It Takes a Village
Reducing the Threat Gap by Allying with Your Competition

Presented by: Scott Maring (smaring@checkpoint.com)
Developed by: Michael A. Barkett (mbarkett@checkpoint.com)
SecTor: October, 2013
Foundation: The Patch Gap

- 0-day is relevant from the moment an exploit exists
  - Regardless of whether the vendor is aware
- Patching is a window, not a point in time
It Never Ends: The Threat Gap

- Attackers more determined, sophisticated
- More precise targeting
- 0-day became a real threat
We fight back, but staying ahead is difficult...

- Can’t proxy the entire Internet, so we add technology

- IPS
- App FW
- Web Security
- Anti-bot
- URLF
- Anti-spam
- DLP
The Unpredictable Nature of Users

- Too many logs?
- How are you correlating the massive amount of information?
- Trusted vs. untrusted (BYOD complications)
Let’s breathe some life into the situation!

Alive, yet not sentient ...
Industry Applicability

Healthcare & Financial Services?

2012: SCADA / Critical Infrastructure
How can we collaborate?

- ISACs
- Don’t discuss the details of the proceedings
- Actively participate!
- Be truthful and forthcoming
- No product pitches
- Shirts and shoes ok
The World’s Largest Neighbourhood Watch
Ephemeral: Flash in the pan

- Customized for a specific moment in time
- Designed to evade detection

<table>
<thead>
<tr>
<th>Country</th>
<th>Attack Name</th>
<th>Number of reports</th>
<th>First seen</th>
<th>Last seen</th>
</tr>
</thead>
<tbody>
<tr>
<td>PT</td>
<td>c960035c42e5e6097bd828dad777aad6</td>
<td>27</td>
<td>2013-07-29 10:31:15.0</td>
<td>2013-07-29 14:14:41.0</td>
</tr>
<tr>
<td>IL</td>
<td>c960035c42e5e6097bd828dad777aad6</td>
<td>22</td>
<td>2013-07-29 11:23:58.0</td>
<td>2013-07-29 13:40:31.0</td>
</tr>
<tr>
<td>US</td>
<td>c960035c42e5e6097bd828dad777aad6</td>
<td>7</td>
<td>2013-07-29 12:08:19.0</td>
<td>2013-07-29 13:08:19.0</td>
</tr>
</tbody>
</table>

VirusTotal Analysis:
- SHA256: 9072692314416ec5501011a01da99463c76aeeca7242b3d94464b6c9d7285e00e
- File name: cachedstream-DA8-6.tmp
- Detection ratio: 28 / 47
- Analysis date: 2013-09-26 06:01:22 UTC (1 week, 4 days ago)
Real-time Collaboration Regardless of Industry Vertical

Real-time sharing for immediate protection
Real-world Zero-Day: Findings

• Over 50 unique instances in the same day

• Nearly 1000 **targeted** attack attempts originated from domains such as:
  • Collegeclub.com
  • Injersey.com
  • Teacher.com
  • Techauto.net
  • Wiredsolutions.net

• Threat Emulation detected characteristics such as files and processes created or destroyed, etc.

Real-world Example

• Never before seen document, late July, 2013:

From: Sir Brown <sirbrown@>
To: Mike Barkett
Subject: Watch out for these addresses

Message

This is the latest update to the blocked IP addresses. Please make sure your systems are up to date.

Regards.

• Turns out it is malware

• Creates processes, replicates, steals passwords, etc.
The Alliance

Global **Sharing** of Symptoms

- Malware Research
- Signature Development
- Update all gateways

- >100k enterprise customers
- Millions of hosts

Collaboration of Data ➞ Research ➞ Distribution
Q&A

Image credits
Oak tree: http://fc01.deviantart.net/fs28/f/2008/133/7/c/Oak_tree_by_attila0427.jpg
Thank you!

Scott Maring (smaring@checkpoint.com)

SecTor: October, 2013