INTRODUCTION:

EXPLOIT KITS
EXPLOIT KITS

Software exploits take advantage of unpatched flaws or misconfigurations in operating systems, applications and supporting libraries or frameworks. These exploits can allow an attacker to install malicious software on a vulnerable device. Exploit kits are software packages commonly sold in hacking forums and IRC channels. They include software exploits for known vulnerabilities across a range of end-user technologies (Internet Explorer, Adobe Flash, etc.). Exploit kits enable their users (in this section, when we use the term attackers, we are discussing Exploit Kit users) to execute large-scale attacks against vulnerable systems without the user needing to develop their own exploits. However, exploit kits don’t enable attack capabilities for completely inexperienced criminals who have decided to become hackers. Successful execution of a large-scale attack campaign requires considerable knowledge and skill, and an exploit kit is only one component of a successful attack.

This chapter provides an overview of the exploit kit development process, as well as the role which exploit kits play in large-scale attacks. These discussions will help the reader understand the lifecycle of exploit kits and the role they play as a component of large-scale attacks. Appropriate use of an exploit kit requires skill; exploit kits help automate and manage one component of the attack process. The development of exploit kits requires an entirely different set of skills, but is key to the success and longevity of the exploit kit. The proliferation of exploit kits is a result of the increased commoditization and specialization of the cybercrime economy.

This chapter also provides an analysis of exploit kit trends observed by NTT Group in 2014. Increased competition between available exploit kits is driving these developers to use newer exploits in their kits. For example, as one key evolution in exploit kits during 2014, NTT Group observed an increase in the use of Adobe Flash exploits.

Read more at the Global Threat Intelligence Report Online at: https://nttgroupsecurity.com/
EXPLOIT KITS:

DEVELOPMENT AND OPERATION LIFECYCLES
DEVELOPMENT AND OPERATION LIFECYCLES

This section provides a walkthrough of the lifecycle of an exploit kit (EK), from both a developer and attacker perspective.

The following diagram presents two exploit kit processes. The first presents the process for development and maintenance of exploit kits. The second presents the process for use of an exploit kit by an attacker.
Exploit Kit Development

Build exploit delivery infrastructure and web application → Exploit selection and implementation → Exploit kit is offered for sale via IRC/Forums

Exploit Kit Maintenance

Exploits are modified and tested to evade detection → Ineffective exploits are identified and removed → New exploits acquired

Exploit Kit End of Life

Lack of maintenance, merger, law enforcement lead to end of life

Exploit Kit User (Attacker) Process

Command Infrastructure
Infrastructure for payload control and communication

Payload Identification
(ransomware, spambot, banking trojan)

Victim Targeting Technique
(phishing, drive-by downloads)

Exploit Kit Acquisition
Attacker purchase kit receives and custom URL for exploitation

Campaign Execution

Campaign Conclusion
When purchased time expires, access to EK is revoked

Caption: Exploit kit development and operational lifecycles rely on each other.
EXPLOIT KIT DEVELOPER PROCESS

Exploit Kit Development

Building exploit delivery infrastructure and web application

Exploit kits are Software as a Service (SaaS) for attackers, and the development cycle for exploit kits resembles the software development lifecycle used by legitimate organizations. The first steps in exploit kit development are the creation of the exploit delivery infrastructure, along with administrative and attacker interfaces. Exploit kits typically include the following components:

- **Attacker access console (Exploit Kit Panel)** – Attackers who use Exploit kits access the console via secure login to the exploit kit control panel. This console typically allows the attacker to monitor the status of exploit attempts and identify the number of compromised devices, as well as measure rates of exploitation success against different technology profiles, as shown in the following screenshot of the Fiesta exploit kit².

² From http://blog.0x3a.com/post/62375513265/fiesta-exploit-kit-analysis-serving-msie-exploit
### Global Threat Intelligence Report 2015

#### Copyright 2015 NTT Innovation Institute 1 LLC

<table>
<thead>
<tr>
<th>Country</th>
<th>ALL</th>
<th>LOAD</th>
<th>PER</th>
<th>HOUR</th>
<th>DAY</th>
</tr>
</thead>
<tbody>
<tr>
<td>GB</td>
<td>1488</td>
<td>52</td>
<td>3.42</td>
<td>0</td>
<td>1488</td>
</tr>
<tr>
<td>OT</td>
<td>37</td>
<td>2</td>
<td>5.40</td>
<td>0</td>
<td>37</td>
</tr>
<tr>
<td>US</td>
<td>10</td>
<td>2</td>
<td>20.0</td>
<td>0</td>
<td>10</td>
</tr>
<tr>
<td>JP</td>
<td>2</td>
<td>0</td>
<td>0.00</td>
<td>0</td>
<td>2</td>
</tr>
<tr>
<td>CN</td>
<td>2</td>
<td>0</td>
<td>0.00</td>
<td>0</td>
<td>2</td>
</tr>
<tr>
<td>IL</td>
<td>1</td>
<td>0</td>
<td>0.00</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>FR</td>
<td>1</td>
<td>0</td>
<td>0.00</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>CH</td>
<td>1</td>
<td>0</td>
<td>0.00</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>NL</td>
<td>1</td>
<td>0</td>
<td>0.00</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>DE</td>
<td>1</td>
<td>0</td>
<td>0.00</td>
<td>0</td>
<td>1</td>
</tr>
</tbody>
</table>

*`s other country

<table>
<thead>
<tr>
<th>Platform</th>
<th>ALL</th>
<th>LOAD</th>
<th>PER</th>
<th>HOUR</th>
<th>DAY</th>
</tr>
</thead>
<tbody>
<tr>
<td>VISTA</td>
<td>626</td>
<td>3</td>
<td>0.47</td>
<td>0</td>
<td>626</td>
</tr>
<tr>
<td>SP1</td>
<td>611</td>
<td>31</td>
<td>5.07</td>
<td>1</td>
<td>611</td>
</tr>
<tr>
<td>SP2</td>
<td>233</td>
<td>19</td>
<td>8.15</td>
<td>0</td>
<td>233</td>
</tr>
<tr>
<td>OTHER</td>
<td>69</td>
<td>1</td>
<td>1.44</td>
<td>0</td>
<td>69</td>
</tr>
<tr>
<td>2K</td>
<td>5</td>
<td>1</td>
<td>20.0</td>
<td>0</td>
<td>5</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Platform</th>
<th>ALL</th>
<th>LOAD</th>
<th>PER</th>
<th>HOUR</th>
<th>DAY</th>
</tr>
</thead>
<tbody>
<tr>
<td>MSIE</td>
<td>1093</td>
<td>55</td>
<td>5.03</td>
<td>0</td>
<td>1093</td>
</tr>
<tr>
<td>FFOX</td>
<td>322</td>
<td>0</td>
<td>0.00</td>
<td>1</td>
<td>322</td>
</tr>
<tr>
<td>CHROME</td>
<td>73</td>
<td>0</td>
<td>0.00</td>
<td>0</td>
<td>73</td>
</tr>
<tr>
<td>OTHER</td>
<td>53</td>
<td>0</td>
<td>0.00</td>
<td>0</td>
<td>53</td>
</tr>
<tr>
<td>OPERA</td>
<td>3</td>
<td>0</td>
<td>0.00</td>
<td>0</td>
<td>3</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Platform</th>
<th>ALL</th>
<th>LOAD</th>
<th>PER</th>
<th>HOUR</th>
<th>DAY</th>
</tr>
</thead>
<tbody>
<tr>
<td>OPERA</td>
<td>2</td>
<td>0</td>
<td>0.00</td>
<td>0</td>
<td>2</td>
</tr>
<tr>
<td>OPERA</td>
<td>1</td>
<td>0</td>
<td>0.00</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>OPERA</td>
<td>1</td>
<td>0</td>
<td>0.00</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>MSIE</td>
<td>187</td>
<td>28</td>
<td>14.9</td>
<td>0</td>
<td>187</td>
</tr>
<tr>
<td>MSIE</td>
<td>859</td>
<td>27</td>
<td>3.14</td>
<td>0</td>
<td>859</td>
</tr>
<tr>
<td>MSIE</td>
<td>46</td>
<td>0</td>
<td>0.00</td>
<td>0</td>
<td>46</td>
</tr>
<tr>
<td>FFOX</td>
<td>1</td>
<td>0</td>
<td>0.00</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>FFOX</td>
<td>1</td>
<td>0</td>
<td>0.00</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>FFOX</td>
<td>1</td>
<td>0</td>
<td>0.00</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>FFOX</td>
<td>2</td>
<td>0</td>
<td>0.00</td>
<td>0</td>
<td>2</td>
</tr>
<tr>
<td>FFOX</td>
<td>1</td>
<td>0</td>
<td>0.00</td>
<td>0</td>
<td>1</td>
</tr>
</tbody>
</table>

Caption: Fiesta exploit kit user console.
• Administrator console – The administrator console may or may not extend the Exploit Kit Panel but is used by the exploit kit developer to monitor overall application use and exploit effectiveness.

• Landing page – Intended victims are directed to the exploit kit’s landing page via a custom URL provided by the developer. This page profiles remote victim systems, and attempts to execute exploits targeted against the victim system profile.

Exploit selection and implementation
Different developers use different approaches for exploit selection. Some scavenge published exploit code. Others pay for private exploits, or have resources to develop exploits in-house. In some instances, as with recent exploits included in the Angler exploit kit, they have taken advantage of zero-day vulnerabilities, sometimes including their own. This can dramatically increase exploitation success rates (since no patches exist for the vulnerability). Increased success rates allow the developer to charge significantly higher fees for exploit kit use.

Exploit kits offered for sale
Exploit kits are typically only offered for sale to individuals who have earned a level of trust on the message boards or in IRC channels frequented by the exploit kit developer. The developer is offering access to illegal software, and their profit depends on how long their software remains in use. Allowing unskilled or “untrustworthy” buyers to utilize their product can pose a significant risk to the developer’s business (and her freedom).

Payment for exploit kits can be arranged in a number of different ways. Bitcoin is a popular option. Alternatively, exploit kit developers may permit user access to their kit as long as developer malware is installed on victim devices along with user malware. This profit sharing agreement allows the developer to piggyback
their own malware onto victims obtained by exploit kit users. The developer then takes advantage of the attacker’s work, giving them greater access to victims with less direct effort.

Exploit Kit Maintenance and End-of-Life
An effective exploit kit is not just a fixed set of exploits bundled together. Like any product in a dynamic market, an exploit kit must be actively maintained to maximize effectiveness and value.

Testing and Modification
Once an exploit kit is released and used, the developer monitors success statistics for the exploits in the kit. If particular exploits have lower success rates than others, they can be modified to improve effectiveness or better evade detection until the exploit lifespan ends. Evasion techniques can include detection of installed security software on the client, so that the exploit kit can make informed decisions about the types of exploits known to be effective against the security profile, as well as obfuscation and encryption of payloads.

Removal of end-of-life exploits
The exploit’s value to an exploit kit dissipates over time as detection mechanisms are implemented into endpoint protection technologies and vulnerabilities are remediated. As exploit kit administrators identify end-of-life exploits, these are removed from exploit kits.

Acquisition of new exploits
As ineffective or end-of-life exploits are removed, new exploits must be acquired to take their place. This process proceeds similarly to the initial acquisition of exploits, by purchase or in-house development of private exploits, or acquisition and customization of public exploit code.
End-of-Life of the entire exploit kit

The exploit kit industry is highly competitive. Exploit kits, which do not maintain current or effective exploits, which are not priced competitively, or which do not offer the features and functionality of competitors, will rapidly lose users. Exploit kit end-of-life is usually triggered by lack of maintenance, lack of competitiveness, mergers with other kits, or law enforcement action.

EXPLOIT KIT ATTACKER LIFECYCLE

Attack Campaign Requirements

An attacker can’t simply purchase an exploit kit, click a button, and start exploiting victims. Exploitation is just one component necessary for execution of a large-scale attack. The attacker usually has a clear motive to justify their attack campaign. The primary motivating factor for a large-scale attack campaign is often one of the following:

- Profit
- Botnet Infrastructure
- Extortion
- Fame/Notoriety
- Hacktivism

In addition to exploitation, a large-scale attack requires a mechanism to attract victims, a malicious payload to be delivered, and a command and control infrastructure to send and receive data from compromised victim devices. Exploit kits do not provide these resources.

An overview of the components of an effective campaign is presented below. There is no definitive sequence in which these components must be performed, but all must be in place for a large-scale exploit-based attack to be successfully executed.
• **Payload identification** – An attacker needs to identify the malicious payload to be delivered by an exploit kit to suit the goals of the attack. Most payloads in exploit kit attacks are banking Trojans, ransomware, or botnet applications. Exploit kits may or may not provide these payloads, so attackers may be on their own to obtain, upload, and deploy them.

• **Victim Targeting** – Attacks using exploit kits require a mechanism to lure users to the exploit kit landing page. This can be accomplished in a number of ways. The most common are:

  - Phishing emails designed to lure victims to a hostile landing page
  - Compromised public websites which redirect unsuspecting site visitors to the landing page
  - Malvertising, where a malicious or compromised advertisement redirects a website visitor to the landing page

Exploit kits do not provide target acquisition functionality. However, an attacker could purchase this functionality from a different malicious software developer, such as a spambot operator.

• **Exploitation and Payload Delivery** – This is the role played by exploit kits. Once a victim is lured to the exploit kit landing page, the kit profiles the victim, identifies potentially effective exploits, exploits systems, and delivers the attacker’s payload.

• **Post Exploitation** – Once victims have been compromised, the attacker requires a mechanism to control and retrieve data from victim systems. A command and control infrastructure is generally not provided by exploit kits and the attacker may have to develop or purchase this capability as well.

**Campaign execution and conclusion**

Purchase of an exploit kit typically grants the user access to the exploit kit console for a limited period of time. After that period ends, the user’s access is revoked, use of the exploit kit stops, and the campaign concludes.

Read more at the Global Threat Intelligence Report Online at:
https://nttgroupsecurity.com/
EXPLOIT KITS:

VULNERABILITIES TARGETED IN EXPLOIT KITS
VULNERABILITIES TARGETED IN EXPLOIT KITS

Unique exploits targeted by exploit kits released in years 2012, 2013, and 2014, organized by the technology targeted, is presented in the following graph. There are four clear trends in this data:

- Decrease in Adobe Acrobat exploitation
- Decrease in Java exploitation
- Increase in Adobe Flash exploitation
- Consistent exploitation of Internet Explorer

PERCENTAGE OF UNIQUE VULNERABILITIES TARGETED IN EXPLOIT KITS BY TECHNOLOGY, 2012-2014

Caption: Percent of vulnerabilities targeted in exploit kits by technology.

---

1 This chart includes data from http://contagiodump.blogspot.com, an excellent resource for historical and current exploit kit data.
The trends observed in this graph are discussed below.

- **Decrease in Adobe Acrobat targeting** – Adobe Acrobat exploit usage in exploit kits has steadily decreased from 2012 to 2014. One contributing factor to this drop-off is that Adobe Acrobat exploits require a higher degree of user interaction than browser or Flash-based exploits. Between 2013 and 2014 there has been a 33 percent drop in Adobe Acrobat vulnerabilities published, as shown in the following graph.

![Adobe Acrobat vulnerabilities published by year](image)

- **Decrease in Java targeting** – The number of Java vulnerabilities targeted in exploit kits has decreased significantly from 2013 to 2014. This is due to the 36 percent decrease in Java vulnerabilities identified in 2014, as shown in the following graph.
Increase in Adobe Flash targeting – There has been an increase in Adobe Flash exploit usage in exploit kits from 2012 to 2014. Exploit researchers have increasingly focused on Flash after significant improvements were made to Java and Internet Explorer security in 2014. The number of Flash vulnerabilities identified in 2014 was the highest ever, with a 36 percent increase over 2013 as shown in the following graph.

---

FireEye has recently published a technical discussion of existing Adobe Flash weaknesses at [https://www.fireeye.com/blog/threat-research/2015/03/flash_in_2015.html](https://www.fireeye.com/blog/threat-research/2015/03/flash_in_2015.html)
Consistent targeting of Internet Explorer – Internet Explorer is still distributed as the default browser on the Windows operating system and is common on end-user systems in the corporate environment. Internet Explorer continues to be a target of choice, not only because it is common, but because there has been no shortage of vulnerabilities in Internet Explorer over the past few years. Even more importantly, a significant number of those vulnerabilities (71 percent) allow the attacker great control, such as the ability to execute remote code or to bypass restrictions.
Vulnerabilities targeted in 2014 exploit kits by age of vulnerability

Exploit kits continue to use recent vulnerabilities. The following figures show the distribution of vulnerabilities by year included in exploit kits from 2012 through 2014. In 2012, NTT Group observed the average age of vulnerabilities included in exploit kits was slightly less than two years, while in 2013 and 2014 the average vulnerability age was just over a year. This trend indicates that attackers are growing their sophistication and ability to rapidly update exploit kits before organizations have the chance to react.
CVEs in exploit kits by year of release, 2012

CVEs in exploit kits by year of release, 2013

Caption: CVEs in exploit kits by year of release, 2012.

Caption: CVEs in exploit kits by year of release, 2013.
Over 80 percent of vulnerabilities in exploit kits released in 2014 were published in 2013 and 2014. This data is similar to 2013 and this trend is likely to continue due to strong competition in exploit kits, as developers look to differentiate their product by including newer exploits with a higher likelihood of success.
Most popular vulnerabilities targeted in 2014 exploit kits

The 10 most popular vulnerabilities in exploit kits released in 2014 are presented in the following table.

### 10 Most Popular Vulnerabilities in Exploit Kits

<table>
<thead>
<tr>
<th>CVE</th>
<th>Percentage of Kits in Which Exploit This Vulnerability</th>
<th>Affected Technology</th>
</tr>
</thead>
<tbody>
<tr>
<td>CVE-2013-2551</td>
<td>62%</td>
<td>Microsoft Internet Explorer</td>
</tr>
<tr>
<td>CVE-2014-0515</td>
<td>52%</td>
<td>Adobe Flash</td>
</tr>
<tr>
<td>CVE-2013-0074</td>
<td>38%</td>
<td>Microsoft Silverlight</td>
</tr>
<tr>
<td>CVE-2013-2465</td>
<td>38%</td>
<td>Oracle Java SE</td>
</tr>
<tr>
<td>CVE-2013-0634</td>
<td>29%</td>
<td>Adobe Flash</td>
</tr>
<tr>
<td>CVE-2013-2460</td>
<td>29%</td>
<td>Oracle Java SE</td>
</tr>
<tr>
<td>CVE-2014-0322</td>
<td>29%</td>
<td>Microsoft Internet Explorer</td>
</tr>
<tr>
<td>CVE-2014-0497</td>
<td>29%</td>
<td>Adobe Flash</td>
</tr>
<tr>
<td>CVE-2014-0569</td>
<td>29%</td>
<td>Adobe Flash</td>
</tr>
<tr>
<td>CVE-2012-0507</td>
<td>24%</td>
<td>Oracle Java SE</td>
</tr>
<tr>
<td>CVE-2012-1723</td>
<td>24%</td>
<td>Oracle Java SE</td>
</tr>
</tbody>
</table>

Caption: 10 most popular vulnerabilities in exploit kits released in 2014.

In 2013, only one Adobe Flash exploit was among the 10 most popular exploits included in exploit kits. In 2014, four Adobe Flash exploits were included in the top 10. In 2013, eight of the top 10 exploits were related to Java. In 2014, only four of the top 10 exploits involved Java.

---

1 This table also uses data from contagiodump.blogspot.com.
A Microsoft Internet Explorer exploit (for CVE-2013-2551) was the most popular exploit included in exploit kits in 2014. This vulnerability was originally discovered by Vupen Security. Vupen Security specializes in discovery of zero-day vulnerabilities, and used an exploit for CVE-2013-2551 to win the 2013 Pwn2Own hacking competition. Vupen subsequently published a blog post\(^6\) which provided a detailed walkthrough of how the vulnerability was exploited. These published details may explain its popularity in exploit kits. This was a highly reliable exploit against Internet Explorer, which likely also accounts for its popularity.

Read more at the Global Threat Intelligence Report Online at:

https://nttgroupsecurity.com/
EXPLOIT KITS:

DETECTION BY MONTH
DETECTION BY MONTH

Monthly trending of the top 10 exploit kits detected by NTT in 2014 is presented in the following graph.

EXPLOIT KITS DETECTED BY MONTH, 2014

Exploit kits are difficult to detect reliably. The best exploit kit detection mechanism is identification of landing pages, which constantly change. There is also a natural ebb and flow to the popularity of exploit kits, which explains some of the month to month variation observed in detection. Exploit kits undergo release cycles similar to enterprise applications. An exploit kit may experience a decrease in popularity as exploits in the kit become stale or ineffective, but once
outdated exploits are replaced with newer and more effective exploits, usage of the kit can increase.

A number of trends can be identified from this data:

- **Final dissipation of Blackhole** – After the arrest of Blackhole exploit kit creator “Paunch” in October 2013, support for Blackhole ended. NTT observed use of the once popular kit dwindle throughout 2014, and completely disappear during the 4th quarter. Blackhole was the premier exploit kit for more than two years and was actively maintained to achieve that status.

- **Demise of Phoenix Exploit Kit** – Similar to Blackhole, NTT observed the final demise of the Phoenix exploit kit in 2014. After the arrest of Phoenix’s developer in April 2013, NTT observed a steady decline in Phoenix exploit kit activity. This kit is now considered retired.

- **Increase in Angler usage** – Angler appears to be the most active exploit kit due to inclusion of the latest exploits and retiring older exploits. Angler has also included zero-day Adobe Flash exploits, differentiating itself from competition. These characteristics led to a rise in its popularity in the second half of 2014, and this popularity has continued into 2015, with the release of Adobe Flash zero day vulnerabilities (CVE-2015-0311, CVE-2015-0313) in Angler.

Read more at the Global Threat Intelligence Report Online at: https://nttgroupsecurity.com/
RECOMMENDATIONS TO PROTECT AGAINST EXPLOIT KITS
RECOMMENDATIONS TO PROTECT AGAINST EXPLOIT KITS

To reduce risks associated with exploit kits, organizations should consider the following steps:

- **Ensure effective patch management** – Exploit kits typically use exploits for vulnerabilities where patches exist but are not applied. The speed with which exploit kit developers deploy new exploits takes advantage of the gap in time between initial vulnerability disclosure and the implementation of patches at the organization. Ensuring that effective patch management processes exist for end-user devices is a critical first step to protect against exploit kits. Organizations should pay particular attention to web plugins and technologies, such as Java and Adobe Flash. These technologies do not have the same types of enterprise class rollout capabilities which are associated with Microsoft technologies, and organizations need to ensure that there are tools in place to deploy and measure adoption of patches.

- **Social engineering (phishing) training** – Standard security awareness training alone is not adequate for organizations, which maintain or access highly sensitive data. Real world social engineering testing should be implemented for key employees, to confirm their ability to detect and respond to actual phishing scenarios.

- **Ad blocking software** – Attackers frequently use malvertising to lure victims onto exploit kit landing pages. Use of ad blocking software, or web proxies with content filtering, can limit the effectiveness of this attack approach.
• **IP reputation services** – Use of IP reputation services which can warn or block users from visiting known bad IP addresses and domains can protect organizational users from inadvertently accessing those addresses. IP reputation services should only be considered a supplemental control. Addresses of exploit kits are constantly changing in order to evade detection, and the services are unlikely to maintain accurate and comprehensive real-time lists of landing page URLs.

• **Threat intelligence** – Threat intelligence services can be used to help organizations identify vulnerabilities, which are being actively exploited in the wild. These services can act as a complementary control to patch management processes, to ensure that patching is prioritized for vulnerabilities.

• **Endpoint Protection** – Implementation of endpoint protection can help organizations detect the existence of malware dropped on a device by an exploit kit before significant damage occurs.

Read more at the Global Threat Intelligence Report Online at: https://nttgroupsecurity.com/