ANALISIS *MALWARE* "*HUMMINGBAD*" PADA PERANGKAT *SMARTPHONE* MENGGUNAKAN METODE HYBRID

TUGAS AKHIR

Oleh :

Nama : Fitri Amalia Febriandiny
Npm : 157006081

PROGRAM STUDI INFORMATIKA
FAKULTAS TEKNIK UNIVERSITAS SILIWANGI
TASIKMALAYA

2021

LEMBAR PENGESAHAN TUGAS AKHIR

ANALISIS *MALWARE "HUMMINGBAD"* PADA PERANGKAT *SMARTPHONE* MENGGUNAKAN METODE HYBRID

TUGAS AKHIR

Oleh:
Fitri Amalia Febriandiny
157006081

Menyetujui,
Tasikmalaya, tanggal bulan 2021

Pembimbing I	Pembimbing II
Dr. Aradea, S.T., M.T.	**Nur Widiyasono, S.Kom., M.Kom**
NIDN. 0424097601	NIDN. 0310127203

Mengetahui,

Dekan Fakultas Teknik Universitas Siliwangi Tasikmalaya	Ketua Jurusan Informatika
Prof. Dr. Eng. H. Aripin	**Nur Widiyasono, S.Kom., M.Kom**
NIP. 196708161996031001	NIDN. 0310127203

LEMBAR PENGESAHAN PENGUJI SIDANG TUGAS AKHIR

ANALISIS *MALWARE "HUMMINGBAD"* PADA PERANGKAT *SMARTPHONE* MENGGUNAKAN METODE HYBRID

Oleh:
Fitri Amalia Febriandiny
157006081

Menyetujui,

Telah dipertanggung jawabkan di dalam Sidang Tugas Akhir
Pada Tanggal, Tanggal Bulan 2021

Tim Penguji Sidang Tugas Akhir :

Rianto, S.T., M.T. _____
NIDN. 0424128401
Ketua Sidang TA

Alam Rahmatulloh, S.T., M.T. _____
NIDN. 0021128703
Anggota

Pembimbing I	Pembimbing II
Dr. Aradea, S.T., M.T.	**Nur Widiyasono, S.Kom., M.Kom**
NIDN. 0424097601	NIDN. 0310127203

JURUSAN INFORMATIKA
FAKULTAS TEKNIK UNIVERSITAS SILIWANGI

LEMBAR PERNYATAAN KEASLIAN TUGAS AKHIR

Saya yang bertanda tangan dibawah ini:

Nama : Fitri Amalia Febriandiny

NPM : 157006081

Jurusan/Program Studi : Informatika

Menyatakan bahwa Tugas Akhir yang berjudul:

ANALISIS *MALWARE "HUMMINGBAD"* PADA PERANGKAT *SMARTPHONE* MENGGUNAKAN METODE HYBRID

Benar – benar merupakan hasil karya pribadi dan bukan merupakan hasil karya orang lain atau pihak manapun, serta **BUKAN PLAGIAT**. Seluruh sumber yang dijadikan rujukan dan dikutip dalam laporan Tugas Akhir ini telah saya nyatakan dengan benar. Apabila dikemudain hari penryataan saya ini tidak benar, maka saya bersedia menanggung semua akibat atau sanksi yang berlaku.

Tasikmalaya, Bulan 2021

FITRI AMALIA FEBRIANDINY
NPM. 157006081

ABSTRAK

Seiring dengan pesatnya penetrasi jaringan global dan kemajuan mobile internet di Indonesia, semakin menambah kerentanan keamanan informasi sebuah organisasi dari ancaman siber. Malware didefinisikan sebagai semua perangkat lunak jahat, program komputer jahat, atau perangkat lunak jahat, seperti virus (komputer), trojans, spyware, dan worm. Menurut hasil penelitian dari Check Point telah menemukan varian baru yang tersembunyi dari malware HummingBad di lebih dari 20 aplikasi di Google Play. HummingBad muncul sebagai malware yang sangat canggih dan berkembang dengan baik, yang menggunakan taktik rootkit dan chain-attack untuk mendapatkan kontrol penuh atas perangkat yang terinfeksi. Ponsel yang terinfeksi menampilkan iklan ilegal dan memasang aplikasi palsu pada saat setelah ponsel dihidupkan layarnya, dihidupkan ulang atau dimatikan ponselnya, dan melakukan perubahan dalam konektivitas internet. Hal tersebut dilakukan dengan menggunakan perangkat yang terinfeksi untuk meniru klik pada tombol instal, beli, dan terima. Indonesia menempati urutan keempat dalam hal infeksi malware HummingBad terhadap ponsel dengan sistem operasi Android dengan jumlah sebanyak 489.336 perangkat yang terinfeksi. Diketahuinya jenis malware tersebut maka dapat dilakukan "counter measure" untuk melindungi perangkat terinfeksi malware jenis ini. Metode yang digunakan untuk analisa malware tersebut dengan Reverse engineering dan Dinamis analisis sehingga dapat diketahui bahwa malware tersebut membaca da mengirim pesan, melakukan pengabilan data log panggilan, membaca versi android, ime, melakukan singkronisasi pada ip address 185.38.111.1. netname neroso, country ip tersebut CZ, admin-c ip addres tersebut JH24160-RIPE, person ip addres Jan Horak.

Kata Kunci: *Analisa Malware, HummingBad, Hybrid, Virus.*

ABSTRACT

Along with the rapid penetration of the global network and the advancement of the mobile internet in Indonesia, it is increasingly adding to the vulnerability of an organization's information from cyber threats. Malware is defined as any malicious software, malicious computer program, or malicious software, such as viruses (computers), trojans, spyware, and worms. According to the results of research from Check Point has found a new hidden variant of the HummingBad malware in more than 20 applications on Google Play. HummingBad appears as a highly sophisticated and well-developed malware, which uses rootkit and chain-attack tactics to gain complete control over infected devices. Mobile phones that display illegal advertisements and install fake applications when the screen is turned on, restarts or turns off the phone, and make changes to internet connectivity. It does this by using the infected device to mimic a click on the install, buy, and accept buttons. Indonesia ranks fourth in terms of HummingBad malware infection on cellphones with the Android operating system with a total of 489,336 infected devices. If the type of malware is seen, a "countermeasure" can be carried out to protect devices infected with this type of malware. The method used to analyze the malware is reverse engineering and dynamic analysis so that it can be seen that the malware reads and sends messages, retrieves call log data, reads the android version, IMEI, synchronizes on the IP address 185.38.111.1. netname neroso, country ip is CZ, admin-c ip address is JH24160-RIPE, person ip address is Jan Horak.

Keywords: *Malware Analysis, HummingBad, Hybrid, Virus.*

KATA PENGANTAR

Puji syukur kehadirat Allah SWT yang telah memberikan segala berkah dan karunia-Nya, sehingga penulis dapat menyelesaikan penyusunan laporan tugas akhir yang berjudul "Analisis *Malware "Hummingbad"* Pada Perangkat *Smartphone* Dengan Munggunakan Metode Hybrid". Tugas akhir ini merupakan salah satu syarat akademik bagi seluruh mahasiswa Jurusan Informatika di Universitas Siliwangi.

Dalam penyusunan laporan tugas akhir ini penulis banyak menerima bimbingan, arahan, motivasi, dan bantuan dari berbagai pihak, baik langsung maupun tidak langsung. Ucapan terimakasih yang sebesar-besarnya kepada semua pihak yang telah membantu dalam menyelesaikan penelitian ini, khususnya kepada:

1. Bapak Prof. Dr. Eng. H. Aripin selaku dekan Fakultas Teknik Universitas Siliwangi Tasikmalaya.
2. Bapak Nur Widiyasono, S.Kom., M.Kom., selaku ketua Jurusan Informatika Fakultas Teknik Universitas Siliwangi Tasikmalaya.
3. Bapak Dr., Aradea, S.T., M.T., selaku Dosen Pembimbing I yang senantiasa sabar memberikan bimbingan, arahan dan meluangkan waktu serta pikirannya dalam menyempurnakan laporan tugas akhir ini.
4. Bapak Nur Widiyasono, S.Kom., M.Kom., selaku Dosen Pembimbing II yang senantiasa sabar memberikan bimbingan, arahan dan meluangkan waktu serta pikirannya dalam menyempurnakan laporan tugas akhir ini.
5. Seluruh staf dosen pengajar serta segenap karyawan di lingkungan Fakultas Teknik Universitas Siliwangi Tasikmalaya.

6. Kepada orang tua Bapak Iman Firman dan Ibu Rany Trihayatini yang telah memberikan dukungan doa baik secara materil maupun moril,motivasi, kesabaran dan pengorbanan yang senantiasa tulus menyertai penulis selama ini.
7. Kepada kakak tercinta Tegar Januar Dikri R dan teteh Winny Putri Lestari yang telah memberikan dukungan, motivasi dan kesabaran dalam melakukan penyusunan Tugas Akhir ini.
8. Sahabat terdekat Rifqi Muliawan yang selalu mendengarkan keluh kesah, memberikan motivasi, dukungan & meluangkan waktunya selama penyusunan Tugas Akhir.
9. Sahabat – sahabat selama perkuliahan (Santi, Sinta, Resa, Meitha, Gantina, Nadilla) yang selalu memberikan dukungan dan semangat selama melakukan penyusunan Tugas Akhir.
10. Sahabat – sahabat SMK (Nabila, Sri, Dita) yang selalu memberikana motivasi dan dukungan kepada penulis dalam melakukan penyusunan Tugas Akhir.
11. Dan semua pihak-pihak yang tidak dapat disebutkan satu persatu yang telah memberi bantuan dan dorongan baik moral maupun materil.

Penulis sadar dalam penulisan laporan tugas akhir ini masih banyak kekurangannya, untuk itu dengan senang hati penulis akan menerima kritik dan saran untuk perbaikannya. Akhirnya penulis dapat menyelesaikan laporan tugas akhir ini, yang tentunya tidak terlepas dari bantuan semua pihak. Terima kasih atas bantuannya dan semoga Allah SWT. membalas segala kebaikan dan bantuan yang telah diberikan kepada penulis dan semoga laporan tugas akhir ini memberikan manfaat bagi kita semua, Insyaallah. Aamiin.

Tasikmalaya, bulan 2021

Penulis

DAFTAR ISI

BAB III METODE PENELITIAN

BAB IV HASIL DAN PEMBAHASAN

BAB V KESIMPULAN DAN SARAN

DAFTAR GAMBAR

DAFTAR TABEL