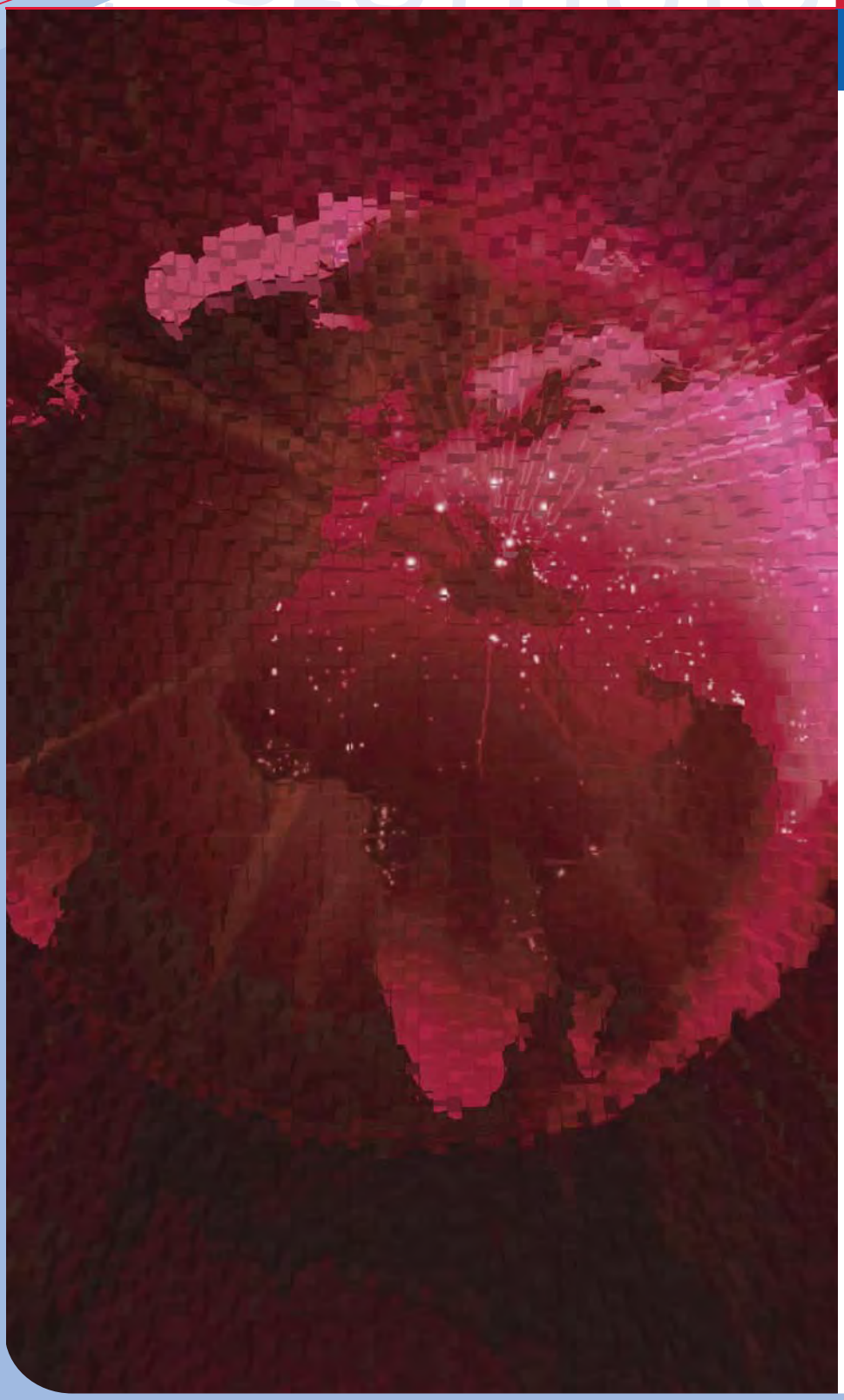
ENISA Quarterly Review

Vol. 4, No. 2, Apr-Jun 2008



IN THIS EDITION

enisa European Network and Information Security Agency

ISSN1830-3609

considerable effort is needed and several parties are involved in order to take it down. Botnets are highly dynamic and can evade countermeasures.

Unfortunately, botnets are not only used for spamming, but also for other kinds of misuse, such as hosting phishing sites, mounting distributed denial of service attacks or spying on confidential data on the infected computers. Among these abusive actions, spam is the most obvious because the bots play an active role – they send out messages that can be detected by spam filters. Thus, detecting spam sources may not only protect against spam in the future, but might also protect against other potential threats such as phishing or denial of service attacks. One mechanism that has an important side-effect when detecting spam is the creation of a reputation service, which could summarise and collect different kinds of abuse and make that information available to others to use.

Challenges

A couple of challenges remain if such a reputation service concept is to actually work. Spam is sent in a very distributed fashion. On the one hand, this could make it difficult to detect a sufficiently large number of spam sources from only a small number of vantage points. This means that, from the perspective of effectiveness and benefit, many different vantage points are required. On the other hand, the lack of one sole vantage point, where all mail is screened, is a big advantage in terms of data protection. Thus, a reputation service should be designed and set up in a distributed fashion. A distributed system prevents a single entity from having control over all data. Moreover, the distributed system enables many reputation sources to feed and store information, which solves the problem of having one single point of data storage.

Another challenge is posed by the fact that spammers may switch to sending spam at a low volume in order to evade spam detection techniques. In fact, even today, some spammers already send only a very few spam messages from one source.

Fortunately, as the quality of spam filters improves, sending spam at low volume will probably render spamming unprofitable by its very nature. In addition, spammers need web space where they can set up their on-line stores and where people can buy the spamvertised products. Nowadays, these hosts are part of a botnet, too. Thus, detecting botnets by spam sources could also reduce the success of fake on-line stores – another advantage of a distributed reputation service.

Both challenges, the distributed nature of spam as well as the adaptation of spammers' tactics, can be mitigated by strong co-operation in the distributed system. If a sufficient number of service providers exchanged information about abused sources, for example spam-sending hosts, such a system could be put in place and would actually help to prevent other abuses.

Christian J. Dietrich (dietrich@internet-sicherheit.de) is a researcher at the Institute for Internet Security, University of Applied Sciences Gelsenkirchen in Germany.

Christian Rossow (rossow@internet-sicherheit.de) was a research student at the Institute for Internet Security, University of Applied Sciences Gelsenkirchen in Germany and worked as a trainee at ENISA.

Norbert Pohlmann (norbert.pohlmann@informatik.fh-gelsenkirchen.de) is a Professor at the Institute for Internet Security, University of Applied Sciences Gelsenkirchen in Germany and a member of ENISA's Permanent Stakeholders' Group (PSG).

Real-world Polymorphic Attack Detection

Michalis Polychronakis, Evangelos Markatos, Yannis Mitsos, Slavko Gajin, Goran Muratovski





The number of attacks against Internet-connected systems continues to grow at an alarming rate. Besides the constantly increasing number of security incidents, we have also been witnessing a steady increase in the sophistication and diversity of attacks. Indeed, during the last few years, there has been a decline in the number of massive, easy-to-spot global worm epidemics, and a shift towards more stealthy and localised attacks against selected targets – a consequence of cyber-criminals trying to keep infected systems under their control for as long as possible without being detected, so that they can continue to make significant financial gains from spam, phishing, malware propagation, denial of service attacks and other illegal activities.

The constant increase in the amount, sophistication and diversity of remote system compromise attacks, and the consequent increase in the deployment and effectiveness of defences, have resulted in an arms race between attack detection and evasion techniques – that is, as detection mechanisms improve, attackers employ increasingly sophisticated methods to evade them. For

>>

example, attackers have already started using techniques such as code obfuscation and polymorphism, which make each instance of the attack 'look' completely different, posing significant challenges to existing network-level detectors. Indeed, using polymorphism, the code in the attack vector – which is usually referred to as 'shellcode' – is mutated so that each instance of the same attack acquires a unique byte pattern, thereby making fingerprinting of the whole breed very difficult. At the same time, accurate attack fingerprinting is becoming increasingly important for the already inherently difficult problem of identifying previously unknown attacks – also known as 'zero-day' attacks – while trying to minimise the rate of false positives.

To detect this new breed of polymorphic attacks, the authors have recently proposed, implemented and deployed network-level emulation – a passive network monitoring approach for the detection of zero-day polymorphic attacks. In contrast with previous work, network-level emulation uses a CPU emulator to dynamically analyse every potential instruction sequence in the inspected traffic, aiming to identify the execution behaviour of certain malicious code classes, such as self-decrypting polymorphic shellcode. Network-level emulation does not rely on any exploit- or vulnerability-specific signatures, which allows the detection of previously unknown attacks, while the actual execution of the attack code on the emulator makes the detector robust to evasion techniques such as self-modifying code. Furthermore, each input is inspected autonomously, making the approach effective against targeted attacks.

We have deployed our prototype implementation, called 'Nemu', as part of LOBSTER (www.ist-lobster.org), a large-scale distributed passive network monitoring infrastructure (featured in EQ Vol. 3, No. 1, Jan-Mar 2007, p5). After almost a year of continuous operation, Nemu has detected **more than a million attacks** against real systems (not honeypots) in the monitored networks, without any false positives. In each installation, Nemu runs on a passive monitoring sensor which inspects all the traffic of the access link that connects the protected network to the Internet. In this article, we collectively report statistics from four deployments in three European National Research Networks and one Educational Network. Barring occasional daily downtimes, the sensors have been continuously operational since 9 March 2007.

As of 13 February 2008, Nemu had captured 1,052,332 attacks targeting 21 different port numbers. Of these attacks, 31.35% were launched from 8981 different external IP addresses against internal hosts, while the other 68.65% originated from a few infected hosts in the monitored networks that were attempting to propagate malware within their own domains on a massive scale. The distribution of external attack source addresses according to country of origin is presented below. Hundreds of thousands of compromised computers all over the world are used by attackers for launching attacks and to further propagate malware. In our observations, the captured external attacks originated from 117 countries, a

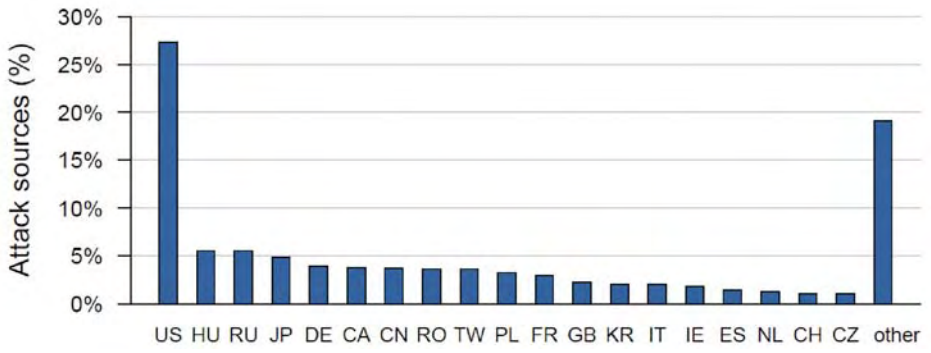


Figure 1: Distribution of attack sources according to country of origin. Category 'other' includes 98 countries.

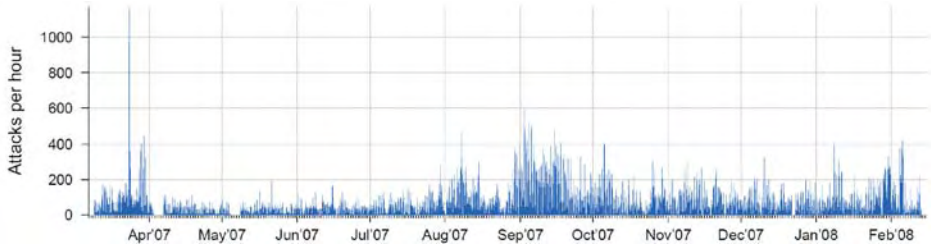


Figure 2: Overall attack activity from deployments of Nemu in four national networks. The graph shows only the attacks that were launched from external hosts against hosts in the protected networks.

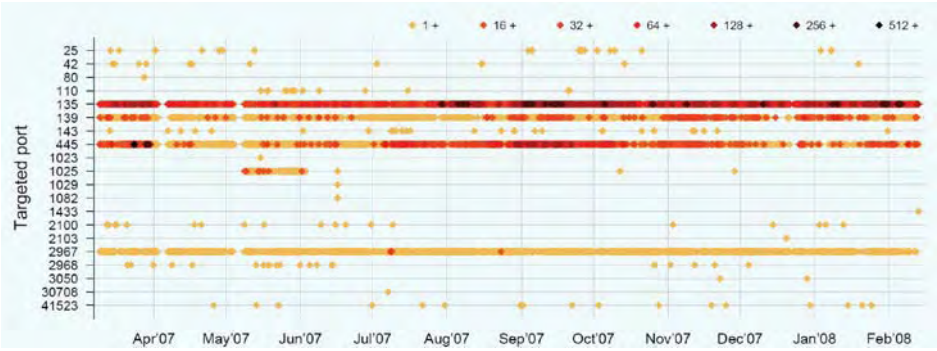


Figure 3: Attack activity according to the targeted port. Although most of the attacks target well known vulnerable services (such as ports 135, 139 and 445), there are also sporadic attacks against less widely used services.

>>

result indicative of the widespread prevalence of malware-infected hosts.

In the following discussion we focus only on those external attacks that targeted hosts within the protected networks.

An overall view of the external attack activity is presented in figure 2. There are occasions with several hundreds of attacks in one hour, mostly due to bursts from a single source attacking all active hosts in local neighbouring subnets.

Figure 3 shows attack activity according to the targeted port. The lower part shows the number of external attacks per hour. As expected, the port numbers of popular Operating System (OS) services associated in the past with well known vulnerabilities, such as 135, 139 and 445, receive the highest number of attacks. Besides common exploits against popular OS services, it is interesting to note that there are also sporadic attacks to less commonly attacked ports such as 1051, 5000, 41523 and so on. These ports correspond to corporate virus scanners, mail servers, backup servers, database management systems and other network services. With firewalls and OS-level protections now being widely deployed, attackers have turned their attention to less well maintained third-party services and applications. Although such services are not very popular among typical home-users, they are commonly found in corporate environments and, most importantly, they usually do not attract sufficient attention when it comes to patching, maintenance and security hardening. Nemu scans the traffic into any service and does not rely on exploit- or vulnerability-specific signatures. Thus it is able to detect polymorphic attacks destined for even less widely used or 'forgotten' services.

In an effort to foster the sharing of real attack activity data among the security research community, anonymised full payload network packet traces of some of the captured attacks are publicly available from http://lobster.ics.forth.gr/traces/.

The attack activity observed so far clearly shows that polymorphic attacks are extensively used in the wild, although attackers usually employ naïve encryption methods, mostly for concealing restricted payload bytes. However, we have also been observing an increasing number of attacks that use more sophisticated polymorphic shellcode engines and obfuscation techniques. Along with the increased diversity in the targeted services – which now include third-party applications and less popular services – these observations are indicative of the change in attackers' tactics and goals.

Michalis Polychronakis (mikepo@ics.forth.gr) is a member of the Distributed Computing Systems Laboratory at FORTH-ICS and a Ph.D. candidate at the University of Crete.

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.

Dr. Yannis Mitsos (ymitsos@admin.grnet.gr) is the Project Co-ordinator of the SEEREN2 project and is responsible for the deployment of regional infrastructure projects within GRNET, the Greek Research and Academic Network.

Dr. Slavko Gajin (slavko.gajin@rcub.bg.ac.yu) is the Deputy Director of Belgrade University's Computing Centre and the designer of the NetIIS network information and management system.

Goran Muratovski (gone@marnet.mk) is Network Manager of Ss. Cyril and Methodius University. In the past he was Chief Technical Officer responsible for the foundation of the MARNet Network Operations Centre.

DNS Infrastructure Resilience Task Force

Paul Kane

Historically, most country code Top Level Domain (ccTLD) registries have operated in the belief that Distributed Denial of Service (DDoS) attacks are targeted only at larger, more prominent global TLDs such as .com, .net, or even large ccTLDs. However, recent attacks have shown that the landscape has changed and that all TLD registries are now at risk of attack. The Internet industry is waking up and looking to community-based solutions to mitigate the threat and effects of such attacks. A robust infrastructure for every TLD registry and service provider is critical to this effort.

An initiative currently being considered by the European Commission is the Domain Name System (DNS) Infrastructure Resilience Task Force (www.dir.org), which comprises participants from industry, universities and government regulators, and is looking at how best to design a robust system that inherently prevents and reduces the impact of any attack. The DNS Infrastructure Resilience Task Force is working with partners such as CommunityDNS.eu (Europe's fastest growing Anycast supplier), providing the Task Force with ample capacity to thwart even the most sophisticated DDoS attacks. This 'black hole technology' essentially attracts – and deals with – malicious, bogus requests to shield genuine traffic during an attack.

>>