L-019

危険な挙動を引き起こす可能性がある USB の検知方法の提案
A Proposal of Suspicious USB Detection Method

西山 魁人† 鈴木 海斗† 田中 雅浩†
Kaito Nishiyama Kaito Suzuki Masahiro Tanaka
松田 健† 園田 道夫‡
Takeshi Matsuda Michio Sonoda

1. はじめに

外部とのデータのやりとりには USB メモリーが利用される場面は多く，その際に想定されるセキュリティに関するリスクについては一定のユーザには認識されていると考えられるものの，その意識は希薄になっていることも念頭に置きながらセキュリティの対策を講じていく必要があるといえる．文献[1]は配布された USB が使用されるかどうかを調査したものであり，およそ半数のユーザが端末で中身のファイルをクリックしたと報告している．USB を悪用した脅威としてはマルウェアの感染や，Bad USB による第三者による端末のユーザが意図しない不正な操作などが考えられる．いずれの場合も，現状では多くのユーザがこのような USB を悪用した攻撃の被害に遭遇した場合，その瞬間にそういう事態に陥ったことに気付くことや，その時点で攻撃に気付くことは難しいと考えられる．そこで本研究では，何らかの仕掛けがある USB と何もデータが含まれていない USB のファイルの中身を解析し，USB を用いた攻撃に対する検知や防御に関する方法について検討する．

2. 従来研究

USB のセキュリティに関する従来研究には，BMC ベースのファイルシステムによってアプリケーションがリソースを直接管理することで OS やカーネルに関わる脅威を排除する方法[2]や，PC の周辺機器接続に関わるセキュリティリスク分析のアセット導出方法[3]が提案されている．本研究では，USB メモリー自体が持つ情報を解析するとこで，不正な USB を検知する手法について検討する．

図１　本研究で使用した USB メモリー

3. USB のデータ解析

3.1 USB と PC との通信

USB を挿入した際の PC と USB の通信のやりとりを Wireshark で記録して生成された pcap ファイルの解析を行った．USB の通信は 1 ミリ秒周期でフレームと呼ばれるデータが繰り返し転送されており，USB を端末に挿入するだけでも大量のデータが観測される．図 2 は LinuxOS がインストールされている端末と USB との通信を記録した pcap ファイルの一部である．

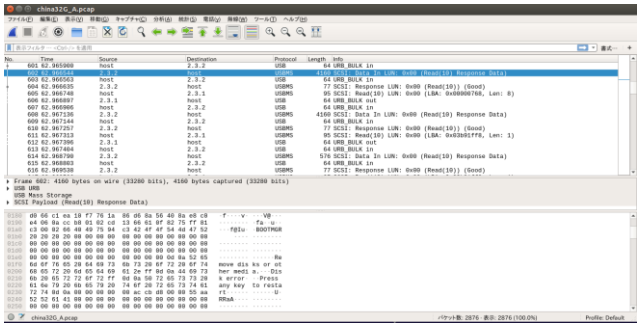

図２　本研究で使用した USB メモリー

図３　ダンプファイルの中身

†長崎県立大学
‡国立研究開発法人情報通信研究機構

3.2　ダンプファイルの解析

ダンプファイルの中身（図３はその一部）を解析するために，一定の意味をなすような文字列の抽出を行った．図４はその結果の一部である．

図４　抽出した文字列

抽出された文字列には，例えば，「@SVWAUH」というものが含まれており，この情報を Web で検索すると，

ZwiftApp.exe

という exe ファイルの情報と一致する部分が USB ファイルの中身にもみられた．これは，あるゲームソフトの情報と類似しており，解析した USB には元々ゲームソフトが入っていたものと考えられる．参考までに，この USB はインターネットを通じて購入したものである．同様に，本研究で解析した USB の中には「@ATAUAWH」という文字列が含まれていて，Web で検索すると図５のような情報が得られ，このような情報を元にすることで，さらに USB の中身を解析できるものと考えられる．

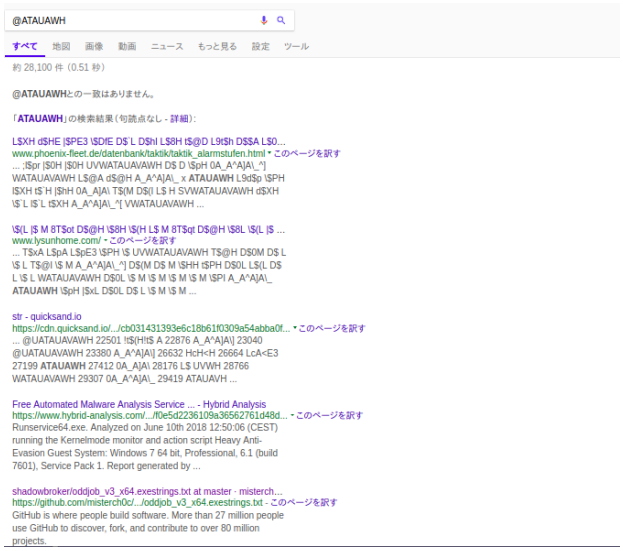

図５　「@ATAUAWH」の検索結果

図６　通常の USB メモリー

図６に Sony 製の通常の USB メモリーのダンプファイルを示す．図３と４に示したものとは異なり，通常はこのようにファイルの中身に特殊な文字列が入っていることは無いと考えられる．

4. おわりに

本研究では，USB メモリーの中身に含まれる情報を基にして，USB を用いた攻撃を検知する手法の開発ができるかどうかについて，実際に USB ファイルの中身を調査することで考察した．購入した時点で USB の中に予め何らかのデータが含まれる場合があることを今回の研究で確認することができたため，このような USB に対して，中身に含まれているデータが不正な挙動を示すかどうか判別する手法を確立することが今後の課題である．

参考文献

[1] Matthew Tischer, Zakir Durumeric, Sam Foster, Sunny Duan, Alec Mori, Elie Bursztein Michael Bailey, “Users Really Do Plug in USB Drives They Find”, IEEE Symposium on Security and Privacy (SP), pp. 306-319 (2016).
[2] Songjie Liang, Bharat S. Rawal, “Secure USB Based File System for BMC Applications”, 2017 Second International Conference on Recent Trends and Challenges in Computational Models (ICRTCCM), pp. 228-233 (2017).
[3] 城間 政司, 西尾 泰彦, 井上 博之, “USB 周辺機器接続のセキュリティリスク分析におけるアセット導出手法”, 情報処理学会論文誌 59(1), pp.199-210 (2018).