Temet Nosce: Know Thy Endpoint Through and Through

Thomas V. Fischer
I am ...

- Threat Researcher
- 25+ years experience in InfoSec
- Spent number years in IR team positions

Contact
  - tfischer@digitalguardian.com
  - tvfischer+sans@gmail.com
  - @Fvt
A Journey

- Transformation of a tool
- Real time actionable intelligence
- (re)Enabling the end point as an active defence mechanism
- Detecting behaviour...
Are we in the Wrong Place

- Network based solutions
- Post incident end point technology
- Forensics ~ what changed ≠ necessarily what happened
Those Cool Tools...

- Current Arsenal & Key Tools
- Procexp; procmon; tcpview
Single Footprint Intelligence

- Arsenal tools on steroids
- High level of visibility:
  - File ops
  - Network ops
  - Registry ops
  - DLL activity
  - Process data
- Application DNA ~ identifiable events
### Real Time Forensics Evidence

- Detect compromise events
- Log the foot prints

#### PROCESS_NAME | EVENT_NAME | EVENT_DISPLAY | BEGIN_TIME | COMPUTER_NAME | SRC_FILE_NAME | PROTO_NETWORK_ADDR | LOCAL_IP_REMOTE_HOSTNAME | OURLAYOUT
|-----------------|------------|---------------|------------|---------------|---------------|----------------------|---------------------------|------------------|

© DIGITAL GUARDIAN INC.
It’s Doing This so Probably Suspicious

- Enable behavioural analysis
- phishing : - (a+b),(c,(d|e)),!(x,y,z)
- Response?
  Kill any point in the chain
Keeping the Story Alive

- Increase Visibility:
  - More DLL events
  - Memory events

- Capture More...
Thank you...

- tfischer@digitalguardian.com
- tvfischer+sans@gmail.com
- @Fvt