

IMPLEMENTASI *MONITORING AUTONOMOUS SPREADING MALWARE* DI ITS-NET DENGAN DIONAEA DAN CUCKOO

Nama Mahasiswa : Febian Bramanta Alfiansyah
NRP : 5210 100 087
Jurusan : Sistem Informasi FTIF-ITS
Dosen Pembimbing I : Bambang Setiawan, S.Kom., M.T
Dosen Pembimbing II : Bekti Cahyo Hidyanto, S.Si., M.Kom

ABSTRAK

Akhir tahun 2013 Indonesia berada di posisi teratas sebagai Negara dengan traffic malware tertinggi. Hal ini membuat miris, Indonesia yang pengguna internetnya baru seperempat dari total populasi bisa menciptakan masalah malware sedemikian besar. ITS (Institut Teknologi Sepuluh Nopember) sebagai perguruan tinggi yang mengedepankan TI (teknologi informasi) patut mempertimbangkan masalah malware ini. Kebutuhan akan traffic informasi yang tinggi membuat seluruh sistem harus handal dan tersedia setiap kali pengguna ingin mengaksesnya.

Berdasarkan dari permasalahan ini, maka akan dilakukan penelitian untuk mengetahui ancaman malware yang ada di jaringan ITS. Penelitian dilakukan dengan melakukan implementasi Honeypot Dionaea dan Cuckoo di infrastuktur ITS-Net untuk memonitor autonomous spreading malware. Monitoring dilakukan untuk mengetahui jenis dan persebaran malware yang ada di lingkungan jaringan ITS-Net.

Hasil analisis malware akan membantu ITS-Net untuk mengantisipasi ancaman malware dengan memperkuat keamanan komputer berdasarkan hasil analisis sederhana malware. Selain itu, hasil informasi malware yang didapatkan dapat dibagi ke komunitas lain untuk mengakui tentang tren

malware saat ini dan dapat menggambarkan penerapan honeynet di lingkungan perguruan tinggi.

Kata Kunci: Malware, Honeynet, Keamanan Komputer, Honeypot Dionaea, Cuckoo Sandbox

IMPLEMENTATION OF AUTONOMOUS SPREADING MALWARE IN ITS-NET BY DIONAEA AND CUCKOO

Student Name : Febian Bramanta Alfiansyah
NRP : 5210 100 087
Departement : Sistem Informasi FTIF-ITS
Supervisor I : Bambang Setiawan, S.Kom., M.T
Supervisor II : Bekti Cahyo Hidyanto, S.Si., M.Kom

ABSTRACT

In the end of 2013 Indonesia is in the top position as the country with the highest malware traffic. This makes sad, Indonesia, which has internet users amounted to a quarter of the total population could create such a large malware problems. ITS (Institute of Technology) as a college that emphasizes of IT (information technology) should consider this malware problem. The need for high traffic information makes the entire system must be reliable and available whenever the user wants to access it.

Based on this problem, it will be held research about the malware threats that exist in the ITS network. This research conducted by the implementation Honeypot Dionaea and Cuckoo on infrastructure ITS-Net to monitor autonomous spreading malware. Monitoring was conducted to determine the types and distribution of malware that exist in the network environment ITS-Net.

Results of malware analysis will help the ITS-Net to anticipate the threat of malware to strengthen computer security based on a simple analysis of malware. Moreover, the results obtained malware information can be shared to other communities to acknowledge about current malware trends

and can describe the application of honeynet in the college environment.

Keywords: Malware, Honeynet, Computer Security, Honeypot Dionaea, Cuckoo Sandbox