Veille n°5 — « Explosion du phishing 2.0 et des campagnes de ransomware-as-a-service fin 2025 »

• Contexte & ce qu'il s'est passé récemment

- En novembre 2025, plusieurs firmes de cybersécurité ont alerté sur l'essor des offres de "ransomware-as-a-service" (RaaS) sur le dark web : des kits prêts à l'emploi, accessibles à quasi tout acteur malveillant, ce qui facilite la multiplication des attaques.
- Dans le même temps, le "phishing 2.0" — c'est-à-dire des campagnes d'hameçonnage beaucoup plus personnalisées — se généralise : les attaquants utilisent parfois l'IA pour rédiger des mails extrêmement convaincants, imitant le style d'une entreprise ou d'un contact connu, rendant la détection plus difficile pour les utilisateurs.

• Pourquoi c'est important

- L'apparition de RaaS transforme la menace : plus besoin d'être un pirate chevronné pour lancer un ransomware. Même des "amateurs du dark web" peuvent acheter ou louer ces outils, ce qui augmente fortement le volume d'attaques, y compris contre des PME, des TPE, ou des petits organismes — des structures comme celle que tu pourrais reprendre.
- Le phishing 2.0 met en évidence la dimension humaine de la cybersécurité : la sophistication des messages rend les utilisateurs moins vigilants, la confiance exploitable, ce qui rend les défenses techniques seules insuffisantes.

• Impacts attendus

- Accroissement des demandes de rançon, des fuites de données sensibles, des arrêts de service ou des pertes financières pour les entreprises victimes.
- Montée en flèche des intrusions "automatisées" : des attaques massives, menées à l'échelle industrielle, ciblant tout type d'organisation — administrations, entreprises, prestataires.
- Besoin accru de sensibilisation des employés, de formation à la détection des tentatives d'hameçonnage, et de politiques internes (double validation, vérification des liens, etc.).

• Que retenir pour un futur administrateur / chef d'entreprise

- Être capable de **mettre en place des outils de défense complets** (antivirus/antimalware, sauvegardes régulières, isolation de systèmes critiques, accès restreint).
- **Former les utilisateurs** : sensibilisation aux mails suspects, usage prudent du web, vérification des expéditeurs, scepticisme sur les demandes inhabituelles.
- **Mettre en place une politique de sauvegarde et de restauration** performante, et prévoir un plan de réponse aux incidents — indispensable face au ransomware.
- **Adopter une approche "hybride"** : combiner sécurité technique + sensibilisation + organisation / processus interne.

Sources :

- Capture the Bug. "Latest Cybersecurity News November 2025." capturethebug.xyz.
- Oodrive. "Top 10 des Cyberattaques de 2025." oodrive.com.