UKRAINE

TÉLÉCHARGEZ LE RAPPORT COMPLET EN ANGLAIS

Le soutien continu de Talos à l'Ukraine a été au cœur de nos efforts opérationnels cette année. Guidé par notre mission principale consistant à protéger la population et les infrastructures ukrainiennes, Talos a mis en place un groupe de travail de plus de 40 volontaires dédiés à la défense de nos clients et de nos partenaires. Cette équipe d'experts supervise les infrastructures stratégiques afin d'identifier les menaces, de contrer les attaques et de collecter des informations.

PRINCIPALES MENACES

La liste suivante présente un aperçu des menaces observées par Talos qui ont ciblé les entités ukrainiennes et leurs alliés en 2022 :

- Avant et après l'invasion, nous avons vu un grand nombre de wipers destructeurs et d'autres programmes malveillants s'attaquer à des cibles ukrainiennes, notamment WhisperGate, HermeticWiper, CaddyWiper, DoubleZero et CyclopsBlink.
- Les cybercriminels ont exploité la situation en promouvant des outils informatiques qui étaient en réalité des programmes malveillants conçus pour cibler des entités russes. Ils ont également eu recours à des leurres par e-mail autour de thèmes liés à la crise afin d'effectuer des arnaques financières et de déployer des chevaux de Troie d'accès à distance.
- Le groupe d'État russe Gamaredon a distribué des programmes malveillants qui dérobaient des informations, tandis qu'un acteur soupçonné d'être commandité par l'État a tenté de perpétrer une attaque (baptisée « GoMet ») contre la chaîne d'approvisionnement.
- Le groupe Mustang Panda basé en Chine a mené des campagnes d'hameçonnage contre des entités en Europe et en Russie en utilisant de faux documents « officiels » comme leurres.
- Le groupe d'hacktivistes pro-russe Killnet a lancé des attaques par déni de service contre des sites web dans des pays pro-ukrainiens.

TENDANCES COMPORTEMENTALES

Sur la base de nos données collectées depuis début 2022, nous avons observé les tendances suivantes révélant des comportements malveillants actifs en Ukraine :

- Les utilitaires courants comme PowerShell et Windows Management Instrumentation (WMI) restent une cible de choix pour les hackers friands des attaques de type « living-off-the-land » et qui cherchent à échapper à la détection.

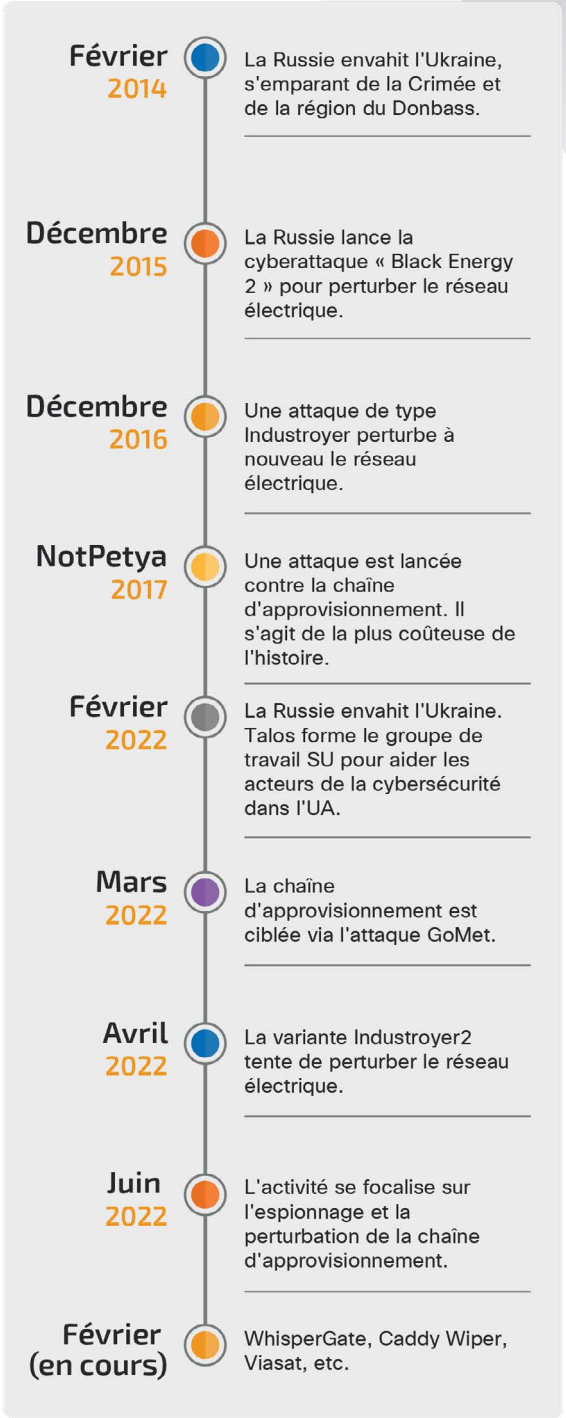

Figure 1: *Des cyberattaques majeures contre l'Ukraine.*

UKRAINE

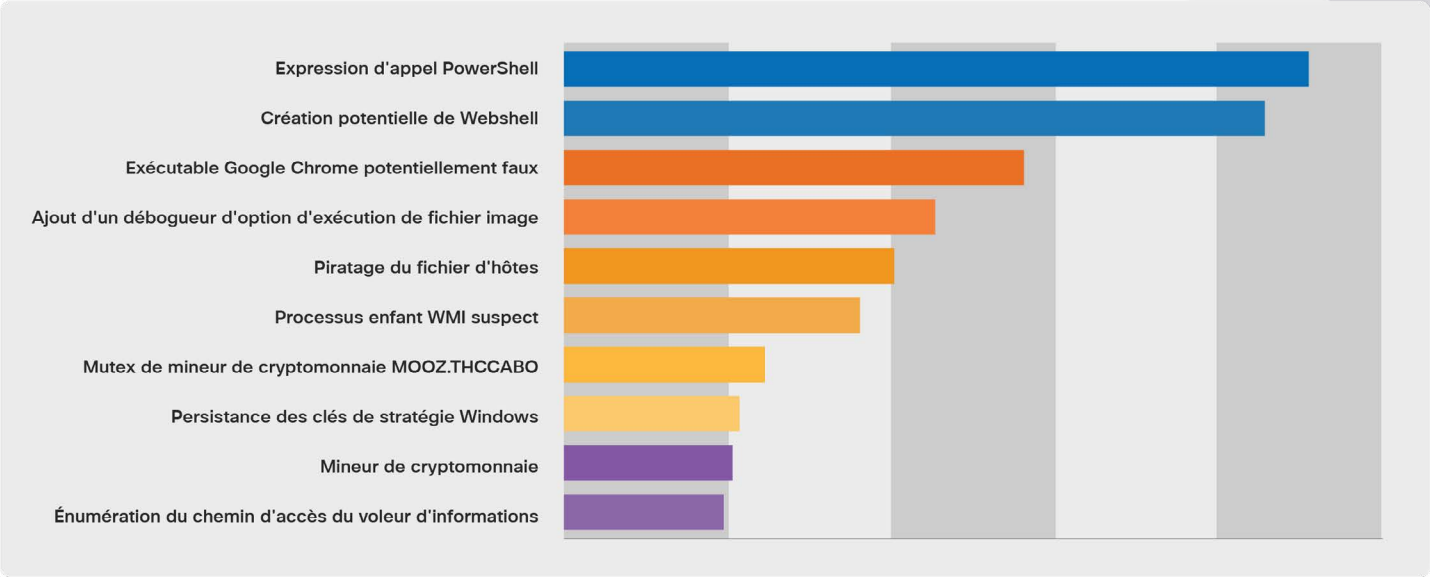

Figure 2: *Les règles de protection comportementale les plus actives de Cisco Secure Endpoint pour les clients ukrainiens auprès de qui la solution a été déployée.*

- Nous avons observé une hausse des techniques fondées sur l'utilisation d'exécutables Google Chrome et de clés de stratégie Windows pour établir la persistance.
- Les détections de vol d'informations et de minage de cryptomonnaie ont également augmenté. Il apparaît cependant que des acteurs de tous niveaux opèrent principalement dans une logique de destruction.
- Nous avons enregistré un pic d'alertes pour « Exécution d'un proxy binaire signé à l'aide de rundll32 » en Ukraine, mais aussi à l'échelle mondiale. Cette technique utilise la bibliothèque de liens dynamiques (DLL) pour exécuter du code malveillant.

Malgré l'augmentation de l'activité contre les cibles ukrainiennes, notre équipe de réponse aux incidents a constaté globalement moins de menaces visant les clients de Cisco au cours du premier semestre de 2022. Il est possible que le conflit ait attiré des hackers qui, en d'autres circonstances, auraient sévi ailleurs.

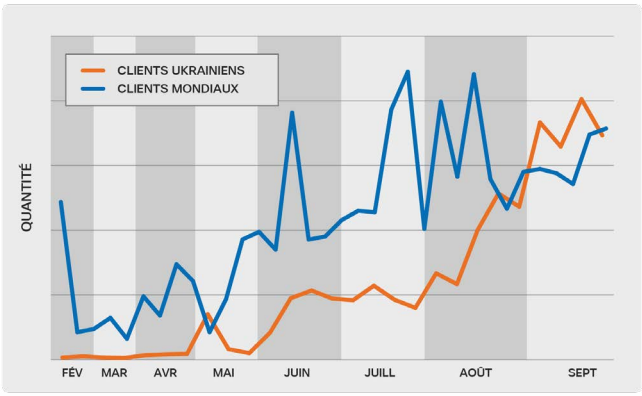

Figure 3: *Détections de prévention d'exploits pour « Exécution d'un proxy binaire signé à l'aide de rundll32 » chez des clients ukrainiens et mondiaux, entre février et septembre 2022.*

CONCLUSION

Rien n'indique que le rythme des cyberattaques contre l'Ukraine ralentisse et que le cyberconflit se terminera à la fin des hostilités. En effet, les tensions régionales et la diversité des acteurs impliqués suggèrent que les attaques contre l'Ukraine vont probablement se poursuivre. En outre, nous estimons que les hackers russes sont susceptibles de se livrer à des attaques destructrices pour affecter l'issue de la guerre.