# Mise en évidence de chemins d'attaque implicites en environments Windows

Manuel POISSON
*CentraleSupelec, CNRS, Inria, Univ. Rennes, IRISA*
Rennes, France
manuel.poisson@irisa.fr

Valérie VIET TRIEM TONG
*CentraleSupelec, CNRS, Inria, Univ. Rennes, IRISA*
Rennes, France
valerie.viettriemtong@centralesupelec.fr

Gilles GUETTE
*Univ. Rennes, CNRS, Inria, IRISA*
Rennes, France
gilles.guette@univ-rennes.fr

Erwan ABGRALL
*CentraleSupélec, Inria*
Rennes, France
erwan.abgrall@centralesupelec.fr

***Abstract*—Un attaquant ciblant un système cherche en général à rester indétectable le plus longtemps possible. Il doit éviter autant que possible d'exécuter des actions caractéristiques d'attaques connues. Une façon d'éviter la détection est d'exécuter seulement des actions qui semblent légitimes. Il s'agit d'actions qui sont, soit autorisées par la configuration du système, soit possibles en détournant l'usage de services légitimes. Cet article présente AWARE (Attacks in Windows Architectures REvealed), un outil défensif pour requêter une infrastructure Windows et construire un graphe de positions d'attaque révélant les chemins d'attaque que pourrait suivre un attaquant durant la phase de propagation de sa campagne d'attaque. Les chemins d'attaque découverts par AWARE se basent uniquement sur des actions légitimes du système et l'utilisation de services dits Living-Off-The-Land. Ces chemins sont donc critiques pour le défenseur car difficiles à surveiller.**

***Index Terms*—graphe d'attaque, campagne d'attaque, intrusion, LotL**

## I. Introduction

Avec les avancées de la recherche en sécurité, les attaquants inventent de nouvelles façons de contrer les solutions existantes. L'attaquant et le défenseur sont deux joueurs au jeu du chat et de la souris. Généralement, un défenseur utilise une solution de supervision ou des outils de sécurité pour surveiller les actions effectuées sur le système et détecter les actions en cours pouvant être symptomatiques d'une attaque. Les outils du défenseur peuvent implémenter une approche basée sur des signatures, qui consiste à comparer en temps réel les observations faites sur le système avec les caractéristiques d'attaques connues. L'attaquant peut rester furtif en employant de nouvelles techniques d'attaque ou des variations d'attaques connues. Cela est néanmoins couteux car il lui faut constamment renouveler ses outils et procédures d'attaque. Plus simplement, l'attaquant peut utiliser les outils légitimes du système cible et détourner leur usage pour progresser dans sa campagne d'attaque. Une tactique d'attaque évasive devenue populaire est l'utilisation de techniques Living-Off-The-Land (LotL) [1]. Les LotL détournent l'utilisation habituelle d'outils préexistants pour réaliser des actions malveillantes. La vaste portée de ces outils leur permet d'être utilisés à toutes les étapes de la *killchain* [2] : de la compromission initiale à l'effet final sur la cible.

Pour le défenseur, le principal problème des LotL est qu'ils sont difficiles à retirer du système car leur déploiement sert à l'utilisation et à l'administration du système en question. Nous traitons ce problème dans cet article et proposons AWARE (Attacks in Windows Architectures REvealed), un outil pour calculer l'ensemble des positions d'attaque existantes dans un système et dévoiler comment un attaquant peut bouger d'une position à l'autre en exploitant uniquement des privilèges et outils légitimes. AWARE est spécialisé dans les techniques qui permettent un mouvement entre les différents comptes et machines légitimes du système. Ces mouvements servent à un attaquant à progresser dans le système à la recherche de sa cible. On parle habituellement de propagation dans les modèles de *killchain* [3]. Dans la matrice ATT&CK[1], ces mouvements couvrent les tactiques *discovery*, *privilege escalation* et *lateral movement*. Cet article traite ainsi la question critique :

> **Comment un administrateur système peut-il être au courant des chemins d'attaque permettant à un attaquant de se propager furtivement grâce à la configuration système et aux outils légitimes déployés?**

Pour répondre à cette question, nous proposons AWARE, un outil capable de requêter les machines et l'Active Directory (AD) du système d'information (SI) afin de générer un graphe de positions d'attaque qu'un attaquant peut traverser en utilisant seulement des actions légitimes sur le SI. AWARE permet ainsi au défenseur d'analyser son SI de façon préventive.

Le lien avec les travaux existants dans ce domaine d'étude est fait en Section II. La Section III explique la structure et la signification du graph de positions d'attaque calculé par AWARE. La construction de ce graph est détaillé en Section IV. Enfin, la Section V présente les résultats obtenus.

[1]https://attack.mitre.org/

## II. État de l'art

AD est certainement la solution la plus populaire pour les entreprises pour gérer les comptes informatique de leurs employés [4]. Il sert à la gestion d'identité et offre un mécanisme d'authentification et d'autorisation centralisé dans une architecture utilisant le système d'expoitation Windows. L'annuaire stocke des données sur tous les utilisateurs du système et leurs droits. C'est donc une cible privilégiée des cyberattaques [5]. Les architectures AD sont compliquées à gérer et administrer de façon sécurisée. Des outils dédiés ont donc été développés pour les auditer. Certains d'entre eux, comme Oradad[2], PingCastle[3] et Bloodhound[4], sont comparés dans [6]. PingCastle récupère des données sur les contrôleurs de domaine (ordinateurs utilisé pour gérer d'autres ressources dans l'architecture) et les postes de travail client dans l'AD. Puis, il utilise ces données pour générer un rapport avec une liste de vulnérabilités trouvées associées à un score de sécurité, une description et un lien vers plus de documentation. PingCastle peut aussi générer un graphe représentant des relations logiques entre objets AD, comme l'appartenance d'un utilisateur à un groupe. Ce graphe aide à comprendre la structure globale d'une architecture AD, mais ne permet pas de montrer facilement les chemins d'attaque.

Dans une architecture standard, AD stocke beaucoup d'objets différents et leurs relations, qui peuvent être très subtiles à détecter. Bloodhound sert à révéler les relations (éventuellement involontaires) entre des objets AD. Le graphe de Bloodhound, contrairement à celui de PingCastle, montre la possibilité pour des utilisateurs d'agir sur des machines distantes (*e.g.* avec RDP[5] ou PSRemote[6]). Cela le rend meilleur pour représenter des chemins d'attaque.

Cependant, ces outils ne permettent pas de vérifier s'il est possible pour un utilisateur d'élever localement ses privilèges du fait de la configuration spécifique d'une machine telle qu'une permission faible sur un service (local) par exemple. Il faut néanmoins le considérer pour trouver le maximum de chemin d'attaque existant réellement sur une architecture et ainsi les désactiver ou au moins les surveiller avec attention.

Des outils spécialisés dans la détection des possibilités d'élévations de privilèges existent. Par exemple, Mimikatz [7] permet, dans certains cas, de récupérer les identifiants sauvegardés sur une machine. De même, WinPEAS [8] vérifie si une ou plusieurs élévations de privilèges existent sur une machine utilisant Windows (*e.g.* en exploitant une configuration de service faible). Ces outils dévoilent la possibilité pour un utilisateur de prendre le contrôle d'un autre compte utilisateur sans expliquer précisément comment le faire. De plus, c'est la succession de mouvements entre comptes utilisateur qui est le plus difficile à détecter et donc le plus dangereux. Enfin, il faut garder en tête que l'accès à un nouvel utilisateur peut n'être qu'une étape pour accéder à une nouvelle machine.

[2]https://github.com/ANSSI-FR/ORADAD
[3]https://www.pingcastle.com/
[4]https://bloodhound.readthedocs.io/en/latest/
[5]Remote Desktop Protocol
[6]Powershell Remote

Notre solution permet de visualiser, à l'aide d'un graphe, les chemins d'attaque existants dans une architecture. AWARE représente plusieurs façons dont un attaquant peut se propager en se connectant d'une machine à l'autre ou prenant le contrôle de nouveaux comptes utilisateurs.

## III. Construction d'un graphe de positions d'attaque dans un système Windows

Nous considérons un réseau $\mathcal{M}$ de machines utilisées par un ensemble $\mathcal{U}$ d'utilisateurs avec des comptes légitimes. Nous faisons l'hypothèse qu'un attaquant avancé à déjà réussi une compromission initiale et a donc accès à un compte légitime sur une machine. Nous étudions la phase de propagation durant laquelle un attaquant progresse dans le réseau pour atteindre sa cible. L'espace de propagation de l'attaquant est représenté par un graphe orienté de positions d'attaque. Une position d'attaque, telle que définie dans [9], est une paire $(m, u)$ représentant le fait qu'un attaquant a compromis le compte de l'utilisateur $u \in \mathcal{U}$ sur la machine $m \in \mathcal{M}$. L'attaquant peut ensuite se déplacer entre les positions d'attaque avec :

- un mouvement latéral : l'attaquant prend le contrôle d'une autre machine en conservant le même compte utilisateur
- un mouvement vertical (*aka* élévation de privilèges) : l'attaquant prend le contrôle d'un autre utilisateur en restant sur la même machine.

AWARE traque les mouvements qu'un attaquant peut effectuer en utilisant exclusivement des techniques Living-Off-The-Land (LotL). Les LotL sont des binaires déjà présents sur les systèmes (*e.g.* outils d'administrations légitimes signés) et exploités lors d'activité post-exploitation. Une analyse de l'utilisation de ces techniques par les *malwares* sur les systèmes Windows a été réalisée par Barr-Smith *et al.* [1]. Elle confirme un taux de détection faible pour plusieurs techniques LotL documentées pour presque chaque produit antivirus évalué tandis que $9.6\%$ des *malwares* utilisent des binaires natifs du système pour accomplir des actions malveillantes.

*a) Positions d'attaque dans un système Windows:* un système Windows est classiquement gouverné par un ou plusieurs contrôleurs de domaine en charge d'authentifier et autoriser les utilisateurs et les machines dans le domaine. Du point de vue d'un attaquant, AD définit donc l'ensemble des positions d'attaque sur le système, à l'exception des comptes purement locaux. Les droits requis pour un utilisateur pour se connecter à une machine située dans un AD ont été étudiés afin de définir l'ensemble des positions d'attaque.

*b) Graphe dirigé des positions d'attaque:* ce travail s'intéresse à la façon dont un attaquant peut bouger d'une position d'attaque à l'autre et ainsi progresser dans le système, en utilisant uniquement des comportements légitimes. Nous enrichissions d'abord notre graphe, dont les nœuds représentent des positions d'attaque, avec des arcs liés aux droits d'accès. Nous ajoutons ensuite les arcs liés à l'abus de services légitimes.

## IV. Le graphe de positions d'attaque de AWARE

AWARE collecte d'abord sur le système les données qui lui servent à construire un graphe de positions d'attaque. Cette étape consiste en des requêtes légitimes depuis une unique machine du système analysé. L'ensemble des machines et utilisateurs enregistrés dans l'AD ainsi obtenus servent à calculer les positions d'attaque et les liens entre ces dernières.

*a) Calcul des positions d'attaque:* l'ensemble des positions d'attaque est formé par l'ensemble des paires $(m, u)$ où $m$ est une machine et $u$ un utilisateur tel que $u$ a un compte sur $m$. Cet ensemble de positions forme l'ensemble des nœuds du graphe d'attaque. Notre calcul considère à la fois les comptes AD et ceux purement locaux.

*b) Calcul des arcs dans le graphe d'attaque:* nous représentons les mouvements entre deux positions d'attaque dus à la configuration du système et à l'abus de services légitimes. Pour commencer, sont ajoutés les arcs dus aux mouvements latéraux possibles grâce à la configuration des droits d'accès (*i.e.* RDP et PSRemote). Puis, AWARE considère les mouvements liés à l'abus de services légitimes existants (*i.e.* mouvement lateral avec `wmic`[7] et mouvements verticaux avec `runas` et les services ayant un exécutable modifiable).

## V. Experimentations

Nous avons configuré une architecture expérimentale avec différentes possibilités de bouger entre ses six machines et vingt-deux utilisateurs. Sur cette architecture, AWARE trouve toutes les positions d'attaque, représentées par des nœuds dans un graphe. Les arcs qu'il ajoute ensuite révèlent des chemins d'attaque.

Le graphe de positions d'attaque est fait de 55 nœuds et 164 arcs. Il est (partiellement) représenté sur la Figure 1, sans les 15 nœuds n'ayant aucun arc sortant ni entrant et avec des nœuds rouges représentants les positions liées à des utilisateurs à hauts privilèges. Les arcs sont répartis comme suit : • 30 liés à PSRemote • 62 liés à RDP • 54 liés à `wmic` • 5 liés à des identifiants sauvegardés exploitables avec `runas` • 13 liés à un service avec executable modifiable.

Nous pouvons d'abord noter que le graphe est constitué de deux parties distinctes. En bas à droite, 4 positions d'attaque sont complètement déconnectées des autres. Par ailleurs, deux zones particulièrement denses ressortent en haut. Leur densité illustre la forte valeur de leurs utilisateurs pour un attaquant car accéder à une position d'attaque dans l'une de ces zone signifierait accéder à de nombreuses nouvelles positions d'attaque. Les arcs entrant dans ces zones sont donc critiques.

Le graphe de positions d'attaque a ainsi permis de révéler le plus court chemin entre deux positions d'attaque présentes dans notre architecture expérimentale. Ce chemin, composé de 5 positions d'attaque différentes, exploite 2 mouvements latéraux différents et 2 mouvements verticaux différents. Il constitue un scénario d'attaque exploitable complet.

Pour conclure, AWARE collecte sur l'architecture complète, les données utiles pour construire un graphe représentant toutes les positions d'attaque et des mouvements entre elles. Ce graphe révèle des chemins d'attaque exploitables dans notre architecture expérimentale. Cette connaissance est cruciale pour un administrateur système afin de rapidement identifier et appliquer les contre-mesures pour protéger son système.

[7]Windows management Instrumentation command-line

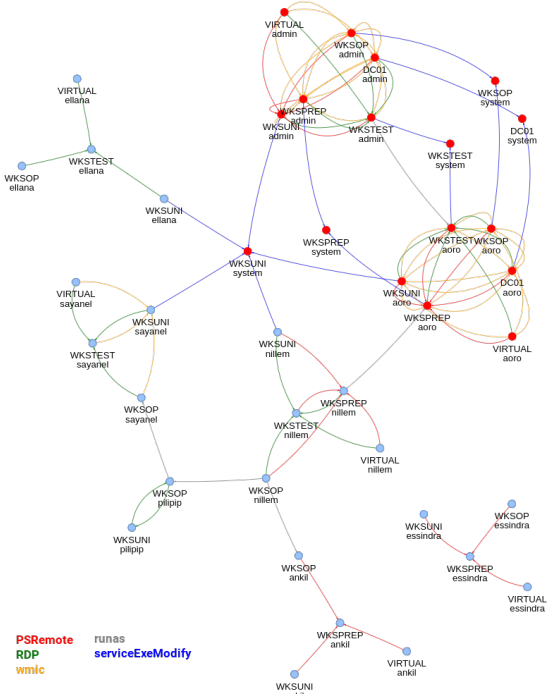


Fig. 1. Graphe de positions d'attaque dans l'architecture experimentale.

## References


[1] F. Barr-Smith, X. Ugarte-Pedrero, M. Graziano, R. Spolaor, and I. Martinovic, "Survivalism: Systematic analysis of windows malware living-off-the-land," in *2021 IEEE Symposium on Security and Privacy (SP)*, 2021, pp. 1557–1574.

[2] A. Berady, V. Viet Triem Tong, G. Guette, C. Bidan, and G. Carat, "Modeling the Operational Phases of APT Campaigns," in *CSCI 2019 - 6th Annual Conf. on Computational Science & Computational Intelligence*, Las Vegas, United States, Dec. 2019, pp. 1–6. [Online]. Available: https://hal.inria.fr/hal-02379869

[3] M. Ring, S. Wunderlich, D. Scheuring, D. Landes, and A. Hotho, "A survey of network-based intrusion detection data sets," *Computers & Security*, vol. 86, pp. 147–167, 2019. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0167404819301188X

[4] G. McDonald, P. Papadopoulos, N. Pitropakis, J. Ahmad, and W. J. Buchanan, "Ransomware: Analysing the impact on windows active directory domain services," *Sensors*, vol. 22, no. 3, 2022.

[5] W. Matsuda, M. Fujimoto, and T. Mitsunaga, "Detecting apt attacks against active directory using machine leaning," in *2018 IEEE Conference on Application, Information and Network Security (AINS)*, 2018, pp. 60–65.

[6] T. Loret, "Active Directory : Comparaison de différents outils d'audit et d'entretien," Nov. 2021. [Online]. Available: https://evabssi.com/active-directory-comparaison-de-differents-outils-daudit-et-dentretien/

[7] S. DUCKWALL and B. Delpy, "Abusing microsoft kerberos: Sorry you guys don't get it," *Blackhat*, 2014.

[8] E. Caroscio, J. Paul, J. Murray, and S. Bhunia, "Analyzing the ransomware attack on d.c. metropolitan police department by babuk," in *2022 IEEE International Systems Conference (SysCon)*, 2022, pp. 1–8.

[9] A. Berady, M. Jaume, V. Viet Triem Tong, and G. Guette, "PWNJUTSU: A dataset and a semantics-driven approach to retrace attack campaigns," *IEEE Transactions on Network and Service Management*, pp. 1–13, 2022. [Online]. Available: https://hal.inria.fr/hal-03694719