Monthly Research

EMET 4.0の調査

株式会社ＦＦＲＩ
http://www.ffri.jp

Ver 2.00.01

EMET概要

- Enhanced Mitigation Experience Toolkit
- マイクロソフトが提供する脆弱性緩和ツール
- 最新版4.0が2013年6月にリリース

EMET 4.0の主な新たな機能・更新

- Certificate Trust
  - 4.0で新たに登場した機能。IEのSSL証明書のより厳格な検証
- 脆弱性防御の強化、回避策のブロック
  - ROP対策を回避する手法をブロック
  - ASLR, DEPを回避する攻撃に利用されるAPI呼び出しの禁止
- Early Warning Programs
  - EMETが攻撃を検知した際に、その検知内容をMicrosoftに通知するようにできるオプション
- Audit Mode
  - EMETが攻撃を検知した際にプロセスを終了せず、アラートのみを上げるオプション

Certificate Trustおよび脆弱性防御の強化について今回は注目

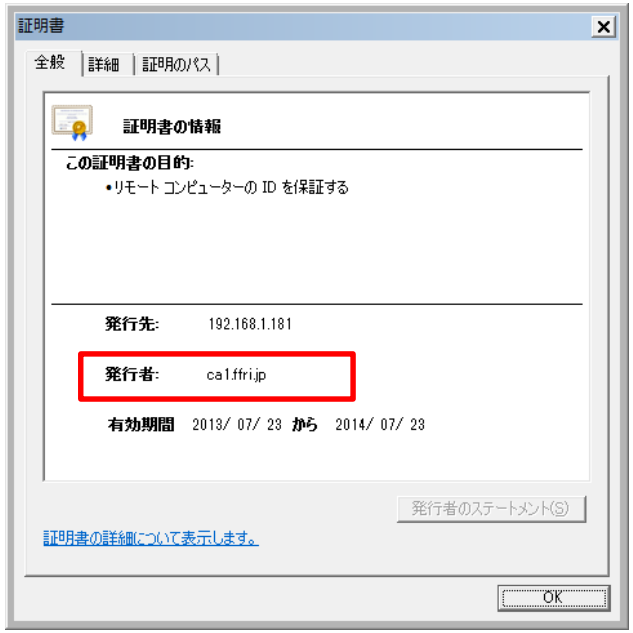
Certificate Trust

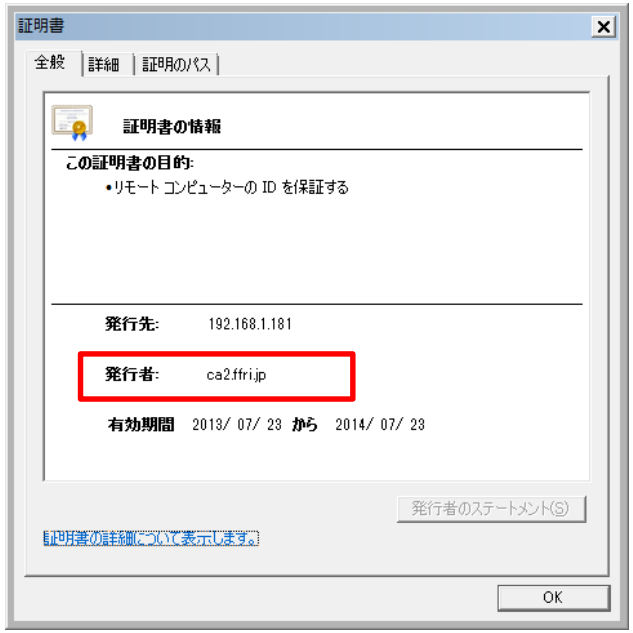
- Internet Explorerの証明書のチェックを厳格なルールにすることが可能
- SSL通信のMan in the Middle攻撃に対する対策

- これまでの問題
  - Windowsは証明書を一括管理
  - ルート証明機関として複数の証明書が登録されている
  - どれか一つのルート証明機関の秘密鍵が漏洩する（または証明機関に何らかの不備がある）と、偽のSSL証明書が作成される可能性がある。（IEのSSL証明書チェーンのチェックでは、信頼するルート証明機関の**いずれか**の署名があることを確認する）
- EMET 4.0での対策
  - 予め、特定のWebサイトのSSL証明書の署名として許されるルート証明機関を指定し、限定する

Certificate Trust

- 実際の動作について検証
  - 2つの認証局をテスト用に用意
  - それぞれから発行された証明書を作成

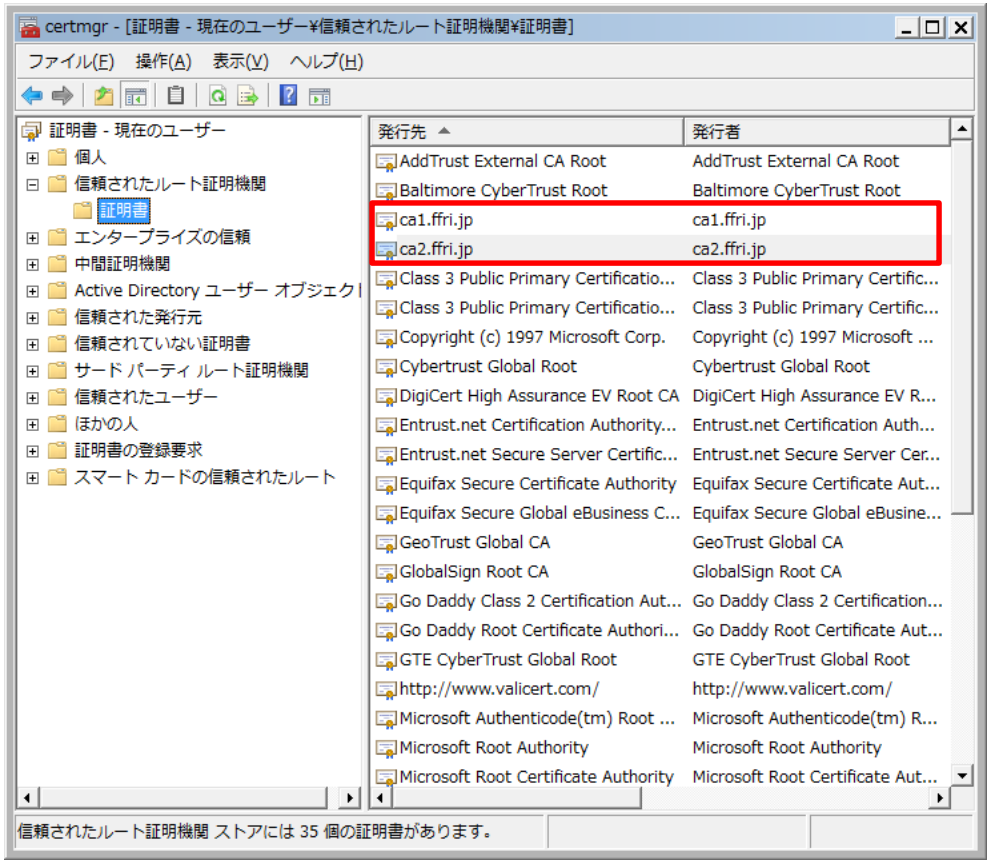




2つの認証局から192.168.1.181向けに発行された証明書

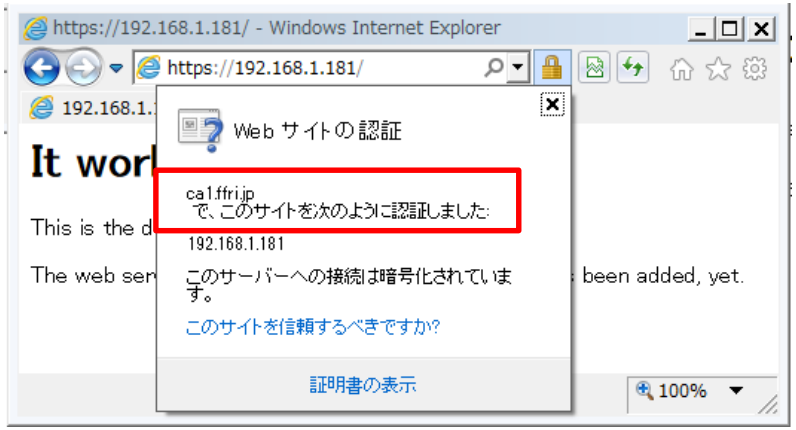
Certificate Trust

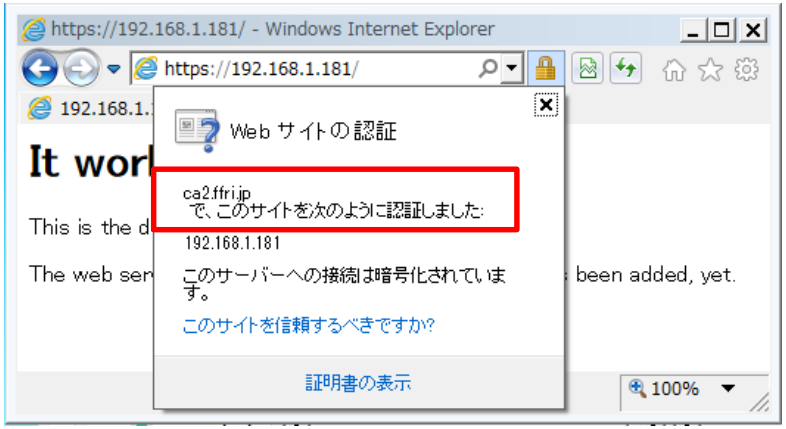
- 両テスト用認証局をルート証明機関として登録



Certificate Trust

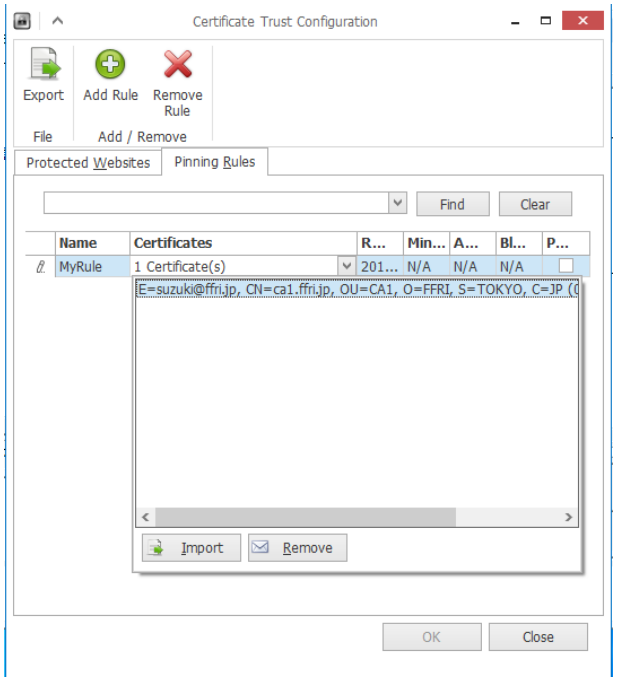
- どちらの証明書も、SSL証明書としてIEは問題なく受け付ける

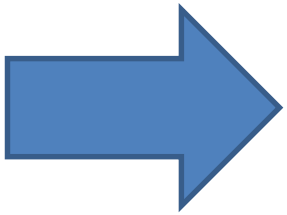


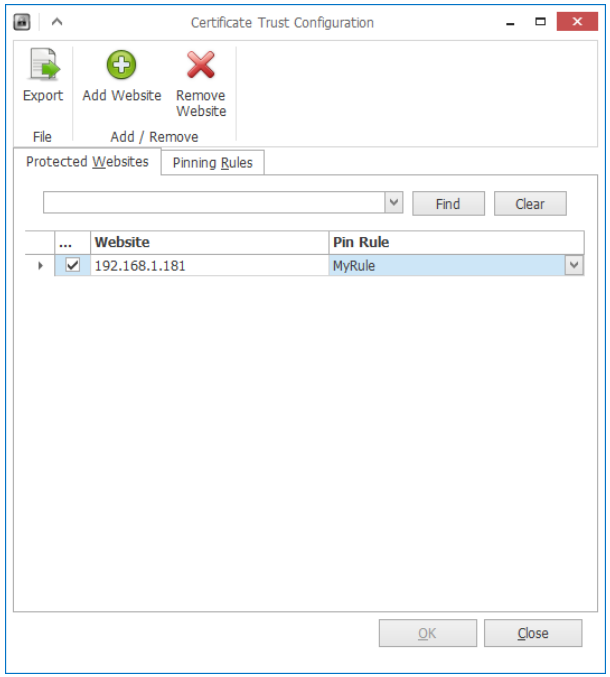


Certificate Trust

- EMET 4.0で、ca1.ffri.jpから発行された証明書のみを192.168.1.181で有効とみなすように設定





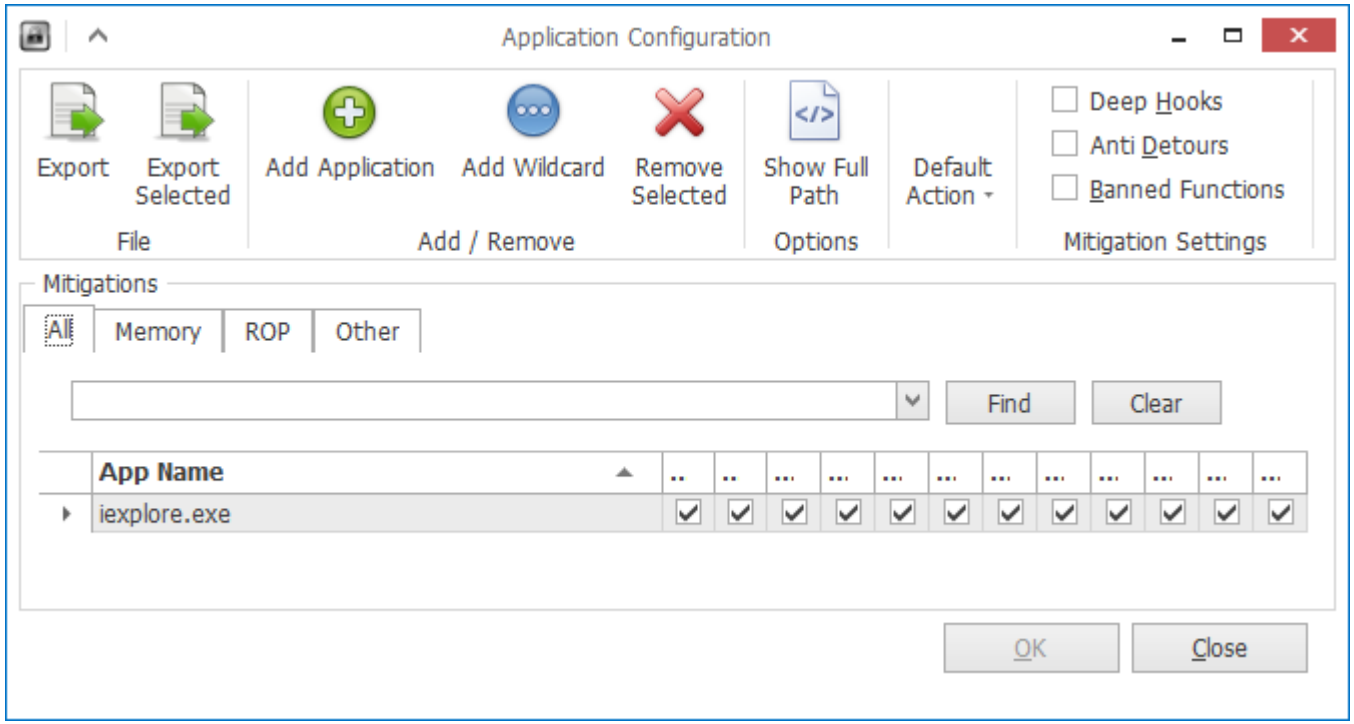


MyRuleとしてca1.ffri.jpを認証局として設定

192.168.1.181にMyRuleを設定

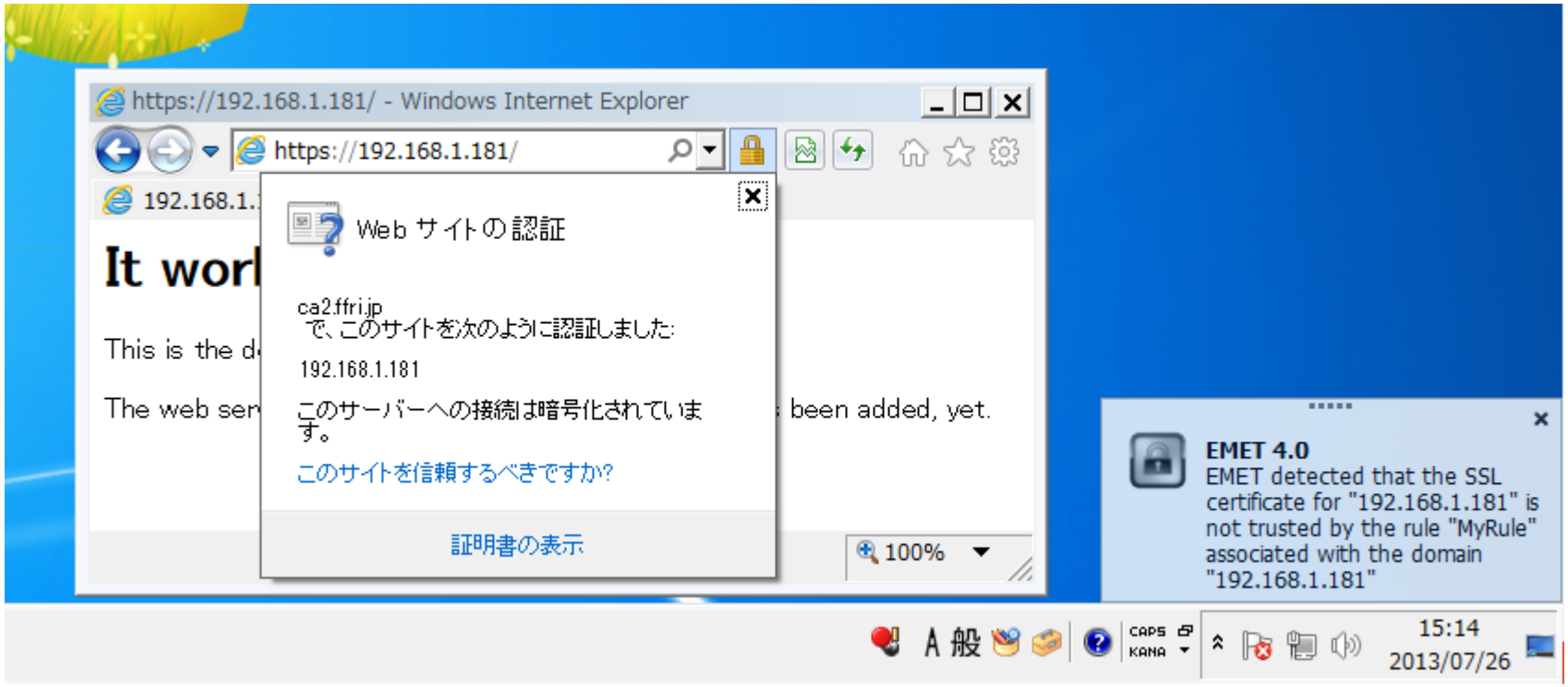
Certificate Trust

- iexplore.exeをEMETの保護対象に指定



Certificate Trust

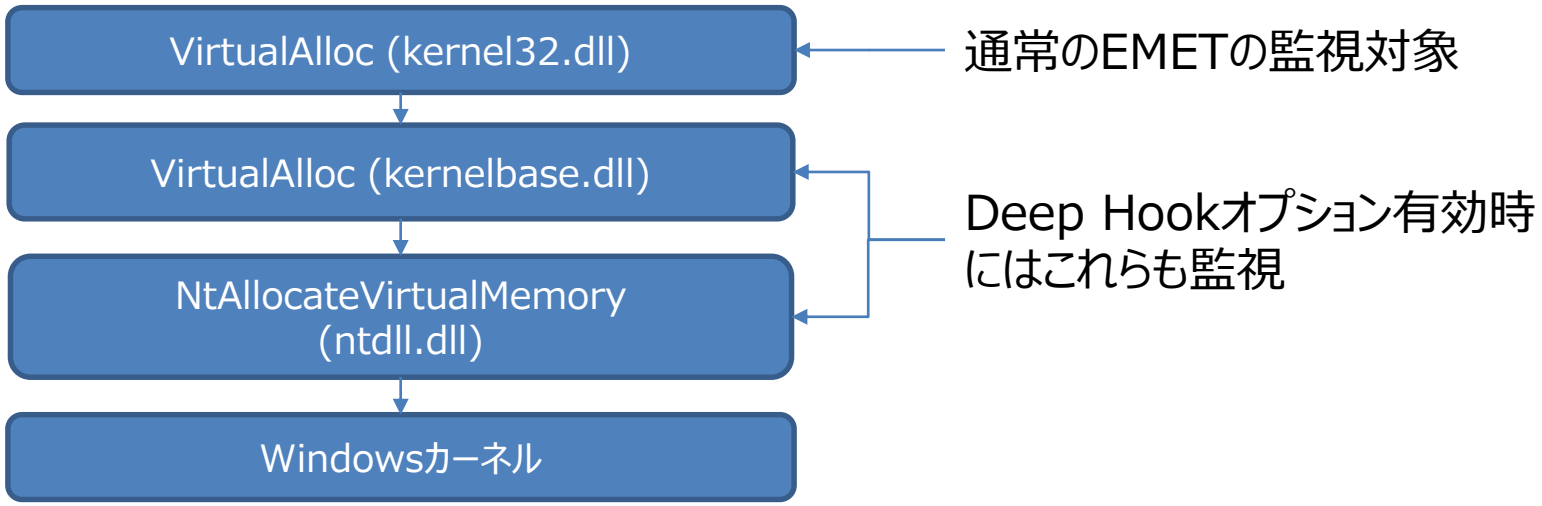
- IEでca2.ffri.jpの発行した証明書を利用して192.168.1.181と通信しようとした場合、アラートが表示される



※アラートの表示はあるが、ブロックはしない

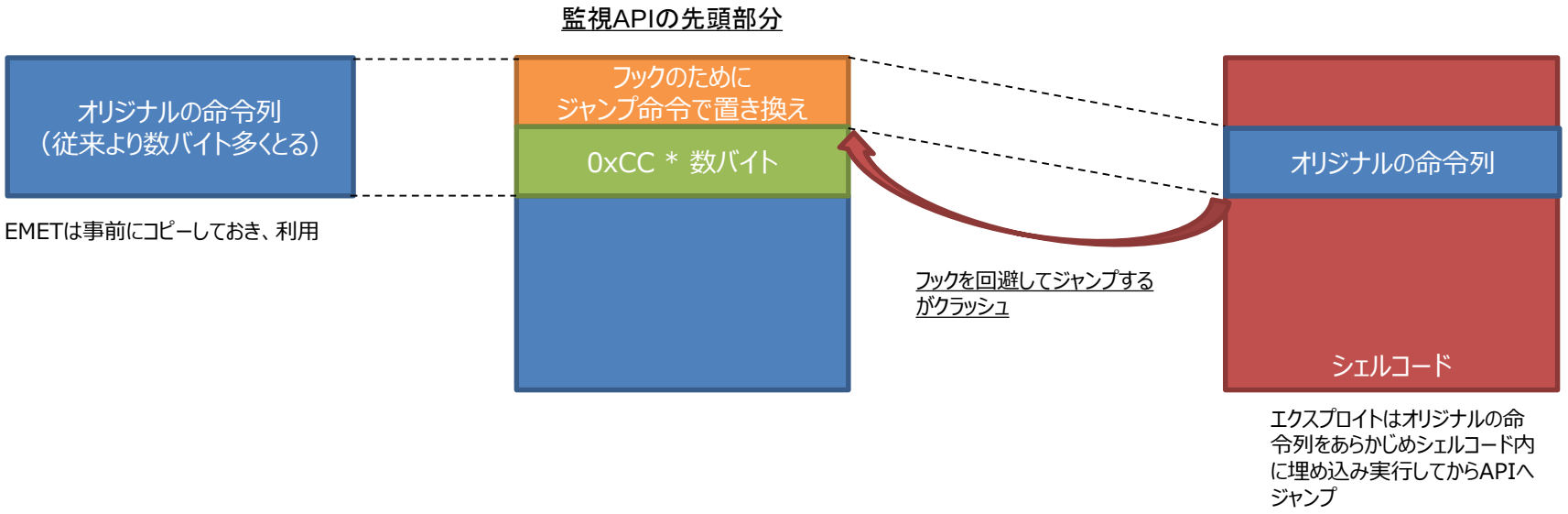
脆弱性防御の強化 – Deep Hook

- これまでのROP検知では、監視するAPIのひとつとしてkernel32.dll内のVirtualAlloc APIがあった。
- VirtualAllocより下位層のkernelbase.dll内のVirtualAllocまたは、ntdll.dll内のNtAllocateVirtualMemoryを直接利用された場合、検知できない
- Deep Hookオプションを有効にすることで、これらも監視
- VirtualAlloc以外の監視APIも同様に対応するAPIが監視される



脆弱性防御の強化 – Anti Detours

- EMETはAPIフックを利用（関数の先頭部分を書き換える）してAPI呼び出しを監視
- APIフックをバイパスするエクスプロイトが出現
  - シェルコード内で関数のオリジナルの先頭部分を実行してから、APIフックのために書き換えた部分をバイパスしてAPIへジャンプ
- Anti Detoursは書き換え部分の後、数バイト（ランダムな数）を0xCC（実行すると例外発生）で埋めることで、このエクスプロイトを失敗させる



脆弱性防御の強化 – Banned API

- CanSecWest 2013にて、ASLR, DEPをバイパスするエクスプロイト方法が発表された
  http://cansecwest.com/slides/2013/DEP-ASLR%20bypass%20without%20ROP-JIT.pdf
- その攻撃過程でntdll.dll内のLdrHotPatchRoutineが利用された
- Banned APIオプションを有効にすると、特定のAPI呼び出しが禁止される
  (4.0ではLdrHotPatchRoutineのみが対象となっている)

参考資料

- 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