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

May 26, 2017 Editor: Kitani

Most malicious software (malware) in April 2017 was a variant of “Win32/HackTool.Crack.BD”. This is a crack tool for an illegal use of software, an illegal access to a PC (ex. Password crack tool), and so on. The CSEAS security software detects it and block the activity when a potentially unwanted program is downloaded or run. It may be lurking inside a free software. Of course, it’s blocked by the Center’s security software, but especially please pay attention for your removable medias.

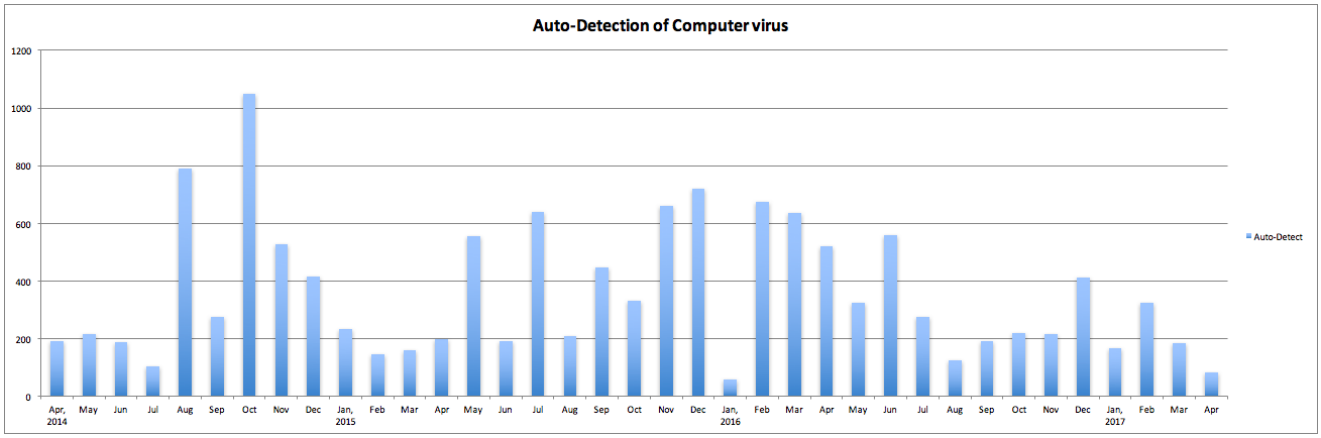
At least, **PLEASE check the following prevention measures.**

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

   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.**

2. **Update of the computer security**
   http://www.cseas.kyoto-u.ac.jp/info/security (in English and Japanese)

Since 2014



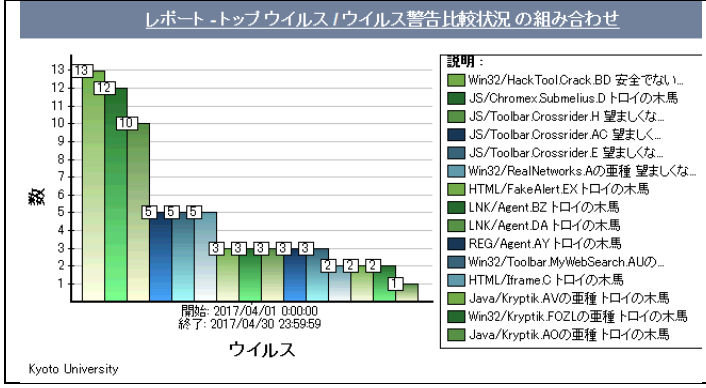
* “Auto-Detection” is the number of malware which can be detected by our anti-virus software.

[Auto-Detention Total]: 19,502 (since August 2009)

FY	FY2014	FY2015	FY2016	FY2017	FY2018	FY2019	FY2020	FY2021
Total	4,275	5,315	3,503	81				
AVG(day)	15.83	14.56	9.6	2.7				

[Status Report of detection computer virus in April 2017]
*** 81 computer viruses were detected among 12PCs.**

Detection Rate



Detection each date