Check Point
SOFTWARE TECHNOLOGIES LTD.

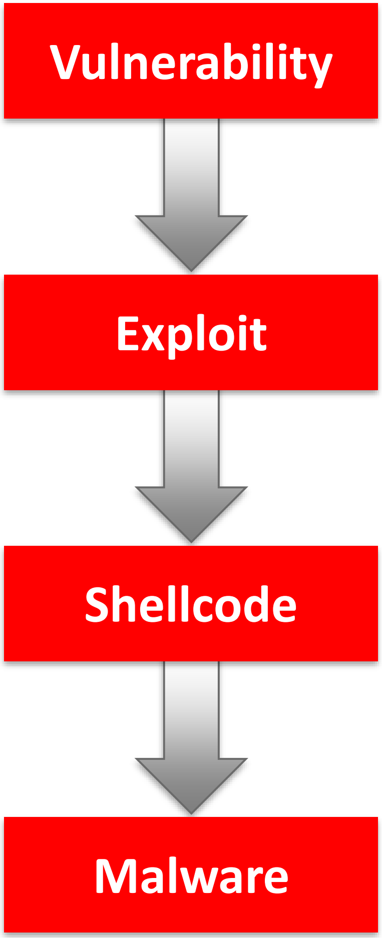
YOUR TRADITIONAL SANDBOX WON'T STOP ZERO-DAYS

Bill Nikolopoulos
Security Engineer, Greece and Cyprus

From an attackers point of view

I’ll need to learn how to break into system…

How Attackers Operate



Vulnerability

An exploitable weakness, typically a software “bug”

Exploit

A sequence that takes advantage of a vulnerability to run the Shellcode

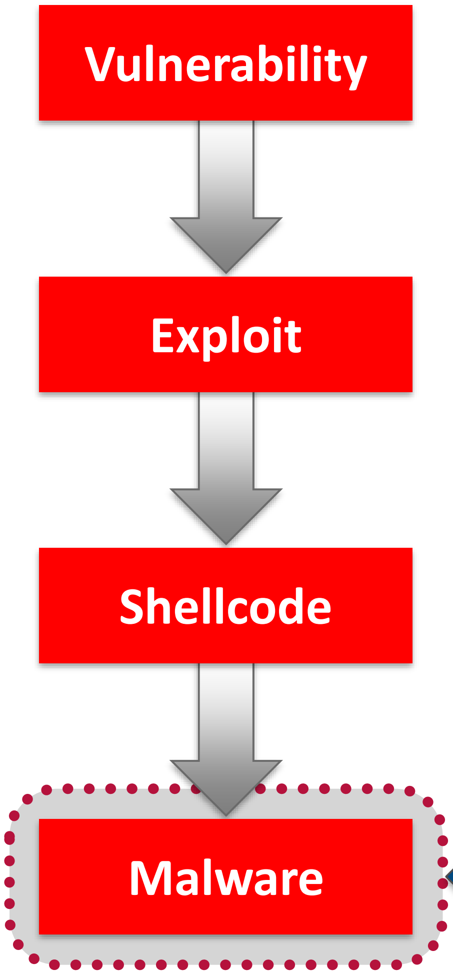
Shellcode

Short code sequence that retrieves the malware

Malware

The malicious software

The Industry Tried to Fight Back



Vulnerability

Exploit

Shellcode

Malware

I'll just change a few bytes and no one will recognize me…

...ering methods to lure users into ...er may, directly or indirectly, cause ...ormed. It attempts to steal sensitive online ...h as user names and passwords. It sends the ...athered in... via HTTP POST to a remote URL.

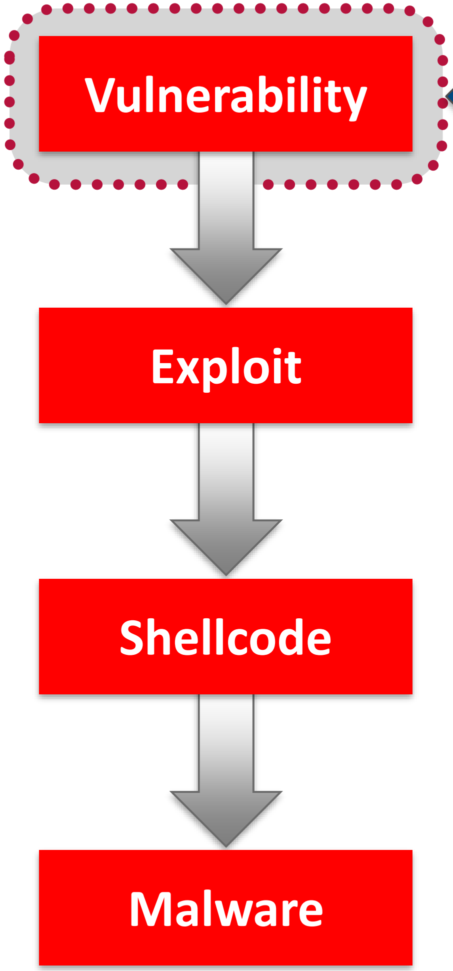
□ Do not block this application again

Recommended: Please click "Remove All" button to heal all infected files and protect your PC

Anti-Virus technologies:

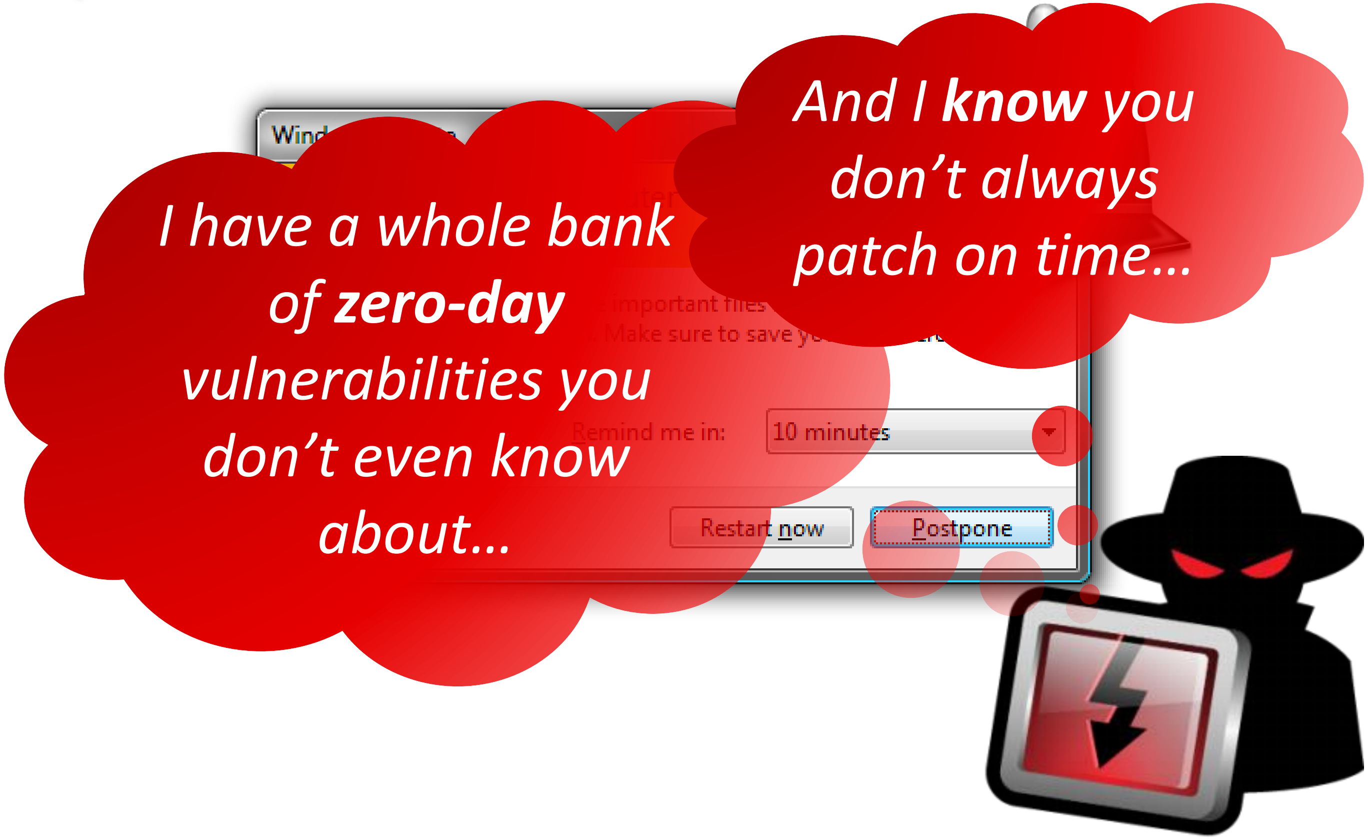
Identify the ***Malware*** *signature*

The Industry Tried to Fight Back



Automatic Patching:

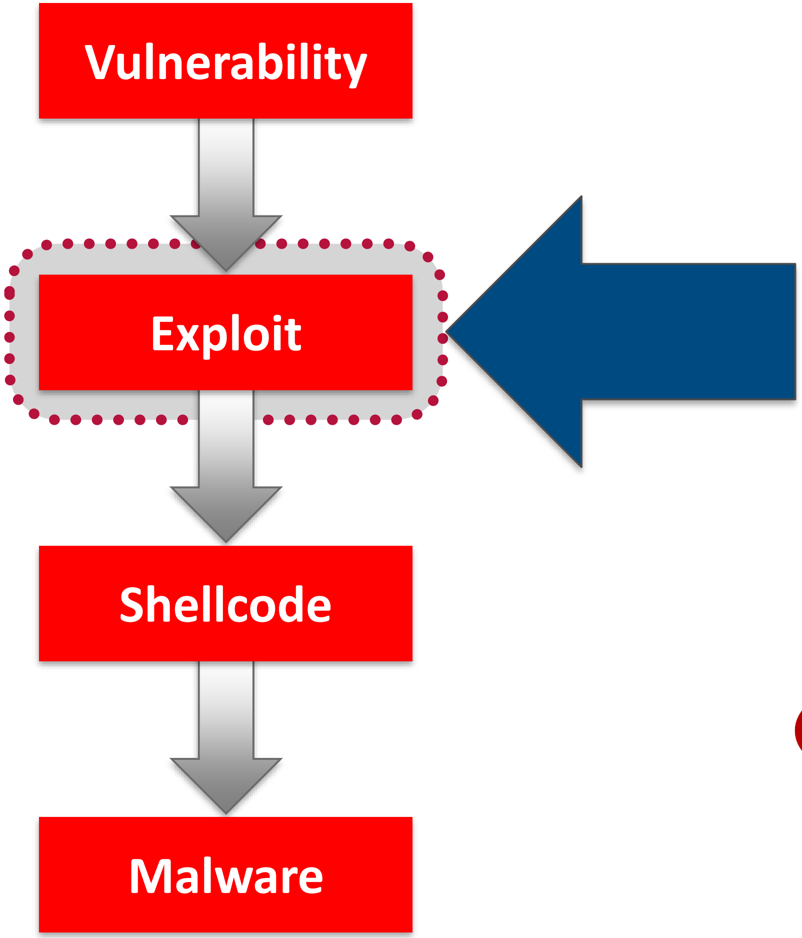
Minimize the number of ***Vulnerabilities***



I have a whole bank of ***zero-day*** *vulnerabilities you don't even know about…*

And I ***know*** *you don't always patch on time…*

The Industry Tried to Fight Back



OS and CPU Security Controls:
Block ***Exploits*** *even if a vulnerability exists*

OS and CPU Security Controls

Check Point
SOFTWARE TECHNOLOGIES LTD.

DEP: Data Execution Prevention

Since: *Windows XP SP2+; Linux 2.6.8+; iOS x86 versions*

ASLR: Address Space Layout Randomization

Since: *Windows Vista+; Visual Studio 2010+*

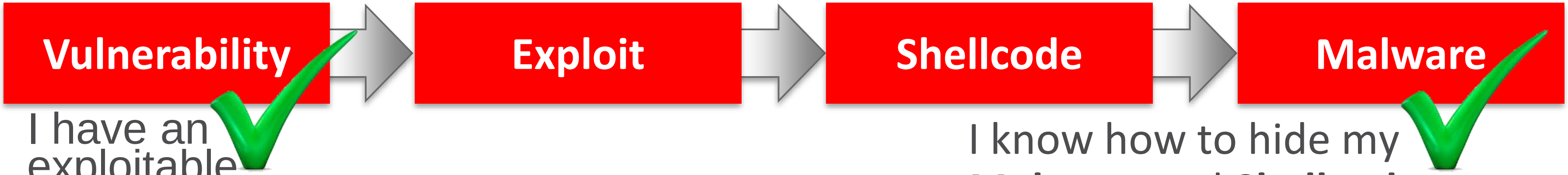
SMEP: Superior Mode Execution Protection

Since: *Windows 8*

CFG: Control Flow Guard

Since: *Windows 8.1 SP3+*

But I’m an Attacker – What Can I Do?



Vulnerability → Exploit → Shellcode → Malware

I have an exploitable **vulnerabilit y**

I know how to hide my **Malware** and **Shellcode** from Anti-Viruses

I’ll need some clever modern ***EXPLOIT*** *technique…*

Bypassing OS and CPU Security Controls

ROP: Return Oriented Programming

~~Load my code and move the instruction pointer to it~~

Re-use pieces of code that are already loaded as executable

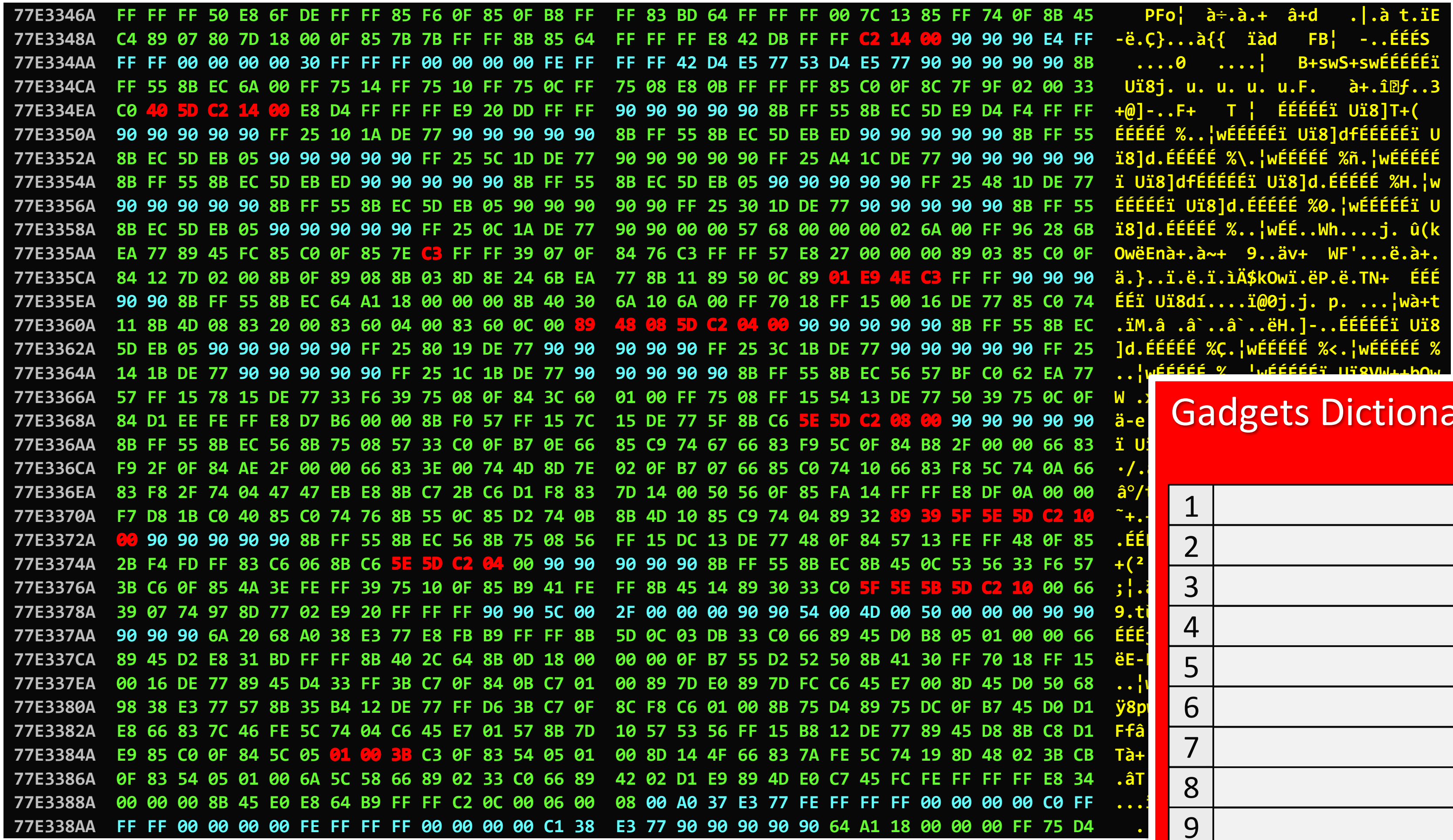
Bypassing OS and CPU Security Controls

ROP: Return Oriented Programming

- Examine code known to be loaded when the exploit is activated
  - Executable and DLLs of the **target OS**
  - Executable and DLLs of the **target application**
- Search for useful "**Gadgets**"
  - Short sequences of code immediately followed by a Return
- Program an exploit using Gadgets as code primitives

Building a ROP Gadgets Dictionary

Check Point
SOFTWARE TECHNOLOGIES LTD.



```
77E3346A  FF FF FF 50 E8 6F DE FF FF 85 F6 0F 85 0F B8 FF  FF 83 BD 64 FF FF FF 00 7C 13 85 FF 74 0F 8B 45     PFo¦  à÷.à.+  â+d   .|.à t.ïE
77E3348A  C4 89 07 80 7D 18 00 0F 85 7B 7B FF FF 8B 85 64  FF FF FF E8 42 DB FF FF C2 14 00 90 90 90 E4 FF  -ë.Ç}...à{{  ïàd   FB¦  -..ÉÉÉS
77E334AA  FF FF 00 00 00 00 30 FF FF FF 00 00 00 00 FE FF  FF FF 42 D4 E5 77 53 D4 E5 77 90 90 90 90 90 8B    ....0   ....¦   B+swS+swÉÉÉÉÉï
77E334CA  FF 55 8B EC 6A 00 FF 75 14 FF 75 10 FF 75 0C FF  75 08 E8 0B FF FF FF 85 C0 0F 8C 7F 9F 02 00 33   Uï8j. u. u. u. u.F.   à+.î.ƒ..3
77E334EA  C0 40 5D C2 14 00 E8 D4 FF FF FF E9 20 DD FF FF  90 90 90 90 90 8B FF 55 8B EC 5D E9 D4 F4 FF FF  +@]-..F+   T ¦  ÉÉÉÉÉï Uï8]T+(
77E3350A  90 90 90 90 90 FF 25 10 1A DE 77 90 90 90 90 90  8B FF 55 8B EC 5D EB ED 90 90 90 90 90 8B FF 55  ÉÉÉÉÉ %..¦wÉÉÉÉÉï Uï8]dfÉÉÉÉÉï U
77E3352A  8B EC 5D EB 05 90 90 90 90 90 FF 25 5C 1D DE 77  90 90 90 90 90 FF 25 A4 1C DE 77 90 90 90 90 90  ï8]d.ÉÉÉÉÉ %\.¦wÉÉÉÉÉ %ñ.¦wÉÉÉÉÉ
77E3354A  8B FF 55 8B EC 5D EB ED 90 90 90 90 90 8B FF 55  8B EC 5D EB 05 90 90 90 90 90 FF 25 48 1D DE 77  ï Uï8]dfÉÉÉÉÉï Uï8]d.ÉÉÉÉÉ %H.¦w
77E3356A  90 90 90 90 90 8B FF 55 8B EC 5D EB 05 90 90 90  90 90 FF 25 30 1D DE 77 90 90 90 90 90 8B FF 55  ÉÉÉÉÉï Uï8]d.ÉÉÉÉÉ %0.¦wÉÉÉÉÉï U
77E3358A  8B EC 5D EB 05 90 90 90 90 90 FF 25 0C 1A DE 77  90 90 00 00 57 68 00 00 00 02 6A 00 FF 96 28 6B  ï8]d.ÉÉÉÉÉ %..¦wÉÉ..Wh....j. û(k
77E335AA  EA 77 89 45 FC 85 C0 0F 85 7E C3 FF FF 39 07 0F  84 76 C3 FF FF 57 E8 27 00 00 00 89 03 85 C0 0F  OwëEnà+.à~+  9..äv+  WF'...ë.à+.
77E335CA  84 12 7D 02 00 8B 0F 89 08 8B 03 8D 8E 24 6B EA  77 8B 11 89 50 0C 89 01 E9 4E C3 FF FF 90 90 90  ä.}..ï.ë.ï.ìÄ$kOwï.ëP.ë.TN+  ÉÉÉ
77E335EA  90 90 8B FF 55 8B EC 64 A1 18 00 00 00 8B 40 30  6A 10 6A 00 FF 70 18 FF 15 00 16 DE 77 85 C0 74  ÉÉï Uï8dí....ï@0j.j. p.  ...¦wà+t
77E3360A  11 8B 4D 08 83 20 00 83 60 04 00 83 60 0C 00 89  48 08 5D C2 04 00 90 90 90 90 90 8B FF 55 8B EC  .ïM.â  .â`..â`..ëH.]-..ÉÉÉÉÉï Uï8
77E3362A  5D EB 05 90 90 90 90 90 FF 25 80 19 DE 77 90 90  90 90 90 FF 25 3C 1B DE 77 90 90 90 90 90 FF 25  ]d.ÉÉÉÉÉ %Ç.¦wÉÉÉÉÉ %<.¦wÉÉÉÉÉ %
77E3364A  14 1B DE 77 90 90 90 90 90 FF 25 1C 1B DE 77 90  90 90 90 90 8B FF 55 8B EC 56 57 BF C0 62 EA 77  ..¦wÉÉÉÉÉ %  ¦wÉÉÉÉÉï Uï8VW++bOw
77E3366A  57 FF 15 78 15 DE 77 33 F6 39 75 08 0F 84 3C 60  01 00 FF 75 08 FF 15 54 13 DE 77 50 39 75 0C 0F  W .x
77E3368A  84 D1 EE FE FF E8 D7 B6 00 00 8B F0 57 FF 15 7C  15 DE 77 5F 8B C6 5E 5D C2 08 00 90 90 90 90 90  ä-e
77E336AA  8B FF 55 8B EC 56 8B 75 08 57 33 C0 0F B7 0E 66  85 C9 74 67 66 83 F9 5C 0F 84 B8 2F 00 00 66 83  ï U
77E336CA  F9 2F 0F 84 AE 2F 00 00 66 83 3E 00 74 4D 8D 7E  02 0F B7 07 66 85 C0 74 10 66 83 F8 5C 74 0A 66  ·/.
77E336EA  83 F8 2F 74 04 47 47 EB E8 8B C7 2B C6 D1 F8 83  7D 14 00 50 56 0F 85 FA 14 FF FF E8 DF 0A 00 00  â°/
77E3370A  F7 D8 1B C0 40 85 C0 74 76 8B 55 0C 85 D2 74 0B  8B 4D 10 85 C9 74 04 89 32 89 39 5F 5E 5D C2 10  ˜+.
77E3372A  00 90 90 90 90 90 8B FF 55 8B EC 56 8B 75 08 56  FF 15 DC 13 DE 77 48 0F 84 57 13 FE FF 48 0F 85  .ÉÉ
77E3374A  2B F4 FD FF 83 C6 06 8B C6 5E 5D C2 04 00 90 90  90 90 90 8B FF 55 8B EC 8B 45 0C 53 56 33 F6 57  +(²
77E3376A  3B C6 0F 85 4A 3E FE FF 39 75 10 0F 85 B9 41 FE  FF 8B 45 14 89 30 33 C0 5F 5E 5B 5D C2 10 00 66  ;¦.
77E3378A  39 07 74 97 8D 77 02 E9 20 FF FF FF 90 90 5C 00  2F 00 00 00 90 90 54 00 4D 00 50 00 00 00 90 90  9.t
77E337AA  90 90 90 6A 20 68 A0 38 E3 77 E8 FB B9 FF FF 8B  5D 0C 03 DB 33 C0 66 89 45 D0 B8 05 01 00 00 66  ÉÉÉ
77E337CA  89 45 D2 E8 31 BD FF FF 8B 40 2C 64 8B 0D 18 00  00 00 0F B7 55 D2 52 50 8B 41 30 FF 70 18 FF 15  ëE-
77E337EA  00 16 DE 77 89 45 D4 33 FF 3B C7 0F 84 0B C7 01  00 89 7D E0 89 7D FC C6 45 E7 00 8D 45 D0 50 68  ..¦
77E3380A  98 38 E3 77 57 8B 35 B4 12 DE 77 FF D6 3B C7 0F  8C F8 C6 01 00 8B 75 D4 89 75 DC 0F B7 45 D0 D1  ÿ8p
77E3382A  E8 66 83 7C 46 FE 5C 74 04 C6 45 E7 01 57 8B 7D  10 57 53 56 FF 15 B8 12 DE 77 89 45 D8 8B C8 D1  Ffâ
77E3384A  E9 85 C0 0F 84 5C 05 01 00 3B C3 0F 83 54 05 01  00 8D 14 4F 66 83 7A FE 5C 74 19 8D 48 02 3B CB  Tà+
77E3386A  0F 83 54 05 01 00 6A 5C 58 66 89 02 33 C0 66 89  42 02 D1 E9 89 4D E0 C7 45 FC FE FF FF FF E8 34  .âT
77E3388A  00 00 00 8B 45 E0 E8 64 B9 FF FF C2 0C 00 06 00  08 00 A0 37 E3 77 FE FF FF FF 00 00 00 00 C0 FF  ...
77E338AA  FF FF 00 00 00 00 FE FF FF FF 00 00 00 00 C1 38  E3 77 90 90 90 90 90 64 A1 18 00 00 00 FF 75 D4    .
```

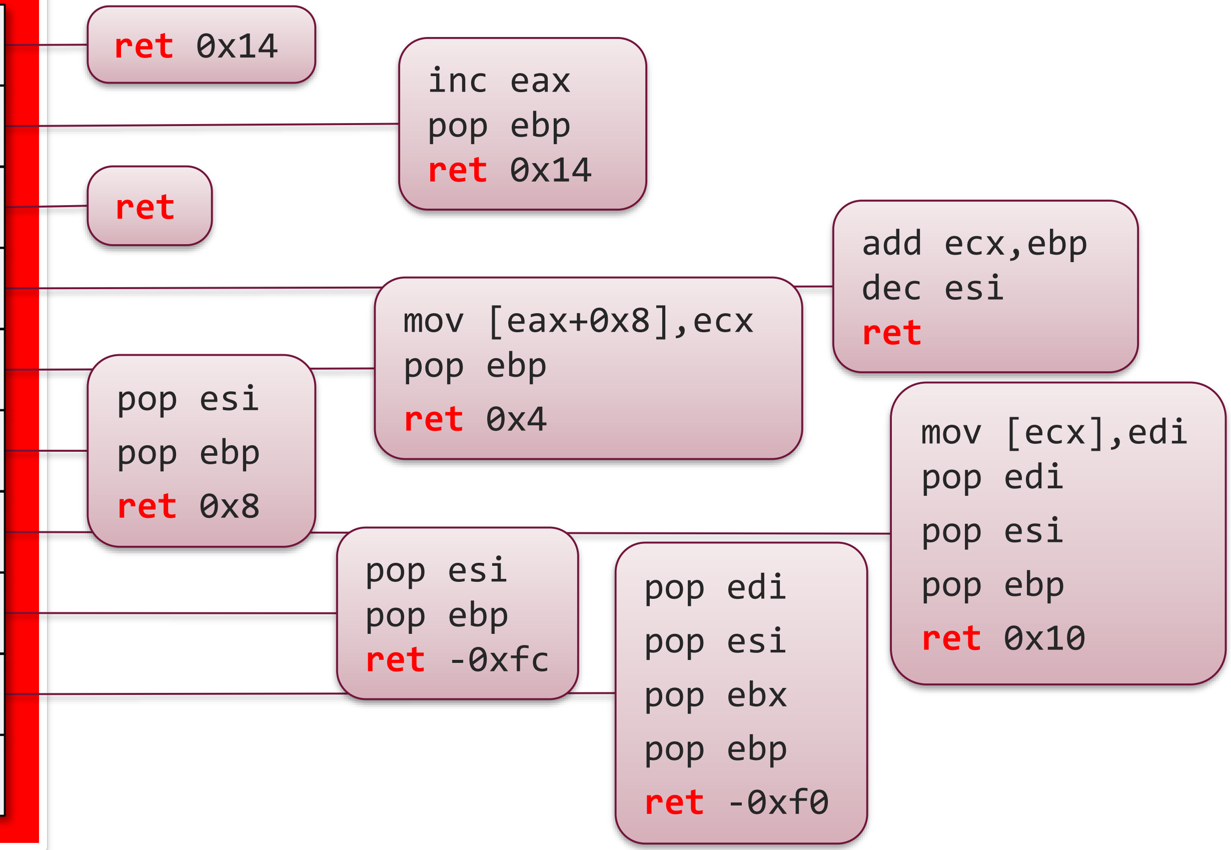
Gadgets Dictionary

1	
2	
3	
4	
5	
6	
7	
8	
9	
10	

A New Programming “Language”

Gadgets Dictionary

1	C2 14 00
2	40 5D C2 14 00
3	C3
4	01 E9 4E C3
5	89 48 08 5D C2 04 00
6	5E 5D C2 08 00
7	89 39 5F 5E 5D C2 10 00
8	5E 5D C2 04
9	5F 5E 5B 5D C2 10
10	...



```
ret 0x14
```

```
inc eax
pop ebp
ret 0x14
```

```
ret
```

```
add ecx,ebp
dec esi
ret
```

```
mov [eax+0x8],ecx
pop ebp
ret 0x4
```

```
pop esi
pop ebp
ret 0x8
```

```
mov [ecx],edi
pop edi
pop esi
pop ebp
ret 0x10
```

```
pop esi
pop ebp
ret -0xfc
```

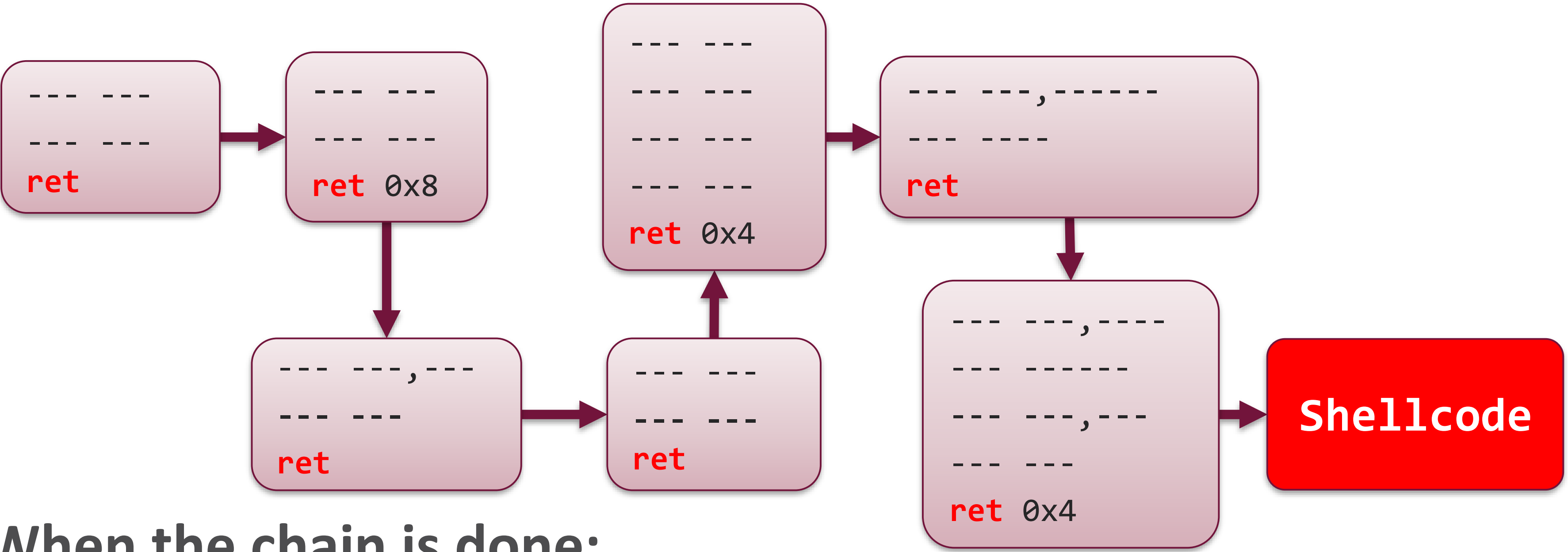
```
pop edi
pop esi
pop ebx
pop ebp
ret -0xf0
```

Exploit Using a ROP Chain

Check Point
SOFTWARE TECHNOLOGIES LTD.

Program an **EXPLOIT** by chaining ROP gadgets

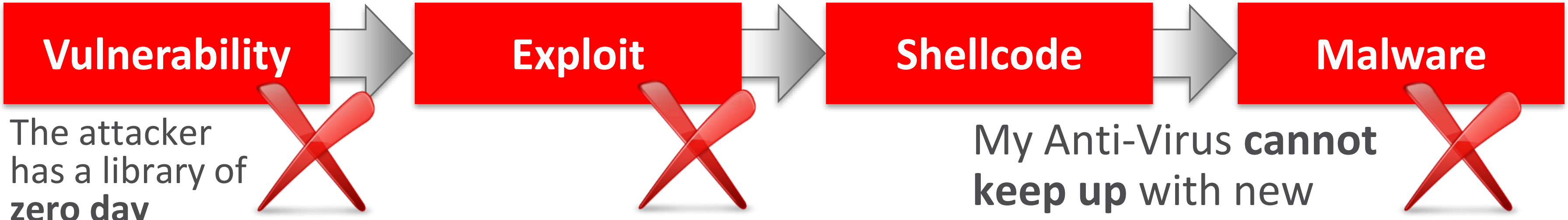
Manipulate the CPU Instruction Pointer to move between preloaded Gadgets



When the chain is done:

- Shellcode is loaded to executable memory
- Instruction Pointer is pointing to the beginning of the Shellcode

I’m a Defender – What Can I Do?



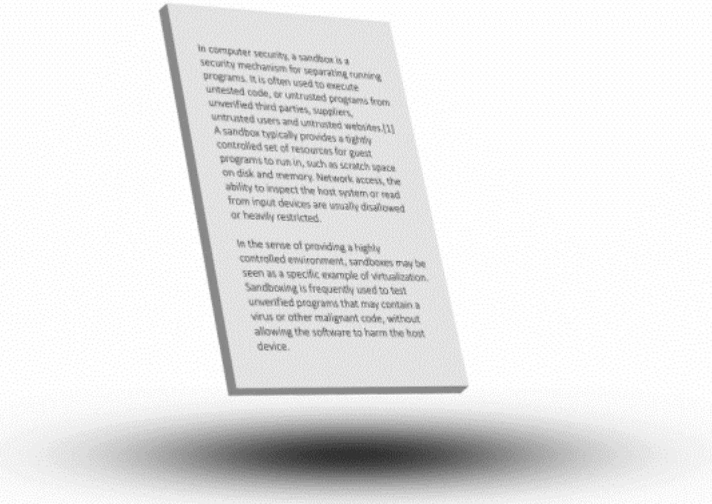
Vulnerability → Exploit → Shellcode → Malware

The attacker has a library of **zero day vulnerabilities**

My Anti-Virus **cannot keep up** with new Malware variants

Clearly, those OS Protections are not enough…

The solution: Sandboxing



In computer security, a sandbox is a security mechanism for separating running programs. It is often used to execute untested code, or untrusted programs from unverified third parties, suppliers, untrusted users and untrusted websites.[1] A sandbox typically provides a tightly controlled set of resources for guest programs to run in, such as scratch space on disk and memory. Network access, the ability to inspect the host system or read from input devices are usually disallowed or heavily restricted.

In the sense of providing a highly controlled environment, sandboxes may be seen as a specific example of virtualization. Sandboxing is frequently used to test unverified programs that may contain a virus or other malignant code, without allowing the software to harm the host device.

- System Registry
- Network Connections
- File System Activity
- System Processes

Sandbox Evasion Techniques

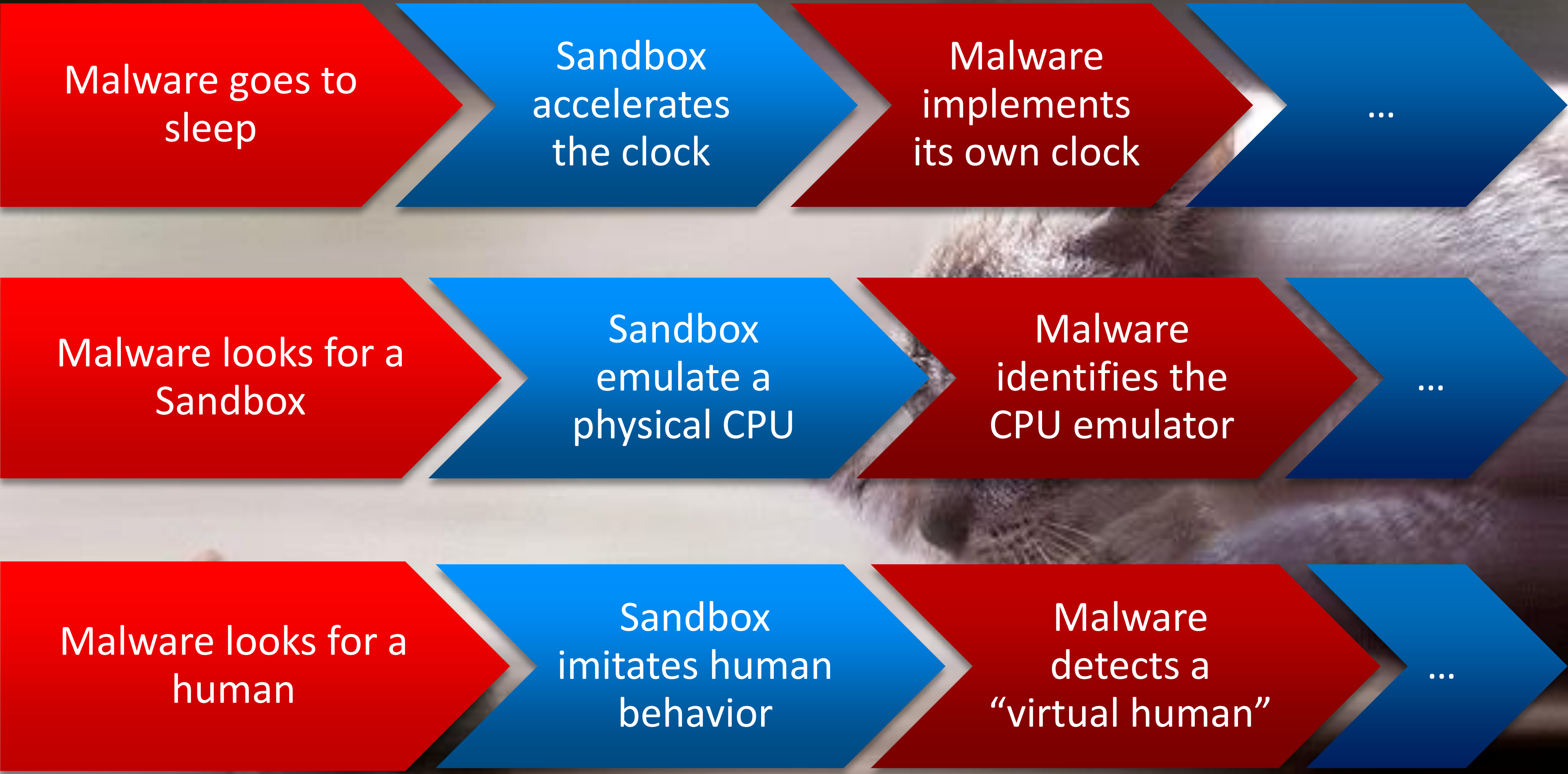
Check Point
SOFTWARE TECHNOLOGIES LTD.

Deferred Activation

Detect the Sandbox

Look for a Human

For Every Evasion There’s an Anti-Evasion



Malware goes to sleep

Sandbox accelerates the clock

Malware implements its own clock

…

Malware looks for a Sandbox

Sandbox emulate a physical CPU

Malware identifies the CPU emulator

…

Malware looks for a human

Sandbox imitates human behavior

Malware detects a “virtual human”

…

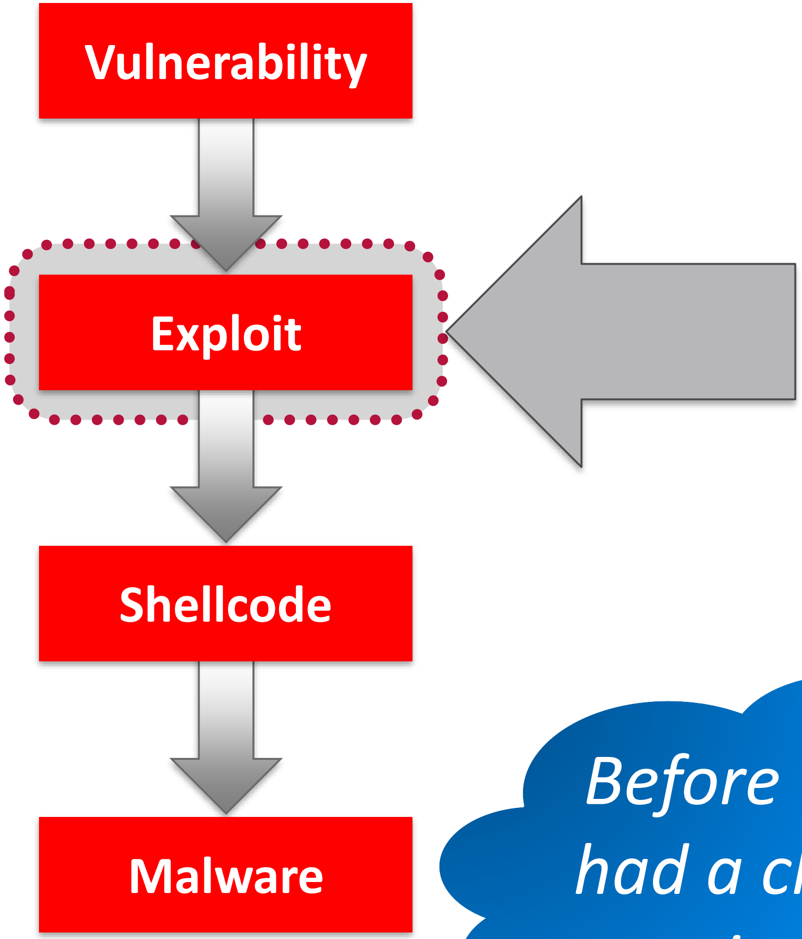
I’m a Defender – What CAN I Do?

Check Point
SOFTWARE TECHNOLOGIES LTD.

- ✗ Anti-Virus is **not enough**
- ✗ IPS is **not enough**
- ✗ Anti-Bot is **not enough**
- ✗ Even a regular Sandbox is **NOT ENOUGH**

I need a smarter technology that cannot be evaded…

Detect Where There is No Place to Hide



Identify the Exploit

Only a handful of exploit methods to keep up with

Before the attacker had a chance to use evasion techniques

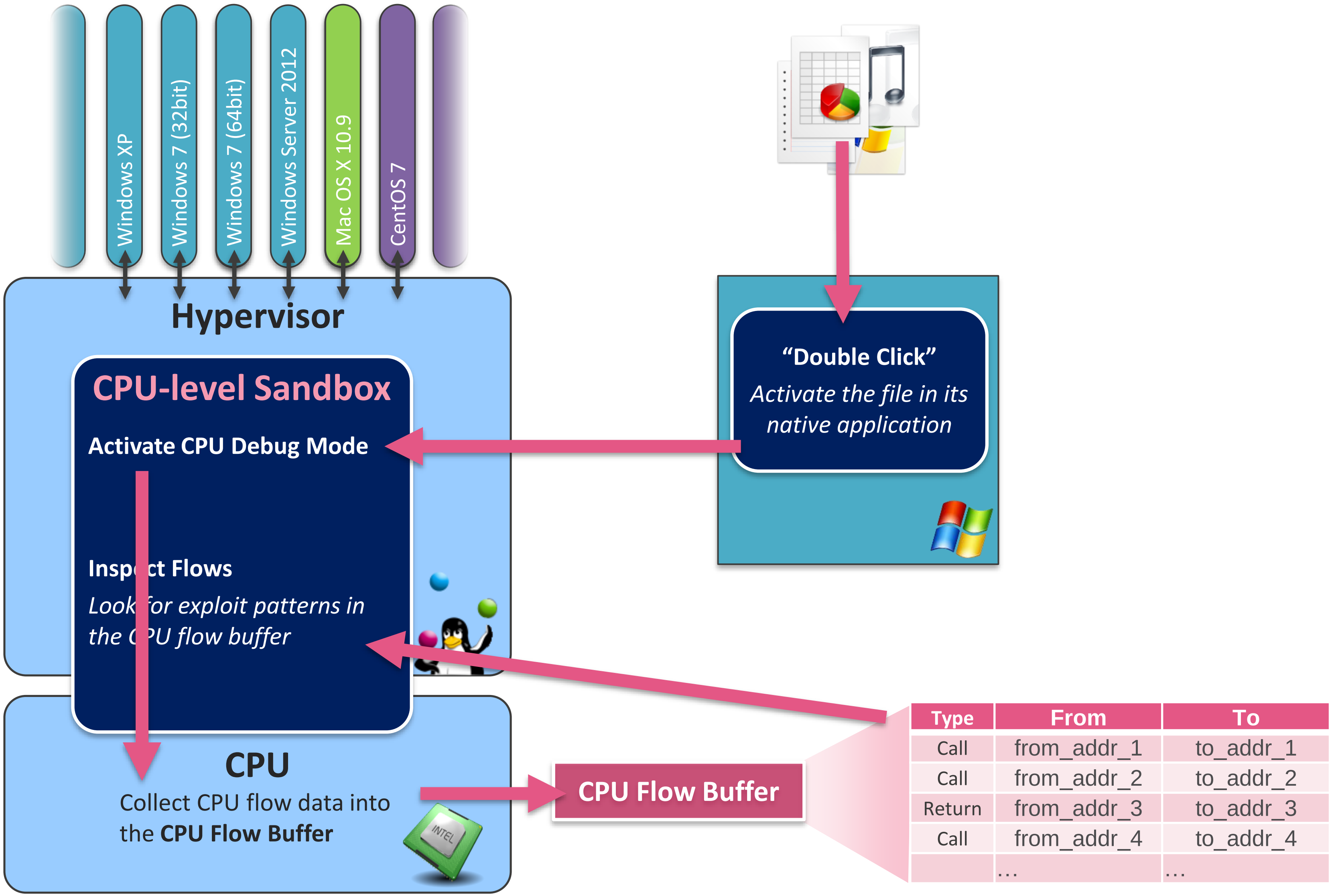
CPU-Level Sandbox Technology

Look for the **EXPLOIT**

~~Monitor the OS and look for abnormal activity~~

Monitor the CPU instructions flow and look for exploit patterns

Under the Hood: **CPU-Level Sandbox**



"Double Click"

Activate the file in its native application

Activate CPU Debug Mode

Inspect Flows

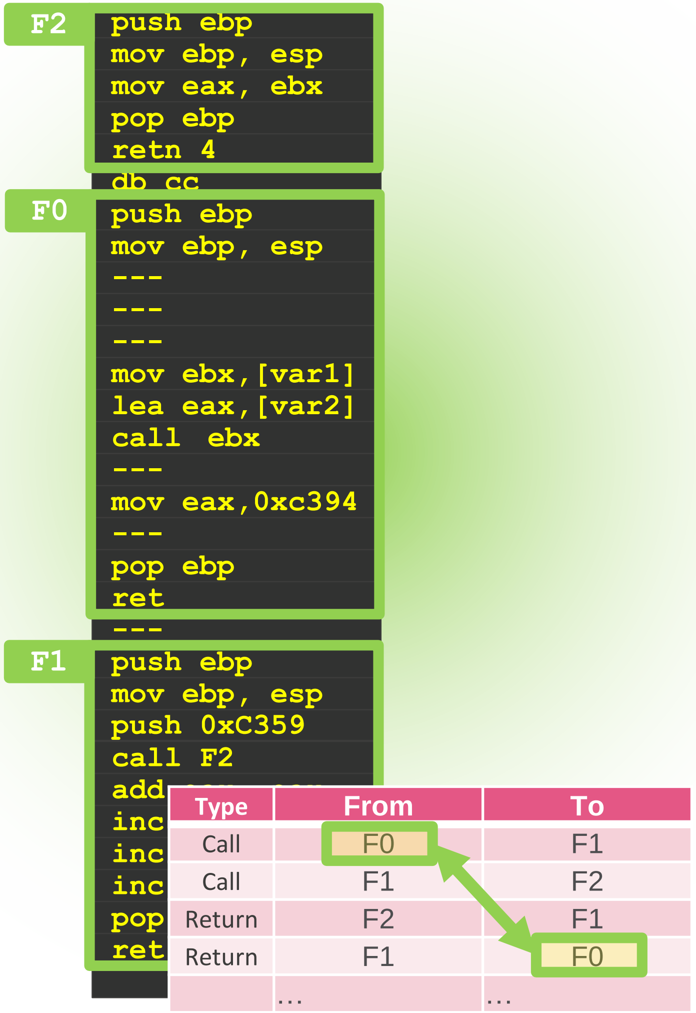
Look for exploit patterns in the CPU flow buffer

Collect CPU flow data into the **CPU Flow Buffer**

Type	From	To
Call	from_addr_1	to_addr_1
Call	from_addr_2	to_addr_2
Return	from_addr_3	to_addr_3
Call	from_addr_4	to_addr_4
	…	…

ROP in the CPU Flow Buffer

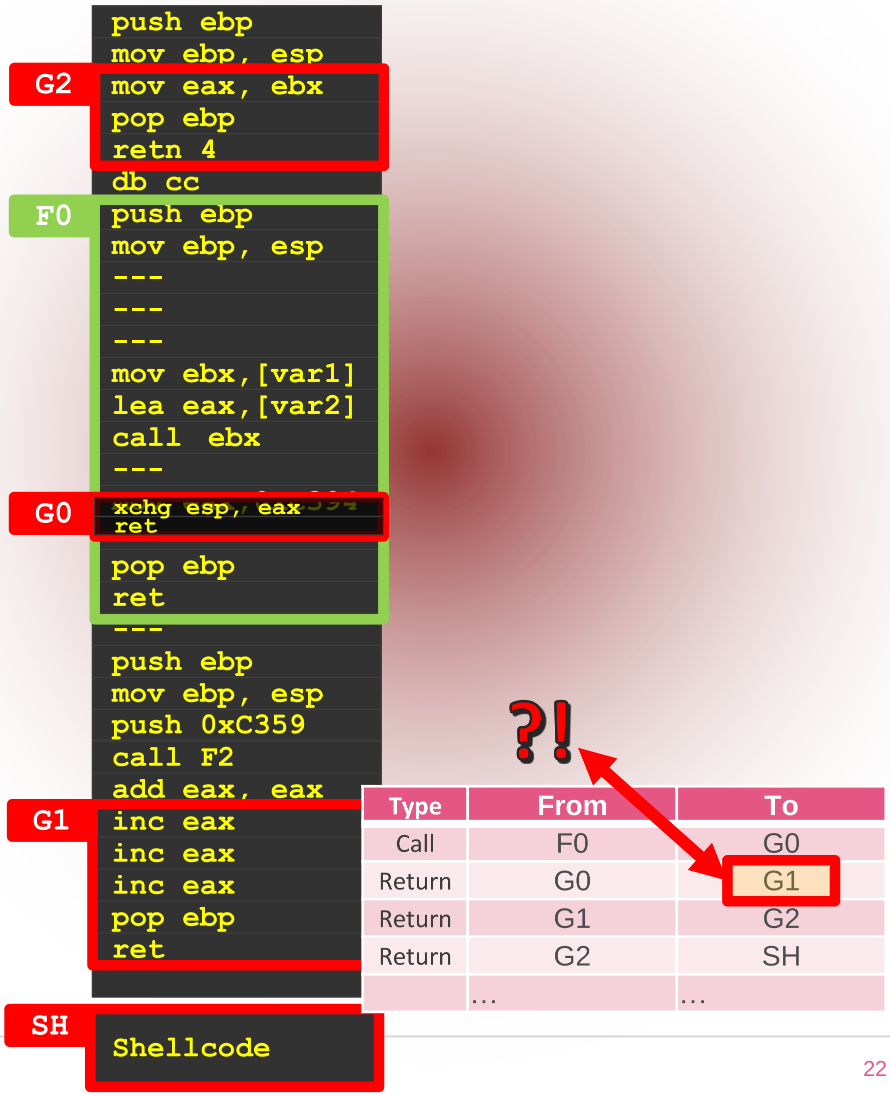
Normal Execution



```
F2  push ebp
    mov ebp, esp
    mov eax, ebx
    pop ebp
    retn 4
    db cc
F0  push ebp
    mov ebp, esp
    ---
    ---
    ---
    mov ebx,[var1]
    lea eax,[var2]
    call  ebx
    ---
    mov eax,0xc394
    ---
    pop ebp
    ret
    ---
F1  push ebp
    mov ebp, esp
    push 0xC359
    call F2
    add
    inc
    inc
    inc
    pop
    ret
```

Type	From	To
Call	F0	F1
Call	F1	F2
Return	F2	F1
Return	F1	F0
	…	…

ROP Execution



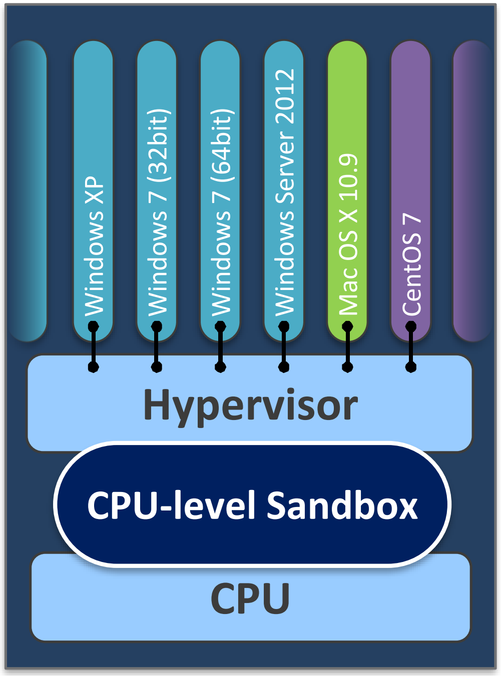
```
    push ebp
    mov ebp, esp
G2  mov eax, ebx
    pop ebp
    retn 4
    db cc
F0  push ebp
    mov ebp, esp
    ---
    ---
    ---
    mov ebx,[var1]
    lea eax,[var2]
    call  ebx
    ---
G0  xchg esp, eax
    ret
    pop ebp
    ret
    ---
    push ebp
    mov ebp, esp
    push 0xC359
    call F2
    add eax, eax
G1  inc eax
    inc eax
    inc eax
    pop ebp
    ret

SH  Shellcode
```

?!

Type	From	To
Call	F0	G0
Return	G0	G1
Return	G1	G2
Return	G2	SH
	…	…

CPU-Level Sandbox Technology Advantages

- **Highest accuracy**
  - No guesswork required, detection is definitive
  - Not based on heuristics or statistics
- **Evasion-resistant**
  - Detection occurs “outside” the Virtual machine
- **Efficient and fast**
  - CPU-level technology identifies the attack at its infancy



Check Point
SOFTWARE TECHNOLOGIES LTD.

THANK YOU!

Bill Nikolopoulos
Security Engineer, Greece and Cyprus