Understanding EXPLOIT KITS

What do they do?
- Specialized to deliver online malicious content
- Phishing with fake software
- Download malicious software
- Stealing user credentials
- Redirecting to malicious sites

How common are they?
- 6,000 / 0.5 HOUR
- 3,000 / 0.5 HOUR
- 2.6% / Month
- 60% of Infections
- 55 Years

Which users are vulnerable?
- Downloading files
- Clicking links
- Installing third-party software
- Opening suspicious emails

Most commonly affected software

<table>
<thead>
<tr>
<th>Software</th>
<th>Exploit Kit</th>
</tr>
</thead>
<tbody>
<tr>
<td>MS Office</td>
<td>45%</td>
</tr>
<tr>
<td>Adobe</td>
<td>30%</td>
</tr>
<tr>
<td>Flash</td>
<td>20%</td>
</tr>
<tr>
<td>Java</td>
<td>5%</td>
</tr>
</tbody>
</table>

How do Exploit Kits work?

1. The Exploit Kit downloads a browser plug-in that can be used to run malicious code.
2. The plug-in is distributed through phishing emails or social engineering.
3. Once the plug-in is installed, it can run malicious code on the user's computer.

What can you do about it?

1. Keep your software up to date.
2. Use a browser add-on to block plug-ins.
3. Use security software to protect against malicious code.