Help! I Think I’ve Been Hit with Malware

Todd Fitkin
Leader, America’s Security Response Liaisons

Kari Ann Christensen
Product Marketing Manager Endpoint Protection
Why do we need this discussion?
If 2007 Threats = 1 Pint of Beer

2007 SEP 11 Released

Yearly: < 500,000 worldwide threats
2011 Threats = 8 Kegs

2007 SEP 11 Released

Yearly: < 500,000 worldwide threats

2011 SEP 12 Released

Daily: 500,000 threats by lunch

Help! I Think I’ve Been Hit with Malware
Best Practices

1. Prepare
2. Planned Response
3. Defined Process
4. Manage Expectations
5. Prioritize
## Preparing for the Inevitable

<table>
<thead>
<tr>
<th>Incident Response</th>
<th>Review or prepare a plan for each team and ORG</th>
</tr>
</thead>
<tbody>
<tr>
<td>Inside Teams</td>
<td>Review your list of teams to involve and their contact information (update DLs, emergency phone numbers)</td>
</tr>
<tr>
<td>Outside Teams</td>
<td>Be prepared to take actions that may involve teams outside the AV group in your company</td>
</tr>
<tr>
<td>Protection Technologies</td>
<td>Review installed/available protection technologies</td>
</tr>
</tbody>
</table>
Layered Protection
Defends against known and unknown threats

Symantec Endpoint Protection 12

- Network IDS
- Boundary Firewall
- Verify All Machines Are Protected
## Preparing for the Inevitable

<table>
<thead>
<tr>
<th>Incident Response</th>
<th>Review or prepare a plan for each team and ORG</th>
</tr>
</thead>
<tbody>
<tr>
<td>Inside Teams</td>
<td>Review your list of teams to involve and their contact information (update DLs, emergency phone numbers)</td>
</tr>
<tr>
<td>Outside Teams</td>
<td>Be prepared to take actions that may involve teams outside the AV group in your company</td>
</tr>
<tr>
<td>Protection Technologies</td>
<td>Review installed/available protection technologies</td>
</tr>
<tr>
<td>Relevant</td>
<td>Know what data you need when contacting your security partners</td>
</tr>
</tbody>
</table>
Three Main Inquiries

Am I protected from X?

Infected? Can’t find it.

Outbreak. What do I do?
Three Main Inquiries

Am I protected from X?

Infected? Can’t find it.

Outbreak. What do I do?
Does Symantec know about X threat and am I protected?

- Trj/Cl.A
- W32.Changeup
- W32/Autorun.worm.aaeh
- Worm.Win32.VBNA.b
- W32/VBNA-X
- Win32/Vobfus.MD
Three Main Inquiries

Do you know about X Threat, and am I protected?

I think I have a Threat but I can’t detect or find it

I’m in an Outbreak, what do I do?
Steps for Troubleshooting a Suspected Threat

1. **ID Threat**
2. **ID Infected Computers**
3. **Quarantine Network**
4. **Clean Infection**
5. **Post Op**

Help! I Think I’ve Been Hit with Malware
SymHelp – Load Point Tool

- Installed products:
  - Symantec Endpoint Protection Client
  - Symantec Endpoint Protection Console
  - System Recovery

- Other products:
  - Symantec Backup Exec Agent for Windows
  - Symantec Backup Exec Server
  - Symantec DLP Detection Server
  - Symantec DLP Endpoint Agent
  - Symantec DLP Enforce Server
  - Symantec Mail Security for Microsoft Exchange

- Run Product Scans
  - Click to Start Scan
  - Selected Product Scan
    - Health check (installed products)
    - Best practices (installed products)
    - Pre-install check
    - Full data collection for support

- Scan Status
  - Check one or more products and scans options. Then click the Scan button.

- Run Threat Analysis Tools
  - Symantec Power Eraser
  - Symantec Load Point Analysis

- Support Resources
  - Search Knowledge Base
  - Browse Forums
  - Open a Case Online
  - Contact Technical Support
  - Contact Customer Care

- System Usage
  - Memory: 32%
  - CPU: 1%
  - Disk: H: / 29%, G: / 39%, F: / 22%
SymHelp – Load Point Tool

Analysis was performed on 3206 files. 99.1% (3178) of the files were verified as good using their digital signature. 0.8% (25) of the files were verified as good using the Symantec Reputation database. 0.1% (2) of the files were verified as bad by the Symantec Reputation database. 0.0% (1) of the files had additional checks run.

0.0% (1) of the files should be manually verified or sent to Symantec Security Response for verification.

Copy files to a folder...

Found 1 files whose score indicate they should be manually verified or sent to Symantec Security Response for verification or Suspect or Malicious files should be never be sent directly to Symantec Support or hosted in a non-secure location. For review by Symantec Security Response, please submit the files through the secure website provided by you.

Score File

-250  F:\Documents and Settings\sealchan\Desktop\botsetup.exe

Autorun.inf is not present on the following drives: F:\, G:\, H:\.

...\Winlogon\Shell is set to 'Explorer.exe'.

...\Winlogon\userinit is set to 'F:\WINDOWS\system32\userinit.exe'.
Help! I Think I’ve Been Hit with Malware

Steps for Troubleshooting a Known Threat

ID Threat → ID Infected Computers → Quarantine Network → Clean Infection → Post Op
Steps for Troubleshooting a Known Threat

1. ID Threat
2. ID Infected Computers
3. Quarantine Network
4. Clean Infection
5. Post Op

Help! I Think I’ve Been Hit with Malware
Steps for Troubleshooting a Known Threat

1. ID Threat
2. ID Infected Computers
3. Quarantine Network
4. Clean Infection
5. Post Op
Steps for Troubleshooting a Known Threat

1. ID Threat
2. ID Infected Computers
3. Quarantine Network
4. Clean Infection
5. Post Op
Three Main Inquiries

1. Do you know about X Threat, and am I protected?
2. I think I have a Threat but I can’t detect or find it
3. I’m in an Outbreak, what do I do?
W32.Changeup

- Very Successful threat due to open shares, mixed AV versions, no AV and AutoPlay
- Does not rely on vulnerabilities to propagate
- Downloads repacked variants once a day
- One of three pieces of this attack. Each piece can download others
Expedite the Support Process

✔ Call Support
  – Severity 1 case for outbreaks

✔ Submit a sample

✔ Duty Manager
  – If the issue appears stalled, call and ask for a Duty Manager!
  – For both internal and external callers

✔ Key words
  – Outbreak
  – Breach
  – Escalate
In Case of a Breach...

CYBER INCIDENT ADVISORY & RESPONSE

EMAIL: Cyber_Incident_Advisory@symantec.com
TEL (US): +1-650-527-9200 | TEL (EMEA): +44 (0)20 8280 1702

REACT

REVIEW AND ASSESS THE SITUATION
ENGAGE WITH SPECIALIST TEAMS
ALERT STAKEHOLDERS
COLLECT EVIDENCE AND DATA TO ANALYSE TRENDS
TAKE STEPS TO REDUCE THE IMPACT AND RECOVER

Help! I Think I’ve Been Hit with Malware
## Best Practices

<table>
<thead>
<tr>
<th></th>
<th>Prepare</th>
<th>Planned Response</th>
<th>Defined Process</th>
<th>Manage Expectations</th>
<th>Prioritize</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Preparation = quicker resolution</td>
<td>Prior to an emergency, plan how you will respond</td>
<td>Follow a process from identify to remediation</td>
<td>It may affect users and be time consuming</td>
<td>Clarify the impact and the urgency</td>
</tr>
</tbody>
</table>

Help! I Think I’ve Been Hit with Malware

Symantec Vision 2013
Best Practices

1. Prepare
   Preparation = quicker resolution

2. Prioritize
   Clarify the impact and the urgency

3. Response
4. Process
5. Expectations

Prior to an emergency, plan how you will respond.
Follow a process from identify to remediation. It may affect users and be time-consuming.

Help! I Think I’ve Been Hit with Malware
Thank you!

Todd Fitkin
tfitkin@symantec.com

Kari Ann Christensen
Kariann_christensen@symantec.com
Appendix

• Best Practices for Troubleshooting Viruses on a Network
• Using Application and Device Control in Symantec Endpoint Protection (SEP) to block activity in common loading points for threats
• How to create custom policies in SEPM to prevent a threat from spreading.
• SymHelp Tool
• Norton Power Eraser
Symantec Endpoint Protection Training Offerings

To make sure that your team can get the most from your purchase of Endpoint Protection, Symantec Education provides training on

- Installing, Configuring, Monitoring, and Managing Endpoint Protection
- Using SNAC and SPC
- Guarding against hackers and viruses

Symantec Education can help your team get the most from security investment and trains you on optimizing the powerful antivirus software solution for both virtual and physical environments.

For more information on Endpoint Protection training offerings, Visit: http://go.symantec.com/education_sep

Endpoint Protection education is available as a prepackaged training bundle that maximizes proficiency and you can gain industry recognized expertise through the Symantec Certification Program.

The bundle includes:
- Instructor-led training
- On-demand instructor-led training (via video)
- Symantec eLibrary subscription (includes extensive training on SNAC and SPC).
- Certification voucher

For more information: please contact your local Symantec Education office.
Symantec Education for Symantec Endpoint Protection

Training Credits
• Credits can be used on most training offerings.
• Volume Discount

eLibrary
• Allows access to training across Symantec products.
• On-demand format allows for anytime, anywhere training.

Endpoint Protection Tech Center
• Annual subscription offering for SMB customers. This extensive collection of short, on-demand modules describes how it improves your productivity, saves you time, saves your business money.

Learn more:  http://go.symantec.com/education_sep.

For more information: please contact your local Symantec Education office.

Special Offer: FREE Training Modules are available via the Symantec Endpoint Protection Tech Center.
Steps for Troubleshooting a Suspected Threat

Customer:
- Run Load Point tool (SymHelp)
- Submit sample to Symantec
- Submit sample to Threat Expert
- Full system scan with Rapid Release
- Call Symantec Support

Symantec:
- Why is a threat suspected?
- Determine priority/impact of incident
- Request submission if one has not been made
- Review Load Point Logs
- Create Plan of Action

ID Threat -> ID Infected Computers -> Quarantine Network -> Clean Infection -> Post Op

Help! I Think I’ve Been Hit with Malware
Steps for Troubleshooting a Suspected Threat

**ID Threat**
- Why is a threat suspected?
- Determine priority/impact of incident
- Review Load Point Logs
- Prioritize submission(s)
- Notate threat name if possible
- Create Plan of Action

**ID Infected Computers**
- Locate suspect machine(s)
- Run Load Point tool (SymHelp)
- Submit sample to Symantec
- Submit sample to Threat Expert
- Full system scan with Rapid Release
- Call Symantec Support

**Quarantine Network**

**Clean Infection**

**Post Op**

Help! I Think I’ve Been Hit with Malware
Steps for Troubleshooting a Known Threat

1. Why is a threat suspected?
   - Determine priority/impact of incident
   - Request submission if one has not been made
   - Review Load Point Logs
   - Create Plan of Action

2. Customer
   - Run Load Point tool (SymHelp)
   - Submit sample to Symantec
   - Submit sample to Threat Expert
   - Full system scan with Rapid Release
   - Call Symantec Support

3. Symantec

Help! I Think I’ve Been Hit with Malware
Steps for Troubleshooting a Threat

ID Threat

ID Infected Computers

Quarantine Network

Clean Infection

Post Op

Customer

Download/install correct definitions
Deploy definitions to network
Run scans
Review Threat Expert data
Review perimeter firewall logs

Symantec

Review SEP configuration
Review threat report/info
Review threat potential
Work with customer on a POA for containment

Help! I Think I’ve Been Hit with Malware
Steps for Troubleshooting a Threat

ID Threat

ID Infected Computers

Quarantine Network

Clean Infection

Post Op

Customer

If possible, physically remove infected systems
If network aware, enable Network AP
Create a VLAN/restricted network for infected systems
Create SEPM client group for infected systems
Locate unprotected machines and install AV

Symantec

Determine “what’s important right now”
Review threat behavior
Recommendations on what activity to block
Provide updates of detection/analysis info

Help! I Think I’ve Been Hit with Malware
**Steps for Troubleshooting a Threat**

1. **ID Threat**
   - Assess cost effectiveness to “start from scratch”
   - Assess if a system scan removes threat
   - Assess system changes
   - Be prepared to reboot infected systems
   - Assess when it is safe to claim a system is clean
   - Determine best clean-up method

2. **ID Infected Computers**
   - Help determine best clean-up method
   - Help assessments if possible
   - Monitor for term “re-infected” and research claims
   - Continue to ask questions and review logs/progress
   - Keep focus on the threat(s) and remediation

3. **Quarantine Network**
4. **Clean Infection**
5. **Post Op**

---

**Customer**

**Symantec**

---

*Help! I Think I’ve Been Hit with Malware*
Steps for Troubleshooting a Threat

**Steps:**

1. **ID Threat**
2. **ID Infected Computers**
3. **Quarantine Network**
4. **Clean Infection**
5. **Post Op**

**Customer**
- Locate entry point
- Assess how to close entry point and close if possible
- Review event and teams involved

**Symantec**
- Prepare for non-technical questions
- Review case timeline