Malicious Software Detection Report

マルウェア検出報告

February 14th, 2022 Editor: Kitani

Recent Malware Trends（最近のマルウェア動向）

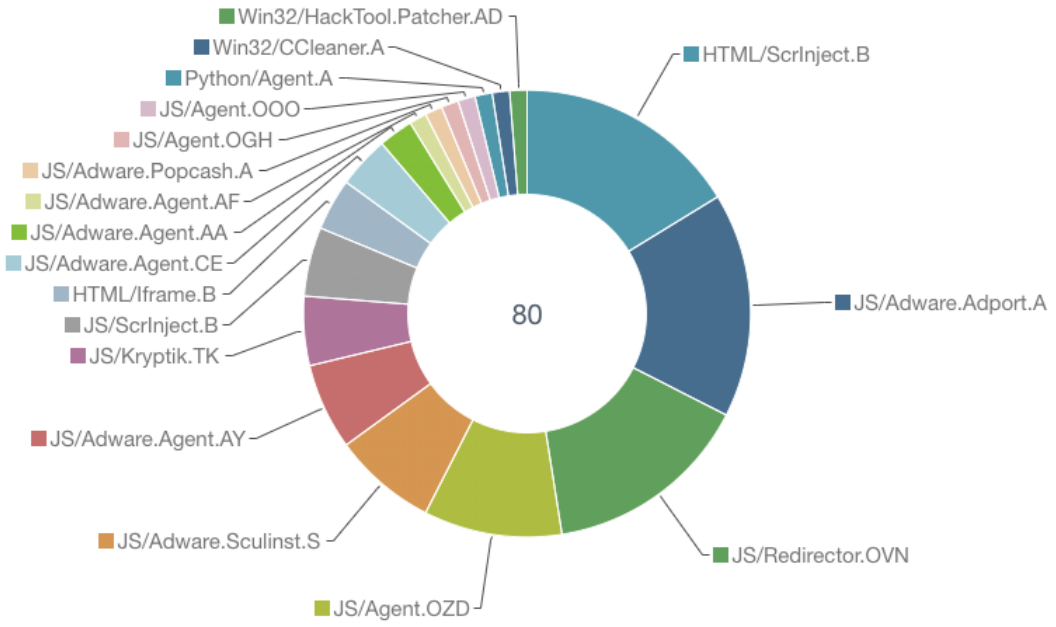
FY2021	Malware	PCs	TOP Malware
April	318	30	JS/Adware.Agent.AY
May	847	28	JS/Adware.Agent.AY
June	256	22	JS/Adware.Agent.AY
July	245	25	Win64/DriverReviver.A
August	353	24	Win64/DriverReviver.A
September	442	23	JS/Adware.Agent.AA
October	346	27	JS/Adware.Agent.AA
November	323	25	JS/Adware.Agent.AA
December	398	26	JS/Adware.Agent.AA
January	80	16	HTML/ScrInject.B
February			
March			
TOTAL	3,608	246	

[January 2022]

Most malicious software (malware) on January 2022 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.

2022年1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。カテゴリー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に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。

Detection Rate

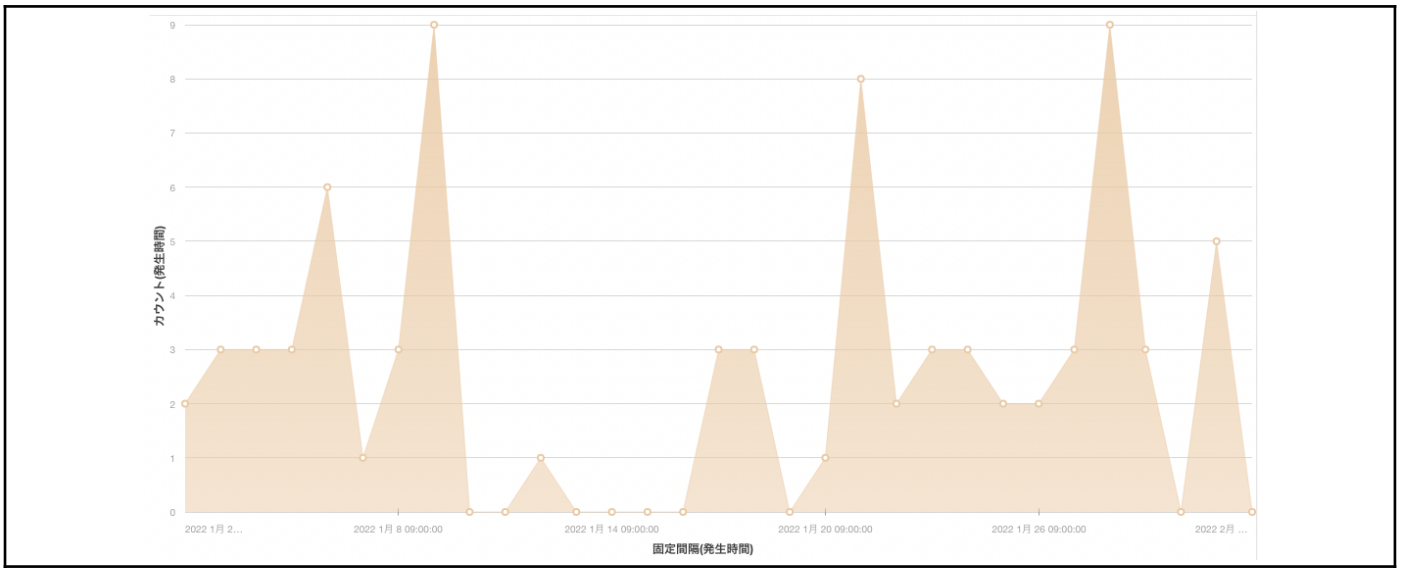


Detection each date

Malicious Software Detection Report

マルウェア検出報告

February 14th, 2022 Editor: Kitani



For the Center's members.

The Center's security software has 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.

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。

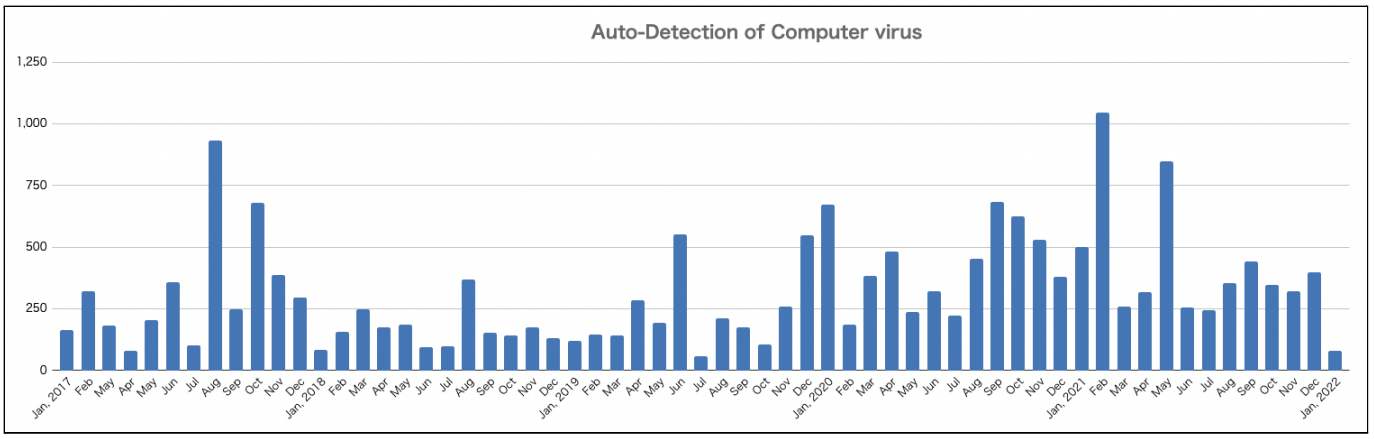
2. **Update of the computer security**（OSやアプリのセキュリティ更新を忘れずに！）
   http://www.cseas.kyoto-u.ac.jp/info/security (in English and Japanese)

Transition of Malware Detections since 2017

Malicious Software Detection Report

マルウェア検出報告

February 14th, 2022 Editor: Kitani



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

[Auto-Detention Total]: 38,136 (since August 2009) , 19,385 (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	3,608
AVG(day)	15.83	14.56	9.6	10.37	5.29	9.72	15.76	11.89