Détection des Anomalies d'Exécution Automatique au Démarrage (MITRE T1547) avec Wazuh : Renforcer la Sécurité des Systèmes contre les Menaces Persistantes

MAI 2025

Article rédigé par **KAMGA FODOUOP Armel**

Consultant Informatique Analyste Soc chez RHOPEN Labs.

Avertissement de Non-Responsabilité

L'information contenue dans cet article est destinée à des fins éducatives et de sensibilisation uniquement, en particulier pour les professionnels de la cybersécurité dans les pays d'Afrique francophone.

Les exemples et les scénarios décrits ici ne doivent en aucun cas être utilisés pour des activités illégales ou non éthiques. Les auteurs et distributeurs de cet article déclinent toute responsabilité quant à l'utilisation incorrecte ou malveillante des informations fournies.

Les entreprises et les individus doivent consulter des professionnels en cybersécurité pour obtenir des conseils spécifiques adaptés à leurs besoins et contextes uniques. Toute tentative d'exploiter les failles de sécurité décrites dans cet article pour des gains personnels ou professionnels illégitimes est fortement condamnée et peut entraîner des poursuites judiciaires.

INTRODUCTION

La cybersécurité est devenue une préoccupation majeure pour les organisations à travers le monde, alors que les attaquants adoptent des stratégies de plus en plus sophistiquées et coordonnées. Dans ce contexte, le Red Report 2025 fournit une analyse approfondie des tactiques, techniques et procédures (TTP) les plus répandues observées au cours de l'année précédente. Parmi les techniques mises en lumière, la technique MITRE T1547, **Boot or Logon Autostart Execution**, se distingue comme l'une des méthodes les plus couramment utilisées par les malwares en 2024.

La technique T1547 permet aux attaquants d'assurer la **persistance ; Élévation de Privilèges ; Furtivité ; Contournement des Logiciels de Sécurité ; Exécution de Commandes à Distance.** Les attaquants assurent la persistance de leurs logiciels malveillants en s'intégrant aux processus de démarrage du système ou d'ouverture de session utilisateur. Cela signifie que même après une tentative de suppression, le malware peut continuer à se réactiver à chaque démarrage du système. Cette capacité à échapper à la détection et à maintenir un accès prolongé aux systèmes compromis en fait une technique redoutablement efficace.

Cet article se penche sur l'analyse de la technique MITRE T1547 à travers le prisme de Wazuh, une solution de sécurité ouverte qui permet de détecter et de répondre aux menaces. En s'appuyant sur les conclusions du Red Report 2025, nous examinerons comment T1547 est exploitée par les attaquants, son impact sur la sécurité des systèmes, et les mesures que les équipes de sécurité peuvent prendre pour renforcer leur défense contre cette menace.

I. Compréhension de la Technique MITRE T1547

Définition et fonctionnement de T1547

La technique MITRE T1547, connue sous le nom de **Boot or Logon Autostart Execution**, désigne les méthodes par lesquelles un logiciel malveillant s'assure de son exécution automatique lors du démarrage du système ou de la connexion d'un utilisateur. Cette technique est particulièrement redoutable car elle permet aux attaquants de maintenir une présence persistante sur les systèmes compromis, même après des tentatives de désinfection ou de redémarrage.

Description de la manière dont cette technique permet la persistance des malwares

T1547 exploite les mécanismes d'initialisation du système d'exploitation pour se réinstaller ou se relancer automatiquement. Les attaquants peuvent manipuler divers points d'entrée, tels que les clés de registre, les dossiers de démarrage ou les tâches planifiées, pour s'assurer que leur code malveillant s'exécute à chaque démarrage ou connexion. En intégrant leurs payloads dans ces processus de démarrage, les cybercriminels peuvent contourner les solutions de sécurité qui ne surveillent généralement pas ces mécanismes.

Cette technique comprend un ensemble de sous-techniques qui permettent aux attaquants de garantir l'exécution automatique de leur code malveillant lors du démarrage du système ou de la connexion d'un utilisateur. Ces sous-techniques exploitent divers mécanismes du système d'exploitation pour maintenir la persistance des malwares, rendant leur détection et leur suppression plus difficiles.

Voici les 14 sous-techniques identifiées sous T1547 :

T1547.001 - Registry Run Keys / Startup Folder
T1547.002 - Authentication Package
T1547.003 - Time Providers
T1547.004 - Winlogon Helper DLL
T1547.005 - Security Support Provider
T1547.006 - Kernel Modules and Extensions
T1547.007 - Re-opened Applications
T1547.008 - LSASS Driver
T1547.009 - Shortcut Modification
T1547.010 - Port Monitors
T1547.012 - Print Processors
T1547.013 - XDG Autostart Entries
T1547.014 - Active Setup
T1547.015 - Login Items

Chacune de ces sous-techniques représente une méthode spécifique par laquelle un logiciel malveillant peut s'assurer qu'il sera exécuté automatiquement, exploitant ainsi les fonctionnalités normales du système pour masquer ses activités malveillantes. La compréhension de ces sous-techniques est essentielle pour renforcer la sécurité des systèmes et détecter les comportements suspects.

Exemples de mise en œuvre

Le **Red Report 2025** met en lumière plusieurs exemples d'attaques utilisant la technique T1547, illustrant sa prévalence croissante dans le paysage des menaces. Les cas de malwares suivants sont évoqués dans le rapport à titre d'illustration:

- **SneakThief** : sous-technique T1547.001 - Registry Run Keys / Startup Folder

Ce malware fictif, utilisé comme exemple dans le rapport, incarne les comportements sophistiqués des nouvelles menaces. SneakThief utilise des techniques de persistance pour s'ancrer profondément dans les systèmes cibles, rendant son élimination difficile. En intégrant ses composants dans les processus de démarrage, SneakThief parvient à exfiltrer des données tout en restant indétecté par les systèmes de sécurité.

- **Medusalocker**: sous-technique T1547.001 - Registry Run Keys / Startup Folder

Ce ransomware utilise également la technique T1547 pour garantir sa persistance. En s'insérant dans les mécanismes de démarrage du système, Medusalocker s'assure que son code est exécuté à chaque démarrage, augmentant ainsi les chances de chiffrer les données de la victime et de demander une rançon.

II. Analyse de la Prévalence de T1547 dans le Red Report 2025

Statistiques et tendances

Dans le **Red Report 2025**, la technique MITRE T1547 est mise en avant comme l'une des techniques les plus observées au cours de l'année 2024. Elle figure parmi les dix principales méthodes utilisées par les cybercriminels pour garantir la persistance de leurs malwares. Les statistiques montrent que près de 40 % des incidents de sécurité analysés impliquaient l'utilisation de T1547, soulignant ainsi l'importance croissante de cette technique dans le paysage des menaces.

Impact sur les systèmes ciblés

L'impact de la technique T1547 sur les systèmes ciblés est significatif. Les malwares qui exploitent cette technique réussissent à rester actifs sur les systèmes compromis, même après des tentatives de nettoyage. Cela entraîne des conséquences telles que :

- **Perte de données** : Les attaquants peuvent accéder et exfiltrer des informations sensibles, entraînant des pertes financières et de réputation pour les entreprises.
- **Interruption des services** : La persistance des malwares peut provoquer des interruptions de services critiques, affectant la productivité et la continuité des activités.
- **Coûts de remédiation** : Les entreprises doivent investir des ressources considérables pour détecter, éradiquer et remédier aux effets des infections, ce qui peut peser lourdement sur leur budget.

Discussion des implications pour les entreprises et les organisations

Pour les entreprises et les organisations, la prévalence de T1547 souligne l'importance d'une approche proactive en matière de cybersécurité. Les implications incluent:

- **Renforcement de la sécurité des systèmes** : Il est crucial d'implémenter des mesures de sécurité robustes pour surveiller et bloquer les modifications non autorisées dans les clés de registre et les processus de démarrage.
- **Formation et sensibilisation** : La formation des employés sur les menaces potentielles et les meilleures pratiques en matière de sécurité peut réduire le risque d'infection par des malwares.
- **Planification de la réponse aux incidents** : Les organisations doivent élaborer des plans de réponse aux incidents qui incluent des procédures spécifiques pour traiter les infections persistantes telles que celles résultant de T1547.

En conclusion, la prévalence de la technique T1547 dans les incidents de sécurité met en évidence la nécessité d'une vigilance accrue et d'une stratégie de cybersécurité renforcée pour protéger les systèmes contre ces menaces persistantes.

III. Rôle de Wazuh dans la Détection de T1547

Fonctionnalités de Wazuh

Wazuh est une plateforme de sécurité open-source qui offre des fonctionnalités avancées pour la détection des menaces, la surveillance de l'intégrité des fichiers et la gestion des journaux. Ses principales fonctionnalités incluent :

- **Analyse des journaux** : Wazuh collecte et analyse les journaux d'activité des systèmes pour détecter des comportements suspects.
- **Surveillance de l'intégrité des fichiers** : Il surveille les modifications apportées aux fichiers critiques, y compris ceux liés aux clés de registre et aux processus de démarrage.
- **Alertes en temps réel** : Wazuh génère des alertes en temps réel basées sur des règles prédéfinies, permettant une réponse rapide aux incidents.
- **Détection des anomalies** : Grâce à l'apprentissage machine, Wazuh peut identifier des comportements anormaux qui peuvent indiquer une attaque.

Comment Wazuh détecte et répond aux attaques basées sur T1547

Wazuh détecte les attaques basées sur la technique T1547 en mettant en œuvre plusieurs stratégies :

- **Surveillance des clés de registre** : Wazuh peut être configuré pour surveiller les clés de registre spécifiques associées aux techniques de démarrage automatique, alertant les administrateurs en cas de changements non autorisés.
- **Analyse des fichiers de démarrage** : Il peut analyser les dossiers de démarrage et les fichiers associés pour déceler toute modification suspecte.
- **Règles personnalisées** : Wazuh permet la création de règles personnalisées qui spécifient des comportements ou des signatures associées à des malwares exploitant T1547.

Mises en œuvre pratiques

Voici quelques exemples concrets de règles et configurations Wazuh adaptées pour T1547.001 :

1. **Surveillance des clés de registre**

Configuration : Ajouter une règle pour surveiller les clés de registre sous

·HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
·HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce
·HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
·HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce
·HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Session Manager

En octobre 2024, une variante plus récente du ransomware Medusalocker a été identifiée, démontrant comment les attaquants personnalisent les Clés d'Exécution pour servir leurs objectifs malveillants. Les indicateurs de compromission (IoCs) associés à cette variante incluent des entrées telles que :

·HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\BabyLockerKZ
·HKEY_USERS\%SID%\Software\Microsoft\Windows\CurrentVersion\Run\BabyLockerKZ

Comment Wazuh détecte et répond aux attaques basées sur T1547

Wazuh détecte les attaques basées sur la technique T1547 en mettant en œuvre plusieurs stratégies :

- **Surveillance des clés de registre** : Wazuh peut être configuré pour surveiller les clés de registre spécifiques associées aux techniques de démarrage automatique, alertant les administrateurs en cas de changements non autorisés.

- **Analyse des fichiers de démarrage** : Il peut analyser les dossiers de démarrage et les fichiers associés pour déceler toute modification suspecte.

- **Règles personnalisées** : Wazuh permet la création de règles personnalisées qui spécifient des comportements ou des signatures associées à des malwares exploitant T1547.

2. Analyse des dossiers de démarrage

Configuration : Surveiller le dossier de démarrage pour détecter l'ajout de nouveaux fichiers.

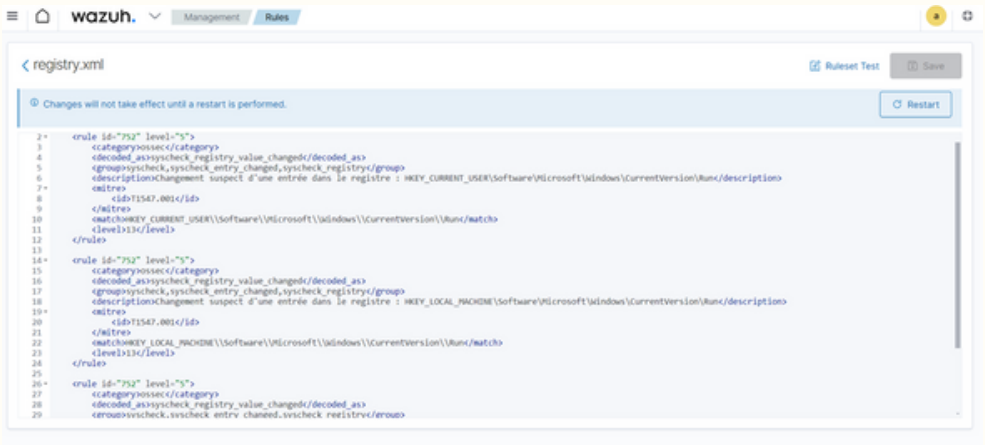
- **Dossier de démarrage de l'utilisateur individuel :**
- **C:\Users\[NomUtilisateur]\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup**
- **Dossier de démarrage système :**
- **C:\ProgramData\Microsoft\Windows\Start Menu\Programs\StartUp**

En plantant des fichiers malveillants dans ces dossiers, les attaquants peuvent garantir l'exécution automatique de leurs charges utiles chaque fois que l'utilisateur affecté se connecte. Cela prolonge non seulement la durée de vie de leur malware dans l'environnement, mais améliore également leur capacité à lancer d'autres attaques sous les permissions de l'utilisateur compromis.

Exemple de configuration des clés de registre de démarrage sur les pc windows dans le fichier C:\Program Files (x86)\ossec-agent\ossec.conf :

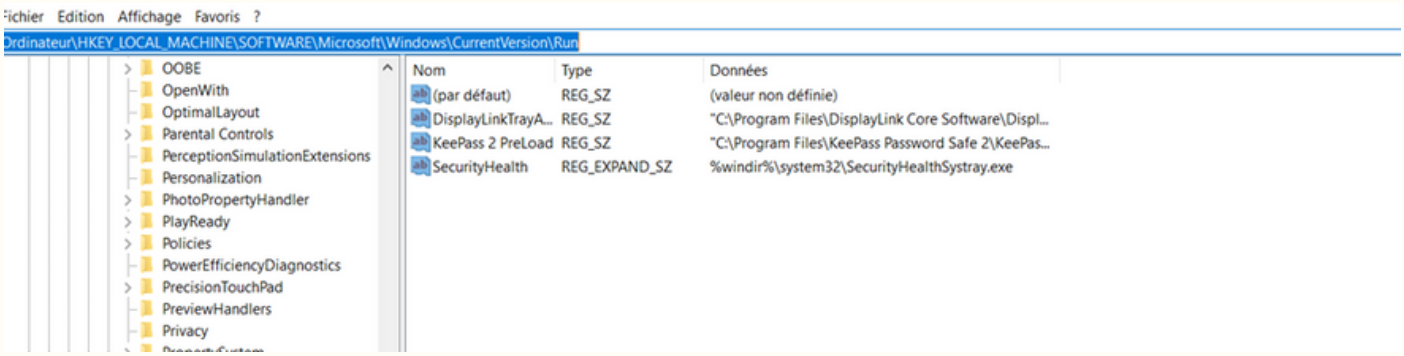
```
<registry_ignore>HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\ADOVMPPackage\Final</registry_ignore>
<windows_registry arch="both">HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run</windows_registry>
<windows_registry arch="both">HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce</windows_registry>
<windows_registry arch="both">HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run</windows_registry>
<windows_registry arch="both">HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunOnce</windows_registry>
```

Exemple de règle



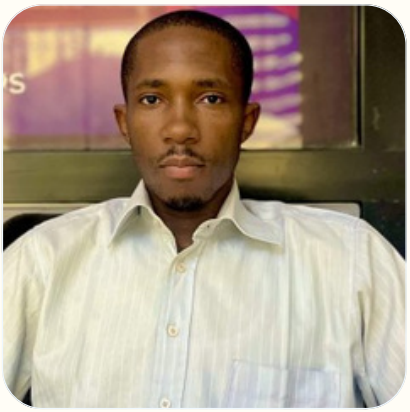
Exemple de configuration des clés de registre de démarrage sur les pc windows dans le fichier C:\Program Files (x86)\ossec-agent\ossec.conf :

En cas de compromission, nous aurions observé **l'ioc** ici



Ces configurations permettent à Wazuh de jouer un rôle crucial dans la détection et la réponse aux attaques basées sur T1547, contribuant ainsi à renforcer la sécurité des systèmes. En

surveillant proactivement les comportements associés à cette technique, les organisations peuvent réagir rapidement aux menaces potentielles et minimiser les risques de compromission.



Lien LinkedIn

A propos du réacteur de l'article :

KAMGA FODOUOP ARMEL
Consultant Informatique Analyste Soc

Actif dans le domaine de la cybersécurité, **KAMGA Armel** exerce en tant qu'analyste SOC au sein de RHOPEN Labs, où il contribue à la protection des actifs numériques. Sous la direction de **François-Xavier DJIMGOU NGAMENI,** Président de RHOPEN Labs et expert en cybersécurité, il participe à des projets visant à renforcer la sécurité des organisations africaines contre les menaces numériques

À propos de RHOPEN Labs

Filiale de l'entreprise technologique française RHOPEN, RHOPEN Labs est une société de droit camerounais au capital de 20.000.000 de Fcfa, entreprise innovante dans le domaine de la Cybersécurité et du Cloud/DevOps et dédiée à la protection des organisations africaines contre les menaces numériques. Avec une équipe d'experts et des solutions endogènes de pointe, RHOPEN Labs s'engage à fournir des services de sécurité de premier ordre.