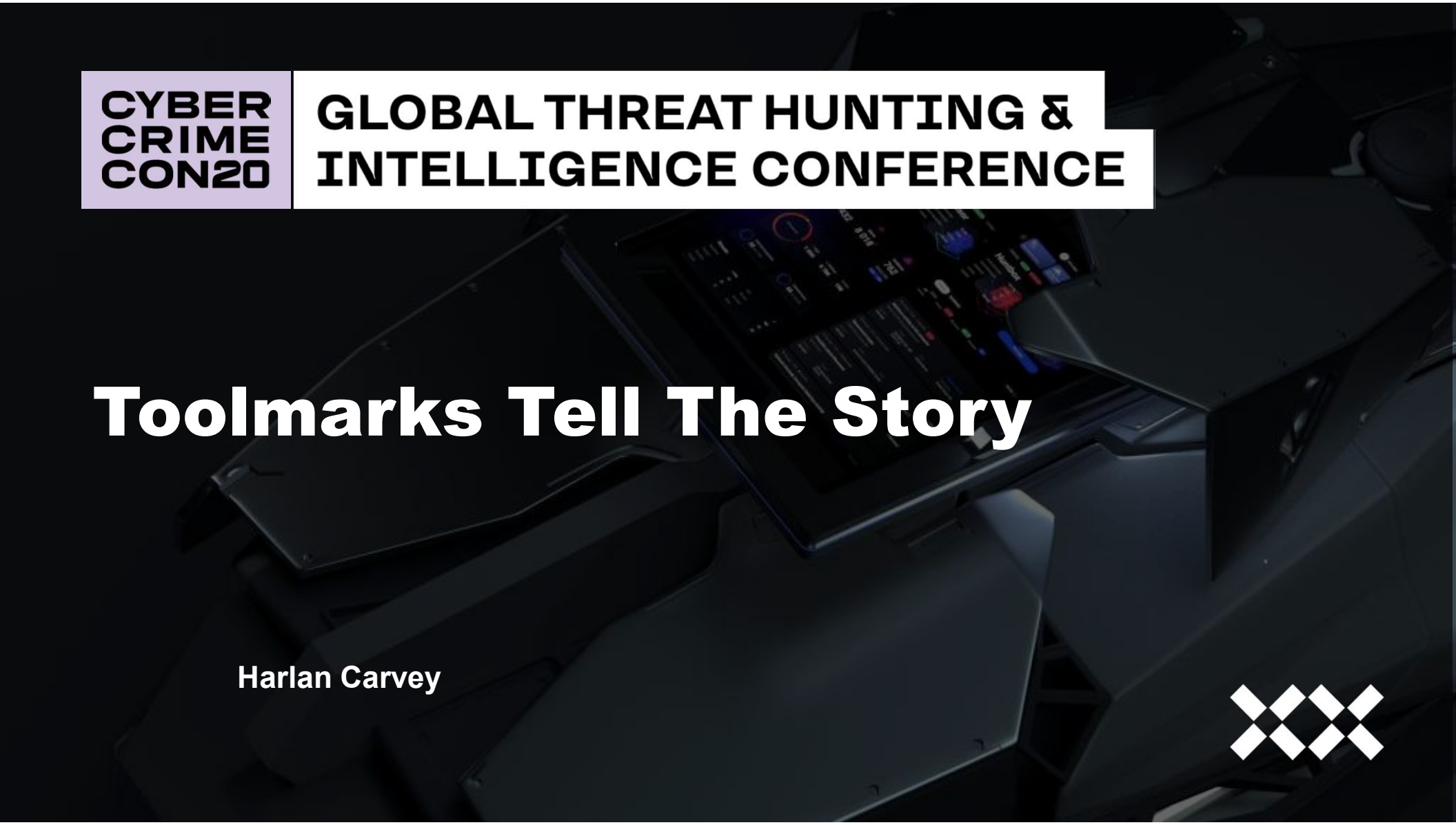


Toolmarks Tell The Story

Harlan Carvey

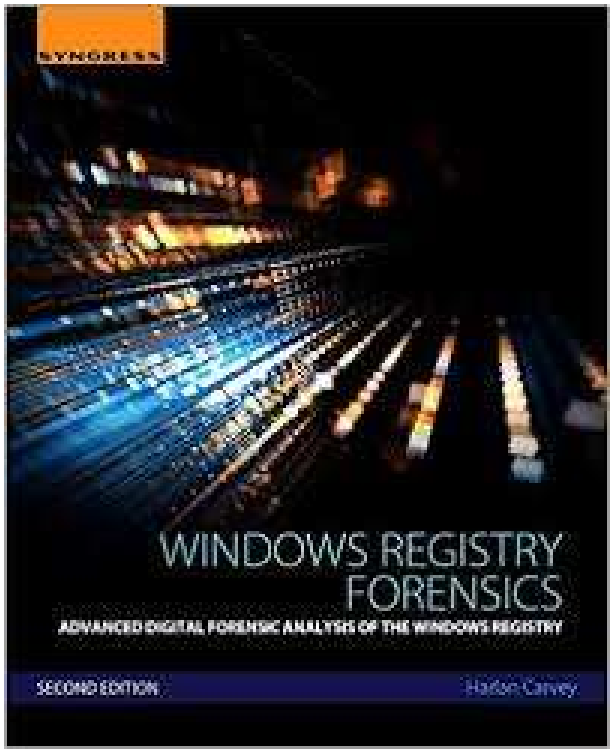
Intro

CYBER CRIME CON20

Whoami

Researcher, speaker, author

Maintain open source tools, including RegRipper (since 2008)



What are “toolmarks”?

CYBER CRIME CON20

Encyclopedia.com – impression left by the contact of a tool on a surface

DFIR - Clusters of artifacts associated with indicating a behavior, based on temporal proximity and causality

DFIR toolmarks can include:
- Modifications made to the system to “prepare” the environment for follow-on activities
- Running programs and the artifacts they leave on the system

Can be critical to attribution, as toolmarks identify the “how” and “when” of a behavior
- Action taken by a threat actor prior to moving malware to system, or
- Command embedded in EXE?

Ex: circa late 2018 thru mid-2019, Ryuk ransomware actors were observed setting the UseLogonCredential value an average of 7 – 9 days prior to running mimikatz. When they did run mimikatz, lateral movement occurred within seconds.

Ex: Opening a door

CYBER CRIME CON20

Ex: Disable Windows Defender

CYBER CRIME CON20

Different ways to do this; each method has its own toolmarks

Snatch ransomware actors -> Defender Control (GUI app)

- GUI vs CLI vs GPO

Reg.exe vs. PowerShell (vs encoded PowerShell)

- Prefetch files
- Registry modifications
- Windows Event Log entries

Disable Windows Defender Service

- Sc.exe vs reg.exe vs 'net stop'

PowerShell: Set-MpPreference –DisableRealtimeMonitoring $false (or, try it encoded)

Reg.exe: REG ADD "HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows Defender" /v DisableAntiSpyware /t REG_DWORD /d 1 /f

Ex: Disable Windows Defender

CYBER CRIME CON20

How WinDefend is disabled, and ***when*** during the attack cycle this occurs, identifies behavior. This behavior can then be attributed to an actor.

Some ransomware EXEs contain lists of ‘net stop’ commands embedded within the EXE
  A version of ProLock ransomware from the spring of 2020 contained 156 unique commands

Note: Batch files vs individual command lines

Timing of the commands will be different than if the threat actor takes steps to prepare the environment prior to deploying malware/ransomware

Toolmarks - Summary

CYBER CRIME CON20

Concept of toolmarks applies to other behaviors, as well

Clusters of indicators or artifacts (cluster size will vary) with temporal proximity

Developed through timeline analysis (file system, Registry, Windows Event Log metadata, Registry data, etc.)


CYBER
CRIME
CON20
GLOBAL THREAT HUNTING &
INTELLIGENCE CONFERENCE
Thank you!
Questions?
Harlan Carvey