



Welcome to Atomics on a Friday!


Agenda

- Who are we?
-
- Detection & Mitigation
- Discussion
- Next time on *Atomics On A Friday*

Who Are We?




Michael Haag
Sr. Threat Connoisseur

 @M_Haggis



Paul Michaud
Principal Handler of Shenanigans

 @Burning_PM

Demo

Atomic Red Team

[T1569.002 - sc.exe](#)

[T1569.002 - psexec remote host](#)

Atomic Test Harnesses

[Windows Service](#) - New-ATHDriverService

Atomic Tests

[Hunting Drivers](#)

Logs


Sysmon

- Event ID 1 - Process Creation
- Event ID 11 - File Create
- Event ID 12 - Registry Event - Object Create and Delete
- Event ID 13 - Registry Event - Value Set

Windows Event Logs

- 4697 - A service was installed in the system
- 7045 - A service was installed in the system

Mitigations

- Disable SMB Ingress
 - <https://www.fireeye.com/content/dam/fireeye-www/current-threats/pdfs/wp-ransomware-protection-and-containment-strategies.pdf>
- Limit Admin Access
- Attack Surface Reduction
 - Prevent PsExec from running
- Turn off Computer 

Thank you

- [Atomic Red Team - T1569.002 - Service Execution](#)
- [AtomicTestHarness - WindowsService](#)
- <https://github.com/redcanaryco/invoke-atomicredteam>
- <http://atomicredteam.io>

