ASEC REPORT

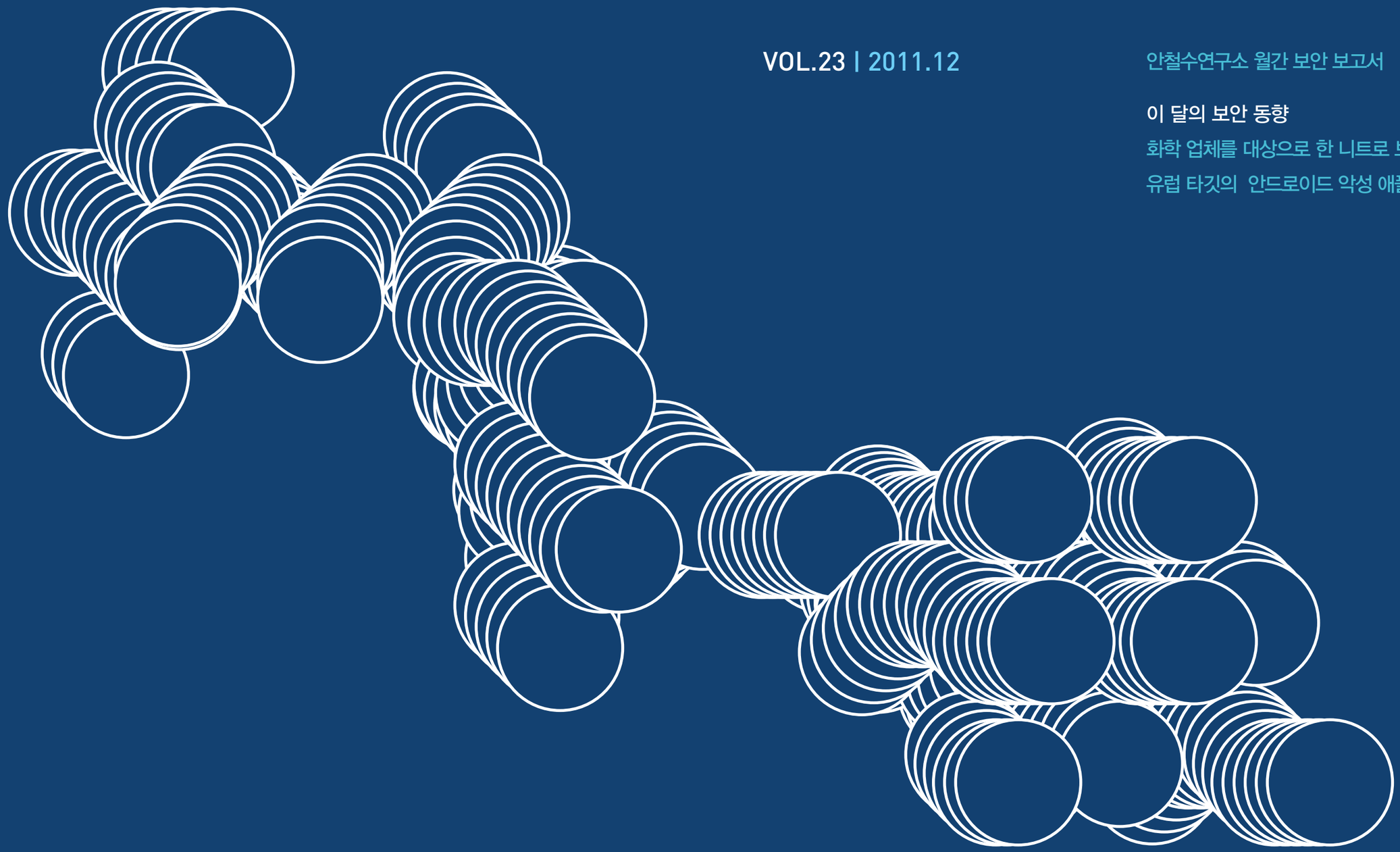
VOL.23 | 2011.12

안철수연구소 월간 보안 보고서

이 달의 보안 동향

화학 업체를 대상으로 한 니트로 보안 위협

유럽 타깃의 안드로이드 악성 애플리케이션



AhnLab

AhnLab Security Emergency response Center

ASEC (AhnLab Security Emergency response Center)은 악성코드 및 보안 위협으로부터 고객을 안전하게 지키기 위하여 보안 전문가로 구성된 글로벌 보안 조직입니다. 이 리포트는 ㈜안철수연구소의 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.

CONTENTS

01. 악성코드 동향
a. 악성코드 통계

악성코드 감염보고 Top 20

2011년 11월 악성코드 통계 현황은 다음과 같다. 2011년 11월의 악성코드 감염 보고는 JS/Agent가 가장 많았으며, JS/Downloader와 Exploit/Cve-2011-21400이 그 뒤를 이었다. 새로 Top20에 진입한 악성코드는 총 8건이다.

순위	등락	악성코드명	건수	비율
1	—	JS/Agent	1,165,455	21.1 %
2	NEW	JS/Downloader	989,033	17.9 %
3	▲3	Exploit/Cve-2011-2140	524,956	9.5 %
4	▼2	Textimage/Autorun	513,620	9.3 %
5	NEW	Win-Trojan/Agent.465408.T	384,719	6.9 %
6	NEW	Swf/Cve-2011-2140	290,108	5.2 %
7	NEW	Win-Trojan/Bho.65536.AV	214,805	3.9 %
8	▼3	JS/Redirector	169,398	3.1 %
9	NEW	Swf/Dropper	168,381	3.0 %
10	NEW	Html/Agent	135,588	2.5 %
11	NEW	JS/Exploit	130,755	2.4 %
12	▼2	Als/Bursted	119,703	2.2 %
13	▼5	Swf/Agent	117,136	2.1 %
14	▼5	Win-Trojan/Downloader.217088.AE	110,757	2.0 %
15	▼4	Win32/Induc	96,926	1.8 %
16	▼3	Win32/Palevo1.worm.Gen	89,723	1.6 %
17	NEW	Win-Trojan/Agent.129536.EM	88,023	1.6 %
18	▼11	Dropper/Malware.495616.HT	79,038	1.4 %
19	▼1	Win32/Olala.worm	72,436	1.3 %
20	—	RIPPER	66,185	1.2 %
			5,526,745	100.0 %

[표 1-1] 악성코드 감염보고 Top 20

악성코드 대표진단명 감염보고 Top 20

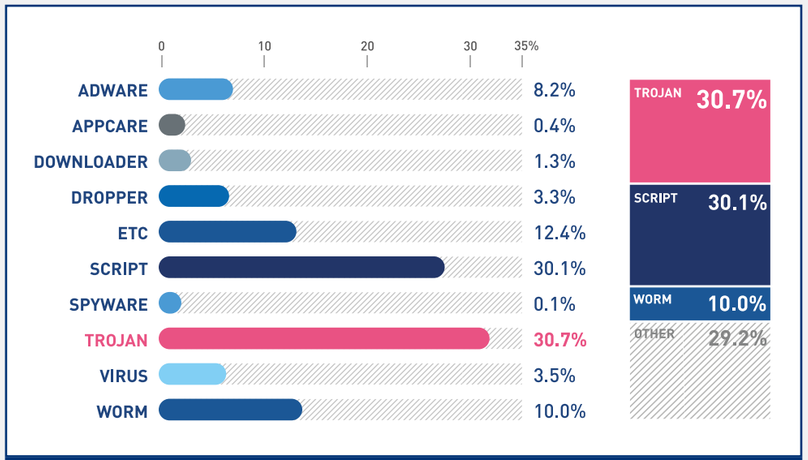
[표 1-2]는 악성코드별 변종 종합 감염 보고 순위를 악성코드 대표 진단명에 따라 정리한 것이다. 이를 통해 악성코드의 동향을 파악할 수 있다. 2011년 11월의 최다 감염 보고 건수는 JS/Agent가 총 1,275,839건으로 16.6%의 비율을 보였다. 또한 Win-Trojan/Agent가 998,945건/12.9%, JS/Downloader가 989,033건/12.8%로 조사됐다.

순위	등락	악성코드명	건수	비율
1	—	JS/Agent	1,275,839	16.6 %
2	—	Win-Trojan/Agent	998,945	12.9 %
3	NEW	JS/Downloader	989,033	12.8 %
4	▲11	Exploit/Cve-2011-2140	524,956	6.8 %
5	▲2	Win-Adware/Korad	515,227	6.7 %
6	▼3	Textimage/Autorun	513,718	6.7 %
7	▼2	Win-Trojan/Downloader	411,548	5.3 %
8	NEW	Swf/Cve-2011-2140	290,108	3.8 %
9	▼3	Win-Trojan/Onlinegamehack	264,039	3.4 %
10	▼2	Win32/Conficker	228,761	3.0 %
11	NEW	Win-Trojan/Bho	223,556	2.9 %
12	▼1	Win32/Autorun.worm	207,543	2.7 %
13	▼4	Win32/Virut	196,769	2.6 %
14	▼1	Win32/Kido	178,100	2.3 %
15	▼1	JS/Redirector	169,398	2.2 %
16	NEW	Swf/Dropper	168,381	2.2 %
17	▼5	Dropper/Malware	156,605	2.0 %
18	NEW	Html/Agent	135,588	1.8 %
19	NEW	JS/Exploit	130,755	1.7 %
20	NEW	Win-Downloader/Korad	123,765	1.6 %
			7,702,634	100 %

[표 1-2] 악성코드 대표진단명 감염보고 Top 20

악성코드 유형별 감염보고 비율

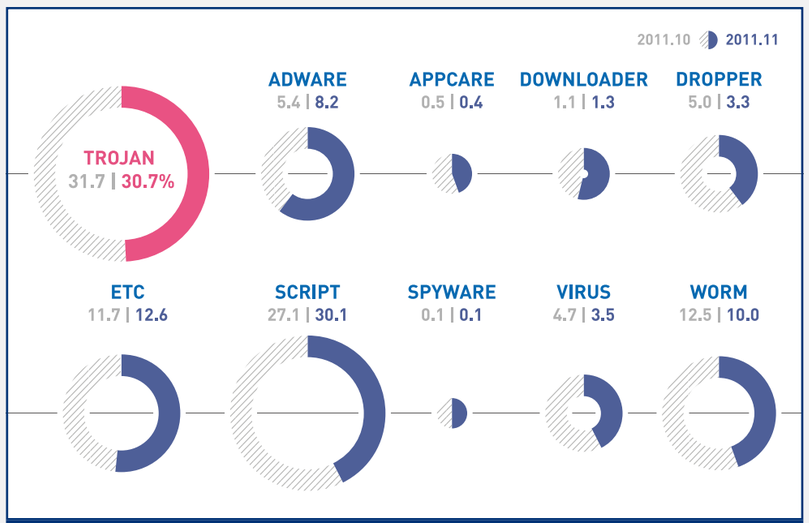
[그림 1-1]은 2011년 11월 한 달 동안 안철수연구소가 고객으로부터 감염이 보고된 악성코드의 유형별 감염 비율을 집계한 결과다. 2011년 11 월의 악성코드를 유형별로 살펴보면, 감염 보고 건수 비율은 트로이목마(TROJAN)가 30.7%로 가장 많았으며, 스크립트(SCRIPT)가 30.1%, 웜(WORM)이 10%로 나타났다.



[그림 1-1] 악성코드 유형별 감염보고 비율

악성코드 유형별 감염보고 전월 비교

악성코드 유형별 감염 보고 비율을 전월과 비교하면, 스크립트와 애드웨어(ADWARE), 다운로더(DOWNLOADER)는 전월에 비해 증가세를 보이고 있는 반면, 트로이목마, 웜, 바이러스(VIRUS), 드롭퍼(DROPPER), 애프케어(APPCARE)는 전월에 비해 감소했다. 스파이웨어(SPYWARE)는 전월 수준을 유지하고 있다.



[그림 1-2] 악성코드 유형별 감염보고 전월 비교

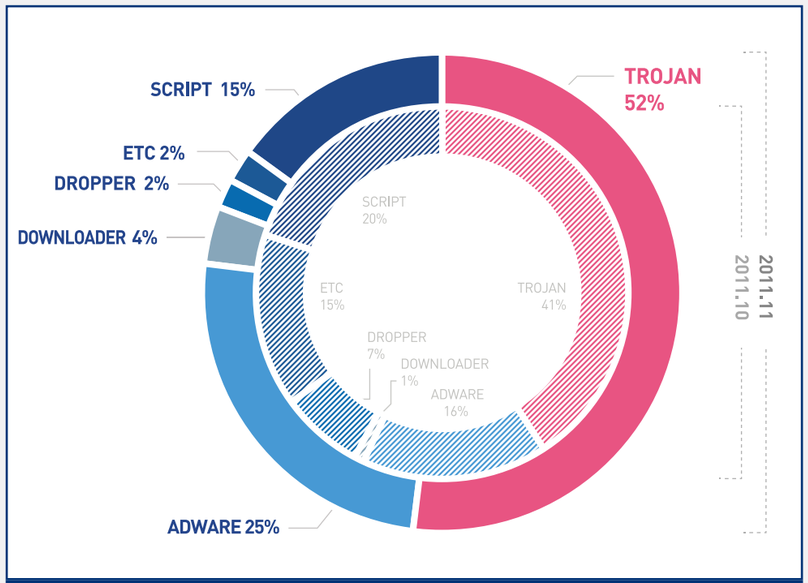
악성코드 월별 감염보고 건수

11월의 악성코드 월별 감염 보고 건수는 12,559,154건으로 10월의 10,498,643건에 비해 2,060,511건이 증가하였다.

[그림 1-3] 악성코드 월별 감염보고 건수

신종 악성코드 유형별 분포

11월의 신종 악성코드 유형을 보면 트로이목마가 52%로 가장 많았고, 애드웨어가 25%, 스크립트가 15%였다.



[그림 1-4] 신종 악성코드 유형별 분포

신종 악성코드 감염보고 Top 20

[표 1-3]은 11월에 신규 접수된 악성코드 중 고객으로부터 감염이 보고된 악성코드 Top20이다. Win-Trojan/Agent.465408.T가 384,719건으로 전체 26.1%, SWF/Cve-2011-21400이 290,108건/19.7%인 것으로 나타났다.

순위	악성코드명	건수	비율
1	Win-Trojan/Agent.465408.T	384,719	26.1 %
2	SWF/Cve-2011-2140	290,108	19.7 %
3	Win-Trojan/Bho.65536.AV	214,805	14.6 %
4	Win-Trojan/Agent.129536.EM	88,023	6.0 %
5	JS/Agent.E	58,518	4.0 %
6	Win-Trojan/Adload.413184.B	51,786	3.5 %
7	Win-Adware/OneStep.536064	48,344	3.3 %
8	Win-Trojan/Agent.434176.CO	34,585	2.3 %
9	Win-Adware/KorAd.438272.C	34,256	2.3 %
10	Win-Adware/OneStep.495616	33,749	2.3 %
11	Win-Adware/KorAd.499712.W	32,006	2.2 %
12	Win-Trojan/Downloader.65536.WR	28,759	1.9 %
13	Win-Trojan/Fakeav.2178560	28,499	1.9 %
14	Win-Trojan/Korad.660480	25,373	1.7 %
15	Win-Adware/Shortcut.WooriZip.1009152	23,720	1.6 %
16	Win-Downloader/KorAd.1760768	21,328	1.4 %
17	Win-Trojan/Agent.660480.F	20,690	1.4 %
18	Win-Adware/KorAd.450560	19,730	1.3 %
19	Win-Adware/KorAd.274432.L	19,632	1.3 %
20	Win-Trojan/Pcclient.434176	17,451	1.2 %
		1,476,081	100 %

[표 1-3] 신종 악성코드 감염보고 Top 20

01. 악성코드 동향
b. 악성코드 이슈

DNS 서버 이상? BIND 제로데이

DNS BIND 애플리케이션에 크래쉬가 발생하여 DSN 서비스가 중지되는 제로데이(Zero-day) 공격이 발생했다. BIND(Berkeley Internet name Daemon)는 네임서버를 운영하기 위해 설치하는 서버 측 소프트웨어로, 미국의 경우 90% 이상의 DNS가 이 소프트웨어를 사용하고 있다. 이번에 발견된 제로데이(CVE-2011-4313)는 캐시에 존재하지 않는 레코드를 돌려주는 과정에서 발생하는 취약점이었는데, 크래쉬가 발생하면 "INSIST(! dns_rdataset_isassociated(sigrdataset))"라는 로그를 남긴다.

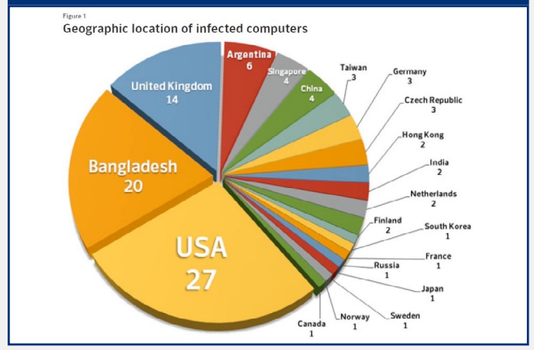
DNS에 취약점이 생기면 전 세계 수만 대의 DNS 중 1대만 공격을 받아도 매우 위험할 수 있다. 예를 들어 웹 주소가 원하지 않는 곳으로 접속되거나 메일이 잘못 전송될 수도 있다. 따라서 소프트웨어의 최신 업데이트는 DNS 관리자에게 매우 중요한 일이다.

[그림 1-5] CVE-2011-4313 BIND 취약점

화학 업체를 대상으로 한 니트로 보안 위협

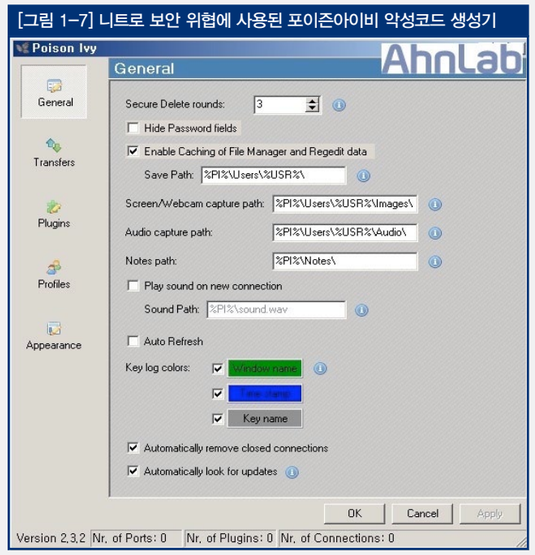
2011년 10월 31일 미국 보안 업체인 시만텍(Symantec)은 '니트로(Nitro)'라고 명명된 보안 위협을 공개하였다. 니트로 보안 위협은 4월 말경 인권 관련 NGO를 대상으로 처음 시작됐다. 화학 업체들을 대상으로 한 니트로 보안 위협은 2011년 7월에 시작되어 위협이 탐지된 9월까지 진행되었으며, 원격 제어를 위한 C&C(Command and Control) 서버는 4월경에 구축된 것으로 알려졌다. 공격 대상이 된 기업은 총 48개인데, 화학 관련 업체 29개, 군수 업체를 포함한 다른 업종의 기업이 19개다. 시만텍이 발표한 바에 따르면, 니트로 보안 위협에 의한 시스템 감염 사례는 미국과 방글라데시에서 가장 많았다.

[그림 1-6] 니트로 보안 위협에 의한 시스템 감염 사례의 국가별 분포



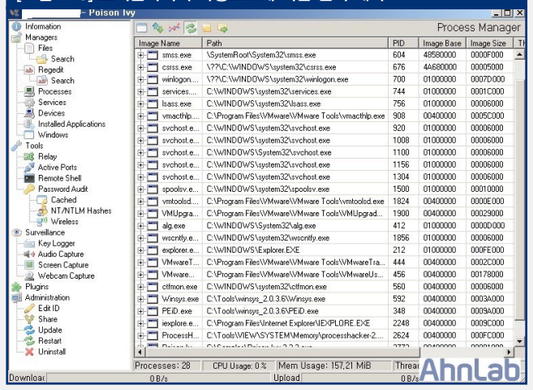
니트로 보안 위협은 전형적인 APT(Advance Persistent Threat) 형태의 공격으로 사회공학(Social Engineering) 기법을 포함하고 있는 이메일에 원격 제어 형태의 백도어인 포이즌아이비(Poisonlvy)가 첨부파일로 사용되었다. 니트로 보안 위협의 공격자는 [그림 1-7]과 유사한 포이즌아이비 툴 킷들을 이용하여 악성코드를 제작한 것으로 추정된다.

[그림 1-7] 니트로 보안 위협에 사용된 포이즌아이비 악성코드 생성기



공격에 사용된 악성코드 대부분은 RARSfx로 압축된 파일로, 해당 파일들이 실행되면 사용자 계정의 Temp 폴더에 자신의 복사본을 생성한다. 생성된 복사본은 인터넷 익스플로러의 스레드(Thread)에 자신의 코드를 삽입하여 C&C 서버와 통신을 시도하고 공격자의 명령에 따라 악의적인 기능을 수행한다. 수행되는 악의적인 기능은 [그림 1-8]과 같이 감염된 시스템에서 실행 중인 프로세스(Process) 리스트에서부터 레지스트리(Registry) 및 키로깅(Keylogging)까지 다양하다.

[그림 1-8] 포이즌아이비 악성코드에 의한 원격 제어



이번에 공개된 니트로 보안 위협에 대해 ASEC에서 추가 조사를 진행했는데 해당 보안 위협에 악용된 악성코드들은 약 50개인 것으로 나타났다. 니트로 보안 위협에 사용된 악성코드들은 V3 제품군에서 다음과 같이 진단한다.

[표 1-4] 니트로 보안 위협에 사용된 악성코드 진단명

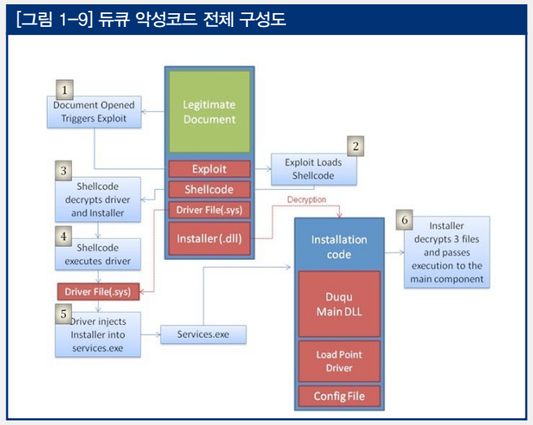
Dropper/Agent.136569	Win-Trojan/Poison.111104.M
Dropper/Agent.136569	Win-Trojan/Poison.133951
PDF/Exploit	Win-Trojan/Poison.147456
Win-Trojan/Adsagent.132031	Win-Trojan/Poison.150937
Win-Trojan/Adsagent.132031	Win-Trojan/Poison.150937
Win-Trojan/Adsagent.136314	Win-Trojan/Poison.154539
Win-Trojan/Adsagent.141530	Win-Trojan/Poison.155705
Win-Trojan/Adsagent.141530	Win-Trojan/Poison.155705
Win-Trojan/Adsagent.153026	Win-Trojan/Poison.27136.R
Win-Trojan/Adsagent.153026	Win-Trojan/Poison.43520.P
Win-Trojan/Adsagent.7680.E	Win-Trojan/Poison.62464.AA
Win-Trojan/Agent.159762	Win-Trojan/Poisoniv.128204
Win-Trojan/Agent.159762	Win-Trojan/Poisoniv.128204
Win-Trojan/Bumat.111104	Win-Trojan/Poisoniv.128405
Win-Trojan/Downbot.153938	Win-Trojan/Poisoniv.128421
Win-Trojan/Gendal.62464	Win-Trojan/Poisoniv.133511
Win-Trojan/Hupigon.133007	Win-Trojan/Poisoniv.133511
Win-Trojan/Injecter.62464.D	Win-Trojan/Poisoniv.135794
Win-Trojan/Injector.26624.AN	Win-Trojan/Poisoniv.135794
Win-Trojan/Injector.3073	Win-Trojan/Poisoniv.150357
Win-Trojan/Injector.89088.AL	Win-Trojan/Poisoniv.150357
Win-Trojan/Injector.89600.BP	Win-Trojan/Poisoniv.154827
Win-Trojan/Magania.240239	Win-Trojan/Poisoniv.154827
Win-Trojan/Magania.3399704	Win-Trojan/Poisoniv.173068
	Win-Trojan/Poisoniv.173068
	Win-Trojan/Poisoniv.177722
	Win-Trojan/Poisoniv.532499
	Win-Trojan/Poisoniv.536397

이러한 APT 형태의 보안 위협은 단일 보안 제품만으로는 대응할 수 없으므로 사내 보안 정책과 직원들을 대상으로 한 보안 인식 교육, 그리고 유기적으로 동작하는 각 단계에 맞는 보안 제품들의 다단계적인 대응(Defense in Depth)이 함께 이루어져야 한다.

윈도우 커널 제로데이 취약점을 이용한 '듀큐' 악성코드

지난 2011년 10월 18일 시만텍은 스턱스넷(Stuxnet)의 변형인 듀큐(Duqu) 악성코드가 발견되었다고 블로그('W32.Duqu: The Precursor to the Next Stuxnet')와 분석 보고서('W32.Duqu The precursor to the next Stuxnet')를 통해 공개하였다. 시만텍은 "듀큐 악성코드가 2009년 발견되었던 스턱스넷 악성코드와 유사한 형태를 보이고 있으며, 동일 인물이나 동일 그룹이 제작한 것으로 추정된다"고 밝혔다.

[그림 1-9] 듀큐 악성코드 전체 구성도



듀큐는 스턱스넷과 달리 산업 제어 시스템과 관련된 코드와 자체 전파 기능은 존재하지 않았지만, C&C 서버를 통한 원격 제어, 키로깅을 통한 정보 수집 기능, 시스템에 감염된 지 36일이 지나면 자동 삭제하는 기능이 포함되어 있다. 블로그 〈Duqu: Status Updates Including Installer with Zero-Day Exploit Found〉에서는 듀큐가 [그림 1-9]와 같이 마이크로소프트 윈도우 제로데이 취약점을 악용했다고 분석했다.

제로데이 취약점은 마이크로소프트 워드 파일을 이용한 윈도우 커널(Windows Kernel) 관련 취약점으로 윈도우의 Win32k 트루타입 폰트 파싱 엔진(TrueType font parsing engine)에 존재하며, 이로 말미암아 임의의 코드가 실행될 수 있다. 11월 현재 이 취약점은 CVE-2011-3402인데, 마이크로소프트에서는 〈Microsoft Security Advisory (2639658) Vulnerability in TrueType Font Parsing Could Allow Elevation of Privilege〉라는 보안 권고문에서 이를 자세하게 공개하였다. 마이크로소프트는 또한 〈Microsoft Security Advisory: Vulnerability in TrueType font parsing could allow elevation of

privileges〉를 통해 임시로 이 취약점을 제거할 수 있는 Fix It 툴도 공개하였다. 이 취약점은 보안 패치가 제공되지 않는 제로데이 상태이며, 다른 악성코드나 보안 위협에서 악용할 가능성이 있으므로 공개된 Fix It을 통해 취약점을 제거해야 한다. 그러나 이 Fix It은 임시 방편이므로 향후 정식 보안 패치를 설치하는 것이 필요하다. 해당 듀큐 악성코드들은 V3 제품군에서 다음과 같이 진단한다.

Win-Trojan/Duqu.6656
Win-Trojan/Duqu.68096
Win-Trojan/Duqu.24960.B
Win-Trojan/Duqu.29568
Win-Trojan/Duqu.24960
Win-Trojan/Duqu
Win-Trojan/Agent.85504.HN
Worm/Win32.Stuxnet

네트워크 분석기, 와이어샤크를 겨냥한 exploit

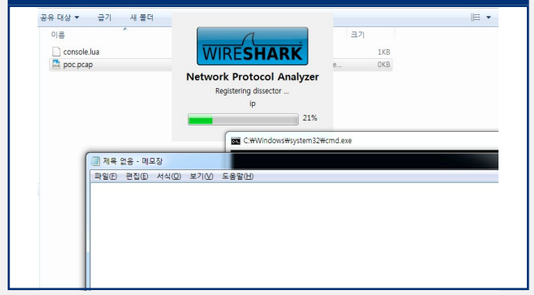
분석가들이 가장 많이 사용하는 네트워크 캡처 & 분석기인 와이어샤크(wireshark.org) 자체의 취약점을 이용한 Overflow 공격 형태는 오래전부터 알려져 있었다. 이번에 발견된 취약점은 1.6.1 이하 버전의 와이어샤크가 실행될 때 로딩하는 console.lua 파일을 조작하는 것이다. 이 프로그램이 실행될 때, 현재 디렉터리에 console.lua 파일이 있으면 파일의 코드를 실행한다. 공격자는 이 파일에 원하는 공격 코드를 삽입하여 WebDAV나 SMB로 파일을 공유하고, 같은 위치에 있는 .pcap 파일이 실행될 때, console.lua 파일 내에 있는 공격 코드가 실행된다. [그림 1-10]은 정상적인 console.lua 파일 내용이다.

[그림 1-10] 정상적인 wireshark console.lua 파일 내용

```
-- By Gerald Combs <gerald@wireshark.org>
-- Copyright 1998 Gerald Combs
--
-- This program is free software; you can redistribute it and/or
-- modify it under the terms of the GNU General Public License
-- as published by the Free Software Foundation; either version 2
-- of the License, or (at your option) any later version.
--
-- This program is distributed in the hope that it will be useful,
-- but WITHOUT ANY WARRANTY; without even the implied warranty of
-- MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE.  See the
-- GNU General Public License for more details.
--
-- You should have received a copy of the GNU General Public License
-- along with this program; if not, write to the Free Software
-- Foundation, Inc., 59 Temple Place - Suite 330, Boston, MA  02111-1307, USA.


if (gui_enabled()) then
    -- Note that everything is "local" to this "if then"
    -- this way we don't add globals

    -- Evaluate Window
    local function evaluate_lua()
        local w = TextWindow.new("Evaluate Lua")
        w:set_editable()

        -- button callback
        local function eval()
            -- get the window's text and remove the result
            local text = string.gsub(w:get_text(),"%c*--%[%[.*--%]%]$","")
```

[그림 1-11]은 취약한 와이어샤크 버전에서 console.lua 파일에 notepad.exe를 실행하도록 작성한 코드가 실행된 결과다.

[그림 1-11] console.lua 파일의 notepad.exe를 실행하도록 작성한 코드가 실행된 결과



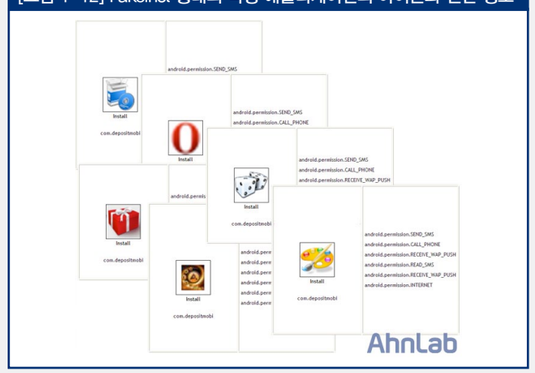
타깃 공격이 극성을 부리고 있는 요즘, 어느 소프트웨어 하나 무심코 지나칠 수 없다. 특히 와이어샤크는 자동 업데이트를 지원하지 않으므로 특히 주의해야 한다.

안드로이드 악성코드 FakeInst 변종 1600개로 급증

최근 안드로이드 악성코드의 변종 중 FakeInst 형태의 안드로이드 악성코드가 급증하고 있다. FakeInst는 다른 애플리케이션의 설치를 가장하여 악의적인 행위를 하는 악성 애플리케이션을 뜻한다. 아래의 내용은 패키지 'com.depositmobi'인 안드로이드 악성 애플리케이션을 대상으로 확인한 결과다.

1. Android Manifest 정보가 6개의 애플리케이션 모두 동일

[그림 1-12] FakeInst 형태의 악성 애플리케이션의 아이콘과 권한 정보

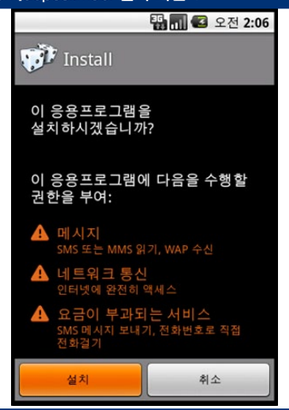


[그림 1-13] Android Manifest 정보

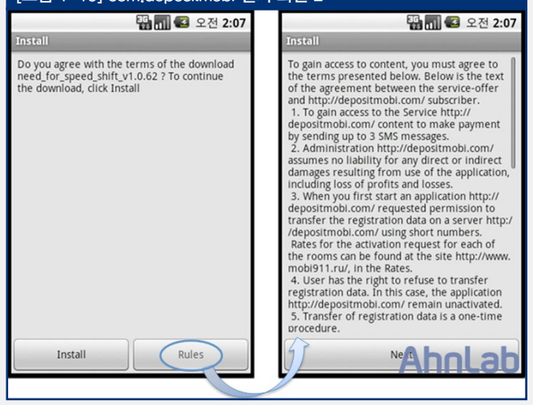
2. 설치 과정의 특징

[그림 1-14]의 Rules를 선택하면 애플리케이션의 행위에 대한 정보를 보여준다. 과금이 발생할 수 있음을 알리고 있지만, 추가 설치되는 애플리케이션에 대한 지급은 아니다.

[그림 1-14] com.depositmobi 설치 화면 1

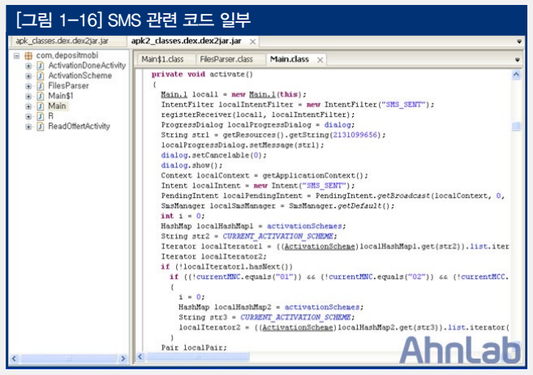


[그림 1-15] com.depositmobi 설치 화면 2



3. SMS 과금 유발 코드 존재

[그림 1-16] SMS 관련 코드 일부



다운로드되는 애플리케이션과 URL이 존재한다.

[그림 1-17] 다운로드 URL 정보

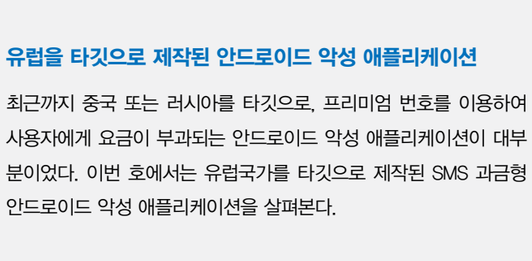
```
1  Opera-Mini-6
2  http://dow***-free-files.ru/o****-android.php
3
4  12
5  469+16+p+a
```

AhnLab

premium numbers 과금 관련 안내 코드가 존재한다.

ex) 7151 : 33.87 ~ 40.00 루브

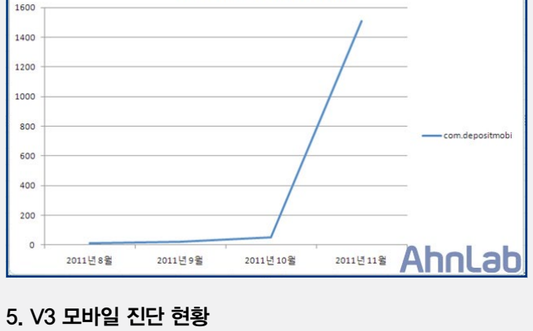
[그림 1-18] 과금 안내 코드 일부



4. 변종 추이

8월부터 꾸준히 발생했으며, 현재는 1600개를 넘어섰다.

[그림 1-19] Android-Trojan/FakeInst 변종 추이 (대상 패키지 : com.depositmobi)



5. V3 모바일 진단 현황

V3 모바일 제품군에서 다음과 같이 진단한다.

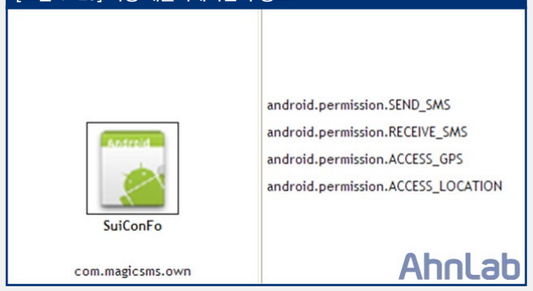
Android-Trojan/SmsSend
Android-Trojan/FakeInst
Android-Trojan/Agent
Android-Trojan/Boxer

유럽을 타깃으로 제작된 안드로이드 악성 애플리케이션

최근까지 중국 또는 러시아를 타깃으로, 프리미엄 번호를 이용하여 사용자에게 요금이 부과되는 안드로이드 악성 애플리케이션이 대부분이었다. 이번 호에서는 유럽국가를 타깃으로 제작된 SMS 과금형 안드로이드 악성 애플리케이션을 살펴본다.

1. SuiConFo 안드로이드 악성 애플리케이션 정보

[그림 1-20] 악성 애플리케이션의 정보



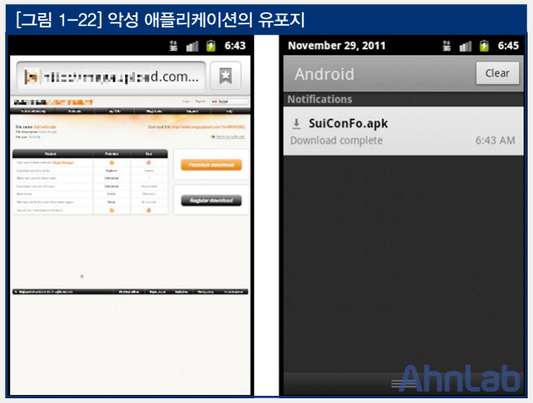
– Android 2.2(Froyo 2.2) 이상에서 설치 가능하다.
– SEND_SMS 권한으로 보아 과금 발생 가능성이 추정된다.

[그림 1-21] Android Manifest 정보

2. 설치 및 특징

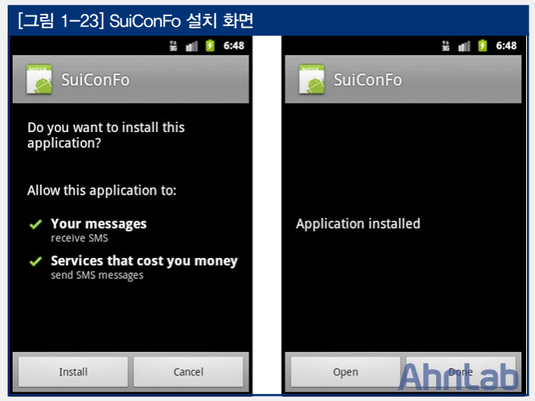
– SMSReceiver class 기능
– 81001, 35064, 63000 등의 번호로 수신된 SMS를 사용자가 알 수 없도록 숨긴다.
– SMS 수신하는 기능과 함께, 제작자로 추정되는 번호로 SMS를 전송한다(통계를 위한 전송으로 추정된다).

[그림 1-22] 악성 애플리케이션의 유포지



– 웹 사이트가 저장되어 있으며, 다운로드가 가능하다.

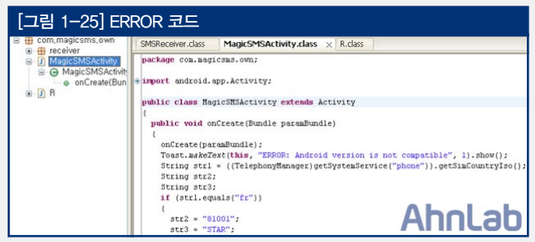
[그림 1-23] SuiConFo 설치 화면



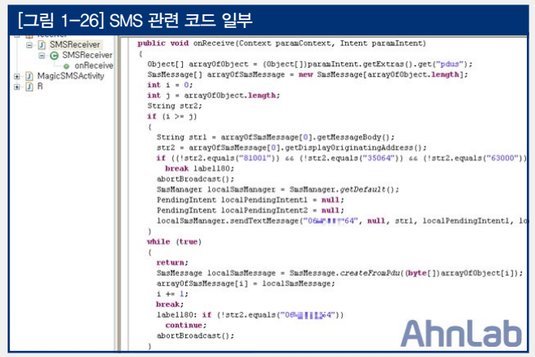
[그림 1-24] 설치된 악성 애플리케이션/실행화면(ERROR)

– 애플리케이션 실행 시 화면의 ERROR는 아래의 코드에 의해 실행된 것이다.

[그림 1-25] ERROR 코드



[그림 1-26] SMS 관련 코드 일부



[그림 1-27] 국가별 SMS 코드

– 악성 애플리케이션 제작자는 캐나다를 코딩하면서 실수 한 것으로 추정된다. str2 str3 부분이 반대로 코딩되어 있다.

– SuiConFo의 애플리케이션이 모두 악성은 아니다. 해당 이름으로 제작된 정상적인 애플리케이션도 존재한다.

3. 스마트폰 안전수칙

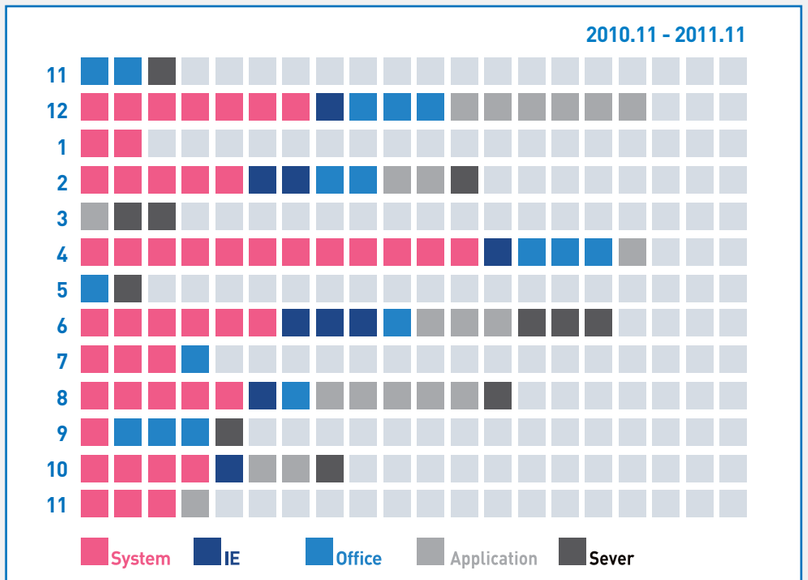
다음과 같은 수칙을 반드시 지켜 악성코드로부터 스마트폰을 안전하게 보호할 것을 권장한다.

1. 애플리케이션을 설치하거나 이상한 파일을 다운로드한 경우에는 반드시 악성코드 검사를 실시한다.
2. 게임 같은 애플리케이션을 다운로드할 때는 먼저 다른 사용자가 올린 평판 정보를 면밀히 확인한다.
3. 브라우저나 애플리케이션으로 인터넷에 연결 시 이메일이나 문자 메시지에 있는 URL은 신중하게 클릭한다.
4. PC로부터 파일을 전송받을 경우 악성코드 여부를 꼭 확인한다.
5. 백신의 패치 여부를 확인해서 최신 백신 엔진을 유지한다.
6. 스마트폰의 잠금 기능(암호 설정)을 이용해서 다른 사용자의 접근을 막는다. 잠금 기능에 사용한 비밀번호는 수시로 변경한다.
7. 블루투스 기능 같은 무선 기능은 필요할 때만 켜놓는다.
8. ID, 비밀번호 등을 스마트폰에 저장하지 않는다.
9. 주기적으로 백업해서 분실 시 정보의 공백이 생기지 않도록 한다.
10. 임의로 개조하지 않고 복사 방지 같은 기능을 해제하지 않는다.

02. 시큐리티 동향
a. 시큐리티 통계

11월 마이크로소프트 보안 업데이트 현황

마이크로소프트가 제공하는 이달의 보안 업데이트는 4건이며 총 4건의 패치가 발표되었다.



[그림 2-1] 공격 대상 기준별 MS 보안 업데이트

위험도	취약점
긴급	TCP/IP 취약점으로 인한 원격 코드 실행 문제점 (MS11-083)
중요	Windows Mail 및 Windows meeting Space의 취약점으로 인한 원격 코드 실행 문제점 (MS11-085)
중요	Active Directory의 취약점으로 인한 권한 상승 문제점 (MS11-086)
보통	Windows 커널 모드 드라이버의 취약점으로 인한 서비스 거부 문제점 (MS11-084)

[표 2-1] 2011년 11월 주요 MS 보안 업데이트

● MS11-083은 Reference Counter Overflow 취약점으로 Vista, Windows7, Windows Server 2008시스템에 닫힌 포트로 조작된 UDP 패킷을 연속적으로 보내면 TCP/IP의 취약점으로 말미암아 원격 코드가 실행될 수 있다. 해당 취약점에 관련된 공개된 PoC는 없으나 YouTube나 pastebin 사이트에서 관련 동영상과 exploit을 실행한 흔적을 찾아볼 수 있다. 일각에서 사실 여부가 논란이 되고 있지만, 위험도가 높은 만큼 각별한 주의와 업데이트가 필요하다.

[그림 2-2] MS11-083 공격 가능성 시연 동영상 (www.youtube.com/watch?v=4aBE6o0oDlo)

● MS11-084는 트루타입 폰트 파싱 취약점으로 조작된 트루타입 글꼴 파일을 열거나 조작된 트루타입 글꼴 파일이 있는 네트워크 공유 또는 WebDAV 위치로 이동하는 경우 서비스 거부 상태에 도달할 수 있다. 공격자는 메일이나 메신저로 링크를 통해 파일을 열도록 유도한다.

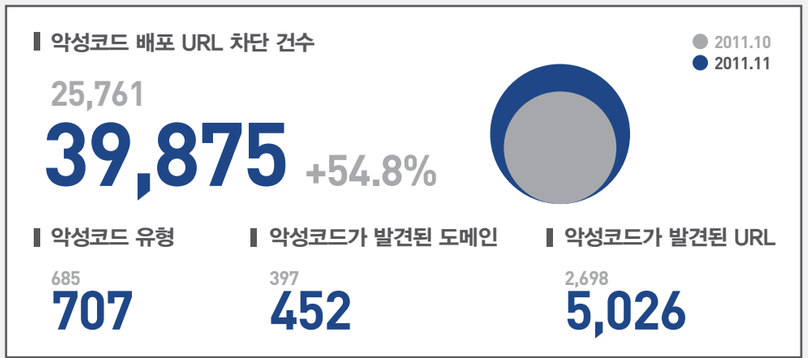
● MS11-085는 Windows Mail Insecure Library Loading 취약점으로 조작된 DLL 파일과 동일한 네트워크 디렉터리에 있는 .eml, .wcinv 파일을 여는 경우, 원격 코드가 실행 될 수 있다.

● MS11-086은 LDAPS Authentication Bypass 로 Active 디렉터리가 LADAPS를 사용하도록 설정한 후 공격자는 해지된 인증서를 이용하여 도메인에 인정받는 경우 권한이 상승될 수 있다.

03. 웹 보안 동향
a. 웹 보안 통계

웹사이트 보안 요약

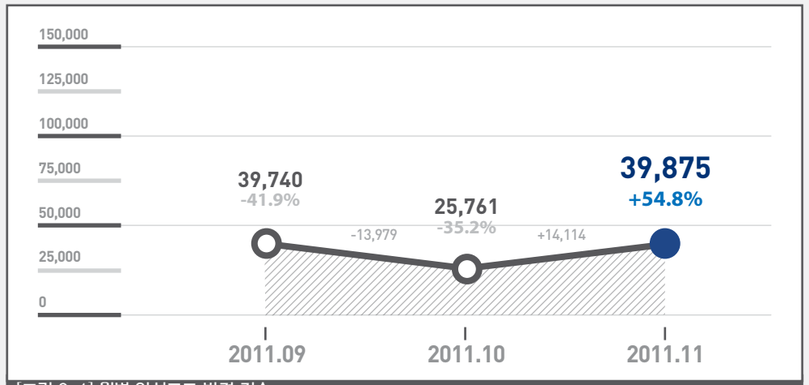
안철수연구소의 웹 브라우저 보안 서비스 사이트가드(SiteGuard)를 활용한 웹 사이트 보안 통계 자료에 따르면, 2011년 11월 악성코드를 배포하는 웹 사이트의 차단 건수는 총 39,875건이다. 또한 악성코드 유형은 707건이며, 악성코드가 발견된 도메인은 452건, 악성코드가 발견된 URL은 5,026건으로 2011년 10월보다 전반적으로 증가하였다.



[표 3-1] 웹 사이트 보안 요약

월별 악성코드 배포 URL 차단 건수

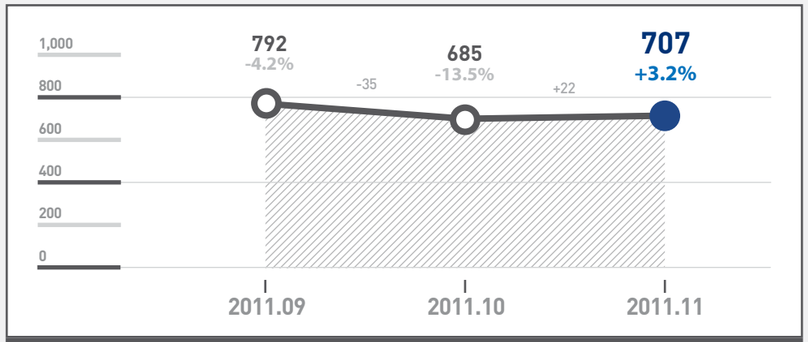
2011년 11월 악성코드 배포 웹 사이트 URL 접근에 따른 차단 건수는 지난달 25,761건에 비해 55% 증가한 39,875건이다.



[그림 3-1] 월별 악성코드 발견 건수

월별 악성코드 유형

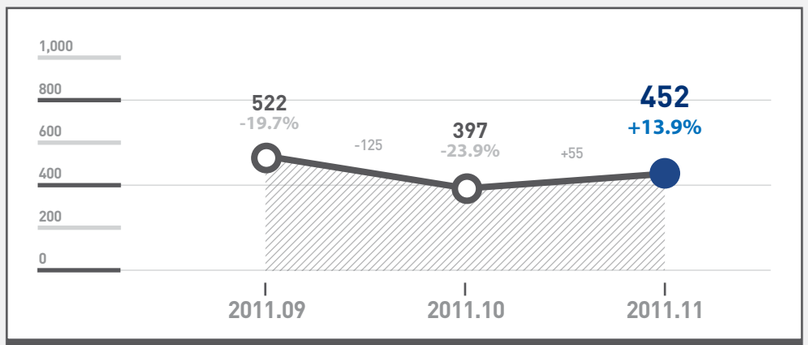
2011년 11월 악성코드 유형은 전달의 685건에 비해 3% 늘어난 707건이다.



[그림 3-2] 월별 악성코드 유형

월별 악성코드가 발견된 도메인

2011년 11월 악성코드가 발견된 도메인은 10월의 397건에 비해 14% 증가한 452건이다.



[그림 3-3] 월별 악성코드가 발견된 도메인

월별 악성코드가 발견된 URL

2011년 11월 악성코드가 발견된 URL은 전달의 2,698건에 비해 86% 늘어난 5,026건이다.

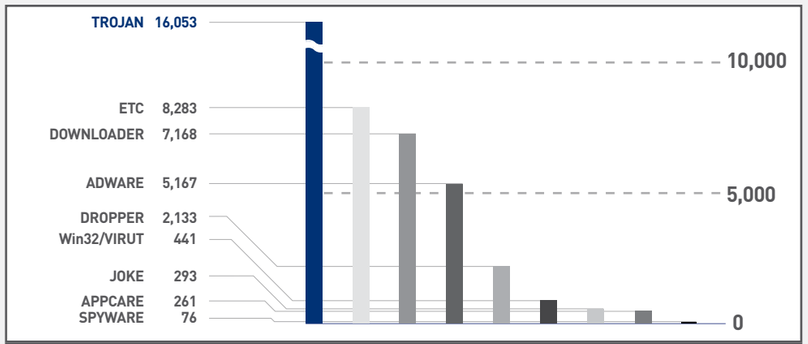
[그림 3-4] 월별 악성코드가 발견된 URL

악성코드 유형별 배포 수

악성코드 유형별 배포 수를 보면, 트로이목마가 16,053건/40.3%로 가장 많았고, 다운로더가 7,168건/18.0%인 것으로 조사됐다.

유형	건수	비율
TROJAN	**16,053**	**40.3 %**
DOWNLOADER	7,168	18.0 %
ADWARE	5,167	13.0 %
DROPPER	2,133	5.3 %
Win32/VIRUT	441	1.1 %
JOKE	293	0.7 %
APPCARE	261	0.7 %
SPYWARE	76	0.2 %
ETC	8,283	20.7 %
	39,875	**100.0 %**

[표 3-2] 악성코드 유형별 배포 수



[그림 3-5] 악성코드 유형별 배포 수

악성코드 배포 순위

악성코드 배포 건수는 Win-Trojan/Agent.1314816.M이 4,604건으로 가장 많았다. 또 Win-Trojan/Agent.1314816.M 등 8건이 Top10에 새로 등장하였다.

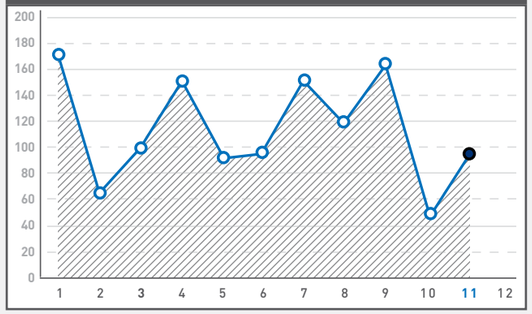
순위	등락	악성코드명	건수	비율
1	**NEW**	**Win-Trojan/Agent.1314816.M**	**4,604**	**22.7 %**
2	NEW	Downloader/Win32.Genome	3,604	17.8 %
3	NEW	Trojan/Win32.Amber	2,778	13.7 %
4	▼3	Win-Adware/ToolBar.Cashon.308224	1,663	8.2 %
5	NEW	Downloader/Win32.Korad	1,588	7.8 %
6	NEW	Unwanted/Win32.WinKeygen	1,456	7.2 %
7	NEW	Win32/Parite	1,355	6.7 %
8	NEW	Downloader/Win32.Totoran	1,328	6.5 %
9	▼6	Win-Trojan/Buzus.430080.J	1,066	5.3 %
10	NEW	VBS/Agent	855	4.1 %
			20,297	**100.0 %**

[표 3-3] 악성코드 배포 Top 10

03. 웹 보안 동향
b. 웹 보안 이슈

2011년 11월 침해 사이트 현황

[그림 3-6] 2011년 11월 악성코드 유포 목적의 침해 사이트 현황



[그림 3-6]은 악성코드 유포를 목적으로 하는 침해 사고가 발생했던 사이트의 현황이다. 2011년 11월의 경우, 10월보다 2배 정도 증가하였는데, 다른 웹 페이지에 취약점이 존재했거나 공격 대상에서 일시적으로 제외되었다가 공격이 재개되면서 악성코드를 유포했기 때문인 것으로 추정된다.

[표 3-4] 침해 사이트를 통해서 유포된 악성코드 Top 10

순위	악성코드명	건수
1	**Dropper/Win32.OnlineGameHack**	**38**
2	Dropper/Win32.OnlineGameHack	36
3	Trojan/Win32.OnlineGameHack	29
4	Dropper/Win32.OnlineGameHack	27
5	Trojan/Win32.OnlineGameHack	26
6	Dropper/Win32.OnlineGameHack	25
7	Dropper/Win32.OnlineGameHack	22
8	Trojan/Win32.OnlineGameHack	22
9	Dropper/Win32.OnlineGameHack	20
10	Dropper/Onlinegamehack.106115.C	19

[표 3-4]는 한 달간 침해 사이트를 통해서 가장 많이 유포된 악성코드 Top 100이다. 2011년 11월의 경우 Dropper/Win32.OnlineGameHack이 대부분이며 Trojan/Win32.OnlineGameHack 역시 드롭퍼에 의해서 파생된 특정 온라인 게임 사용자의 계정 정보를 탈취하기 위한 DLL이다.

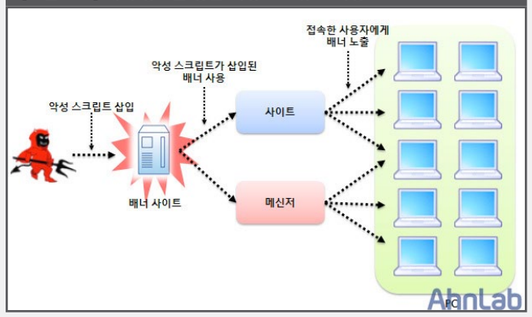
보통 해킹된 사이트를 통해서 유포되는 악성코드들은 imm32.dll을 패치하는 것과 ws2help.dll을 교체하는 것들이 대부분이었다. 그 비율은 보통 4:6이었으나 11월 마지막 주에는 imm32.dll을 패치하는 경우는 거의 찾아볼 수 없었고 ws2help.dll을 교체하는 악성코드의 비율이 높았다. 이처럼 imm32.dll을 패치하는 경우가 급격히 감소한 것은 V3에서 지속적으로 패치된 imm32.dll을 광범위하게 진단 및 치료할 수 있도록 Win-Trojan/PatchedImm7.Gen 등으로 대응해 왔기 때문인 것으로 보인다.

안철수연구소는 ASEC 블로그에서 배너 광고를 통한 악성코드 유포 사례에 대해서 여러 차례 다룬 바 있다.

1. 악성코드 유포는 어떻게?

이번에 발견된 사례는 [그림 3-7]과 같은 형식으로 유포 됐다.

[그림 3-7] 배너 광고를 통한 악성코드 유포 과정



2. 악성코드 감염은 어떻게?

[그림 3-8]처럼 악성 스크립트가 삽입된 배너 광고에 노출된 PC에 보안 취약점이 존재했다면 악성코드에 감염되었을 확률이 높다.

악성 스크립트가 정상적으로 동작하면 브라우저 버전, 취약점 등 조건에 따라 최종적으로 아래 주소에서 악성코드를 다운로드 및 실행한다.
'http://***.78.***.175/Ags/AGS.gif '

배너 광고에 노출된 PC에 악성코드를 다운로드 및 실행하기 위해서

사용된 취약점은 아래와 같다.

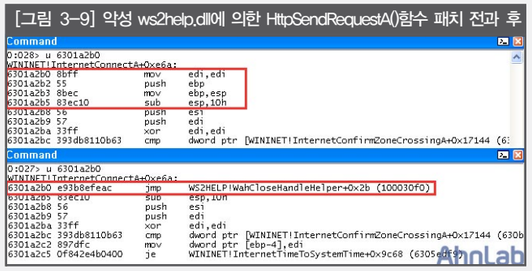
– CSS 메모리 손상 취약점(MS11-003, CVE-2010-3971)
http://technet.microsoft.com/ko-kr/security/bulletin/ms11-003

– Adobe Flash Player 취약점: CVE-2011-2140
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2140
http://www.adobe.com/support/security/bulletins/apsb11-21.html

위 취약점들을 사용한 악성 스크립트에 포함된 쉘코드는 암호화된 URL을 가지고 있으며 복호화한 후 다운로드 및 실행하도록 되어 있다.

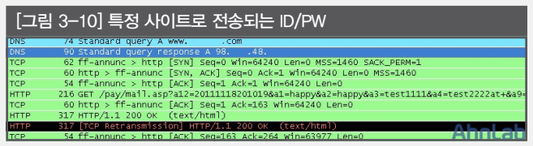
3. 악성코드에 의한 계정 탈취는 어떻게?

[그림 3-9] 악성 ws2help.dll에 의한 HttpSendRequestA()함수 패치 전과 후



[그림 3-9]를 보면 악성 ws2help.dll에 의해서 HttpSendRequestA() 함수가 패치될 경우 0x100030f0란 주소로 분기하도록 되어 있음을 알 수 있다. 위와 같이 하는 이유는 사용자가 입력한 ID/PW를 정상 사이트로 전송하기 전에 악성 ws2help.dll에 의해서 입력된 계정 정보를 탈취하기 위한 것이고 [그림 3-10]에서 보는 것처럼 특정 사이트로 전송된다.

[그림 3-10] 특정 사이트로 전송되는 ID/PW



VOL. 23
ASEC REPORT Contributors

집필진
선임 연구원 안 창 용
선임 연구원 장 영 준
주임 연구원 이 도 현
연구원 박 정 우

참여연구원 ASEC 연구원
SiteGuard 연구원

편집장
선임 연구원 안 형 봉

편집인 안철수연구소
마케팅실

디자인 안철수연구소
UX디자인팀

감 수
상 무 조 시 행

발행처 (주)안철수연구소
경기도 성남시 분당구
삼평동 673
(경기도 성남시 분당구
판교역로 220)
T. 031-722-8000
F. 031-722-8901

AhnLab