enisa European Network and Information Security Agency

Quarterly

IN THIS EDITION

Vol. 2, No. 3, Oct 2006

A WORD FROM THE EXECUTIVE DIRECTOR

Executive Director, Andrea Pirotti (right), with security expert Bruce Schneier at ISSE2006

Dear Readers,

The third quarter of 2006 has been extremely productive for ENISA. While we are pleased when we look back, at the same time we look forward, having received the European Commission's Communication on 'A Strategy for a Secure Information Society', which outlines an increased role for ENISA.

Bringing our flagship conference, ISSE2006, to a close, I was delighted to present speakers such as the European Commissioner for Information Society and Media, Viviane Reding, the Minister of Communications of Italy, Hon. Paolo Gentiloni, and security expert, Bruce Schneier, CEO of Counterpane Internet Security, among many other prominent names.

Over the three intensive days of the conference, more than 350 key policy-makers from governments, experts from academia, business and industry exchanged their experiences of best practice, participating in almost 70 workshops and seminars and debating the future of Network and Information Security (NIS). We are now looking forward to next year's ISSE2007, which will take place in Warsaw, Poland. We invite you, therefore, to mark the dates 25-27 September 2007 in your diary and hope that you will join us at this key event for policy-makers, experts and stakeholders.

ENISA's activities during this last quarter included the organisation of workshops and the delivery of a number of reports. For example, the Agency organised the ENISA Risk Management Workshop in conjunction with ISSE2006. A milestone for us has been the creation of the unique European database, www.enisa.europa.eu/rmra, which offers methods and tools for risk management. I would warmly recommend you to visit this site.

ENISA also organised two workshops in Brussels. One, on Computer Emergency Response Teams (CERTs), was a follow-up to the launch of the very first 'Step-by-Step' manual on creating CERTs, and the update and expansion of the map showing more than 112 'CERTS in Europe'. At the second workshop, on Awareness Raising, ENISA presented the 'Users' Guide: How to Raise Information Security Awareness', targeted at Small to Medium-sized Enterprises (SMEs). In response to a request from the Commission, ENISA also published a study on anti-spam measures by Internet Service Providers (ISPs).

Looking ahead, let's bear in mind that our efforts for enhanced NIS are really aimed at the policy level. To quote Commissioner Reding's speech at the i2010 conference in Finland, which was organised by the Finnish EU Presidency:

"To strengthen the European Information Society, we have to get people on board by showing practical benefits for citizens of the

➲

ISSN1830-3609

On Exploiting a File Sharing System for DDoS Attacks

Elias Athanasopoulos, Kostas Anagnostakis and Evangelos Markatos



Over the last few years we have witnessed an increasing number of Distributed Denial of Service (DDoS) attacks on the Internet. These attacks usually rely on previously compromised hosts, known in the colourful language of cyberspace as 'zombies', which repeatedly request a seemingly legitimate service from a targeted (victim) server on the Internet.

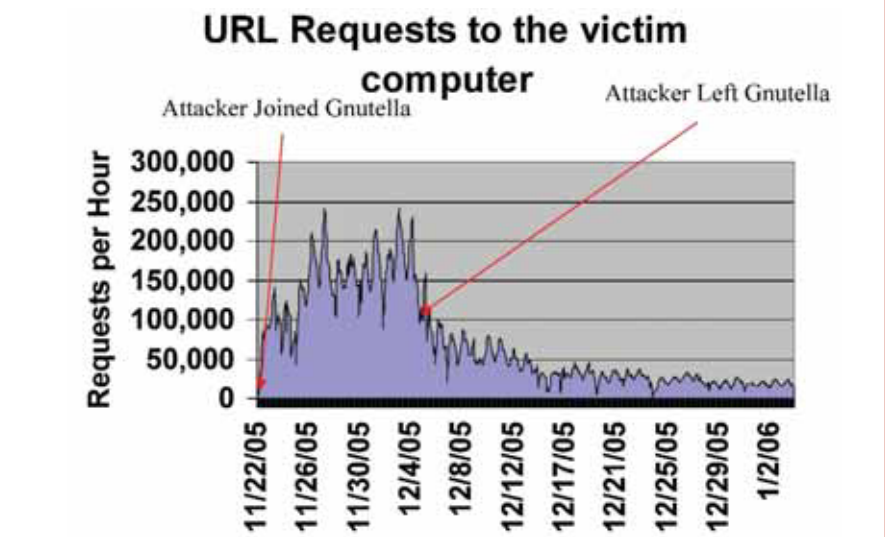
The larger the number of compromised hosts which participate in the attack and the more frequently these hosts request service from the victim computer, the larger the magnitude and ferocity of the attack against the victim. When the magnitude of this DDoS attack reaches a certain threshold, the victim's resources are overwhelmed, making it difficult, if not impossible, to serve any of its legitimate clients. Although it has been widely known that DDoS attacks are not rare, it is astonishing to learn that such attacks exceed several thousand distinct events per week, targeting all sorts of computers ranging from popular web servers to humble dial-up PCs.

Since Denial of Service attacks require control of zombie computers, the fire power of DDoS attackers is limited by the number of compromised computers they control. Recently, however, researchers at FORTH-ICS – http://dcs.ics.forth.gr/ and http://dcs.ics.forth.gr/Activities/papers/gdos.acns06.pdf – have discovered that even non-compromised computers participating in file sharing systems can be used to inadvertently take part in such a Denial of Service attack. Indeed, by exploiting the technical details of the Gnutella protocol, a popular peer-to-peer file sharing system, it is possible to direct a large number of Gnutella peers towards an unsuspecting victim computer which may not even be part of the Gnutella network.

> "it is astonishing to learn that such attacks exceed several thousand distinct events per week"

Transforming the Gnutella network into a Denial of Service attack weapon against a victim computer is based on a simple observation: when a Gnutella peer searches for a file, the attacker always responds that the victim computer has a copy of this file. In this way, the victim computer becomes increasingly popular among a large number of Gnutella peers which repeatedly request all sorts of files from the victim.

Denial of Service attack to a victim computer through the Gnutella file sharing network



Between 22 November 2005 and 4 December 2006 the attacker joined the Gnutella network and tricked Gnutella peers into believing a victim computer had interesting files to download. This resulted in about 150,000 requests per hour to the victim computer. After the attacker left the network in December 2005, tricked Gnutella peers continued to send requests to the victim computer for several more weeks.

Real-world experiments

A series of experiments performed in a controlled environment enabled researchers at FORTH-ICS to measure the validity, magnitude and duration of such a Gnutella-based DDoS attack. To jump-start the attack, they inserted one 'malicious' node in the Gnutella network, which, for a period of about two weeks, responded to all the queries it received, stating that a victim computer has the content requested in the query. The 'victim' computer was a carefully crafted and heavily monitored web server located at FORTH. In this way, over this period of two weeks, the 'victim' web server at FORTH became increasingly popular among Gnutella peers and was the recipient of an increasing number of requests. Indeed, as the graph above suggests, during the period of the first two weeks (when the attacker was an active member of the Gnutella network), the victim computer received an increasing number of requests reaching close to a quarter of a million per hour. Even after the attacker left the Gnutella network and stopped responding to any queries, the victim computer still continued to receive more than 10,000 requests per hour. In total, over the 6-week period of the experiment, more than 300,000 Gnutella peers connected to the 'victim' server and requested to download a file. These Gnutella peers resided in countries practically all over the world. (See diagram below, which provides a colourful and interesting mosaic. All but a handful of grey-coloured countries hosted peers which requested files from our victim server.)

The number of Gnutella peers (which requested files from our 'victim' server) hosted per country varied from low (green) to very high (deep red).

To make matters worse, if the victim computer is hosting a web server, the attacker's response can be carefully crafted so that it contains a URL that matches a file served by the victim web server, effectively deceiving the Gnutella peer into downloading an existing file from the victim computer. Therefore, by tricking Gnutella peers into requesting content from a victim web server, and by tricking the victim web server into thinking that it serves ordinary web clients, the attacker can direct a flood of seemingly legitimate URL requests to the victim computer, abusing its resources. Interestingly enough, these requests towards the victim computer continue to arrive even several weeks after the attacker leaves the Gnutella network and stops sending fake replies on behalf of the victim computer.

> "attackers do not need compromised computers in order to launch their attacks. They have managed to effectively masquerade the attacks as ordinary activities of everyday Internet applications"

Although there is ongoing research underway at FORTH-ICS to detect and avoid such Denial of Service attacks, the potential and effective magnitude of these incidents has yet to be fully quantified. One thing is certain though: we have now moved into an era where attackers do not need compromised computers in order to launch their attacks. They have managed to effectively masquerade the attacks as ordinary activities of everyday Internet applications.

Elias Athanasopoulos is a Research Assistant at FORTH-ICS.

Kostas Anagnostakis is a researcher at I²R and visiting associated researcher at FORTH-ICS.

Evangelos Markatos is the director of the Distributed Computing Systems laboratory at FORTH-ICS, a Professor of Computer Science at the University of Crete, and member of the Permanent Stakeholders Group established by ENISA.