SOLAR SECURITY
software&services

Построение скрытого канала передачи данных с использованием протокола DNS

Алексей Павлов, аналитик JSOC

Сводка атак на банковские структуры

Здравствуйте, коллеги!

Информация по массовой атаке на банковский сегмент 20.01.2016 и по распространению вредоносного кода Trojan.ProxyChanger, нацеленного на онлайн-банкинг.

С уважением,
Центр мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере

Главное управление безопасности и защиты информации
E: FinCERT@cbr.ru

Банк России

www.cbr.ru

Здравствуйте, коллеги!

Информация по возможной компрометации АРМ КБР. Коллеги, уделите **ОСОБОЕ ВНИМАНИЕ** данной рассылки!

С уважением,
Центр мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере

Главное управление безопасности и защиты информации
E: FinCERT@cbr.ru

Банк России

www.cbr.ru

LENTA.RU Интернет и СМИ

08:46, 16 февраля 2015

Хакеры украли миллиард долларов в ходе крупнейшей атаки на банки

МВД рассказало о попытке хищения денег у большинства российских банков

531 103 63 Прочитали 165 188 раз

МВД России выявило кибербанду, поставившую под угрозу безопасность всей банковской системы страны. Как заявил глава управления «К», мошенники пытались похитить деньги практически из всех банков России

Правоохранительным органам удалось пресечь в 2015 году попытку масштабного хищения денег практически из всех банков России. Об этом

Хакеры похитили £20 млн со счетов британского банка

Москва, 14 октября - АиФ-Москва.
Хакерам удалось похитить 20 млн фунтов стерлингов (около $30 млн) со счетов британского банка, используя троянскую программу Dridex, сообщает Mashable со ссылкой на Национальное агентство по борьбе с преступностью (National Crime Agency).

LENTA.RU

14:19, 3 января 2016

Хакеры сняли почти 100 миллионов рублей со счетов коммерческого банка

Рекомендации по защите

Рекомендации ЦБ:

- Строгая парольная политика;
- Антивирусные проверки;
- Изоляция АРМ КБР от корпоративного сегмента и Интернет;
- Контроль действий пользователей

Рекомендации Fincert:

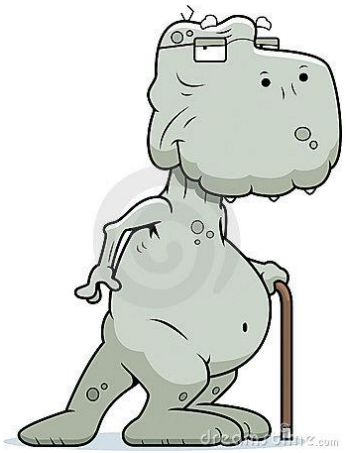
- Контроль и профилирование сетевых соединений;
- Контроль за АРМ, формирующих рейсы
- Усиление контроля за ключевыми сотрудниками и АРМ

Типовые атаки, связанные с:

- Вредоносным ПО, обращающихся по 443 порту к C&C
- Использование RAT
- Компрометация данных ключевых сотрудников

DNS tunneling

DNS tunneling - метод, позволяющий организовать скрытый канал передачи данных, за счёт построения туннеля поверх протокола DNS.

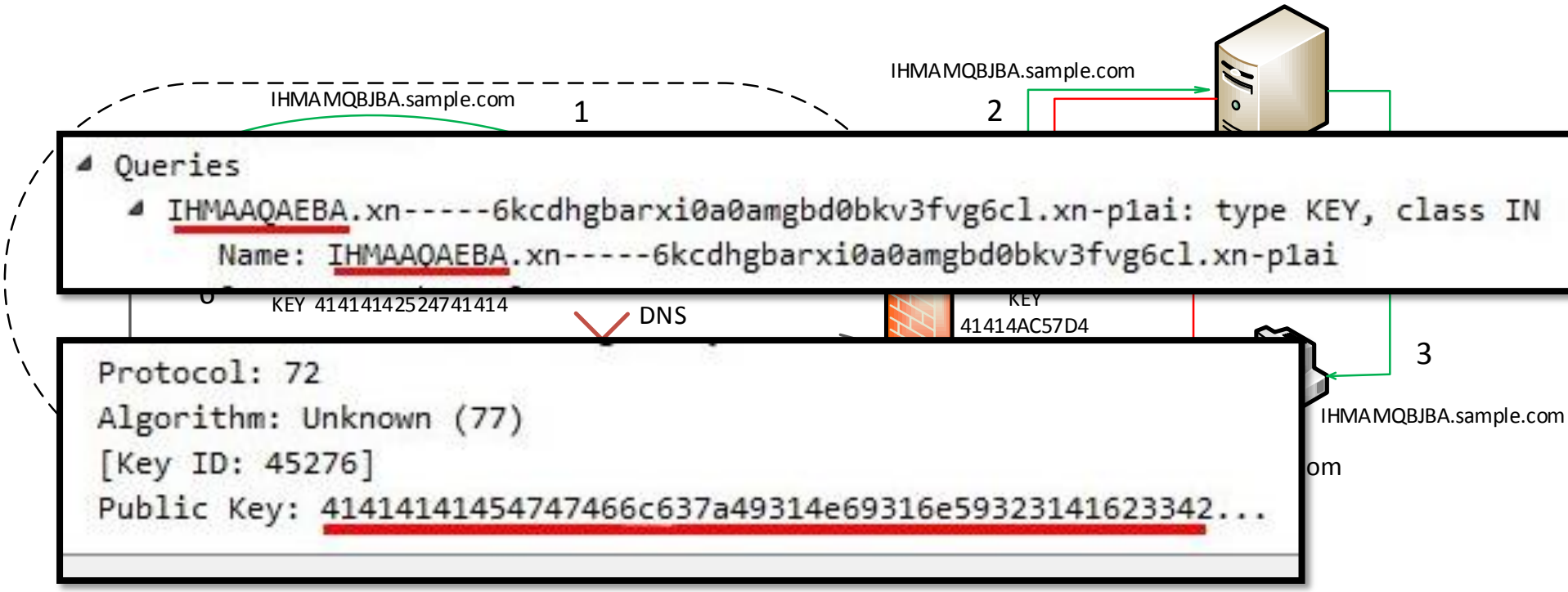


Имеем:

- свой зарегистрированный домен (sample.com)
- клиент в инфраструктуре компании

DNS tunneling

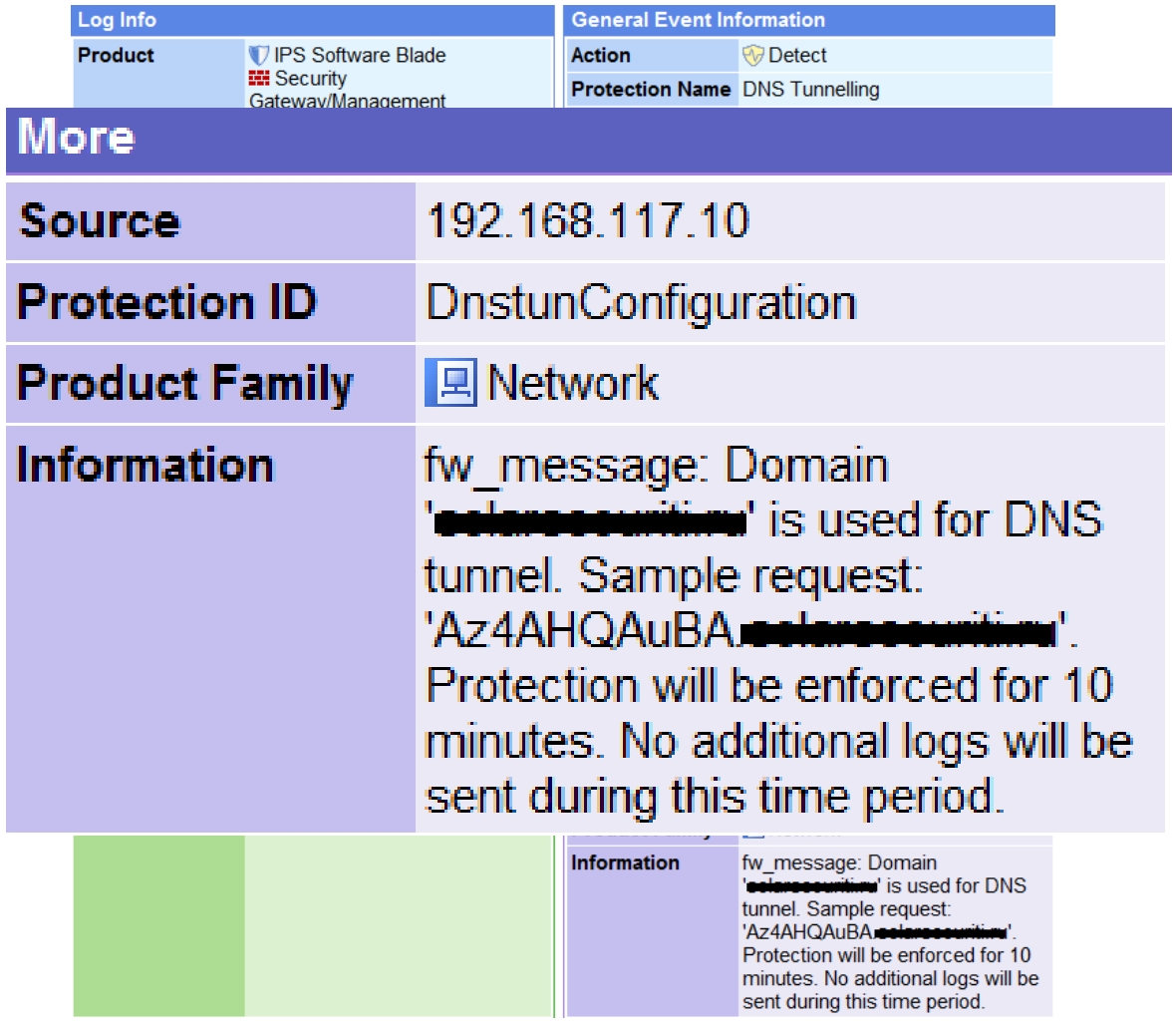
DNS Query-Answer sample.com:



Вариант №1. DNS_TNG_QNAME Детектирование

- Поиск ключевых слов в пакете. Очень редко детектируется. В нашем случае – никогда, благодаря использованию преобразования в хекс или шифрования
- Поиск по длинному имени (большому пакету). Очень много ложных срабатываний на поисковики, облака, сайты, использующие русские символы, adware и прочее
- Поиск по большому количеству запросов на резолв доменов третьего уровня при одном домене второго уровня с одного ip. Так же большое количество ложных срабатываний т.к. все облачные ресурсы работают так.
- Поиск по энтропии (алгоритм DGA) – генерации случайных символов
- Поиск по запросам на резолв УНИКАЛЬНЫХ доменов 3-го уровня при одном домене 2-го уровня с одного ip с ОДНОГО ПОРТА.

Вариант №1. DNS_TNG_QNAME Детектирование



Log Info	
Product	IPS Software Blade Security Gateway/Management

General Event Information	
Action	Detect
Protection Name	DNS Tunnelling

More

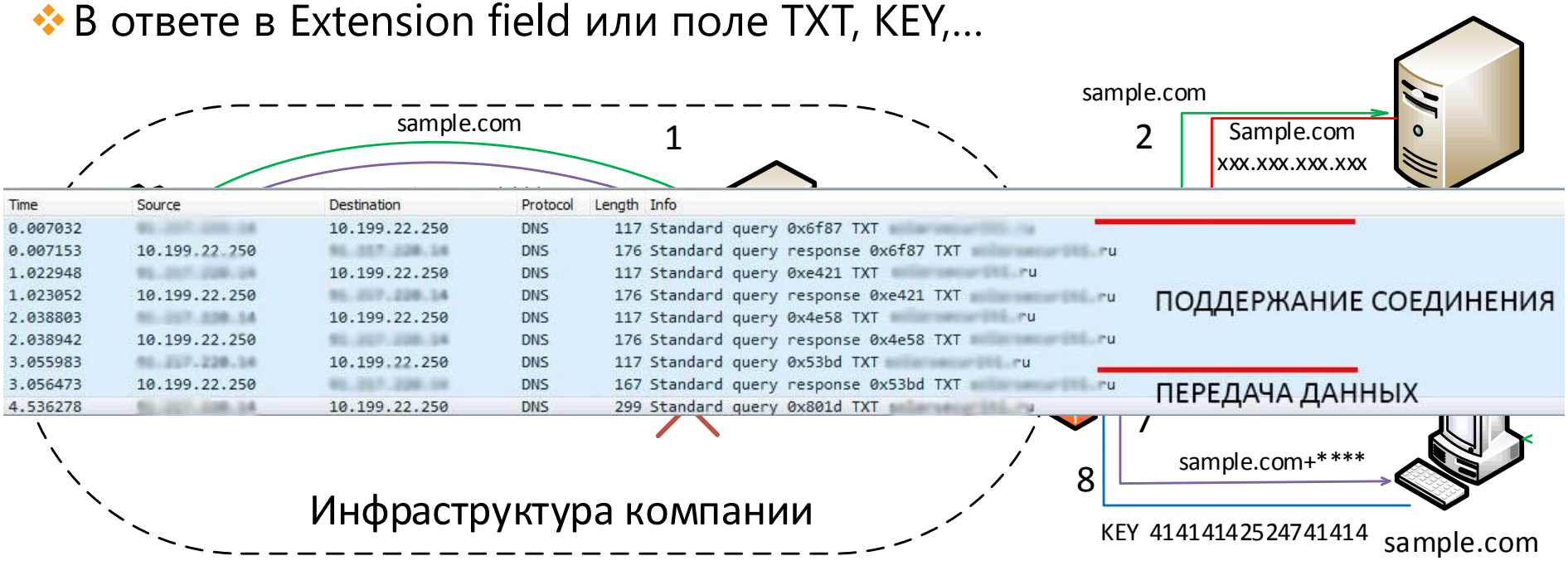
Source	192.168.117.10
Protection ID	DnstunConfiguration
Product Family	Network
Information	fw_message: Domain '[redacted]' is used for DNS tunnel. Sample request: 'Az4AHQAuBA[redacted]'. Protection will be enforced for 10 minutes. No additional logs will be sent during this time period.

Information	fw_message: Domain '[redacted]' is used for DNS tunnel. Sample request: 'Az4AHQAuBA[redacted]'. Protection will be enforced for 10 minutes. No additional logs will be sent during this time period.

Вариант №2. DNS_TNG_PAYLOAD

Основной принцип:

- В запросе идет передача данных за пределами DNS (Extension field)
- В ответе в Extension field или поле TXT, KEY,…



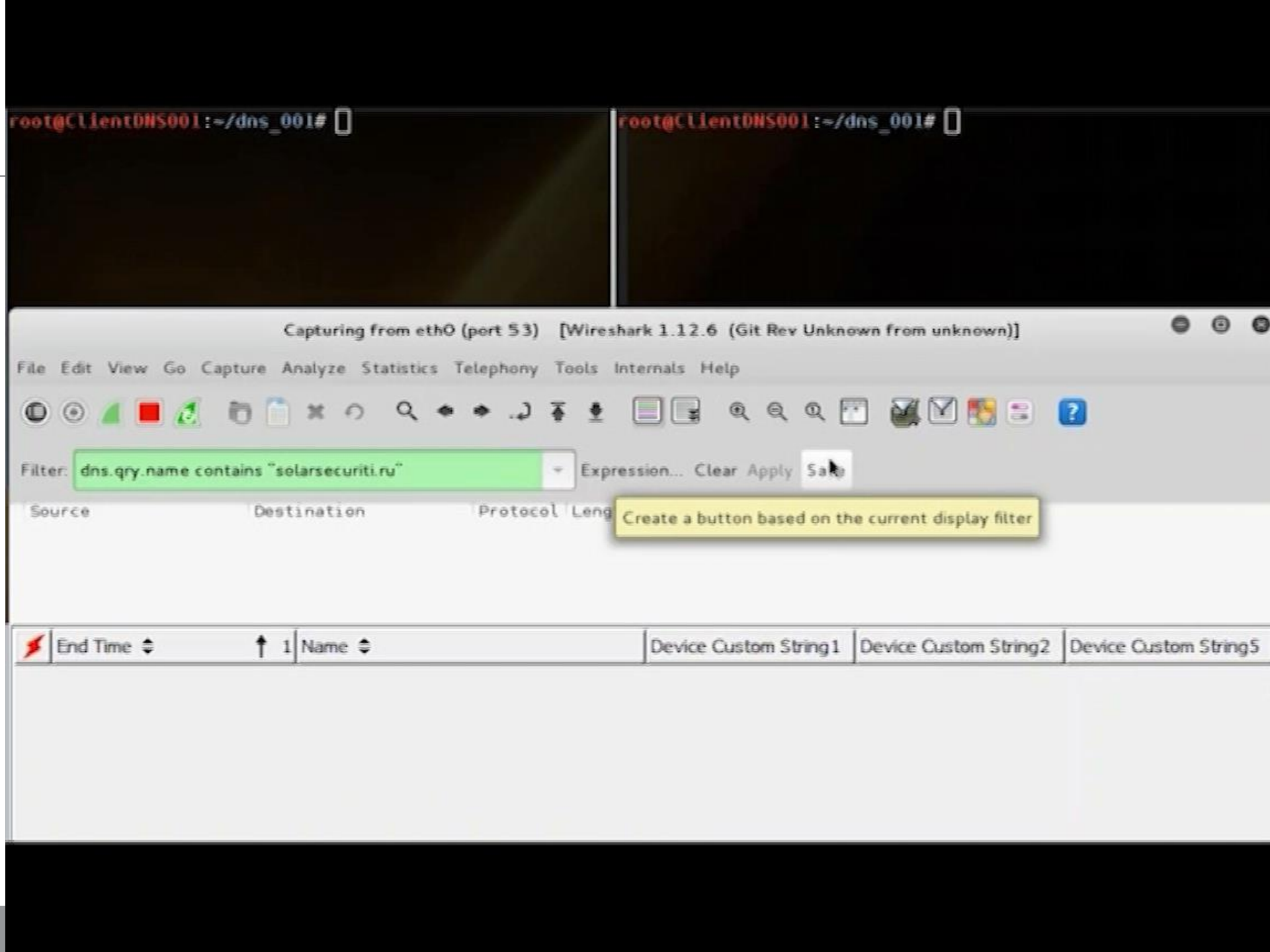
Вариант №2. DNS_TNG_PAYLOAD

```
Answers
▲ [redacted]: type TXT, class IN
    Name: [redacted]
    Type: TXT (Text strings) (16)
    Class: IN (0x0001)
    Time to live: 0
    Data length: 33
    TXT Length: 32
    TXT: exec;6988716471920370182;ls -l /
```

```
3c 08 f6 d9 c7 06 00 50  56 88 2e 82 08 00 45 00   <......P V.....E.
00 99 62 bf 40 00 40 11  7d ec 0a c7 16 fa 5b d9   ..b.@.@. }.....[.
dc 0e 00 35 fd 7a 00 85  5a 3f 53 bd 85 80 00 01   ...5.z.. Z?S.....
00 01 00 00 00 00 0d 73  6f 6c 61 72 73 65 63 75   .......s olarsecu
72 69 74 69 02 72 75 00  00 10 00 01 c0 0c 00 10   rity.ru. ........
00 01 00 00 00 00 00 21  20 65 78 65 63 3b 36 39   .......!  exec;69
38 38 37 31 36 34 37 31  39 32 30 33 37 30 31 38   88716471 92037018
32 3b 6c 73 20 2d 6c 20  2f 00 c0 0c 00 10 00 01   2;ls -l  /.......
00 00 00 00 00 21 20 65  78 65 63 3b 36 39 38 38   .....! e xec;6988
37 31 36 34 37 31 39 32  30 33 37 30 31 38 32 3b   71647192 0370182;
6c 73 20 2d 6c 20 2f                               ls -l /
```

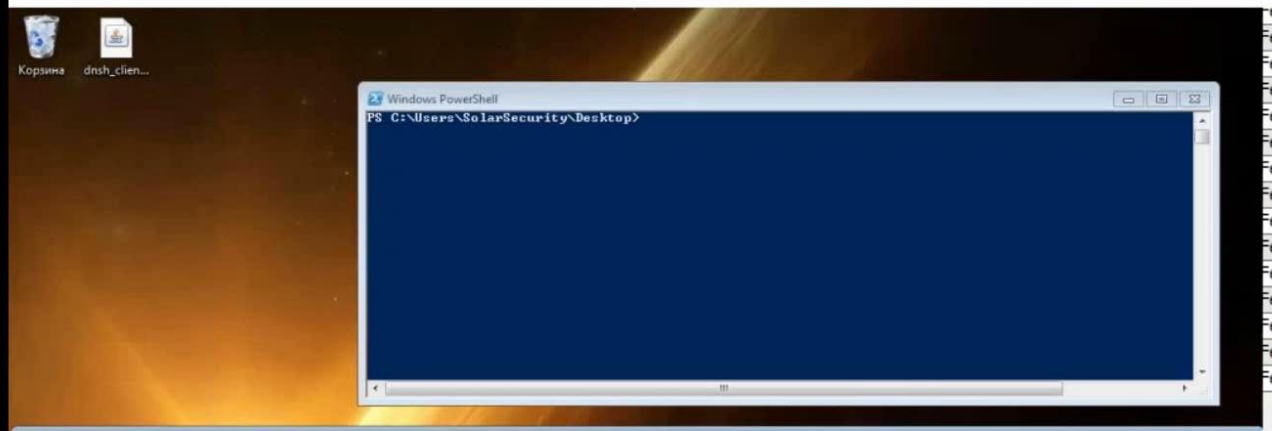
```
Queries
▲ [redacted]: type TXT, class IN
    Name: [redacted]
    [Name Length: 16]
    [Label Count: 2]
    Type: TXT (Text strings) (16)
    Class: IN (0x0001)
```

```
00 50 56 88 2e 82 3c 08  f6 d9 c7 06 08 00 45 00   .PV...<. ......E.
01 1d 1b e5 00 00 78 11  cc 42 5b d9 dc 0e 0a c7   ......x. .B[.....
16 fa e9 db 00 35 01 09  93 ae 80 1d 00 00 00 01   .....5.. ........
00 00 00 00 00 00 0d 73  6f 6c 61 72 73 65 63 75   .......s olarsecu
72 69 74 69 02 72 75 00  00 10 00 01 c0 0c 00 10   rity.ru. ........
72 73 00 60 fc e8 9a 78  bc 22 06 00 00 00 07 00   rs.`...x ."......
00 00 c8 74 6f 74 61 6c  20 37 30 0a 6c 72 77 78   ...total  70.lrwx
72 77 78 72 77 78 2e 20  20 20 31 20 72 6f 6f 74   rwxrwx.    1 root
20 20 20 20 20 72 6f 6f  74 20 20 20 20 20 20 20   roo t
20 20 37 20 4a 75 6c 20  32 30 20 20 32 30 31 35   7 Jul  20  2015
20 62 69 6e 20 2d 3e 20  75 73 72 2f 62 69 6e 0a   bin ->  usr/bin.
64 72 2d 78 72 2d 78 72  2d 78 2e 20 20 20 35 20   dr-xr-xr -x.   5
72 6f 6f 74 20 20 20 20  20 72 6f 6f 74 20 20 20   root       root
20 20 20 31 30 32 34 20  4a 75 6c 20 32 30 20 20     1024  Jul 20
32 30 31 35 20 62 6f 6f  74 0a 64 72 77 78 72 2d   2015 boo t.drwxr-
78 72 2d 78 20 20 20 31  38 20 72 6f 6f 74 20 20   xr-x   1 8 root
20 20 20 72 6f 6f 74 20  20 20 20 20 20 33 30 38      root       308
30 20 4a 61 6e 20 31 38  20 31 34 3a 31 31 20 64   0 Jan 18  14:11 d
65 76 0a 64 72 77 78 72  2d 78 72                  ev.drwxr -xr
```

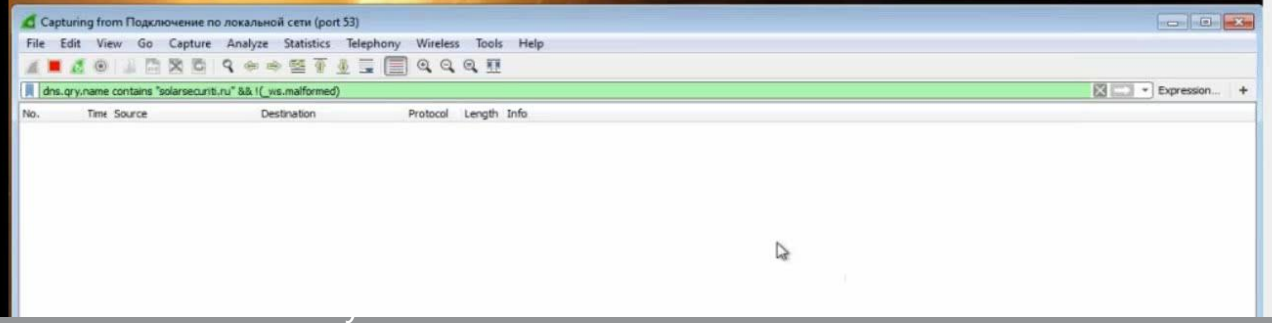

root@ClientDNS001:~/dns_001#
root@ClientDNS001:~/dns_001#
Capturing from eth0 (port 53) [Wireshark 1.12.6 (Git Rev Unknown from unknown)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter: dns.qry.name contains "solarsecuriti.ru"
Expression... Clear Apply Save
Source
Destination
Protocol
Create a button based on the current display filter
End Time
Name
Device Custom String1
Device Custom String2
Device Custom String5

```
root@j001:/home/dns_002#
```

No.	Time	Source	Destination	Protocol	Len



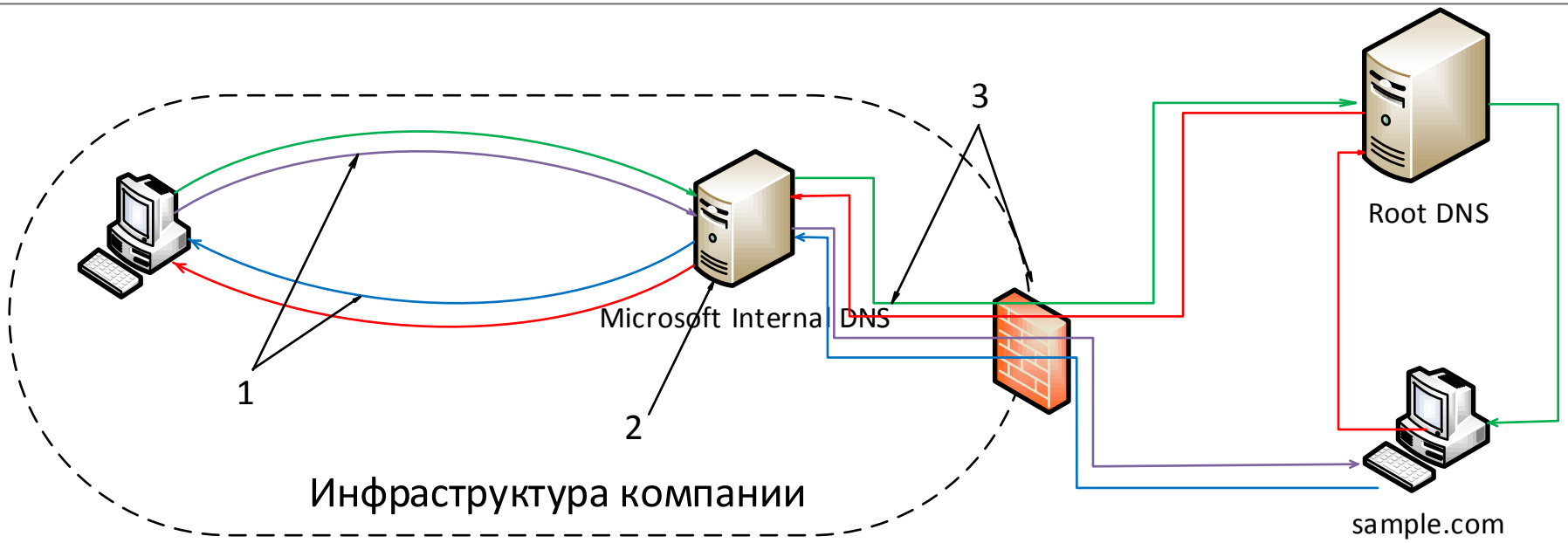
Feb 2016 17:43:12 MSK	INC_JSOC_DNS_001-002_TNG_QNAME	Query:KEY
Feb 2016 17:43:10 MSK	INC_JSOC_DNS_001-002_TNG_QNAME	Query:KEY
Feb 2016 17:43:09 MSK	INC_JSOC_DNS_001-002_TNG_QNAME	Query:KEY
Feb 2016 17:43:03 MSK	INC_JSOC_DNS_001-002_TNG_QNAME	Query:KEY
Feb 2016 17:42:53 MSK	INC_JSOC_DNS_001-002_TNG_QNAME	Query:KEY
Feb 2016 17:42:47 MSK	INC_JSOC_DNS_001-002_TNG_QNAME	Query:KEY
Feb 2016 17:42:44 MSK	INC_JSOC_DNS_001-002_TNG_QNAME	Query:KEY
Feb 2016 17:42:43 MSK	INC_JSOC_DNS_001-002_TNG_QNAME	Query:KEY
Feb 2016 17:40:38 MSK	INC_JSOC_DNS_001-002_TNG_QNAME	Query:TXT
Feb 2016 17:40:35 MSK	INC_JSOC_DNS_001-002_TNG_QNAME	Query:TXT
Feb 2016 17:40:24 MSK	INC_JSOC_DNS_001-002_TNG_QNAME	Query:TXT
Feb 2016 17:40:13 MSK	INC_JSOC_DNS_001-002_TNG_QNAME	Query:TXT
Feb 2016 17:40:07 MSK	INC_JSOC_DNS_001-002_TNG_QNAME	Query:TXT
Feb 2016 17:40:04 MSK	INC_JSOC_DNS_001-002_TNG_QNAME	Query:TXT
Feb 2016 17:40:04 MSK	INC_JSOC_DNS_001-002_TNG_QNAME	Query:TXT



DNS tunneling
Меры предосторожности

- Мониторинг DNS-трафика с помощью IPS (а лучше SIEM) + написание сигнатур
- Запрет использования публичных DNS-серверов для всех машин - настройка как на самих машинах, так и на периметровых межсетевых экранах
- Запрет (по мере возможности) на использование DNS для критичных систем - используйте (etc/hosts)

Пару слов о мониторинге



2 – DNS Server logs

1 – IPS

3 – Perimeter FW/IPS

Спасибо!
Вопросы?

Павлов Алексей
av.pavlov@solarsecurity.ru
+7 (916) 178 98 90