

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)

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...

Speaker	Introduction
	<p>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.</p> <p>•Experience (2010 ~ 2013)</p> <ul style="list-style-type: none">- 2013 Vulnerability Analysis of NSHC's R3d4i3rt Teams. (Discovered 0-day many times.)- 2011 Black-Hat Abu Dhabi Speaker- 2010 CSO Conference Speaker
	<p>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.</p> <p>He is a frequent speaker on Internet security issues and has appeared as an expert on various media outlets, including MBC, KBS, JTBC.</p> <p>•Experience (2010 ~ 2013)</p> <ul style="list-style-type: none">- 2013 Vulnerability Analysis of NSHC's R3d4i3rt 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 applications.



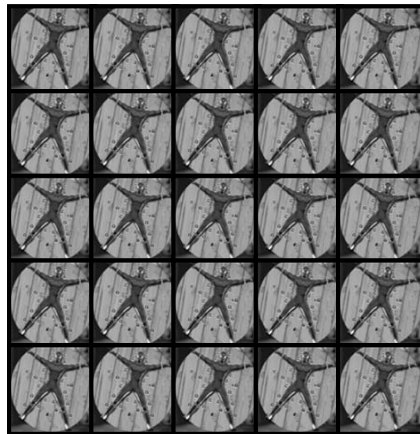
HITCON 2013

6

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 applications.
- But, If there are many target software ...



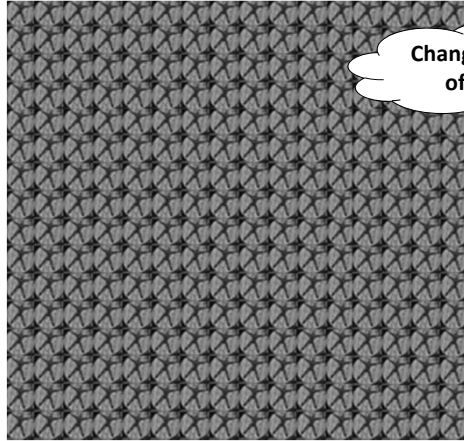
HITCON 2013

7

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 applications.
- If you can fuzz many applications? - The net of the sleeper catches fish



Change one's way
of thinking



HITCON 2013

8

Project Overview

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.**



HITCON 2013

9

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?

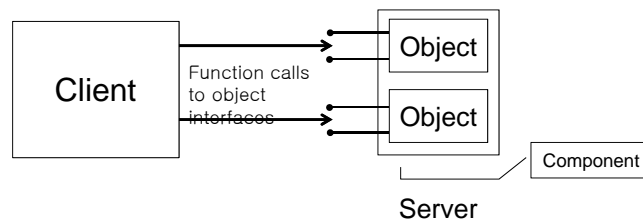


- ✓ Each module's size is Small
- ✓ Easy to collect ActiveX
- ✓ There are exist so many vulnerability
- ✓ The extend of damage is huge

Project Overview

About Active X

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.



On March 20th an attack that brought down three major media broadcasters and at least two financial institutions computer systems in South Korea was launched. The Red Alert team which is part of NSHC Security has provided access to their ongoing reports of the malware attack (PDF - Korean).

The attack was first detected on March 20, 2013 around 2:20PM (UTC+9) South Korean broadcasters KBS, MBC and YTN as well as three banks. (제주은행) Jeju, (농협은행) Nonghyup (Bank and Insurance) and (신한은행) Shinhan all reported having their computer networks knocked offline after PCs were infected by data-deleting malware believed to have spread from update/patch servers on the network.

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)

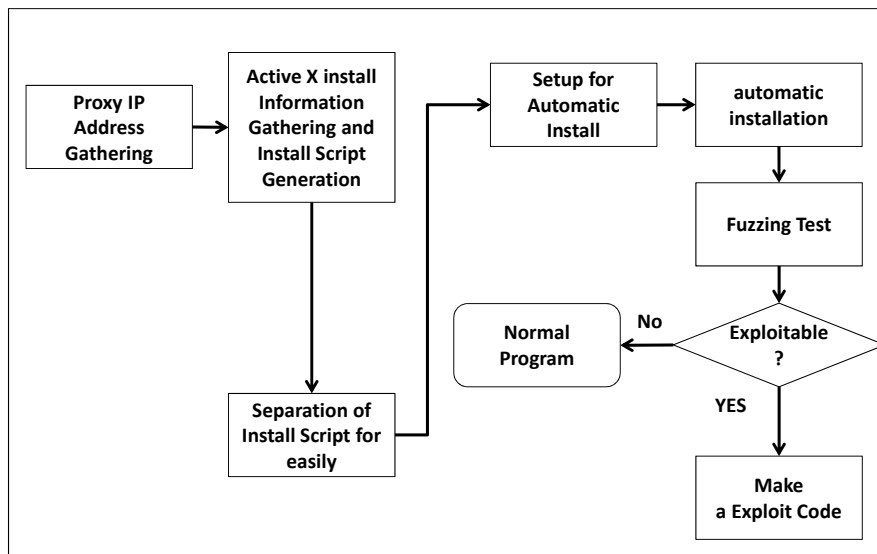
III. How can I found bug easily?

- 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 can I found bug easily?



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.

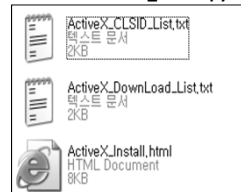
```
python active_x_tool.py
-----
windowactivex.com?activex
-----
-----
##### Proxy IP Count : 97 #####
[*] Proxy IP 0 : 202.121.96.34:8086
[*] Parsing 9800 : ['https://illcentre.vodafone.co.uk/par/content/4diprinter
inn.cab', '(76392179-6008-462d-8961-b95c140a00f0)']
[*] Parsing 9801 : ['https://www.select2perform.com.au/cabs/QOLCheck.ocx', '(c
33e1d4d-9f1c-9f54-8180-4e2841e27f92)']
[*] Parsing 9802 : ['http://img.koransame.co.kr/cj/gugun/CJ50Lib.cab', '(E11
E50F-51D9-40C3-8414-18D01FE8B4D0)']
[*] Parsing 9803 : ['https://www.webhm.jp/activex/webhmicntrl.cab', '(4620
b48-EE00-4858-47E7-D97640C5E086)']
[*] Parsing 9804 : ['http://91.231.4.134:8098/program/SonyNetworkGeneralInser
.cab', '(64E9F9E7-9215-440F-8094-46C608492320)']
[*] Parsing 9805 : ['http://gita.ajnews.ca/hr/Msa/cab/MSJleuer.cab', '(07BE31
8B-C542-4051-8286-2E1E22706263)']
[*] Parsing 9806 : ['https://desk.ajnews.ca/hr/MT6/QRB/01tpjtrans.cab', '(CFB1
85F2-387F-4B05-8267-08F2E1805724)']
[*] Parsing 9807 : ['http://desk.ajnews.ca/hr/MT6/QRB/qjexecuter.cab', '(7523
86-6402-4887-8088-2E370A123521)']
[*] Parsing 9808 : ['http://desk.ajnews.ca/hr/MT6/QRB/9JFtpjload.cab', '(22
701D-868F-DC7-8572-9858E2391282)']
[*] Parsing 9809 : ['https://msnui.edu-l.org/MSnuiEditor.cab', '(F1955CF2-D1
54-411F-8276-F246E8004258)']
[*] Parsing 9810 : ['http://msnui.edu-l.org/MSnuiReader.cab', '(1302D048-0
8-4029-929F-295232301022)']
[*] Parsing 9811 : ['http://msnui.edu-l.org/MSnuiWriter.cab', '(06E3F0164-0
8-4029-929F-295232301022)']
[*] Parsing 9812 : ['http://setup.ohdcom.co.kr/files/application/ohdcom/ohdcom
Control6.CAB', '(979781C1-96A7-4028-894E-7018479230F7)']
```

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 Installing Script for install.

Result of ActiveX_Parser.py ↓

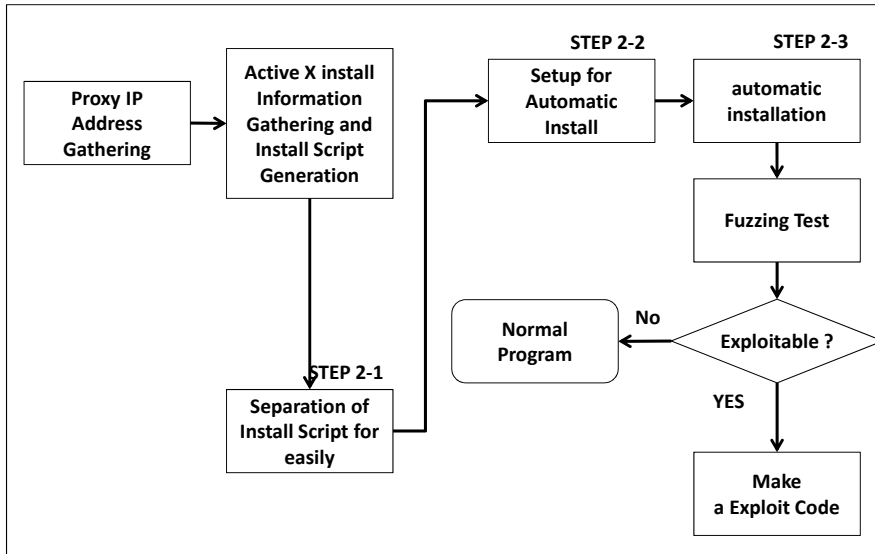


How can I found bug easily?

Introduction Automatic sample collections tool

DEMO

How can I found bug easily?



HITCON 2013

20

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.

```

C:\ActiveX>03.ActiveX_List_Div.py
Change Dir : C:\ActiveX_7000_10000
0.html
1.html
2.html
3.html
4.html
5.html
6.html
7.html
8.html
9.html
10.html
11.html
12.html
13.html
14.html
15.html
16.html
17.html
18.html
19.html
20.html
21.html
22.html
  
```

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.

HITCON 2013

21

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.

```

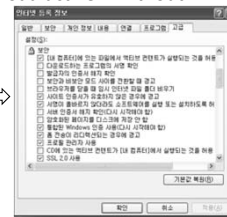
#####
# Internet Explorer 6
# ActiveX option Down for Automatic Installation.
# Internet security level of Security tab
# Secure area of advanced tab
# - secure and performance improvement option check
#####
Press any key to continue . . .

The operation completed successfully
The operation completed successfully
The operation completed successfully
The operation completed successfully
The operation completed successfully
The operation completed successfully
The operation completed successfully
The operation completed successfully
The operation completed successfully
The operation completed successfully
The operation completed successfully
Press any key to continue . . . _
    
```

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.

Change of explorer options →



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.

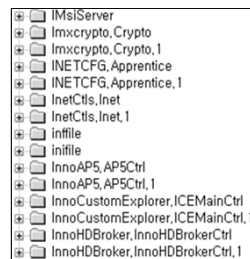
```

C:\WINDOWS\system32\cmd.exe
SUCCESS: The process with PID 1016 has been terminated.
6.html
SUCCESS: The process with PID 720 has been terminated.
7.html
SUCCESS: The process with PID 768 has been terminated.
8.html
SUCCESS: The process with PID 1816 has been terminated.
9.html
SUCCESS: The process with PID 2000 has been terminated.
10.html
SUCCESS: The process with PID 1984 has been terminated.
11.html
SUCCESS: The process with PID 228 has been terminated.
12.html
SUCCESS: The process with PID 1296 has been terminated.
13.html
SUCCESS: The process with PID 1424 has been terminated.
14.html
SUCCESS: The process with PID 1016 has been terminated.
15.html
SUCCESS: The process with PID 892 has been terminated.
16.html
    
```

AxInstallRun.bat

'AxInstallRun.bat' is batch file. It runs individual script files for automatic install.

Installed active-x list →



How can I found bug easily?

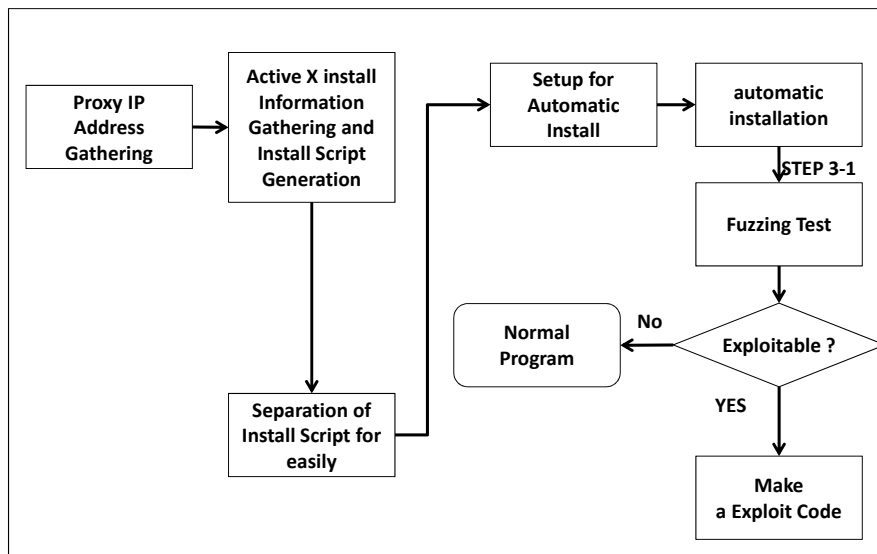
Introduction Auto Install sample tool

DEMO

HITCON 2013

24

How can I found bug easily?



HITCON 2013

25

How can I found bug easily?

Introduction Fuzzer

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.

```
:\Program Files\Red_Alert_AxFuzzer\Red_Alert_AxFuzzer\Release>Red_Alert_AxFuzzer
.exe -d baseline.txt -p -o p.txt
Loaded DLL
Display Hooked
Testing COM Object PARAMS in IE (Property Bag) - (00000010-0000-0010-8000-00000000
5D2E84) DAO.DBEngine.35
Testing COM Object PARAMS in IE (Property Bag) - (00000011-0000-0010-8000-00000000
5D2E84) DAO.PrivateDBEngine.35
Testing COM Object PARAMS in IE (Property Bag) - (00000013-0000-0010-8000-00000000
5D2E84) DAO.TableDef.35
Testing COM Object PARAMS in IE (Property Bag) - (00000014-0000-0010-8000-00000000
5D2E84) DAO.Fields.35
Testing COM Object PARAMS in IE (Property Bag) - (00000015-0000-0010-8000-00000000
5D2E84) DAO.Index.35
Testing COM Object PARAMS in IE (Property Bag) - (00000016-0000-0010-8000-00000000
5D2E84) DAO.Group.35
Testing COM Object PARAMS in IE (Property Bag) - (00000017-0000-0010-8000-00000000
5D2E84) DAO.User.35
Testing COM Object PARAMS in IE (Property Bag) - (00000018-0000-0010-8000-00000000
5D2E84) DAO.QueryDef.35
Testing COM Object PARAMS in IE (Property Bag) - (00000019-0000-0010-8000-00000000
5D2E84) DAO.Relation.35
Testing COM Object PARAMS in IE (Property Bag) - (0000002F-0000-8000-C000-00000000
000046) CLSID_RecordInfo
```

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.



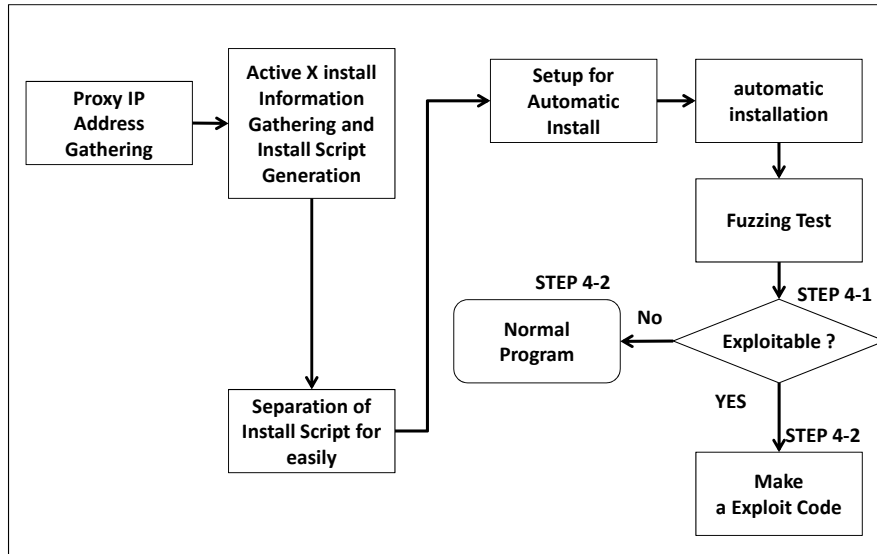
Collected POC List →

How can I found bug easily?

Introduction Fuzzer

DEMO

How can I found bug easily?



How can I found bug easily?

Introduction Exploit

STEP 4-1 :

Selection crashed Active-X Information for Exploit in the result of fuzzing.

```

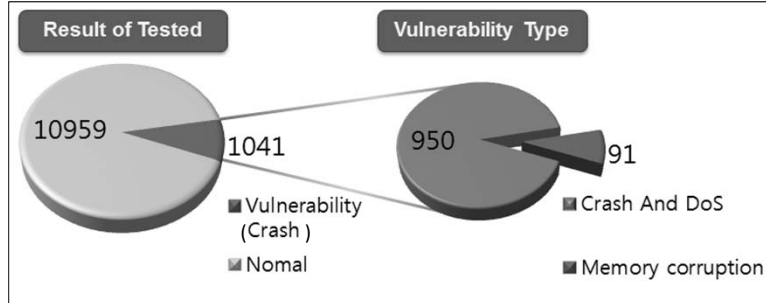
.....
{.....} AttachList Class
ERROR - Internet Explorer Crashed (0x7fffffff)
.....
Testing COM Object PARAMS (Property Bag) in IE - {.....} AttachList Class
.....
COM Object Filename : .....
Major Version : .....
Minor Version : .....
Build Number : .....
Revision Number : .....
Product Version : .....
Product Name : .....
Company Name : .....
Legal Copyright : ..... All rights reserved.
Comments : .....
File Description : .....
File Version : .....
Internal Name : .....
Legal Trademarks : .....
Private Build : .....
Special Build : .....
Language : ..... not found
.....
*** IE Exception ***
***** EXCEPTION ACCESS VIOLATION(0xc0000005) - instruction address: 0x41414141, invalid read from 0x41414141 *****
.....
    
```

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 many Zero-Day vulnerability to find a day?

Result of Tested (just tested simply BoF Vulnerability)



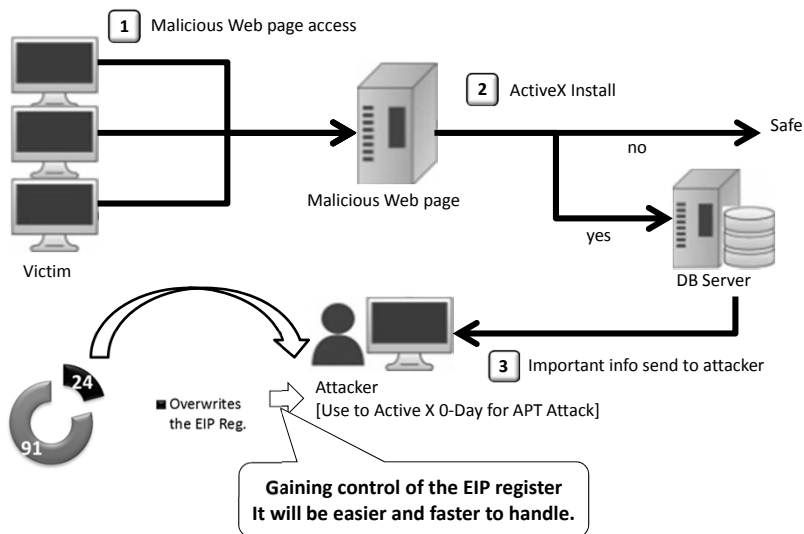
How many active-X vulnerability use to ATP Attack?



- 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)





**Thanks you
for Listening**