

Malicious Detection Report

マルウェア検出報告

February 28, 2015 Editor: Kitani

Most detected malware in Jan 2015 was a variant of “Win32/Kryptik.BWXD” (46 reports). This is false detection due to the Microsoft OneDrive. Secondly, a variant of “Win32Agent.NML” came to the Center. This is compositive malicious software with Trojan horse function. The software creates the security vulnerability in the infected PC for opening the hacker’s invasion pathway and blocks the activity of security software. Moreover, it strives to drastically reduce the PC performance.

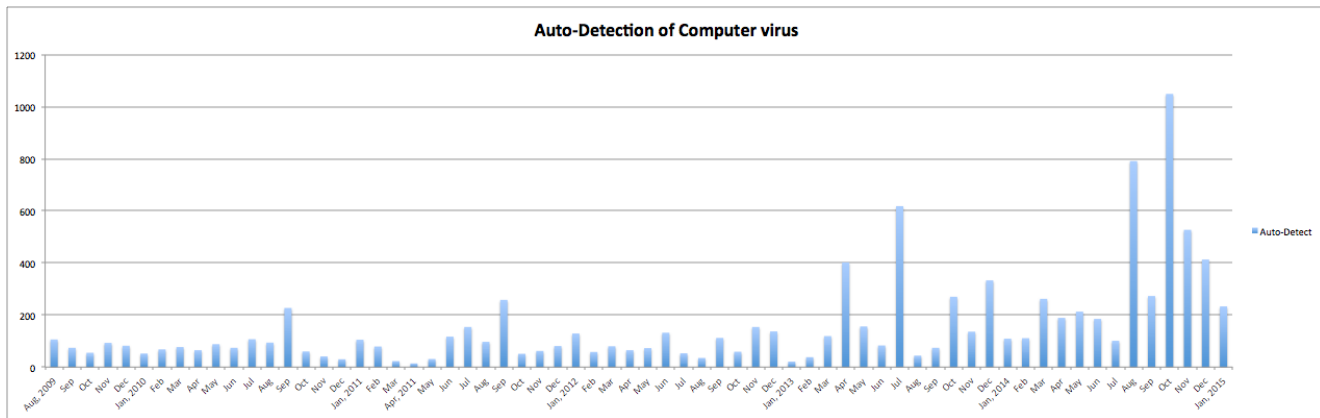
[PLEASE pay attention about Prevention Measure]

The information security risks (including the information leak) exist in various routes. The Center’s security software has been detecting most of them, but it cannot be perfect even if the highest technology and the enough cost are used. Finally, the crisis awareness of PC users is required.

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

1. Create "Autorun.inf" folder on the top of removable media.
2. Update of the computer security

Please see <http://www.cseas.kyoto-u.ac.jp/info/security> (in English and Japanese)



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

[Auto-Detection Total]: 10,069 (since August 2009)

FY	FY2009	FY2010	FY2011	FY2012	FY2013	FY2014
Total	607	993	1,132	998	2,598	3,974
AVG(day)	1.67	2.72	3.10	2.73	7.12	14.72 ↑

[Status Report of detection computer virus on Jan 2015

*233 malware were detected among 21 PCs.

