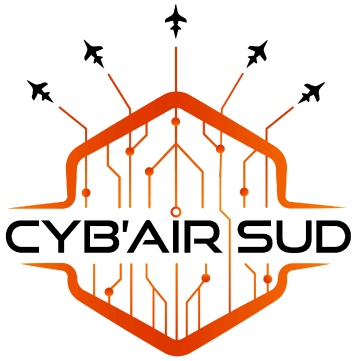


Talk Proposal

For Cyb'Air Sud 2025

Title: Trust Me, I'm a Shortcut: New LNK Abuse Methods

Suggested duration

30 minutes

Abstract

Windows shortcut (.LNK) files have remained a consistent attack vector for over several decades, yet their underlying format is still largely archaic and remains the "gift that keeps on giving" by presenting new opportunities for abuse, even in 2025. This talk provides, after showing an overview of the LNK file structure that outlines its quirks and legacy design choices that contribute to persistent security weaknesses, several novel and previously undocumented techniques will be presented that enable more stealthy, deceptive, and flexible payload delivery/command execution through LNK files than those currently known. We will look at why these new techniques 'work', compare them to existing LNK tricks, and discuss the implications for defenders. The research involved developing a custom testing framework aimed at black-box testing and probing Microsoft's LNK parsing implementation, revealing subtle flaws and unexpected behaviours exploitable by attackers. We will discuss how adopting a "hacker's mindset" helps in uncovering new methods for abuse like this; and how this way of thinking can benefit everyone active in cyber security, regardless of your sub-discipline or specialisation. Finally, this session will also introduce an open-source tool designed to assist security professionals, red teams, and researchers in generating and experimenting with advanced LNK payloads. This tool aims to enhance the ability to simulate and defend against sophisticated shortcut-based attacks, thereby improving Windows endpoint security.

Abstract (short version)

Windows shortcut (.LNK) files have been a reliable vector for attackers for over two decades, yet their underlying structure remains archaic and under-scrutinized. In this talk,

we'll examine the quirks and limitations of the LNK file format and demonstrate several novel abuse techniques that have not been previously documented. These methods enable stealthier, more deceptive, and more flexible payload delivery than existing approaches. The research behind these findings, including the development of a custom testing framework to probe Microsoft's LNK handling, will be shared to illustrate how adopting a "hacker's mindset" can drive effective security research. The session will conclude with the release of a new tool that allows security professionals to generate and test these advanced shortcut-based attacks in their own environments.

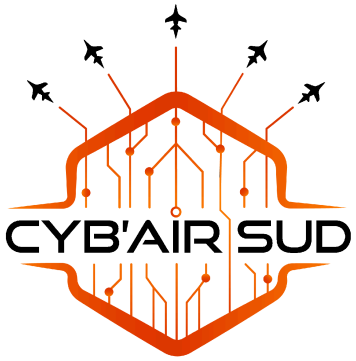
Outline

1. **Introduction & Context Setting (4 min)** • Brief speaker intro: who is Wietze and what gives him credibility?
   • What are LNK files and why do they matter in security?
   • Real-world examples of LNK abuse to hook all experience levels
2. **LNK Format Fundamentals - A Gentle Technical Dive (6 min)** • Explain the core structure of LNK files with simple visuals/examples
   • Highlight quirks and legacy design decisions that create abuse opportunities
   • Brief overview of common, well-known LNK abuse techniques
3. **Adopting the Hacker's Mindset: Research Methodology (5 min)** • Explain the importance of curiosity and creative testing in security research
   • Detail the custom testing framework: fuzzing LNK parsing and probing Windows internals
   • Share interesting low-level findings and unexpected behaviours discovered
4. **Deep Dive: Novel LNK Abuse Techniques (10 min)** • Present several new, previously undocumented methods with technical depth
   • Demonstrate (ideally live, alternatively a video) how these techniques manipulate LNK internals
   • Discuss detection/DFIR challenges and practical implications
5. **Tool Release: Empowering Research and Red Teams (3 min)** • Introduce my new tool that automates crafting these new LNK abuse cases
   • Show key features and practical uses for blue and red teams
   • Quick demo (ideally live, alternatively a video)
6. **Summary (2 min)** • Recap core insights and defence implications
   • Announce public availability of the tool and resources

Speaker Bio

Wietze has been hacking around with computers for years. Originally from the Netherlands, he currently works as a Lead Threat Detection & Response Engineer in London. As a cyber security enthusiast and threat researcher, he has presented his findings on topics including attacker emulation, obfuscation techniques and DLL Hijacking at a variety of security conferences. By sharing his research, publishing related tools and his involvement in the

open-source projects such as LOLBAS, HijackLibs and ArgFuscator, he aims to give back to the community he learnt so much from.



Proposition de conférence

Pour Cyb'Air Sud 2025

Titre : Trust Me, I'm a Shortcut : New LNK Abuse Methods

Durée suggérée

30 minutes

Résumé

Les fichiers de raccourci Windows (.LNK) sont restés un vecteur d'attaque constant depuis plusieurs décennies, et pourtant leur format sous-jacent reste archaïque et continue d'offrir de nouvelles opportunités d'abus, même en 2025. Cette présentation propose, après un aperçu de la structure des fichiers LNK mettant en lumière leurs bizarreries et choix de conception hérités, plusieurs techniques inédites et non documentées permettant une exécution de commandes ou une livraison de charges utiles plus furtive, trompeuse et flexible que les méthodes connues à ce jour. Nous verrons pourquoi ces nouvelles techniques fonctionnent, les comparerons aux astuces LNK existantes, et discuterons de leurs implications pour les défenseurs. La recherche s'est appuyée sur le développement d'un cadre de test personnalisé visant à tester en boîte noire l'implémentation du parsing LNK de Microsoft, révélant des failles subtiles et des comportements inattendus exploitables. Nous discuterons de l'intérêt d'adopter une « mentalité hacker » pour découvrir de nouvelles méthodes d'abus, et comment cette approche peut bénéficier à tous les professionnels de la cybersécurité, quel que soit leur domaine. Enfin, cette session présentera un outil open-source destiné à aider les professionnels de la sécurité, les red teams et les chercheurs à générer et expérimenter des charges utiles avancées via des fichiers LNK. Cet outil vise à améliorer la capacité à simuler et contrer les attaques sophistiquées basées sur les raccourcis, renforçant ainsi la sécurité des postes Windows.

Résumé (version courte)

Les fichiers de raccourci Windows (.LNK) sont un vecteur fiable pour les attaquants depuis plus de vingt ans, mais leur structure reste peu étudiée. Dans cette présentation, nous examinerons les bizarreries et limitations du format LNK et démontrerons plusieurs

techniques d'abus inédites. Ces méthodes permettent une livraison de charges utiles plus furtive, trompeuse et flexible que les approches existantes. Nous partagerons les résultats de la recherche, incluant le développement d'un cadre de test personnalisé pour analyser le traitement des LNK par Microsoft, afin d'illustrer comment une « mentalité hacker » peut stimuler la recherche en sécurité. La session se conclura par la présentation d'un nouvel outil permettant aux professionnels de générer et tester ces attaques avancées dans leurs propres environnements.

Plan

1. **Introduction & Contexte (4 min)** • Présentation de l'intervenant : qui est Wietze et pourquoi est-il légitime ?
   • Que sont les fichiers LNK et pourquoi sont-ils importants en sécurité ?
   • Exemples concrets d'abus de LNK pour capter tous les niveaux d'expérience
2. **Fondamentaux du format LNK (6 min)** • Structure de base des fichiers LNK avec visuels simples
   • Bizarreries et choix hérités favorisant les abus
   • Tour d'horizon des techniques d'abus LNK bien connues
3. **Adopter une mentalité hacker : méthodologie (5 min)** • Importance de la curiosité et des tests créatifs en recherche sécurité
   • Détails du cadre de test personnalisé : fuzzing et analyse des internals Windows
   • Découvertes intéressantes et comportements inattendus
4. **Approfondissement : nouvelles techniques d'abus LNK (10 min)** • Présentation de méthodes inédites avec détails techniques
   • Démonstration (en direct ou vidéo) de manipulation des LNK
   • Défis de détection et implications pratiques
5. **Présentation de l'outil (3 min)** • Introduction de l'outil facilitant la création de cas d'abus LNK
   • Fonctionnalités clés pour les équipes bleues et rouges
   • Démo rapide (en direct ou vidéo)
6. **Conclusion (2 min)** • Récapitulatif des points clés et implications défensives
   • Annonce de la mise à disposition de l'outil et des ressources

Biographie de l'intervenant

Wietze bidouille les ordinateurs depuis de nombreuses années. Originaire des Pays-Bas, il travaille actuellement à Londres comme Lead Threat Detection & Response Engineer. Passionné de cybersécurité et chercheur en menaces, il a présenté ses travaux sur l'émulation d'attaquants, les techniques d'obfuscation et le DLL Hijacking dans diverses conférences. En partageant ses recherches, ses outils et sa participation à des projets open-source comme LOLBAS, HijackLibs et ArgFuscator, il souhaite contribuer à la communauté dont il a tant appris.