Malicious Software Detection Report
マルウェア検出報告

January 24, 2019 Editor: Kitani

Recent Malware Trends（最近のマルウェア動向）

FY2018	Malware	PCs	TOP Malware
April	175	26	JS/Redirector.NDS
May	185	34	Win32/PSW.OnLineGames.NNU
June	94	34	JS/Mindpsark.G
July	99	28	JS/Mindpsark.G
August	370	35	JS/Adware.Revizer.E
September	152	28	JS/Adware.Revizer.E
October	143	28	JS/Adware.Agent.AA
November	175	25	JS/Adware.Agent.AA
December	130	26	JS/Adware.Agent.AA
January			
February			
March			
TOTAL	1,523	264	

Most malicious software (malware) for recent 2 months (11-12/2018) was a variant of "JS/Adware.Agent.AA". This aims to make a user input private information (including a password, a credit card, and so on) using a fake clever advertisement (etc. prize draw scam). Please don't believe a message. Firstly, you should contact the information processing office. The Center's security software had been blocking it 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.

2018 年 11 月−12 月の 2 ヶ月間で最も検知されたマルウェアは「JS/Adware.Agent.AA」でした。これは不正広告（当選詐欺等）を表示させ、パスワードやクレジットカード等を含む個人情報を盗むなどします。予期しないメッセージ（高額当選した等）が出ても信じず、不安なら情報処理室へご相談ください。なお、本マルウエアは、本研究所セキュリティソフトウェアでは検知・駆除していますが、自前でセキュリティ対策をする必要のある端末は、導入しているセキュリティソフトウェア（最新のウィルス定義が適用されている、古すぎるソフトではないこと）について気をつけて下さい。

At least, **PLEASE check the following prevention measures.**
少なくて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

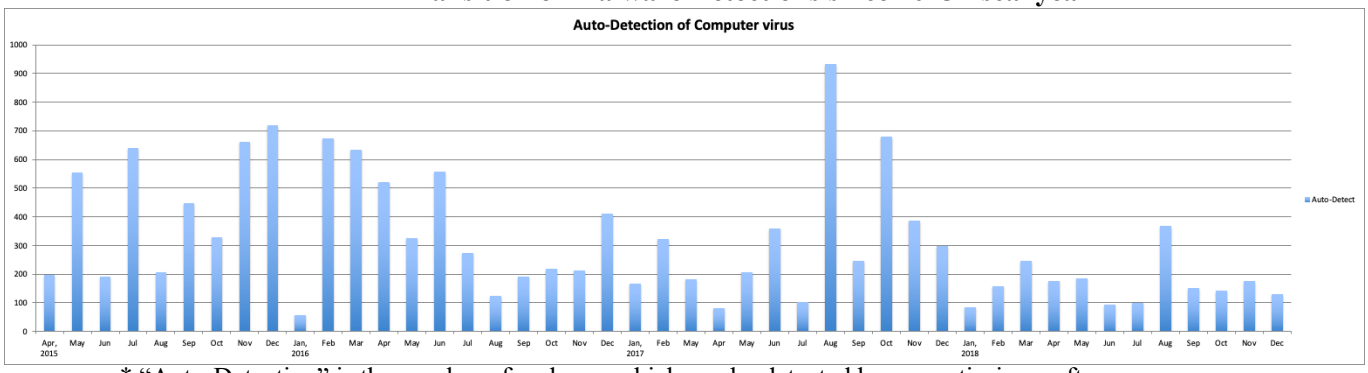
   A lot of malware tries to overwrite "Autorun.inf" file on the top of a removable media because Windows OS automatically carries out a program by loading "Autorun.inf" setting when the media inserts to a PC. b Therefore, the malware is lurked into a hidden area and it tries to act by loading "Autorun.inf" 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！）
   http://www.cseas.kyoto-u.ac.jp/info/security (in English and Japanese)

Malicious Software Detection Report
マルウェア検出報告

January 24, 2019 Editor: Kitani

Transition of Malware Detections since 2015 fiscal year



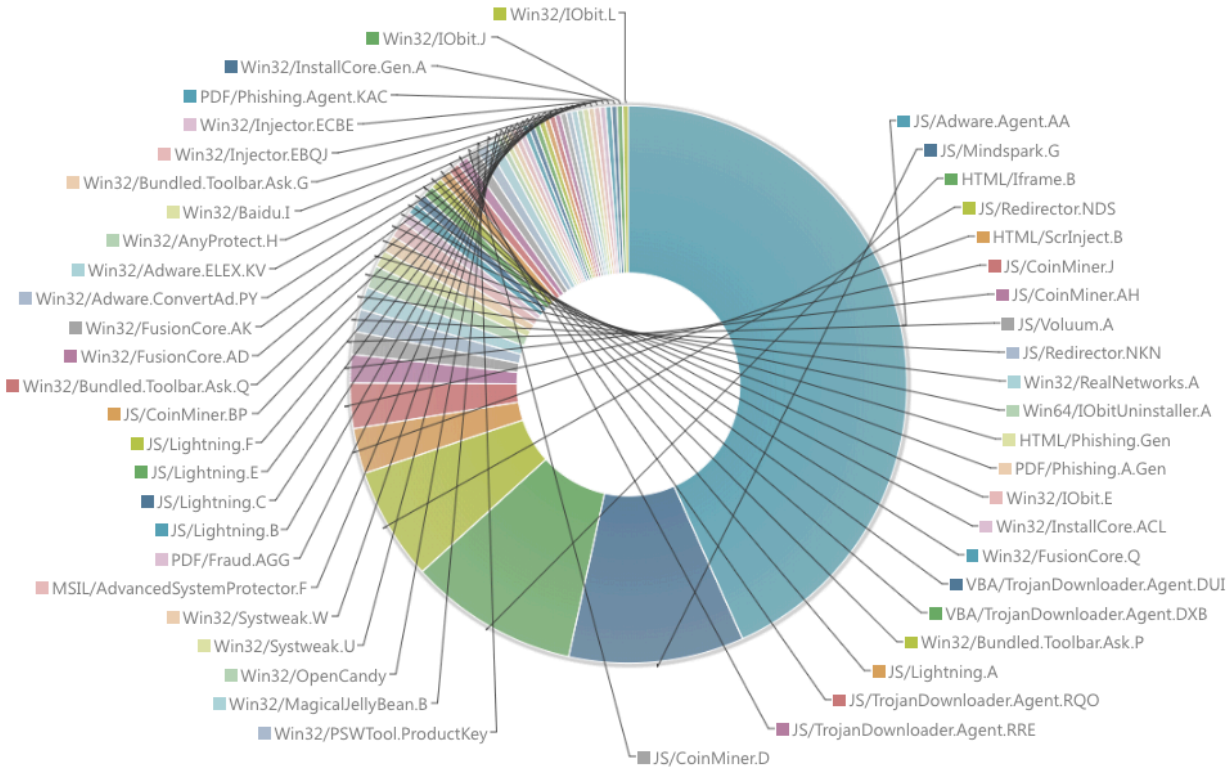
* “Auto-Detection” is the number of malware which can be detected by our anti-virus software.

[Auto-Detention Total]: 23,740 (since August 2009)

FY	FY2014	FY2015	FY2016	FY2017	FY2018	FY2019	FY2020	FY2021
Total	4,275	5,315	3,503	3,784	1,523			
AVG(day)	15.83	14.56	9.6	10.37	5.54			

[Status Report of detection computer virus in November-December 2018]
*** 305 computer viruses were detected among 51 PCs (duplicated).**

Detection Rate



Malicious Software Detection Report
マルウェア検出報告

January 24, 2019 Editor: Kitani

Detection each date