

Welcome

SF Bay Area InfraGard Chapter
Summer Quarterly Meeting
August 19, 2010

“PLAN FOR THE INEVITABLE”

Hosted by Microsoft



Agenda

- 8:00-9:00 Registration
- 9:00-9:15 Welcome, chapter business
- 9:15-10:15 Panel I: "Plan for the Inevitable: Assume You've Been Compromised"
- 10:15-10:30 Break
- 10:30-11:30 Panel II: "Plan for the Inevitable: Respond to the Breach"
- 11:30-11:45 Closing remarks
- 11:45 Adjourn



Next Meeting

- Thursday, November 18, 2010
- Venue: South Bay (looking for sites)
- Board elections to be held
 - If you're interested in becoming a board member, please contact us
 - BOD@sfbay-infragard.org
- See www.sfbay-infragard.org for info



SecureWorld Expo



- Santa Clara Convention Center
- Discounts for InfraGard members
- InfraGard breakfast Sept. 23
- See <http://www.sfbay-infragard.org/MEETINGS.htm> for more



Assume You've Been Compromised

PLAN FOR THE INEVITABLE



Why Assume You're Compromised?

Security > Endpoint Protection (AntiVirus) Forum

Tech Blog

Personal technology

Intel says it had “sophisticated” hacking attempt

February 24, 2010 1:02am by Joseph Menn | Share

In what may be the first of many such formal disclosures, Intel included an unusual admission in its annual 10k filing to the SEC on Tuesday: It had been subjected to a “sophisticated incident” of computer hacking that might have been an act of “industrial or other espionage”.

...

What may be worse is what the company doesn't know: “We seek to detect and investigate these security incidents and to prevent their recurrence, but in some cases we might be unaware of an incident or its magnitude and effects”, the filing said.

identify the perpetrator of an electronic crime, 32% were committed by insiders.

Sources: <http://www.darkreading.com/security/antivirus/showArticle.jhtml?articleID=220000718>, <http://www.symantec.com/connect/forums/endpoint-consistently-allows-fake-av-malware>, <http://www.sfoxaminer.com/local/Network-engineer-Terry-Childs-found-guilty-of-network-tampering-92257309.html>, <http://www.sei.cmu.edu/library/abstracts/news-at-sei/securitymatters200702.cfm>, <http://blogs.ft.com/techblog/2010/02/intel-says-it-had-sophisticated-hacking-attempt/>.



Who are the Actors?

- External Threats
 - Botherders
 - Criminal organizations
 - Foreign actors/Competitors
 - “Businessmen”
- Internal Threats
 - Disgruntled workers
 - Profit seekers/fraudsters
 - Short-timers



What Motivates the Actors?

- They all want what you've got
- External actors
 - Use your systems
 - Steal your data/information
- Internal actors
 - Seek revenge
 - Seek profit
 - Seek another job



Links

- Insider Threat
 - http://www.cert.org/insider_threat/
 - <http://www.sei.cmu.edu/newsitems/Mitigating-Insider-Threats.cfm>
- Zeus overview
 - <http://www.fortiguard.com/analysis/zeusanalysis.html>



Our Panel

- John Landwehr
- Jeff Fenton
- Neal McCarthy
- Ron LaPedis



Don't rely on the



John's Recommendations

- 1 Information Classification System
(what to protect)
- 2 Content-centric encryption
(how to protect it)
- 3 Education and automation
(make sure it's happening properly)



Our Panel

- John Landwehr
- Jeff Fenton
- Neal McCarthy
- Ron LaPedis



Break



Respond to the Breach

PLAN FOR THE INEVITABLE



Our Panel

- Jeff Klaben
- Jeff Fenton
- Ron LaPedis
- Neal McCarthy
- Will Ng, Supervisory Special Agent, FBI



Thanks to our panels, the FBI,
and our hosts at Microsoft.

