Proactively Discovering Malicious Activity On Your Network

Mark Guntrip
Product Marketing, Symantec

Mark Feeney
Manager, IT Security, AMETEK
Agenda

1. The Best Place to Detect Malicious Behavior
2. Different Viewpoints
3. AMETEK Real-World Case Study
The big question...

“Where is the best place to detect malicious behavior?”
Your poll will show here

1
Install the app from pollev.com/app

2
Make sure you are in Slide Show mode

Still not working? Get help at pollev.com/app/help
or
Open poll in your web browser
The big question...

At what point do you believe advanced threats are stopped or identified?

- **Gateway**
- **Endpoint**
- **Network**
- **Cloud**
- **Server**
What does this question mean to different people?

- Where my core data resides
- I’m blocking threats before they get in
- What I think malicious activity is
- Where I believe I might be vulnerable
- Within the bounds of my control
What does this question mean to different people?

I’m blocking threats before they get in
Shortened URLs

Dear Sir/Madam,

Please find enclosed my resume.

http://bit.ly/O0ecdf

Many Thanks

George Wallis
Real Time Link Following
Active Content

What I think malicious activity is

Where my core data resides

Where I believe I might be vulnerable

I'm blocking threats before they get in

Within the bounds of my control
Disarm Technology

• **Problem**: attacks using malicious, attached email documents
  – Primarily used in spear phishing emails – Advanced Persistent Threat (APT)
  – Contain malicious active content, or exploit payloads targeting parser vulnerabilities

• **Solution**: reconstruct attachment documents from scratch before presenting to the user
Content Download

What I think malicious activity is

Where my core data resides

What I believe I might be vulnerable

Within the bounds of my control

I'm blocking threats before they get in
Symantec Insight

Insight makes decisions based on who downloads what from where...

Not just how many times a file is downloaded.

When one machine downloads a file, all reputations must be re-calculated!

That’s over 100 billion associations that must be refreshed every few hours!
Drive-by Download

What I think malicious activity is

Where I believe I might be vulnerable

I’m blocking threats before they get in

Where my core data resides

Within the bounds of my control
Network Threat Protection

- Threat Protection Efficacy from Drive-by Downloads
- Prevent browser exploitation

- Blocks attacks where endpoint protection may not be in place such as BOYD support
- Detect internal malware proliferation

64% of Symantec malware blocks due to network threat detection
Devices Outside The Network

- Where I believe I might be vulnerable
- Where my core data resides
- Within the bounds of my control
- I'm blocking threats before they get in
- What I think malicious activity is
Cloud Security
Unmanaged Devices

What I think malicious activity is

Within the bounds of my control

I'm blocking threats before they get in

Where I believe I might be vulnerable

Where my core data resides

Within the bounds of my control
Protect Technologies

• Gateway/cloud
  – Email Security – on-premise and cloud – strip active content, follow links
  – Web Security – on premise and cloud – detect botnet activity, protect remote devices when they are off-network
  – Protect unmanaged devices

• Server/Endpoint
  – Prevent malicious content from installing
  – Detect malware post-infection
Shift in viewpoint

Realization

Customer Needs Shift

I'm blocking threats before they get in
Detecting and stopping malware activity

I'm blocking threats before they get in
Gateway

- Command & Control Communications
- Botnet activity
- Inactive botnets
Detecting and stopping malware activity

- Managed Security Services

Symantec MSS

- Threats
- Vulnerabilities
- Malcode
- File & Site Reputation
- Compliance Restriction
- Organization
- Asset Value
- System Function
- Network
- Server
- Endpoint
- Data

I'm blocking threats before they get in.
Shift in viewpoint

Realization

Customer Needs Shift

Breach is Inevitable

From Protection Only

To Protection + Detection and Response
How AMETEK Found, Watched & Beat a Malware Campaign

Mark Feeney
Manager, IT Security - AMETEK
• $3.6B global manufacturer of electronic instruments and electro-mechanical devices
• AMETEK is a component of the S&P 500 Index. (AME)
• Over 120 Manufacturing and 80 sales and services locations
• 30 Countries
• 4 Data Centers. Boston MA, Horsham PA, Leicester UK, Singapore
• 14,000 employees worldwide
## Timeline

<table>
<thead>
<tr>
<th>Date</th>
<th>Event Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>June 2013</td>
<td>• Just a little “noise”</td>
</tr>
<tr>
<td>Sept 2013</td>
<td>• FBI, San Diego</td>
</tr>
<tr>
<td>Oct 2013</td>
<td>• Aahh. There it is!</td>
</tr>
<tr>
<td>Nov 2013</td>
<td>• FBI, Boston</td>
</tr>
<tr>
<td></td>
<td>• Ongoing process begins</td>
</tr>
</tbody>
</table>
Key Takeaways

• If the FBI wants to talk to you, talk to them
• Don’t be afraid to ask your vendors for help
• If you haven’t already, upgrade to SEP 12.1
• Reduce lateral movement
• Eliminate password reuse

• Look to gateway security measures to maximize visibility
• Devices outside your control are still critical
• Plan to Protect, Detect, Respond, Recover
For more information on Symantec future plans for malware and targeted attack detection:

Gateway, Cloud and Targeted Attacks: Symantec’s Vision, Strategy and Roadmap
10.15 – 11.15AM
AUGUSTUS BALLROOM 2
Thank you!

YOUR FEEDBACK IS VALUABLE TO US!

Please take a few minutes to fill out the short session survey available on the mobile app—the survey will be available shortly after the session ends. Watch for and complete the more extensive post-event survey that will arrive via email a few days after the conference.

To download the app, go to https://vision2014.quickmobile.com or search for Vision 2014 in the iTunes or Android stores.