Исследование вредоносных программ с точки зрения расследования инцидентов

Александр Матросов
Руководитель Центра вирусных исследований и аналитики

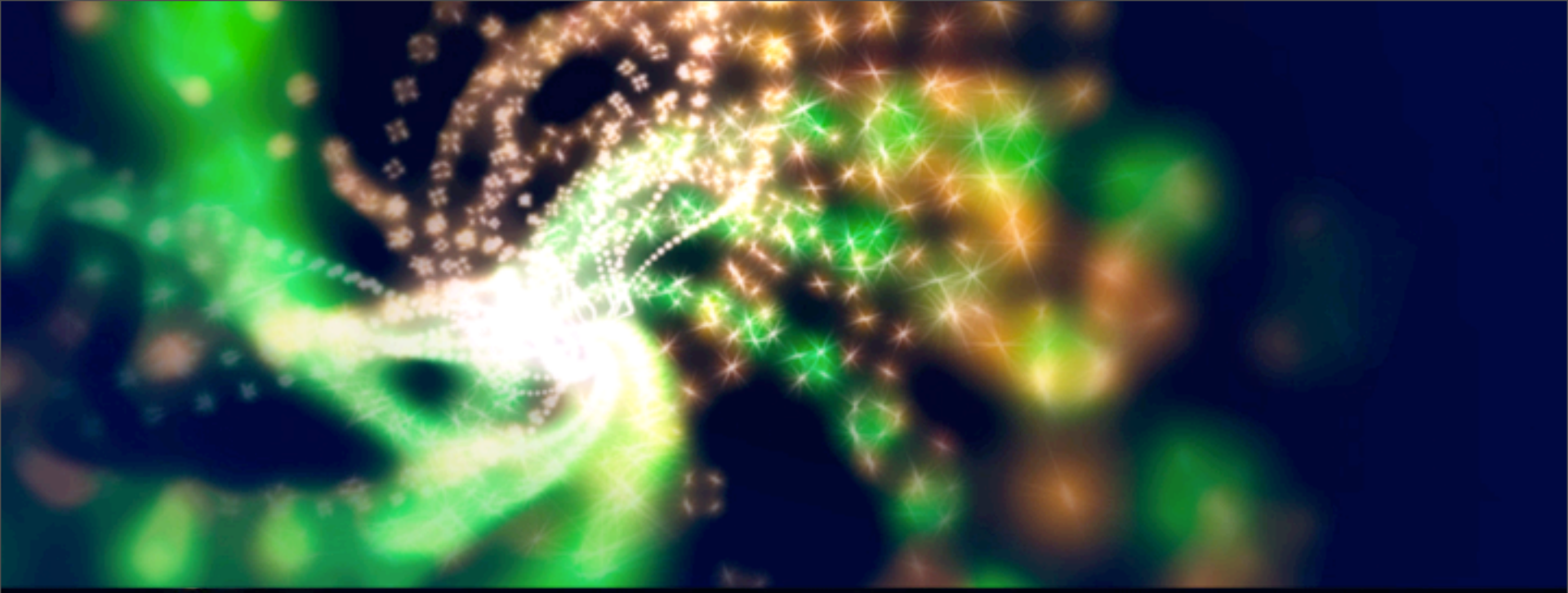
План доклада

★ Какие бывают атаки с использованием вредоносных программ?

★ Распространение вредоносных программ по схеме Pay-Per-Install (PPI)

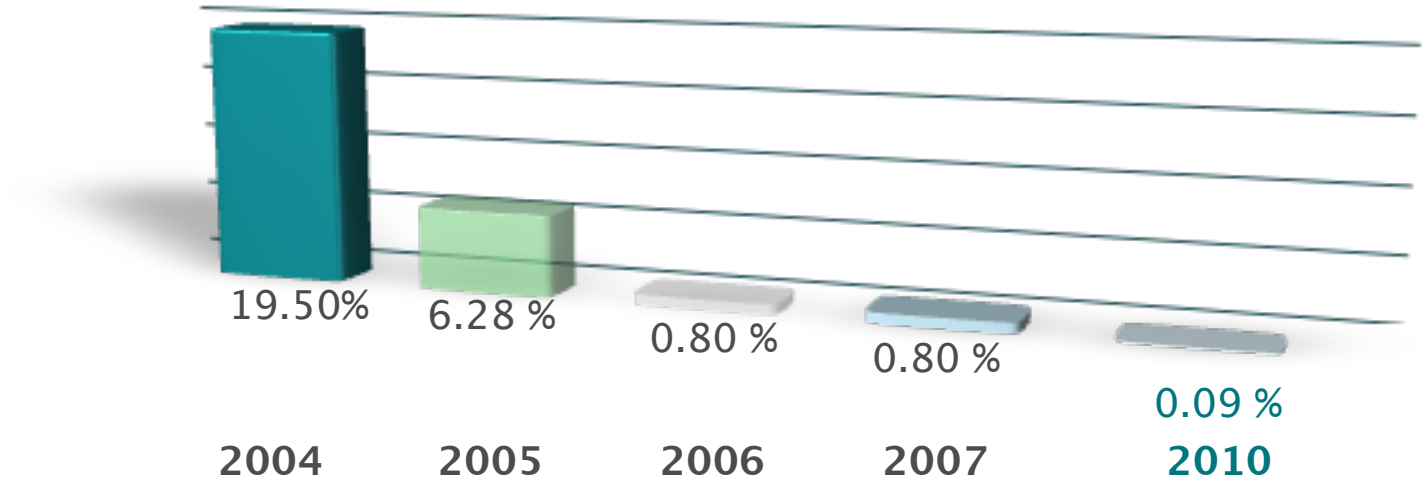
★ Почему антивирусным компаниям проще расследовать инциденты с участием вредоносных программ?

Киберпреступность – это криминальный бизнес



Мы обрабатываем 300,000 уникальных сэмплов в день

Вредоносные программы создаются для извлечения финансовой выгоды



Начиная с 2004 года идет резкий спад количества вредоносных программ разработанных не с целью извлечения финансовой выгоды. На данный момент их процентное соотношение, относительно общего потока, составляет менее одного процента.


Атаки с использованием вредоносного ПО
Случайные
Целенаправленные

Какая информация важна для расследования?

★ Какие цели преследовали злоумышленники

★ Какая информация могла быть похищена

★ Каким образом украденная информация была передана злоумышленникам

★ Есть ли постоянный обмен информацией между вредоносной программой и злоумышленниками

★ Каким образом происходит информационный обмен и каким конкретно образом она передается

Распространение вредоносных по схеме Pay-Per-Install (PPI)

Pay-Per-Install (PPI) – это способ распространения ПО, когда оплачивается каждая инсталляция владельцу ресурса с которого установленная программа была загружена

Dogma Millions - Вы уже не ждали?! А они вернулись с новым взрывным решением!

Рад Вам представить, а я действительно ОЧЕНЬ РАД это сделать - **DogmaMillions.com**

Считаю, не нужно долго расписывать, чтобы понять - DOGMA вернулась! Она снова будет радовать Вас конвертом и звоном заработанных денег в ВАШИХ кошельках.
Да, Вы правильно поняли - это та самая команда, которая взорвала нишу софта своим конвертом в прошлом году и при закрытии, в отличии от многих других софт партнерок, вовремя выплатила всё своим адвертам до единого цента!

Итак, что же предлагается в этот раз?! Новый антивирус?! Нет, подмена выдачи!
Это подмена которая даёт выхлоп не хуже, чем на софте и даже лучше! При чистом траффе, без примесей других exe, в среднем выходит 500 у.е. с 1к US инсталлов. При тестах, у людей с хорошим траффом доходило до 700-800 у.е., а в некоторых случаях до 1000 у.е. с 1к инсталлов. Также хочу отметить, что 500-700-2К-N денег у Вас в статистике не появится на следующий день после слития N-го кол-ва инсталлов, т.к. деньги зарабатываются на кликах в течении двух-трех недель равномерно. Но сказанное не означает, что по прошествии этого времени слитые инсталлы перестанут приносить прибыль! Они ещё будут долго увеличивать Ваше благосостояние!

За счет чего достигается такой выхлоп:
- низкой агрессией, в результате чего достигается долгоживучесть
- широким набором фид-провайдеров
- хорошо проработанной схемой снижающей риск обнаружения

Вам выдается exe, который можете загружать как угодно! Будь то: ботнеты, ваше промо, ломаные ресурсы, эксплоиты и т.д. Полёт фантазии не ограничен:)

Exe криптуется на лету! После регистрации сможете сами проверить, что каждый раз при скачивании его с админки, он будет иметь разный размер:)

Также хочу отметить, что Dogma Millions *идеально* подходит как дополнительный заработок, а именно - exe хорошо подгружать с AB и другими решениями.:)

Выплаты 2 раза в месяц без холда.

Подведу черту под всем написанным.
Многие уже не один раз теряли «последнюю выплату» исчисляющуюся десятками К долларов. И многие понимают, что главное надежность и стабильность, а если к этому добавить ещё отличный конверт, который в 1.5-2 раза лучше других аналогичных решений на рынке, то Вы получите - Dogma Millions!


DOGMA MILLIONS
Главная
Регистрация
FAQ
Топ10
Саппорт
ru
Vpodpolie
Присоединяйся СЕЙЧАС!
Логин
Пароль
помнить меня
забыли пароль?
Войти
60-70%
От дохода
3-5%
С рефералов
Наши преимущества
- Лучший выхлоп среди аналогичных решений
- Стабильные выплаты
- Надежность сотрудничества
- Индивидуальный подход
- Дружественный саппорт
- Активное совершенствование конвертации
Дополнительная информация
Успешно конвертируем следующие страны: US, CA, AU, GB, DE, FR. Увеличена долгосрочность работы и выхлоп с каждого инсталла. Мы готовы предложить индивидуальные рейты и условия оплаты постоянным партнерам. Вы можете использовать собственные лендинги для слива веб траффика.
Стандартные условия
Вы получаете 60% от общего дохода с инсталлов.
Вы получаете 3% от дохода привлеченных Вами мастеров.
Стабильные выплаты 2 раза в месяц, 1-го и 16-го числа.
Большой выбор способов оплаты - WebMoney, Epese, Банковский перевод, Egassport, PayPal и
Новости
29-03-2010
Пересчет статы
Уважаемые партнёры! Для улучшения качества работы партнёрки, проводится техническое переоснащение текущих серверов, а так же добавление новых. В следствии этого некоторое время возможна разбежность баланса с текущим заработком. Данная погрешность будет ликвидирована по окончанию технических работ. Ожидаемый срок завершения до 1.04.2010
20-01-2010
возросшие инсталы
В данный момент так как мы исправили проблему отстука к нам возвращается часть старых инсталов и поэтому, если вы видите что у вас прибавились инсталы сверх нормы - это доходят старые сделанные вами когдато инсталы.


DOGMA MILLIONS
Статистика
Новости
Саб-аккаунты
Промо
Профиль
Настройки выплат
История выплат
Рефералы
ru
Добро пожаловать
Время сервера:
Имя:
Последнее IP:
Дата логина:
Аккаунт
Прибыль за сегодня: $ 0.73
Прибыль за месяц: $ 15.78
Баланс: $ 15.78
Всего выплачено: $ 54.91
Менеджер аккаунта
Ваш менеджер:
Icq:
Icq:
Email:
Выйти
Новости:
28.12.2009
Обновление модуля
Сделали критические доработки в exe и обновили криптор. Обязательно заберите новую версию и пожалуйста отпишите в саппорт о результатах.
10.12.2009
Teen Adult лендинг
По вашим просьбам открыли teen adult лендинг.
17.11.2009
Внимание!
Уважаемые адверты! Убедительноая просьба: не тестируйте модуль на бесплатных публичных тестерах, они предназначенны для того, чтобы собирать информацию о вредоносных программах и соответственно обнаруживать их. Тестируя билд на вирустотале, к примеру, вы ускоряете его запал и делаете себе же хуже.
Спасибо за внимание.
06.11.2009
Свежий модуль - залог здоровья:)
Уважаемые адверты! Обязательно каждый день забирайте новый модуль, это решит множество проблем связанных с запалом и прочими глюками, которые могут выскочить. Не грузите \\\"вчерашний\\\" модуль! Пользуйтесь только свежим:)
05.11.2009

Дата	Уники (промо)	Клики (промо)	Инсталлы	Сёрчи	Клики	Ратио(u/i)	Средний Бид	Ратио(u/$)	Заработок с рефералов	Заработок
2009-10-23	0	0	0	575	62	0	$0.0292	$0.00	$0.00	$1.81
2009-10-22	0	0	2	13928	823	0	$0.0282	$0.00	$0.00	$23.22
2009-10-21	0	0	0	15752	975	0	$0.0286	$0.00	$0.00	$27.89
2009-10-20	0	0	0	16121	1029	0	$0.0321	$0.00	$0.00	$33.04
2009-10-19	0	0	2	16120	1121	0	$0.0321	$0.00	$0.00	$36
2009-10-18	0	0	6	16719	1197	0	$0.0243	$0.00	$0.00	$29.03
2009-10-17	0	0	41	16259	1201	0	$0.0319	$0.00	$0.00	$38.37
2009-10-16	0	0	8	16525	1264	0	$0.0296	$0.00	$0.00	$37.39
2009-10-15	0	0	237	19559	1324	0	$0.0343	$0.00	$0.00	$45.45
2009-10-14	0	0	514	18385	1273	0	$0.0355	$0.00	$0.00	$45.14
2009-10-13	0	0	315	19847	1376	0	$0.0329	$0.00	$0.00	$45.33
2009-10-12	0	0	17	22260	1602	0	$0.0328	$0.00	$0.00	$52.59
2009-10-11	0	0	165	22545	1466	0	$0.0341	$0.00	$0.00	$50.06
2009-10-10	0	0	416	24576	1631	0	$0.0343	$0.00	$0.00	$55.89
2009-10-09	0	0	621	24345	1637	0	$0.0322	$0.00	$0.00	$52.76
2009-10-08	0	0	750	23742	1525	0	$0.0336	$0.00	$0.00	$51.18
2009-10-07	0	0	261	24240	1430	0	$0.0351	$0.00	$0.00	$50.25
2009-10-06	0	0	203	24492	1540	0	$0.035	$0.00	$0.00	$53.93
2009-10-05	0	0	290	25984	1613	0	$0.035	$0.00	$0.00	$56.48
2009-10-04	0	0	590	25190	1628	0	$0.0346	$0.00	$0.00	$56.39
2009-10-03	0	0	547	18579	1194	0	$0.0369	$0.00	$0.00	$44.02
2009-10-02	0	0	430	14924	1014	0	$0.0358	$0.00	$0.00	$36.27
2009-10-01	0	0	136	13868	890	0	$0.0353	$0.00	$0.00	$31.42
2009-09-30	0	0	350	12548	838	0	$0.0373	$0.00	$0.00	$31.26
2009-09-29	0	0	45	10877	762	0	$0.0402	$0.00	$0.00	$30.61
2009-09-28	0	0	20	13575	977	0	$0.04	$0.00	$0.00	$39.09
2009-09-27	0	0	44	16398	1157	0	$0.0358	$0.00	$0.00	$41.39
2009-09-26	0	0	707	15312	1257	0	$0.0361	$0.00	$0.00	$45.39
2009-09-25	0	0	753	6457	462	0	$0.0395	$0.00	$0.00	$18.26
2009-09-24	0	0	305	2339	155	0	$0.0492	$0.00	$0.00	$7.63
2009-09-23	0	0	5	743	65	0	$0.0286	$0.00	$0.00	$1.86

Faq

Сколько я буду получать?

- При стандартных условиях Вы будете получать 60% от общего объема доходов с инсталлов.

Есть ли у вас минималка?

- Нет.

В какие системы вы платите?

- WebMoney, Epass, Wire Transfer, Paypal, Epese. О возможности оплаты в другие системы можно получить информацию у саппорта.

Как часто у вас выплаты?

- Два раза в месяц, 1-го и 16-го числа.

Есть ли у вас холд?

- На данный момент холд не предусмотрен.

Как получить инвайт?

- Обратиться в саппорт и постараться предоставить исчерпывающую информацию о источнике Ваших инсталлов и, по возможности, о себе.

Какой траффик вы принимаете?

- О возможности работы с Вашим траффом уточняйте в саппорте.

Делаете ли вы епас?

- Да, делаем.

Партнёрская программа «Earning4u» - самый простой путь заработать.
Для того чтобы начать работать с нами, Вам необходимо просто зарегистрироваться.

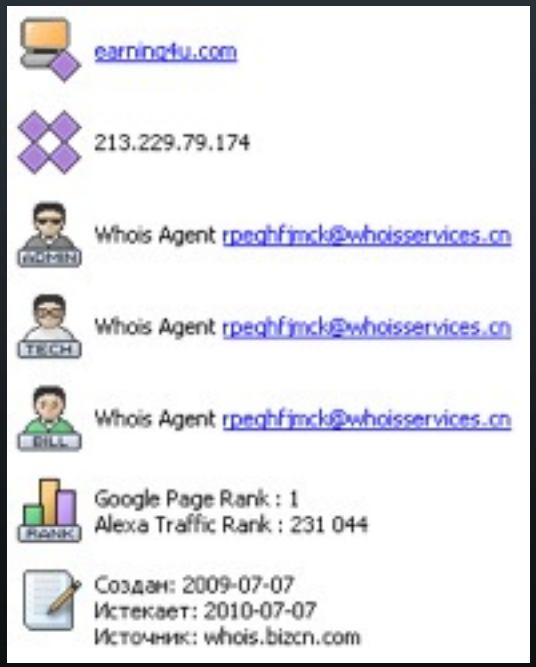
Вы зарабатываете **от 6$**(Азия) **до 180$**(USA) за 1000 инсталлов. Все цены можете посмотреть в разделе «Тарифы».

Наши Тарифы

Страна:	Цена $ за 1000 загрузок:
United States	180
United Kingdom	110
Netherlands	30
France	30
Poland	20
Italy	65
Germany	30
Spain	30
Australia	55
Greece	30
Other	20
Asia	6

* Мы также оставляем за собой право удалять любой аккаунт
* И помните – любой СПАМ запрещен!

Куда ведут домены?



Способ учета трафика и инсталяций

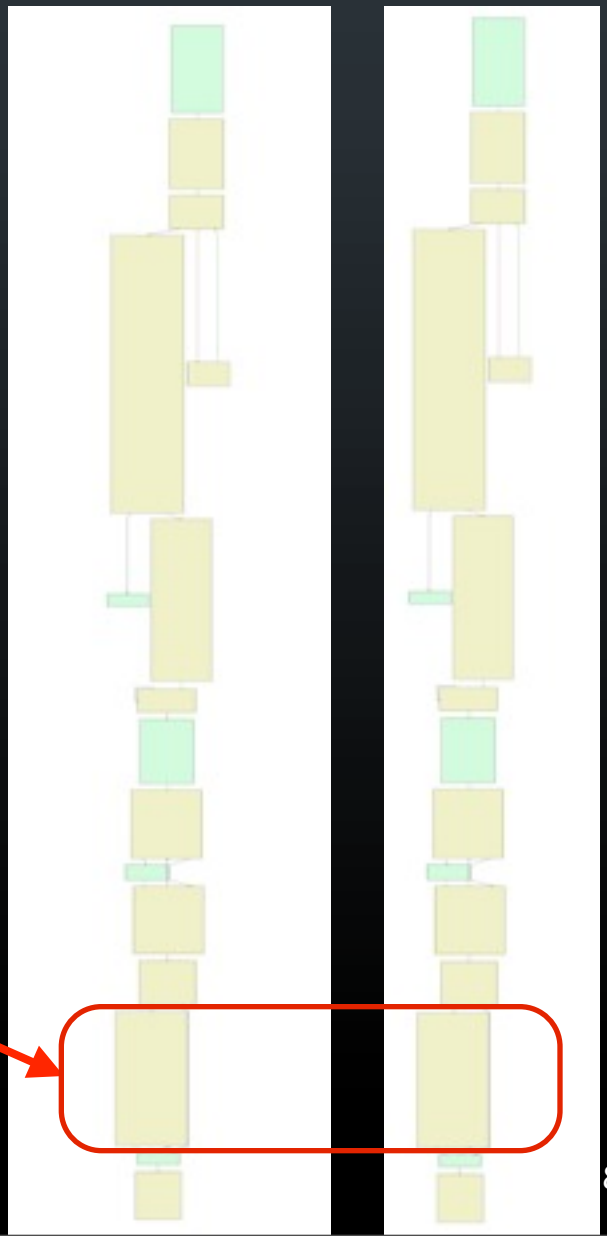
http://dogmamillions.com/download.html?
login=b0bah&**key=**2b15ea4e5eb2bbd734081c051a14

a variant of Win32/Kryptik.BQU (TDSS v3)

1) **MD5:** b7d1de5c6dc87092af22972e8bc30f65

2) **MD5:** b0caaa71835de2c725c150e03f40e492

```
xor     ecx, ecx
push    ecx
lea     ecx, [eax+1]
pop     ecx
mov     cl, [esp+edx+18h+var_18]
push    ecx
lea     ecx, [eax+1]
pop     ecx
mov     ch, [edi]
push    ecx
lea     ecx, [eax+1]
pop     ecx
xor     ch, cl
push    ecx
lea     ecx, [eax+1]
pop     ecx
mov     [edi], ch
push    ecx
lea     ecx, [eax+1]
pop     ecx
inc     edi
push    ecx
lea     ecx, [eax+1]
pop     ecx
```



```
00401534  movzx   edx,dl
00401537  push    ecx
00401538  lea     ecx,[eax+1]
0040153b  pop     ecx
0040153c  mov     esi,edx
0040153e  jmp     loc_401417
00401417  mov     bh,byte ptr[esp+esi+28h+var_14]
0040141b  jmp     loc_40154C
0040154c  mov     byte ptr[esp+eax+28h+var_14],bh
00401550  push    ecx
00401551  lea     ecx,[eax+1]
00401554  pop     ecx
00401555  mov     bh,cl
00401557  push    ecx
00401558  lea     ecx,[eax+1]
0040155b  pop     ecx
0040155c  xchg    eax,esi
0040155d  push    ecx
0040155e  lea     ecx,[eax+1]
00401561  pop     ecx
00401562  mov     byte ptr[esp+eax+28h+var_14],bh
00401566  push    ecx
00401567  lea     ecx,[eax+1]
0040156a  pop     ecx
0040156b  xchg    eax,esi
0040156c  push    ecx
0040156d  lea     ecx,[eax+1]
00401570  pop     ecx
00401571  mov     edx,[esp+eax+28h+var_14]
00401575  push    ecx
00401576  lea     ecx,[eax+1]
00401579  pop     ecx
0040157a  push    ecx
0040157b  add     [esp+2Ch+var_2C],edx
0040157e  pop     edx
0040157f  push    ecx
00401580  lea     ecx,[eax+1]
00401583  pop     ecx
00401584  movzx   edx,dl
00401587  jmp     loc_4010D8
004010d8  add     edx,14h
004010db  jmp     loc_401596
00401596  xor     ecx,ecx
00401598  push    ecx
00401599  lea     ecx,[eax+1]
0040159c  pop     ecx
0040159d  mov     cl,[esp+edx+18h+var_18]
004015a0  push    ecx
004015a1  lea     ecx,[eax+1]
004015a4  pop     ecx
004015a5  mov     ch,[edi]
004015a7  push    ecx
004015a8  lea     ecx,[eax+1]
004015ab  pop     ecx
004015ac  xor     ch,cl
004015ae  push    ecx
004015af  lea     ecx,[eax+1]
004015b2  pop     ecx
```

```
movzx   edx,dl
push    ecx
lea     ecx,[eax+1]
pop     ecx
mov     esi,edx
push    ecx
lea     ecx,[eax+1]
pop     ecx
mov     bh,byte ptr[esp+esi+144h+var_130]
push    ecx
lea     ecx,[eax+1]
pop     ecx
mov     byte ptr[esp+eax+144h+var_130],bh
jmp     loc_401244
mov     bh,cl
jmp     loc_401568
xchg    eax,esi
push    ecx
lea     ecx,[eax+1]
pop     ecx
mov     byte ptr[esp+eax+144h+var_130],bh
push    ecx
lea     ecx,[eax+1]
pop     ecx
xchg    eax,esi
push    ecx
lea     ecx,[eax+1]
pop     ecx
mov     edx,[esp+eax+144h+var_130]
push    ecx
lea     ecx,[eax+1]
pop     ecx
push    ecx
add     [esp+148h+var_148],edx
pop     edx
push    ecx
lea     ecx,[eax+1]
pop     ecx
movzx   edx,dl
jmp     loc_4012DF
add     edx,14h
jmp     loc_40159E
xor     ecx,ecx
push    ecx
lea     ecx,[eax+1]
pop     ecx
mov     cl,[esp+edx+144h+var_144]
push    ecx
lea     ecx,[eax+1]
pop     ecx
mov     ch,[edi]
push    ecx
lea     ecx,[eax+1]
pop     ecx
xor     ch,cl
push    ecx
lea     ecx,[eax+1]
pop     ecx
```


pxshadow
OFF
Gimme some bytes [MOD]
PXCrypter 1.1 Fully undetected (private) (was shadow crypter)
PXCrypter 1.1 Fully undetected
PXCrypter 1.1 build 231
Crypter
1.1
Input Filename:
Browse
Change Icon
Icon Filename:
Browse
Adv Settings
Anti Virtualization (Microsoft VPC,VMware,VirtualBox)
Anti Debug (Ollydbg,Soft-Ice,IDA,Generic Debuggers)
Anti SandBoxie/ThreatExpert
Anti SandBoxes (Norman,Anubis,CW,Generic Sandboxes)
Melt on exit
Start Hidden (Without GUI)
Try to Unpack the Executable before Crypting
UPX Packing Mode
Automatic (Recommended)
Overlay Detection/Processing
Automatic (Recommended)
Injection Target
Default Self (Recommended)
Delay
0
Seconds
Build
Private Version for Current Customers

Конфигурационный файл от установленного бота

[main]
quote = You people voted for Hubert Humphrey, and you killed Jesus
version = 3.26
subid = 0
installdate = 29.03.2.2010 18:44:7
builddate = 29.03.2010 14:25:24
[injector]
*=tdlcmd.dll
[tdlcmd]
servers = **https://d45648675.cn**/;https://d92378523.cn/;https://91.212.226.65/
wspservers = http://j00k877x.cc/;http://b11335599.cn/
popupservers = http://m3131313.cn/
version = 3.741

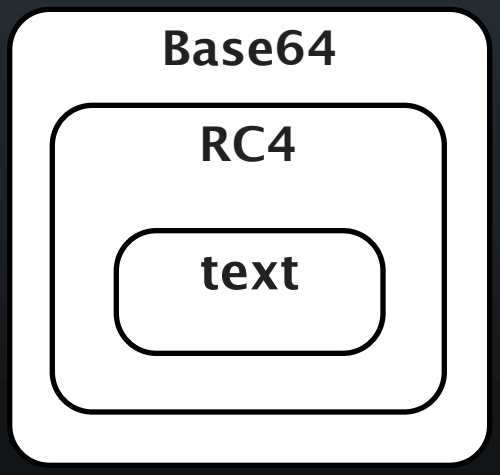
http://d45648675.cn/yPFerNxCiUwohhnNF1XPN7wCVLPrcxfMAEYo74O8FjWd57Vkd52hOMrIkrkf1fTjpxf9W8ISKJzBh8s7NAV4hy4=

http://m3131313.cn/shcJJbktZ5rjkqA/c2zqsMcZYkW+RDfopILj0TaL032JHpgmeQuo1z1PaKGwyxOtBq3HsJeJDHEmMwD5rgGxqPGqPvbtPsIe1eC6oFhT00ZI9P6VNSaEMlQjYojyiLu6CzdTR7ie8dzTUC1XegPoP10+g0UKVMeYJ/LY1HgkWYBGaIFF4kH5brf0i/qw/kWpjYpeuD+dm8C83PJCysvPrbc1wjoVGlhVS170+0oFQO8=

7b8f5d01-d790-453b-96af-c1c0b77abeb3|20375|0|1|6be|5.1 2600 SP2.0

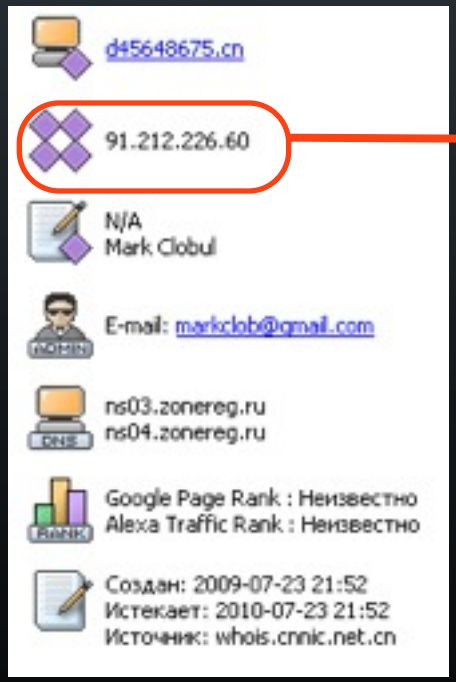
1.5|7b8f5d01-d790-453b-96af-c1c0b77abeb3
|20375|0|iastor.sys+download|http://www.mastercard.com/ru/personal/ru/
promotions/giftseason/promo_description.html|http://www.yandex.ru/

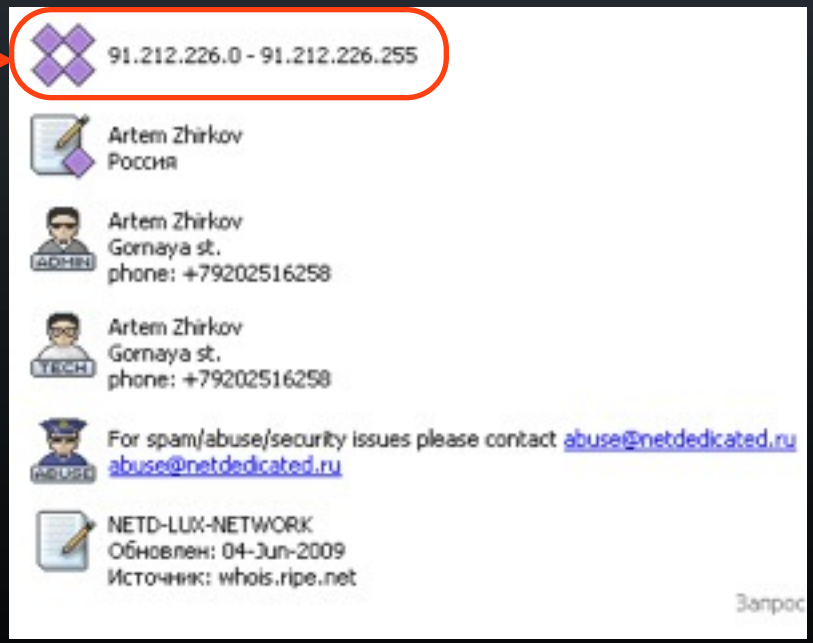
Алгоритм шифрования трафика




```
key = array.array("B", domain)
data = array.array("B", base64.standard_b64decode(param))
rc4(key, data)
```

Опять китайцы?






d45648675.cn
A
91.212.226.60
NET
91.212.226.0/24
AS
AS5577

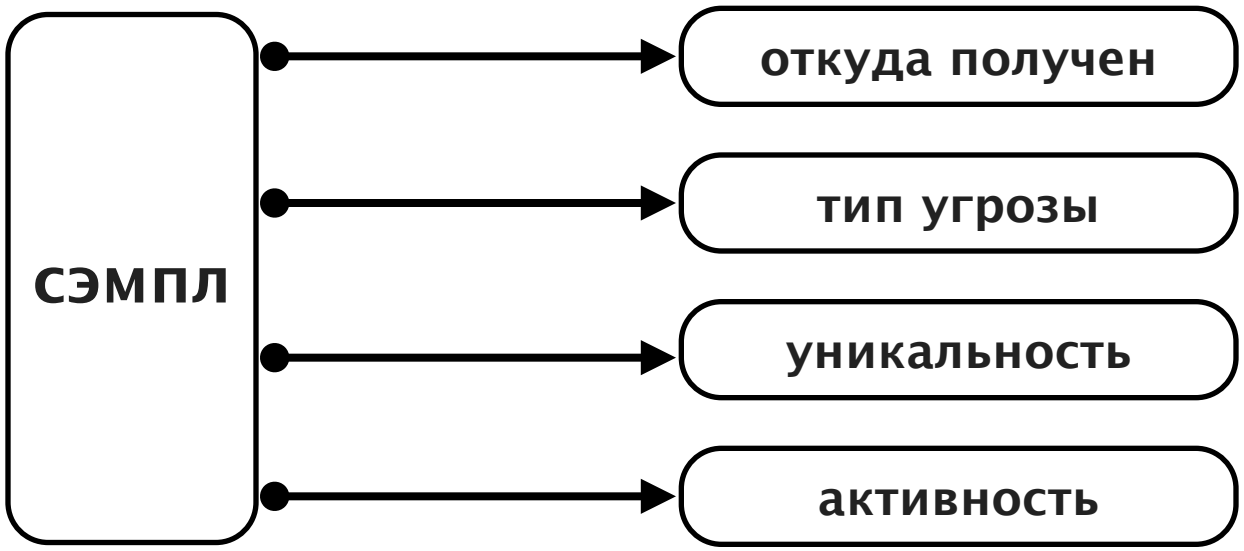
Почему антивирусным компаниям проще расследовать инциденты с участием вредоносных программ?

Подозрительные сэмплы передаются с компьютеров наших пользователей

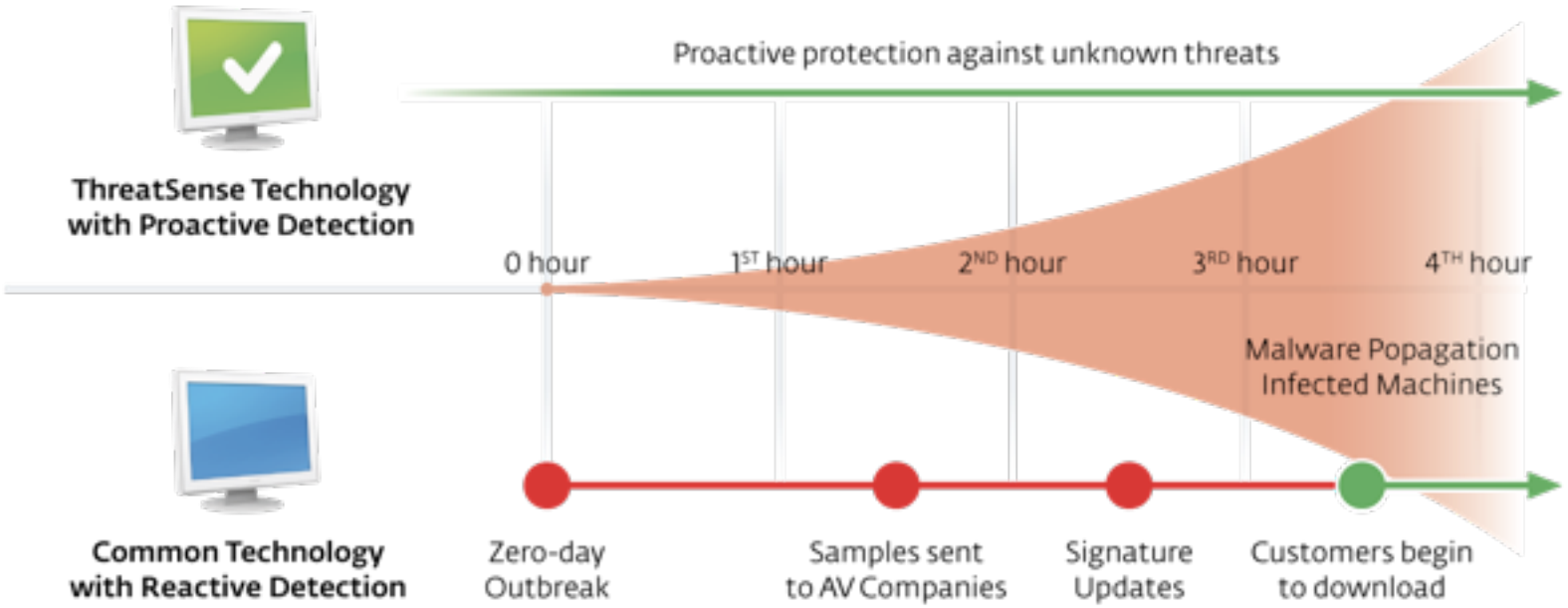
Вирусная лаборатория анализирует переданные и принимает решение о дальнейших действиях по конкретной угрозе

Обновление сигнатурных и эвристических баз. Сбор статистики по инцидентам со всего мира.

Технология глобального мониторинга ThreatSense.NET



- Мета информация помогает осуществлять расширенный поиск по заданным параметрам в хранилище сэмплов



Многоуровневая система реагирования на появление новых угроз

Наша вирусная лаборатория

Вопросы?

Александр Матросов
matrosov@esetnod32.ru

twitter.com/matrosov
amatrosov.blogspot.com