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

October 26, 2017 Editor: Kitani

Most malicious software (malware) in July-September 2017 was a variant of “JS/Mindspark”. This is the toolbar software for a web browser and the malware type is a browser hijacker (adware/spyware). It tries to change various settings on your browser or to get a private information on your browser without the user’s acceptance. You don’t worry it because the Center’s security software blocked the activity.

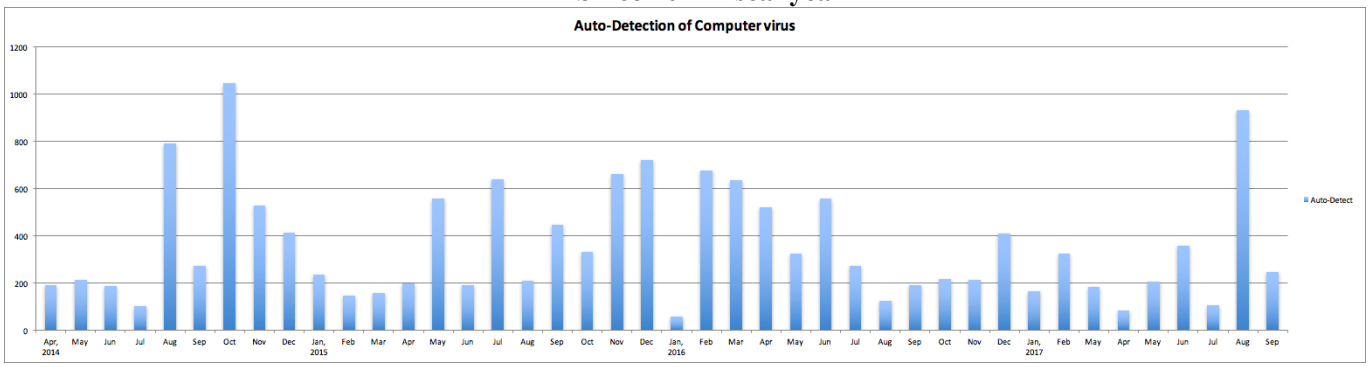
However, At least, **PLEASE check the following prevention measures.**

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 fiscal year



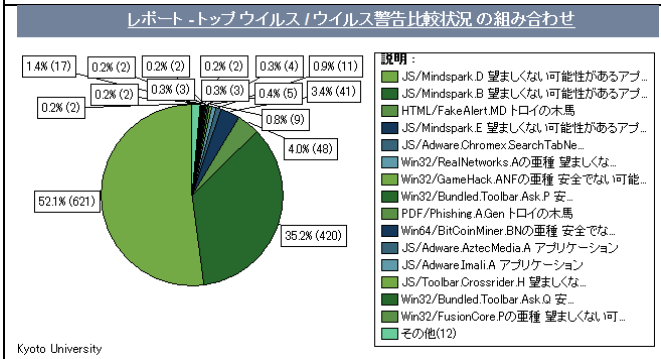
* “Auto-Detection” is the number of malware which can be detected by our anti-virus software.

[Auto-Detention Total]: 20,066 (since August 2009)

FY	FY2014	FY2015	FY2016	FY2017	FY2018	FY2019	FY2020	FY2021
Total	4,275	5,315	3,503	1929				
AVG(day)	15.83	14.56	9.6	10.54				

[Status Report of detection computer virus in July-September 2017]
*** 1,284 computer viruses were detected among 36PCs.**

Detection Rate



Detection each date