Konferensi Internasional 2018 tentang Teknologi Komputasi, Matematika dan Rekayasa – iCoMET 2018

Cybercrime Kontemporer: Taksonomi Ancaman Ransomware & Teknik Mitigasi

Ibrahim Nadir, Taimur Bakhshi
Departemen Ilmu Komputer
Universitas Nasional Ilmu Komputer & Emerging
Lahore, Pakistan
ibrahim.nadir@nu.edu.pk

***Abstrak*— Jumlah perangkat yang mendukung Internet yang terus meningkat selama dekade terakhir telah menyoroti persyaratan untuk primitif keamanan siber yang kuat untuk secara efektif menangani bentuk-bentuk kejahatan dunia maya kontemporer. Di antara kanvas ancaman kejahatan dunia maya baru-baru ini, ransomware telah menjadi pusat perhatian sebagai bentuk virus kripto yang menonjol, yang bertujuan untuk menghambat operasi perangkat pengguna sehari-hari melalui enkripsi data perangkat yang tidak diminta. Pelaku yang berhasil mengenkripsi data pengguna, memerlukan pembayaran atau tebusan, seringkali dalam bentuk mata uang digital untuk memberikan kunci dekripsi. Bergantung pada urgensi dan kekritisan pemulihan data, baik pengguna pemula maupun organisasi perusahaan telah diamati membayar kompensasi yang signifikan untuk memulihkan operasi normal, seringkali tanpa jaminan pasca-pembayaran. Makalah ini berusaha untuk meninjau sejarah dan evolusi terbaru dari serangan ransomware, memberikan klasifikasi taksonomi rinci dari vektor serangan yang melekat dan teknik mitigasi yang tersedia saat ini. Selanjutnya, rekomendasi pencegahan dibahas untuk membantu pengguna dan organisasi dalam mengamankan perangkat dari ancaman ransomware. Akhirnya, implikasi keuangan dan jangka panjang dari melakukan pembayaran tebusan, bersama dengan sumber daya online yang disediakan oleh masalah keamanan dan penegakan hukum ditinjau untuk meningkatkan kesadaran pengguna akhir dan membekali mereka terhadap bentuk kejahatan dunia maya yang semakin sukses ini. rekomendasi pencegahan dibahas untuk membantu pengguna dan organisasi dalam mengamankan perangkat dari ancaman ransomware. Akhirnya, implikasi keuangan dan jangka panjang dari melakukan pembayaran tebusan, bersama dengan sumber daya online yang disediakan oleh masalah keamanan dan penegakan hukum ditinjau untuk meningkatkan kesadaran pengguna akhir dan membekali mereka terhadap bentuk kejahatan dunia maya yang semakin sukses ini. rekomendasi pencegahan dibahas untuk membantu pengguna dan organisasi dalam mengamankan perangkat dari ancaman ransomware. Akhirnya, implikasi keuangan dan jangka panjang dari melakukan pembayaran tebusan, bersama dengan sumber daya online yang disediakan oleh masalah keamanan dan penegakan hukum ditinjau untuk meningkatkan kesadaran pengguna akhir dan membekali mereka terhadap bentuk kejahatan dunia maya yang semakin sukses ini.**

Kata kunci— Ransomware, malware, kejahatan dunia maya, bitcoin

sayaPENDAHULUAN

Istilah ransomware berasal dari kombinasi dua kata tebusan dan malware. Pada dasarnya, malware apa pun yang mencuri beberapa fungsi perangkat pengguna dan mengharuskan pengguna membayar uang tebusan untuk pemulihan layanan termasuk dalam domain ransomware. Sejak dimulainya kripto-virologi, beberapa bentuk ransomware telah dikembangkan. Mulai dari taktik Scareware yang baru lahir, memaksa pengguna untuk membeli perangkat lunak antivirus yang sangat dibutuhkan yang mengakibatkan penguncian sistem, ransomware telah berkembang menjadi beberapa varian canggih. Contoh terbaru adalah Reveton, meniru sebagai pesan dari lembaga penegak hukum dan menyarankan pengguna untuk membayar penalti untuk penggunaan yang melanggar hukum sebelumnya atau menghadapi penguncian sistem [1]. Contoh menonjol lainnya termasuk CyrptoLocker yang terkenal mengenkripsi data pengguna menggunakan algoritma enkripsi yang kuat seperti RSA dan AES [2]. Menggunakan kunci RSA yang sangat panjang (misalnya, 2048 bit), dekripsi menjadi hampir tidak mungkin [3]. Sementara sejumlah alat komersial menawarkan dekripsi file, sebagian besar terbukti tidak efektif meninggalkan pengguna tanpa pilihan kecuali membayar uang tebusan kepada penyerang [4]. Selain pengguna komputer, ransomware juga dapat menargetkan ponsel cerdas. LockerPin [5] misalnya, adalah ransomware yang menargetkan perangkat android. Malware mengubah PIN perangkat menuntut uang tebusan yang harus dibayarkan kepada pelaku untuk membuka kunci perangkat. Sebuah varian dari LockerPIN adalah LeakerLocker [6] yang mengambil cadangan data pengguna dan menuntut tebusan jika tidak mengancam untuk melepaskan informasi pribadi pengguna [7] .

Penyerang Ransomware dapat meminta pembayaran dengan cara yang berbeda, namun metode yang lazim adalah melakukan dan menerima pembayaran dalam bentuk digital atau cryptocurrency seperti Bitcoin [8]. Pembayarannya sulit dilacak dan merupakan pilihan ideal bagi penyerang yang menginginkan anonimitas [9]. Bentuk pembayaran lain mungkin termasuk memaksa pengguna untuk membeli produk di situs web, mengklik tautan, dll. sehingga penyerang dapat menghasilkan pendapatan dari interaksi tersebut. Dengan meningkatnya serangan ransomware, permintaan tebusan rata-rata telah meningkat menjadi hampir $1077 pada akhir tahun 2016 dari hanya $294 pada tahun 2015, peningkatan substansial hampir 266% hanya dalam satu tahun [10]. Sepanjang waktu yang sama jumlah serangan ransomware meningkat dari 18% pada Januari 2016 menjadi sekitar 66% pada November 2016 [11]. Munculnya teknologi seperti Internet of Things (IoT) berarti bahwa jumlah serangan tersebut akan terus meningkat karena penyerang menemukan perangkat yang lebih rentan secara online yang menghasilkan skema tambahan untuk memaksa pengguna membayar uang tebusan untuk normalisasi layanan [12]. Makalah ini mengulas state-of-the-art dalam teknologi ransomware yang membahas secara rinci vektor serangan yang ada dan teknik mitigasi yang tersedia. Selain itu, rekomendasi dibuat untuk mencegah pengguna dari viktimisasi online dengan memasukkan praktik terbaik dan makalah ini juga mengulas sumber daya online yang tersedia untuk korban ransomware. Makalah ini mengulas state-of-the-art dalam teknologi ransomware yang membahas secara rinci vektor serangan yang ada dan teknik mitigasi yang tersedia. Selain itu, rekomendasi dibuat untuk mencegah pengguna dari viktimisasi online dengan memasukkan praktik terbaik dan makalah ini juga mengulas sumber daya online yang tersedia untuk korban ransomware. Makalah ini mengulas state-of-the-art dalam teknologi ransomware yang membahas secara rinci vektor serangan yang ada dan teknik mitigasi yang tersedia. Selain itu, rekomendasi dibuat untuk mencegah pengguna dari viktimisasi online dengan memasukkan praktik terbaik dan makalah ini juga mengulas sumber daya online yang tersedia untuk korban ransomware.

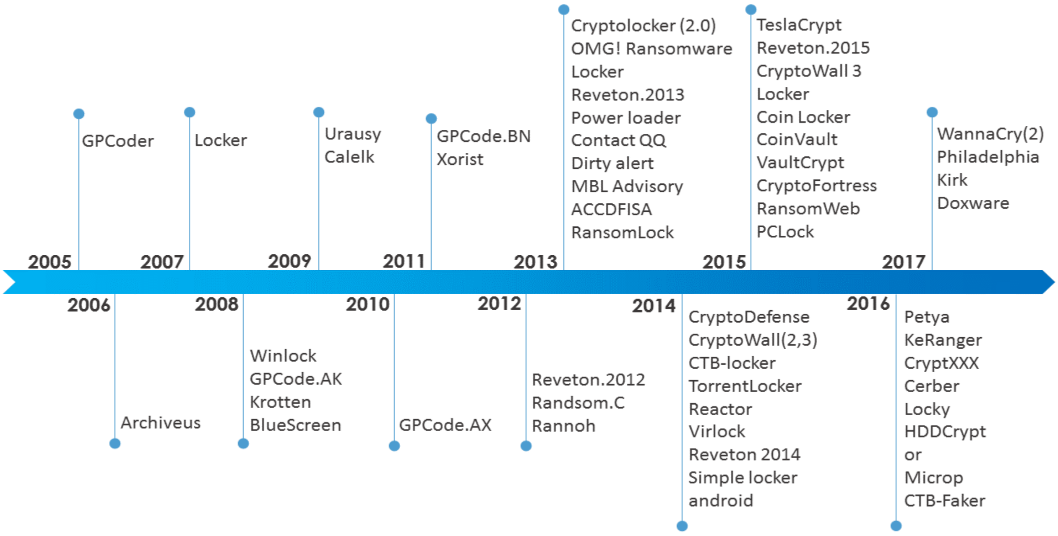
Penjelasan selanjutnya dari makalah ini akan dijelaskan sebagai berikut. Bagian 2 menyoroti sejarah ransomware dan kripto-virologi. Bagian 3 membahas dan mengklasifikasikan serangan ransomware yang lazim menurut penyebaran ancaman dan cara pembayaran tebusan. Bagian 4 mengeksplorasi teknik mitigasi ransomware yang tersedia yang merinci praktik terbaik. Bagian 5 meninjau implikasi keuangan dan konsekuensi jangka panjang dari pembayaran ransomware, serta merinci sumber daya online yang tersedia untuk meningkatkan kesadaran ransomware dan membantu korban. Kesimpulan akhir ditarik pada bagian 6.

978-1-5386-1370-2/18/$31.00 ©2018 IEEE

II. HCERITA

Seperti yang terdengar baru-baru ini, sejarah ransomware kembali ke tahun 1989 ketika Joseph L. Popp, seorang ahli biologi revolusioner dari Harvard, pertama kali menciptakan sebuah malware yang disebut PC Cyborg [13] [14]. Popp membuat dan mengirim 20.000 eksemplar disket ke peserta Organisasi Kesehatan Dunia. Malware mengenkripsi file di komputer setelah reboot ke-90 dan meminta tebusan $189 ke alamat pos di Panama. Sejarah singkat timeline pengembangan ransomware selama tahun-tahun sebelumnya digambarkan pada Gambar. 1. Ransomware modern pertama kemudian, datang dalam bentuk spyware palsu atau alat peningkatan kinerja yang tidak hanya menginfeksi Microsoft Windows OS tetapi juga MAC OS X. Alat palsu berjanji untuk memecahkan masalah tertentu dengan sistem operasi baik dengan menghapus beberapa malware atau memperbaiki beberapa masalah registri yang menuntut jumlah uang yang relatif kecil (antara $30 dan $90). Setelah jumlah dibayarkan, tidak ada yang benar-benar terjadi, karena pada kenyataannya tidak ada masalah yang harus diperbaiki. Kemudian muncul Trojan GPCode yang mengenkripsi file menggunakan kunci simetris dan asimetris dalam varian yang berbeda. Meskipun varian awal cacat dan alat dekripsi bekerja dengan baik melawan Trojan, pengembang GPCode lebih menyempurnakan dan meningkatkan pembelajaran malware dari kesalahan di versi sebelumnya [1]. Kemudian muncul Trojan GPCode yang mengenkripsi file menggunakan kunci simetris dan asimetris dalam varian yang berbeda. Meskipun varian awal cacat dan alat dekripsi bekerja dengan baik melawan Trojan, pengembang GPCode lebih menyempurnakan dan meningkatkan pembelajaran malware dari kesalahan di versi sebelumnya [1]. Kemudian muncul Trojan GPCode yang mengenkripsi file menggunakan kunci simetris dan asimetris dalam varian yang berbeda. Meskipun varian awal cacat dan alat dekripsi bekerja dengan baik melawan Trojan, pengembang GPCode lebih menyempurnakan dan meningkatkan pembelajaran malware dari kesalahan di versi sebelumnya [1].

Pada tahun 2006, Archiveus Trojan muncul yang menyalin file dari folder "My Documents" ke file zip yang dilindungi kata sandi dan menghapus dokumen asli [5]. Para korban serangan ransomware terus berlanjut, dengan kuartal ketiga tahun 2011 melaporkan peningkatan 50.000 sampel ransomware jika dibandingkan dengan kuartal pertama. Namun, sebagian besar kode ransomware adalah pembaruan dan salinan dari versi sebelumnya. Variasi baru dari crypto-virus muncul pada tahun 2012, bernama Reveton [1]. Idenya adalah untuk menggunakan taktik scareware, menampilkan pesan palsu kepada pengguna akhir dari lembaga penegak hukum setempat yang memberikan pemberitahuan yang mengkhawatirkan tentang penggunaan komputer yang melanggar hukum seperti menonton pornografi anak atau pelanggaran hak cipta. Para korban disarankan untuk membayar denda sebagai akibat dari kegiatan ilegal ini. Tonggak sejarah lainnya di tahun 2012, adalah pengenalan formal kata "ransomware" dalam kamus Oxford English Language [15]. Kasus besar pertama ransomware yang mempengaruhi jumlah pengguna global muncul dalam bentuk malware CyrptoLocker pada tahun 2013 [16][17]. CryptoLocker menggunakan enkripsi kelas militer RSA-2048 bit untuk mengenkripsi file. Sedangkan serangan ransomware sebelumnya umumnya digunakan untuk meninggalkan kunci dekripsi pada pembuatan komputer korban memungkinkan untuk menyediakan kunci pembayaran dengan cepat serta menyediakan administrator sistem sarana untuk mengambil kunci lokal, penulis CryptoLocker meningkatkan skema ini dan menyimpan kunci dekripsi di server. Penyimpanan kunci dari jarak jauh membuat sangat tidak mungkin bagi pengguna untuk mendekripsi data kecuali kunci tersebut diambil pada saat enkripsi. Pindah pada 2014, melihat rilis sejumlah ransomware terutama CryptoWall [18] dan CryptoDefence [19][16]. Kedua bentuk malware menggunakan enkripsi simetris yang kuat menggunakan AES. Untuk sepenuhnya mengeksploitasi pengguna dan memaksa mereka melakukan pembayaran, sebagian data korban diizinkan untuk didekripsi untuk membuktikan bahwa data pengguna dapat dipulihkan sepenuhnya jika pembayaran dilakukan. Diperkirakan 500.000 komputer secara global terinfeksi oleh salah satu malware. Lebih-lebih lagi, penyerang juga mulai menggunakan jaringan anonim seperti TOR [20] untuk komunikasi dan teknologi baru seperti Bitcoin [8] untuk lebih meningkatkan dan merampingkan model bisnis tebusan. Evolusi ancaman ransomware baru terus berlanjut, TelsaCrypt [18] dirilis pada tahun 2015, lagi-lagi menggunakan enkripsi AES, bersama dengan kebangkitan varian Reveton dan CryptoWall. TelsaCrypt mampu mengenkripsi lebih dari 170 ekstensi file dan menggunakan Bitcoin sebagai mata uang pilihan untuk pembayaran tebusan. Baru-baru ini, pada tahun 2016, telah dilaporkan bahwa hampir 65% hingga 70% dari semua malware yang digunakan terdiri dari ransomware [10]. Beberapa nama baru ke dalam daftar virus kripto yang ada termasuk Locky [21][10], Cerber [21][10], CryptXXX [21][10] dengan peningkatan substansial dalam permintaan tebusan berkisar antara $500 hingga $1200. Pada untai terpisah, tingkat deteksi ransomware oleh alat antivirus meningkat hampir 36% selama 2016 dibandingkan dengan 2015. Selain itu, sekitar 101 keluarga baru ransomware terdeteksi pada tahun 2016 dibandingkan dengan 2015 di mana 30 keluarga baru ditemukan [10]. Serangan terbaru dan terkenal pada tahun 2017 adalah ransomware WannaCry [13] yang menginfeksi lebih dari 200.000 komputer dan menuntut uang tebusan sebesar $300. Malware Philadelphia [22] contoh terbaru lainnya terutama menargetkan industri kesehatan. Beberapa nama layak lainnya adalah Kirk [23] yang terutama mengenkripsi file dan Doxware [24] yang mirip dengan LeakerLocker, mengancam untuk mempublikasikan data pengguna pribadi secara online dengan maksud jahat. Secara keseluruhan, tren ransomware telah meningkat dan mendapatkan momentum dalam beberapa tahun terakhir. Sampai sekarang,



Gambar 1. Garis waktu yang menggambarkan evolusi Ransomware

pada individu (57%) daripada perusahaan (43%) [21]. Seperti disebutkan sebelumnya, penggabungan IoT dalam domain pengguna akhir akan meningkatkan peluang lebih lanjut pengguna menjadi mangsa serangan ransomware. Oleh karena itu, kebutuhan akan kesadaran pengguna akhir dalam mengenali serangan ransomware, ketersediaan alat online untuk membantu pengguna dalam menghadapi ancaman keamanan siber, dan perangkat lunak keamanan yang tangguh, sangat dibutuhkan. Bagian selanjutnya mengklasifikasikan vektor serangan ransomware yang menonjol.

AKU AKU AKU. RPERANGKAT LUNAK CLASIFIKASI

Serangan Ransomware dapat diklasifikasikan sehubungan dengan jenis vektor serangan yang digunakan untuk propagasi serta cara pembayaran yang digunakan. Deskripsi singkat dan sifat masing-masing kategori tercantum dalam Tabel 1. Vektor divergen ada di setiap kategori yang memiliki keunggulan relatifnya sendiri. Meskipun mengirim Email spam yang berisi lampiran berbahaya mungkin merupakan cara propagasi yang dinamis dan murah, secara teknis masih pemula dibandingkan dengan program afiliasi canggih yang menawarkan ransomware-as-a-service. Program afiliasi mengandalkan jaringan botnet dan broker yang ada untuk menyebarkan malware. Setiap vektor serangan dilengkapi dengan taktik rekayasa sosialnya sendiri untuk memikat pengguna agar tunduk pada mekanisme pengiriman. Demikian pula, penyerang ransomware dapat memanfaatkan layanan situs web pihak ketiga untuk meminta uang dari korban atau menggunakan pendekatan yang lebih langsung untuk menyetor/mentransfer mata uang kripto seperti Bitcoin di dompet penyerang. Klasifikasi lebih lanjut dalam dua kategori yang didefinisikan secara luas dibahas dalam sub-bagian berikut.

A. Propagasi Ransomware

Terutama, serangan ransomware secara umum dapat diklasifikasikan dalam tiga kategori berbeda dalam hal mekanisme propagasi crypto-virus: sebagai kombinasi alat pra-paket bernama exploit kits (EK), program afiliasi yang menyediakan layanan ransomware dan kampanye malware.

- **Kit Eksploitasi:** Eksploitasi kit (EK) adalah paket paket alat yang dapat dibeli atau disewa untuk tujuan mendistribusikan malware umum termasuk ransomware [25] [26]. Kode direkayasa untuk berfungsi sebagai saluran komunikasi terbuka yang dapat digunakan oleh penyerang untuk berkomunikasi dengan sistem yang disusupi dan mengelola instruksi jarak jauh. Oleh karena itu, penulis ransomware baru tidak perlu berburu atau mengembangkan sistem pengiriman baru tetapi menggunakan EK untuk mendistribusikan malware kepada korban. EK biasanya dibangun di atas kerentanan browser dan lubang keamanan untuk menyuntikkan kode JavaScript berbahaya yang melakukan serangkaian serangan berurutan hingga berhasil. Salah satu EK paling populer adalah kit exploit Angler yang digunakan oleh penyerang yang tidak memiliki pengetahuan teknis yang mendalam dan membutuhkan kemampuan serangan berbasis web otomatis. Menurut laporan analisis kerentanan oleh Proofpoint security [27], sebanyak 10 juta perangkat Android diperkirakan telah disusupi oleh EK yang memungkinkan penyerang mengambil kendali perangkat pengguna. Kit eksploitasi sangat memudahkan pekerjaan ransomware untuk menemukan bug yang diketahui di plug-in browser web dan prosedur kerja untuk mengubah bug tersebut menjadi eksploitasi lebih lanjut dan untuk menarik korban.

- **Program Afiliasi:** Saat ini penyerang ransomware tidak perlu menulis kode malware lengkap, menjalankan server hosting dan melacak pembayaran dari korban, mengambil dan memanen informasi pengguna seperti kata sandi karena semuanya dapat dialihdayakan [28]. Seluruh sindikat yang kemudian dikenal sebagai Crimeware-as-a-Service memungkinkan individu untuk berspesialisasi dalam satu bidang bisnis kejahatan dunia maya. Program afiliasi memungkinkan penyerang untuk memanfaatkan malware yang ada dan mendukung infrastruktur untuk mengirimkan vektor menular dengan banyak efektivitas dan dengan kesederhanaan [29].

TABEL I. RPERANGKAT LUNAK THEAT CLASIFIKASI

Parameter	**Properti**	
	Pendekatan Utama	***Keterangan***
Perambatan	Kit Eksploitasi	Paket pra-paket dari peralatan.
	Program Afiliasi	Kode outsourcing perkembangan, propagasi.
	Kampanye Malvertising	Spam berbasis email kampanye yang menargetkan pengguna.
Pembayaran	Pembayaran langsung	Transfer kawat, pembayaran mata uang kripto.
	Pembayaran Tidak Langsung	Voucher prabayar, pembelian online, dan panggilan/SMS dengan tarif premium.

- **Kampanye Malvertising dan Spam:** Terlepas dari ketersediaan EK dan program afiliasi yang canggih, penggunaan iklan malware dasar (malvertising) dan kampanye Email spam yang menawarkan metode murah dan nyaman bagi penyerang untuk menghasilkan vektor serangan tidak dapat dikesampingkan. Pesan Email yang sangat terlokalisasi dan kampanye iklan yang menggunakan taktik rekayasa sosial dapat memikat korban untuk mengunduh dan membuka lampiran Email [30] atau mengunjungi pemasok lokal yang relatif baru lahir yang mengakibatkan kompromi sistem. Satu ransomware baru-baru ini disebut sebagai CryptoLocker.f Trojan (atau Locky), mendominasi kampanye Email. Di antara serangan yang diluncurkan menggunakan email yang berisi lampiran berbahaya, 69% dilaporkan mengandung virus Locky pada kuartal kedua 2016 dibandingkan dengan 24% pada kuartal pertama [31][21].

B. Pembayaran Ransomware

Klasifikasi Ransomware menurut cara pembayaran secara umum dapat diidentifikasi sepanjang metode pengumpulan pembayaran, langsung atau tidak langsung. Rincian mengenai masing-masing kategori klasifikasi dijelaskan dalam subbagian berikut.

- **Pembayaran Langsung:** Selain metode de-facto penyerang yang menerima pembayaran menggunakan transfer tunai, penggunaan mata uang dunia maya seperti Bitcoin baru-baru ini meningkat. Bitcoin mengacu pada pembayaran digital dan sistem pelacakan aset yang dirilis sebagai proyek open source pada tahun 2009 [8]. Sistem pertukaran bitcoin menggunakan jaringan peer-to-peer dan transaksi terjadi secara langsung antar individu tanpa perantara atau broker. Verifikasi transaksi dilakukan melalui node jaringan dan semua pertukaran dicatat dalam buku besar akuntansi publik (terdistribusi) yang disebut sebagai blockchain [33]. Badan pengatur keuangan menganggap bitcoin sebagai mata uang virtual (cryptocurrency) yang terdesentralisasi dan seharusnya menjadi yang terbesar di antara mata uang virtual dalam hal pangsa pasarnya. Bitcoin sering disebut sebagai metode pembayaran pilihan dalam ransomware karena sangat sulit untuk diselidiki dan melacak jejak yang mungkin ditinggalkan oleh transaksi tanpa afiliasi langsung dengan penyerang. Menurut sebuah laporan oleh Citrix [12], sejumlah perusahaan yang berbasis di Inggris menimbun bitcoin untuk membayar penyerang jika terjadi kompromi ransomware yang berhasil. Dari 250 spesialis TI yang disurvei oleh Citrix, hampir 33% menyarankan memiliki persediaan bitcoin untuk melayani ransomware [31][34].

- **Pembayaran Tidak Langsung:** Bentuk pembayaran tidak langsung juga dapat digunakan dalam serangan ransomware, di mana penyerang mengkhawatirkan tingkat anonimitas yang tinggi. Beberapa metode yang menonjol termasuk penggunaan kartu voucher prabayar, pembelian produk online serta panggilan ke nomor tarif premium. Saat menggunakan voucher prabayar sebagai mode pembayaran, penyerang menyarankan para korban untuk melakukan pembayaran menggunakan kartu voucher yang dibeli dari toko ritel yang berbeda. Karena kartu-kartu tersebut harus dibeli oleh para korban, transaksi tersebut kembali meninggalkan jejak minimal (jika ada) bagi para penyerang. Kartu voucher prabayar cukup terlihat dalam beberapa investigasi ransomware tingkat tinggi. Bentuk pembayaran lainnya termasuk memaksa pengguna untuk membeli produk online dari situs web tertentu untuk menebus peralatan komputasi mereka. Taktik ini sebagian besar telah digunakan di scareware dan selain mengharuskan pengguna untuk membeli produk juga memungkinkan penyerang untuk menangkap rincian kartu pembayaran pengguna untuk eksploitasi selanjutnya [35][36]. Akhirnya, panggilan dan teks tarif premium juga telah dilaporkan sebagai metode pembayaran pilihan dalam ransomware. Penyerang menyarankan korban untuk menelepon nomor tarif premium di lokasi panggilan yang tersebar secara geografis dan mahal untuk mendapatkan kode validasi untuk layanan yang dikunci, misalnya masa berlaku Windows, dll. Panggilan dan pesan teks pada gilirannya menghasilkan keuntungan bagi penyerang dengan sebagian besar titik akhir berada di wilayah yang sama dengan mereka sementara panggilan dan teks dialihkan melalui negara asing [37]. Bagian selanjutnya mengulas teknik mitigasi yang tersedia saat ini terhadap vektor serangan ransomware rahasia. Panggilan dan pesan teks pada gilirannya menghasilkan keuntungan bagi penyerang dengan sebagian besar titik akhir berada di wilayah yang sama dengan mereka sementara panggilan dan teks dialihkan melalui negara asing [37]. Bagian selanjutnya mengulas teknik mitigasi yang tersedia saat ini terhadap vektor serangan ransomware rahasia. Panggilan dan pesan teks pada gilirannya menghasilkan keuntungan bagi penyerang dengan sebagian besar titik akhir berada di wilayah yang sama dengan mereka sementara panggilan dan teks dialihkan melalui negara asing [37]. Bagian selanjutnya mengulas teknik mitigasi yang tersedia saat ini terhadap vektor serangan ransomware rahasia.

IV. MITIGASI TTEKNIK

Selama bertahun-tahun, sejumlah solusi telah disarankan untuk menghindari atau memulihkan dari ancaman ransomware. Dengan setiap solusi, penulis ransomware datang dengan teknik serangan baru yang memperkenalkan variasi baru dan metodologi serangan yang ditingkatkan. Jumlah deteksi ransomware meningkat dari 933 pada tahun 2015 menjadi 1271 pada tahun 2016 per hari [10]. Karena peningkatan ini, hampir tidak mungkin bagi perangkat lunak antimalware untuk menangkap setiap varian ransomware. Bahkan jika tanda tangan untuk ransomware tertentu ada, itu mungkin dienkripsi dan terbang di bawah radar alat keamanan. Memberikan keamanan yang memadai ke sistem menggunakan sejumlah teknik mungkin terbukti membantu jika tidak sepenuhnya aman. Apa pun alat atau teknik keamanan yang digunakan, versi terbarunya harus selalu dipastikan. Baik itu sistem operasi atau perangkat lunak keamanan, industri keamanan siber merekomendasikan pembaruan dan tambalan setiap saat. Di bawah ini kami menyajikan beberapa teknik yang mengurangi terhadap ransomware dan juga dapat membantu dalam pemulihan jika serangan ransomware dijalankan.

A. Backup data

Mencadangkan data terhadap serangan keamanan apa pun menyenangkan[38][39][40][41][42]. Bisnis Ransomware bergantung pada gagasan untuk memaksa pengguna membayar uang tebusan untuk mengambil data sensitif mereka. Jika cadangan reguler (dapat dipulihkan) dikelola oleh pengguna secara ideal pada sumber daya eksternal (seperti cloud, USB, hard drive), serangan ransomware hampir tidak berguna. Sejumlah solusi cloud tersedia yang memungkinkan Anda menyinkronkan data komputer Anda dengan salinan redundan di cloud. Dalam kasus ini, meskipun data dienkripsi oleh ransomware, salinan online data tersebut masih dapat diambil. Beberapa solusi cloud seperti Dropbox bahkan dapat mengambil versi data yang lebih lama. Jika data dienkripsi atau dihapus dan alat desktop menyinkronkan data yang diserang ransomware, Dropbox dapat mengambil data asli [43].

B. Antivirus & alat keamanan

Antivirus dan perangkat lunak keamanan terkait adalah langkah keamanan penting terhadap ransomware. Meskipun alat ini mungkin hanya tahan terhadap tanda tangan ancaman yang ada, beberapa alat canggih memiliki kemampuan pembelajaran mesin yang dapat melakukan analisis komprehensif terhadap ransomware. Memperbarui alat keamanan sangat diperlukan, apa pun perangkat lunak keamanan yang digunakan untuk melawan semua jenis ancaman [21][44][45]. ShieldFS, alat keamanan, yang mendeteksi perilaku seperti ransomware dan secara otomatis mencadangkan file membuat sistem operasi modern lebih tangguh [46].

C. Memperbarui semua perangkat lunak & sistem operasi

Semua pembaruan dan tambalan sistem operasi bukan untuk tujuan keamanan tetapi banyak yang. Oleh karena itu, pembaruan dan penambalan otomatis secara teratur wajib dilakukan untuk menghindari kerentanan baru yang dapat dieksploitasi [47]. Penyerang Ransomware mencari kelemahan dalam sistem operasi atau perangkat lunak aplikasi agar berhasil mengeksekusi serangan mereka. Selama infeksinya, salah satu tujuan dari ransomware terkenal yang disebut CryptoWall 3 adalah untuk menonaktifkan Layanan Pembaruan Windows dan Windows defender [19][48][42].

D. Keamanan email

Email telah menjadi salah satu vektor infeksi yang paling luas untuk distribusi ransomware [9]. Dengan pengurangan penggunaan Exploit Kits dan peningkatan kemampuan menangkap perangkat lunak antimalware, email tetap menjadi vektor infeksi yang menarik [47]. Filter email yang layak dapat meminimalkan persentase serangan dengan jumlah yang layak [21][48]. Tentu saja, kewaspadaan pribadi pengguna penting di samping alat dan filter keamanan. Server surat juga memiliki peran penting dalam hal ini. Beberapa filter spam dasar selalu diinstal pada server surat yang dapat diandalkan [49]. Pengguna, bagaimanapun, harus berhati-hati setiap saat untuk tidak mengunduh atau mengklik file mencurigakan dari kontak yang tidak dikenal dan dikenal.

E. Kontrol Akses/Otorisasi dan Izin

Tingkat izin dan akses yang berbeda harus diterapkan di perusahaan. Tergantung pada pengguna, tingkat hak istimewa harus ditetapkan. Bahkan pengguna dengan hak istimewa harus bekerja dengan akun yang memiliki tingkat otorisasi lebih rendah karena semua orang membuat kesalahan. Kontrol akses dan izin dapat diimplementasikan melalui sistem pencegahan intrusi sehingga peran dan kebijakan ditetapkan dalam hak serendah mungkin untuk menyelesaikan tugas [4]. File dan izin akses perlu dikerjakan dengan hati-hati sehingga hanya mengizinkan akses akun yang diperlukan untuk membuat perubahan seperti enkripsi karena banyak keluarga ransomware baru-baru ini bergantung pada enkripsi. Karena ransomware juga menyerang ponsel cerdas, penting untuk memperhatikan izin yang diminta oleh ransomware saat menginstal aplikasi dari toko aplikasi [21] [13]. Pada waktu bersamaan, aplikasi smartphone harus diperbarui secara berkala. Di bisnis dan kantor, ponsel cerdas, tablet, dan laptop pribadi staf dan karyawan harus dijaga di bawah kebijakan keamanan. Semua perangkat, dengan demikian, harus dikelola oleh jaringan karena mereka adalah bagian dari jaringan [16].

F. Daftar Putih Aplikasi

Administrasi sistem yang efektif hanya memerlukan serangkaian aplikasi tepercaya tertentu untuk dimasukkan dalam daftar putih di registri sistem untuk pembaruan otomatis dan membuat perubahan pada parameter sistem dan file lainnya [50][51]. Ini sangat membatasi sejauh mana malware yang diunduh. Misalnya, melalui web browser plug-in akan menyebar dan membuat perubahan lebih lanjut ke data pengguna. Selain aplikasi, pengguna juga perlu waspada terhadap add-on untuk browser web populer yang memungkinkan kontrol terbatas dengan menyesuaikan fitur plug-in.

G. Volume Salinan Bayangan

Di sistem Windows, jika sistem file yang digunakan adalah NTFS, salah satu layanan windows mengambil cadangan file secara manual atau otomatis yang disebut Volume Shadow Copies. Juga disebut sebagai Volume Snapshot Service (VSS) dapat digunakan untuk memulihkan sebagian data jika tidak semuanya. Jika implementasi ransomware tidak canggih, itu akan mengabaikan penghapusan salinan bayangan volume drive dan sebagian data dapat dipulihkan bahkan setelah enkripsi [45]. Ransomware berorientasi detail, misalnya TeslaCrypt menghapus salinan volume bayangan jendela [52].

H. Alat dekripsi

Sejumlah alat gratis tersedia online gratis untuk mendekripsi data terenkripsi ransomware. Perusahaan seperti AVG, AVAST [2], Kaspersky, dan Windows Defender dll. menyediakan alat dekripsi. Meskipun, mereka hanya akan berfungsi jika teknik enkripsi, algoritme, atau kunci yang digunakan oleh pembuat ransomware tidak cukup kuat, pengguna mungkin masih memiliki kesempatan untuk mendapatkan kembali data tanpa membayar tebusan.

I. Alat pemulihan data

Setelah data dihapus dari sistem file, mungkin tidak akan hilang sepenuhnya sampai digantikan oleh data baru di drive yang sama. Korban ransomware yang datanya dienkripsi atau hilang dapat mencoba memulihkan data mereka yang terhapus menggunakan alat pemulihan data [19].

Bagian berikut merinci implikasi keuangan bagi korban yang melanjutkan dan melakukan pembayaran tebusan untuk memulihkan data, tren negosiasi, serta sumber daya online untuk membantu dan mendidik pengguna tentang ransomware.

V.ATACK SayaMPLIKASI & USER HAIPTIONS

Selama beberapa tahun terakhir, korban ransomware telah membayar sejumlah besar uang tebusan kepada penyerang. Ransomware telah berkembang lebih jauh dengan munculnya "Ransomware-as-a-service (RaaS)", memungkinkan bahkan script kiddie berhasil mengeksekusi serangan ransomware menggunakan alat otomatis. Penulis alat ransomware mendapat persentase dari uang tebusan yang dibayarkan oleh korban dan sisa uangnya dibayarkan ke skrip kiddie. Dalam skenario yang canggih, bahkan dukungan pelanggan ditawarkan kepada korban untuk pembayaran tebusan dan negosiasi [53]. Mengingat meningkatnya jumlah serangan ransomware, pertanyaan kunci muncul bagi korban, apakah akan membayar uang tebusan dengan harapan pemulihan data cepat, dapatkah uang tebusan dinegosiasikan, dan terakhir bagaimana melaporkan kejahatan dunia maya. Subbagian berikut secara singkat membahas masing-masing masalah ini.

A. Implikasi Membayar Uang Tebusan – Membayar atau Tidak Membayar!

Jika individu atau bisnis tidak memiliki kebijakan cadangan, serangan ransomware yang berhasil bermuara pada pertanyaan ini: apakah akan membayar uang tebusan atau tidak? Juga, setelah pembayaran, apakah data dapat dipulihkan? Jaminan macam apa yang ada bahwa penjahat dunia maya akan memberikan kunci yang dapat berhasil mendekripsi data setelah uang tebusan dibayarkan. Ransomware terbaru WannaCry [13] adalah contoh masalah di mana ransomware tidak memiliki cara untuk mengaitkan ID dengan pembayar tebusan. Jadi bahkan setelah pembayaran dilakukan, data korban tidak pernah pulih. Menurut laporan keamanan oleh Symantec, secara global sekitar 34% korban akhirnya membayar uang tebusan. Rata-rata cukup tinggi di AS, di mana 64% korban membayar uang tebusan. Membayar uang tebusan memperkuat serangan dan mau tidak mau AS telah melaporkan jumlah tertinggi serangan ransomware baru-baru ini [10]. untuk tidak membayar tebusan. Beberapa alasan kuat untuk tidak membayar tercantum sebagai berikut.

- Model bisnis dasar di balik ransomware bergantung dan berkembang karena korban membayar uang tebusan. Jika tidak ada pembayaran yang dilakukan, model bisnis akan runtuh.
- Meskipun melakukan pembayaran tidak ada jaminan apapun, bahwa korban mungkin tidak mendapatkan data kembali.
- Setelah pembayaran dilakukan, penyerang sangat menyadari kerentanan korban serta kapasitas untuk melakukan pembayaran. Oleh karena itu kemungkinan serangan di masa depan pada korban yang sama tidak dapat dikesampingkan.

B. Negosiasi dengan Penyerang – Ada jaminan!

Mendapatkan lebih sedikit uang tebusan lebih baik daripada tidak ada uang tebusan sama sekali, yang umumnya merupakan jiwa dasar di balik serangan ransomware. Biasanya, negosiasi dengan penyerang telah menghasilkan pembayaran dalam beberapa kesempatan di mana korban dapat membeli lebih banyak waktu untuk melakukan pengaturan pembayaran atau berhasil mengurangi jumlah uang tebusan yang harus dibayarkan. Laporan keamanan siber F-Secure menyatakan bahwa rata-rata, 3 dari 4 penjahat ransomware bernegosiasi dengan memberikan diskon rata-rata 29 persen [47]. Penggambaran dasar dari beberapa keluarga ransomware populer dan tren pembayaran dan negosiasi sesuai dengan perusahaan keamanan F-Secure [47] disediakan di Tabel 2. Baru-baru ini kasus pembayaran tebusan tingkat tinggi muncul, yaitu dari Hollywood Presbyterian Medical Center di mana penyerang menuntut tebusan sebesar $3,7 juta karena sensitivitas data medis yang dikompromikan. Para korban dikurangi menjadi penggunaan pena dan kertas untuk mempertahankan laporan harian dan menegosiasikan jalan mereka ke $ 17.000 sebagai tebusan untuk operasi normalisasi [13]. Meskipun berhasil mendapatkan diskon mungkin tampak ide yang layak bagi korban pada awalnya, pada saat yang sama ini akan memikat lebih banyak korban untuk membayar uang tebusan. Seorang korban yang mampu membayar uang tebusan sebesar $100 untuk mendapatkan sesuatu yang dipulihkan mungkin tidak dapat membayar $300. Oleh karena itu penyerang bisa mendapatkan keuntungan dari memberikan potongan harga tebusan dan memaksa lebih banyak korban untuk membayar dalam jangka panjang. Negosiasi, bagaimanapun juga, adalah tanda korban siap membayar sejumlah uang dan itulah alasan beberapa penyerang juga mulai meng-hosting situs web untuk memberikan “dukungan pelanggan” kepada korban untuk negosiasi [54]. Meskipun demikian pembayaran tebusan tidak menjamin bahwa data dapat dipulihkan, dan pada dasarnya korban dapat berakhir dalam situasi di mana pembayaran telah dilakukan tetapi data tetap dalam keadaan terenkripsi atau terkunci. Lebih buruk lagi, saat menerima pembayaran, penyerang mungkin meminta uang tambahan dengan harapan mendapatkan sesuatu yang ekstra dari korban. Sub-bagian berikut menyoroti beberapa sumber online khusus untuk pendidikan dan dukungan pengguna akhir tentang kejahatan dunia maya yang muncul ini.

C. Sumber Daya Pendukung

Sejak kemunculan kembali ransomware baru-baru ini, beberapa inisiatif telah diambil baik oleh organisasi keamanan informasi maupun lembaga penegak hukum untuk membantu meningkatkan kesadaran tentang kejahatan dunia maya yang aneh ini. Daftar singkat sumber daya yang tersedia saat ini untuk membantu populasi pengguna umum serta korban ransomware dirinci sebagai berikut.

- **Tidak Ada Lagi Proyek Tebusan:** Situs web “No More Ransom” telah diprakarsai oleh dua lembaga penegak hukum, Unit Kejahatan Teknologi Tinggi Nasional dari kepolisian Belanda, Pusat Kejahatan Dunia Maya Eropa dari Europol bersama dengan dua perusahaan keamanan dunia maya – Kaspersky Lab dan McAfee [55]. Tujuan utama dari proyek ini adalah untuk membantu korban ransomware mengambil data terenkripsi mereka tanpa harus membayar penjahat [55]. Proyek ini menyediakan umum

TABEL II. SCUKUP PAYMENT NEGOSI TRENDS (F-SECURE 2017)

Keluarga Ransomware	Mulai Tuntutan	Terendah Tuntutan	% Diskon
CERBER	$30	$30	0%
KRIPTOMIX	$1900	$635	67%
GERGAJI UKIR	$150	$125	17%
NAUNGAN	$400	$280	30%
Nilai rata-rata	$620	$267,5	29%

informasi tentang ransomware, saran pencegahan, alat dekripsi serta formulir yang mudah digunakan untuk merekam ciri-ciri jenis ransomware yang dialami oleh pengguna (termasuk opsi untuk mengunggah file terenkripsi) dan saran tentang opsi pemulihan data yang tersedia.

- **Pencegahan & Tanggapan Ransomware FBI:** Departemen Kehakiman AS, Biro Investigasi Federal, telah menyiapkan halaman web khusus di bawah bagian keamanan siber untuk mendidik dan memberikan informasi kepada pengguna mengenai ancaman ransomware [56]. Di antara berbagai informasi bermanfaat yang disediakan termasuk dokumen yang memberikan informasi agregat tentang praktik terbaik dan strategi mitigasi pemerintah federal dan industri swasta yang sudah ada. Dokumen-dokumen tersebut ditargetkan baik untuk khalayak umum maupun kepentingan perusahaan untuk membatasi dan mencegah insiden ransomware.

- **Pusat Pengaduan Kejahatan Internet (IC3):** IC3 menerima pengaduan kejahatan Internet online dari korban ransomware yang sebenarnya dan juga dari pihak ketiga [57]. Pusat ini berada dalam naungan FBI dan mendorong pengguna untuk berbagi pengalaman ransomware mereka. Beberapa data yang diperlukan termasuk tanggal dan spesifik kejadian. Instruksi umum juga memberikan informasi tambahan terutama mendidik pengguna agar tidak melakukan pembayaran ransomware yang mungkin memberanikan musuh dan seperti yang dibahas sebelumnya masih belum menjamin untuk mendapatkan kunci dekripsi.

- **Pusat Keamanan Cybercrime Nasional (NCSC, Inggris):** Pusat keamanan cybercrime nasional di Inggris, telah mendedikasikan halaman web yang menawarkan dukungan dan meningkatkan kesadaran tentang ransomware [58]. Halaman tersebut mencakup informasi umum tentang ransomware, jenis dan teknik mitigasi atau praktik terbaik. Sebagai masalah kebijakan, NCSC menyatakan bahwa masalah melakukan pembayaran sepenuhnya terserah pada korban, namun, mendorong untuk tidak melakukannya karena alasan yang sama untuk mendorong penyebaran lebih lanjut dan meningkatkan kepercayaan penyerang yang disebutkan sebelumnya. Situs web ini juga berisi tautan bagi korban untuk melaporkan serangan ransomware dan memberikan detail yang relevan dari kejahatan dunia maya.

Secara keseluruhan, semakin banyak perusahaan keamanan dan organisasi komersial juga berpartisipasi secara aktif dan menciptakan sumber daya online, halaman wiki, dan FAQ yang bermanfaat untuk membantu pengguna dalam memahami dan menangani ransomware.

VI. CKESIMPULAN

Keseriusan ancaman ransomware terhadap individu dan bisnis tidak dapat disangkal terutama mengingat hype baru-baru ini yang diciptakan oleh bentuk kejahatan dunia maya baru-baru ini. Sementara teknik dan skema dasar yang digunakan untuk ransomware telah ada selama lebih dari satu dekade, semakin banyak perangkat pengguna yang mendukung Internet telah menciptakan vektor serangan baru bagi para pelakunya. Makalah ini memberikan klasifikasi vektor serangan ransomware di sepanjang cara penyebaran serangan serta cara pembayaran. Selanjutnya, strategi mitigasi dipertimbangkan secara rinci untuk membantu pengguna melawan ancaman ransomware dan teknik pemulihan yang tersedia jika serangan berhasil juga dibahas. Tercatat bahwa kunci untuk mengurangi atau mengurangi jumlah serangan ransomware yang berhasil secara langsung berkaitan dengan tingkat kesadaran pengguna yang tinggi dan respons yang tepat. Sumber daya online utama yang disediakan oleh lembaga penegak hukum juga dirinci dengan tujuan untuk membantu pengguna dalam memperluas pengetahuan mereka tentang ransomware. Diperkirakan bahwa evolusi masa depan perangkat yang terhubung ke Internet, terutama penyertaan Internet of Things (IoT), tingkat pengetahuan pengguna yang memadai, alat keamanan yang efektif, dan ketersediaan sumber daya online yang tepat waktu diperlukan untuk meminimalkan ancaman yang ditimbulkan oleh serangan ransomware.

REFERENSI

[1] N. Hampton dan ZA Baig, “Ransomware: Munculnya ancaman pemerasan dunia maya,” 2015.

[2] “AVAST, 'Alat Dekripsi Ransomware Gratis'.,”*https://www.avast.com/ransomware-decryption-tools*. .

[3] K. Zetter, *Kamus peretas: Panduan untuk Ransomware, peretasan menakutkan yang sedang naik daun*. Diperoleh dari Keamanan, https://www. kabel. com/ 2015/09/hacker-lexicon-guideransomware-scary-hack-thats-rise, 2015.

[4] F. Mercaldo, V. Nardone, A. Santone, dan CA Visaggio, “Ransomware mencuri telepon Anda. metode formal menyelamatkannya,” dalam*Konferensi Internasional tentang Teknik Formal untuk Objek, Komponen, dan Sistem Terdistribusi*, 2016, hlm. 212–221.

[5] MHU Salvi dan MRV Kerkar, “Ransomware: Pemerasan dunia maya,”*ASIA J. Konvergen. teknologi. Daftar AJCT-UGC.*, jilid. 2, 2016.

[6] “McAfee, 'LeakerLocker: Ransomware Seluler Bertindak Tanpa Enkripsi.'” .

[7] “Philip B., 'Waspadalah terhadap LeakerLocker: Ransomware yang Mengunci Ponsel Anda.'” .

[8] S. Nakamoto, *Bitcoin: Sistem uang elektronik peer-to-peer*. 2008.

[9] J. Hernandez-Castro, E. Cartwright, dan A. Stepanova, “Analisis Ekonomi Ransomware,” 2017.

[10] Symantec, “ISTR: Laporan Ancaman Keamanan Internet,” 22, April 2017.

[11] MalwareBytes Lab, “'Laporan Status Malware,'” 2017.

[12] S.Cobb, *RoT: Ransomware of Things*. Tren, 2017.

[13] TA Mattei, “Privasi, Kerahasiaan, dan Keamanan Informasi Perawatan Kesehatan: Pelajaran dari Serangan Cyber WannaCry Terbaru,” *Bedah Saraf Dunia.*, jilid. 104, hlm. 972–974, 2017.

[14] “Buletin Virus: Publikasi Internasional Resmi tentang Pencegahan, Pengenalan, dan Penghapusan Virus Komputer. Abingdon, Inggris: Virus Bulletin, 1900. Cetak.,” 2005.

[15] J. Jouhal, “Munculnya ransomware dan cara menghindari sandera. New Statesman, Spotlight on cybersecurity,” Feb. 2017.

[16] R. Richardson dan M. North, “Ransomware: Evolusi, Mitigasi, dan Pencegahan,” *Int. Kelola. Putaran.*, jilid. 13, tidak. 1, hal. 10, 2017.

[17] A. Kharraz, W. Robertson, D. Balzarotti, L. Bilge, dan E. Kirda, “Cutting the gordian knot: A look under the hood of ransomware attacks,” di *Konferensi Internasional tentang Deteksi Intrusi dan Malware, dan Penilaian Kerentanan*, 2015, hlm. 3–24.

[18] J. Wyke dan A. Ajjan, “Kondisi Ransomware Saat Ini,” *Teknologi SophosLabs. pap.*, 2015.

[19] K. Savage, P. Coogan, dan H. Lau, “Evolusi ransomware,”*Pemandangan Gunung Symantec*, 2015.

[20] D. McCoy, K. Bauer, D. Grunwald, T. Kohno, dan D. Sicker, “Bersinar terang di tempat gelap: Memahami jaringan Tor,” di *Simposium Internasional tentang Simposium Teknologi Peningkatan Privasi*, 2008, hlm. 63–76.

[21] “ISTR ransomware & bisnis 2016.”

[22] L. Abrams, “Philadelphia Ransomware menawarkan Tombol Rahmat untuk Penjahat yang Penuh Kasih,” *https://www.bleepingcomputer.com/news/security/the-philadelphiaransomware-offers-a-mercy-button-for-compassionate-criminals/*. .

[23] L. Abrams, “Bleeping Computer, 'Star Trek Bertema Kirk Ransomware Membawa kita Monero dan Spock Decryptor!,'” *https://www.bleepingcomputer.com/news/security/star-trek-themedkirk-ransomware-brings-us-monero-and-a-spock-decryptor/*. .

[24] Panda Security, “Doxware, Evolusi Baru yang Menakutkan dari Pembajakan Digital.”

http://www.pandasecurity.com/mediacenter/security/doxware-evolutiondigital-hijacking/. .

[25] A. B, SGVB, V. A, dan S. H, “Ransomware: Ancaman yang Meningkat dari Pemerasan Digital zaman baru,” *India J.Sci. teknologi.*

[26] MJ Sheehan, R. Cheng, dan D. Gray, "Serangan Ransomware menghadirkan ancaman yang berkembang," *Kelola. Kesehatanc. eksekutif*, jilid. 26, hal. 7, 2016.

[27] “Peringkasan Kit Eksploitasi Ransomware Proofpoing.” .

[28] J. Wyke, "Bonet zeroaccess: Penambangan dan penipuan untuk keuntungan finansial besar-besaran," *Teknologi Sophos. pap.*, 2012.

[29] Kafeine, “'Crypto Ransomware' CTB-Locker (Critroni.A) sedang naik daun'.” 2014.

[30] IM Shohet dan S. Lavy, “Manajemen fasilitas kesehatan: tinjauan mutakhir,” *Fasilitas*, jilid. 22, tidak. 7/8, hlm. 210–220, 2004.

[31] “Ransomware: Menguntungkan bagi Penjahat, Sulit Dihentikan untuk Perusahaan, Citrix,” *https://www.citrix.com/blogs/2016/06/15/ransomwareprofitable-for-criminals-hard-to-stop-for-enterprises/*. .

[32] X. Luo dan Q. Liao, “Pendidikan kesadaran sebagai kunci pencegahan ransomware,” *Inf. Sistem Aman.*, jilid. 16, tidak. 4, hlm. 195–202, 2007.

[33] “Jaringan Pembayaran Inovatif Bitcoin dan Jenis Uang Baru,”*https://bitcoin.org/en/*. .

[34] “CoinDesk pada Survei Citrix, saham BTC di bisnis Inggris,”*http://www.coindesk.com/survey-uk-bitcoin-ransomware/*. .

[35] C. Van Alstin, “Ransomware: Ini menakutkan seperti kedengarannya. Tetapi dengan praktik terbaik keamanan, Anda dapat melawan.”*Manajer Kesehatan. teknologi.*, jilid. 37, tidak. 4, hal. 26, 2016.

[36] T. Yang, Y. Yang, K. Qian, DC-T. Lo, Y. Qian, dan L. Tao, “Deteksi dan analisis otomatis untuk ransomware android,” di*Komputasi dan Komunikasi Kinerja Tinggi (HPCC), Simposium Internasional IEEE 7 tahun 2015 tentang Keamanan dan Keamanan Dunia Maya (CSS), Konferensi Internasional IEEE ke-12 tahun 2015 tentang Perangkat Lunak dan Sistem Tertanam (ICESS), Konferensi Internasional ke-17 IEEE 2015 tentang*, 2015, hlm. 1338–1343.

[37] “Polisi memperingatkan pesan pemerasan yang dikirim atas nama mereka,” *Helsingin Sanomat*, 09-Mar-2016.

[38] AL Young dan M. Yung, “Kriptovirologi: Kelahiran, pengabaian, dan ledakan ransomware,” *komuni. ACM*, jilid. 60, tidak. 7, hlm. 24-26, 2017.

[39] G. Rhoades, “Ransomware dan malware lainnya,” *Pengindeks*, jilid. 34, tidak. 3, hlm. 126–128, 2016.

[40] S. Mustaca, “Apakah profesional TI Anda siap menghadapi tantangan yang akan datang?,” *Hitung. Penipuan Aman.*, jilid. 2014, tidak. 3, hlm. 18–20, 2014.

[41] PR DeMuro, “Menjaga Perompak Internet di Teluk: Negosiasi Ransomware di Industri Perawatan Kesehatan,” *Nova Rev*, jilid. 41, hal. 349, 2016.

[42] DP Pathak dan YM Nanded, “Tren kejahatan dunia maya yang berbahaya: tantangan pertumbuhan ransomware,” *Int. J. Adv. Res. Hitung. Ind. teknologi. IJARCET Vol.*, jilid. 5, 2016.

[43] “Apa yang harus dilakukan jika file Anda rusak atau diganti namanya oleh ransomware.” .

[44] S. Mohurle dan M. Patil, “Sebuah studi singkat tentang ancaman wannacry: serangan Ransomware 2017,” *Int. J.*, jilid. 8, tidak. 5, 2017.

[45] N. Scaife, H. Carter, P. Traynor, dan KR Butler, “Cryptolock (dan lepaskan): menghentikan serangan ransomware pada data pengguna,” di *Sistem Komputasi Terdistribusi (ICDCS), Konferensi Internasional ke-36 IEEE 2016 tentang*, 2016, hlm. 303–312.

[46] A. Continella *dkk.*, “Shieldfs: sistem file yang dapat menyembuhkan diri sendiri, sadar akan ransomware,” di *Prosiding Konferensi Tahunan ke-32 tentang Aplikasi Keamanan Komputer*, 2016, hlm. 336–347.

[47] “B-Aman. 'Keadaan Keamanan Cyber.'” .

[48] “McAfee Labs. Memahami Ransomware dan Strategi untuk Mengalahkannya.” .

[49] GV Cormack dan lainnya, "Pemfilteran spam email: Tinjauan sistematis," *Ditemukan. Trends® Inf. Retr.*, jilid. 1, tidak. 4, hlm. 335–455, 2008.

[50] DF Sittig dan H. Singh, “Pendekatan sosio-teknis untuk mencegah, mengurangi, dan memulihkan dari serangan ransomware,” *aplikasi klinik Memberitahukan.*, jilid. 7, tidak. 2, hal. 624, 2016.

[51] FBI, “Apa itu Ransomware dan apa yang harus dilakukan?,”*https://www.fbi.gov/news/stories/incidents-of-ransomware-ontherise/incidents-of-ransomware-on-the-rise*. .

[52] “T. Dewan. 'Teslacrypt bergabung dengan bidang ransomware.'” .

[53] JA Sherer, ML McLellan, ER Fedeles, dan NL Sterling, “Pertimbangan Praktis dan Hukum Ransonware untuk Menghadapi Mesin Ekonomi Baru dari Web Gelap,” *Kaya JL Tech*, jilid. 23, hal. 1, 2016.

[54] “H. weisbaum. Penjahat CryptoLocker meluncurkan situs 'layanan pelanggan'.” 2013.

[55] “Tidak Ada Lagi Proyek Ransomware,”*https://www.nomoreransom.org/en/about-the-project.html*. .

[56] “Informasi Ransomware FBI,”*https://www.fbi.gov/news/stories/incidents-of-ransomware-on-the-rise*. .

[57] “Pusat Pengaduan Kejahatan Internet (IC3),” *https://www.ic3.gov/media/2016/160915.aspx*

[58] “Pusat Keamanan Cybercrime Nasional (NCSC, Inggris),”*https://www.ncsc.gov.uk/guidance/protecting-your-organisationransomware*. .