Who Watches the Watchmen?

How Kernel-Level Anti-Cheat Systems are Similar to Rootkits

IT-SECX 2024

Christoph Dorner

- **I am a...**
  - Teaching and Research Assistant @ fhstp
  - Cybersecurity Enthusiast
  - Part-Time Gamer
- **Focus:**
  - Kernel-Level Security
  - Anti-Cheat Research
  - Cyber Range Development
  - Pentesting & Taming Kerberos
  - Teaching

Favorite Editor: vim

Beats unfair cheaters in Counter-Strike

Spends more time in terminal than sunlight

christoph.dorner@fhstp.ac.at
@Chris5011 / @Itz_Chris5011

Anti-Cheat Systems

Should prevent players of online games from gaining an unfair advantage

Anti-Cheat Systems

Cheater waren schon immer ein Problem

Vermiesen Spielspaß & vertreiben Spieler

Anti-Cheat Systeme implementiert

Nur für User-Mode konzipiert

Flucht in den Kernel

Anti-Cheat dort wirkungslos

Monetäre Verluste für Spielhersteller

Rootkits

A type of malware that provides adversaries unauthorized access while remaining hidden

Rootkits

Types

Firmware Rootkits

Zielen auf Software von Hardwarekomponenten (z. B. BIOS) und infiziert die Firmware

Virtualized Rootkits

Starten vor dem Betriebssystem, führen einen bösartigen Hypervisor aus, bevor das Betriebssystem geladen wird.

Kernel-Mode Rootkits

Modifizieren das Betriebssystem, die Infektion erfolgt oft in Form von Treibern oder Modulen.

Rootkits
Metrics

Evasion

Täuschen und Verstecken vor Scannern.

Virtualization

Virtualisierung der Binaries auf custom Architektur

Removability

Wie einfach der Entfernungsprozess ist.

Remote access and controllability

Möglichkeit der Fernsteuerung (z. B. Command-and-Control, etc.).

Information Exfiltration

Wird Information an einen externen Server oder Dienst gesendet?

Network Manipulation

Scans und Manipulation des lokalen Netzwerks

Time of Execution

Startzeitpunkt (bei Bedarf / während des Bootvorgangs).

Rootkit oder Anti-Cheat? #1

Scannt periodisch Prozesse und snapshotted diese

Durchsucht DNS-Cache / offene TCP-Verbindungen

Hooked LSA

System-Crashes

Streamed Shell-Code von Server in RAM

Rootkit oder Anti-Cheat? #1

Scannt periodisch Prozesse und snapshotted diese

Durchsucht DNS-Cache / offene TCP-Verbindungen

Hooked LSA

System-Crashes

Streamed Shell-Code von Server in RAM

BATTLEYE Anti-Cheat

Rootkit oder Anti-Cheat? #2

Sucht nach spezifischen installierten Anwendungen

Spooft Anwendungsdaten

Überprüft MAC-Adressen & Geolocation

Treiber versteckt Dateien am System

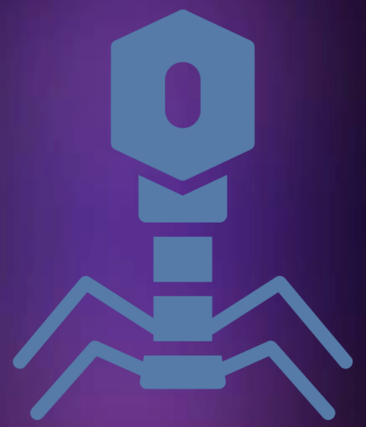
Rootkit oder Anti-Cheat? #2

Sucht nach spezifischen installierten Anwendungen

Spooft Anwendungsdaten

Überprüft MAC-Adressen & Geolocation

Treiber versteckt Dateien am System



Created by Andre Buand
from Noun Project

STUXNET

Rootkit oder Anti-Cheat? #3

Remote Access / Kill Switch

Hooking Memory-Management Syscalls & "Shadow"-Paging

Startet beim Booten

Scannt und Blockt Treiber

Rootkit oder Anti-Cheat? #3

Remote Access / Kill Switch

Hooking Memory-Management Syscalls & "Shadow"-Paging

Startet beim Booten

Scannt und Blockt Treiber

Vanguard Anti-Cheat

Anti-Cheat Systems

Vanguard

BattlEye

Games: Rainbow Six Siege, PUBG:Battlegrounds, Destiny 2, etc.

Game protection mechanisms

- Memory scans
- Scans of running processes
- Window enumeration
- TCP connections
- Module streaming

Self-protection mechanisms

- Tamper protection (self-scans)
- Binary virtualization

Easy Anti-Cheat

Games: Apex Legends, Fortnite, etc.

Uses Hardware-IDs (HWID)

- UEFI variables
- Disk serial numbers

Self-protection mechanisms

- Tamper protection
- Binary virtualization

Game protection mechanisms

- Memory scans
- Driver scanning and blocking
- Hypervisor detection
- Window enumeration

FACEIT Anti-Cheat

Games: Counter-Strike, Dota 2

Combined approach

Uses Hardware-IDs (HWID)

Very restrictive

- Hyper-V disabled
- Requires TPM 2.0
- Memory Integrity must be disabled
- DEP enabled
- Must start with boot

Game protection mechanisms

- Memory scans
- Hypervisor detection

Self-protection mechanisms

- Binary virtualization

No clear way of uninstalling

- Leaving the system in an insecure state

Vanguard

Games: Valorant, League of Legends

Game-protection mechanisms

- Shadow Memory System
- Memory scans
- Driver scanning and blocking
- Must start with boot

Self-protection mechanisms

- Tamper protection
- Binary virtualization

Remotely controllable by the developers

- Disabling / Uninstalling

Vergleich der Systeme

System	Evasion	Virtualization	Time of Execution	Remote Access	Information Exfiltration	Network Manipulation	Removability	Sum
BattlEye	○	●	○	●	●	○	○	3
Easy Anti-Cheat	○	●	○	○	●	○	○	2
FACEIT Anti-Cheat	●	●	●	○	●	○	●	5
Vanguard	●	●	●	○	●	○	○	4
Flame	●	○	○	●	●	●	●	5

Anti-Cheat

Fazit

Rootkits

FACEIT & Vanguard

Angemessen?

BattlEye &
Easy Anti-Cheat

HWID

Datenschutz?

Eindeutige Identifikation von Systemen

Player-Tracking & Verhaltens-analyse

Anti-Cheat

Fazit

Rootkits

FACEIT & Vanguard

Angemessen?

BattlEye &
Easy Anti-Cheat

HWID

Datenschutz?

Kompromittierung

Auswirkungen?

ESEA Bitcoin-Miner

Crowdstrike

Questions?

Christoph Dorner
Christoph.dorner@fhstp.ac.at
IT-SECX 2024
ST. PÖLTEN UNIVERSITY OF APPLIED SCIENCES

Sources

- Christoph Dorner and Lukas Daniel Klausner. 2024. If It Looks Like a Rootkit and Deceives Like a Rootkit: A Critical Examination of Kernel-Level Anti-Cheat Systems. In Proceedings of the 19th International Conference on Availability, Reliability and Security (ARES '24). Association for Computing Machinery, New York, NY, USA, Article 62, 1–11. https://doi.org/10.1145/3664476.3670433
- BattlEye Logo: https://www.battleye.com
- Easy Anti-Cheat Logo: https://www.easy.ac/
- FACEIT Logo: https://blog.faceit.com/brand-guidelines-presskit-5c317db077ea
- Vanguard Logo: https://en.wikipedia.org/wiki/Riot_Vanguard
- Icons and Illustrations: https://thenounproject.com