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

Certificate Trust

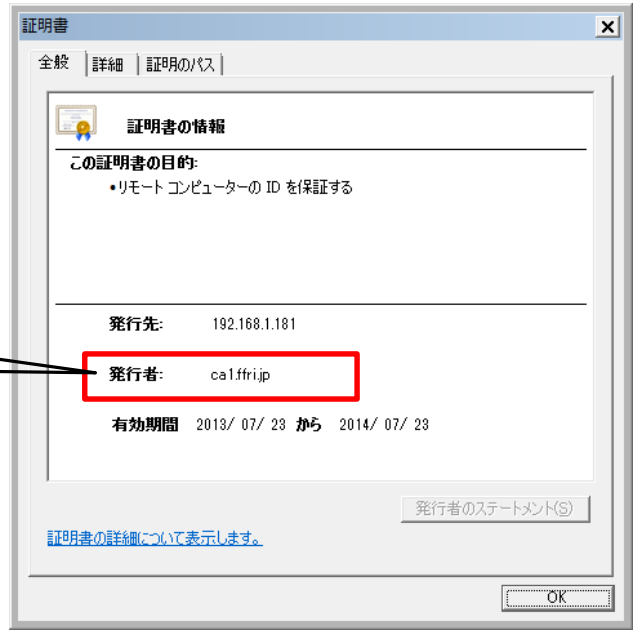
- This enables IE to check SSL certifications against more strict rules.
- This is a mitigation to Man in the Middle attacks of SSL communications

- 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.)

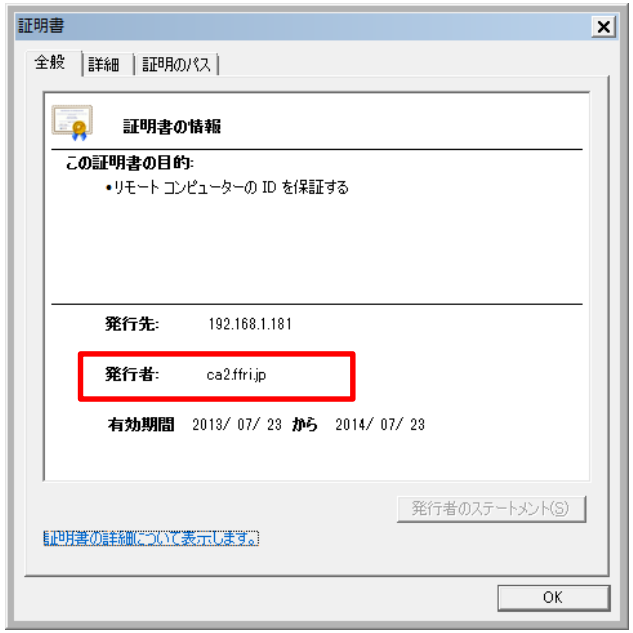
- Mitigation in EMET 4.0
  - Limit the root CAs permitted to sign the certification of a web site by setting the permitted CAs beforehand.

Certificate Trust

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



Publisher

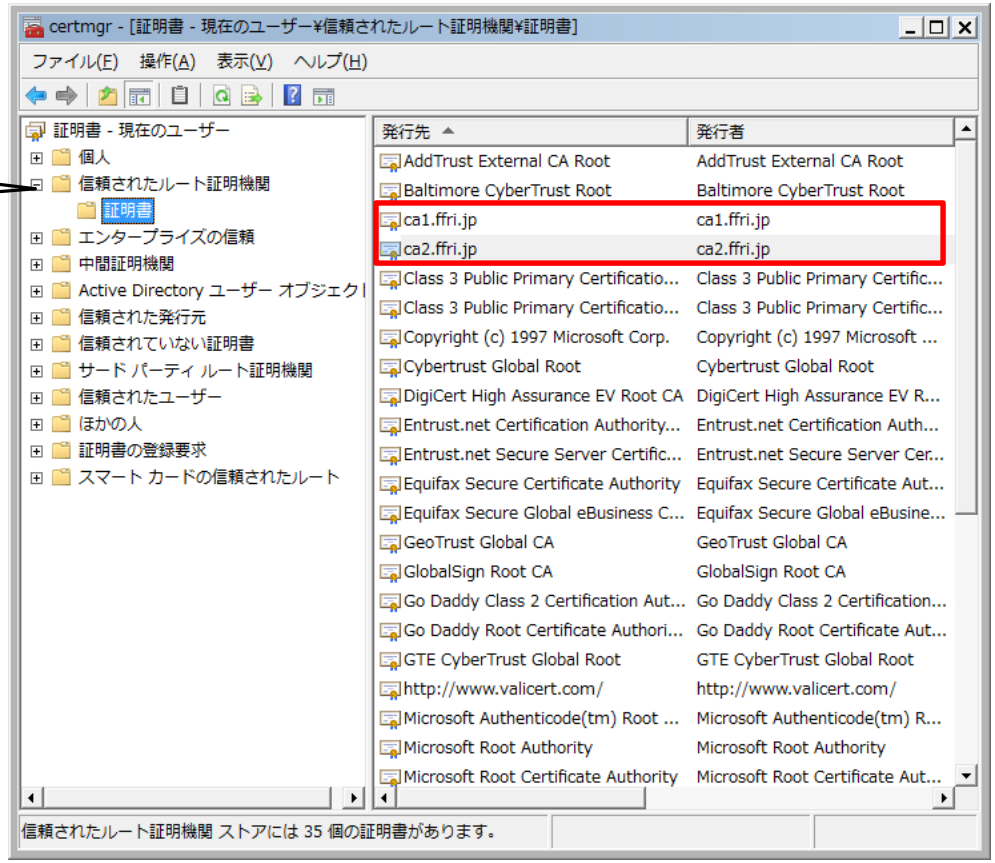


Certifications published to 192.168.1.181 by each CA.

Certificate Trust

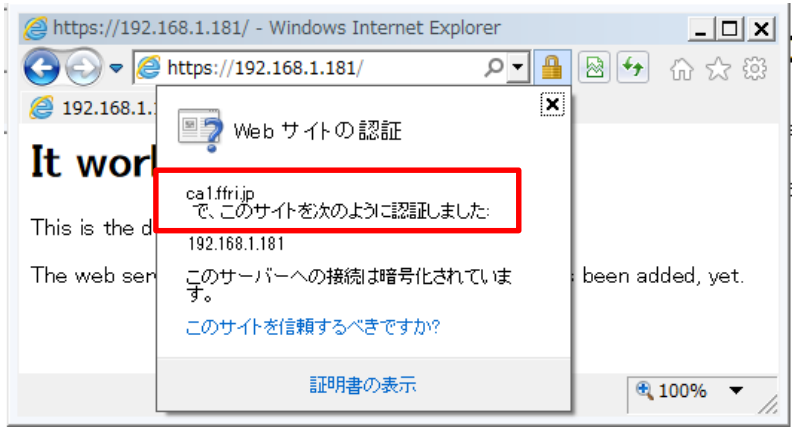
- Register both CAs as root CAs

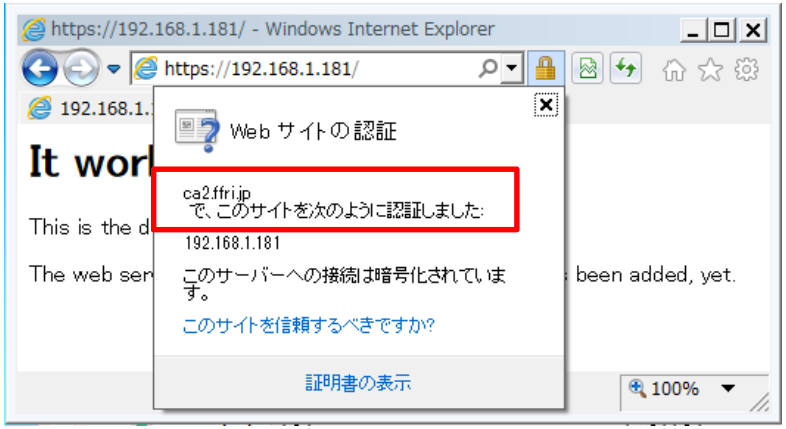
Trusted Root CAs



Certificate Trust

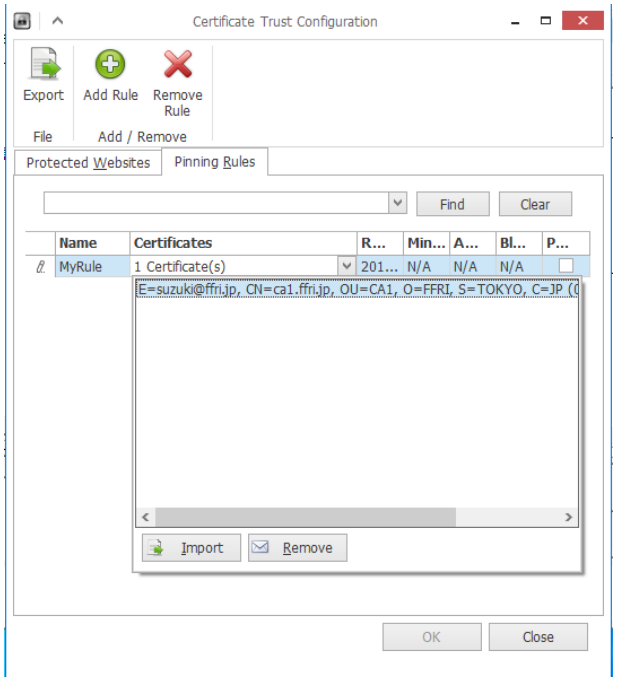
- Both certifications are accepted by IE as SSL certifications

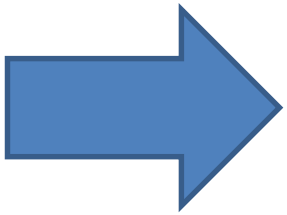


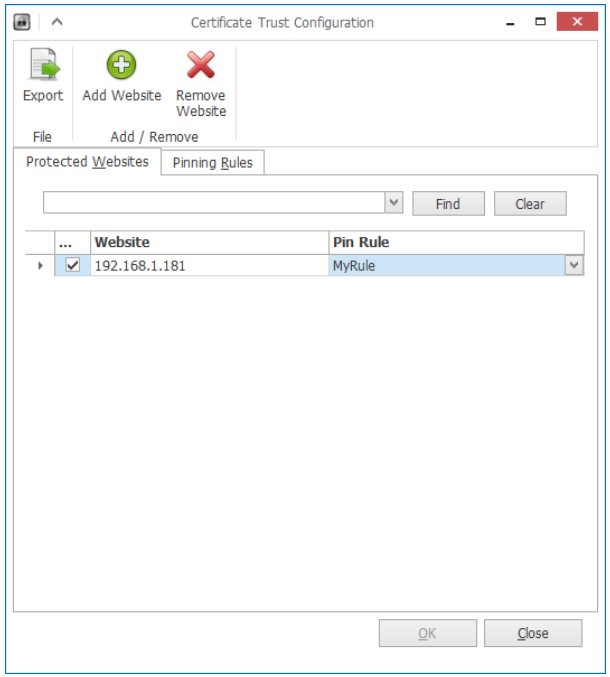


Certificate Trust

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





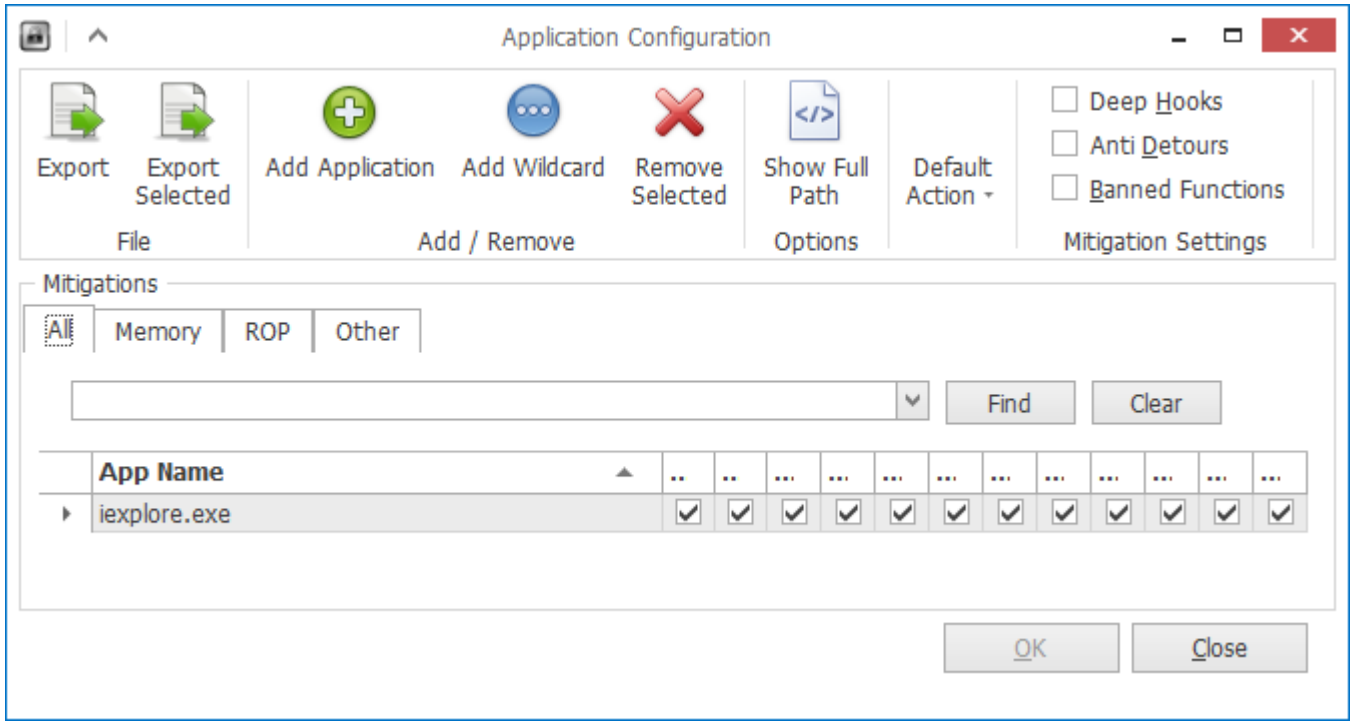


Configure ca1.ffri.jp as a CA as “MyRule”

Set “MyRule” to web site 192.168.1.181

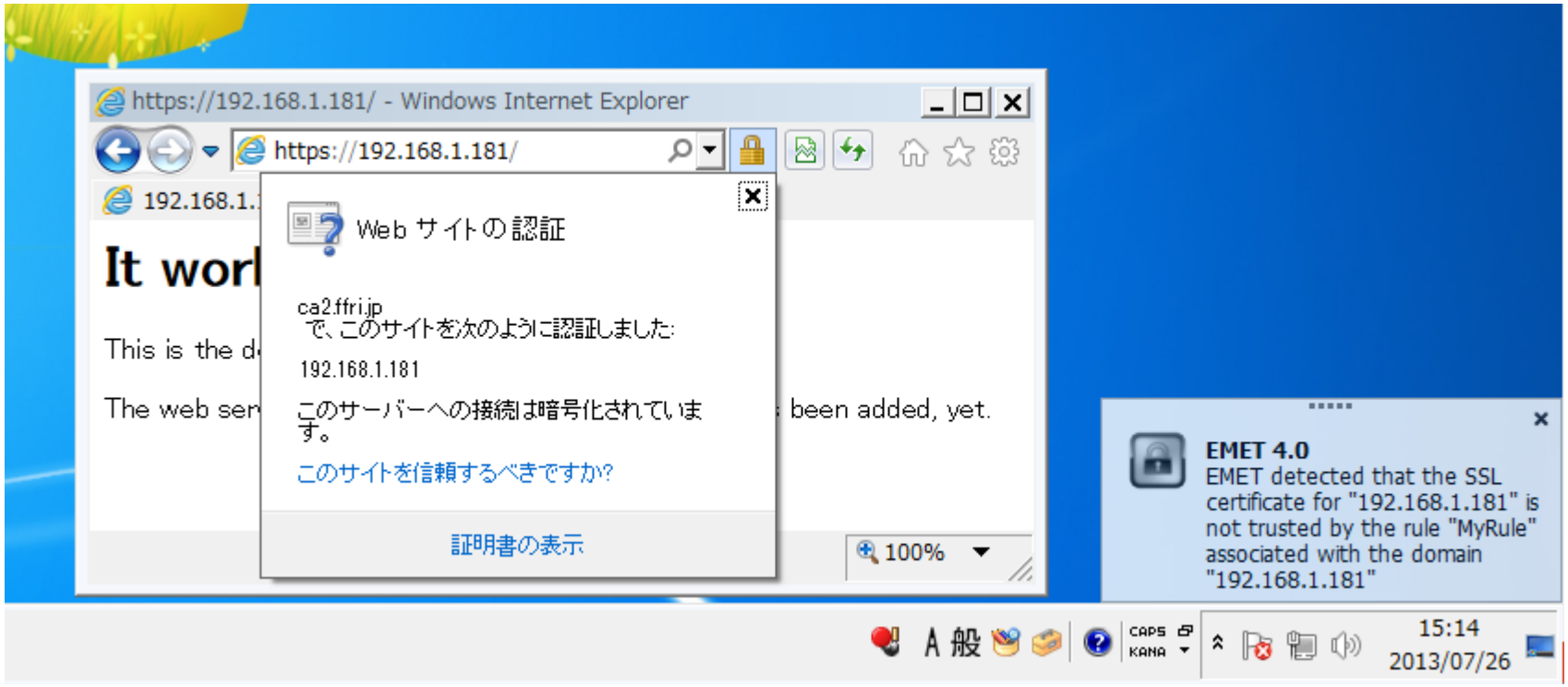
Certificate Trust

- Set iexplore.exe as a protected executable



Certificate Trust

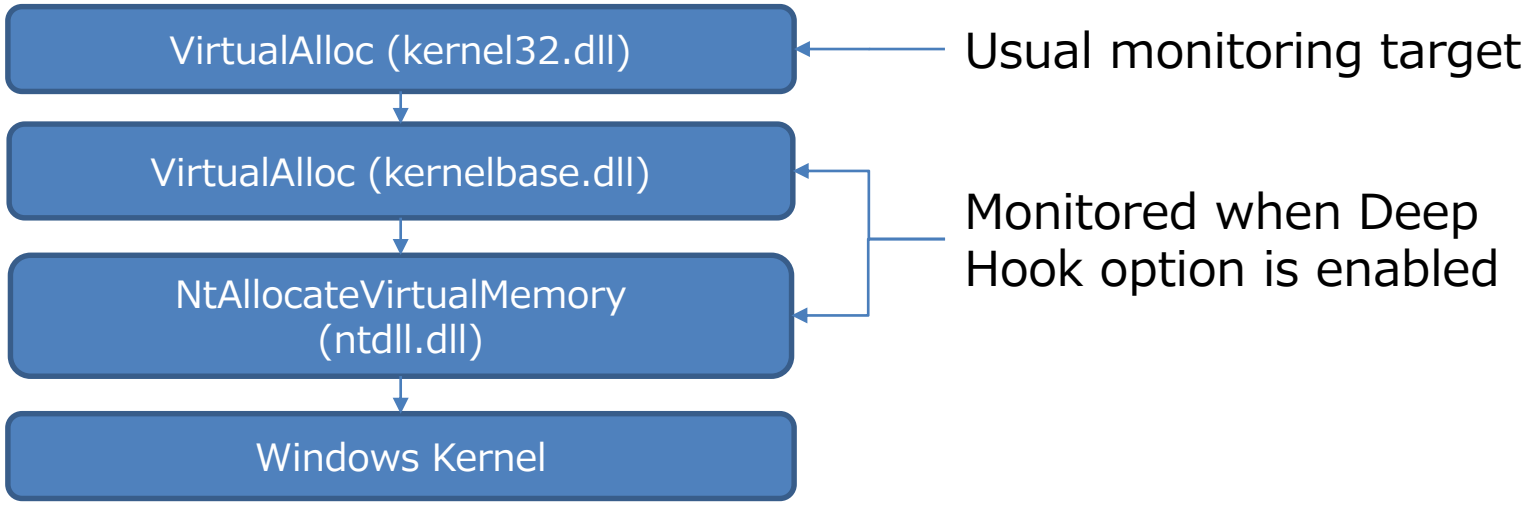
- Under the configuration when IE tries to communicate to 192.168.1.181 with the certification published by ca2.ffri.jp, EMET make an alert.



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

Strengthened Mitigations – Deep Hook

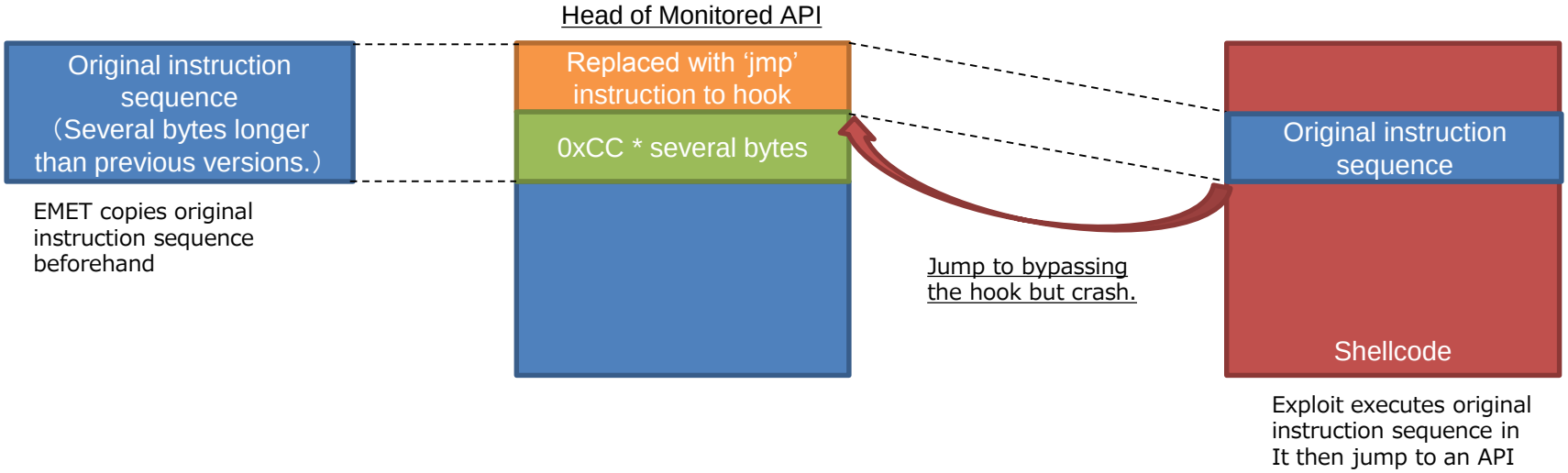
- In previous ROP detection, one of the APIs EMET monitoring is VirtualAlloc in kernel32.dll.
- It can not detect ROP if a shellcode uses VirtualAlloc in kernelbase.dll or NtAllocateVirtualMemory in ntdll.dll
- Deep Hook option enables monitoring these APIs too.
- APIs which corresponds to other than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



Path of VirtualAlloc API call

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 http://cansecwest.com/slides/2013/DEP-ASLR%20bypass%20without%20ROP-JIT.pdf
- 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

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

Contact Information

E-Mail ： research—feedback@ffri.jp
Twitter： @FFRI_Research