

Malicious Software Detection Report

マルウェア検出報告

December 16th, 2019 Editor: Kitani

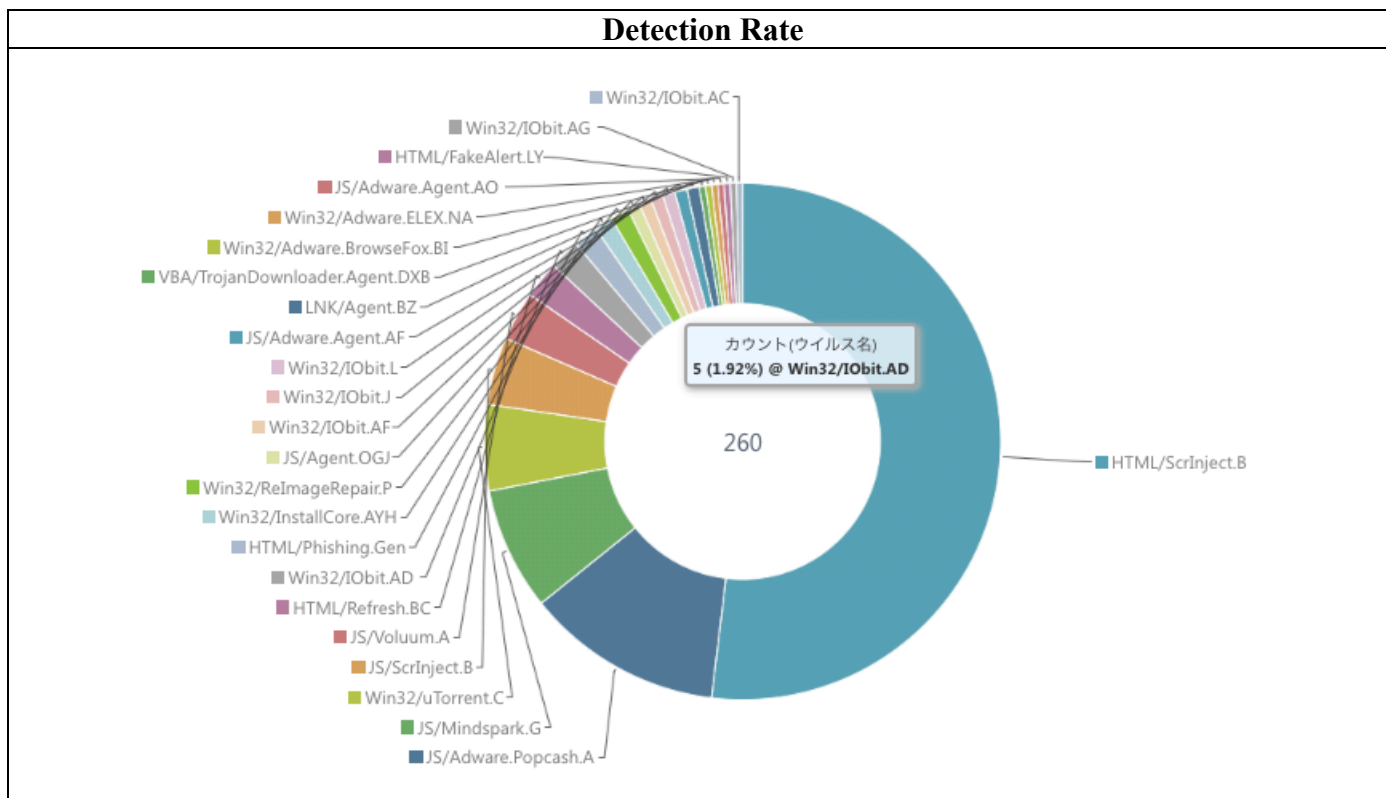
Recent Malware Trends (最近のマルウェア動向)

FY2018	Malware	PCs	TOP Malware
April	287	29	JS/Adware.Agent.AA
May	192	33	JS/Agent.OCJ
June	553	36	JS/Adware.Subprop.D
July	58	24	JS/Midspark.G
August	213	22	JS/Adware.Subprop.J
September	177	33	JS/Adware.Subprop.J
October	106	24	JS/Midspark.G,
November	260	33	HTML/ScrInject.B
December			
January			
February			
March			
TOTAL	1,846	234	

[November 2019]

Most malicious software (malware) on November 2019 was a variant of “HTML/ScrInject.B”. This case is an unwanted potential website which an illegal code is embedded. The category is trojan horse. By making a user access a cracked website, the malware will try to download a malware, to forcibly display an illegal advertisement, or to rip off a web browsing history.

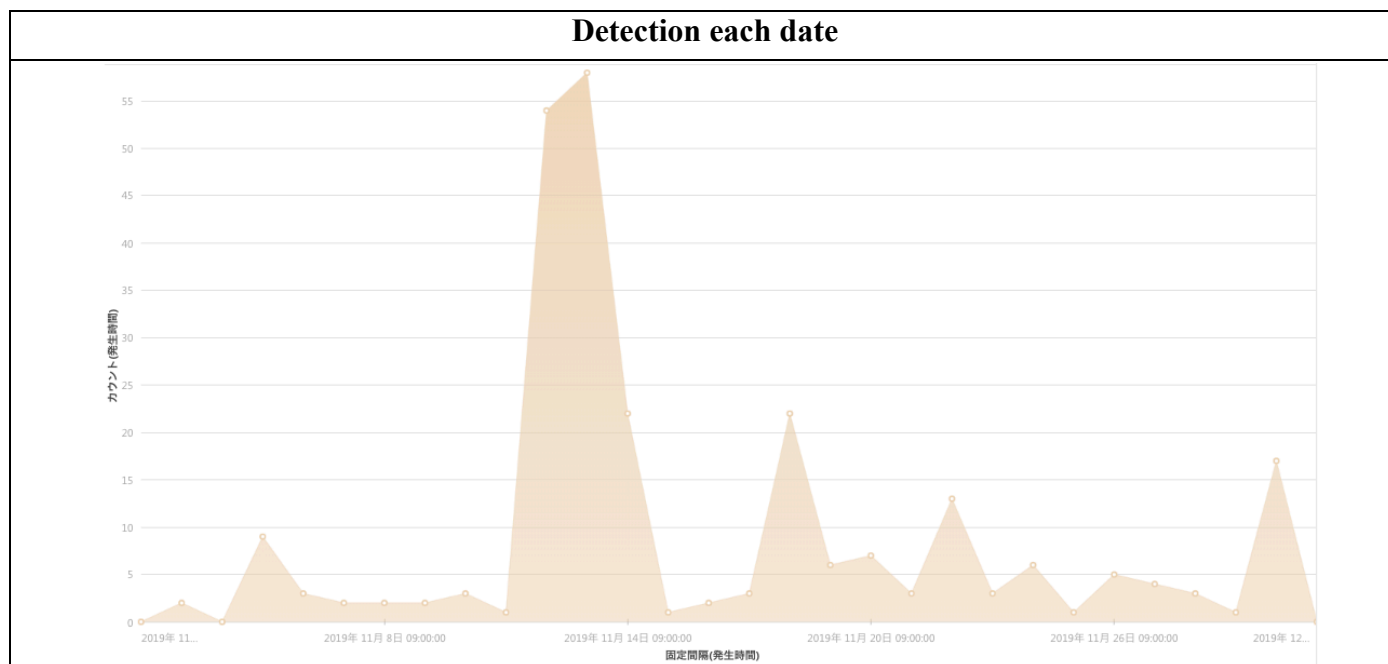
2019年11月で最も検知されたマルウェアは「HTML/ScrInject.B」の亜種でした。これは、不正なコードが埋め込まれた望ましくないウェブサイトの場合です。カテゴリとしてはトロイの木馬系になります。不正なコードを埋め込まれたウェブサイトアクセスさせることで、マルウェアのダウンロード、不正な広告の表示、ブラウザの閲覧履歴の奪取などを試みます。



Malicious Software Detection Report

マルウェア検出報告

December 16th, 2019 Editor: Kitani



For the Center's members.

The Center's security software had been blocking the detected malware but please check your security software (latest virus definition, not too old software) in your PC if you have a private PC which needs to protect a malware by yourself. Then, if you worry the information infrastructure regarding the information security, please contact the information processing office.

本研究所構成員の皆様へ

本研究所セキュリティ対策ソフトウェアは、これらの検知したマルウェアをブロックしましたが、各セキュリティ対策ソフトウェアのウィルス定義が最新かどうか（古すぎる日付ではないかどうか）確認しておいてください。また、情報セキュリティに関して不安に思うことがあれば、情報処理室へお問い合わせください。

At least, **PLEASE** check the following prevention measures.

また、少なくとも下記の対策は常日頃からチェックしてください。

1. Create "Autorun.inf" folder on the top of your removable media.

外部メディアのトップに「Autorun.inf」フォルダを作成する

A lot of malware tries to overwrite "Autorun.inf" file on the top of a removable media because Windows OS automatically carries out a program by loading "Autorun.inf" setting when the media inserts to a PC. b Therefore, the malware is lurked into a hidden area and it tries to act by loading "Autorun.inf" file. **A simple malware is failure the overwriting of "Autorun.inf" file if "Autorun.inf" folder exists. This is a small-scale security prevention measure, but please cooperate for reducing the infection to removable medias.**

マルウェアの多くは、外部メディアのトップに Autorun.inf ファイルを作成し、感染を広げようとします。これは、Windows OS が外部メディアを接続する際に、そのファイルに書かれた命令をチェックして実行しようとするためです。もし Autorun.inf フォルダが存在すると、単純なマルウェアの場合、Autorun.inf への書き込みに失敗します。これは小規模で手軽なセキュリティ対策になりますが、過去に効果が出たことがあります。

2. Update of the computer security (OS やアプリのセキュリティ更新を忘れずに！)

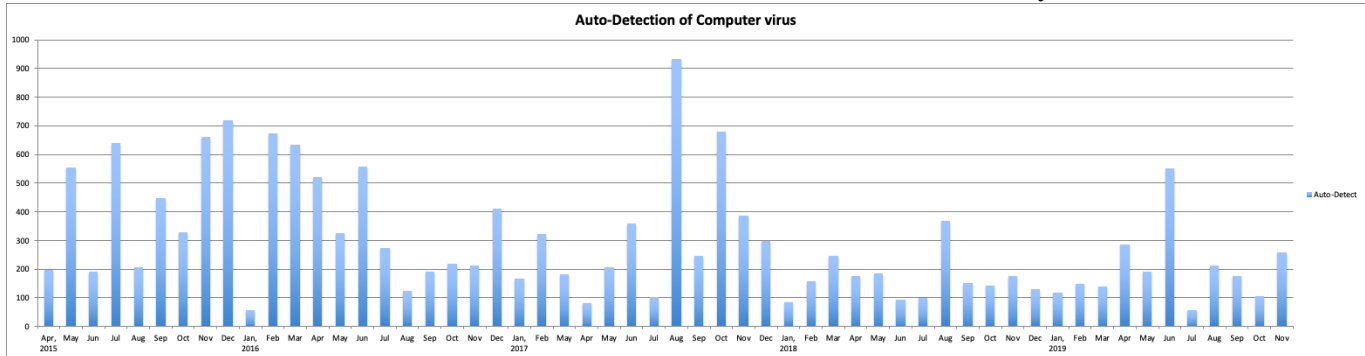
Malicious Software Detection Report

マルウェア検出報告

December 16th, 2019 Editor: Kitani

<http://www.cseas.kyoto-u.ac.jp/info/security> (in English and Japanese)

Transition of Malware Detections since 2015 fiscal year



*“Auto-Detection” is the number of malware which can be detected by our anti-virus software.

[Auto-Detection Total]: 26,439(since August 2009)

FY	FY2014	FY2015	FY2016	FY2017	FY2018	FY2019	FY2020	FY2021
Total	4,275	5,315	3,503	3,784	1,931	1,846		
AVG(day)	15.83	14.56	9.6	10.37	5.29	7.57		