Endpoint Intrusion Prevention

How Cisco IT Uses Intrusion Prevention to Protect User Endpoint Devices

A Cisco on Cisco Case Study: Inside Cisco IT

© 2007 Cisco Systems, Inc. All rights reserved.

Overview

- Challenge:

  Protect individual assets like PCs and handhelds at the desktop level, to cut costs of virus remediation and associated loss of productivity

- Solution:

  Deploy Cisco Security Agent to 37,000 Windows desktops

- Results:

  Met challenge, and reaped rewards in April 2004, when 99.86% of protected computers escaped infection from the bagle.aa virus

- Next Steps:

  Make policy stricter and deploy on internal and customer-facing Windows 2000 servers

© 2007 Cisco Systems, Inc. All rights reserved. Cisco Public

Challenge: Protect assets, reduce costs

- Reduce time and expense of remediation of growing numbers of viruses and worms

  Cost of virus remediation and associated loss of productivity was $28 billion in 2003 and will rise to $75 billion in 2007 (source: Radicati Group, 2003)

- Protect individual assets like PCs and handhelds at the desktop level

  Desktop not specifically addressed by Cisco PIX® Firewalls, Cisco NIDS, and anti-virus software

- Protect employee productivity by ensuring the solution doesn't interfere with normal work habits

© 2007 Cisco Systems, Inc. All rights reserved. Cisco Public

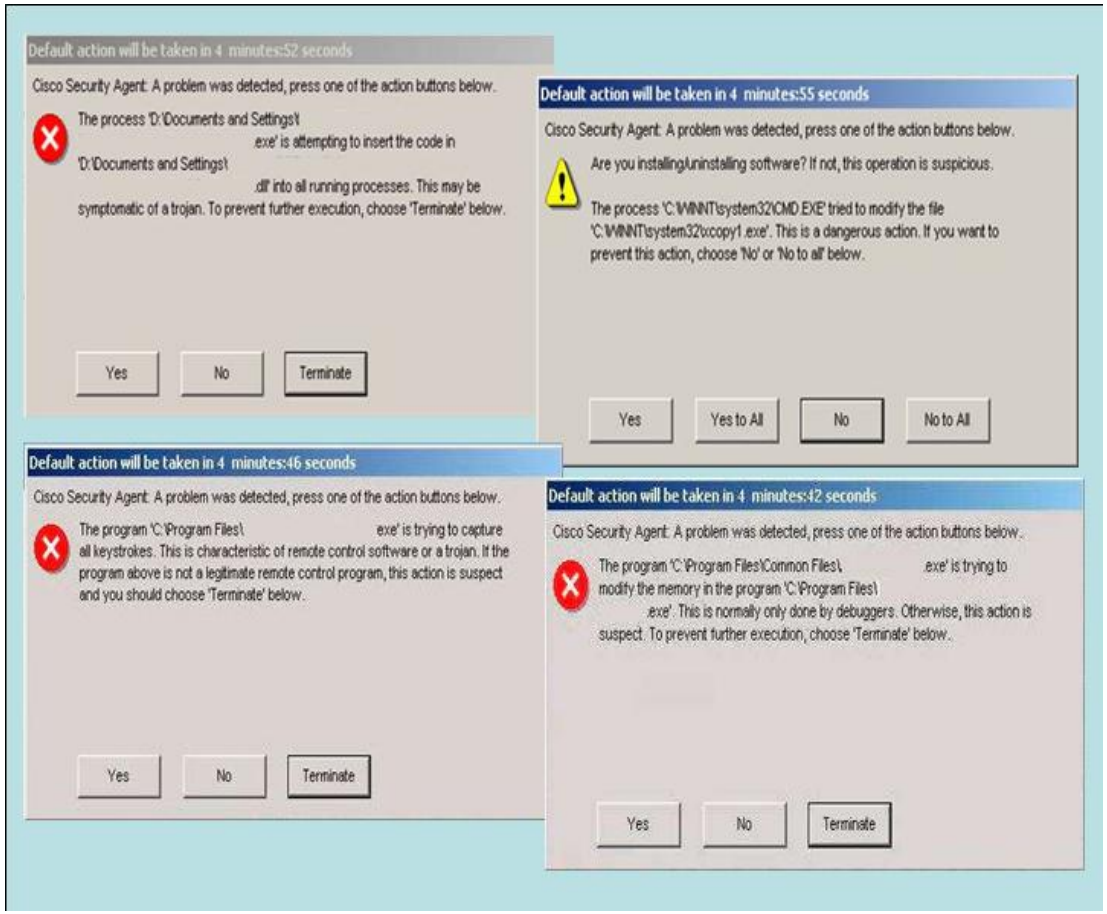
Solution: Deploying behavior based defense

- Deploy Cisco Security Agent on employee desktops

  "Behavior-based" rather than "signature-based" protection

- Develop application behavior policies

  When application behavior deviates from the norm, allow it, deny it, or query the user



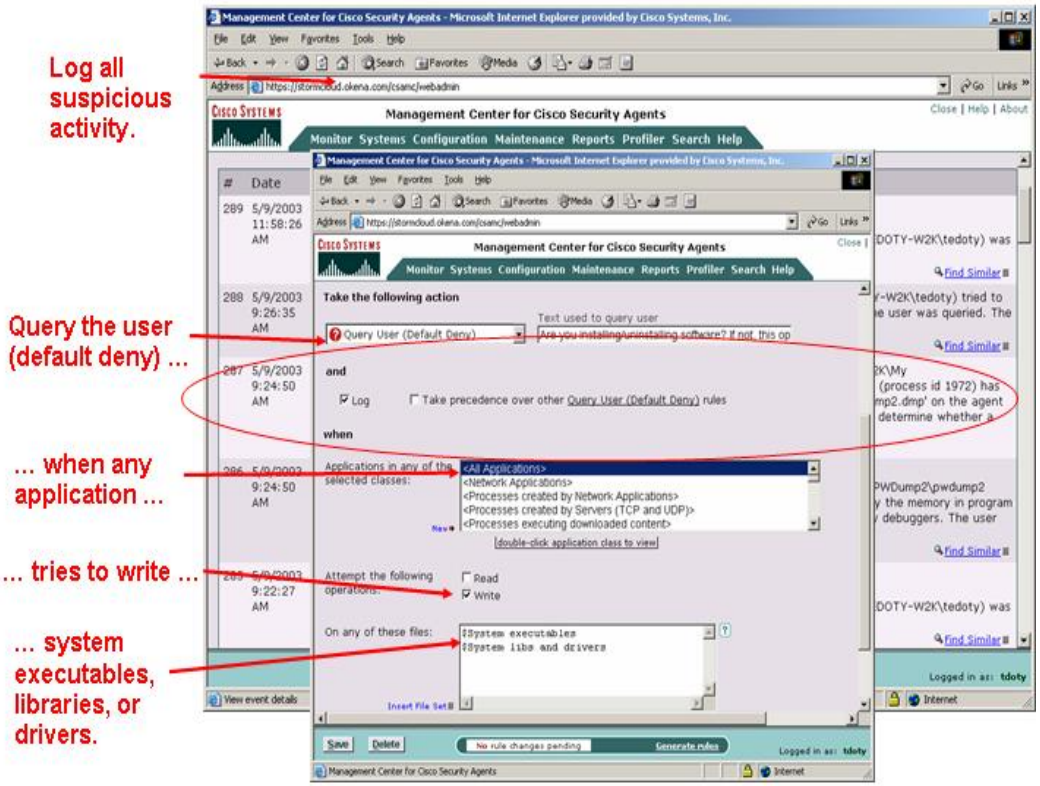
© 2007 Cisco Systems, Inc. All rights reserved. Cisco Public

Solution: Define Policies, Deploy Globally

- Fine-tune policies during a 500-user pilot

  Strike a balance between protection and employee convenience; minimize number of queries about allowing application behavior

- Push software to all employees globally
- Educate users on desktop security and effective use of Cisco Security Agent



© 2007 Cisco Systems, Inc. All rights reserved. Cisco Public

Results: Increased Security, Reduced Cost

- Slashed costs associated with virus and worm remediation
- Increased employee productivity by slowing virus progress
  - Even with very liberal policies chosen for roll-out
- Detected previously-infected systems

© 2007 Cisco Systems, Inc. All rights reserved. Cisco Public

Results: Thwarting the bagle.aa Virus

- Virus struck in April 2004
- No time to patch or update .DAT files
- Of 38,370 desktops running Cisco Security Agent, over 600 could have been compromised – 620 users opened the infected file
- Cisco Security Agent kept all but 54 people from releasing the virus, by warning them of suspicious activity (rewriting the registry)

  Infected users had clicked “Yes” when warned that a suspicious application was trying to access e-mail resources

© 2007 Cisco Systems, Inc. All rights reserved. Cisco Public

Results: Thwarting the bagle.aa Virus (Contd.)

- This 90% reduction made cleanup much easier and less costly
  - Also resulted in steps to improve policy to reduce user ability to open this kind of file

© 2007 Cisco Systems, Inc. All rights reserved. Cisco Public

Next Steps: Summary

- Make policy stricter
- Use network admissions control (NAC) to restrict network access to employees who have installed Cisco Security Agent
- Install Cisco Security Agent on internal and customer-facing Windows 2000 servers
  - Including Cisco Call Manager and Cisco Unity software
- Assemble comprehensive view of network general health by combining information from Cisco Security Agent and Cisco Network Intrusion Detection Systems (NIDS) and sending to Cisco Works VMS/SecMon or Cisco Security Information Management System

© 2007 Cisco Systems, Inc. All rights reserved. Cisco Public

Lessons Learned: Summary

- Take your time with policy testing
- Conduct the pilot with a broad variety of people and applications
- Educate users, who sometimes must decide whether to allow or deny application behaviors

© 2007 Cisco Systems, Inc. All rights reserved. Cisco Public

To read the entire case study, or for additional Cisco IT case studies on a variety of business solutions, visit Cisco on Cisco: Inside Cisco IT
www.cisco.com/go/ciscoit

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Asia Pacific Headquarters
Cisco Systems, Inc.
168 Robinson Road
#28-01 Capital Tower
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

Europe Headquarters
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: +31 0 800 020 0791
Fax: +31 0 20 357 1100

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **www.cisco.com/go/offices.**

©2007 Cisco Systems, Inc. All rights reserved. CCVP, the Cisco logo, and the Cisco Square Bridge logo are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networking Academy, Network Registrar, Packet, PIX, ProConnect, RateMUX, ScriptShare, SlideCast, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0704R)