ASEC REPORT

안철수연구소에서 발행하는 월간 보안 보고서

2010. Volume. 01

안철수연구소

목 차

이달의 보안 동향

Ⅰ. 이달의 보안 동향

1. 악성코드 동향

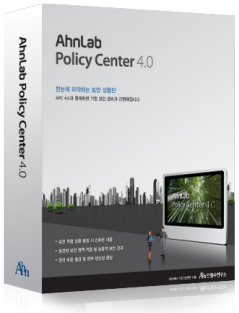
악성코드 통계

2010년 1월 악성코드 통계현황은 다음과 같다.

순위	등락	악성코드명	건수	비율
1	–	Win32/Induc	519,723	20.1 %
2	–	TextImage/Autorun	360,417	13.9 %
3	↑ 1	JS/Shellcode	171,991	6.7 %
4	↑ 2	Win32/Parite	155,207	6 %
5	New	JS/Redirect	142,969	5.5 %
6	New	JS/ShellCode	137,801	5.3 %
7	↓ 2	Win32/Virut.B	120,914	4.7 %
8	New	Win-Trojan/Scar.464896	95,738	3.7 %
9	↓ 1	Win32/Virut	91,962	3.6 %
10	New	HTML/Shellcode	89,705	3.5 %
11	↓ 4	Win32/Conficker.worm.Gen	88,009	3.4 %
12	↓ 3	TextImage/Sasan	84,253	3.3 %
13	↓ 3	Win32/Olala.worm.57344	83,354	3.2 %
14	↑ 1	TextImage/Viking	75,001	2.9 %
15	↓ 4	ALS/Bursted	74,111	2.9 %
16	New	Win-Adware/PointKing.722944	64,124	2.5 %
17	↓ 14	Win-Trojan/Daonol.Gen	57,502	2.2 %
18	–	Win32/Traxg.worm.61440	57,488	2.2 %
19	New	Win-Adware/ColorSoft.106496	56,979	2.2 %
20	New	Win-AppCare/HideWin.31232	56,952	2.2 %
합계			2,584,200	100 %

[표 1-1] 악성코드 감염보고 Top 20

2010년 1월의 악성코드 감염 보고는 Win32/Induc이 1위를 차지하였으며, TextImage/Autorun과 JS/Shellcode가 각각 2위와 3위를 차지 하였다. 신규로 Top 20에 진입한 악성코드는 총 7건이다.



AhnLab Policy Center 4.0

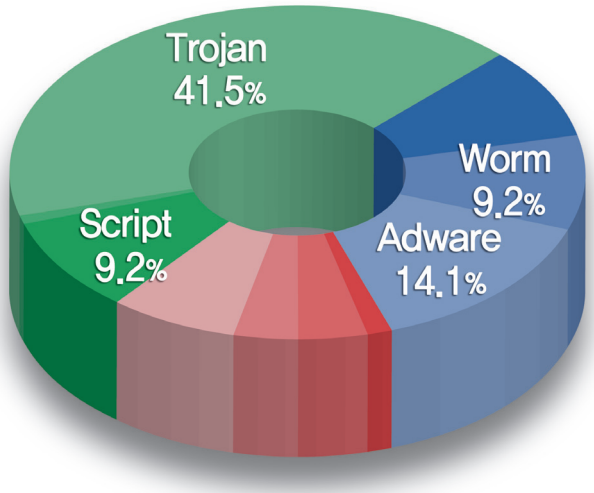
아래 표는 악성코드의 주요 동향을 파악할 수 있는 악성코드 별 변종을 종합한 악성코드 대표진단명 감염보고 Top 200이다.

순위	등락	악성코드명	건수	비율
1	–	Win-Trojan/Agent	755,522	14.1 %
2	↑ 1	Win-Trojan/OnlineGameHack	751,815	14 %
3	↓ 1	Win32/Induc	519,879	9.7 %
4	–	Win-Trojan/Downloader	451,156	8.4 %
5	–	TextImage/Autorun	360,807	6.7 %
6	↑ 2	Win32/Virut	254,641	4.8 %
7	↑ 2	Win32/Conficker	249,850	4.7 %
8	↓ 2	Win-Adware/Lastlog	248,456	4.6 %
9	↑ 1	Win32/Autorun.worm	211,981	4 %
10	↑ 2	JS/Shellcode	171,991	3.2 %
11	–	Win-Trojan/Malware	168,293	3.1 %
12	↑ 1	Win-Trojan/Genome	160,533	3 %
13	↑ 7	Win32/Parite	157,890	2.9 %
14	New	JS/Redirect	142,969	2.7 %
15	↑ 2	Win32/Kido	139,458	2.6 %
16	New	JS/ShellCode	137,801	2.6 %
17	↓ 3	Win-Adware/KorAdware	130,480	2.4 %
18	–	Dropper/OnlineGameHack	126,734	2.4 %
19	↓ 4	Win-Adware/BHO	110,943	2.1 %
20	New	Win-Trojan/Scar	109,268	2 %
합계			5,360,467	100 %

[표 1-2] 악성코드 대표진단명 감염보고 Top 20

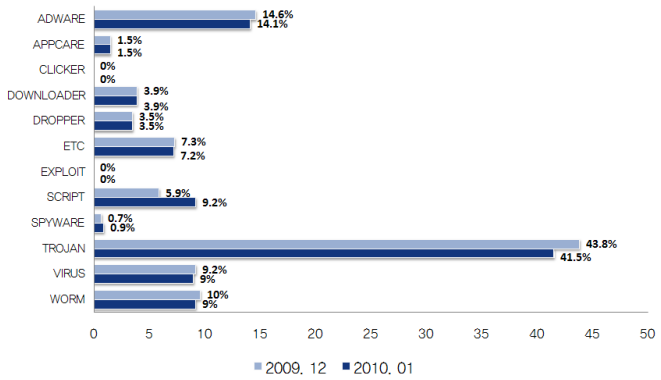
2010년 1월의 악성코드 감염보고 건수는 Win32-Trojan/Agent가 총 755,522건으로 Top 20 중 14.1%의 비율로 1위를 차지하였으며, Win-Trojan/OnlineGameHack이 751,815건으로 2위, Win32/Induc이 519,879건으로 3위를 차지 하였다.

아래 차트는 고객으로부터 감염이 보고된 악성코드 유형별 비율이다.



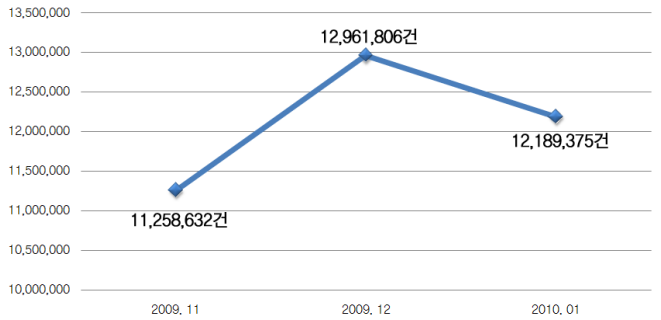
[그림 1-1] 악성코드 유형별 감염보고 비율

악성코드 유형별로 감염보고 건수 비율은 트로잔(Trojan)류가 41.5%로 가장 많은 비율을 차지 하였고, 애드웨어(Adware)가 14.1%, 웜(Worm)과 스크립트(Script)가 9.2%의 비율을 각각 차지 하였다.



[그림 1-2] 악성코드 유형별 감염보고 전월 비교

악성코드 유형별 감염보고 비율을 전월과 비교하면, 스크립트와 스파이웨어(Spyware)가 전월에 비해 증가세를 보이고 있는 반면, 트로잔과 애드웨어, 웜, 바이러스(Virus)는 전월에 비해 감소한 것을 볼 수 있다. 다운로더(Downloader), 드롭퍼(Dropper) 계열들은 전월 수준을 유지하였다.



[그림 1-3] 악성코드 월별 감염보고 건수

1월의 악성코드 월별 감염보고 건수는 12,189,375건으로 12월의 악성코드 월별 감염보고 건수 12,961,806건에 비해 772,431건이 감소하였다.

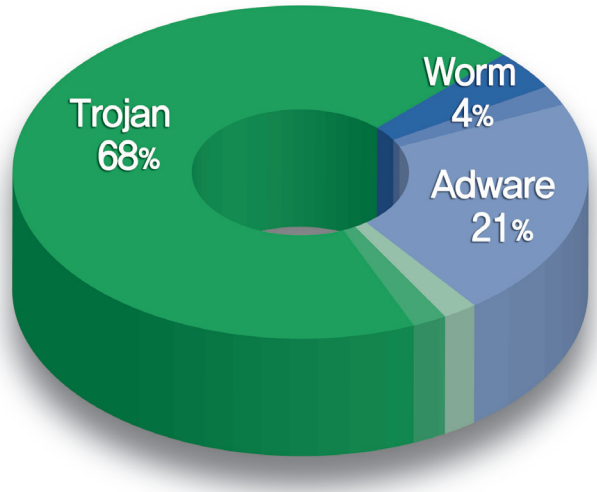
AhnLab V3 MSS

아래 표는 1월에 신규로 접수된 악성코드 중 고객으로부터 감염이 보고된 악성코드 Top 200이다.

순위	악성코드명	건수	비율
1	Win-Trojan/Scar.464896	95,738	12.3 %
2	Win-Adware/PointKing.722944	64,124	8.2 %
3	Win-Adware/ColorSoft.106496	56,979	7.3 %
4	Win-Trojan/OnlineGameHack.2732115	56,597	7.3 %
5	Win-Trojan/OnlineGameHack.324096.C	51,602	6.6 %
6	Win-Trojan/Lineplus.118784	49,867	6.4 %
7	Win-Trojan/Downloader.684032.C	45,451	5.8 %
8	Win-Trojan/Downloader.268800.D	40,037	5.1 %
9	Win-Trojan/Unovt.718336	37,044	4.7 %
10	Win-Adware/Elog.666112	35,902	4.6 %
11	Win-Adware/Shortcut.290816	32,794	4.2 %
12	Win-Adware/WiseBar.360448.D	29,766	3.8 %
13	Win-Trojan/QHost.102102	28,749	3.7 %
14	Win-Trojan/Unovt.718336.B	28,228	3.6 %
15	Win-Trojan/QHost.102108	27,046	3.5 %
16	Win-Spyware/Gever.769536	26,469	3.4 %
17	Win-Downloader/IEShow.339968.H	18,883	2.4 %
18	Win-Adware/KwSearchGuide.180384	18,463	2.4 %
19	Win-Adware/Lastlog.257536	18,393	2.4 %
20	Win-Trojan/OnlineGameHack.18944.GL	18,128	2.3 %
합계		780,260	100 %

[표 1-3] 신종 악성코드 감염보고 Top 20

1월의 신종 악성코드 감염보고의 Top 20은 Win-Trojan/Scar.464896가 95,738건으로 전체 12.3%를 차지하여 1위를 차지하였으며, Win-Adware/PointKing.722944가 64,124건으로 2위를 차지하였다.



[그림 1-4] 신종 악성코드 유형별 분포

1월의 신종 악성코드 유형별 분포는 트로잔이 68%로 1위를 차지하였다. 그 뒤를 이어 애드웨어가 21%, 웜이 4%를 각각 차지하였다.

악성코드 이슈

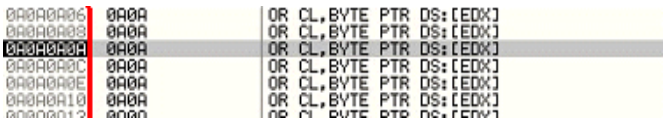
2010년 시작하는 첫 해 인터넷 익스플로러 제로데이 보안 취약점(CVE-2010-0249)이 보고되었다. 취약점은 바로 악성코드 제작에 이용되었으며 이를 손쉽게 만들어주는 도구들도 속속 발견 되었다. 취약점을 이용하

여 다운로드 되는 악성코드는 다양했지만 도구에서 제작된 스크립트 유형은 크게 다르지 않았다. 인터넷 익스플로러는 사용자 점유율이 높은 웹 브라우저인 만큼 많은 사용자들이 잠재적인 보안 위협에 노출되고 말았다. 또한 해당 취약점이 미국 내 위치한 주요한 IT 회사들을 공격하는데 사용되었다는 해외뉴스가 흘러 나오기도 하였다.

국내에서는 작년에도 큰 피해를 주었던 Win32/Palevo.worm 변형이 지속적으로 보고되었다. 휴지통 폴더로 위장한 폴더에 자신의 복사본을 생성하는 등의 유사한 행위 형태로 동작하는 변형들이 발견되기도 하였다. 팔레보(Palevo) 웜은 C&C서버와 통신시 암호화된 명령을 받아 오토런(autorun) 및 메신저 등으로 전파 될 수가 있으며 또한 DDoS 공격에 이용될 수도 있다. 윈도우 시스템 파일 중 특정 드라이버 파일만을 감염시키는 Win32/Dnis.C 변형이 발견되었다. 암호화 키 값이 변경된 단순한 변형이었다. 파일을 감염시키는 로더는 최초 감염 시 로컬에 자신을 생성하지 않고 메모리에서만 일련의 행위를 거쳐 특정 드라이버 파일을 감염시킨다. 시스템 파일이 감염된 경우 진단, 치료가 어려운 경우도 있다. 감염되어도 그 사실을 일반 사용자가 모르는 경우가 많은 만큼 주의가 요구된다. 또한 국내 온라인 게임업체의 공지사항을 위장한 형태의 메일로 대량 유포된 사례도 있었다. 비슷한 유형으로는 국내 특정 블로그를 만들어 두고 백신 프로그램으로 위장하여 악성코드를 배포한 사례도 있었다. 이렇듯 국내 사용자를 노리는 정교한 사회공학기법을 이용한 위장 메일, 블로그, 카페 등이 올 초부터 등장한 만큼 올 한해 역시 과거의 메신저나 메일 피싱을 넘어 다양한 경로로 알려지거나 유입될 수 있는 고도화된 사회공학기법이 적용된 위협에 주의와 관심을 가질 필요가 있다.

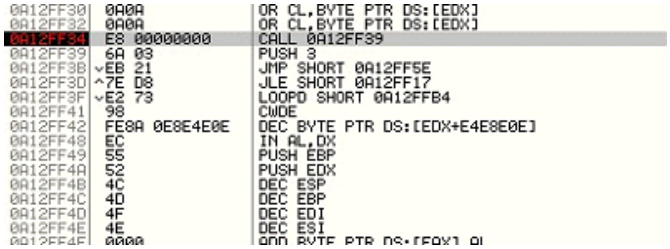
인터넷 익스플로러 제로데이 취약점 (CVE-2010-0249)

이번 달에 발견된 취약점은 중국에서 제작된 다수의 생성기로 인한 변형 유입의 결과로 보인다. [그림 1-5]를 통해 알려진 취약점이 사용하는 주소가 다른 곳으로 변경 되었음 확인 할 수 있다.



[그림 1-5] 변형 취약점 코드가 사용하는 메모리 주소

또한 변형된 취약점 코드는 다운로드 후 실행하는 코드로만 간결하게 되어 있다.



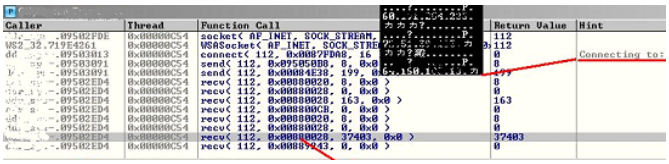
[그림 1-6] 변형 취약점 코드 예 -1

[그림 1-7] 변형 취약점 코드 예 -2

일반적으로 취약점 코드의 구성은 쉘코드가 포함 되어 있는 악의적인 스크립트를 실행 후 쉘코드에 의한 악의적인 파일 다운로드 및 실행이 일반적으로 일어나도록 되어있다. 다른 형태로는 악성코드 파일을 다운로드 하지 않고 문서 파일의 취약점의 형태의 경우에는 문서 파일 자체에 악의적인 파일을 숨겨 쉘코드 실행 -> 악의적인 파일 드롭 -> 실행 순으로 동작 되는 것이 있다.

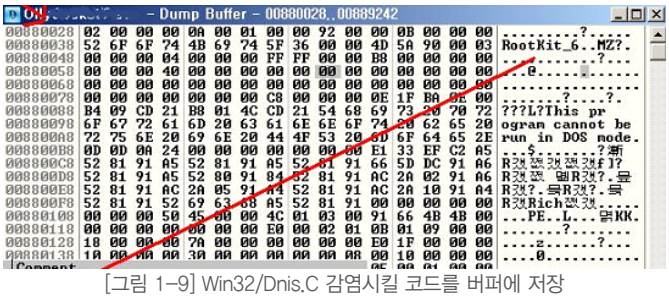
윈도우 시스템 파일을 감염 시키는 바이러스 변형 – Win32/Dnis.C

Win32/Dnis.C는 작년 5월 발견, 보고 되었다. 이후 지속적으로 변형이 등장하고 있다. 또한, 윈도우 시스템 파일인 Ndis.sys 파일을 감염 시키는 것으로 잘 알려져 있다. 감염을 시키는 로더는 다음과 같이 실행 후 특정 호스트로 접속하여 파일을 받아와 실행하는데 이러한 과정은 모두 메모리에서 수행된다.



[그림 1-8] Win32/Dnis.C 형 악의적인 호스트 접속

다음과 같이 감염 시킬 코드를 버퍼에 두고 내부적으로 버퍼 내 코드를 실행하여 파일을 감염 시킨다.



[그림 1-9] Win32/Dnis.C 감염시킬 코드를 버퍼에 저장

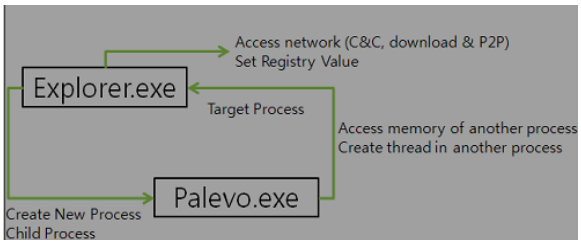
감염된 파일은 원래의 크기보다 증가하거나 변형마다 자신의 키 값을 다르게 하거나 키 값이 정의된 옵셋의 크기를 매번 변형하는 등의 방식으로 감염 될 때마다 변형을 만들게 된다. 이후 스팸을 보내거나 다른 악성코드를 다운로드 하는 등의 악의적인 증상을 수행하게 된다.

시스템 파일은 감염 여부를 사용자가 모르는 경우가 많으며 또한 외부와 접속도 허용되는 경우가 많으므로 차단되지 않는 것이 보통이다. 이러한 점을 악용하여 악성코드 제작자들이 시스템 파일을 감염시키거나 패치하는 경우가 많이 발생하고 있다. 시스템 파일을 패치하는 형태의 경우 악성코드의 시작점을 숨기기 위하여 사용된다. 보통 악성코드는 부팅 시 매

번 실행 되기 위하여 윈도우 시작 관련 레지스트리 키를 이용하는 경우가 대부분이다. 그러나 시스템 파일은 부팅 시 OS 에 의해서 자동으로 로드가 되므로 이때 패치한 시스템 파일을 이용하면 악성코드 파일을 시작점에 등록하지 않고도 실행 할 수 있다.

Win32/Palevo.worm 변형의 기승

팔레보 웜은 다양한 이름으로 불리어질 만큼 많은 변형이 존재한다. 대부분의 증상은 Explorer.exe에 자신의 스레드를 만들어 동작하는데 이때 특정 호스트로부터 명령을 받아 악의적인 기능을 수행 할 수 있다. 실행 후 발생하는 행동은 다음으로 정리 된다.



[그림 1-10] Win32/Palevo.worm 실행 관계

또한 자신을 복사(생성)하는 경로가 윈도우나 시스템 폴더가 아닌 휴지통 폴더 (C:₩RECYCLER)의 하위 폴더명을 특정하게 생성 후 자신을 위치시킨다. 특히 이 웜은 자신을 전파 시키기 위해서 이동식 디스크나 MSN으로 명령을 받은 후 전파 될 수 있다. 또한 특정 시스템을 공격하는 방법 중에 TCP/UDP Flooding 공격을 수행 하는 행위는 감염 후 C&C로부터 명령을 받아야만 동작하게 되어 있다. 스스로 자신을 업데이트 하고 전파력도 강한 것이 이 웜의 변형을 확산 시키는데 어느 정도 일조한 것으로 보인다.

정상 프로그램으로 위장하는 스파이웨어

정상적인 윈도우 시작 프로그램을 자신으로 변경하고 본래 프로그램은 파일이름 뒤에 공백을 덧붙여 윈도우 부팅 시 마다 자동으로 실행 되는 스파이웨어가 발견되었다.

"vmware-tray.exe" -> "vmware-tray .exe"
"ietoy.exe" -> "ietoy .exe"

[그림 1-11] 스파이웨어에 의해 변조된 실행 파일명

그림과 같이 실행된 프로세스를 살펴보면 그냥 봐서는 잘 모르지만 자세히 보면 파일명 뒤에 약간의 공백이 추가된 것을 확인할 수 있다. 이와 같은 스파이웨어에 감염되면 "vmware-tray.exe" 라는 스파이웨어가 먼저 실행되고 그 후 "vmware-tray .exe" 라는 정상 프로그램이 실행된다. 문제는 이 뿐만이 아니다. 해당 스파이웨어를 보안 제품에서 치료 했을 경우 윈도우는 부팅 시 "vmware-tray.exe" 를 실행하려고 하지만 실제 파일은 "vmware-tray .exe" 로 변경되어 실행이 불가능하다. 따라서 일부 프로그램은 정상 동작하지 않는 문제도 발생할 수 있다.

국산 리워드(reward) 프로그램의 확산

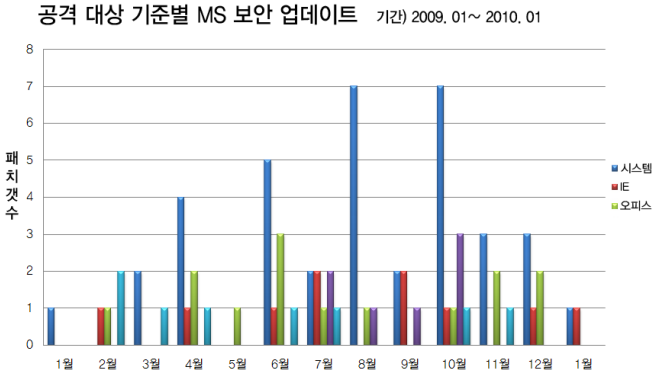
국내에서 제작된 리워드 프로그램에 의한 피해가 날이 갈수록 늘어나고 있다. 특히 애드웨어 포인트킹(Win-Adware/PointKing.722944)의 경우 2010년 1월 신종 악성코드 감염 건수 중 두 번째로 많은 것으로 보고 되었다. 쇼핑몰 구매금액 중 일부를 되돌려주는 리워드 프로그램은 일정 금액 이상 적립 되었을 경우에만 현금으로 돌려 받을 수 있어 일반적인 경우에는 환급이 거의 불가능하다. 이런 맹점을 이용해 수 많은 리워드 프로그램이 우후죽순처럼 생겨나고 있다. 하지만 대부분 웹 하드 다운로드 프로그램이나 무료 게임 서비스의 번들로 설치되어 보안 제품에서 진단하지 못하는 경우가 많다. 일부 리워드 프로그램은 인터넷 익스플로러 등의 웹 브라우저에 BHO(Browser Helper Object)로 동작하여 잦은 오류를 일으키거나 키워드 검색 결과를 변조하기도 한다. 따라서 웹 하드나 무료 게임 등을 하기 전에 설치되는 프로그램의 목록을 꼼꼼히 살펴보고 자신에게 불필요한 서비스는 설치하지 않는 것이 좋다.

2. 시큐리티 동향

시큐리티 통계

1월 마이크로소프트 보안 업데이트 현황

마이크로소프트사로부터 발표된 이번 달 보안 업데이트는 총 2건으로 모두 긴급(Critical)에 해당 한다.



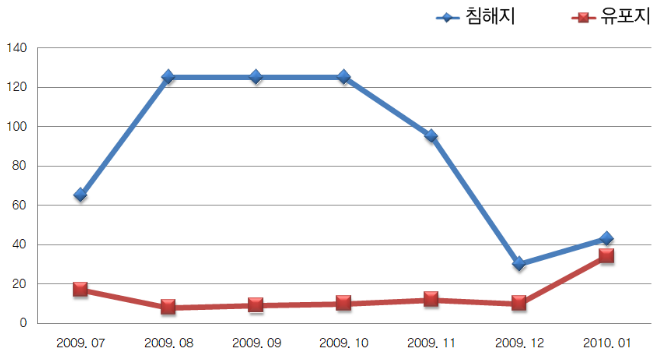
[그림 2-1] 공격 대상 기준별 MS 보안 업데이트

위험도	취약점	PoC
긴급	MS10-001 Embedded OpenType 글꼴 엔진의 취약점으로 인한 원격 코드 실행 문제점	무
긴급	MS10-002 Internet Explorer 누적 보안 업데이트	유

[표 2-1] 2010년 1월 주요 MS 보안 업데이트

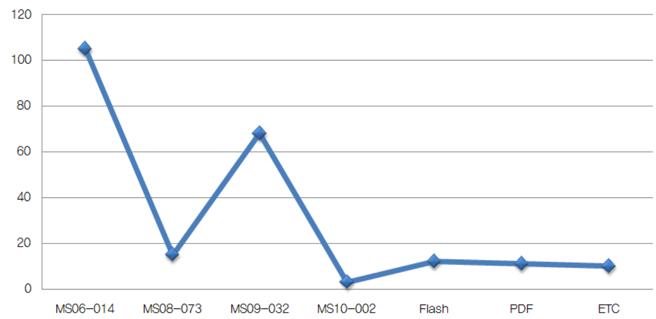
이번 달에는 지난 달에 발표된 3건 보다 적은 2건의 보안패치가 발표되었다. 이 중, MS10-002 Internet Explorer 취약점은 제로데이 공격이 발생한 이후에 긴급으로 보안 패치가 적용된 것으로 위험하다고 볼 수 있다. 또한 MS10-002 취약점을 이용하여 악성코드 배포가 많이 이루어 짐으로, 신뢰되지 않은 웹사이트 접속에 유의해야 하며, 백신 설치와 더불어 보안 패치를 반드시 업데이트 해야 안전한 인터넷 환경을 사용할 수 있다.

악성코드 침해 웹사이트 현황



[그림 2-2] 악성코드 배포를 위해 침해된 사이트 / 배포지 수

[그림 2-2]를 보면 2010년 1월 악성코드 침해 사이트 현황은 2009년 12월보다 다소 증가했다. 악성코드가 유포될 때 사용했던 취약점은 오래 전에 보고된 취약점이 대부분인데 이에 대해서는 아래 통계에서 좀더 자세히 살펴보겠다.



[그림 2-3] 악성코드 배포를 위해 사용된 취약점

[그림 2-3]은 2010년 1월 한달 동안 침해사고가 발생한 웹사이트들에서 악성코드를 유포하기 위해서 사용했던 취약점들에 대한 통계인데 이를 통해서 몇 가지 사실을 알 수가 있다.

악성코드 유포경로 측면에서 살펴보면 고전적인 방법(E-mail, 메신저, P2P 등)이 조금씩 증가하고 있긴 하지만 침해사고 사이트와 악성코드의 결합이 상대적으로 우위를 점하고 있으며, 악성코드 유포를 위한 공격대상 측면에서 살펴보면 OS의 취약점 보다는 사용자들이 가장 많이 사용하는 응용프로그램의 취약점을 공격하는 사례가 빈번하게 발생하고 있다는 것이다.

[그림 2-3]에서 보면 MS06-014의 경우를 보면 공격빈도 수가 다른 취약점보다 월등히 많음을 알 수가 있는데, 해당 취약점이 2006년에 보고된 후 4년이 지난 지금까지도 가장 빈번하게 사용되고 있는 이유가 무엇일까? 그건 바로 보안패치에 대한 사용자들의 무관심에서 비롯됐다고 해도 과언이 아닐 것이다. 물론 이것은 MS06-014에만 국한된 것이 아니며 지금으로부터 또 다시 4년이 지난 시점에서 통계를 내보면 MS06-014가 아닌 [그림 2-3]에서 보여진 다른 취약점이 지금과 비슷한 상황이 될 수 있을 것이다.

시큐리티 이슈

MS10-002 Internet Explorer DOM(Document Object Model) Memory Corruption 제로데이 취약점 등장

2010년 1월 초부터 발생한 제로데이 공격으로 인하여 악성코드 유포가 많이 발생을 하였는데, 해당 제로데이 공격은 인터넷 익스플로러의 취약점을 이용하는 것으로 판명되었다.

해당 취약점은 인터넷 익스플로러의 DOM(Document Object Model) 처리과정에서 HTML 엔진에 존재하는 EVENTPARAM::EVENTPARAM 함수에서 발생한다.

공격자는 악의적인 HTML 코드를 생성하여 사용자의 컴퓨터에서 메모리 오류를 발생시킨 뒤 원하는 코드를 실행할 수 있다. 실제 공격자는 힙-스프레이(Heap-Spray)기법을 이용하여 메모리 상에 공격자의 쉘코드를 위치시키고, 다음 코드 상에서 쉘코드가 위치한 주소로 프로그램 실행 흐름(EIP)을 바꾸어 원하는 코드가 실행되도록 만든다.

```
mshtml!CElement::Doc:
046aa467 8b01        mov     eax,dword ptr [ecx]
046aa469 8b5034       mov     edx,dword ptr [eax+34h]
046aa46c ffd2        call    edx                    *** 쉘코드로 점프하
046aa46e 8b400c       mov     eax,dword ptr [eax+0Ch]

CallStack:
3:mshtml!CElement::Doc
2:mshtml!CEventObj::GenericGetElement
1:mshtml!CEventObj::get_srcElement

......
```

[그림 2-4] mshtml.dll 쉘코드 분기지점

일반적으로 공격자는 웹 서버를 해킹하여 MS10-002 취약점이 포함된 악성 스크립트를 특정 웹 페이지에 넣어두어 일반 사용자들이 해당 페이지를 열었을 경우 악성코드 등에 감염이 되게 한다. 아래는 MS10-002 취약점을 이용한 실제 공격 패킷이다.

```
                HEXA Code                        |   ASCII Code
75 30 63 30 64 5C 75 30  63 30 64 5C 75 30 63 30   u0c0d\u0c0d\u0c0
64 5C 75 30 63 30 64 5C  75 30 63 30 64 5C 75 30   d\u0c0d\u0c0d\u0
63 30 64 5C 75 30 63 30  64 5C 75 30 63 30 64 5C   c0d\u0c0d\u0c0d\
75 30 63 30 64 5C 75 30  63 30 64 5C 75 30 63 30   u0c0d\u0c0d\u0c0
64 5C 75 30 63 30 64 5C  75 30 63 30 64 5C 75 30   d\u0c0d\u0c0d\u0
63 30 64 5C 75 30 63 30  64 5C 75 30 63 30 64 5C   c0d\u0c0d\u0c0d\
75 30 63 30 64 5C 75 30  63 30 64 5C 75 30 63 30   u0c0d\u0c0d\u0c0
64 5C 75 30 63 30 64 5C  75 30 63 30 64 5C 75 30   d\u0c0d\u0c0d\u0
63 30 64 5C 75 30 63 30  64 5C 75 30 63 30 64 5C   c0d\u0c0d\u0c0d\
75 30 63 30 64 5C 75 30  63 30 64 5C 75 30 63 30   u0c0d\u0c0d\u0c0
64 5C 75 30 63 30 64 5C  75 30 63 30 64 22 3B 20   d\u0c0d\u0c0d";
0D 0A 20 20 20 66 6F 72  20 28 69 20 3D 20 30 3B   .. for (i = 0;
20 69 20 3C 20 78 31 2E  6C 65 6E 67 74 68 3B 20   i < x1.length;
69 20 2B 2B 20 29 0D 0A  20 20 20 20 7B 0D 0A 20   i ++ ).. {..
20 20 20 20 20 20 20 78  31 5B 69 5D 2E 64 61 74   x1[i].dat
61 20 3D 20 70 3B 0D 0A  20 20 20 20 7D 3B 0D 0A   a = p;.. };..
20 20 20 20 76 61 72 20  74 20 3D 20 65 31 2E 73   var t = e1.s
72 63 45 6C 65 6D 65 6E  74 3B 0D 0A 7D 0D 0A 0D   rcElement;..}...
0A 3C 2F 73 63 72 69 70  74 3E 0D 0A 0D 0A 3C 73   .</script>....<s
70 61 6E 20 69 64 3D 22  73 70 31 22 3E 3C 49 4D   pan id="sp1"><IM
47 20 53 52 43 3D 22 47  53 6C 2E 67 69 66 22 20   G SRC="GS1.gif"
6F 6E 6C 6F 61 64 3D 22  65 76 31 28 65 76 65 6E   onload="ev1(even
74 29 22 3E 3C 2F 73 70  61 6E 3E 3C 2F 62 6F 64   t)"></span></bod
79 3E 3C 2F 68 74 6D 6C  3E 0D 0A 0D 0A 0D 0A 3C   y></html>......<
73 63 72 69 70 74 20 6C  61 6E 67 75 61 67 65 3D   script language=
22 6A 61 76 61 73 63 72  69 70                     "javascrip
```

[그림 2-5] MS10-002 공격 발생 네트워크 패킷

일반적으로 인터넷 익스플로러 취약점은 위험함으로 반드시 보안 패치가 필요하며, 실제 유명 프로그램 웹사이트가 해킹되어 MS10-002 취약점을 이용하여 악성코드 유포에 이용되는 일도 발생하였다. 그리고 아직도 많은 수의 웹사이트에서 해당 취약점을 이용함으로 주의가 필요하다.

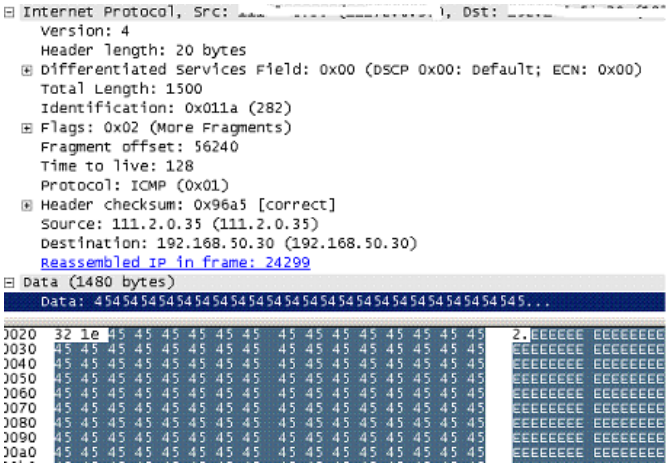
중국산 DoS 툴의 위험성

최근에 자동화된 DDoS(분산 서비스 거부 공격) 및 DoS(서비스 거부 공격) 툴들이 많이 등장을 하고 있는데, 이 중에서 이번달에 발견된 DoS 툴을 살펴보면 아래와 같다.

GUI로 제작이 되어 있으며 주된 공격 대상은 ICMP Flooding 기법을 사용한다. 공격 목표가 되는 IP를 직접 입력할 수 있도록 되어 있으며 시간 설정 및 공격 데이터 크기를 최대 63kb까지 설정 가능하다.

[그림 2-6] 중국산 DoS 툴

기본 설정의 DoS 공격패킷은 ICMP Flooding 기법으로 패킷 당 1480bytes 데이터를 전송하며 초당 9.5M DoS 공격이 발생하게 된다.



[그림 2-7] DoS 공격시 발생하는 네트워크 패킷

이 경우 해당 DoS 툴이 IP Spoofing 방법을 이용하지 않고 있어, 만약 위와 같은 패킷이 발생이 되면 해당 IP를 차단하는 방식을 이용하는 것이 효과적이라고 볼 수 있다. 이러한 DDoS 또는 DoS를 방어하기 위해서는 DDoS 방어 장비와 방화벽 등에서 소스 추적(Source Tracking)과 접속 제한(State Limit)을 적용하며 부하를 분산하기 위해서 로드밸런싱 등을 적용하는 방법도 있다.

Case Study: MS10-002 취약점을 사용한 악성코드 유포사례

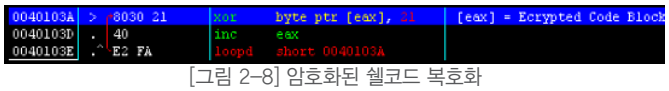
지금부터 MS10-002 취약점을 사용한 악성코드 유포사례에 대해서 살펴보도록 하자.

현재 운영 중인 Active Honeypot을 통해서 중국의 한 사이트에 침해사고가 발생하여 MS10-002 취약점을 사용한 악성코드를 탐지하였다.

http://www.*****qq.cn/
http://www. *****qq.cn/AkeleD/200804/3.js
http://down. *****.com/QQ/logo.js
http://00. *****.in/ba*****.htm <---- MS10-002 Exploit Script
http://00. *****.in/xbb.gif

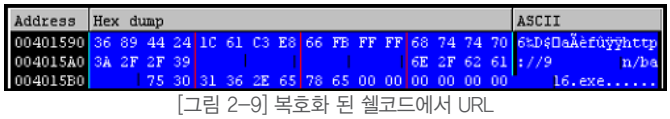
[표 2-2] MS10-002 Exploit Script 유포방식

[표 2-2]에서 보면 붉은 색으로 표시된 ba******.htm이 MS10-002취약점을 공격하는 Exploit Script이며 실행되면 스크립트 내부에 포함된 쉘코드가 실행되면서 특정 사이트로부터 실행파일을 받아온 후 실행한다.



[그림 2-8] 암호화된 쉘코드 복호화

쉘코드를 분석해 보면 [그림 2-8]처럼 암호화된 코드블록을 XOR을 사용하여 복호화하면 아래 [그림 2-9]에서 처럼 또 다른 악성코드를 다운로드 하는 URL이 존재함을 알 수가 있다.



[그림 2-9] 복호화 된 쉘코드에서 URL

[그림 2-9]에서 다운로드 되는 파일은 V3에서 Win-Trojan/Injector.28672.Y로 진단한다.

우리는 지금까지 언급된 내용을 통해서 보안이 고려되지 않는 인터넷 환경은 악성코드 감염과 그로 인해서 발생하는 부작용(개인정보 유출, 금전적/정신적인 피해 등)이 되풀이 될 수 밖에 없는 것을 알 수 있었다. 지금의 인터넷 환경은 편리함과 속도 그리고 보안이라는 이 세가지 요소를 동시에 고려해야 하는 상황인 것이다.

국가나 보안업체의 역할은 사용자들이 안전한 인터넷 환경을 사용할 수 있도록 제공하는 것이며, 보안의 중심은 국가나 보안업체가 아닌 사용자여야 한다. 즉 사용자 입장에서의 보안이라 함은 적어도 자신이 사용하는 OS 그리고 응용 프로그램을 어떤 것들이 있는지 알아두는 것이 필요하며

주기적인 보안패치 설치와 백신검사를 해주는 것이 좋다.

3. 웹 보안 동향

웹 보안 통계

웹 사이트 보안 요약

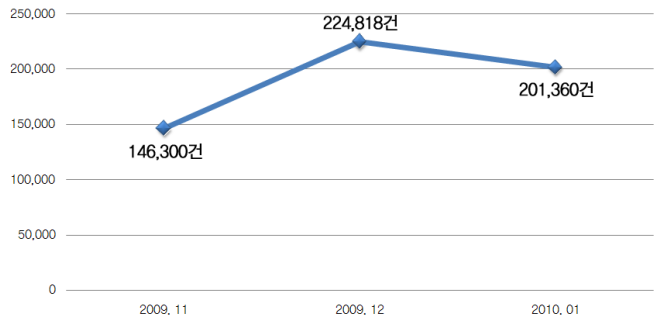
구분	건수
악성코드 발견 건수	201,360
악성코드 유형	1,084
악성코드가 발견된 도메인	983
악성코드 발견된 URL	6,106

[표 3-1] 웹 사이트 보안 요약

악성코드 발견 건수는 201,360건이고, 악성코드 유형은 1,084건이며, 악성코드가 발견된 도메인은 983건이며, 악성코드 발견된 URL은 6,106건이다.

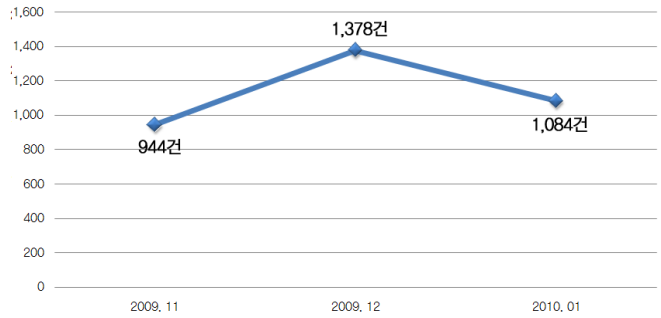
2010년 1월은 2009년 12월 보다 악성코드 발견건수와 악성코드 유형은 다소 감소하였으나, 발견된 도메인 및 URL은 증가하였다. 이와 같이 악성코드가 발견되는 도메인과 URL 수가 증가하는 것은 취약점을 가지고 있는 사이트가 많다는 것을 반증하며, 향후 악성코드 확산수가 급격히 증가할 소지가 있다는 것을 의미한다.

월별 악성코드 발견 건수



[그림 3-1] 월별 악성코드 발견 건수

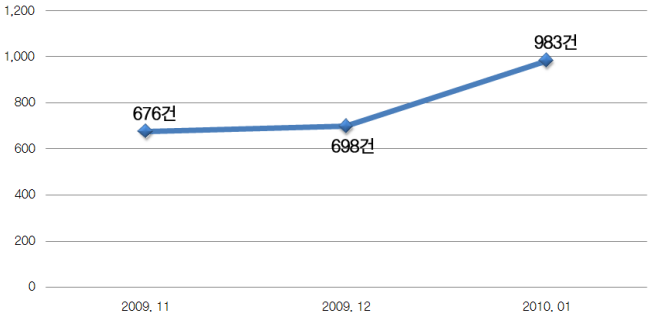
2010년 1월 악성코드 발견 건수는 전달의 224,818건에 비해 90% 수준인 201,360건이다.



[그림 3-2] 월별 악성코드 유형

2010년 1월 악성코드 유형은 전달의 1,378건에 비해 79% 수준인 1,084건이다.

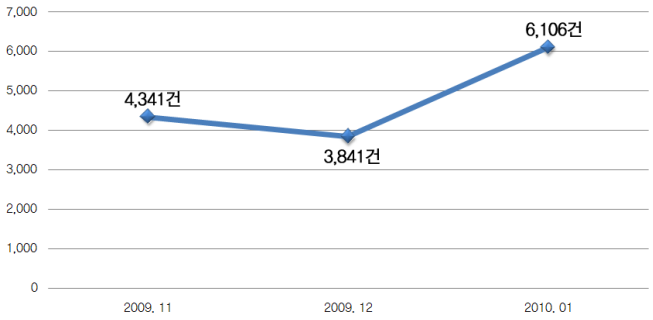
월별 악성코드가 발견된 도메인



[그림 3-3] 월별 악성코드가 발견된 도메인

2010년 1월 악성코드가 발견된 도메인은 전달의 698건에 비해 140% 수준인 983건이다.

월별 악성코드가 발견된 URL



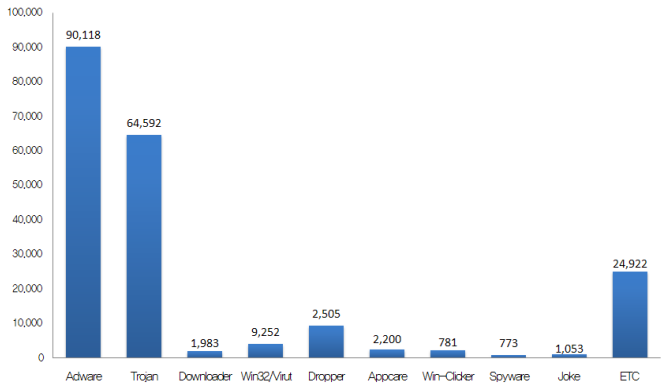
[그림 3-4] 월별 악성코드가 발견된 URL

2010년 1월 악성코드가 발견된 URL은 전달의 3,841건에 비해 159% 수준인 6,106건이다.

악성코드 유형별 배포 수

유형	건수	비율
Adware	90,118	44.8 %
Trojan	64,592	32.1 %
Downloader	1,983	1 %
Win32/Virut	3,954	2 %
Dropper	9,252	4.6 %
AppCare	2,505	1.2 %
Win-Clicker	2,200	1.1 %
Spyware	781	0.4 %
JOKE	1,053	0.5 %
기타	24,922	12.4 %
합계	201,360	100 %

[표 3-2] 월별 유형별 배포 수



[그림 3-5] 월별 유형별 배포 수

악성코드 유형별 배포 수에서 애드웨어(Adware)류가 90,118건 전체의 44.8%로 1위를 차지하였으며, 트로잔(Trojan)류가 64,592건으로 전체의 32.1%로 2위를 차지하였다.

악성코드 배포 Top 10

순위	등락	악성코드명	건수	비율
1	–	Win-Adware/Shortcut.InlivePlayerActiveX.234	42,845	34.7 %
2	↑ 7	Win-Trojan/Agent.57344.AHB	20,814	16.9 %
3	–	Win32/Induc	15,000	12.2 %
4	New	Win-Trojan/OnlineGameHack.324096.C	14,751	12 %
5	↓ 1	Win-Adware/Shortcut.IconJoy.642048	7,938	6.4 %
6	–	Win-Dropper/KorZlob.5132206	5,067	4.1 %
7	–	Win-Adware/Shortcut.K2Com.Sobang.266240	4,778	3.9 %
8	↓ 3	Win-Adware/BHO.HiMyCar.237568	4,520	3.7 %
9	New	Win32/Parite	3,862	3.1 %
10	New	Win-Adware/Rogue.PCCare.281160	3,745	3 %
합계			102,807	100 %

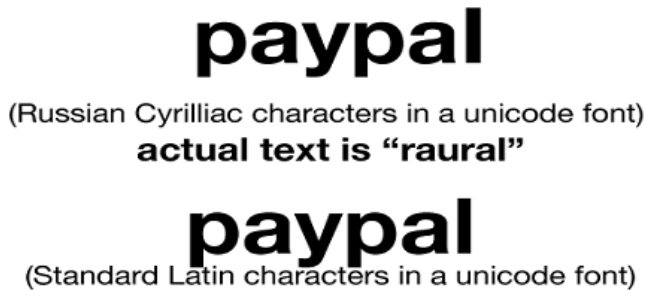
[표 3-3] 악성코드 배포 Top 10

악성코드 배포 Top 10에서 Win-Adware/Shortcut.InlivePlayerActiveX.234가 지난달과 같이 42,845건으로 1위를 차지하였으며, Top 10에 Win-Trojan/OnlineGameHack.324096.C 등 3건이 새로 등장하였다.

웹 보안 이슈

도메인 명 정책 변경으로 인한 피싱 주의!

2010년부터 도메인 명에 영어가 아닌 제3의 외국문자를 사용하는 것이 허용되었다. 각 국가에서는 다국어를 사용함으로써 편리한 점도 많지만, 다국어를 사용하게 되면서 발생할 수 있는 여러 보안 취약점 중 피싱과 관련한 보안 문제가 우려된다.

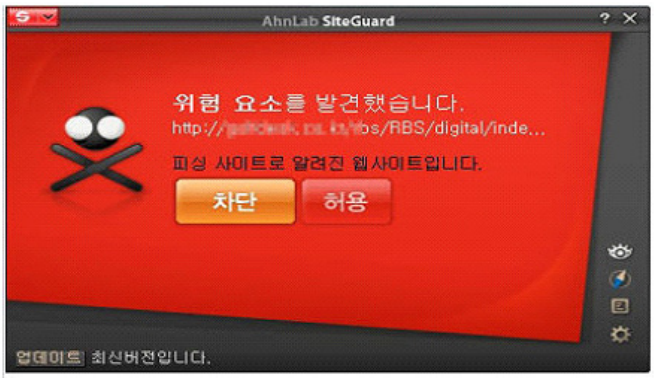


[그림 3-6] 다국어 사용시 피싱사이트로 사용가능성이 있는 도메인명

[그림3-6]은 그냥 보기엔 같아 보이지만 아래 문자가 영문자 “paypal”이며 위에 있는 문자는 러시아어로 실제 단어는 “raural”이다. 실제 단어는 다르나 눈으로 보기엔 동일한 형태로 구현이 가능하기 때문에 이러한 문제점을 이용한 피싱 사이트가 생겨 날 수 있다.

위와 같은 피싱 사이트를 예방하기 위해서는 이전까지는 자신이 접속한 사이트에 대한 도메인 명에 대해서 주의를 기울이는 등의 예방법이 있었지만, 이제는 단순 주의만으로는 이러한 피싱 사이트를 확인하기에는 불가능하다고 볼 수 있다.

따라서, 해당 사이트의 위험성을 확인할 수 있는 사이트가드(http://www.siteguard.co.kr)와 같은 웹 보안 제품 사용을 권한다.



[그림 3-7] 피싱 사이트 접속 시 사이트가드 알림창

AhnLab SiteGuard Pro

2010년 Vol. 01

ASEC REPORT 집필진

편 집 장 선임 연구원 허 종 오

집 필 진 선임 연구원 정 진 성
선임 연구원 이 정 형
선임 연구원 허 종 오
주임 연구원 박 종 석
주임 연구원 안 창 용
주임 연구원 박 시 준

감 수 상 무 조 시 행

참여연구원 ASEC 연구원
SiteGuard 연구원