Communications in Applied Analysis, **23**, No. 2 (2019), 359-382 ISSN: 1083-2564

A NEW ANALYSIS OF CRYPTOLOCKER RANSOMWARE AND WELCHIA WORM PROPAGATION BEHAVIOR. SOME APPLICATIONS. III

NIKOLAY KYURKCHIEV[1], ANTON ILIEV[2], ASEN RAHNEV[3], AND TODORKA TERZIEVA[4]

[1,2,3,4]Faculty of Mathematics and Informatics
University of Plovdiv Paisii Hilendarski
24, Tzar Asen Str., 4000 Plovdiv, BULGARIA

ABSTRACT: In this paper we receive new models that in some situations can be applied to model computer viruses propagation. Welchia worm and Cryptolocker ransomware have a long growing phase in contrast to many other threats. In September 2013 the CryptoLocker malware starting its invasion using mainly P2P ZeuS (aka Gameover ZeuS) malware. CryptoLocker' main aim was to receive money from the unsuspecting victims for decrypting their files. Welchia worm uses a vulnerability in the Microsoft remote procedure call service. Welchia firstly checks for Blaster worm and if it is exists continues with Blaster deletion as well as takes care for computer to be immunised for Blaster worm. Also we modeled Malicious high–risk Android App volume growth; Malware evolution; Number of users attacked by Trojan-Ransom malware; Number of users attacked by crypto-ransomware; Number of unique users attacked by Trojan-Ransom.AndroidOS.Fusob; and "Seasonal data". As the authors in [3] mention: "Even traffic traces used in research papers (e.g. Slammer [4] and Code-red [5]) are not public. From the published papers [4], [5] we are not able to find parameters that can be used in our model". Many researchers make a hard efforts to describe adequately situation connected to worm propagation [15]–[63].

AMS Subject Classification: 97N50

Key Words: cryptolocker ransomware, Welchia worm, Malicious high-risk Android applications, Trojan-Ransom malware, crypto-ransomware, "Seasonal data", Trojan-Ransom.AndroidOS.Fusob, superposition of sigmoidal functions

Received: November 12, 2018 ; **Accepted:** March 7, 2019 ;
Published: March 8, 2019. **doi:** 10.12732/caa.v23i2.7
Dynamic Publishers, Inc., Acad. Publishers, Ltd. http://www.acadsol.eu/caa

1. PRELIMINARIES

From the perspective of applied mathematics and modeling sigmoid functions find their place in numerous areas of life and social sciences, physics and engineering, to mention a few familiar applications: population dynamics, artificial neural networks, signal and image processing antenna feeding techniques, finances and insurance.

For $r \in \mathbb{R}$ denote by $h_r \in \mathbb{H}(\mathbb{R})$ the (interval) Heaviside step function given by

$$h_r(t) = \begin{cases} 0, & \text{if} \quad t < r, \\ [0,1], & \text{if} \quad t = r, \\ 1, & \text{if} \quad t > r. \end{cases}$$

For $r = 0$ we obtain the basic Heaviside step function $h_0(t)$.

Sums of sigmoid functions. For a given vector $r = (r_1, r_2, ..., r_k) \in \mathbb{R}^k$, such that $r_1 < r_2 < ... < r_k$, and a vector $\alpha = (\alpha_1, \alpha_2, ..., \alpha_k) \in \mathbb{R}^k$ denote

$$H(r, \alpha; t) = \sum_{i=1}^{k} \alpha_i h_{r_i}(t).$$

Function $H(r, \alpha; t)$ is a step function with k steps (jumps).

Several practically important families of smooth sigmoid functions arise from population dynamics.

Sigmoid functions find multiple applications to neural networks and cell growth population models.

A classical example is the Verhulst population growth model.

Verhulst model makes an extensive use of the *logistic* sigmoid function

$$s_0(t) = \frac{a}{1 + e^{-kt}}.$$

Theorem 1. *[64] For the Hausdorff distance $d = \rho(h_0, s_0)$ between the Heaviside step function h_0 and the sigmoid Verhulst function s_0 (with $a = 1$) the following inequalities hold for $k \geq 2$:*

$$\tilde{d}_l = \frac{\ln(k+1)}{k+1} - \frac{\ln\ln(k+1)}{(k+1)\left(1 + \frac{1}{\ln(k+1)}\right)} < d$$
$$< \frac{\ln(k+1)}{k+1} + \frac{\ln\ln(k+1)}{(k+1)\left(\frac{\ln\ln(k+1)}{1-\ln(k+1)} - 1\right)} = \tilde{d}_r. \quad (1)$$

The Verhulst logistic model is considered as a basic example to introduce several related mathematical problems: approximation of step and cut functions by means of logistic function, fitting a sigmoid model to time course measurement data, etc.

Similarly, one can construct sums of other suitably shifted sigmoid functions.

Here we are interested in arbitrary shifted (horizontally translated) logistic functions.

Both the step function and the logistic function preserve their form under horizontal translation—note that Verhulst equation possess constant isoclines.

Focusing on the shifted logistic function we have

$$s_r(t) = s_0(t - r) = \frac{a}{1 + e^{-k(t-r)}}.$$

Here we consider the following superposition of sigmoid functions:

$$S(t) = \sum_{i=1}^{n} \frac{a_i}{1 + e^{-k_i(t-r_i)}}. \quad (2)$$

For typical example of superposition of three sigmoids see Fig. 1.

In more complicated growth situations a more precise way for describing is by our new approach by superposition of more sigmoids.

Constructive approximation theory by superposition of sigmoidal functions can be found in [67], [66].

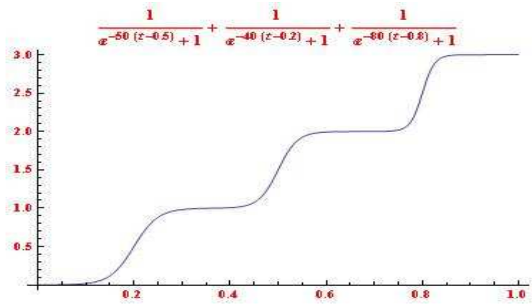

Figure 1: Superposition of three sigmoids.

2. ANALYSIS OF CRYPTOLOCKER RANSOMWARE INFECTION BEHAVIOR

The Cryptolocker ransomware was initialed on September 5, 2013 to May, 2014. The target of this cyberattack was OS Windows.

The malware is encrypted known types of files on the local and shared hard drives using RSA public-key cryptography.

The decryption keys are managed only by Cryptolocker servers. On the computer display window opens which contains the text for the users that they have limited time to pay using bitcoins.

There no way to control that the paying of offered amount will give back encrypted information.

Firstly we photographed the data from Fig. 2 [61].

After that we made them cumulative data:

$$data\_Cryptolocker := \{\{0, 29032\}, \{1, 185484\}, \{2, 274194\}, \{3, 309678\},$$

$$\{4, 364517\}, \{5, 393549\}, \{6, 433872\}, \{7, 493549\}, \{8, 545162\}\}$$

We use the following model:

$$M^*(t) = \frac{a_1}{1 + e^{-(t-0.9)}} + \frac{a_2}{1 + e^{-(t-4)}} + \frac{a_3}{1 + e^{-(t-8)}}.$$

The fitted model for

$$a_1 = 319354; \;\; a_2 = 100814; \;\; a_3 = 260940$$

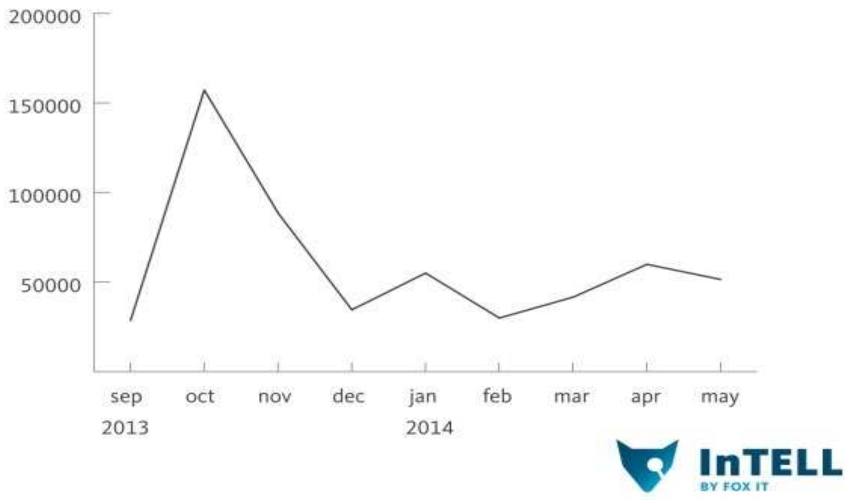

Figure 2: Infections per month [61].

has the form:

$$M^*(t) = \frac{319354}{1+e^{0.9-t}} + \frac{100814}{1+e^{4-t}} + \frac{260940}{1+e^{8-t}}.$$

Here we will show how modelling approach given here will approximate these data, see Fig. 3.

For contemporary applicable study on sigmoids and some of their applications see the monographs [9]–[14].

3. ANALYSIS OF WELCHIA WORM INFECTION BEHAVIOR

For epidemic as Welchia worm it is appropriately to use a model

$$M^{**}(t) = \frac{a_1}{1+e^{-(t-3)}} + \frac{a_2}{1+e^{-(t-8)}} + \frac{a_3}{1+e^{-(t-13)}} + \frac{a_4}{1+e^{-(t-18)}} + \frac{a_5}{1+e^{-(t-25)}},$$

for approximating data from the statistics collected on an individual Welchia [62] honeypot administered by Frederic Perriot between August 24th, 2003 and February 24th, 2004, shown in Fig. 4.

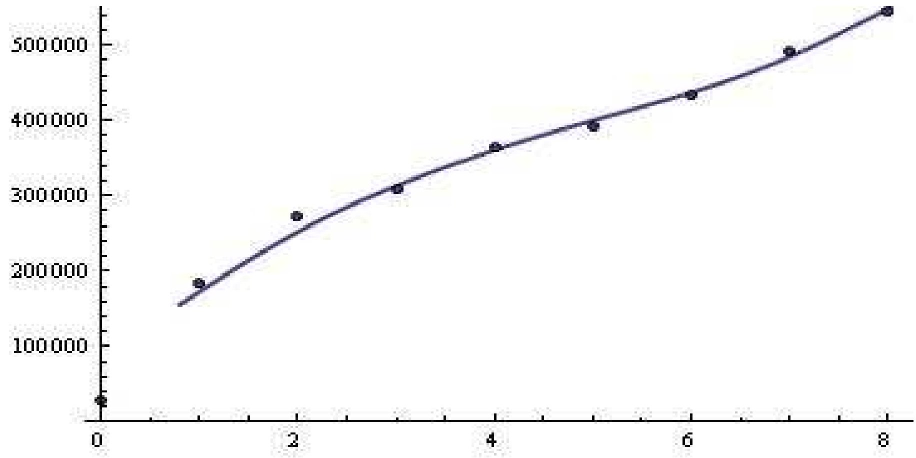

Figure 3: The fitted model $M^*(t)$.

We will explore this example by photographing the data from Fig. 4.

$data\_Welchia := \{\{1.1, 1000\}, \{2, 2333\}, \{3, 3500\}, \{4, 5000\}, \{5, 6833\},$
$\{6, 8000\}, \{7, 9333\}, \{8, 10500\}, \{9, 12000\}, \{10, 14000\}, \{11, 16333\},$
$\{12, 18167\}, \{13, 19667\}, \{14, 21000\}, \{15, 22667\}, \{16, 23667\},$
$\{17, 25000\}, \{18, 26333\}, \{19, 27500\}, \{20, 28333\}, \{21, 29333\},$
$\{22, 29500\}, \{23, 29500\}, \{24, 29500\}, \{25, 29500\}, \{26, 29500\},$
$\{27, 29500\}, \{28, 29500\}, \{29, 29500\}, \{30, 29500\}, \{31, 29667\}, \{32, 29667\}\}$

The fitted model for

$$a_1 = 7028.35; \ \ a_2 = 8037.49; \ \ a_3 = 8426.91; \ \ a_4 = 5903.66; \ \ a_5 = 173.405$$

has the form:

$$M^{**}(t) = \frac{7028.35}{1+e^{3-t}} + \frac{8037.49}{1+e^{8-t}} + \frac{8426.91}{1+e^{13-t}} + \frac{5903.66}{1+e^{18-t}} + \frac{173.405}{1+e^{25-t}}.$$

We receive an impressive result when approximating these data, see Fig. 5.

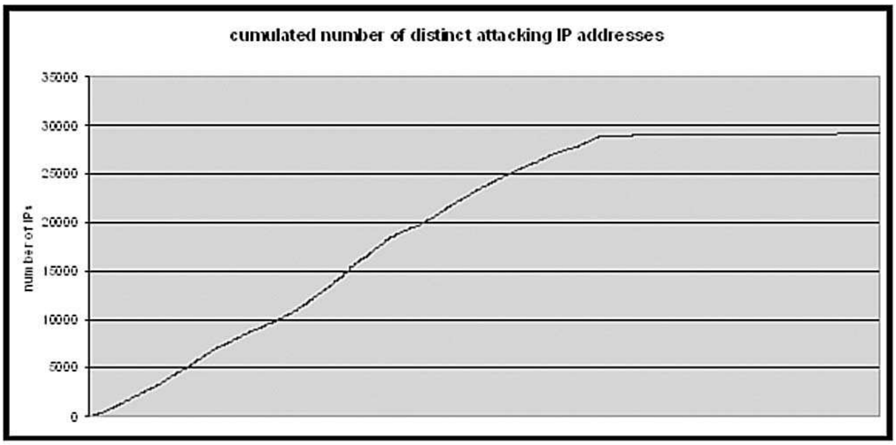

Figure 4: The cumulative number of Welchia attackers [62].

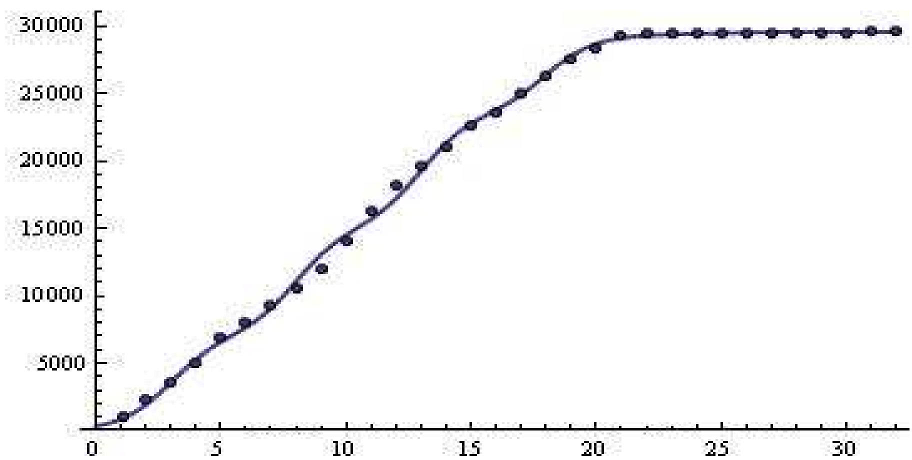

Figure 5: The fitted model $M^{**}(t)$.

4. ANOTHER APPLICATIONS

The model can be used for "seasonal data" fitting. Firstly we photographed the data from [63], see Fig. 6:

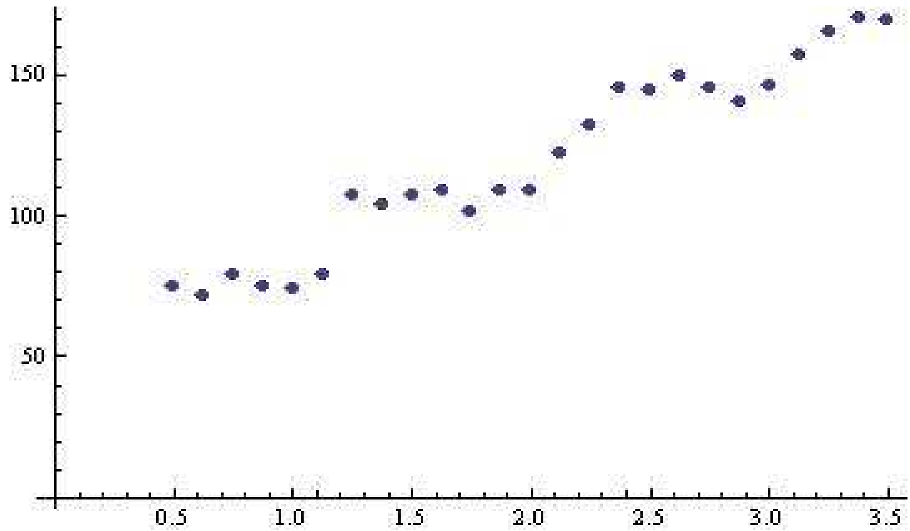

Figure 6: The "Seasonal data" [63].

$Seasonal\_data := \{\{0.5, 76\}, \{0.625, 72\}, \{0.75, 80\}, \{0.875, 76\}, \{1, 75\},$

$\{1.125, 80\}, \{1.25, 108\}, \{1.375, 105\}, \{1.5, 108\}, \{1.625, 110\}, \{1.75, 102.5\},$

$\{1.875, 110\}, \{2, 110\}, \{2.125, 122.5\}, \{2.25, 132.5\}, \{2.375, 146\}, \{2.5, 145\},$

$\{2.625, 150\}, \{2.75, 146\}, \{2.875, 141\}, \{3, 147\}, \{3.125, 158\}, \{3.25, 166\},$

$\{3.375, 171\}, \{3.5, 170\}\}$

The fitted model

$$M^{***}(t) = \frac{2874.17}{1+e^{1-t}} - \frac{10420.4}{1+e^{1.5-t}} + \frac{16581.7}{1+e^{2-t}} - \frac{13286.6}{1+e^{2.5-t}} + \frac{4580.11}{1+e^{3-t}}$$

is visualized on Fig. 7.

5. MALICIOUS AND HIGH–RISK ANDROID APP VOLUME GROWTH

We will show how it can be modelled data in [68] for Malicious and High–Risk Android App Volume Growth, see Fig. 8.

The fitted model

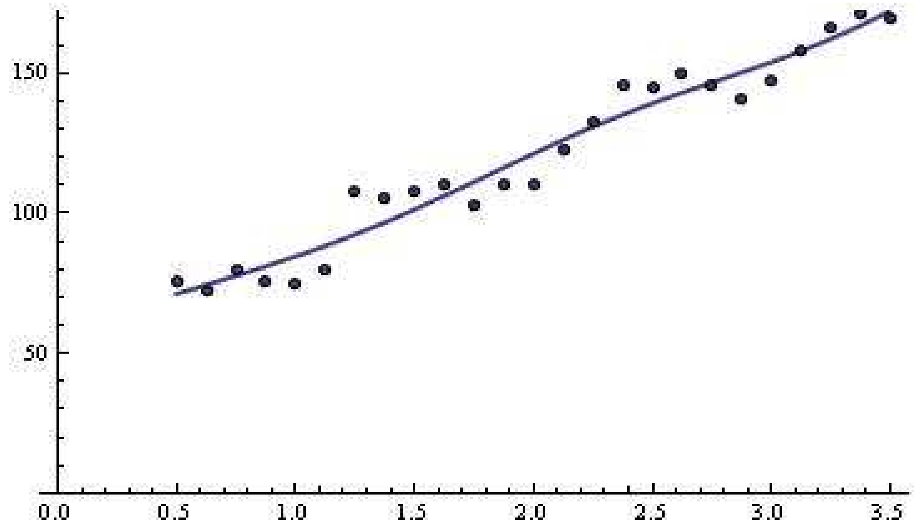

Figure 7: The fitted model $M^{***}(t)$ for "Seasonal data".

$$M^{****}(t) = \frac{2.70186 * 10^6}{1+e^{1-t}} - \frac{1.17754 * 10^7}{1+e^{1.5-t}} + \frac{2.11802 * 10^7}{1+e^{2-t}} - \frac{1.85889 * 10^7}{1+e^{2.5-t}} + \frac{6.71282 * 10^6}{1+e^{3-t}}$$

is depicted on Fig. 9.

6. MALWARE EVOLUTION

We will describe how it can be modelled data in [68] for Malware Evolution, see Fig. 10.

The fitted model

$$M^{*****}(t) = \frac{1207.4072532972086}{1+e^{-0.5(-9+t)}} + \frac{860.7667574563771}{1+e^{-0.5(-6+t)}}$$

is shown on Fig. 11.

Figure 8: Malicious and High–Risk Android App Volume Growth [68].

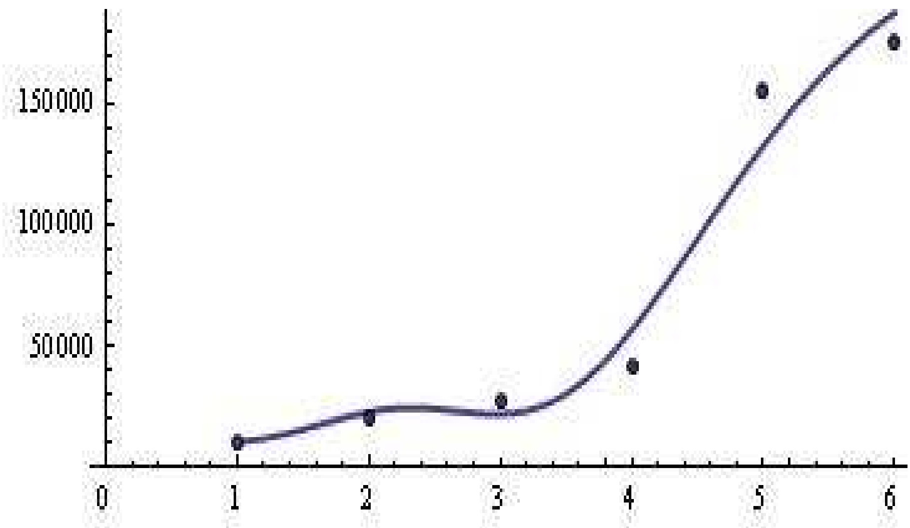

Figure 9: The fitted model $M^{****}(t)$ for Malicious and High–Risk Android App Volume Growth.

7. NUMBER OF USERS ATTACKED BY TROJAN-RANSOM MALWARE

We will study how it can be modelled data in [69] for the number of users attacked by Trojan-Ransom malware (Q4 2014 - Q3 2015), see Fig. 12. The

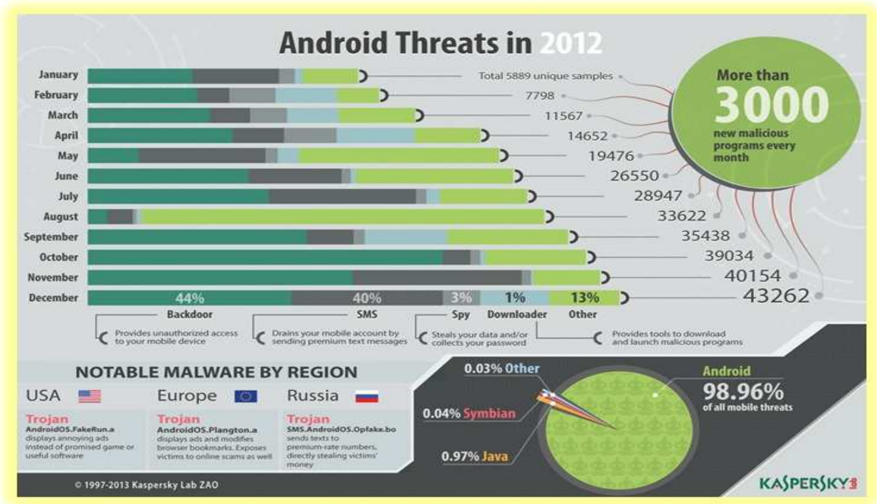

Figure 10: Malware Evolution [68].

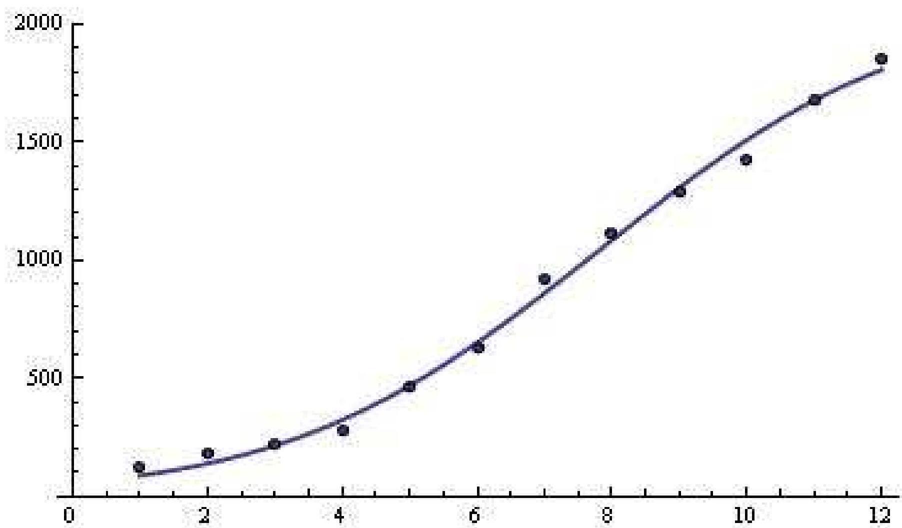

Figure 11: The fitted model $M^{*****}(t)$ for Malware Evolution.

cumulative data is:

$Number\_of\_users\_attacked\_by\_Trojan - Ransom\_malware$

$\_(Q4\_2014 - Q3\_2015)\_data := \{\{1, 128132\}, \{2, 278706\}, \{3, 543089\}, \{4, 880294\}\}$

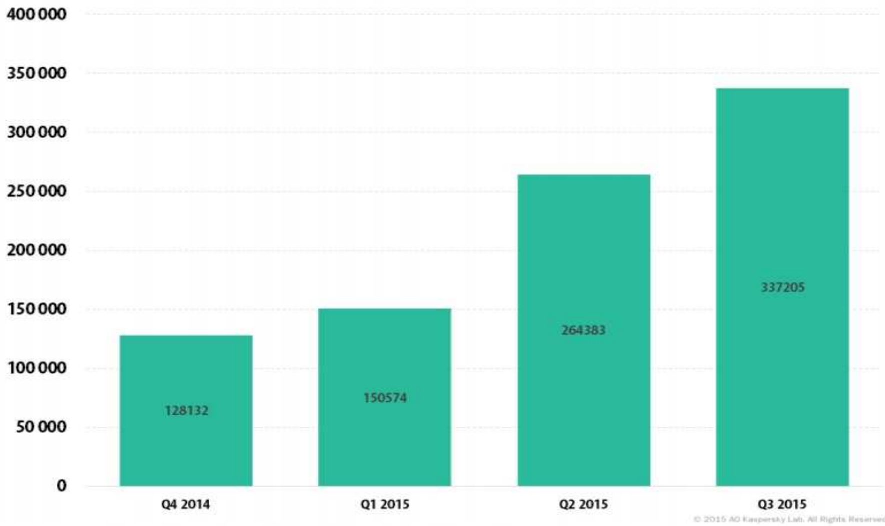

Figure 12: Number of users attacked by Trojan-Ransom malware (Q4 2014 - Q3 2015) [69].

The fitted model

$$M^{******}(t) = \frac{1.09329 * 10^6}{1 + e^{-1.17649(-2.9+t)}}$$

is presented on Fig. 13.

8. NUMBER OF USERS ATTACKED BY CRYPTO-RANSOMWARE

We will explore how it can be modelled data in [70] for the number of users attacked by crypto-ransomware (November 2016 - October 2017), see Fig. 14. The cumulative data is:

$$Number\_of\_users\_attacked\_by\_crypto - ransomware$$

$$\_(November\_2016 - October\_2017)\_data := \{\{1, 192729\}, \{2, 398928\},$$

$$\{3, 497471\}, \{4, 585681\}, \{5, 660043\}, \{6, 726802\}, \{7, 824067\},$$

$$\{8, 925574\}, \{9, 980112\}, \{10, 1048504\}, \{11, 1128389\}, \{12, 1237842\}\}$$

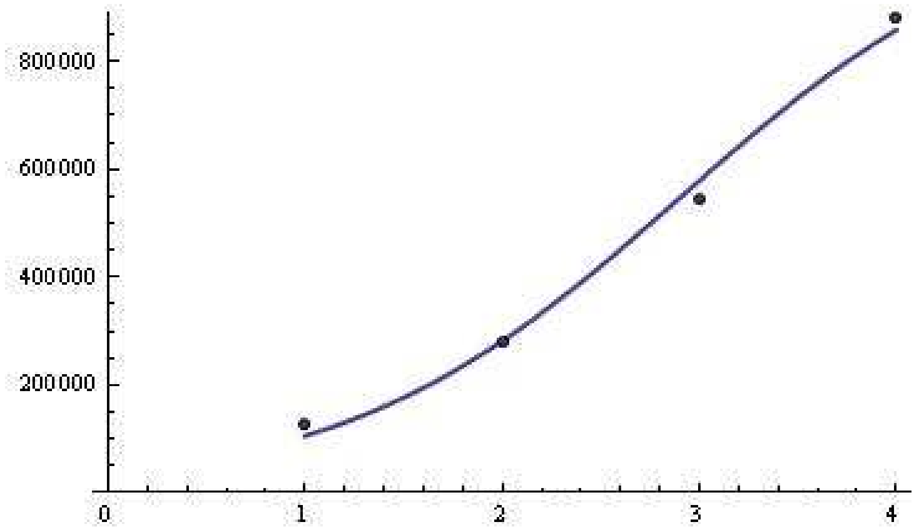

Figure 13: The fitted model $M^{******}(t)$ for the data in Fig. 12.

The fitted model

$$M^{*******}(t) = \frac{1.39988 * 10^6}{1 + e^{-0.5(-8.5+t)}} - \frac{1.08595 * 10^6}{1 + e^{-0.5(-7+t)}} + \frac{1.03641 * 10^6}{1 + e^{-0.5(-3+t)}}$$

is given on Fig. 15.

With the proposed methodology, it can also describe attacks from other viruses, for example:

– "Number of new crypto-ransomware modifications November 2016 - October 2017" [70],

– "The number of users targeted by financial malware November 2016 - October 2017" [70],

– "The number of users attacked by financial malware November 2014 - October 2015" [69],

– "Number of Trojan-Ransom encryptor modifications in Kaspersky Labs Virus Collection 2013 - 2015" [69],

– "Number of users attacked by Trojan-Ransom encryptor malware (2012 - 2015)" [69],

– "Novel ransomware attacks between 2010 and 2015" [72], [71].

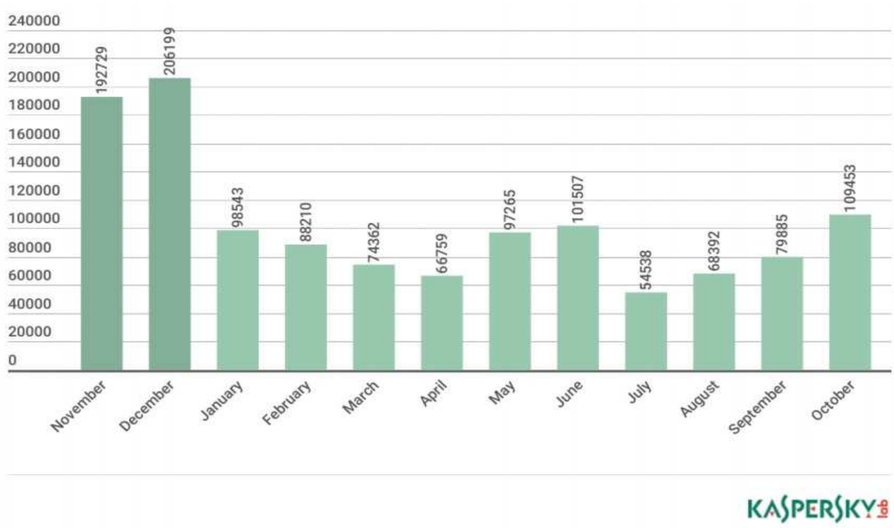

Figure 14: Number of users attacked by crypto-ransomware (November 2016 - October 2017) [70].

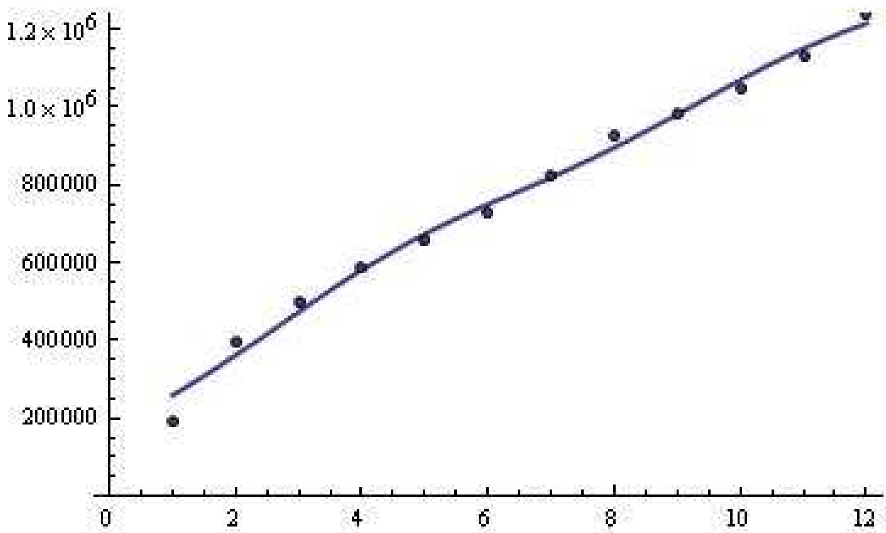

Figure 15: The fitted model $M^{*******}(t)$ for the data in Fig. 14.

9. NUMBER OF UNIQUE USERS ATTACKED BY TROJAN-RANSOM.ANDROIDOS.FUSOB

We will examine how it can be modelled data in [73] for the number of unique users attacked by Trojan-Ransom.AndroidOS.Fusob in 2016, see Fig. 16. The

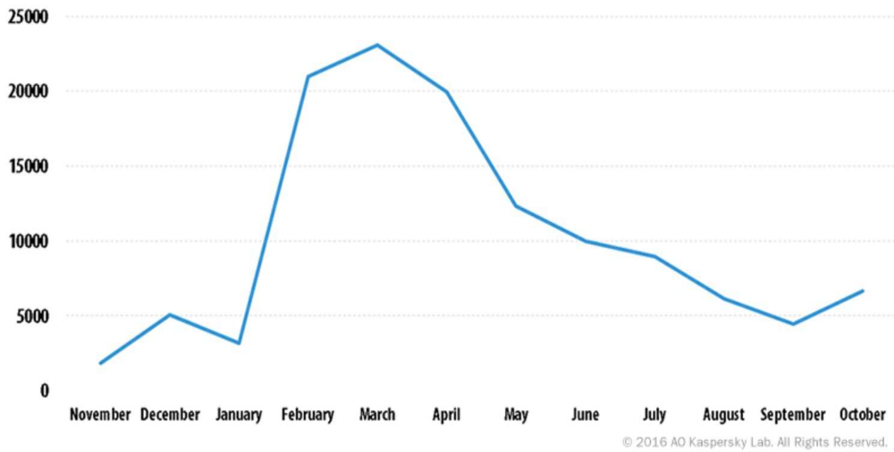

Figure 16: Trojan-Ransom.AndroidOS.Fusob in 2016 [73].

cumulative data is:

$$Number\_of\_unique\_users\_attacked\_by$$

$$\_Trojan - Ransom.AndroidOS.Fusob\_data := \{\{1, 1950\}, \{2, 6950\},$$

$$\{3, 10100\}, \{4, 31100\}, \{5, 54100\}, \{6, 74100\}, \{7, 86600\},$$

$$\{8, 96600\}, \{9, 106100\}, \{10, 112500\}, \{11, 117100\}, \{12, 124100\}\}$$

The fitted model

$$M^{********}(t) = -\frac{178591.}{1 + e^{-0.5(-8.5+t)}} + \frac{359263.}{1 + e^{-0.4(-7+t)}} - \frac{62421.5}{1 + e^{-0.09(-3+t)}}$$

is depicted on Fig. 17.

10. CONCLUDING REMARKS

The fitting of data to the common model (2) does not always gives good results due to large number of unknown parameters: $a_i, k_i, r_i, i = 1, 2, ..., n$.

Frivolous minimization of this functional of many variables using, for example, CAS Mathematica leads to an expected comment of the type: "...a local extremum cannot be found...".

This indicates that the user must make the following preliminary steps:

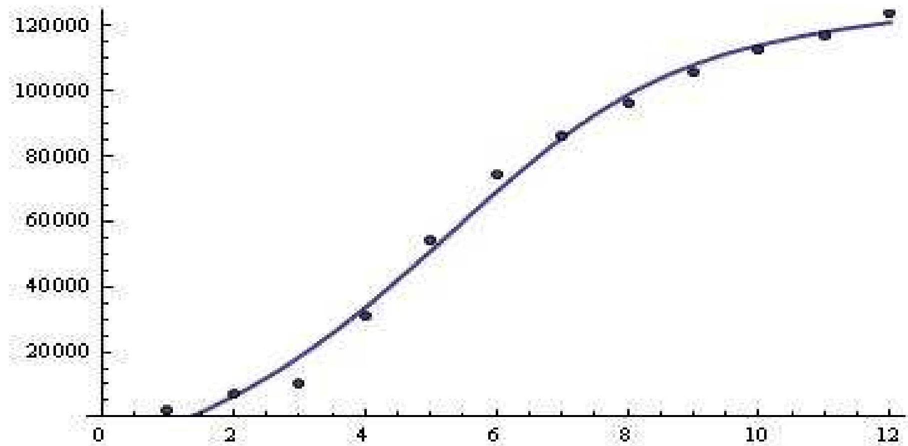

Figure 17: The fitted model $M^{********}(t)$ for the data in Fig. 16.

a) careful selection of the most typical parameters for the proposed model;
b) serious data analysis and approximate determination of the parameters r_i.

The construction of an interpolation polynomial for these data is not appropriate due to the high degree of polynomial (see, for example Fig. 18).

Of course, the user can use, for example, the simplified model

$$M(t) = \frac{142.159}{1 + e^{-0.01(t-1.25)}} + \frac{144.481}{1 + e^{-1.5(t-2.25)}} - \frac{49.5313}{1 + e^{-(t-3.125)}}$$

to approximate the "seasonal data" (see Fig. 19).

This is true in studying the cumulative number of virus attacks.

Knowing the explicit appearance of the debugging function is of paramount importance for recognizing "known viruses".

The proposed model can be applied to model computer viruses propagation.

ACKNOWLEDGMENTS

This paper is supported by the National Scientific Program "Information and Communication Technologies for a Single Digital Market in Science, Education and Security (ICTinSES)", financed by the Ministry of Education and Science.

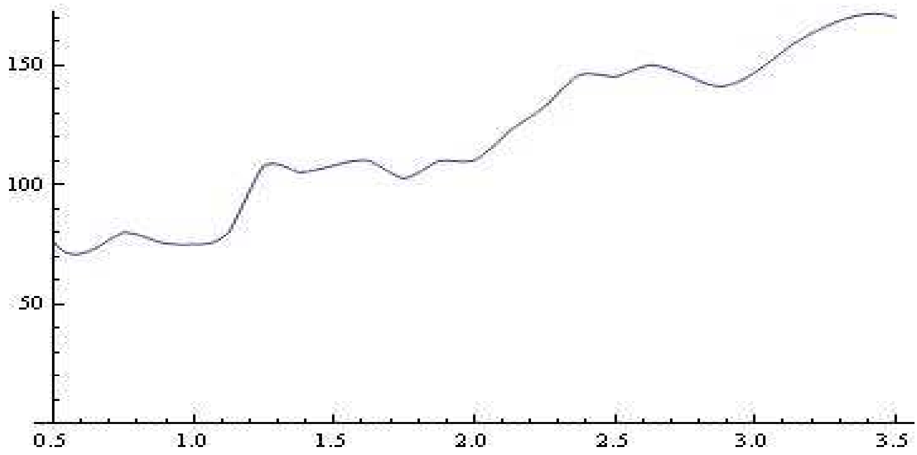

Figure 18: Interpolation of the "Seasonal data" [63].

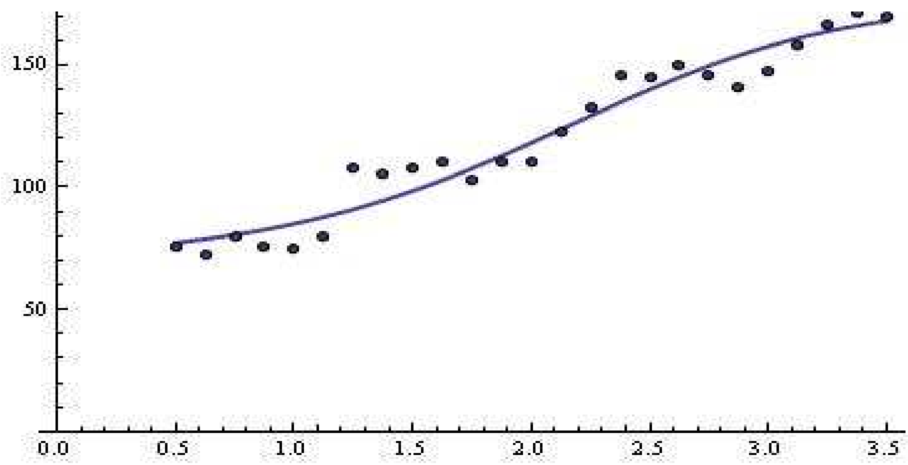

Figure 19: The fitted model $M(t)$.

REFERENCES

[1] F. Palmieri, U. Fiore, Containing large-scale worm spreading in the Internet by cooperative distribution of traffic filtering policies, *Computers & Security*, **27** (2008), 48–62.

[2] U. Zurutuza, D. Zamboni, A Data Mining Approach for Analysis of Worm

Activity Through Automatic Signature Generation, *AISec'08 Proceedings of the 1st ACM workshop on Workshop on AISec*, (2008), 61–70.

[3] O. A. Toutonji, S.-M. Yoo, M. Park, Stability analysis of VEISV propagation modeling for network worm attack, *Applied Mathematical Modelling*, **36** (2012), 2751–2761.

[4] D. Moore, V. Paxson, S. Savage, C. Shannon, S. Staniford, N. Weaver, Inside the slammer worm, *IEEE Magaz. Secur. Privacy*, **1** No. 4 (2003), 33–39.

[5] C. Shannon, D. Moore, The Spread of the Code-Red Worm, http://www.caida.org/analysis/security/code-red/coderedv2_analysis.xml.

[6] R. Banks, Growth and Diffusion Phenomena: Mathematical Frameworks and Applications, Springer Verlag, Berlin (1991).

[7] N. Kyurkchiev, A. Iliev, A note on the power law logistic model, Proc. of the NTADES Series of AIP, (2019). (to appear)

[8] F. Hausdorff, *Set theory (2 ed.)*, Chelsea Publ., New York (1962) [1957], ISBN 978-0821838358, Republished by AMS-Chelsea (2005).

[9] N. Kyurkchiev, S. Markov, *Sigmoid functions: Some Approximation and Modelling Aspects*, LAP LAMBERT Academic Publishing, Saarbrucken (2015), ISBN 978-3-659-76045-7.

[10] N. Kyurkchiev, A. Iliev, S. Markov, *Some Techniques for Recurrence Generating of Activation Functions: Some Modeling and Approximation Aspects*, LAP LAMBERT Academic Publishing (2017), ISBN: 978-3-330-33143-3.

[11] N. Kyurkchiev, A. Iliev, *Extension of Gompertz-type Equation in Modern Science: 240 Anniversary of the birth of B. Gompertz*, LAP LAMBERT Academic Publishing (2018), ISBN: 978-613-9-90569-0.

[12] N. Kyurkchiev, A. Iliev, A. Rahnev, *Some Families of Sigmoid Functions: Applications to Growth Theory*, LAP LAMBERT Academic Publishing (2019), ISBN: 978-613-9-45608-6.

[13] N. Pavlov, A. Iliev, A. Rahnev, N. Kyurkchiev, *Some software reliability models: Approximation and modeling aspects*, LAP LAMBERT Academic Publishing (2018), ISBN: 978-613-9-82805-0.

[14] N. Pavlov, A. Iliev, A. Rahnev, N. Kyurkchiev, *Nontrivial Models in Debugging Theory: Part 2*, LAP LAMBERT Academic Publishing (2018), ISBN: 978-613-9-87794-2.

[15] D. Moore, C. Shannon, J. Brown, Code-Red: a case study on the spread and victims of an Internet worm, *Internet Measurement Workshop* (IMW), (2002), 273–284.

[16] C. Zou, W. Gong, D. Towsley, Code red worm propagation modeling and analysis, *CCS '02 Proceedings of the 9th ACM conference on Computer and communications security*, (2002), 138–147.

[17] C. Zou, W. Gong, D. Towsley, Worm propagation modeling and analysis under dynamic quarantine defense, *Proceedings of the 2003 ACM workshop on Rapid malcode*, October 27–27, (2003), Washington, DC, USA.

[18] C. Zou, D. Towsley, W. Gong, On the performance of internet worm scanning strategies, *Performance Evaluation*, **63**, No. 7 (2006), 700–723.

[19] C. Zou, W. Gong, D. Towsley, L. Gao, The monitoring and early detection of internet worms, *IEEE/ACM Transactions on Networking (TON)*, **13**, No. 5 (2005), 961–974.

[20] P. Wang, L. Wu, R. Cunningham, C. Zou, Honeypot detection in advanced botnet attacks, *International Journal of Information and Computer Security*, **4**, No. 1 (2010), 30–51.

[21] A. Visheratin, M. Melnik, D. Nasonov, N. Butakov, A. Boukhanovsky, Hybrid scheduling algorithm in early warning systems, *Future Generation Computer Systems*, **79**, No. P2 (2018), 630–642.

[22] J. Jerkins, J. Stupiansky, Mitigating IoT insecurity with inoculation epidemics, *Proceedings of the ACMSE 2018 Conference*, March 29–31, (2018), 1–6, Richmond, Kentucky.

[23] Q. Xiao, S. Chen, M. Chen, Y. Ling, Hyper-Compact Virtual Estimators for Big Network Data Based on Register Sharing, *ACM SIGMETRICS Performance Evaluation Review*, **43**, No. 1 (2015), 417–428.

[24] H. Asghari, M. Ciere, M. Van Eeten, Post-mortem of a zombie: conficker cleanup after six years, *Proceedings of the 24th USENIX Conference on Security Symposium*, August 12–14, (2015), 1–16, Washington, D.C.

[25] A. Dainotti, A. King, K. Claffy, F. Papale, A. Pescape, Analysis of a "/0" stealth scan from a botnet, *IEEE/ACM Transactions on Networking (TON)*, **23**, No. 2 (2015), 341–354.

[26] D. Lee, J. Kim, K. Kim, A study on abnormal event correlation analysis for convergence security monitor, *Cluster Computing*, **16**, No. 2 (2013), 219–227.

[27] E. Magkos, M. Avlonitis, P. Kotzanikolaou, M. Stefanidakis, Toward early warning against Internet worms based on critical-sized networks, *Security and Communication Networks*, **6**, No. 1 (2013), 78–88.

[28] S. Xu, W. Lu, L. Xu, Push- and pull-based epidemic spreading in networks: Thresholds and deeper insights, *ACM Transactions on Autonomous and Adaptive Systems (TAAS)*, **7**, No. 3 (2012), 1–26.

[29] C. Shannon, D. Moore, The Spread of the Witty Worm, *IEEE Security & Privacy*, **July/August**, (2004), 46–50.

[30] A. Mohammed, S. Nor, M. Marsono, Analysis of Internet Malware Propagation Models and Mitigation Strategies, *IRACST International Journal of Computer Networks and Wireless Communications (IJCNWC)*, **2**, No. 1 (2012), 16–20.

[31] S. Staniford, V. Paxsony, N. Weaver, How to own the Internet in Your Spare Time, *Proceedings of the 11th USENIX Security Symposium, San Francisco*, California, USA, August 5-9, (2002).

[32] S. Fei, L. Zhaowen, M. Yan, A survey of Internet Worm Propagation Models, *Proceedings of IC-BNMT2009*, (2009), 453–457.

[33] S. Fei, L. Zhaowen, M. Yan, Worm Propagation based on Two-Factor Model, *Proceedings of 2009 5th International Conference on Wireless Communications, Networking and Mobile Computing*, (2009), 4 pp.

[34] D. Smith, L. Moore, The SIR model for the Spread of Diseases, *JOMA*, (2004).

[35] J. Kim, S. Radhakrishnan, S. Dhall, Measurement and Analysis of worm propagation on Internet network topology, *Proceedings of 13th International Conference on Computer Communications and Networks (IEEE Cat. No.04EX969)*, 495–500.

[36] T. Li, Z. Guan, Y. Wang, The Stability of a Worm Propagation Model with Time Delay on Homogeneous Networks, *Proceedings of International Conference on Intelligent Control and Information Processing*, August 13-15, (2010) - Dalian, China, 753–755.

[37] T. Li, Z.-H. Guan, Y. Wang, Y. Li, Impulsive Control of the Spread of worm with Nonlinear Incidence Rates, *Proceedings of 2010 Chinese Control and Decision Conference*, (2010), 966–969.

[38] Y. Wang, Z.-H. Guan, T. Li, S. Zhang, Modeling and Analyzing the Spread of Worm with Impulsive Effect on Homogeneous Network, *Proceedings of 2010 International Conference on Computer Application and System Modeling (ICCASM 2010)*, (2010), V7-501–V7-504.

[39] C. Junhua,W. Shengjun, Modeling and Analyzing the Spread of worms with Bilinear Incidence Rate, *Proceedings of 2009 Fifth International Conference on Information Assurance and Security*, (2009), 167–170.

[40] W. Shaojie, L. Qiming, D. Bo, M. Weining, Analysis of a Mathematical Model for Worm Virus Propagation with time delay, *Proceedings of 2009 Second International Conference on Environmental and Computer Science*, (2009), 375–379.

[41] D. Zhang, Y. Wang, SIRS: Internet Worm Propagation and Application, *Proceedings of 2010 International Conference on Electrical and Control Engineering*, (2010), 3029–3032.

[42] Q. Liu, R. Xu, S. Wang, Modeling and Analysis of an SIRS Model for worm Propagation, *Proceedings of 2009 International Conference on Computational Intelligence and Security*, (2009), 361–365.

[43] S. Fei, L. Zhao-wen, M. Yan, Modeling and Analysis of Internet worm propagation, *The Journal of China Universities of Posts and Telecommunications*, **17**, No. 4 (2010), 63–68.

[44] J. Wang, C. Xia, Q. Liu, A novel Model for the Internet Worm Propagation, *Proceedings of 2010 Sixth International Conference on Natural Computation (ICNC 2010)*, (2010), 2885–2888.

[45] F. Wang, J. Song, Y. Dong, J. Gu, Epidemic models applied to worms on internet, *Proceedings of 2009 Second International Conference on Intelligent Networks and Intelligent Systems*, (2009), 160–163.

[46] Z. Wei, Q. Facheng, C. Shiqi, W. Ruchuan, The Study of Network Worm Propagation Simulation, *Proceedings of 2010 International Conference on Computer Application and System Modeling (ICCASM 2010)*, (2010), V9-295–V9-299.

[47] M. Liuqi, The research and development of worm defense strategies, *Proceedings of 2010 3rd International Conference on Computer Science and Information Technology*, (2010), 168–171.

[48] F.Wang, Y. Zhang, C. Wang, J. Ma, S. Moon, Stability analysis of a SEIQV epidemic for rapid spreading worms, *Computer & Security*, **29** (2010), 410–418.

[49] Y. Yao, H. Guo, F. Gao, G. Yu, The Worm Propagation Model with pulse Quarantine Strategy, *Proceedings of 2010 International Conference on Multimedia Information Networking and Security*, (2010), 269–273.

[50] H. Zhang, W. Su, W. Quan, *Smart Collaborative Identifier Network: A Promising Design for Future Internet*, Springer-Verlag, Berlin (2016).

[51] X. Wang, J. Zhu, H. Lin, X. Su, Y. Jiang, Modeling Propagation of Active P2P Worm in Chord Network, In: *Advances in Intelligent and Soft Computing*, J. Kacprzyk eds., **133** (2012), S. Sambath & E. Zhu (Eds.), *Frontiers in Computer Education*, 383–390.

[52] Y. Xiao, F. Li, H. Chen, eds., *Handbook of Security and Networks*, World Scientific, Singapore (2011).

[53] S. Sellke, N. Shroff, S. Bagchi, Modeling and Automated Containment of Worms, *Proceedings of the 2005 International Conference on Dependable Systems and Networks (DSN05)*, (2005), 10 pp.

[54] W. Yu, C. Boyer, S. Chellappan, D. Xuan, Peer-to-peer system-based active worm attacks: modeling and analysis, *IEEE International Conference on Communications, 2005*, (2005), 295–300.

[55] S. Zhang,Z. Jin, J. Zhang, The Dynamical Modeling Analysis of the Spreading of Passive Worms in P2P Networks, *Discrete Dynamics in Nature and Society*, **2018**, Article ID 1656907, (2018), 13 pp.

[56] G. Yan, S. Eidenbenz, Modeling Propagation Dynamics of Bluetooth Worms (Extended Version), *IEEE Transactions on Mobile Computing*, **8**, No. 3 (2009), 353–367.

[57] S. Sellke, N. Shroff, S. Bagchi, Modeling and Automated Containment of Worms, *IEEE Transactions on Dependable and Secure Computing*, **5**, No. 2 (2008), 71–86.

[58] S. Peng, M. Wua, G. Wang, S. Yu, Propagation Model of Smartphone Worms Based on Semi-Markov Process and Social Relationship Graph, *Computers & Security*, **44** (2014), 92–103.

[59] N. Kyurkchiev, A. Iliev, A. Rahnev, T. Terzieva, A new analysis of Code Red and Witty worms behavior, *Communications in Applied Analysis*, **23**, No. 2 (2019), 267–285.

[60] A. Iliev, N. Kyurkchiev, A. Rahnev, T. Terzieva, Some New Approaches for Modelling Large–Scale Worm Spreading on the Internet. II, *Neural, Parallel, and Scientific Computations*, **27** (2019), 23–32.

[61] M. Sandee, CryptoLocker ransomware intelligence report, *Fox-IT*, (2014).

[62] P. Szor, *The Art of Computer Virus Research and Defense*, Addison Wesley Professional, (2005), ISBN: 0-321-30454-3.

[63] < http : //www.pisces – conservation.com/growthhelp/ index.html?von_bertalanffy.htm >.

[64] Kyurkchiev N., S. Markov, On the Hausdorff distance between the Heaviside step function and Verhulst logistic function, *J. Math. Chem.*, **54**, No. 1 (2016), 109–119.

[65] R. Anguelov, S. Markov, Hausdorff Continuous Interval Functions and Approximations, In: *SCAN 2014 Proceedings*, LNCS, ed. by J.W.von Gudenberg, Springer, Berlin, (2015).

[66] L. Coroianu, D. Costarelli, S. Gal, G. Vinti, The max-product generalized sampling operators: convergence and quantitative estimates, *Applied Mathematics and Computation*, (2019), doi: 10.1016/j.amc.2019.02.076.

[67] Costarelli, D., R. Spigler, Constructive Approximation by Superposition of Sigmoidal Functions, *Anal. Theory Appl.*, **29**, No. 2 (2013), 169–196.

[68] C. A. Visaggio, Android Security, *Universita degli Studi del Sannio*, (2014).

[69] Kaspersky Security Bulletin 2015, Kaspersky Lab (2016).

[70] Kaspersky Security Bulletin: Overall Statistics for 2017, Kaspersky Lab (2018).

[71] B. Al-rimy, M. Maarof, S. Shaid, Ransomware threat success factors, taxonomy, and countermeasures: A survey and research directions, *Computers & Security*, **74** (2018), 144–166.

[72] L. I. McAfee, Security, editor, Understanding Ransomware and strategies to defeat it, (2016).

[73] Kaspersky Security Bulletin 2016, Kaspersky Lab (2017).