

Computer Security Group (ICSG)

Industry Connections Activity Initiation Document

Version: 1.0 (Approved), 13 June 2009

1. Background and Purpose

The initial meeting of a computer security interest group was called in October 2008, out of the desire by many in the security industry to pool their experience and resources in response to the systematic and rapid rise in new malware being introduced to the market. It was recognized that the bad actors have been able to leverage the underground economy to gain economies of scale and leverage of specialist tools and services, whereas the security industry was generally responding to threats as individual entities. The term “malware” is not restricted to viruses, Trojans and worms but should cover all forms of malicious content, including web threats such as phishing, scamware, botnet command and control systems, and the tools and services used. While there has been some ad-hoc co-operation in the industry in areas such as malware and phish URL sharing, this co-operation has not been standardized or documented in a format that lends itself to systematic improvement in operational efficiency, or visibility and review by people outside the vertical industries.

An outcome of the October 2008 meeting was the agreement to continue efforts to formalize the cooperative relationships among companies in the computer security area. Based on this agreement, it was decided to form an Industry Connections Security Group (ICSG) activity within the IEEE Standards Association (IEEE-SA), to allow the work to be performed within a safe harbor environment. The IEEE-SA will also provide ICSG with support and act as an arbitrator, if required.

2. Charter and Scope

Within the IEEE-SA, the ICSG activity will be overseen by the IEEE-SA Board of Governors (BOG). The charter of ICSG focuses its activities as follows:

- Providing a forum for discussions related to the sharing of computer security information and best practices.
- Developing, documenting and promoting proposals for computer security information sharing formats, best practices and computer security industry guides. The resulting documents may subsequently be submitted for broader formal review and dissemination as IEEE-SA Standards Information Network (SIN) publications, or submitted for formal standardization using the open processes of the IEEE-SA.
- Creating a roadmap of planned deliverables related to computer security, and reviewing the business reasons and implications behind them.

The work of ICSG should be guided by the following considerations:

- The documents it creates should have tangible benefits throughout the industry to improve the quality and efficiency of protection against security threats.

- To avoid duplication of efforts, problems addressed by ICSG should not already be covered in other industry groups.
- ICSG activities shall not be dominated by any single individual or organization.
- Start with a small, focused and achievable initial deliverable, and later expand the effort to address more challenging issues related to computer security.

3. Proposed Deliverables

ICSG will develop one or more documents concerning the exchange of malware and the meta-data describing and associated with malware. The documents will be created and extended to cover an increasing variety of meta-data exchanges. The initial version will cover malware sample exchange, URLs, and big events such as Conficker. Later versions will cover other types of data, as more extensive use cases are determined.

In addition to specifying formats for exchanging malware related information, ICSG may also document best practices, and may produce other related industry guides, position papers, and technical reports. Additional deliverables and forms of output related to computer security may also be identified as the roadmap is developed.

4. Funding Requirements

No additional contracted services or other expenses are currently anticipated, beyond the basic support services provided to all Industry Connections activities.

5. Initial Members

The membership of ICSG should include broad industry representation from companies that specialize or have a substantive portion of their business in computer security. As the activity grows, ICSG membership will be open to a wide variety of entities that have an active involvement and interest in computer security, including security vendors, industry content contributors (e.g. Banks, ISPs, etc.), educational institutions and governmental organizations.

The initial members in ICSG are the following:

Entity	Address	Contact
McAfee Inc.	3965 Freedom Circle Santa Clara, CA 95054 USA	Jeff Green Jeff.Green@avertlabs.com +1 408 431 0208
Sophos Plc	The Pentagon Abingdon Science Park Abingdon OX14 3YP United Kingdom	Mark Harris Mark.Harris@sophos.com
Symantec Corporation	20330 Stevens Creek Blvd. Cupertino, CA 95014 USA	Vincent Weafer VWeafer@symantec.com

Microsoft Corporation	One Microsoft Way Redmond, WA 98052 USA	Jimmy Kuo JKuo@microsoft.com
AVG Technologies	1901 Summit Tower Blvd., Suite 350 Orlando, FL 32810 USA	Matt Williamson Matt.Williamson@avg.com
Trend Micro Inc.	10101 N. De Anza Blvd. Cupertino, CA 95014 USA	Jamz Yaneza Jamz_Yaneza@trendmicro.com

Revision History:

Revision Number	Author/Editor	Date
0.1 (Draft)	Jeff Green, McAfee	11 December 2008
0.2 (Draft)	Jeff Green, McAfee	07 January 2009
0.3 (Draft)	James Wendorf, IEEE	25 February 2009
0.4 (Draft)	James Wendorf, IEEE	09 March 2009
0.5 (Draft)	James Wendorf, IEEE	25 March 2009
0.6 (Draft)	James Wendorf, IEEE	27 April 2009
0.7 (Draft)	James Wendorf, IEEE	14 May 2009
0.8 (For BOG Approval)	James Wendorf, IEEE	29 May 2009
1.0 (Approved)	James Wendorf, IEEE	13 June 2009