ATTACKS ON EVENT TRACING FOR WINDOWS: TECHNIQUES AND COUNTERMEASURES

Ing. Matěj Havránek, Supervisor: Ing. Josef Kokeš, Ph.D.
Department of Computer Security, Faculty of Information Technology, Czech Technical University in Prague

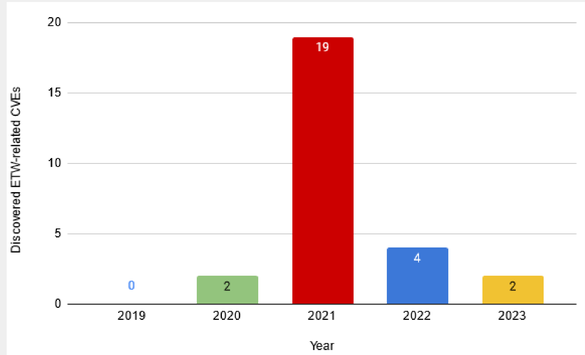
FACULTY OF INFORMATION TECHNOLOGY CTU IN PRAGUE

Motivation and Aims

- Event Tracing for Windows (ETW) is a **crucial component** of Windows security
- Most Antivirus and security solutions depend on data from ETW to protect the system
- Attackers are motivated to attack ETW to prevent being detected
- **Large impact** of such attacks on system security
- Research in cooperation with ESET

Analysis of Specific Attacks Against ETW

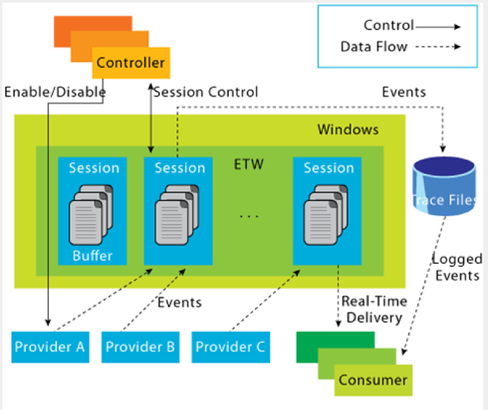
- **Malicious rootkit** designed to blind security software by stealthily **disabling event logging**
- Attributed to the **Lazarus APT group** affiliated with North Korea
- Sophisticated nation-sponsored threat actor
- **Elevation of privilege** via BYOVD (Bring Your Own Vulnerable Driver)
- Abusing vulnerable third party kernel drivers to gain **access to kernel memory**
- **Overwriting ETW configuration** directly in kernel memory to disable logging - **hard to detect** by conventional means
- This makes subsequent malicious activity harder to identify for security software



Published vulnerabilities related to ETW in recent years

Event Tracing for Windows (ETW)

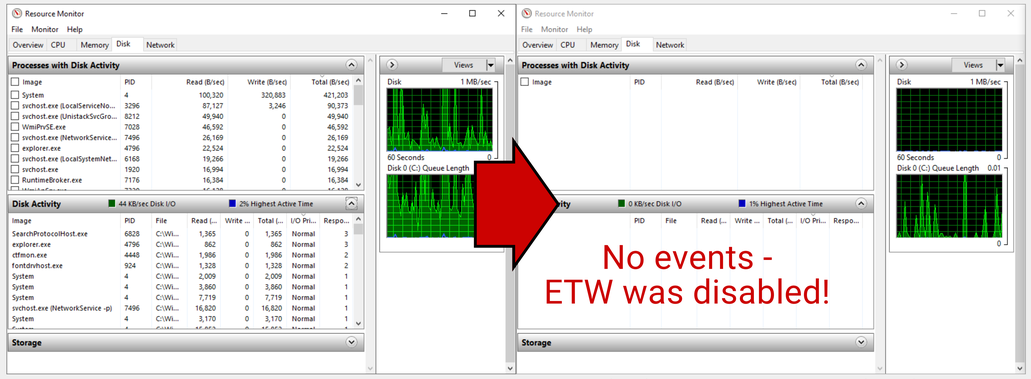
- **Event logging platform** integrated in Microsoft Windows since Windows Vista
- Live event processing, event storage and filtering
- Logs events from:
  - Windows kernel
  - System programs and components
  - User programs
- Provides these events to:
  - System tools (event viewer)
  - Monitoring tools
  - Resource management
  - Antimalware and security software
- Disabling this functionality **blinds most system monitoring and security tools**



Schema displaying the operation of the ETW framework

Proof of Concept

- Analyzed the malicious rootkit and discovered two methods to attack ETW:
  - **Removing kernel provider callbacks**
  - **Disabling system loggers**
- Created a Proof of Concept of these two attacks in order to develop countermeasures



Resource monitor showing system activity before (left) and after the attack (right).

Conclusion

- Analyzed a series of sophisticated blinding attacks against ETW
- Described undocumented parts of the Windows kernel and the ETW framework
- Implemented and evaluated a Proof of Concept based on these attacks
- Created and implemented a two methods of **reliably detecting and identifying** such blinding attacks against ETW
- Proposed two approaches to **prevent such attacks from succeeding** in the future
- **Results were published** on two conferences
- **Real-world impact** in pointing out weaknesses in the ETW framework

Detecting the attacks

- Created an implemented two methods for detecting such attacks on ETW
- **Statistical approach** from user-mode, monitoring message volumes per provider. A drop in message volume indicates a possible ongoing attack
- **Monitoring ETW structures** from kernel-mode, detecting changes to ETW configuration using a **kernel-mode driver** and alerting the user via a **usermode app**

Mitigating the attacks

- Proposed two preventive measures
- **Expanding windows kernel protection mechanisms** (kernel patch protection) - verifying checksums of memory regions and using a secure api to update them when the data changes
- Implementing **access control in kernel memory**, for example by segmentation as demonstrated by the MemoryRanger tool *(github.com/IgorKorkin/MemoryRanger)*.

Publications

This work was presented as part of two conference contributions [1, 2] and published as part of a conference journal article [1].

1. KÁLNAI, Peter; HAVRÁNEK, Matěj. Lazarus & BYOVD: evil to the Windows core. In VirusBulletin conference. 2022.
2. KÁLNAI, Peter; HAVRÁNEK, Matěj. Lazarus declares war on system monitoring. In AVAR conference. 2022.