Legal Issues:

In prosecuting cyber crime

Uwe Manuel Rasmussen
Legal counsel, Microsoft EMEA
Digital Crimes Unit

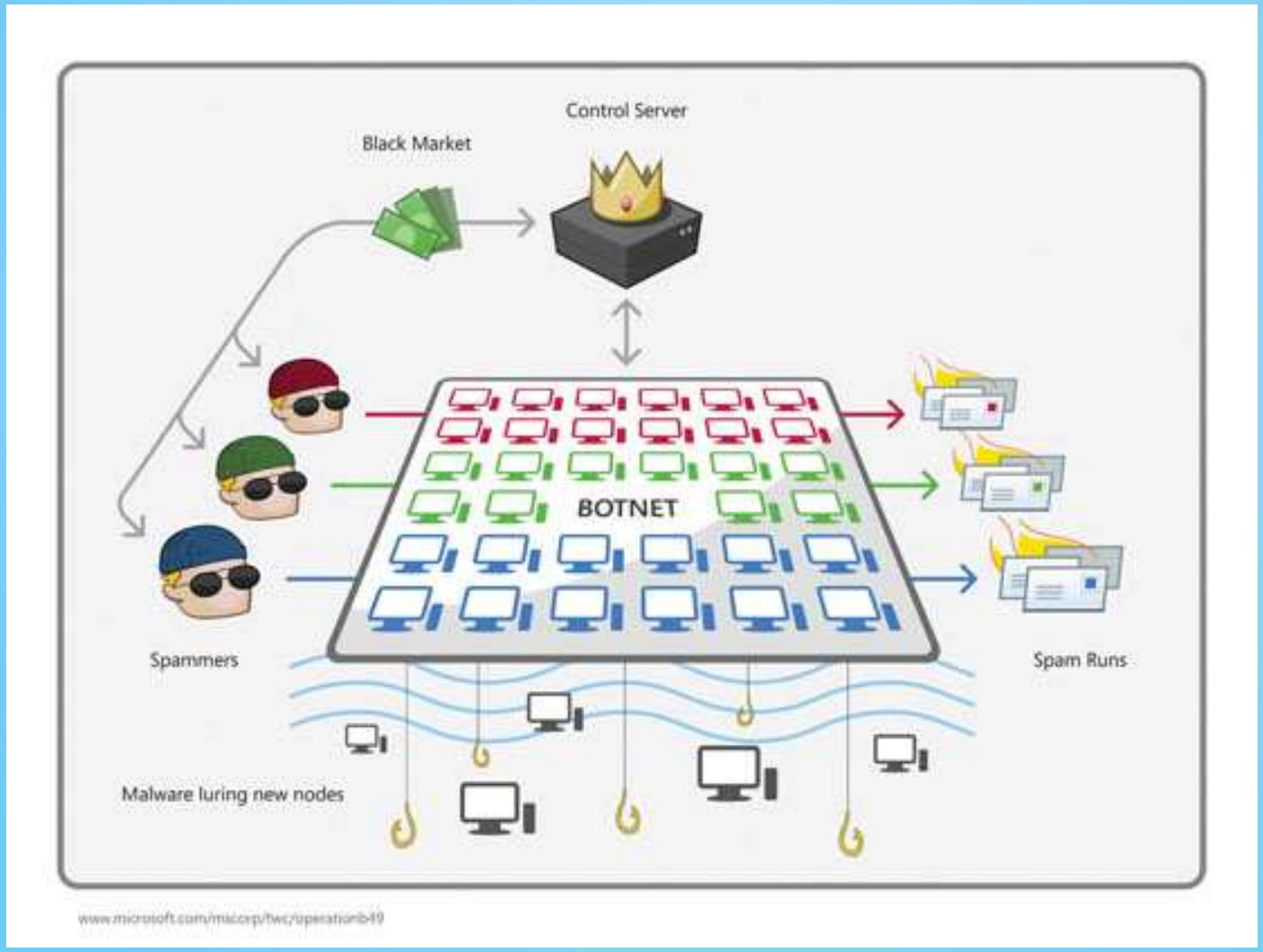
Microsoft Digital Crimes Unit

A worldwide team of lawyers, investigators, technical analysts and other specialists whose mission is **to make the Internet safer and more secure** through strong enforcement, global partnerships, policy and technology solutions that help:

- Promote a secure Internet
- Defend against fraud and other threats to online safety
- Protect children from technology-facilitated crimes
- Champion a healthy Internet marketplace for advertisers and businesses

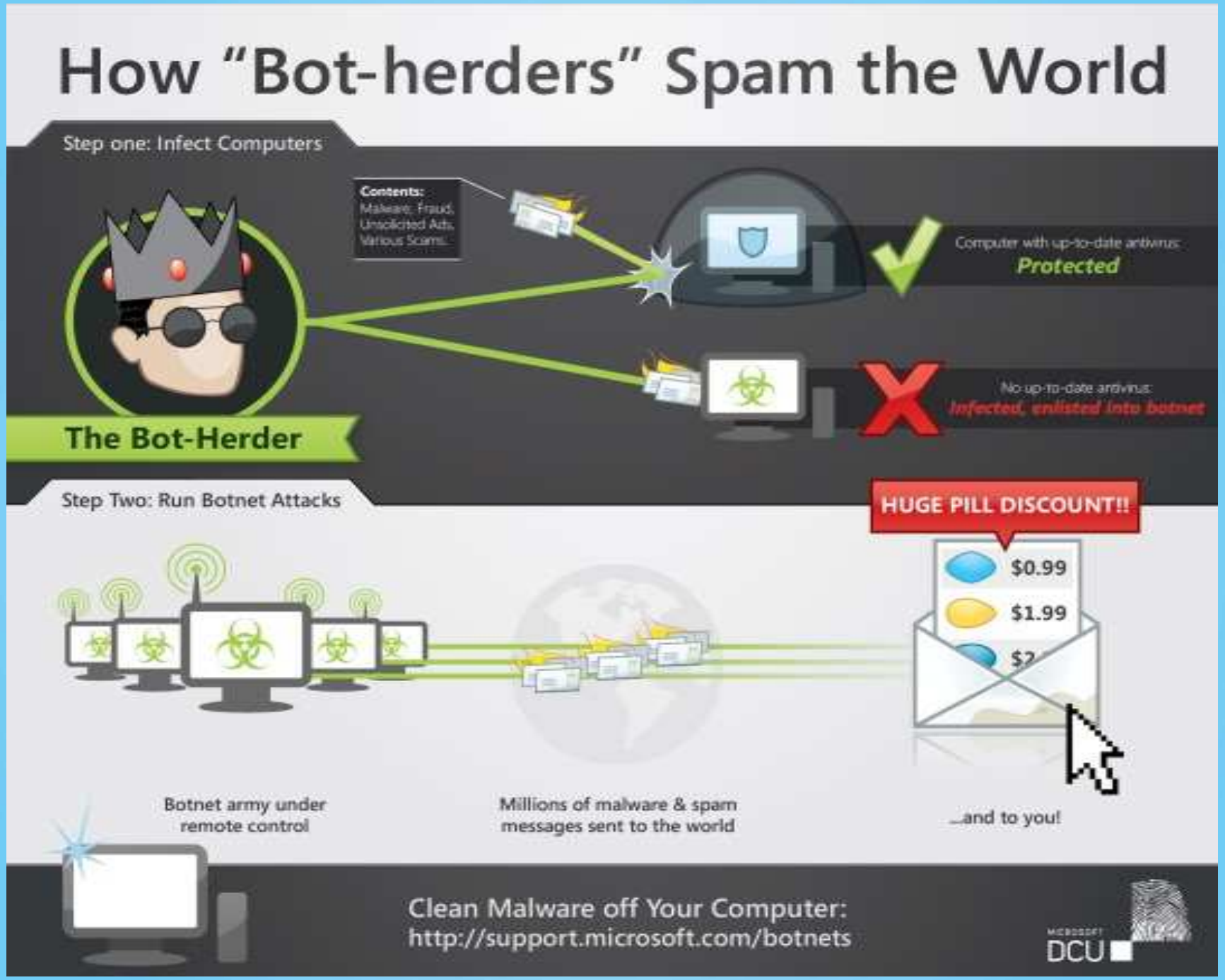
MICROSOFT DCU

Going after the criminals' own infrastructure: "Botnets"



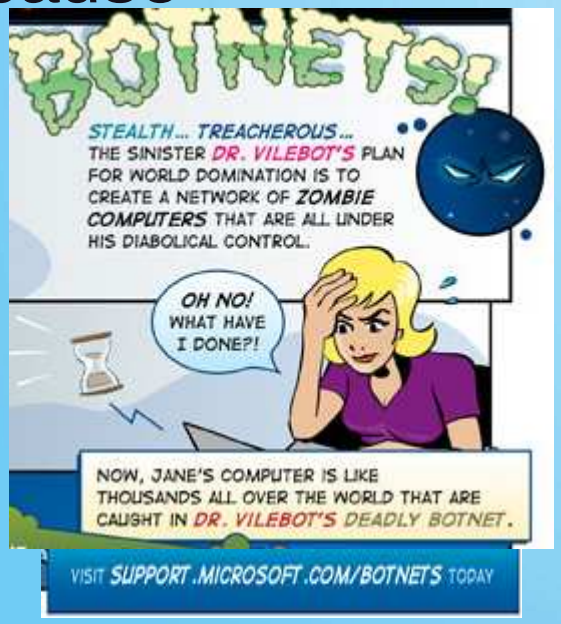
MICROSOFT DCU

How "Bot-herders" Spam the World



Case Study: Project MARS

Project MARS (Microsoft Active Response for Security) is a joint effort between Microsoft's Digital Crimes Unit, Microsoft Malware Protection Center and the Trustworthy Computing team to proactively combat botnets and help undo the damage they cause



- Operation b49: The Waledac botnet takedown - *February 2010*
- Operation b107: The Rustock botnet takedown - *March 2011*

Trustworthy Computing

Malware Protection Center
Threat Research and Response

MICROSOFT DIGITAL CRIMES UNIT

Operation b49: Waledac takedown

MICROSOFT DCU

Operation b49: Waledac takedown

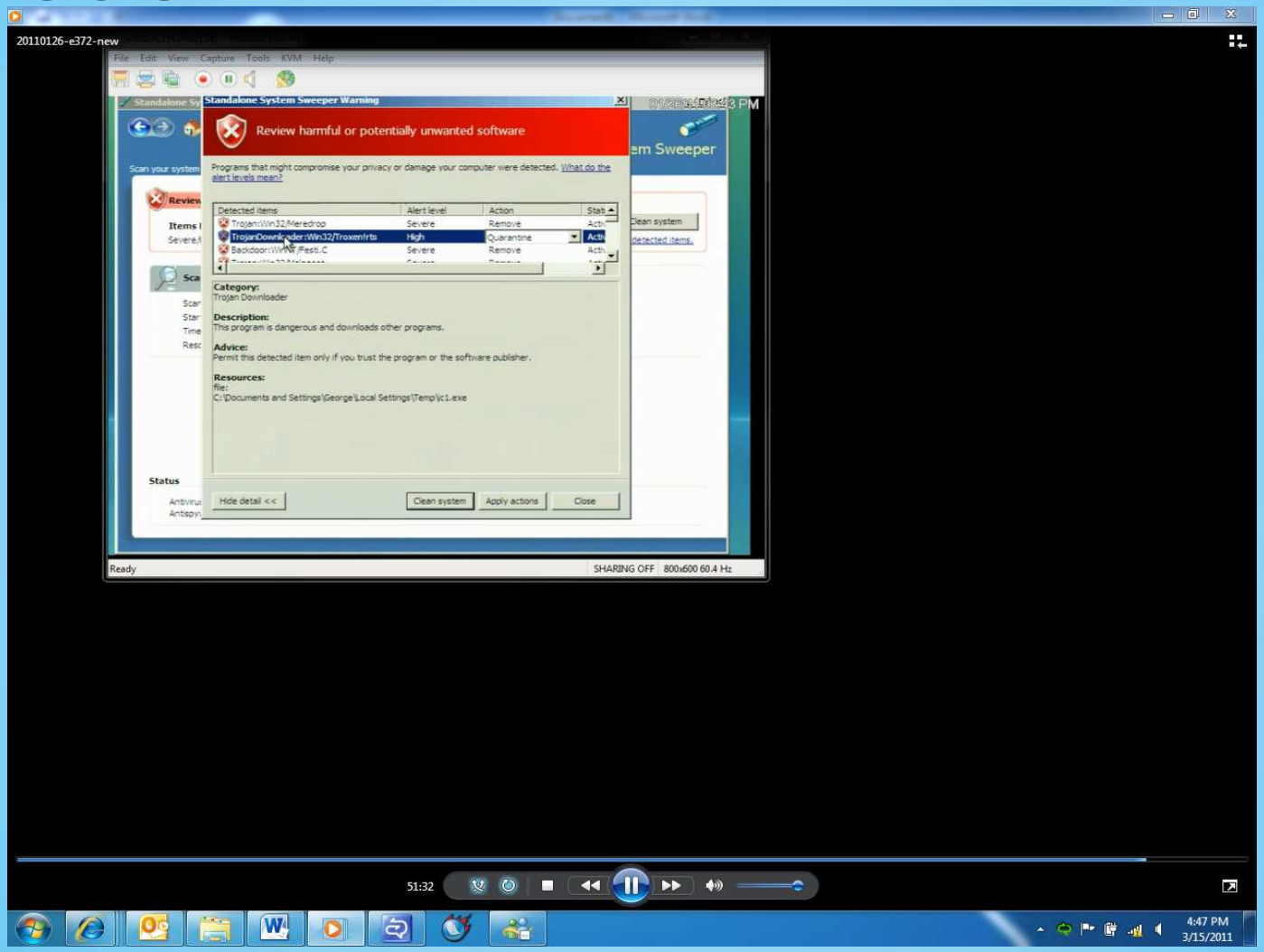
- In February 2010, Microsoft got a court order to sever 277 domains believed to be part of the Waledac botnet
- Operation b49 effectively severed ~70,000-90,000 computers from the botnet
- In October 2010, the court permanently awarded the 277 domains to Microsoft so they are never used for cybercrime again
- Due to cleanup efforts with ISPs/CERTs worldwide and natural decay of the inactive botnet, we estimate there are ~22,000 remaining infected IPs (as of March 2011)

MICROSOFT DCU

Operation b107: Rustock takedown

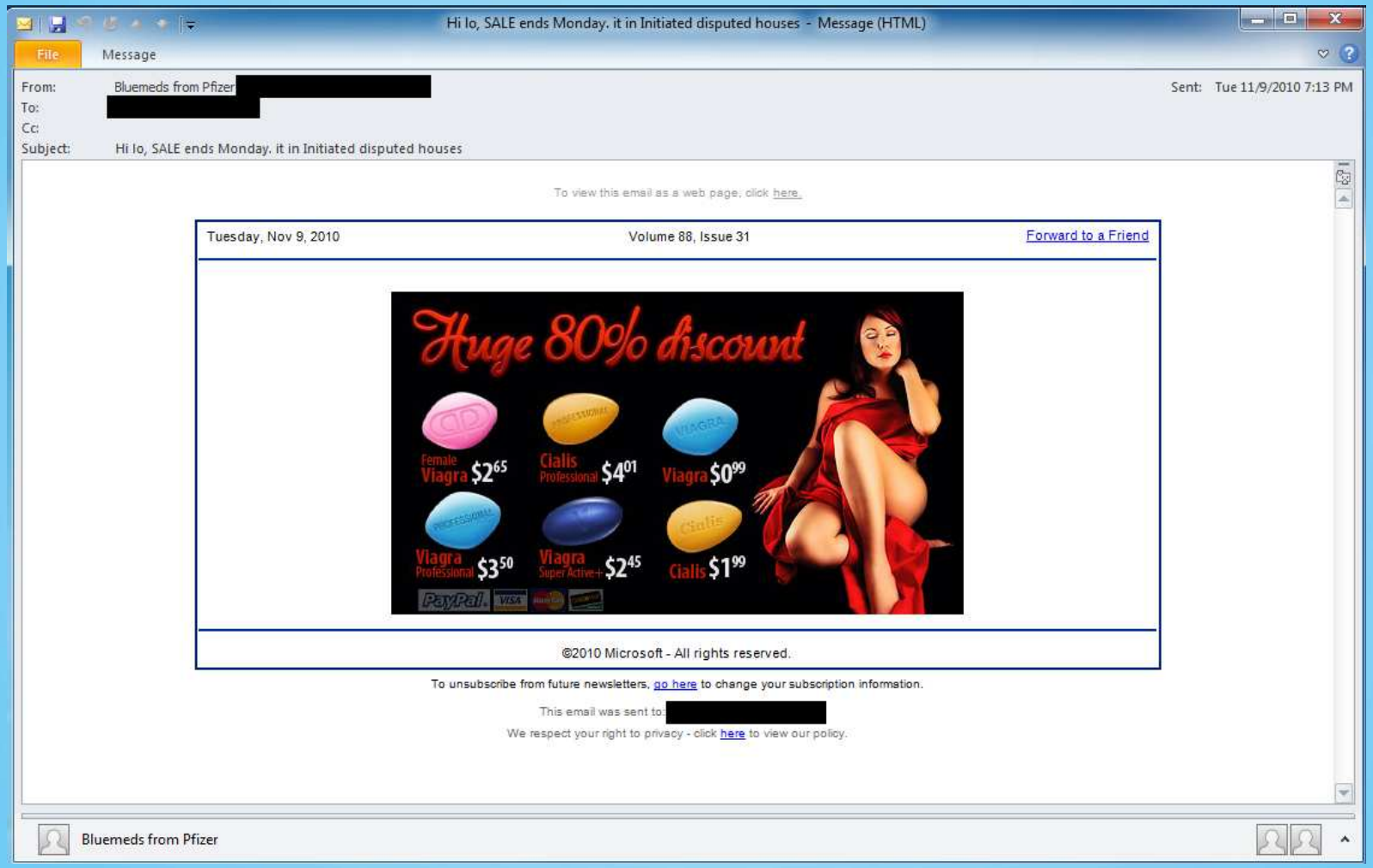
MICROSOFT DCU

Operation b107: Rustock takedown



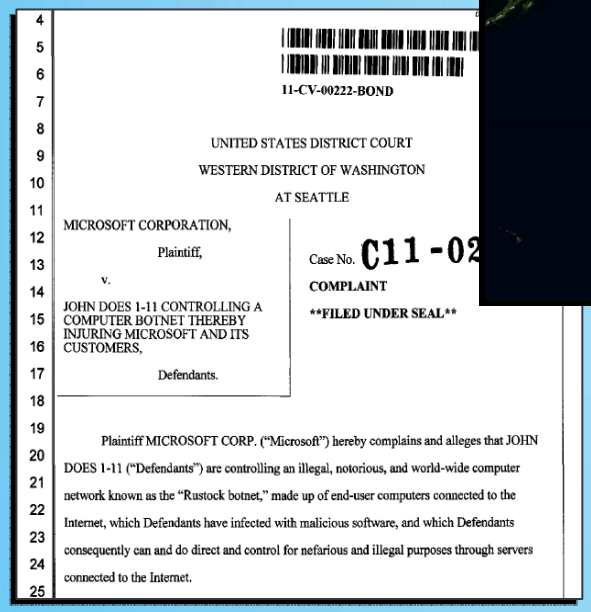
MICROSOFT DCU

Operation b107: Rustock takedown



MICROSOFT DCU

Operation b107: Rustock takedown



11-CV-00222-BOND

UNITED STATES DISTRICT COURT

WESTERN DISTRICT OF WASHINGTON

AT SEATTLE

MICROSOFT CORPORATION,

Plaintiff,

v.

JOHN DOES 1-11 CONTROLLING A COMPUTER BOTNET THEREBY INJURING MICROSOFT AND ITS CUSTOMERS,

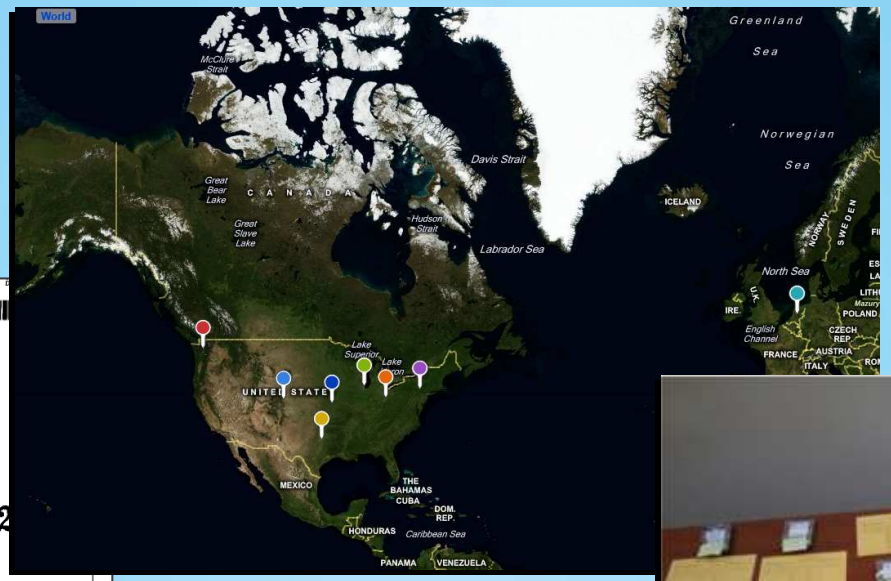
Defendants.

Case No. C11-02

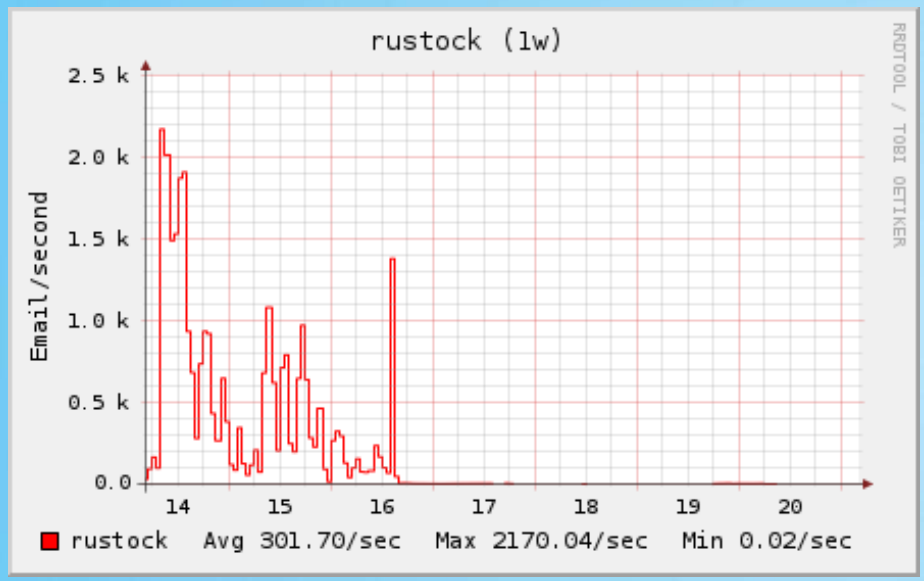
COMPLAINT

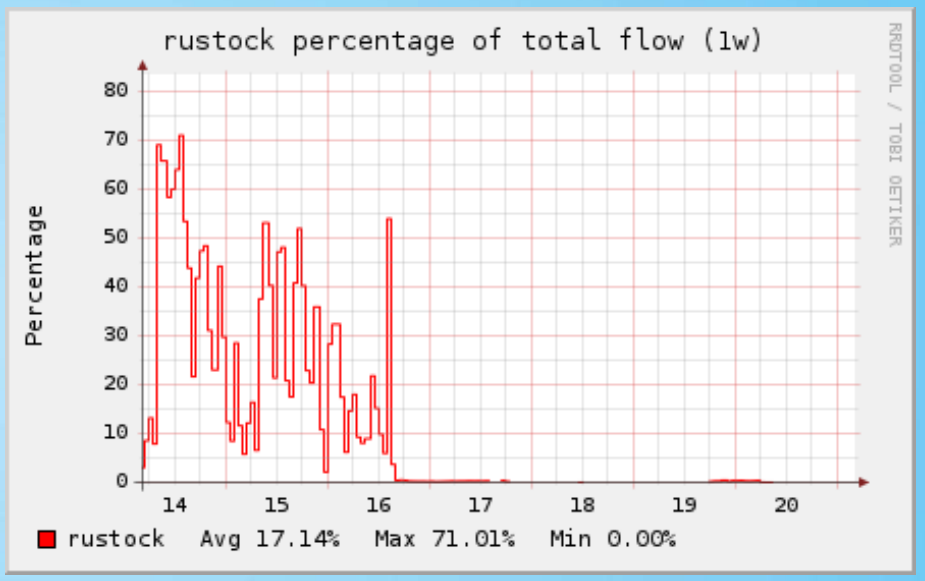
FILED UNDER SEAL

Plaintiff MICROSOFT CORP. ("Microsoft") hereby complains and alleges that JOHN DOES 1-11 ("Defendants") are controlling an illegal, notorious, and world-wide computer network known as the "Rustock botnet," made up of end-user computers connected to the Internet, which Defendants have infected with malicious software, and which Defendants consequently can and do direct and control for nefarious and illegal purposes through servers connected to the Internet.



Operation b107: Impact on Spam





http://cbl.abuseat.org/rustock.html

MICROSOFT DCU

Legal Issues

- **Cross jurisdictional crime**
  victims, perpetrators, resources in different places
- **Technical subject matter requiring training**
- **Public right of action**
- **Balancing freedom and security through the protection of personal information**
  - Person identifying information
  - Secrecy of correspondence
  - Data ownership and sovereignty

Follow us on

Facebook and Twitter!

facebook.com/MicrosoftDCU

twitter.com/MicrosoftDCU