

Technical Assistance against Cybercrime from a vendors perspective



Greg Day
Director of Security strategy, EMEA

March 26, 2010



Goal – Share intelligence and drive knowledge transfer!

- Information on Global Threat Intelligence
 - What's real and relevant – helping define the scope of the problem
- Training and Education
- Support in the Governments/local agencies
 - Law enforcement agencies assistance - PCeU
 - EU parliament & national governments
- Cybercrime Response Unit

Collaborative Global Intelligence



Physical World



Intelligence Agents

Deploy agents: Officers around the globe (*MI5, MI6, FBI, CIA, Interpol.*)
Global intelligence system: Share intelligence information. (e.g. criminal history, global finger printing system)

Results
Effective - Accurate detection of offenders
Pro-active - Stop them from coming in the country



Cyber World



Intelligence Probes

Deploy security probes: Around the globe (*firewall, email gateways, web gateways*)
Global intelligence system: Share cyber communication info. (e.g.: hackers, spammers, phishers)

Results
Effective - Accurate detection of bad IPs, domains
Pro-active - Deny connection to intruders to your enterprise



Collaborative Intelligence



McAfee
McAfee Avert Workflow (1.2.484)

Dashboard Malware Reports Configuration

Analyst Researcher Downloads Available

Sample ID	Filename	Owner	Occurrences	Status	Assignor	Detections
4902638	WebShare	isa@hphd.com	1	1	0	16 Oct 21:38:43 Solved handled by automation
Samples						
4902638	statement_jan-04.doc.exe	isa@hphd.com	1-15-15	closed	isa@hphd.com	A1 012 -...-M-...- RA 3 MIA SAC spy-agent_bv DET spy-agent_bv
4902646	Non-Serialized FW: [SPAM-McAfee]account data	isa@hphd.com	1	1	0	16 Oct 18:38:11 Solved handled by automation
4902602	WebShare	isa@hphd.com	1	1	0	16 Oct 18:09:06 Solved handled by automation
4902596	PO QM Statement_MH-OCT.doc.exe	isa@hphd.com	1	1	0	16 Oct 17:55:33 Solved handled by automation
4902511	PO QM sample	isa@hphd.com	1	1	0	16 Oct 17:04:08 Solved handled by automation

Industry Connections Security Group



Initial Goal: How do we improve the efficiency of the collection & processing of the millions of malware file samples we all handle each and every month ?

- ISCG was started by AVG, McAfee, Microsoft, Sophos, Symantec and Trend Micro, and is open to others...
- Facilitate the pooling of industry experience and resources
 - Focused on development of a XML based metadata sharing standard to augment existing malware sample sharing
- A forum for development of proposed standards and best practices related to computer security
 - IEEE is a recognized brand known to deliver standards
- Goes beyond Malware Issues !

Google for: "IEEE ICSG"

Email: joinicsg@ieee.org

Education – Hands-on malware training



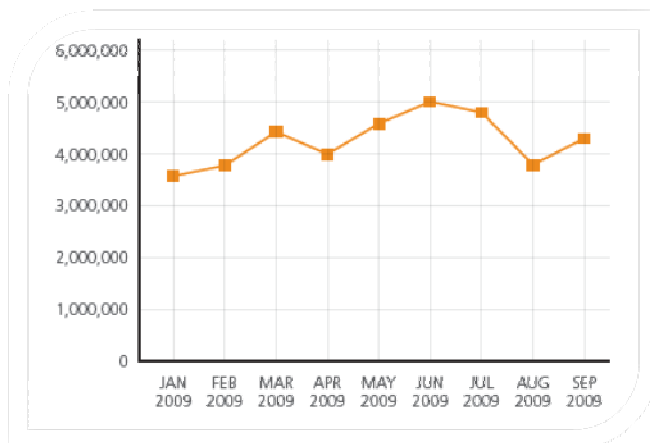
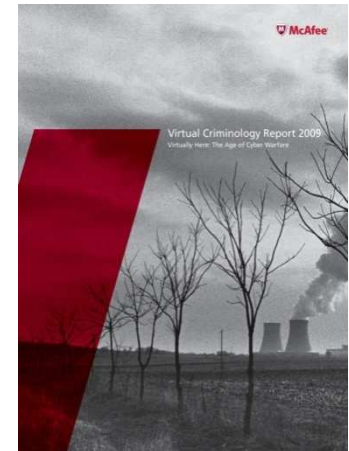
On 7-8 December 2009

- the SPMU in cooperation with McAfee, the Serbian Ministry of Interior and the OSCE Mission in Serbia organized a two-day regional cybercrime investigator training course in Belgrade, Serbia.
- Experts from Serbia, Montenegro, Croatia, Bosnia and the Republic of Srpska participated in the event.
- The training was provided at no cost by McAfee engineers and focused on Malware, Botnets and denial of service attacks.
- A member of the ATU participated in the Belgrade training as an observer to identify aspects of the McAfee training that would be applicable for future anti terrorism activities.

Working with the government to tackle cyber crime



- UK Police eCrime Unit (PCeU)
 - Direct line to McAfee Labs to support field work
 - Planned hands on Malware training
- EU parliament, OSCE & UK government briefings
 - Sharing research report on scope of the problem
 - CIP report briefings
 - 54% experience large scale denial of service attacks
 - Cost of downtime as a result of a cyber-attack on critical infrastructure ave. **\$6 million per day**
 - Trending reports and annual Cybercrime reports



- **40M+ Botnet'ed PC's in 2009**
- **That's over 148,000 per day**

Global Initiative to Fight Cybercrime



Advisory Council

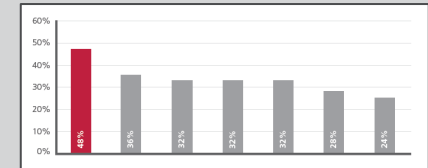
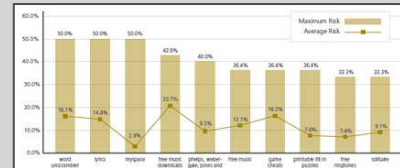


Grants

- Influence adoption of **cybercrime laws**, CoE Cybercrime Convention
- Increase **training for prosecutors**, others involved in the fight



Research and Reports



Cybercrime Response Unit

- Online 911 response
- “Street Smarts” Education

Cybercrime Response Unit

Are you a victim of cybercrime? We can help...

[Assess Your Risks](#)

H-Commerce Documentary

EPISODE GUIDE • NOW PLAYING TRAILER • UNEXPECTED BEGINNINGS

SIGN UP FOR UPDATES

1. HCommerce History

2. The Trap is Set

3. Caught in the Web

4. Help is on the Way

5. Ending the Scam

6. Moving Forward



Greg Day
Director of Security Strategy, EMEA
Greg_Day@McAfee.com