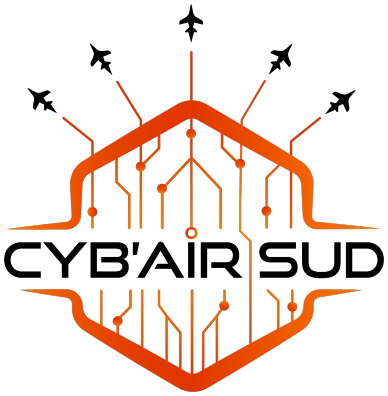


Vshell: The V stands for Verbose

CFP 2025 - English Version

Speaker: Maxime THIEBAUT

Speaker Biography

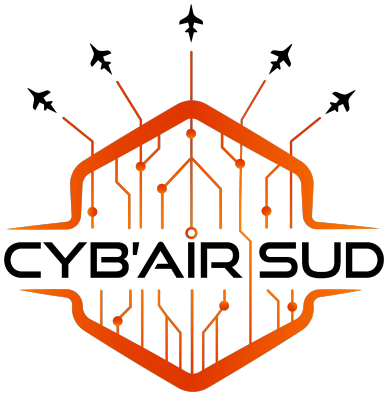
Maxime is an Incident Response & Threat Research expert at NVISO, where he dedicates his time to intrusion analysis and technical research. Outside of work, Maxime contributes to The DFIR Report where he has a keen interest in reverse engineering samples encountered in the wild.

Talk Abstract

Over the last months, Vshell has been leveraged in multiple high-profile intrusions affecting government and critical sectors. Through this presentation, attendees will be introduced to the Vshell command & control framework. The session will disclose how Vshell C2s can be fingerprinted worldwide and showcase how combined netflow data allows for effective victim identification. NVISO will furthermore cover Vshell's network communication encryption and showcase how network captures can subsequently be decrypted, providing law enforcement with on-the-wire attacker monitoring capabilities.

Other Information

— Talk duration: 30 minutes
— Language: English
— TLP classification: TLP:GREEN
— Speaker details: Maxime THIEBAUT, 1996-05-24, Belgium



Vshell : Le V signifie Verbose

CFP 2025 - Version Française

Intervenant : Maxime THIEBAUT

Biographie de l'intervenant

Maxime est un expert en Incident Response et recherche sur les menaces chez NVISO, où il se consacre à l'analyse d'intrusions et à la recherche technique. En dehors de son travail, Maxime contribue à The DFIR Report, s'intéressant particulièrement à la rétro-ingénierie des échantillons rencontrés sur le terrain.

Résumé de la présentation

Au cours des derniers mois, Vshell a été utilisé dans plusieurs intrusions de haut niveau touchant des gouvernements et des secteurs critiques. Cette présentation introduira aux participants le framework de commande et contrôle Vshell. La session expliquera comment identifier les C2 Vshell dans le monde et montrera comment l'analyse combinée des flux réseau permet d'identifier efficacement les victimes. NVISO couvrira également le chiffrement des communications réseau de Vshell et présentera comment les captures réseau peuvent ensuite être décryptées, offrant aux forces de l'ordre des capacités de suivi en temps réel des attaquants.

Autres informations

- Durée de la présentation : 30 minutes
- Langue : Anglais
- Classification TLP : TLP :GREEN
- Détails de l'intervenant : Maxime THIEBAUT, 1996-05-24, Belgique