SNESTIK

Seminar Nasional Teknik Elektro, Sistem Informasi, dan Teknik Informatika

https://ejurnal.itats.ac.id/snestik dan https://snestik.itats.ac.id

Informasi Pelaksanaan :
SNESTIK IV - Surabaya, 27 April 2024
Ruang Seminar Gedung A, Kampus Institut Teknologi Adhi Tama Surabaya

Informasi Artikel:
DOI : 10.31284/p.snestik.2024.5588

Prosiding ISSN 2775-5126

Fakultas Teknik Elektro dan Teknologi Informasi-Institut Teknologi Adhi Tama Surabaya
Gedung A-ITATS, Jl. Arief Rachman Hakim 100 Surabaya 60117 Telp. (031) 5945043
Email : snestik@itats.ac.id

Ransomware: Evolution, Classification, Attack Phase, Detection and Prevention

Ahmad Sainuri Mubarak[1], Mutahira Nur Insirat[2], Muhajira Nurul Lutfiya[3]

SMK Negeri 4 Gowa[1], Universitas Muhammadiyah Makassar[2], Universitas Negeri Makassar[3]

e-mail: ahmadsainurimubarak@gmail.com

ABSTRACT

The modern cybercrime, namely ransomware, has grown exponentially over the past few years. Ransomware is a type of malware that is the result of sophisticated efforts to infiltrate modern computer systems. Most of these threats are aimed at directly or indirectly making money from victims by demanding a ransom in exchange for a description key. Governments and large corporations are investing heavily to combat cyber threats to their critical infrastructure. Ransomware first appeared in 1980, at that time one had to pay by mail. Ransomware is considered to be malware that has spread widely since 1989 and has caused global financial losses for both individuals and large organizations. Every year losses due to ransomware continue to increase. Therefore, data protection from ransomware is very necessary. Currently, ransomware originators request payment via bitcoin or cryptocurrency. This research provides an overview of ransomware, its evolution, classification, attack phases, detection, prevention, description of research limitations, and finally provides conclusions.

Keywords: *Ransomware; evolution; classification; attack phases; detection; prevention*

ABSTRAK

Kejahatan dunia maya modern yakni ransomware telah tumbuh secara eksponensial selama beberapa tahun terakhir. Ransomware adalah salah satu jenis malware yang merupakan hasil upaya canggih untuk menyusupi sistem komputer modern. Sebagian besar ancaman ini ditujukan untuk secara langsung atau tidak langsung menghasilkan uang dari para korban dengan meminta uang tebusan sebagai imbalan atas kunci deskripsi. Pemerintah dan perusahaan besar berinvestasi besar-besaran untuk memerangi ancaman siber terhadap infrastruktur penting mereka. Ransomware pertama kali muncul pada tahun 1980, pada saat itu seseorang harus

membayar melalui surat. Ransomware dianggap sebagai malware yang tersebar lyas sejak tahun 1989 dan telah menyebabkan kerugian finansial global baik bagi individu maupun organisasi besar. Setiap tahun kerugian akibat ransomware terus meningkat. Oleh karena itu, perlindungan data dari ransomware sangat diperlukan. Saat ini, pencetus ransomware meminta pembayaran melalui bitcoin atau mata uang kripto. Penelitian ini memberikan gambaran tentang ransomware, evolusinya, klasifikasinya, fase serangannya, deteksinya, pencegahannya, uraian keterbatasan penelitian, dan terakhir memberikan kesimpulan.

Kata kunci: Ransomware; evolusi; klasifikasi; fase serangan; deteksi; pencegahan

PENDAHULUAN

Dalam beberapa tahun terakhir, ransomware sering kali mendominasi berita utama laporan kejahatan dunia maya, ketika serangan ransomware yang berulang-ulang terhadap organisasi dan individu telah menimbulkan kerugian finansial yang sangat besar dan gangguan terhadap kehidupan norma. Meningkatnya ancaman ransomware menjadikan pertumbuhan penelitian yang eksponensial untuk menganalisis dan memitigasi serangan ransomware dari berbagai perspektif, seperti mendeteksi adanya ransomware yang diketahui atau ciri-ciri serangannya yang diketahui, melindungi OS dan file pengguna dari modifikasi atau akses yang tidak diinginkan, dan mencegah ransomware agar tidak menjangkau atau menyerang korban. Hingga saat ini, banyak penelitian yang menggunakan pendekatan terprogram atau berpusat pada data dan didasarkan pada pembelajaran mesin. Namun pelaku kejahatan cyber terus mencari cara baru untuk menghindari tindakan pencegahan yang ada saat ini. Beberapa telah menjajaki vektor serangan baru atau platform baru yang dapat dengan mudah mengalahkan mekanisme mitigasi yang ada. Misalnya skrip ransomware tanpa file akan membuat analisis apapun terhadap file yang dapat dieksekusi menjadi tidak berguna. Memahami isu ransomware terhadap penelitian akan memungkinkan untuk meninjau pemahaman terkait ransomware, evolusinya, klasifikasinya, fase serangannya, deteksinya, dan mengusulkan pencegahan yang lebih baik dan lebih efektif dalam jangka waktu yang lebih lama.

METODOLOGI PENELITIAN

Penelitian ini menggunakan metode penelitian sebagai berikut.

1. Mencari sumber data
   Prosedur penelitian yang diadopsi dalam artikel ini mencakup artikel yang relevan dengan judul penelitian.
2. Kriteria inklusi dan eksklusi yang jelas hal ini dilakukan agar dapat fokus langsung pada pokok bahasan dan menghindari bias dalam bentuk apa pun.
3. Pengumpulan data dan sintesis hasil
   Artikel-artikel yang diulas sejalan dengan kenyataan saat ini, mengakui bahwa serangan ransomware semakin besar di dunia digital modern.

HASIL DAN PEMBAHASAN

Ransomware

Ransomware adalah keluarga malware yang menggunakan teknik keamanan seperti kriptografi untuk membajak file pengguna dan sumber daya terkait serta meminta mata uang kripti sebagai imbalan atas data yang dikunci. Tidak ada batasan siapa yang dapat menjadi sasaran ransomware karena dapat ditularkan melalui internet. Seperti malware tradisional, ransomware dapat memasuki sistem menggunakan “rekayasa sosial, iklan malware, email spam, memanfaatkan kerentanan, unduhan drive-by atau melalui port terbuka atau dengan memanfaatkan pintu belakang. Namun berbeda dengan malware tradisional, bahkan setelah penghapusan, pengaruhi ransomware tidak dapat diperbaiki dan sulit untuk mengurangi dampaknya tanpa bantuan penciptanya. Serangan semacam ini mempunyai dampak finansial langsung, yang dipicu oleh teknologi enkripsi, mata uang siber. Oleh karena itu, ransomware telah berubah menjadi bisnis menguntungkan yang semakin populer di kalangan penyerang.

Evolusi Ransomware

Ransomware seperti Ragnar Locker, Ryuk, Egregor, Conti dan organisasi jahat lainnya yang memiliki dana besar dapat mengancam semua orang, termasuk pedagang, bank, pemerintah kota, dan

perguruan tinggi, untuk mendapatkan keuntungan. Meskipun ransomware bukanlah bentuk malware paling umum yang berdampak pada pengguna akhir, risiko kerugian sangatlah penting, dan bahata tersebut terus meningkat hari demi hari. Ransomware sudah berkembang pesat selama dua dekade, dan belum menunjukkan tanda-tanda akan berhenti dalam waktu dekat. Mengenkripsi ransomware adalah tantangan dunia maya yang canggih karena menggunakan semua teknik yang tersedia untuk menghasilkan sejumlah besar uang bagi peretas jahat

Ransomware pertama kali muncul 35 tahun lalu tepatnya tahun 1989. Pada Mei 2017 lalu, ransomware wannacry menjadi wabah yang meluas [9]. Ransomware muncul untuk mendorong mesin penghasil keuntungan sebagai ransomware pilihan ketika para peretas jahat beralih dari peretasan dunia maya ke kejahatan dunia maya perusahaan. Pengenalan dan kemajuan bitcoin dalam algoritma kriptografi membuat konteksnya siap untuk penemuan ransomware juga. Berdasarkan studi baru dari Purple Sec [19], frekuensi serangan ransomware telah meningkat 350 kali lipat sejak tahun 2018. Total permintaan tebusan telah meningkat lebih dari 100 persen pada tahun ini dan rata-rata harga per serangan meningkat.

Klasifikasi Ransomware

Banyak penelitian yang mencoba mengklasifikasikan ransomware dengan berbagai cara, misalnya berdasarkan silsilah atau kesamaan binernya, seperti penelitian yang dilakukan oleh Atapour-Abarghouei dkk [3]; Cuzzocrea dkk [8] serta berdasarkan platform yang umumnya digunakan oleh industri. Artikel ini mengklasifikasikan ransomware berdasarkan evolusi teknik penghindaran yang digunakan oleh ransomware. Penghindaran oleh ransomware adalah fitur penting yang digunakan oleh ransomware. Penghindaran oleh ransomware adalah fitur penting untuk menyelesaikan serangan ransomware sebelum kendali penuh atas sumber daya pengguna yang diambil [12],[11],[20]. Ditemukan bahwa varian ransomware yang dikembangkan pada waktu yang sama cenderung menggunakan teknik penghindaran yang serupa. Oleh karena itu, metode klasifikasi ransomware ini menawarkan pandangan progresif tentang bagaimana ransomware berevolusi untuk menghindari solusi deteksi, melewati mekanisme pertahanan, dan menghindari teknik pencegahan.

1. Pengunci layar. Pengunci layar dapat berupa perangkat lunak sah yang mengunci sistem komputer saat pengguna pergi, atau malware yang mengunci antarmuka pengguna untuk memeras korban agar membayar uang tebusan [12]. Dalam konteks ransomware, pengunci layar ransomware dapat mengunci seluruh antarmuka OS untuk menonaktifkan operasi pengguna, memaksa pengguna untuk tetap menggunakan UI ransomware saat ini, atau membuat peringatan palsu berulang kali untuk mengancam pengguna, seringkali tanpa benar-benar menyerang file dan data pengguna [10].
2. Ransomware Tanpa File. Ransomware tanpa file dikembangkan untuk menghindari pengawasan yang semakin ketat terhadap file yang dapat dieksekusi yang melakukan enkripsi file dan data pengguna. Dalam evolusi malware tanpa file yang menyerang sistem komputer tanpa file berbahaya yang dapat dieksekusi diantaranya file exe file pada platform Windows [16].
3. Crypto-Ransomware. Crypto-ransomware menyerang sistem file agar dapat menyandera file pengguna dan data [10],[17]. Pengguna umumnya disarankan untuk tidak melakukan pembayaran uang tebusan kepada penjahat dunia maya karena pembayaran apa pun akan mendanai kegiatan kriminal lebih lanjut; tidak semua korban yang membayar mendapatkan kunci deskripsi; dan tidak semua kunci deskripsi berfungsi untuk mendapatkan file dan data korban [5],[6].
4. Ransomware dengan Eksfiltrasi Data. Ransomware dengan eksfiltrasi data adalah ketika ransomware tidak lagi memeras pengguna dengan hilangnya akses data, melainkan dengan potensi kebocoran data sensitif. Ini dikembangkan untuk menghindari pengawasan yang semakin ketat terhadap perilaku enkripsi file apa pun, dan skema pencadangan yang lebih kuat.

Fase Serangan Ransomware

Ransomware menemukan tren yang menarik dalam kemampuannya untuk mendistribusikan ke beberapa perangkat dan karenanya memaksakan pembayaran yang lebih besar kepada musuh. Untuk mengatasi ancaman cyber tersebut secara efektif, langkah-langkah serangan harus dipahami.

1. Infeksi

a. Korban penerima email spam dengan lampiran file Zip berisi dokumen MS Word dengan macro VBA atau link
b. Email ini memiliki subjek yang beragam seperti invoice yang belum dibayar, pelacakan paket, dan lain sebagainya.

2. Instalasi
   a. Dropper mengenkripsi dan menjalankan peluncur. Ini akan menciptakan proses baru.
   b. Peluncur menggunakan teknik pengosongan proses untuk memasukkan kode berbahaya ke explore.exe atau svchost.exe.
   c. Registry diubah untuk persistensi reboot
   d. Salinan bayangan volume dihapus.
3. Komunikasi
   a. Ransomware menggunakan URL hardcode di dalam file yang dapat dieksekusi. Jika terjadi kegagalan, ia menggunakan DGA.
   b. Ia berkomunikasi dengan server Command & Control melalui permintaan POST melalui HTTPS dan mengandalkan SSL untuk mengenkripsi lalu lintasnya. Command & Control mengirimkan catatan tebusan.
   c. Alamat email yang dikumpulkan, kredensial SMTP, dan daftar kontak dikirim ke Command & Control.
4. Eksekusi
   a. Ia mencari file di semua drive yang terpasang dan sumber daya jaringan
   b. Untuk mengenkripsi file, kunci AES 256-bit dibuat
   c. File dengan ekstensi tertentu dienkripsi
   d. Enkripsi AES dilakukan dengan kunci publik RSA-2048 sebelum dikirim dan ditempatkan di server perintah dan kontrol.
   e. Kunci AES di mesin korban dimusnahkan.
5. Pemerasan
   a. Catatan tebusan ditampilkan di layar
   b. Pembayaran harus dalam bitcoin
   c. Halaman pembayaran dapat dijangkau melalui jaringan Tor.
6. Lepaskan
   a. Setelah memverifikasi rincian pembayaran, perangkat lunak deskripsi dikirimkan yang berisi kunci pribadi.
   b. Sebuah Deskripsi File Tunggal ditawarkan untuk layanan tidak terbatas.

Deteksi Serangan Ransomware

1. Tingkat Perangkat Keras. Di tingkat perangkat keras, deteksi ransomware dapat diterapkan pada sensor perangkat keras atau pada tingkat firmware perangkat keras.
2. Tingkat Mode Kernel. Di tingkat OS Modus Kernel, banyak implementasi deteksi ransomware memilih untuk menambahkan lapisan eksekutif OS guna menangkap aktivitas mencurigakan seperti ransomware dan informasi OS untuk analisis lebih lanjut. Implementasi pada tingkat model kernel [7], [11], [18] semua memanfaatkan fitur khusus OS untuk mencegat aktivitas sistem file mirip ransomware untuk dianalisis.
3. Tingkat Mode Pengguna. Sebagian besar penerapan teknis deteksi ransomware tampaknya beroperasi pada tingkat mode pengguna mungkin karena ransomware itu sendiri lebih cenderung berjalan dalam mode pengguna tanpa menyerang kernel OS [17] dan karena implantasi seperti itu biasanya tidak memerlukan pemrograman kernel OS yang rumit.

Pencegahan Ransomware

1. Tingkat Perangkat Keras
   Di tingkat perangkat keras, pencegahan ransomware dapat diimplementasikan sebagai kontrol akses berbasis firmware [1], [21]. Pencegahan ransomware pada tingkat perangkat keras sering kali menggunakan pendekatan “semua atau tidak sama sekali” dan sering kali tidak dapat membedakan secara memadai antara penggunaan yang sah atau penggunaan yang berbahaya, yang keduanya dapat berasal dari OS atau aplikasi pengguna.
2. File dan Data Pengguna

Pada tingkatan file dan data fisik, beberapa penelitian [13] menganjurkan di tingkat aplikasi pengguna untuk menegakkan daftar putih aplikasi. Aplikasi memasukkan ke dalam daftar putih mungkin dapat memitigasi beberapa serangan ransomware dengan mencegah eksekusinya. Pada tingkat pemeliharaan file dan data, pencegahan ransomware dapat diterapkan sebagai kontrol akses tingkat file [2],[14] dan folder yang dilindungi sebagai bagian dari produk antivirus.

3. Pengguna, Admin Sistem dan Organisasi
   Pada tingkatan pengguna, admin sistem dan organisasi, uang tebusan pencegahan dapat diimplementasikan sebagai pendidikan dan kesadaran pengguna [4], [15].

KESIMPULAN

Ransomware akan terus berkembang dengan fitur-fitur baru, vektor serangan, dan upaya yang lebih baik untuk mengurangi atau sepenuhnya mengabaikan proposal mitigasi yang ada. Peneliti memperkirakan lebih banyak penelitian mengenai berbagai kombinasi sampel ransomware, pemilihan fitur, dan strategi mitigasi akan terus dilakukan oleh para peneliti, namun penelitian apa pun yang tidak mengenal evolusi, klasifikasi, fase serangan, deteksi, mengatasi masalah mendasar kontrol akses dapat dengan mudah menjadi usang seiring berjalannya waktu ketika varian ransomware yang lebih baru mengaburkan atau mengabaikan fitur yang diketahui dalam tindakan anti ransomware. Masalah mendasar dari serangan ransomware yang berulang, baik yang melibatkan enkripsi data atau eksfiltrasi data adalah kurangnya kontrol akses yang tepat terhadap file dan sumber daya OS untuk memastikan bahwa perilaku kode pada cara penilaian file dan data pengguna harus konsisten dengan niat pengguna; ini adalah kesenjangan penelitian besar yang ditunjukkan oleh hasil survei peneliti.

.

REFERENSI

[1] Ahn, J., Park, D., Lee, C.-G., Min, D., Lee, J., Park, S., Chen, Q., & Kim, Y. (2019). KEY-SSD: Access-Control Drive to Protect Files from Ransomware Attacks.

[2] Ami, O., Elovici, Y., & Hendler, D. (2018). Ransomware prevention using application authentication-based file access control. ACM Symposium on Applied Computing, 1610–1619. https://doi.org/10.1145/3167132.3167304

[3] Atapour-Abarghouei, A., Bonner, S., & Mcgough, A.S. (2019). A King's Ransom for Encryption: Ransomware Classification using Augmented One-Shot Learning and Bayesian Approximation. https://github.com/atapour/ransomware-classification

[4] Bello, A., & Maurushat, A. (2020). Technical and Behavioral Training and Awareness Solutions for Mitigating Ransomware Attacks. Computer Science On-Line Conference, 1226 AISC, 164–176. https://doi.org/10.1007/978-3-030-51974-2_14

[5] Cartwright, E., Hernandez Castro, J., & Cartwright, A. (2019). To pay or not: game theoretical models of ransomware. Journal of Cybersecurity, 5(1). https://doi.org/10.1093/CYBSEC/TYZ009

[6] Conti, M., Gangwal, A., & Ruj, S. (2018). On the economic significance of ransomware campaigns: A Bitcoin transactions perspective. Computers & Security, 79, 162–189. https://doi.org/10.1016/J.COSE.2018.08.008

[7] Continella, A., Guagnelli, A., Zingaro, G., De Pasquale, G., Barenghi, A., Zanero, S., & Maggi, F. (2016). ShieldFS: A Self-healing, Ransomware-aware Filesystem. ACM International Conference Proceedings Series, 9-5-December-2016, 336–347. https://doi.org/10.1145/2991079.2991110

[8] Cuzzocrea, A., Martinelli, F., & Mercaldo, F. (2018). A Novel Structural-Entropy-based Classification Technique for Supporting Android Ransomware Detection and Analysis. IEEE

International Conference on Fuzzy Systems, 2018-July. https://doi.org/10.1109/FUZZ-IEEE.2018.8491637

[9] Goodin. (2017). A new ransomware outbreak similar to WCry is shutting down computers worldwide. https://arstechnica.com/information-technology/2017/06/a-new-ransomware-outbreak-similar-to-wcry-is-shutting-down-computers-worldwide/

[10] Kharaz, A., Arshad, S., Mulliner, C., Robertson, W., & Kirda, E. (2016). UNVEIL: A Large-Scale, Automated Approach to Detecting Ransomware. https://www.usenix.org/conference/usenixsecurity16/technical-sessions/presentation/song

[11] Kharraz, A., & Kirda, E. (2017). Redemption: Real-time Protection Against Ransomware at End-Hosts.

[12] Kharraz, A., Robertson, W., Balzarotti, D., Bilge, L., & Kirda, E. (2015). Cutting the Gordian Knot: A Look Under the Hood of Ransomware Attacks.

[13] Kim, D.Y., & Lee, J. (2020). Blacklist vs. Whitelist-Based Ransomware Solutions. IEEE Consumer Electronics Magazine, 9(3), 22–28. https://doi.org/10.1109/MCE.2019.2956192

[14] Lee, S., Kim, H.K., & Kim, K. (2019). Ransomware protection using the moving target defense perspective. Computers & Electrical Engineering, 78, 288–299. https://doi.org/10.1016/J.COMPELECENG.2019.07.014

[15] Luo, X., & Liao, Q. (2007). Awareness education as the key to ransomware prevention. Information Systems Security, 16(4), 195–202. https://doi.org/10.1080/10658980701576412/ASSET//CMS/ASSET/A36F90C4-6E1F-4640-8E49-1E8D35D4FAA9/10658980701576412.FP.PNG

[16] Mansfield-Devine, S. (2017). Fileless attacks: compromising targets without malware. Network Security, 2017(4), 7–11. https://doi.org/10.1016/S1353-4858(17)30037-5

[17] McIntosh, T.R., Jang-Jaccard, J., & Watters, P.A. (2018). Large Scale Behavioral Analysis of Ransomware Attacks. International Conference on Neural Information Processing, 11306 LNCS, 217–229. https://doi.org/10.1007/978-3-030-04224-0_19

[18] Mehnaz, S., Mudgerikar, A., & Bertino, E. (2018). RWGuard: A real-time detection system against cryptographic ransomware. Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 11050 LNCS, 114–136. https://doi.org/10.1007/978-3-030-00470-5_6

[19] PurpleSec. (2023). 2023 Cyber Security Statistics: The Ultimate List Of Stats, Data & Trends. https://purplesec.us/resources/cyber-security-statistics/

[20] Scalas, M., Maiorca, D., Mercaldo, F., Visaggio, A., Martinelli, F., & Giacinto, G. (2019). On the Effectiveness of System API-Related Information for Android Ransomware Detection. http://pralab.diee.unica.it/en/RPackDroid

[21] Siddiqui, A.S., Lee, C.C., & Saqib, F. (2017). Hardware based protection against malwares by PUF based access control mechanism. Midwest Symposium on Circuits and Systems, 2017-August, 1312–1315. https://doi.org/10.1109/MWSCAS.2017.8053172