

value/costs of new centre establishment;

- to define and pilot a business model that could be used in resource-limited member states and EU regions;
- to pilot the joint development of training programs and common international trainer groups for the selected competence areas;
- to establish cross continental/regional (USA, Latin, Asia, Africa, Australia) partnerships with other networks of similar nature;
- to create a long term partnership and collaboration model with related EU agencies.

Having mobilised the European cyber-crime centres of excellence, SENTER is by definition a project with a wide European base and with ambitious European goals. From Greece to Lithuania and from Spain to Poland, national centres of excellence in cyber-crime will join their activities in order to collectively improve their work: by reducing fragmentation, by avoiding duplication, by sharing experience, and by sharing resources. The collaborating centres will align their agendas, will expose and elaborate on their areas of expertise, will create a common portal, a common identity, and above all, a joint community: a community with a clear European identity so that individual centres break through the barriers of their member states to benefit from and have impact on the wider European family. The network will create joint internet groups in a few highly-focused and carefully-selected

areas: network forensics, computer forensics, open source intelligence. Within these groups member states will be able to collaborate, exchange ideas, plan common activities, exchange staff and test prototypes. In this way the network will be much more than the sum of its parts: it will create expertise which would not have been created otherwise.

The network, however, will not cater only to its current members. To spread the impact to other member states, the network will establish best practices – guides for new centres of excellence being planned in countries that do not yet have such a centre, but would like to create one, and could benefit from previous experiences. The network will create the pathways that enable the expertise to roll from one member state to another and eventually to all the rest of the member states across Europe.

SENER is a joint effort of the Mykolas Romeris University, the Lithuanian Cybercrime Centre of Excellence for Training, Research and Education (L3CE), the Ekonomines konsulatcijos ir tyrimai (EKT), the Masaryk University (MU), the Howest University, the French Cybercrime Centre of Excellence (CECyF), the Tallinn University of Technology (TTU), the University of Applied Science Albstadt-Sigmaringen (UASAS), the International Cyber Investigation Training Academy (ICI), the Foundation for Research and Technology – Hellas (FORTH), the Jožef Stefan Institute (JSI), and the States of Jersey Police.

This work is co-funded by the Internal Security Fund of the European Union. This project has been funded with support from the European Commission.

SENER may be contacted at egidija@l3ce.eu and may be followed on twitter @senterproject.

References:

- [1] Steve Morgan: “Cybersecurity Market Reaches \$75 Billion In 2015; Expected To Reach \$170 Billion By 2020”, *Forbes/Tech* Dec 20, 2015.
- [2] Wall, David: “Cybercrime: The transformation of crime in the information age”, Vol. 4. Polity, 2007.
- [3] Canadian Underwriter: “Global annual tab for cyber crime US\$445 billion, cyber insurance market forecast to grow to US\$20 billion-plus by 2025: AGCS”, September 9 2015, <http://www.canadianunderwriter.ca/insurance/global-annual-tab-for-cyber-crime-us-445-billion-cyber-insurance-market-forecast-to-grow-to-us-20-1003793978/>

Please contact:

Egidija Veršinskienė, Evaldas Bružė
Lithuanian Cybercrime Centre of Excellence for Training, Research, Development and Education (L3CE)
egidija@l3ce.eu, evaldas@l3ce.eu

Evangelos Markatos
FORTH-ICS, Greece
markatos@ics.forth.gr

A Network of Internet Probes for Fighting Cyber Attacks

by Ernő Rigó and Mihály Héder (MTA SZTAKI)

This article introduces a network of advanced internet honeypot probes for gaining situational awareness relating to cyber-attacks. The system is being built on behalf of Hun-CERT. The project is run by MTA SZTAKI and is sponsored by the Council of Hungarian Internet Providers (CHIP).

Individuals with criminal intent will attempt to gain access to any computer that is connected to the internet. Their goal may be to steal data, to gain control over the computer and use it to attack further targets, or to limit the user’s access to their data to extort a ransom.

One way of attacking computers connected to the internet is by trying to break into them from the network. This is done by exploiting vulnerabilities in the operating system, additional software or their insecure configuration. Of course, not all computers have the same software and there are differences in the

way they are updated and configured. A viable strategy for an attacker is, therefore, to attempt an attack on every computer that is accessible – usually by employing an automated script or attack bot. More sophisticated attackers discover the network in a less intrusive way before an attack. They even create

databases of targets so when a new zero-day exploit is discovered, they can attack quickly and in a targeted fashion [1].

To discover attackers and their activity patterns, MTA SZTAKI has started to deploy honeypot probes on various subnets managed by the Hungarian ISPs. The probes are physically implemented as Raspberry Pi computers. In the future, these will be supplemented by virtualized probes – there is already an express demand for them.

The honeypot activity means that the nodes mimic the functionality of real internet services. Currently, the research is focused on implementing the SSH, SMTP and HTTP services. These facilities all run in Docker containers to maximise their isolation while maintaining a low-resource profile. Besides these sources, the firewall of the probe is able to record suspicious network activity on other network ports.

The implemented SSH facility allows attackers to gain access to the honeypot and to issue shell commands. In this way, the nature and the method of attack can be identified. The system also collects the username and password pairs that are being tried by the attackers, which can help in designing passwords that are more secure.

The goal of the SMTP functionality is to mimic a mail server. In a similar fashion to the SSH component, the attackers are allowed to issue commands that are recorded and later analysed. In the final version, the HTTP port will be able to act like a known content-management-system, like Drupal or Joomla.

The probes connect to the operations centre by establishing a VPN connection. This is how the data are collected. Each probe has a unique certificate and each is treated as a potentially hostile host by the centre. This is a safety measure for the unlikely event that a probe actually becomes hacked. The centre itself utilises Logstash, Elasticsearch and Kibana for processing, storing and analysing the logs.

Many R&D problems have been identified and overcome in this project. An important issue was the limited resources of the probe Pi hardware – the available honeypot software needed too

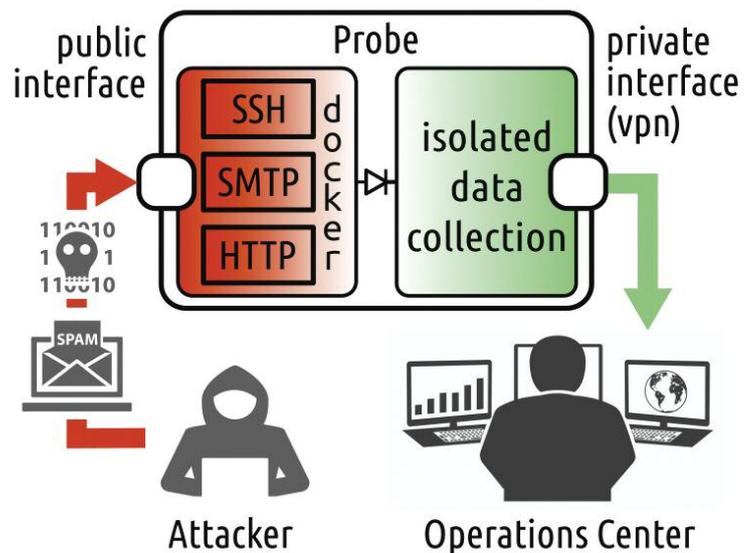


Figure 1: The role of the probe in collecting cybersecurity data.

many resources; therefore, new SSH, SMTP and HTTP honeypot components were necessary.

An interesting problem is defining the actual behaviour of the honeypots in a way that the real nature and purpose of the system remain unknown to an attacker for as long as possible. Another important research problem is that the probes must have different profiles at all levels of the network protocols, even TCP/IP. Otherwise, once an attacker has identified a probe, it could discover the rest easily. This requires advanced, kernel-level customisation of the host operating system. We handle these recurring configuration and customisation tasks with the Ansible orchestration tool.

An interesting question is the optimal number of probes on the network operated by the Hungarian ISPs. In our current batch, we have 60 probes, some of which are not yet deployed. However, we believe that the final number should be around 300 – one in each IP autonomous subnet. This estimate, of course, might change as experience is accumulated with the current probe network.

The data collected have many uses. Some aggregated information will be made available to the general public. Other more detailed information will be accessible to the ISPs that are participating in the project (currently around 80% of the Hungarian ISPs). Naturally, each ISP will access the details of their

own network and only limited information about the other ISPs. Finally, all of the information will be available to Hun-CERT – allowing it to warn every ISP about potential threats and to coordinate countermeasures.

Besides human consumption, the data can be used to feed DNS-based blacklists, which everyone can use to configure their firewall, and SSH, HTTP and SMTP servers. As well, the data can be used for BGP black hole routing at the ISP level.

Reference:

[1] L. Bilge, T. Dumitras: “Before we knew it: an empirical study of zero-day attacks in the real world”, in Proc. of the ACM conference on Computer and Communications Security, 2012.

Please contact:

Ernő Rigó, Mihály Héder
MTA SZTAKI, Hungary
+36 1 279 6266, +36 1 279 6027
rigo.erno@sztaki.mta.hu,
mihaly.heder@sztaki.mta.hu