

Борьба Корпорации Майкрософт с киберпреступностью: Ботнеты

Александр Страх
Юрист
Майкрософт

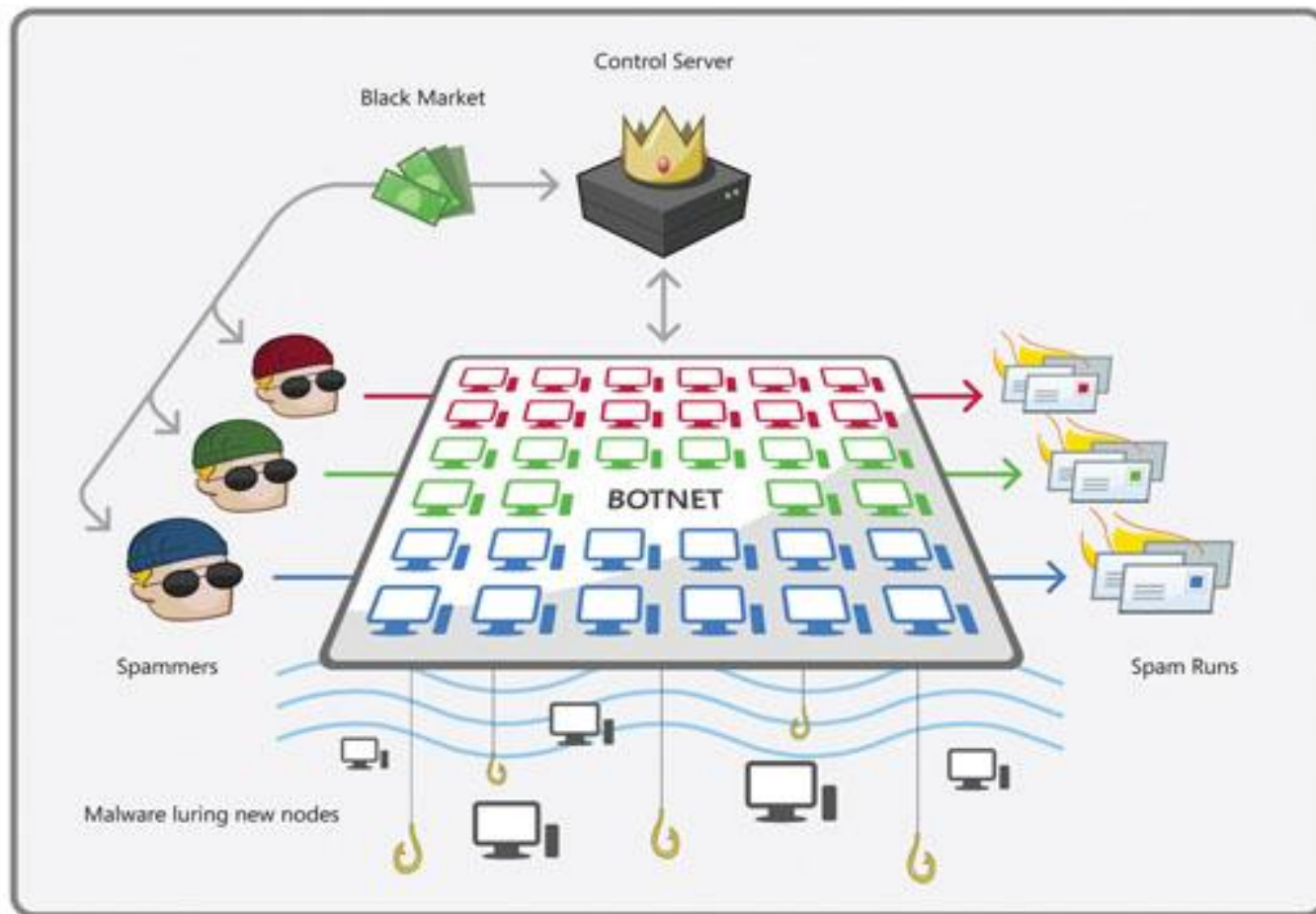


Microsoft Digital Crimes Unit

Группа Майкрософт по борьбе с киберпреступлениями (Microsoft Digital Crimes Unit) состоит из юридических и технических специалистов по всему миру, осуществляющих защиту пользователей Microsoft от мошенничеств и других незаконных действий в сети Интернет, а также обеспечивающих юридическую и техническую поддержку расследований. Основные задачи группы:

- Обеспечивать безопасность интернет
- Противодействовать мошенничествам и другим незаконным действиям в онлайн среде
- Защита детей от киберпреступности
- Создание здорового интернет рынка для индустрии программного обеспечения и для бизнеса в целом

Ботнеты - Механизм работы



www.microsoft.com/mscorp/twc/operationb49

Схема создания ботнета и использования ее спамером

Step one: Infect Computers



The Bot-Herder

Contents:
Malware, Fraud,
Unsolicited Ads,
Various Scams.



Computer with up-to-date antivirus:
Protected

No up-to-date antivirus:
Infected, enlisted into botnet

Step Two: Run Botnet Attacks



Botnet army under remote control



Millions of malware & spam messages sent to the world

HUGE PILL DISCOUNT!!



...and to you!



Clean Malware off Your Computer:
<http://support.microsoft.com/botnets>



Проект MARS

Проект MARS (Microsoft Active Response for Security – Оперативный Ответ Майкрософт на проблему безопасности) это совместные усилия группы Майкрософт по борьбе с киберпреступлениями (Microsoft's Digital Crimes Unit), центра Майкрософт по защите от вредоносных программ (Microsoft Malware Protection Center) и команды компьютерных специалистов (Trustworthy Computing team) по борьбе с ботнетами и устранения причиненного ими вреда.



- Операция b49: Закрытие ботнета Waledac - *Февраль 2010*
- Операция b107: Закрытие ботнета Rustock - *Март 2011*

VISIT SUPPORT.MICROSOFT.COM/BOTNETS TODAY

Trustworthy
Computing



Malware Protection Center
Threat Research and Response



Операция b49: Закрытие ботнета Waledac



Операция b49: Заккрытие ботнета Waledac

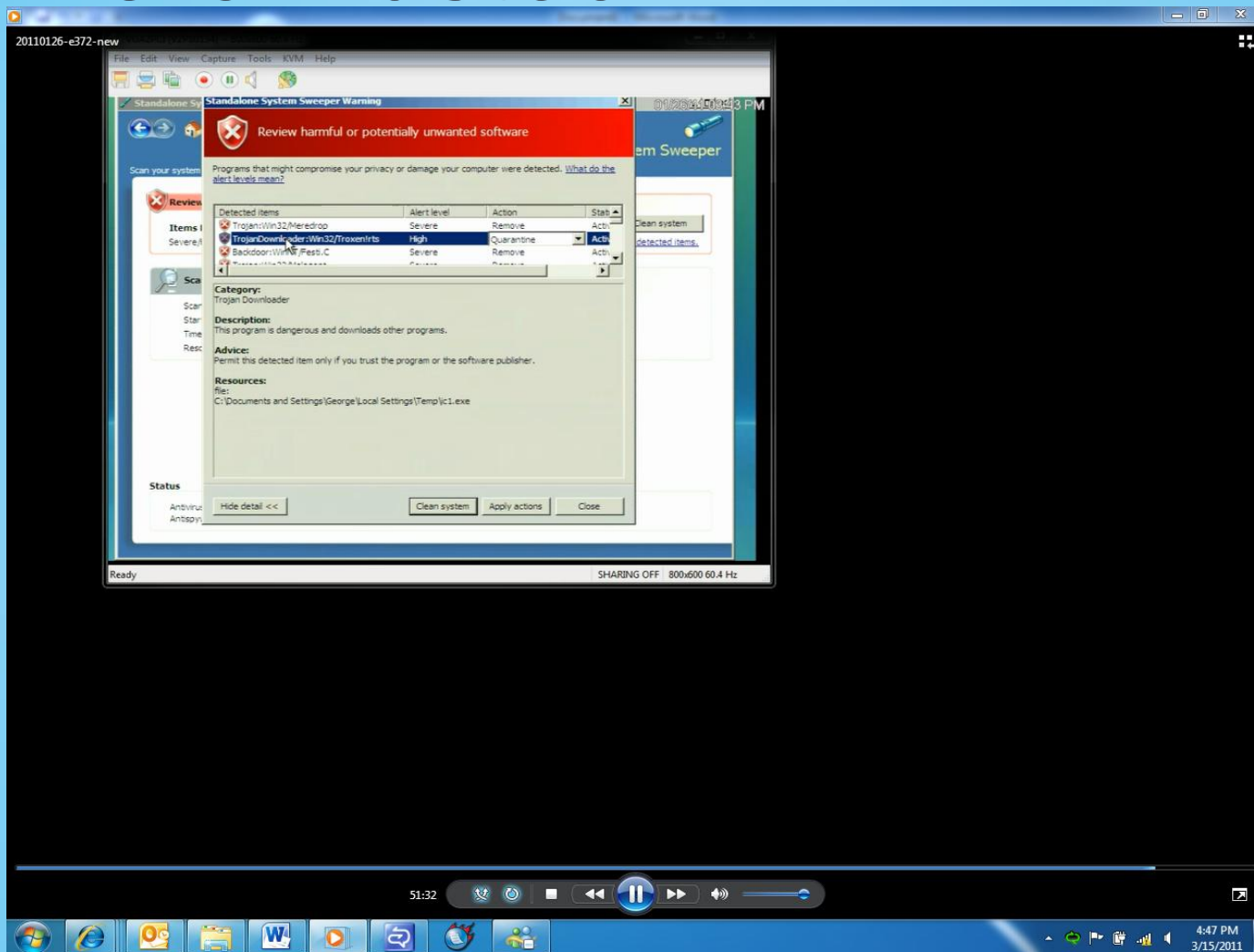
- В феврале 2010, окружной суд в штате Виргиния удовлетворил ходатайство компании Microsoft на закрытие Waledac, компьютерной сети, рассылающей спам . Была временно приостановлена деятельность 277 доменных имен, являющимися так называемыми командными центрами управления ботнетнетом Waledac.
- С помощью операции b49 удалось разрушить связь между ~70,000-90,000 компьютерами, составляющими ботнет



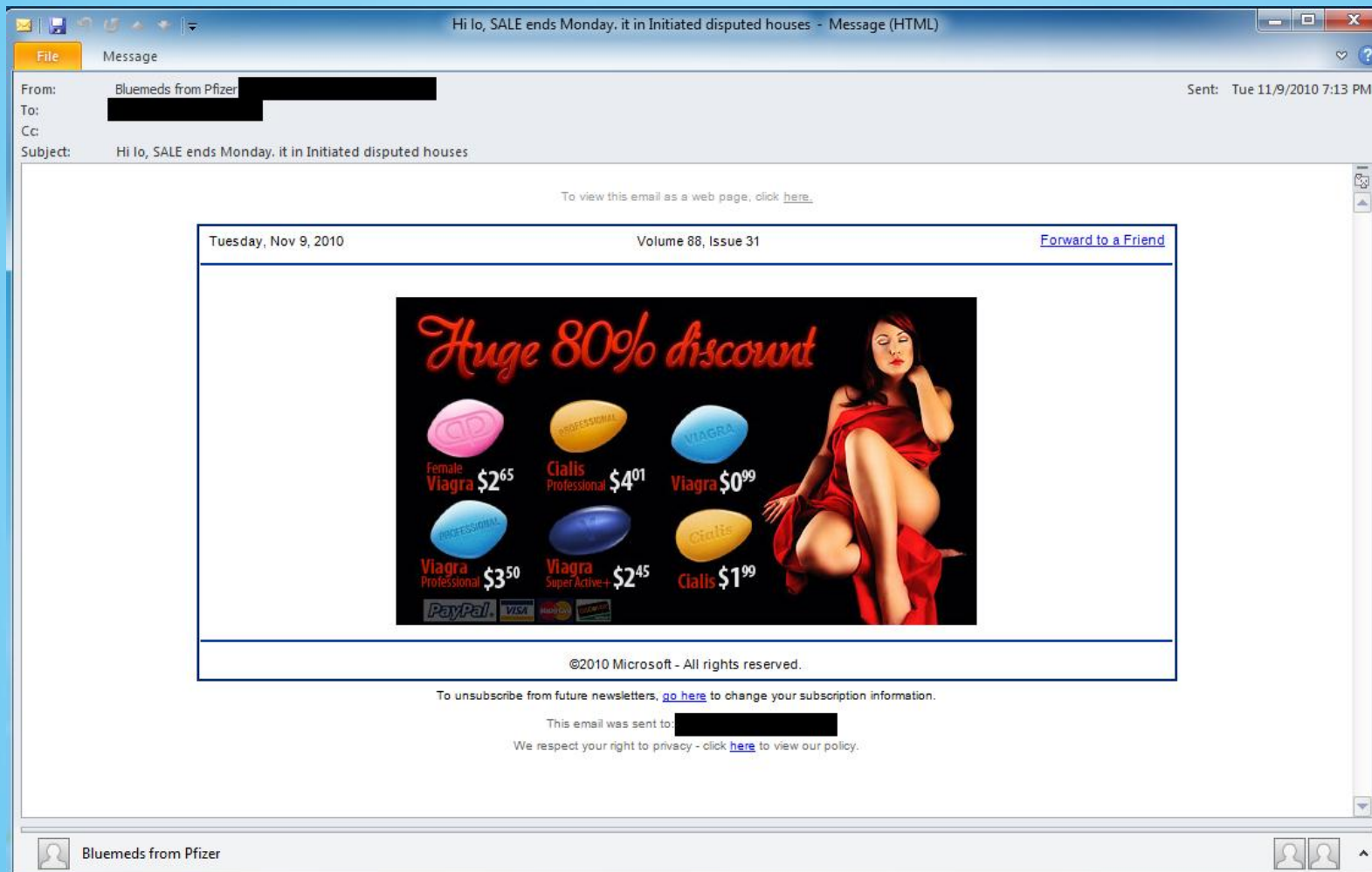
Операция b107: Заккрытие ботнета Rustock



Операция b107: Заккрытие ботнета Rustock



Операция b107: Заккрытие бот-сети Rustock



Операция b107: Закрытие ботнета Rustock



- Photo provided courtesy of Pfizer Corporation

Операция b107: Заккрытие ботнета Rustock

4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25

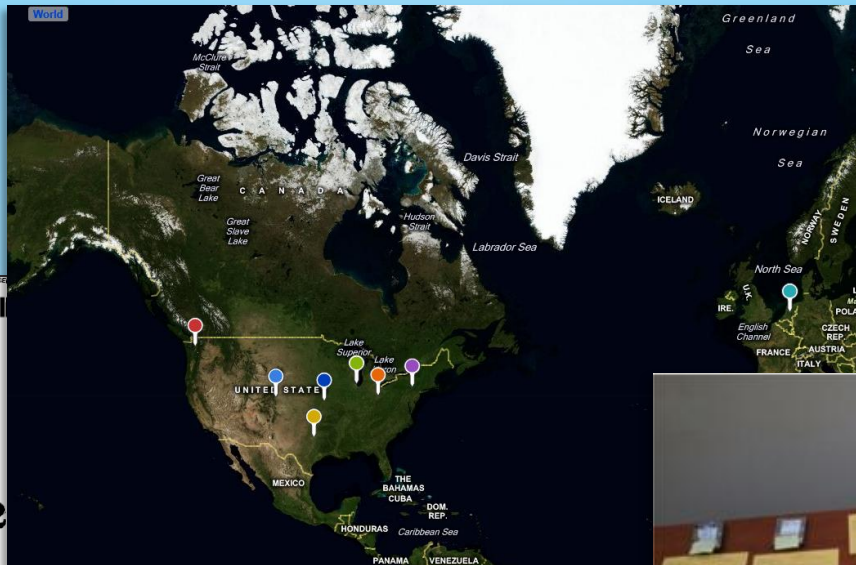
11-CV-00222-BOND

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.



Операция b107: освещение в СМИ

Microsoft Prescribes Lethal Dosage of "Offline" to the Rustock Botnet

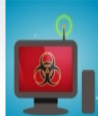
Like 34 people like this.

Adjust text size: A- A+
March 18th, 2011, 13:43 GMT By Marius Oiaga

Ads by Google Botnet Security Wordpress Spam Bot Stop Spam

When Microsoft took down Waledac in 2010, the company was just warming fights with the heavyweights of the botnet universe.

But it appears that shutting down Waledac was nothing but good practice for the Microsoft Digital Crimes Unit (DCU) which announced that it prescribed a lethal dosage of "offline" to Rustock, largest botnets and a primary source of prescription drugs spam.



Microsoft wins case against giant botnet Waledac

Posted by Sharon Pian Chan

With Rustock, a New Twist on Fighting Internet Crime

By Robert McMillan, IDG News

Microsoft помогла закрыть бот-сеть Rustock

Microsoft Drives the Last Nail into Waledac's Coffin

Like 4 people like this.

Adjust text size: A- A+
September 9th, 2010, 14:18 GMT By Marius Oiaga

PCWorld Business Center

Software & S

SECURITY

Microsoft for W

By Jeremy Kir



Начнем с того, что Rustock это крупнейший в мире ботнет – генератор спама. Как сообщают многочисленные источники, совсем недавно он прекратил свою, благодаря совместным действиям американских властей и Microsoft. Интернет гигант Microsoft подал судебный иск, который был направлен против анонимных операторов ботнета. Это позволило властям провести ряд скоординированных рейдов, благодаря которым прекратили работу контролирующие центры Rustock.

Tweet

Microsoft M

Share this: Like 19 Tweet 139

Microsoft's Digital Crimes Unit has disrupted one of the world's largest purveyors of spam, a complex "botnet" that was capable of sending billions of deceptive emails every day. Operated anonymously under the name Rustock, the botnet sent emails for Microsoft lottery scams as well as fake prescription drugs.

As many as one million computers have been infected by the Rustock botnet, a tool used by cybercriminals to deliver spam emails and engage in other illicit activities.



Court order helps Microsoft tear down Waledac botnet

By Robert McMillan
February 25, 2010 03:44 AM ET

Microsoft legal punch may change botnet battles forever

by Elinor Mills

Font size Print E-mail Share 87 comments

Security

February 25, 2010 8:38 AM PST

With legal nod, Microsoft ambushes Waledac botnet

by Lance Whitty

Microsoft is intent on eliminating the Waledac botnet and is using the legal system to help.

Tim Cranlon, Microsoft's associate general counsel, wrote Thursday on the company's blog that Microsoft has issued on Monday a temporary restraining order to criminals spreading the Waledac spambot.

For more security spam!



Благодаря корпорации Microsoft в четверг, 17 марта, была проведена совместная с федеральным правительством США акция по ликвидации одного из крупнейших генераторов спам-рассылок.

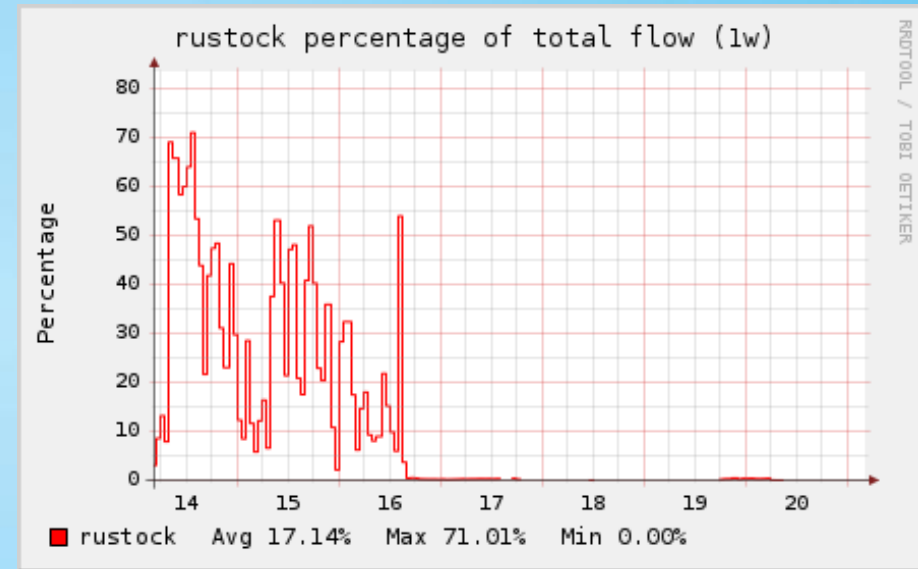
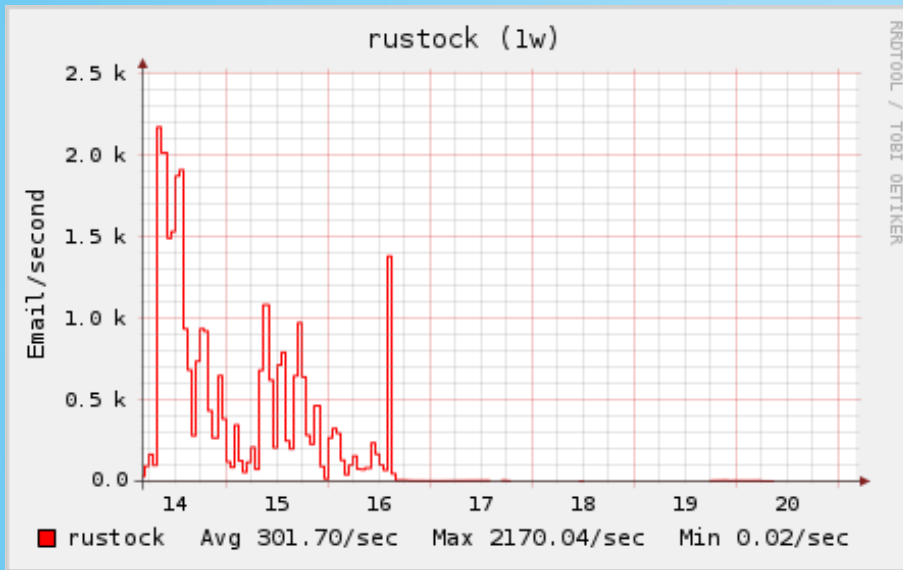
Microsoft подала судебный иск против операторов Rustock - бот-сети, состоящей из инфицированных компьютеров, запрограммированных на рассылку спама. В результате иска было санкционировано проведение крупномасштабной операции по всей стране, которая фактически привела к закрытию бот-сети.

Rustock Botnet Beaten Down by Microsoft

On the heels of last year's successful takedown of another giant botnet, Microsoft has taken down a bigger and more sophisticated botnet this week.



Опреация b107: влияние на количество мирового спама



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

Новые шаги по борьбе с ботнетами

The screenshot shows the Microsoft Support website interface. At the top, there is a search bar with the text "Search Microsoft Support". Below this is a navigation bar with links for "Support Home", "Solution Centers", "Advanced Search", and "Buy Products". The main heading is "Virus and Security Solution Center".

Below the heading is a section for "Ask Casey", featuring a text input field with the placeholder "Type your question here" and an "Ask" button. To the right of the input field is a small image of a woman, identified as a "Microsoft Automated Customer Service Agent".

On the left side, there is a vertical navigation menu with the following items: "Operation b49 and Operation b107", "Virus information", "Security information", "Hoaxes and scams", "Ask the Community", and "IT Professionals".

The main content area contains the following text:

Operation b49 is a Microsoft-led initiative to take down a known botnet - [Waledac](#) - through industry collaboration and legal process. Operation b49 is just one action in a long term effort by Microsoft to combat cyber threats and advance the security of the Internet for everyone.

Operation b49 has been followed now by **Operation b107**, a similar legal and technical operation to take down the notorious [Rustock](#) botnet. These operations are part of a sustained effort by Microsoft known as Project MARS (Microsoft Active Response for Security) to disrupt botnets and begin to undo the damage the botnets have caused by helping victims regain control of their infected computers.

This webpage is dedicated to helping provide people with information on how to remove Waledac, Rustock or other malware from their computers, so the computers are no longer operating under the remote control of bot-herders.

<http://support.microsoft.com/botnet>

S

MICROSOFT
DCU



Спасибо!

