ENISA Quarterly Review

Vol. 4, No. 4, Oct-Dec 2008

IN THIS EDITION

enisa
European Network
and Information
Security Agency

ISSN1830-3609

From the World of Security – A Word from the Experts

Tracing the Changing Nature of Cyber-attacks

Evangelos Markatos, Sotiris Ioannidis and Christopher Kruegel

In recent years we have been witnessing a change in the nature, magnitude, visibility and purpose of cyber-attacks on the Internet. These 'winds of change' began in the early '00s with the explosion of a new generation of computer worm cyber-attacks. Propagating as automated self-replicating programmes and fuelled by software vulnerabilities such as buffer overflows, these worms were able to compromise hundreds of thousands of computers in as little as a few minutes. Computer worms with colourful names such as 'Code Red' and 'Slammer' were released into the wild and left their mark on the way we think about cyber-security and the Internet.

Once it was demonstrated that it is possible to compromise a large number of computers on the Internet, organised crime, sensing there was money to be made, started moving onto the scene, hosting their illegal activities on compromised computers and using them, among other things, for sending spam, performing Denial of Service attacks, stealing passwords and even for blackmail. To ensure the longevity of its activities in cyber-space and contrary to massive self-replicated computer worms, organised crime has always kept a low profile. Enlisting new compromised computers, otherwise known as 'bots', became a *stealthy* activity, generating as little traffic as possible, always trying to stay below the radar of detection. Computer worms, being massively large-scale flamboyant events, were no longer the tool of choice to enlist bots, since they attracted the attention of the world (and the police) within minutes.

Traditionally, software vulnerabilities, often in the form of a buffer overflow, have been the vehicles of choice to compromise a computer system. However, cyber-criminals soon realised that the weakest link in the security chain is people. Thus, social engineering is quickly becoming a form of art and the favourite tool for taking over victim computers. Manifesting as business-type, legitimate email messages, phishing emails entice users with the offer of 'free' software (which is actually infected with malware) or various schemes for making easy money on the Internet. The unprecedented success of these schemes has made social engineering a preferred path for taking over personal computers.

As cyber-attacks have moved from large scale worms to below the radar attacks, and from buffer overflows to social engineering, it is time to take a moment to contemplate the future of cyber-attacks. As computers shrink, communications become invisible and continuous, and more and more dependent on the seamless operation of our cyber-infrastructure. It is important therefore to try to envisage the next weakest link in the security chain and thus to predict the next tool of choice for cyber-attackers.

To address these issues, European researchers, supported by the European Commission, have started FORWARD, a co-ordination action whose purpose is to draw up an agenda of research problems by mobilising the critical mass of European researchers in network and systems security. There are three main dimensions along which the researchers have been working:

- smart environments
- malware and fraud
- critical systems.

The results of FORWARD are expected to be used not only by researchers, but also by policy-makers seeking to facilitate a more secure cyber-space. Thus, researchers, policy-makers, decision-makers and practitioners are all encouraged to provide their feedback and follow the activities of FORWARD at www.ict-forward.eu/.

Evangelos Markatos (markatos@ics.forth.gr) is the Director of the Distributed Computing Systems Laboratory at FORTH-ICS, a Professor of Computer Science at the University of Crete, and a member of ENISA's Permanent Stakeholders' Group.

Sotiris Ioannidis (sotiris@ics.forth.gr) is an Associate Researcher at the Distributed Computing Systems Laboratory of FORTH-ICS, and an Adjunct Professor at the Computer Science Department of the University of Crete.

Christopher Kruegel (chris@cs.ucsb.edu) is an Assistant Professor and the holder of the Eugene Aas Chair in Computer Science in the Computer Science Department of the University of California, Santa Barbara.