Metamorphic code examples from *Metamorphic Virus: Analysis and Detection*, by Evgenios Konstantinou.

Garbage Code Insertion Example

Early version of Win32.Evol:

```
C7060F000055    mov [esi], 5500000Fh
C746048BEC5151  mov [esi+0004], 5151EC8Bh
```

Later generation:

```
BF0F00055     mov edi, 5500000Fh
893E          mov [esi], edi
5F            pop edi              ;garbage
52            push edx             ;garbage
B640          mov dh, 40           ;garbage
BA8BEC5151    mov edx, 5151EC8Bh
53            push ebx             ;garbage
8BDA          mov ebx, edx
895E04        mov [esi+0004], ebx
```

Register Exchange Example

Evolution of Win95.Regswap

```
pop   edx
mov   edi,0004h
mov   esi,ebp
mov   eax,000Ch
add   edx,0088h
mov   ebx,[edx]
mov   [esi+eax*4+00001118],ebx
pop   eax

mov   ebx,0004h
mov   edx,ebp
mov   edi,000Ch
```

```
add   eax,0088h
mov   esi,[eax]
mov   [edx+edi*4+00001118],esi
```

Jump Insertion Example

Zperm

```
instruction 1     ; entry point
instruction 2
…
instruction n
```

In later generations the virus changes itself by inserting a random number of jump instructions. A later generation might look like this:

```
instruction 2
jmp instruction 3
instruction 1        ; entry point
jmp instruction 2
instruction 3
jmp instruction n
```

Instruction Replacement Example

Win95.Bistro:

```
55          push ebp
8BEC        mov  ebp, esp
8B7608      mov  esi, dword ptr [ebp + 08]
85F6        test esi, esi
743B        je   401045
8B7E0C      mov  edi, dword ptr [ebp + 0c]
09FF        or   edi, edi
7434        je   401045
31D2        xor  edx, edx
```

After evolution:

```
55          push ebp
54          push esp         ; move replaced by push/
pop
5D          pop  ebp         ; move replaced by push/
pop
8B7608      mov  esi, dword ptr [ebp + 08]
09F6        or   esi, esi    ; test/or interchange
743B        je   401045
8B7E0C      mov  edi, dword ptr [ebp + 0c]
85FF        test edi, edi    ; test/or interchange
7434        je   401045
28D2        sub  edx, ddx    ; xor replaced with sub
```