Malicious Software Detection Report

マルウェア検出報告

April 11th , 2025 Editor: Kitani

Recent Malware Trends（最近のマルウェア動向）

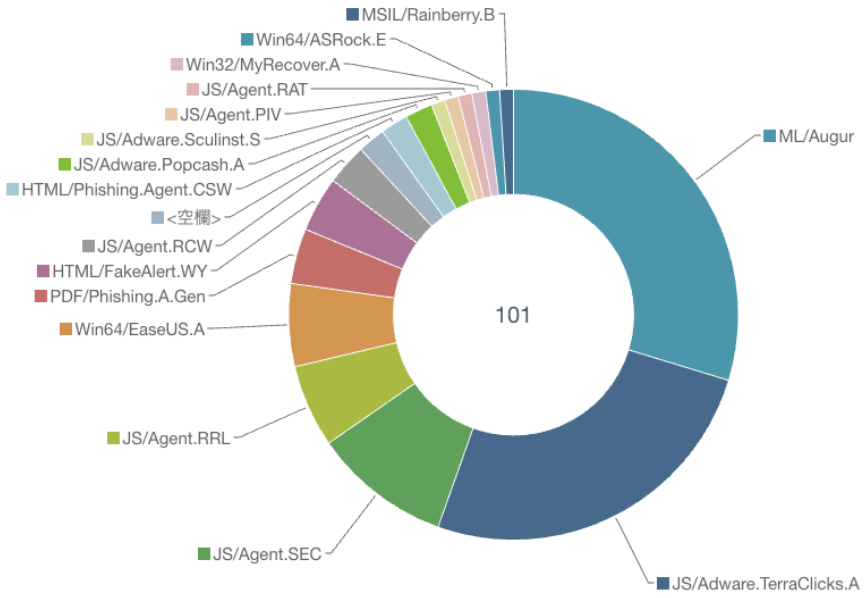
FY2024	Malware	PCs	TOP Malware
April	343	23	DOC/Fraud.AAW
May	1372	19	DOC/Fraud.AAW
June	60	10	JS/Agent.RRO
July	148	21	DOC/Fraud.AAW
Aug	58	8	JS/Adware.TerraClicks.A
Sep	73	13	PDF/Phishing.A.Gen
Oct	143	14	JS/Packed.Agent.N
Nov	175	12	OSX/BuhoCleaner.A
Dec	101	20	ML/Augur
TOTAL	2,467	140	

[Dec 2024]

Most malicious software (malware) in this month was “ ML/Augur”. This uses machine learning (ML) by ESET to detect suspicious processes.

今月最も検知された悪意あるソフトウェア（マルウェア）は、「ML/Augur」でした。これは ESETの機械学習（ML）を使用して疑わしいプロセスを検出したものです。

Detection Rate

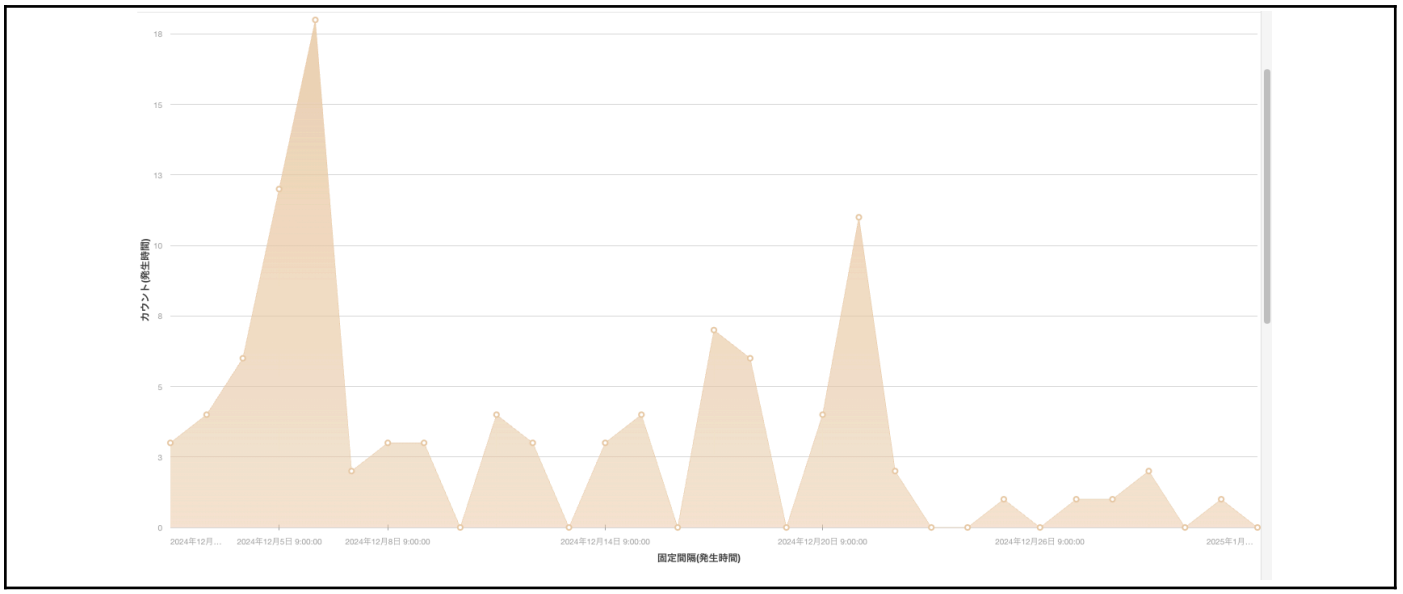


Detection each date

Malicious Software Detection Report

マルウェア検出報告

April 11th , 2025 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. If you are worried about the information infrastructure regarding 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. **<u>Create an "Autorun.inf" folder on the top of your removable media</u>.**
   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 the "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 is inserted into a PC. b Therefore, the malware has lurked in a hidden area, and it tries to act by loading the "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 to reduce 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。

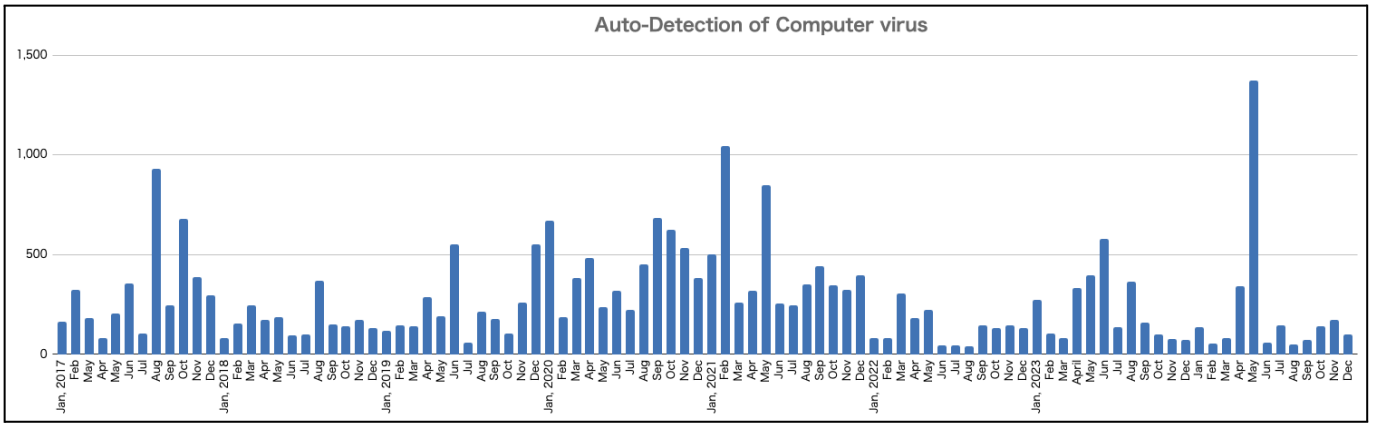
2. **Update of the computer security**（OSやアプリのセキュリティ更新を忘れずに！）
   https://info.cseas.kyoto-u.ac.jp/services-ja/security-ja

Malicious Software Detection Report

マルウェア検出報告

April 11th , 2025 Editor: Kitani

Transition of Malware Detections since 2017



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

[Auto-Detention Total]: 45,045 (since August 2009), 26,294 (since January 2017 / new Center)

FY	FY2017	FY2018	FY2019	FY2020	FY2021	FY2022	FY2023	FY2024
Total	3,784	1,931	3,256	5,752	3,999	1,552	2,499	2,467
AVG(day)	10.37	5.29	9.72	15.76	11.00	4.25	6.83	8.97