TELEGRAMBOT: USING TELEGRAM TO CRAWLING MALWARE THREATS

Faulinda Ely Nastiti [1], Dedy Hariyadi [2], Fazlurrahman[3]
[1] *Fakultas Ilmu Komputer / Universitas Duta Bangsa Surakarta*
Jln. Bhayangkara no. 55, Surakarta, 57155 Indonesia
[2] *Fakultas Teknik dan Teknologi Informasi / Universitas Jenderal Achmad Yani Yogyakarta*
Jl. Siliwangi, Jl. Ring Road Bar., Daerah Istimewa Yogyakarta 55293 Indonesia
[3] *Komunitas NgeSec Yogyakarta*
[1]faulinda.en@gmail.com, [2]milisdad@gmail.com, [3]fazlurbima@gmail.com

Abstrak— **Ancaman serangan siber masih didominasi oleh malware. Beberapa penyedia telah menyediakan peta dan analisis serangan malware berbasis agen yang telah ditempatkan pada beberapa infrastruktur. Namun, ada pihak lain yang menyediakan data serangan Malware yang dapat diakses oleh publik, disebut Sumber OSINT. Penelitian ini bertujuan untuk membangun sebuah perangkat lunak berbasis mobile yang dapat dimanfaatkan untuk melakukan Crawling data Malware tanpa harus melakukan pencarian manual melalui web side. Peneliti memanfaatkan teknologi TelegramBot dan OIST Source untuk melacak data serangan Malware di Indonesia. Tidak hanya di Indonesia, seluruh negara di dunia telah menyadari pentingnya malakukan pengumpulana Data serangan Malware agar tidak membahayakan data pemerintah. Basis data serangan malware dapat digunakan untuk memprediksi dan memproteksi data penting agar terhindar dari cybercrime bahkan cyberterrorism.**

Keywords— **OSINT, Malware, Cyber Threats, Crawling, Telegram, Security, Intelligence**

I. PENDAHULUAN

Serangan malware dari tahun ke tahun berkembang sangat cepat, tercatat bahwa 40% gangguan siber dan perangkat teknologi di dunia bersumber dari serangan malware. Kini penyerangan siber dengan teknologi malware tidak hanya digunakan untuk merusak komputrer seseorang, namun merambat ke arah penyadapan data perorangan bahkan sampai dengan penyadaapan data negara. Politik merupakan salah satu pemicu adanya penyerangan Malware di suatu negara.

Menjelang pemilihan Presiden tahun 2019, keadaan Politik Indonesia di prediksi akan memanas. Pemilihan Presiden di Indonesia sudah menggunakan sistem elektronik. Oleh sebab itu pemerintah Indonesia harus mewaspadai pergerakan malware agar tidak mengganggu proses pemilihan umum Presiden secara elektronik. Lembaga negara yang bertugas mengamankan siber Indonesia Badan Siber dan Sandi Negara (BSSN).

Salah satu kerangka keamanan Siber yang bisa diadopsi adalah *Open Source Intelligence Base Cyber Threat Inspection Framework for Critical Infrastructures.* Kerangka ini terbagi menjadi empat tahapan, yaitu [1]:

1. Establishment of OSINT Plan, proses penyusunan rencana pencatatan terhadap berbagai ancaman siber.
2. Preparation of OSINT, melakukan proses pemeriksaan informasi penting dan memastikan indikator validasi informasi yang didapatkan.
3. Collecting Information from Open Source, mengumpulkan berbagai informasi dari berbagai sumber menggunakan tools pengumpul data OSINT dan memverifikasi data dari sumber-sumber tersebut.
4. Generating Security Intelligence, menganalisis data-data temuan yang selanjutnya disimpan di repositori.

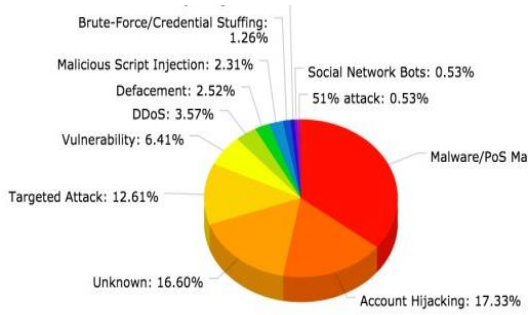
Honeynet Indonesia merupakan oragnisasi nirlaba yang melakukan kolaborasi penelitian dengan industri dan institusi pendidikan tinggi untuk memahami perilaku malware dan berkontribusi kepada komunitas keamanan informasi melalui penelitian [2]. Honeynet Indonesia (Honeynet-ID) bekerjasama dengan Badan Siber dan Sandi Negara (BSSN) membuat peta serangan malware siber yang dapat diakses melalui alamat *http://public.honeynet.id/*. Selain itu BSSN melalui ID-SIRTII/CC juga melakukan pemetaan serangan menggunakan Mata Garuda yang menggunakan metode Intrusion Detection System (IDS) dengan sensor yang terpasang di Network Access Provider (NAP) [3]. Baik Honeynet-ID maupun ID-SIRTII/CC menggunakan sensor atau agent untuk mencatat serangan siber.

Tujuan dari penelitian ini adalah mengusulkan mengembangkan perangkat lunak yang mampu mengumpulkan data ancaman malware dengan teknologi mobile. Proses pengambilan data dilakukan melalui perangkat mobile menggunakan teknologi Instant Messaging dengan memanfaatkan Telegram Robot atau disebut TelegramBot. TelegramBot akan mempermudah pengambilan data serangan malware

yang tersedia bebas di internet tanpa membuka aplikasi web browser untuk mendapatkan data.

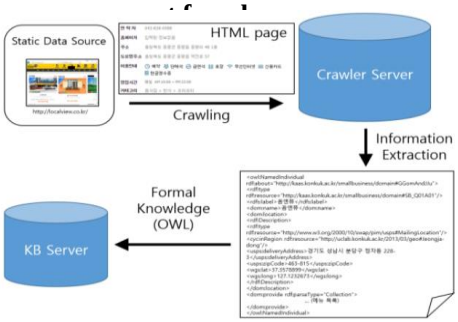
II. LANDASAN TEORI

Malware berasal dari kata malicious software yang dapat berarti sebuah perangkat lunak yang sengaja diciptakan untuk merusak sebuah sistem [4]. Berdasarkan survey yang telah dilakukan Paolo Passeri menunjukan serangan siber masih didominasi serangan Malware [5] lihat **Error! Reference source not found.**. Berdasarkan survey tersebut bisa disimpulakan bahwa serangan Malware merupakan ancaman terbesar dunia siber, sebesar 35.61%.



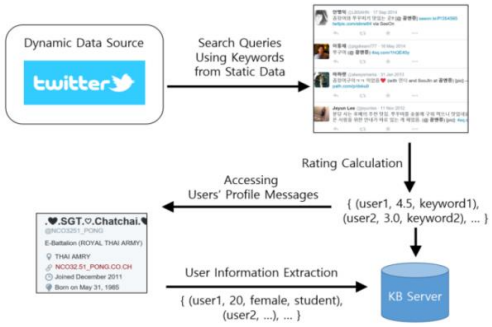
Gbr1. Persentase Jenis Serangan Siber Dunia

Menurut Kim dan Ha dari Konkuk University proses web crawling terbagi menjadi dua, yaitu Collecting Static Data dan Collecting Dynamic Data [6]. Collecting Static Data melakukan crawling pada situs web yang memiliki pola statik, selanjutnya mengekstraksi informasi menggunakan metode yang sesuai kaidah RDF [7] dan OWL[8], lihat **Error! Refe**



Gbr2. Collecting Static Data Process

Sedangkan Collecting Dynamic Data adalah proses pengambilan data pada situs web yang cenderung berubah dari waktu ke waktu, lihat **Error! Reference source not found.**.



Gbr3. Collecting Dynamic Data Process

Departemen Angkatan Darat Amerika Serikat menilai Open-source intelligence (OSINT) adalah disiplin intelijen yang berkaitan dengan kecerdasan yang dihasilkan dari informasi yang tersedia secara publik yang dikumpulkan, dieksploitasi, dan disebarluaskan pada waktu yang tepat kepada khalayak yang tepat untuk tujuan pengalamatan kebutuhan informasi dan intelijen khusus [9]. Dua istilah terkait penting adalah sumber terbuka dan informasi yang tersedia untuk umum:

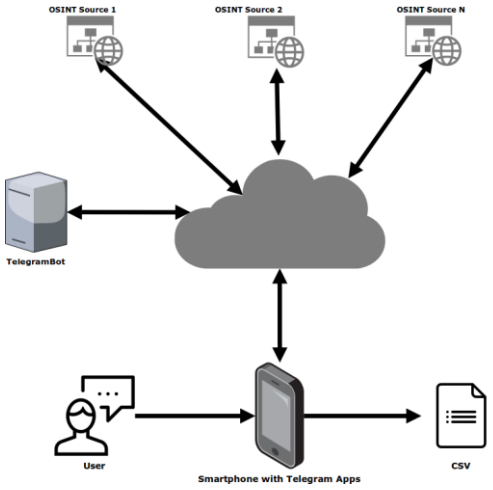
1. Open-source, informasi yang tersedia tanpa terlindungi hak privasi tetapi masih mengikuti aturan undang-undang yang berlaku.
2. Publicly available information, data yang tersedia disebarluaskan dengan tujuan untuk konsumsi publik.

III. METODE PENELITIAN

Penelitian ini menggunakan metode crawling Collecting Static Data karena data yang tersedia memiliki pola statis pada halaman HTML. Sumber data yang peneliti gunakan untuk di crawling adalah Situs *www.malc0de.com.* Web ini merupakan penyedia informasi yang menyimpan berkas Malware pada server di seluruh dunia. Informasi yang peneliti gunakan adalah serangan Malware yang berada di siber Indonesia.

Situs lengkap yang digunakan oleh peneliti adalah *http://www.malc0de.com/database/index.php?search=ID* yang selanjutnya disebut sebagai OSINT Source.

Arsitektur dari Pengeembangan Perangkat Lunak untuk meng-crawling data Malware bisa dilihat pada **Error! Reference source not found.**



Gbr4. arsitektur proses crawling malware

Proses crawling memerlukan sebuah perangkat berupa server yang terhubung ke internet dan mendukung bahasa pemrograman Python versi 2.x. Peneliti memanfaatkan TelegramBot menyesuaikan kaidah dari Telegram [10] dan memanfaatkan kode

yang tersedia di Github *(https://github.com/orangmiliter/malc0de).*

Sisi pengguna cukup menggunakan aplikasi Telegram yang terinstall pada smartphones. Pengguna melakukan instruksi crawling melalui Telegram dengan perintah yang telah ditentukan. Hasil crawling langsung diterima pengguna dalam bentuk berkas berformat Comma Separate Values (CSV). Berkas berformat CSV sebagai sumber data akan memudahkan dalam proses analisis [11].

IV. PEMBAHASAN

A. *Proses Crawling Malware*

Situs web Malc0de menjadi kategori OSINT Source selain menyampaikan informasi serangan Malware tetapi infromasi yang ditampilkan sudah sesuai dengan World Wide Web Consostium (W3C) [12]. Pada bagian view-source yang menampilkan kode HTML, **Error! Reference source not found.** memiliki struktur Tag Row (<tr>) yang didalamnya terdapat Tag Header (<th>) dan Tag Data (<td>) yang memudahkan untuk proses crawling.

Gbr. 1. View Source from Malc0de Site

B. *Proses Klasifikasi Data Crawling Malware*

Pada kode Python menggunakan module argparse untuk melakukan proses parser kode-kode HTML. Module argparse untuk memisahkan header dari Date, Domain, IP, dan Autonomous System Name. Hasil argparse menghasilkan output berupa berkas berformat CSV. Adapun kode Python yang menggunakan module argparse sebagai berikut:

```
i = 0
tempA,tempB = [],[]
for parse in listParse:
    i += 1
    if '<a href=' in parse:
        parse = re.findall(r">(.*?)</", parse, re.I | re.M)[0]
        tempA.append(parse)
        if i >= 7:
            writecsv.writerow([tempA[0], tempA[1], tempA[2], tempA[5]])
            i, tempA = 0, []
```

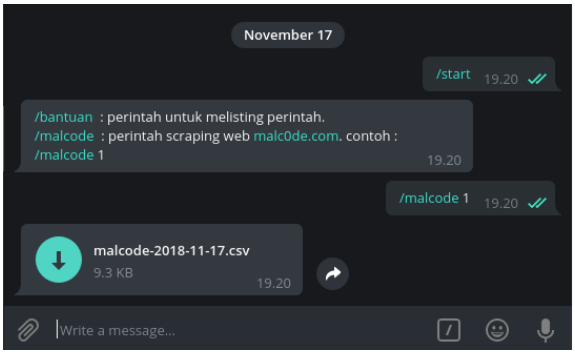
Untuk saat ini TelegramBot masih menyediakan OSINT Source satu situs web, yaitu Malc0de. Pihak Malc0de telah mengklasifikasi sumber penyebaran atau penyerangan Malware berdasarkan negara. Sehingga kode python untuk melakukan pengambilan alamat URL menggunakan kode berikut: requests.get('http://malc0de.com/database/index.php?& search=ID&page=%s'% keyword).text.encode('utf-8').

C. *Pemanfaatan TelegramBot*

TelegramBot mendukung penggunaan secara *multiuser*.Pengguna lain yang membutuhkan data malware hasil crawling dapat dimasukan dalam Chat Groups. Pengguna melakukan instruksi crawling ke mesin TelegramBot melalui Telegram diawali dengan perintah /start.

Perintah untuk melakukan proses crawling dengan perintah /malcode 1 yang artinya melakukan crawling situs web Malc0de halaman pertama. melakukan crawling halaman kedua dengan mengetik /malcode 2, dan seterusnya. Peneliti juga menyediakan petunjuk pengetikan untuk mempermudah penggunaan memahami perintah-perintah yang digunakan untuk meng-crawling data. Pengguna cukup mengetikan perintah /bantuan.

Error! Reference source not found. menunjukan contoh instruksi crawling sistus web Malc0de pada Telegram.



Gbr 2. Perintah Crawling pada Telegram

Hasil dari crawling langsung akan dikirimkan ke Chat Groups berupa berkas berformat CSV. TABLE . Menunjukkan sebagian informasi hasil crawling yang berupa Date, Domain, IP, dan Autonomous System Name.

TABLE I
CONTOH HASIL CRAWLING DARI MALC0DE

Date	Domain	IP	Autonomous System Name
2018-08-04	garduherbal.com/LOL123.exe	103.229.72.33	MWN-AS-ID PT Master Web Network, ID
2018-08-03	garduherbal.com/LOL123.exe	103.229.72.33	MWN-AS-ID PT Master Web Network, ID

Date	Domain	IP	Autonomous System Name
2018-08-02	garduherbal.com/LOL123.exe	103.229.72.33	MWN-AS-ID PT Master Web Network, ID
2018-08-01	garduherbal.com/LOL123.exe	103.229.72.33	MWN-AS-ID PT Master Web Network, ID
2018-07-31	garduherbal.com/LOL123.exe	103.229.72.33	MWN-AS-ID PT Master Web Network, ID
2018-07-30	garduherbal.com/LOL123.exe	103.229.72.33	MWN-AS-ID PT Master Web Network, ID
2018-07-29	garduherbal.com/LOL123.exe	103.229.72.33	MWN-AS-ID PT Master Web Network, ID
2018-07-28	garduherbal.com/LOL123.exe	103.229.72.33	MWN-AS-ID PT Master Web Network, ID
2018-07-27	garduherbal.com/LOL123.exe	103.229.72.33	MWN-AS-ID PT Master Web Network, ID
2018-07-25	garduherbal.com/LOL123.exe	103.229.72.33	MWN-AS-ID PT Master Web Network, ID
2018-07-07	abatii.web.id/ojay/Quotation.exe	202.52.146.120	GMEDIA-AS-ID Global Media Teknologi, PT, ID
2018-07-06	abatii.web.id/ojay/Quotation.exe	202.52.146.120	GMEDIA-AS-ID Global Media Teknologi, PT, ID

V. PENUTUP

Proses crawling pada penelitian ini masih terbatas pada satu sumber, yaitu Malc0de. Walaupun hanya satu sumber mempermudah pengguna yang berprofesi Cyber Threat Hunter untuk menganalisis ancaman serangan siber Malware. Diharapkan penelitian selanjutnya dapat ditambahkan berbagai OSINT Source lainnya untuk memperkaya hasil presentasi peta serangan siber berupa Malware. Selain itu TelegramBot ini belum dilengkapi data analysis terkait serangan siber Malware di Indonesia.

REFERENSI

[1] S. Lee and T. Shon, “Open Source Intelligence Base Cyber Threat Inspection Framework for Critical Infrastructures,” FTC 2016 - Proc. Futur. Technol. Conf., no. December, pp. 1030–1033, 2017.

[2] Indonesia Honeynet Project, “Indonesia Honeynet Project Conference.” [Online]. Available: http://ihpcon.id/. [Accessed: 18-Aug-2018].

[3] F. A. Saputra, I. Winarno, and M. B. Muliawan, “Implementing Network Situational Awareness in Matagaruda,” in 2015 International Electronics Symposium (IES), 2015, pp. 268–273.

[4] A. H. Muhammad, “Metode Klasifikasi dan Analisis Karakteristik Malware Menggunakan Konsep Ontologi,” Universitas Islam Indonesia, 2017.

[5] Paolo Passeri, “January – September 2018 Cyber Attack Statistics,” 2018. [Online]. Available: https://www.hackmageddon.com/2018/10/15/january-september-2018-cyber-attack-statistics/. [Accessed: 17-Oct-2018].

[6] S. M. Kim and Y. G. Ha, “Automated Discovery of Small Business Domain Knowledge using Web Crawling and Data Mining,” 2016 Int. Conf. Big Data Smart Comput. BigComp 2016, pp. 481–484, 2016.

[7] World Wide Web Consortium, “RDF - Semantic Web Standards.” [Online]. Available: https://www.w3.org/RDF/. [Accessed: 27-Oct-2018].

[8] World Wide Web Consortium, “OWL - Semantic Web Standards.” [Online]. Available: https://www.w3.org/OWL/. [Accessed: 27-Oct-2018].

[9] U.S.A. Department of the Army, “Open-Source Intelligence ATP 2-22.9,” vol. 2–22.9, no. July, p. 91, 2012.

[10] Telegram, “Bots: An introduction for developers.” [Online]. Available: https://core.telegram.org/bots. [Accessed: 30-Oct-2018].