

**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

NIDN : 0728088701

Ilyas Nuryasin, S.Kom, M.Kom

NIDN : 0723118601

Ketua Jurusan

Yuda Munarko, M.Sc

NIDN: 0706077902

KATA PENGANTAR

Assalamu'alaikum Wr.Wb

Puji syukur penulis panjatkan kehadiran 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 Dengan Pendekatan Digital Forensik Berdasarkan Memory Volatile Pada Sistem Operasi 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

HALAMAN JUDUL	i
LEMBAR PERSETUJUAN	ii
LEMBAR PENGESAHAN	iii
LEMBAR PERNYATAAN KEASLIAN	iv
ABSTRAK	v
ABSTRACT	vi
LEMBAR PERSEMBAHAN	vii
KATA PENGANTAR	viii
DAFTAR ISI	ix
DAFTAR GAMBAR	xii
DAFTAR TABEL	xiii
DAFTAR GRAFIK	xv
BAB I PENDAHULUAN	1
1.1 Latar Belakang.....	1
1.2 Rumusan Masalah.....	2
1.3 Tujuan.....	2
1.4 Batasan Masalah.....	2
1.5 Metodologi.....	3
1.6 Sistematika Penulisan.....	4
BAB II LANDASAN TEORI	5
2.1 <i>Malware</i>	5
2.1.1 Jenis <i>Malware</i>	5
2.1.2 Infeksi <i>Malware</i>	7
2.1.2.1 <i>Top 20 High Level Infection Malware</i>	8
2.2 <i>Memory Volatile</i>	12
2.3 Perbandingan <i>Security Windows 7 dan Windows XP</i>	12

2.4 Digital Forensik.....	13
2.4.1 Tahapan Digital Forensik.....	14
2.4.1.1 Identifikasi Bukti Digital.....	15
2.4.1.2 Penyimpanan bukti digital.....	15
2.4.1.3 Analisa Bukti Digital.....	15
2.4.1.4 Presentasi.....	16
2.4.2 Pendekatan Digital Forensik.....	16
2.4.2.1 Kelebihan dan kekurangan analisa <i>postmortem</i>	16
2.4.2.2 Kelebihan dan kekurangan analisa <i>liveresponse</i>	17
2.4.3 <i>Malware</i> Forensik.....	17
2.5 <i>Volatility</i>	17
2.5.1 Instalasi <i>Volatility</i> Dan Penggunaannya.....	18
2.6 FTK Imager.....	19
BAB III ANALISA DAN PERANCANGAN SYSTEM.....	20
3.1 Analisa Sistem.....	20
3.2 Analisa Kebutuhan Sistem.....	21
3.3 Arsitektur Sistem.....	22
3.3.1 Perancangan Arsitektur <i>Virtual Machine</i>	22
3.3.2 Perancangan Arsitektur <i>Linux Host</i>	23
3.4 Menjalankan <i>Malware</i>	24
3.5 Langkah <i>Capture Image RAM</i>	25
3.6 Analisa <i>Image RAM</i>	26
BAB IV HASIL PENELITIAN DAN PERBANDINGAN.....	28
4.1 Analisa <i>Malware</i>	28
4.1.1 Analisa <i>Image RAM Zeroaccess</i>	28
4.1.1.1 Analisa <i>image RAM Zeroaccess</i> pada <i>Windows XP</i>	29
4.1.1.2 Analisa <i>image RAM Zeroaccess</i> pada <i>Windows 7</i>	35
4.1.2 Analisa <i>Image RAM Alureon</i>	37

4.1.2.1 Analisa <i>image RAM Alureon.dx</i> pada <i>Windows XP</i>	38
4.1.2.2 Analisa <i>image RAM Alureon.dx</i> pada <i>Windows7</i>	41
4.1.3 Analisa <i>Image RAM Zeus</i>	43
4.1.3.1 Analisa <i>image RAM Zeus</i> pada <i>Windows XP</i>	44
4.1.3.2 Analisa <i>image RAM Zeus</i> pada <i>Windows7</i>	48
4.2 Perbandingan Hasil Analisa.....	49
4.2.1 Perbandingan karakteristik <i>Zeroaccess</i> pada <i>Windows XP</i> dan <i>Windows 7</i>	49
4.2.2 Perbandingan karakteristik <i>Alureon.dx</i> pada <i>Windows XP</i> dan <i>Windows7</i>	50
4.2.2 Perbandingan karakteristik <i>Alureon.dx</i> pada <i>Windows XP</i> dan <i>Windows7</i>	51
BAB V PENUTUP.....	52
5.1 Kesimpulan.....	52
5.2 Saran.....	52
DAFTAR PUSTAKA.....	53

DAFTAR GAMBAR

Gambar 1.1 Design proses analisa.....	3
Gambar 2.1 <i>Top 20 malware infection</i>	8
Gambar 2.2 <i>Zeroaccess</i>	9
Gambar 2.3 <i>Alureon.dx</i>	10
Gambar 2.4 <i>Zeus</i>	11
Gambar 2.5 Diagram Digital Forensik.....	11
Gambar 3.1 Alur penelitian.....	20
Gambar 3.2 Arsitektur <i>Virtual Machine Windows XP</i>	22
Gambar 3.3 Arsitektur <i>Virtual Machine Windows 7</i>	22
Gambar 3.4 Arsitektur <i>Linux Host</i>	23
Gambar 3.5 Konfigurasi <i>network virtual machine</i>	24
Gambar 3.6 Menjalankan <i>malware</i>	25
Gambar 3.7 Mencapture <i>Image RAM</i>	25
Gambar 3.8 Aplikasi Menu <i>Volatility</i>	26
Gambar 4.1 Process tree <i>RAM Windows XP</i> terinfeksi <i>Zeroccess</i>	34
Gambar 4.2 Process tree <i>RAM Windows7</i> terinfeksi <i>Zeroccess</i>	36
Gambar 4.3 Process tree <i>RAM WindowsXP</i> terinfeksi <i>Alureon.dx</i>	40
Gambar 4.4 Process tree <i>RAM Windows7</i> terinfeksi <i>Alureon.dx</i>	42
Gambar 4.5 Process tree <i>RAM WindowsXP</i> terinfeksi <i>Zeus</i>	47
Gambar 4.6 Process tree <i>RAM Windows7</i> terinfeksi <i>Zeus</i>	49

DAFTAR TABEL

Tabel 3.1 Sample <i>malware</i>	24
Tabel 4.1 Rincian File Image <i>RAM Windows XP</i> terinfeksi <i>Zeroaccess</i>	29
Tabel 4.2 Analisa Jaringan Image <i>RAM Windows XP</i> terinfeksi <i>Zeroaccess</i>	30
Tabel 4.3 Analisa Device Object <i>RAM Windows XP</i> terinfeksi <i>Zeroaccess</i>	30
Tabel 4.4 Analisa Driver Object <i>RAM Windows XP</i> terinfeksi <i>Zeroaccess</i>	31
Tabel 4.5 Dump Kernel Driver <i>RAM Windows XP</i> terinfeksi <i>Zeroaccess</i>	31
Tabel 4.6 Analisa Driver Object <i>RAM WindowsXP</i> terinfeksi <i>Zeroaccess</i>	32
Tabel 4.7 Analisa Pslist dan DLLlist <i>RAM Windows XP</i> terinfeksi <i>Zeroaccess</i>	32
Tabel 4.8 Hasil dumping proses <i>RAM Windows XP</i> terinfeksi <i>Zeroaccess</i>	33
Tabel 4.9 Analisa PE Injected <i>RAM Windows XP</i> terinfeksi <i>Zeroaccess</i>	33
Tabel 4.10 Analisa Mutex <i>RAM Windows XP</i> terinfeksi <i>Zeroaccess</i>	33
Tabel 4.11 Hasil analisa <i>Zeroaccess</i> pada <i>Windows7</i>	35
Tabel 4.12 Rincian File Image <i>RAM Windows XP</i> terinfeksi <i>Alureon.dx</i>	38
Tabel 4.13 Hasil analisa jaringan <i>Alureon.dx</i> pada <i>RAM Windows XP</i>	38
Tabel 4.14 Hasil analisa File yang mencurigakan pada <i>RAM Windows XP</i>	38
Tabel 4.15 Hasil proses dumping <i>Alureon.dx</i> pada <i>RAM Windows XP</i>	39
Tabel 4.16 Hasil proses Malfind <i>Alureon.dx</i> pada <i>RAM Windows XP</i>	39
Tabel 4.17 Hasil scan mutex <i>Alureon.dx</i> pada <i>RAM Windows XP</i>	40
Tabel 4.18 Hasil analisa <i>Alureon.dx</i> pada <i>Windows7</i>	41
Tabel 4.19 Rincian File Image <i>RAM Windows XP</i> terinfeksi <i>Zeus</i>	44
Tabel 4.20 Hasil analisa jaringan <i>Zeus</i> pada <i>RAM Windows XP</i>	44
Tabel 4.21 Hasil analisa printkey <i>Zeus</i> pada <i>RAM Windows XP</i>	45
Tabel 4.22 Hasil analisa VAD <i>Zeus</i> pada <i>RAM Windows XP</i>	45

Tabel 4.23 Hasil proses dumping <i>Zeus</i> pada <i>RAM Windows XP</i>	46
Tabel 4.24 Hasil proses Malfind <i>Zeus</i> pada <i>RAM Windows XP</i>	46
Tabel 4.25 Hasil scan mutex <i>Zeus</i> pada <i>RAM Windows XP</i>	46
Tabel 4.26 Hasil analisa <i>Zeus</i> pada <i>Windows7</i>	48

DAFTAR GRAFIK

Grafik 4.1 Perbandingan <i>malicious process Zeroaccess</i>	50
Grafik 4.2 Perbandingan <i>malicious process Alureon.dx</i>	50
Grafik 4.3 Perbandingan <i>malicious process Zeus</i>	51

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.