I Thought I saw a Haxx0R

A Threat Hunting we Will Go!
I am ...

- Security Advocate & Threat Researcher with Digital Guardian
- 25+ years experience in InfoSec
- Spent number years in IR team positions
- Director @BSidesLondon
- ISSA UK Chapter Board Member
Let’s Talk Threat Hunting

- Threat Hunting Background - What is it?
- It’s a challenging game
- Can it be made better?
- Just Do IT
Threat Hunting as a Purpose

- The infrastructure can be at times quite opaque

- Today’s adversary is cunning, creative and adapts
  • They will use your own infrastructure and solutions against you

- Compromise is a given... So deal with it!
Threat Hunting in Practice

- Analyst versus Adversary
- Being creative and adaptive
- No particular indicators
- Deep analysis of potential compromised resources
- Finding what evades automated detection
And So What?

- Build a proactive footprint against attackers
- Understand your Infrastructure
  - System and Application configuration Gap analysis
  - Teams gain knowledge of the environment and infrastructure
- Identify common business workflows
- Never underestimate importance of contextual knowledge & awareness
- Documenting == Organisational Knowledge
Hunting: how it feels

Hunting: reality
War is ninety percent information

- **Firewall Logs**
  - Unusual IP address; Countries; businesses

- **Proxy Logs**
  - Port traffic (e.g. 22)
  - Bytes in = Bytes out
  - Dynamic DNS
  - Unique User String

- **Windows Logs**
  - Logon attempts
  - User added to privileged group

- **Anti-Virus Logs**

- **Process Maps**
  - All running on a system
  - Privileged execution

- **Endpoint Detection Solutions**
  - Reporting of indicators
  - Forensics
  - Logging of general events
Tempting, Tempting, ...

- **Use Analytics**
  - Consider machine-learning
  - User or entity behaviour analytics

- **Situational-Awareness**
  - Drive your hunt with identified critical assets
  - Risk assessments

- **Intelligence Driven**
  - Relying on IoCs and TTPs
  - Feeds
Nothing Better Than A Pair of Eyes

iz not stalking... just

intently staring
The 4 A’s

- Assess
- Analyse
- Articulate
- Adapt
I Twat I Taw a PuDDy Tat

Wait, let’s add some more data points

MANY
Process, Process, Process

- Which process are running?
  - Which are normal?
    - Which don’t belong?
  - Privileged Execution
    - Which user do they normal run under?
    - Abuse by 3rd Party applications
    - Which users run as local admin?

- Network Activity
  - Which process should and need to listen?
  - Which should make network connections?
    - Why is cscript connecting to the Internet
  - Are local FW/Filters being avoided
More System Information

- Know and understand kernel drivers
  - They are abused, e.g. Stuxnet
- Persistence - it’s not just the run key
- Scheduled Tasks - obfuscating and hiding tracks
- Services
  - Do you know what services should be running on your image?
Oh endpoint My endpoint

- It’s the Target of Attackers
  - Endpoint solutions drive to integrate that data
- Collect the configuration
- Pull as much typical indicator as possible
- Negative effect of generating toooooooooooo much data
What’s available...

- **Bit9**
  - Hashes
  - File Properties/Type
  - Registry

- **Carbon Black**
  - Network
  - Hashes
  - File Properties/Type
  - Registry
  - File Ops (PE only)
  - Command Lines

- **Mandiant**
  - Network
  - Hashes
  - File Properties/Type
  - Registry
  - File Ops (PE only)
  - Command Lines

- **CounterTrack**
  - Network (only IP/port)
  - Hashes
  - Registry
  - File Ops (PE Only)
  - Command Lines

- **CrowdStrike**
  - Network
  - Hashes
  - File Properties
  - Registry
  - File Ops (PE only)
  - Command Lines

- **Digital Guardian**
  - Network
  - Hashes
  - File Properties
  - Registry
  - Handles/Mutex
  - Command Lines
  - DLL Loads & Injection

Don’t forget IOCs...

Some also have capabilities to return: file captures, event logs, wmi data, strings
Real Time Forensics Evidence

- Detect compromise events
- Log the footprints

---

<table>
<thead>
<tr>
<th>PROCESS_NAME</th>
<th>EVENT_NAME</th>
<th>EVENT_DISPLAY</th>
<th>BEGIN_TIME</th>
<th>COMPUTER_NAME</th>
<th>SRC_ADDR</th>
<th>DST_ADDR</th>
<th>DST_PORT</th>
<th>PROTO</th>
<th>REMOTE_IP</th>
<th>REMOTE_PORT</th>
<th>REMOTE_HOSTNAME</th>
<th>OUTBOUND</th>
<th>URL_PATH</th>
</tr>
</thead>
</table>
### More Evidence

<table>
<thead>
<tr>
<th>Application</th>
<th>User Name</th>
<th>Operation</th>
<th>Custom String 4</th>
<th>DNS Hostname</th>
<th>IP Address</th>
<th>Remc</th>
<th>Local Port</th>
<th>URL Path</th>
</tr>
</thead>
<tbody>
<tr>
<td>wscript.exe</td>
<td>FVT-WIN7-H002\tfischer</td>
<td>Custom Event</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Command line: "C:\Windows\System32\WScript.exe"

<table>
<thead>
<tr>
<th>Application</th>
<th>User Name</th>
<th>Operation</th>
<th>Custom String 4</th>
<th>DNS Hostname</th>
<th>IP Address</th>
<th>Remc</th>
<th>Local Port</th>
<th>URL Path</th>
</tr>
</thead>
<tbody>
<tr>
<td>a1.exe</td>
<td>FVT-WIN7-H002\tfischer</td>
<td>File Write</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>a1.exe</td>
<td>FVT-WIN7-H002\tfischer</td>
<td>DLL Load</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Application</th>
<th>User Name</th>
<th>Operation</th>
<th>Custom String 4</th>
<th>DNS Hostname</th>
<th>IP Address</th>
<th>Remc</th>
<th>Local Port</th>
<th>URL Path</th>
</tr>
</thead>
<tbody>
<tr>
<td>mshta.exe</td>
<td>FVT-WIN7-H002\tfischer</td>
<td>Application Start</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>cmd.exe</td>
<td>FVT-WIN7-H002\tfischer</td>
<td>Application Start</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>cmd.exe</td>
<td>FVT-WIN7-H002\tfischer</td>
<td>Application Start</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>cmd.exe</td>
<td>FVT-WIN7-H002\tfischer</td>
<td>Application Start</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>a0.exe</td>
<td>FVT-WIN7-H002\tfischer</td>
<td>Custom Event</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>a0.exe</td>
<td>FVT-WIN7-H002\tfischer</td>
<td>Custom Event</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Application</th>
<th>User Name</th>
<th>Operation</th>
<th>Custom String 4</th>
<th>DNS Hostname</th>
<th>IP Address</th>
<th>Remc</th>
<th>Local Port</th>
<th>URL Path</th>
</tr>
</thead>
<tbody>
<tr>
<td>wscript.exe</td>
<td>FVT-WIN7-H002\tfischer</td>
<td>Custom Event</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Behaviour Tree

Outlook creates temp file → File write new location → Open of tagged file → Load of macro subsystem → Write file → Move file to user directory → Network connection → Execute command shell

Other process file open → Tag file

Attachment Opened

Active Attachment

Risk - unknown

Suspicious activity

Risk - elevated
It’s Doing This so Probably Suspicious

- Enable behavioural analysis
- phishing : - (a+b), (c, (d|e)), !(x,y,z)
- Build ALERTS based on behaviour
Intelligence at EndPoint

- Use the endpoint to drive behaviour analysis
  - Watch the activities and record
  - Don’t just collect stale data
- Highlight the pertinent events
- Get more interesting data
- Use that data to better understand behaviour
threat
Let's Get Our Hands Dirty
**Visualise & Analyse the data**

A screenshot showing a web interface with a table displaying event data. The table includes columns for `Time`, `User_Name`, `Computer_Name`, `Application`, `Operation`, `Event_Display_Name`, `Event_ID`, `Source_Name`, `Source_Identifier`, `Source_Process`, `Process_Name`, `Message`, and `Correlated_Rule_Hash`. The page is from the Digital Guardian platform, with the logo visible at the bottom.
Build Regex to Find Starting Point

Application="g64-*" OR "g32-*" OR "pwdump*" OR "gsecdump*" OR "lz77*" OR "cachedump*" OR "1s1sas*" OR "fgdump*" OR "wca.dll" OR "credump*" OR "samdump*" OR "mimikatz*" OR "m64.exe" OR "mimi_morph.exe" OR "wu.psl" OR "getlsasrvaddr" OR "iam.exe" OR "iam-alt" OR "whosthere.exe" OR "whosethere-alt" OR "genhash" OR wce.exe OR Destination_File="minidump.cmd" OR "lsass.dmp"

search = Custom_String_4="Command line: net localgroup administrators"

search = Custom_String_4="Command line: regsvr32*" AND Custom_String_4="*http*" Custom_String_4="Command line: regsvr32 /s ChilkatHttp.dll" Custom_String_4="Command line: regsvr32 /s \"HTTP Wizard2.ocx\"

Application="wmic.exe" Custom_String_4="Command line: \"C:\WINDOWS\system32\wbem\wmic.exe\" process call create*" OR Custom_String_4="Command line: C:\Windows\system32\wbem\wmic.exe process call create *" Custom_String_4="Command line: C:\Windows\system32\wbem\wmic.exe process call create \"cscript.exe \"\127.0.0.1\admin$\hexainstaller.vbs\"\" Custom_String_4="Command line: \"C:\Windows\system32\wbem\wmic.exe\" process call create \"powershell.exe -EncodedCommand JABFAHIAcgBvAHIAQQBjAHQAa*\""
Execution:

- Application_Full_Name="csrss.exe" | regex
  User_Name!="(NT AUTHORITY/SYSTEM|AUTORITE NT/Système|NT-AUTORITÄT/SYSTEM|AUTORIDADE NT/SISTEMA|NT AUTHORITY/система|ZARZĄDZANIE NT/SYSTEM)"

- Application="explorer.exe" | regex
  Application_Directory!="[c-f]:\\(windows|winnt)\\\(syswow64|system32)\"

- Application="lsass.exe" | regex
  Application_Directory!="[c-f]:\\windows\\system32"

- Application="a.exe" OR Application="b.exe" OR Application="c.exe" OR Application="d.exe" OR Application="e.exe" OR Application="f.exe" OR Application="g.exe" OR Application="h.exe" OR Application="i.exe" OR Application="j.exe" OR Application="k.exe" OR Application="l.exe" OR Application="m.exe" OR Application="n.exe" OR Application="o.exe" OR Application="p.exe" OR Application="q.exe" OR Application="r.exe" OR Application="s.exe" OR Application="t.exe" OR Application="u.exe" OR Application="v.exe" OR Application="w.exe" OR Application="x.exe" OR Application="y.exe" OR Application="z.exe" Application_Directory!="c:\agilent_ict\bin\" Application_Directory!="c:\agilent3070\bin\"

- Application="csrss.exe" | regex
  Application_Directory!="[c-f]:\\windows\\system32\\"
## AV Hits

<table>
<thead>
<tr>
<th>VTScanValue</th>
<th>Application_Full_Name</th>
<th>Application_Directory</th>
<th>MD5_Checksum</th>
<th>count</th>
</tr>
</thead>
<tbody>
<tr>
<td>55</td>
<td>product lines.exe</td>
<td>d:\1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>55</td>
<td>system volume information.exe</td>
<td>d:\1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>52</td>
<td>hoomen no m\ving.exe</td>
<td>e:\hoomen no m\ving</td>
<td></td>
<td></td>
</tr>
<tr>
<td>47</td>
<td>nurazadah zanai</td>
<td>a:\1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>47</td>
<td>print.exe</td>
<td>a:\1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>43</td>
<td>130..00.exe</td>
<td>e:\atmeri</td>
<td></td>
<td></td>
</tr>
<tr>
<td>35</td>
<td>updater.exe</td>
<td>c:\user\appldata\roaming\program\update\update\user\</td>
<td></td>
<td></td>
</tr>
<tr>
<td>35</td>
<td>updater.exe</td>
<td>c:\user\appldata\roaming\program\update\update\</td>
<td></td>
<td></td>
</tr>
<tr>
<td>30</td>
<td>prnprint.exe</td>
<td>c:\program files (x86)\print\</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

---

Link to threat feeds...
Looking for suspicious activity on Data

- **Alerts by Day**
  - Graph showing alerts by day from Thu Sep 1 to Thu Sep 29, 2016.
  - High alert on Sep 19, 2016.

- **By Severity**
  - Table showing rules, severity, alerts, and machines.
  - Rules:
    - ATP1201-D-Deletion of volume shadow copies detected
    - ATP3021-D-Launch of Executable from APPDATA
    - ATP3023-D-Launch of Executable from APPDATA-Roaming - secondary
    - ATP3032-D-Hidden Launch of Internet Explorer via DCOM
    - ATP1025-D-Capture file
    - ATP1204-D-Suspicious Process Modifying Local Hosts File
    - ATP3016-D-Process Launch from Archive via Temporary Location
    - ATP9201-IOC Persistence Detected
    - ATP1006-D-Office opens saved email attachment
    - ATP3030-D-Script launch off archive
  - Severity levels: Critical, High, Informational, Low, Medium
  - Alerts and Machines ranges:
    - ATP1201-D: Medium, Alerts 1, Machines 1
    - ATP3021-D: Medium, Alerts 1, Machines 1
    - ATP3023-D: Informational, Alerts 1, Machines 1
    - ATP3032-D: Medium, Alerts 1, Machines 1
    - ATP1025-D: Informational, Alerts 2, Machines 2
    - ATP1204-D: Medium, Alerts 2, Machines 2
    - ATP3016-D: Medium, Alerts 2, Machines 2
    - ATP9201-IOC: High, Alerts 2, Machines 2
    - ATP1006-D: Informational, Alerts 3, Machines 2
    - ATP3030-D: High, Alerts 3, Machines 3
ALRIGHT TEAM

LET'S DO DIS

meme crunch.com
Preparation

- Prepare your Team
  - Allocate time
  - Build a plan for documentation and tools
- Start SMALL
- Refine the process
  - Make sure you have all the right tools
- Move to wider Hunts
- Motiveate
  - Use internal “CTF” challenges with real data
Embedded into IR

- Get Executive Buy IN!
  - Use the results of preparation to show benefits

- Update Policy
  - IR needs to be an active part of Operations

- Augment skill set
  - Enterprise knowledge
  - Hypothesis
  - Statistics

- Incorporate new knowledge into incident handling analysis
Conclusions

- Threat Hunting can provide a great tool to stay ahead
- Minimise footprint where attackers can take a foot hold
  - Remove the dark holes
- Detect Breaches Yourself
  - Kill the 3rd party reporting syndrome
@Fvt Contact Me at

- tfischer@digitalguardian.com
- tvfischer+sec@gmail.com
- @Fvt
- keybase.io/fvt