Analisa Top 3 High Level Infections Malware Zeroaccess, Alureon.dx, Dan Zeus Dengan Pendekatan Digital Forensik Berdasarkan Memory Volatile Pada Sistem Operasi Windows Xp Dan Windows 7

SKRIPSI

RIDHO ADYA PANGESTU

201010370311234

JURUSAN TEKNIK INFORMATIKA

FAKULTAS TEKNIK

UNIVERSITAS MUHAMMADIYAH MALANG

APRIL 2014

LEMBAR PENGESAHAN

Analisa Top 3 High Level Infections Malware Zeroaccess, Alureon.dx, Dan Zeus Dengan Pendekatan Digital Forensik Berdasarkan Memory Volatile Pada Sistem Operasi Windows Xp Dan Windows 7

Ridho Adya Pangestu

201010370311234

Sebagai Persyaratan Guna Meraih Gelar Sarjana Strata 1

Teknik Informatika Universitas Muhammadiyah Malang

Malang, 12 April 2014

Menyetujui,

Dosen Penguji I	Dosen Penguji II
Yufis Azhar, S.Kom, M.Kom	Ilyas Nuryasin, S.Kom, M.Kom
NIDN : 0728088701	NIDN : 0723118601

Ketua Jurusan

Yuda Munarko, M.Sc

NIDN: 0706077902

KATA PENGANTAR

Assalamu'alaikum Wr.Wb

Puji syukur penulis panjatkan kehadirat Allah SWT yang telah melimpahkan rahmat dan hidayahNya sehingga penulis dapat menyelesaikan tugas akhir dengan judul "**Analisa Top 3 High Level Infections Malware Zeroaccess, Alureon.dx, Dan Zeus DenganPendekatan Digital ForensikBerdasarkan Memory Volatile PadaSistemOperasi Windows Xp Dan Windows 7".**

Perkenankan bersama ini penulis mengucapkan terima kasih yang sebesar–besarnya kepada bapak dan ibu dosen dan orang tua yang selama ini turut membantu dan memberi support yang begitu besar kepada penulis. Semoga Allah memberikan balasan yang sepadan atas budi baik yang selama ini diberikan.

Dengan menyadari adanya keterbatasan waktu, kemampuan, pengetahuan, referensi dan pengalaman, Tugas Akhir ini masih jauh dari sempurna. Untuk itu saran dan masukan untuk kesempurnaan sangat penulis harapkan.

Akhir kata penulis berharap semoga Tugas Akhir ini dapat bermanfaat dan menjadi tambahan ilmu pengetahuan. Aamiin.

Wasalamu'alaikum Wr.Wb

Malang, 12 April 2014

Penulis,

Ridho Adya Pangestu

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

DAFTAR GRAFIK

DAFTAR PUSTAKA

Andri P. Heriyanto. (2012). What is the Proper Forensics Approach on Trojan. Banking Malware Incidents?. Australian Digital Forensics Conference

Amer Aljaedi, Dale Lindskog, Pavol Zavarsky, Ron Ruhl, Fares Almari (2011). Comparative Analysis of Volatile Memory Forensics Live Response vs. Memory Imaging. 2011 IEEE International Conference on Privacy, Security, Risk, and Trust, and IEEE International Conference on Social Computing.

Analysts, F., Testers, P., & Engineers, S. (n.d.). *Violent Python A Cookbook for Hackers , Forensic Analysts , Violent Python A Cookbook for Hackers , Forensic Analysts ,*.

Budi Rahardjo (2003), "Hukum dan Dunia Cyber", PT. Indosic, Jakarta.

Budhisantoso, Nugroho, Personal Site www.forensik-komputer.info. 14 Februari 2014, pukul 10.20.

Cutifa Safitri (2013). A Study: Volatility Forensic on Hidden Files. International Journal of Science and Research (IJSR), India Online ISSN: 2319-7064.

Garfinkel, S. (2007). Anti-forensics: Techniques, detection and countermeasures. Paper presented at the The 2nd International Conference on i-Warfare.

Henry B. Wolfe (1997). Privacy Enhancing Technology.

IOActive, Incorporated (2012). Reversal and Analysis of Zeus and SpyEye Banking Trojans.

Kemmish, Rodney Mc., (1999) What is forensic computer,Australian institute of Criminology, Canberra.

Liang Hu, Shinan Song, Xiaolu Zhang, Zhenzhen Xie, Xiangyu Meng, and Kuo Zhao (2013). Analyzing Malware Based on Volatile Memory. College of Computer Science and Technology, Jilin University, Changchun 130012, China.

Marcella, Albert J., and Robert S. Greenfiled (2002), "Cyber Forensics a field manual for collecting, examining, and preserving evidence of computer crimes", by CRC Press LLC, United States of America.

Symantec, Alan Neville, Ross Gibb (2013). Zeroaccess in depth.

The Kindsight Security Labs (2013). Kindsight Security Labs Malware Report – Q2 2013.

Trojan:Win32/Alureon.Dx Technical information http://www.microsoft.com/security/portal/threat/encyclopedia/entry.aspx?Name=Trojan:Win32/Alureon.DX. 15 Februari 2014, pukul 08.10.

Xuejia Lai, Dawu Gu, Bo Jin Yongquan Wang, Hui Li(1998). Forensics in Telecommunication, Information, and Multimedia.