

Post-Breach Black Box Logger - Encrypted, Tamper-Evident Keylogger

Introduction:

This project implements a secure, tamper-evident keylogger that records attacker activity after a breach.

It encrypts keystroke data using AES-256-GCM and verifies integrity with HMAC-SHA256.

Abstract:

Designed for forensic analysts, this logger captures keystrokes, window titles, and process names.

It ensures confidentiality and tamper resistance by encrypting each entry with AES-GCM and signing it

using HMAC. Data is stored as base64-encoded JSON for easy parsing and audit.

Tools Used:


- Python 3.x
- pynput (keyboard listener)
- cryptography (AES-GCM, HMAC)
- psutil, pywin32 (window/process context)
- os, json, base64 (core utilities)

Key Features:

- AES-256-GCM encryption with random nonce
- HMAC-SHA256 tamper detection
- Records active window + process context
- Lightweight, runs without admin rights
- Logs stored locally in encrypted, base64-encoded format
- Stops with ESC key; logs are easily decrypted for analysis

Screenshots & Workflow

1. *Logger running in CMD - starts and stops with ESC*



The screenshot shows a Windows Command Prompt window with the following text:

```
C:\WINDOWS\system32\cmd.  ×  +  ∨  
Microsoft Windows [Version 10.0.26100.4061]  
(c) Microsoft Corporation. All rights reserved.  
  
C:\Users\Asus>cd C:\keyloggerproject  
  
C:\keyloggerproject>python keylogger_encrypted.py  
[+] Keylogger started. Press ESC to stop.  
[+] Logger stopped.  
  
C:\keyloggerproject>|
```

2. Decrypted log showing keystrokes and context

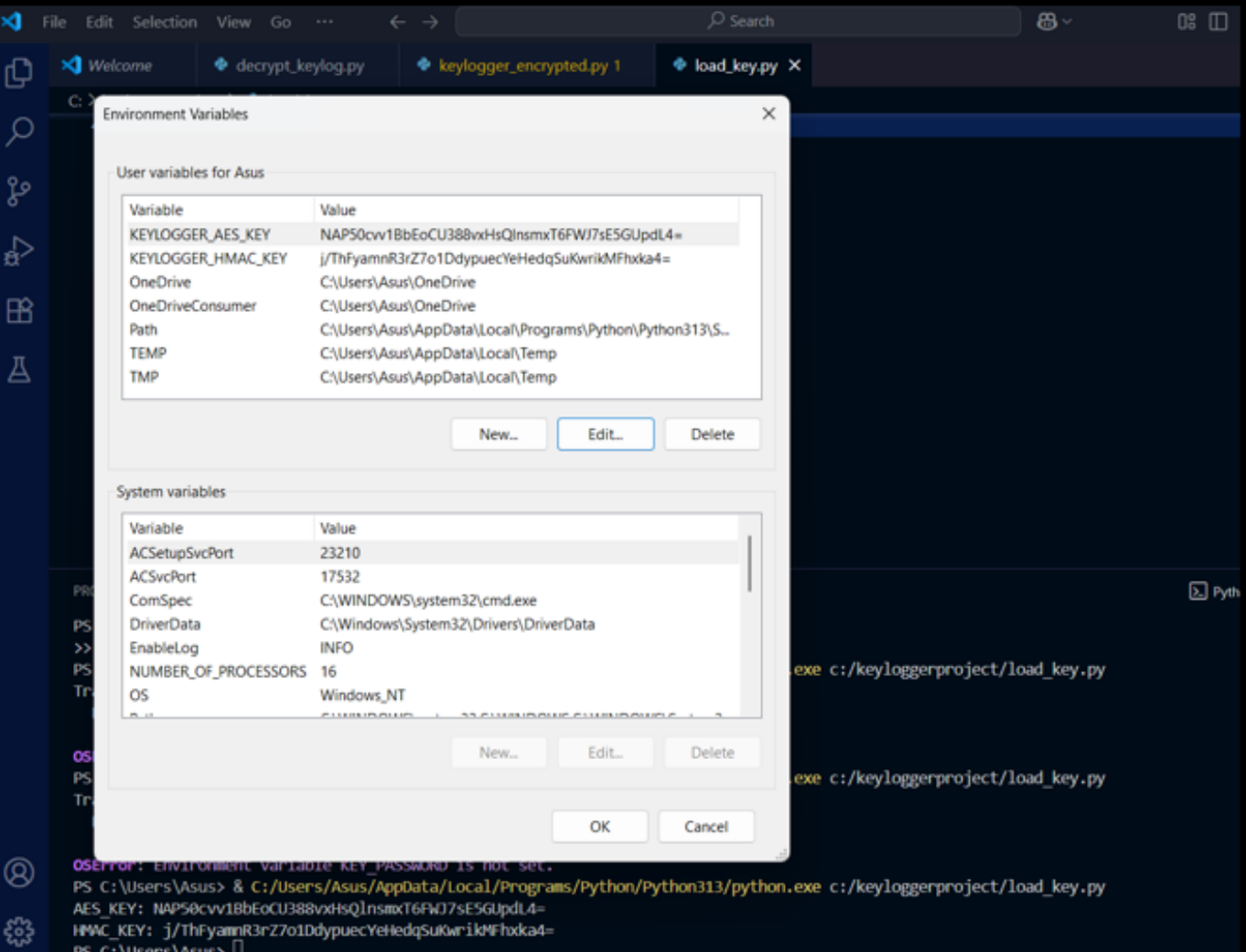
```
[2025-06-15 19:30:21] [New Tab - Google Chrome] j
[2025-06-15 19:30:21] [New Tab - Google Chrome] v
[2025-06-15 19:30:21] [New Tab - Google Chrome] Key.space
[2025-06-15 19:30:22] [New Tab - Google Chrome] j
[2025-06-15 19:30:22] [New Tab - Google Chrome] d
[2025-06-15 19:30:22] [New Tab - Google Chrome] v
[2025-06-15 19:30:22] [New Tab - Google Chrome] Key.backspace
[2025-06-15 19:30:22] [New Tab - Google Chrome] Key.backspace
[2025-06-15 19:30:23] [New Tab - Google Chrome] Key.backspace
[2025-06-15 19:30:23] [New Tab - Google Chrome] Key.backspace
[2025-06-15 19:30:23] [New Tab - Google Chrome] Key.backspace
[2025-06-15 19:30:24] [New Tab - Google Chrome] Key.backspace
[2025-06-15 19:30:24] [New Tab - Google Chrome] Key.backspace
[2025-06-15 19:30:24] [New Tab - Google Chrome] Key.backspace
[2025-06-15 19:30:24] [New Tab - Google Chrome] Key.backspace
[2025-06-15 19:30:24] [New Tab - Google Chrome] Key.backspace
[2025-06-15 19:30:24] [New Tab - Google Chrome] Key.backspace
[2025-06-15 19:30:24] [New Tab - Google Chrome] Key.backspace
[2025-06-15 19:30:24] [New Tab - Google Chrome] Key.shift_r
[2025-06-15 19:30:24] [New Tab - Google Chrome] Key.enter
[2025-06-15 19:30:25] [ffmgknksnvrw - Google Search - Google Chrome] Key.backspace
[2025-06-15 19:30:25] [ffmgknksnvrw - Google Search - Google Chrome] v
[2025-06-15 19:30:26] [ffmgknksnvrw - Google Search - Google Chrome] s
[2025-06-15 19:30:26] [ffmgknksnvrw - Google Search - Google Chrome] f
```

3. Encrypted JSON logs with AES-GCM and HMAC

```
File Edit View
{"nonce": "XKtN4iVTNXlzhWFS", "data":
{"ltjnoHlcbxg3y0QHmHtBQHZI/Dc1lcdjUpX+vpSfj8erG0PWia68wehF0F6xwRxqjS05Z6FhhGfHnZ4bku5Gbb3x0SY5g6QID03lc06ETdJl0UnQ0AFzW0JknZyCf8wdnZJRIjYVE
6KxTSm05H8213cDcRivf5+5uRrdXzUpFvQyrd4vLcWk6Mb910k/2JQRyQ+6viU5yMsx6v3rISH3vt09ddRferFOM3llq6TZJ560dQXEJCw=", "hmac":
"W80mxS17LWRPjINB3b+yIK8SV5Tf8Q05San0oP8rgw="}
{"nonce": "Vx73uzR/KhXaEKye", "data": "Qz9SYoAsPHYrodb8An90tXUj0Vaqd7NyPqohs5QLVYFCV0hw21RjwwB1eowNKFb0fUB0
+/zusXg0E+KakrHKv9VEYm4SaV98Aj7sB0nLE6/DiEK5PaNzpt3yqxFr9h/pSg3exzaNuhiO3U8g5WqhCpJWN/8mT8Gpfft6bU7
+TCLGHdVay0r74R5XXAK1XxdugHzv/y3gTJ8yjsEevyP7C6kiMFip7Hd3Z/AOYShan", "hmac": "lQS3iQcuPDrXzagWl67BpQJbNmox3arpC7Jf05jDKk="}
{"nonce": "fUVD0+voJWfEX93Y", "data":
{"ocKFBJdvMmSQtWtMCXP60iFAWiyK5y2S3mexpf5w4Z5ErWazm/6f1elwCTBTfv4PP+tw11v8SD06f5TmJeTbnwxg5c5tJc/jjXqH3DMXhCkEmTbkyJaeAmGuQXXrFhkX7c/QYVTQ
Dfe+9c6NaXw+obkAHGxowuLF49E/o3AA493F0Q3g0+K6I23XbmDJE6a/msrHvg=", "hmac": "wt29p1pPiBa5tJSNmXvTl4BpVWqrqUKzwwlGpCwtPGi="}
{"nonce": "xvKUr+K6kiPjS05U1", "data":
"xPoLm4zPUGMwDAbPaEeTucAhgLOl9gItjmn6X1PiBTKlnjBFcaia/M7Wt66q6OunHwFrjzlzGpCz2a6YitI2yJ4fHnX1bqDeR0j92zC9yIMAje3BuZrZJlWSieuIHS+
4y0MXH5/7oRm05qsR6T03KH2ey9DN40a38B0lF9hJTMjKekjCfTG+7tA+uo8yqg8Wb0A==", "hmac": "g5w82a0556FU0D1rySf8vgZKmo7YcSrw0117o0hbi0="}
{"nonce": "z0s3N0WFH1Enc69s", "data":
{"soeVYPYX6m410xLtQaIamozuXmLIQB9J5tkfooG/rGPPS4WLXnHF5831xF0omBuJP+UKioohEz8IwvtS0YatBhebtA0tk60WW0Kxv97j9iQ3MZJiQotE1d5MiKSiXD/Rp10Jk15
3c0q0MvZ1706x1Tq/gf5DtIKf9rAX3DvpR8M5+oLaPsw3zaMhbhe7d+gTNA=", "hmac": "x6X3rvyCwA/Oc+38rn90MIqaiF6dILh3WuusuTA6TM="}
{"nonce": "9GUD1xqs9cegxr9K", "data":
{"Mflh6f470CnJrg1hlm81/mvePftSup0900CtM8hniMQTy+Sgz1AEhR0b9SuEx+MwG5hvJ9P0VZgXGL2315t2Ka368J34TaUBZyqL7bEqXIW0SAaAcLWddmai4dQlFuIq+UzxXmScf
jDM/1Cjv5Bbh/gagmQVx5Dy78k0tWRcxQ0tVh8ni4YwV7tUg/w9PFWFES7L+2r8ryIyBfZChBKwc+w03KQowR563Hcn1y51Dv2nw==", "hmac":
"SGwKiH7yUQ36mSKDcR2hcCwTB4kRnXP4+C3fzawKvGy="}
{"nonce": "Xw63xbfp9zP98ppv", "data": "+hlyDHu53e8a7precPyJS3ht+0qU5+OzRZRZhVhg5pgmNXXUHY+7onGow/V2A/EST0/A+pso/R89IngwQT30lKpi6Pe9
+Q1SRwsZIEdXuxhrzEnMGovf3z8f0dks+e4TpxTqJ1SuVXBgJK1PwgUhl6uUzK0K0mWbASkHiTKW5agemWRCJ228fwPymuz6VF+Prtv0ZJNAX0X3YzJ70KquqseLCA0s0jb38HRwjg
GzJyqtkhl", "hmac": "9XMJ1z9o+UGVUP7fUwssrwVDQGBqQBPuM18fCYVlHQ="}

Ln 1, Col 1 99,922 characters 100% Windows (CRLF) UTF-8
```

4. Secure key storage in environment variables



Conclusion:

This project delivers a highly secure, ethical, and forensic-friendly keylogger solution. Its tamper-evident and encrypted logging capabilities help reconstruct breach activity while preserving evidence integrity. It is ideal for analysts working in environments without full-scale EDR solutions.