Internet Topics: About the anti-Malware engineering WorkShop 2009

Here, we introduce the anti-Malware engineering WorkShop 2009 (MWS2009), which was held at the Toyama International Conference Center over three days from October 26, 2009*1. This is a research workshop for malware analysis sponsored by the Information Processing Society of Japan and the Cyber Clean Center Steering Committee. This is the second time the workshop has been held, following on from MWS2008*2 last year, and this year over 100 researchers, students, and corporate engineers actively participated in presentations and discussions. The workshop involved creating CCC DATAset2009 for common analysis from malware activity information (malware specimens and communications data) acquired at the Cyber Clean Center*3, and sharing the achievements of research into technology for analyzing and producing countermeasures by utilizing this data set*4.

■ CCC DATAset2009

Presenters are provided with the following three types of data as CCC DATAset2009.

●Malware specimen data

Hash values for 10 malware specimen varieties (researchers must obtain malware specimens themselves). Analysis results are also provided at a later date.

●Attack communications data

Two day's worth of communications data from two honeypots (CCC DATAset2009 uses data from March 13 to 14, 2009). A packet dump showing actual communications is provided.

●Attack origin data

A year's worth of attack communications records from 94 honeypots (CCC DATAset2009 uses data from May 1, 2008 to April 30, 2009). This includes the time, the source IP address of the attack origin, the destination port number, and the name of malware.

CCC DATAset2009 content has been expanded beyond that of CCC DATAset2008*5. Presenters can verify the effectiveness of their research results using actual observed data by applying them to one of these data sets.

■ MWS2009

Last year there were 22 general oral presentations (including 8 given by students), and for MWS2009 this number rose to 30 (including 15 given by students). Presentations covered a wide range of topics, from methods for carrying out efficient malware analysis, to techniques for improving honeypots, techniques for visualizing malware activity, and attempts at predicting this activity*6. As indicated by the number of presentations given by students, another feature of this year's workshop was the more active role played by students. At IIJ we compared CCC DATAset2009 attack origin data with observed data from the MITF honeypots that we operate ourselves, and presented a big-picture look at differences in the observed results. We believe that by comparing multiple observed results for the same period we can help fuel discussions regarding the locality of events and the accuracy of observation techniques.

The MWS Cup 2009 event was also held for the first time at this workshop. In this event participants vied for the best analysis technology by analyzing malware activity record data they were given as a task within a set time limit. Participants brought tools they had created as part of their research as well as the analysis environment they use on a daily basis, and competed to analyze data handed out on CD on the day of the event as quickly and accurately as possible. Seven teams participated despite this being the first time the event was held, and once again students did remarkably well, with university teams reaching the top ranks.

The anti-Malware engineering WorkShop can be thought of as an effective venue for comparing research results in a fair way through the analysis of common data, and a place for developing human resources that have expertise in measures against malware in the future. IIJ also considers it an invaluable occasion for interacting with the academic community that we seldom have the opportunity to exchange opinions with, and we would like to continue to actively participate in this workshop in the future.

The MWS Cup 2009 event

Author:
Mamoru Saito
General Manager of the Division of Emergency Response and Clearinghouse for Security Information, IIJ Service Business Department

*1 Anti-Malware engineering WorkShop 2009 (http://www.iwsec.org/mws/2009/)(in Japanese). Held concurrently with the Computer Security Symposium 2009 (CSS2009) (http://www.iwsec.org/css/2009/english/index.html) sponsored by the Computer Security (CSEC) Group of the Information Processing Society of Japan. Photos of MWS2009 can be viewed on the MWS2009 activity archive (http://www.iwsec.org/mws/2009/photo.html)(in Japanese).

*2 IIJ also attended MWS2008 held last year. MWS2008 (http://www.iwsec.org/mws/2008/)(in Japanese). This workshop was discussed in a conversation published in IIJ.news Vol.90 (http://www.iij.ad.jp/news/iijnews/2009/vol90.html)(in Japanese).

*3 The Cyber Clean Center is an anti-bot measures project coordinated by the Ministry of Internal Affairs and Communications, the Ministry of Economy, Trade and Industry, and other related organizations (https://www.ccc.go.jp/en_index.html).

*4 Other endeavors involving the sharing of research results based on common data include the DARPA Intrusion Detection Data Sets (1998, 1999) (http://www.ll.mit.edu/mission/communications/ist/corpora/ideval/data/index.html) and the Knowledge Discovery and Data Mining Tools Competition (http://kdd.ics.uci.edu/databases/kddcup99/kddcup99.html).

*5 CCC DATAset 2008 consisted of one variety of malware specimen data, two day's worth of attack communications data, and six month's worth of attack origin data respectively.

*6 MWS2009 papers and presentations for which the author's consent has been received will be published on the following site (http://www.iwsec.org/mws/2009/)(in Japanese).