New Trends of Research and Educational Networks' Security Teams Operation. An Overview of Automated Tools for CERT

Golubev Alexandr, Peter Bogatencov

RENAM Association, Stefan-cel-Mare Bd., 168,
Chisinau, MD-2004, Republic of Moldova; Phone: (373 22) 739827; E-mail: galex@renam.md

ABSTRACT

In the modern networked world the most often criteria of operations are "Quality" and "Speed". These two criteria are cornerstones of the Security Teams operation that make the high quality security research for different incidents through large amount of data and users. This fact makes the work of any security team difficult and has many hidden aspects that are impossible to be handling with the necessary level of quality. The only one solution of simplifying this hard work is to automate this process using different monitoring, ticketing and accounting tools. In this article will be presented an overview of the existing and planned for implementation tools that can be effectively used in various CERTs' especially that operate in Research and Educational networks.

Keywords: CERT, Quality, Speed, Security, Incident analysis tools

1. INTRODUCTION

MD-CERT it is the center of computer security incidents analysis operating as important element of the national research and educational networking infrastructure. MD-CERT is engaged in gathering, registration and analyzing of the facts of all computer incidents (i.e. attempts or the facts of infringements of the owner of the information, or various attacks within network or from the Internet) concerning to the network resources located on the territory of Moldova, but fist of all that are affecting users of the Research and Educational network [1].

Any information about computer incidents, references to useful resources in the field of protection of information technologies, wishes, will be closely considered and as far as possible taken under consideration by Security Teams. MD-CERT guarantees confidentiality of all sent information about incidents. MD-CERT is the noncommercial structure and according to its status is not engaged in the any activity connected with advertising, promotion of those or other decisions and techniques, an exchange of banners, development of commercial projects on information protection, etc.

Realization of CERT in Moldova was initialized by NATO project "Creation of Infrastructure for CERTs in Belarus, Moldova, Ukraine and their Initial Operation" in for operation in Research and Educational networking segment of Moldova.

Specific features of MD-CERT organization and functioning as a part of RENAM networking infrastructure [2,3]:

- MD-CERT in RENAM network was deployed and realizing its functions in close cooperation with other national network security coordinating authorities (e.g. the Center of Special Telecommunications, etc.);
- NREN CERT is a part of the creating at national level common structure of Secure Incident Response Centers;
- RENAM CERT personal training plans include activities at the local level for NREN users and responsible staff and participation in national level and international training events.

2. RENAM COMMUNICATION INFRASTRUCTURE DEVELOPMENT

Basic national research and educational communication infrastructure development has to be accompanied by realization of two principal approaches that affect the networks utility and end users' quality of services:

- New networking and informational services deployment;
- Secure and reliable network operation, operative reaction on any security incident.

Under "New networking and informational services deployment", we understand deployment of the basic networking services and tools, and creating new services for increasing the usability and affectivity of the RENAM network.

However, it is only one path of the RENAM activity. Another path is increasing the level of cyber security for the RENAM users' community and guarantee of confidentiality of information for all RENAM network users. In order to make RENAM network more secure was established and permanently developing its own CERT that is created for providing new security technologies for the whole Moldavian's network community. The main principles of the created MD-CERT operation are [3]:

- Security technologies implementation;
- Organizational measures for effective interaction with users' community.

3. CERT SERVICES

There are many software tools, which can be useful for a CERT team activities support. All of them focused on realization of the presumption that CERT activity has to comprise the following list of actions (some of listed or all) [4]:

- Incident prevention;
- Incident detection;
- Incident analysis;
- Forensic evidence collection;
- Tracing or tracking;
- Incidents post-processing.

In order to follow mentioned activities and providing expected reactions, obtaining necessary results in incident processing there were proposed for implementation some general sets of services, which are listed below.

Reactive Services

- Alerts and Warnings
- Incident Handling
- Incident analysis
- Incident response on site

- Incident response support
- Incident response coordination
- Vulnerability Handling
- Vulnerability analysis
- Vulnerability response
- Vulnerability response coordination

Proactive Services

- Announcements
- Technology Watch
- Security Audits or Assessments
- Configuration and
- Maintenance of Security
- Development of Security Tools
- Intrusion Detection Services
- Security-Related Information Dissemination

Artifact Handling

- Artifact analysis
- Artifact response
- Artifact response coordination

Security Quality Management

- Risk Analysis
- Business Continuity and Disaster Recovery
- Security Consulting
- Awareness Building
- Education/Training
- Product Evaluation or Certification

4. CERT SERVICES IN RESEARCH AND EDUCATIONAL NETWORKS

In order to provide CERT Services for the RENAM network community and connected network's administrators a special CERT server was set up that hosts the CERT web site, incidents databases and other facilities (Figure 1).

This Server must provide the next services to RENAM users [2]:

- Incident form
- Forum
- FAQ
- Links
- Statistics
- Mailing list for notification of CERT Officer.

Using this Server, CERT Officers can access the following services and possibilities:

- Collecting incidents
- Making statistics

- Alerting the constituency.

5. COLLECTING OF THE INCIDENTS

Collecting of the information about the incidents should be done by at least 3 methods [5]:

- Monitoring of the network and fixation of its suspicious parts or actions in the network;
- User will inform by himself about the incident on his part of the network and after CERT officer processes this information, it will be considered as an incident.
- Information about the incident can be received from another CERT system, because these systems and teams must exchange information about the incidents.

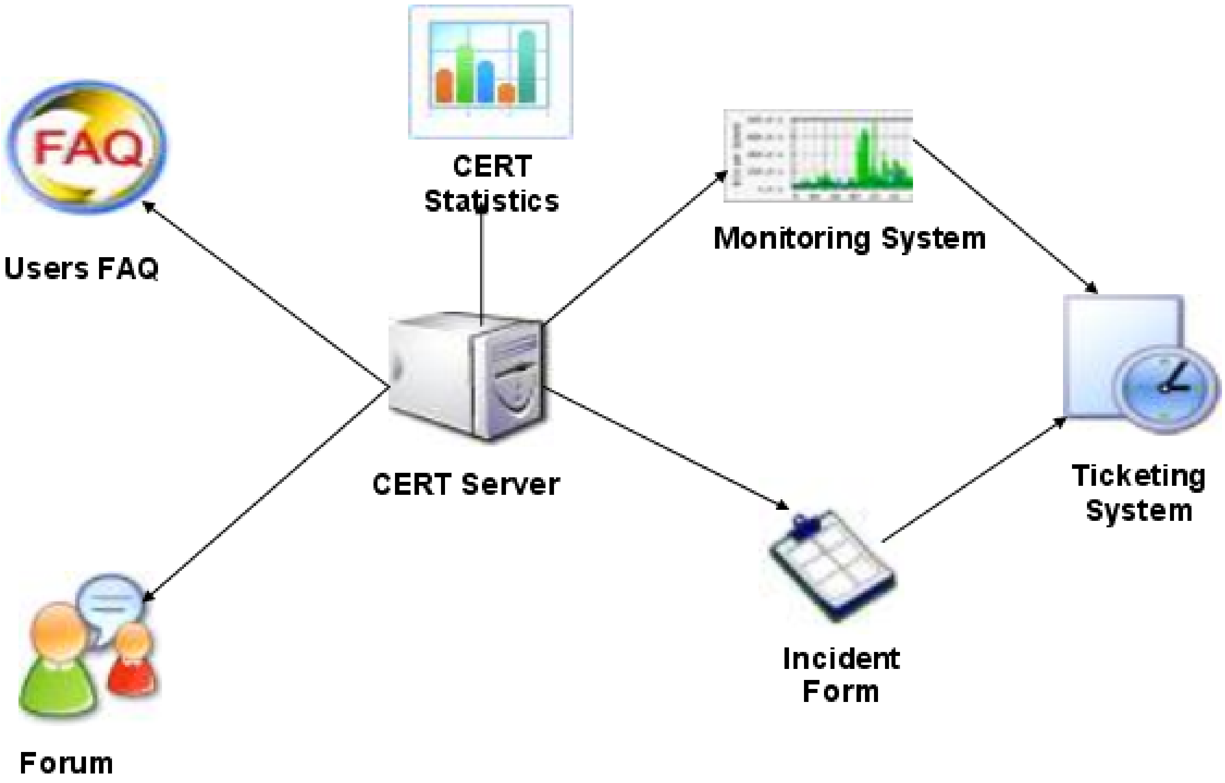

Figure 1. CERT Services.

In the first case, the incident is fixing automatically with help of several software tools and hardware features implemented in the equipment, mostly with help of such protocols as ICMP and SNMP. A lot of software for monitoring networking systems does exist, for example Nagios, NetFlow and NetIIS. These programs are comfortable and well tested, but not always are suitable to monitor of all requests. In addition, there is the necessity for CERT officers to add some specific modules for adjusting existing monitoring system.

Fixation of the incidents via automatic facility of monitoring helps to define existing of the incidents and even avoid the incident automatically. Besides this, the automatic system helps to define statistics and consequence of the incidents and make rudimentary actions to avoid it.

CERT officer also can examine the incident if the incident is registered and sent to CERT officer via one of the following ticketing methods:

- Phone
- Fax
- Registered on the site CERT (as example - www.cert.md);
- Sent via e-mail (as example - inc@cert.md);
- Sending the information about incident using other means.

In this case as in the case of automatic registration of incident on each incident is opening a ticket and it register in the “Ticketing system”.

One of the CERT officers should examine the ticket during one day and if this CERT officer will consider that this is real incident the ticket will be appropriated corresponding priority and information about registering this incident will be sent to user. It means that this incident is already examined by CERT officer. At this time CERT will strive to handle this incident and after successful resolving of the incident this user also will be informed about the result of incident and also will get a manual recommendation about avoiding this incident in the future.

For getting assistance in elimination of the incident the CERT officer could ask not only users but also system administrator of the network that CERT is serving and systems administrators of remote networks, officers of other CERTs as at national and at international level. Every properly registered CERT should either inform each other about danger of incident or assist to each other in its handling.

MD-CERT firstly is functioning for the interests of research community, educational staff and students of Republic of Moldova, though its users can be any people that have any attitude and can be affected by computer incidents. Of course, the priority in examining of the incidents and assisting in their consequences resolving, consultation services have the users of RENAM network.

6. DISTRIBUTED DENIAL OF SERVICE (DDOS) PROTECTION

The development of modern informational technologies, complexity of informational systems increases dependencies of networked resources, individual persons from community and the entire government structures from securing incidents and cyber attacks. Possible blocking and damaging of the main network nodes by hackers can disorganize the normal activity of the society. The similar situation we could see during the cyber war between Russia and Georgia, when in these countries were blocked important networking resources. In Moldova there exists rather developed and permanently extending networking segment as a part of global Internet resources, but unfortunately there aren't any unified system of defense against hackers’ attacks and cyber terrorism.

Creation a system for fighting against DDOS attacks is actual problem that is actively developing in many countries. Creation of effective mechanisms for defending from DDOS attacks of the existing governmental networking infrastructure is a real problem for Moldova too. In the Republic of Moldova exist and functioning large number of Internet resources including commercial and governmental web portals, that are based on poor secured servers’ platforms. According with world experience it is not a problem to crash any server using DDOS. Taking into consideration the experience and recommendations of the cyber-security professionals, now it is clear that not always is necessary to have an illegal botnet to destroy any connected server operation. One server cannot properly defend against attacks. It is impossible to distinguish legacy http request and DDOS attack if intruder use the modern tools for initializing DDOS, and it is impossible to filter these DDOS requests because they come from all over the world. The solution of this problem – is creation of united distributed system for defending against DDOS based on the distributed servers' pools over the territory of the country. It will make possible to distribute identification of the legacy user threw the servers that are not attacked at this moment, that will guard the attacked server from the intruders attacks and will decrease its loading.

6.1 DDOS Attacks classification

The main goal of DoS-Attack is to make online services unavailable (see Figure 2):

- DoS - Attack (Denial of Service) and DDoS - Attack (Distributed Denial of Service) - it is a type of attack at the Information System
- Main goal of these attacks is to block normal work of a web or other Internet connected resource. Hackers try to create such conditions when legacy user will not be able to access this resource.
- If this type of attacks comes from different IP addresses in this case it is called Distributed Denied of service attack (DDOS)

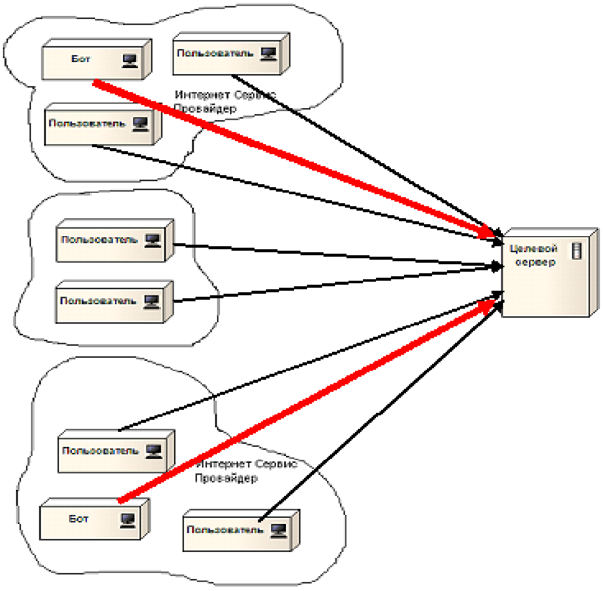

Figure 2. DDOS attack scheme

The main problem of these types of attacks is that it is impossible to make difference between a legacy user and bot.

6.2 Overlay Network – as a measure for defending against DDoS

Overlay network is a global solution for solve DDOS problem for a big network, that allows to redirect and process an request of an legacy user in case if one of the nodes of overlay network is busy. Main idea of using overlay network as a measure for defending against botnets is to use the same tactics like is using by hackers.

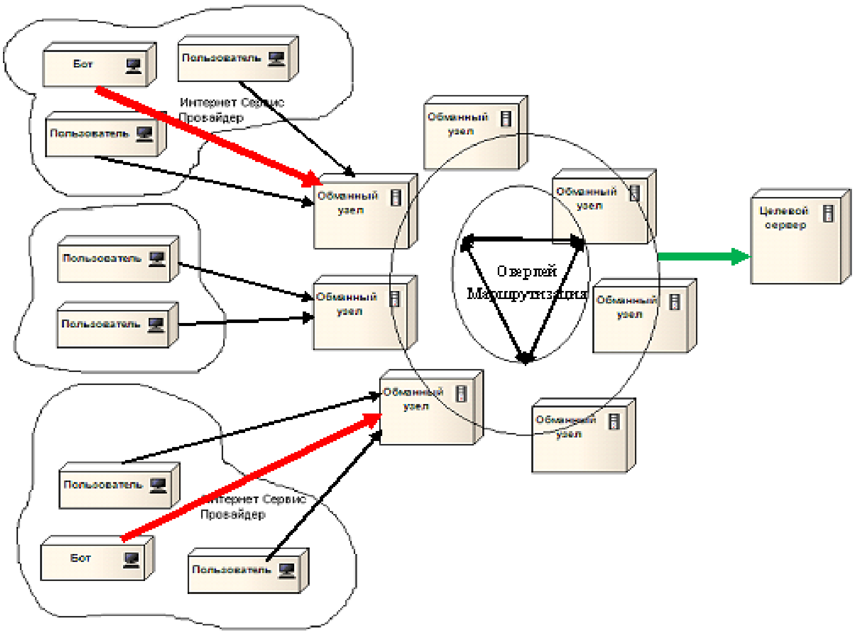

Figure 3. ANTI DDOS overlay

6.3 How DDOS overlay could protect web resources

Main advantages of using of such overlay network:

- Users can access every overlay node even when one of the nodes is under attack;
- Every node have possibility to identify legacy users;
- Request of the user that passed the CAPTHCA - a type of challenge-response test, are processed as secured;
- There is possibility to increase number of nodes in your network;
- One overlay network can offered defense against DDOS for many nodes.

This module can be used as for purposes of securing of commercial resources and can be recommended for implementation in governmental networks at national level. Information about black lists can be distributed for other securing networks that will help with fighting against detected botnets.

Overlay network can be based also on such systems like PlanetLab and GRID. Nodes of the Overlay Network can be distributed by the region, but taking under consideration saving usability of web resources, it is logically that the internet connection speed may be the same for all nodes.

7. CERT STATISTICS

MD-CERT services are collecting a set of valuable statistics:

- General statistic available for every user;
- Statistics for incidents occurred monthly grouped by types;
- Statistics for incidents that were resolved (handled) by CERT officers - for analyzing the work of every CERT officer.

There must be one another SOAP (Simple Object Access Protocol) service that shows the daily and month statistics for publishing on another sites or News boards.

8. CONCLUSIONS

MD-CERT is set up and running. RENAM users and administrators have the main priority in resolving and analysing the incidents. However, simultaneously all Internet users from Moldova and from other countries can use the CERT services providing by RENAM network for resolving the incidents in their networking segments. Another important fact is that results of increasing of network security depend not only from CERT officers, but also from all systems and networks administrators, and from user themselves - from all Internet community.

REFERENCES

1. A. Altuhov, Dr. P. Bogatencov, A. Golubev, Dr. V. Sidorenco. “Development of services for analysis and prevention of incidents in RENAM network”, Proceedings of the 5th International Conference on “Microelectronics and Computer Science”, Volume II, Chisinau, UTM, September 19-21, 2007, pp. 127-130.
2. A. Altuhov, A. Golubev, S. Savchiuk, et al. “Computer Emergency Response Team”, RENAM - National Research and Education Network User’s Conference. Chisinau, May 14, 2007; **http://www.renam.md/uc2007/index.php**
3. Alexei Altuhov, Petru Bogatencov, Alexandr Golubev, Veaceslav Sidorenco. MD-CERT Services for Scientific and Research Communities of Moldova. Proceedings of 7th RoEduNet International Conference 2008. Cluj-Napoca, Romania, 28-30 August, 2008. U.T. Press, Cluj-Napoca, 2008. ISBN 978-973-662-393-6, pp. 58-60.
4. A STEP-BY-STEP APPROACH ON HOW TO SET UP A CSIRT. European Network and information Security Agency (ENISA), 2006
5. Tim Grance, Karen Kent, Brian Kim. "Computer Security Incident Handling Guide". U.S. Department of Commerce, National Institute of Standards and Technology, Computer Security Division Information Technology Laboratory, Special Publication 800-61, Gaithersburg, January 2004, 148 p.