Microsoft Threat Intelligence

Sergio Caltagirone
@cnoanalysis

Microsoft Threat Intelligence Center
Detect. Respond. Protect.

Threat investigations
Threat intelligence
Global cybersecurity analytics
Microsoft Threat Intelligence Practice
Collecting cybersecurity data across Microsoft’s global sensors

- More than 35 billion messages scanned monthly
- Daily tracking of 600,000 addresses sending spam
- More than 250 million Windows Defender users worldwide
- Millions of consumers protected worldwide
- Performs billions of malware removals per year worldwide
- Millions of computers running Microsoft enterprise anti-malware solutions
- More than 420 million active users
- 700 million computers reporting monthly
- 18+ billion web-page scans per month
- More than 40 billion executions since 2005
- 1 billion customers across enterprise and consumer segments
- 200+ cloud services
Intelligent security graph

Operations Management Suite (OMS)
Azure Security Center (ASC)

Azure Active Directory
Microsoft Accounts

Windows Defender Advanced Threat Protection (ATP)
Windows Defender Antimalware

Office 365 Advanced Security Management (ASM)
Exchange Online Protection (EOP)

Advanced Threat Analytics (ATA)
Microsoft Cloud Application Security (MCAS)

Humans

INTERFLOW API & THREAT ATTRIBUTION SERVICE
(Interface into Threat Intel big data platform and attribution reports)

ANALYTICS
(Machine Learning, detonation service, behavioral tracking/heuristics)

DATA COLLECTION & NORMALIZATION
(Data feeds from products)

Privacy/Compliance boundary

Products generate their own data which feeds back into the graph
Products use Interflow APIs to access results
Analytics surfaces findings to help fuel new discoveries
Data is processed
Products send data to graph
Products are instrumented to send data with privacy/compliance in mind
Next-gen analytics built from security awareness and endpoint data

Next-gen Threat Intelligence compiled by indicators of compromise

Enhanced correlation driven by big data + machine learning
Hunters

- Hunters are matrixed by service and threat
- Threats are handled as a virtual team (v-team) of hunters
  - Stretch workload
  - Spread capabilities across the threats
  - Decrease single points of failure
  - Integrates other teams easily

<table>
<thead>
<tr>
<th></th>
<th>Hunter 1</th>
<th>Hunter 2</th>
<th>Hunter 3</th>
<th>Hunter 4</th>
</tr>
</thead>
<tbody>
<tr>
<td>Threats</td>
<td>BORON v-team</td>
<td>DUBNIUM v-team</td>
<td>STRONTIUM v-team</td>
<td>CHLORINE v-team</td>
</tr>
<tr>
<td></td>
<td>HELIUM v-team</td>
<td></td>
<td>DUBNIUM v-team</td>
<td>CARBON v-team</td>
</tr>
<tr>
<td>Services</td>
<td>O365</td>
<td>Azure</td>
<td>Windows</td>
<td>Windows</td>
</tr>
</tbody>
</table>

*Notional organization*
Activity Groups

- DiamondModel.org
- Logical Grouping
  - Infrastructure, Capability, Victimology
- Formal definition
- Labeled for ease
SCUBA Pivot
Applied analytics at Microsoft
• Active since 2009
• Small number of campaigns focused on governments and related in Southeast Asia
• Multiple zero-days
• Attempts to hide using self-deletion and operations within victim working hours
• Access victims for years
# Leveraging Threat Intel Informed Protection

<table>
<thead>
<tr>
<th>Activity Group Reports</th>
<th>Campaign Reports</th>
<th>Technical Reports</th>
</tr>
</thead>
<tbody>
<tr>
<td>Adversary goals and intent</td>
<td>Live campaigns (tied to adversary)</td>
<td>Actor implants</td>
</tr>
<tr>
<td>Targeted Industries</td>
<td>Tactics Techniques Procedures (TTP)</td>
<td>Lateral movement</td>
</tr>
</tbody>
</table>
Detect. Respond. Protect.

Global cybersecurity analytics
Threat intelligence
Threat investigations