Joseph Efezokhae

Presents:

Mitigating Persistence Hunting with Autoruns.exe

March 27, 2025

ASU Cybersecurity Class of 2025

Confidential

> “Accountability and Integrity - a SOC’s internal AI Goal”
>
> –Joseph Efezokhae

Persistence Hunting

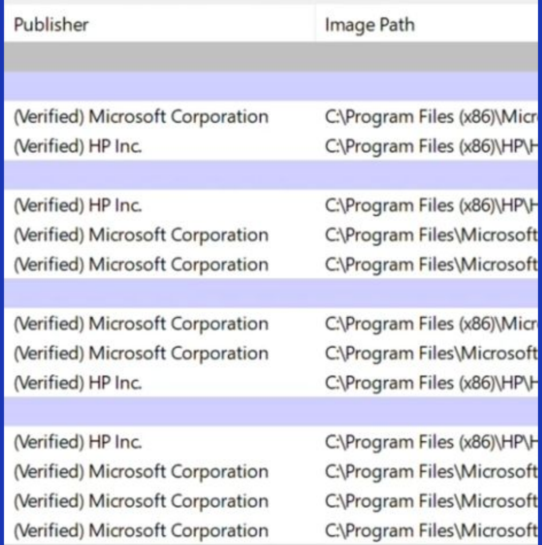
Today, I will present a demo to help us explore how attackers maintain persistence (chiefly on a Windows system) — and how **IR** and **SOC** Analysts can mitigate these threats by hunting and confirming the host machine's registry, and autorun components.

I'll be demonstrating how to spot suspicious entries, data parse through the system and provide a new tool for our toolkits as we compose Playbooks and isolate threats as they come!! — Get ready for a little excitement and maybe even a little **paranoia**.

So WHY Autoruns.exe for my journey?

Autoruns.exe provides fast and responsive real-world relevance in detecting **persistence** techniques used by RATs, malware, and threat actors to maintain access on compromised systems.

This is designed to increase your tool kit and have you more well-rounded in today's changing **threat landscapes**.



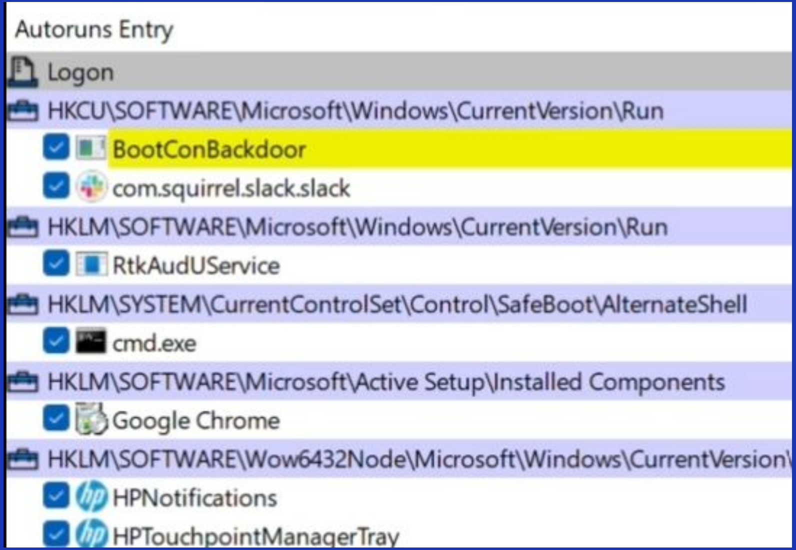
Publisher	Image Path
(Verified) Microsoft Corporation	C:\Program Files (x86)\Micr
(Verified) HP Inc.	C:\Program Files (x86)\HP\H
(Verified) HP Inc.	C:\Program Files (x86)\HP\H
(Verified) Microsoft Corporation	C:\Program Files\Microsoft
(Verified) Microsoft Corporation	C:\Program Files\Microsoft
(Verified) Microsoft Corporation	C:\Program Files (x86)\Micr
(Verified) Microsoft Corporation	C:\Program Files\Microsoft
(Verified) HP Inc.	C:\Program Files (x86)\HP\H
(Verified) HP Inc.	C:\Program Files (x86)\HP\H
(Verified) Microsoft Corporation	C:\Program Files\Microsoft
(Verified) Microsoft Corporation	C:\Program Files\Microsoft
(Verified) Microsoft Corporation	C:\Program Files\Microsoft

Live Captures from Autorun.exe

Key Concepts Applied:

- ❖ Threat Hunting Methodologies
  - ★ MITRE ATT&CK
  - ★ PEAK & Sqrrl Threat Hunting
  - ★ TaHiTI methodology
  - ★ DUTCH methodology (AML)

- ❖ Windows OS internals
- ❖ Registry Analysis Awareness
- ❖ Mechanisms of Persistence (IOCs)
- ❖ Great Hands-on Experience!!!

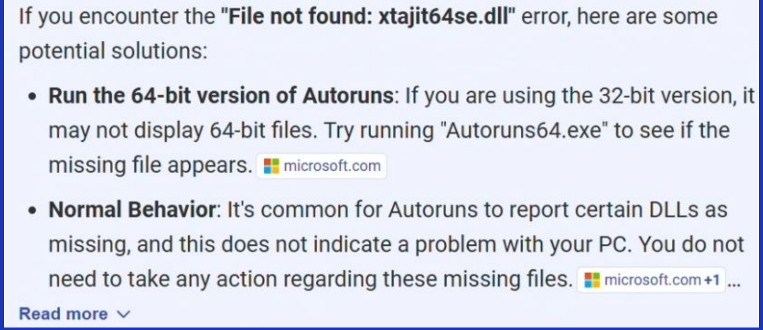


```
Autoruns Entry
Logon
HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
   ☑ BootConBackdoor
   ☑ com.squirrel.slack.slack
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
   ☑ RtkAudUService
HKLM\SYSTEM\CurrentControlSet\Control\SafeBoot\AlternateShell
   ☑ cmd.exe
HKLM\SOFTWARE\Microsoft\Active Setup\Installed Components
   ☑ Google Chrome
HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\
   ☑ HPNotifications
   ☑ HPTouchpointManagerTray
```

Live Captures from Autoruns.exe

Research Steps Taken:

- Studied Sysinternals Suite and **Autoruns.exe** usage.
- Analyzed common persistence techniques in malware.
- Reviewed Various Methodologies of Threat Hunting.
- Practiced detecting anomalies in startup entries on test systems.



If you encounter the **"File not found: xtajit64se.dll"** error, here are some potential solutions:

- **Run the 64-bit version of Autoruns**: If you are using the 32-bit version, it may not display 64-bit files. Try running "Autoruns64.exe" to see if the missing file appears. microsoft.com
- **Normal Behavior**: It's common for Autoruns to report certain DLLs as missing, and this does not indicate a problem with your PC. You do not need to take any action regarding these missing files. microsoft.com +1 ...

Read more

Leverage the AI around you and start with a Google search

Autoruns.exe is Easy to Find and Execute!

1. `curl -O https://download.sysinternals.com/files/Autoruns.zip`
2. `powershell -command "Expand-Archive -Path 'Autoruns.zip' -DestinationPath 'Autoruns'"`
3. `cd Autoruns`
4. `Autoruns.exe`

Easy to Complete from the Windows Command Line

Now.....

A Presentation to Show these skills in Action!!!

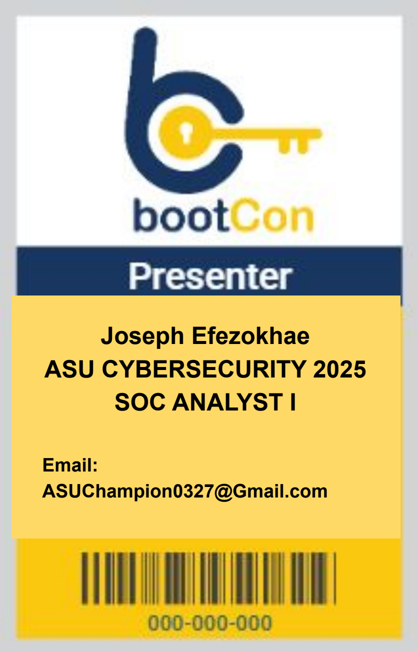
Demonstration Summary:

We **Successfully** deterred this Remote Access Trojan : **BootConBackdoor**

- Using **Autoruns.exe,** we identified, mitigated and deterred an active IOC
- **Autoruns.exe** highlights threats in gold and pink to draw much needed attention to their locations.
- We experienced the ease of use of a well recognized threat hunting tool (autoruns.exe) that helps us meet the challenges of today's modern threat landscapes.

Thank you for Listening!!!

Time for Questions??



bootCon

Presenter

Joseph Efezokhae
ASU CYBERSECURITY 2025
SOC ANALYST I

Email:
ASUChampion0327@Gmail.com

000-000-000

ReadMe.txt

# Cybersecurity ReadMe: ASU Graduate Study Path
Focused on Security+ & Network+ Preparation

##Objective
Document the tools, methodologies, and learning resources used to prepare for the CompTIA **Security+** and **Network+** certifications, with emphasis on practical threat hunting and Windows internals.

##Study Methodologies
###TaHiTI (Targeted Hunting and Threat Intelligence)
- Structured approach to threat hunting using intelligence to guide investigative paths.
- Focus on high-value assets and suspected threat actor TTPs (Tactics, Techniques, and Procedures).

###DUTCH Methodology
- **D**etect **U**nderstand **T**riage **C**onfirm **H**arden
- A systematic way to break down, validate, and respond to security incidents with respect to AML and banking.

###PEAK Threat Hunting Framework (By Sqrrl, now AWS)
- Hunt hypothesis development
- Use of analytic techniques
- Iterative feedback and learning
- [PEAK Hunting PDF Guide](https://sqrrl-public.s3.amazonaws.com/PEAK-Threat-Hunting-Model.pdf)

##Concepts Covered
- **Windows Registry Forensics** via `Autoruns.exe` and registry keys
- **Persistence Mechanisms** detection
- **Indicators of Compromise (IOCs)** vs **Indicators of Attack (IOAs)**
- **Command Line Tools** for Windows Incident Response
- **Networking Fundamentals**: ports, protocols, OSI/TCP-IP models
- **Cryptography & Authentication Protocols**: SSL/TLS, hashing, PKI

##Key Learning Resources

### Official Sites & Documentation
Documentation](https://learn.microsoft.com/en-us/windows/win32/sysinfo/registry)
- [Sysinternals Suite (Autoruns)](https://learn.microsoft.com/en-us/sysinternals/downloads/autoruns)

###Tools Explored
- `Autoruns.exe` and `Autorunsc.exe`
- `netstat`, `ipconfig`, `tracert`, `nslookup`, `PowerShell`
- `Wireshark` for network packet analysis
- CompTIA Security+ (SY0-601) Official Study Guide
- CompTIA Network+ (N10-008) Study Guide
- Used **ChatGPT** (OpenAI) for:
  - Clarifying complex concepts
  - Drafting summaries and demos
  - Creating structured study plans
  - Generating realistic threat scenarios

## Summary
This document is a self-paced, hybrid learning map combining practical skills, certification prep, and hands-on tooling. Leveraging both vendor documentation and threat hunting frameworks ensures readiness not just for exams, but also for real-world cybersecurity roles.

——------

Accountability and Integrity are the main components of AI for a SOC Analyst

Congratulations Class of 2025!!!

Ignite Your Passion!!!