Monthly Research

Windows 10 Technical Preview Security Overview

株式会社ＦＦＲＩ
http://www.ffri.jp

Ver 1.00.01

Agenda

- Background
- Windows Defender
- Project Spartan
- Control Flow Guard
- Conclusions

Background

- Windows 10 Technical Preview Build 10049 has been published on March 30, 2015.

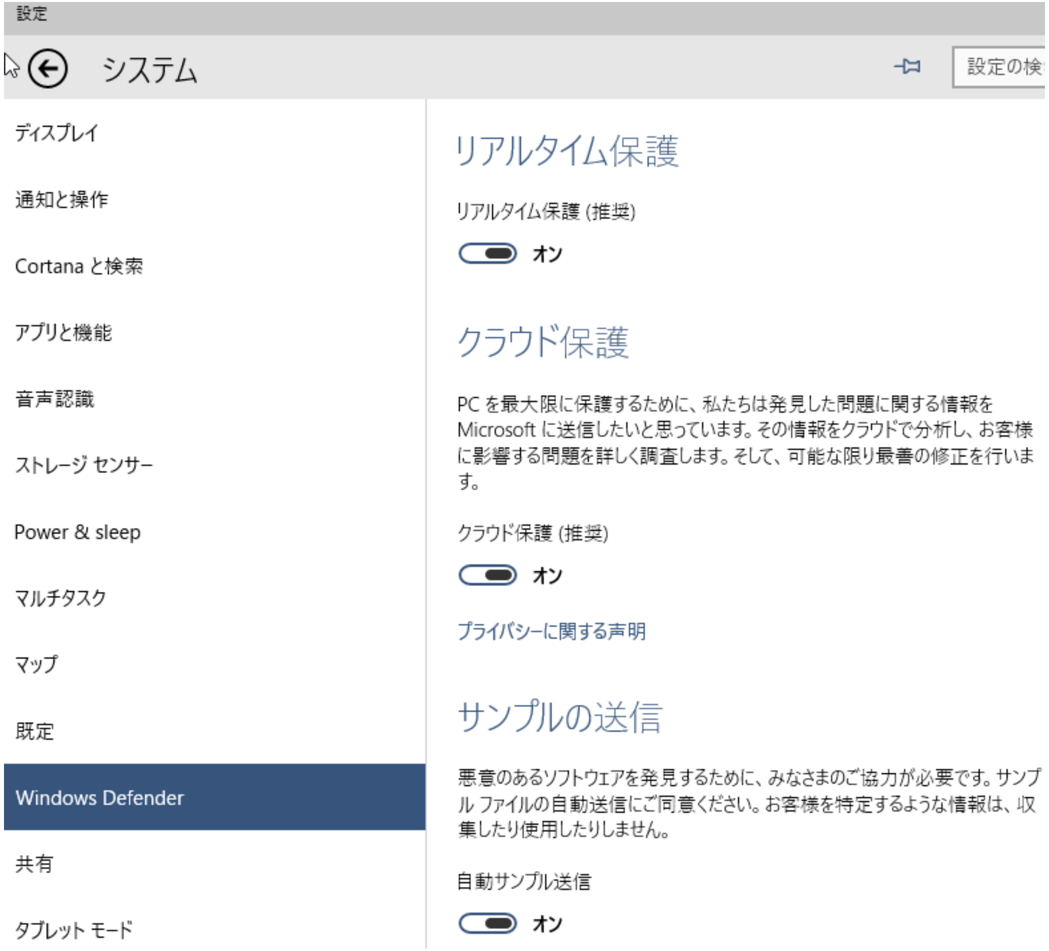
- In this report, we describe overview of security features in Windows 10 Technical Preview Build 10041 and 10049. (We tested x64 version)

- Note: The items described in this report, there is likely to be changed in the Windows 10 official release.

Windows Defender

- Anti-virus software is a standard feature
  - Windows 7: Windows Defender was anti-spyware
  - Windows 10: It has been enhanced to anti-virus
    - Equivalent to the Microsoft Security Essentials
    - Its malware detection is based on pattern matching
    - In Build 10041, there was a Settings tab to Security Essentials similar UI, In Build 10049, it is removed, it is integrated with a system config UI.

Windows Defender Config UI



リアルタイム保護

リアルタイム保護 (推奨)

● オン

クラウド保護

PC を最大限に保護するために、私たちは発見した問題に関する情報を Microsoft に送信したいと思っています。その情報をクラウドで分析し、お客様に影響する問題を詳しく調査します。そして、可能な限り最善の修正を行います。

クラウド保護 (推奨)

● オン

プライバシーに関する声明

サンプルの送信

悪意のあるソフトウェアを発見するために、みなさまのご協力が必要です。サンプル ファイルの自動送信にご同意ください。お客様を特定するような情報は、収集したり使用したりしません。

自動サンプル送信

● オン

- Three default functions
- Real Time Protection
- Cloud Protection
  - Reporting file-meta info based on MAPS(Microsoft Active Protection Service)
- Automatic sample submission

Project Spartan

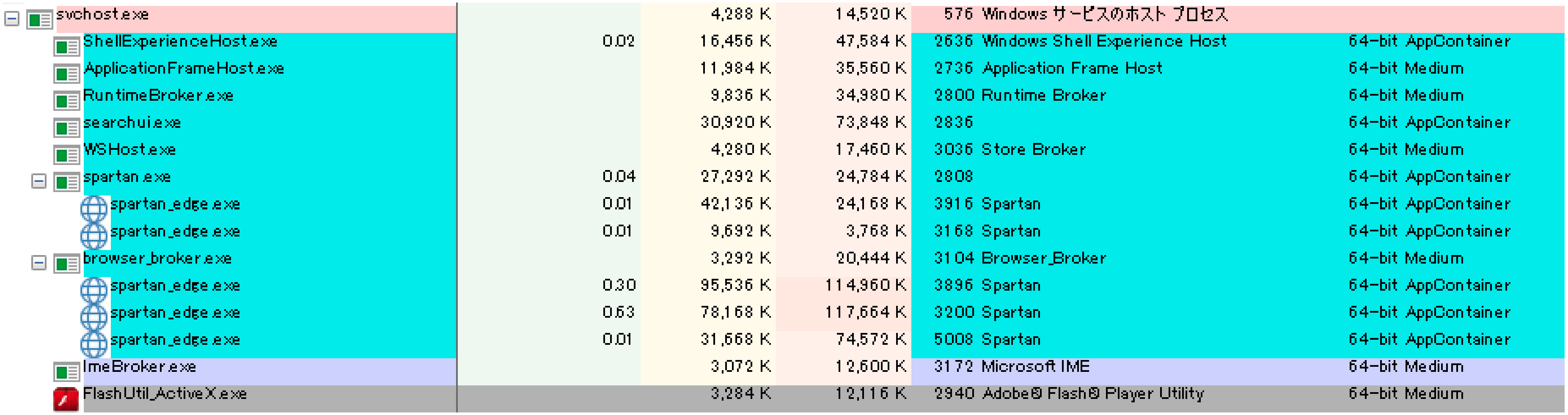
- Standard Web browser to replace the IE that has been published in Build 10049
- Version 0.10.10049.0
- At this time, the following settings are present for security
  - Popup block
  - Cookie block
  - Do Not Track Request
  - SmartScreen Filter
- Add-on
  - Flash Player is installed by default
  - Version 17.0.0.134, Active X
- 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 related processes

- spartan.exe and browser_broker.exe is executed as a child process of svchost.exe
- spartan_edge.exe is executed as child process of spartan.exe or browser_broker.exe
- Integrity Level
  - browser_broker.exe, WebCache.exe => Medium
  - others => AppContainer
- FlashUtil_ActiveX.exe is executed when you view a page that contains Flash
- JavaScript engine is Chakra.dll

Project Spartan related processes

- Browser-related processes are performed as a 64bit process
- Therefore, code injection from 32bit malware would be impossible
  - There is a possibility that 64bit malware increase



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

- We found executable modules which is enabled Control Flow Guard.
  - cf. FFRI Monthly Research of Dec. 2014

- Control Flow Guard is enabled on many of the system components
  - Spartan
    - spartan_edge.exe, spartan_legacy.exe browser_broker.exe
  - IE
    - iexplore.exe
  - Flash
    - Flash.ocx, FlashUtil_ActiveX.exe, FlashUtil_ActiveX.dll

Summary and Discussion

- Standard security features have been enhanced even Windows 10
  - Windows Defender
  - Project Spartan
  - Control Flow Guard
- If Windows 10 is used in smart devices and IoT devices, Security features that were developed for PC is directly available
- On the other hand, there is a risk of malware threats spread to various devices

Contact Information

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