ASEC REPORT

2013 | ANNUAL REPORT

AhnLab

CONTENTS

ASEC(AhnLab Security Emergency response Center)은
악성코드 및 보안 위협으로부터 고객을 안전하게 지키기
위하여 보안 전문가로 구성된 글로벌 보안 조직입니다.
이 리포트는 ㈜안랩의 ASEC에서 작성하며,
매월 발생한 주요 보안 위협과 이슈에 대응하는
최신 보안 기술에 대한 요약 정보를 담고 있습니다.
자세한 내용은 안랩닷컴(www.ahnlab.com)에서
확인하실 수 있습니다.

2013년 보안 동향 분석

악성코드 동향

2013년 보안 동향 분석

01. 악성코드 통계

2013년 악성코드, 6049만 6654건

ASEC이 집계한 바에 따르면 2013년 감염이 보고된 악성코드는 전체 6049만 6654건인 것으로 조사됐다. 이 가운데 가장 많이 보고된 악성코드는 Win-Trojan/Patched.kg였으며, Textimage/Autorun과 Als/Bursted가 그 뒤를 이었다. 또한 총 10건의 악성코드가 최다 20건 목록에 이름을 추가했다([표 1-1]).

표 1-1 | 2013년 악성코드 감염보고 최다 20건

순위	등락	악성코드명	건수	비율
1	NEW	Win-Trojan/Patched.kg	1,010,212	19.9 %
2	▲3	Textimage/Autorun	593,319	11.7 %
3	▲15	Als/Bursted	378,515	7.5 %
4	▲11	Trojan/Win32.onlinegamehack	372,871	7.4 %
5	NEW	Win-Trojan/Wgames.Gen	305,620	6 %
6	▲11	RIPPER	272,881	5.4 %
7	▲5	Trojan/Win32.agent	252,907	5 %
8	NEW	Trojan/Win32.urelas	188,657	3.7 %
9	NEW	BinImage/Host	175,374	3.5 %
10	NEW	Win32/Autorun.worm.307200.F	170,266	3.4 %
11	▼7	JS/Agent	167,230	3.3 %
12	▼11	ASD.PREVENTION	164,878	3.3 %
13	▼10	Trojan/Win32.Gen	163,771	3.2 %
14	NEW	Win-Trojan/Onlinegamehack140.Gen	141,253	2.8 %
15	▼13	Trojan/Win32.adh	139,048	2.7 %
16	NEW	Win-Trojan/Malpacked5.Gen	130,315	2.6 %
17	NEW	Win-Trojan/Asd.variant	126,835	2.5 %
18	▲2	JS/Iframe	108,363	2.1 %
19	NEW	Win32/Virut.f	104,416	2.1 %
20	NEW	Win-Trojan/Agent.149246	104,319	2.1 %
		TOTAL	5,071,050	100.0 %

악성코드 대표진단명 감염보고 최다 20

[표1-2]는 악성코드 대표 진단명 중 가장 많이 보고된 20건을 추린 것이다. 2013년에는 Trojan/Win32가 총 211만 7519건으로 가장 많았다. Win-Trojan/Patched가 110만 3596건으로 그 뒤를 이었는데 새롭게 이름을 올린 악성코드라는 점에서 눈에 띈다. 그 다음으로 Win-Trojan/Agent가 85만 5646건을 기록했다.

표 1-2 | 2013년 대표진단명 감염보고 최다 20건

순위	등락	악성코드명	건수	비율
1	—	Trojan/Win32	2,117,519	24 %
2	NEW	Win-Trojan/Patched	1,103,596	12.5 %
3	▼1	Win-Trojan/Agent	855,646	9.7 %
4	▲6	Textimage/Autorun	593,409	6.7 %
5	▲6	Win-Trojan/Onlinegamehack	432,792	4.9 %
6	NEW	Als/Bursted	378,515	4.3 %
7	—	Win-Trojan/Downloader	352,516	4 %
8	▲6	Win32/Conficker	312,348	3.5 %
9	NEW	Win-Trojan/Wgames	305,620	3.5 %
10	▲9	Win32/Autorun.worm	292,732	3.3 %
11	▼8	Adware/Win32	285,864	3.2 %
12	NEW	RIPPER	272,881	3.1 %
13	▲3	Win32/Virut	267,520	3 %
14	▲4	Win32/Kido	236,880	2.7 %
15	▼10	Malware/Win32	192,747	2.2 %
16	NEW	BinImage/Host	175,374	2 %
17	▼9	JS/Agent	167,870	1.9 %
18	▼14	ASD	164,878	1.9 %
19	▼13	Downloader/Win32	158,293	1.8 %
20	NEW	Win-Trojan/Avkiller	146,087	1.7 %
		TOTAL	8,813,087	100.0 %

2013년 최다 신종 악성코드

[표1-3]은 2013년 신규로 보고 접수된 악성코드 중 최다 20건이다. 2013년 신종 악성코드는 Win-Trojan/Rootkit.83909376이 3만 4781건으로 전체의 18.4%를 차지, Win-Trojan/ Patched.25600.C가 2만 6849건으로 뒤를 이었다.

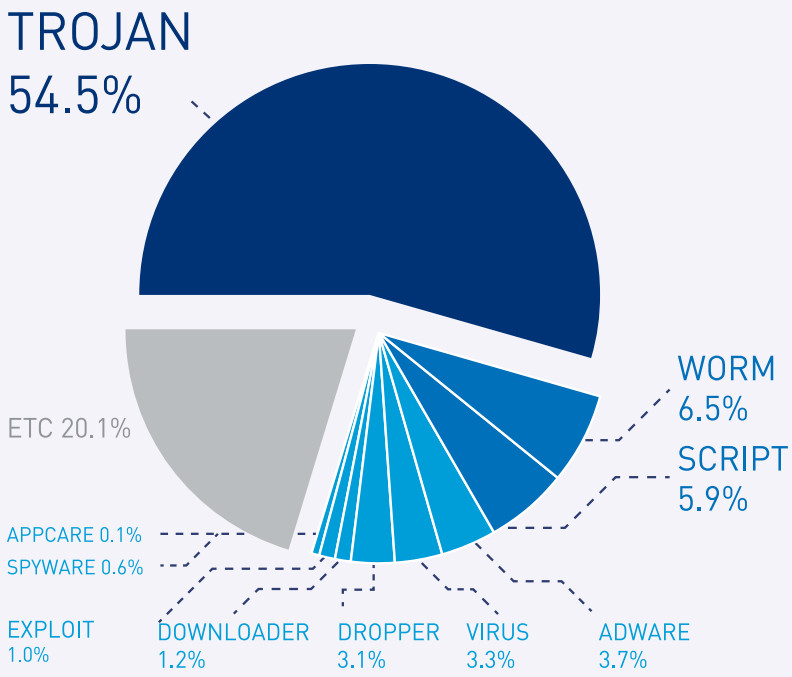
표 1-3 | 2013년 신종 악성코드 최다 20건

순위	악성코드명	건수	비율
1	Win-Trojan/Rootkit.83909376	34,781	18.4 %
2	Win-Trojan/Patched.25600.C	26,849	14.2 %
3	JS/Donxref	25,662	13.5 %
4	Win-Trojan/Avkiller.23488	25,317	13.4 %
5	Win-Trojan/Agent.59392.LE	12,231	6.5 %
6	JAVA/Cve-2013-0422	10,768	5.7 %
7	Win-Trojan/Onlinegamehack.205350	7,961	4.2 %
8	Java/Cve-2013-0422	6,557	3.5 %
9	Win-Trojan/Guntior.4416	4,354	2.3 %
10	Win-Trojan/Onlinegamehack.26048	4,351	2.3 %
11	Win-Trojan/Onlinegamehack.14336.AG	3,599	1.9 %
11	Win-Trojan/Onlinegamehack.105984.O	3,537	1.9 %
13	Win-Trojan/Avkiller.28320	3,397	1.8 %
14	Win-Trojan/Agent.65024.JS	3,373	1.8 %
15	Win-Trojan/Patchedmidimap.17408	3,135	1.6 %
16	Win-Trojan/Avkiller.5248	3,073	1.6 %
17	Win-Dropper/Anyad.621721	3,024	1.6 %
18	Win-Trojan/Onlinegamehack.13824.BF	2,483	1.3 %
19	Win-Trojan/Agent.656600	2,424	1.3 %
20	Win-Trojan/Onlinegamehack.201216.K	2,312	1.2 %
	TOTAL	189,188	100.0 %

2013년도 트로이목마가 최다

[그림1-1]은 2013년 안랩 고객으로부터 감염이 보고된 악성코드의 유형별 비율을 집계한 결과다. 트로이목마가 54.4%로 가장 높았고 웜 6.5%, 스크립트가 5.9%로 집계됐다.

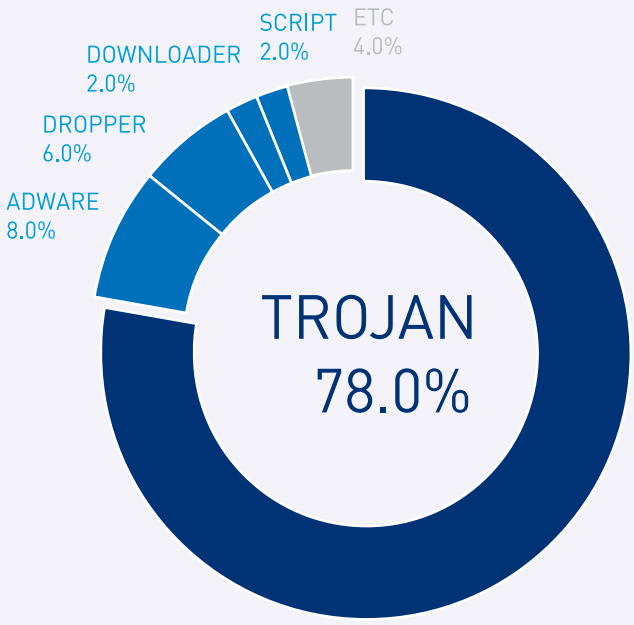
그림 1-1 | 2013년 악성코드 유형별 비율



신종 악성코드 유형별 분포

2013년 신종 악성코드를 유형별로 보면 트로이목마가 78%로 가장 많았고, 애드웨어가 6%, 드롭퍼가 6%였다.

그림 1-2 | 2013년 신종 악성코드 유형별 분포도



2013

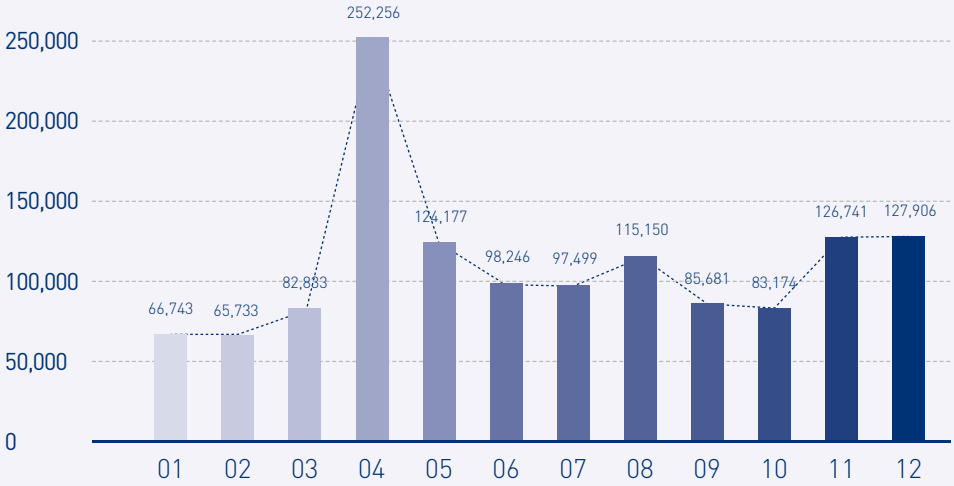
2013년 보안 동향 분석

02. 모바일 악성코드 통계

2013년 월별 모바일 악성코드 접수량

[그림2-1]은 2013년 한 해 동안 접수된 모바일 악성코드 중 V3 모바일에 진단이 추가된 악성앱의 접수량 추이다. ASEC이 집계한 바에 따르면, 2013년 1년간 총 132만 6139건이 악성앱으로 진단됐다. 이 중 상반기에 67만 3599건, 하반기에 65만 2540건이 추가로 진단됐다.

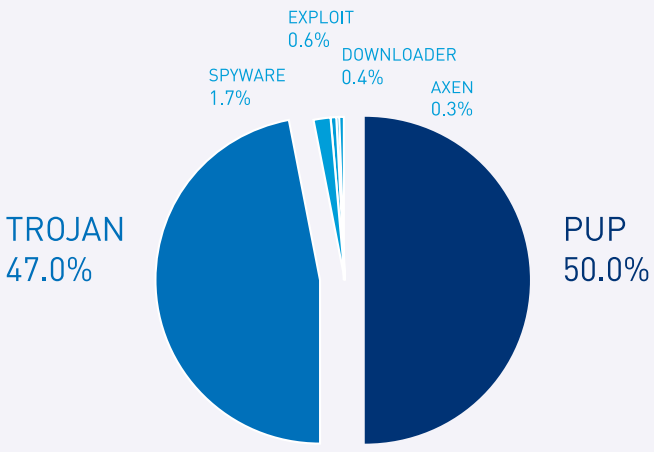
그림 2-1 | 2013년 월별 모바일 악성코드 접수량



2013년 유형별 모바일 악성코드

[그림 2-2]는 지난 해 접수된 모바일 악성코드의 유형별 비율이다. 상반기까지는 사용자의 정보를 유출하거나 사용자 모르게 과금을 발생시키는 유형의 트로이목마가 가장 많이 발견됐다. 그리고 지난 한 해 동안 앱이 실행되지 않은 상태에서도 광고를 노출해 사용자의 불편을 일으키는 PUP유형이 가장 많이 발견된 것으로 확인됐다.

그림 2-2 | 2013년 접수된 모바일 악성코드 유형



2013년 상위 10개 모바일 악성앱

[표2-1]은 각각 2013년 상반기와 하반기에 접수된 모바일 악성앱 중 접수량이 가장 많았던 상위 10개의 진단명이다. 2013년 상반기와 마찬가지로 FakeInst, Opfake의 변형이 꾸준히 가장 많이 발견되고 있으며 익스플로이트킷이 10위권내에서 사라지고 새로운 유형의 PUP가 Top 10에 포함됐다.

표 2-1 | 2013년 접수량이 많은 상위 10개 모바일 악성앱

	2013 상반기			2013 하반기		
순위	진단명	건수	비율	진단명	건수	비율
1	Android-Trojan/FakeInst	158,663	24%	Android-Trojan/FakeInst	303,077	23%
2	Android-PUP/Airpush	90,218	13%	Android-PUP/Airpush	184,820	14%
3	Android-Trojan/Opfake	49,309	7%	Android-Trojan/Opfake	108,463	8%
4	Android-PUP/Kuguo	33,730	5%	Android-PUP/Kuguo	82,482	6%
5	Android-PUP/Wapsx	32,890	5%	Android-PUP/Wapsx	60,061	5%
6	Android-Exploit/Rootor	28,000	4%	Android-PUP/Adwo	36,626	3%
7	Android-PUP/Plankton	23,329	3%	Android-PUP/Plankton	36,392	3%
8	Android-PUP/Leadbolt	22,028	3%	Android-PUP/Admogo	35,377	3%
9	Android-PUP/Admogo	18,842	3%	Android-Trojan/GinMaster	34,092	3%
10	Android-Trojan/GinMaster	18,214	3%	Android-PUP/Dowgin	31,809	2%

2013년 스미싱앱 유형 30종 발견

[표 2-2]는 국내 사용자를 대상으로 한 스미싱앱 유형이다. 2013년 한 해 동안 발견된 스미싱앱은 총 30종으로 확인됐다.

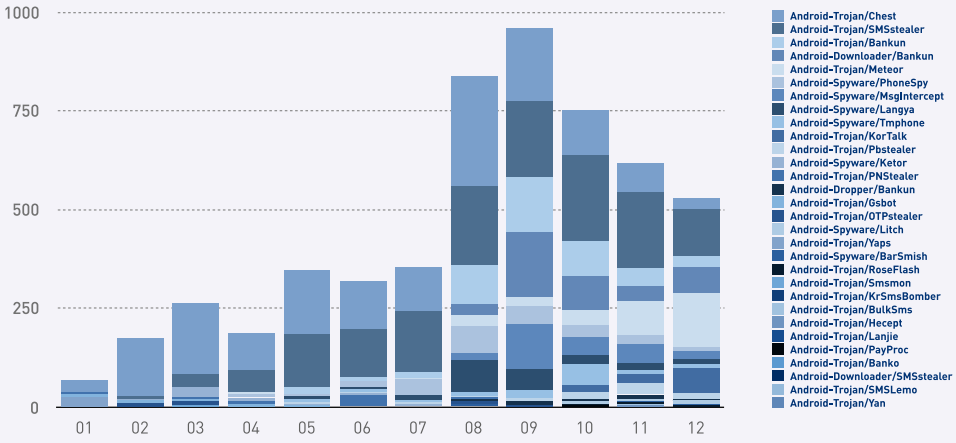
표 2-2 | 2013년 스미싱앱 유형

1	Android-Trojan/Chest	11	Android-Trojan/Pbstealer	21	Android-Trojan/Smsmon
2	Android-Trojan/SMSstealer	12	Android-Spyware/Ketor	22	Android-Trojan/KrSmsBomber
3	Android-Trojan/Bankun	13	Android-Trojan/PNStealer	23	Android-Trojan/BulkSms
4	Android-Downloader/Bankun	14	Android-Dropper/Bankun	24	Android-Trojan/Hecept
5	Android-Trojan/Meteor	15	Android-Trojan/Gsbot	25	Android-Trojan/Banko
6	Android-Spyware/PhoneSpy	16	Android-Trojan/OTPstealer	26	Android-Trojan/Lanjie
7	Android-Spyware/MsgIntercept	17	Android-Spyware/Litch	27	Android-Trojan/PayProc
8	Android-Spyware/Langya	18	Android-Trojan/Yaps	28	Android-Trojan/Yan
9	Android-Spyware/Tmphone	19	Android-Spyware/BarSmish	29	Android-Trojan/SMSLemo
10	Android-Trojan/KorTalk	20	Android-Trojan/RoseFlash	30	Android-Downloader/SMSstealer

2013년 스미싱 악성앱 월별 접수 건수 추이

[그림2-3]은 스미싱 악성앱 변형의 월별 접수 건수 추이를 나타낸 것이다. 상반기 꾸준히 접수되던 스미싱 앱은 9월 최고점에 달했으나 4분기에는 그 수가 조금씩 감소한 것으로 나타났다. 10월까지는 새로운 유형의 악성앱이 지속적으로 증가했으며 12월에는 17종의 악성앱이 배포되었다. 상반기는 Android-Trojan/Chest와 Android-Trojan/SMSstealer의 변형이 가장 많이 확인됐으나 하반기부터 Android-Trojan/Bankun과 Android-Trojan/Meteor을 포함한 다양한 유형의 악성앱이 나타나고 있다.

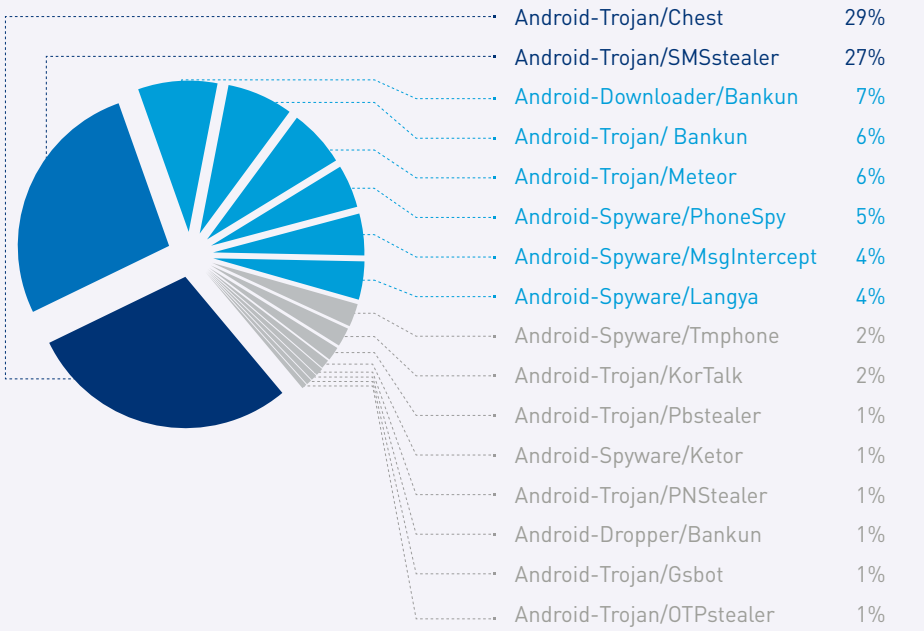
표 2-3 | 스미싱 악성앱의 월별 접수 건수 추이



2013년 스미싱 악성코드 유형별 접수량

[그림 2-4]는 2013년 한 해 동안 국내 스마트폰 사용자를 대상으로 전파된 스미싱 악성코드의 유형별 접수량을 나타낸 것이다. 가장 많은 변형이 확인된 악성앱은 상반기부터 가장 많이 배포됐던 Android-Trojan/Chest(29%), Android-Trojan/SMSstealer(27%)다. 이 앱들은 초기 소액결제 인증 문자를 가로채는 기능만 포함하고 있었으나 점차 기능을 확대해 스마트폰에 저장된 인증서 정보를 유출하고 사용자의 은행정보를 유출하는 기능을 포함하는 변형 악성앱도 확인됐다. 하반기 이후 많이 접수된 Android-Trojan/Metor(8%), Android-Downloader/Bankun(7%), Android-Trojan/Bankun(6%)은 기존 설치된 은행앱을 삭제하고 계좌정보와 비밀번호를 유출하는 기능을 가진 가짜 은행앱을 다운로드 하는 형태다. 상반기 소액결재 인증 문자를 외부로 유출해 금전적인 이득을 취하는 유형의 악성앱이 대부분이었다. 하반기부터는 스마트폰에 저장된 공인인증서와 은행 계좌정보 유출을 통해 금전적인 이득을 취하는 유형의 새로운 악성앱이 등장하고 있으며, 기존의 악성앱도 이러한 기능을 추가하고 있다.

그림 2-4 | 스미싱 악성코드의 유형별 접수량



2013년 보안 동향 분석

03. 보안 통계

2013년 연간 마이크로소프트 보안업데이트 현황

2013년 한 해 동안 마이크로소프트사는 총 105 건의 보안 업데이트를 발표했다. 한 해 동안 발표된 보안 패치 중 윈도 시스템 상의 취약점을 해결하는 패치가 43%로 가장 큰 비중을 차지했다. 또 2012년에 비해 보안 업데이트 수도 증가했다. 전체적으로 보안 업데이트의 분류 비율은 크게 달라지지 않았지만, 인터넷 익스플로러와 오피스 상의 보안 업데이트 횟수가 크게 증가했다. 이를 통해 인터넷 익스플로러와 오피스 취약점을 통한 위협이 크게 증가했음을 알 수 있다. 이러한 취약점을 이용한 보안 위협의 피해를 막기 위해서는 적극적인 보안 업데이트 적용이 반드시 필요하다.

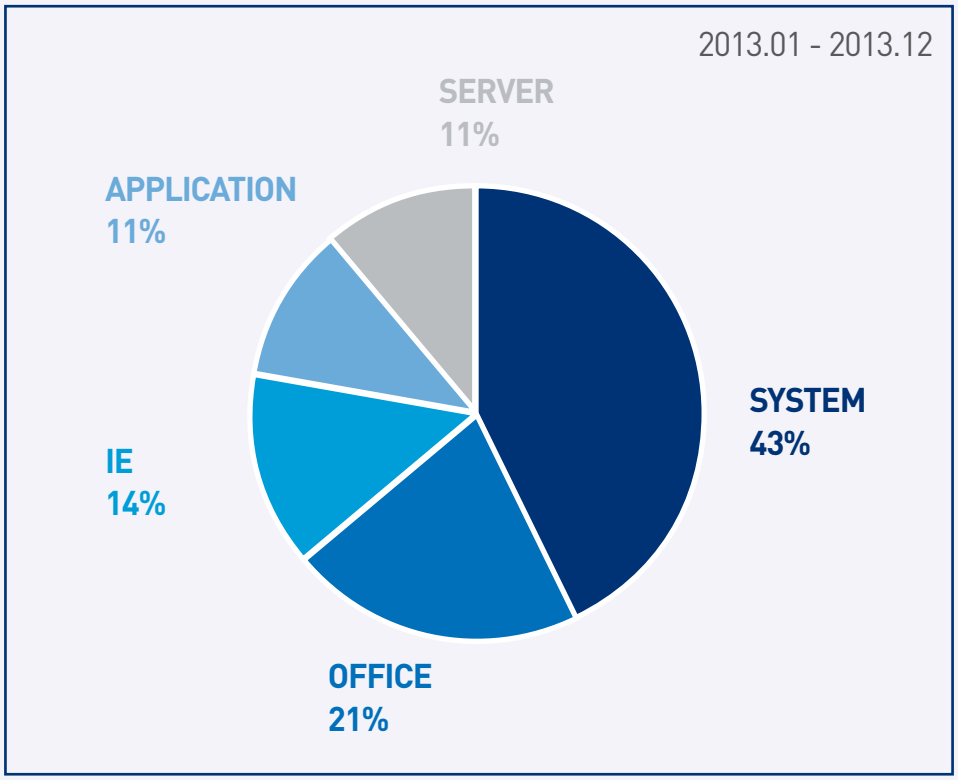


그림 3-1 | 공격대상 기준별 MS 보안 업데이트 분류

2013년 보안 동향 분석

04. 웹 보안 통계

웹사이트 악성코드 동향

안랩의 웹 브라우저 보안 서비스인 사이트가드(SiteGuard)를 활용한 웹 사이트 보안 통계 자료에 의하면, 2013년 악성코드 발견 건수는 9만 702건이고 악성코드 유형은 2872건이며 악성코드가 발견된 도메인은 1982개, 악성코드가 발견된 URL은 7414건으로 집계됐다.

표 4-1 | 2013년 웹사이트 악성코드 현황

악성코드 발견 건수

2013 2012

243,989

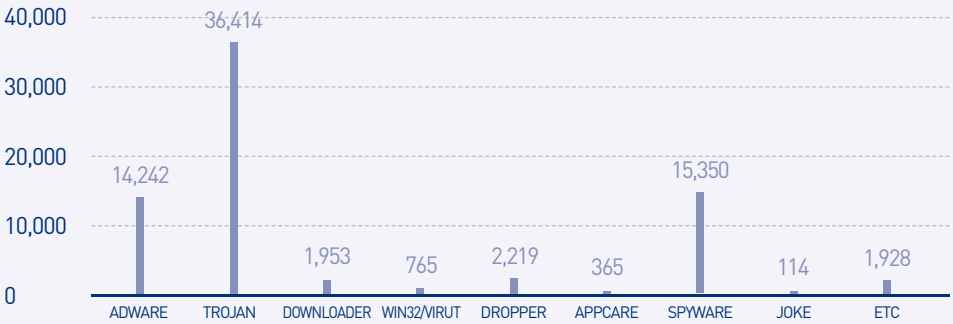
90,702 -62.82%

악성코드 유형	악성코드가 발견된 도메인	악성코드가 발견된 URL
2,872 5,249	1,982 3,455	7,414 26,952

월별 악성코드 발견 건수

2013년 악성코드 발견 건수는 9만 702건이다.

그림 4-1 | 2013년 악성코드 발견 건수



2013년 보안 동향 분석

05. 2013년 주요 보안 이슈

(1) 대규모 APT 보안 사고 '동시다발적 피해'

2013년 3월 20일 금융사와 방송사를 대상으로 한 대규모 공격(안랩 진단명 Trojan /Win32(64).XwDoor), 석 달 뒤인 6월 25일 정부와 공공기관에 대한 DDoS 공격(안랩 진단명 Trojan/Win32(64).Ddkr)은 사회적으로 큰 파장을 일으킨 보안 사고였다. 이 공격들은 좀비 PC를 이용했던 지난 2009년 7 • 7 DDoS나 2011년 3 • 4 DDoS와는 달리, APT 유형의 공격이 국내 기반 시설에 동시다발적으로 피해를 준 사례로 꼽힌다.

이전에는 불특정 다수에 대한 무차별적인 악성코드 유포 형태가 많았다. 하지만 최근에는 특정 프로그램의 업데이트 기능 취약점, 웹 취약점, 스피어피싱 이메일, 혹은 장시간 분석을 통한 내부 인프라 공격 등의 기법이 활용되고 있다.

특히 2013년 6월 25일 공격은 3월 20일 공격 이후 취해진 민관 합동조사단과 보안 업체의 조치에 대응하여 MBR 삭제 및 MBR 코드 수정, 5.3MB에서 524KB로 데이터 영역 삭제 간격의 축소, 계정 암호 변경 등 분석과 복구가 어렵도록 단기간 내 악성코드를 업그레이드하는 기민함을 보여주었다. 이 같은 APT와 안티포렌식(Anti Forensic) 혼합 공격 기법의 사용에 따라, 2013년은 디지털 포렌식(Digital Forensic) 기법과 포렌식 준비도(Forensics readiness)의 필요성이 어느 때보다 증대된 한 해였다.

(2) 치밀한 APT 공격 그룹 '국제적 규모'

2013년 국내 APT 공격은 특정 국가와 기관의 지원을 받아 국내 국방기술이나 제조 관련 기업의 첨단 기술 유출을 목적으로 하는 것과, 게임 소스 및 인프라 구축 기술 유출을 목적으로 하는 활동이 활발했다. 국내에서 활동 중인 APT 공격 그룹은 다음과 같은 특징을 보였다.

1) 외부 업데이트 서버 또는 서드파티 제품을 통한 내부 네트워크 침투
2) 특정 산업군에서 업무상 필요한 웹 사이트를 수정하여, 해당 사이트로 접속할 때 악성코드에 감염되는 워터링홀(Watering-Hole) 기법을 사용하여 기업 다수에 동시 침투
3) 안티포렌식 기능 적용, MBR 코드 패치와 메모리에 로드된 뒤 삭제되는 기능을 갖는 악성코드를 제작해 보안 프로그램의 진단 • 치료 시 생존율 높임
4) 기업에서 주로 사용하는 AD(Active Directory) 서버를 공격해 도메인 간 이동, 기업 내 PC 복구를 위해 자체 제작한 복구 CD의 비활성화 처리가 되지 않은 마스터 계정과 암호, 키로거, 패스더해시(Pass The Hash) 공격 기법 등을 이용하여 탈취된 인증을 통해 내부 자원에 자유롭게 접근 및 작업 수행
5) 공격을 통해 획득한 인증서를 즉각적으로 다른 기업 공격에 사용 및 공격 그룹별로 다른 악성코드 사용
6) 피해 기업의 대응에 즉각적인 반응(주요 악성코드의 기능 변경, 침해 대상 변경, 재작성된 스피어피싱 메일을 통한 침해 대상 확대)
7) 공격 대상의 내부 메일, 유출 정보 독해 및 위조할 수 있는 한국어에 능통한 인력 활용

이와 같은 APT 공격 기법을 사용하는 국제적 사이버 산업스파이 그룹은 공격 목적에 따라 국가, 군사 기관이나 범죄 집단의 지원을 받고 있는 것으로 추정되며 다국어에 대한 처리가 가능한 인력으로 구성되어 있다. 풍부한 자본과 체계적인 공격조 구성, 기술력을 바탕으로 여러 국가의 고급 정보를 유출하는 것뿐만 아니라 유출된 인증서, 침해된 서버를 이용하여 지속적인 국내외 공격을 수행하고 있다.

(3) 스미싱 모바일 악성코드 '폭발적 증가'

2012년 30여 건에 불과했던 스미싱 악성코드는 2013년에는 11월까지 4868건이 확인됐다. 초기에는 소액 결제 인증 문자를 유출하는 기능으로 시작했으나 최근에는 스마트폰에 설치된 은행 앱의 종류를 식별하고 설치된 은행 앱을 악성 앱으로 교체하는 파밍 형태가 많이 발견되고 있다. 또 보이스피싱과 결합한 악성 앱도 확인됐다. 정부와 보안 업체들은 다양한 방법을 통해 스미싱 악성코드의 피해를 예방하기 위해 노력하고 있으나, 스미싱 악성코드는 여전히 발견되고 있으며 스마트폰 사용자의 금전 피해도 계속해서 늘어나고 있다.

(4) 관리자 계정 정보를 직접 노리는 악성코드 변형 확산

2013년 초부터 발견된 특정 사이트들의 '관리자 계정 정보 탈취 악성코드' 의 변형이 IE(Internet Explorer) 제로데이 취약점(CVE-2013-3897)을 이용해 급속히 국내에 유포됐다. 해당 보안 취약점에 대한 패치가 10월에 발표됐으나 상당히 많은 시스템이 감염된 것으로 추정되고 있다.

확인된 바로는, 국내 특정 CDN(Contents Delivery Network) 업체를 통해 운영 중인 일부 웹사이트들이 악성코드 배포지로 악용됐다. 악성코드는 취약점 셀 코드부터 백신 무력화 증상이 나타나는데, 이후 다운로드 되는 악성코드에도 같은 기능이 있는데 감염된 시스템에 설치된 보안 프로그램을 무장해제한다.

변형에 따라 탈취하려는 관리자 계정의 웹사이트 목록은 다르지만, 2013년 10월에 마지막으로 확인된 변형은 무려 95곳의 웹사이트 관리자 계정을 노렸다. 여기에는 언론사와 기업들이 다수 포함돼 있었다. 탈취된 계정을 이용해 서버를 장악하면 기업 내부에 침투하거나 민감한 정보를 훔쳐낼 수도 있으며, 해당 웹사이트를 악성코드 유포지나 경유지로도 사용할 수 있다.

이 악성코드는 DDoS 증상도 유발하는 것으로 확인됐다. 내부에 존재하는 관리자 계정 탈취 웹사이트와 별도의 특정 도메인들(2013년 10월 발견 변형 기준 19곳)에 대해 차례로 파일 다운로드 및 실행 기능을 수행했다. 그러나 실제 파일이 존재하지 않는 경우가 대부분이었고 웹서버에 부하를 발생시키는 DDoS 증상을 일으키기도 했다.

(5) 국지화되는 소프트웨어 취약점 악용 사례 증가

악성코드는 교회, 학교, 관공서, 호텔, 택배, 웹하드 등 일상생활에서 손쉽게 접근하는 다수의 국내 웹사이트에서 더욱 기승을 부렸다.

특히 어도비의 플래시 플레이어(Flash Player)보다 오라클의 자바와 마이크로소프트의 인터넷 익스플로러(IE) 취약점을 이용하는 공격 사례가 더 많았다. 자바는 주요 제품군에 비해 상대적으로 보안 업데이트가 소홀할 수 있기 때문에 웹 공격 툴킷(Web Exploit Toolkit) 같은 경우 버전별 자바 취약점들을 골고루 활용하고 있다. 또한 IE상의 Use-After-Free(할당된 메모리 해제후 사용) 취약점은 MS의 보안 업데이트 속에서 매월 빠지지 않고 등장할 정도로 꾸준히 보고되는 취약점이다. 이와 같은 유형인 CVE-2013-3897 취약점은 제로데이 취약점으로 등장, 대표적인 웹 공격 툴킷 'Chinese Kit(CK)' 에 포함돼 지금도 활발하게 이용되고 있다.

이러한 웹을 통한 글로벌 제품군을 대상으로 하는 공격 사례 외에도 몇 년 전부터는 국내 소프트웨어의 취약점을 악용하는 사례가 점차 증가하고 있다. 국내의 대표적인 문서 작성 소프트웨어인 '아래아한글' 에서 보고되는 취약점 수가 눈에 띄게 증가했고, 스프레드시트 프로그램인 '한셀' 에서도 2013년 6월 처음으로 유사 공격 형태가 발견됐다.

(6) 인터넷 뱅킹 악성코드 '금전 피해 확대'

2013년 6월 발견된 온라인 게임핵(OnlineGameHack) 악성코드에서 기존에 없었던 국내 인터넷 뱅킹 사이트에 대한 정보 유출 기능이 확인됐다. 국내 감염자가 많은 온라인 게임핵 악성코드에 인터넷 뱅킹 정보 유출 기능이 추가됨으로써 금전적인 피해 규모는 클 수밖에 없었다.

이 악성코드에서 사용한 각 인터넷 뱅킹 사이트별 '보안 모듈 무력화' 및 '이체 정보 변조'의 기능은 기존의 인터넷 뱅킹 악성코드에서 볼 수 없었던 새로운 기법이다.

'보안 모듈 무력화' 는 각 인터넷 뱅킹 사이트에서 사용하는 보안 모듈 중 인증서 패스워드 및 이체 정보 암호화를 담당하는 부분을 무력화하는 것으로 메모리상의 특정 코드에 대한 패치를 통해 이뤄진다. 이 악성코드의 최초 발견 이후 공격 대상 보안 모듈도 지속적으로 추가됐다. 보안 모듈이 업데이트될 때마다 변경된 코드 패턴에 맞춰 악성코드도 변경됐다.

'이체 정보 변조' 는 2013년 9월부터 새롭게 추가된 기능이다. 정상적인 계좌이체 과정 중에 '이체계좌번호' 와 '이체금액' 을 수정해 공격자에게 이체되도록 했다. 이러한 공격을 위해 악성코드는 인터넷 뱅킹 사이트별로 사용하는 고유한 자바스크립트 패턴 정보를 갖고 있으며, 이 중 이체에 필요한 정보를 변조, 공격을 시도한다. 이러한 '이체 정보 변조' 공격은 은행 두 곳에서만 제한적으로 이뤄졌다.

이 같은 새로운 공격 방식은 인터넷 뱅킹 시 지정 PC 및 OTP를 사용할 때도 피해를 줄 수 있다. 또한, 피해를 막기 위해서는 뱅킹 사이트별로 다양한 보안 업체의 모듈들에 대한 업데이트가 필요한데, 이러한 점에서 피해 예방이 쉽지 않다.

두 가지 형태의 공격에 대한 예방을 위해서 인터넷 뱅킹 사용자는 비정상적으로 은행 거래가 종료(강제 로그아웃)된 경우, 인증서를 갱신하거나 금융기관을 통해 해당 계좌에 대한 거래 중지를 요청하고 악성코드 감염 여부를 확인하는 것이 필요하다. 또한, 이체 후에는 반드시 이체 내용 확인을 통해 잘못된 계좌로 이체가 됐는지 점검해야 한다.

(7) 랜섬웨어(Ransomware)의 고도화

국내에서는 아직 큰 문제가 되지 않았지만, 여러 나라에서 랜섬웨어(Ransomware) 피해가 발생하고 있다. 랜섬웨어는 시스템 부팅 시 암호를 요구하거나 파일을 암호화해 시스템을 정상적으로 사용하지 못

하게 하고 금전을 요구하는 악성코드 종류이다.

랜섬웨어의 시초는 1989년으로 거슬러 올라간다. 1989년 12월 8일부터 12일까지 PC 사이보그사 (PC Cyborg Corporation)의 '에이즈 정보(AIDS Information)' 디스켓이 영국, 유럽, 아프리카, 오스트레일리아 등으로 보내졌다. 이 프로그램은 에이즈(AIDS, 후천성면역결핍증)에 대해 다루고 있다고 주장하지만 실제로는 하드디스크의 루트 디렉터리 정보를 암호화하는 트로이목마였다.

대표적인 최신 랜섬웨어는 2005년 러시아에서 발견된 Gpcode이다. 당시 랜섬웨어의 상당수는 간단한 암호화 기법을 이용해 악성코드 분석으로 복구 도구를 만들 수 있었다.

2013년 하반기 사용자 사진, 동영상, 문서 등을 암호화하는 크립토락커(Cryptolocker)가 여러 나라에서 피해를 일으켰다. 감염되는 순간 암호를 해제할 수 있는 키를 서버에 생성하고 암호 해제를 위한 금전을 요구한다. 달러, 유로, 비트코인류의 가상화폐 등 다양한 방식으로 지불할 수 있다. 특정 시간에 돈을 입금하지 않거나 사용자가 악성코드 제거를 시도하면 서버에 생성한 키를 파괴해 복구하지 못하도록 만든다.

국내에서는 2011년 중앙아시아 지역에서 제작된 랜섬웨어를 번역기를 이용해 만든 조잡한 한국어판이 발견된 바 있지만, 현재까지 대규모 피해는 확인되지 않고 있다. 그러나 다른 나라에서는 시스템을 사용하지 못하게 하고 협박하는 방식이 널리 이용되고 있다. 국내외 악성코드 제작자와 범죄 조직에서 국내 사용자를 대상으로 한 한국형 랜섬웨어가 등장할 가능성을 배제할 수 없다.

ASEC REPORT CONTRIBUTORS

집필진	선임연구원	박 종 석
	선임연구원	강 동 현
	선임연구원	이 도 현
	연구원	이 영 욱
	연구원	강 민 철
참여연구원	ASEC 연구원	
편집	안랩 콘텐츠기획팀	
디자인	안랩 UX디자인팀	
발행처	주식회사 안랩 경기도 성남시 분당구 삼평동 673 (경기도 성남시 분당구 판교역로 220) T. 031-722-8000 F. 031-722-8901	

AhnLab