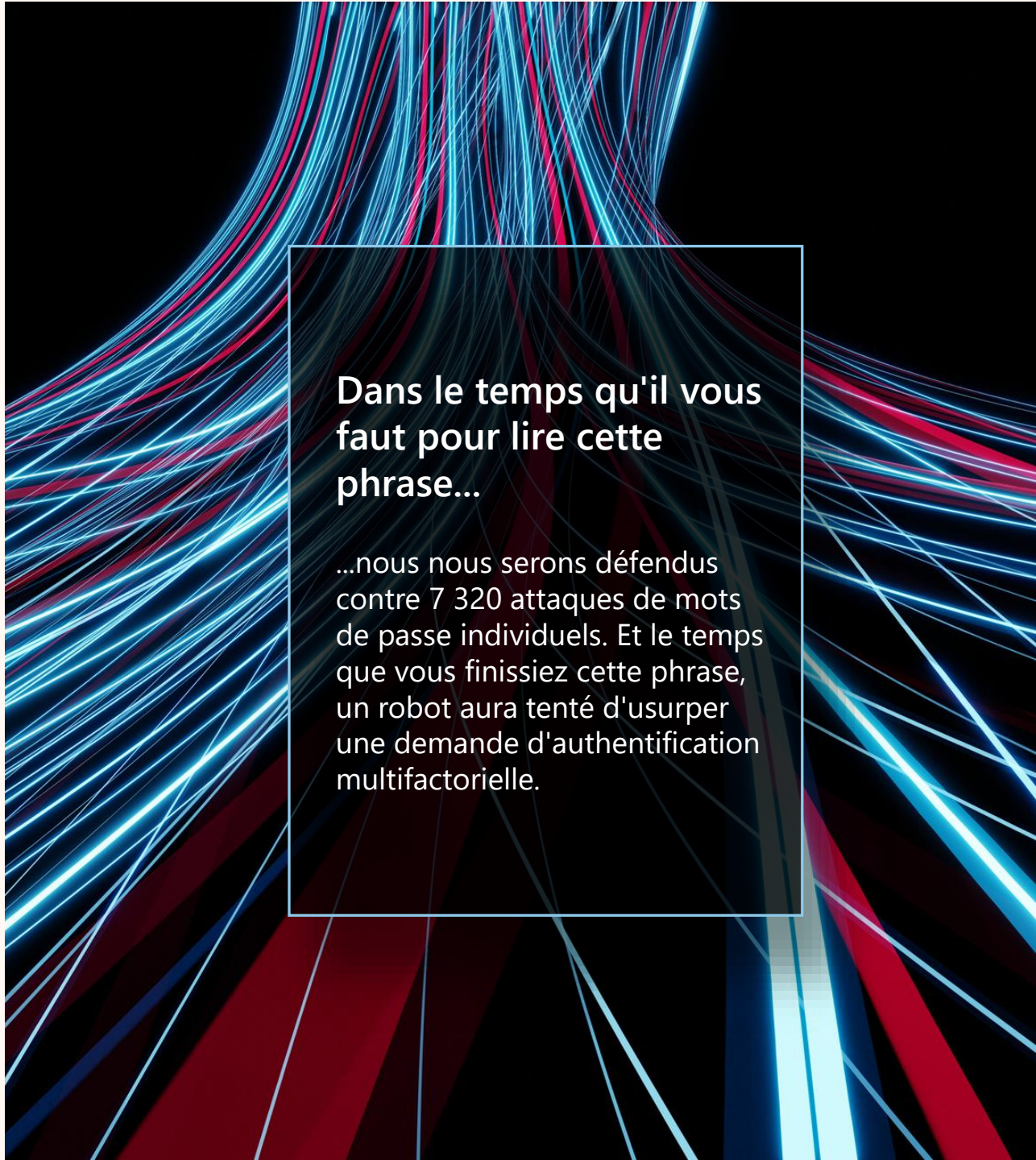
L'évolution des menaces



Attaques et réduction des menaces

- 4 000 attaques par mot de passe bloquées par seconde en moyenne au cours de l'année écoulée.
- 156 000 tentatives de compromission du courrier électronique des entreprises observées chaque jour
- Atténuation de 1 700 attaques DDoS par jour
- Suivi et surveillance de 14 sites de DDoS à louer

Augmentation annuelle de 23 % des cas traités par les équipes du Microsoft Security Response Center et du Security Operations Center.

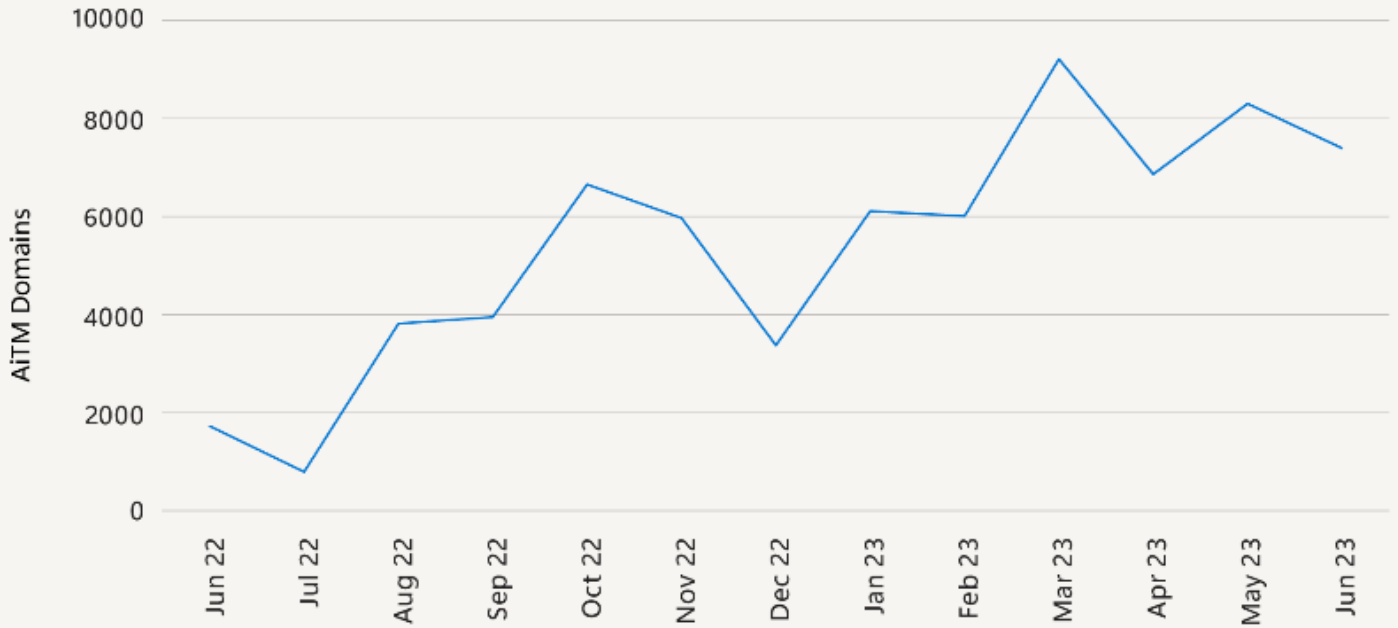


Aperçu de Phishing

- Évolution des techniques de phishing
- Adversary-in-the-middle (AiTM) attacques

AiTM domaines se multiplient à mesure que les attaques deviennent plus fréquentes

Le nombre de domaines que nous avons suivis et qui mènent à des pages de phishing AiTM a augmenté de façon constante au cours des 12 derniers mois.



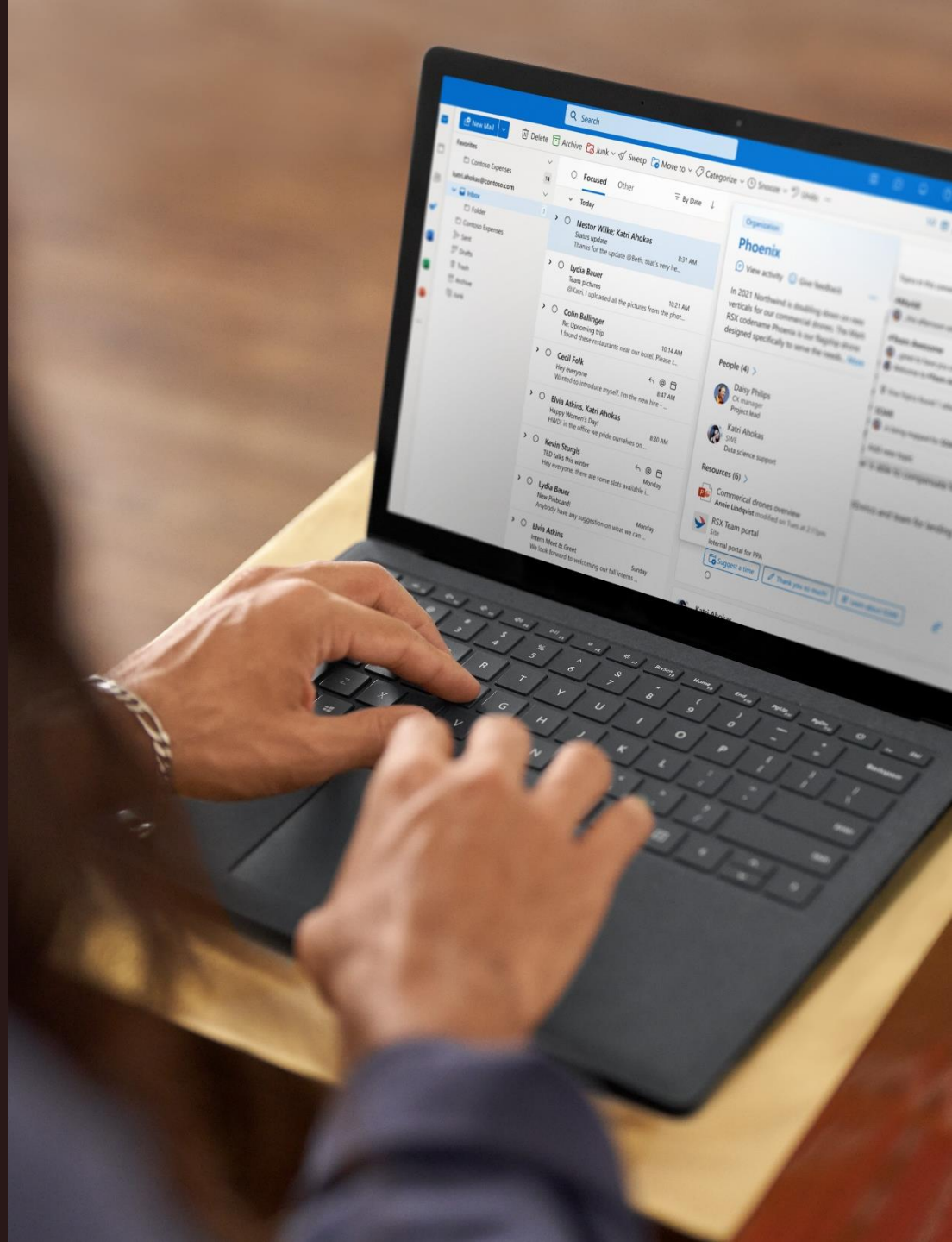
Source: Microsoft Defender for Office 365

Aperçu de **business email compromise (BEC)**

- Fraude financière
- Mouvement latéral par phishing interne

L'évolution du BEC:

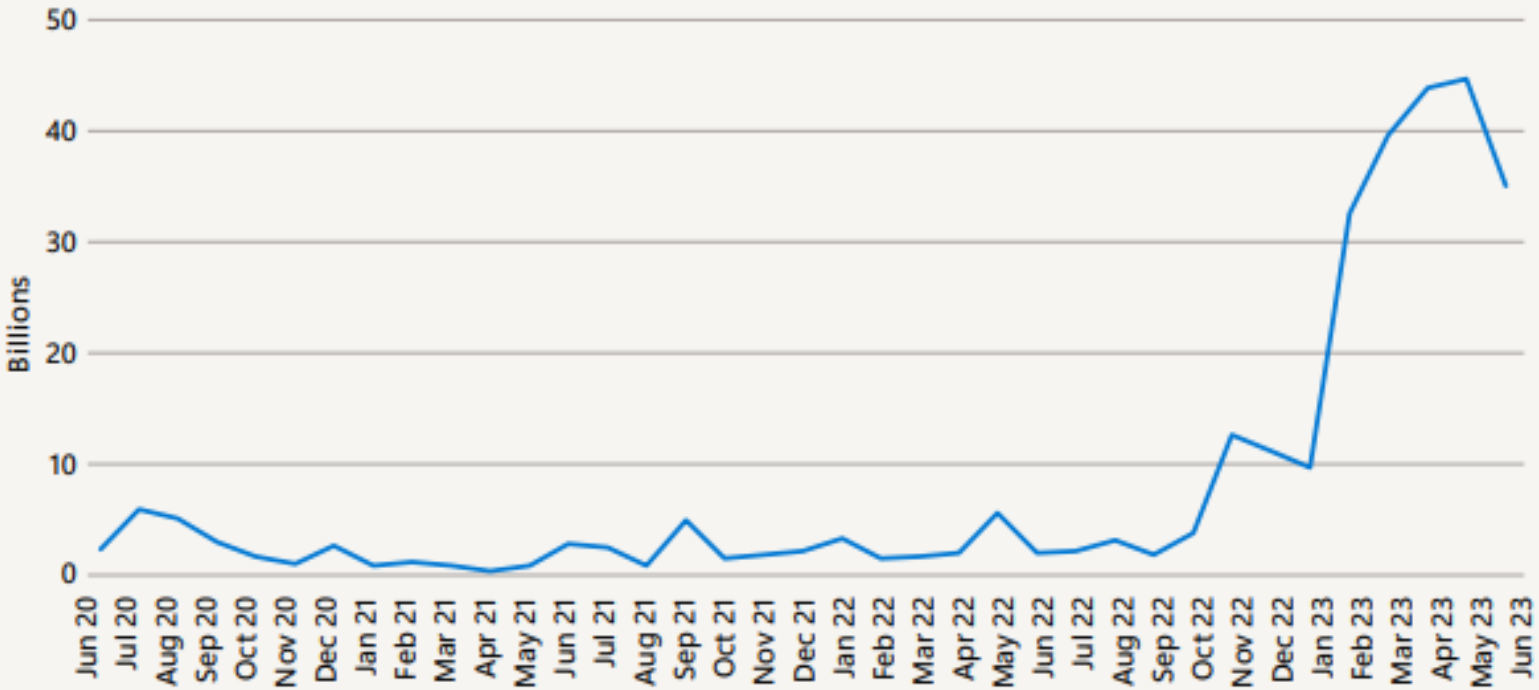
- Utilisation accrue de l'infrastructure basée sur l'informatique en Cloud
- Exploitation de relations commerciales de confiance : compromission du courrier électronique d'un fournisseur
- Les acteurs de la menace se perfectionnent



Aperçu des attaques d'identité

- Bots à mot de passe unique
- la fatigue multifactorielle (MFA) est une menace
- Token replay reste une menace courante

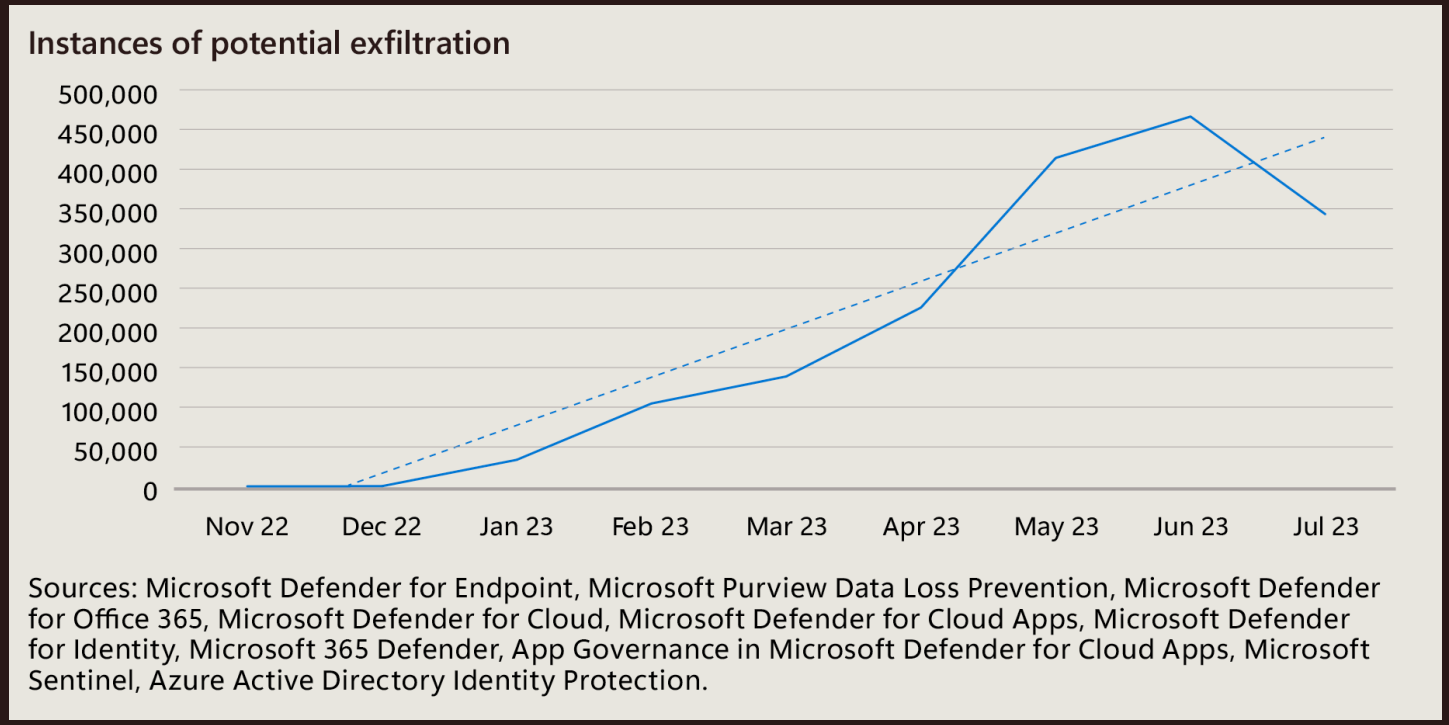
Les attaques par mot de passe ont augmenté en 2023



Source: Microsoft Entra data

Aperçu des ransomwares et de l'extorsion

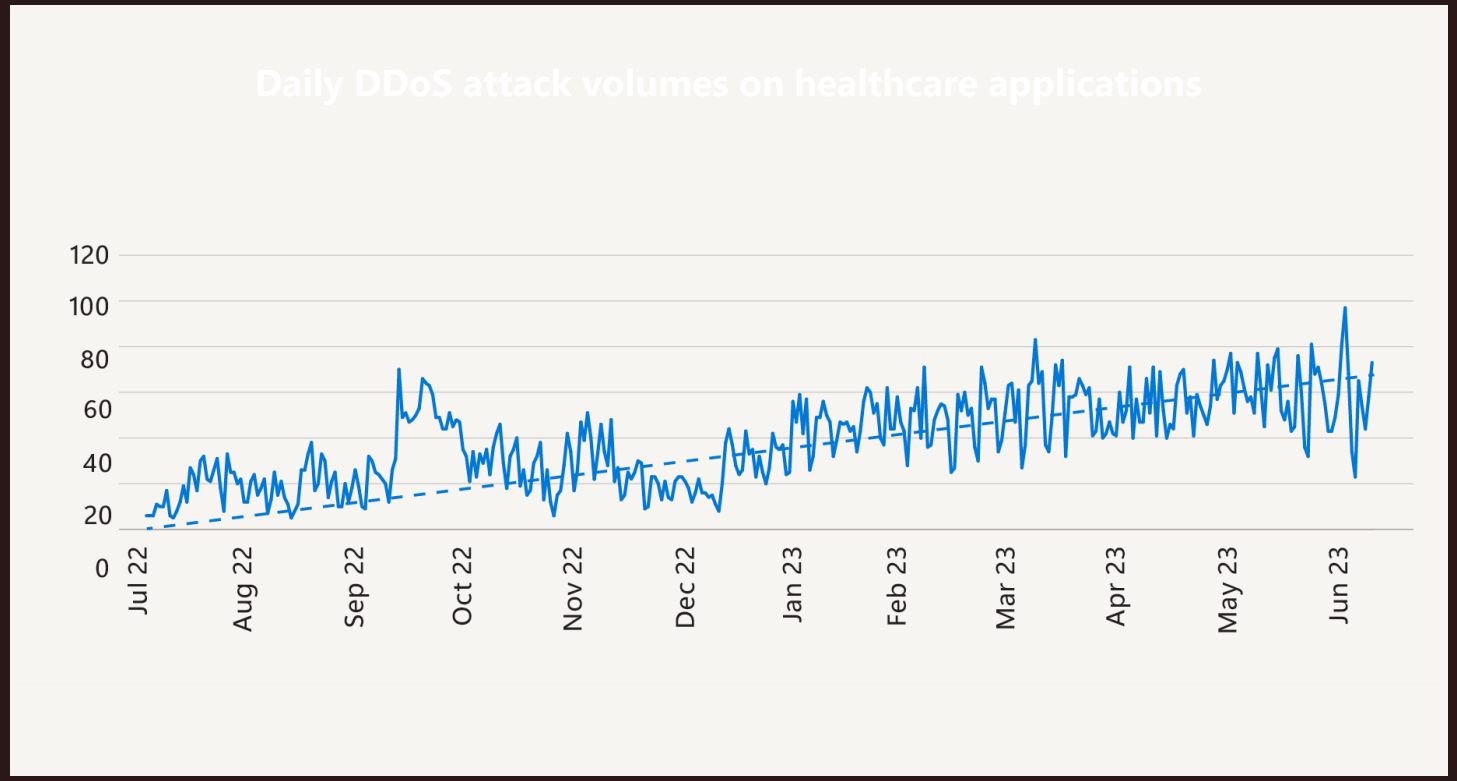
- >Augmentation de 200 % des attaques de ransomware par des humains
- 13% des attaques impliquent désormais l'exfiltration de données
- 79% des attaques réussies sont dirigées contre des organisations comptant < 500 employés
- 80 à 90 % des attaques réussies proviennent de dispositifs non gérés



Sources: Microsoft Defender for Endpoint, Microsoft Purview Data Loss Prevention, Microsoft Defender for Office 365, Microsoft Defender for Cloud, Microsoft Defender for Cloud Apps, Microsoft Defender for Identity, Microsoft 365 Defender, App Governance in Microsoft Defender for Cloud Apps, Microsoft Sentinel, Azure Active Directory Identity Protection.

Aperçu des attaques par déni de service distribué (DDoS)

- DDoS for hire services
- L'essor des botnets à grande échelle
- Les soins de santé et le secteur public comme cible



Source: Microsoft Global DDoS Mitigation Operations tracking healthcare applications in Azure

Nation-State Threats

Comment le paysage des menaces a-t-il évolué ?

Nation-State Threats

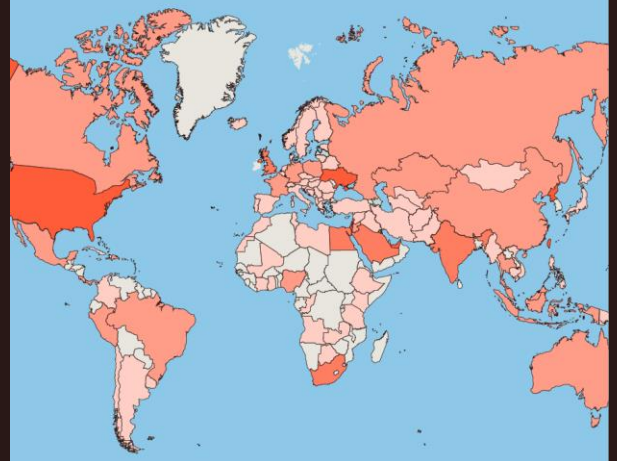
> “Nation-state actors are showing increased investment and use of cyber operations as a tool to achieve their geopolitical goals.”

— John Lambert
Corporate Vice President, Distinguished Engineer,
Microsoft Security Research

Nation-State Threats

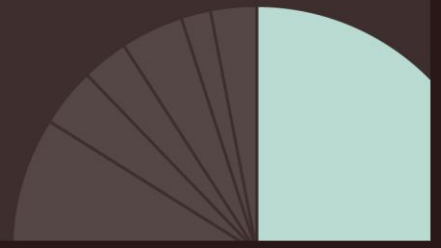
Principales évolutions

Nation-state and state-affiliated threat actor activities pivoted away from high volume destructive attacks in favor of espionage campaigns.



The unchecked expansion of the cyber mercenary marketplace threatens to destabilize the broader online environment.

Russian state-sponsored threat actors used diverse means to access devices and networks in NATO member states.



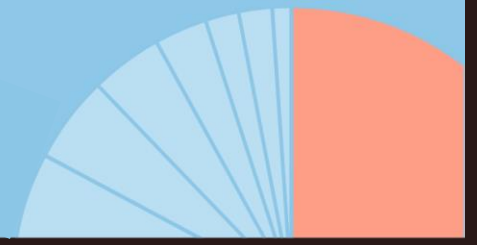
Iranian state actors are using increasingly sophisticated tradecraft

including enhancing operations in cloud environments, regularly using custom implants, and exploiting newly released vulnerabilities faster.

Chinese cyber threat groups carried out sophisticated worldwide intelligence collection campaigns.

At the same time, China's cyber influence campaigns continue to operate at an unmatched scale.

North Korean actors conducted a supply chain attack using an existing supply chain compromise.

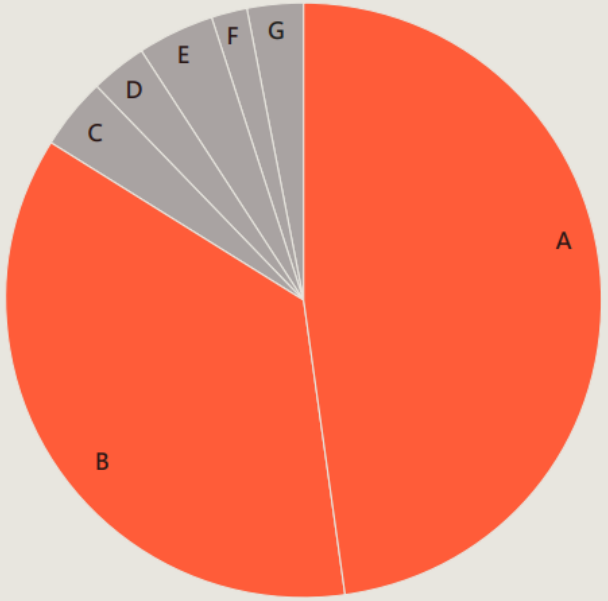


Nation-State Threats

Russia

Les relations diplomatiques et de défense des membres de l'OTAN diplomatiques, de la défense, et des transports des membres de l'OTAN sont menacés

Most targeted regions

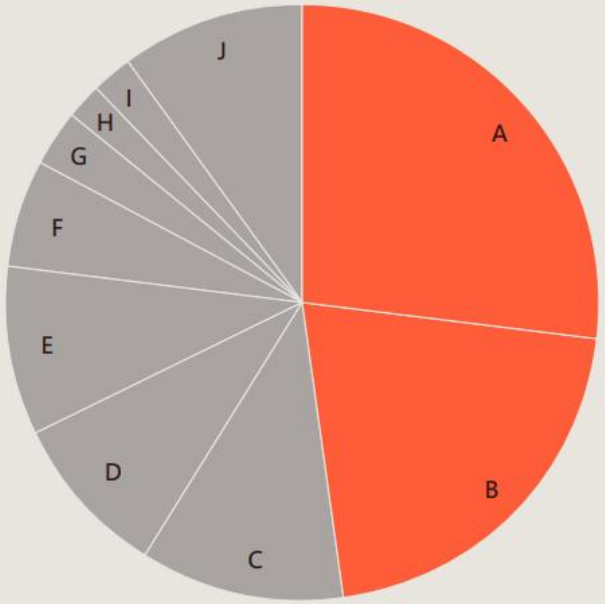


- A 48% Ukraine
- B 36% NATO Member states
- C 4% Europe
- D 3% MENA
- E 4% Latin America
- F 2% Africa
- G 3% Asia

36%

of observed network intrusions were directed against organizations within NATO member states, particularly the United States, United Kingdom, and Poland.

Most targeted sectors



- A 27% Government
- B 21% Think tanks/NGOs
- C 11% Education
- D 9% IT
- E 9% Intergovernmental organizations
- F 6% Defense Industry
- G 3% Energy
- H 2% Health
- I 2% Transportation
- J 10% Other

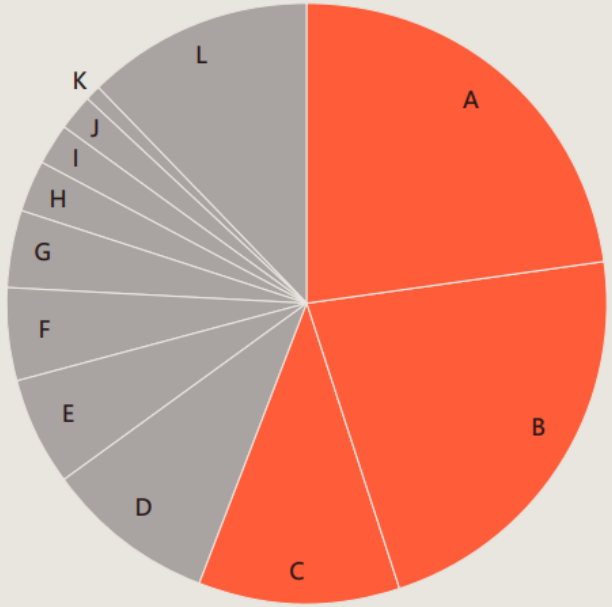
Nation-State Threats

North Korea

Cibler les entreprises de défense et gouvernments, en particulier en Europe

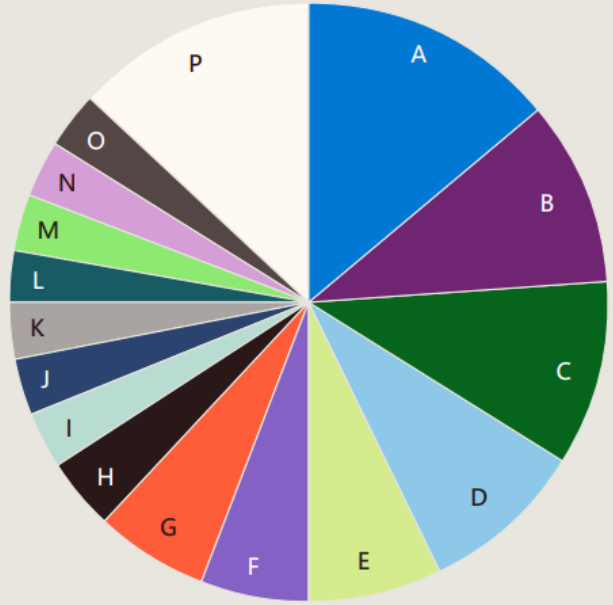
Most targeted sectors by North Korea

North Korea is particularly interested in spying on institutions and individuals that study North Korea itself.



- A 23% Think tanks/ NGOs
- B 22% Education
- C 11% Government
- D 9% Finance
- E 6% Inter-Government Organization
- F 5% IT
- G 4% Media
- H 3% Defense Industry
- I 2% Manufacturing
- J 2% Transportation
- K 1% Food, Agriculture
- L 12% Other

North Korea targeting of national defense industries



- A 14% Russia
- B 10% United States
- C 10% Israel
- D 9% Germany
- E 7% India
- F 6% Africa
- G 6% South Korea
- H 4% Türkiye
- I 3% Brazil
- J 3% Czechia
- K 3% Finland
- L 3% France
- M 3% Italy
- N 3% Poland
- O 3% Norway
- P 13% Other

Quel est l'état optimal de résilience face aux ransomwares ??

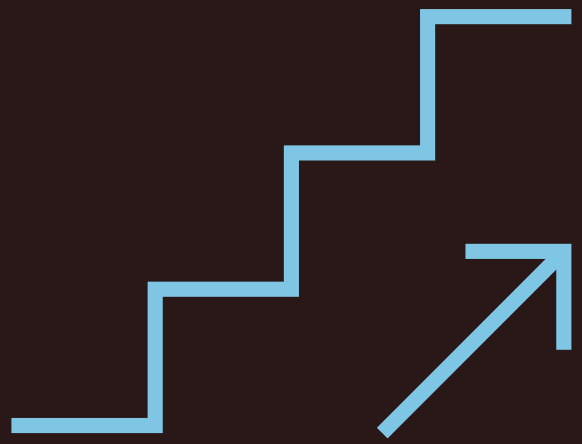
Les cinq principes fondamentaux

1. Authentification moderne avec des informations d'identification résistantes au phishing
2. Least privileged access appliqué à l'ensemble de la pile technologique
3. Des environnements sans menaces ni risques
4. Posture management pour la conformité et la santé des appareils, des services et des actifs
5. Automatic cloud backup and file-syncing pour les données critiques des utilisateurs et de l'entreprise

Un appel à l'action

Les auteurs de ransomwares sont motivés par le profit facile, Il est donc essentiel d'augmenter leur coût en renforçant leur sécurité. **perturber l'économie cybercriminelle.**

Opportunités pour le Secteur Public d'améliorer encore ses cyberdéfenses



1. Défendre grâce à la puissance et à l'échelle de « cloud”
2. Appliquer les principes de la Zero Trust
3. Utiliser des systèmes de détection et de réponse étendus et des logiciels anti-malware
4. Faire de la cybersécurité une priorité essentielle pour les organes et agences du gouvernement central
5. Patch Patch Patch

Trois leçons essentielles

Innovation

Nous devons utiliser le Cloud, les dernières innovations, telles que l'IA, pour renforcer notre cyberdéfense.

Partnerships

Nous devons collaborer avec toutes les parties prenantes, qu'elles soient publiques ou privées.

Skills

Nous devons investir dans l'amélioration des compétences et collaborer avec les partenaires du secteur

Sharing Microsoft's unique vantage point

65 trillion
signals synthesized daily

That is over 750 billion signals per second, synthesized using sophisticated data analytics and AI algorithms to understand and protect against digital threats and criminal cyberactivity.

10,000+
security and threat intelligence experts

10,000+ engineers, researchers, data scientists, cybersecurity experts, threat hunters, geopolitical analysts, investigators, and frontline responders across the globe.

4,000
identity attacks blocked per second

4,000 identity authentication threats blocked per second.

15,000+
partners in our security ecosystem

15,000+ partners with specialized solutions in our security ecosystem, who increase cyber resilience for our customers.

300+
threat actors tracked

Microsoft Threat Intelligence has grown to track more than 300 unique threat actors, including 160 nation-state actors, 50 ransomware groups, and hundreds of others.

100,000+
domains removed

100,000+ domains utilized by cybercriminals, including over 600 employed by nation-state threat actors, have been removed (all time).

135 million
managed devices

135 million managed devices providing security and threat landscape insights.

Microsoft

Thank You