Современные методы борьбы с ботнетами

Бешков Андрей
Руководитель программы информационной безопасности Microsoft

http://beshkov.ru
http://twitter.com/abeshkov
abeshkov@microsoft.com

Бешков? А это кто?

Ныне сотрудник MS отвечающий за ИБ программы в странах СНГ

Консультант в области телекома и крупных инфраструктур

Специалист в области UNIX и Windows

В прошлом пропагандист опенсорса

Каждый месяц ужасы!

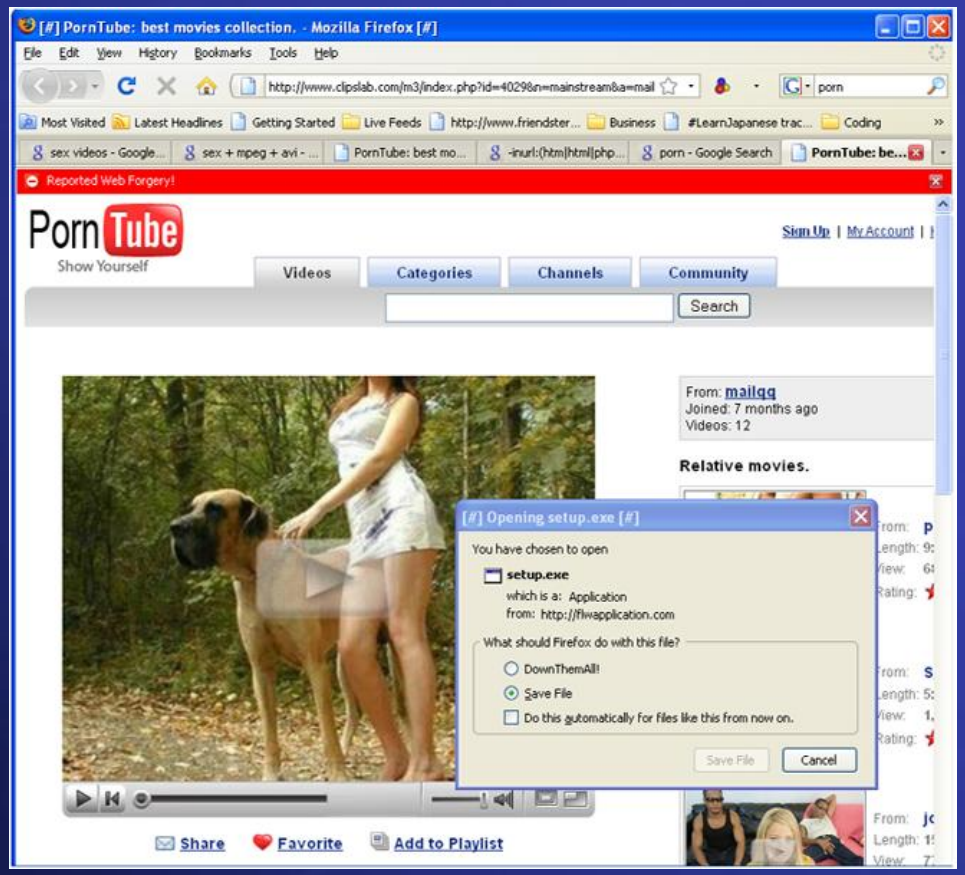
Откуда данные о зловредах?

- 600 000 000 сенсоров антивируса Microsoft
- 300 000 000 сенсоров собирающих образцы вредоносного ПО из почты Outlook.com
- Поисковые роботы Bing
- SmartScreen в Windows 8 собирает хэши файлов скачиваемых и запускаемых файлов

http://www.microsoft.com/security/sir

Win32/Alureon

Семейство	Категория	1 кв 2010	2 кв 2010	Годовой график
Win32/Alureon	Miscellaneous Trojans	1,463,885	1,035,079	



Предлагает поставить кодеки для проигрывания видео.

Кто же откажется? Бесплатно!

Вызывает BSOD при обновлении ОС

Win32/Zwangi

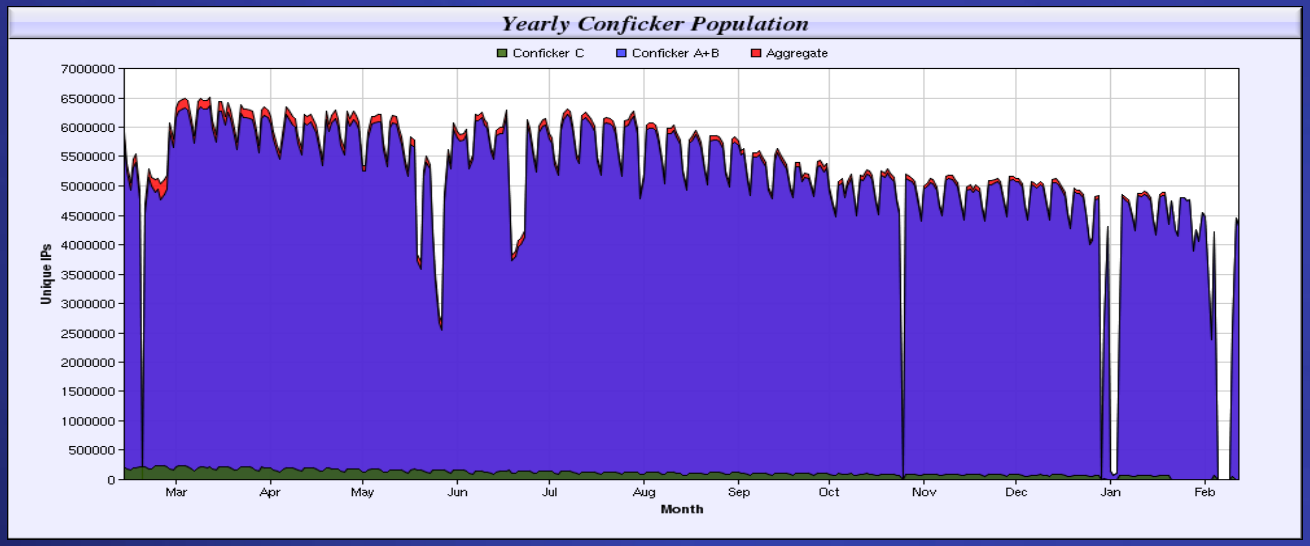
Семейство	Категория	1 кв 2010	2 кв 2010	Годовой график
Win32/Zwangi	Misc. Potentially Unwanted Software	542,011	859,801	

Предлагает бесплатный скринсейвер.

Устанавливается с разрешения пользователя.

Win32/Conficker - Kido

Семейство	Категория	1Q10	2Q10	Годовой график
Win32/Conficker	Worms	1,496,877	1,663,349	



Использует для распространения 3 уязвимости в Windows. В пике эпидемии доходил до 6,5 млн зараженных хостов.

Обновление устраняющее уязвимость выпущено за 3 месяца до эпидемии! Более 90% клиентов обновилось в течении первой недели. Заражены те, кто не установили обновление в течении трех лет.

Технологическая проблема?

9 из 10 широко распространенных злонамеренных приложений устанавливаются в систему с согласия пользователя!

Или не технологическая?

По данным AVG Technologies заражение через социальную инженерии происходит в 4 раза чаще чем с помощью уязвимостей в ОС и приложениях любого производителя.

SmartScreen блокирует 99,9% известных зловредов

Both Figure 1 and Figure 2 illustrate this challenge.

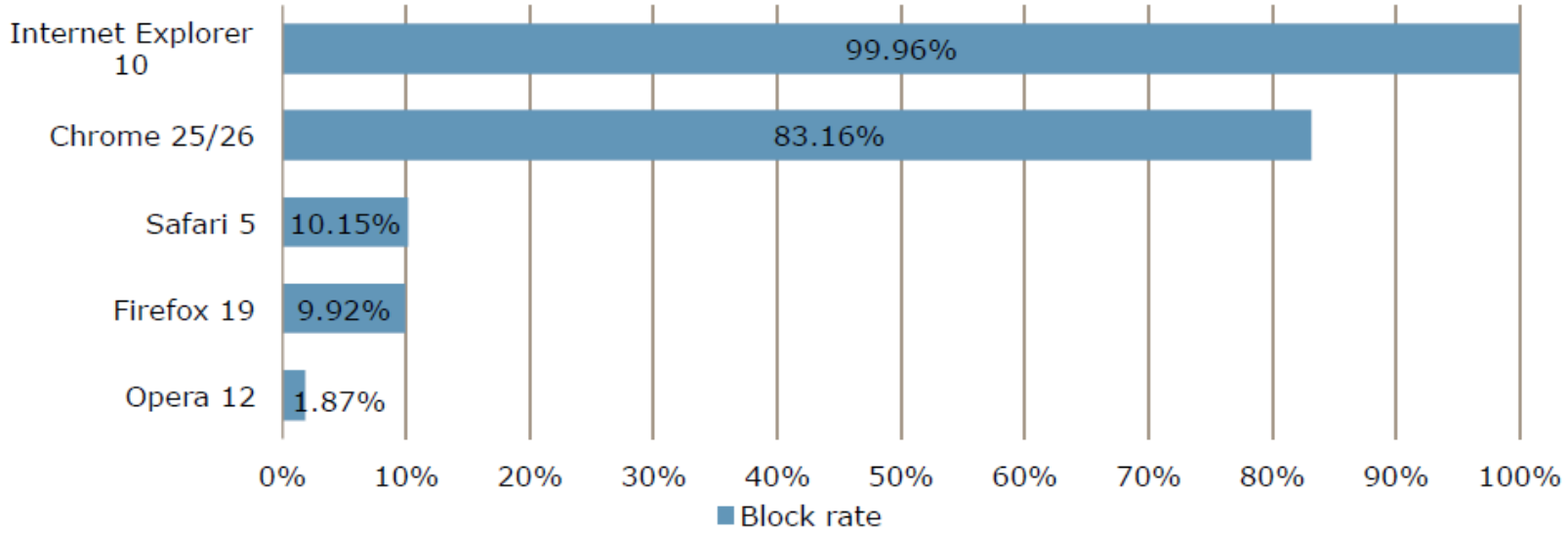
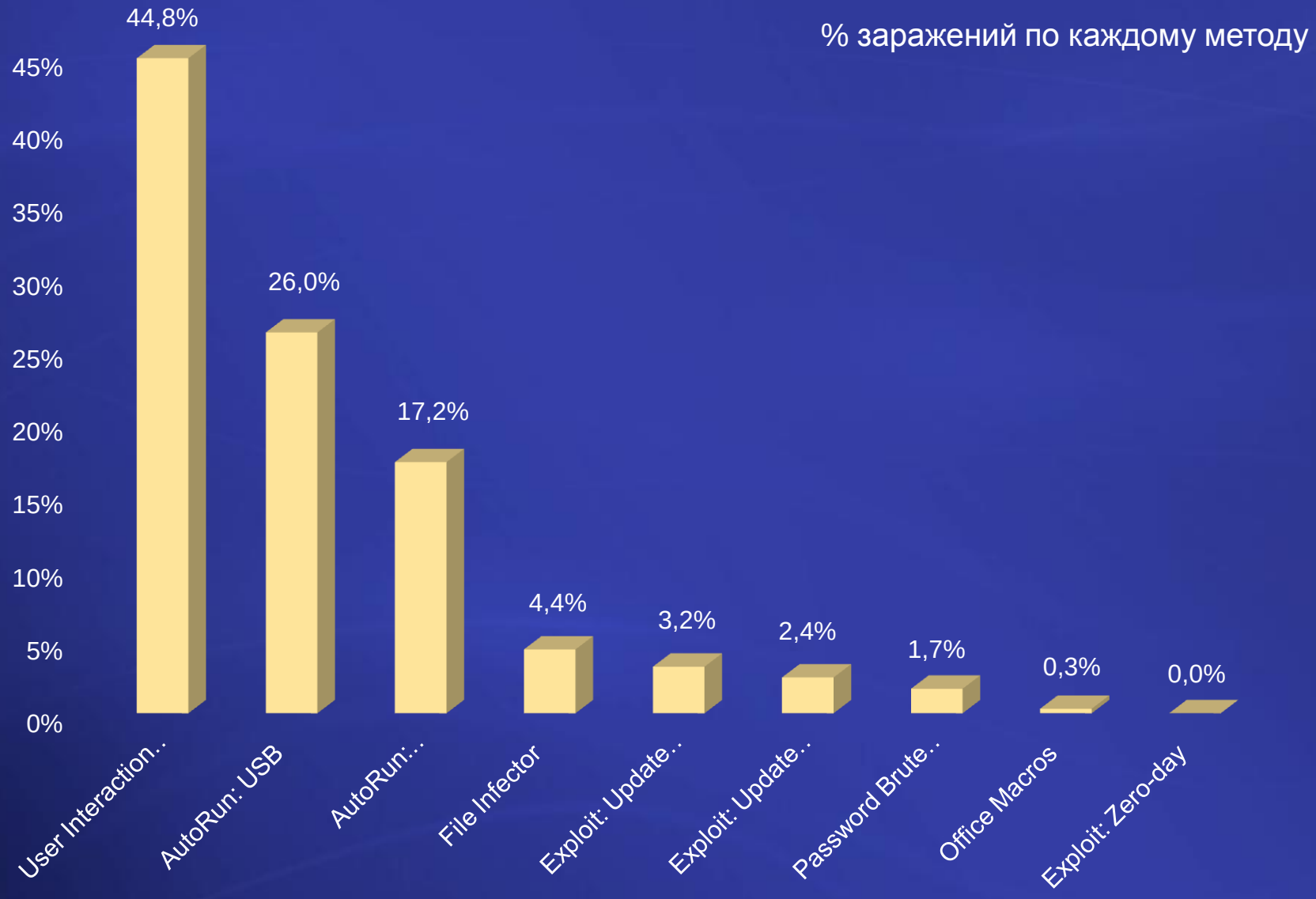


Figure 1 - Overall Malware Block Rate By Browser (Higher Values Are Better).

Методы распространения зловредов



Microsoft Security Intelligence Report выпуск 11

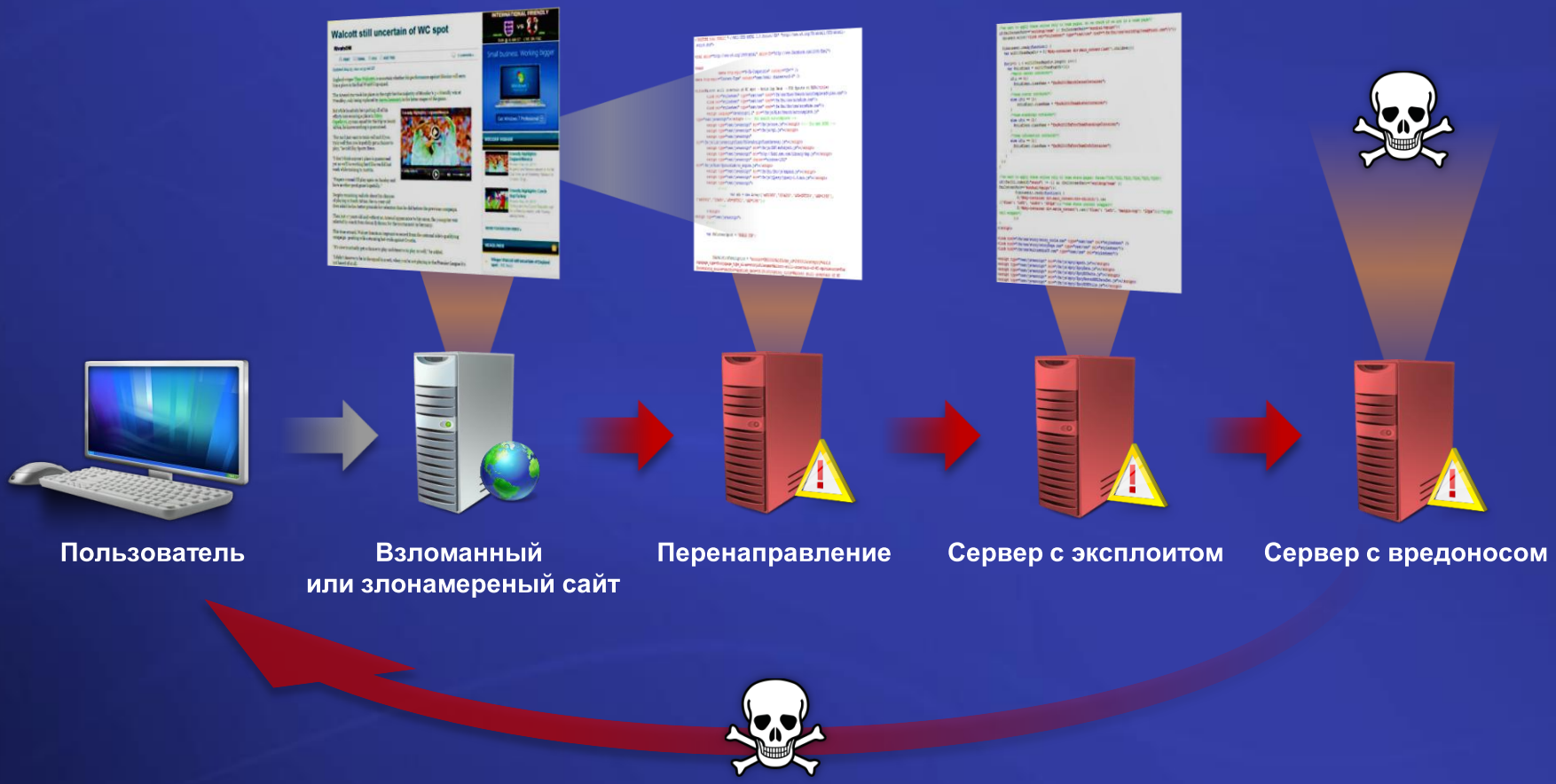
Атаки Drive-By Download

1. Пользователь с уязвимой системой посещает страницу с невидимым IFrame

2. IFrame секретно загружает другую страницу

3. Страница перенаправляет на другую страницу с эксплоитом

4. Если эксплоит сработал, скачивается зловред и заражает жертву



Что сейчас выгодно атаковать?

5 продуктов с множественными уязвимостями не обновленных на пользовательских ПК и наиболее часто атакуемых злоумышленниками

- Oracle Java
- Adobe Flash Player
- Apple QuickTime
- Apple iTunes
- Winamp
- Adobe Shockwave Player

23% пользователей посещают интернет с устаревших браузеров. 14.5% используют предыдущую версию, 8.5% отстают на несколько версий .

Kaspersky IT Threat Evolution Q3 2012

Zero day?

Zero day уязвимости - фетиш ИБ индустрии?

Распределение эксплоитов используемых в зловредном ПО 1П11

Microsoft Security Intelligence Report выпуск 11

Кто любит обновления?

Как дела с обновлениями в мире?

Статус обновления безопасности	Microsoft Windows	Microsoft Word	Adobe Reader	Oracle Java	Adobe Flash Player
Нет последнего обновления	34%	39%	60%	94%	70%
Нет последних трех обновлений	16%	35%	46%	51%	44%

Статистика по состоянию на октябрь 2011. Последнее обновление ядра Windows выпущено за 9 месяцев до даты сбора статистики, обновление для Word выпущено за год до этого.

Microsoft Security Intelligence Report выпуск 13

Упрощение обновлений SUVP

- Security Update Validation Program
- **Бесплатно**
- Можно получать обновления для продуктов Microsoft за месяц до их официального выпуска. Это позволяет тестировать их тщательнее перед развёртыванием их у себя в инфраструктуре.
- Включение в программу по приглашениям. Необходимо подписать соглашение о неразглашении

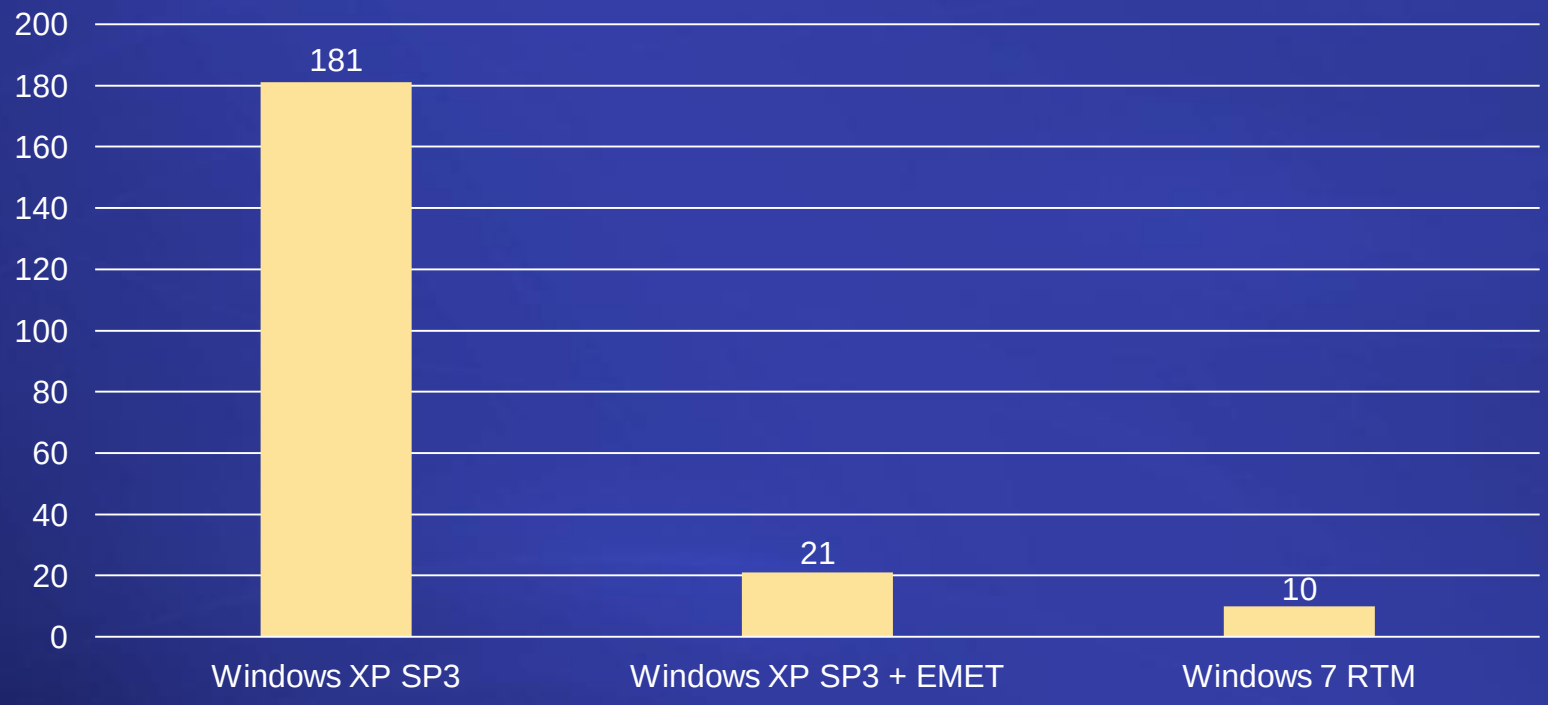
Как защищаться?

Работа в системе с правами обычного пользователя предотвращает атаки на:

75% - критических уязвимостей Windows 7
100% - уязвимостей Microsoft Office опубликованных в 2010 г.
100% - уязвимостей Internet Explorer опубликованных за 2010 г.
64% всех уязвимостей в продуктах Microsoft опубликованных в 2010 г.

Исследование BeyondTrust за 2010 г

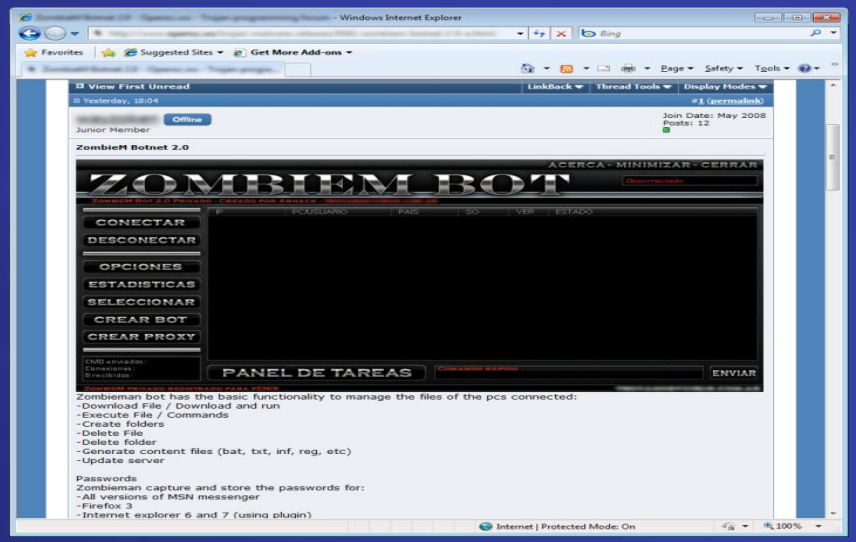
EMET блокирует 89% эксплоитов

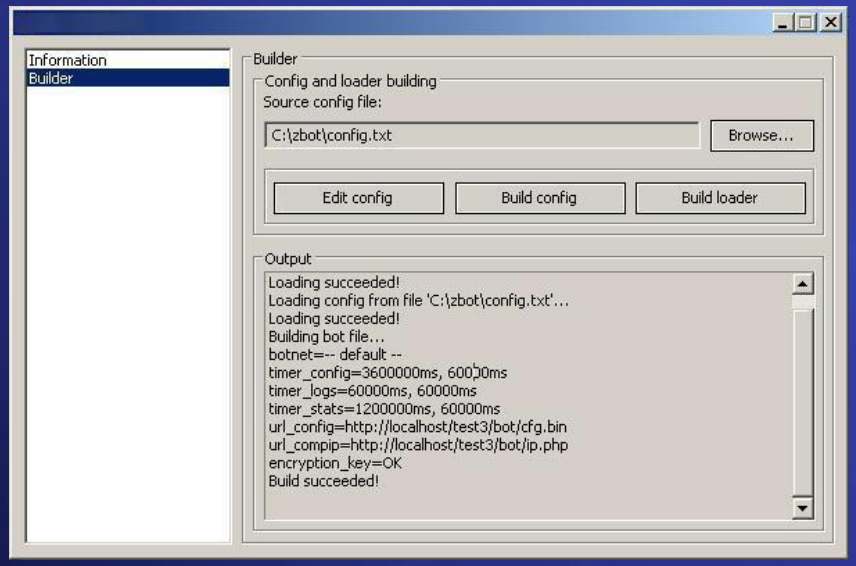


Для тестирования EMET использовались 184 наиболее популярных эксплоита

Борьба с ботнетами

Изготовление ботнетов





Ботнет комплекты в продаже:

- Zbot (Zeus)
- Spyeye
- Mariposa
- Black Energy
- ButterFly
- Reptile
- Zombiem
- Ice-X

Цена на комплект варьируется от 10000$ до 5$.

Справится даже ребенок!

Linux и Android ботнеты

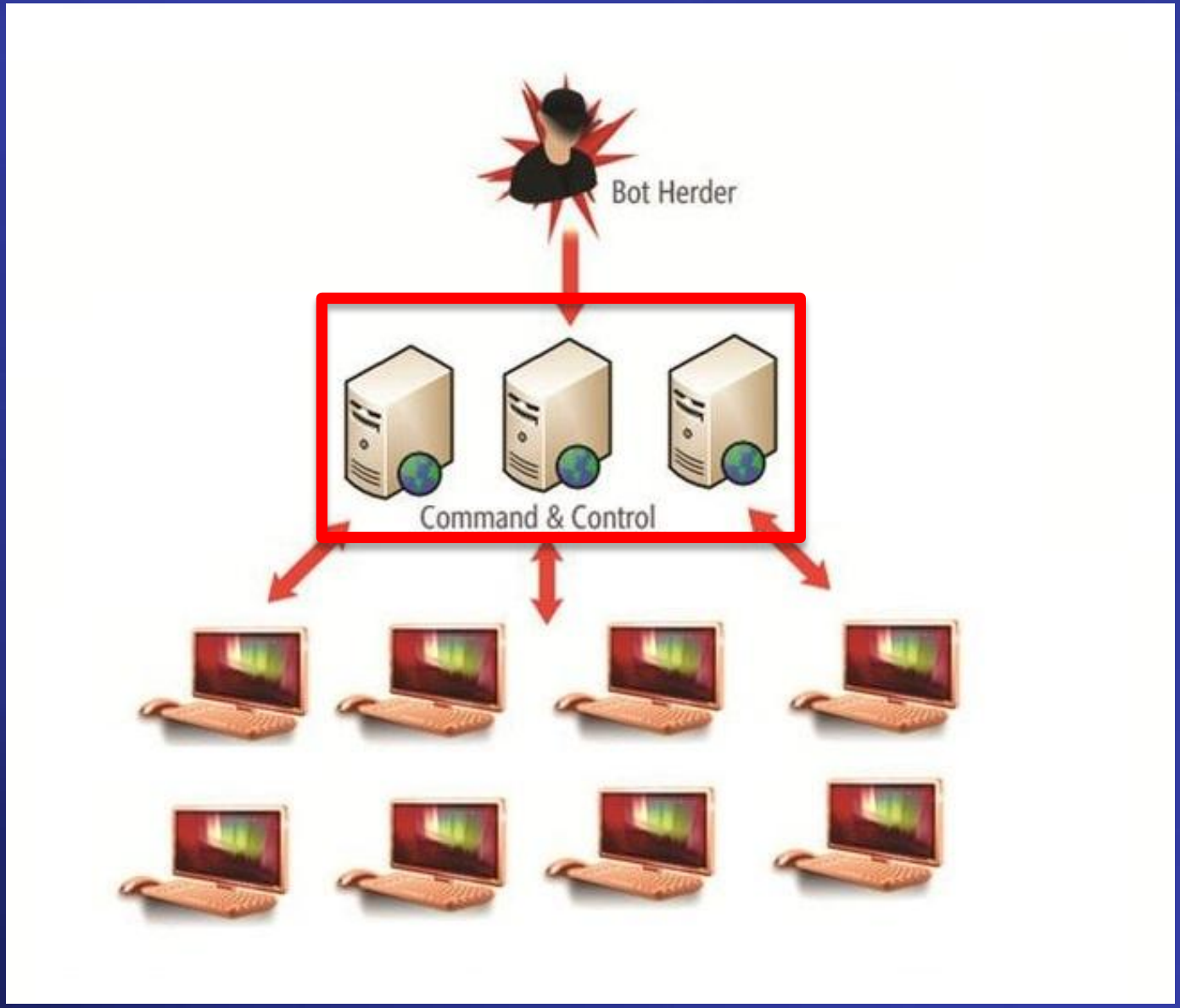
Psyb0t
100.000 ADSL зараженных маршрутизаторов Netcomm NB5.

Заражает прошивки OpenWRT и DD-WRT.
Подбирает пароли SSH, FTP, telnet
Атакует phpMyAdmin и MySQL.

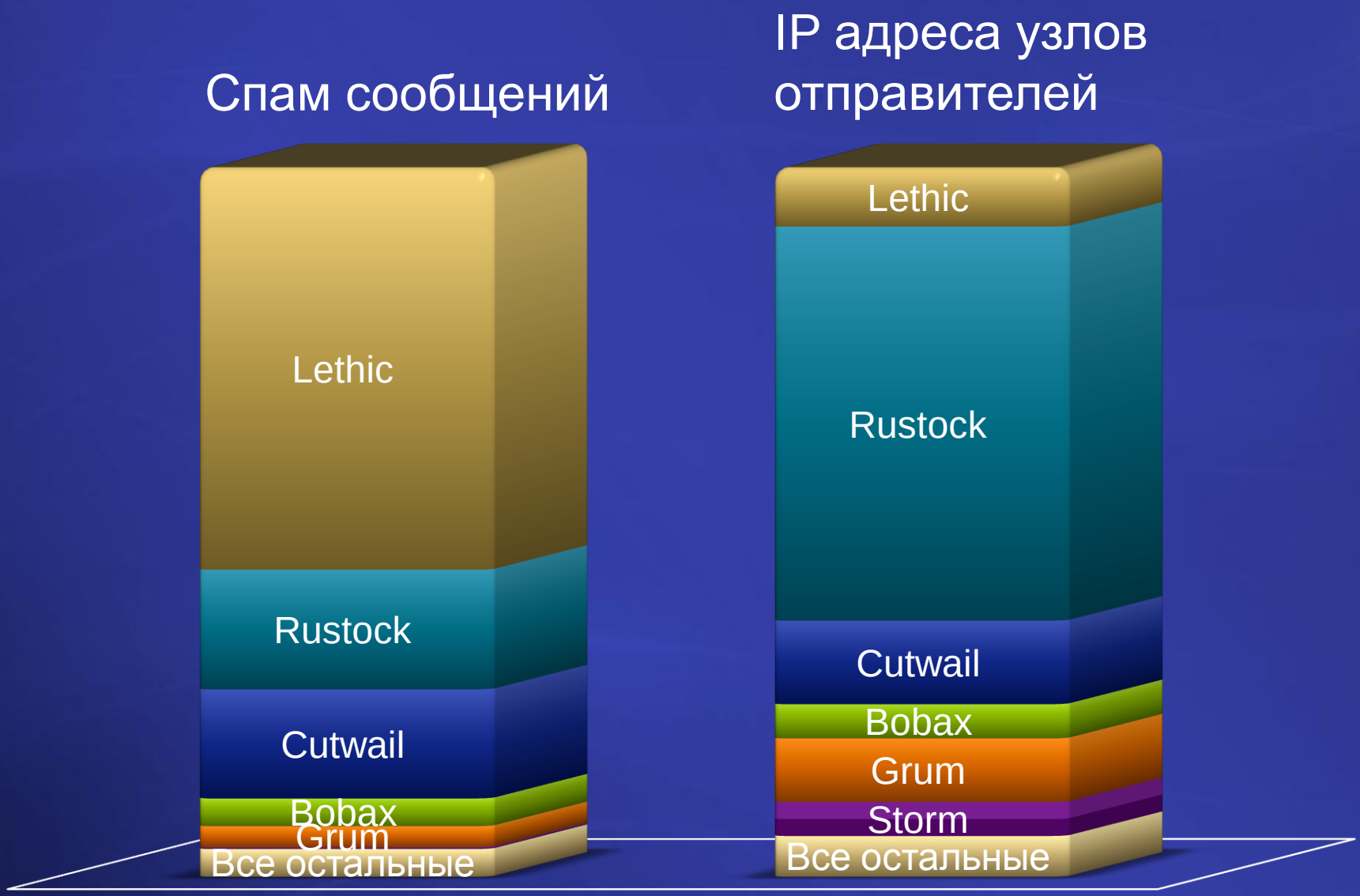
Chuck Norris - Аналогичен PsyB0t + атакует ТВ приставки

Ботнеты на Android от 40 до 150000
http://s1.securityweek.com/report-reveals-emerging-trend-android-botnet-infections
http://www.xakep.ru/post/58265/default.asp

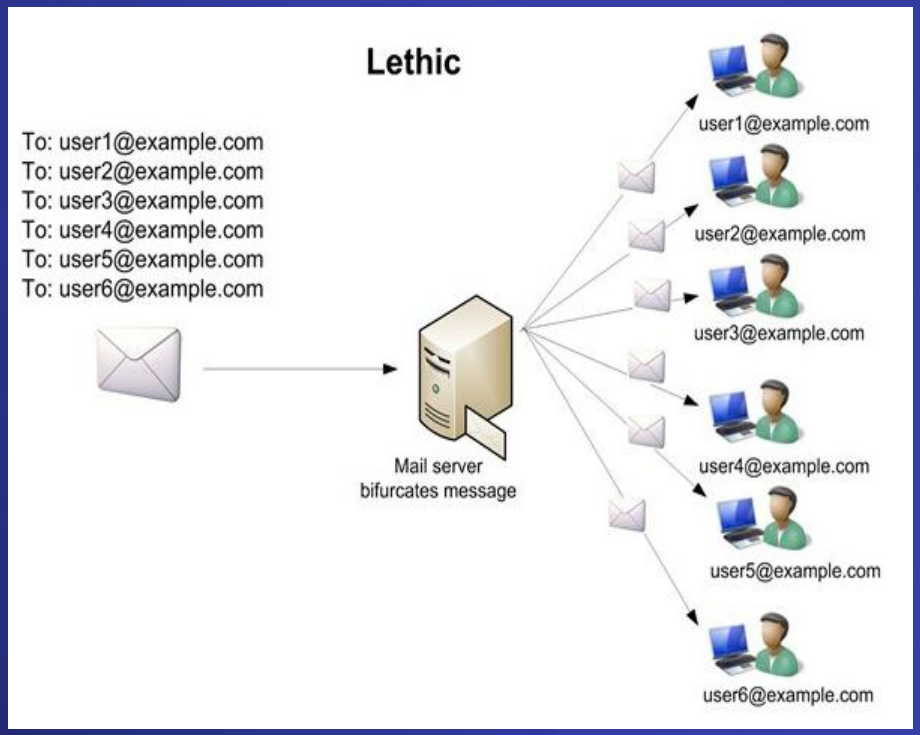
Типовая структура ботнета

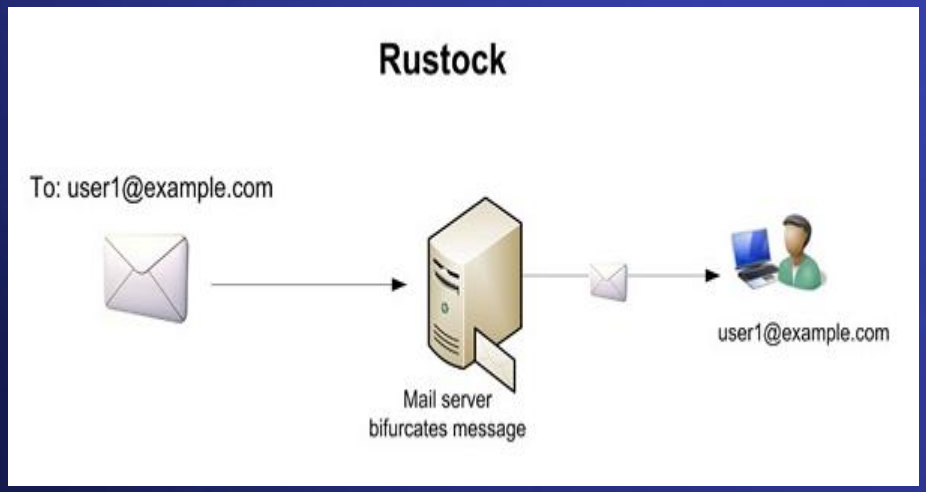


Обнаружение активности ботнетов



Поведение ботнета при рассылке спама



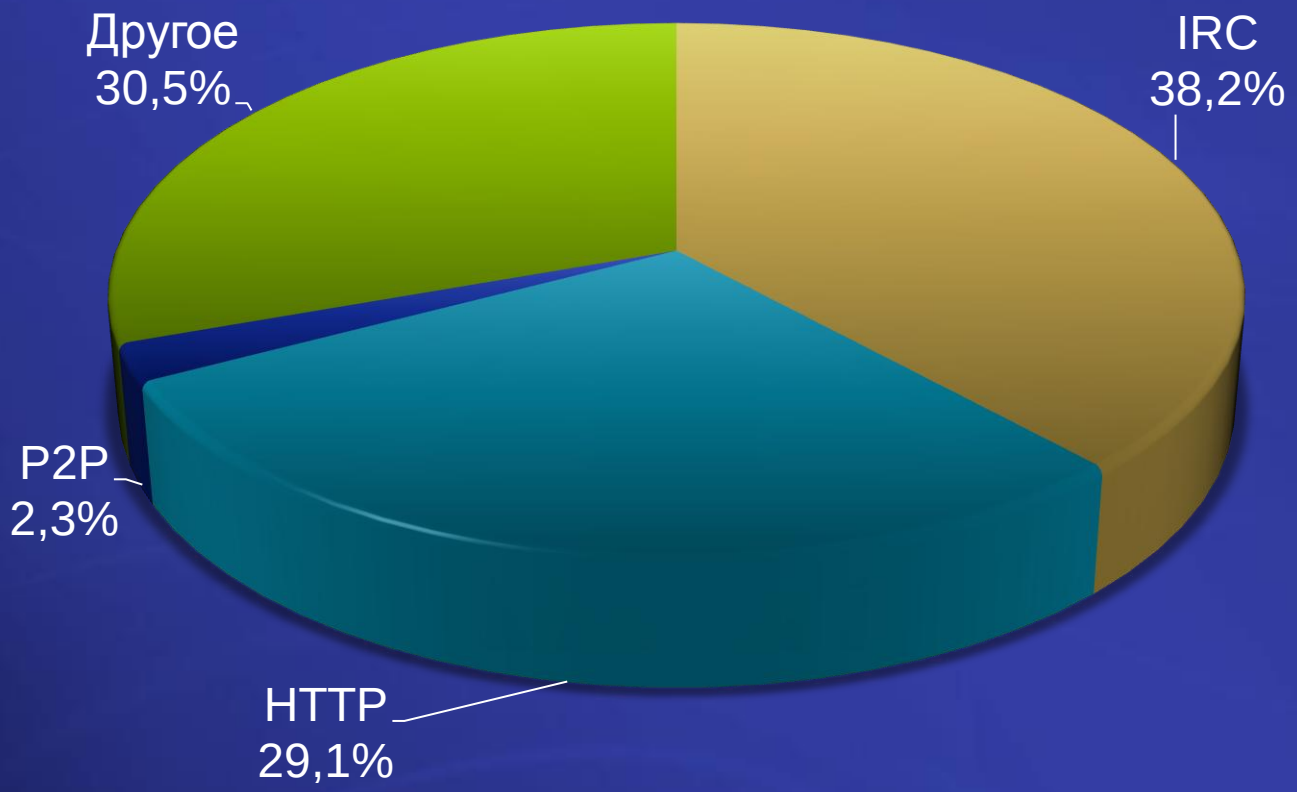


Lethic крайне агрессивно рассылает спам с малого количества IP адресов.

Rustock использует много IP адресов и шлет с каждого понемногу.

За счет этого обнаружить Rustock сложнее.

Механизмы управления C&C узлами



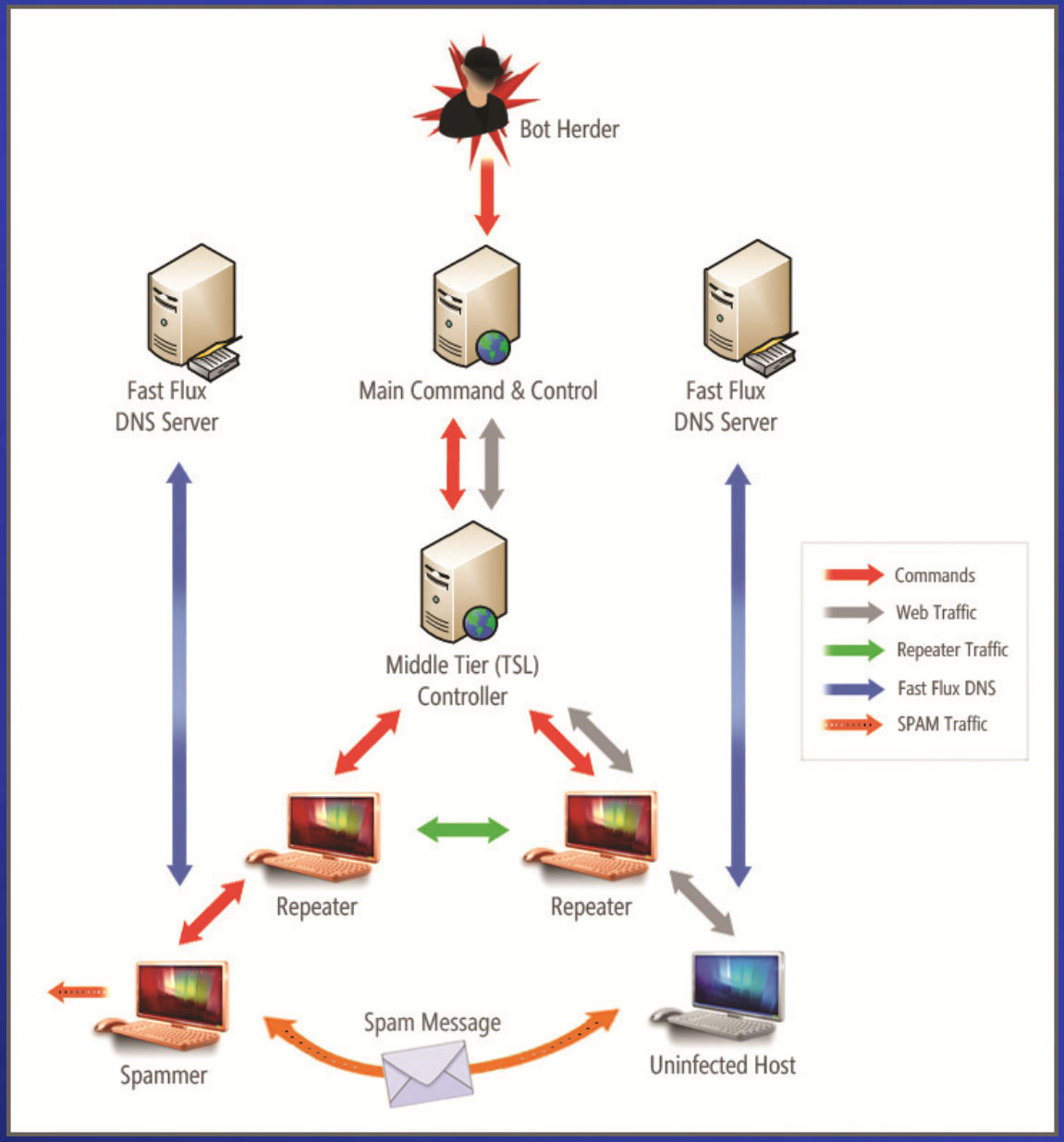
Варианты уничтожения ботнета

- Судебный иск и захват C&C узлов
- DDoS на C&C узлы
- Жалобы провайдеру
- Захват DNS имен
- Блокирование IP адресов
- Арест владельца ботнета

Операция b49

Захват ботнета Waledac

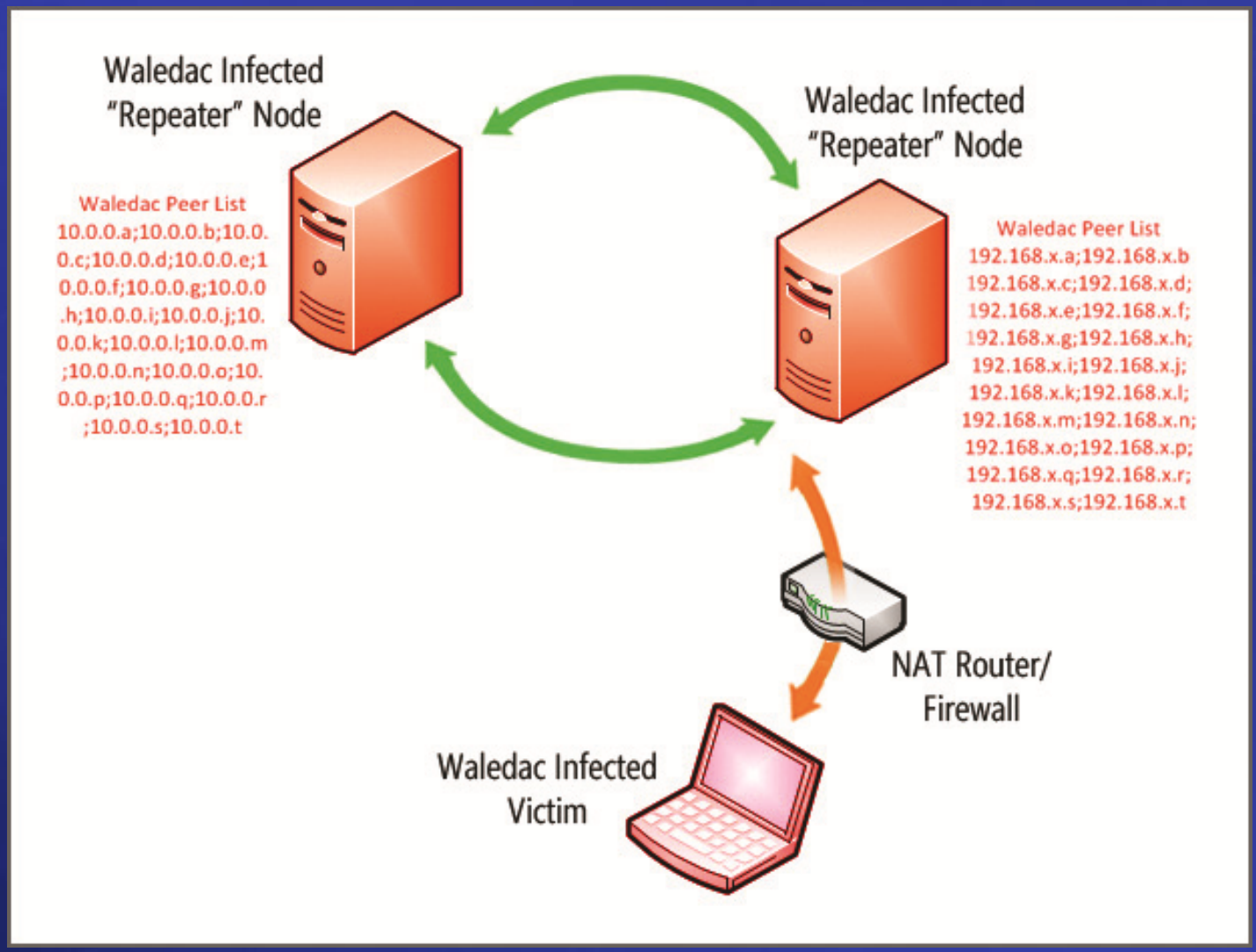
Структура ботнета Waledac



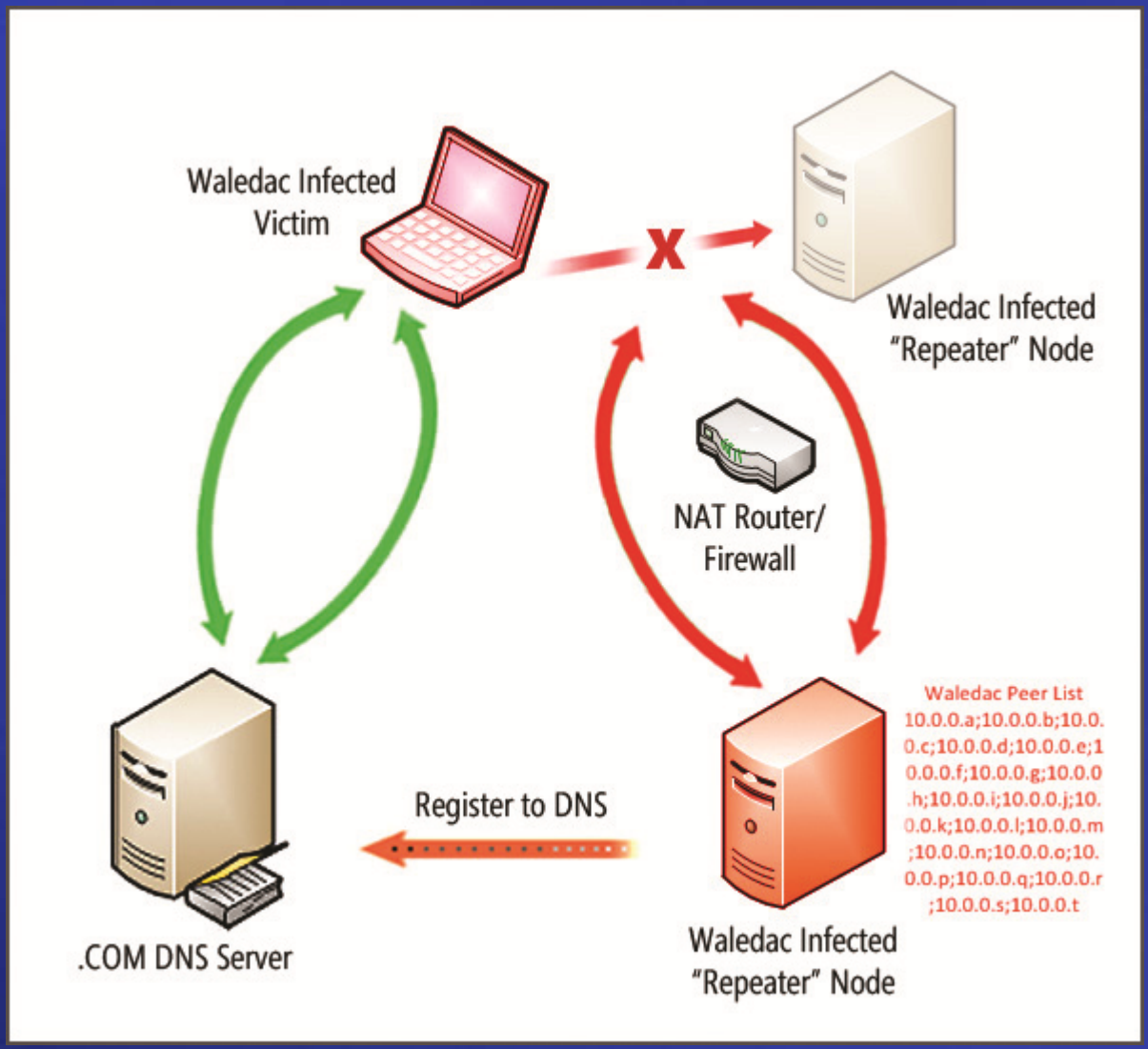
277 DNS имен Waledac

- bestchristmascard.com
- bestmirabella.com
- bestyearcard.com
- blackchristmascard.com
- cardnewyear.com
- cheapdecember.com
- christmaslightsnow.com
- decemberchristmas.com
- directchristmasgift.com
- eternalgreetingcard.com
- freechristmassite.com
- freechristmasworld.com
- freedecember.com
- funnychristmasguide.com
- greatmirabellasite.com
- greetingcardcalendar.com
- greetingcardgarb.com
- greetingguide.com
- greetingsupersite.com
- holidayxmas.com
- topgreetingsite.com
- whitewhitechristmas.com
- worldgreetingcard.com
- yourchristmaslights.com
- yourdecember.com
- yourmirabelladirect.com
- newyearcardcompany.com
- newyearcardfree.com
- newyearcardonline.com
- newyearcardservice.com
- smartcardgreeting.com
- superchristmasday.com
- superchristmaslights.com
- superyearcard.com
- themirabelladirect.com
- themirabellaguide.com
- themirabellahome.com
- yourregards.com
- youryearcard.com
- bestbarack.com
- greatobamaguide.com
- greatobamaonline.com
- jobarack.com
- superobamadirect.com
- superobamaonline.com
- thebaracksite.com
- topwale.com
- waledirekt.com
- waleonline.com
- waleprojekt.com
- goodnewsdigital.com
- goodnewsreview.com
- linkworldnews.com
- reportradio.com
- spacemynews.com
- wapcitynews.com
- worldnewsdot.com
- worldnewseye.com
- worldtracknews.com
- bestgoodnews.com
- adorelyric.com
- adorepoem.com
- adoresongs.com
- bestbaracksite.com
- bestobamadirect.com
- expowale.com
- bestadore.com
- bestlovelong.com
- funloveonline.com
- youradore.com
- yourgreatlove.com
- orldlovelife.com
- romanticsloving.com
- adoresong.com
- bestlovehelp.com
- chatloveonline.com
- cherishletter.com
- cherishpoems.com
- lovecentralonline.com
- lovelifeportal.com
- whocherish.com
- worldlovelife.com
- worshiplove.com
- yourteamdoc.com
- yourdatabank.com
- alldatanow.com
- alldataworld.com
- cantlosedata.com
- justchristmasgift.com
- lifegreetingcard.com
- livechristmascard.com

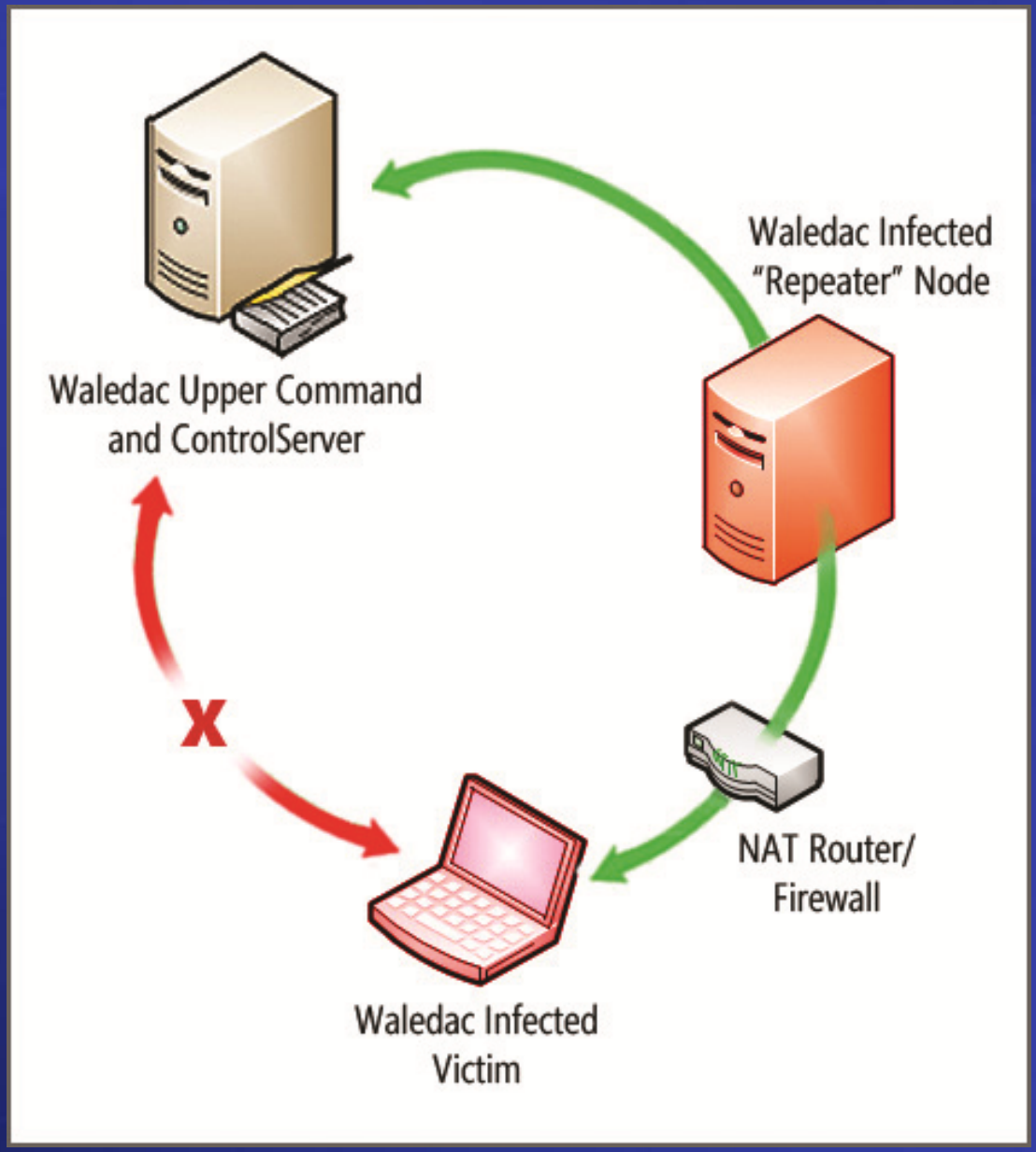
Узлы маршрутизаторы Waledac



P2P обмен внутри Waledac с помощью fast flux DNS



Проксирование траффика Waledac



Захват Waledac

Hotmail заблокировал 651 миллион соединений от ботнета Waledac- за 18 дней

Waledac входит в 10 крупнейших ботнетов в 39 странах

Уведомление о решении суда www.noticeofpleadings.com

Date of First Publication: February 24, 2010

UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA
Alexandria Division

MICROSOFT CORPORATION,
a Washington corporation,

Plaintiff,

vs.

JOHN DOES 1-27, CONTROLLING
A COMPUTER BOTNET THEREBY
INJURING MICROSOFT AND ITS
CUSTOMERS,

Defendants.

CIVIL ACTION NO. 1:10 CV 156 (LMB/JFA)

NOTICE AND SERVICE IN ENGLISH

Plaintiff Microsoft has sued defendants John Does 1 -27 associated with the Internet domains listed below. Microsoft alleges that Defendants have violated Federal and state law by operating a computer botnet through 276 internet domains, causing unlawful intrusion and dissemination of unsolicited bulk email to the injury of Microsoft. Microsoft seeks a preliminary injunction directing Verisign to take all steps necessary to lock these domains at the registry level and remove them from the zone file to ensure that changes to the domains cannot be made absent a court order and that all such domains be held in escrow by Verisign pending resolution of the dispute. Microsoft seeks a permanent injunction and damages. Full copies of the pleading documents are available at http://www.noticeofpleadings.com.

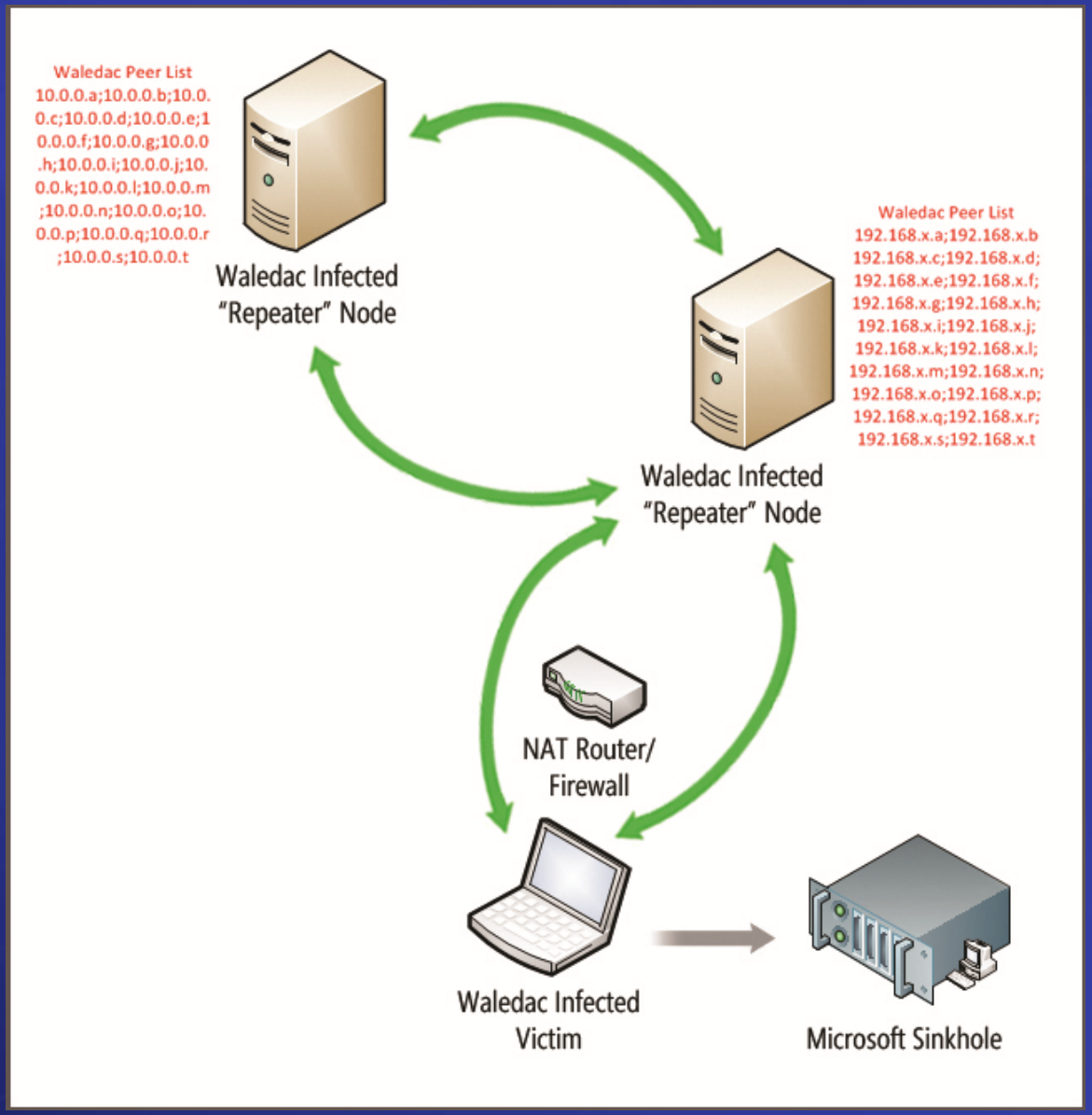
NOTICE TO DEFENDANT: READ THESE PAPERS

NOTICE AND SERVICE IN CHINESE

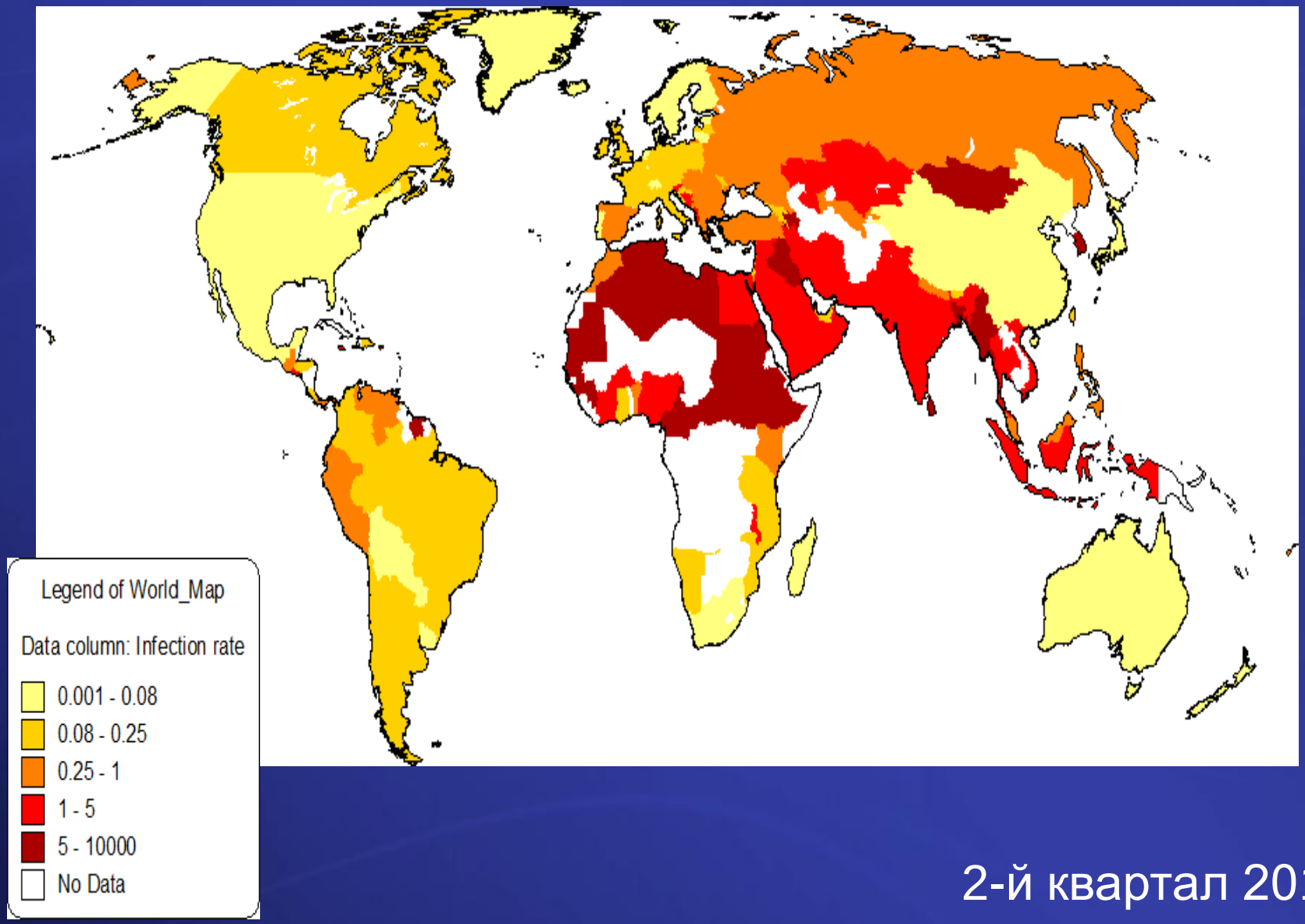
原告微软已经对27位与以下列出的因特网域名有关的身份不明的被告1至27（被告John Doe 1-27）提起诉讼。微软指控该等被告通过276个因特网域名操作计算机僵尸网络、导致非法入侵和散布未经请求的的大量邮件而给微软造成伤害，其行为已违反联邦和州法律。微软寻求初步禁令：命令威瑞信（Verisign）采取所有必需的步骤在注册管理机构级别锁定这些域名以确保在没有法院命令的情况下不得对这些域名做出变更，并且在该争议未解决之前，所有这些域名都由威瑞信进行提存监管。微软寻求永久禁令和损害赔偿。诉讼文件的完全副本可从 http://www.noticeofpleadings.com获取。

致被告的通知：请仔细阅读这些文件！你必须在本案中□正式出面□，否则另一方将自动胜诉。要□正式出面□，你必须向法院提交称为□动议□或者□答辩□的法律文件。□动议□或者□答辩□必须自在此指定的首次公告日之日起21天内被提交给法庭秘书或者行政管理人员。该□动议□或者□答辩□必须以合适的形式并且有证据证明已送达原告律师Preston Burton，奥睿律师事务所，华盛顿特区第15西北大街1152号哥伦比亚中心

Отравление Waledac

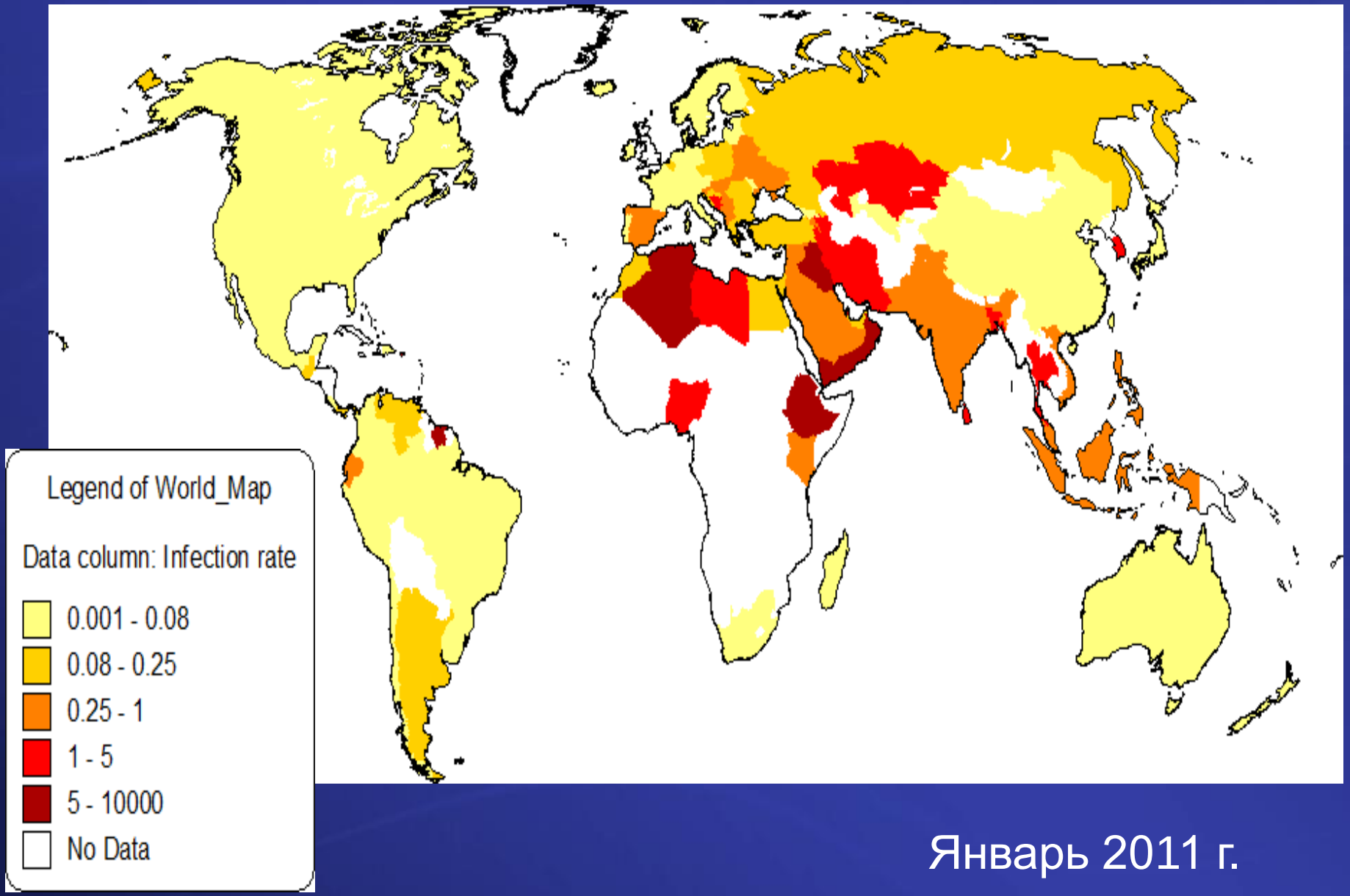


Активные IP адреса ботнета Waledac



2-й квартал 2010 г.

Активные IP адреса ботнета Waledac



Январь 2011 г.

Аналитика и угрозы в OTIS

- Online Threat Information Sharing
- **Бесплатно**
- Список рассылки о проблемах безопасности
- Участвуют группы разработки MS и специалисты ИБ
- Канал между специалистами ИБ клиентов использующих наши продукты и специалистами ИБ Microsoft
- Требует подписания NDA

После захвата

Без команд с C&C сервера боты впадают в спячку.

MS не может удалить ботов с зараженных ПК. Это будет вмешательством в частную жизнь.

Образцы ботов добавляются в антивирусные продукты MS и других производителей. Обмен образцами идет через Microsoft Active Protection Program (MAPP)

Интернет провайдерам сообщаются адреса зараженных машин через программу Global Infrastructure Alliance for Internet Safety

Пользователям рекомендуется использовать:
Malicious Software Removal Tool
Microsoft Safety Scanner
Microsoft Security Essentials

Постепенно боты удаляются антивирусами.

MICROSOFT DIGITAL CRIMES UNIT

Уничтожение других ботнетов

Операция b49

Захват ботнета Waledac

1.5 миллиардов спам сообщений ежедневно. В процессе исследования найдено полмиллиона паролей от почтовых ящиков пользователей и ftp серверов.

Операция b107

Захват ботнета Rustock. В пике своей активности рассылал 80% мирового спама. Примерно 2000 спам сообщений в секунду.

Захват ботнета Coreflood

ФБР при содействии Microsoft захватила ботнет Coreflood отвечающий за финансовые преступления на сумму 100 миллионов долларов

Операция b79

Захват ботнета Kelihos

Совместная операция Лаборатории Касперского и Microsoft. Kelihos можно назвать Waledac 2.0

Вопросы?

http://twitter.com/abeshkov
abeshkov@microsoft.com

Дополнительные ресурсы

http://blogs.technet.com/mmpc/
http://blogs.technet.com/msrc/
http://www.microsoft.com/security/sdl/
http://www.microsoft.com/security/sir/