A Hunting We Must Go

May 16, 2018

John Strand
A Hunting We Must Go!
We are doing the same thing
Over and Over Again
We are doing the same thing
Over and Over Again
We are doing the same thing
Over and Over Again
We are doing the same thing
Over and Over Again
We are doing the same thing
Over and Over Again
We are doing the same thing
Figure 44: Discovery methods

- **Overall**
  - Unrelated party (Ext): 34%
  - Fraud detection (Ext): 24%
  - Customer (Ext): 9%
  - Law enforcement (Ext): 8%
  - Actor disclosure (Ext): 7%
  - Unknown: 5%
  - Reported by user (Int): 4%
  - Financial audit (Int): 3%
  - NIDS (Int): 1%
  - Log review (Int): 1%
  - Fraud detection (Int): 1%
  - HIDS (Int): 1%
  - Incident response (Int): 1%
  - IT audit (Int): 1%
  - Monitoring service (Ext): 1%

- **Small**
  - Unrelated party (Ext): 23%
  - Fraud detection (Ext): 35%
  - Customer (Ext): 10%
  - Law enforcement (Ext): 14%
  - Actor disclosure (Ext): 6%
  - Unknown: 4%
  - Reported by user (Int): 2%
  - Financial audit (Int): 2%
  - NIDS (Int): 1%
  - Log review (Int): 1%
  - Fraud detection (Int): 1%
  - HIDS (Int): 1%
  - Incident response (Int): 1%
  - IT audit (Int): 1%
  - Monitoring service (Ext): 1%

- **Large**
  - Unrelated party (Ext): 52%
  - Fraud detection (Ext): 7%
  - Customer (Ext): 7%
  - Law enforcement (Ext): 1%
  - Actor disclosure (Ext): 5%
  - Unknown: 7%
  - Reported by user (Int): 9%
  - Financial audit (Int): 1%
  - NIDS (Int): 1%
  - Log review (Int): 1%
  - Fraud detection (Int): 1%
  - HIDS (Int): 4%
  - Incident response (Int): 4%
  - IT audit (Int): 2%
  - Monitoring service (Ext): 1%

Legend: Financial, Espionage, Other
## Cash Cow Tipping

<table>
<thead>
<tr>
<th>Name</th>
<th>Modified</th>
<th>Members</th>
</tr>
</thead>
<tbody>
<tr>
<td>AVG_Rick</td>
<td>--</td>
<td>4 members</td>
</tr>
<tr>
<td>McAfee_Mobile_Bea</td>
<td>--</td>
<td>4 members</td>
</tr>
<tr>
<td>SEP_Fletch</td>
<td>--</td>
<td>4 members</td>
</tr>
<tr>
<td>sophos_home_bbk</td>
<td>--</td>
<td>4 members</td>
</tr>
<tr>
<td>Sophos_Joff</td>
<td>--</td>
<td>4 members</td>
</tr>
<tr>
<td>Webroot_Fehrman</td>
<td>--</td>
<td>4 members</td>
</tr>
<tr>
<td>AV_Assignments.docx</td>
<td>1/5/2017 10:41 AM</td>
<td>4 members</td>
</tr>
<tr>
<td>BypassingAntiviruswithBashonWindows.docx</td>
<td>1/5/2017 10:41 AM</td>
<td>4 members</td>
</tr>
<tr>
<td>BypassingAntiviruswithBashonWindows(1).docx</td>
<td>1/5/2017 10:41 AM</td>
<td>4 members</td>
</tr>
</tbody>
</table>

---

**Secu360**

[Logo]

---

---

---
Why Current Strategies Aren’t Working

- Offensive: You will need to attack
- Defensive: Know our limitations
- Go back 5 or 6 years... What were they saying to defend networks?
  - Patch
  - AV
  - IDS/IPS
- What are they saying now?
  - Patch
  - AV
  - IDS/IPS
- Do you see the beginning of a bad pattern?
- This section is good for defense and for your attacks against the bad guys
Hunt Teaming

• **Actively** looking for advanced attackers
  – You probably have been compromised

• If we can bypass AV/IDS/IPS.. Attackers can too!

• Intelligent analysis of all data sources at your disposal
  – Lots of logs and data to analyze
  – Oh... And math, there’s lots of math as well
Automated Solution Aren’t Hunting
Data Analysis Problems

• Most advanced attackers can and will bypass traditional security tools with ease
• Constant nagging questions…
  – “Are we compromised now?”
  – “How can we analyze 1000’s of connections?”
• Intense need for advanced analytical tools
• Don’t break the bank
The RITA AI-Hunter Solution

• Builds on RITA for quicker analysis of complex data
• Only loads metadata, no privacy issues
• Rapid sorting and filtering
• Instant white-listing
• Dynamic pivot view and sorting
What Did You Think Security Was?
OODA

Whomever can do these things the fastest lives:
  - Observe
  - Orient
  - Decide
  - Act

Originally developed for fighter pilots

With current security models how many can you impact?

Works both ways, Disorient Attackers!
Another Way to Put It

\[ D_t + R_t < A_t \]

Or...

All Warfare is Based On Deception
“It’s one thing to cause a stolen computer to report its IP address or its geographical location in an effort to track it down. It is something entirely different to violate federal wiretapping laws by intercepting the electronic communications of the person using the stolen laptop.”

-Judge Walter Rice
Ethan Robish, Ben Donnelly, Tim Tomes, PaulDotCom, SecureIdeas, Mick Douglas, Ben Jackson, NOVA Team, John Strand, Dave Kennedy, Mark Baggett, Bill Swearingen, Trent Lo, John Hoyt
ANNOYANCE
ATTRIBUTION
ATTACK
ATTRIBUTION
Target: Demo_Page
Agent: JavaScript @ 118.209.173.68:50119
Time: 07/08/2013 05:37:49
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64)
            AppleWebKit/537.36 (KHTML, like Gecko)
            Chrome/27.0.1453.116 Safari/537.36
Latitude: -37.81175599999995
Longitude: 144.95826259999998
Accuracy: 20
Comment:
No Attacker Would Run This
Network User Authentication

Network User Authentication is required.

Log In Now

You are not logged in.
User IP: 209.177.194.130
Or This
Big Scary Bank

YOU SHALL NOT PASS GO.
Or... They Would
.Jar Combiner
Is It Time to Pray?
“God, grant me the serenity to accept people that will not secure their networks, the courage to face them when they blame me for their problems, and the wisdom to go out drinkin’ afterwards!”

-A.P. Delchi
An Invitation
RITA

https://github.com/activecm/rita

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>240 commits</td>
<td>5 branches</td>
</tr>
<tr>
<td>Analysis</td>
<td>- GOMAXPROCS on all operations</td>
</tr>
<tr>
<td>Commands</td>
<td>We don’t need this.</td>
</tr>
<tr>
<td>Config</td>
<td>Adding a version field to the config. This will be inserted into the...</td>
</tr>
<tr>
<td>Database</td>
<td>Adding a version field to the config. This will be inserted into the...</td>
</tr>
<tr>
<td>Datatypes</td>
<td>Fixed merge conflicts between staging and hannah-beacon</td>
</tr>
<tr>
<td>Etc</td>
<td>- GOMAXPROCS on all operations</td>
</tr>
<tr>
<td>Logmover/push</td>
<td>Wrote a push based mechanism for delivering logs from bro collector n...</td>
</tr>
</tbody>
</table>

Latest commit on 2023-07-07 2 days ago
John Strand

- www.blackhillsinfosec.com
- www.activecountermeasures.com
- @strandjs
- +1 303-710-1171
- Tinyurl.com/504extra2
One More Thing

- Free Webcasts
- Register here: tinyurl.com/ybo7aolm