



The Botnet Ecosystem

Vitaly Kamluk
Chief Security Expert
Kaspersky Labs Japan



About Vitaly



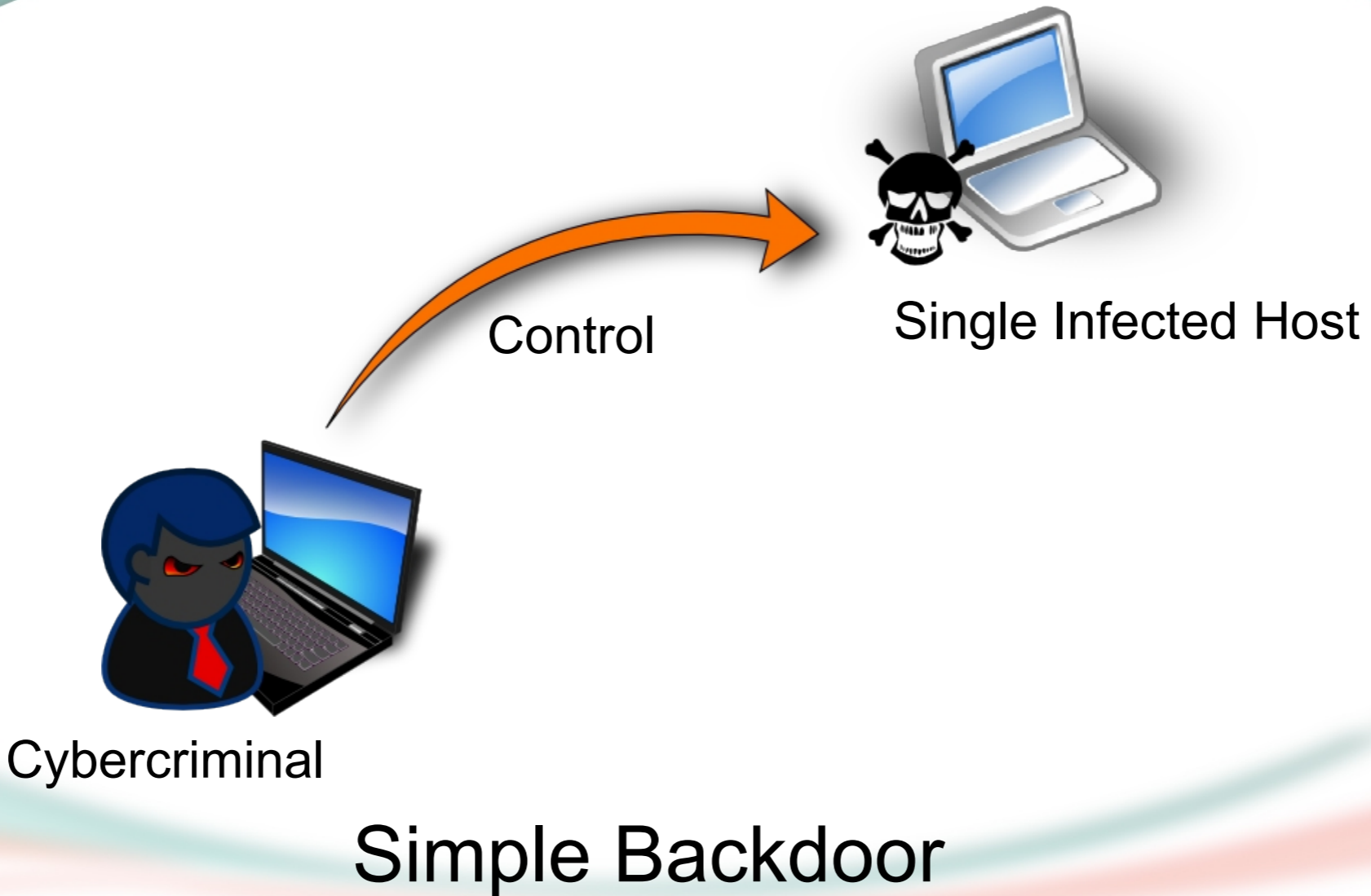
About Vitaly



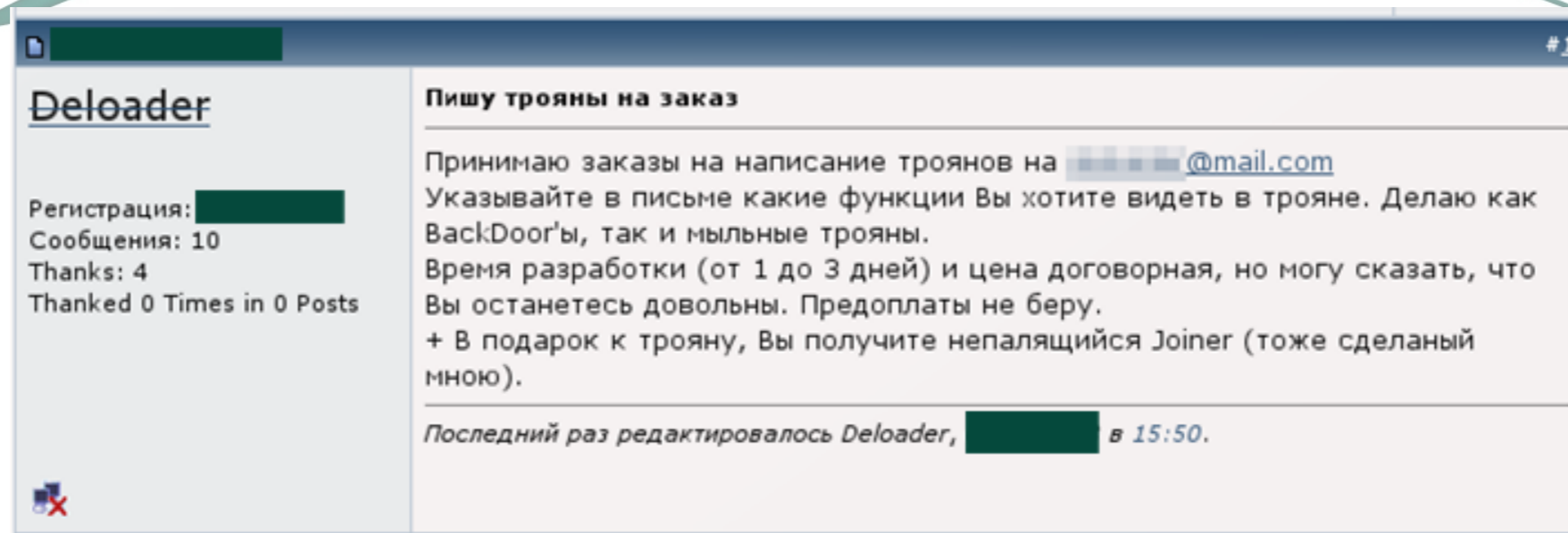
About Vitaly



Evolution of botnets

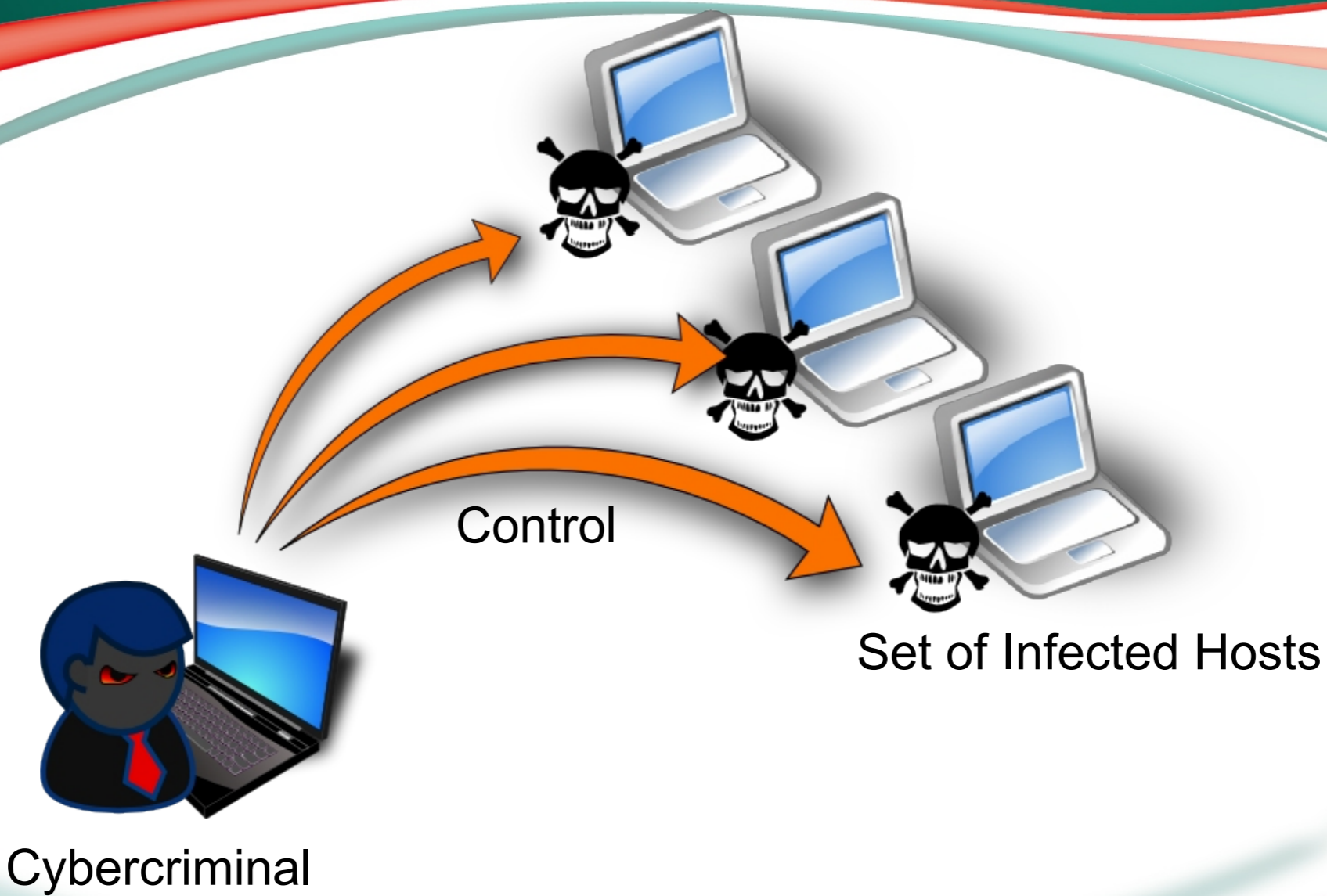


Evidence: malware development



The poster says he can develop Trojans; the customer should specify the functions desired. In addition, the poster offers potential customers a "Joiner" program which makes it possible to inject any malicious program into the executable file of a legitimate application.

Evolution of botnets




The first botnet

Evidence: multiple bot control (DdoS bot)

09.03.2009, 01:41 #1

sw_max
Почётный участник



Регистрация: 08.03.2007
Сообщений: 307

DDos бот нового поколения. Приват.

В связи с высоким интересом темы ДДоС и большим количеством заказов такого софта нами был разработан собственный, серийный продукт.

Первые же тесты показали что бот намного эффективнее предшественников (Black Energy, Illusion, etc...), его основные преимущества...

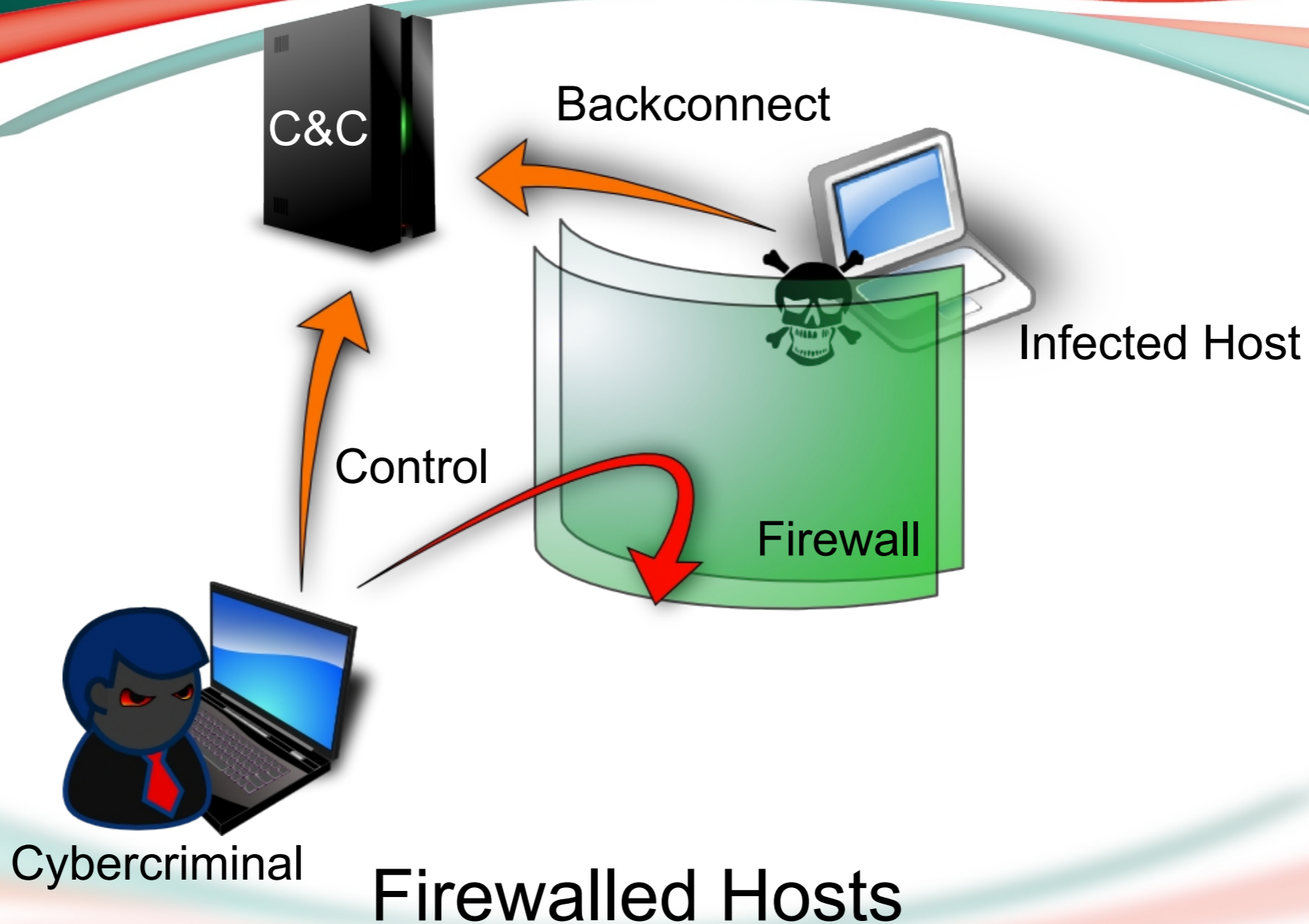
- 1) Работа в 100 потоков. без таймаутов. Потоки хорошо синхронизированы между собой, что дает возможность генерировать максимальное количество http трафика в единицу времени.
- 2) Возможность атаки по нескольким урл сервера (например форум, новостной блок, файловое хранилище). При таком виде атаки таргеты выбираются каждым экземпляром бота отдельно, это в разы увеличивает нагрузку на сервер, ведь закешировать ответ невозможно.
- 3) Выбор ID случайным образом для каждой копии, не возможно закрыть атаку фильром браузера.
- 4) Малый вес, хорошая приживаемость в системе.
- 5) Бот "оборудован" анти-эвристикой.
- 6) Удобная и приятная панель управления, максимально оптимизированная для уменьшения нагрузки на свой сервер и бд. Имеет русский и английский интерфейс по выбору.
- 7) Автоапдейт. Боты обновляются до новой версии полностью автоматически.
- 8) Улучшенный, хитрый механизм прогрузки EXE с партнерских программ, сводящий к минимуму риск блокировки аккаунта.

Так же присутствуют все стандартные "фишки" п/о подобного класса - выбор типа атаки, загрузка и запуск EXE и прочее...

Из личной статистики:
30 ботов загружают форум средней посещаемости. Да, всего 30...
300 ботов - средний сайт.
1000 ботов - крупный сайт.
5000 кластер с сайтом, даже при использовании анти ддос, блокировки и прочих приблуд.
15-20 тысяч ботов, теоретически могут урботать "вконтакте.ру"

100 Threads, No timeouts. 1000 bots take down a big website.

Evolution of botnets



Evidence: backconnect implementation

Просмотр полной версии : [RadmTroj, приватный троян, продаю](#) PDA

Exebilis 03.04.2006, 01:56

Продаю трояна, сделан мною, сборка каждому персонализированная
Что делает:

- 1) Ставит радмина на машину
- 2) Приводит файры(большую их часть) в режим молчания и нереагирования ни на что
- 3) Рапортует вам на мыло о себе, прилагая результат выполнения ipconfig(информация об ип адресе машины) и systeminfo(и общая инфа о железе и ОС) на машине, можно добавить желаемые вами команды
- 4) Вырубает нафиг все антивири, для того чтобы вы туда могли залить туда любые палящиеся трояны(например пинча)

Пункты 2-4 опциональны, тойсть любой из них могу отключить.
Естественно антивири молчат на него абсолютно, в процессах висит под именем svhost.exe, вешается на любой порт который пожелает заказчик.
1 бесплатный апдэйт на случай если антивири начнут его палить гарантирую.
Иконку делаю любой, по желанию покупателя могу склеить с любым другим exe файлом покупателя
Для тех кто не знает что такое радмин - прога позволяющая контролировать машину удаленно, имеет несколько режимов, полноэкранный контроль, по типу своей мышкой клавиой контролировать его экран, просмотр экрана онлайн, удаленная консоль, передача файлов(заливка туда чеголибо, и скачивание оттуда чеголибо)
Цена 16 WMZ
ICQ 20000-22-02

З.Ы. Вопросы плиз сюда [Только зарегистрированные пользователи могут видеть ссылки.]

K1PI 03.04.2006, 06:25

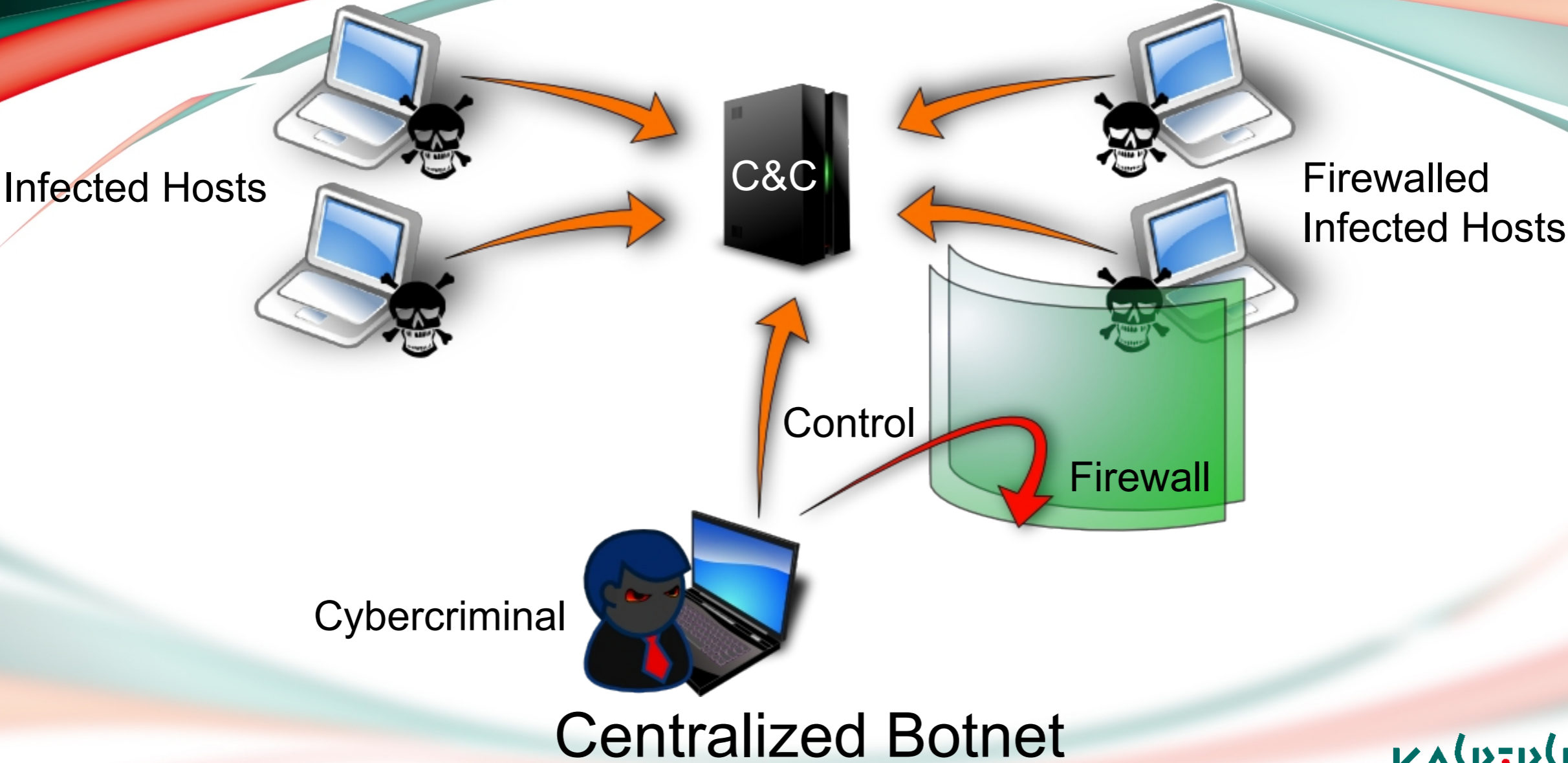
То, что он заливает РАдмина, конечно хорошо. Но если человек сидит за NAT'ом, то от РАдмина толко будет никакого

Exebilis 03.04.2006, 15:13

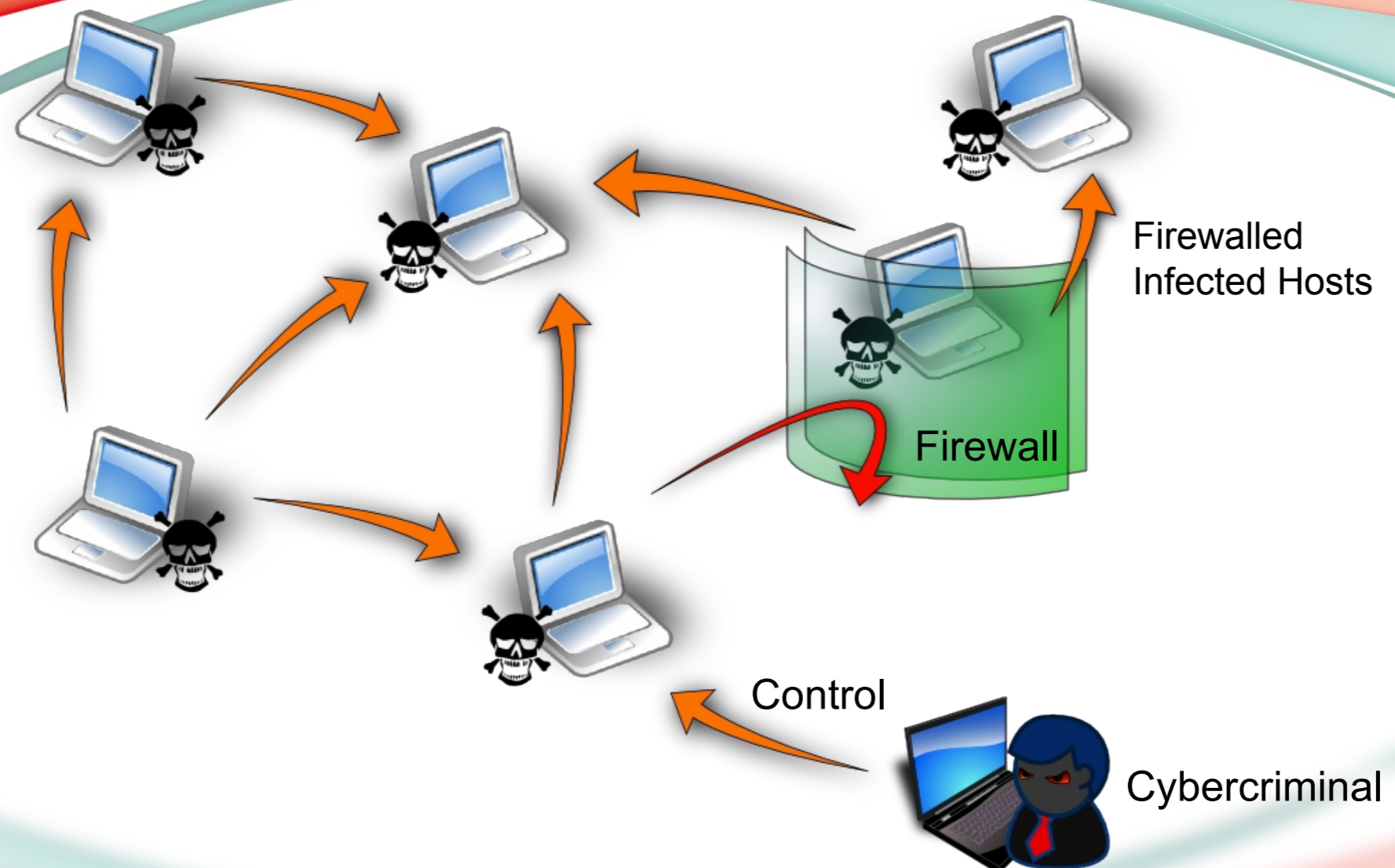
пораскинул мозгами - теперь к трояну еще опциональная возможность - бэкконнект бэктор => На цену не влияет

Updated: now the bot has “backconnect” feature and it's free of charge!

Evolution of botnets

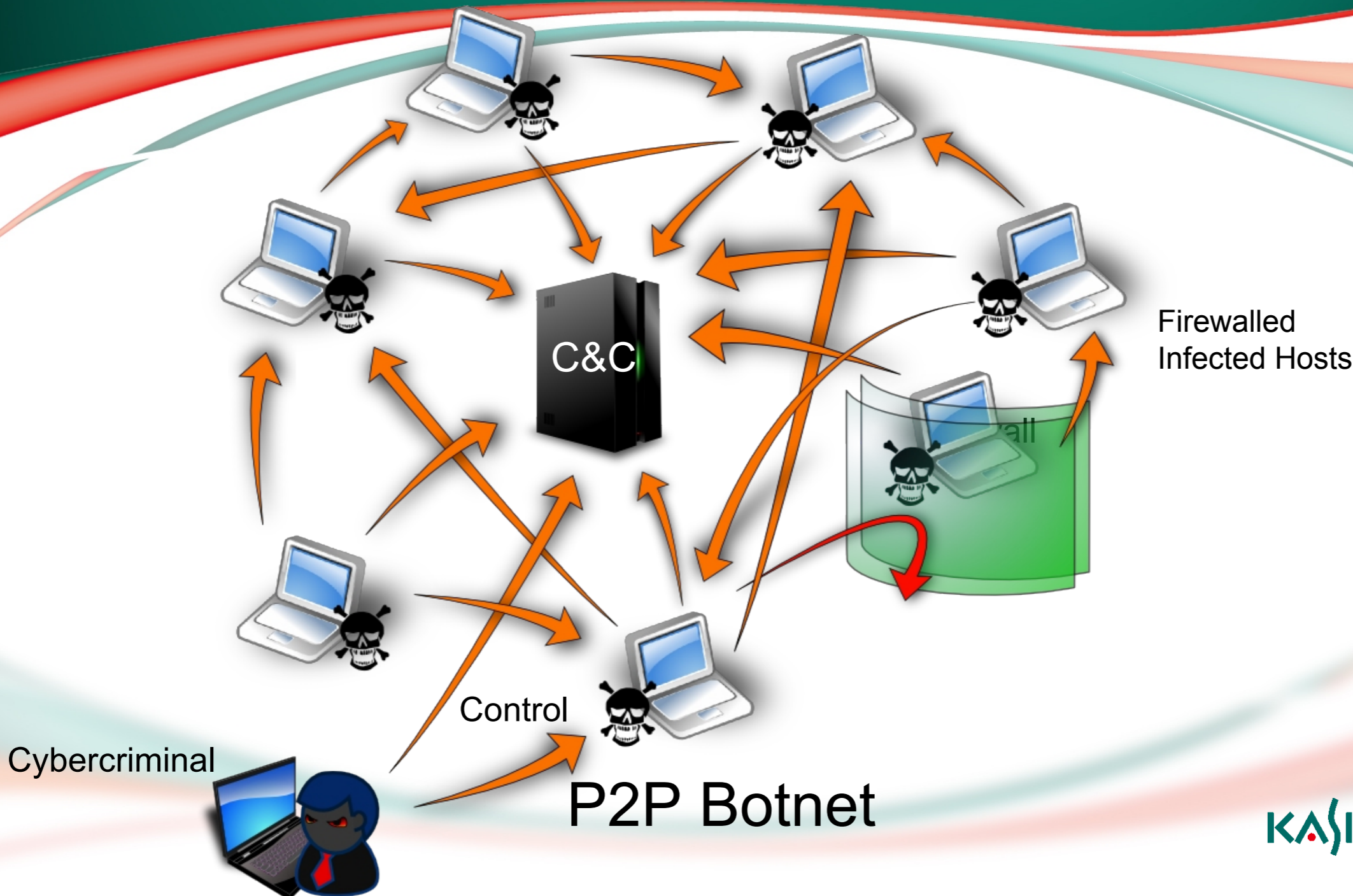


Evolution of botnets



Headless P2P Botnet

Evolution of botnets



More evidence: protectors/packers

| Автор | Сообщение |
|---|--|
| <p data-bbox="452 571 644 643">stosd (Рейтинг: 1)</p>  <p data-bbox="441 890 655 956">личность не установлена</p> | <p data-bbox="762 575 1264 609">Добавлено: 21:33, 11.12.2008 цитата</p> <p data-bbox="762 659 880 693">Прайс:</p> <p data-bbox="762 709 861 743">Зевсы</p> <ul data-bbox="762 760 1105 840" style="list-style-type: none">- первый крипт 50\$- последующие 40\$ <p data-bbox="762 857 1045 891">Прочая малварь</p> <ul data-bbox="762 908 861 942" style="list-style-type: none">- 10\$. <p data-bbox="762 959 1127 993">Обращаться [redacted]</p> |

Zeus protection costs 50\$ for the first time, 40\$ after. Others - 10\$.

More evidence: protected

Features:

- antiemulator NOD32
- antiemulator OneCare
- bypass NOD32 generic
- bypass Ikarus generic
- bypass BitDefender heur
- bypass Kaspersky heur
- bypass DrWeb signatures

...

09.09.2009, 14:52

demien

-- Уровень: 0 --



demien вне форума

Регистрация: 24.09.2006

Сообщений: 0

Репутация: 0

Приватный криптор exe файлов - demEnergy

demEnergy v3.0.2

Автор: demien

icq: 414-8888-18

сайт: [Для просмотра данной ссылки нужно [зарегистрироваться](#)]

нововведения (3.0.2):

[+] размер не пакованного стаба ~ 24 кб (может криптовать файлы упакованные urx, rescompact, mew [опционально])

[+] работа в OS: **WinNT/XP, WinVista/Win7.**

// возможность работы с иконками и версией файла (**dEFW**)

[+] возможность клонировать версию (versioninfo) файлы в криптуемый файл (clone fileinfo)

[+] возможность выдрать иконку из exe файла и вставить в криптуемый файл

[+] возможность очистить версию (versioninfo) файла (**null peinfo**)

[+] возможность очистить иконку файла (**null icon(s)**)

// работоспособность... (не используются сторонние программы!)

[+] криптор работает с любыми 32bit exe файлов (**UPX 1.25-3.x, WinUpack, Pe-Compact, Mew**)

[+] добавлен антиэмулятор ESET NOD32 (no more fucking TRJ/Injector.xx)

[+] добавлен антиэмулятор Microsoft OneCare (Обходит OneCare... 😊)

// детекты...

[+] наконец... **обход детекта Avira Trj.Dropper.Gen new**

[+] обход детекта NOD32 Trj.Injector new <

[+] обход детекта Ikarus T3 и a-squared (**trj.Buzus.xx new**)

[+] обход эвристики BitDefender

[+] обход эвристики Kaspersky AV (обход **Trj.HEUR.Genetic**)

[+] обход сигнатурного анализа DrWeb (trj.Packed и т.д. регулярно убирается детект)

[+] изменен алгоритм крипования (используется библиотека **advapi32.dll new**)

// функции...

[+] выходной крипованный файл имеет **правильный PE заголовок**

[+] **индивидуальная сигнатура** каждому клиенту (для крипта и для криптора!)

[+] немного изменен диз (отображается размер файла до\после криповки) 😊

[+] еще что-то... 😊

внешний вид:

[Для просмотра данной ссылки нужно [зарегистрироваться](#)]

проверка:

[Для просмотра данной ссылки нужно [зарегистрироваться](#)] (FUD 100%) [0/26]

условия продажи:[*] Запрещается перепродажа криптора или крипта на заказ третьим лицам![*] Оплата товара осуществляется на virustotal и подобных сервисах проверки.

цена:

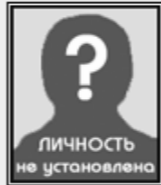



криптор с приватной сигнатурой - 55 wnz (цену не меняю! 😊)

More evidence: exploit packs


Features:


- detailed stats: country/browser/OS/...
- iframe encryptor
- file upload via C&C
- no MySQL dependency
- double access restriction
- switch for exploits crashing browsers
- unique signatures for clients

...

| Автор | Сообщение |
|---|--|
| RealNeo (Рейтинг: 11) | Добавлено: 14:10, 09.12.2008 цитата |
|  | ----- Neon (exploit system) 1.0.2 ru ----- |
|  | --- Описание --- |
| Тут с 06.03.2007 | [01] Ведение статистики по продавцам трафика, а именно, сколько было отгружено трафа, для того, чтобы убедиться в честности продавца, в тех случаях, когда траф идет с разных источников. Для каждого создается уникальный линк для полива трафика; |
|  | [02] Удобный графический дизайн; |
| | [03] Отображает как пробив по MSIE, так и по общему трафику; |
| | [04] Встроенный криптофреймворк; |
| | [05] Возможность отключать эксплоиты роняющие браузер; |
| | [06] Возможность загрузки файла прямо с админки; |
| | [07] Блокировка повторного захода; |
| | [08] Минимальная нагрузка на сервер; |
| | [09] Простота установки; |
| | [10] Не требует БД MySQL; |
| | [11] Статистика по системам; |
| | [12] Статистика по браузерам; |
| | [13] Статистика по рефералам; |
| | [14] Статистика по зараженным IP; |
| | [15] Статистика по странам; |
| | [16] Автоматически находит путь до себя; |
| | [17] Каждому клиенту индивидуальная сигнатура; |
| | Включенные в связку сплоиты: MDAC - эксплоит бьющий старенькие IE, но еще дающий хороший %; |
| | PDF эксплоит - уникальный эксплоит бьющий все браузеры при условии установленного adobe reader. Состоит из двух уязвимостей Collab.collectEmailInfo и Util.printf (новый); |
| | Snapshot (Office) - эксплоит бьющий MSIE 6 и MSIE 7 с запуском (не пишется в автозагрузку, а сразу запускается); |
| | Flash - отличный эксплоит, пробивает все браузеры при наличии установленного Macromedia Flash 9 или более раннего; |
| | BOF - связка Buffer Overflow эксплоитов. Добавлены только самые актуальные на данный момент и дающие небольшой прирост к пробиву; |
| | Связка будет постоянно совершенствоваться: добавление функционала, добавление новых эксплоитов (с хорошим показателем), улучшение крипто и т.п. При этом цена может возрасти, но никак не отразится на уже существующих клиентах. |
| | На данный момент цена связки составляет 400\$. ICQ  |

More evidence: abuse-proof hosting

UltraSecure  **Дата** Oct 20 2008, 20:33:52 [\[Цитировать\]](#)

Проверенный сервис 

Профиль
Группа: Rise Sellers
Сообщений: 207
Зарегился: 11-July 05
Проживает: CN

Рейтинг:
< -5 (1) 5 >

Наш сервис предоставляет вам услуги регистрации **Абузоустойчивых доменов**.


Уже достаточно продолжительное время мы регистрируем домены под:

- DNS
- Pharma
- Spam (редиректы и основные домены, недорогие варианты под массовую регистрацию и надежные штучные экземпляры)
- Scam
- Phishing (от мелких биллингов до интернет-банков)
- Дроп-проекты
- Трояны в любом виде (в т.ч. антивирусы, кодеки и др.)
- Ботнеты
- etc.

Словом, тематика ваших проектов может быть почти любой (исключение: Child porn).

“Registering domains for Spam, Phishing, Scam, Trojans, Botnets...”

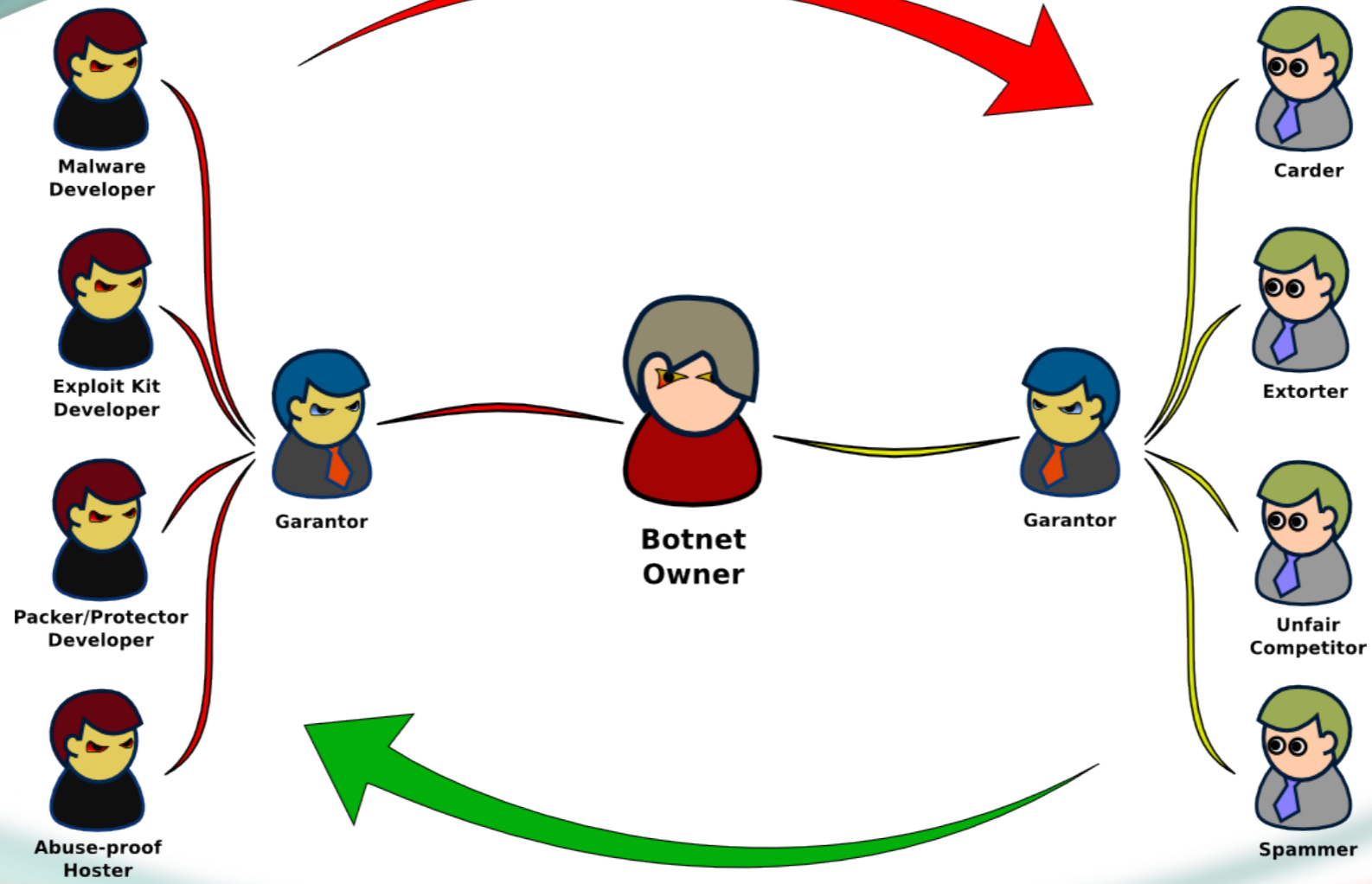
More evidence: abuse-proof hosting

| | Тема | Форум | Автор | Ответов | Просмотров | Обновление |
|---|--|--|---------------------------------|---------|------------|---|
|  |  АБУЗОУСТОЙЧИВЫЕ СЕРВЕРА, VDS/VPS, ХОСТИНГ и ДОМЕНЫ (Страниц 1 2 3) BulletProof Service #1. | Покупка/Продажа/Работа | RoyalHost | 44 | 12583 | Dec 14 2008, 13:59:48 Автор: void3r |
|  |  ABUSE'IMMUNITY HOSTING SERVICE (Страниц 1 2 3 ...6) Сервера Хостинг Домены | Покупка/Продажа/Работа | Sollhost | 89 | 5639 | Dec 12 2008, 00:58:33 Автор: Sollhost |
|  |  Абузоустойчивый хостинг сервис. Нет альтернативы Bulletproof Hosting Service | Покупка/Продажа/Работа | VeX | 6 | 577 | Dec 11 2008, 21:10:14 Автор: VeX |
|  |  Абузоустойчивые домены Bulletproof Domains | Покупка/Продажа/Работа | UltraSecure | 4 | 475 | Dec 9 2008, 03:05:52 Автор: UltraSecure |
|  |  Хостинг и серверы под "что угодно" (Страниц 1 2 3 ...5) Качественный хостинг для вашей работы | Покупка/Продажа/Работа | ...CyberHost... | 62 | 4929 | Nov 27 2008, 00:43:16 Автор: ...CyberHost... |
|  |  PPTP & OpenVPN Service (Страниц 1 2 3 ...5) | Покупка/Продажа/Работа | secreTSlime | 68 | 5734 | Nov 27 2008, 00:25:42 Автор: secreTSlime |
|  |  Professional bulletproof service from AbdAllah(VN) (Страниц 1 2 3 ...41) 5 лет в деле | Покупка/Продажа/Работа | Abdullah | 613 | 33272 | Nov 24 2008, 14:38:01 Автор: Abdullah |
|  |  OpenVPN сервис в собственном ДЦ в европе (Страниц 1 2) OpenVPN сервис в собственном ДЦ в европе | Покупка/Продажа/Работа | ovpn lux | 28 | 594 | Nov 21 2008, 16:21:33 Автор: ovpn lux |
|  |  VPS/VDS from AbdAllah - грандиозный проект (Страниц 1 2 3) NEW SERVICE !!! | Покупка/Продажа/Работа | Abdullah | 35 | 3272 | Oct 6 2008, 21:00:57 Автор: erafl4me |

All kinds of hostings for ANY projects

Self-supporting system

SERVICES

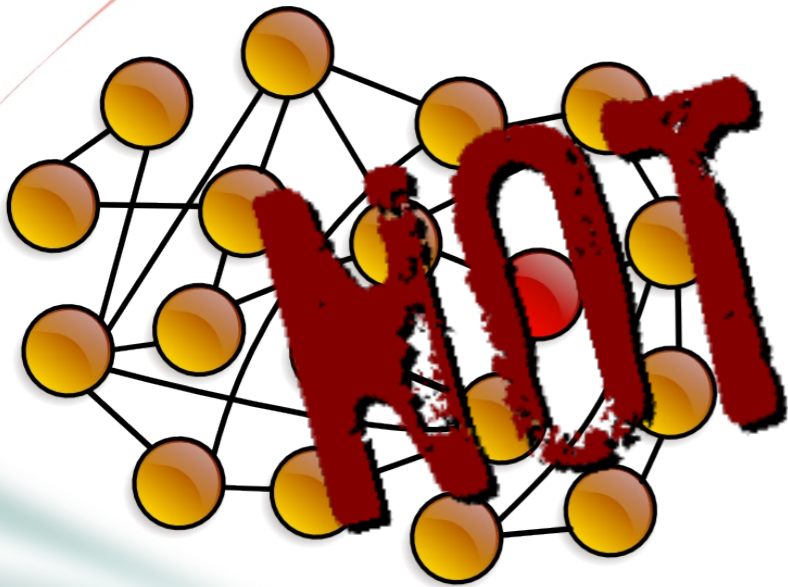


MONEY

What could change the landscape

Conficker/Kido Poisoning

Conficker P2P Botnet



Poisoned P2P

Facts:

- ~7,000,000 infected hosts
- Over 100 countries infected
- Obfuscated code
- Multiple encryption
- Digital signature of updates
- Distributed P2P control
- Self-replication
- Network exploit
- Still online

What could change the landscape

Gumblar

Backdoor self-removal

Gumblar
Backdoor

NOT

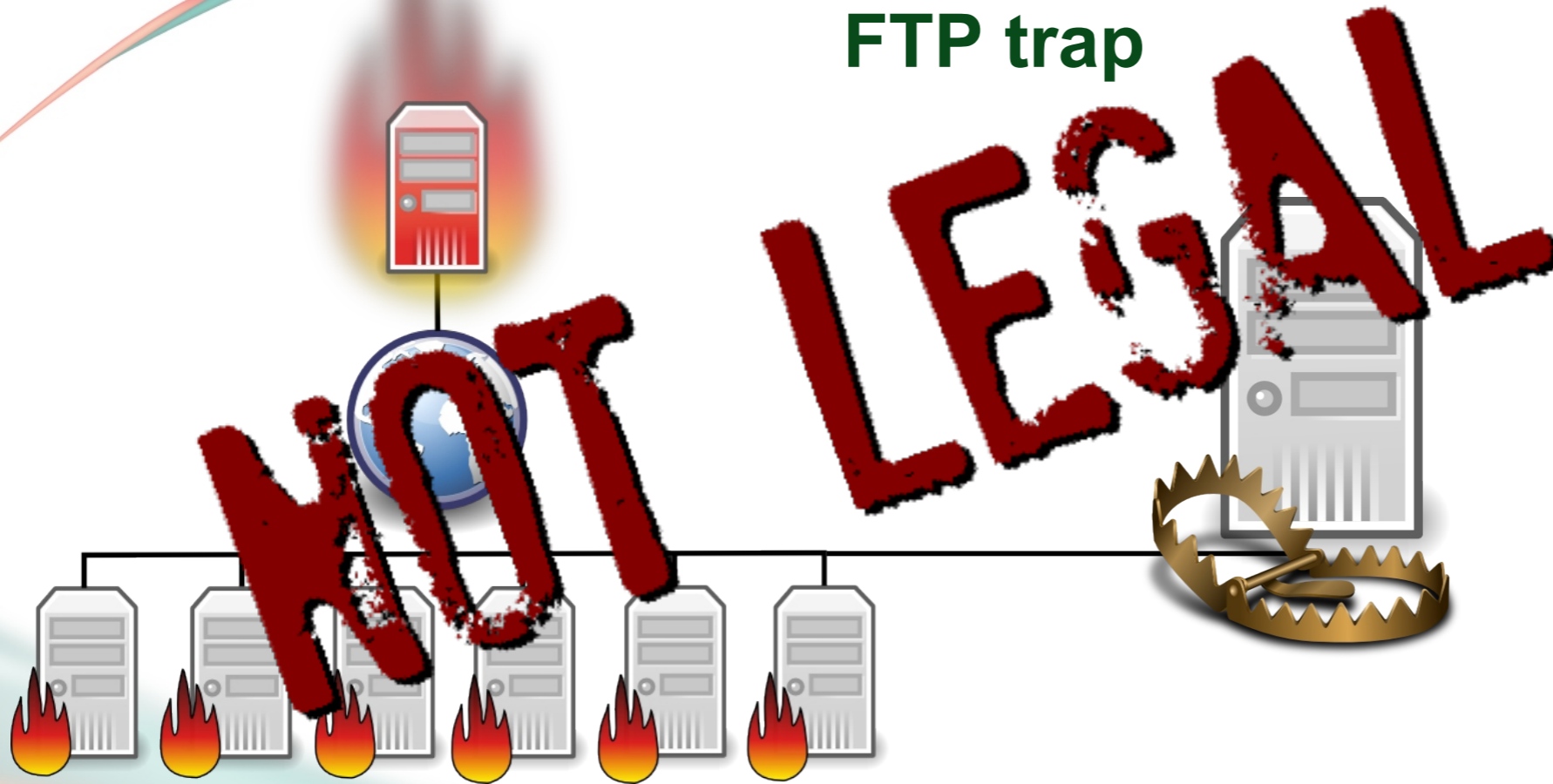


Gumblar
Backdoor

LEGAL

Pegel/Gumblar/...

FTP trap



Facts:

1. Most of infections are coming from the WWW
2. The highest number of infections is possible due to injection of malicious script on legitimate website
3. Injection in most of cases is done by using FTP spiders

Logo of our team



Logo of our team



Dream



Reality



Thank you!

Vitaly Kamluk
Chief Security Expert
Kaspersky Labs Japan

