

### Monthly Research Investigation into EMET 4.0

FFRI,Inc. http://www.ffri.jp

Ver 2.00.01



## **About EMET**

- Enhanced Mitigation Experience Toolkit
- Vulnerability mitigation tool provided by Microsoft
- Latest version 4.0 was released in June 2013



## New/Updated Features in EMET 4.0

- Certificate Trust
  - New feature added in ver. 4.0. More strict verification of SSL certification on IE.
- Strengthened mitigations blocking known bypasses
  - Blocks bypassing ROP mitigations
  - Bans API used by bypassing ASLR, DEP
- Early Warning Programs
  - An option to report a set of information of an attack detected by EMET to Microsoft.
- Audit Mode
  - An option not to terminate process but only to make an alert when EMET detects an attack.

Focus on Certificate Trust and Strengthened mitigations on this slide



- This enables IE to check SSL certifications against more strict rules.
- This is a mitigation to Man in the Middle attacks of SSL communications
- Known problem about SSL certifications
  - Windows manages certifications collectively
  - There are multiple certifications as root CAs
  - Once the private key of one of the CAs is leaked (or occurs some errors in one of the organizations), fake certification may be created. (IE checks if the certification is signed by one of the root CAs to verify SSL certification chain.)
- Mitigation in EMET 4.0
  - Limit the root CAs permitted to sign the certification of a web site by setting the permitted CAs beforehand.



- Demonstration of actual workings
  - Prepare two certification authority for the demonstration.
  - Create certifications published by each CA.

	证明書 🛛 🗙	証明書
	全般  詳細  証明のパス	全般  詳細  証明のパス
	正明書の情報 この証明書の目的:	正明書の情報 この証明書の目的:
	・リモート コンピューターの ID を保証する	・リモート コンピューターの ID を保証する
	<b>発行先</b> : 192.168.1.181	<b>雅行先:</b> 192.168.1.181
Publisher	発行者: ca1.ffrijp 有効期間 2013/ 07/ 23 から 2014/ 07/ 23	<b>発行者:</b> ca2.ffri.jp 有効期間 2013/ 07/ 23 <b>から</b> 2014/ 07/ 23
	1-ε 3 30,891 μεα 2018/07/28 χμησ 2014/07/28	19,99,99/ma 2013/07/23 (0°) 2014/07/23
	発行者のステートメント(S) 証明書の詳細について表示します。	発行者のステートメンド(S)
	СОК	ОК

Certifications published to 192.168.1.181 by each CA.



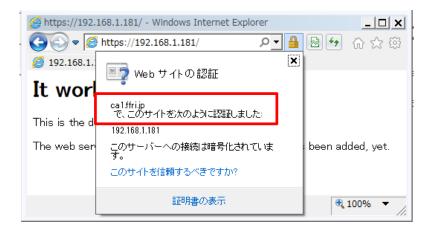
#### • Register both CAs as root CAs

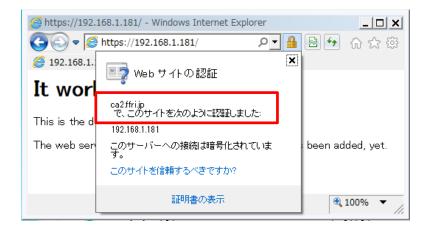
□ 証明書 - 現在のユーザー □ □ 個人 □ □ 信頼されたルート証明機関 □ □ □ □ 1000000000000000000000000000000	発行先 ▲ □ AddTrust External CA Root	発行者
<ul> <li>田 ニ エンタープライズの信頼</li> <li>田 中間証明機関</li> <li>田 ニ Active Directory ユーザー オブジェク</li> <li>田 ニ 信頼された発行元</li> <li>田 ニ サード パーティ ルート証明機関</li> <li>田 ニ サード パーティ ルート証明機関</li> <li>田 ニ 信頼されたユーザー</li> <li>田 ニ 証明書の登録要求</li> <li>田 ニ スマート カードの信頼されたルート</li> </ul>	Baltimore CyberTrust Root	Class 3 Public Primary Certific Copyright (c) 1997 Microsoft Cybertrust Global Root DigiCert High Assurance EV R Entrust.net Certification Auth Entrust.net Secure Server Cer Equifax Secure Certificate Aut GeoTrust Global eBusine GeoTrust Global CA GlobalSign Root CA Go Daddy Class 2 Certification Go Daddy Root Certificate Aut GTE CyberTrust Global Root http://www.valicert.com/ Microsoft Authenticode(tm) R Microsoft Root Authority





• Both certifications are accepted by IE as SSL certifications









• Configure EMET 4.0 to accept only a certification published by ca1.ffri.jp for a web site 192.168.1.181

Certificate Trust Configuration	<b>•</b> ^		Certificate Trust Config	guration	- 🗆 🗙
Export Add Rule Remove Rule	Export	G Add Website	Website		
File Add / Remove	File	Add / Re			
Protected Websites Pinning Rules	Protecte	ed <u>W</u> ebsites	Pinning <u>R</u> ules		
Y Find Clear				✓ Find	Clear
Name Certificates R Min A Bl P				Pin Rule	
MyRule         1 Certificate(s)         V         201         N/A         N/A         I           E=suzuki@ffri.jp, CN=ca1.ffri.jp, OU=CA1, O=FFRI, S=TOKYO, C=JP (d)         I		192.168.1.	181	MyRule	¥
<> Import Remove					
OK Close				<u>О</u> К	Close

Configure ca1.ffri.jp as a CA as "MyRule"

Set "MyRule" to web site 192.168.1.181





• Set iexplore.exe as a protected executable

			- 🗆 X					
Export	Export Selected	Add Application	Add Wildcard	Remove Selected	Show Full Path	Default Action +	<ul> <li>Deep <u>H</u>ooks</li> <li>Anti <u>D</u>etours</li> <li><u>B</u>anned Functions</li> </ul>	
	File	Ad	d / Remove		Options		Mitigation Settings	
– Mitigat	ions							
All     Memory     ROP     Other       Find     Clear								
A	pp Name			▲				
▶ ie	xplore.exe							
							<u>O</u> K <u>C</u> lose	

•



## **Certificate Trust**

Under the configuration when IE tries to communicate to 192.168.1.181 with the certification published by ca2.ffri.jp, EMET make an alert.

	What I have				
	<i>(intersection)</i> (intersection) (int	168.1.181/ - Windows Internet Explorer	<u> </u>		
	<b>OO</b> - <b>O</b>	https://192.168.1.181/	🗟 😏 🏠 🛠 戀		
	🥔 192.168.1.:				
	It worl	■🦻 Web サイトの認証			
	This is the d	ca2.ffri.jp で、このサイトを次のように認証しました: 192.168.1.181			
	The web ser	このサーバーへの接続は暗号化されていま す。	been added, yet.		×
_		このサイトを信頼するべきですか?			EMET 4.0 EMET detected that the SSL certificate for "192.168.1.181" is
		証明書の表示 	€ 100% ▼		not trusted by the rule "MyRule" associated with the domain "192.168.1.181"
			💐 A 般   🤞	? Сарз В Кана ▼	* 🍡 🗎 🕩 15:14 💻

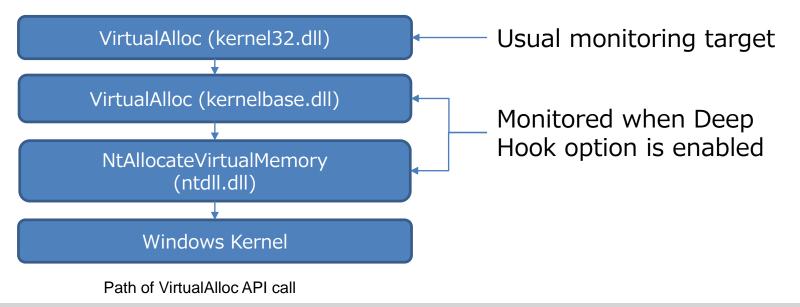
times It only makes an alert but does not block the communication





## **Strengthened Mitigations – Deep Hook**

- In previous ROP detection, one of the APIs EMET monitoring is VirtualAlloc in kernel32.dll.
- It can not detect ROP if a shellcode uses VirtualAlloc in kernelbase.dll or NtAllocateVirtualMemory in ntdll.dll
- Deep Hook option enables monitoring these APIs too.
- APIs which corresponds to other than VirtualAlloc are also monitored in the same manner.

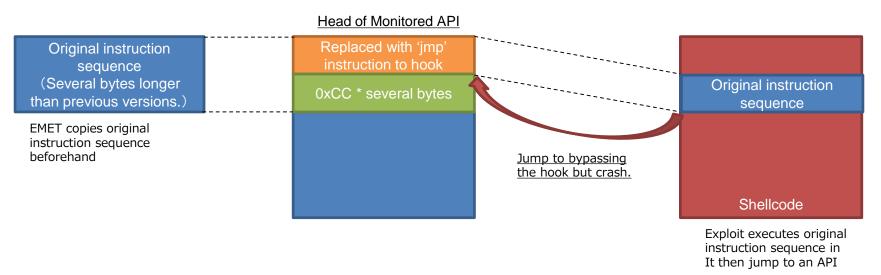






## **Strengthened Mitigations – Anti Detours**

- EMET uses API hook(rewriting head of API function) to monitor API calls.
- An exploit which bypasses API hook has been appeared
  - The exploit executes original head of API and jump to next to the rewritten head of API to bypass the hook.
- Anti Detours pads several bytes with 0xCC(which causes exception when executed) after the rewritten head of API for the hook. It makes the exploit fail.







## **Strengthened Mitigations – Banned API**

- Bypassing ASLR, DEP has been published in CanSecWest 2013 <u>http://cansecwest.com/slides/2013/DEP-ASLR%20bypass%2</u> <u>Owithout%20ROP-JIT.pdf</u>
- In the attack it uses LdrHotPatchRoutine in ntdll.dll
- When Banned API option is enabled specific APIs are banned to be called. (Only LdrHotPatchRoutine is the target in ver. 4.0)



## References

- <u>http://blogs.technet.com/b/srd/archive/2013/06/17/emet-4-</u> <u>0-now-available-for-download.aspx</u>
- <u>http://blogs.technet.com/b/srd/archive/2013/05/08/emet-4-</u> <u>0-s-certificate-trust-feature.aspx</u>
- <u>http://recon.cx/2013/slides/Recon2013-Elias%20Bachaalany-</u> <u>Inside%20EMET%204.pdf</u>



## **Contact Information**

E-Mail : <u>research—feedback@ffri.jp</u> Twitter: <u>@FFRI\_Research</u>