



WMI Abuse

Windows Management Instrumentation Tactics and Techniques



Whoami.exe



Gerry Johansen
Principal
IR Proactive

 @irproactive



10+ Years of Incident Response,
Digital Forensics and Threat
Intelligence



BS – Justice and Law Admin, MA–
Information Assurance, GCTI, GCFA,
GNFA, GRID, CISSP Detective / Task
Force Agent (FBI)



Digital Forensics and Incident
Response, 3rd Edition

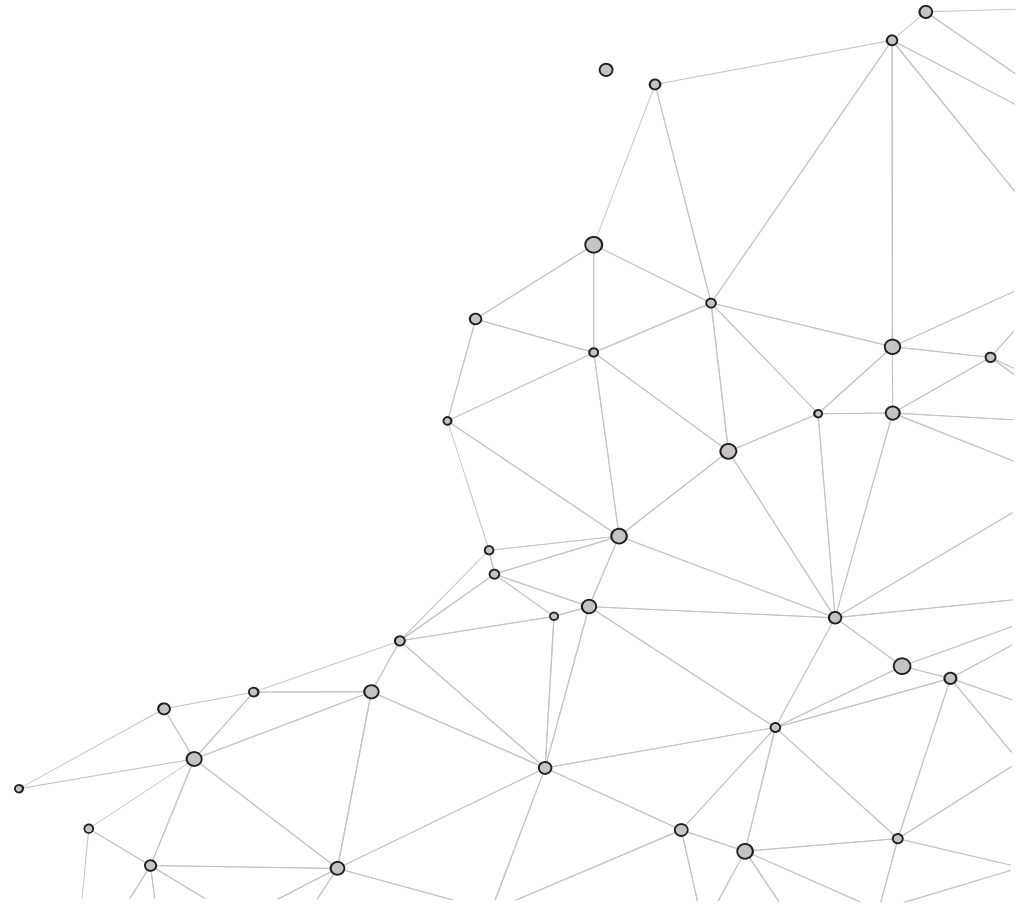


Rapid City, South Dakota

dir /ad



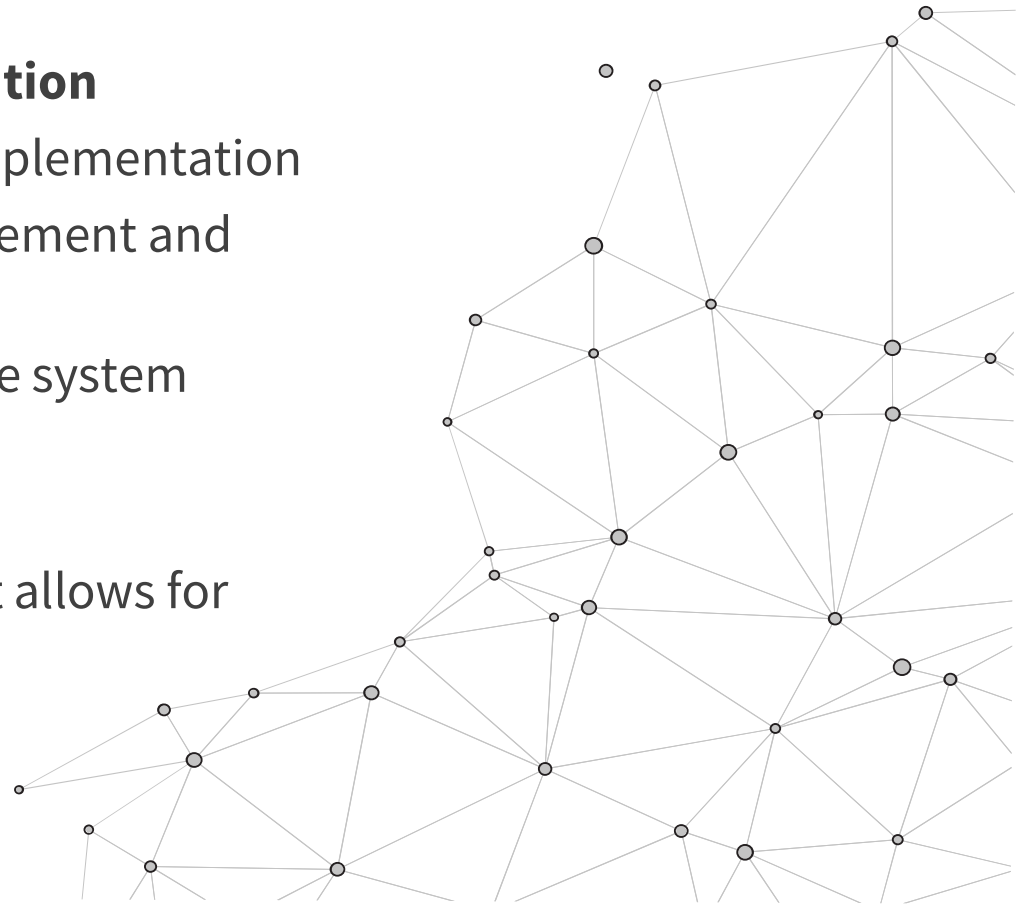
- WMI Overview
- Why discuss WMI abuse?
- A Brief History of WMI Abuse
- Leveraging WMI
- Demo
 - Emulating WMI Abuse
 - Local use
 - Remote use
 - Event Consumer



WMI Overview

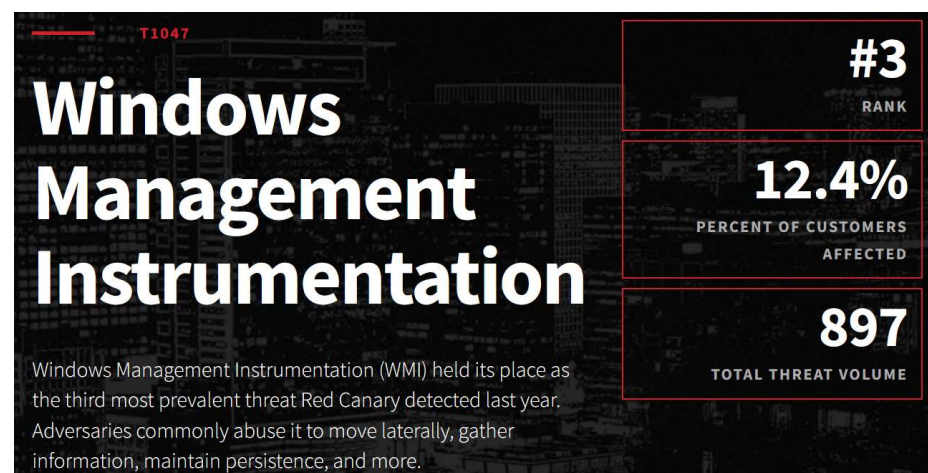


- WMI: **Windows Management Instrumentation**
- Microsoft's Common Information Model implementation
- Windows OS infrastructure for data management and operations
- Automates administrative tasks and remote system management
- Great deal of functionality and capability
- **Wmic.exe** is the Command-Line utility that allows for interaction with WMI ^[1]



Why discuss WMI Abuse?

- Used by threat actors for Execution, Persistence and Lateral Movement
- Consistently shows up in threat intel reports: M-Trends, Threat Detection Report ^[2]
- Tied to other more common tools: CMD & PowerShell
- WMI Abuse is baked into many post exploitation frameworks



A short history of WMI Abuse



- Stuxnet: Propagation through network shares [3]
- APT33: Persistence using suspicious Event Subscriptions [4]
- FireEye FLARE Team white paper on WMI Forensics [5]
- BlackEnergy2: WMI for host reconnaissance [6]
- Scattered Spider: Lateral movement [7]



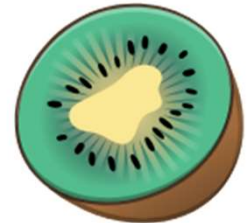
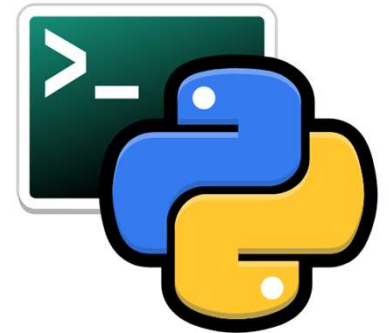
How do threat actors use WMI



- WMI Abuse can run through a variety of Tactics and Techniques:
 - Executing malicious code or scripts on local and remote systems
 - Reconnaissance on compromised system such as identifying processes or accounts
 - Discovery of network systems
 - Persistence through Event Consumers
 - Delete Volume Shadow Copies as part of ransomware attack

Leveraging WMI

- WMI Modules exist in several common post-exploitation tools
 - Cobalt Strike
 - PowerShell Empire
 - Mimikatz
 - Metasploit
 - **Impacket – lots of Impacket**
- WMI can be leveraged with PowerShell or Command-Line

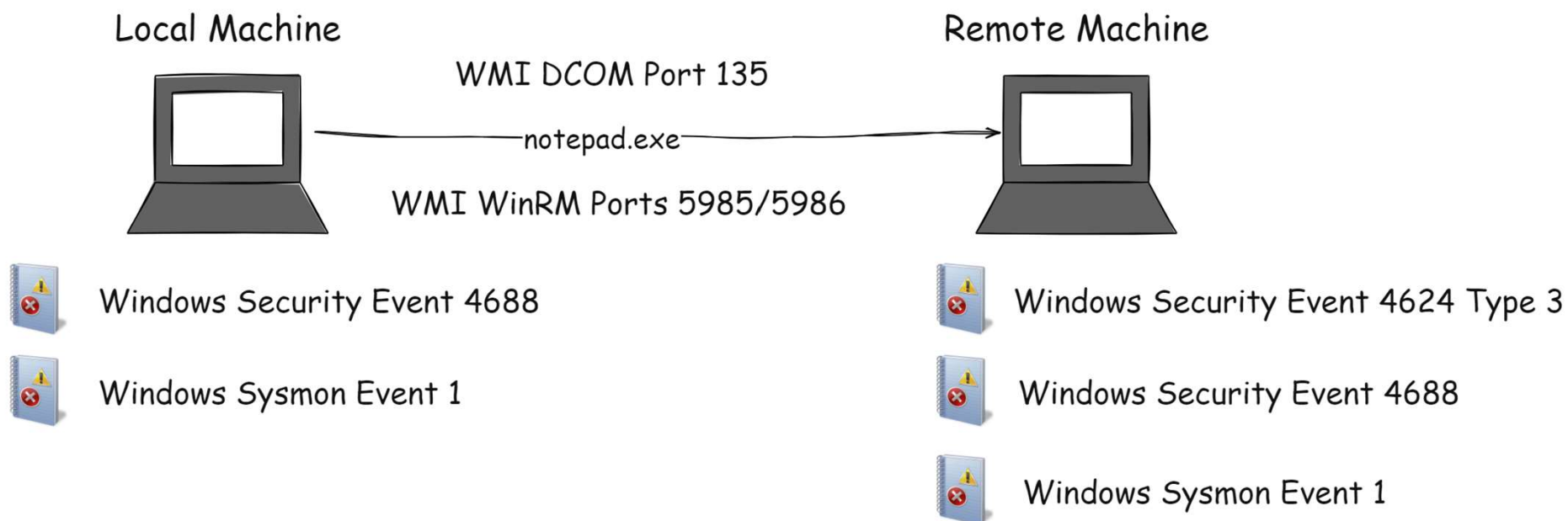


Investigating WMI Abuse



- Make investigating WMI abuse part of the overall triage process:
 - Think WMI use when looking at CMD and PowerShell execution
- Network Connections:
 - TCP 135, http 5985, & https 5986
- Windows Event Logs:
 - Windows Security Event ID 4688 – Process Creation (sometimes)
 - Windows Sysmon Event ID 1 – Process Creation
 - Windows Sysmon Event ID 19, 21, 22 – Event Consumer Activity
 - Windows WMI-Operational Logs
 - Windows PowerShell Operational Logs
- OBJECTS.Data located in \Windows\System32\wbem\Repository^[8]

WMI Remote Execution

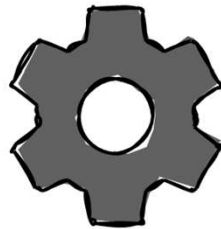


WMI Event Subscription



- **Event Filter:** The condition that triggers the script/executable. Can be on uptime, user-logon, file creation.
- **Event Consumer:** Executable or script that is triggered to run. PowerShell or executable.
- **Binding:** This ties the Event Filter and Consumer together

Event Filter



Binding



Event Consumer



WMI Event Subscription



- Extract and analyze the **Microsoft-Windows-WMI-Activity/Operational** logs.
- Search for Event ID 5861. Look for:
 - Executables: .exe, .dll
 - Scripts: .vbs, .ps1
 - ActiveXObjects
 - Script Text



Sample WMI Abuse



- T1047: Windows Management Instrumentation
 - Discovery
 - System reconnaissance: identify running processes
 - Lateral Movement Technique
 - Remote Command Execution
- T1546.003: Event Triggered Execution WMI Event Subscription
 - Privilege Escalation & Persistence
 - Using the Event Subscription

T1047: Windows Management Instrumentation



- Recon what processes are on a system



`Invoke-AtomicTest T1047 -TestNumbers 2`

- Recon what remote service is running on a system



`Invoke-AtomicTest T1047 -TestNumbers 4`

- Execute remote executable



`Invoke-AtomicTest T1047 -TestNumbers 6`

T1546.003: Event Triggered Execution – WMI Event Subscription



- Maintain persistence using PowerShell



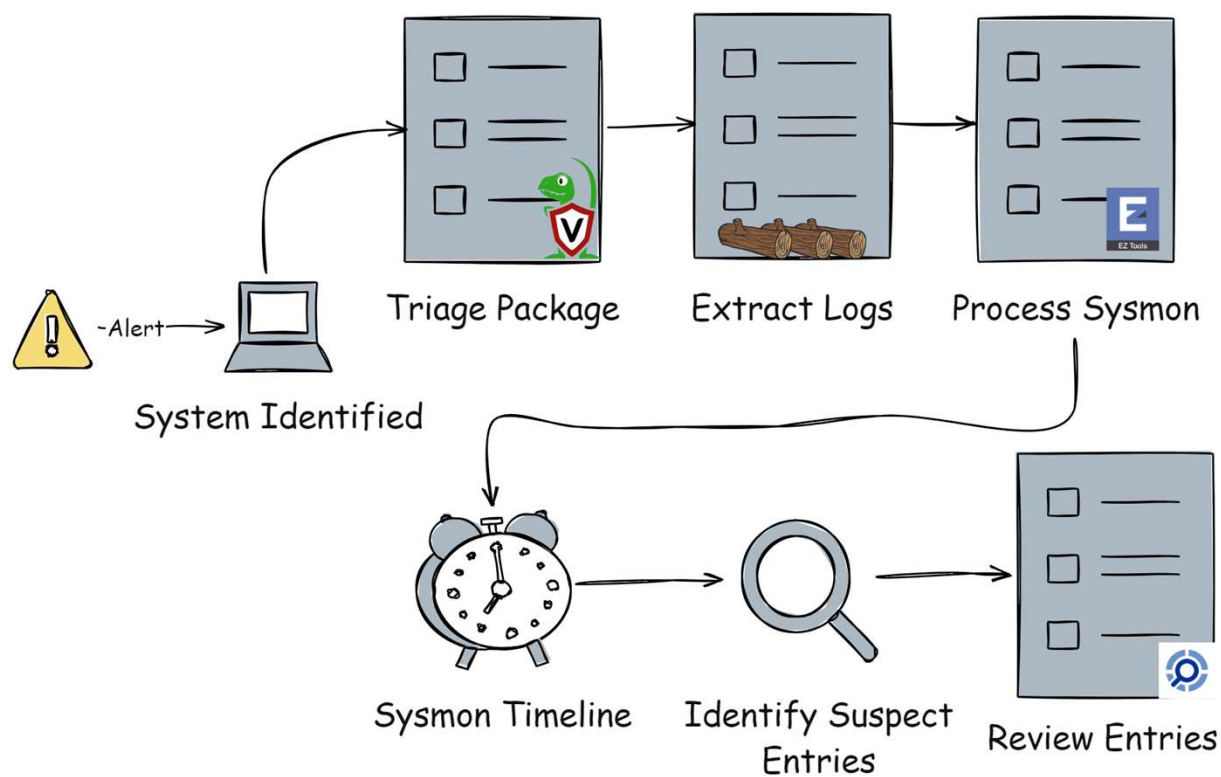
`Invoke-AtomicTest T1546.003 -TestNumbers 2`

- Maintain persistence with MOFComp.exe to load Managed Object File (MOF)

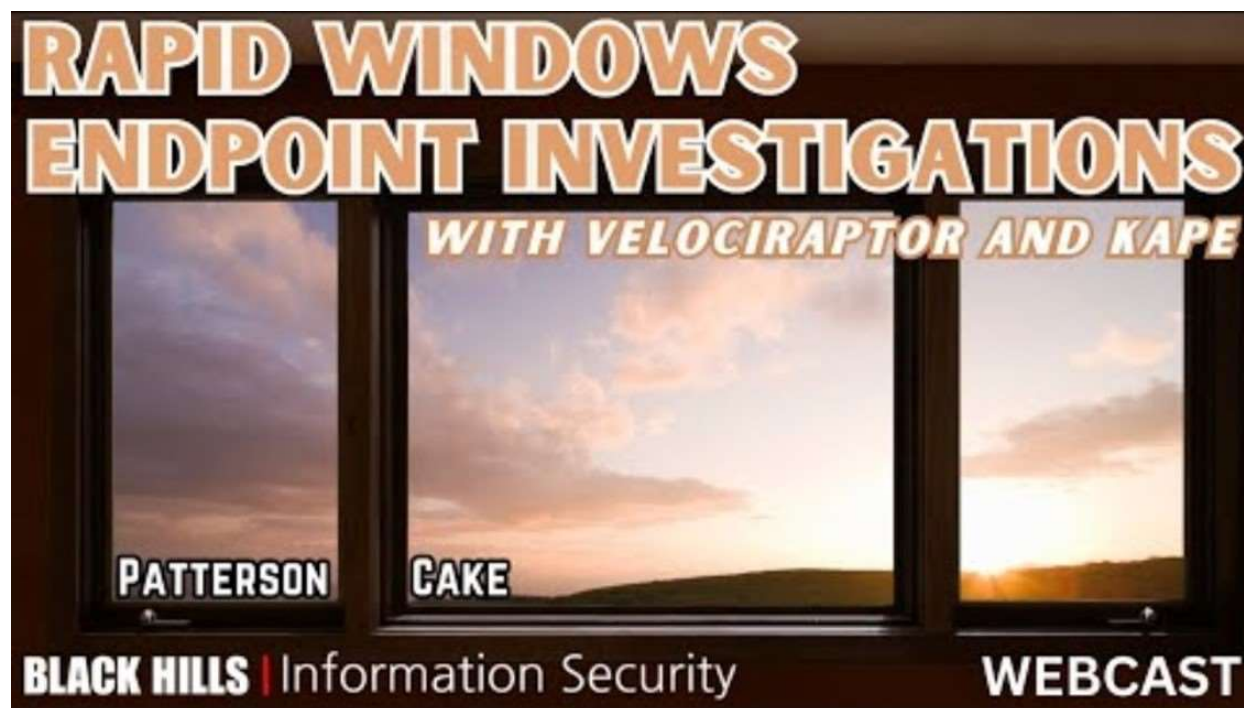


`Invoke-AtomicTest T1546.003 -TestNumbers 3`

WMI Investigation Workflow



Velociraptor Overview



<https://www.youtube.com/watch?v=rqEjxZph96c>

IR PROACTIVE

Questions



Sources



1. <https://lolbas-project.github.io/lolbas/Binaries/Wmic/>
2. <https://redcanary.com/threat-detection-report/techniques/windows-management-instrumentation/>
3. https://www.wired.com/images_blogs/threatlevel/2010/11/w32_stuxnet_dossier.pdf
4. <https://www.microsoft.com/en-us/security/blog/2020/06/18/inside-microsoft-threat-protection-mapping-attack-chains-from-cloud-to-endpoint/>
5. <https://www.mandiant.com/sites/default/files/2021-09/wp-windows-management-instrumentation.pdf>
6. <https://securelist.com/be2-extraordinary-plugins-siemens-targeting-dev-fails/68838/>
7. <https://www.crowdstrike.com/blog/analysis-of-intrusion-campaign-targeting-telecom-and-bpo-companies/>
8. <https://www.sans.org/blog/finding-evil-wmi-event-consumers-with-disk-forensics/>



Thank You

gjohansen@irproactive