J Comput Virol (2008) 4:159–160
DOI 10.1007/s11416-008-0083-3

FOREWORD

Editorial

Eric Filiol

During the recent years the notorious and man-made phenomenon of malware has been a constant factor in the equation of computer security and probably will be for the foreseeable future. It is thus not surpising that major research efforts are undertaken to get a handle to the problem. One outgrowth of these efforts is the international conferences series on Detection of Intrusions and Malware and Vulnerability Assessment (DIMVA), and it is a pleasure for us to present three selected papers from the fourth and most recent DIMVA conference, held in July 2007 in Lucerne, Switzerland.

The three selected papers look both into the past and the future of browser-related Malware and propose new approaches for detecting worms.

The first paper "On JavaScript Malware and Related Threats" provides the first survey on an important recent class of known attack vectors for Malware that leverage legal and general facilities of the JavaScript language in web browsers, rather than exploiting specific vulnerabilities of the browser code.

The second paper "Enhancing Web Browser Security Against Malware Extensions" presents an entirely new way of undermining the security of web browsers by using the extension (or plugin-in) mechanism of web browsers that does not require any special privileges to seize complete control over the browser.

While the first two papers provide in-depth technical information on imminent browser-related threats and propose first approaches paving the way for appropriate defense, we must not lose sight of continuous threats.

E. Filiol (✉)
Ecole Supérieure et d'Application des Transmissions,
Laboratoire de virologie et de cryptologie,
BP 18, 35998 Rennes, France
e-mail: efiliol@esat.terre.defense.gouv.fr; efiliol@wanadoo.fr

The third paper "On the Adaptive Real-Time Detection of Fast-Propagating Network Worms" accommodates this need by presenting two novel advanced methods based on sequential hypothesis testing for detecting fast-spreading worms, while exhibiting a low false alarm rate.

The three papers were selected in a stringent review process:

The initial submissions to DIMVA were reviewed by an internationally recognized program committee with a competitive acceptance rate of less than 25%. After the presentation of the papers on the conference the programme committee selected high-quality papers with special interest for the audience of the Journal in Computer Virology and invited the authors to submit revised and extended versions of their papers for this special issue. These submissions were further reviewed by at least two reviewers from the DIMVA program committee and at least two reviewers chosen by the editorial board of the journal. The three papers selected as a result of this process constitute novel and significant contributions to the area covered by the Journal in Computer Virology.

The conference series DIMVA is specially relevant for researchers and experts working in the area of computer virology and malware:

Since its inception in 2004 DIMVA provides an academic forum for presentation and discussion of novel mature research in three crucial areas of computer security: intrusion detection, malware detection, and vulnerability assessment. The main focus of DIMVA is thus on reactive methods of computer security, in contrast to proactive mechanisms such as firewalls and secure communication. Due to the fundamental lag between the time when a new vulnerability is discovered and a preventive mechanism gets in place, these three fields are a significant part of a strong security concept. Despite much prior work, both in academia and industry,

new attacks are developed at an ever-increasing pace and constantly challenge existing technology.

The main objectives of DIMVA are to foster scientific exchange in the international security community and to facilitate the dialogue between academics and practitioners. DIMVA has been conceived and is supported by the German Informatics Society (GI). It is organized by GI special interest group Security—Intrusion Detection and Response (SIDAR). Each year the conference features a dynamic two-day scientific program; exciting invited talks; active participation of academic, commercial and governmental institutions; and, last but not the least, an informal, productive atmosphere.

We would like to thank all the authors who spent a significant amount of time preparing their manuscripts for the conference and for this special issue, as well as the reviewers whose diligent work was instrumental in securing the high scientific level of the contributions. We hope that the papers included in this issue will provide valuable insights to scientists as well as practitioners, and will contribute to further progress in such a vital field as computer security.

January 2008 Ulrich Flegel, Guest Editor
Eric Filiol, Editor-in-Chief