How can I have 100 0-day for just 1-day
Version : Draft

Speak by R3d4l3rt

Outline

I. Introduction
   • Introduction of speaker

II. Project Overview
   • I just want to find a lot of vulnerability
   • Think it easier and Change one’s way of thinking
   • How can we found vulnerabilities
   • About ActiveX
   • APT Attacks via Active-X (Cases Study)

III. How can I found bug easily?
   • Introduction Automatic sample collections tool (Demo)
   • Introduction Auto Install sample tool (Demo)
   • Introductions Fuzzer
   • Introductions Exploit

IV. How can I have about one hundred vulnerability for just 1 days
   • Result of Tested
   • Examples (Active X Vulnerability)
Introduction

Who...

<table>
<thead>
<tr>
<th>Speaker</th>
<th>Introduction</th>
</tr>
</thead>
<tbody>
<tr>
<td>Louis Hur</td>
<td>Louis Hur is corporate president and Chief Executive Officer (CEO) of NSHC Corporation. He co-founded NSHC with four Hackers in 2003 while studying at the University, and was the first CEO until now. Mr. Louis brings more than 15 years of field-proven experience security and bug hunting businesses that help clients reduce their enterprise-wide IT security risk. Prior to starting NSHC, He is a frequent speaker on Internet security issues and has appeared as an expert on various media outlets, including HK TV and MBC, KBS.</td>
</tr>
<tr>
<td></td>
<td>Experience (2010 ~ 2013) - 2013 Vulnerability Analysis of NSHC’s R3d4l3rt Teams. (Discovered 0-day many times.) - 2011 CSO Conference Speaker</td>
</tr>
</tbody>
</table>

He is working the new vulnerability analysis and bug hunting, mobile security research in NSHC Red Alert Team. Also He is currently serving for Security Response Center at NSHC Company and responsible for malicious code analysis and anti-virus products. He is a frequent speaker on Internet security issues and has appeared as an expert on various media outlets, including MBC, KBS, JTBC.

Experience (2010 ~ 2013) - 2013 Vulnerability Analysis of NSHC’s R3d4l3rt Teams. (Discovered 0-day many times.) - 2012 CSO Conference Speaker in KOREA - 2011 Army Investigation Division served as an instructor |
Outline

I. Introduction
   • Introduction of speaker

II. Project Overview
   • I just want to find a lot of vulnerability
   • Think it easier and Change one's way of thinking
   • How can we found vulnerabilities
   • About ActiveX
   • APT Attacks via Active-X (Cases Study)

III. How can I found bug easily?
   • Introduction Automatic sample collections tool (Demo)
     Introduction Auto Install sample tool (Demo)
   • Introductions Fuzzer
   • Introductions Exploit

IV. How can I have about one hundred vulnerability for just 1 days
   • Result of Tested
   • Examples (Active X Vulnerability)

Project Overview

I just want to find a lot of vulnerability

• I just want to find a lot of vulnerability. But, It’s hard to find vulnerabilities.

• What is the Vulnerability?

Vulnerability is Weakness, Flaw From Hardware or software of computer

Weakness, Flaw
There are key to our Red Alert Project.

Again and Again Remember
This Key Word is

Weakness, Flaw
Project Overview

Think it easier and Change one's way of thinking

- In a short time, it's hard to find many vulnerabilities in just one application.
- But, if there are many target software ...
Project Overview

Think it easier and Change one’s way of thinking

- In a short time, it’s hard to find many vulnerabilities in just one application.
- If you can fuzz many applications? - The net of the sleeper catches fish

How can we find vulnerabilities

- One of Answers this question, It’s Fuzzing
  - Throw random bits at the program and see if it handles them
  - Popular robust testing mechanism for software
  - Fast and effective, easy to implement

- I think that there are best solution which can found many vulnerability in the short time.
Project Overview

How can we find vulnerabilities

- Almost all of the software is intended to find vulnerabilities.
  - File Format
  - Network Protocol
  - ActiveX
  - Browser
  - Etc

Why did we decide to fuzz Active-X?

- Each module’s size is Small
- Easy to collect ActiveX
- There are exist so many vulnerability
- The extend of damage is huge

About ActiveX

Microsoft technology introduced in 1996 and based on the Component Object Model (COM) and Object Linking and Embedding (OLE) technologies.

The intention of COM has been to create easily reusable pieces of code by creating objects that offer interfaces which can be called by other COM objects or programs.

But ActiveX controls, like any other browser plugin, provide a ripe attack surface for the malicious. Finding an exploitable flaw in a popular control gets MSRC attention at Microsoft, and similar attention at other large companies.
Project Overview

About Active X

ActiveX controls are typically native code (e.g. C++) compiled binaries registered with the Windows operating system. Through a registration process the ActiveX control is considered scriptable, meaning that Internet Explorer can load the control and HTML or JavaScript can interact with it. Because ActiveX controls run native code in the browser, they can serve as an extension to the browser. This can lead to numerous security threats not the least of which being that the control can bypass Internet Explorer’s most precious security defenses.

Security issues seems to be a constant problem with ActiveX controls. In fact, it seems most vulnerabilities in Windows nowadays are actually due to poorly written third-party controls which allow malicious websites to exploit buffer overflows or abuse command injection vulnerabilities. Quite often these controls make the impression of their authors not having realized their code can be instantiated from a remote website. The following chapters will describe methods to find, analyze, and exploit bugs in ActiveX controls will be presented to the reader.

Project Overview

APT Attacks via Active X(3.20 Cyber Terror from Active-X)

2013.03.20 large-scale cyber attacks occurred in the Republic of Korea. Target for the financial institutions and the media, they suffered a lot of damage. North Korea has a cyber terrorist attacks and ActiveX vulnerability was used. Attack is prepared a long period of time and we think that attacks of similar form will continue to occur.
How can I found bug easily?

- Introduction Automatic sample collections tool (Demo)
- Introduction Auto Install sample tool (Demo)
- Introductions Fuzzer
- Introductions Exploit

How can I have about one hundred vulnerability for just 1 days

- Result of Tested
- Examples (Active X Vulnerability)
How can I found bug easily?

**Introduction Automatic sample collections tool**

**STEP 1-1**:  
For collect the active-x applications, Our tools gets on the internet and search the site that include active-x application. at this moment, Our Search Engine uses to many kind of IP Address to evasion auto detect search engine.

**STEP 1-2**:  
Setup for Automatic Install  
Automatic installation  
Fuzzing Test  
Normal Program  
No  
Exploitable ?  
YES  
Make a Exploit Code

**Proxy Grabber**  
For collect proxy ip address list, We can use ‘Proxy Grabber’. This program can help you scan any range of addresses on present Proxy list. This tool made by Hidemyass and this is python script language. ‘Proxy Grabber’ is also open source, so everyone can use that. We can collect many ip address via Proxy Grabber

**Proxy IP Address list**

---

**HITCON 2013**

Page 16

---

**HITCON 2013**

Page 17
How can I found bug easily?

Introduction Automatic sample collections tool

STEP 1-2:
In this step, We can gather information of active-x. for example download link and CLSID, application name in HTML Source Code, So target applications are chose at random through Web search Engine.

ActiveX_Parser.py

‘ActiveX_Parser.py’ is the python script for gathering the active-x information via web search engine. This script used to many ip address from step 1-1

As a result, we can have 3 kinds of file first is download information, And 2nd files is CLSID Info. Last is Install Script for fuzzing.
How can I found bug easily?

Introduction Auto Install sample tool

STEP 2-1 :
By Step 1-2, we're able to make individual install script from united script.

ActiveX_List_Div.py

'ActiveX_List_Div.py' are able to separate the install script from united script via step 1-2. It makes individual install script for quick and easy.
How can I found bug easily?

Introduction Auto Install sample tool

STEP 2-2 :
Before you perform a auto installation, Change a few options Internet Browser.

ActiveX_Option_Setting.bat
ActiveX_Option_Setting.bat is a batch file. This file’s change the internet explorer options for easily installd. It include that allow active-x execute without warring, allow the any certification for using active x, allow the download active-x without signing.

How can I found bug easily?

Introduction Auto Install sample tool

STEP 2-3 :
In this case, Our batch file’s run individual script for install.

AxInstallRun.bat
AxInstallRun.bat is batch file. It runs individual script files for automatic install.
How can I found bug easily?

Introduction Auto Install sample tool

DEM0

How can I found bug easily?

- Proxy IP Address Gathering
- Active X install Information Gathering and Install Script Generation
- Separation of Install Script for easily
- Setup for Automatic Install
- automatic installation
  - STEP 3-1
  - Fuzzing Test
  - Exploitable ?
    - No
    - YES
      - Make a Exploit Code

HITCON 2013
STEP 3-1:
It’s test the target application by fuzzing. So all of installed applications tested by Our fuzzer. Result of Fuzzing, we can know that how many crash occurred during fuzzing.

How can I found bug easily?

Introduction Fuzzer

AxFuzzer.py

‘Red_Alert_AxFuzzer.py’ is our active-x fuzzing tool. It refer the dranzer what is open source project. Dranzer is active-x vulnerability discovery tool. It developed by CERT in USA.

DEMO
How can I found bug easily?

Introduction Exploit

**STEP 4-1**: Selection crashed Active-X Information for Exploit in the result of fuzzing.

Exploitable PoC

This PoC information inform that EIP Register address is overwrite “41414141”. So It can change the exploit very easy and there is no need to spend a time for weaponizing.
How can I found bug easily?

Introduction Exploit

STEP 4-1:
To Seek what is the vulnerable Value in the PoC Data’s values.

How can I found bug easily?

look for value for crash

To Seek what is the vulnerable Value in the PoC Data’s values.

Outline

I. Introduction
   - Introduction of speaker

II. Project Overview
   - I just want to find a lot of vulnerability
   - Think it easier and Change one’s way of thinking
   - How can we found vulnerabilities
   - About ActiveX
   - APT Attacks via Active-X (Cases Study)

III. How can I found bug easily?
   - Introduction Automatic sample collections tool (Demo)
   - Introduction Auto Install sample tool (Demo)
   - Introductions Fuzzer
   - Introductions Exploit

IV. How can I have about one hundred vulnerability for just 1 days
   - Result of Tested
   - Examples (Active X Vulnerability)
How many Zero-Day vulnerability to find a day?

Result of Tested (just tested simply BoF Vulnerability)

<table>
<thead>
<tr>
<th>Vulnerability Type</th>
<th>Result of Tested</th>
</tr>
</thead>
<tbody>
<tr>
<td>Crash</td>
<td>10959</td>
</tr>
<tr>
<td>Normal</td>
<td>1041</td>
</tr>
<tr>
<td>Crash And DoS</td>
<td>950</td>
</tr>
<tr>
<td>Memory corruption</td>
<td>91</td>
</tr>
</tbody>
</table>

How many active-X vulnerability use to APT Attack?

- Vulnerability possible attack now of Discovered ActiveX vulnerability confirmed 24 count. North Korea has often used ActiveX when carry out a large-scale cyber attacks. We estimate that North Korea finished the pre-survey and ready to use cyber terrorism.

How many Zero-Day vulnerability to find a day?

Examples (Active X Vulnerability)

1. Malicious Web page access
2. ActiveX Install
3. Important info send to attacker

Gaining control of the EIP register. It will be easier and faster to handle.
Thanks you for Listening