SESSION ID: HT-F03

Malware and Misconfigurations
The 2nd Annual RSAC SOC Report

Jessica Bair - @jessicambair
Percy Tucker
Neil “Grifter” Wyler - @grifter801
New Presentation, Who dis?
RSAC SOC

- Conference Span/TAP
- Purely Educational
- RSA NetWitness Orchestrator
- RSA NetWitness Logs
- RSA NetWitness Packets
- Cisco Threat Grid
- Cisco Umbrella
- Cisco FirePower
- Cisco Talos Intelligence
- Random Python Scripts
- 4 Years Running
- 4 US Shows & 3 Asia Shows
- 15 Tours - 20-50 people each
- Countless “Private” Tours
- Multiple Press Interviews
The Team

- 10 RSA Analysts
- 4 Cisco Analysts
The Dashboards
More Dashboards!!!
The Stats

- Total Packets Captured: 12.7 Billion
- Total Logs Captured: 88.3 Million
- Total Sessions: 187,301,858
- 13,253 Unique Devices
- 8.08 TB of packet data
- 50.52 GB of log data
- Peak Bandwidth Usage: 1.3Gbps
  - Double last year
- ~37 Million DNS Requests
- ~78% Encrypted Traffic
- ~22% Mayhem

SSL & TLS
- Version - Session Count
  - SSL 3.0 - 217032
  - TLS 1.0 - 4909626
  - TLS 1.1 - 201061
  - TLS 1.2 - 131423097
It’s Raining Passwords

96,361 - Cleartext Passwords
2,178 - Unique Accounts
Threat Grid Malware Analysis

Over 10,000 samples

About 8 minutes to analyze

4,665 malware samples
## Malware Behavior

<table>
<thead>
<tr>
<th>Registry Persistence Mechanism Refers to an Executable in a System Directory</th>
<th>Orbital Queries</th>
<th>persistence</th>
<th>persistence</th>
<th>autorun</th>
<th>compound</th>
<th>process</th>
<th>registry</th>
</tr>
</thead>
<tbody>
<tr>
<td>Process Modified a File in a System Directory</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Artifact Flagged by Antivirus</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Process Checked for SoftICE</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Process Checked for SoftICE

**Score:** 66
**Hits:** 1

**Description**

A process attempted to open a connection to the SoftICE drivers. SoftICE is a kernel-mode debugger for Windows, often used as a reverse-engineering tool. Malware may do this to detect the presence of SoftICE as a means of anti-analysis.

**Trigger**

This indicator is triggered when a file handle for one of the SoftICE drivers is requested.

<table>
<thead>
<tr>
<th>Process</th>
<th>Process Name</th>
<th>Path</th>
</tr>
</thead>
<tbody>
<tr>
<td>Process 4</td>
<td>02f2bc9ab2648f702b7232002f68157f.exe</td>
<td>ntice</td>
</tr>
</tbody>
</table>
Moscone NOC built their own DNS resolution servers… wayyyy cool.

In 2020, pointed their DNS to Cisco Umbrella. Monday traffic ~7.5m requests.

Thus ~7.9m
Umbrella Total Requests ~37m

<table>
<thead>
<tr>
<th>Requests</th>
<th>Security</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Prevent</td>
</tr>
<tr>
<td></td>
<td>Malware</td>
</tr>
<tr>
<td></td>
<td>Dynamic DNS</td>
</tr>
<tr>
<td></td>
<td>Newly Seen Domain</td>
</tr>
<tr>
<td></td>
<td>Potentially Harmful</td>
</tr>
<tr>
<td></td>
<td>Dns Tunneling</td>
</tr>
<tr>
<td></td>
<td>Cryptomining</td>
</tr>
<tr>
<td></td>
<td>Contain</td>
</tr>
<tr>
<td></td>
<td>Command &amp; Control</td>
</tr>
<tr>
<td></td>
<td>Phishing</td>
</tr>
<tr>
<td></td>
<td>Integrations</td>
</tr>
</tbody>
</table>

Categories

Destination Lists

Permitted

Total: 37,182,378
# DNS App Discovery ~4k Applications

<table>
<thead>
<tr>
<th>Application</th>
<th>Weighted Risk</th>
<th>Application</th>
<th>Weighted Risk</th>
<th>Application</th>
<th>Weighted Risk</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sophos Security</td>
<td>Medium</td>
<td>Facebook Social Networking</td>
<td>Medium</td>
<td>London Trust Media VPN</td>
<td>Medium</td>
</tr>
<tr>
<td>Google Safe Browsing Security</td>
<td>Low</td>
<td>LinkedIn Social Networking</td>
<td>Low</td>
<td>Luminati Anonymizer</td>
<td>Very High</td>
</tr>
<tr>
<td>Facebook Connect Security</td>
<td>Medium</td>
<td>Twitter Social Networking</td>
<td>Medium</td>
<td>NordVPN Anonymizer</td>
<td>High</td>
</tr>
<tr>
<td>Google Accounts Security</td>
<td>Low</td>
<td>Instagram Social Networking</td>
<td>Medium</td>
<td>Mullvad Anonymizer</td>
<td>Medium</td>
</tr>
<tr>
<td>McAfee Endpoint Protection</td>
<td>Medium</td>
<td>Tik Tok Social Networking</td>
<td>Medium</td>
<td>Hola Anonymizer</td>
<td>Medium</td>
</tr>
<tr>
<td>Carbon Black Security</td>
<td>Medium</td>
<td>Pinterest Social Networking</td>
<td>Medium</td>
<td>Touch VPN Anonymizer</td>
<td>Medium</td>
</tr>
<tr>
<td>TrustArc Privacy Management</td>
<td>Medium</td>
<td>Exchange Online Office</td>
<td>Low</td>
<td>CyberGhost VPN Anonymizer</td>
<td>Medium</td>
</tr>
</tbody>
</table>
Firepower IDS Security Incidents

Network File Trajectory for ff190475...0141aaa2

- **File SHA256**: ff190475...0141aaa2
- **File Name**: ff190475...0141aaa2
- **File Size (KB)**: 85.0322
- **File Type**: MEXE
- **File Category**: Executables
- **Current Disposition**: Malware
- **Threat Score**: None
- **Detection Name**: W32.FF.190475F6-95.SB.X.TG

**Trajectory**
- **First Seen**: 2020-02-26 13:09:03 on 208.67.174.37 by No Authentication Required
- **Last Seen**: 2020-02-26 17:33:31 on 10.65.200.240 by No Authentication Required
- **Event Count**: 2
- **Seen On**: 3 hosts (2 displayed)
- **Seen On Breakdown**: 2 senders → 2 receivers (1 → 1 displayed)

**Events**
- 2020-02-26 13:09:03: Transfer from 208.67.174.37 to 10.65.200.240 by No Authentication Required
  - File Name: ff48a4259a750c7f6bc8d09f8262 
  - Disposition: Unknown
  - Action: Malware Cloud Lookup
  - Protocol: HTTP
  - Client: Wget
  - Description: Retrospective Event...

- 2020-02-26 17:33:31: Retrospective Event...
  - File Name: ff48a4259a750c7f6bc8d09f8262 
  - Disposition: Malware
Story Time
Who’s watching the watchers?
Can you hear me meow?
Insecurity as a Service
Sign me up!
G...D...P...Are you freaking kidding me?
Location! Location! Location!
What did you do for the Opening Reception?
Outlaw Country Countries
Three’s a Crowd?
Phishing site beacon…on the hour, every hour

Bullet point here (see slides 5–8 for instructions)

Bullet point here

Bullet point here
Are you the apple or the worm?

- Connections on port 139 and 445
- Continuous scanning
- Not stealth, very chatty
“Apply” Slide

- Encrypt
- Encrypt
- Encrypt...wait...no...Trust But Verify!
Thanks!

Jessica Bair - @jessicambair
Percy Tucker
Neil “Grifter” Wyler - @grifter801