Guerre hybride en Ukraine : quels rôles les entreprises technologiques jouent-elles dans le conflit et quels défis sont à relever dans l'avenir ?

Quang-Minh Lepescheux
Directeur, Affaires Publiques Européennes
Microsoft

Contexte de cybersécurité

78 trillions

de signaux chaque jour

600 millions

d’attaques chaque jour

34 000

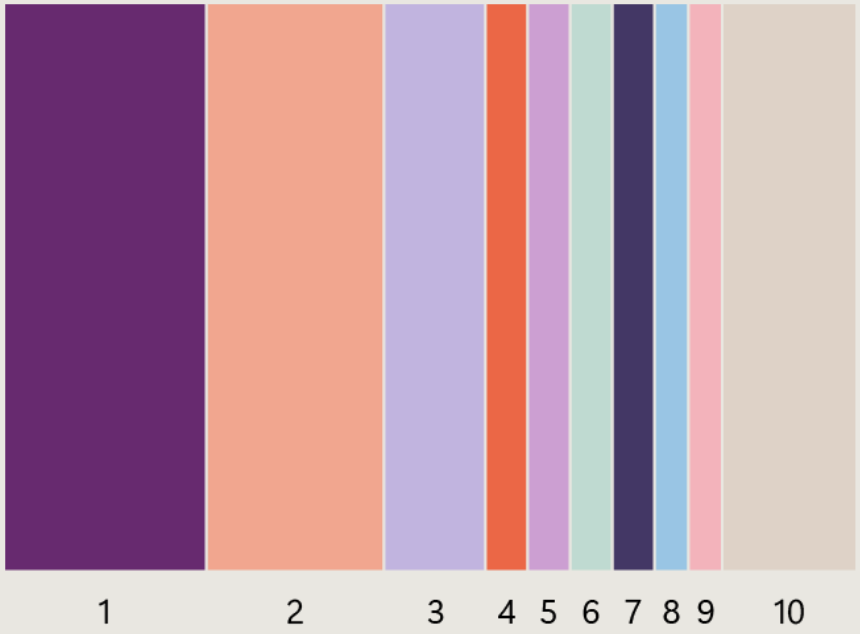
ingénieurs dédiés

15 000

partenaires spécialisés

Menaces cyber conduites par des Etat-nations

Top 10 targeted sectors worldwide



	Sector	Percentage
1	IT	24%
2	Education and Research	21%
3	Government	12%
4	Think tanks and NGOs	5%
5	Transportation	5%
6	Consumer Retail	5%
7	Finance	5%
8	Manufacturing	4%
9	Communications	4%
10	All others	16%

Threat actors from Russia, China, Iran, and North Korea pursued access to IT products and services, in part to conduct supply chain attacks against government and other sensitive organizations.

Source: Microsoft Threat Intelligence, nation-state notification data

Source: Microsoft Threat Intelligence

Russie

Targeting by region

Sector		Percentage
1	Europe & Central Asia	68%
2	North America	20%
3	Middle East & North Africa	5%
4	East Asia & Pacific	3%
5	Latin America & Caribbean	3%
6	South Asia	1%
7	Sub-Saharan Africa	1%

Most targeted sectors

Sector		Percentage
1	Government	33%
2	IT	15%
3	Think tanks and NGOs	15%
4	Education and Research	9%
5	Inter-governmental organization	4%
6	Defense Industry	4%
7	Transportation	3%
8	Energy	2%
9	Media	2%
10	All others	13%

Source: Microsoft Threat Intelligence

Une pléthore d'acteurs

01 **États :** Agents au sein du gouvernement d'un pays, y compris, par exemple, les agences militaires et de renseignement qui dirigent les cyber-opérations dans le cadre de la conduite plus large de la politique étrangère.

02 **Cybercriminels :** Acteurs non étatiques, individus et groupes, qui mènent des cyber-opérations principalement motivées par le profit.

03 **Hacktivistes :** Acteurs non étatiques ayant des motivations politiques, qui limitent leur activisme au domaine cybernétique. Ils peuvent ou non avoir de la sympathie pour un État particulier.

04 **Groupes terroristes :** Acteurs non étatiques qui sont motivés par des idéologies et cherchent souvent à semer la discorde ou à diffuser des campagnes d'influence parallèlement aux attaques physiques.

05 **Cyber-mercenaires :** cyber-agents privés pour compte d'autrui qui sont engagés par un acteur étatique ou non étatique pour une opération spécifique ou pour la vente d'une technologie spécifique.

La première guerre hybride à grande échelle

Engagement du secteur privé

01 Protéger le personnel en Ukraine et en Russie

02 Dons philanthropiques

03 Soutenir la migration vers le cloud

04 Partage de renseignements sur les cybermenaces

La stratégie Cyber russe

Cyber-attaques destructrices

Cyber-espionnage

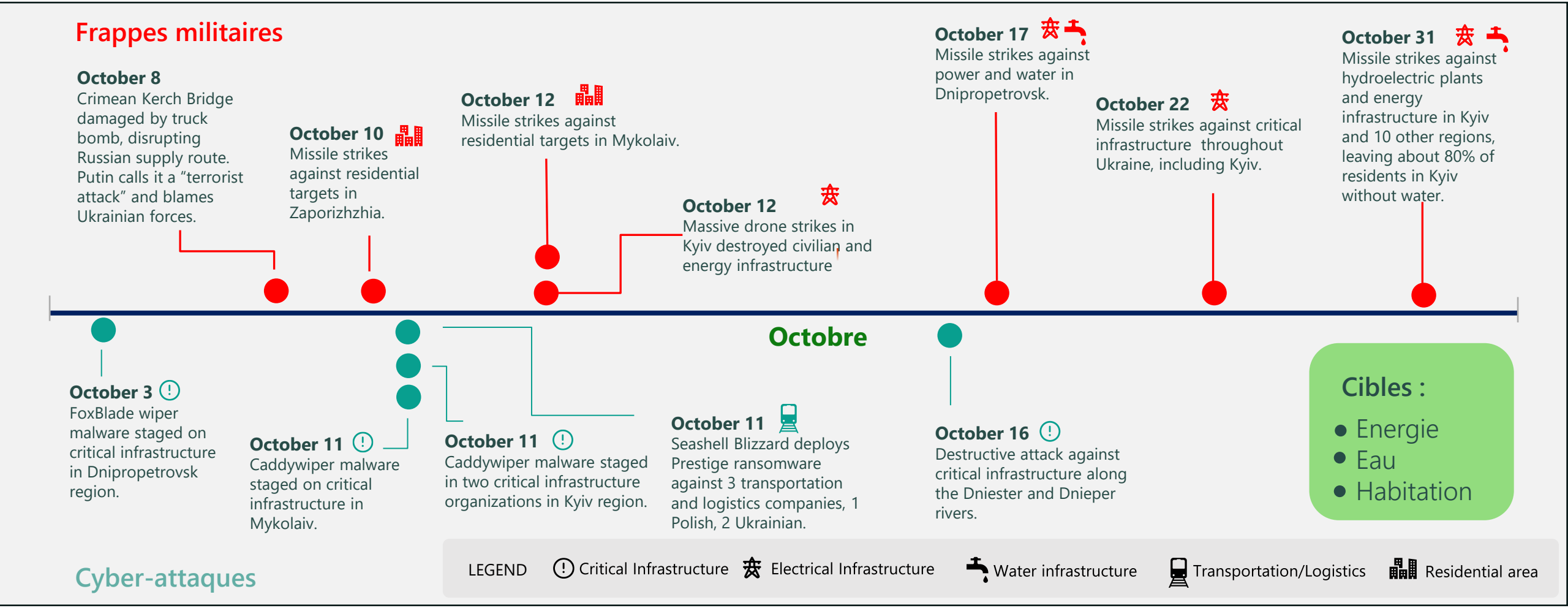
Cyber-influence

Cyber-attaques destructrices

Entités gouvernementales russes responsables des cyber-attaques

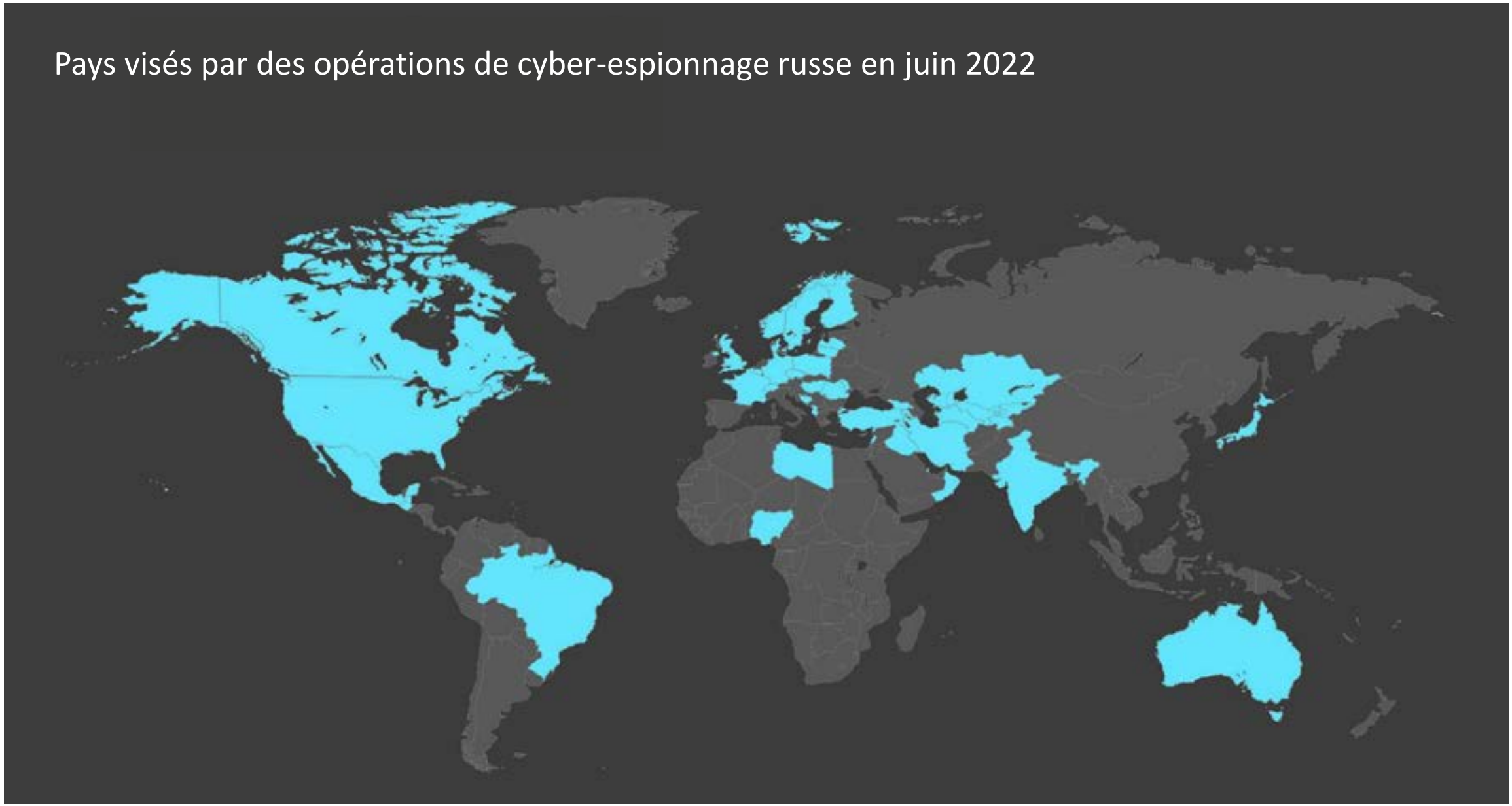
Attaques cyber et militaires coordonnées

Attaques cyber et militaires coordonnées

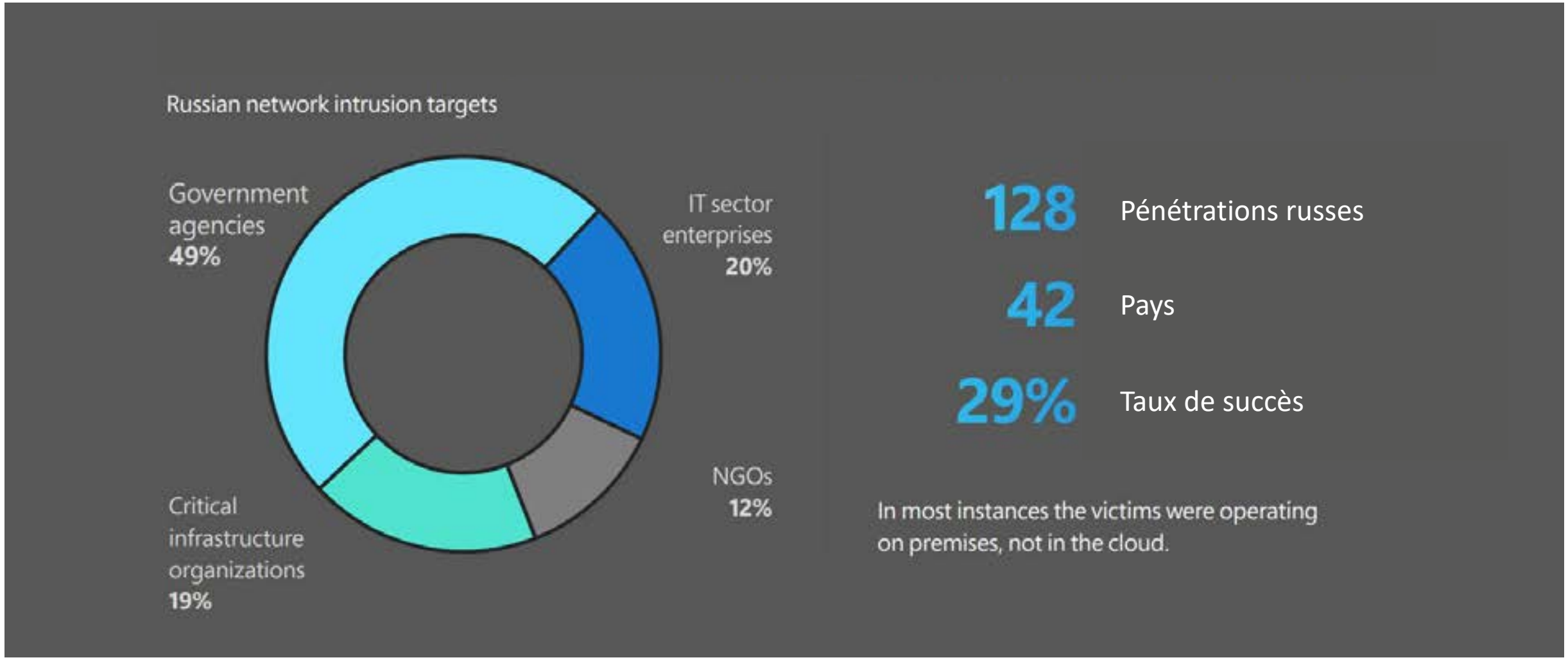


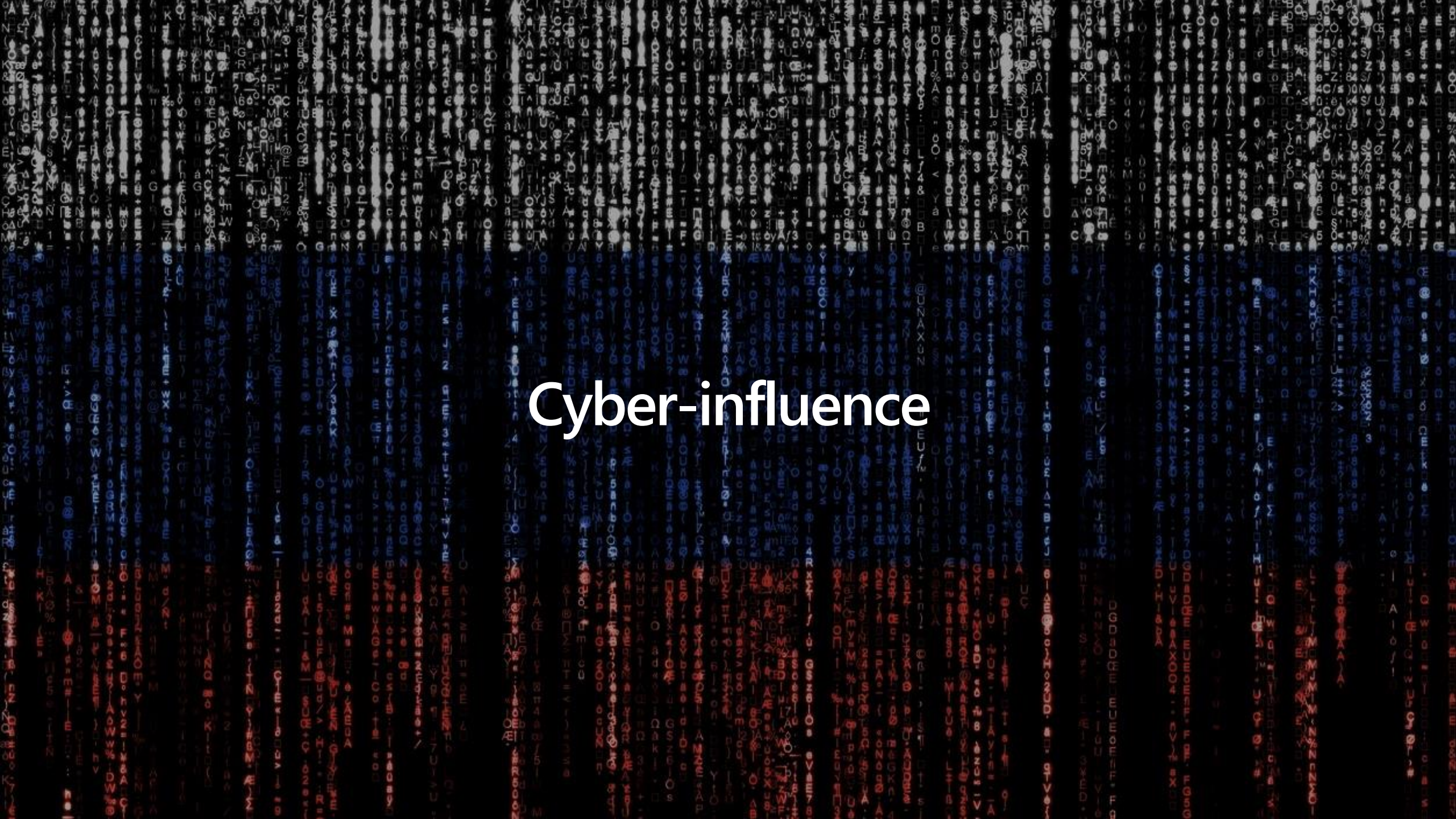

Cyber-espionnage

Pays visés par des opérations de cyber-espionnage russe en juin 2022



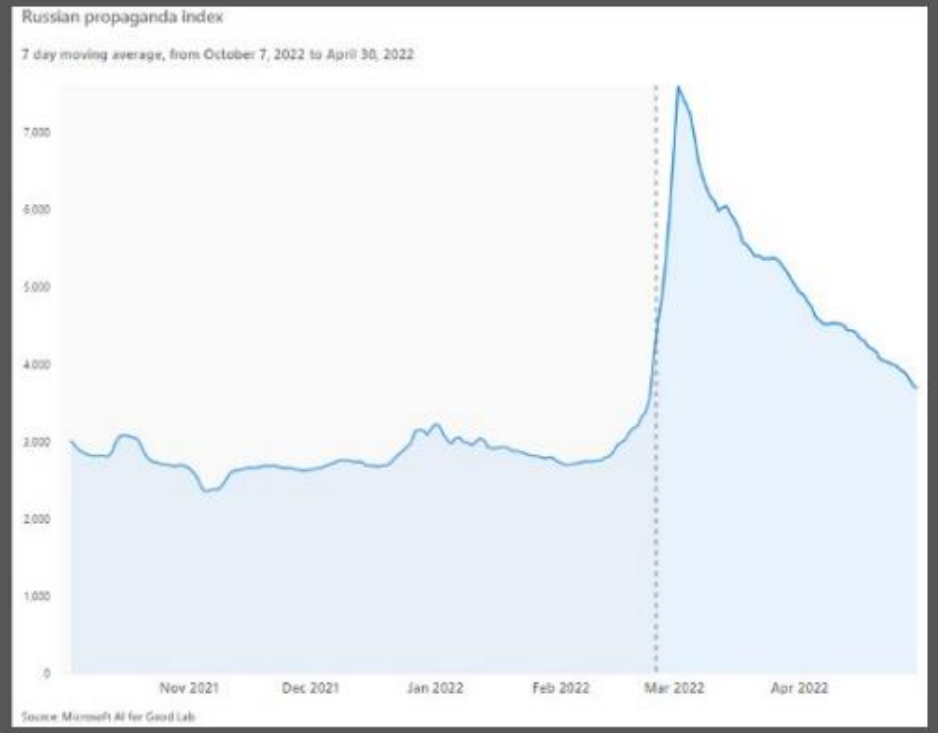
Pénétrations russes et cyber-espionnage à l'extérieur de l'Ukraine (Juin 2022)



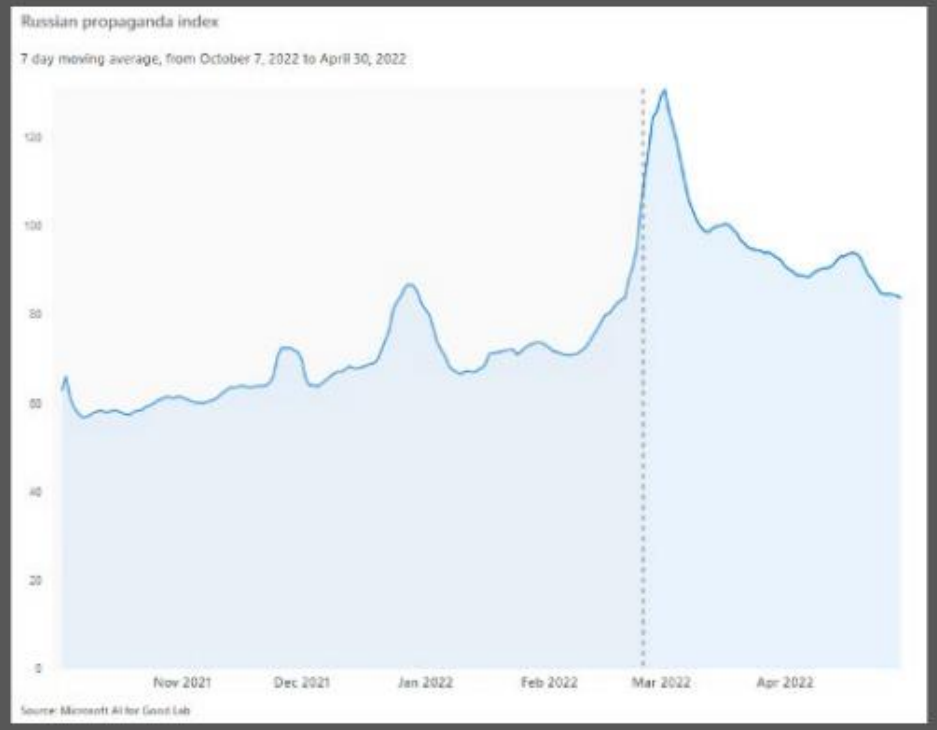

Cyber-influence

Russian Propaganda Index (RPI)

Russian propaganda consumption in Ukraine



Russian propaganda consumption in the US



Propagande anti-Ukraine

À l'intérieur de la Russie

La Russie contre le monde

À l'intérieur de l'Ukraine

L'Ukraine est russe pour toujours

Reste du monde

Délégitimer l'Ukraine

IA et désinformation

Développement des deepfakes

Cibles : élections, partis politiques, candidats, dirigeants politiques

Solutions existantes

Principaux enseignements

4 principaux enseignements

1. IA et transformation numérique
2. Interopérabilité du cloud et des données
3. Cyber-dissuasion
4. Coopération public-privé

Tendances

Cyber

- Augmentation des attaques de cyber-espionnage
- Les attaques wiper se poursuivent
- Déploiement de nouvelles variantes de ransomware

Influence indirecte

- Seashell Blizzard (IRIDIUM, Sandworm) se coordonne probablement avec le groupe d'hacktivistes pro-russe Cyber Army of Russia
- Groupes Xaknet et InfoCenter ayant des liens possibles avec les services de renseignement russes
- Utilisation de cyber-proxies

Influence

- Autres campagnes de propagande visant la diaspora ukrainienne en Europe
- Déplacement de l'influence de l'Ukraine vers l'Europe au sens large
- La Russie courtise un public réceptif dans les pays du Sud et dans les Balkans

Merci !

Quang-Minh Lepescheux
quangle@microsoft.com

Microsoft Threat Analysis Center
https://blogs.microsoft.com/on-the-issues/tag/mtac/

Microsoft Digital Defense Report 2024
https://www.microsoft.com/en-us/security/security-insider/intelligence-reports/microsoft-digital-defense-report-2024#modal-dialog