SCARECROW DETECTION

Detection of ScareGrow EDR Bypass Payloads
ABOUT ME
WHAT IS ENDPOINT DETECTION AND RESPONSE?

• Provides alerting and investigative capabilities
• Trusted tool
• But what if…
WHAT IS SCARECROW?

- EDR bypass payload generation framework
- Written by Matthew Eidelberg
- See Matthew’s talk: “Remaining Invisible in the Age of EDR”
HOW DOES SCARECROW WORK?

- Framework generates loader
- Various delivery methods
- Once loaded, flushes hooks for system DLLs
- Executes payload
HOW DOES SCARECROW WORK?

- Multiple techniques for hiding
  - Property strings within binary
  - Realistic code signing
  - File naming
CAN WE DETECT IN EDR?

- Potentially...
- If other phases of attack are noisy
CAN WE DETECT IN EDR?

- Potentially...
  - If using a binary payload (exe), may see that file being written to disk
  - Prevalence
CAN WE DETECT IN EDR?

- Potentially...
- If using a binary payload (exe), may see that file being written to disk
- Location of binary
CAN WE DETECT IN EDR?

• Carbon Black may show an Invalid certificate signing chain:

• CrowdStrike may hit on an AV detection or something within Overwatch
CAN WE DETECT IN EDR?

• Carbon Black EDR search query for console applications with an invalid certificate chain and Microsoft as the publisher:

-DIGSIG_RESULT: "SIGNED" AND DIGSIG_PUBLISHER:MICROSOFT* AND CHILDPROC_NAME=CONHOST.EXE
CAN WE DETECT IN EDR?

- Potentially...
- Once executed... lack of activity being recorded
- Comparing against other sources may be interesting.
CAN WE DETECT WITH YARA?

• Signatures provided in Optiv GitHub:

Note: This YARA signature may not work for various tools depending on which version of YARA is compiled into the product or feature.
CAN WE DETECT IN AV?

• Initial version generates .exe that may be caught by Windows Defender.

• Once executing, shellcode may be detected if using something that has been well signatured.
  • Like Meterpreter...
CAN WE DETECT IN MEMORY?

- Process listings -> baseline
CAN WE DETECT IN MEMORY?

- Process listings -> baseline
- Network connections -> EDR/SIEM
CAN WE DETECT IN MEMORY?

• Process listings -> baseline
• Network connections -> EDR/SIEM
• DLL and file dumps -> AV/YARA
CAN WE DETECT IN MEMORY?

• Process listings -> baseline
• Network connections -> EDR/SIEM
• DLL and file dumps -> AV/YARA
• Malfind -> interesting sections of memory marked with PAGE_EXECUTE_READWRITE
CAN WE DETECT ON DISK?

- Check active files around EDR timestamps
- Check NTFS journal
- Existing or carved binaries
  - Certificate chains
  - Hashes
  - Odd locations
  - AV/YARA
CAN WE DETECT ON THE WIRE?

• Beaconing activity – RITA from BHIS
• Domain reputation
• Domain age
• Large transfers
• IPs/Domains vs what is seen in EDR
CAN WE DETECT ON THE WIRE?

• Tradecraft matters!
SUMMARY

• EDR Bypass
• ScareCrow
• Means for identifying attack
THANK YOU

- Matthew Eidelberg
- "Remaining Invisible in the Age of EDR"
- Ryan Boyle
- "Open Source Forensic Threat Hunting"
QUESTIONS?

• SourceZeroCon Discord
• Twitter: @vrain_