Exploit Kits
A Weapon Of Mass Infection

Omri Herscovici
Meet “Paunch”
Exploit Kit
Motivation

1. Malware
2. Traffic
3. Infect traffic with malware
Malware

Your personal files are encrypted!

Your files have been safely encrypted on this PC: photos, videos, documents, etc. Click "Show encrypted files" Button to view a complete list of encrypted files, and you can personally verify this.

All your important files are encrypted.

At the moment, the cost of private key for decrypting your files is 1.5 BTC ~ 415 USD. Your Bitcoin address for payment: 1JVR7hJ2wmdVrogHcd6fYWMiElRynMkWF2

Follow the instruction on the web-site. We remind you that the sooner you do so, the more chances are left to recover the files.

Any attempt to remove or corrupt this software will result in immediate elimination of the private key by the server.

Click for Free Decryption on site

Show files
Traffic

- Emails
  - Compromised Website
  - Malvertisement
Large Malvertising Campaign Takes on Yahoo!

AUGUST 3, 2015 | BY JÉRÔME SEGURA
Exploit Kit-as-a-Service

- Automated Toolkits
- Scan Victim’s Web Browser
- Find Vulnerabilities
- Exploit
- Deliver Payload
Infection Process

Victim visits a hacked website
Redirect to Exploit Kit

Comromised Website

Start process of infection
Exploit Kit-as-a-Service

RIG exploit kit Official HF Sales thread $30 Day | $100 Week | $500 Month
02-03-2015, 09:03 AM

Are pleased to introduce you to RIG exploits v2.0

I see people are trying to sell fake and scamming people off these ek etc. So we have decided to officially post here so everyone knows where to obtain us.

-Work On all WinOS 32 / 64bi
-Bypass UAC on exploits
-Fast cleaning + cleaning on request
-Keep Large volumes of traffic, no traffic limits
-We provide always clean and trust domains with automatic check on the blacklist
-We use CVE-2013-7331 for detect and stop AV or virtual machines.
-API with automatic delivery

Each account has a 2 stream and can ship 2 different exe

Current exploits:

- **Java**: CVE-2012-0507
- **Java**: CVE-2013-2465
- **IE7-8-9**: CVE-2013-2551
- **IE10**: CVE-2013-0322
- **Flash**: CVE-2014-0497
- **Flash**: CVE-2015-0311
- **Silverlight**: CVE-2013-0074

An average rate of 10-20%

Cost:
- 1 day - 30 usd
- Week - 100 usd
- month - 500 usd

Jabber:

We Accept English Speaking Users, You can Pay Only bitcoin
Exploit Kit

- Automates the exploitation of client-side vulnerabilities.
- Who is the Client – The cyber criminal.
- Who is the Target – Users of the internet.
Angler exploit kit rings in 2016 with CryptoWall ransomware
Exploit Kits In The Wild

MOST WANTED

Null Hole    "Hanjuan EK"
"SedKit"    "SPL2 Pack"    "Archie EK"
"Astrum EK"    "Angler Exploit Kit"
Niteris Exploit Kit    LightsOut Exploit Kit
"Zuponic"    Neutrino waves    Sweet Orange
Nuclear Pack v3.0    "FlashPack"

DEAD OR ALIVE
What Makes a Good Exploit Kit?

- Prevalence of vulnerabilities exploited by the EK
- Exploit stability and updates
- Evasion from researchers
- Evasion from IPS and IDS, Anti-Virus products
- Client support (statistics and technical support)

- Eventually all these effect the infection rate of the EK and it’s life cycle
Infection Process – Quick Overview

Redirected to the exploit kit server

Landing Page

Exploit

Asks for the flash file (exploit)

Malware

Asks for the malware (payload)
01
LANDING PAGE
Infection Process – Landing Page

Evasion
- Serve once for given IP
- Check for ‘referrer’ header

redirected to exploit kit’s server

Serves the landing page

Code that infects the machine;)

```html
<html>
<head>
</head>
<body>

Code that infects the machine ;)

</body>
</html>
```
De-Obfuscation Example
More **Landing Page Protections**

- Evasion from web emulators
- Evasion from AV products by enumerating drivers
- Evasion from Chrome
- Network encryption scheme
02

EXPLOIT
Exploit

• “A piece of software, a chunk of data, or a sequence of commands that takes advantage of a bug, glitch or vulnerability.” (Wikipedia)

• What types of exploits are included in exploit kits?
Exploits Distribution – 2013-2016

Exploits used by exploit kits per technology 2016:

- Flash: 100%
- Java: 0%
- IE: 0%
- Silverlight: 0%

Exploits used by exploit kits per technology 2015:

- Flash: 100%
- Java: 0%
- IE: 0%
- Silverlight: 0%

Exploits used by exploit kits per technology 2014:

- Flash: 2, 14%
- Java: 1, 9%
- IE: 0, 0%
- Silverlight: 0, 0%

Exploits used by exploit kits per technology 2013:

- Flash: 2, 22%
- Java: 4, 29%
- IE: 0, 0%
- Silverlight: 0, 0%
Where do you get exploits?

<table>
<thead>
<tr>
<th>Software</th>
<th>Price Range</th>
</tr>
</thead>
<tbody>
<tr>
<td>Adobe Reader</td>
<td>$5,000-$30,000</td>
</tr>
<tr>
<td>Mac OS X</td>
<td>$20,000-$50,000</td>
</tr>
<tr>
<td>Android</td>
<td>$30,000-$60,000</td>
</tr>
<tr>
<td>Flash or Java Browser Plug-Ins</td>
<td>$40,000-$100,000</td>
</tr>
<tr>
<td>Microsoft Word</td>
<td>$50,000-$100,000</td>
</tr>
<tr>
<td>Windows</td>
<td>$60,000-$120,000</td>
</tr>
<tr>
<td>Firefox or Safari</td>
<td>$60,000-$150,000</td>
</tr>
<tr>
<td>Chrome or Internet Explorer</td>
<td>$80,000-$200,000</td>
</tr>
<tr>
<td>iOS</td>
<td>$100,000-$250,000</td>
</tr>
</tbody>
</table>

Since Java introduced support for plug-ins via feedback from users in Flash, exploit kits for different versions of the same component can be bought for different prices.
Old Vulnerabilities

WHAT DO WE SAY TO THE JAVA UPDATE?

NOT TODAY.
Exploit Obfuscation

- Researcher challenge is to identify the vulnerability
Exploit Delivery

- Landing page with obfuscated code
- Need to maximize hit rate – use multiple exploits

**SeCios Method - Infinity**

<table>
<thead>
<tr>
<th>#</th>
<th>Host</th>
<th>Method</th>
<th>URL</th>
<th>Params</th>
<th>Edited</th>
<th>Status</th>
<th>Length</th>
<th>MIME type</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td><a href="http://tooped.lucloids.com:8000">http://tooped.lucloids.com:8000</a></td>
<td>GET</td>
<td>/sxwcbbguyeypfbko.js</td>
<td>✔️</td>
<td></td>
<td>200</td>
<td>92846</td>
<td>script</td>
</tr>
<tr>
<td>3</td>
<td><a href="http://tooped.lucloids.com:8000">http://tooped.lucloids.com:8000</a></td>
<td>GET</td>
<td>/etmnhjksd</td>
<td></td>
<td></td>
<td>200</td>
<td>104843</td>
<td>text</td>
</tr>
<tr>
<td>4</td>
<td><a href="http://tooped.lucloids.com:8000">http://tooped.lucloids.com:8000</a></td>
<td>POST</td>
<td>/dpqvangwii</td>
<td>✔️</td>
<td>✔️</td>
<td>200</td>
<td>883</td>
<td>text</td>
</tr>
<tr>
<td>5</td>
<td><a href="http://tooped.lucloids.com:8000">http://tooped.lucloids.com:8000</a></td>
<td>GET</td>
<td>/lnfqsao?ilbbbxml=eaveqxd</td>
<td>✔️</td>
<td>✔️</td>
<td>200</td>
<td>19482</td>
<td>text</td>
</tr>
<tr>
<td>6</td>
<td><a href="http://tooped.lucloids.com:8000">http://tooped.lucloids.com:8000</a></td>
<td>GET</td>
<td>/META-INF/services/java.xml.datatype...</td>
<td></td>
<td></td>
<td>404</td>
<td>741</td>
<td>HTML</td>
</tr>
<tr>
<td>7</td>
<td><a href="http://tooped.lucloids.com:8000">http://tooped.lucloids.com:8000</a></td>
<td>GET</td>
<td>/lyzeisxynchw?isabx=eaveqxd</td>
<td>✔️</td>
<td>✔️</td>
<td>200</td>
<td>8409</td>
<td>text</td>
</tr>
</tbody>
</table>

**Detection Phase - Constant**

1. Landing page
2. Minified jQuery 1.9.1
3. Plugin Detector
4. Exploit request

**Exploitation Phase – Changeable; depends on the exploit decided**
03

MALWARE
Malware

- Malware is encrypted
- Neutrino – simple xor for each download
- Infinity – one time (per campaign) RC4 encrypted
4. 22.11.2013: Increased infection rates by 30% due to the cardinal change in the way we serve the payloads, hurry up and send your traffic!

5. 10.10.2013: We are no longer accepting traffic from the following countries (Former USSR countries, small countries from Asia, the Middle East, Africa and South America):
A1 A2 O1 SU RU UA BY UZ KZ GE AZ LT MD LV KG TJ AM TM JP JA CN TH VN ID MY TZ PH RO SG TT YE LK PK SA BG UY RS OM IQ KW DO SV TN KE EU NP BD MN SK CR JO LU BB MU NI AP BS MQ NG CY BO AO PY MK GU BH SI NA LB BA BN GD LA BZ PG ZM SY LY SD HT MO PS UG GF RE AF SN LR NC KH GP BW HN AW PF CW VI IS KN AG BM GY DM MT BT MZ EE GL CI MG MV MC GA CD LI GQ ZW CM SR JE DJ CV SZ ME FJ LC KY GH SB VU ET RW MW ER LS EG AE TW ZA
Latest Intelligence for April 2016

Our latest intelligence reveals that the Nuclear exploit kit comprised 42 percent of all web attacks, and 71 percent of all social scams spread through manual sharing.
Statistics

- 15 Active Control Panels
- $100,000 Monthly Revenue for the developer
- 5 Exploits
- 72.6% Ransomware
- 27.4% Banking Trojan
- 1,846,678 Attacked Machines
- 184,568 Success (9.95%)