GATEWATCHER

Cyber threats SEMESTER REPORT_

Janvier - Juin 2023

Menaces cyber décodées par la Purple Team de Gatewatcher

Executive Summary

Fournir davantage de visibilité à vos équipes dans un paysage de risques toujours plus changeant.

LES ESSENTIELS :

Classement des *malwares* les plus utilisés par les cyberattaquants_

Impacté par la désactivation par Microsoft des macros office, son principal vecteur d'attaque, Emotet sort du trio de tête, remplacé par Qbot. Malgré les actions des autorités, Mirai conserve une écrasante suprématie avec des capacités d'infection multi-architecture soutenues par ses nombreux variants. Payload est secondaire mais reste plus fréquemment utilisé dans la chaine d'infection. Cobalt strike conforte également sa position.

Les types de *fichiers exploités* par les attaquants et leur évolution_

Le classement reste dominé par les binaires Windows, HTML et ELF, porté par les attaques cross-plateform contre Linux, soulignant ainsi l'évolution rapide du paysage des menaces informatiques. L'évolution la plus notable concerne la progression des fichiers portables exécutables contenant pour certains des capacités d'exploitation des DLL à des fins malveillantes comme des attaques sans fichiers.

Les *threat actors* les plus actifs_

Analyse des tactiques employées avec un focus sur les attaques par la chaine d'approvisionnement au travers des exemples PyPI/W4SP, 3CX, MOVEit et Jumpcloud ainsi que sur le groupe russe Turla.

Les *secteurs d'activités* particulièrement visés par les menaces_

L'éducation défraie régulièrement la chronique des cyberattaques et s'est hissée en troisième position des secteurs les plus visés derrière la technologie et l'énergie : analyse détaillée. Focus également sur les nouvelles menaces visant les systèmes OT dans le cadre de la croissance de l'industrie 4.0.

Impact des *fuites d'identifiants*_

Nouveauté de ce rapport semestriel, le résumé des identifiants (adresses mail + mots de passe) ayant le plus fuité à cause de malware, phishing, etc. Noms de domaine entrepreneuriaux, entreprises technologiques, ONG et système éducatif sont en place de tête. Focus sur les vulnérabilités des secteurs publics.

RETROUVEZ ÉGALEMENT LE DECRYPTAGE TECHNIQUE DE NOS ANALYSTES SUR :

- La popularisation du détournement d'outils légitimes par les cybercriminels à travers l'exemple de WMI.
- L'augmentation de l'utilisation de PowerShell par les cybercriminels dans le cadre des intrusions.

Pour maintenir le plus haut niveau de protection, nos experts de la Purple Team mènent une veille active et analysent de manière détaillée les cybermenaces en se basant sur la riche télémétrie des plateformes #NDR et #CTI de Gatewatcher.

Retrouvez les éclairages de nos équipes sur les grandes tendances de l'activité cyber des six derniers mois au sein de ce troisième Cyber Threat Semester Report !

ACCÉDEZ AU RAPPORT