Collecting Malicious Particles from Neutrino Botnets

journal.cecyf.fr/ojs/index.php/cybin/article/view/22

- Jakub Souček ESET
- Jakub Tomanek ESET
- Peter Kálnai ESET

DOI: https://doi.org/10.18464/cybin.v4i1.22
Keywords: Neutrino Bot, Kasidet, bot, botnet, reverse engineering

Abstract

Neutrino Bot (also known and detected as Win/Kasidet) is a rapidly changing threat. It first became known around December 2013. It has been actively developed ever since resulting in version 5.4 at the very beginning of 2018. It is being sold for an attractive price to a large variety of cybercriminals.
This paper shows an extensive summary of the history of the bot while focusing on the most recent versions. It presents methods how to analyse Neutrino botnets and provides key findings that have been discovered during the year 2018.

References

Malware don't need coffee, "Neutrino Bot (aka MS:Win32/Kasidet)," June 2014. https://malware.dontneedcoffee.com/2014/06/neutrino-bot-aka-kasidet.html.

"ESET GitHub, SHA-256 hashes of Neutrino Bot files." https://github.com/eset/malwareioc/tree/master/kasidet.

S. Yunakovsky, "Jimmy Nukebot: from Neutrino with love," tech. rep., Kaspersky lab, August 2017. https://securelist.com/jimmy-nukebot-from-neutrino-with-love/81667/.

V. Tom, "Kasidet POS malware spread through fake security update," tech. rep., ThreatSTOP, June 2017. https://blog.threatstop.com/kasidet-pos-malware-spread-through-fake-security-update.

S. Yunakovsky, "Neutrino modification for POS-terminals," tech. rep., Kaspersky lab, June 2017. https://securelist.com/neutrino-modification-for-pos-terminals/78839/.

Wikipedia. https://en.wikipedia.org/wiki/Luhn_algorithm.

Y. Oyama, "Investigation of the Diverse Sleep Behavior of Malware," Journal of Information Processing, vol. 26, pp. 461–476, June 2018. https://www.jstage.jst.go.jp/article/ipsjjip/26/0/26_461/_pdf/char/en.

P. Kálnai and M. Poslušný, “Browser Attack Points Still Abused by Banking Trojans,” tech. rep., Virus Bulletin, 2017. https://www.virusbulletin.com/uploads/pdf/magazine/2018/VB2017-Kalnai-Poslusny.pdf.

P. Kálnai and M. Poslušný, “Browser Attack Points Still Abused by Banking Trojans - 2018 update,” tech. rep., Virus Bulletin, 2018. https://www.virusbulletin.com/blog/2018/07/vb2017-paper-and-update-browserattack-points-still-abused-banking-trojans/.

O. Kubovic, “Ammyy Admin compromised with malware again; World Cup used as cover,” tech. rep., ESET, July 2018. https://www.welivesecurity.com/2018/07/11/ammyy-admin-compromised-malware-world-cupcover/.

“TinyNuke.” https://github.com/rossja/TinyNuke/blob/master/Bot/WebInjects.cpp.

Volume 4, Issue 1, December 2018

Volume 4 Numéro 1, Décembre 2018

Le Journal de la Cybercriminalité & des Investigations Numériques

The Journal on Cybercrime & Digital Investigations

botconf

The botnet fighting conference 2018

TOULOUSE

Ateliers le 4 décembre 2018

Conférences du 5 au 7 décembre 2018

sixième édition 6 sixième édition

Proceedings of Botconf 2018

The botnet fighting conference, 6th edition

Ce journal est publié par:
This journal is published by:

ISSN : 2494-2715

CECyF

Centre Expert contre la Cybercriminalité Français
https://www.cecyf.fr/

PDF

Published

2018-12-10

Issue

Vol 4 No 1 (2018): Botconf 2018
Section

Conference proceedings