

게임 산업에서의 Vista(ActiveX) 파급효과와 보안의 이슈

NHN 보안분석 팀장 전 상훈(바다란)

p4ssion@nhncorp.com

요약:

게임 산업에서 Vista 출시가 의미하는 보안 환경의 변화와 위협요소에 대해 설명을 하고 어떤 위협이 존재 하고 있는지 인지 하는 것이 필요하다. 현재의 게임산업이 처한 보안상의 위협요소들을 먼저 확인을 하며 Vista로 인해 달라지는 보안상의 위협요소에 대해 명시 하도록 한다. Vista에서 강화된 보안기능으로는 ActiveX의 실행제한과 UAC (User Access Control) 기능을 들 수 있는데 온라인 게임에 미치는 영향과 보안상의 이슈에 대해서 관계를 확인 하여 보고 향후 방향에 대해 조망한다.

1. 서론

현재의 게임의 환경에서 운영체제가 가지는 의미는 중요한 요소를 포함하고 있다. 온라인 게임의 개발에는 특정 운영체제에 한정되어 개발되는 부분이 많았으며 다양한 운영체제로부터의 접근성을 보장하지는 않는다. 따라서 운영체제의 실행 환경이 변경 된다면 다양한 구조적인 변화를 할 수 밖에 없다. 2007년 Vista™의 출시와 함께 촉발되고 현실화된 온라인 게임의 위험요소와 보안의 관점에서 바라본 Vista™ 출시로 인한 문제점들을 짚어보고 향후 방안에 대해서 고민을 하는 과정이 필요하다.

2. 온라인 게임의 환경과 위험요소

2.1. 게임의 환경

게임의 환경 측면에서는 보안적인 이슈와 관련이 있는 부분에 대해서 한정하여 살펴보고 전체적인 게임의 환경에 대해서는 언급을 하지 않도록 한다. 게임에서 운영체제의 급격한 정책 변경은 큰 영향을 받을 수 밖에 없다. 운영체제에 부여된 일반적인 기능과 접근 방법을 통해 실행이 된다는 점에서 보면 정책의 변경은 큰 영향을 미칠 수 밖에 없다. 국내의 온라인 게임 상황에서는 대부분의 게임이 Windows 베이스의 게임을 제작하고 있으며 온라인 상에서 실행을 시키는 메소드를 활용 함으로써 사용자의 접근을 유도하고 있는데 IE7과 Vista로 인해 변경된 정책은 큰 영향을 미칠 수 밖에 없다.

성공적인 게임의 런칭 이후에 운영에서 가장 중요한 영향을 미치는 이슈가 보안이며 단계별 보안이 이루어 지지 않는 게임은 안정적인 운영을 하기 어려운 상황에 쉽게 처할 수 밖에 없다. IE7과 Vista에서 가장 중요하게 강조되는 기능이 보안 기능의 강화라는 측면에서 온라인 게임은 영향을 받을 수 밖에 없으며 다소간의 긍정적인 효과와 부정적인 효과를 동시에 받을 수 밖에 없다. 본 논문에서는 긍정적인 효과와 부정적인 효과를 찾아보고 영향력과 파급효과는 어느 정도 인지 확인을 하도록 한다.

온라인 게임에 직접적인 영향을 미치는 보안적인 이슈 측면에서는 크게 세 가지 유형으로 살펴 볼 수 있다. 직접 해킹을 통한 게임의 피해, 게임내의 Abusing을 통한 피해, 악성코드를 이용한 사용자 정보의 유출로 구분을 할 수 있다.

2.2. 직접 해킹을 통한 게임의 피해

게임의 웹서버 및 Database서버와 같은 Game Infra 구성요소에 대한 직접 해킹을 시도 함으로 인해 발생하는 피해를 총칭하며 2005년부터 급증하기 시작한 웹 서버에 대한 해킹 시

도 및 Database에 대한 직접 해킹 시도들이 다 포함이 된다. 웹 서버의 웹 어플리케이션의 취약성을 이용한 (SQL Injection , File Upload / Download , Privilege Escalation ...) 공격 유형이며 공격을 통해 웹 서버의 관리자 권한을 획득한 이후 자유자재로 조작하는 것을 의미하며 Database 서버에 대해 직접 Query 등을 통해 사이버 머니 혹은 아바타 획득과 같은 인위적인 조작을 가하는 것을 의미한다. 직접 해킹으로 인한 피해는 단계별 보안 대책 수립과 웹 어플리케이션 보안성 강화에 따라 점차 감소 추세를 보이고 있으나 여력이 부족한 신규 게임업체나 중소 게임업체에는 여전히 위협이 되고 있는 실정이다.

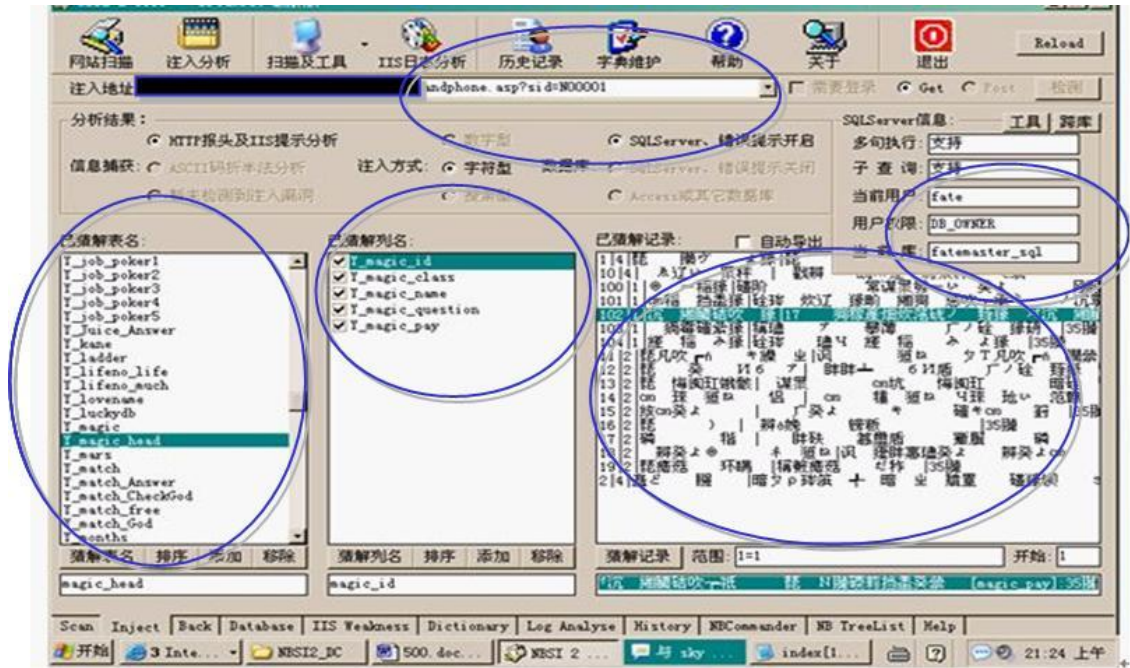


그림 1. SQL Injection Attack Example

그림 1의 경우는 웹 어플리케이션의 취약성을 이용하여 웹 서비스의 권한을 획득한 이후 데이터베이스에 접근하는 계정을 통해 데이터베이스의 내용을 가져오는 공격도구의 모습이다. 웹 어플리케이션에서 사용되고 있는 URL의 인자에 대해 Validation 검증이 제대로 되지 않은 취약성을 이용하여 SQL Query를 실행 시킴으로써 권한을 획득하는 SQL Injection 공격 기법을 사용 하였다.

그림 1에서 보인 SQL Injection 공격 이외에도 다양한 공격 기법으로 웹 서버와 서비스를 공격하여 권한을 획득하거나 제어 함으로써 직접적인 피해를 입히는 경우는 일반적인 유형 이라 볼 수 있다.

2005년 이후의 공격 유형의 특징을 보면 시스템 및 운영체제에 대한 직접적인 해킹은 줄어드는 경향을 보이고 있으며 Application에 대한 공격 유형이 일반화 되는 경향을 보이고 있다. 즉 운영체제를 이용하여 동작을 하는 Application의 취약성을 이용하여 공격하는 동향을 볼 수 있으며 공개 소프트웨어의 취약성을 이용하는 Application Attack의 일반화를 확

인 할 수 있다.

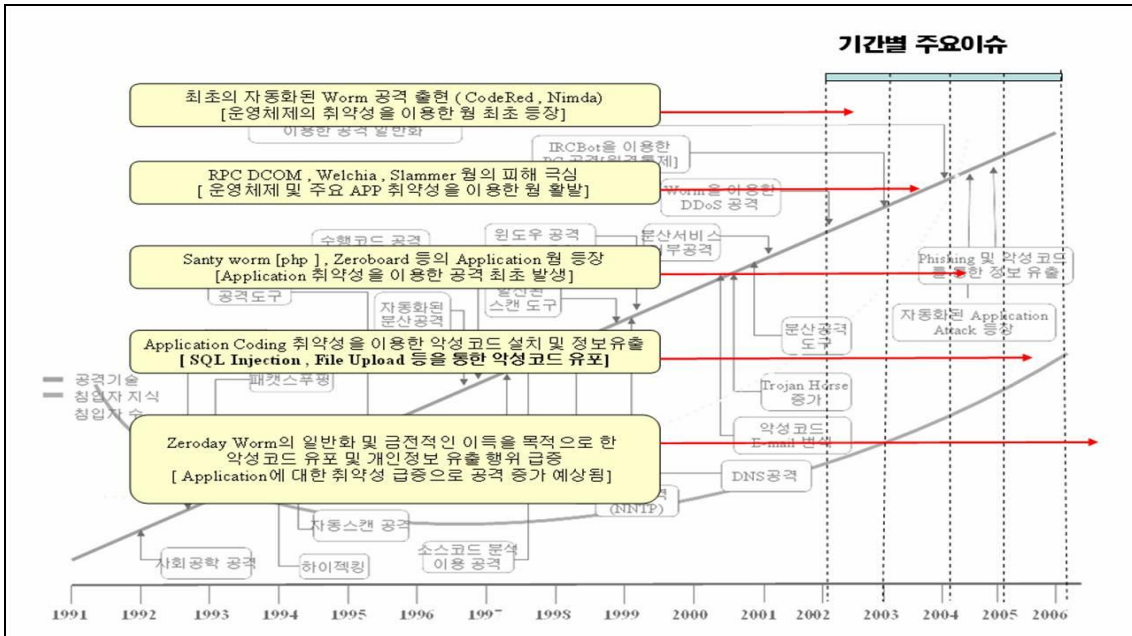


그림 2. Attack flow

그림 2 에서 전체 해킹 동향의 변화 흐름을 보이고 있다. 2004년 이후부터 개별 Application에 대한 공격이 증가됨을 볼 수 있으며 2005년에 이르러 자동화된 Application 공격이 나타나고 2006년 이후로 계속 Application에 대한 공격이 증가 되는 경향을 나타내고 있다. 전체 취약성의 발견 비율에서도 Application 취약성에 대한 발견 비율은 급증함을 볼 수 있다.

Microsoft Internet Explorer XmlHttpRequest Parameter Validation Weakness 2007-02-05 http://www.securityfocus.com/bid/14969
Microsoft Word 2000 Unspecified Code Execution Vulnerability 2007-02-05 http://www.securityfocus.com/bid/22225
Microsoft Office Malformed String Remote Code Execution Vulnerability 2007-02-05 http://www.securityfocus.com/bid/22383
Microsoft Internet Explorer Malformed HTML For Script Denial of Service Vulnerability 2007-02-05 http://www.securityfocus.com/bid/22408
Windows Vista Voice Recognition Command Execution Vulnerability 2007-02-01 http://www.securityfocus.com/bid/22359
Microsoft Excel Malformed Palette Record Remote Code Execution Vulnerability 2007-02-01 http://www.securityfocus.com/bid/21922
Microsoft Excel Opcode Handling Unspecified Remote Code Execution Vulnerability 2007-02-01 http://www.securityfocus.com/bid/21952
Microsoft Excel Malformed String Remote Code Execution Vulnerability 2007-02-01 http://www.securityfocus.com/bid/21877
Microsoft Excel Malformed Column Record Remote Code Execution Vulnerability 2007-02-01 http://www.securityfocus.com/bid/21925
Microsoft Excel IMDATA Record Remote Code Execution Vulnerability 2007-02-01

그림 3. securityfocus의 MS 관련 취약성

그림 3에서 Securityfocus (www.securityfocus.com) 사이트에 보고된 Microsoft 사의 제품 취약성에서도 운영체제가 아닌 개별 Application에 대한 취약성 보고가 증가됨을 확연하게 확인 할 수 있다.

Application 취약성은 계속 증가하고 있으며 취약성에 따른 웹 서버와 서비스에 대한 해킹은 계속 증가하는 것을 확인 할 수 있다. 온라인 게임 서비스에서도 동일한 규칙이 적용되고 있으며 부실한 웹 서비스 코딩 과 게임 관련된 데이터베이스 서버의 관리의 부실로 인해 전체적인 취약성과 공격 동향에 따른 위험성은 계속 증가되고 있는 상황이다. 특히 웹 어플리케이션을 통해 온라인 게임 유저와의 접촉을 유지하고 있는 온라인 게임사의 경우 웹 어플리케이션의 문제는 대외적인 신뢰도 하락 및 게임사의 인프라 내부망까지 침입을 입을 수 있다는 개요를 포함하고 있어서 치명적인 이슈가 될 수 있다.

2.3. 게임내의 Abusing유형

직접적인 해킹 이외에도 온라인 게임에 영향을 미칠 수 있는 보안적인 이슈로는 Abusing을 예로 들 수 있으며 각 Abusing유형은 특정 온라인 게임에 한정되어 발전이 되는 경향을 보이고 있다. 즉 특정 온라인 게임에만 특화된 Abusing 솔루션들을 통해 선의의 게임 사용자에게 영향을 미칠 수 있고 피해를 입힘으로써 사용자의 접근성을 떨어뜨리게 되고 정상적인 게임 사용자가 피해를 입음으로써 사용자의 이탈까지도 유발하게 되는 중요한 이슈가 된다. 게임 내에서 이루어지는 Abusing 영역은 다음과 같이 세분화 하여 나열 할 수 있다.

기술적인 부분과 작동 방식에 따른 분류이다. 가장 기본적인 부분은 온라인 게임의 실행 클라이언트 프로그램에 대한 Binary 분석과 실행구조의 분석을 통해서 이루어 지며 간단한 기술부터 전문적인 기술 영역까지 혼재하고 있다.

Memory Hack : 온라인 게임 클라이언트 프로그램에서 사용하는 메모리 주소를 조작함으로써 게임의 아이템 비율을 조작하거나 승부를 조작할 수 있는 유형

Macro: 사용자의 입력 없이 자동으로 게임을 진행 하도록 하는 유형

Speed Hack: 클라이언트 PC의 속도를 조작하여 게임의 속도를 조작하는 유형

Debugging: 게임의 로직을 분석하고 게임 클라이언트 내의 숨겨진 정보를 분석하여 활용하는 유형

Packet Hack: 게임 클라이언트와 서버간에 주고 받는 패킷을 조작하여 게임을 컨트롤 하는 유형

Client Manipulation: 게임 클라이언트 프로그램의 변경 및 조작을 통한 컨트롤을 하는 유형

표 1. Abusing 방식과 대응

Abusing 유형	방식	대응
Memory Hack	Memory를 외부 프로세스에서 접근하여 조작함, 커널레벨에서는 타 프로세스 접근 가능한 점을 이용하여 조작	Memory Hack 관련 process의 접근 차단 , Memory I/O 관련 함수 Hooking 차단
Macro	키보드 및 마우스 이벤트를 프로그램적으로 발생 시키고 발생된 이벤트에 의해 게임이 반응	Port IO 모니터링 , Filter Driver 사용 , System Function call 차단 방식을 활용
Speed Hack	PIT (Programmable Interval Timer)변조 , Time 관련 함수의 Hooking	Time 관련 함수 Hooking 차단 , CPU의 Clock을 검사하여 변조 감시
Debugging	OllyDbg 나 SoftIce와 같은 Debugging 도구를 이용하여 조작	게임 실행 process hiding , 실행파일 변조여부 확인 , 실행파일 protect를 통한 차단
Packet Hack	Socket 관련 함수 Hooking , TDI , NDIS 등의 packet filter 활용	악의적인 process 접근 차단 , API Hooking 차단
Client Manipulation	Client에 다운된 게임 관련 파일의 직접조작 , 파일 관련 함수를 Hooking하여 조작	게임 실행 파일의 Checksum 검사 , 중요 기능에 대한 검토 이후 실행 루틴 적용등

각 Abusing 유형에 대해 대응 하는 방식은 표 1에서 기술된 것과 같은 유형으로 대응을 진행하고 있다. 그러나 표 1과 같은 다양한 Abusing 유형에 대해 대응 하기 위해 게임 클라이언트 프로그램 차원에서 protect를 하는 것은 매우 어려운 일이며 게임을 위한 게임 프로그램보다 차단을 하기 위한 프로그램적인 기능이 더욱 구현하기 어렵고 큰 영역을 지니고 있다. 따라서 일반적으로 다양한 Abusing 위협을 제거 하고 게임 클라이언트를 보호하기 위해 게임보안툴을 적용하는 것이 일반적이다. 게임보안툴의 적용은 게임 실행 초기에 실행이 되고 정상 상태를 확인 한 이후 게임실행 중의 Abusing 행위를 방어하는 역할을 수행한다.

719E4289	90	NOP	
719E428A	8BFF	MOU EDI,EDI	ws2_32.send
719E428C	. 55	PUSH EBP	
719E428D	. 8BEC	MOU EBP,ESP	
719E428F	. 83EC 10	SUB ESP,10	
719E4292	. 56	PUSH ESI	
719E4293	. 57	PUSH EDI	
719E4294	. 33FF	XOR EDI,EDI	
719E4296	. 813D 28409F71	CMP DWORD PTR DS:[719F4028],WS2_32.719E94C1	
719E42A0	..0F84 AD730000	JE WS2_32.719EB653	
719E42A6	> 8D45 F8	LEA EAX,DWORD PTR SS:[EBP-8]	
719E42A9	. 50	PUSH EAX	[Arg1
719E42AA	. E8 12520000	CALL WS2_32.719E94C1	WS2_32.719E94C1
719E42AF	. 3BC7	CMP EAX,EDI	

그림 4 packet 조작을 위한 send 함수

719E4289	90	NOP	
719E428A	-E9 21D01997	JMP WpeSpy.08B812B0	ws2_32.send
719E428F	. 83EC 10	SUB ESP,10	
719E4292	. 56	PUSH ESI	
719E4293	. 57	PUSH EDI	
719E4294	. 33FF	XOR EDI,EDI	
719E4296	. 813D 28409F71	CMP DWORD PTR DS:[719F4028],WS2_32.719E94C1	
719E42A0	..0F84 AD730000	JE WS2_32.719EB653	
719E42A6	> 8D45 F8	LEA EAX,DWORD PTR SS:[EBP-8]	
719E42A9	. 50	PUSH EAX	[Arg1
719E42AA	. E8 12520000	CALL WS2_32.719E94C1	WS2_32.719E94C1
719E42AF	. 3BC7	CMP EAX,EDI	

그림 5. packet 조작을 위한 send 함수 변경

그림 4, 그림 5에서는 packet hack을 위해 packet 전송을 하는 루틴을 debugger로 확인을 한 내용이다. 그림 4에서 선택된 send 함수가 그림 5에서는 packet을 가로채어 전송하는 packet manipulation 도구의 send 함수로 바뀌어 진 것을 볼 수 있다. 위와 같은 Packet Hack의 기능은 게임 실행 프로세스에 packet 전송을 가로채는 도구를 간단하게 Attach만 시키면 되는 조작 기법이다.

게임보안툴의 사용을 통해서 표 1에 기술된 다양한 영역의 Abusing을 방어하여 게임을 보호하고 있으나 공격 기술의 발전이 빨라 대응에 어려운 점이 있다. 게임보안툴의 사용 이외에도 게임의 구조를 서버 단위의 실행 구조로 변경 함으로써 대응을 하고 있으나 전체의 기능을 변경 할 수 없는 게임의 특성상 발전하는 Abusing에 대해 모니터링을 통한 감시와 게임보안툴과 게임 실행 구조의 변경을 통한 안정성 확보만이 주된 방안이라 할 수 있다.

표 1의 대응 방식에서 보듯이 게임클라이언트는 사용자가 클라이언트 프로그램을 사용자의 PC에 다운로드 받고 설치 한 이후에 실행을 하는 구조이다. 따라서 사용자 시스템의 주요 기능들을 이용할 수 밖에 없다. Abusing 유형에서도 보듯이 시스템의 기능들을 이용하여 실제 클라이언트의 기능이나 효과를 변경 함으로써 게임에 영향을 미치는 것을 볼 수 있다.

게임보안툴의 사용은 사용자의 시스템에 일정부분에 대해 제한을 가하는 구조이며 시스템의 하위 권한까지도 충분히 부여가 되어야만 한다. Vista™와의 충돌은 시스템 권한의 부여에서 시작된다.

2.4. 악성코드를 이용한 사용자 정보 도용 위험

2005년 이후 온라인 게임업체 및 IT 관련 서비스 업체에 영향을 미치는 중요요소로서 사용자 정보를 유출 하기 위한 악성코드의 설치를 들 수 있다. 현재까지도 줄어들지 않고 있는 상황이며 향후에도 지속될 것으로 예상이 된다.

주된 악성코드의 유형은 사용자의 계정정보를 유출하기 위한 Key logging 기능이 일반적이며 사용자의 ID와 Password를 공격자가 지정된 장소로 전달 되도록 하는 유형이 가장 큰 피해를 입히고 있다.

Key logging 을 시도하는 악성코드를 유포하기 위해 국내 대규모 사이트를 해킹하여 다수의 사용자에게 유포하도록 함으로써 피해를 입힌 경우가 다수 존재 하였다. 사이트를 해킹한 이후 사용자 정보를 유출하는 악성코드를 해당 사이트에 접근 하는 사용자에게 Windows 취약성을 이용하여 자동 실행 되도록 하였으며 사용자의 ID/ Password를 유출하도록 동작 되었다. 그림 6 은 한게임에서 제공하는 온라인 게임백신에서 탐지된 한게임 관련된 악성코드 제거 결과로서 한게임 사용자를 대상으로 한 악성코드를 제거한 결과이다.

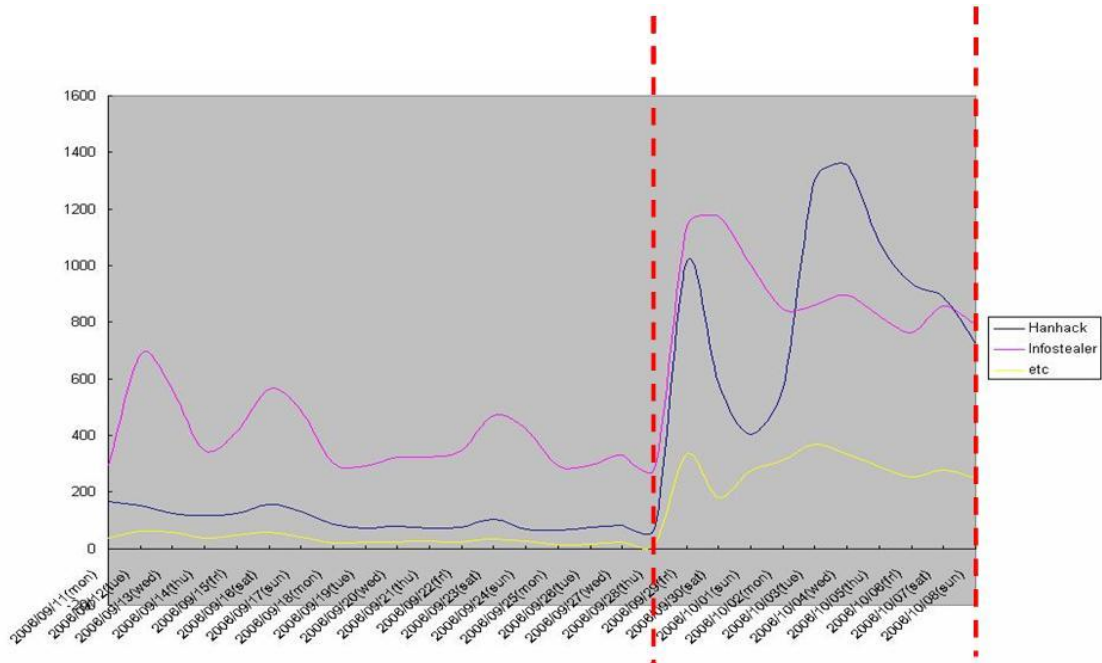


그림 6. 악성코드 제거 결과 - Hangame 전용백신

그림 6의 결과는 2006년 9월에서 10월까지의 한달 가량의 탐지 결과로서 특정 기간에 탐지 횟수가 급증하는 것을 확인 할 수 있다. 결과가 급증된 구간은 대규모 사이트를 통해 악

성코드가 사용자에게 유포된 이후 악성코드에 대한 분석이 완료된 이후 한게임 전용백신을 통해 온라인 상에서 사용자의 PC의 악성코드를 탐지 및 제거한 내용이다. 최초 악성코드 발견 이후 평균 이틀 정도의 시간 간격으로 악성코드를 제거 하도록 업데이트를 하였는데 탐지 결과가 대폭 증가하는 것을 확인 할 수 있다. 그림 6과 같은 증가 유형은 전용백신 서비스를 시작한 2006년 1월 이래 줄곧 반복되어온 유형이며 대규모 사이트가 해킹 되어 악성코드가 유포될수록 매우 많은 탐지 및 제거 결과가 나오는 것을 확인 할 수 있다.

현재에도 온라인 게임에 직접적인 위협이 되는 사용자 계정 유출 악성코드는 변형이 계속 나오고 있으며 기법적으로도 다양하고 수준 높은 공격유형들이 출현하고 있어서 대응이 어려운 면이 존재한다. 사용자의 PC에 설치된 백신의 경우 탐지 및 업데이트까지 걸리는 주기가 길어 실제적인 효과를 보는 것이 어려운 경우도 있다. 규모가 큰 온라인 게임사 이외에도 주요 온라인 게임 전체를 대상으로 하고 있어서 지금도 많은 계정 유출 피해가 우려되고 있다.

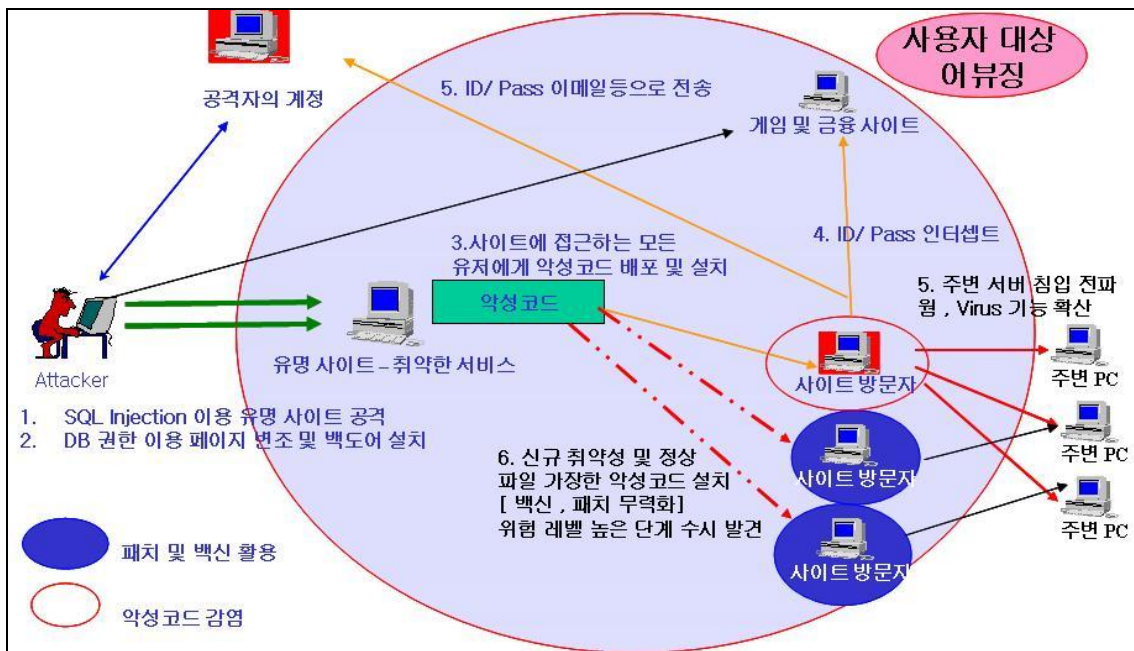


그림 7. 온라인 게임에 대한 악성코드 공격 분석

그림 7은 사용자 정보 탈취를 위한 악성코드의 실행 과정 및 진행 상황을 도식화한 것이다. 그림 7의 설명에서 볼 수 있듯이 2006년 하반기 이후에는 신규 취약성 및 백신에 탐지가 되지 않는 형식의 악성코드를 유포하여 보안패치와 보안 솔루션을 사용하는 사용자에게도 일부 피해가 발생하고 있는 실정이다.

악성코드를 이용한 사용자 정보 유출로 인해 온라인 게임업체들은 많은 비용과 전문인력을 투입하여 게임을 보호하고 사용자를 보호하는 방안을 고민 할 수 밖에 없는 상황이다.

현재 유포되고 있는 악성코드는 종결형이 아닌 현재 진행형이고 앞으로도 끊임 없이 나타날 현상이라 할 수 있다. 키보드보안 솔루션과 보안패치 서비스, 온라인게임 전용백신서비스 등 다양한 보호방안을 만들어 전체 위협요소의 대다수를 제거하여도 새롭게 발전하는 공격 기술의 진화속도를 따라 가는 것은 어려움이 따를 수 밖에 없다. 일부 피해는 계속 발생할 것이고 피해를 줄이기 위한 노력도 계속 될 수 밖에 없다.

3. Vista™의 보안과 온라인게임

3.1 Vista™의 보안기능

Vista™의 출시와 더불어 Microsoft사에서 가장 강조한 부분은 보안성의 강화라고 할 수 있다. Vista™에 포함된 보안 기능은 무엇이 있으며 어떤 역할을 하는지 간략하게 살펴보도록 한다. 제품 출시와 더불어 대대적으로 홍보가 된 보안기능은 UAC (User Access Control) 기능과 ActiveX의 실행제한 부분을 꼽을 수 있다. 중요한 부분은 구조적으로 시스템에 접근할 수 있는 영역을 제한하고 권한을 제한했다는 점에 있다. 일반적인 사용자 권한과 시스템의 관리자 권한을 분리 시켜 두고 실행 권한까지도 제한을 두고 있다는 점이 가장 강화된 기능이며 권한 제어 기능에 따라 ActiveX에 대한 실행 모듈들도 변경이 될 수 밖에 없다. 지금까지는 시스템에 접근 할 수 있고 설치가 웹을 통해서 진행 될 수 있도록 ActiveX가 프로그래밍 되어 있었다면 ActiveX에 대한 설치 이슈는 시스템적인 접근을 상당부분 배제하는 유형으로의 접근으로 전환이 되어야만 한다.

국내에서 발생하는 ActiveX 관련 이슈는 대부분 기능의 제한과 시스템에 접근하는 실행 모듈 부분의 변경에 따라 일정 수준 이상 해결 될 수 있는 부분이다.

Vista™의 권한 모델은 총 5가지로 나눌 수 있다.

System ,High , Medium , Low , Untrusted 의 5가지 유형으로 권한을 나눌 수 있다. Explorer의 경우에는 Medium 권한이 주어지고 IE의 경우에는 Low 권한이 주어지고 있다. ActiveX를 활용할 경우 레지스트리에 대한 접근 및 파일 시스템에 대한 접근에서 권한 상승을 위한 UAC (User Access Control) Alert을 볼 수 있다. 그림 8에서 UAC의 실제 모습을 볼 수 있다. 즉 권한에 따른 실행 및 설치에 대한 제어를 명확하게 한다는 의미라고 볼 수 있다. 지금까지는 사용자의 동의 없이 실행 되거나 최초 동의 (사용자의 선택에 의한 선별적 동의) 이후에는 지속적으로 실행이 되는 구조를 지니고 있었으나 현재 Vista™와 IE의 제한 환경에서는 매번 실행 시마다 권한 상승을 요구하는 승인 창이 뜨게 된다.

사용자의 동의에 따라 최초 설치가 된 ActiveX라 할지라도 시스템에 접근할 경우에는 반드시 권한 상승을 요구하는 승인 창이 활성화 되는 것이 기본 개요라 할 수 있다.

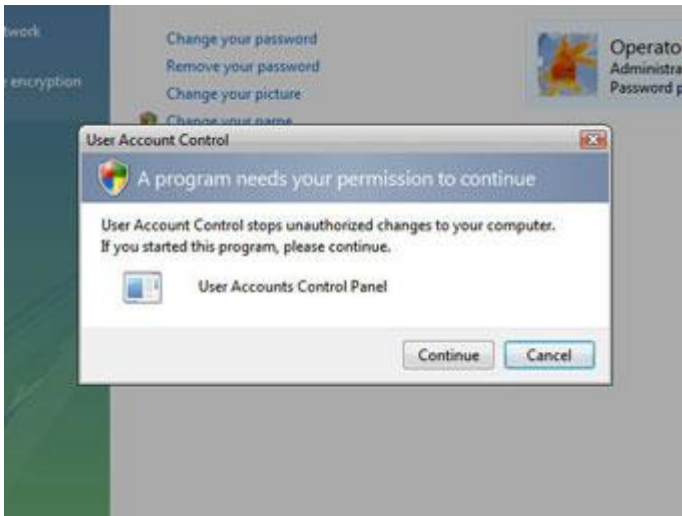


그림 8. UAC (User Access Control)

그림 8 에서 보여지는 UAC를 통한 강력한 권한 통제 부분은 사용자의 인식 없이 실행 되던 무분별한 ActiveX에 대한 폐해를 막을 수 있다는 점에서 긍정적이며 무분별하게 시스템에 접근하여 원하는 행위를 하도록 코딩이 된 ActiveX의 구조적인 환경 변화를 피할 수 있다는 점에서 긍정적이라 볼 수 있다.

지금까지처럼 사용자가 인터넷 환경에서 보안패치와 바이러스 백신에 의존하여 불안한 인터넷 사용을 할 수 밖에 없었다면 Vista™와 IE에서의 UAC를 통한 권한 통제 부분과 ActiveX 실행제한 부분은 일정부분 안전한 환경을 보장해 줄 수 있다. ActiveX를 이용한 광고 솔루션 및 악성코드 부분은 Vista™ 사용시에 대폭 줄어들 수 밖에 없을 것이다.

다만 Vista™의 취약성 혹은 IE7의 취약성을 이용한 새로운 공격이 나오거나 Vista™에 탑재된 기본 Application (시스템 접근을 위한 권한을 지니고 있는 Application)에 신규 취약성이 발견될 경우는 문제가 된다. 악성코드 설치 유형이나 사용자에게 피해를 입히는 유형이 ActiveX 유형만 존재하는 것이 아니며 System 권한 획득까지 가능한 취약성의 유형은 매우 심각한 위협을 발생 시킬 수도 있을 것이다.

취약성을 이용하는 직접적인 공격은 IE가 가지고 있는 Low Level 권한에서 권한 상승을 시킬 수도 있으며 사회적인 해킹 방법을 이용하여 사용자를 속일 경우 일시적인 권한 획득이 가능한 문제들은 계속 될 수 밖에 없다. 피싱에 대한 위험요소도 이전의 운영체제와 동일하게 유효하다.

보안상 가장 안전하다고 적극 주장 한 제품이지만 그 어떤 제품이라도 완벽 할 수 없다. 2007년 1월에는 Graphic Rendering Engine 기능을 수행하는 시스템 파일에서 원격에서 실행이 가능한 취약성이 발견되어 공식적으로 Vista 상에서 발표된 보안패치 1호가 되었다.

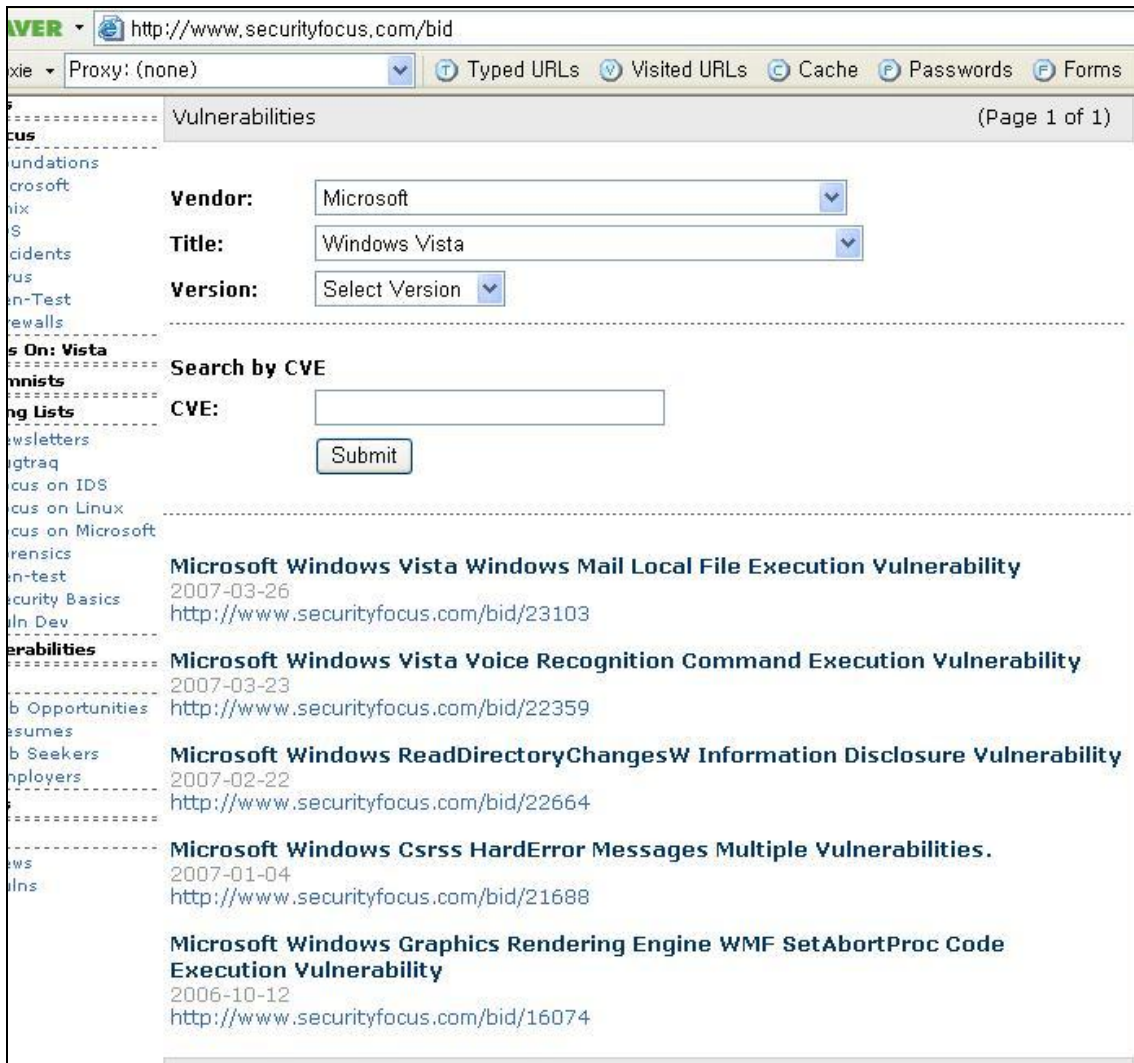


그림 9. Vista security vulnerability

그림 9의 내용은 SecurityFocus 사이트의 BugTraq에 올려진 일반적인 취약성 항목에서 Vista™로 검색을 한 내용이다. Vista™의 내부 시스템과 직접 관련이 있는 심각한 취약성은 아직 발견되지 않았으나 Vista™ 상에서 기본적으로 실행이 되도록 포함이 된 기능들에서 문제가 발견이 되었으며 외부에서 명령 실행 및 권한 획득이 가능한 문제들이 발견이 되었다.

주의 깊게 보아야 하는 부분은 공식적으로 발표된 Vista™의 보안패치는 2007년 1월에 발표가 되었으나 (<http://www.microsoft.com/downloads/details.aspx?familyid=228f2cdc-7148-4002-86bb-e4ade080ea86&displaylang=en>) 취약성에 관련된 항목은 2006년 10월에 WMF 파일에 대한 Graphics Rendering Engine Code Execution 문제에 대한 패치와 관련이 있다. Windows 계열의 모든 운영체제에서 문제가 발견이 되었으며 Vista™에서

는 Vista December CTP 버전에서 문제가 발견이 되었다. 물론 사용자에게 출시된 버전에서는 문제가 수정된 상태에서 출시가 되었다.

WMF 파일 처리 루틴에서 발견된 취약성의 의미는 운영체제 위에서 실행되는 Application에 대한 취약성은 운영체제의 구조가 변경이 되어도 완전히 새롭게 개발이 되지 않는 이상 동일하게 유지가 된다는 점이다. 사실상 운영체제에서 커널 부분을 제외하고는 모두가 Application이라 할 수 있다. 그리고 운영체제 위에 설치가 되는 프로그램들도 모두 Application이라 할 수 있다. 그림 9에 나타난 취약성들은 운영체제에서 기본으로 설치가 되는 Application에서 문제가 발견이 된 것이라 할 수 있다. 앞으로 더욱 많은 취약성들이 발견이 될 것이고 현재의 Vista™의 보호대책으로는 이전의 운영체제들이 그러 하였듯이 보안패치를 통해서 문제점들을 해결 할 수 있을 뿐이다.

3.2 Vista와 온라인게임

온라인 게임에서 발생하는 위협의 요소들을 설명을 하였고 Vista™에서 제공이 되는 보안기능과 나타나는 문제점들에 대해서 앞서 살펴 보았다. 사용자 입장에서 바라보는 관점과 서비스를 운영하는 입장에서는 보안상의 위협요소를 막는 다는 부분이 상반된 입장으로 제기되기도 한다. 현재 Vista™가 지니고 있는 보안적인 요소들이 특정 서비스산업에는 향후 치명적인 영향을 줄 수도 있다고 보며 그 서비스 산업의 처음은 온라인게임이 될 수도 있을 것이다.

사용자의 보안 강화를 위해 Vista™에는 보안기능이 추가 되었고 보안기능들은 광고를 하기 위한 spyware나 ActiveX를 이용한 악성코드들의 설치를 막을 것이다. 그리고 ActiveX를 부분적으로 이용하는 온라인게임들도 Vista™호환코드로의 전환이나 기능에서 시스템적인 접근 요소들을 다 제외하고 동작하도록 전환이 될 것이다. ActiveX에 대한 대응은 이 정도 수준에서 충분히 처리가 될 수 있다고 본다.

대부분의 온라인게임들은 비교적 빠르게 새로운 운영체제와의 호환성을 갖추려 할 것이다. 온라인 상에서 이루어 지는 웹보드 게임 및 RPG 계열의 게임들 모두 새로운 운영체제에 대한 호환성을 조기에 확보하려고 노력을 할 수 밖에 없다. 지금까지 새로운 운영체제의 출시 때마다 온라인 게임 업체들은 호환성을 확보하기 위해 많은 노력을 기울여 왔다. XP 상의 SP2 배포의 경우에도 ActiveX의 자동 실행이 안 되는 부분으로 인하여 많은 변경들이 있었고 노력을 한 적이 있다. 새로운 운영체제 위에서 실행이 안 되는 부분은 일정 기간을 투입하여 소스코드를 변경할 경우 충분히 실행을 시키도록 할 수 있다. 그러나 가장 중요한 보안적인 이슈 부분에 대한 고려가 빠져 있다. 악성코드에 대한 대응, Abusing에 대한 대응과 같은 측면에서는 다른 관점에서도 볼 수 있다.

Vista™의 강력한 보안기능을 활용할 경우 사용자의 정보 유출 시도를 하는 다양한 ActiveX유형의 악성코드로부터 벗어날 수 있음에도 불구하고 현재의 현실은 그리 쉽게 정의 내릴 수 있는 것은 아니다.

현재의 상황에서는 많은 위협들로부터 사용자를 보호하고 악성코드에 대한 대응을 하기 위해 다양한 종류의 ActiveX 혹은 시스템에 접근이 필요한 솔루션들을 사용할 수 밖에 없었다. 온라인 상에서 동의를 받은 사용자에게 설치를 하고 자동으로 업데이트를 진행하는 보안패치 서비스와 게임 전용 백신 서비스, Abusing 방지를 위한 게임보안 솔루션의 사용은 사용자 정보의 보호와 온라인 게임 서비스의 보호를 위해서는 필수요소중의 하나이다. 더 이상 충분조건이 아닌 필요조건으로서 보안 서비스가 존재하고 있다. Vista™에서 보장된 보안 기능은 매우 미흡한 기능으로서 온라인 게임 서비스의 문제들을 해결 할 수 없다. 그리고 개인정보보호의 관점에서 큰 효과를 기대 할 수 없다. 개인 사용자의 PC 상에서의 ActiveX의 실행제한과 시스템에 대한 접근 제한은 애드웨어와 ActiveX를 이용한 공격에 노출되는 것을 방지 하는 기능을 수행하나 전체 온라인 게임의 위협 요소들 중에서 애드웨어와 ActiveX를 이용한 공격이 차지하는 비율은 무시해도 좋을 정도로 낮은 비율이다.

향후 Vista™의 취약성은 계속 발견이 될 것이고 그 중에는 치명적인 취약성들도 반드시 발견이 될 것이다. 또한 운영체제에서 가동이 되는 Application에 대한 치명적인 취약성들도 계속 발견이 될 수 밖에 없다. 애드웨어와 ActiveX의 실행제한은 분명한 효과를 지니고 있으나 전체 위협요소에서 차지하는 비율은 낮으며 운영체제에 대해 직접적인 취약성을 공격하거나 Application에 대한 취약성 공격을 시도할 경우 UAC를 통한 권한제어는 깨어질 수 밖에 없다.

온라인 게임에 영향을 미치는 또 한 가지 요소로서는 Abusing과 관련된 문제이며 개인 사용자 PC 단위에서 사용자가 직접 Abusing을 시도할 경우 당연히 공격자 이므로 권한 승인창에서 High 권한을 주고 Abusing을 시도할 것이다. 온라인 게임에서는 지금까지 시스템에 대한 일정 수준의 제어를 하는 게임보안 솔루션으로 대응을 하였으나 게임 실행 시마다 매번 권한 승인 창이 활성화 된다면 접근성을 중요시 하는 게임으로서는 사용자의 이탈을 우려할 수 밖에 없으며 아마도 High 권한이 아닌 Medium 권한에 해당하는 기능만 수행을 하도록 할 것이다. 지금 온라인 게임에서 활성화 되고 있는 Abusing 유형들은 대부분 시스템에 대한 직접적인 조작을 통해 이루어 지고 있는 상황에서 Medium 권한으로 할 수 있는 Abusing 방지는 거의 없다고 볼 수 밖에 없다.

주요 기능	성능
Macro	80%
Speed Hack	90%
Debugging	80%
Packet Hack	90%
Memory Hack	50%
Client Packing	90%
Client Manipulation	95%

그림 10. 온라인 게임에서의 Abusing 대응

그림 10에서는 현재 게임보안툴을 활용하여 온라인 게임상에서 차단하는 Abusing 유형들에 대한 차단 비율을 보여주고 있다. 전체 7가지 영역에서 일정 수준 이상의 차단 성능을 발휘하는 것들도 있으나 공격 기술의 발전에 따라 계속 새로운 영역이 발견되고 새로운 공격 기법들이 발견 되는 영역들도 다수 있다. 지금 적용이 되고 있는 High 권한 수준의 Abusing 대응책에서도 그림 10 과 같은 부족한 면들이 나타나고 있는데 Medium 권한 수준으로 동작을 하였을 경우에는 전체 7가지의 Abusing 영역 대부분에서 차단 성능과 효율이 대폭 떨어 질 수 밖에 없다.

시스템에 대한 통제를 할 수 있는 권한이 부족하여 통제를 하고 Abusing에 대해 방지를 할 수가 없는 상황이다. 게임 실행 시마다 매번 승인창을 활성화 시키고 권한 상승을 승인한다 하여도 일회적인 성격이라 Vista™의 확산 정도에 따라 온라인 게임에 대한 사용자 이탈을 고민해야 할 것이고 Abusing에 대한 대응 방안 부재로 인해 온라인 게임 업체들은 피해를 감내 할 수 밖에 없는 상황이라 할 수 있다.

온라인 게임업체에서 사용자의 정보 보호를 위해 시행하고 있는 보안 강화 프로세스는 일반적인 사용자가 간과하기 쉬운 부분을 보강해 주는 측면의 서비스로서 제공이 되고 있다. 백신 서비스와 보안패치 서비스가 예가 된다. 보안패치 서비스는 ActiveX를 통해 활성화가 되고 웹을 통해 접근하는 온라인 사용자에게 설치가 되도록 하고 있다. 백신 서비스의 경우에도 마찬가지이다. 백신과 보안패치 서비스 모두 시스템에 대한 일정 수준 이상의 권한을 지니고 있어야 되는데 현재 Vista™의 보안모델 하에서는 일회적인 승인을 통해 지속적인 사용이 가능한 형태가 아니기 때문에 온라인 게임 서비스 업체에서는 보안 강화 프로세스의

시행에 상당한 부담을 느낄 수 밖에 없다. 사용자의 이탈과 보안서비스의 강화 측면에서 선택을 해야 하는 상황이 될 것이다.

4. 결론

지금까지 Vista™ 출시에 따른 효과와 현재 온라인 게임업체의 보안적인 위협요소와 현황에 대해서 정리를 한 결과를 보았다. 결론적으로 현재 사용자의 정보보호 측면에서의 Vista™의 보안적인 효과는 한정적이며 한계를 지닌 효과라고 할 수 있다. 반면에 온라인 게임업체가 노출되는 위협요소는 Vista™의 사용자 저변 확대에 따라 매우 심각하게 높아질 가능성이 있다.

효과적인 대책을 수립하지 않을 경우에는 향후 온라인 게임에 대한 Abusing 증가로 인해 심각한 피해를 입을 수 있으므로 단계적인 강화 조치와 운영체제 개발사에서의 특수성 인정이 필요하다. ActiveX의 활용 부분은 중요한 기술 이라는 측면 보다는 사용자의 웹 서비스 접근 환경에서 직접적인 효과를 실행 할 수 있는 접근 도구로서의 측면을 보아야만 한다. 사용자의 PC에 악의적인 소프트웨어를 설치하는 유형만 존재하는 것이 아니라 긍정적으로 활용되는 부분도 존재 하였으므로 다른 시각에서 바라보는 것도 필요하다. 운영체제 개발사의 적극적인 의지가 없이는 어려운 대책이 많은 관계로 향후에도 어려움은 지속되고 심화될 것으로 보인다.

운영체제의 구성환경의 극단적인 변화는 특정 온라인 서비스 산업의 흥망과도 직접적인 관련이 존재한다. 특히 권한제어 부분에 대한 것은 상당히 민감할 수 밖에 없는 사안이다. 온라인 게임에 대한 Abusing 대응이 운영체제 개발사에 있는 것도 아니며 일차적으로 온라인 게임사에 책임이 있는 상황에서 현재 Vista™에 적용된 보안모델은 일정 수준의 협의가 되지 않을 경우 문제가 될 수밖에 없으며 근 시일 내에 직접적인 영향을 미칠 것이다. ActiveX의 실행제한은 부수적인 문제이나 UAC를 통한 권한 승인 부분은 점진적으로 확대되는 문제라고 볼 수 있다.

온라인 게임 유저들을 정보유출로부터 보호하고 온라인 게임 서비스를 보호하기 위해서는 현재 활성화된 보호대책들을 선별하여 해당 보호 대책들이 적극적으로 활성화 될 수 있도록 협의 하는 것이 필요하며 적극적으로 노력 해야만 한다. 위협요소는 앞으로 새로운 운영체제가 대중화 될수록 심화될 것이다.

단기적으로는 악성코드 유형과 사용자 보호를 위한 유형을 구분 하는 방안 수립을 진행 하여야 하며 장기적으로는 특정 플랫폼에 편향된 방향을 극복하도록 노력하는 것이 중요한 과제라 할 수 있다.

온라인 게임에 대한 보안적인 측면에서만 보았을 때 현재 Vista™의 출시는 악재에 가깝다고 할 수 있다. 장기적으로 좋지 않은 영향을 확대 시키는 악재이지만 지금 이 순간 눈에 보이지 않을 뿐이다.

위험성 확대 이전에 적극적인 해결책을 모색하는 것이 필요한 시점이다.

참고문헌

- [1] 온라인 게임 해킹 대응 세미나 발표자료 - 2005.10 전 상훈
- [2] 온라인 게임 해킹 대응 세미나 발표자료 - 2006.10 전 상훈
- [3] 민관 전문가 세미나 발표 - 2006.10 전상훈
- [4] www.securityfocus.com/bip Microsoft Vista에 대한 취약성
- [5] www.microsoft.com/security Security Patch에 대한 Bulletin