

### How secure am I with EMET?

Benedikt Tröster btroester@ernw.de









- IT-Security Service Provider
- Vendor-independent
- Based in Heidelberg
- Founded in 2001
- 40 Employees
- ¬ Troopers (<u>www.troopers.de</u>)
  - We invite you to come to Heidelberg ;)



Agenda

- About EMET
- Mitigation Techniques
- Demo
- EMET (5.1) Bypassing
- Demo
- Wrap-up



#### What is EMET?



- Application to further harden a Windows system (XP+)
- (Additional) GUI for system mitigation techniques
- Can be used to enforce certificate rules
  - Binding of SSL certificates to legitimate Root CAs
- Enables exploit protection features for applications
  - Stops program on detected exploit (or lists details)



#### What is EMET?

	Enhanced	Hitigation Experience Toolkit		- 8	×
Emport	1 mit 207	Quick Profile Name;	NZ w	Indows Event	Log
P. Papers		Reconvended security *	NO 10	ay Icon	
Export W	zerd Appe Trust	Skin: EMET Style *	V.	why Warreng	
144	CanAgaration	Tylter Settings		Reporting	
iystem Status					
Deta Exi	ecution Prevention (DEP)	<b>T</b>	Applicat	ion Opt In	
Studie	ed Ecosption Handler Over	rvrite Protection 😡	Applicat	ion Opt In	1
Address	Space Layout Randomzat	oon (ASUR)	Applicat	lari Opt 1n	
Cartifica	le Trust (Pereng)	<b>V</b>	Enabled		2
			Enabled		
Lunning Process			करतवन		
Lunneng Procese Procese 10	Process Name	<b>2</b>	करतवन	ming EHET	
Naming Process Process ID 1544	Process Name Class: - cyber Jack PC/		करतवन		1
Lunneng Procese Procese 10	Process Name Class: - cyber Jack PC/	plug-In Connection Center	करतवन		i
Process ID 1544 2316	Process Name goos: - cyber Jaol PC/ concent - Citris online carsa - Client Server Ru	plug-in Connection Center Intime Process	करतवन		i
Lanning Process Process ID 1544 2336 #60	Process Name cpoce: - cyber Jack PC/f concentr - Citmi onkne	plug-in Connection Center Intere Process Intere Process	करतवन		
Process ID 1544 2316 460 404	Process Name Galace - cyber Jack PC/6 concentr - Citris online carsa - Client Server Ru carsa - Client Server Ru	plug-in Connection Center Intene Process Intene Process I	करतवन		
Lanning Process ID 1544 2316 450 454 4242	Process Name cpose - cyber Jack PC/6 concentr - Citris online caras - Cient Server Ru caras - Cient Server R difficet - CCM Surrogal	plug-in Cannection Center antana Process antane Process # Monager	करतवन		
Lanning Process ID 1544 2316 450 454 4240 2460	Process Name ciposc - cyber Jadi PC/f concentr - Citris online carsa - Cient Server Ra difficat - COM Surrogal difficat - COM Surrogal dwm - Desktop Window	plug-in Cannection Center antane Process artime Process ii Monager gent	करतवन		
Process ID 1544 2316 450 454 4240 2460 1728	Process Name cpocer - cyber Jack PC/5 concentr - Citris online carsis - Cient Server Ru dRivet - COM Serrogal dwm - Desktop Window ENET_Agent - ENET_A	plug-in Cannection Center artime Process artime Process ii Manager gent	करतवन		
Process ID 1544 2316 454 454 4242 2466 1728 1744	Process Name cpoce - cyber Jack PC/ concentr - Citra online caras - Cient Server Ru citras - Cient Server Ru diffuet - COM Samopal dwm - Desktop Window ENET_Apent - ENET_AL BHET_GUT - ENET_CUT	olug-in Connection Center Intens Process Intens Process Intense Process Intense Manager gent Service	करतवन		

- Recommended settings are a good starting-point
- Applications that process untrustworthy data should be hardened:
  - Adobe Reader, MS Office, Wordpad, Java, Browser, E-Mail Clients, Instant Messanger, ZIP-Packer
- (Small) compatibility List is available online:
  - http://support.microsoft.com/kb/2909257



## What is EMET?

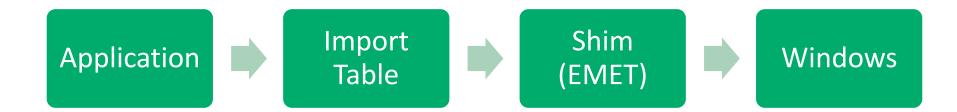
🗃 🗠		Application Configuration														
Export Selected	Add	(C) Applicatio		 Wildcard	Remov Select		now Full Path	Show All Settings	0	<u>S</u> top on e A <u>u</u> dit onl		$\checkmark$	Deep <u>H</u> o Anti <u>D</u> et Banned I	ours	;	
File		Add / Remove					Options			Default Action			Mitigation Settings			
							-	Find	Cle	ar						
App Name	•		SEHOP	NullP		EAF	EAF+	Man	Bott	LoadLib	Mem	Caller	SimE	Stac	ASR	
Acrobat.exe	•	$\checkmark$	$\checkmark$	$\checkmark$	$\checkmark$	$\checkmark$	EAF+	Man	Bott	LoadLib	$\checkmark$	$\checkmark$	$\checkmark$	$\checkmark$		
Acrobat.exe AcroRd32.exe	*	$\checkmark$	$\checkmark$	$\checkmark$	$\checkmark$	$\checkmark$	EAF+	Man	Bott	LoadLib	$\checkmark$	$\checkmark$	$\checkmark$	$\checkmark$		
Acrobat.exe AcroRd32.exe	•		$\checkmark$				EAF+	Man	Bott	LoadLib	$\checkmark$	$\checkmark$		√ √ √		
Acrobat.exe AcroRd32.exe EXCEL.EXE	•	$\checkmark$	$\checkmark$	$\checkmark$	$\checkmark$	$\checkmark$	EAF+	Man	Bott	LoadLib	$\checkmark$	$\checkmark$	$\checkmark$	$\checkmark$		
Acrobat.exe AcroRd32.exe EXCEL.EXE	*		$\checkmark$				EAF+	Man	Bott	LoadLib	$\checkmark$	$\checkmark$		√ √ √		
Acrobat.exe AcroRd32.exe EXCEL.EXE iexplore.exe	•						EAF+	Man	Bott							

- Applications can be added by:
  - Executable name/path
  - Wildcard (for different names)
- Protection settings can be configured per application



# How it works

- Works via Application Compatibility Framework
- Intercepts function calls
- Monitors and modifies the process





### EMET – Mitigations (1)



## Data Execution Prevention (DEP)

- Marks Stack and Heap as nonexecutable to prevent shellcode execution
- Structured Exception Handling
   Overwrite Protection (SEHOP)
  - Prevents exploitation of the exception handler to execute exploit code
  - Validates Exception Handlers



### EMET – Mitigations (2)



- Address Space Layout Randomization (ASLR)
  - Randomizes where modules will be loaded in memory to prevent prediction of mappings
- Bottom Up ASLR Security Mitigation
  - Bottom up allocations (e.g. VirtualAlloc(), VirtualAllocEx()) are now randomized
- NullPage Security Mitigation
  - Prevents code accessing to a NULL page



### EMET – Mitigations (3)



## - ASR (Attack Surface Reduction)

- A way to stop DLL plugins from loading into processes (e.g. block Flash from loading into Excel)
- Heapspray Allocation Security Mitigation
  - Prevents allocation of reoccurring typical code byte patterns (by preoccupying them)



#### Export Address Filtering(+)



## Prevents reading of critical APIs in the EAT

- Kernel32.dll
- Ntdll.dll
- Kernelbase.dll
- **+** 
  - Detects mismatch of stack and frame pointer registers
  - Detection of read access to MZ/PE header



#### **ROP Mitigations**



#### - Load Library Check

- Monitors LoadLibrary calls
- Prevents loading dlls from UNC paths (i.e. \\evil\my.dll)
- Memory Protection
  - Checks if VirtualProtect marks stack memory as executable
- Caller checks (32-bit only)
  - Critical functions can only be called via CALL (not RET)
- Stack Pivot
  - Checks if the stack pointer is within the threads upper and lower specified stack limit



### ROP Mitigations (2)



### - Deep hooks

- Protection of related functions of critical API calls
  - Kernel32!VirtualAlloc
    - Kernelbase!VirtualAlloc
    - Ntdll!NtAllocateVirtualMemory
- Anti detours
  - Prevents code from taking detours around hooked functions
- Banned functions
  - Allows to ban the use of API calls



# Demo





EMET 5.1 Bypassing – What to do?

Props to offensive-security.com!

struct FRAME {
 size;
 CONFIG;
 writable;

- Analysis of the EMET.dll shows:

- Encoded Pointer to a structure "FRAME"
- FRAME holds the enabled mitigations as a struct (CONFIG)
- Memory area is write protected



#### EMET 5.1 Bypassing – What to do?



### Pointer to the structure is encoded

- Decoding needed to resolve the address! (Can be found at EMET+0x67372)
- We can't write directly to the CONFIG/FRAME structure
  - Enable write access to the memory area first!



EMET 5.1 Bypassing – How to do it



- Find EMET.dll base address
- Call the decoding code at address EMET+0x67372
- Return into EMET+0x67372 and obtain the CONFIG address (EDX register)



EMET 5.1 Bypassing – How to do it



- Call ntdll!NtProtectVirtualMemory at CONFIG+0x1b8
  - Make CONFIG writeable
- Disable the EMET mitigations switch at CONFIG+0x558



# Demo





#### Conclusions



## EMET should be used in corporate environments

- Can be deployed fairly easy (e.g. via CMD)
- Manageable with low effort (ruleset updates)
- Adds findings to Windows Event Log
- (Mostly) reliable 0-day protection
- Protect outdated environments
- Cheap way to "raise the bar"



#### Conclusions



## - Drawbacks:

- May raise compatibility issues with applications
- Additional workload
- Surely no "perfect" solution
- Social engineering attacks impose a bigger threat than 0-day exploits



# There's never enough time...





#### Further links

- http://www.microsoft.com/emet
- <u>https://www.offensive-</u> <u>security.com/vulndev/disarming-and-</u> <u>bypassing-emet-5-1/</u>
- <u>https://prezi.com/z0kjt1wi\_9nl/ruxcon</u> \_2014-emet-50-armor-or-curtain/
- <u>http://casual-</u> scrutiny.blogspot.in/2015/03/defeating -emet-52-protections-2.html



# Disclaimer

All products, company names, brand names, trademarks and logos are the property of their respective owners!

