Search and Destroy the Unknown

FROM MALWARE ANALYSIS TO INDICATIONS OF COMPROMISE
Who am I?

- Michael Boman, Malware Researcher
- Malware Research Institute
- Provide the community with knowledge and tools
Detecting the Unknown

- FBI: There are only two types of companies: those that have been hacked, and those that will be.
- Always assume that you have been compromised and look for signs to confirm the assumption
Where to look

- There is gold in those logfiles!
  - Firewall
  - IDS / IPS
  - Proxy
  - DNS
  - System logfiles
  - Netflow data
Firewall

- New sessions are enough, no need to log every packet
- Ingress (incoming) AND Egress (outgoing)
- Denied AND Permitted
IDS / IPS

- Detecting attacks are "nice", detecting compromises are "cool"
- You need **actionable** information from your IDS / IPS system
- Custom rules are the path to salvation
Proxy

- Detecting known bad sites
- Trace infections to source
- Detecting outliers
- Log queries
- Establish DNS query & response baseline
- Analyze NXDOMAIN responses
- Analyze successful DNS lookups
- Identify domain name abnormalities
<table>
<thead>
<tr>
<th>Windows 7 regular expressions</th>
<th>SOURCE</th>
<th>EventID Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>.<em>APPCRASH.</em></td>
<td>Application</td>
<td>1001</td>
</tr>
<tr>
<td>.<em>he protected system file.</em></td>
<td>Application</td>
<td>64004</td>
</tr>
<tr>
<td>.<em>EMET_DLL Module logged the following event:.</em></td>
<td>Application</td>
<td>2</td>
</tr>
<tr>
<td>.<em>your virus/spyware.</em></td>
<td>Application</td>
<td>Depends</td>
</tr>
<tr>
<td>.<em>A new process has been created..</em></td>
<td>Security</td>
<td>4688</td>
</tr>
<tr>
<td>.<em>A service was installed in the system..</em></td>
<td>Security</td>
<td>4697</td>
</tr>
<tr>
<td>.<em>A scheduled task was created..</em></td>
<td>Security</td>
<td>4698</td>
</tr>
<tr>
<td>.<em>Logon Type:[$W]</em>(3</td>
<td>10).*</td>
<td>Security</td>
</tr>
<tr>
<td>.<em>\Software\Microsoft\Windows\CurrentVersion\Run.</em></td>
<td>Security</td>
<td>4657</td>
</tr>
<tr>
<td>.<em>service terminated unexpectedly..</em></td>
<td>System</td>
<td>7034</td>
</tr>
<tr>
<td>.<em>service was successfully sent a.</em></td>
<td>System</td>
<td>7035</td>
</tr>
<tr>
<td>.<em>service entered the.</em></td>
<td>System</td>
<td>7036</td>
</tr>
<tr>
<td>.<em>service was changed from.</em></td>
<td>System</td>
<td>7040</td>
</tr>
</tbody>
</table>
Netflow data

- WHO is talking to WHOM
- When doing incident response, being able to narrow down the scope is key
Aquire the sample

- Extraction from network traffic
- File on disk
- Memory dump
Extracting from Network Traffic

- Wireshark
  - GUI
- Network Miner
  - GUI
- Foremost
  - foremost -v -i /path/to/pcap
- Dshell
  - DShell> decode -d rip-http --rip-output_dir=output/ /path/to/pcap
Creating the memory dump

```
PsExec.exe \HOSTNAME_OR_IP -u DOMAIN\privileged_account -p passwd -c mdd_1.3.exe -o C:\MEMORY.DMP
```

Extracting the executable / DLL from the memory dump

```
volatility dlldump -f MEMORY.DMP -D dumps/
volatility procmemdump -f MEMORY.DMP -D dumps/
```
Analyze the sample

- Confirm the malicious nature of the suspected sample
- Identify behavior that can be used to identify infected machines
Confirming the sample

- Static analysis
- Dynamic analysis
Cuckoo Sandbox

- Uses DLL-injection techniques to intercept and log specific API calls
- Uses TCPDump to capture network traffic
Minibis

- Uses Microsoft ProcMon inside the instrumented environment
- Uses TCPDump to capture network traffic
- ProcDOT can be used to analyze / visualize the execution process
Identify IOCs

- Identifiable patterns in the sample
- Created files
- Created / Modified registry keys
- Network traffic
- Memory patterns
rule silent_banker : banker
{
    meta:
        description = "This is just an example"
        thread_level = 3
        in_the_wild = true
    strings:
        $a = {6A 40 68 00 30 00 00 6A 14 8D 91}
        $b = {8D 4D B0 2B C1 83 C0 27 99 6A 4E 59 F7 F9}
        $c = "UVODFRYSIHLNWEJXQZAKCBGMT"
    condition:
        $a and $b and $c
}

alert tcp $HOME_NET any -> $EXTERNAL_NET 443 ( \
  content: "| 6A 40 68 00 30 00 00 6A 14 8D 91 |"; \
  content: "| 8D 4D B0 2B C1 83 C0 27 99 6A 4E 59 F7 F9 |"; \
  content: " UVODFRYSIHLNWPEJXQZAKCBGMT"; \
  msg: " silent_banker : banker C2 Traffic"; \
)
Mandiant IOC Finder

Collecting:
mandiant_ioc_finder collect [-o output_dir] [[-d drive]...] [-q] [-v] [-h]

Reporting:
mandiant_ioc_finder report [ [-i input_iocs]...] [-s source_data] [-t html|doc] [-o output_folder (html) or file (doc)] [-q] [-v] [-h] [-w verbose|summary|off]
Searching Network Traffic

- Firewall
  - Detection, Block specific communication

- IDS / IPS
  - Create signatures to Detect and Prevent C2 communication, additional infections

- Proxy
  - Detection, Block specific communication

- DNS
  - Detection, Block communication to sites
Contact information

- Website: blog.malwarereasearch.institute
- Twitter: @mboman
- Email: michael@michaelboman.org

Tools mentioned

Snort, DaemonLogger, PassiveDNS, SANCP, Wireshark, Network Miner, Xplico, Dshell, PsExec, MDD, Volatility, Cuckoo Sandbox, Minibis, ProcDot, Mandiant OpenIOC Editor, Yara, Mandiant IOC Finder, Mandiant Redline