

ANALISIS MALWARE FLAWED AMMY RAT DENGAN METODE REVERSE ENGINEERING

TUGAS AKHIR

DISUSUN OLEH:
Nama: Tesa Pajar Setia
NPM: 147006076



JURUSAN INFORMATIKA
FAKULTAS TEKNIK UNIVERSITAS SILIWANGI
TASIKMALAYA
2018

ABSTRACT

Malware is currently growing rapidly, diverse and complex. But, human resources that can carry out malware analysis is limited, because special expertise is needed. Reverse engineering is one of many solution that can carry out malware analysis, because reverse engineering techniques can reveal malware code. On March 5, 2018, found spam email containing files, the file contained malware flawed ammyy. This flawed ammyy is a software that comes from Ammyy Admin version 3 and then misused by hackers TA505. This study aims to identify the malware, especially the Flawed Ammyy RAT malware.

This research uses descriptive methodology, then to do malware analysis used dynamic analysis and reverse engineering methods.

The results of the study show that the Flawed Ammyy RAT malware works by hiding in the Ammyy Admin application then connecting to the attacker with ip address 103.208.86.69. netname ip address 103.208.86.69 is zappie host. There are 50 registry changes that are carried out by malware on infected systems. After the attacker has been connected with the victim, the attacker can easily do the remote control without the victim's knowledge.

Keyword: Analysis, Engineering Reverse, Flawed Ammyy, Malware,

ABSTRAK

Malware saat ini berkembang dengan pesat, beragam dan kompleks. Namun kurangnya sumber daya manusia yang dapat melakukan analisis *malware* karena diperlukan keahlian khusus. *Reverse engineering* merupakan salah satu solusi untuk melakukan analisis *malware* karena menggunakan teknik *reverse engineering* kode pada *malware* dapat diketahui. 5 Maret 2018 ditemukan *spam email* yang berisi *file*, *file* tersebut terdapat *malware flawed ammyy*. *Flawed ammyy* ini merupakan *software* yang berasal dari *Ammyy Admin* versi 3 kemudian disalah gunakan oleh hacker TA505.

Penelitian ini bertujuan untuk melakukan proses identikasi *malware* kususnya *malware Flawed Ammyy RAT*. Penelitian ini menggunakan metodologi deskriptif, kemudian untuk melakukan analisis *malware* digunakan metode analisis dinamis dan *reverse engineering*.

Hasil dari penelitian menunjukan bahwa *malware Flawed Ammyy RAT* bekerja dengan bersembunyi pada aplikasi *Ammyy Admin* kemudian melakukan koneksi dengan *attacker* dengan *ip address* 103.208.86.69. *netname ip address* 103.208.86.69 adalah *zappie host*. Perubahan 50 registry yang dilakukan *malware* pada system yang terinfeksi. Setelah *attacker* terkoneksi dengan korban maka *attacker* dengan mudah melakukan *remote control* tanpa sepengetahuan korban.

Kata kunci: Analysis, Engineering Reverse, Flawed Ammyy, Malware,

KATA PENGANTAR

Dengan mengucapkan syukur kepada Allah swt Yang Maha Esa atas berkat, rahmat serta karunia-Nya, Penulis dapat menyelesaikan skripsi berjudul: *Analisis Malware Flawed Ammy RAT Dengan Metode Reverse Engineering*. Skripsi ini ditujukan untuk memenuhi salah satu persyaratan ujian guna memperoleh gelar Sarjana Teknik (S.T) pada Prodogram Studi Informatika, Fakultas Teknik, Universitas Siliwangi Tasikmalaya

Terselesaikannya skripsi ini tidak terlepas dari bantuan banyak pihak, sehingga pada kesempatan ini dengan segala kerendahan hati dan penuh rasa hormat penulis menghaturkan terima kasih yang sebesar-besarnya bagi semua pihak yang telah memberikan bantuan moril maupun materil baik langsung maupun tidak langsung dalam penyusunan skripsi ini hingga selesai, terutama kepada yang saya hormati:

1. Bapak Prof. Dr. H. Rudi Priyadi, Ir., M.S. selaku Rektor Universitas Siliwangi
2. Bapak Ir. H. Asep Kurnia Hidayat., M.T selaku Dekan Fakultas Teknik Universitas Siliwangi
3. Bapak R. Reza El Akbar, M.T., M.Kom., selaku Ketua Jurusan Informatika Universitas Siliwangi
4. Bapak Nur Widiyasono, M.Kom., CEH., CHFI. dan bapak Aldi Putra Aldya., S.T., M.T., selaku dosen pembimbing skripsi saya yang telah memberikan kritik dan saran bimbingan maupun arahan yang sangat berguna dalam penyusunan skripsi ini.

5. Bapak atau Ibu dosen dan staff di lingkungan Fakultas Teknik Unsil, khususnya Program Studi Informatika yang telah banyak membantu kami untuk dapat melaksanakan penulis dalam studi.
6. Teristimewa kepada Orang Tua penulis Uus Muhamad Husna dan Dede Judliah yang selalu mendoakan, memberikan motivasi dan pengorbanannya baik dari segi moril, materi kepada penulis sehingga penulis dapat menyelesaikan skripsi ini. Buat sahabat – sahabat saya TI-B 2014 dan Kader Anti Narkotika Unit Kegiatan Mahasiswa Universitas Siliwangi
7. Terima kasih juga kepada semua pihak yang telah membantu dalam penyelesaian skripsi ini yang tidak dapat disebutkan satu per satu.

Penulis menyadari dalam penulisan skripsi ini masih jauh dari sempurna, dan banyak kekurangan baik dalam metode penulisan maupun dalam pembahasan materi. Hal tersebut dikarenakan keterbatasan kemampuan Penulis. Sehingga Penulis mengharapkan saran dan kritik yang bersifat membangun mudah-mudahan dikemudian hari dapat memperbaiki segala kekurangannya.

Tasikmalaya. Agustus 2018

Penulis

Tesa Pajar Setia

DAFTAR ISI

ABSTRAK.....	i
ABSTRACT	ii
KATAPENGANTAR	iii
DAFTAR ISI.....	v
DAFTAR TABEL	vii
DAFTAR GAMBAR.....	viii
 BAB I PENDAHULUAN	
1.1 Latar Belakang	I-1
1.2 Rumusan Masalah	I-7
1.3 Tujuan Penelitian	I-7
1.4 Batasan Masalah	I-7
1.5 Manfaat penelitian.....	I-8
1.6 Metodologi.....	I-8
1.7 Sistematika Penulisan	I-8
 BAB II LANDASAN TEORI	
2.1 Malware	II-1
2.2 Klasifikasi malware.....	II-1
2.3 Flawed Ammyy RAT	II-4
2.4 Anaisis Malware	II-5
2.5 Reverse Engineering	II-9
2.6 Kajian Penelitian Sebelumnya	II-12
2.7 Matrik	II-19
2.8 Peta Penelitian	II-21
2.9 Diagram Fishbone	II-23
 BAB III METODOLOGI	
3.1 Metodologi Penelitian	III-1
3.2 Study literature	III-1
3.3 Analisis Dinamis	III-2
3.4 Reverse Engineering	III-5
3.5 Dokumentasi	III-5
 BAB IV HASIL DAN PEMBAHASAN	
4.1 Hasil	IV-1
4.1.1 Study Literature	IV-1
4.1.2 Tahap Analisis Dasar	IV-1
4.1.3 Analisis Dinamis	IV-2
4.1.4 Reverse Engineering	IV-14
4.2 Pembahasan	IV-16

4.2.1 Malware workflow	IV-16
4.2.2 Pencegahan malware	IV-17
4.2.3 Ciri-ciri komputer terinfeksi malware flawed ammyy rat	IV-19
4.2.4 Pemulihan system setelah terinfeksi malware	IV-19

BAB V SIMPULAN DAN SARAN

5.1 Simpulan.....	V-1
5.2 Saran	V-3

DAFTAR PUTAKA

LAMPIRAN

DAFTAR TABEL

Tabel 2.1 contagious threats klasifikasi dan deskripsi	II- 2
Tabel 2.2 Masked threats klasifikasi dan deskripsi	II-3
Tabel 2.3 financial threats klasifikasi dan deskripsi	II-4
Tabel 2.4 Penelitian Terkait	II-12
Tabel 2.5 Penelitian yang mendekati	II-15
Tabel 2.6 Matrik Penelitian Analisis Malware Flawed Ammyy RAT	II-19
Tabel 3.1 Spesifikasi computer	III-2
Tabel 3.2 Spesifikasi Virtual	III-3
Tabel 3.3 Perbandingan Virtual dengan Real	III-3
Tabel 4.1 informasi malware Flawed Ammyy RAT	IV-1
Tabel 4.2 Penggunaan system pada vmware	IV-4
Tabel 4.3 string malware Flawed Ammyy RAT	IV-8
Tabel 4.4 hasil dissembler malware Flawed Ammyy RAT	IV-14

DAFTAR GAMBAR

Gambar 1.1 distribusi berbagai malware	I-2
Gambar 1.2 Contoh email dari 5 Maret 2018, kampanye FlawedAmmyy	I-4
Gambar 1.3 isi file .url	I-4
Gambar 1.4 Dialog peringatan ditampilkan setelah mengklik dua kali file .url.....	I-5
Gambar 1.5 Screenshot dari lampiran dokumen dari 1 Maret 2018, kampanye Flawed Ammyy	I-6
Gambar 2.1 klasifikasi Malware	II-2
Gambar 2.2 representasi hierarchal berbagai teknik deteksi malware	II-5
Gambar 2.3 Peta Penelitian Malware	II-21
Gambar 2.4 diagram fishbone	II-24
Gambar 3.1 alur metodologi penelitian	III-1
Gambar 3.2 alur metode analisis dinamis	III-2
Gambar 4.1 flowchart Analisis Dinamis Flawed Ammyy RAT	IV-2
Gambar 4.2 virtual mesin	IV-3
Gambar 4.3 ApateDNS	IV-5
Gambar 4.4 ping google pada cmd virtual mesin	IV-6
Gambar 4.5 tampilan process hacker	IV-7
Gambar 4.6 tampilan process hacker setelah running malware	IV-7
Gambar 4.7 tampilan string search pada fitur process hacker	IV-8
Gambar 4.8 tampilan Regshot	IV-10
Gambar 4.9 compare 1th dan 2nd	IV-11
Gambar 4.10 tampilan WireShark	IV-12
Gambar 4.11 hasil capture WireShark terhadap paket data malware	IV-12
Gambar 4.12 informasi <i>ip address</i> 103.208.86.69 pada <i>tools Whois Ip Look Tool</i>	IV-13
Gambar 4.13 proses dari malware Flawed Ammyy RAT	IV-16