Document details

‹ Back to results | ‹ Previous 98 of 195 Next ›

CSV export Download Print E-mail Save to PDF Save to list More... ›

View at Publisher

Proceedings - 2019 International Conference on Information Systems and Software Technologies, ICI2ST 2019
November 2019, Article number 8940381, Pages 71-78
1st International Conference on Information Systems and Software Technologies, ICI2ST 2019; Escuela Politecnica NacionalQuito; Ecuador; 13 November 2019 through 15 November 2019; Category numberCFP19V56-ART; Code 156415

Profits at the dawn of cybercrime-as-a-service (Conference Paper)

[Ganancias del Cibercrimen como Servicio]

Vidal, J.M.[a], Monge, M.A.S.[b], Monterrubio, S.M.M.[c], Lopez, L.I.B.[d], Caraguay, A.L.V.[d]

Save all to author list

[a]Indra, Digital Lab, Madrid, Spain
[b] Universidad de Lima, Peru
[c]Departamento de Ingeniería Del Software e Inteligencia Artificial, Universidad Complutense de Madrid, Spain

View additional affiliations

Abstract

View references (28)

The growing of Information and Communication Technologies (ICT) that has been experienced in recent years, has led to new and more sophisticated ways of doing business. Consequently, worldwide organized criminal groups have been able to adapt their activities to new trends in the area of information security. In this paper the problem of cyber-crime as a profitable business and the model Cybercrime-as-a-service (CaaS) are exposed. For this purpose, the ransomware, which is one of the threats that have generated more profit in the last two years, is analyzed. This kind of malware is able to block assets in the victim systems and blackmail their owners with their deletion, if they fail to pay a ransom. In this sense, a game theory model of the behavior of actors involved in a ransomware attack is proposed. The proposed model describes the extortion process between the attacker and victim and estimates the probability of payment of ransom. © 2019 IEEE.

Author keywords

CaaS Cibercrimen Malware Ransomware

Indexed keywords

Engineering controlled terms: Crime Game theory Information systems Information use Profitability

Engineering uncontrolled terms: CaaS Cibercrimen Cyber-crimes Cybercrime Game theory models Information and Communication Technologies

Engineering main heading: Malware

ISBN: 978-172814886-1
Source Type: Conference Proceeding
Original language: Spanish

DOI: 10.1109/ICI2ST.2019.00017
Document Type: Conference Paper
Volume Editors: Hallo M.,Molina M.,Valdivieso L.
Publisher: Institute of Electrical and Electronics Engineers Inc.

References (28)

View in search results format >

All | CSV export | Print | E-mail | Save to PDF | Create bibliography

1 An, J., Kim, H.-W.

A Data Analytics Approach to the Cybercrime Underground Economy (Open Access)

(2018) *IEEE Access*, 6, pp. 26636-26652. Cited 6 times.
http://ieeexplore.ieee.org/xpl/RecentIssue.jsp?punumber=6287639
doi: 10.1109/ACCESS.2018.2831667

View at Publisher

2 Enbody, R., Sood, A.K., Bajpai, P.

A key-management-based taxonomy for ransomware

(2018) *eCrime Researchers Summit, eCrime*, 2018-May, pp. 1-12. Cited 6 times.
http://ieeexplore.ieee.org/xpl/conferences.jsp
ISBN: 978-153864922-0
doi: 10.1109/ECRIME.2018.8376213

View at Publisher

3 Cleary, G., Cox, O., Lau, H., Nahorney, B., Gorman, B., O'Brien, D., Wallace, S., (...), Wueest, C.
(2018) *Internet Security Threat Report Symantec*, p. 8089.

4 Conti, M., Gangwal, A., Ruj, S.

On the economic significance of ransomware campaigns: A Bitcoin transactions perspective

(2018) *Computers and Security*, 79, pp. 162-189. Cited 13 times.
doi: 10.1016/j.cose.2018.08.008

View at Publisher

5 (2014) *Police Ransomware Threat Assessment 2014*. Cited 2 times.
Europol

6 Goode, L.

Anonymous and the Political Ethos of Hacktivism

(2015) *Popular Communication*, 13 (1), pp. 74-86. Cited 15 times.
http://www.tandfonline.com/toc/hppc20/current
doi: 10.1080/15405702.2014.978000

View at Publisher

7 Hernandez-Castro, J., Cartwright, E., Stepanova, A.
(2017) *Economic Analysis of Ransomware*. Cited 10 times.
http://dx.doi.org/10.2139/ssrn.2937641

8 Silva, J.A.H., López, L.I.B., Caraguay, Á.L.V., Hernández-álvarez, M.

A survey on situational awareness of ransomware attacks-detection and prevention parameters (Open Access)

(2019) *Remote Sensing*, 11 (10), art. no. 1168. Cited 3 times.
https://res.mdpi.com/remotesensing/remotesensing-11-01168/article_deploy/remotesensing-11-01168.pdf?filename=&attachment=1
doi: 10.3390/rs11101168

View at Publisher

9 Huang, K., Siegel, M., Madnick, S.
Systematically understanding the cyber attack business: A survey (Open Access)

(2018) *ACM Computing Surveys*, 51 (4), art. no. 3199674. Cited 6 times.
http://dl.acm.org/citation.cfm?id=J204
doi: 10.1145/3199674

View at Publisher

10 Kim, D.W., Yan, P., Zhang, J.
Detecting fake anti-virus software distribution webpages

(2015) *Computers and Security*, 49, pp. 95-106. Cited 12 times.
doi: 10.1016/j.cose.2014.11.008

View at Publisher

11 Kolodenker, E., Koch, W., Stringhini, G., Egele, M.
PayBreak : Defense against cryptographic ransomware

(2017) *ASIA CCS 2017 - Proceedings of the 2017 ACM Asia Conference on Computer and Communications Security*, pp. 599-611. Cited 52 times.
ISBN: 978-145034944-4
doi: 10.1145/3052973.3053035

View at Publisher

12 Kshetri, N.
Cybercrimes in the Former Soviet Union and Central and Eastern Europe: Current status and key drivers

(2013) *Crime, Law and Social Change*, 60 (1), pp. 39-65. Cited 13 times.
doi: 10.1007/s10611-013-9431-4

View at Publisher

13 Manky, D.
Cybercrime as a service: A very modern business

(2013) *Computer Fraud and Security*, 2013 (6), pp. 9-13. Cited 15 times.
doi: 10.1016/S1361-3723(13)70053-8

View at Publisher

14 (2017) *The Economic Impact of Cybercrime No Slowing Down, McAfee White Paper*
McAfee

15 Me, G., Pesticcio, L.
Tor black markets: Economics, characterization and investigation technique

(2018) *Advanced Sciences and Technologies for Security Applications*, pp. 119-140.
https://link.springer.com/bookseries/5540
doi: 10.1007/978-3-319-97181-0_6

View at Publisher

16 Naqvi, S.
Challenges of cryptocurrencies forensics: A case study of investigating, evidencing and prosecuting organised cybercriminals
(2018) *Proceedings of the 13th International Conference on Availability, Reliability and Security*
ACM, New York, NY, USA, 1-5 August

17 Ben Naseir, M.A., Dogan, H., Apeh, E., Richardson, C., Ali, R.
Contextualising the National Cyber Security Capacity in an Unstable Environment: A Spring Land Case Study

(2019) *Advances in Intelligent Systems and Computing*, 930, pp. 373-382.
http://www.springer.com/series/11156
ISBN: 978-303016180-4
doi: 10.1007/978-3-030-16181-1_35

View at Publisher

18 Phelps, A., Watt, A.
I shop online - Recreationally! Internet anonymity and Silk Road enabling drug use in Australia

(2014) *Digital Investigation*, 11 (4), pp. 261-272. Cited 18 times.
http://www.elsevier.com/wps/find/journaldescription.cws_home/702130/description#description
doi: 10.1016/j.diin.2014.08.001

View at Publisher

19 Ring, T.
Why bug hunters are coming in from the wild

(2014) *Computer Fraud and Security*, 2014 (2), pp. 16-20. Cited 3 times.
doi: 10.1016/S1361-3723(14)70463-4

View at Publisher

20 Schirrmacher, N.B., Ondrus, J., Tan, F.T.C.
Towards a response to ransomware: Examining digital capabilities of the wannacry attack
(2018) *Proceedings of Pacific Asia Conference on Information Systems*, pp. 1-9. Cited 3 times.
Yokohama, Japan, June

21 Schrittwieser, S., Katzenbeisser, S., Kieseberg, P., Huber, M., Leithner, M., Mulazzani, M., Weippl, E.
Covert Computation - Hiding code in code through compile-time obfuscation

(2014) *Computers and Security*, 42, pp. 13-26. Cited 7 times.
doi: 10.1016/j.cose.2013.12.006

View at Publisher

22 Snader, R., Borisov, N.
Improving security and performance in the tor network through tunable path selection

(2011) *IEEE Transactions on Dependable and Secure Computing*, 8 (5), art. no. 5560675, pp. 728-741. Cited 20 times.
doi: 10.1109/TDSC.2010.40

View at Publisher

23 Sood, A.K., Enbody, R.J.
Crimeware-as-a-service-A survey of commoditized crimeware in the underground market

(2013) *International Journal of Critical Infrastructure Protection*, 6 (1), pp. 28-38. Cited 40 times.
doi: 10.1016/j.ijcip.2013.01.002

View at Publisher

24 Wainwright, P., Kettani, H.
An analysis of botnet models

(2019) *ACM International Conference Proceeding Series*, pp. 116-121.
http://portal.acm.org/
ISBN: 978-145036634-2
doi: 10.1145/3314545.3314562

View at Publisher

25 Young, Adam, Yung, Moti
Cryptovirology: extortion-based security threats and countermeasures

(1996) *Proceedings of the IEEE Computer Society Symposium on Research in Security and Privacy*, pp. 129-140. Cited 77 times.

View at Publisher

26 Monika, Zavarsky, P., Lindskog, D.
Experimental Analysis of Ransomware on Windows and Android Platforms: Evolution and Characterization (Open Access)

(2016) *Procedia Computer Science*, 94, pp. 465-472. Cited 25 times.
http://www.sciencedirect.com/science/journal/18770509
doi: 10.1016/j.procs.2016.08.072

View at Publisher

27 (2013) *Security Watch: The Crimeware-As-A-Service Reality*
Sunday Business Post, N/a

28 Dupont, B.
Bots, cops, and corporations: on the limits of enforcement and the promise of polycentric regulation as a way to control large-scale cybercrime

(2017) *Crime, Law and Social Change*, 67 (1), pp. 97-116. Cited 16 times.
http://www.kluweronline.com/issn/0925-4994
doi: 10.1007/s10611-016-9649-z

View at Publisher