ASEC REPORT

안철수연구소에서 발행하는 월간 보안 보고서

2009. Volume.10

Ahn 안철수연구소

Table Of Contents

이달의 보안 동향

Ⅰ. 이달의 보안 동향

1. 악성코드 동향

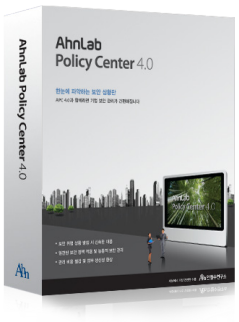
2009년 10월 ASEC 리포트부터는 기존의 고객신고에 기반한 통계치의 한계를 넘어, 현 상황을 정확하게 반영하고자, AhnLab에서 독자 개발한 "AMP[1] " 을 이용하여 산출한 통계데이터를 사용하도록 개선하였다.

악성코드 통계

순위	등락	악성코드명	건수	비율
1	–	Win32/Induc	804,573	32.5 %
2	–	TextImage/Autorun	347,871	14 %
3	–	Win32/Virut.B	158,088	6.4 %
4	New	JS/Shellcode	105,339	4.3 %
5	–	Win32/Virut	103,966	4.2 %
6	New	HTML/Agent	96,764	3.9 %
7	↑ 2	Win32/Parite	94,379	3.8 %
8	↓ 2	Win32/Conficker.worm.Gen	93,462	3.8 %
9	↓ 2	TextImage/Sasan	87,069	3.5 %
10	New	Win32/Olala.worm.57344	66,698	2.7 %
11	New	HTML/Crypted	61,452	2.5 %
12	New	ALS/Bursted	61,242	2.5 %
13	↓ 9	VBS/Agent	58,497	2.4 %
14	New	VBS/Autorun	54,744	2.2 %
15	New	Dropper/Malware	53,373	2.2 %
16	New	Win32/Traxg.worm.61440	52,505	2.1 %
17	New	Win32/IRCBot.worm.variant	51,298	2.1 %
18	New	Win-Trojan/Agent.299008.AY	43,168	1.7 %
19	New	Win-Trojan/MalPacked.Gen	42,251	1.7 %
20	New	Win-AppCare/HideWin.31232	41,628	1.7 %
합계			2,478,367	100%

[표 1-1] 악성코드 감염 보고 Top 20

2009년 10월의 악성코드 감염 보고는 Win32/Induc이 1위를 차지하고 있으며, 신규로 Top 20에 진입한 악성코드는 총 12건이다.



AhnLab Policy Center 4.0

1 AhnLab Malicious code Processing : 각종 피해 자료들을 수집하여 정제, 분석을 통해 현 상황에 대한 객관적인 판단이 가능하도록 사실에 기반한 통계 Data를 제공하는 위협 종합 분석 시스템.

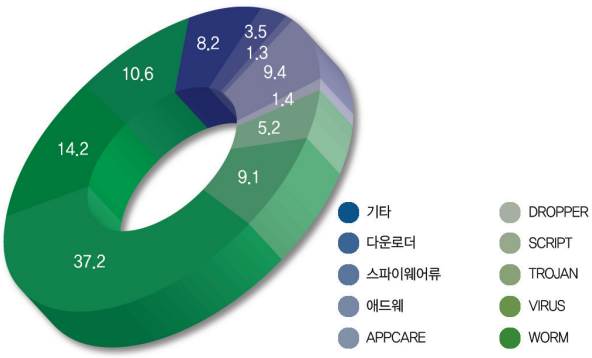
아래 표는 악성코드의 주요 동향을 파악하기 위하여, 악성코드별 변종을 종합한, 악성코드 대표 진단명별 감염보고 Top 200이다.

순위	등락	악성코드명	건수	비율
1	–	Win32/Induc	804,575	17.5 %
2	–	Win-Trojan/Agent	579,891	12.6 %
3	–	Win-Trojan/OnlineGameHack	524,844	11.4 %
4	↑ 1	TextImage/Autorun	348,282	7.6 %
5	↓ 1	Win32/Virut	302,782	6.6 %
6	–	Win32/Conficker	275,627	6 %
7	–	Win-Trojan/Downloader	259,799	5.7 %
8	–	Dropper/OnlineGameHack	163,781	3.6 %
9	↑ 2	Win32/Autorun.worm	148,477	3.2 %
10	↓ 1	Win32/Kido	145,118	3.2 %
11	↑ 1	Win-Trojan/Magania	135,830	3 %
12	↑ 5	Win-Trojan/Bho	116,047	2.5 %
13	–	Dropper/Agent	114,900	2.5 %
14	New	JS/Shellcode	105,339	2.3 %
15	New	Win-Adware/KorAdware	101,751	2.2 %
16	–	Win32/Parite	97,780	2.1 %
17	New	HTML/Agent	96,775	2.1 %
18	New	Win-Adware/BHO	93,815	2 %
19	New	Dropper/Malware	90,100	2 %
20	↓ 6	TextImage/Sasan	87,069	1.9 %
합계			4,592,582	100 %

[표 1-2] 악성코드 대표진단명 감염보고 Top 20

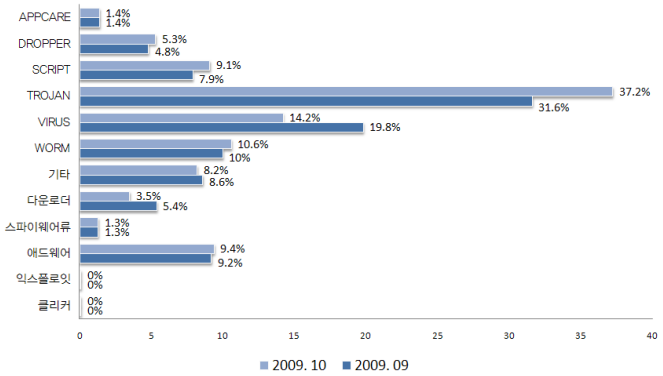
2009년 10월의 악성코드 감염보고 건수는 Win32/Induc이 총 804,575건으로 Top 20 중 17.5%의 비율로 1위를 차지하고 있으며, Win-Trojan/Agent가 579,891건으로 2위에 올랐다.

아래 차트는 고객으로부터 감염이 보고된 악성코드 유형별 비율이다.



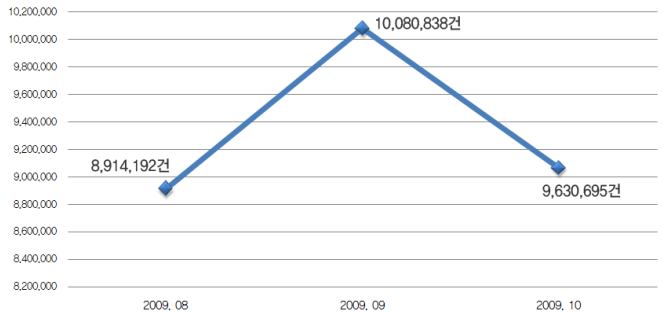
[그림 1-1] 악성코드 유형별 감염보고 비율

악성코드 유형별로 감염보고건수 비율은 Trojan류가 37.2%로 가장 많은 비율을 차지하고 하고 있으며, 다음으로 Virus가 14.2% 차지하고 있다.



[그림 1-2] 악성코드 유형별 감염보고 전월 비교

악성코드 유형별 감염보고 비율을 전월과 비교하면, Trojan은 전월에 비해 증가하였으며, Virus는 전월에 비해 감소하는 추세이다.



[그림 1-3] 악성코드 월별 감염보고 건수

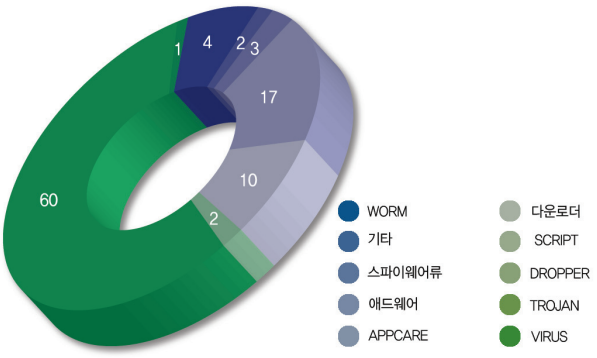
10월의 악성코드 월별 감염보고건수는 9,630,695건으로 9월의 10,080,838건으로 전월에 비해 450,143건이 감소하였다.

아래 표는 10월에 신규로 접수된 악성코드 중 고객으로부터 감염이 보고된 악성코드 Top 20이다.

순위	악성코드명	건수	비율
1	Dropper/Malware	53,373	11.9 %
2	Win-Adware/Sbplus.45056	34,460	7.7 %
3	Win-Trojan/Bho.234496.C	33,740	7.5 %
4	VBS/Solow.Gen	32,963	7.4 %
5	Win-Trojan/Downloader.281600.H	28,880	6.4 %
6	Win-Trojan/Adload.392704.B	28,844	6.4 %
7	Win-Adware/KorAdware.81920	22,891	5.1 %
8	Win-Trojan/OnlineGameHack.62590	22,884	5.1 %
9	Win-Trojan/OnlineGameHack.60563	21,076	4.7 %
10	Win-Adware/KorAdware.81920.B	20,041	4.5 %
11	Win-Trojan/Bho.594944	18,835	4.2 %
12	Win-Trojan/Agent.18944.ML	17,032	3.8 %
13	Win-Trojan/Downloader.182784.H	15,058	3.4 %
14	Dropper/Malware.16384.K	14,914	3.3 %
15	Win-Spyware/Blowfish.506368	14,709	3.3 %
16	Win-Adware/Overtls.614912	14,355	3.2 %
17	Win32/Palevo.worm.116736.BM	14,309	3.2 %
18	Dropper/Malware.16384.E	13,452	3 %
19	Win-Trojan/Agent.69632.VU	13,062	2.9 %
20	Win-Adware/KorAdware.45056.C	12,950	2.9 %
합계		447,828	100 %

[표1-3] 신종 악성코드 감염보고 Top20

10월의 신종 악성코드 감염보고의 Top20은 Dropper/Malware가 53,373건으로 전체 11.9%를 차지하여 1위를 차지하였으며, Win-Adware/Sbplus.45056가 34,460건으로 2위를 차지하였다.



[그림 1-4] 신종 악성코드 유형별 분포

10월의 신종 악성코드 유형별 분포는 Trojan이 60%로 1위를 차지하였으며, 애드웨어류가 17%로 2위를 차지하였다.

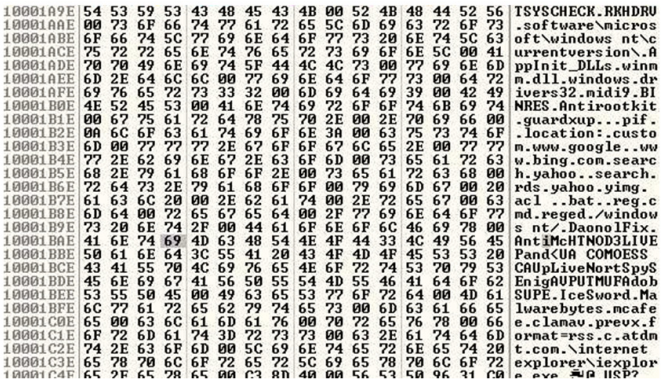
악성코드 이슈

Win-Trojan/Daonol 의 재등장

10월에는 '검은 화면에 마우스 포인트'만 나타나는 증상을 보이며 시스템이 정상적으로 부팅이 되지 않는다는 문의가 빗발쳤다. 부팅이 되지 않아서 샘플도 제대로 수집 되지 못할 뻔 했고 위와 같은 증상이 제대로 재현되지 않아 애를 먹은 경우도 있었다. 그럼, 이번 소란의 중심이 되었던 Win-Trojan/Daonol에 대하여 알아보자.

Daonaol 트로이목마는 지난 5월 이미 큰 이슈를 일으켰다. 악성코드는 Geno 혹은 Gumblar 라고 매스컴 등에 보도 되기도 하였다. 해당 악성코드의 이름은 악성코드가 발견된 유포 웹 사이트 또는 악성코드가 실제 업로드 된 웹 사이트 이름 등에서 유래 되었다. 일반적으로 안티 바이러스 업체에서는 Daonol이라고 명명한다. 해당 악성코드의 감염경로는 특정 보안 취약점에 노출된 인터넷 익스플로러와 PDF 및 SWF 취약점에 의한다. 따라서 자신이 인터넷 익스플로러와 PDF 문서를 즐겨 사용한다면 해당 응용 프로그램에 대한 보안 패치를 반드시 수행해야 한다. 또한 SWF 취약점 역시 해당 플레이어에 대한 보안 패치를 서둘러 받는 게 중요하다. 해당 악성코드의 정보와 보안 취약점에 대한 안내는 안철수연구소 홈페이지나 블로그 등에서 확인 할 수 있다. 검은 화면에 마우스 포인트만 보인다는 증상 때문에 한 동안 해당 악성코드에 대한 정확한 진단명이 확인되지도 못했고 단지 그 증상만으로 불리어지기도 하였다. 그러나 악성코드의 동작과 암호화된 문자열을 복호화 해보니 지난 5월에 문제를 일으켰던 Daonol 변형임을 알 수가 있다.

AhnLab V3 MSS



[그림1-5] 복호화된 Daonol 트로이목마 내부 문자열

해당 악성코드는 자신을 재부팅 후에도 자동 실행 되도록 다음 레지스트리 키에 자신을 등록 해둔다.

[HKEY_LOCAL_MACHINE₩SOFTWARE₩Microsoft₩Windows NT₩CurrentVersion₩Drivers32]
"midi9" ="?:₩..₩랜덤한 파일명". 확장자는 DAT, BAK, TMP, OLD 중 하나

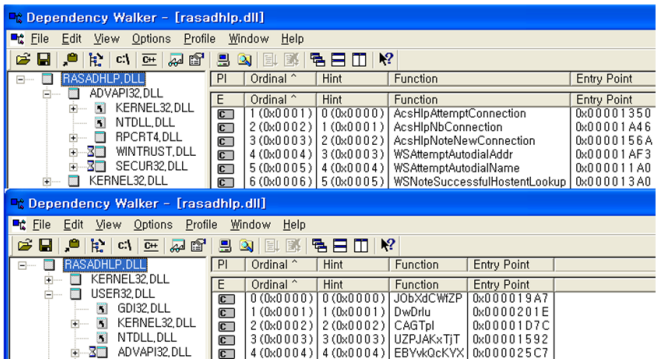
악성코드는 앞서 언급한 것처럼 '검은 화면에 마우스 포인터'만 나타나는 증상과 함께 일부 변형은 특정 응용 프로그램 실행을 방해하는 것이 보고 되었다. 이것은 일부 변형에 따른 다른 증상 보다는 2가지 모두 악성코드의 버그로 밝혀졌다. Daonol의 버그는 자신이 동작 중에 ZwOpenKey, ExitProcess 함수 등이 호출 되면 응용 프로그램들이 제대로 실행 되지 못하며 자신을 로드 시 간헐적으로 특정 Sleep 루틴으로 빠지게 되는데 이때 자신이 실행 되지 못하여 이후 부팅 과정도 정상적으로 진행되지 못한다. 안철수연구소에서는 이러한 악성코드의 버그를 전용백신을 통하여 메모리 패치하여 프로그램들을 정상적으로 동작시킨다. 아울러 프로세스마다 생성된 악의적인 쓰레드를 제거하여 악성코드가 더 이상 동작하지 못 하도록 해둔다. 이번 달 국내 핫 이슈였던 Daonol 트로이목마의 의도하지 않는 동작 때문에 일부 사용자는 시스템을 정상적으로 사용하지 못하는 피해를 입었다. 여기서, 우리가 알아야 할 것은 해당 악성코드가 여전히 보안 취약점을 이용하여 감염된다는 것이다. 자신이 사용하는 웹 브라우저와 PDF 리더기 그리고 SWF 관련 응용 프로그램에 대한 보안 패치에 대한 관심을 다시 한번 갖도록 하는 계기가 되었으면 한다.

Win32/Induc 의 꾸준한 1위 행진?

Win32/Induc이 꾸준하게 악성코드 감염보고 건수에서 1위를 하는 이유는 무엇일까? 이유를 알기 위해서는 먼저 Win32/Induc이 무엇인지부터 정체를 알아보자. Win32/Induc 은 Delphi 컴파일러가 설치된 시스템(Delphi4~7)의 "SysConst.dcu"(Delphi 상수 및 문자열 정의 라이브러리)파일을 감염시키며 자체적으로 다른 실행파일을 감염시키지 않는다. 감염된 Delphi 컴파일러에 의해서 제작된 실행파일은 "SysConst.dcu"를 바이너리상에 내포하게 되고 프로그램 시작 시 SysConst 프로시저가 호출되어 다시 해당 시스템의 Delphi 컴파일러의 "SysConst.dcu" 파일을 감염시킨다. 이와 같이 Win32/Induc은 델파이 소스상에 바이러스가 감염된 것을 개발자가 모르고 컴파일 한 경우에 발생하는 악성코드이다. 컴파일 한 실행파일은 크기를 줄이거나 설치본을 만들기 위하여 실행 압축하거나 인스톨 프로그램을 사용하게 된다. 이런 파일 내부에 Win32/Induc 이 존재하는 경우 안티 바이러스 업체의 정책에 따라서 진단 하지 않거나 진단 하여도 치료 하지 않는 등의 정책을 사용하게 된다. 현재 대부분의 안티 바이러스에서는 정책상 해당 파일을 진단 및 치료하지 않으며, V3에서는 사용자에게 정확한 정보를 제공하기 위해 지속적으로 진단은 하고 있으나, 치료는 하지 않고 있다. 따라서, 치료되지 않은 Win32/Induc이 계속적으로 재진단 됨으로써 지속적으로 감염보고 건수가 1위를 차지하고 있다. 앞으로 이러한 문제를 해결 하기 위해서는 델파이 개발자들이 자신이 개발한 파일을 재점검해보고, Win32/Induc에 감염되었을 경우에는 해당 파일을 새로 제작하여 배포하는 작업을 수행하여야 한다. 델파이 개발자들은 지금부터라도 본인이 개발한 파일을 점검해보기 바란다.

스파이웨어의 새로운 동작 방법

윈도우에서는 물리적 메모리 절약 및 코드 재사용 등 다양한 목적으로 DLL(Dynamic Link Library)을 사용하고 있다. 이 DLL이 로드 될 때는 DLL 검색 모드에 따라 달라지지만 가장 최우선적으로 찾는 곳은 바로 해당 어플리케이션이 실행된 디렉토리이다. 이런 구조적인 부분을 악용한 스파이웨어가 발견되었다. 해당 스파이웨어는 윈도우 시스템 관련 DLL과 동일한 이름을 가지고 있으며 해당 DLL 파일을 사용하는 어플리케이션이 설치되어 있는 디렉토리에 설치된다. 이렇게 하면 사용자가 해당 어플리케이션을 실행하면 자동으로 스파이웨어도 함께 실행되게 된다.



[그림 1-6] 동일 파일명을 가진 다른 DLL파일 (Export function)

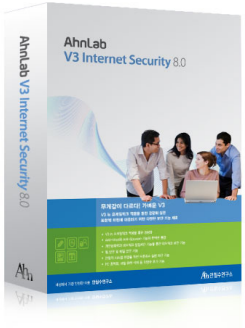
[그림 1-6]을 보면 파일 이름만 동일하고 호출되는 함수 구조는 완전히 달라 다른 파일이 존재함을 알 수 있다. 이 경우 윈도우에서 자동으로 시작하는 항목에 등록되지 않아도 동작이 되므로 스파이웨어 존재 사실을 손쉽게 은폐할 수 있다. 하지만, 해당 DLL에서 제공하는 export 함수를 호출할 경우 정상적인 동작을 할 수 없어 해당 어플리케이션이 비정상적으로 동작하거나 종료될 수도 있는 등 다양한 부작용이 발생될 수 있다.

늘어나는 온라인 사행성 게임

최근 온라인 사행성 게임이 증가하고 있다. 이들은 스팸메일, 가짜 블로그, 블로그 댓글, 휴대폰 SMS(Short Message Service)등을 통해 사용자의 접속을 유도한다. 이들은 서버를 한국이 아닌 외국에 두고 게임 이름과 사이트를 수시로 변경하면서 불법적으로 운영을 하고 있다.

[그림 1-7] 온라인 사행성 게임 사이트

온라인 사행성 게임은 게임당 일정량의 수수료를 받고 있으며, 게임 확률상 질 수 밖에 없는 구조로 만들어져 있다. 즉, 게임을 하면 할수록 돈을 잃게 만들어져 있다. 작년 유명 연예인과 운동선수들은 물론 일반인들이 온라인 사행성 게임을 해 수사를 받는 보도를 자주 접할 수 있었다. 즉, 우리나라에선 이런 온라인 사행성 게임이 불법으로 규정되어 있기 때문에 한 순간 호기심에서 즐긴 게임으로 인해 법의 처벌까지 받을 수 있다. 이들은 보다 짧은 시간 내 많은 이용자들을 모으기 위해 다양한 방법을 통해 사용자의 접속과 게임을 유도하기 때문에 이런 광고에 노출될 가능성 또한 더욱 더 높아지고 있다. 이런 온라인 사행성 게임은 도박임을 명심하고 게임을 하지 않는 것이 바람직하다.



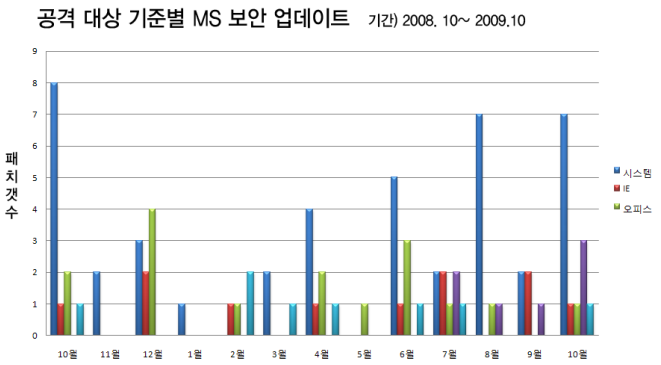
AhnLab V3 Internet Security 8.0

2. 시큐리티 동향

시큐리티 통계

10월 마이크로소프트 보안 업데이트 현황

마이크로소프트사로부터 발표된 이달 보안 업데이트는 총 13건으로 긴급(Critical) 8건, 중요(Important) 5건이다.



[그림 2-1] 2009년 10월 주요 MS 보안 업데이트 건수

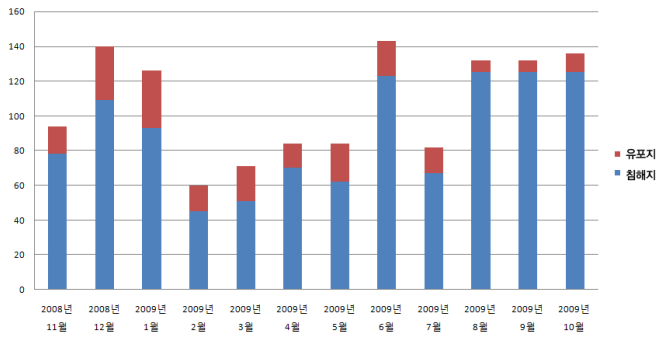
위험도	취약점	PoC
긴급	(MS09-050) SMBv2의 취약점으로 인한 원격 코드 실행 문제점	유
긴급	(MS09-051) Windows Media Runtime의 취약점으로 인한 원격 코드 실행 문제점	유
긴급	(MS09-052) Windows Media Player의 취약점으로 인한 원격 코드 실행 문제점	유
긴급	(MS09-054) Internet Explorer 누적 보안 업데이트	유
긴급	(MS09-055) ActiveX 킬(Kill) 비트 누적 보안 업데이트	무
긴급	(MS09-060) Microsoft Office용 Microsoft ATL(액티브 템플릿 라이브러리) ActiveX 컨트롤의 취약점으로 인한 원격 코드 실행 문제점	무
긴급	(MS09-061) Microsoft .NET 공용 언어 런타임의 취약점으로 인한 원격 코드 실행 문제점	무
긴급	(MS09-062) GDI+의 취약점으로 인한 원격 코드 실행 문제점	유

[표 2-1] 2009년 10월 주요 MS 보안 업데이트 목록

지난 9월에 발표된 SMB 취약점에 이어 SMBv2의 취약점이 발표되어 해당 프로토콜을 이용한 악성행위가 증가할 것으로 추정된다. 또한 Windows Media Player, Internet Explorer, Microsoft Office 어플리케이션에서도 원격으로 코드를 실행할 수 있는 문제를 가지고 있기 때문에 패치가 적용되지 않았을 경우 심각한 문제를 일으킬 수 있다.

악성코드 침해 웹사이트 현황

2009년 10월 악성 코드를 위해 침해된 웹사이트의 수와 악성코드 유포지 수는 127/9 로 2009년 9월의 127/7와 비교하여 유포지가 2건 더 늘어났다.



[그림 2-2] 악성코드 배포를 위해 침해된 사이트 수/ 배포지 수

웹 브라우저와 관련된 취약점이 발표되지 않은 지금, 악성코드 배포를 위해 현재 가장 널리 사용되고 있는 취약점은 지난달과 같은 OWC10.Spreadsheet 취약점이다. 이 취약점은 다음과 같은 특징을 가지고 있다.

```
var obj = new ActiveXObject( "OWC10.Spreadsheet" );
e=new Array();
e.push(1);
```

현재 대부분의 Anti Virus 제품은 이런 형식을 가진 HTML 문서를 진단한다. 따라서 사용자의 시스템을 이러한 공격으로부터 보호하기 위해서는 항상 운영체제의 보안업데이트를 최신 상태로 유지하고 Anti Virus 제품을 설치하여 사용하여야 한다.

시큐리티 이슈

Win-Trojan/SynAttack.64874 트래픽 유발

지난달 Win32/Palevo.worm을 통한 네트워크 트래픽 유발에 이어, 또 다시 네트워크 트래픽을 유발 시키는 Win-Trojan/SynAttack.648740이 고객에게 피해를 주었다.

전체적인 동작원리는 서비스로 등록된 후, 공격에 필요한 정보를 원격컨트롤 서버로부터 동적으로 받아와서 SYN Flooding공격을 수행하는 악성코드이다.

AhnLab Trusguard

```
#설치 제거: CLI 모드 상에서 /install or /uninstall 옵션에 따라 설치/제거된다.
#실행 방법: 특정 시간대 스케쥴링에 의해서 공격을 수행하도록 설계되어 있다.
    install 시 Service 로 등록된다. (Service Name : SYNC)
    서비스 실행 시 원격컨트롤서버(118.xxx.xxx.125) 로부터 정보 받아와 SYN 공격 수행한다.

        ---------- 요청 URL ----------
        hxxp://118.xxx.xxx.125/attackSchedule.php (JP)
        [응답메시지] OK, 1254063600,1254236400,  61.xxx.xxx.61,      80,      0
                    --------[공격시간]---------  --[공격대상]--  [공격포트] [플래그주정]--
-       ----------
 # 상기 공격시간/대상/포트는 지속적으로 변경되고 있었다.
   - 공격시간: 2009-09-27 15:00:00 ~ 2009-09-29 15:00:00 UTC
   - 공격대상: 61.xxx.xxx.61(JP)
   - 공격포트: 80/TCP
```

아래와 같이 감염 PC 1대당, 평균 초당 34Kbps로, 2.1Mbytes의 상당한 트래픽 유발시켰다.

Traffic	Captured	Displayed	Marked
Packets	8385	8385	0
Between first and last packet	0.248 sec		
Avg. packets/sec	33770.888		
Avg. packet size	62.000 bytes		
Bytes	519870		
Avg. bytes/sec	2093795.049		
Avg. MBit/sec	16.750		

[그림 2-3] Syn Flooding 공격 패킷

이러한 악성코드를 차단하기 위해서는 보안 프로그램을 최신 업데이트 버전으로 유지하는 것이 중요하다. 현재 AhnLab의 TrusGuard와 V3에서는 다음과 같은 진단명으로 진단/치료하고 있다.

TrusGuard : malicious_url_20090924_1619(HTTP)

V3 : Win-Trojan/SynAttack.648704
(V3진단/치료 엔진버전 : 2009.09.28.04)

Adobe Acrobat and Adobe Reader Deflate Parameter Integer Overflow

PDF 파일을 만드는 어플리케이션 프로그램은 특정 정보를 인식이 가능한 아스키 표현으로 변환하거나 압축하여 encoding할 수 있다. 그리고, PDF 파일을 읽는 어플리케이션은 오리지널 형식으로 정보를 변환하기 위해 그에 상응하는 decoding filter를 부를 수 있다. 이 데이터는 streams 내에 저장되며 각각의 stream은 Filter와 관련이 있다. Filter는 stream내 데이터가 이용되기 전에 어떻게 decoding 하는지 지시하게 된다. 몇몇 Filter는 그들이 어떻게 동작할지 컨트롤할 수 있는 파라미터를 허용하며, 이 파라미터들은 DecodeParms 엔트리에 명시된다.

FlateDecode 필터는 zlib/deflate 압축 방식을 이용하여 암호화된 데이터를 오리지널 텍스트 또는 바이너리 데이터로 재생시키기 위해 푼다. 암호를 푸는 처리과정을 컨트롤하기 위해 파라미터들이 허용되고, 이들 파라미터들 중 몇몇의 값은 아래와 같다.

Name	Type	Value
Predictor	Integer	1,2,10,11,12,13,14,15 (Default: 1, no prediction)
Colors	Integer	1 to 4 (PDF 1.0, and 1 or greater for PDF 1.3 and later - Default:1)
BitsPerComponent	Integer	1,2,4,8 (and 16 for PDF 1.5 and later - Default:8)
Columns	Integer	arbitrary positive integers (Default:1)

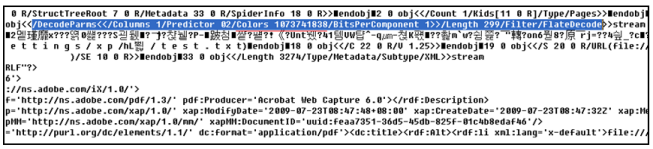
[그림 2-4] 암호 해제에 사용되는 파라미터

이들 파라미터들의 값은 FlateDecode Filter의 행동을 변경시킨다. 예를 들어 만약 Predictor 파라미터가 1보다 큰 다른 값을 가졌을 때, 이 필터는 연관된 데이터가 암호화되기 이전과는 달라졌다고 생각하고 Predictor는 prediction algorithm (PNG 또는 TIFF 이미지)를 선택하게 된다. 이번 경우 이 파라미터 (Colors, BitsPerComponent, Columns) 들은 요구되는 이미지 데이터 점유를 위한 버퍼사이즈 결정을 위해 특정 계산에 이용된다.

Adobe Reader와 Acrobat에는 정수 오버플로우 취약점이 존재한다. PDF 파일 내에 포함되어진 FlateDecode Filters를 처리할 때, 부적당한 input값의 원인이 취약점이 된다. Predictor 값이 2(TIFF predictor)로 셋팅 되었을 때, 취약한 코드는 버퍼사이즈 결정을 위한 계산 작업을 수행하기 전에 Colors 파라미터의 값을 체크하지 않는다. 이러한 작업으로부터 나온 힙 버퍼 사이즈의 할당이 있기 전에 아래와 같은 Colors 파라미터 값을 기반으로 계산이 수행된다.

$$colors * 4 + 48$$

만약 Colors 파라미터의 값이 0x3FFFFFEE 또는 큰 값으로 제공 된다면, 작은 버퍼 할당의 결과로 정수 오버플로우가 발생한다. 아래는 해당 취약점을 이용한 악성 PDF 파일의 일부이다.



[그림 2-5] 악성 PDF 파일 예

해당 취약점은 공격자가 특정 코드를 실행 시킬 수 있는 취약점으로 이미 악성코드로 배포되었으며, 따라서 신속한 보안 업데이트가 필요하다.

3. 웹 보안 동향

웹 보안 통계

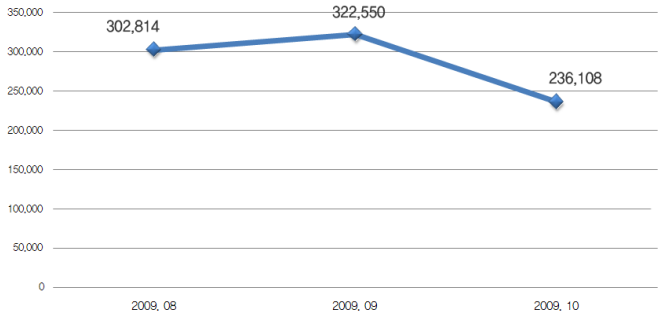
웹 사이트 보안 요약

구분	건수
악성코드 발견 건수	236,108
악성코드 유형	937
악성코드가 발견된 도메인	849
악성코드 발견된 URL	6,801

[표 3-1] 웹 사이트 보안 요약

악성코드 발견 건수는 236,108건이고, 악성코드 유형은 937건이며, 악성코드가 발견된 도메인은 849건이며, 악성코드 발견된 URL은 6,801건이다.

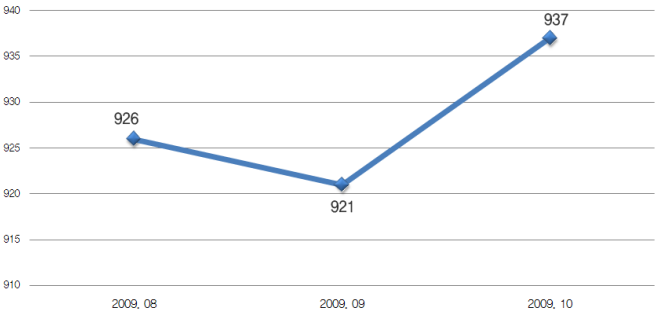
월별 악성코드 발견 건수



[그림 3-1] 월별 악성코드 발견 건수

2009년 10월 악성코드 발견 건수는 전달의 322,550건에 비해 73% 수준인 236,108건이다.

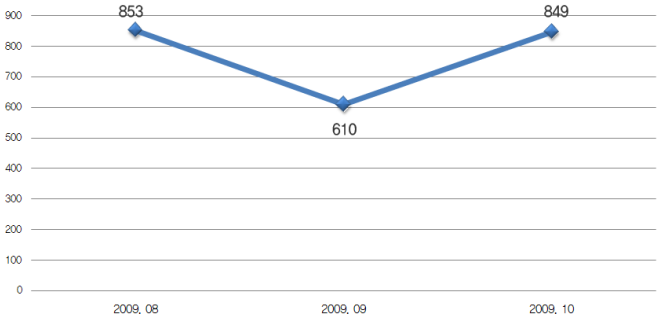
월별 악성코드 유형



[그림 3-2] 월별 악성코드 유형

2009년 10월 악성코드 유형은 전달의 921에 비해 101% 수준인 937건이다.

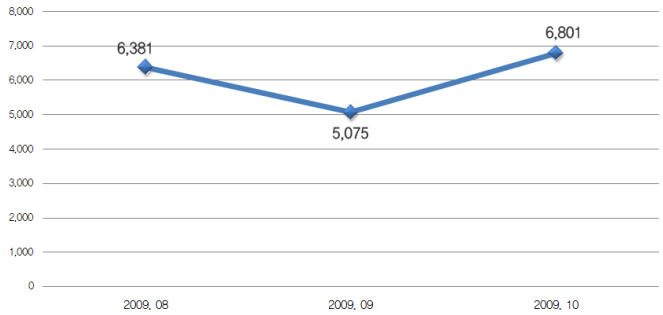
월별 악성코드가 발견된 도메인



[그림 3-3] 월별 악성코드가 발견된 도메인

2009년 10월 악성코드가 발견된 도메인은 전달의 610건에 비해 139% 수준인 849건이다.

월별 악성코드가 발견된 URL



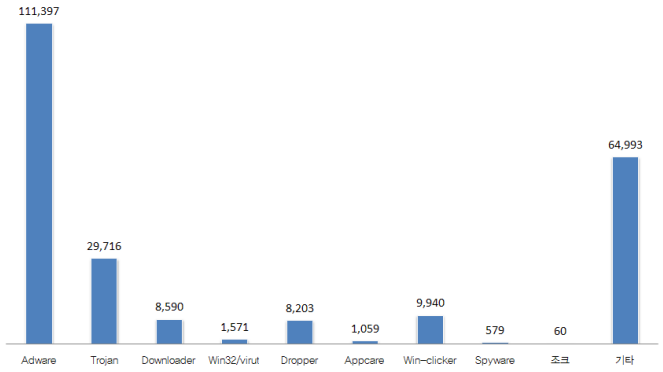
[그림 3-4] 월별 악성코드가 발견된 URL

2009년 10월 악성코드가 발견된 URL은 전달의 5,075건에 비해 134% 수준인 6,801건이다.

악성코드 유형별 배포 수

유형	건수	비율
Adware	111,397	47.2 %
Trojan	29,716	12.6 %
Downloader	8,590	3.6 %
Win32/Virut	1,571	0.7 %
Dropper	8,203	3.5 %
AppCare	1,059	0.4 %
Win-Clicker	9,940	4.2 %
Spyware	579	0.2 %
조크	60	0 %
기타	64,993	27.5 %
합계	236,108	100 %

[표 3-2] 월별 유형별 배포 수



[그림 3-5] 월별 유형별 배포 수

악성코드 유형별 배포 수에서 Adware류가 111,397건 전체의 47.2%로 1위를 차지하였으며, Trojan류가 29,716건 전체의 12.6%로 2위를 차지하였다.

악성코드 배포 Top 10

악성코드 배포 Top 10에서 Win-Adware/Shortcut.InlivePlayerActiveX.234가 지난달 보다 1단계 상승한 67,225건으로 1위를 차지하였으며, Top 10에 Win-Clicker/SPro.32768.C 등 4건이 새로 등장하였다.

순위	등락	악성코드명	건수	비율
1	↑ 1	Win-Adware/Shortcut.InlivePlayerActiveX.234	67,225	40.5 %
2	↓ 1	Win32/Induc	52,316	31.5 %
3	↑ 1	Win-Adware/Shortcut.IconJoy.642048	12,111	7.3 %
4	New	Win-Clicker/SPro.32768.C	8,152	4.9 %
5	–	Win-Adware/BHO.HiMyCar.237568	7,184	4.3 %
6	↑ 4	Win-Downloader/Rogue.PCPlus.402944.B	5,493	3.3 %
7	New	Win-Dropper/KorZlob.5132206	4,303	2.6 %
8	New	Win-Adware/Shortcut.K2Com.Sobang.266240	3,629	2.2 %
9	New	VBS/Downloader	2,945	1.8 %
10	↓ 2	Win-Adware/Shortcut.INBEE.iomeet.267270	2,498	1.5 %
합계			165,856	100 %

[표 3-3] 악성코드 배포 Top 10

웹 보안 이슈

지속적인 악성코드 배포에 사용되는 웹 사이트 증가

중국 발 해킹부터 지속적으로 웹 사이트 보안에 대한 관심과 조치를 여러 번 강조하였으나, 결과적으로 악성코드 배포 경로로 사용되는 웹 사이트는 지속적으로 증가하는 추세이다. 웹 보안 통계부문에서 "월별 악성코드가 발견된 URL"을 보면 6,801건으로 전달의 5,075건에 비해 134% 증가한 것을 알 수 있다. "월별 악성코드 발견 건수"가 전달의 236,108건으로 전달에 비해 27%가 감소하였지만, 악성코드가 발견되는 URL이 증가하였다는 것은 사용자가 웹 사이트를 통해 악성코드에 감염될 위험은 더 높아 진 것을 알 수 있다. 따라서, 웹 사이트 관리자에게는 본인이 관리하는 사이트에 대한 악성코드 감염여부를 실시간으로 체크할 수 있는 사이트 가드와 같은 웹 보안 제품의 사용을 권고한다. 하지만 무엇보다, 사이트 관리자는 다수의 고객들에게 자사의 제품이나 정보를 제공하는 것뿐 아니라, 보안까지 제공한다는 사고를 가지는 것이 가장 중요할 것이다.

Win-Adware/Shortcut 류의 증가

최근에는 인터넷 사이트에 접속 시 ActiveX가 설치되며 사용자의 동의 없이 특정 웹 사이트로 바로 가기를 유도하는 악성코드들의 배포가 증가하고 있다. 이는 방문자수의 증가를 통한 금전적 이익 취득과 함께 웹 사이트 홍보를 위한 용도로 사용되고 있다. 10월의 배포 Top 10에도 Shortcut 류인 Win-Adware/Shortcut.InlivePlayerActiveX.234가 67,225건으로 1위를 차지 하였으며 그 외에도 Win-Adware/Shortcut.IconJoy.642048가 4위, Win-Adware/Shortcut.K2Com.Sobang.266240가 9위를 차지하고 있어, 웹 사이트를 통한 악성코드 배포의 주요 위험군으로 자리 잡고 있다. 따라서, 사용자들은 웹 사이트 접속 시 ActiveX 설치 전에 동의를 요구하는 대화 창에 대한 각별한 주의를 기울여, 문제가 발생할 수 있는 ActiveX 프로그램(제공하는 인증서가 유효하지 않거나, 신뢰할 수 없는 공급자가 제공하는 프로그램)은 설치하지 않아야 한다.

ASEC REPORT 집필진

2009년 Vol.10

편 집 장 선임 연구원 허 종 오

집 필 진 선임 연구원 정 진 성
선임 연구원 박 태 환
선임 연구원 허 종 오
선임 연구원 이 재 호
주임 연구원 박 시 준
주임 연구원 조 주 봉

감 수 상 무 조 시 행

참여연구원 ASEC 연구원
SiteGuard 연구원

Ahn 안철수연구소

AhnLab