Evasive Malware

A Field Guide to Detecting, Analyzing, and Defeating Advanced Threats

by Kyle Cucci

Errata updated to print 2

<table>
<tr><th>Page</th><th>Error</th><th>Correction</th><th>Print corrected</th></tr>
<tr><td>44</td><td>For example, the x64 RAX register, which can store 64 bits of data, “contains” four additional smaller general registers: EAX (the last 32 bits of data in RAX), AX (the upper 16 bits of EAX), AH (the upper 8 bits of EAX), and AL (the lower 8 bits of EAX).</td><td>For example, the x64 RAX register, which can store 64 bits of data, “contains” four additional smaller general registers: EAX (the last 32 bits of data in RAX), AX (the lower 16 bits of EAX), AH (the upper 8 bits of AX), and AL (the lower 8 bits of AX).</td><td>Print 2</td></tr>
<tr><td>45</td><td>
<table>
<tr><th>x86 register</th><th>x64 register</th><th>Description</th></tr>
<tr><td>EAX</td><td>RAX</td><td>The accumulator register, used for tasks such as arithmetic, interrupts, and storing return values</td></tr>
<tr><td>AX, AH, AL</td><td>Same as x86</td><td>Upper 16 bits of EAX, upper 8 bits of EAX, and lower 8 bits of EAX, respectively</td></tr>
<tr><td>EBX</td><td>RBX</td><td>Used for referencing variables and arguments</td></tr>
<tr><td>BX, BH, BL</td><td>Same as x86</td><td>Upper 16 bits of EBX, upper 8 bits of EBX, and lower 8 bits of EBX, respectively</td></tr>
<tr><td>ECX</td><td>RCX</td><td>The counter register, used for counting and loop control</td></tr>
<tr><td>CX, CH, CL</td><td>Same as x86</td><td>Upper 16 bits of ECX, upper 8 bits of ECX, and lower 8 bits of ECX, respectively</td></tr>
<tr><td>EDX</td><td>RDX</td><td>The data register, used primarily for arithmetic operations and sometimes as a backup for EAX</td></tr>
<tr><td>DX, DH, DL</td><td>Same as x86</td><td>Upper 16 bits of EDX, upper 8 bits of EDX, and lower 8 bits of EDX, respectively</td></tr>
</table>
</td><td>
<table>
<tr><th>x86 register</th><th>x64 register</th><th>Description</th></tr>
<tr><td>EAX</td><td>RAX</td><td>The accumulator register, used for tasks such as arithmetic, interrupts, and storing return values</td></tr>
<tr><td>AX, AH, AL</td><td>Same as x86</td><td>Lower 16 bits of EAX, upper 8 bits of AX, and lower 8 bits of AX, respectively</td></tr>
<tr><td>EBX</td><td>RBX</td><td>Used for referencing variables and arguments</td></tr>
<tr><td>BX, BH, BL</td><td>Same as x86</td><td>Lower 16 bits of EBX, upper 8 bits of BX, and lower 8 bits of BX, respectively</td></tr>
<tr><td>ECX</td><td>RCX</td><td>The counter register, used for counting and loop control</td></tr>
<tr><td>CX, CH, CL</td><td>Same as x86</td><td>Lower 16 bits of ECX, upper 8 bits of CX, and lower 8 bits of CX, respectively</td></tr>
<tr><td>EDX</td><td>RDX</td><td>The data register, used primarily for arithmetic operations and sometimes as a backup for EAX</td></tr>
<tr><td>DX, DH, DL</td><td>Same as x86</td><td>Lower 16 bits of EDX, upper 8 bits of DX, and lower 8 bits of DX, respectively</td></tr>
</table>
</td><td>Print 2</td></tr>
</table>