Malicious Software Detection Report

マルウェア検出報告

May 3rd, 2021 Editor: Kitani

Recent Malware Trends（最近のマルウェア動向）

FY2020	Malware	PCs	TOP Malware
April	483	34	JS/Adware.Agent.AF
May	238	32	JS/Adware.Atocari.B
June	321	46	JS/Midspark.G
July	224	32	Generik.FMEKJJY
August	453	30	JS/Midspark.G
September	683	20	JS/Midspark.G
October	627	26	JS/Midspark.G
November	532	32	JS/Midspark.G
December	382	27	Win32/DriverReviver.C
January	502	29	JS/PopunderJS.D
February	1047	26	JS/PopunderJS.D
March	260	26	Win32/DriverReviver.C
TOTAL	5,752	356	

[March 2021]

Most malicious software (malware) in March 2021 was a variant of "Win32/DriverReviver". This is fake antivirus software. It is classified as adware that displays fake warnings and tries to get you to purchase software.

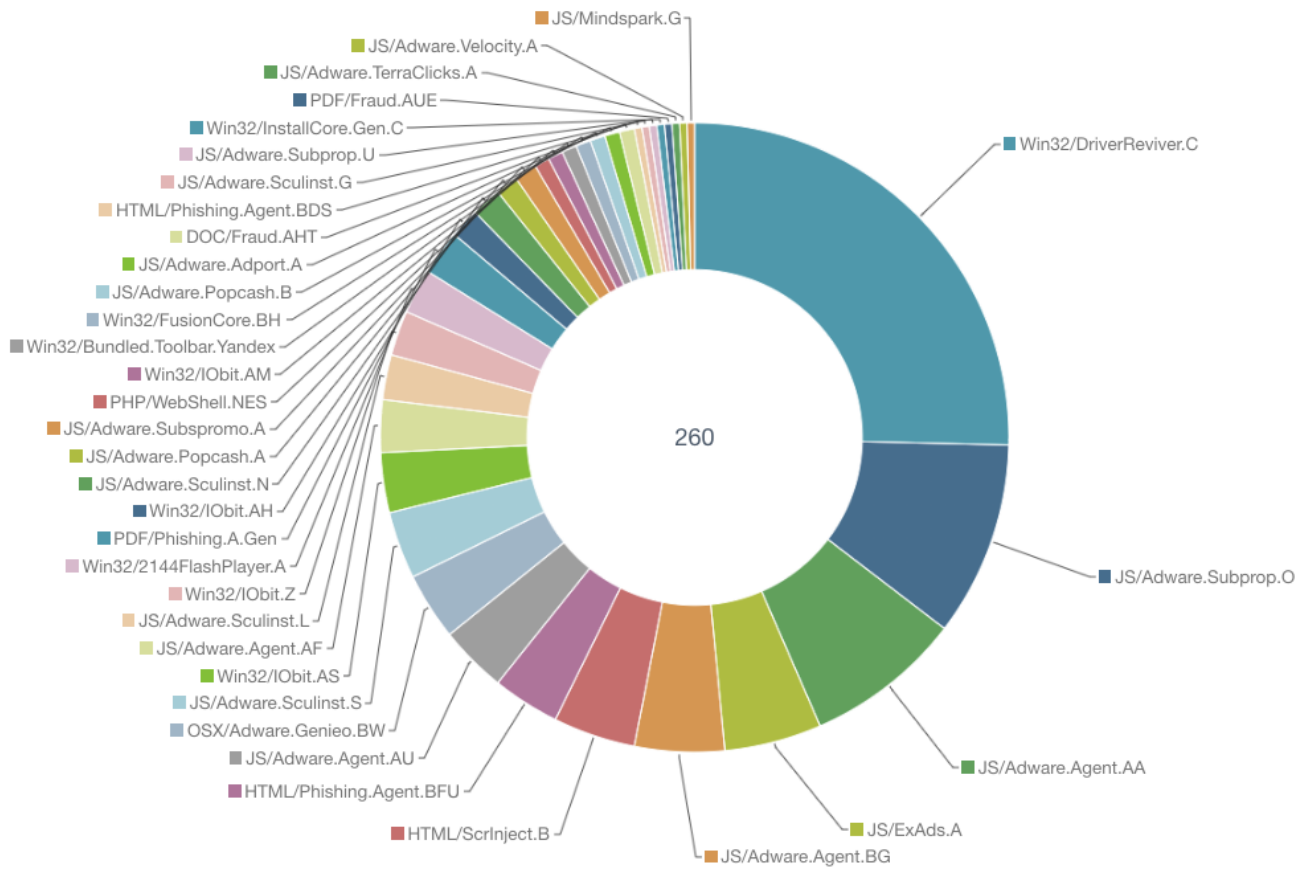
2021年3月で最も検知されたマルウェアは「Win32/DriverReviver」の亜種でした。これは偽ウィルス対策ソフトウェアに該当します。偽の警告を表示し、ソフトウェアを購入させようというアドウェアに分類されるマルウェアになります。

Detection Rate

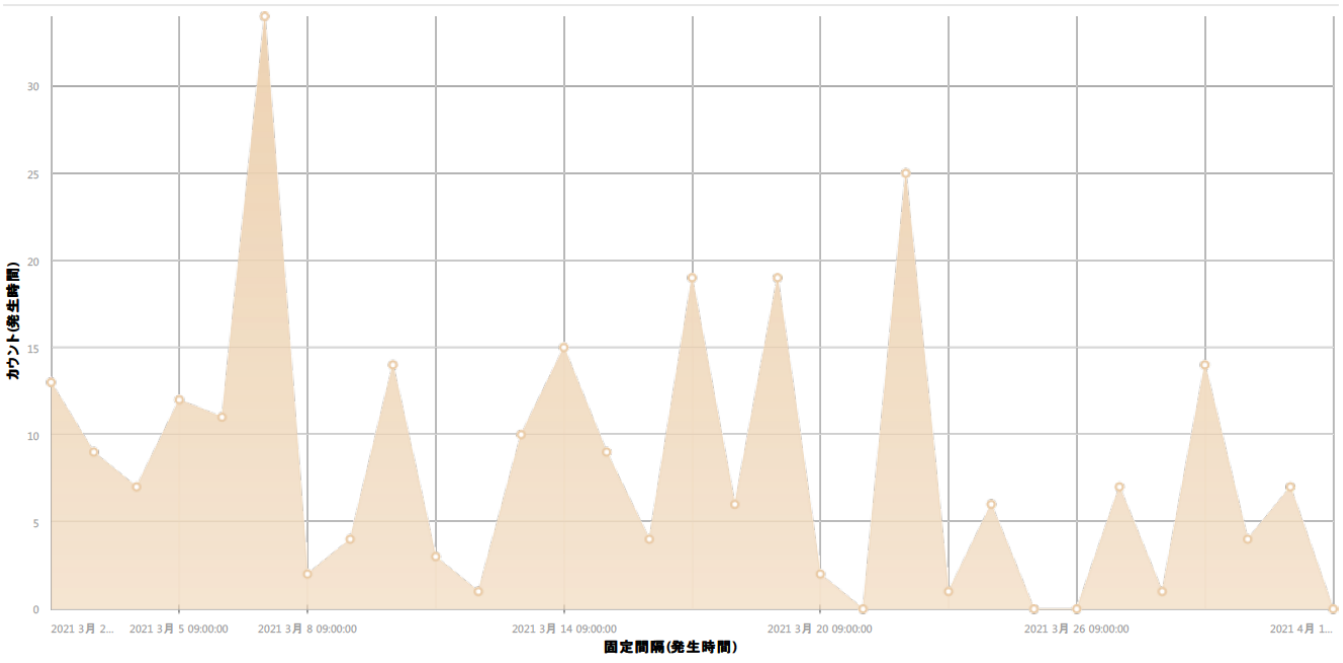
Malicious Software Detection Report

マルウェア検出報告

May 3rd, 2021 Editor: Kitani



Detection each date



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 that needs to protect malware by yourself. Then, if you worry about the information infrastructure regarding the information security, please contact the information processing office.

Malicious Software Detection Report

マルウェア検出報告

May 3rd, 2021 Editor: Kitani

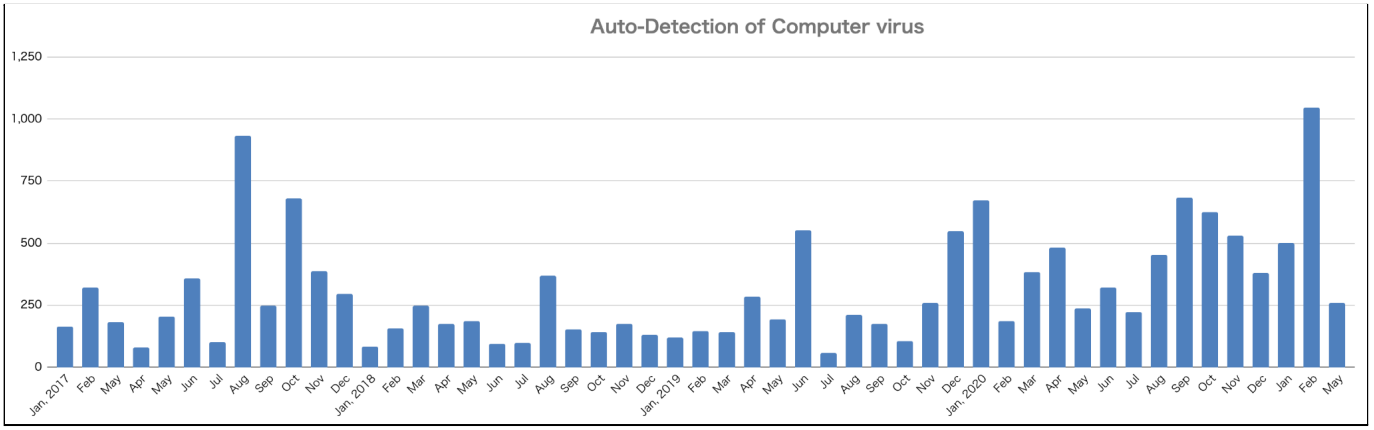
本研究所構成員の皆様へ
本研究所セキュリティ対策ソフトウェアは、これらの検知したマルウェアをブロックしましたが、各セキュリティ対策ソフトウェアのウィルス定義が最新かどうか（古すぎる日付ではないかどうか）確認しておいてください。また、情報セキュリティに関して不安に思うことがあれは、情報処理室へお問い合わせください。

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 has lurked into a hidden area and it tries to act by loading “Autorun.inf” file. **Simple malware is a failure of the overwriting of the “Autorun.inf” file if the “Autorun.inf” folder exists. This is a small-scale security prevention measure, but please cooperate for reducing the infection to removable media.**
   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)

Transition of Malware Detections since 2017



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

[Auto-Detention Total]: 32,337 (since August 2009) , 13,586 (since January, 2017 / new Center)

FY	FY2014	FY2015	FY2016	FY2017	FY2018	FY2019	FY2020	FY2021
Total	4,275	5,315	3,503	3,784	1,931	3,256	5,752	
AVG(day)	15.83	14.56	9.6	10.37	5.29	9.72	15.76	