Monthly Research

Windows 10 Technical Preview
セキュリティ機能概要

株式会社ＦＦＲＩ
http://www.ffri.jp

Ver 1.00.01

アジェンダ

- はじめに
- Windows Defender
- Project Spartan
- Control Flow Guard
- まとめと考察

はじめに

- 2015年3月30日に Windows 10 Technical Preview Build 10049 が公開された。

- 本資料では、Windows 10 Technical Preview Build 10041 および 10049 におけるセキュリティに関係する機能や仕様について概要を説明する。(調査はx64版で実施)

- 注意点：本資料の記載の内容は、Windows 10 正式リリース版では変更になる可能性がある。

Windows Defender

- アンチウイルスソフトが標準で搭載されている
  - Windows 7 では標準搭載の Windows Defender はスパイウェア対策ソフトだったが、Windows 10 では、スパイウェア以外のマルウェアも検出するアンチウイルスソフトに強化されている。
  - マルウェア検出は、パターンマッチング方式を核としている。
    - Microsoft Security Essentials 相当
    - Build 10041 では、Security Essentials 同様の UI に設定タブがあったが、Build 10049 では無くなり、OS のシステム設定 UI に統合されている (次頁参照)

Windows Defender の設定画面

- デフォルトで有効な3つの機能
- リアルタイム保護
  - リアルタイムスキャン機能
- クラウド保護
  - MAPS(Microsoft Active Protection Service)ベースの検出ファイルおよび関連するメタ情報のレポーティング機能
- サンプル自動送信
  - 検出ファイルの送信

Project Spartan

- Build 10049 で公開された IE を置き換える標準 Web ブラウザ
- バージョン 0.10.10049.0
- 現時点では、セキュリティに関して下記の設定が存在
  - ポップアップブロック
  - クッキーブロック
  - Do Not Track リクエスト
  - SmartScreen フィルター
  - アドオン
    - Flash Player が標準でインストールされている。
    - バージョン 17.0.0.134 Active X 版
- User-Agent
  - Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/39.0.2171.71 Safari/537.36 Edge/12.0

Project Spartan 関連プロセス（１）

- svchost.exe の子プロセスとして、spartan.exe と browser_broker.exe が実行される。
- spartan.exe と browser_broker.exe の子プロセスとして、spartan_edge.exe が実行される。
- プロセスの Integrity Level は、browser_broker.exe, WebCache.exe が Medium でその他は AppContainer
- Flash を含むページを表示すると FlashUtil_ActiveX.exe が実行される。
- JavaScript エンジンは Chakra.dll (IEと同じ)

Project Spartan 関連プロセス（２）

- IE と異なり、ブラウザ関連プロセスが 64bit プロセスとして実行される。
- そのため、32bit マルウェアからのコードインジェクションは不可能と考えられる
  - 64bit マルウェアが増えることが懸念される

svchost.exe		4,288 K	14,520 K	576	Windows サービスのホスト プロセス	
ShellExperienceHost.exe	0.02	16,456 K	47,584 K	2636	Windows Shell Experience Host	64-bit AppContainer
ApplicationFrameHost.exe		11,984 K	35,560 K	2736	Application Frame Host	64-bit Medium
RuntimeBroker.exe		9,836 K	34,980 K	2800	Runtime Broker	64-bit Medium
searchui.exe		30,920 K	73,848 K	2836		64-bit AppContainer
WSHost.exe		4,280 K	17,460 K	3036	Store Broker	64-bit Medium
spartan.exe	0.04	27,292 K	24,784 K	2808		64-bit AppContainer
spartan_edge.exe	0.01	42,136 K	24,168 K	3916	Spartan	64-bit AppContainer
spartan_edge.exe	0.01	9,692 K	3,768 K	3168	Spartan	64-bit AppContainer
browser_broker.exe		3,292 K	20,444 K	3104	Browser_Broker	64-bit Medium
spartan_edge.exe	0.30	95,536 K	114,960 K	3896	Spartan	64-bit AppContainer
spartan_edge.exe	0.63	78,168 K	117,664 K	3200	Spartan	64-bit AppContainer
spartan_edge.exe	0.01	31,668 K	74,572 K	5008	Spartan	64-bit AppContainer
ImeBroker.exe		3,072 K	12,600 K	3172	Microsoft IME	64-bit Medium
FlashUtil_ActiveX.exe		3,284 K	12,116 K	2940	Adobe® Flash® Player Utility	64-bit Medium

Control Flow Guard

- 2014年12月 の FFRI Monthly Research でとりあげた Control Flow Guard が有効になっている実行モジュールを調査

- 多くのシステムコンポーネントで Control Flow Guard が有効になっている。下記に一部のコンポーネントを示す。
  - Spartan
    - spartan_edge.exe, spartan_legacy.exe browser_broker.exe
  - IE
    - iexplore.exe
  - Flash
    - Flash.ocx, FlashUtil_ActiveX.exe, FlashUtil_ActiveX.dll

まとめと考察

- Windows 10 でも OS 標準の基本的セキュリティ機能が強化されている
  - Windows Defender
  - Project Spartan
  - Control Flow Guard

- Windows 10 が PC だけでなく、スマートデバイスや IoT デバイスにて利用されれば、PC で培われたセキュリティ機能がそのまま利用可能で、効率的である。

- 一方で、PC 以外のデバイスにもマルウェアの脅威が広がるリスクがある。

Contact Information

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