Minimising the Damage Caused by Malware When Infection is Inevitable

Phil Wood
Consulting Security Engineer
Advanced Threat Solutions Group
Malware is an ever-growing problem
How did we get here?

Cybercrime is lucrative, barrier to entry is low
Hackers are smarter and have the resources to compromise your organization
Malware is more sophisticated
Organizations face tens of thousands of new malware samples per hour

95% of large companies targeted by malicious traffic
100% of organizations interacted with websites hosting malware

Why has detection failed?

• Malware no longer infects as individual files
• The initial virus is often bespoke – custom written for a single attack campaign
• Once the infection has taken place, more unique malware is downloaded and the cycle is repeated.
• Local detection lacks the processing power, storage and perspective necessary
• The bad-guys are clever, resourceful and well motivated
Selecting your malware protection technology based upon detection rates is really just selecting your method of failure...
Compromise is the new normal
It’s time for a different approach
Cisco AMP delivers a better approach

Detect what you can… …Deal with what you can’t

Point-in-Time Detection

Retrospective Security

File Reputation & Behavioral Detection

Continuous Protection
Cisco Advanced Malware Protection
Built on unmatched collective security intelligence

- 1.6 million global sensors
- 100 TB of data received per day
- 150 million+ deployed endpoints
- 600 engineers, technicians, and researchers
- 35% worldwide email traffic

- 13 billion web requests
- 24x7x365 operations
- 4.3 billion web blocks per day
- 40+ languages
- 1.1 million incoming malware samples per day

- AMP Community
- Private/Public Threat Feeds
- Talos Security Intelligence
- AMP Threat Grid Intelligence
- AMP Threat Grid Dynamic Analysis
- 10 million files/month
- Advanced Microsoft and Industry Disclosures
- Snort and ClamAV Open Source Communities
- AEGIS Program

Automatic Updates in real time
Cisco AMP defends with reputation filtering and behavioral detection

Reputation Filtering

Behavioral Detection

But ALL Detection will fail at some point!
Cisco AMP defends with Retrospective Security

- Retrospection
- Attack Chain Weaving
- Behavioral Indications of Compromise
- Trajectory
- Breach Hunting
### Complete environment protection with AMP

<table>
<thead>
<tr>
<th>Address Threat Vector</th>
<th>Each deployment option offers extensive protection across its particular threat vector</th>
</tr>
</thead>
<tbody>
<tr>
<td>Prevent Infection</td>
<td>Since infections are designed to spread, protecting against one or two attack vectors is insufficient for today’s threats</td>
</tr>
<tr>
<td>Working Together</td>
<td>Deploying AMP for Content, Network and Endpoint together is the best available means of complete environment protection, quarantine and remediation</td>
</tr>
</tbody>
</table>
Protection across networks

The Network platform uses indications of compromise, file analysis, and in this example file trajectory to show you exactly how malicious files have moved across the environment.
## Network Trajectory

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Unknown file is downloaded to device</td>
</tr>
<tr>
<td>2</td>
<td>Fingerprint is recorded and sent to cloud for analysis</td>
</tr>
<tr>
<td>3</td>
<td>The unknown file travels across the network to different devices</td>
</tr>
<tr>
<td>4</td>
<td>File trajectory automatically records time, method, point of entry, systems impacted and prevalence of the file</td>
</tr>
<tr>
<td>5</td>
<td>Sandbox analytics determines the file is malicious and notifies all devices</td>
</tr>
<tr>
<td></td>
<td>File trajectory provides greater visibility into the extent of an infection</td>
</tr>
</tbody>
</table>

### Diagram:

- **Collective Security Intelligence Cloud**
- **Network**
- **Virtual Machine**
- **Mobile**
- **Computer**

Connections between devices illustrate the spread of an unknown file across the network.
Protection across endpoints

The Endpoint platform has device trajectory, elastic search and outbreak control which in this example is shown quarantining recently detected malware on a device that has the FireAMP connector installed.
Firefox user connects to http://www.downloaders.com

Downloads an unknown .zip

Two files are accessed when the .zip is opened, it creates a DLL, and a PDF.

PDF Reader application is opened to read the PDF.

Acrobat launches svchost.exe

3 files are downloaded.

svchost.exe connects to http://192.168.1.12

2 files detected by AMP.

Our last unknown file opens a dialog window and awaits response.

File #3, connects to 4 IP addresses and downloads another undetected file.

The last unknown file launches calc.exe, hollows the process and begins listening for remote connections.

Our last unknown file launches calc.exe, hollows the process and begins listening for remote connections.
Protection across web and Email

AMP for Content protects against web and email threats by issuing retrospective alerts when malware or malicious signatures are detected.
Cisco Zero-Hour Malware Protection
Cisco AMP Retrospective Alerts

Retrospective alerts and reports

- Give updates on files that have passed through the system
- Alert administrators to files that have changed disposition
- Inform you of files that had delayed payloads or other techniques designed to bypass sandboxing
In conclusion

• You can no longer rely on detection
• What’s needed is visibility and control
• In a world where infection is inevitable you need to have the tools in place to find and eliminate the threat
• The goal is to remove the Persistence from Advanced Persistent Threats

Decreasing the Time to Respond...

...Decreases the Cost of the Breach
Q&A/Thank You