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

April 24, 2018 Editor: Kitani

Most malicious software (malware) in March 2018 was a variant of "JS/Redirector". This is a potentially unwanted application, which has also been categorized as trojan house. The program leads to a malicious web site using a web browser redirection. The program code hides in JavaScript on a web site. The Center's security software had been blocking the activity but please check your security software (latest virus definition, not too old software) in your PC if you have a private PC which needs to protect a malware by yourself.

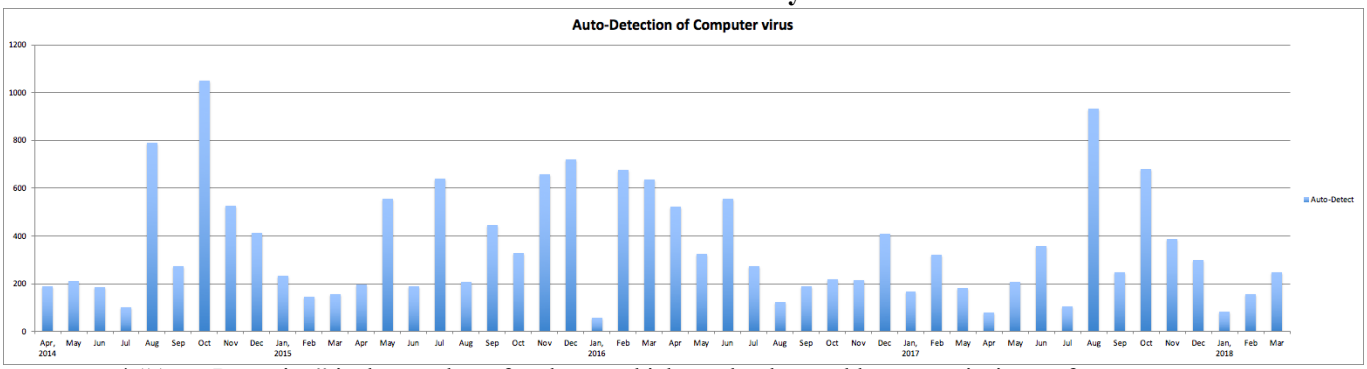
However, At least, **PLEASE check the following prevention measures.**

1. **<u>Create "Autorun.inf" folder on the top of your removable media</u>.**

   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]: 23,205 (since August 2009)

FY	FY2014	FY2015	FY2016	FY2017	FY2018	FY2019	FY2020	FY2021
Total	4,275	5,315	3,503	3,784				
AVG(day)	15.83	14.56	9.6	10.37				

[Status Report of detection computer virus in February 2018]
*** 247 computer viruses were detected among 30 PCs.**

Detection Rate	Detection each date