RANCANG BANGUN APLIKASI DETEKSI *MALWARE* BERBASIS *COLLECTIVE INTELLIGENCE FRAMEWORK (CIF)* PADA *HONEYPOT*

SKRIPSI

disusun oleh

Restu Pratama

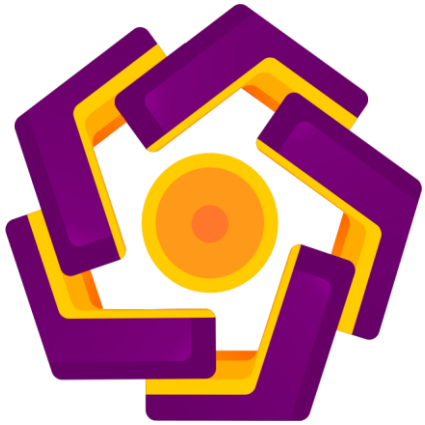
14.11.7976

PROGRAM SARJANA
PROGRAM STUDI INFORMATIKA
UNIVERSITAS AMIKOM YOGYAKARTA
YOGYAKARTA
2018

RANCANG BANGUN APLIKASI DETEKSI *MALWARE* BERBASIS *COLLECTIVE INTELLIGENCE FRAMEWORK (CIF)* PADA *HONEYPOT*

SKRIPSI

untuk memenuhi sebagian persyaratan
mencapai gelar Sarjana
pada Program Studi Informatika



disusun oleh

Restu Pratama

14.11.7976

PROGRAM SARJANA
PROGRAM STUDI INFORMATIKA
UNIVERSITAS AMIKOM YOGYAKARTA
YOGYAKARTA
2018

PERSETUJUAN

SKRIPSI

RANCANG BANGUN APLIKASI DETEKSI *MALWARE* BERBASIS *COLLECTIVE INTELLIGENCE FRAMEWORK (CIF)* PADA *HONEYPOT*

yang dipersiapkan dan disusun oleh

Restu Pratama

14.11.7976

telah disetujui oleh Dosen Pembimbing Skripsi

pada tanggal 8 Februari 2018

Dosen Pembimbing,

Nila Feby Puspitasari, S.Kom., M.Cs

NIK. 190302161

PENGESAHAN

SKRIPSI

RANCANG BANGUN APLIKASI DETEKSI *MALWARE* BERBASIS *COLLECTIVE INTELLIGENCE FRAMEWORK (CIF)* PADA *HONEYPOT*

yang dipersiapkan dan disusun oleh

Restu Pratama

14.11.7976

telah dipertahankan di depan Dewan Penguji
pada tanggal 21 Februari 2018

Susunan Dewan Penguji

Nama Penguji	Tanda Tangan
Nila Feby Puspitasari, S.Kom., M.Cs. **NIK. 190302161**	
M. Rudyanto Arief, M.T. **NIK. 190302098**	
Ferry Wahyu Wibowo, S.Si., M.Cs. **NIK. 190302235**	

Skripsi ini telah diterima sebagai salah satu persyaratan
untuk memperoleh gelar Sarjana Komputer
Tanggal 12 Maret 2018

DEKAN FAKULTAS ILMU KOMPUTER

Krisnawati, S.Si., M.T.
NIK. 190302038

PERNYATAAN

Saya yang bertandatangan dibawah ini menyatakan bahwa, skripsi ini merupakan karya saya sendiri (ASLI), dan isi dalam skripsi ini tidak terdapat karya yang pernah diajukan oleh orang lain untuk memperoleh gelar akademis di suatu institusi pendidikan tinggi manapun, dan sepanjang pengetahuan saya juga tidak terdapat karya atau pendapat yang pernah ditulis dan/atau diterbitkan oleh orang lain, kecuali yang secara tertulis diacu dalam naskah ini dan disebutkan dalam daftar pustaka.

Segala sesuatu yang terkait dengan naskah dan karya yang telah dibuat adalah menjadi tanggung jawab saya pribadi.

Yogyakarta, 12 Maret 2018

Restu Pratama

NIM. 14.11.7976

MOTTO

You gotta step out of your comfort zone.

Be broke for a while.

Lose some friends.

Have some sleepless nights.

Most people don’t get it though.

PERSEMBAHAN

بِسْمِ اللَّهِ الرَّحْمَٰنِ الرَّحِيمِ

Alhamdulillahirabbil'alamin puji syukur atas kehadirat Allah SWT berkat rahmat dan karunia-Nya lah penulis dapat menyelesaikan skripsi ini sebagai salah satu persyaratan untuk mencapai gelar Sarjana Komputer. Skripsi ini saya persembahkan kepada :

1. Kedua Orang Tua, Bapak Suroto dan Ibu Maryati serta seluruh keluarga besar yang senantiasa memberikan semangat, doa, serta motivasi yang tiada henti.
2. Ibu Nila Feby Puspitasari, S.Kom., M.Cs selaku dosen pembimbing yang selalu mengarahkan dan memberikan masukan dalam proses penyusunan skripsi ini.
3. Keluarga besar 14-S1TI-06 atas segala bentuk dukungan yang telah diberikan.
4. Teman – teman Universitas Amikom Yogyakarta yang senantiasa memberikan semangat dan dukungan selama penelitian dan penyusunan skripsi.

KATA PENGANTAR

Puji dan syukur penulis panjatkan kehadirat Allah SWT yang telah melimpahkan kasih sayang dan sayang-Nya sehingga penulis dapat menyelesaikan skripsi yang berjudul "Rancang Bangun Aplikasi Deteksi *Malware* Berbasis *Collective Intelligence Framework* (CIF) Pada *Honeypot*".

Maksud dari penyusunan skripsi ini adalah untuk memenuhi salah satu syarat untuk mendapatkan gelar sarjana pada Program Studi Informatika di Universitas Amikom Yogyakarta.

Dalam penyusunan skripsi ini, banyak pihak yang membantu dalam berbagai hal. Oleh karena itu, penulis menyampaikan rasa terima kasih kepada :

1. Ibu Nila Feby Puspitasari, S.Kom., M.Cs. selaku pembimbing.
2. Seluruh dosen Program Studi Informatika Universitas Amikom Yogyakarta.
3. Orang tua dan keluarga tercinta yang telah memberikan banyak dukungan baik secara moril maupun materiil.
4. Sahabat dan rekan yang selalu memberikan dukungan yang selalu memberikan dukungan dan motivasi.
5. Semua pihak yang telah membantu dalam penyusunan skripsi ini.

Yogyakarta, Februari 2018

Penulis

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

INTISARI

Perkembangan *malware* semakin meningkat dan bervariasi dari tahun ke tahun. Tidak hanya menargetkan sistem komputer sebagai korbannya, *malware* juga menyerang *smartphone* dan perangkat IoT. Menurut survey yang dilakukan oleh symantec, pada tahun 2016 terdapat 357 juta jenis *malware* baru yang secara aktif menyerang sistem komputer dan smartphone. Beberapa pencegahan telah dilakukan di berbagai instansi termasuk dengan memasang *honeypot* untuk menangkap *malware* yang menyerang melalui jaringan komputer.

Penggunaan *honeypot* untuk menangkan *malware* pada jaringan komputer dianggap cukup efektif karena selain mendapatkan salinan *malware*, *honeypot* juga dapat mencatat informasi tentang pengirim *malware*. Namun demikian, kemampuan *honeypot* dalam mendeteksi *malware* masih sangat sederhana sehingga dibutuhkan aplikasi untuk meningkatkan kemampuan *honeypot* dalam mendeteksi *malware*.

Aplikasi yang dibuat dalam penelitian ini mampu meningkatkan kemampuan *honeypot* dalam mendeteksi *malware* dengan memanfaatkan *collective intelligence framework (CIF)*. CIF tidak hanya mendeteksi *hash malware* melainkan juga *ip address* pengirim sehingga dapat dilakukan pencegahan. Hasil yang diperoleh adalah serangan *malware* dapat dideteksi dan dicegah walaupun dengan persentase deteksi yang masih kecil.

Kata Kunci: *malware, honeypot, threat intelligence, dionaea, CIF.*

ABSTRACT

The development of malware is increasing and varies from year to year. Not only targeting computer systems as a victim, malware also attacks smartphones and IoT devices. According to a survey conducted by Symantec, by 2016 there are 357 million new types of malware that actively attack computer and smartphone systems. Some precautions have been done in various instances including by installing a honeypot to capture the malware that is attacking through a computer network.

The use of honeypot to capture malware on computer networks is considered quite effective because in addition to getting a copy of malware, honeypot can also record information about the sender of malware. However, the ability of honeypot in detecting malware is still very simple so that the application needed to improve the ability of honeypot in detecting malware.

Applications created in this study are able to improve the ability of honeypot in detecting malware by utilizing collective intelligence framework (CIF). CIF not only detects malware hash but also the sender ip address so the attack can be prevented. The results obtained are malware attacks can be detected and prevented even with a small percentage of detection.

Keyword: *malware, honeypot, threat intelligence, dionaea, CIF.*