Email-flooder attacks: the estimation and regulation of damage

Vladimir Vyacheslavovich Butuzov, Alexander Grigorievich Ostapenko, Pavel Aleksandrovich Parinov, Grigory Aleksandrovich Ostapenko

Voronezh State Technical University, Moskovsky prospect, 14, Voronezh, 394026, Russian Federation

Abstract. The article considers the theoretical damage function for an information telecommunication system attacked with the help of the Email-flooder malware. Besides, it discusses the dynamics of damage at different stages of attack depending on the actions of attacking subject and attacked object. The authors suggest ways to regulate damage by changing object's parameters. These ways are based on the obtained analytic expression. Moreover, the authors suggest using management efficiency indicator based on integral damage estimation.
[Butuzov V.V., Ostapenko A. G., Parinov P.A., Ostapenko G.A. **Email-flooder attacks: the estimation and regulation of damage.** *Life Sci J* 2014;11(7s):213-218] (ISSN:1097-8135). http://www.lifesciencesite.com. 42

Keywords: damage, Email-flooder, flood attack, management

Introduction

Today, the risk analysis of an information telecommunication system is impossible without damage estimation [1-4] which describes negative effects of the destructive impact of attack.

In this connection, we will consider flood attacks [1, 3, 5] not intended to exhaust the resources of the system attacked and thereby to make it unavailable. The peculiarity of mailbox attack is that user has access to his mailbox but he cannot operate in normal mode due to the huge number of incoming messages [3, 6, 7]. User will have to look through, respond and delete undesirable messages [3, 5, 8]. So, the damage will depend on the number of incoming messages.

Main part

It is possible to mark out the stages of mailbox flood attack with the Email-flooder malware [1, 3, 5, 9, 10]:

1) the attack has began but did not reach success;

2) the attack has succeed;

а) the attack is going on;

б) the attack is complete;

3) the attacked user detected the attack and began to use protection;

4) the elimination of the attack and its aftermaths.

Now let us consider how damage changes depending on the stage of attack and the behavior of attacked user. In common situation, useful messages with intensity $[lambda]_u$ and undesirable messages with intensity $[lambda]_a$ will be received by the mailbox. Thus total intensity of incoming messages will be equal to $([lambda]_a + [lambda]_u)$. The user will operate with intensity $[lambda]_o$.

Suppose user receives m_{kp} messages if attack succeeds at time point t_0. The intensity of message accumulation will be determined by expression (1) because user processes messages, incoming with intensity $([lambda]_a + [lambda]_u)$, with constant intensity $[lambda]_o$:

$$\lambda = (\lambda_a + \lambda_u - \lambda_o). \quad (1)$$

Let X(t) designate the function of message income (the number of incoming messages) and Y(t) designates the function of message processing (the number of processed messages). Figure 1 illustrates their time dependence. Hence the number of messages m_{kp} with a glance to (1) can be expressed this way (2):

$$m_{kp} = (\lambda_a + \lambda_u - \lambda_o)t_0. \quad (2)$$

Other kinds of flood attacks [11-15] are usually based on numerous and as rule meaningless or incorrect requests to a certain computer system or network equipment. However in case of the attack under study, the damage caused by its elimination will not diminish by itself [3, 8, 10]. The amount of damage will be fixed at the value that was at the moment when the attack ended or was detected. Since the mailbox receives m messages, the victim will have to spend its resources to eliminate the aftermaths [5, 8].

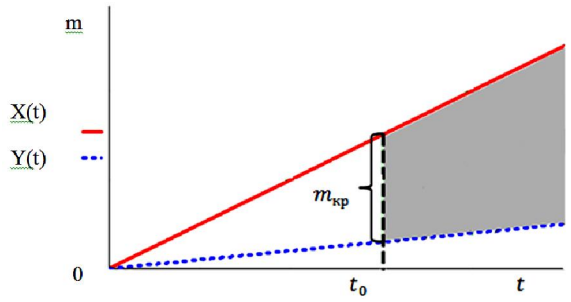

Figure 1. The graph of incoming and processed messages

After the attack succeeds it can end. Then only useful messages will income to the mailbox. The aftermaths of the attack will be eliminated at the time point $t_н$ and the system will return to the processing of only useful messages. In this case user may not notice the attack and will not start applying protection. Figure 2 illustrates this occasion.

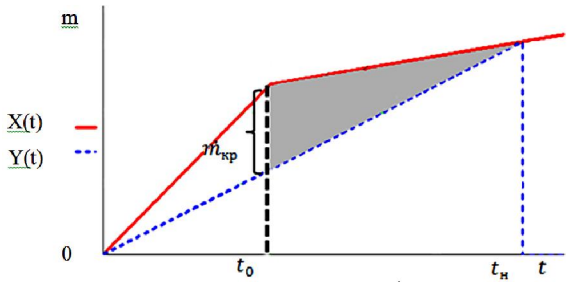

Figure 2. The case when the attack ends after the success

If the attack continues after the success, the damage will increase until user begins to apply protective measures. User should detect attack to start applying protection. The start needs some time during which the damage function will not change. Let user detects the attack at time point t_p, and protection starts at time point $t_з$. Figure 3 illustrates this.

In order to fight with this flood attack, user can enable spare capacity. Thus the intensity of processing the incoming messages will increase. We will designate it as $[lambda]_u$. The damage caused by the attack will be eliminated at time point $t_н$. The intensity $[lambda]_u$ should be maintained until the attack ends. Figure 4 illustrates this.

The increase of processing intensity is not an efficient way to fight with this flood attack because one should maintain the fixed intensity until the end of the attack. The attack can go on for a long time.

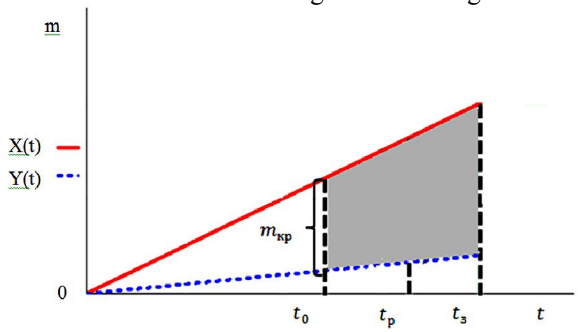

Figure 3. The case when the attack continues after the success

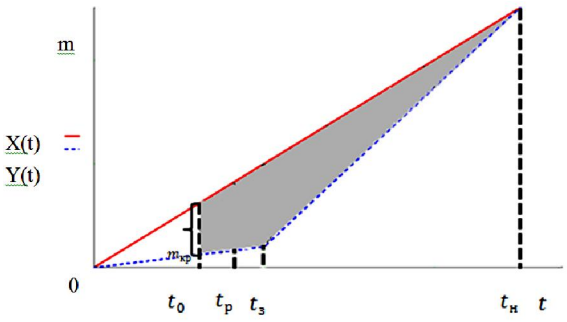

Figure 4. The case when processing intensity is increased to fight with the attack

Moreover, user can block the undesirable sources of information. Such blocking is performed by a certain criterion. For example, if n_u messages from one source are recognized as undesirable, this source will be blocked and all its messages will be deleted. Blocking is performed with intensity $[lambda]_б$.

For blocking, it is necessary to analyze n_u messages. So we can determine the blocking intensity by the following expression (3):

$$\lambda_б = \frac{\lambda_y}{n_u}. \quad (3)$$

Suppose the intensity of all sources is the same and equal to λ_i, then $\lambda_д = \sum \lambda_i$. After the source is blocked, the number of messages goes down by $\lambda_i t$ because all messages of this source are deleted. Then the processing of undesirable messages will be performed by the following function (4):

$$Y(t) = \lambda_i\lambda_б(t-t_з)t - \lambda_o(t-t_з) = \frac{\lambda_i\lambda_y}{n_u}t^2 - \frac{\lambda_i\lambda_y}{n_u}t_з t - \lambda_o(t-t_з). \quad (4)$$

Besides, after the source is blocked, the attack intensity will go down by λ_i. Then the attack intensity will change by the following function (5):

$$\lambda_a^{'} = \lambda_a - \lambda_б \lambda_i t. \quad (5)$$

Then messages will income by the following function (6):

$$X(t) = (\lambda_a^{'} + \lambda_n)t = (\lambda_a - \lambda_б \lambda_i t + \lambda_u)t = -\lambda_б \lambda_i t^2 + (\lambda_a + \lambda_u)t = -\frac{\lambda_y}{n_u}\lambda_i t^2 + (\lambda_a + \lambda_u)t. \quad (6)$$

At time point $t_н$, all the sources will be blocked. The intensity of income will be equal to $[lambda]_u$. All the messages will be processed/deleted, and the processing intensity will return to normal mode – $[lambda]_o$. Figure 5 illustrates this situation.

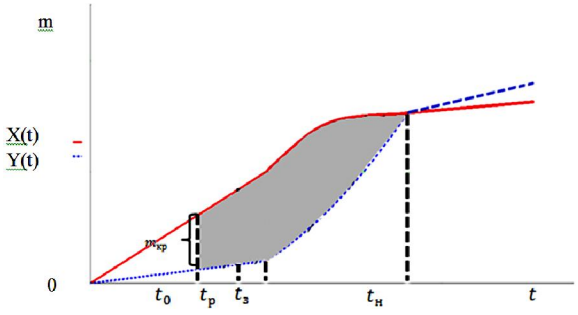

Figure 5. Blocking the sources of attack

Among the variants studied above, the most general and interesting is the last one when the attack continues after the success and user fights with it by both increasing the intensity at the expense of spare capacity and blocking attack sources on the basis of a certain criterion. Let us determine the damage function on grounds of the above analysis. The damage depends on the number of incoming messages. That is why he will be equal to $m_{кр}$ at time point t_0. Now we will determine the damage function (7):

$$u(t) = m_{кр} + \lambda(t - t_0). \quad (7)$$

Substituting (1) and (2) into (7), we get (8):

$$u(t) = (\lambda_a + \lambda_u - \lambda_o)t_0 + (\lambda_a + \lambda_u - \lambda_o)(t - t_0). \quad (8)$$

Simplifying expression (8), we get (9):

$$u(t) = (\lambda_a + \lambda_u - \lambda_o)t. \quad (9)$$

This function will be true until time point $t_з$ (the start of protection). The number of messages received by time point $t_з$ is equal to (10):

$$U(t_з) = (\lambda_a + \lambda_u - \lambda_o)t_з. \quad (10)$$

Messages will income according to expression (6), and be processed according to (4).

On the basis of (4), (6) and (10), we will write down damage function (11):

$$u(t) = (\lambda_a + \lambda_u - \lambda_o)t_з + X(t - t_з) - Y(t). \quad (11)$$

Now we simplify expression (11) and (12):

$$u(t) = -2\frac{\lambda_i \lambda_y}{n_n}t^2 + \left(3\frac{\lambda_i \lambda_y}{n_u}t_з + \lambda_a + \lambda_u - \lambda_o\right)t - \frac{\lambda_i \lambda_y}{n_u}t_з^2. \quad (12)$$

Hence we write down damage function (13):

$$u(t) = \begin{cases} (\lambda_a + \lambda_n - \lambda_o)t, & t_0 \le t \le t_з; \\ -2\frac{\lambda_i \lambda_y}{n_u}t^2 + \left(3\frac{\lambda_i \lambda_y}{n_u}t_з + \lambda_a + \lambda_u - \lambda_o\right)t - \frac{\lambda_i \lambda_y}{n_u}t_з^2, & t > t_з. \end{cases} \quad (13)$$

Figure 6 illustrates the graph of function (13):

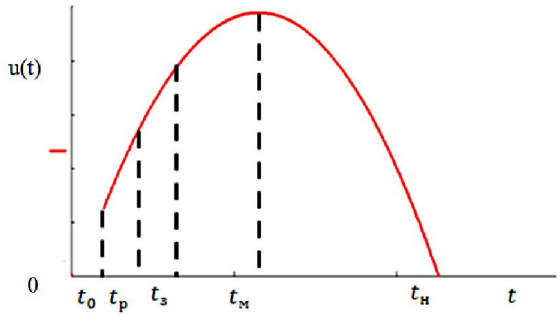

Figure 6. The dynamics of damage caused by a flood attack in the periods of attack and during the elimination of its aftermaths

The obtained expression of damage (13) can be normalized by the maximum value of damage. Damage takes its maximum value in time point $t_м$. Now we will find the value of $t_м$ by finding the derivative of (13) and set it equal to 0:

$$t_м = \frac{3\frac{\lambda_i\lambda_y}{n_п}t_з+\lambda_д+\lambda_п}{4\frac{\lambda_i\lambda_y}{n_п}}. \quad (14)$$

Then we substitute (14) in (12) and obtain the maximum damage (15):

$$u(t_м) = \frac{\left(3\frac{\lambda_i\lambda_y}{n_п}t_з+\lambda_д+\lambda_п\right)^2}{8\frac{\lambda_i\lambda_y}{n_п}} - \frac{\lambda_i\lambda_y}{n_п}t_з^2 - \lambda_о t_з. \quad (15)$$

The normalized damage will simplify to (16):

$$\overline{u(t)} = \begin{cases} \frac{8\lambda_i\lambda_y n_п(\lambda_д+\lambda_п-\lambda_о)t}{\left(3\lambda_i\lambda_y t_з+n_п(\lambda_д+\lambda_п-\lambda_о)\right)^2-8(\lambda_i\lambda_y t_з)^2}, t_0 \le t \le t_з; \\ 8\lambda_i\lambda_y\frac{(-2\lambda_i\lambda_y t^2+(3\lambda_i\lambda_y t_з+(\lambda_д+\lambda_п-\lambda_о)n_п)t-\lambda_i\lambda_y t_з^2)}{\left(3\lambda_i\lambda_y t_з+n_п(\lambda_д+\lambda_п-\lambda_о)\right)^2-8(\lambda_i\lambda_y t_з)^2}, t > t_з. \end{cases} \quad (16)$$

Expression (16) makes it possible to estimate the damage of an Email-flooder attack at an arbitrary point of time.

Let us consider the ways of damage control. In order to reduce the damage, one should influence system parameters the following way [3, 4, 8]:

- to implement the protective measure;
- to change the settings of protection;
- to increase the productivity.

Let us consider how the damage curve will change if these methods of minimization are applied.

If the protective measures are implemented, the attack will be detected earlier and the counteraction will start earlier. So, parameter $t_з$ will be reduced. Figure 7 shows the curves of risk when parameter $t_з$ changes by $\Delta t_з$.

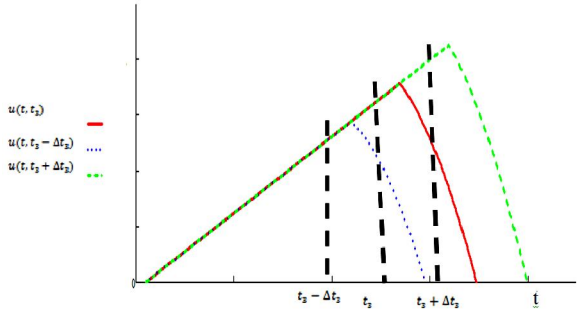

Figure 7. The graphs of damage function if parameter $t_з$ changes by $\Delta t_з$

If we change the criterion by which the source is recognized undesirable, we will be able to diminish the time period of undesirable source detection. Figure 8 shows the graphs of damage function in case when parameter $n_ц$ changes by $\Delta n_ц$.

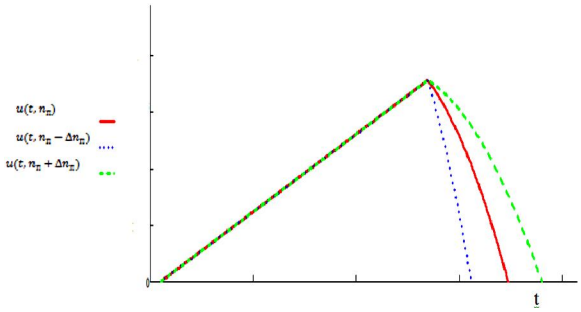

Figure 8. The graphs of damage function if parameter $n_п$ changes by $\Delta n_п$

In addition to protective measures and changing their setting, we can increase the intensity of undesirable message detection $[lambda]_y$ by value $\Delta[lambda]_y$ at the expense of spare capacity. Figure 9 shows the graphs of risk function if parameter $[lambda]_y$ changes by $\Delta[lambda]_y$.

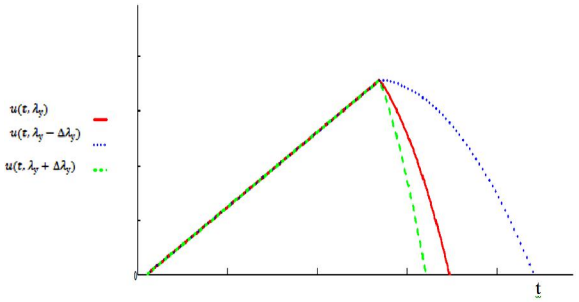

Figure 9. The graphs of damage function if parameter $[lambda]_y$ changes by value $\Delta[lambda]_y$

In order to assess the results and choose the way of loss minimization, we will use the integral damage because this parameter is the expected damage and has the sense of designated average damage value caused for the system at the time interval studied. The integral estimation of damage can be found from expression (17):

$$u_{\Sigma} = \frac{8\lambda_i\lambda_y n_n}{(2\lambda_i\lambda_y t_z + n_n(\lambda_a+\lambda_n-\lambda_o))^2-(2\lambda_i\lambda_y t_z)^2}\left(\frac{(\lambda_a+\lambda_n-\lambda_o)t_z^2}{2}-\right.$$

(17)

$$\left.2\frac{\lambda_i\lambda_y}{2n_n}(t_n^3 \quad t_3^3)+\left(3\frac{\lambda_i\lambda_y}{n_n}t_z+\lambda_n+\lambda_o\right)(t_n^2 \quad t_3^2)\quad\left(\frac{\lambda_i\lambda_y}{n_n}t_z^2\right)(t_n \quad t_3)\right)$$

where t_n is the moment when the attack ends.

The following parameters can be used as the criteria of damage control quality:

- the efficiency of damage control (18):

$$E_{md} = \frac{u_{bd\Sigma} - u_{ad\Sigma}}{C_{md}}, \quad (18)$$

where $u_{bd\Sigma}$ is the integral damage before control measures;

$u_{ad\Sigma}$ is the integral damage after control measures;

C_{md} is the total cost of damage control measures совокупная стоимость;

- the economic efficiency of damage control (19):

$$E_e = \frac{P_{md}}{C_{md}}, (19)$$

where P_{md} is the expected profit of damage control;

C_{md} is the total cost of damage control measures.

These criteria allow us both to take into account both the results of control – risk level – and to choose the most efficient control method from the point of view of expenditure.

Conclusion

So, we obtained expression (16) which makes it possible to estimate the extent of damage at an arbitrary time point if we know the intensity of flood attack $[lambda]_a$, the intensity of undesirable message processing $[lambda]_o$, the intensity of undesirable message deletion $[lambda]_y$ and the detection time of flood attack t_p. Besides, we obtained expression (17) which makes it possible to estimate the integral damage. Its value can be used for the assessment of damage control (18, 19).

Findings

The obtained results can be used for further assessment and regulation of risk for information telecommunication system in case of Email-flooder attack.

Corresponding Author:
Dr.Butuzov Vladimir Vyacheslavovich
Voronezh State Technical University
Moskovsky prospect, 14, Voronezh, 394026, Russian Federation

References

1. Ostapenko A.G., S.S. Kulikov, N.N. Tolstykh, Y.G. Pasternak and L.G. Popova, 2013. Denial of Service in Components of Information Telecommunication Systems Through the Example of “Network Storm” Attacks. World Applied Sciences Journal 25 (3): 404-409.
2. Ostapenko G.A., L.V. Parinova, V.I. Belonozhkin, I.L. Bataronov and K.V. Simonov, 2013. Analytical Models of Information-Psychological Impact of Social Information Networks on Users. World Applied Sciences Journal 25 (3): 410-415.
3. Ostapenko G. A., D. G. Plotnikov, O. Y. Makarov, N. M. Tikhomirov and V. G. Yurasov, 2013. Analytical Estimation of the Component Viability of Distributed Automated Information Data Systems. World Applied Sciences Journal 25 (3): 416-420.
4. Kalashnikov A.O., Y.V. Yermilov, O. N. Choporov, K.A. Razinkinv and N.I. Barannikov, 2013. Ensuring the Security of Critically Important Objects and Trends in the Development of Information Technology. World Applied Sciences Journal 25 (3): 399-403.
5. Empirical Analysis of Denial of Service Attack Against SMTP Servers Boldizsar Bencsath, Miklos Aurel Ronai Laboratory of Cryptography and Systems Security (CrySyS) Department of Telecommunications. International Journal of Computer Science and Security (IJCSS), 4 (6): 537-550.
6. Mengjun X., Heng. Yin, and H. Wang, 2006. An effective defense against email spam laundering. In CCS ’06: Proceedings of the 13th ACM conference on Computer and communications security, New York, pp: 179-190.

7. Microsoft Corporation. Microsoft Security Bulletin MS10-024: Vulnerabilities in microsoft exchange and windows smtp service could allow denial of service (981832), 2010.
8. Boldizsar Bencsath, Miklos Aurel Ronai, 2007. Empirical analysis of denial of service attack against smtp servers. In Proceedings of The 2007 International Symposium on Collaborative Technologies and Systems, pp: 72-79.
9. Ying X. and R. GuÃl'rin, 2005. On the robustness of router-based denial-of-service (DoS) defense systems. SIGCOMM Comput. Commun. Rev., 35(3): 47–60.
10. Hussain, A., J. Heidemann, and C. Papadopoulos, 2003. A framework for classifying denial of service attacks. In SIGCOMM '03: Proceedings of the 2003 conference on Applications, technologies, architectures, and protocols for computer communications, New York, pp: 99-110.
11. Kulikov, S. S., 2013. Calculation the overall risk of information and telecommunication system caused by effect "unicast flooding" in several components. Information and Security, Voronezh, 2: 199-202.
12. Ostapenko, G. A., 2013. Analytical modelling of implementation process of DDoS-attack such as HTTP-flood. Information and Security, Voronezh, 2: 107-110.
13. Kornev, D. A., 2012. An active methods of detecting SYN-flood attacks. Information and Security, Voronezh, 2: 189-196.
14. Kulikov, S. S., 2013. Generic risk assessment of information and telecommunication systems with asynchronous "unicast flooding" effects. Information and Security, Voronezh, 2: 251-252.
15. Bursa, M. V., 2013. DDoS-attack oninformation and telecommunication systems: risk-management. Information and Security, Voronezh, 2: 255-256.

5/1/2014