LABS
CON
22
LABS CON 2022 SCOTTSDALE AZ

LABSCON

LABScon Replay | Blasting Event-Driven Cornucopia: WMI-based User-Space Attacks Blind SIEMs and EDRs

LABSCON / JANUARY 11, 2023

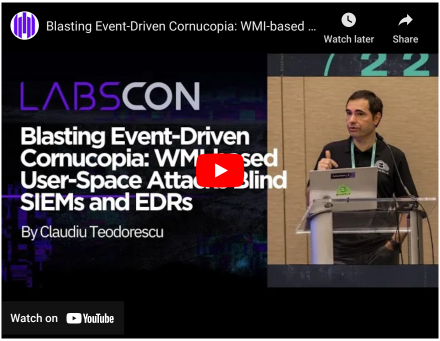
Security solutions engineers always find new ways to monitor OS events to mitigate threats on endpoints. These approaches typically reuse different built-in Windows mechanisms that were never designed with security first in mind.

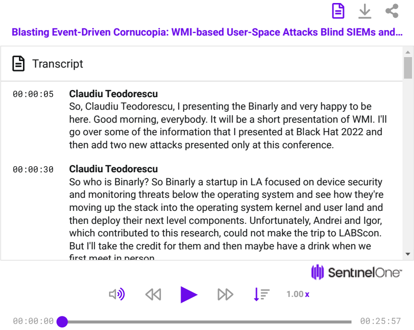
WMI provides rich information about the computing environment, which allows monitoring via event filters, consumers, and bindings to get notifications about important OS events. These features make WMI critical for solutions such as EDRs, AVs, SIEMs. The bad news: Malware countermeasures can disable WMI, making these defense solutions useless.

In this talk, Binarly's Claudiu Teodorescu provides an analysis of the WMI architecture by reversing user-mode variables and functions from DLLs to demonstrate several new user-mode attacks.

WMI-based user-space attacks impact all versions of Windows. The core vulnerability of WMI is that the DLLs loaded into the WMI core process (WinMgmt), leverage "flags" to perform WMI operations. Attackers can block the access to WMI – receiving new OS events, installing new WMI filters – by modifying these flags. There are no built-in features to block these attacks or repair WMI.

WMI-based attacks can be detected by inspecting the memory of WMI core service, which can disclose other attacks on Windows OS components including privilege escalation, token hijacking, and ETW blinding.


Blasting Event-Driven Cornucopia: WMI-based ...
Watch later
Share
LABSCON
Blasting Event-Driven Cornucopia: WMI-based User-Space Attacks Blind SIEMs and EDRs
By Claudiu Teodorescu
Watch on YouTube


Blasting Event-Driven Cornucopia: WMI-based User-Space Attacks Blind SIEMs and...
Transcript
SentinelOne
1.00 x
00:00:00
00:25:57

00:00:05 **Claudiu Teodorescu**
So, Claudiu Teodorescu, I presenting the Binarly and very happy to be here. Good morning, everybody. It will be a short presentation of WMI. I'll go over some of the information that I presented at Black Hat 2022 and then add two new attacks presented only at this conference.

00:00:30 **Claudiu Teodorescu**
So who is Binarly? So Binarly a startup in LA focused on device security and monitoring threats below the operating system and see how they're moving up the stack into the operating system kernel and user land and then deploy their next level components. Unfortunately, Andrei and Igor, which contributed to this research, could not make the trip to LABScon. But I'll take the credit for them and then maybe have a drink when we first meet in person

About the Presenter

Claudiu Teodorescu is CTO at firmware security firm Binarly. He has an extensive background in Computer Forensics, Cryptography, Reverse Engineering, and Program Analysis. While at Cylance, he focused on program analysis to augment the ML model feature space with code-specific artifacts. Claudiu is the author of the WMI-parser tool to help IR teams forensically identify malware persistence.

About LABScon

This presentation was featured live at LABScon 2022, an immersive 3-day conference bringing together the world's top cybersecurity minds, hosted by SentinelOne's research arm, SentinelLabs.

EDR LABSCON WMI

LABSCON

LABScon brings together the world’s top cybersecurity minds to share cutting-edge research and push the envelope of threat landscape understanding.

©2023 SentinelOne, All Rights Reserved.