Threat Analysis of Complex Attacks

Dmitry Bestuzhev
Head of Global Research and Analysis Team, Latin America
twitter.com/dimitribest
Traditional malware

- Analysis
- Cleaning
- Detection
- Updates
Complex attacks malware
Uncovering Complex Attacks

Think like you’re already infected
Outgoing Network Traffic

**Advantages**
- Suricata powered boxes
- DNS queries are not encrypted

**Problems**
- The Equation (Proxying)
- Duqu 2.0 (Tunneling to GW)
Memory Pots
Technical Analysis of the samples

Reversing
“Photographic Code based memory” required
DNS / IPs intelligence
Mapping victims
Profiles and Geo locations
Cloud detection
Yara rules and VirusTotal

<table>
<thead>
<tr>
<th>Date</th>
<th>File name</th>
<th>Source</th>
<th>Country</th>
</tr>
</thead>
<tbody>
<tr>
<td>2015-07-03 11:31:18</td>
<td>do not open this email_message.doc</td>
<td>8e71b01 (web)</td>
<td>US</td>
</tr>
<tr>
<td>2015-07-01 13:45:23</td>
<td>email_message.doc</td>
<td>39809e55 (web)</td>
<td>FR</td>
</tr>
<tr>
<td>2015-06-30 10:54:20</td>
<td>email_message.doc.txt</td>
<td>587760c1 (web)</td>
<td>GB</td>
</tr>
<tr>
<td>2015-06-29 03:34:39</td>
<td>email_message.doc</td>
<td>b6571eef (web)</td>
<td>TW</td>
</tr>
<tr>
<td>2015-06-26 20:15:45</td>
<td>spam.doc</td>
<td>20ae7f64 (community)</td>
<td>CA</td>
</tr>
<tr>
<td>2015-06-26 16:00:05</td>
<td>email_message.doc</td>
<td>3c0d45a0b (web)</td>
<td>US</td>
</tr>
<tr>
<td>2015-06-25 09:30:07</td>
<td>email_message.doc</td>
<td>8cd08a4 (web)</td>
<td>LT</td>
</tr>
<tr>
<td>2015-06-25 08:55:41</td>
<td>email_message.doc</td>
<td>ac54a51d (web)</td>
<td>RU</td>
</tr>
<tr>
<td>2015-06-26 03:19:11</td>
<td>email_message.doc</td>
<td>b6571eef (web)</td>
<td>TW</td>
</tr>
</tbody>
</table>
Sinkholing
Attribution

Don’t make conclusions by what you see
Guide to attribute properly

• Who are the victims?
• Level of expertise used in the code ($)
• Time zones from time stamps when available
• Remember it is only a vehicle
• Have a linguist expert in the team
• Got access to C2?
Cyber-weapons provisioning example

• CTwoPENC.dll (CVE-2015-2360)

  2014.08.25 01:20:04 (GMT)
  2014.08.25 01:19:03 (GMT)
  2014.07.06 09:17:03 (GMT)
Epic fail attribution

- Strings in the code
- Email addresses used to register C2 domains
Real life example of a wrong attribution
Arid Viper / Desert Falcons
Protection

The most complex task
The Australian Signals Directorate Top35 list

Stopping 85% of all complex attacks

<table>
<thead>
<tr>
<th>Whitelisting and Default Deny</th>
<th>Patching apps</th>
<th>Patching OS</th>
<th>Restrict admin privileges</th>
</tr>
</thead>
<tbody>
<tr>
<td>Essential</td>
<td>Medium</td>
<td>High</td>
<td>Medium</td>
</tr>
<tr>
<td>Essential</td>
<td>Low</td>
<td>High</td>
<td>High</td>
</tr>
<tr>
<td>Essential</td>
<td>Low</td>
<td>Medium</td>
<td>Medium</td>
</tr>
<tr>
<td>Essential</td>
<td>Medium</td>
<td>Medium</td>
<td>Low</td>
</tr>
</tbody>
</table>
Network / System

Internal OS instrumentation

DNS filtering
Thank you

@dimitribest