Cross-Platform Malware: Write Once, Infect Everywhere

Martina Lindorfer, Matthias Neumayr, Juan Caballero, Christian Platzer
Vienna University of Technology, IMDEA Software Institute

Introduction

- Programmers aim at writing a program once and then using it on different computing platforms: „Write once, run everywhere“
- Benefits include code reuse, reduced development time and easier maintenance.
- This paradigm is extended in benign software, but it is not yet prevalent in malware: The majority targets Windows with Android Malware recently growing.
- Supporting a new platform boils down to a cost-geneefit analysis: the income from supporting new platforms vs. the additional investment in software development and distribution.
- A cost-effective way of distributing malware is through drive-by downloads leveraging exploits for X-platform vulnerabilities.

In this work we explore:
- X-platform malware and how it achieves portability.
- X-platform vulnerabilities and their availability in commercial exploit kits.

Overview

A X-platform program is a program that is portable across different OS families.

Programs become portable ...
- using programming languages compiling to bytecode e.g. Java, .NET
- on source code level using standardized interfaces e.g. POSIX
- on source code using interpreted languages e.g. Perl, Python
- running on top of other X-platform programs e.g. web browsers, office applications

A X-platform vulnerability is a software defect present in platform-independent code of a X-platform program.

Contact:
mindorfer@iseclab.org
mneumayr@iseclab.org
juan.caballero@imdea.org
cplatzer@iseclab.org

X-Platform Malware

- We found 14 X-platform malware families already observed in the wild.
- We found three proof-of-concept malware samples.
- Four families use exploits to get installed on the target hosts, while the remaining nine rely on social engineering (SE) for distribution.
- X-platform malware is distributed as:
  - Source code: Python, JavaScript, Perl, Ruby
  - Binary code: PE, ELF, MACH-O
  - Bytecode: Java, .NET

<table>
<thead>
<tr>
<th>Family</th>
<th>Date</th>
<th>Distribution</th>
<th>Platforms</th>
</tr>
</thead>
<tbody>
<tr>
<td>Badbunny</td>
<td>07/09</td>
<td>SE</td>
<td>JavaScript, Perl, Ruby</td>
</tr>
<tr>
<td>Boonana</td>
<td>10/10</td>
<td>SE</td>
<td>Java, Java</td>
</tr>
<tr>
<td>ZitMo</td>
<td>09/10</td>
<td>SE</td>
<td>Java*, Java*</td>
</tr>
<tr>
<td>Olyx</td>
<td>06/11</td>
<td>Exploit</td>
<td>PE, MACH-O</td>
</tr>
<tr>
<td>Tibet</td>
<td>03/12</td>
<td>Exploit</td>
<td>PE, MACH-O</td>
</tr>
<tr>
<td>Flsplysc</td>
<td>04/12</td>
<td>Exploit</td>
<td>PE, Python</td>
</tr>
<tr>
<td>Crisis</td>
<td>04/12</td>
<td>SE</td>
<td>PE, MACH-O, PE*</td>
</tr>
<tr>
<td>LillyJade</td>
<td>05/12</td>
<td>Exploit</td>
<td>JavaScript, JavaScript</td>
</tr>
<tr>
<td>GetShell</td>
<td>07/12</td>
<td>SE</td>
<td>Java, Java</td>
</tr>
<tr>
<td>Netweirdc</td>
<td>08/12</td>
<td>SE</td>
<td>PE, ELF, MACH-O</td>
</tr>
<tr>
<td>JvRAT</td>
<td>10/12</td>
<td>SE</td>
<td>Java, Java</td>
</tr>
<tr>
<td>Ssucel</td>
<td>01/13</td>
<td>SE</td>
<td>PE, Java</td>
</tr>
<tr>
<td>MinecraftHack</td>
<td>03/13</td>
<td>SE</td>
<td>Java</td>
</tr>
<tr>
<td>Janicab</td>
<td>07/13</td>
<td>Exploit/SE</td>
<td>VB Script, Python</td>
</tr>
<tr>
<td>Cit10 (PoC)</td>
<td>07/12</td>
<td>Exploit/SE</td>
<td>ASM, ASM</td>
</tr>
<tr>
<td>Yakzake (PoC)</td>
<td>08/07</td>
<td>Exploit/SE</td>
<td>NET, .NET</td>
</tr>
<tr>
<td>Clapzok (PoC)</td>
<td>05/13</td>
<td>Exploit/SE</td>
<td>ASM, ASM</td>
</tr>
</tbody>
</table>

Future Work

- Collect samples of the identified malware families.
- Measure the amount of code reuse.
- Collect exploits for the identified X-platform vulnerabilities and examine their X-platform capabilities.
- Analyze X-platform exploits and malware in the wild through multi-platform honeymoons.

X-Platform Vulnerabilities

- X-platform vulnerabilities exist in:
  - Browser plugins (Java, PDF, Flash)
  - Web browsers (Firefox, WebKit)
  - Desktop applications (Microsoft Word)
  - Java is by far the most vulnerable application.

Source: http://xkcd.com/934/

Overview

A X-platform program is a program that is portable across different OS families.

Programs become portable ...
- using programming languages compiling to bytecode e.g. Java, .NET
- on source code level using standardized interfaces e.g. POSIX
- on source code using interpreted languages e.g. Perl, Python
- running on top of other X-platform programs e.g. web browsers, office applications

A X-platform vulnerability is a software defect present in platform-independent code of a X-platform program.

Contact:
mindorfer@iseclab.org
mneumayr@iseclab.org
juan.caballero@imdea.org
cplatzer@iseclab.org

Overview

A X-platform program is a program that is portable across different OS families.

Programs become portable ...
- using programming languages compiling to bytecode e.g. Java, .NET
- on source code level using standardized interfaces e.g. POSIX
- on source code using interpreted languages e.g. Perl, Python
- running on top of other X-platform programs e.g. web browsers, office applications

A X-platform vulnerability is a software defect present in platform-independent code of a X-platform program.

Contact:
mindorfer@iseclab.org
mneumayr@iseclab.org
juan.caballero@imdea.org
cplatzer@iseclab.org