Behavior and Misbehavior: The First Ever RSAC SOC Report

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

- Conference Span/TAP
- Packets
- Malware Analysis
- Cisco Threat Grid
- Educate Attendees

- 3 Years Running
- 3 US Shows & 2 Asia Shows
- 15 Tours - 20-75 people each
- Countless “Private” Tours
- Multiple Press Interviews
The Team

- 10 RSA Analysts
- 4 Cisco Analysts
The Dashboards
Cleartext or encrypted?

PERCENTAGE OF TRAFFIC ENCRYPTED – NO DECRYPTION
Cleartext or encrypted?

STRONG PASSWORDS OVER UNENCRYPTED TRANSPORTS?
All things are not configured equally

12:30AM: Arrive SFO Signature Flight Support
12:30AM: Five Emerald Limo (confirmation xxxxxx) will p/u and take xxxxxx to the SF Four Seasons (conf. # xxxxxx)
1:00AM: Arrive at Four Season, (xxx will be pre-registered)

10:45AM: Five Emerald (conf. # xxxxxx) will p/u xxxxxx at Four Seasons and take to Moscone West (This is actually the loading dock entrance on Howard St. between 4th and 5th St. I will meet the car as it comes down the ramp)
11:10AM-11:30AM: Blocking Rehearsal
11:30AM-12:45PM: Lunch/relax in private dressing room
1:00PM-1:45PM: xxxxxx presentation
1:55PM-2:15PM: Photo Op
2:20PM: Five Emerald (conf. # xxxxxx) will p/u xxxxxx and take to SFO (Signature Flight Support)
3:00PM: Flight Leaves SFO (xxxxx)
11:30PM: Arrive at xxxxxx
Cleartext or encrypted?

WEBCAMS
The RSAC Dating Pool

Harry, 17
About Harry:
Ginger fever. Very famous. Must be into scars.

Mashable
When Your Privacy Officer...
Malware Submissions

RSAC SOC Monthly Report

In March 2019, a total of 2,269 samples were submitted to Threat Grid by 1 user. Of these sample submissions, 2,081 received a Threat Score, and 1,094 were considered to be malicious.

This report covers the partial current month, so prior month comparisons are not yet available.

Submission Environment

- **Windows 7 64-bit**: 2,269
- **Other**: 0
- **Convicted**: 2,269

**Threat Score**

- **Completed**: 2,081 (92%)
- **Not Supported**: 99 (4%)
- **Innocuous**: 88 (4%)
- **Pending**: 1 (<1%)

**Top Indicators**

- Potential Code Injection Detected: 1,259
- Machine Learning Model Identified Executable Artifact as Likely Malicious: 1,014
- Artifact Flagged Malicious by Antivirus Service: 995
- Artifact Flagged as Malicious by Antivirus: 946
- Artifact Flagged by Anti-Malware and Machine Learning: 895
- Process Modified or Executable File: 818
- Artifact Flagged as Known Trojan by Antivirus: 724
- Static Analysis Flagged Artifact as Malicious: 672
- PE Has Sections Marked Executable: 647
- Executable with Indications of Malicious Intent: 448

**Submission Status**

2,269 Submissions
### Top Applications

<table>
<thead>
<tr>
<th>Application</th>
<th>Vendor</th>
<th>Weighted Risk</th>
</tr>
</thead>
<tbody>
<tr>
<td>Linode Hosting Services</td>
<td>Linode</td>
<td>High</td>
</tr>
<tr>
<td>Apple iCloud Cloud Storage</td>
<td>Apple</td>
<td>Medium</td>
</tr>
<tr>
<td>Google Search</td>
<td>Google</td>
<td>Low</td>
</tr>
<tr>
<td>Google Cloud Platform Application Development and Testing</td>
<td>Google</td>
<td>Low</td>
</tr>
<tr>
<td>Akamai Intelligent Platform Content Delivery Network</td>
<td>Akamai Technologies</td>
<td>Very Low</td>
</tr>
<tr>
<td>Apple iTunes Media</td>
<td>Apple</td>
<td>Low</td>
</tr>
<tr>
<td>Office 365 Office Productivity</td>
<td>Microsoft</td>
<td>Low</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Application</th>
<th>Vendor</th>
</tr>
</thead>
<tbody>
<tr>
<td>NordVPN Anonymizer</td>
<td>NordVPN</td>
</tr>
<tr>
<td>Windscribe Anonymizer</td>
<td>Windscribe</td>
</tr>
<tr>
<td>Private Tunnel Anonymizer</td>
<td>OpenVPN</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Application</th>
<th>Vendor</th>
</tr>
</thead>
<tbody>
<tr>
<td>Facebook Social Networking</td>
<td>Facebook</td>
</tr>
<tr>
<td>Twitter Social Networking</td>
<td>Twitter</td>
</tr>
<tr>
<td>Linkedin Social Networking</td>
<td>Linkedin</td>
</tr>
<tr>
<td>V Kontakte Social Networking</td>
<td>V Kontakte</td>
</tr>
<tr>
<td>Instagram Social Networking</td>
<td>Facebook</td>
</tr>
<tr>
<td>QQ Social Networking</td>
<td>Tencent</td>
</tr>
<tr>
<td>Google Plus Social Networking</td>
<td>Google</td>
</tr>
<tr>
<td>Pinterest Social Networking</td>
<td>Pinterest</td>
</tr>
<tr>
<td>Disqus Social Networking</td>
<td>Disqus</td>
</tr>
<tr>
<td>Tumblr Social Networking</td>
<td>Tumblr</td>
</tr>
</tbody>
</table>
Drivers from China
Selling in the Clear

ALL CURRENT LEADS – DEALS STARTED AT RSAC - ETC

And so...many...POs.
Pentesting
We Broke It!!
“Apply” Slide

- Encrypt
- Encrypt
- Encrypt
- Encrypt
Thanks!

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