Document details

< Back to results | 1 of 2 Next >

Download Print Save to PDF Add to List More... >

Full Text View at Publisher

Proceedings of the 2018 7th International Conference on Computer and Communication Engineering, ICCCE 2018
16 November 2018, Article number 8539257, Pages 135-140
Computer and Communication Engineering, ICCCE 2018; Kuala Lumpur; Malaysia; 19 September 2018 through 20 September 2018; Category numberCFP1839D-USB; Code 142740

Analysis of THUG: A Low-Interaction Client Honeypot to Identify Malicious Websites and Malwares (Conference Paper)

Zulkurnain, N.F., Rebitanim, A.F., Malik, N.A.

Electrical and Computer Engineering, International Islamic University Malaysia Kuala Lumpur, Malaysia

Abstract

View references (9)

Cybersecurity is becoming more relevant throughout time. As information and technologies expand, so does the potential for it to be exploited. Computer and media have become more widespread in every modern country in the world. Unfortunately, certain community uses this opportunity to exploit the vulnerabilities that these computers left behind. Black hat, which is more identified as hackers and exploiters, uses the networks and servers that are commonly used to gain unauthorized information and data on the innocent victim. This work analyzes several honeypots and makes comparisons between them. Analysis has been done on the results to figure the disadvantages between each honeypot and try to improve one of the honeypots based on programming. The honeypot is deployed to simulate its effectiveness in combating cybercrime by detecting and collecting the information captured on the web browsers. © 2018 IEEE.

SciVal Topic Prominence

Topic: Websites | Computer crime | drive-by download

Prominence percentile: 83.846

Author keywords

Black Hat Cybersecurity Honeypot

Indexed keywords

Engineering controlled terms: Malware Personal computing Web browsers

Engineering uncontrolled terms: Black Hat Client Honeypot Cyber security Cybercrime Honeypots Information and technologies Malwares

Engineering main heading: Network security

Funding details

Funding sponsor	Funding number	Acronym
International Islamic University Malaysia	FRGS16-067-0566	IIUM
International Islamic University Malaysia		IIUM

Metrics

0 Citations in Scopus

0 Field-Weighted Citation Impact

PlumX Metrics
Usage, Captures, Mentions, Social Media and Citations beyond Scopus.

Cited by 0 documents

Inform me when this document is cited in Scopus:

Set citation feed >

Related documents

HoneyDrone: A medium-interaction unmanned aerial vehicle honeypot

Daubert, J. , Boopalan, D. , Muhlhauser, M.
(2018) IEEE/IFIP Network Operations and Management Symposium: Cognitive Management in a Cyber World, NOMS 2018

Don't steal my drone: Catching attackers with an unmanned aerial vehicle honeypot

Vasilomanolakis, E. , Daubert, J. , Boopalan, D.
(2018) IEEE/IFIP Network Operations and Management Symposium: Cognitive Management in a Cyber World, NOMS 2018

Honeypot based intrusion management system: From a passive architecture to an ips system

Bendriss, E. , Regragui, B.
(2013) Journal of Theoretical and Applied Information Technology

View all related documents based on references

Find more related documents in Scopus based on:

Authors > Keywords >

Login based features of Scopus are presently deactivated due to a technical issue. We apologize for this and are actively working to resolve this matter with urgency.

Funding text

The authors would like to thank the Malaysian Government and International Islamic University Malaysia (IIUM) for the research grant under Fundamental Research Grant (FRGS16-067-0566).

ISBN: 978-153866991-4
Source Type: Conference Proceeding
Original language: English

DOI: 10.1109/ICCCE.2018.8539257
Document Type: Conference Paper
Publisher: Institute of Electrical and Electronics Engineers Inc.

References (9)

View in search results format >

□ All | Export | Print | E-mail | Save to PDF | Create bibliography

□ 1 Nawrocki, M., Wahlisch, M., Schmidt, T.C., Keil, C., Matthias, W.
(2016) *A Survey on Honeypot Software and Data Analysis*. Cited 16 times.
arXiv preprint arXiv: 1608.06249

□ 2 Mairh, A., Barik, D., Verma, K., Jena, D.
Honeypot in network security: A survey
Proceedings of the 2011 International. Cited 2 times.

□ 3 (2011) *Conference on Communication, Computing &Security. ACM*, pp. 600-605.

□ 4 Provos, N., Holz, T.
(2007) *Virtual Honeypots: From Botnet Tracking to Intrusion Detection*. Cited 159 times.
Addison-Wesley Professional, Reading

□ 5 (2017) *Welcome to Thug's Documentation!-Thug 0.8.33 Documentation*
Angelo Del'Aera [Accessed: 10-Apr2017]
https://buffer.github.io/thug/doc/index.html

□ 6 Mansoori, M., Welch, I., Fu, Q.
YALIH, yet another low interaction honeyclient
(2014) *Conferences in Research and Practice in Information Technology Series*, 149, pp. 7-15. Cited 7 times.
ISBN: 978-192177032-6

□ 7 (2016) *PyClamd: Clamav with Python*
Alexandre norman [Accessed: 9-May2017]
http://xael.org/pages/pyclamd-en.html

□ 8 (2016) *Chapter 1. First steps*
[Accessed: 9-May2017]
https://www.virtualbox.org/manual/ch01.html

□ 9 (2016)
[Accessed: 09-May-2017]
PyCharm

Login based features of Scopus are presently deactivated due to a technical issue. We apologize for this and are actively working to resolve this matter with urgency.

© Copyright 2019 Elsevier B.V., All rights reserved.

< Back to results | 1 of 2 Next >

^ Top of page

About Scopus

What is Scopus
Content coverage
Scopus blog
Scopus API
Privacy matters

Language

日本語に切り替える
切换到简体中文
切換到繁體中文
Русский язык

Customer Service

Help
Contact us

ELSEVIER

Terms and conditions ↗ Privacy policy ↗

Copyright © 2019 Elsevier B.V ↗. All rights reserved. Scopus® is a registered trademark of Elsevier B.V.
We use cookies to help provide and enhance our service and tailor content. By continuing, you agree to the use of cookies.

RELX Group™

Login based features of Scopus are presently deactivated due to a technical issue. We apologize for this and are actively working to resolve this matter with urgency.