Ransomware dan Upaya Pencegahannya dalam Kehidupan Berdigital

Andrean Dwika P.[1*], Sholeh Abdul I. T.[2], Juantino Brata A.[3]

[1]*S1 Teknik Informatika*
Universitas Duta Bangsa Surakarta
andredwika734@gmail.com

[2]*S1 Teknik Informatika*
Universitas Duta Bangsa Surakarta
sairfant@gmail.com

[3] *S1 Teknik Informatika*
Universitas Duta Bangsa Surakarta
juantinobr.as@gmail.com

Abstrak— **Di era digital saat ini, hampir semua aspek kehidupan manusia telah terhubung dengan teknologi informasi, membuka peluang bagi berbagai ancaman baru, termasuk ransomware. Ransomware adalah jenis malware yang mengenkripsi data korban dan meminta tebusan untuk memulihkannya, menyebabkan kerugian finansial dan operasional yang signifikan. Tujuan dari penelitian ini adalah memberikan edukasi terkait ransomware, penyebab serangan, dan upaya pencegahannya. Metode penelitian meliputi identifikasi dan seleksi sumber data, evaluasi literatur, serta analisis dan interpretasi data. Hasil penelitian menunjukkan peningkatan signifikan dalam serangan ransomware dari tahun ke tahun, dengan evolusi teknik dan metode distribusi yang semakin canggih. Pencegahan yang efektif meliputi backup data secara teratur, pembaruan software dan sistem operasi, penggunaan antivirus, dan kewaspadaan terhadap link serta email mencurigakan. Dengan pemahaman yang lebih baik tentang ransomware, diharapkan individu, perusahaan, dan pemerintah dapat lebih waspada dan terlindungi dari ancaman ini.**
Kata kunci— Ransomware, Keamanan Informasi, Pencegahan, Informatika.

Abstract— **In digital era, almost all aspects of human life have been connected to information technology, opening up opportunities for various new threats, including ransomware. Ransomware is a type of malware that encrypts victims' data and demands a ransom to restore it, causing significant financial and operational losses. The purpose of this research is to educate readers about ransomware, the causes of attacks, and prevention efforts. The research methods include identifying and selecting data sources, evaluating literature, and analyzing and interpreting data. The results show a significant increase in ransomware attacks year after year, with the evolution of techniques and distribution methods becoming more sophisticated. Effective prevention includes regular data backups, software and operating system updates, antivirus usage, and vigilance against suspicious links and emails. With a better understanding of ransomware, individuals, companies, and governments are expected to be more aware and protected from this threat.**
Keywords— Ransomware, Information Security, Prevention, Informatics.

I. PENDAHULUAN

Di era digital saat ini, hampir semua aspek kehidupan manusia telah terhubung dengan teknologi informasi. Aktivitas sehari-hari seperti berbelanja, bekerja, dan bahkan urusan pemerintahan kini lebih efisien berkat digitalisasi. Meski kemajuan teknologi ini memberikan banyak kemudahan, ia juga membuka peluang bagi berbagai ancaman baru. Teknologi digital tidak hanya menawarkan manfaat tetapi juga menciptakan tantangan keamanan yang kompleks dan membutuhkan perhatian khusus.

Salah satu ancaman terbesar yang muncul dari perkembangan teknologi adalah kejahatan siber atau cybercrime. Kejahatan ini mencakup berbagai tindakan ilegal yang dilakukan melalui jaringan komputer dan internet. Ancaman dari cybercrime sangat beragam, mulai dari pencurian identitas, pelanggaran privasi, hingga sabotase sistem informasi kritis. Dampak dari kejahatan siber dapat sangat merugikan, baik dari segi finansial, reputasi, maupun keamanan nasional. Oleh karena itu, perlindungan terhadap ancaman siber menjadi prioritas utama bagi individu, perusahaan, dan pemerintah.

Ransomware adalah salah satu bentuk kejahatan siber yang paling mengkhawatirkan. Malware jenis ini bekerja dengan mengenkripsi data korban dan meminta tebusan agar data tersebut bisa diakses kembali. Serangan ransomware tidak hanya menyebabkan kerugian finansial yang signifikan, tetapi juga dapat mengganggu operasi secara besar-besaran. Dalam beberapa tahun terakhir, serangan ransomware telah meningkat drastis, menjadikannya salah satu ancaman paling serius di dunia digital[1].

Oleh karena itu tujuan dari riset ini adalah memberikan edukasi terkait ransomware kepada pembaca untuk memahami apa itu ransomware, serta apa saja penyebab yang dapat memicu terjadinya serangan dari ransomware, serta upaya pencegahannya agar para pembaca dapat terhindar dari serangan ransomware. Dengan adanya riset ini

diharapkan semakin banyak orang yang waspada terhadap ancaman cybercrime di era digital ini.

II. METODOLOGI PENELITIAN

Penelitian ini menggunakan tahapan sebagai berikut.

1. Identifikasi dan seleksi sumber data
   Mengidentifikasi dan memilih artikel serta jurnal yang relevan sesuai dengan topik penelitian kami.
2. Evaluasi literatur
   Mengevaluasi kualitas dan relevansi artikel dan jurnal yang telah diseleksi untuk mendapatkan pemahaman yang komprehensif.
3. Analisis dan interpretasi data
   Menganalisis data yang telah dikumpulkan untuk menghasilkan kesimpulan yang berdasarkan pada kenyataan yang ditemukan dalam literatur.

III. HASIL DAN PEMBAHASAN

A. Ransomware

Ransomware adalah jenis malware yang menggunakan teknik keamanan seperti kriptografi untuk mengunci file dan sumber daya pengguna, kemudian meminta pembayaran dalam bentuk mata uang kripto sebagai tebusan. Tidak ada batasan siapa yang bisa menjadi target ransomware, karena penyebarannya dapat terjadi melalui internet. Mirip dengan malware tradisional, ransomware dapat masuk ke dalam sistem melalui rekayasa sosial, iklan berbahaya, email spam, eksploitasi kerentanan, unduhan drive-by, port terbuka, atau memanfaatkan back-door. Namun, berbeda dengan malware tradisional, efek ransomware tidak bisa diperbaiki hanya dengan penghapusan, dan mengurangi dampaknya sangat sulit tanpa bantuan penciptanya. Serangan seperti ini memiliki dampak finansial langsung, didorong oleh teknologi enkripsi dan mata uang siber. Karena itu, ransomware telah menjadi bisnis yang menguntungkan dan semakin populer di kalangan penyerang[1][6].

B. Evolusi Ransomware

Berikut ini adalah garis timeline yang dibuat dengan tanggal perkiraan berdasarkan informasi yang diketahui tentang ransomware. Karena sifat ilegal dari ransomware, para penulis mengakui bahwa mungkin ada beberapa detail yang hilang. Namun, timeline ini tetap menunjukkan evolusi umum dan pertumbuhan ransomware dari waktu ke waktu. Penting juga untuk dicatat bahwa sumber-sumber tidak konsisten dalam penggunaan nama untuk berbagai versi ransomware, meskipun cenderung mirip.

Pada tahun 1989, ransomware pertama, yang dikenal sebagai AIDS Trojan atau PC Cyborg, diciptakan oleh Joseph L. Popp, seorang ahli biologi evolusioner lulusan Harvard. Ransomware ini disebarkan melalui disket pada konferensi AIDS Internasional yang diselenggarakan oleh Organisasi Kesehatan Dunia. Menggunakan kriptografi simetris sederhana untuk mengenkripsi nama file, alat untuk mendekripsinya segera ditemukan [1].

Pada tahun 2005, Trojan. Gpcoder, ransomware modern pertama yang juga dikenal sebagai GP Code dan GPCoder, dirilis pada bulan Mei. Awalnya, malware ini menggunakan teknik enkripsi simetris khusus yang lemah dan mudah dipecahkan. Para pembuat terus menyempurnakannya (Savage, Coogan, & Lau, 2015). Trojan.Gpcoder menyebar melalui lampiran email spam yang menyamar sebagai lamaran pekerjaan [1].

Ransomware pada tahap awal sebagian besar dikembangkan oleh penjahat terorganisir di Rusia. Target utamanya adalah korban di Rusia serta negara-negara tetangga seperti Belarus, Ukraina, dan Kazakhstan (Cawley, 2016).

Pada awal 2006, ransomware mulai populer, dan lebih banyak penyerang mulai mencobanya. Trojan.Cryzip muncul pada bulan Maret 2006, dengan cara kerja menyalin file data ke dalam file arsip yang dilindungi kata sandi dan menghapus file aslinya. Karena kata sandi disertakan dalam kode malware, pemulihan file menjadi cukup mudah.

Pada tahun 2006, Trojan.Archiveus juga muncul. Sama seperti Trojan.Cryzip, malware ini mengunci file, namun alih-alih meminta tebusan uang, korban diminta untuk membeli obat dari apotek online tertentu dan mengirimkan ID pesanan untuk mendapatkan kata sandi (Savage, Coogan, & Lau, 2015).

Pada tahun 2007, ransomware locker mulai bermunculan. Pada versi awal menargetkan Rusia dan menampilkan gambar pornografi di komputer, kemudian meminta pembayaran melalui pesan SMS atau menelepon nomor telepon premium untuk

menghapusnya. Serangan ini dengan cepat menyebar ke Eropa dan Amerika Serikat (Zetter, 2015).

Pada tahun 2008, muncul varian dari Trojan.Gpcoder yang dikenal sebagai GPcode.AK. Ransomware ini menggunakan kunci RSA 1024-bit dan meninggalkan file teks dengan instruksi di setiap subdirektori yang dienkripsi. Pembayaran yang diminta berkisar antara $100 hingga $200 dalam bentuk e-gold atau Liberty Reserve (Tromer, 2008).

Pada pertengahan tahun 2011, terjadi wabah ransomware besar-besaran pertama kali, terutama karena munculnya layanan pembayaran anonim. Pada kuartal pertama, ada sekitar 30.000 sampel ransomware baru, diikuti dengan tambahan 30.000 sampel pada kuartal kedua. Jumlah ini meningkat menjadi 60.000 sampel baru pada kuartal ketiga (Sjouwerman, 2015b).

Pada tahun 2012, toolkit bernama Citadel dirilis dengan harga sekitar $3.000, memudahkan pembuatan dan penyebaran ransomware (Segura, 2016). Toolkit lain, Lyposit, juga diperkenalkan pada tahun yang sama, dirancang untuk membuat ransomware yang berpura-pura berasal dari lembaga penegak hukum tertentu sesuai dengan pengaturan regional komputer ("Lyposit Malware | win32/Lyposit.A," n.d.). Salah satu ransomware yang dibuat dengan Lyposit dikenal sebagai Reveton, menampilkan pesan pop-up yang menyatakan bahwa komputer terlibat dalam aktivitas ilegal seperti pornografi anak atau mengunduh materi berhak cipta, dan dikunci oleh FBI atau Departemen Kehakiman (Sjouwerman, 2015b; Savage, 2015). Trojan.Randsom.C adalah ransomware awal lainnya yang meniru pesan dari Windows Security Center dan meminta pengguna menelepon nomor telepon premium untuk mengaktifkan kembali lisensi Windows mereka (Savage, Coogan, & Lau, 2015).

Karena kekurangan dalam ransomware locker dan skema pemerasan lainnya, pada tahun 2013 terjadi peralihan kembali ke ransomware jenis crypto. Serangan biasanya meminta tebusan sekitar $300, dan menjadi lebih canggih (Savage, Coogan, & Lau, 2015).

Pada tahun 2013, ransomware terkenal bernama CryptoLocker dirilis pada bulan Agustus oleh peretas yang dikenal sebagai Slavik. Ransomware ini menggunakan kunci kriptografi publik dan privat untuk mengenkripsi dan kemudian mendekripsi file korban. Awalnya, ransomware ini didistribusikan melalui botnet Trojan perbankan Gameover ZeuS, kemudian melalui email yang tampak berasal dari UPS atau FedEx (Zetter, 2015). Versi asli CryptoLocker mengenkripsi sekitar 67 jenis file, termasuk semua file data Microsoft Office (Cannell, 2016).

CryptoLocker memberi korban waktu tiga hari untuk membayar tebusan, yang berkisar sekitar dua Bitcoin, atau $100 pada saat itu. Metode pembayaran lain termasuk CashU, Ukash, Paysafecard, dan MoneyPak. Pada beberapa versi, jika batas waktu tiga hari tidak terpenuhi, korban dapat membayar tebusan yang jauh lebih tinggi untuk mendapatkan kembali file mereka. Jumlah tebusan ini bervariasi tergantung pada versinya [1].

Pada bulan November, nilai dua Bitcoin meningkat menjadi sekitar $460, dan melewati batas waktu awal menaikkan harga menjadi sepuluh Bitcoin. Pada bulan Desember, sebanyak 250.000 mesin terinfeksi, dan 41.928 Bitcoin tebusan telah dibayarkan [1]. Pada bulan Desember, muncul ransomware tiruan bernama Locker yang meminta tebusan sebesar $150, yang dibayar melalui Perfect Money atau nomor Kartu Virtual QIWI Visa. Kemudian, CryptoLocker 2.0 dirilis, ditulis dalam bahasa yang berbeda sehingga kemungkinan besar dirilis oleh penyerang yang berbeda (Sjouwerman, 2015b). Symantec memperkirakan jumlah serangan meningkat dari 100.000 pada bulan Januari menjadi 600.000 pada bulan Desember, dan memperkirakan tiga persen dari pengguna yang terinfeksi membayar tebusan (Rosenberg, 2015).

Dari September 2013 hingga Mei 2014, lebih dari 500.000 korban diperkirakan terinfeksi oleh CryptoLocker. Sekitar 1,3 persen dari mereka membayar tebusan (Cannell, 2016). Pada bulan Juni, Operasi Tovar, sebuah koalisi dari lembaga penegak hukum, vendor keamanan, dan akademisi, berhasil menutup server distribusi CryptoLocker. FireEye dan Fox-IT menemukan basis data kunci dekripsi untuk semua korban CryptoLocker dan merilis layanan yang memungkinkan semua korban mendekripsi file mereka secara gratis (Cawley, 2016).

Pada bulan Februari, CryptoDefense dirilis. Meskipun relatif lemah, ransomware ini berhasil

menghasilkan $34.000 dalam bulan pertamanya. Versi yang lebih baik, CryptoWall, dirilis pada bulan April, menggunakan kerentanan Java dan disebarkan melalui iklan berbahaya. Versi ini menghasilkan lebih dari $1.000.000 dalam bentuk tebusan (Sjouwerman, 2015b).

Pada akhir 2015, FBI memperkirakan bahwa korban telah membayar tebusan sebesar $27 juta kepada para penyerang di balik CryptoLocker (Cannell, 2016). CryptoWall menjadi versi ransomware terkemuka, melampaui CryptoLocker (Sjouwerman, 2015b).

Menurut studi Kaspersky, serangan ransomware meningkat sebesar 17,7 persen pada 2014-2015, namun serangan crypto ransomware melonjak hingga 448 persen (Townsend, 2016). Pada bulan Mei, layanan ransomware-as-a-service mulai muncul, memungkinkan penyerang membuat ransomware secara gratis melalui situs web TOR. Situs ini mengelola pembayaran dan mengambil 20 persen dari tebusan (Sjouwerman, 2015b). Pada bulan September, LockerPin dirilis, yang menginfeksi sistem Android dan mengubah PIN, meminta tebusan sebesar $500. Pada bulan Oktober, laporan dari Cyber Threat Alliance melaporkan total kerusakan ransomware sebesar $325 juta (Sjouwerman, 2015b). Pada bulan November, Dr.Web, sebuah perusahaan keamanan komputer Rusia, menemukan Linus.Encoder.1, ransomware yang menargetkan sistem Linux dan mengenkripsi file data serta file yang terkait dengan aplikasi web (Cawley, 2016). Pada bulan yang sama, iterasi keempat dari CryptoWall muncul, dengan protokol yang dimodifikasi untuk menghindari deteksi dan kemampuan mengubah nama file saat mengenkripsi, sehingga lebih sulit untuk mengenali file yang dienkripsi (Pauli, 2015).

Pada Januari 2016, ditemukan layanan ransomware-as-a-service berbasis JavaScript, memungkinkan serangan multi-platform termasuk Linux dan MacOS X. Pada Februari, ribuan situs WordPress, platform blogging populer, terinfeksi ransomware. Pada April, muncul ransomware Petya yang membuat seluruh hard disk tidak dapat diakses hingga tebusan dibayar (Fitzpatrick & Griffin, 2016). Petya menimpa master boot record (MBR) komputer yang terinfeksi, sehingga sistem operasi tidak bisa merekonstruksi file yang tidak terenkripsi (Constantin, 2016). Apple harus merilis pembaruan untuk memblokir ransomware KeRanger, yang diyakini sebagai serangan ransomware pertama yang menargetkan komputer Apple. KeRanger membutuhkan waktu tiga hari untuk aktif setelah terinstal dan dirancang untuk mengenkripsi lebih dari 300 jenis file (Kirk, 2016a).

Pada Februari, ditemukan malware Xbot yang menargetkan perangkat Android di Australia dan Rusia. Selain mengenkripsi file, Xbot juga mencoba mencuri informasi perbankan online (Kirk, 2016b). Pada Juli, ransomware Locky memperkenalkan mekanisme failsafe yang memungkinkan enkripsi file meskipun ransomware tidak dapat meminta kunci enkripsi unik dari server penjahat karena komputer target sedang offline atau memblokir komunikasi (Constantin, 2016c).

FBI memperkirakan bahwa ransomware menghasilkan $209 juta dalam tiga bulan pertama tahun 2016 dan diprediksi akan menjadi kejahatan bernilai satu miliar dolar pada tahun ini (Fitzpatrick & Griffin, 2016). Pada kuartal pertama, McAfee Labs mencatat 1,2 juta serangan ransomware, meningkat 24 persen dari kuartal keempat tahun 2015 (McAfee Labs Threats Report, 2016). Tiga versi ransomware utama yang aktif saat ini adalah CryptoWall, CTB-Locker, dan TorrentLocker. CryptoWall adalah versi yang lebih baik dari CryptoDefense, mengenkripsi file di komputer yang terinfeksi serta penyimpanan eksternal atau drive bersama yang terhubung ke target. CTB-Locker, singkatan dari curve-Tor-Bitcoin, dan CryptoWall keduanya memiliki program afiliasi penjualan. TorrentLocker mengumpulkan alamat email saat menginfeksi komputer untuk mengirim spam ke pengguna lain [2][7][8].

C. Beberapa Kasus Ransomware

a. Pada tahun 2017, serangan ransomware WannaCry menyerang banyak organisasi di seluruh dunia. Ransomware ini memanfaatkan kerentanan dalam sistem operasi Windows yang belum diperbarui, menyebar dengan cepat melalui jaringan. Serangan ini mengenkripsi data dan meminta pembayaran tebusan dalam bentuk Bitcoin.
b. Pada tahun 2017, serangan ransomware NotPetya menyasar perusahaan-perusahaan

besar di seluruh dunia, termasuk Ukraina, tempat serangan ini bermula. NotPetya menggunakan metode yang mirip dengan WannaCry, yaitu memanfaatkan kerentanan dalam sistem operasi Windows. Namun, NotPetya lebih bersifat destruktif daripada sekadar pemerasan, karena tidak memungkinkan dekripsi data meskipun tebusan telah dibayar.

c. GandCrab adalah salah satu jenis ransomware yang aktif antara tahun 2018 dan 2019. Ransomware ini menyebar melalui kampanye email spam dan exploit kit. GandCrab mengenkripsi data korban dan meminta tebusan dalam bentuk mata uang kripto. Meskipun operasinya dihentikan setelah para peneliti keamanan berhasil memecahkan algoritma enkripsinya, ransomware ini tetap menyebabkan kerugian finansial yang signifikan[3].

D. Pencegahan Ransomware

Setelah mengetahui seberapa bahayanya ransomware. Ada beberapa langkah yang dapat dilakukan untuk mencegah agar kita tidak terkena dampak dari ransomware, yang diantaranya :

a. Backup data secara teratur
   Lakukan backup beberapa data dan file penting kedalam cloud dan beberapa penyimpanan lain untuk menghindari jika semisal dekstop terkena ransomware kita tetap dapat mengakses data penting tersebut.
b. Update software dan operating system secara berkala
   System operasi dan software terbaru biasanya memiliki beberapa perbaikan terhadap bug dan peningkatan keamanan dari beberapa serangan ransomware
c. Menggunakan antivirus
   Antivirus berfungsi mendeteksi aplikasi dan file yang kita dapat dari internet yang dimana dapat berisi ancaman ransomware.
d. Mewaspadai link dan email mencurigakan
   User jangan sembarangan membuka link dan email yang dikirim oleh anonim yang biasanya bersifat menjebak agar user mendownload sebuah file yang dimana terdapat ransomware yang mengancam[9][10].

D. Menangani Dekstop Yang Terkena Ransomware

Ransomware tidak menghapus data, tetapi mengenkripsi data tersebut sehingga tidak dapat diakses tanpa membayar tebusan. Meskipun infeksi ransomware dihapus, data tetap terenkripsi (Bradley, 2015). Beberapa versi ransomware menggunakan enkripsi yang sangat kuat sehingga tidak memungkinkan pemulihan tanpa membayar tebusan, sementara versi lain memiliki celah keamanan yang memungkinkan dekripsi tanpa pembayaran. Layar peringatan ransomware biasanya menampilkan nama ransomware, yang dapat digunakan sebagai titik awal untuk mencari metode dekripsi.

AVG yang merupakan perusahaan antivirus, menyarankan beberapa langkah spesifik untuk menangani infeksi ransomware, yang diantaranya:

a) Melakukan pemindaian menyeluruh pada desktop yang terinfeksi untuk mengidentifikasi jenis ransomware yang menyerang
b) Menyalin file-file yang terinfeksi ke USB Drive untuk mencoba dekripsi di komputer yang tidak terinfeksi.
c) Menggunakan alat dekripsi yang tersedia, seperti yang disediakan oleh AVG untuk beberapa jenis ransomware seperti Apocalypse, BadBlock, Crypt888, Legion, SZFLocker, dan TeslaCrypt. (Buckingham, 2016).

Baik file-file dipulihkan dengan alat dekripsi, dari cadangan, atau setelah membayar tebusan, penting untuk menghapus sepenuhnya ransomware dari komputer yang terinfeksi. Para ahli merekomendasikan menyalin file-data dari komputer, memformat ulang hard drive, dan menginstal ulang sistem operasi dan file-file dari awal untuk memastikan penghapusan ransomware secara total (Rosenberg, 2015). Pendekatan ini membantu mengurangi risiko dari ancaman ransomware yang mungkin masih ada.

IV. KESIMPULAN

Penelitian ini menyoroti bahaya yang ditimbulkan oleh ransomware di era digital, dengan fokus pada peningkatan frekuensi dan kompleksitas serangan dari waktu ke waktu. Melalui analisis literatur dan studi kasus, ditemukan bahwa ransomware telah berevolusi menjadi ancaman siber yang sangat merusak, mengakibatkan kerugian finansial dan

gangguan operasional yang luas. Upaya pencegahan yang disarankan meliputi backup data secara berkala, pembaruan sistem secara rutin, penggunaan perangkat lunak keamanan, dan edukasi pengguna mengenai potensi ancaman dari email dan tautan mencurigakan. Dengan menerapkan langkah-langkah ini, diharapkan risiko terkena serangan ransomware dapat diminimalkan. Pentingnya kesadaran dan tindakan proaktif dalam menghadapi ancaman siber ini tidak dapat diremehkan, terutama dalam melindungi data dan sistem informasi yang kritis.

REFERENSI

[1] R. Richardson and M. M. North, "Ransomware : Evolution , Mitigation and Prevention," *Auth. Adm. Digit. State Univ.*, vol. 13, no. 1, pp. 10–21, 2017, [Online]. Available: https://digitalcommons.kennesaw.edu/facpubs Recommended

[2] R. Zetter, "Migration and forced migration," *Step by Step UN Interag. Proj. Newsl.*, vol. First Quar, no. 10, pp. 1–17, 2003.

[3] A. S. Mubarak, M. N. Insirat, and M. N. Lutfiya, "Ransomware: Evolution, Classification, Attack Phase, Detection and Prevention," *Semin. Nas. Tek. Elektro, Sist. Informasi, dan Tek. Inform.*, pp. 1–6, 2024, doi: 10.31284/p.snestik.2024.5588.

[4] B. Hartono, "Ransomware: Memahami Ancaman Keamanan Digital," *Bincang Sains dan Teknol.*, vol. 2, no. 02, pp. 55–62, 2023, doi: 10.56741/bst.v2i02.353.

[5] H. Alshaikh, N. Ramadan, and H. A. Hefny, "Ransomware Prevention and Mitigation Techniques," *Int. J. Comput. Appl.*, vol. 177, no. 40, 2020, doi: 10.5120/ijca2020919899.

[6] Anggrahito, R. Ibrahim, and J. S. Pramudito, "Metode Cepat Identifikasi Dan Mitigasi Malware Ransomware Ketika Terjadi Serangan Siber Ramadhan Ibrahim," *Conf. Inf. Technol. Electr. Eng.*, 2020.