Blantika : Multidisciplinary Jornal
Volume 1 Number 2, February, 2023
p- ISSN xxxx-xxxx e-ISSN 2985-4199

ANALISIS MALWARE DENGAN METODE DINAMIK MENGGUNAKAN *FRAMEWORK CUCKOO SANDBOX*

Hairil Novansyah[1], Tata Sutabri[2]
Universitas Bina Darma Palembang, Indonesia[12]
E-mail: hairilnovansyah@gmail.com[1], tatasutabri@binadarma.ac.id[2]

INFO ARTIKEL
Diterima: 15 Februari 2023
Direvisi: 20 Februari 2023
Disetujui: 25 Februari 2023

ABSTRAK

Di era revolusi 4.0 yang menerapkan teknologi otomatis dan pertukaran data dalam teknologi manufaktur. Penerapan industri 4.0 di Indonesia dapat ditemui di berbagai bidang industri, salah satunya yaitu bidang teknologi informasi. Perkembangan revolusi 4.0 ini mempunyai dampak positif di bidang informasi, yang memudahkan tiap individu untuk mendapatkan informasi dimana saja. Namun, hal ini juga memiliki dampak negative yaitu munculnya berbagai macam tindak kejahatan siber, seperti penyebaran malware. Tujuan dari penelitian ini adalah untuk menganalisis karakteristik *malware* yang ditemukan pada jaringan Institut Teknologi Pagar Alam. Adapun metode yang digunakan dalam penelitian ini adalah *Dynamic Analysis* dan menggunakan *tool Cuckoo Sandbox*, sehingga tidak ada resiko untuk terinfeksi *malware*. Berdasarkan Analisa yang dilakukan tentang karakteristik dari *malware*, dapat disimpulkan bahwa terdapat *signature*, *string*, dan perubahan pada *value registry*.

Kata Kunci: Perangkat perusak; Kotak Pasir *Cuckoo*; Analisis dinamis; Teknologi informasi

ABSTRACT

The era of the 4.0 revolution which implemented automated technology and data exchange in manufacturing technology. The application of industry 4.0 in Indonesia can be found in various industrial fields, which is the information technology sector. The development of the 4.0 revolution has had a positive impact on the information sector, which makes it easier for each individual to get information anywhere. However, this also has a negative impact, that is the emergence of various types of cybercrimes, such as the spread of malware. The purpose of this study is to analyze the characteristics of the malware found on the Institute of Technology Pagar Alam network. The method used in this study is Dynamic Analysis and uses the Cuckoo Sandbox tool, so there is no risk of being infected with malware. Based on the analysis conducted on the

characteristics of the malware, it can be concluded that there are signatures, strings, and changes to the registry values.
Keyword; Malware; Cuckoo Sandbox; Analyzes dinamik; Information technology

PENDAHULUAN

Era revolusi industri ditandai dengan adanya perubahan pada pola hidup dan pola piker masyarakat dan negara. Perubahan terjadi seiring dengan kemampuan manusia dalam melahirkan inovasi. Revolusi industri 4.0 yaitu era yang ditandai dengan adanya konektivitas manusia, data, dan mesin dalam bentuk virtual atau dikenal dengan istilah *cyber physical*. Pada era revolusi industri 4.0 ini ada pergeseran trend inovasi ke arah teknologi digital yaitu memungkinkan otomatisasi di semua bidang untuk mencapai produktivitas yang efektif dan efisien (Ghufron, 2018).

Istilah lain untu revolusi industri 4.0 adalah revolusi digital dan era disrupsi teknologi. Semua bidang akan menggunakan otomatisasi sistem pencatatn dengan komputer. Salah satu karakteristik unik dari revolusi industri 4.0 adalah penerapan kecerdasan buatan dalam semua bidang industry (Ghufron, 2018). Pada era revolusi industri 4.0, bidang informatika sangat berpengaruh dalam perkembangannya. Perkembangan revolusi 4.0 memiliki dampak positif dan dampak negative bagi masyarakat dan negara. Terdapat pihak-pihak yang memanfaatkan dalam sisi negative yaitu seperti mengembangkan sebuah *software* yang dapat melakukan tindak kejahatan atau yang biasa disebut dengan *cybercrime* (Indrajit, 2011). Salah satu bentuk dari kejahatan ini yaitu dengan menyebarkan malware.

Malware atau malicious software merupakan perangkat lunak yang secara eksplisit didesain untuk melakukan aktifitas berbahaya atau perusak perangkat lunak lainnya seperti Trojan, Virus, *Spyware* dan *Exploit* (Cahyanto et al., 2017). *Malware* atau *Malicious Software* merupakan program yang dirancang untuk merusak ke dalam sebuah sistem dengan tujuan untuk melakukan beraneka ragam aktivitas yang bersifat merugikan pemiliknya seperti memperlambar kinerja sistem himgga merusak bahkan menghancurkan data penting yang tersimpan dalam sistem yang dimaksud (Kramer & Bradfield, 2010).

Tidak hanya merusak sistem secara langsung *malware* juga dapat membuat sistem rusak secara perlahan dengan cara memperbanyak aktivitas dari sistem atau menggandakan dirinya sendiri sehingga sistem akan melambat dan rusak secara perlahan (Ilman et al., 2014). Pada umumnya dalam mendeteksi penyalahgunaan dan anomali pada sebuah aplikasi menggunakan analisa seperti dynamic analysis dilakukan dengan mengeksekusi contoh malware untuk kemudian dipelajari perilaku yang ditimbulakn oleh malware tersebut (Ghaffari et al., 2017). Analisa dinamik dapat dilakukan dengan dua cara yaitu secara manual dan menggunakan tool analisa otomatis yaitu *cuckoo sandbox. Cuckoo Sandbox* merupakan tool yang

digunakan untuk mengalisa malware dan dapat memberikan beberapa informasi mengenai malware yang sedang berjalan dalam lingkungan yang terisolasi (Alfalqi et al., 2015). Beberapa hal yang dapat dilakukan *Cuckoo Sandbox* adalah sebagai berikut :

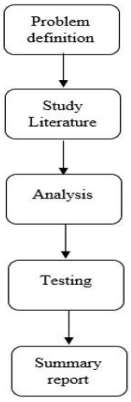
1. *Native function* dan *Windows* API *Calls Trace* yang dapat mencatat setiap eksekusi kode dari suatu file yang diupload ke dalam *Cuckoo Sandbox*.
2. Melakukan pencatatan pada setiap file yang dibuat atau dihapus dari sistem.
3. Memory dump dari hasil analisis malware.
4. Jejak aliran jaringan dalam format PCAP.
5. Screenshot desktop selama aktivitas analisis malware berlangsung.
6. Full memory dump dari mesin VM.

Cuckoo sandbox dapat melakukan analisa *malware* secara otomatis dan menampilkan informasi-informasi yang dilakuakn oleh sampel malware (Sibarani et al., 2019). Berdasarkan latar belakang masalah di atas *malware* merupakan perangkat lunak yang sangat merugikan pengguna sehingga kita perlu mengetahui bagaimana cara kerja dan apa saja dampak yang ditimbulkan oleh malware dengan menggunakan metode dinamik secara otomatis yaitu *cuckoo sandbox*.

METODE PENELITIAN

Metode penelitian yang digunakan untuk menganalisis malware menggunakan analisi dinamik yang terbagi menjadi dua yaitu tahapan penelitian dan rencana pengerjaan untuk menganalisa malware sebagai berikut (Sibarani et al., 2019) :

Tahapan Penelitian



Gambar 1. Tahapan Penelitian

1) Problem Definition, pada tahap ini, identidikasi permasalahan dalam penelitian, latar belakang maupun Batasan masalah yang digunakan pada penelitian ini.
2) Study Literature, pada tahap ini mempelajari berbagai informasi dari berbagai jenis jurnal maupun buku mengenai malware dan analisis *malware* serta cuckoo sandbox.
3) Analysis, pada tahap ini dilakukan analisis terhadap sampel *file malware*, *tool*. Data yang digunakan adalah data sampel yang diambil pada website Institut Teknologi Pagar Alam. *Tools* yang dipakai adalah *cuckoo sandbox* untuk proses analisa dinamis.

4) *Testing*, tahap ini merupakan tahap percobaan *malware* menggunakan tool *cuckoo sandbox* dan mengamati segala aktivitas yang ditimbulkan oleh malware tersebut.
5) Summary Report, tahap ini dilakukan evaluasi keseluruhan tahapan penelitian dan mendokumentasikan dalam bentuk laporan.

Rencana Pengerjaan

Pengerjaan yang dilakukan pada penelitian ini yaitu dengan menggunakan *tool cuckoo sandbox* versi 2.0.7 secara online dengan memasukkan *malware* yang akan dianalisa. Dan menganalisis setiap segala aktivitas yang terjadi serta mendokumentasikan dalam bentuk laporan.

HASIL DAN PEMBAHASAN

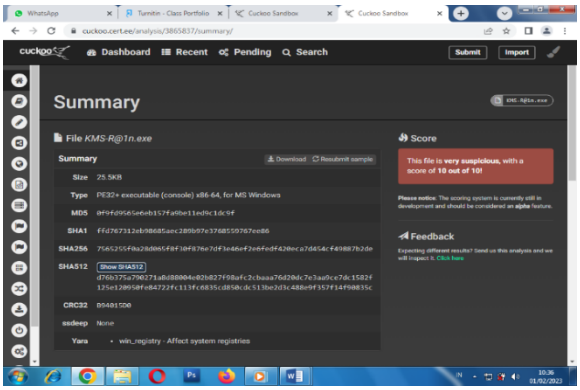
Analisis *malware*, menggunakan tahap pengujian yang digunakan sebagai acuan dalam menentukan karakteristik dan menggali informasi terkait dari perilaku yang akan ditimbulkan oleh program *malware* tersebut.

Pengujian

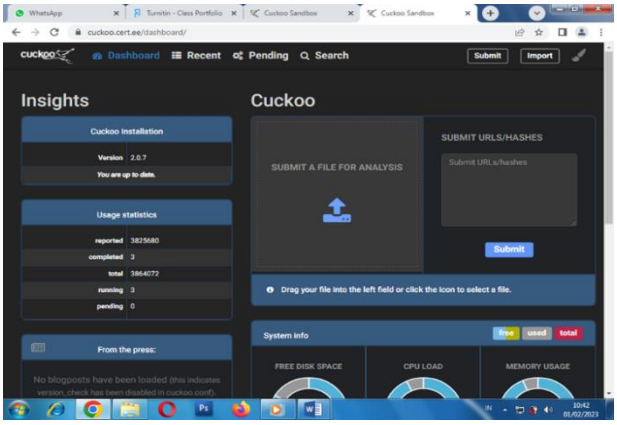
Analisa *malware* yang digunakan adalah analisa dinamis yaitu dengan menjalankan *malware* pada komputer serta mempelajari perilaku *malware* tersebut pada komputer. Ketika menginfeksi komputer, *malware* biasanya melakukan modifikasi pada sistem, misalnya merubah *registry*, menghapus file, menjalankan *service* tertentu dan lain-lain. Ketika melakukan analisa *malware* selalu ada risiko pada komputer terinfeksi *malware*. Sebaiknya analisa *malware* dilakukan pada lab malware. Atau untuk mengurangi resiko kerusakan pada komputer karena malware, bisa juga menggunakan *Cuckoo Sandbox*. *Sandbox* merupakan cara untuk melakukan isolasi sebuah program/malware dari sistem komputer. Selain digunakan untuk melakukan analisa malware, *Sandbox* juga digunakan para developer untuk menguji sebuah kode.

Cuckoo dapat digunakan untuk melakukan analisa malware dan memberi report secara otomatis apa saja yang dilakukan malware terhadap komputer . *Malware* akan dijalankan dalam sebuah *sandbox* yang menggunakan OS Windows. *Cuckoo* dapat melakukan analisa terhadap berbagai macam sampel malware. Pada penelitian *cuckoo sandbox* yang digunakan secara *online* dengan langsung memasukkan file KMS-R@1n.exe. Pada Gambar 1. merupakan

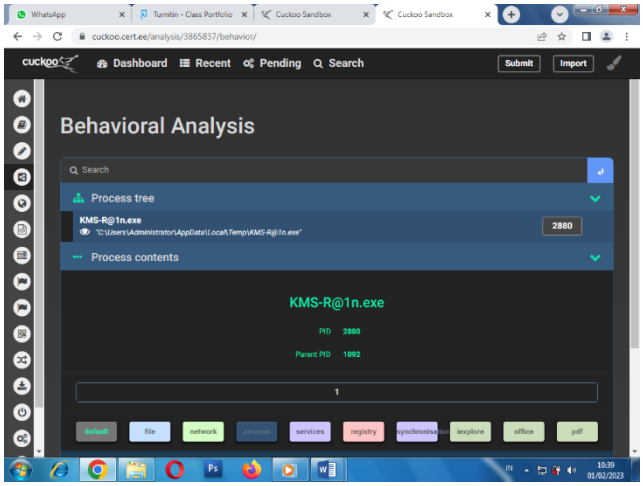
Informasi malware yang digunakan untuk dianalisa.



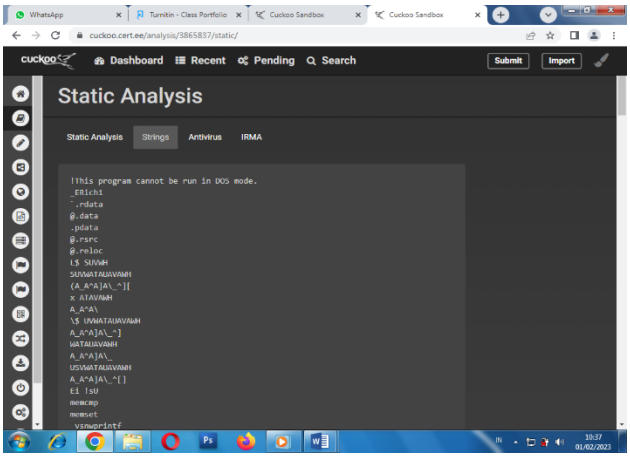
Gambar 2. Informasi File *Malware*



Gambar 3. Halaman Utama *Cuckoo Sandbox*



Gambar 4. Proses Upload Sampel *Malware* ke *Cuckoo Sandbox*



Gambar 5. *Strings* dari sampel *malware*

Analisa yang digunakan dalam penilitian ini adalah analisa dinamis dengan menjalankan malware pada komputer serta mempelajari perilaku malware tersebut

pada komputer. Ketika menginfeksi komputer, *malware* biasanya melakukan modifikasi pada sistem, misalnya merubah registry, menghapus file, menjalankan service tertentu dan lain-lain. Ketika melakukan analisa malware selalu ada risiko pada komputer terinfeksi *malware* (Ghaffari et al., 2017). Berdasarkan hasil Analisa dengan menggunakan tools cuckoo sandbox pada tahap pengujian telah memberikan informasi mengenai *malware* yang sedang berjalan dalam lingkungan yang terisolasi.

Cuckoo sandbox yang digunakan merupakan aplikasi yang tersedia secara *online* dan file sampel *malware* yang digunakan adalah KMS-R@1n.exe. Setelah file di analsis menunjukkan informasi mengenai file tersebut dan saat proses upload sampel malware muncul string dari sampel. Hal ini menunjukkan bahwa *Cuckoo sandbox* dapat melakukan analisa *malware* secara otomatis dan menampilkan informasi-informasi yang dilakukan oleh sampel *malware*.

Summary Result

Berikut adalah beberapa signatures summary yang menunjukkan perilaku sampel A-W ketika dijalankan pada ruang lingkup mesin virtual. Informasi yang didapat dari file KMS-R@1n.exe File ini sangat mencurigakan dengan score 10 dari 10, pada table di atas terdapat summary pada file KMS-R@1n.exe.

Tabel 1. Informasi File *Malware*

Engine	Sampel	Mesin Virtual	Keterangan
Cuckoo Sandbox	Kms-R@1n.exe	Windows 7	Aplikasi sebagai Alat peretas Mengancam Resiko Keamanan (Privasi) Pada komputer sistem operasi windows 32 dan 64 bit. Telah diidentifikasikan sebagai apk berbahaya dari 30 antivirus pada antivirus total

Tabel 2. *Summary Signature*

Mesin	Sampel	Mesin Virtual	Kategori Malscore	Difinisi Virus Total Rasio	Jenis Malware
Cuckoo Sandbox	Kms-R@1n.exe	Windows 7	Malicious	100% terdeteksi sebagai malware	Trojan

Berdasarkan hasil yang telah didapat, menunjukkan bahwa *sampel malware* yang dianalisis memberikan *signature* bahwa sampel tersebut sebagai alat peretas, mengancam keamanan pada system operasi windows 32 bit dan 64 bit dan juga telah teridentifikasi sebagai file berbahaya dari 30 antivirus pada antivirus total. Sampel yang di analisis pada *Cuckoo sandbox* terdeteksi sebagai *malware* jenis trojan.

Trojan atau *Trojan Horse* merupakan program *malicious* yang dimasukkan ke dalam sistem melalui sebuah program atau aktivitas yang legal (Ramadhani, 2018), seperti: melalui proses instalasi perangkat lunak aplikasi, melalui proses "*upgrading*" versi *software* yang baru, melalui proses "*download*" program - program *freeware*, melalui file - file multimedia (seperti gambar, lagu, dan video), dan lain sebagainya. Terdapat beberapa jenis trojan yaitu *remote access trojan, proxy trojan, FTP Trojan, keylogger, password sending trojan,* dan *software detection killer* (Manoppo et al., 2020).

KESIMPULAN

Dengan menggunkan metode dinamik kita dapat mempermudah dalam menganalisa malware karena dengan metode dinamik kita langsung menjalankan malware tersebut dilinkungan yang terisolasi , Hasil analisa *malware* menggunakan tool cuckoo sandbox yang didapatkan adalah informasi *malware*, karakteristik dari *malware, behaviour analysis, static analysis* dan tingkat *maliciousness malware*.

DAFTAR PUSTAKA

Alfalqi, K., Alghamdi, R., & Waqdan, M. (2015). Android platform malware analysis. *International Journal of Advanced Computer Science and Applications (IJACSA)*.

Cahyanto, T. A., Wahanggara, V., & Ramadana, D. (2017). Analisis dan deteksi malware menggunakan metode malware analisis dinamis dan malware analisis statis. *JUSTINDO (Jurnal Sistem Dan Teknologi Informasi Indonesia)*, *2*(1).

Ghaffari, F., Abadi, M., & Tajoddin, A. (2017). AMD-EC: anomaly-based android malware detection using ensemble classifiers. *2017 Iranian Conference on Electrical Engineering (ICEE)*, 2247–2252.

Ghufron, G. (2018). Revolusi Industri 4.0: Tantangan, Peluang, dan solusi bagi dunia pendidikan. *Seminar Nasional Dan Diskusi Panel Multidisiplin Hasil Penelitian Dan Pengabdian Kepada Masyarakat 2018*, *1*(1).

Ilman, Z. Y., MM, M., & Yesi, N. K. (2014). *Analisis Forensik Pada Platform Android*.

Indrajit, R. E. (2011). Pengantar konsep keamanan informasi di dunia siber. *APTIKOM. Jakarta*.

Kramer, S., & Bradfield, J. C. (2010). A general definition of malware. *Journal in Computer Virology*, *6*, 105–114.

Manoppo, V. A., Lumenta, A. S. M., & Karouw, S. D. S. (2020). Analisa Malware Menggunakan Metode Dynamic Analysis Pada Jaringan Universitas Sam Ratulangi. *Jurnal Teknik Elektro Dan Komputer*, *9*(3), 181–188.

Ramadhani, A. (2018). Keamanan Informasi. *Nusantara Journal of Information and Library Studies (N-JILS)*, *1*(1), 39–51.

Sibarani, M. C., di Marco, M., Rondinini, C., & Kark, S. (2019). Measuring the surrogacy potential of charismatic megafauna species across taxonomic, phylogenetic and functional diversity on a megadiverse island. *Journal of Applied Ecology*, *56*(5), 1220–1231.