Jurnal ICT : Information Communication & Technology
Vol. 21, No.1, Juli 2021, pp. 42-52
p-ISSN: 2302-0261, e-ISSN: 2303-3363, DOI:

Mitigasi Ancaman Resiko Keamanan Siber Di Masa Pandemi Covid-19

Yudi Herdiana[1*], Zen Munawar[2], Novianti Indah Putri[3]
[1,3]Program Studi Teknik Informatika, Universitas Bale Bandung (UNIBBA), Indonesia
[2]Program Studi Manajemen Informatika, Politeknik LP3 Bandung, Indonesia
Email: [1]ydherdn@gmail.coml, [2]munawarzen@gmail.com, [3]noviantiindahputri2021@gmail.com

INFORMASI ARTIKEL

Histori artikel:

Naskah masuk, 9 Maret 2021
Direvisi, 18 April 2021
Diiterima, 21 April 2021

Kata Kunci:

Keamanan Komputer, Sistem Komputer, Pendemi COVID-19, Keamanan Siber

ABSTRAK

Abstract- Cybersecurity mitigation is needed as protection from theft and interference with information systems, software and hardware. The increasing anxiety caused by the pandemic increases the likelihood that cyberattacks will succeed as the number and range of cyberattacks increases. The increasing rate of cyberattacks has a wider impact. This research studies cybersecurity issues that occurred during the Covid-19 pandemic. This research analyzes the current conditions and the actions of cybercrime as well as attacks types of cyber attacks. This research has also provided various practical approaches to cyber attack risk mitigation for organizations. It is important for organizations to improve the protection of their critical data and assets by adopting a comprehensive approach to cybersecurity. In the conclusion section, techniques for detecting and avoiding these threats even after a pandemic are recommended are presented so that the damage caused by cybercrime can be reduced. For future research, cybersecurity needs to be developed with the latest technology integration, such as Artificial Intelligence, Blockchain, Internet of Things, and many more.

Abstrak- Mitigasi keamanan siber diperlukan sebagai perlindungan dari pencurian dan gangguan pada sistem informasi, perangkat lunak dan perangkat keras. Meningkatnya kecemasan yang disebabkan oleh pandemi meningkatkan kemungkinan serangan siber berhasil sesuai dengan peningkatan jumlah dan jangkauan serangan siber. Peningkatan tingkat serangan siber memiliki dampak yang lebih luas. Penelitian ini mempelajari masalah keamanan siber yang terjadi selama masa pandemi Covid-19. Penelitian ini menganalisis kondisi saat ini dan tindakan kejahatan siber serta serangan jenis serangan siber secara. Penelitian ini juga telah menyediakan berbagai pendekatan praktis mitigasi risiko serangan siber untuk organisasi. Penting bagi organisasi untuk meningkatkan perlindungan data dan aset penting mereka dengan menerapkan pendekatan komprehensif terhadap keamanan siber. Pada bagian kesimpulan, disampaikan beberapa teknik untuk mendeteksi dan menghindari ancaman ini bahkan setelah pandemi direkomendasikan sehingga kerusakan yang disebabkan oleh kejahatan siber dapat dikurangi. Untuk penelitian di masa depan, keamanan siber perlu dikembangkan dengan integrasi teknologi terkini, seperti *Artificial Intelligence*, *Blockchain*, *Internet of Things*, dan masih banyak lagi.

Jurnal ICT : Information Communication & Technology p-ISSN: 2302-0261
Vol. 20, N0.1, Juli 2021, pp. 42-52 e-ISSN: 2303-3363

***Penulis Korespondensi**:*

Yudi Herdiana
Program Studi Teknik Informatika,
Universitas Bale Bandung
Jl. Raden AA Wiranatakusumah No.7, Baleendah, Kec. Baleendah, Bandung, Indonesia
Email: ydherdn@gmail.com

1. Pendahuluan

Hampir seluruh dunia saat ini sedang dilanda salah satu wabah penyakit terbesar abad ini. Wabah Covid-19 yang dinyatakan sebagai pandemi oleh Organisasi Kesehatan Dunia atau WHO telah mempengaruhi kehidupan individu, organisasi, dan masyarakat luas. Wabah virus corona telah dan masih berdampak pada semua industri, termasuk penggunaan teknologi informasi dan komunikasi [1]. Akibat krisis ini, banyak karyawan sekarang mengandalkan ponsel, laptop, dan akses internet untuk bekerja dari jarak jauh dari rumah. Selain itu, sebagian besar bisnis sekarang dilakukan secara online untuk mengurangi interaksi fisik. Sektor kesehatan tidak ketinggalan dengan peningkatan telekonsultasi dan manajemen jarak jauh. Sebagian besar sekolah telah beralih ke digital untuk memastikan pembelajaran tidak terganggu. Semua kondisi ini telah menyebabkan peningkatan mendadak dalam penggunaan teknologi internet dan secara tidak langsung meningkatkan kejahatan komputer di siber.

Keamanan bukan hanya jenis "*set and forget*" masalah, keamanan yang efektif melibatkan analisis menyeluruh, implementasi, emmperbaharui dan memantau [2]. Penjahat siber telah memanfaatkan kesempatan untuk menyerang individu dan organisasi untuk melakukan banyak kejahatan menggunakan berbagai teknik. Penelitian ini memberikan gambaran tentang berbagai ancaman keamanan komputer yang dilakukan selama pandemi COVID-19 dan melakukan analisis dan solusi terkait keamanan komputer. Solusi dilakukan dengan beberapa teknik untuk mendeteksi dan menghindari ancaman ini bahkan setelah pandemi direkomendasikan sehingga kerusakan yang disebabkan oleh kejahatan komputer siber dapat dikurangi.

Pandemi COVID-19 telah menciptakan ketidakpastian, kecemasan, dan perubahan drastis terkait gaya hidup kita. Organisasi harus beradaptasi dengan permintaan untuk bekerja jarak jauh dengan kecepatan dan skala. Banyak yang terpaksa mengubah kantor fisik mereka dan kebijakan yang dibuat dengan panik untuk memungkinkan karyawan bekerja dari rumah tanpa pelatihan yang diperlukan atau pengaturan yang disiapkan dengan baik. Sebagian besar perusahaan dan institusi ini tidak memiliki rencana di lapangan untuk memfasilitasi perubahan drastis dan mendadak ini dalam waktu singkat [3]. Faktanya, hanya 38% bisnis yang memiliki kebijakan keamanan siber [3]. Dengan berpindah ke lingkungan online, organisasi dan perusahaan di seluruh dunia telah menerapkan model bisnis work-from-home (WFH) yang meningkatkan vektor serangan dan risiko pada data internal. Perlu dicatat bahwa WFH telah menjadi normal baru bagi orang-orang di seluruh dunia. Dalam sebagian besar skenario, ini menyiratkan persyaratan karyawan untuk menggunakan perangkat pribadi dan jaringan rumah mereka sendiri, yang sebagian besar sifatnya tidak aman dan tidak memiliki standar keamanan industri yang diperlukan. Ada banyak faktor yang mengancam keamanan jaringan komputer, yang dapat dibagi menjadi faktor subyektif dan faktor obyektif [4]. Untuk institusi yang sudah menyediakan perangkat bisnis bagi karyawannya, ini biasanya dijamin dengan hak administratif minimal atau tanpa hak administratif. Sebaliknya, pengaturan umum di mana staf diberi hak sementara untuk menginstal perangkat lunak yang diperlukan menjadi masalah. Karenanya, bisnis perlu memberikan solusi yang lebih realistis dan memberi karyawan lebih banyak hak, yang secara tidak langsung menyiratkan lebih banyak potensi masalah keamanan. Keamanan siber selama pandemi penyakit coronavirus 2019 (Covid-19) adalah masalah yang benar-benar mengkhawatirkan karena munculnya ancaman siber dan insiden keamanan yang menargetkan orang-orang dan sistem yang rentan secara global [5]. Penelitian ini berfokus pada mityigasi keamanan siber yang muncul di berbagai lingkungan di masa pandemi. Oleh karena itu, sangat menantang bagi organisasi untuk mengembangkan tindakan mitigasi keamaman siber.

2. Tinjauan Pustaka

Dengan adopsi teknologi digital yang luas, banyak aspek masyarakat telah beralih ke online, dari belanja dan interaksi sosial ke bisnis, industri, dan sayangnya, juga kejahatan. Karena sifatnya yang menguntungkan dan tingkat risikonya yang rendah karena penjahat siber dapat meluncurkan serangan dari mana saja di seluruh dunia, jelas bahwa kejahatan siber akan tetap ada [6].

Kejahatan siber, sebagai kejahatan tradisional, sering digambarkan dengan segitiga kejahatan [7],

yang menentukan bahwa untuk kejahatan siber terjadi, tiga faktor harus ada: korban, motif dan peluang. Korban adalah sasaran serangan, motifnya adalah aspek yang mendorong penjahat untuk melakukan serangan, dan peluang adalah kesempatan untuk melakukan kejahatan, misalnya, dapat berupa kerentanan bawaan dalam sistem atau perangkat yang tidak dilindungi.

Maka jelaslah bahwa para penyerang berusaha memanfaatkan gangguan yang disebabkan oleh pandemi, terutama mengingat gangguan itu terus berlanjut. Panduan ini sangat penting untuk mengurangi ancaman yang meningkat, tetapi untuk memperkuat dasarnya, pertama-tama perlu ada pemahaman inti tentang serangan siber yang diluncurkan. Bahkan dalam keadaan normal, kejahatan online seperti penipuan memberikan hasil yang lebih baik dengan risiko paling kecil bagi penyerang. Melihat fakta tersebut, semakin banyak orang yang menganggur, menghabiskan lebih banyak waktu di rumah dan menggunakan Internet untuk bekerja dan bersosialisasi.

Selain itu, pemerintah telah memberikan insentif untuk membantu orang secara finansial dan begitu juga bisnis lain untuk berusaha menarik atau mempertahankan pelanggan. Seiring dunia mengantisipasi potensi obat untuk mengendalikan penyebaran Covid-19, semua informasi terkait Covid-19 akan menarik perhatian masyarakat. Para *scammer* memanfaatkan cara ini untuk mengirimkan serangan jahat [phi, smi, vi] shing3 kepada korban yang menyamar sebagai pemerintah, otoritas pajak. Dengan tautan untuk mengklaim bantuan terkait Covid-19.

Penipuan ini jauh lebih efektif sekarang selama pandemi karena sebagian besar orang yang rentan lebih cemas dan mengharapkan email, teks, panggilan. Yang berkaitan dengan Covid-19 dari pihak berwenang. Ketika penjahat siber menjadi lebih sadar akan situasi ini, jauh lebih mudah bagi mereka untuk membuat pesan palsu atau situs web yang meniru penampilan otoritas yang relevan dan akrab, memasukkan kata-kata yang menggunakan urgensi untuk mengeksploitasi faktor ketakutan yang dirasakan secara global karena pentingnya penanganan. keadaan darurat dan kebutuhan. Oleh karena itu, penjahat siber dapat meningkatkan efektivitas serangan phishing mereka. Serangan ini dapat datang dalam berbagai bentuk, seperti pembaruan internal dan eksternal, keuntungan pribadi, dan amal. Perlu disebutkan bahwa pelaku kejahatan dapat menggunakan materi asli yang ada sebagai umpan untuk mendorong orang melakukan tindakan berisiko seperti mengklik tautan atau membuka lampiran. Penting bagi pengguna untuk melihat pengirim email dan memeriksa tautan apa pun yang ada di dalamnya sebelum bertindak. Penjahat siber sering menggunakan teknik peniruan yang menyamar sebagai Organisasi Kesehatan Dunia (WHO), Perserikatan Bangsa-Bangsa (PBB) atau perusahaan populer sementara orang-orangnya adalah WFH, Zoom, untuk mengelabui pengguna agar mengeklik tautan atau membuka dokumen yang terinfeksi.

Sebagai akibat dari pandemi, kami telah melihat penguncian total di hampir semua bagian dunia. Pergeseran ke cara kerja baru di mana karyawan bekerja dari rumah terutama menggunakan sistem rumah mereka yang diamankan oleh pemberi kerja mereka telah menciptakan tingkat perhatian di dalam sektor ini. Berkat pengaturan karantina massal ini, tantangan baru yang berkaitan dengan ketahanan solusi teknologi untuk sebagian besar ekosistem menjadi penting; khususnya, ketahanan teknologi saat ini dalam infrastruktur siber pemberi kerja yang ada.

2.1 Serangan siber selama pandemi COVID-19

Serangan siber selama pandemi dapat dikategorikan menjadi tiga kategori: penipuan dan phishing, malware, dan penolakan layanan terdistribusi (DDoS). Contoh-contoh tertentu dari serangan siber selama pandemi. Pada bulan Maret 2020, Rumah Sakit Universitas Brno sebagai salah satu laboratorium penguji COVID-19 di negara Republik Ceko telah dilanda serangan siber berupa ransomware dan terpaksa ditutup seluruh jaringan IT [8]. Pada bulan Juni tahun 2020 di Jerman terjadi serangan email phishing ke eksekutif senior di perusahaan yang memasok pribadi alat pelindung pribadi (APD). Tautan phishing telah dirancang untuk mengarahkan eksekutif ke halaman login Microsoft palsu untuk mencuri kredensial mereka [9]. Penjahat siber dan Ancaman Persisten Tingkat Lanjut (APT) [10][11] kelompok meluncurkan serangan siber ke orang-orang dan organisasi yang rentan melalui penipuan dan phishing terkait Covid-19. Mereka memanfaatkan pandemi untuk berbagai motivasi, misalnya untuk keuntungan komersial atau untuk mengumpulkan informasi terkait vaksin Covid-19 dengan menerapkan berbagai teknik seperti phishing atau ransomware dan malware lainnya. Contoh aktivitas APT selama pandemi termasuk Hades, Patchwork (alias Dropping Elephant, APT-C-09), TA5058, dan APT299.

Penipuan dan *Phishing*: Serangan paling umum dan efektif selama pandemi ini adalah melalui berbagai jenis penipuan dan *phishing* [12] [13].

Faktanya, serangan phishing memiliki tingkat keberhasilan 30% atau lebih tinggi. Sangat meresahkan bahwa penyerang hanya membutuhkan persentase kecil klik untuk mendapatkan keuntungan finansial atau kepentingan lainnya. Oleh karena itu, mengirimkan jutaan email kepada para korban yang ingin mengajukan bantuan dana yang disediakan oleh pemerintah., akan menghasilkan imbalan yang cepat dan sangat besar. Ada berbagai serangan phishing (email, SMS, suara) yang menargetkan orang dan sistem yang rentan menggunakan virus corona atau COVID-19 sebagai judul untuk memikat orang [12][13]. Terdapat peningkatan 600% serangan email phishing terkait virus corona pada Q1 2020 [14]. Penjahat siber juga menggunakan teknik yang lebih canggih untuk memikat korban seperti menggunakan protokol enkripsi HTTPS di situs web mereka. Faktanya, sekitar 75% situs phishing telah dilengkapi dengan SSL [13]. Selain itu, pengguna webmail dan Software-as-a-Service (SaaS) adalah sektor phishing yang paling ditargetkan [13].

Malware: Malware termasuk virus komputer, worm, Trojan horse, spyware, dan ransomware [15]. Selama pandemi, penjahat siber dan kelompok APT telah mengambil keuntungan dalam menargetkan orang dan sistem yang rentan dengan menyebarkan berbagai jenis malware melalui email dan situs web. Faktanya, 94% komputer yang dirusak oleh malware telah terinfeksi oleh email.

3. Serangan Siber

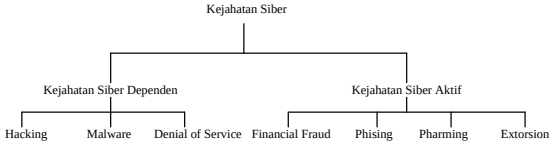
Insiden kejahatan siber yang muncul dari pandemi Covid-19 menimbulkan ancaman serius bagi keselamatan dan ekonomi global populasi dunia, oleh karena itu memahami mekanisme mereka, serta penyebaran dan jangkauan ancaman ini sangat penting. Banyak solusi telah diusulkan dalam literatur untuk menganalisis bagaimana peristiwa tersebut terungkap mulai dari definisi formal hingga pendekatan sistemik yang meninjau sifat ancaman [16] [17]. Meskipun pendekatan ini memungkinkan kategorisasi serangan, namun seringkali tidak memiliki kemampuan untuk memetakan peristiwa yang lebih besar dan terdistribusi seperti yang disajikan dalam manuskrip ini, di mana banyak peristiwa yang berasal dari pandemi, namun tidak terkait. Untuk tujuan ini, dipilih visualisasi temporal, memungkinkan untuk memetakan peristiwa tanpa mengorbankan narasinya [18]. Selain itu, jenis visualisasi ini digunakan di seluruh domain keamanan siber untuk mewakili serangan siber yang diakibatkan [19].

Tabel 1. Contoh Serangan Siber di Masa Pandemi

No	Jenis Serangan	Negara	Ref
1	P.M	Cina	[20]
2	H	Czech	[21]
3	P.M.F	Filipina	[22]
4	P	Amerika	[23]

Ket : Phishing(P), Malware (M), Hacking(H), Financial fraud(F)

Penting juga untuk dicatat bahwa serangan siber mungkin pertama kali ditampilkan di domain ini, sebelum disorot oleh outlet media arus utama. Berkenaan dengan penyertaan laporan berita ke dalam tabel serangan dan *timeline* berikutnya, harus diakui bahwa serangan ini disajikan melalui lensa jurnalistik, dan dengan demikian dapat ditulis dalam upaya untuk menjadi berita utama. Namun demikian, serangan siber yang dilaporkan ini masih menjadi ancaman nyata bagi masyarakat umum selama pandemi Covid-19. *Timeline* berupaya memberikan gambaran umum tentang serangan yang telah terjadi.



Gambar 1. Kejahatan Siber Dependen dan Aktif

Definisi ini mencakup keamanan siber secara default dan telah mengilhami banyak definisi internasional tentang kejahatan siber. Kejahatan yang bergantung pada siber adalah pelanggaran, "yang hanya dapat dilakukan dengan menggunakan komputer, jaringan komputer, atau bentuk lain dari teknologi informasi komunikasi [24]. Kategori ini serta contoh subkategori mereka dapat dilihat pada Gambar 1. Beberapa elemen yang dijelaskan oleh CPS sering saling terkait dalam serangan siber. Misalnya, email atau pesan teks phishing, misalnya SMS atau WhatsApp dapat digunakan untuk memikat korban ke situs web penipuan. Situs web tersebut kemudian dapat mengumpulkan data pribadi yang digunakan untuk melakukan penipuan finansial, atau mungkin menginstal malware, lebih khusus lagi, ransomware yang kemudian digunakan untuk melakukan pemerasan. Demikian pula serangan Denial of Service (DoS) semakin banyak digunakan oleh penjahat siber untuk mengalihkan bisnis selama upaya peretasan [25] [26]. Berikut ini, perlu mempertimbangkan jenis serangan ini dan merefleksikan bagaimana serangan itu diluncurkan, termasuk faktor manusia atau aspek teknis (misalnya, kerentanan) yang mereka coba eksploitasi.

Phishing, atau Social Engineering secara lebih luas, mencakup upaya pihak tidak sah untuk meyakinkan individu agar melakukan tindakan, misalnya, berbagi informasi atau mengunjungi situs web dengan dalih bahwa mereka terlibat dengan pihak

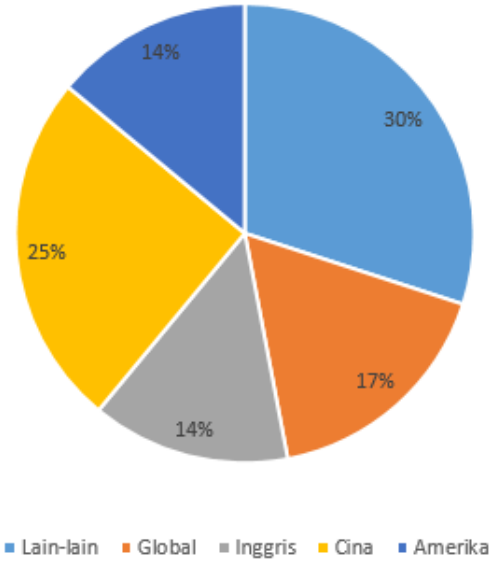
yang sah. Cukup sering pesan email digunakan, terkadang pesan SMS atau WhatsApp digunakan sering disebut sebagai smishing. Pharming mirip dengan phishing, tetapi alih-alih menipu pengguna untuk mengunjungi situs berbahaya, penyerang mengandalkan sistem yang menyusup, misalnya perangkat pengguna atau server DNS untuk mengarahkan individu ke situs tidak sah. Jenis serangan ini kurang umum secara umum, karena memerlukan lebih banyak akses atau kemampuan teknis. Penipuan finansial umumnya melibatkan penipuan individu atau organisasi dengan menggunakan teknologi untuk keuntungan finansial bagi penyerang atau penjahat.

Pemerasan mengacu pada tindakan yang memaksa, mengancam, atau memaksa individu untuk melakukan beberapa tindakan, paling umum, mengeluarkan uang. Serangan Peretasan, Malware, dan Denial of Service (DoS) adalah bentuk kejahatan yang sering disukai oleh penyerang yang lebih teknis. Peretasan melibatkan kompromi terhadap kerahasiaan atau integritas sistem, dan membutuhkan keterampilan yang wajar; tekniknya dapat melibatkan eksploitasi kerentanan sistem untuk membobol sistem.

Malware mengacu pada perangkat lunak berbahaya dan dapat digunakan untuk mengganggu layanan, mengekstrak data, dan berbagai serangan lainnya. Ransomware adalah salah satu jenis malware yang paling umum saat ini [27], dan menggabungkan malware dengan percobaan pemerasan. DoS menyerang ketersediaan sistem target dan bekerja dengan membanjiri layanan utama dengan permintaan yang tidak sah. Tujuannya di sini adalah untuk menggunakan *bandwidth* yang digunakan untuk permintaan *server* yang sah, dan pada akhirnya memaksa *server offline*.

Jenis serangan ini memberikan dasar untuk analisis kami dalam garis waktu dan bagaimana kami mendekati diskusi kami di bagian selanjutnya dari penelitian ini. Tabel 1 menjelaskan sejumlah serangan siber. Serangan siber telah diatur berdasarkan tanggal serangan. Jika tanggal penyerangan tidak tersedia dalam referensi, maka tanggal artikel telah digunakan. Negara target dari setiap serangan siber telah terdaftar, bersama dengan deskripsi singkat tentang metode yang terlibat.

Gambar 2 memberikan ringkasan negara-negara yang menjadi target serangan siber awal selama pandemi, yang diatur berdasarkan tanggal serangan. Seperti yang ditunjukkan, China dan AS menyumbang 39% dari serangan yang dilaporkan. Untuk lebih meningkatkan kemungkinan keberhasilan serangan phishing, penjahat siber telah diidentifikasi mendaftarkan sejumlah besar domain situs web yang berisi kata 'covid' dan 'coronavirus' [28]. Domain semacam itu kemungkinan besar dapat dipercaya, dan oleh karena itu diakses, terutama jika dipasangkan dengan kata-kata terkemuka seperti WHO atau Pusat Pengendalian dan Pencegahan Penyakit atau kata-kata kunci , misalnya, Corona-virusapps.com, anticovid19-pharmacy.com, yang telah disorot seperti yang digunakan [29]. Platform komunikasi, seperti Zoom, Microsoft dan Google, juga telah ditiru, baik melalui email dan nama domain [28].



Gambar 2. Distribusi serangan siber lintas negara

Ini patut diperhatikan mengingat fakta bahwa ini adalah teknologi utama yang digunakan oleh jutaan orang di seluruh dunia untuk berkomunikasi, baik untuk bekerja maupun bersenang-senang. Fakta-fakta ini, dikombinasikan dengan email manipulasi psikologis yang meyakinkan, pesan teks dan tautan, menyediakan beberapa jalan penting bagi penjahat untuk menyerang. Serangan Pharming jauh lebih jarang tetapi terjadi pada 13% kasus. Seperti yang dapat dilihat pada Tabel 1, serangan ini sering terjadi bersamaan dengan serangan lainnya.

Penipuan yang diilhami Covid-19 telah memanfaatkan pengumuman pemerintah / ilmiah untuk mengeksploitasi kecemasan pengguna dan mencari keuntungan finansial. Dari hasil analisis, penipuan biasanya dilakukan melalui phishing dan serangan email juga dapat melihat ini dalam urutan kami di atas. Dalam satu kasus, penjahat menyamar dalam email dan dengan sopan meminta sumbangan untuk mengembangkan vaksin, dan juga pembayaran apa pun dilakukan dalam Bitcoin [30]. Teknik phishing yang umum digunakan, tetapi pada kesempatan ini termasuk permintaan uang: “Pendanaan untuk proyek di atas membutuhkan biaya yang cukup besar dan kami memohon atas niat baik Anda untuk berdonasi, tidak ada yang terlalu kecil”. Poin penting tentang serangan khusus ini adalah bahwa ia juga meminta penerima untuk berbagi pesan dengan sebanyak mungkin orang. Hal ini mengkhawatirkan karena orang lebih cenderung

mempercayai email yang mereka yakini telah diperiksa oleh orang terdekat [31].

Ada berbagai upaya penipuan lainnya, sebagian besar didasarkan pada ancaman atau banding. Misalnya, analisis kami mengidentifikasi penawaran investasi di perusahaan yang mengklaim mencegah, mendeteksi, atau menyembuhkan Covid-19, dan investasi dalam skema / opsi perdagangan yang memungkinkan pengguna memanfaatkan kemungkinan penurunan ekonomi yang didorong Covid-19 [32]. Serangan pemerasan disaksikan dalam analisis kami tetapi kurang lazim (muncul hanya dalam 13% kasus) dibandingkan dengan yang lain di atas. Kasus paling menonjol dari serangan ini adalah email pemerasan yang mengancam akan menginfeksi penerima dan anggota keluarganya dengan Covid-19 kecuali pembayaran Bitcoin dilakukan [33]. Untuk meningkatkan kepercayaan pesan, itu termasuk nama individu dan salah satu kata sandinya (kemungkinan dikumpulkan dari pelanggaran kata sandi sebelumnya). Setelah menuntut uang, pesan tersebut selanjutnya berbunyi: "Jika saya tidak mendapatkan pembayaran, saya akan menulari setiap anggota keluarga Anda dengan virus corona". Ini mencoba menggunakan rasa takut untuk memotivasi individu agar membayar, dan menggunakan sandi (yaitu, item yang bersifat pribadi) untuk membangun kepercayaan pada pesan penjahat.

Malware yang terkait dengan Covid-19 semakin menonjol selama pandemi dan memengaruhi individu serta organisasi di seluruh dunia. Serangan malware yang tersisa adalah varian dari malware yang ada, khususnya, adalah ancaman penting dan contohnya adalah COVIDLock, aplikasi Android yang menyamar sebagai peta panas yang bertindak sebagai ransomware; pada dasarnya mengunci layar pengguna kecuali uang tebusan telah dibayarkan [34].

Di tingkat organisasi, ransomware telah berdampak signifikan pada layanan perawatan kesehatan — bisa dibilang sebagai komponen paling rapuh dari infrastruktur nasional penting suatu negara saat ini. Serangan telah dilaporkan di Amerika Serikat, Prancis, Spanyol dan Republik Ceko [35] [36], dan menggunakan ransomware seperti Netwalker. Serangan semacam itu sesuai dengan modus operandi kriminal jika kita berasumsi bahwa pelaku kejahatan akan menargetkan wilayah yang mereka yakini akan dimanfaatkan untuk memanfaatkan serangan mereka; yaitu, organisasi kesehatan mungkin lebih cenderung membayar uang tebusan untuk menghindari hilangnya nyawa pasien. Menariknya, sejak ada janji dari geng kejahatan siber terkemuka bahwa mereka tidak akan (atau berhenti) menargetkan layanan kesehatan. Dalam satu laporan, menekankan bahwa tidak biasanya menargetkan rumah sakit, atau bahwa mereka akan menghentikan sementara semua aktivitas terhadap layanan kesehatan sampai virus stabil [37].

Contoh malware terkenal lainnya selama pandemic : Corona Live 1.1, sebuah aplikasi yang memanfaatkan pelacak COVID-19 resmi yang dirilis oleh Universitas John Hopkins dan mengakses foto perangkat, video, data lokasi, dan kamera [38]. Saat pandemi berlanjut, kemungkinan akan ada lebih banyak jenis malware, menargetkan berbagai jenis bahaya, misalnya, fisik, keuangan, psikologis, reputasi (untuk bisnis) dan sosial [39].

Advanced Persistent Threat (APT) —beberapa di antaranya mungkin selaras dengan negara bagian diidentifikasi sebagai target perusahaan farmasi, organisasi penelitian medis, dan universitas yang terlibat dalam respons Covid-19. Tujuannya tidak selalu untuk mengganggu aktivitas mereka (seperti kasus ransomware), tetapi untuk mencuri data penelitian sensitif atau kekayaan intelektual (misalnya, tentang vaksin, perawatan).

Sementara analisis rinci dari serangan ini belum muncul, penyemprotan kata sandi (serangan brute-force yang menerapkan kata sandi yang umum digunakan dalam mencoba masuk ke akun) dan mengeksploitasi kerentanan di Jaringan Pribadi Virtual (VPN) telah ditandai [40].

4. Mitigasi Resiko

Mengurangi dan mencegah serangan siber bukanlah tugas yang sepele. Ada pendekatan praktis yang dapat mengurangi risiko serangan siber selama WFH [3] [12].

Pendidikan Pengguna: Keamanan hanya sekuat tautan terlemahnya. Orang-orang dianggap sebagai tautan terlemah di banyak sistem keamanan. Oleh karena itu, mengembangkan kesadaran keamanan siber di antara pengguna melalui pelatihan terus-menerus penting untuk mengurangi risiko serangan siber pada suatu organisasi. Sebuah studi baru-baru ini menunjukkan bahwa hanya 11% bisnis yang menyediakan keamanan siber [41].

Virtual PrivateNetwork (VPN): VPN adalah saluran komunikasi terenkripsi antara dua titik di Internet untuk melindungi data yang dikirim dan diterima. Penggunaan VPN untuk menjelajahi Internet adalah hal baru yang normal. VPN menyediakan dua aspek keamanan: kerahasiaan dan integritas dan memungkinkan organisasi untuk memperluas kebijakan keamanan kepada pekerja jarak jauh.

Aktifkan otentikasi multi-faktor (MFA): MFA memperkuat keamanan dengan meminta nama pengguna dan kata sandi ditambah kode sekali pakai yang dikirim ke ponsel melalui SMS atau aplikasi otentikasi. MFA merupakan faktor penting untuk mengurangi dugaan dan pencurian kata sandi seperti serangan siber *brute force*. Seorang karyawan yang mencoba mengakses jaringan perusahaannya dari rumah harus memberikan nama pengguna dan sandi serta kode sekali pakai yang dikirimkan ke ponselnya

untuk memverifikasi identitasnya sebelum diizinkan untuk mengakses jaringan internal.

Pastikan semua *firmware* perangkat adalah yang terbaru: Pastikan bahwa semua perangkat dan firmware perangkat / SO adalah yang terbaru dengan tambahan keamanan terbaru yang diterapkan untuk mengisolasi mereka terhadap kerentanan yang diketahui. Memastikan bahwa perangkat lunak *anti-malware* terbaru diaktifkan di semua perangkat yang terhubung ke jaringan: Penjahat siber menargetkan orang-orang yang rentan dengan menyebarkan berbagai jenis malware. Karena jutaan malware baru dan jenisnya dihasilkan setiap tahun, *anti-malware* reguler dan terbaru dapat mengurangi risiko serangan siber yang disebabkan oleh *malware.*

Aktifkan kebijakan *online* perusahaan yang kuat: Organisasi memiliki sedikit atau tidak ada waktu untuk mempersiapkan skenario WFH. Kebijakan WFH yang kokoh dan komprehensif diperlukan untuk melindungi data dan mencegah serangan siber. Kebijakan WFH yang kuat termasuk menghindari mengadakan percakapan kerja yang sensitif di depan umum, hanya menggunakan saluran konferensi video dan audio yang disetujui perusahaan, dll.

Kebijakan tersebut juga harus mencakup rencana pemulihan dan strategi cadangan yang kuat dan terbukti. Penting juga untuk menguji rencana ini secara rutin karena sebuah studi baru-baru ini menyoroti bahwa 46% bisnis hanya menguji rencana pemulihan dan pencadangan mereka setahun sekali atau kurang [42].

Segmentasi dan pemisahan: Menjauh dari perangkat dan jaringan tujuan tunggal "*all-in-one*". Bagilah jaringan menjadi beberapa zona tepercaya: jaringan kantor rumah (tingkat kepercayaan tinggi), jaringan hiburan tamu dan rumah (tingkat kepercayaan rendah) dan zona Internet (tidak tepercaya). Di rumah pintar, perangkat IoT harus diisolasi dalam jaringan Wi-Fi terpisah. Dengan mengisolasi perangkat IoT pada segmen jaringan terpisah, setiap penyusupan perangkat IoT tidak akan secara otomatis memberikan akses ke perangkat utama pengguna seperti laptop perusahaan.

Keamanan fisik kantor/ rumah: Penting untuk melindungi perangkat kantor rumah secara fisik. Pendekatan praktis termasuk memastikan bahwa perangkat kerja tidak dibiarkan begitu saja, menggunakan layar kunci atau mengunci laptop, selalu log off perangkat setelah digunakan, dll.

Pembaruan keamanan: Sangat penting untuk memastikan bahwa semua sistem dan titik akhir diperbarui dan ditambal secara teratur, misalnya untuk memastikan bahwa perangkat lunak anti-malware terbaru diaktifkan di semua perangkat dan titik akhir yang terhubung ke jaringan. Sebuah resiko penting yang perlu diperiksa adalah resiko keamanan [43].

Selain pendekatan mitigasi umum yang dibahas di atas, contoh mitigasi risiko keamanan terkait perawatan kesehatan diuraikan di bawah ini. Selama pandemi, organisasi perawatan kesehatan yang berurusan dengan COVID-19 telah menjadi target utama serangan siber yang terus-menerus. Organisasi perawatan kesehatan harus melindungi data dan aset berharga mereka dari serangan siber dengan meningkatkan pertahanan mereka. Dua komponen penting dalam mendeteksi perilaku jahat yang dapat membahayakan keamanan dan kepercayaan jaringan adalah sistem deteksi intrusi (IDS) dan insiden keamanan dan manajemen kejadian (SIEM).

Biasanya, IDS menggunakan deteksi anomali, analisis protokol stateful (alias inspeksi paket mendalam), pencocokan tanda tangan, atau kombinasi dari ketiga teknik (hybrid) untuk menganalisis serangan cyber yang masuk. Karena kemampuannya untuk mendeteksi serangan zero-day dengan lebih akurat, IDS deteksi anomali berbasis *Artificial Intelligence* semakin populer untuk mendeteksi serangan siber. Selain itu, penting bagi organisasi perawatan kesehatan untuk mengambil pendekatan komprehensif terhadap keamanan siber dan tidak memandang keamanan dari perspektif teknologi saja, tetapi dalam kerangka proses [44]. Contoh pendekatan komprehensif untuk keamanan siber termasuk Model Manajemen Ketahanan CERT (CERT-RMM) [45], manajemen risiko, dan memasukkan keamanan siber ke dalam perencanaan strategis dan proses penganggaran [44].

Organisasi perlu memprioritaskan ulang strategi keamanan siber mereka dan mengambil tindakan untuk meningkatkan pertahanan siber. Alih-alih terlalu berfokus pada proses bisnis penting yang mungkin memerlukan perhatian segera, organisasi juga harus memprioritaskan risiko siber untuk memastikan bahwa organisasi dapat memimpin bisnis yang tangguh di masa depan, setelah kekacauan pandemi telah diselesaikan.

Organisasi dapat mempertimbangkan beberapa langkah untuk membangun keamanan siber mereka dan mengatasi tantangan jangka pendek dan jangka panjang yang disebutkan di atas. Perusahaan harus memperkuat program intelijen ancaman dan mengintegrasikannya dengan aktivitas kritis lainnya, seperti pemantauan peristiwa keamanan. Organisasi juga harus memastikan penemuan kerentanan aktif dan perburuan ancaman. Selain itu, penting bagi organisasi untuk menjaga komunikasi proaktif dengan karyawan dan pihak ketiga untuk meningkatkan kesadaran tentang ancaman siber dan memastikan pencegahan ancaman tersebut. Libatkan tenaga kerja tentang implikasi keamanan bekerja dari dengan menjelaskan dan mendidik mereka tentang praktik terbaik terkait kerja jarak jauh, misalnya berbagi file dengan aman, menyambungkan ke jaringan perusahaan melalui VPN, dan menggunakan kata sandi yang aman. Untuk memfasilitasi praktik terbaik

ini, organisasi harus memastikan akses jarak jauh yang aman dengan meninjau postur keamanan tata kelola VPN dan penggunaan otentikasi multi-faktor. Organisasi juga harus memperbarui buku pedoman tanggapan insiden keamanan mereka dan membuat laporan setelah tindakan. Mendokumentasikan kegiatan respons yang diambil dalam krisis pandemi ini, termasuk kesenjangan yang teridentifikasi dan area untuk perbaikan dapat menghasilkan wawasan dan pelajaran yang berguna untuk situasi masa depan.

Terakhir, organisasi harus memperkuat keamanan di area berisiko tinggi, misalnya dengan memperbarui arsitektur keamanan mereka dan memastikan perlindungan dari ancaman orang dalam dan uji siber. Selain itu, organisasi harus mempertimbangkan untuk mempercepat implementasi dan optimalisasi solusi keamanan penting, seperti otentikasi multifaktor atau manajemen perangkat seluler, terutama untuk aplikasi atau platform konektivitas berisiko tinggi. Bagaimana jika sistem Anda tetap dikompromikan? Jika serangan siber berhasil, terlepas dari semua tindakan keamanan telah diambil, organisasi harus mengikuti pendekatan langkah demi langkah untuk memulihkan operasi bisnis penting mereka. Pertama-tama, sistem kunci perlu diisolasi untuk perlindungan. Kedua, organisasi perlu sepenuhnya memahami dan menahan insiden tersebut, dan akibatnya, menghilangkan malware apa pun. Setelah itu, tindakan perlindungan yang tepat harus diterapkan untuk memperbaiki postur sistem secara keseluruhan, dan mengidentifikasi serta memprioritaskan pemulihan proses bisnis utamanya untuk memberikan operasi. Akhirnya, rumah sakit harus menerapkan rencana pemulihan yang diprioritaskan.

Teknologi berkembang pesat dan dengan itu terjadi peningkatan serangan siber dan peningkatan frekuensi serangan berbahaya. Kami menyarankan solusi unik di mana kami menggunakan teknologi canggih dari kecerdasan buatan untuk mendeteksi dan mencegah ancaman sebelum mulai melakukan rooting sendiri di sistem komputer.

Program kecerdasan buatan akan bertindak terutama untuk memindai, memverifikasi, dan meningkatkan peringatan paket mencurigakan yang masuk ke sistem. Kita dapat menganggap ini seperti program pembela atau firewall tingkat lanjut. Tugas sekundernya juga akan memindai dan meninjau file yang tersimpan saat ini di sistem komputer dan meningkatkan peringatan untuk mereka.

Implementasi kecerdasan buatan mengumpulkan data dari server yang berhubungan dengannya untuk melihat pola atau serangan umum pada sistem. Oleh karena itu, dalam dua bagian, program akan bertindak untuk menyaring semua file dan data, apakah itu berbahaya, menonaktifkan, menghapus otomatis atau memutus aksesnya ke sistem komputer kecuali jika disetujui oleh pengguna. Sistem kecerdasan buatan akan memanfaatkan kemampuan pembelajaran mesinnya seperti ketika pengguna mengesampingkan potensi ancaman sebagai berbahaya, program akan mempelajari polanya dan mengirim data ke server tempat ia akan menyimpan pola tersebut.

Semua sistem komputer lain yang menggunakan program ini akan dapat merujuk ke pola yang disimpan di server. Dengan pola dalam algoritma akan memudahkan dalam mendeteksi kerentanan system. Peningkatan akurasi algoritma prediksi akan mempengaruhi akurasi sistem dalam memprediksi rekomendasi kepada pengguna [46]. Ini akan memastikan bahwa sistem mempelajari serangan ini dan dapat mencegahnya secara efisien sebelum dimulai.

Solusi ini, seperti yang dinyatakan sebelumnya, bergantung pada teknologi canggih dan maju untuk melakukan pekerjaan yang paling berat. Meskipun sistem akan digunakan secara pasif dan aktif dalam waktu proses, menggunakan sumber daya lebih dari biasanya, dan dapat menyebabkan frustrasi pada awalnya, solusi ini dibuat agar ada secara efektif dalam jangka panjang dengan tumbuh lebih kuat dan lebih cerdas seiring berjalannya waktu. berlalu.

Semakin banyak data yang dikumpulkannya, semakin yakin program tersebut secara otomatis menghilangkan dan mengganggu serangan sebelum menyebabkan kerusakan pada sistem komputer. Ini, dalam bentuk terkecilnya akan sangat efektif pada perangkat yang berdiri sendiri tetapi bekerja lebih baik di server karena lebih banyak data akan dimasukkan. Ini sangat berharga bagi perusahaan seperti Google yang sangat menghargai keamanan data mereka dan data pengguna. Ini juga bisa bekerja sangat baik untuk bisnis kecil dan besar. Selain itu, saat ini pandemi COVID-19, di mana serangan lebih sering terjadi, dapat mempercepat proses pembelajaran mesin program, sehingga sangat efektif dengan cepat.

Program ini berpotensi untuk menghilangkan masalah karena harus melakukan banyak pekerjaan manual pengguna dengan firewall atau program keamanan seolah-olah program tersebut cukup percaya diri, itu akan menjalankan arahan secara otomatis. Program ini juga dapat mendeteksi penipuan dan upaya phishing saat menerima data email. Ini akan mengingatkan dan memperingatkan pengguna tentang potensi penipuan dan dengan alasan. Sistem juga mengesampingkan masalah memiliki bug keamanan dan pintu belakang dalam perangkat lunak karena ia belajar secara progresif dan otomatis "menambal" dirinya sendiri. Terakhir, itu juga akan mendeteksi malware yang ditanamkan ke dalam sistem dan berusaha untuk menghilangkannya sebelum menimbulkan kerusakan yang lebih besar.

Solusi ini, seperti yang dinyatakan sebelumnya, bergantung pada teknologi canggih dan maju untuk melakukan pekerjaan yang paling berat. Meskipun

sistem akan digunakan secara pasif dan aktif dalam waktu proses, menggunakan sumber daya lebih dari biasanya, dan dapat menyebabkan frustrasi pada awalnya, solusi ini dibuat agar ada secara efektif dalam jangka panjang dengan tumbuh lebih kuat dan lebih cerdas seiring berjalannya waktu. berlalu. Semakin banyak data yang dikumpulkannya, semakin yakin program tersebut secara otomatis menghilangkan dan mengganggu serangan sebelum menyebabkan kerusakan pada sistem komputer. Ini, dalam bentuk terkecilnya akan sangat efektif pada perangkat yang berdiri sendiri tetapi bekerja lebih baik di server karena lebih banyak data akan dimasukkan. Ini sangat berharga bagi perusahaan seperti Google yang sangat menghargai keamanan data mereka dan data pengguna. Ini juga bisa bekerja sangat baik untuk bisnis kecil dan besar. Selain itu, saat ini pandemi COVID-19, di mana serangan lebih sering terjadi, dapat mempercepat proses pembelajaran mesin program, sehingga sangat efektif dengan cepat.

Program ini berpotensi untuk menghilangkan masalah karena harus melakukan banyak pekerjaan manual pengguna dengan firewall atau program keamanan seolah-olah program tersebut cukup percaya diri, itu akan menjalankan arahan secara otomatis. Program ini juga dapat mendeteksi penipuan dan upaya phishing saat menerima data email. Ini akan mengingatkan dan memperingatkan pengguna tentang potensi penipuan dan dengan alasan. Sistem juga mengesampingkan masalah memiliki bug keamanan dan pintu belakang dalam perangkat lunak karena ia belajar secara progresif dan otomatis "menambal" dirinya sendiri. Terakhir, itu juga akan mendeteksi malware yang ditanamkan ke dalam sistem dan berusaha untuk menghilangkannya sebelum menimbulkan kerusakan yang lebih besar.

Menyebarkan kesadaran tentang pentingnya keamanan siber harus menjadi prioritas utama. Lebih baik mendidik orang tentang keamanan siber, ancaman dan pencegahan siber yang umum. Seperti yang mereka katakan, mencegah lebih baik daripada mengobati.

Jika diberi tugas menyebarkan kesadaran tentang keamanan siber, kami akan menggunakan beberapa metode. Pertama, kita harus memanfaatkan iklan media sosial. Anehnya, sebagian besar pengguna internet tidak menyadari bahaya penggunaan internet. Beriklan di platform ini, seperti Facebook dan Instagram, telah diketahui secara halus mempengaruhi pengguna media sosial. Oleh karena itu, dengan menggunakan aspek psikologis ini, kita dapat meningkatkan kesadaran atau menanamkan pemikiran sadar tentang keamanan siber. Ini bertujuan bukan untuk menanamkan rasa takut akan serangan siber tetapi untuk memeranginya menggunakan metode pencegahan yang sederhana namun efektif. Selain itu, dalam hal perusahaan dan sisi bisnis, karyawan harus menghadiri seminar yang berkaitan dengan keamanan siber untuk mengetahui taktik dan metode umum penipu. Ini juga akan membantu karyawan yang tidak berada di bidang TI untuk mendeteksi upaya peretasan atau serangan pada workstation mereka jika itu terjadi. Dalam jangka panjang, biaya untuk mengirim karyawan ke seminar akan menjadi jumlah yang kecil dibandingkan dengan jumlah uang yang dihemat dari pemulihan dari serangan dan penipuan dalam prospek perusahaan.

5. Kesimpulan

Pandemi Covid-19 telah menghasilkan keadaan sosial dan ekonomi yang luar biasa dan unik yang dimanfaatkan oleh penjahat siber. Hasil analisis terhadap peristiwa seperti pengumuman dan cerita media telah menunjukkan apa yang tampak sebagai korelasi longgar antara pengumuman dan kampanye serangan siber terkait yang memanfaatkan peristiwa tersebut sebagai pengait sehingga meningkatkan kemungkinan keberhasilan.

Pandemi Covid-19, dan peningkatan tingkat serangan siber yang ditimbulkannya memiliki implikasi yang lebih luas, melebihi target semacam itu. Perubahan pada praktik kerja dan sosialisasi, berarti orang-orang sekarang menghabiskan lebih banyak waktu untuk online. Selain itu, tingkat pengangguran juga meningkat, yang berarti lebih banyak orang yang duduk di rumah secara online-kemungkinan sebagian dari orang-orang ini akan merusak kejahatan siber untuk menghidupi diri mereka sendiri.

Penelitian yang telah dilakukan memberikan peluang untuk penelitian lebih lanjut. Penelitian ini telah menunjukkan apa yang bisa digambarkan sebagai tampilan langsung dan terbalik yang longgar antara peristiwa dan serangan siber. Penelitian lebih lanjut perlu dipersiapkan untuk fenomena ini dan menguraikan apakah model prediksi dapat digunakan untuk mengatur hubungan ini. Ke depan, keamanan siber akan dikembangkan dengan integrasi teknologi terkini, seperti *Artificial Intelligence*, *Blockchain*, Internet of Things, dan masih banyak lagi. Adapun situasi saat ini, setiap pengguna harus mulai mengambil langkah kecil untuk melindungi data pribadi Anda sebelum disusupi oleh pengguna yang tidak sah.

Daftar Pustaka

[1] R. Komalasari, "Manfaat Teknologi Informasi dan Komunikasi di Masa Pandemi Covid 19," *Temat. Teknol. Inf. Dan Komun.*, vol. 7, no. 1, pp. 38–50, 2020.

[2] Z. Munawar, "Keamanan Pada E-Commerce Usaha Kecil dan Menengah," *Temat. - J. Teknol. Inf. dan Komun.*, vol. 5, no. 1 SE-Articles, Jun. 2018.

[3] S. Furnell and J. N. Shah, "Home working and cyber security – an outbreak of unpreparedness?," *Comput. Fraud Secur.*, vol. 2020, no. 8, pp. 6–12, 2020.

[4] N. I. Munawar, Zen and Putri, "Keamanan Jaringan Komputer Pada Era Big Data," *J-SIKA| J. Sist. Inf. Karya Anak Bangsa*, vol. 02, no. 01, pp. 14–20, 2020.

[5] S. Hakak, W. Z. Khan, M. Imran, K. K. R. Choo, and M. Shoaib, "Have You Been a Victim of COVID-19-Related Cyber Incidents? Survey, Taxonomy, and Mitigation Strategies," in *IEEE Access*, 2020, vol. 8, pp. 124134–124144.

[6] M. McGuire, *Growth of Cybercrime Economy*. Bromium, 2018.

[7] M. Cross, *Scene of the cybercrime*, 2nd ed. Syngress Pub, 2008.

[8] C. Cimpanu, "Czech hospital hit by cyberattack while in the midst of a COVID-19 outbreak," 2020. [Online]. Available: https://www.zdnet.com/article/czech-hospital-hit-by-cyber-attack-while-in-the-midst-of-a-covid-19-outbreak/.

[9] S. Lyngaas, "Hackers target senior executives at German company procuring PPE," 2020. [Online]. Available: https://www.cyberscoop.com/germany-ppe-coronavirus-hackers-ibm/.

[10] A. Alshamrani, S. Myneni, A. Chowdhary, and D. Huang, "A Survey on Advanced Persistent Threats: Techniques, Solutions, Challenges, and Research Opportunities," *IEEE Commun. Surv. Tutorials*, vol. 21, no. 2, pp. 1851–1877, 2019.

[11] L. Xiao, D. Xu, N. B. Mandayam, and H. V. Poor, "Attacker-Centric View of a Detection Game against Advanced Persistent Threats," *IEEE Trans. Mob. Comput.*, vol. 17, no. 11, pp. 2512–2523, 2018.

[12] N. C. S. C. (NCSC) and C. and I. S. A. (CISA), "Advisory: COVID- 19 exploited by malicious cyber actors." [Online]. Available: https://www.ncsc.gov.uk/news/covid-19-exploited-by-cyber-actors-advisory. [Accessed: 11-Nov-2021].

[13] World Economic Forum, *COVID19 Risks Outlook: A Preliminary Mapping and Its Implications*, no. May. 2020.

[14] S. S. Sjouwerman, "Q1 2020 Coronavirus-Related Phishing Email Attacks Are Up 600%," 2020. [Online]. Available: https://blog.knowbe4.com/%0Aq1-2020-coronavirus-related-phishing-email-attacks-are-up-600. [Accessed: 11-Nov-2020].

[15] C. P. Service, "Cybercrime - prosecution guidance," 2020. [Online]. Available: https://www.cps.gov.uk/legal-guidance/cybercrime-prosecution-guidance. [Accessed: 01-Jan-2021].

[16] G. Tsakalidis, "A systematic approach toward description and classification of cyber crime incidents," *IEEE Trans. Syst. Man, Cybern. Syst.*, vol. 49, no. 4, pp. 710–729, 2017.

[17] I. Kotenko and A. Chechulin, "A Cyber Attack Modeling and Impact Assessment framework," in *International Conference on Cyber Conflict, CYCON*, 2013, pp. 1–24.

[18] O. Kolomiyets, S. Bethard, and M. F. Moens, "Extracting narrative timelines as temporal dependency structures," *50th Annu. Meet. Assoc. Comput. Linguist. ACL 2012 - Proc. Conf.*, vol. 1, no. February, pp. 88–97, 2012.

[19] R. Van Heerden, S. Von Soms, and R. Mooi, "Classification of cyber attacks in South Africa," in *2016 IST-Africa Conference, IST-Africa 2016*, 2016, no. September.

[20] S. Henderson, G. Roncone, S. Jones, J. Hultquist, and J. Read, "Vietnamese threat actors apt32 targeting wuhan government and chinese ministry of emergency management in latest example of covid-19 related espionage," 2020. [Online]. Available: https://www.fireeye.com/blog/threat-research/2020/04/apt32-targeting-chinese-government-in-covid-19-related-espionage.html. [Accessed: 10-Apr-2021].

[21] K. D. Rosso, "New threat discovery shows commercial surveillanceware operators latest to exploit covid-19," 2020. [Online]. Available: https://blog.lookout.com/commercialsurveillanceware-operators-latest-to-take-advantage-ofcovid-19.

[22] A. Pilkey, "Coronavirus email attacks evolving as outbreak spreads," *F-Secure*, 2020. [Online]. Available: https://blog.f-secure.com/coronavirus-email-attacks-evolving-as-outbreak-spreads/. [Accessed: 10-Apr-2021].

[23] Kaspersky, "Coronavirus phishing," 2020. [Online]. Available: https://www.kaspersky.com/blog/coronavirus-phishing/32395/. [Accessed: 10-Apr-2021].

[24] M. McGuire and S. Dowling, *Cyber crime: A review of the evidence*, no. October. 2013.

[25] Kaspersky, "Research Reveals Hacker Tactics: Cybercriminals Use DDoS as Smokescreen for Other Attacks on Business," *Kaspersky Web*, 2020. [Online]. Available: https://www.kaspersky.com/about/press-releases/2016_research-reveals-hacker-

tactics-cybercriminals-use-ddos-as-smokescreen-for-other-attacks-on-business. [Accessed: 10-Apr-2021].

[26] X. Bellekens *et al.*, "From Cyber-Security Deception to Manipulation and Gratification Through Gamification," *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, vol. 11594 LNCS, no. June, pp. 99–114, 2019.

[27] MalwareBytes Labs, *2020 State of Malware Report*, no. February. 2020.

[28] Check Point, "Coronavirus cyber-attacks update: beware of the phish," *Check Point Blog*, 2020. [Online]. Available: https://blog.checkpoint.com/2020/05/12/coronavirus-cyber-attacks-update-beware-of-the-phish/. [Accessed: 10-Apr-2021].

[29] T. Brewster, "There Are Now More Than 40,000 'High-Risk' COVID-19 Threats On The Web," *Forbes*, 2020. [Online]. Available: https://www.forbes.com/sites/thomasbrewster/2020/04/22/there-are-now-more-than-40000-high-risk-covid-19--threats-on-the-web/?sh=5f54ead42722. [Accessed: 10-Apr-2021].

[30] J. Tidy, "Coronavirus: Israel enables emergency spy powers," *BBC News*, 2020. [Online]. Available: https://www.bbc.com/news/technology-51930681. [Accessed: 10-Apr-2021].

[31] J. R. C. Nurse, "Cybercrime and you: How criminals attack and the human factors that they seek to exploit," in *The Oxford Handbook of Cyberpsychology*, no. October, 2018.

[32] US Department of Justice (DOJ), "COVID-19 Fraud," *United States Departement of Justice*, 2020. [Online]. Available: https://www.justice.gov/usao-edky/covid-19-fraud-1. [Accessed: 10-Apr-2021].

[33] Sophos, "'Dirty little secret' extortion email threatens to give your family coronavirus," *Sophos Web*, 2020. [Online]. Available: https://nakedsecurity.sophos.com/2020/03/19/dirty-little-secret-extortion-email-threatens-to-give-your-family-coronavirus/. [Accessed: 10-Apr-2021].

[34] Domaintools, "Covidlock update: Deeper analysis of coronavirus android ransomware," *Domaintools Web*. [Online]. Available: https://www.domaintools.com/resources/blog/covidlockupdate-coronavirus-ransomware. [Accessed: 10-Apr-2021].

[35] I. Media, "Spanish hospitals targeted with coronavirus-themed phishing lures in Netwalker ransomware attacks," *Computing*, 2020. [Online]. Available: https://www.computing.co.uk/news/4012969/hospitals-coronavirus-ransomware. [Accessed: 10-Apr-2021].

[36] Wired, "Hackers Are Targeting Hospitals Crippled by Coronavirus," *Wired Web*, 2020. [Online]. Available: https://www.wired.co.uk/article/coronavirus-hackers-cybercrime-phishing. [Accessed: 10-Apr-2021].

[37] BleepingComputer, "Ransomware Gangs to Stop Attacking Health Orgs During Pandemic," 2020. [Online]. Available: https://www.bleepingcomputer.com/news/security/ransomware-gangs-to-stop-attacking-health-orgs-during-pandemic/. [Accessed: 10-Apr-2021].

[38] A. Ng, "Fake coronavirus tracking apps are really malware that stalks you," *CNET*, 2020. [Online]. Available: https://www.cnet.com/health/fake-coronavirus-tracking-apps-are-really-malware-that-stalks-its-users/. [Accessed: 10-Apr-2021].

[39] I. Agrafiotis, J. R. C. Nurse, M. Goldsmith, S. Creese, and D. Upton, "A taxonomy of cyber-harms: Defining the impacts of cyber-attacks and understanding how they propagate," *J. Cybersecurity*, vol. 4, no. 1, pp. 1–15, 2018.

[40] N. C. S. Centre, "Advisory: APT groups target healthcare and essential services," *National Cyber Security Centre*, 2020. [Online]. Available: https://www.ncsc.gov.uk/news/apt-groups-target-healthcare-essential-services-advisory. [Accessed: 10-Apr-2021].

[41] UK. National Cyber Security Centre, "Advisory: APT29 targets COVID-19 vaccine development Version 1.1," 2020, no. July.

[42] F. Malecki, "Overcoming the security risks of remote working," *Comput. Fraud Secur.*, vol. 2020, no. 7, pp. 10–12, 2020.

[43] Y. Herdiana, "Manajemen Resiko Kemanan E-Commerce," *Tematik*, vol. 5, no. 1, pp. 17–39, 2018.

[44] S. S. Bhuyan *et al.*, "Transforming Healthcare Cybersecurity from Reactive to Proactive: Current Status and Future Recommendations," *J. Med. Syst.*, vol. 44, no. 5, 2020.

[45] S. E. Institute, *CERT Resilience Management Model (CERT-RMM) Version 1.2*, no. February. 2016.

[46] Z. Munawar, N. Suryana, Z. B. Sa'aya, and Y. Herdiana, "Framework With An Approach To The User As An Evaluation For The Recommender Systems," in *2020 Fifth International Conference on Informatics and Computing (ICIC)*, 2020, pp. 1–5.