



Microsoft
Your potential. Our passion.

Cooperation against cybercrime – an effective response to emerging challenges

Ministry of Justice of Georgia
2 March 2010
Uwe Rasmussen, Microsoft Corporation

Microsoft Internet Safety Team Introduction

- Global team of investigators and lawyers defending against Internet crime and abuse
- Specific missions:
 - Protect children from technology facilitated crimes
 - Advance safety and integrity in the online advertising marketplace
 - Ensure security and safety in cloud computing and emerging technologies

Overview

- Clear legislation on when the data should be provided to law enforcement, including data retention
- Cooperation with law enforcement should be facilitated through meetings and exchanges
- Participation in an international framework to facilitate exchange of evidence



Legally binding requests

- Legislation should specify ISP obligations on data retention, legal process for disclosing customer information
- The definition of ISP or ESP should be unambiguous in the legislation

Facilitating the exchanges

- Appoint people single points of contact for the law enforcement and ESP exchanges
- Prioritize the requests so ESPs can allocate the adequate amount of resources
- Regular meetings to identify and resolve problems

International requests

- International instruments exists to facilitate police cooperation
 - Letters rogatory
 - Mutual Legal Assistance Treaties (MLAT)
 - G8 Contact points
 - Convention on cybercrime

Emergency Requests

- Microsoft Online Services will respond to emergency requests outside of normal business hours.
- Send a letter on official agency letterhead- signed and dated, including:
 - A summary of facts, in English, describing the emergency
 - A statement that there is an emergency "involving danger of death or serious physical injury requiring disclosure of the information without delay."
 - The full name of the requested account (e.g., "bob_compliance@hotmail.com") and what data is requested (e.g., "Subscriber Information and IP History").

13

- 13


Cooperation

On the technology side

[illegible]

Digital Crimes Consortium

12-16 October 2009



Digital Crimes Consortium 2009
Hosted by Microsoft

Tuesday, October 13, 2009

TIME	TOPIC	PRESENTER
11:00 – 13:00	Registration for DCC 2009	
13:00 – 13:10	Lunch	
13:10 – 13:15	Introduction & Welcome	
13:15 – 13:20	Keynote	
13:30 – 14:30	Disruption & Enforcement – How to Win the Battle Against Cybercrime: Examining what approaches have and have not worked well and what changes are needed within the global security and law enforcement communities to effectively tackle the growing issue of cybercrime.	To be confirmed
14:30 – 15:00	Break	
15:00 – 16:00	Controlling West African Advanced Fee Fraud (AFF) Proliferation: The significant threat to citizens, business interests	Paul Zasada CEO, Gov.com, Inc.

16

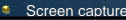
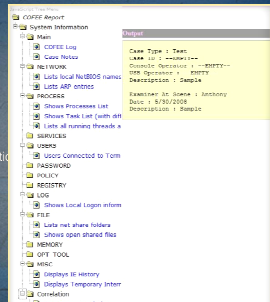
16

COFFEE Computer Forensics Tool

- Computer Online Forensic Evidence Extractor is a tool to obtain evidence from a computer in a uniform, quick, and transparent way
- Design as a script and command line based live forensics tools that can be used by forensics investigator with zero knowledge
- Conduct live evidence extraction before the computer is powered down
- Runs from and stores the volatile evidence on a USB storage key

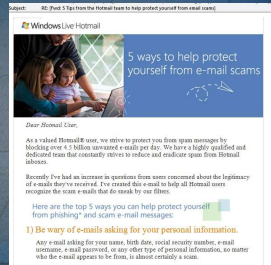
Volatile information

- Date, time of the examination
- Volatile memory
 - Memory Dump from Physical memory
 - SWAP drive
- Network connection
 - Open ports UDP, TCP
 - NetBIOS, neighboring network connections
- User Account
 - Users currently logged on
- Processes
 - Running processes
 - Running services
 - Scheduled Jobs
- Files
 - Open files
- Screen capture



Educating Users

- Microsoft regularly emails online fraud prevention tips to its customers
- Detailed online fraud prevention information is provided on Microsoft's website
- User education and awareness is enhanced through cooperation with public authorities, media, and industry partners



19

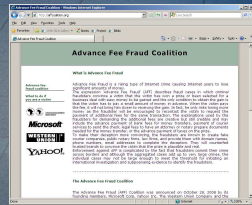
Assisting victims of account hijacking

- Microsoft has a specific program to assist victims of hijacked accounts
- The user friendliness of Windows Live online services support is constantly being improved based on user feedback



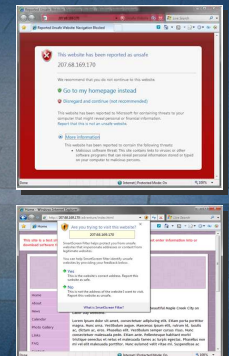
Industry Initiatives to support victims

- The Advance Fee Fraud Coalition is an industry initiative to fight Internet fraud through
 - Public awareness
 - Mitigation
 - Enforcement
- This industry initiative demonstrates an interest and need by the private sector to work together to protect victims for crimes committed across borders



Technical measures – web browsing

- SmartScreen filter
 - Prevents users from going to known phishing and malware websites
 - Warns users against websites exhibiting fraud characteristics
- Domain highlighting
 - Informs users to make it more difficult to spoof domains



22