ANALISIS MALWARE FLAWED AMMYY 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 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 komplek. 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 terkonesi 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 Ammyy 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 pembinbing 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 kekuranganya.

Tasikmalaya. Agustus 2018

Penulis

Tesa Pajar Setia

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR