فصلنامه علمی
مطالعات حقوقی فضای مجازی
سال اول | شماره دوم | تابستان ۱۴۰۱
وبگاه مجله: https://cyberlaw.maragheh.iau.ir
ISSN:2821-126X

Imbalance Between Cybercrime Punishments with Some of the Corresponding Traditional Crimes

*Ali Arman

Assistant Professor, Department of Criminal Law and Criminology, Boroujerd Branch, Islamic Azad University, Boroujerd, Iran
Sahel.ali84@yahoo.com

DOI: 10.30495/CYBERLAW.2022.693897

Keywords:
Coronavirus,
Cyber Security,
Security Threats,
Crime,
Covid-19,

Abstract

Background and purpose: The emergence of the Covid-19 has threatened physical and mental health and has negatively affected the economy of all countries in the world as well as the people's daily life. All countries of the world have imposed restrictions such as travel, quarantine, school closures, social distancing measures. In the current situation, information and communication technologies and cyberspace play a significant role in establishing communication between the people. Most of the countries in the world use remote working systems and online mechanisms of education letting students and staff stay and work from their homes. There has also been a very high demand in activities such as telecommuting, electronic health care systems, food delivery and online shopping. The cyberspace criminals have taken the Covid-19 Pandemic as an opportunity to launch attacks against financial interests and promote their nefarious purposes.Findings: During the outbreak of the Covid-19, ransomware, phishing attacks and botnets have targeted the banking systems, personal virtual space education, health care and resources such as the confidentiality of patient records which have endangered privacy and have compromised the confidentiality and integrity of data. People are falling prey to cyber-attacks through Covid-19 related content.
Results: In this article, several important cyber security threat methods that existed or could occur during this pandemic have been examined. We have also discussed the concerns in the midst of this privacy-centered pandemic and finally examined some of the ways to deal with these threats. Abidance by the ways and methods revealed through this research will enable the people to keep safe in the cyber space to a noticeable degree.

فصلنامه علمی
مطالعات حقوقی فضای مجازی
سال اول | شماره دوم | تابستان ۱۴۰۱

تهدیدهای مخرب با موضوع امنیت سایبری در بحبوحه همه گیری کووید–۱۹ و روشهای پیشگیری

علی آرمان

استادیار، گروه حقوق کیفری و جرم‌شناسی، واحد بروجرد، دانشگاه آزاد اسلامی، بروجرد، ایران

Sahel.ali84@yahoo.com

تاریخ دریافت:۱۰ خرداد ۱۴۰۱ تاریخ پذیرش: ۰۵ مرداد ۱۴۰۱

چکیده

زمینه و هدف: ظهور کووید–۱۹سلامت جسم و روان را تهدید کرده و بر اقتصاد همه کشورهای جهان و زندگی روزمره تأثیر منفی گذاشته است. همه کشورها محدودیت هایی از قبیل سفر، قرنطینه، تعطیلی مدارس، اقدامات فاصله گذاری اجتماعی را اعمال کرده‌اند. در شرایط کنونی، فناوری اطلاعات و ارتباطات و فضای سایبر نقش بسزایی در ایجاد ارتباط بین مردم ایفا می‌کند. اکثر کشورها از دورکاری و سازو کارهای آنلاین سیستم آموزشی استفاده کرده و دانش آموزان، دانشجویان و کارکنان در خانه فعالیت می‌کنند. همچنین ما در انجام فعالیتهایی مانند دورکاری، سیستم‌های مراقبت بهداشتی الکترونیکی، تحویل غذا و خریدهای آنلاین شاهد تقاضای بسیار بالایی بوده ایم. مجرمان سایبری کووید–۱۹ را به عنوان فرصتی برای راه‌اندازی حملات علیه منافع مالی و ترویج اهداف شیطانی خود در نظر گرفته‌اند.

یافته‌ها:همزمان با شیوع همه‌گیری کرونا ویروس باج‌افزارها، حملات فیشینگ و بات نت‌ها، سیستم‌های بانکی، آموزشی فضای مجازی شخصی، مراقبت‌های بهداشتی و منابعی مانند محرمانه بودن سوابق بیمار را مورد تهدید و حمله قرار داده و حریم خصوصی و محرمانگی و یکپارچگی داده‌ها را به خطر انداخته و مردم از طریق محتوای مرتبط با کووید–۱۹ طعمه حملات سایبری می‌شده‌اند.

نتایج : ما چندین روش تهدید مهم امنیت سایبری که در طول این اپیدمی وجود داشته یا می‌تواند رخ دهد، همچنین در مورد نگرانی‌های موجود در بحبوحه این پاندمی با محوریت حریم خصوصی بحث کرده و چند مورد از روشهای مقابله با این تهدیدها را مورد بررسی قرار داده که در نتیجه باعث خواهد شد که افراد با رعایت یکسری اصول اولیه تا حدود زیادی از قربانی شدن در فضای مجازی در امان باشند.

کلید واژگان: کرونا ویروس، امنیت سایبری، تهدیدات امنیتی، جرائم، کووید–۱۹

مقدمه

با شروع همه‌گیری ویروس کرونا و درگیری هزاران نفر به این ویروس؛ یک «اورژانس بهداشت عمومی درسطح بین‌المللی» متعلق به سازمان جهانی بهداشت در ۳۰ ژانویه ۲۰۲۰، شیوع ویروس جدیدی به نام کروناویروس (کووید-۱۹) به عنوان پاندمی تأیید کرد(World Health Organization,2020). مراکز کنترل و پیشگیری از بیماری نیز در ۳۱ ژانویه ۲۰۲۰ وضعیت اضطراری را برای سلامت عمومی در ایالات متحده اعلام کرد. (Bajema et al,2019:166) کووید-۱۹ اکنون در تمام کشورهای جهان گسترش یافته است و موارد جدید ابتلا و گزارش های مرگ و میر روزانه گویای این مطلب است. کووید-۱۹ علاوه بر تهدید زندگی، کسب و کارها را بی ثبات کرده، به زندگی روزمره آسیب رسانده و باعث ایجاد استرس و اضطراب در افراد شده و اقتصاد جهانی را با چالش جدی مواجه کرده است. اجرای قرنطینه به عنوان یک اقدام موثر برای مدیریت تماس انسانی و کنترل انتقال ویروس شناخته می‌شود.

کووید-۱۹ به طرق مختلف بر زندگی روزمره ما تأثیر می‌گذارد و طرح‌های قرنطینه‌ای ساختارها و محیط‌های اجتماعی ما را پیکربندی و بازسازی کرده است. با دستورات ماندن در خانه، ممنوعیت سفر و قوانین فاصله‌گذاری اجتماعی، استفاده از اینترنت و همچنین وابستگی به پلتفرم‌های آنلاین از جمله بانکداری، مراقبت‌های بهداشتی، سرگرمی، تجارت، آموزش و خدمات ضروری دولتی افزایش یافته است. (Hakak,Khan,Imran,Choo&Shoaib,2020:12) بسیاری از مردم از کار در یک محیط اداری به کار در محیط خانه منتقل شده‌اند. برخی نیز در روند رو به رشد خرید آنلاین شرکت می‌کنند و افراد ممکن است به جای دیدار با دوستان یا آشنایی با افراد جدید در دنیای واقعی، در رویدادهای اجتماعی مجازی یا قرار ملاقات مجازی، شرکت کنند. تغییرات در الگوهای مصرف‌کننده و واکنش‌های دولت، بر اکوسیستم‌ها و اقتصادهای دنیای سایبری تأثیر گذاشته است. در حالی که مصرف کنندگان از راحتی دسترسی آنلاین لذت می‌برند و بسیاری از مشاغل آنلاین و ارائه دهندگان خدمات در زمینه کووید-۱۹ شکوفا شده‌اند، همه شرکت کنندگان آنلاین قانونی نیستند و به طور خاص، مجرمان سایبری اکنون فرصت های بیشتری برای سوء استفاده از کاربران خدمات آنلاین به روش‌های خلاقانه مختلف دارند. با تغییر حرکت عمومی از فعالیت‌های حضوری به فعالیت‌های آنلاین، احتمال قربانی شدن به وسیله جرایم سایبری نیز افزایش می‌یابد، که ممکن است منجر به اختلال در خدمات، ضرر مالی، نقض داده‌ها و اضطراب‌های فردی و سازمانی شود. (Hakak et al.,2020: 8–14)

مجرمان سایبری آسیب‌پذیری‌های روانی قربانیان را که بر اثر سرایت ویروس به وجود آمده هدف قرار می‌دهند در نتیجه، به دلیل عدم حمایت اجتماعی و قانونی در بسیاری از جوامع در سراسر جهان، جمعیت زیادی از اضطراب مضاعف به دلیل از دست دادن درآمد و عدم دسترسی به ضروریات اساسی زندگی از جمله غذا و سرپناه رنج می برند. این موضوع ممکن است منجر به افسردگی یا حتی آسیب رساندن به خود شود. (Kumar,&Nayar,2020:12) مجرمان از اضطراب ناشی از کووید-۱۹ از بی‌ثباتی‌های عاطفی قربانیان برای فعال کردن جرائم مالی سایبری سوء استفاده می‌کنند. از آنجایی که این بیماری به شدت از فردی به فرد دیگر قابل انتقال است(WHO,2020)، برای محدود کردن شیوع این بیماری جدید، بسیاری از کشورها تصمیم گرفتند که موسسات آموزشی از جمله مدارس، کالج ها و دانشگاه ها را تعطیل کنند. مدرسان به صورت آنلاین تدریس می کنند. در واقع، این موضوع در مقیاس بسیار بزرگ و آزمایش نشده و بی سابقه ای اتفاق می افتد. ارزیابی ها و امتحانات دانش آموزان نیز به صورت آنلاین انجام می شود.) (Burgess and Sievertsen,2020: 85 یکی از اولین تاثیرات کووید-۱۹ تغییر و تحول از محل کار فیزیکی به محل کار مجازی آنلاین است. به محض اینکه همه گیری بیماری شدیدتر شد و زندگی روزمره را تحت تأثیر قرار داد، بلافاصله در سراسر جهان بسیاری از سازمان ها و نهادها به راه اندازی سیستم دورکاری و آموزشی برخط روی آوردند(Perez,2020: 11). کووید-۱۹ کسب‌وکارهای مجازی را وادار کرده است تا به سرعت کار کنند و دوام سیستم های اینترنتی را بررسی کنند، که قبلاً هرگز این کار با این حجم انجام نشده بود. همانطور که کسب و کارها در حال تغییر هستند، چالش‌ها و اولویت های جدید سیستم های برخط هم در حال افزایش هستند، مانند تصمیم‌گیری در زمان واقعی، آموزش کارکنان آنلاین، خطرات تداوم، و بزرگترین آنها خطرات امنیتی است که در شرایط فعلی باید به سرعت به این مسائل رسیدگی شود.

فصلنامه علمی
مطالعات حقوقی فضای مجازی
سال اول | شماره دوم | تابستان ۱۴۰۱

گسترش سریع و انکوباسیون[1] طولانی مدت این ویروس چالش های اجتماعی منحصر به فردی را ایجاد کرده است. با این حال، یکی از نکات مثبت، این است که همه گیری این بیماری زمانی به وقوع پیوسته است، که ارتباطات از راه دور در اوج پیشرفت است. ابزار و وسایل مورد استفاده برای این ارتباط همه جا وجود دارد. با توجه به تکنولوژی روز، امکان برقراری ارتباط با همکاران، دوستان و خانواده فراهم شده است. برنامه‌های کنفرانس ویدیویی آنلاین مانند زوم،[2] تیم‌های مایکروسافت و گوگل میت[3] شاهد افزایش تصاعدی در ثبت نام روزانه کاربران جدید بوده‌اند. (Perez,2020:15) با این حال، استفاده از فناوری، مسائل و مشکلات و تهدیدات بیشتری را از نظر امنیت سایبری به همراه دارد.(Humayun et al, 2020:1–19) سازمان ها باید با درخواست های ضد امنیتی فزاینده ناشی از افزایش خطر حملات سایبری مقابله کنند. آنها همچنین باید به مشکلاتی که نیاز به ایجاد تعادل بین اطلاعات حساس بهداشتی و مسائل حریم خصوصی افرادی که ممکن است به آنها آلوده شده باشند، توجه ویژه به عمل آورد. (Berman and Gately, 2020: 84) به عنوان مثال، با رشد سریع محبوبیت زوم، این پلتفرم اکنون با واکنش شدیدی از سوی کاربران و نهادهای امنیتی مواجه شده است زیرا متخصصان امنیتی، مدافعان حریم خصوصی، قانونگذاران و حتی FBI هشدار می دهند که تنظیمات پیش فرض آن ایمن نیست. در نتیجه، بسیاری از شرکت ها مانند ناسا، اسپیس ایکس و کشورهایی از جمله تایوان، ایالات متحده آمریکا و نیروی دفاعی استرالیا، زوم را برای ارتباط ممنوع کردند. (Brohi, Jhanjhi, Brohi,and Brohi, 2020:226-226) بنابراین، نیاز به درک این تهدیدات سایبری و نگرانی‌های مربوط به حریم خصوصی وجود دارد که می‌تواند منجر به ایجاد موقعیت‌های نامطلوبی برای کاهش یا اجتناب از آنها شود.

۱. پیشینه و مبانی تحقیق

اکثر تحقیق های انجام شده و مقالات نوشته شده در این خصوص به موضوعات متنوعی در ارتباط با کرونا ویروس یه شکل اما هر کدام به شکل کاملاً جزئی و تخصصی اشاره شده و همه جوانب و خطرات فضای ناامن سایبر را در این بحبوحه همه گیری پوشش نداده است. لذا در این مقاله سعی شده که اثر سوء این پاندمی شوم با توجه به تهدیدات فضای سایبری و مخابراتی مورد مطالعات چند جانبه قرار گیرد . در ذیل به تعدادی از پژوهش های انجام شده در این خصوص اشاره می کنیم:

۱–نقش اهداف استفاده از فضای مجازی در سبک زندگی ارتقادهنده سلامت و اضطراب مربوط به کووید ــ۱۹ در دانشجویان (فتحی, آیت اله, صادقی, شریفی رهنمون – مجله علمی دانشگاه علوم) ۲– بررسی جنبه های علمی و اخلاقی توصیه های درمانی و پیشگیری از کووید ۱۹ با نام درمان های طبیعی، طب سنتی و طب اسلامی در فضای مجازی و رسانه ملی(امیرمحمد کاظمی فر, مرضیه بیگم سیاهپوش – مجله تاریخ پزشکی) ۳–ارتباط بین مدت زمان استفاده از فضای مجازی با شیوع ناهنجاری سندرم متقاطع فوقانی دانش آموزان دختر در دوران همه گیری کووید۱۹ (صمدی, باقریان جبلی – کارگروه اخلاق در پژوهش پژوهشگاه علوم ورزشی) ۴–برنامه درسی خودآفرین در عصر شیوع جهانی کووید۱۹ و کرونا زیستی (شعبانی ورکی, بختیار, علیرضا هوشمند – مجله فلسفه تربیت)۵–ارزیابی کیفیت خدمات دیجیتال در دوره اپیدمی کووید ۱۹ در ایران بر مبنای نظر شهروندان (حیدرزاده, حقی – فصلنامه نامه معماری و شهرسازی ۶–تبیین شاخصه‌های دین‌داری و مصداق‌های آن در فضای مجازی راهی برای آرام‌بخشی و سلامت روان جامعه در دوران کرونا(ادیب زاده – مجله مدیریت بحران) ۷– نقش اضطراب دچارشدن به بیماری کووید ۱۹ بر سلامت روان و کیفیت زندگی با میانجیگری امیدواری(نیکوگفتار, دوستی – پژوهش نامه روانشناسی مثبت) ۸–نقش نیروهای نظامی و انتظامی در مدیریت بحران ناشی از شیوع بیماری کووید ۱۹ در ایران و جهان(شیرزاد هادی, فرنوش غلامرضا, عباسی فرج زاده محسن) ۹– چالش‌های آموزش مجازی در زمان شیوع بیماری کووید ۱۹) موردمطالعه: آموزش‌وپرورش شهرستان نهاوند (یاراحمدی, فتانه)

[1] دوره کمون یا نهفتگی به انگلیسی (Incubation) در یک بیماری، به دوره و مدت‌زمان ورود عامل بیماری‌زا اعم از باکتری، ویروس و غیره به بدن تا ظهور نشانه بیماری و علائم بیماری گفته می‌شود.

2 .ZOOM

3. Google Meet

دانشگاه آزاد اسلامی واحد مراغه

۲. روش تحقیق

ابزار گردآوری اطلاعات تعاریف مفهومی از طریق فیش برداری مطالعه کتابخانه‌ای انجام گرفته وپس از پایان مرحله جمع‌آوری داده‌ها و استخراج و طبقه‌بندی اطلاعات جمع‌آوری شده، اطلاعات و داده‌ها بر مبنای فرضیه ها و ارزیابی های آن مورد و تجزیه و تحلیل استقرایی و انتزاعی قرار گرفته است.

۳. کووید-۱۹،سازمان‌ها و صنایع در معرض خطر از نظر حملات سایبری

شیوع این ویروس خطرناک در سراسر جهان نهادها و سازمانهای مختلفی را تحت تأثیر قرار داده وخطراتی برای آنها ایجاد کرده است که در ذیل چندین نهاد که شاید بیشترین آسیب را از این ویروس منحوس متحمل شده اند در سه حیطه بررسی می کنیم.

۴-۱. سیستم های مراقبت های بهداشتی

سیستم های مراقبت های بهداشتی امروزه مبتنی بر کاربردهای فناوری اطلاعات و ارتباطات است که به کاربران خود، از جمله پزشکان، پرستاران، داروسازان و بیماران، طیف گسترده‌ای از خدمات پزشکی «معروف به مراقبت‌های سلامت الکترونیک» را ارائه می‌دهد. در وضعیت همه گیری اخیر، آنها آسیب پذیرترین و هدفمندترین سیستم‌ها برای مهاجمان سایبری هستند. اگر هر سیستمی دچار اختلال شود، می تواند منجر به شرایط نامطلوبی مانند از دست دادن جان گرانبهای انسان شود. در مقابله با ویروس کرونای جدید، هرگونه حمله سایبری مخرب به احتمال فراوان، نبردی را که در حال حاضر مؤسساتی از قبیل بهداشت و آموزش و... با آن مواجه هستند (با توجه به منابع و پرسنل) تشدید خواهد کرد. در ایالات متحده آمریکا، وزارت بهداشت و خدمات انسانی مورد هدف حملات مختل کننده خدمات [۴] قرار گرفت زیرا سرورهای آن میلیون‌ها درخواست اتصال را طی چند ساعت دریافت کردند. (Stein and Jacobs,2020: 63) اگرچه مقامات مدعی شدند که خوشبختانه این حمله باعث اختلال در سیستم و عملکرد نشده ، اما به طور بالقوه چنین حملاتی می تواند در شرایط خاص فاجعه‌آمیز باشد.

۴-۲. خدمات مالی

به دلیل شیوع کووید-۱۹، وضعیت اقتصاد کشورها و بازارهای سهام در سراسر جهان در مقاطعی به پایین‌ترین سطح در ۳۰ سال گذشته سقوط کرده بودند. قیمت نفت خام هم به کمترین میزان از سال ۱۹۹۱ تاکنون (تا قبل از جنگ اوکراین) رسید. (Stevens,2020:6) این امر اقتصاد کشورهای تولیدکننده نفت را به خطر انداخته بود. به محض شروع این همه‌گیری، رکود مالی که از قبل توسط کارشناسان پیش بینی شده بود به واقعیت پیوست. در عین حال، صنایع مالی مخصوصاً صنایع خرد در برابر تهدیدات سایبری مانند فیشینگ و حملات بدافزاری یا باج افزار به شدت آسیب‌پذیر بودند.(Dion and Brohi,2020:967–981) . علاوه بر این، در شرایط عادی، و حتی قبل از بحران کرونا نیز کاربران فین‌تک[۵] در موارد زیادی طعمه مجرمان سایبری شده بودند اما در زمان بحبوحه کرونا بسیار بیشتر از قبل قربانی مهندسی اجتماعی[۶] شده‌اند، جایی که هکرها با استفاده از ترفندهای خاصی وانمود می‌کنند که فرد قانونی هستند و به اطلاعات شخصی مانند بازیابی رمز عبور دسترسی پیدا می‌کنند.

۴-۳. دولت و رسانه‌ها

همه‌گیری کنونی ناشی از کووید-۱۹یک موضوع بسیار چالش برانگیز برای خود دولت و رسانه‌ها است تا اطلاعات دقیق و به موقع را در اختیار عموم و سازمان‌های بین المللی قرار دهند. هرگونه تأخیر یا اطلاعات گمراه کننده ممکن است به موقعیت‌های

---

4. **D**istributed **D**enial **o**f **S**ervice

[۵] فین تک (Financial technology یا FinTech) به استفاده از تکنولوژی و دنیای دیجیتال در دنیای مالی اشاره دارد که می‌تواند تا حد زیادی عملیاتی مانند انتقال کارت به کارت، پرداخت قبوض، خرید شارژ و غیره را با سرعت و دقت بالاتری انجام دهد. در حال حاضر استارت آپ‌های بسیاری از این ایده برای کارآفرینی استفاده کرده‌اند که بسیاری از آن‌ها موفقیت‌آمیز بوده‌اند

[۶] مهندسی اجتماعی سوء استفاده از اطمینان و یا فریب عوامل انسانی به جهت دسترسی به اطلاعات محرمانه و در مرحله بعد سوء استفاده از این اطلاعات است.

فصلنامه علمی
مطالعات حقوقی فضای مجازی
سال اول | شماره دوم | تابستان ۱۴۰۱

ناخوشایندی منجر شود. مهاجمان و هکرها می توانند حملات سایبری را علیه دولت و رسانه ها برای انتشار اطلاعات نادرست در سطح عمومی انجام دهند. به عنوان مثال، حتی اگر این یک فعالیت غیرسایبری یا فقط یک خبر نادرست باشد، باز هم می‌تواند باعث ایجاد هیاهو و ترس در بین عموم مردم شود و می تواند سؤالاتی را در مورد دولت ها ایجاد کند.(Cook, 2020: 17)

۴. تهدیدهای سایبری در بحبوحه همه‌گیری کرونا

با پیشرفت تکنولوژی، امروزه امنیت سایبری بسیار چالش برانگیز شده است. معمولاً هکرها، مهاجمان و کلاهبرداران از موقعیت‌های اضطراری سوء استفاده می‌کنند، به ویژه در مواقعی که مردم ترسیده، مستأصل و آسیب‌پذیر هستند. شیوع ویروس کرونا یک موقعیت اضطراری است. بازیگران بد در سراسر جهان از ویروس کرونا به عنوان ابزاری جدید برای اعمال شیطانی خود در قالب هک، حمله یا کلاهبرداری استفاده می کنند. طبق تحقیقات انجام شده، در همه‌گیری اخیر، فقط تا آغاز آوریل ۲۰۲۰ در مجموع بیش از ۹۰۷ هزار پیام هرزنامه، ۷۳۷ حمله بدافزار و ۴۸ هزار بازدید لینک‌های مخرب و افزایش ۲۲۰ برابری ایمیل های اسپم و ۲۶۰ درصدی در URL های مخرب در سراسر جهان وجود داشته است. (Cook, 2020: 13) در زیر به تعدادی از تهدیدات سایبری که در زمان این پاندمی وجود داشته اشاره می‌کنیم.

۵-۱. حملات محروم‌سازی از سرویس[۷]

اکثردولت‌ها و سازمان‌های مراقبت‌های بهداشتی در دو سال اخیر شاهد افزایش سریع حملات مختل‌کننده خدمات (Khan,Brohi,and Jhanjhi, 2020:106) به دلیل همه‌گیری کووید-۱۹ بوده اند. هکرها وب سایت‌ها یا سیستم‌های سازمان ها را با کاربران جعلی یا بات پر می‌کنند تا عملکرد عادی سیستم را مختل کنند و در نتیجه کانال ارتباطی را قطع می‌کنند. یک نمونه اخیر از این اتفاق زمانی رخ داد که یک حمله مختل‌کننده خدمات وب سایت وزارت بهداشت و خدمات انسانی[۷] در ایالات متحده را با سیل میلیون‌ها کاربر در یک زمان محدود هدف قرار داد (Stein and Jacobs,2020: 3) .

۵-۲. دامنه های مخرب

واژه‌های «کرونا ویروس»، و «کووید-۱۹» اخیراً در تعداد زیادی از دامنه‌های ثبت‌شده در اینترنت ظاهر شده‌اند و هر روز شاهد افزایش روز افزون آن‌ها هستیم. اگرچه برخی از آنها وب سایت های قانونی هستند، مجرمان سایبری هر روز هزاران سایت جدید ایجاد می‌کنند که در آنها کمپین‌های هرزنامه، فیشینگ، انتشار بدافزار یا سرورها ، دامنه های دسترسی را دچار تخریب می‌کند.

به طور مثال همزمان با ماههای ابتدایی شیوع کرونا در کشور امریکا ، بیش از ۴۰۰۰ دامنه مرتبط با کروناویروس‌ها از ابتدای همه گیری تا ژانویه ۲۰۲۰ در سراسر جهان ثبت شده است. ۳ درصد از این وب سایت ها مخرب و ۵ درصد دیگر مشکوک هستند. مناطق مرتبط با کرونا ۵۰ درصد بیشتر از موارد گزارش شده در همان دوره و همچنین بیشتر از رویدادهای فصلی اخیر، مانند روز ولنتاین است.(Frank Rauch,2020: 9) از این دامنه ها برای انجام کلاهبرداری های مختلف استفاده می شود یا به عنوان یک هانی پات[۸] برای کاربران هدف استفاده می شود. هکرها از طریق این روش داده های شخصی را دریافت می کنند و سپس از آن برای اهداف مورد نظر خود استفاده می‌کنند.

[7] DHoS

[۸] یک منبع سیستم اطلاعاتی با اطلاعات کاذب است که برای مقابله با هکرها و کشف و جمع‌آوری فعالیت‌های غیرمجاز در شبکه‌های رایانه‌ای بر روی شبکه قرار می‌گیرد

دانشگاه آزاد اسلامی واحد مراغه

۵-۳. وب سایت‌های مخرب

وب سایت‌هایی که ادعا می‌کنند برنامه هایی هستند که قرار است از کاربران در برابر کووید-۱۹ محافظت کنند، مانند سایت www.antivirus-covid19 و www.corona-antivirus.com افزایش یافته است. طبق وبلاگ Malwarebytes وب سایت www.antivirus-covid19 که اکنون غیرقابل دسترسی شده است و همچنین وب سایت www.corona-antivirus.com اشاره می کند که برنامه آنها به نام "آنتی ویروس کرونا" توسط دانشمندان دانشگاه هاروارد ساخته شده است. اما در واقع نصب این اپلیکیشن سیستم را با بدافزاری به نام BlackNET RAT آلوده می کند. این بدافزار باعث می شود دستگاه‌های آلوده به عنوان یک بات نت کار کنند. که می‌تواند به عنوان راه‌اندازی یک حمله DDoS[9]، به آپلود برخی از فایل‌های راه دور، اجرای اسکریپت‌های مخرب، جمع‌آوری کوکی‌ها و رمزهای عبور مرورگر و برداشتن کلیدها و غیره کمک کند.

دادگستری ایالات متحده اعلام می‌کند یک وب سایت جعلی ادعا کرده بود کیت‌های واکسن مورد تایید سازمان جهانی بهداشت را برای کووید-۱۹ ارائه می دهد. با این حال، واکسن‌های معتبر کووید-۱۹ تایید شده توسط سازمان جهانی بهداشت در آن زمان در بازار موجود نبودند. وب سایت جعلی از کاربران خواسته بود تا مشخصات کارت اعتباری خود را وارد کنند و برای ادامه تراکنش، مبلغ ۴,۹۵ دلار آمریکا بپردازند.

۵-۴. بدافزار

مجرمان سایبری از طریق نقشه‌ها و وب‌سایت‌های تعاملی تعبیه‌شده برای کروناویروس با انتشار بدافزارها، جاسوس‌افزارها و تروجان‌ها از وضعیت فعلی سوء استفاده می‌کنند. یکی از منابع اصلی برای فریب دادن کاربر کلیک بر روی پیوند یا دانلود بدافزار ایمیل‌های اسپم هستند که کاربر از طریق دستگاه تلفن همراه یا رایانه قربانی می‌شود. برای نشان دادن اطلاعات و تلفات در مورد کروناویروس جدید، دانشگاه جان هاپکینز نقشه‌ای با داشبورد تعاملی ایجاد کردهکرها از آن سوء استفاده کردند و یک بدافزار مبتنی بر جاوا را در آن جاسازی کردند و قربانیان نیز نه تنها نقشه را باز کردند، بلکه اکثر آنها حتی آن را به اشتراک گذاشتند.

طبق تحقیقات TrendMicro، یک Winlocker با مضمون کرونا که باعث قفل شدن ماشین های الکترونیکی می‌شد را تجزیه و تحلیل کردند که می‌تواند تهدیدی برای کاربران در هنگام استفاده از ماشین‌های آسیب‌دیده از قفل شدن باشد. هنگامی که این بدافزار اجرا می شود، برخی از فایل ها را حذف می کند و رجیستری ویندوز را تغییر می دهد. بعداً صدایی پخش می کند و پیامی را نشان می دهد که سیستم قفل شده است، بعد بلا فاصله سیستم مجدداً راه اندازی می شود و سپس برای باز کردن قفل آن به رمز عبور نیاز دارد. بدافزارها و وب‌سایت‌های فیشینگ در مقایسه با سایر تهدیدات و حملات سایبری، بیشترین افزایش را داشته‌اند.

۵-۵. باج افزار

برخی از مجرمان سایبری حملات باج افزاری را در بیمارستان ها، مراکز بهداشتی، آموزشی و موسسات عمومی انجام می دهند. از آنجایی که این مراکز به دلیل شرایط فعلی اپیدمی یا پاندمی نمی توانند از سیستم خود خارج شوند، مجرمان خوشبین هستند که این سازمان ها می توانند باج درخواست شده را بپردازند. باج‌افزار سیستم را از طریق پیوست‌های ایمیل، پیوندها، یا از طریق کارکنان شاغل که اعتبار آنها قبلاً با سوء استفاده از یک آسیب‌پذیری در سیستم‌هایشان به خطر افتاده است، آلوده می‌کند. مجرمان سایبری در حال حاضر حتی باج افزار را به عنوان یک سرویس در وب تاریک ارائه می دهند.

در زمان پاندمی باج افزار جدیدی به نام CoronaVirus آپلود شد که از طریق وب سایت جعلی Wise Cleaner (نرم‌افزار بهینه سازی سیستم) منتشر شده بود . قربانیان به روشهای مختلف توسط طراحان سایت فریب می خوردند تا فایل راه اندازی جعلی را از سایت دانلود کنند. هنگامی که قربانی این بدافزار را روی رایانه خود نصب می‌کند، این بدافزار می‌تواند رمز عبور را بدزدد، داده‌هایی را رمزگذاری کند که بعداً نمی‌توانند رمزگذاری شوند، و همچنین اطلاعات را از سیستم به سرقت می‌برد.

[9] **D**istributed **D**enial **o**f **S**ervice

فصلنامه علمی
مطالعات حقوقی فضای مجازی
سال اول | شماره دوم | تابستان ۱۴۰۱

۵-۶. ایمیل های اسپم

همیشه و در همه حال ایمیل های هرزنامه در مقیاس وسیع توسط کلاهبرداران و هکرها برای رسیدن به اهداف مورد نظر ارسال می گردد. در شرایط اپیدمی کنونی، ایمیل‌های مرتبط با ویروس کرونا با پیوست‌های مخرب در مقیاس بسیار وسیعتری در اوایل فوریه ۲۰۲۰ برای کاربران ارسال شده است. موارد متعددی وجود داشته است که در آنها متجاوزان به حریم خصوصی وانمود می کنند که از سازمان‌های قانونی مانند سازمان جهانی بهداشت هستند. آنها از جعل دامنه استفاده می‌کنند تا قربانی را فریب دهند که ایمیل از طرف سازمان جهانی بهداشت می آید و از آنها می خواهند که در بیت کوین و غیره کمک مالی کنند. (به عنوان مثال، انتهای آدرس ایمیل معمولاً به وب سایت سازمان جهانی بهداشت ختم می شود و افراد می توانند از آنجا بفهمند که آیا در حال ارتباط با شخص یا سازمان مناسب هستند یا خیر). مزاحمان از ایمیلی مانند coronavirusfund@who.org استفاده می کنند. برای آشنایی و جلوگیری از حملات سایبری باید بدانیم وب سایت رسمی سازمان جهانی بهداشت www.who.int با "int" و نه با "org" به پایان می‌رسد. هر کاربری که این ایمیل را تایید نکرده باشد ممکن است قربانی شود.

۵-۷. پیام رسانی مخرب رسانه های اجتماعی

امروزه رسانه‌های اجتماعی بسیار رایج بوده و تقریباً در دسترس هر فردی قرار دارند. هکرها آن را یک فرصت عالی می‌دانند و به سمت پلتفرم های مختلف رسانه‌های اجتماعی مانند فیس بوک و واتس اپ، تلگرام و... گرایش دارند. موارد متعددی وجود داشته است که در آن کلاهبرداری ها و تاکتیک های فیشینگ در فیس بوک مسنجر و بسیاری از برنامه های کاربردی دیگر از این قبیل دست به دست می‌شوند. کلاهبرداری‌ها معمولاً قربانیان را به اشتراک‌های رایگان مانند حساب رایگان Netflix سوق می دهند. هنگامی که قربانی روی پیوند کلیک می کند، آنها را به وب سایت فیشینگ رسانه های اجتماعی خود هدایت می کند. در برخی موارد، ممکن است از شما بخواهد که اعتبار حساب های آنها را وارد کنید. به این ترتیب، آنها یا اعتبار خود را ضبط می کنند یا بدافزار را در سیستم ها، دستگاه های تلفن همراه و مرورگرهای وب خود نصب می کنند تا اطلاعات و کوکی ها را سرقت کنند و در نتیجه کاربر قربانی می شود.

۵-۸. سازش ایمیل تجاری

بخش اطلاعات سایبری ایالات متحده یک حمله سایبری برای به خطر انداختن ایمیل های تجاری را گزارش کرد زیرا مزاحمان از پاندمی کووید-۱۹ سوء استفاده کردند. این حمله توسط Ancient Totoise، یک سازمان جرایم سایبری که در گذشته چندین پرونده BEC[۱۰] را پشت سر گذاشته بود، انجام شد. گمان می رود این حمله مجموعه ای از حملات قبلی باشد که گروه قبلاً انجام داده بود. مهاجمان ابتدا حساب های بانکی را هدف قرار می دهند. سپس از اطلاعات مشتریان استفاده می کنند و برای آنها ایمیل می‌فرستند تا اطلاعات بانکی و روش پرداخت خود را به دلیل ویروس کرونا تغییر دهند. مهاجمان وانمود می‌کنند که از سازمان‌ها یا مشاغل قانونی هستند. (Peterson,2020:19) در شرایط فعلی، کلاهبرداری های مرتبط با ایمیل تجاری از بیماری کرونا به عنوان ابزار استفاده می‌کنند. این کلاهبرداران با متقاعد کردن یا فریب دادن اهداف مد نظر، برای انجام معاملات، به عنوان یک مزاحم، خود را کارمند قانونی نشان می دهند که در همان شرکت کار می‌کنند.

۵-۹. تهدیدات موبایل

در این دوره مدرن از محاسبات فراگیر، کاربری گوشی‌های هوشمند در اوج خود می‌باشند. زندگی بدون گوشی‌های هوشمند و گجت ها غیرممکن شده است و استفاده روزانه در حال افزایش است. در عین حال فرصت خوبی برای بازیگران بد است تا از آن بهره ببرند. برنامه‌ای به نام CovidLock (Ransomware) از یک برنامه مخرب اندروید می‌آید که ظاهراً به ردیابی موارد

[۱۰] ایمیل‌های سازمانی جعلی که با نام "کلاهبرداری مدیرعاملی" یا CEO Fraud نیز شناخته می‌شوند، نوعی کلاهبرداری در فضای اینترنت هستندکه خلافکاران با جعل هویت مدیرعامل یا یکی از مدیران بلند پایه سازمان آن را اجرا می‌کنند.

کووید-۱۹ کمک می‌کند. این باج افزار تلفن‌های قربانیان را قفل می‌کند و به آنها ۴۸ ساعت فرصت داده می‌شود تا ۱۰۰ دلار بیت کوین برای بازیابی بپردازند. تهدیدها شامل حذف داده‌های تلفن و نشت اطلاعات حساب در رسانه‌های اجتماعی است. در مورد دیگر، یک برنامه اندرویدی که ماسک صورت و کیت‌های ایمنی را به افراد نگران ارائه می‌دهد. هنگامی که فردی برنامه را نصب می‌کند، این برنامه یک SMSTrojan را ارائه می‌دهد که فهرست مخاطبین تلفن همراه قربانی را جمع‌آوری می‌کند و پیامک خودکار را برای پخش خود ارسال می‌کند.

۵-۱۰. برنامه‌های مرورگر[۱۱]

با رشد سریع و دسترسی آسان به اینترنت در سراسر جهان، مرورگرها به یک نرم افزار مورد استفاده روزانه تبدیل شده اند و تقریباً هر فردی که به اینترنت دسترسی دارد از آن استفاده می‌کند. یک حمله سایبری جدید برای انتشار یک برنامه اطلاعات جعلی کووید-۱۹ که گفته می شود از سازمان جهانی بهداشت تهیه شده بود، پیدا شد. هکر به تنظیمات سیستم نام دامنه (DNS) روتر در مسیریاب های D-Link یا Linksys دسترسی پیدا می کند که مرورگرها را به طور خودکار باز می کند و اعلان یا هشداری را از برنامه مخرب نمایش می‌دهد. این هشدار فقط دکمه‌ای را نشان می‌دهد که برچسب بارگیری "COVID-19 Inform app" را دارد، هنگامی که کاربر بر روی دکمه دانلود کلیک می کند، بدافزار"Oski info stealer"را روی دستگاه نصب می کند، این بدافزار کوکی‌های مرورگر، رمزهای عبور ذخیره‌شده، تاریخچه مرورگر و اطلاعات تراکنش‌ها و بسیاری موارد دیگر را می‌دزدد.(Stealer, 2020: 53)

۵-۱۱. فیشینگ

یکی از روشهایی که اخیراً بسیار مورد توجه آنها قرار گرفته و البته کمی هم پیچیده می باشد، فیشینگ نام دارد. حملات موسوم به فیشینگ به آن دسته از حملات اینترنتی گفته می شود که معمولا طراحان آنها از ایمیلهای دارای آدرسهای فرستنده جعلی برای کشاندن کاربران به وب سایتهای مورد نظرشان استفاده می کنند. در اینگونه حملات، معمولا ایمیل هایی برای کاربران ارسال می شود که دارای آدرس فرستنده مربوط به شرکتهای معروف و یا بانکهای معتبر هستند و درون آنها نیز لینکهایی قرار دارد که ظاهرا به همان مراکز تعلق دارند اما در حقیقت کاربر را به سوی سایتهای مورد نظر طراحان فیشینگ هدایت می کنند و اطلاعات حساس نظیر کلمات عبور و یا رمز کارتهای اعتباری کاربران را می ربایند این عمل مجرمانه جدید در شبکه اینترنت می رود که به یک پدیده و معضل گسترده تبدیل شود. (ایازی:۱۳۸۶ :۱۳) فیشینگ یک نمونه از تکنیک مهندسی اجتماعی به منظور گمراه کردن کاربران اینترنتی برای بدست آوردن اطلاعت محرمانه آنان است. (آرمان،۱۳۸۶: ۱۸۵) در زمان پاندمی کرونا ویروس که استفاده از فن آوری فضای مجازی به شدت افزایش پیدا کرده آمار فزاینده ای هم از این روش جرائم سایبری به ثبت رسیده است.

Phishing در زبان انگلیسی نیز یک واژه جدید است که برخی آن را مخفف عبارتPassword Harvesting Fishing (شکار کردن رمزعبور کاربر از طریق یک طعمه) و برخی دیگر آن را استعاره ای ازکلمه Fishing (ماهیگیری) تعبیر کرد ه اند .سازندگان این واژه کوشیده اند با جایگزین کردنPh به جایF مفهوم فریفتن را به مخاطب القا کنند.

مراحل فیشینگ

مرحله۱- خرابکار فیشینگ یک ایمیل جعلی درست می کند که به نظر از یک منبع قانونی آمده است. ایمیل فیشینگ پس از آن به قربانیان پتانسیل زیادی فرستاده می شود.

مرحله۲- ایمیل فیشینگ لینکی برای وب سایت جعلی تهیه می کند که به نظر یک وب سایت واقعی می رسد.

مرحله۳- قربانی/ کاربر با وب سایت جعلی ارتباط برقرار می کند و اطلاعات مورد درخواست را بر فرض اینکه که یک وب سایت واقعی است در اختیار می گذارد.

مرحله۴- خرابکار فیشینگ داده های به دست آمده را در یک وب سایت غیرقانونی انباشته می کند تا داده ها را به تهاتری های آنلاین بفروشد.

این اطلاعات پس از آن به منظور اهداف غیرمجاز مثل خریدهای جعلی، دستیابی به وام های جعلی یا شناسایی دزدی مورد استفاده قرار می گیرند. مراحل فیشینگ در نمودار فوق نشان داده شده است. حملات فیشینگ معمولاً در قالب های زیر ظاهر می‌شوند:

ایمیل از طرف فردی که ادعا می کند دوست یا همکار شما است. پیغام یا تبلیغ در شبکه های اجتماعی. وب سایتی قلابی که که برای امور خیریه تقاضای کمک می کند. وب سایتی با نامی مشابه وب سایت هایی که شما متناوباً به آن ها سر می زنید. در برنامه های پیغام فوری مانند یاهو مسنجر یا ویندوز یاهو مسنجر. از طریق پیام های کوتاه تبلیغاتی بر روی تلفن همراه شما. و...

۵-۱۲. روش باتنت

ترکیب لغوی و کارکرد باتنت . botnet از دو کلمه تشکیل شده است: Bot و Net

bot مخفف robot است و غالبا به کامپیوتری که توسط یک بدافزار آلوده شده است اطلاق می شود. کلمه Net شبکه نیز به گروهی از سیستم ها که به هم متصل شده اند گفته می شود.افرادی که بدافزارها را ایجاد کرده اند می توانند به کامپیوترهای آلوده بصورت مستقیم لاگین کنند، اما به جای این کار از بات نت ها برای مدیریت حجم زیادی از کامپیوترهای آلوده استفاده می کنند و این کار را بصورت خودکار انجام می دهند . یک بات نت شبکه ای از کامپیوتر های آلوده است و بدافزار مربوطه نیز از شبکه برای گسترش خود استفاده می کند. دستگاه ها یا سیستم هایی که توسط یک بات آلوده شده اندzombie نیز نامیده می شوند.

زمانی که برنامه بات بر روی دستگاهی نصب شد ، تلاش می کند به وب سایت یا سروری که می تواند دستورالعمل ها و دستورات را از آن دریافت کند متصل شود . این سایت یا سرور به عنوان سرور کنترل-فرمان C&C شناخته می شود C&C. با داشتن فهرستی از ماشین های آلوده آنها را مدیریت کرده و ضمن نظارت وضعیت آنها فرامین عملیاتی را برایشان ارسال می کند. سرور کنترل کننده بات نت که (botmaster نیز نامیده می شود) فعالیت های خود را با استفاده از کانال های ارتباطی ، کنترل می کند. یک بات نت می تواند برای اجرای حملات سایبری مانند DDOS ، علیه یک هدف یا سرقت اطلاعات حساس استفاده شود. لذا انتشار این بات نت ها یکی از تهدیدات سایبری برای امنیت جامعه محسوب می شوند(grow and bush,2008:119).

باتنت ها از تکنولوژیهای بدافزاری مختلفی تشکیل شده اند، توضیح دادن درباره آنها و پیچیدگی کار آنها چندان ساده نیست. افراد مهاجم تکنولوژیهای مختلف را به نحوی با هم ترکیب کرده اند که دسته بندی آنها را سخت می‌کند بات نت ها می‌توانند باعث ایجاد گستره متنوعی از حملات گردند.(آیکاو و همکاران،۱۳۸۳: ۹۴)

۵-۱۲-۱. حملات مختل کننده خدمات: یک بات نت با هزاران عضوی که در سراسر جهان دارد می‌تواند یک حمله گسترده و هماهنگ را برای خراب کردن یا از کار انداختن سایتها و سرویسهای مهم راه اندازی نماید و منابع و پهنای باند این سیستمها را اشغال کند. حملات چندین گیگا بیت بر ثانیه توسط بات نت ها حملاتی کاملا شناخته شده و معمول هستند. اغلب حملات معمول از UDP.[۱۲] ICMP.[۱۳] و TCP SYN.[۱۴] استفاده می‌کنند.

اهداف این حملات ممکن است شامل وب سایتهای تجاری یا دولتی، سرویسهای ایمیل، سرورهای DNS ، ارائه دهنده های سرویس اینترنت، زیرساختهای اساسی اینترنت یا حتی تولید کنندگان ابزارهای امنیتی صنعت فناوری اطلاعات باشد. حملات همچنین ممکن است سازمانهای سیاسی یا مذهبی خاصی را هدف بگیرند. این حملات گاهی با باج گیری همراه می‌شوند.

---

[۱۲] UDP یا (User Datagram Protocol) یک پروتکل ارتباطی جایگزین برای پروتکل کنترل انتقال (TCP) است که در درجه اول برای برقراری اتصالات کم زمان و تحمل ضرر بین برنامه ها در اینترنت استفاده می شود.

[۱۳] به طورکلی، icmp از اساسی‌ترین و پایه‌ترین پروتکل اینترنت است که توسط دیوایس‌های تحت شبکه (برای مثال روتر) جهت نمایش خطای پیام‌های ارسالی مانند عدم برقراری اتصال به روتر یا هاست مورد استفاده قرار می‌گیرد.

[۱۴] پروتکل ارتباطی اساسی برای طیف گسترده ای از برنامه ها ، از جمله سرورهای وب و وب سایت ها ، برنامه های ایمیل و برنامه های همتا است.

هر سرویس اینترنتی ممکن است هدف یک بات نت قرار گیرد. این کار می‌تواند از طریق غرق کردن وب سایت مورد نظر در درخواستهای بازگشتی HTTP انجام شود. این نوع حمله که در آن، پروتکلهای سطوح بالاتر نیز برای افزایش تاثیر حمله به کار گرفته می‌شوند، بعنوان حملات عنکبوتی نیز مشهور است(luehlfing et al, 2003:46).

۵-۱۲-۲. روند آلودگی باتنت

هکر:	» را منتشر می کند و به عنوان «چوپان» شناخته می شود.botهکر کسی است که برنامه «
»bot:«	را مستقیماً آلوده کند یا pc ممکن است Botهای آلوده طراحی می شود. pc برای آلوده کردن و کنترل botبرنامه روی ویروس یا برنامه اسب تروجان سوار می شود.
آلودگی باتنت:	را دربربگیرد باتنت ها را می توان به منظور اهداف مختلف مثل توزیع اسپم یا pcآلودگی باتنت ممکن است هزاران فیشینگ مورد استفاده قرار دارد.

۵. پیامدهای اپیدمی در تهدید و ایجاد نگرانی‌ها در حفظ حریم خصوصی

شرکت های اشتراک‌گذاری داده‌ها توسط فناوری نقش خود را برای کمک به دولت‌های مختلف و مقامات آن دولت ها برای غلبه بر شیوع سرسام‌آور کروناویروس جدید با حفظ قرنطینه و فاصله‌گذاری اجتماعی ایفا می‌کنند، اما در عین حال، کارشناسان حفظ حریم خصوصی را در بروز خطرها وحملات سایبری در زمان همه گیری، نگران نگه می‌دارد. غول های فناوری مانند اپل، گوگل و فیس بوک در حال جمع‌آوری انبوهی از داده‌ها برای استفاده از آن برای مقاصد تبلیغاتی هستند. اکنون، برخی از آنها داده های شخصی مانند مکان و سایر اطلاعات شخصی را در اختیار مقامات بهداشت عمومی، سازمان های دولتی و حتی محققان قرار می دهند. این می تواند برای غلبه بر این وضعیت مفید باشد، اما در عین حال، حریم خصوصی عمومی را به خطر می اندازد، و این ترس وجود دارد که این داده ها حتی زمانی که این بیماری همه گیر به پایان رسیده باشد، قابل استفاده باشد. اخیراً بسیاری از بخش ها مانند صنایع، آموزش و پرورش به صورت آنلاین تغییر کرده اند. کارمندان در سراسر جهان از ابزارها و نرم افزارهای ارتباطی و کنفرانس آنلاین برای ادامه کار از خانه خود استفاده می کنند. برای ثبت نام در برنامه ها، مصرف کنندگان باید با برخی شرایط و ضوابط موافقت کنند که شامل جمع آوری اطلاعات حریم خصوصی و امنیت آنها می شود. تحقیقات اخیر از کاربران در خصوص حریم خصوصی و تجزیه و تحلیل برنامه های مانند گوگل میت،[۱۵] تیم مایکروسافت، و زوم نشان می دهد که آنها اطلاعات بیشتری از آنچه مردم تصور می‌کنند جمع‌آوری می‌کنند (John, 2020:128) ، که نگران‌کننده است.

پرکاربردترین ابزار کنفرانس [آنلاین زوم] اکنون با واکنش شدیدی از نظر حریم خصوصی و ایمنی مواجه است، زیرا کارشناسان امنیتی، مدافعان حریم خصوصی، قانونگذاران و FBI هشدار می دهند که تنظیمات پیش فرض Zoom به اندازه کافی امن نیستند (Warren, 2020: 114). علاوه بر این، اخیراً بسیاری از کشورها نظارت بر مکان و سایر جزئیات تلفن های همراه شهروندان و بازدیدکنندگان خود را برای تعیین شهرها و مناطق خاصی که تعداد قابل توجهی از افراد آلوده به ویروس کرونا در آن ساکن هستند، آغاز کرده اند. به عنوان مثال، دولت چین افراد آلوده را از این ویروس ردیابی می کند تا مطمئن شود که در خانه می مانند تا افراد دیگر آلوده نشوند. اگر کسی باید از خانه خود بیرون برود، باید کد Q.R را اسکن کند، و آنها یک کد رنگی دریافت می کنند که بر اساس نتایج آزمایش کووید-۱۹ آنها است، یعنی سبز برای روشن است، قرمز باید قرنطینه شود و نمی تواند خاموش شود. در کره جنوبی ، آنها از تلفن های هوشمند شهروندان خود برای ردیابی آنها استفاده می کنند تا تأیید کنند که آیا شخصی از نزدیک منطقه

[۱۵] گوگل میت (Google Meet) یکی از بهترین سرویس‌های ویدئو کنفرانسی است که توسط شرکت گوگل طراحی شده و دارای امکانات و قابلیت‌های زیادی می‌باشد. از جمله امکانات این سرویس چت نوشتاری، صوتی و تصویری است که با استفاده از آن می‌توانید به صورت آنلاین، با ۱۰۰ نفر جلسه برگزار کنید. همه افراد با وارد کردن آدرس Gmail ، می‌توانند از گوگل میت استفاده کنند.

آلوده عبور می کند یا نه و سپس به آنها پیامک می دهد تا برای آزمایش کرونا ویروس مراجعه و نتیجه را گزارش دهند. آنها همچنین از کارت اعتباری و دوربین های امنیتی برای ردیابی بیماران مبتلا به ویروس کرونا استفاده می کنند. همین مدل در رژیم اشغالگر قدس نیز دنبال می شود (Boyden, 2020: 8). نمونه ها و کاربردهای بسیار دیگری توسط کشورهای مختلف و سازمان های مختلف وجود دارد که در حال جمع آوری و نقض آن هستند.

حریم خصوصی مصرف کنندگان در حال حاضر، ممکن است آنطور که به نظر می رسد ناامن یا مضر نباشد، اما این داده ها می‌توانند برای اهداف منفی در درازمدت استفاده شوند یا اگر هر یک از داده‌ها به برخی از بازیگران بد، نقض شود. به عنوان مثال، اخیراً دولت پاکستان یک نیروی داوطلب به نام « نیروی امدادکرونای ببر »[۱۶] ایجاد کرده که بر اساس گزارش ها و امنیت سایبری، تحلیلگران از حساب رسمی خود در توییتی اعلام کردند که داده های شخصی مانند هویت ملی، شماره موبایل، آدرس و سایر اطلاعات« نیروی ببر» در فایل های پی دی اف در گروه های مختلف غیررسمی واتس اپ به اشتراک گذاشته شده است(Saeed,2020: 33).

در بند هشتم منشور حقوق شهروندی با عنوان «حق دسترسی به فضای مجازی» آمده که حق شهروندان است که از امنیت سایبری و فناوری‌های ارتباطی و اطلاع‌رسانی، حفاظت از داده‌های شخصی و حریم خصوصی برخوردار باشند. پیش از این هم در قانون تجارت الکترونیکی، درباره حفاظت از داده‌های شخصی مطالبی ذکر شده بود که با توجه به مواد تصویبی این قانون، کسانی که این قوانین را نقض کنند، مجرم محسوب می‌شوند.(آرمان و همکاران ،۱۳۸۸: ۱۲۹)

۶. پیشنهادات مقابله با تهدیدات سایبری

در زیر با تعدادی از روشهای مقابله با جرائم سابری خصوصاً در زمان اپیدمی ویروس کرونا به اختصار آشنا خواهیم شد. این موارد اغلب در زمان همه گیری کووید-۱۹در اکثر کشورهای جهان به انحاء مختلف صورت پذیرفته است.

۷-۱. اعتبار سنجی منبع اطلاعات مورد اعتماد

یکی از روش‌های بالقوه برای کاهش حملات باج‌افزار، بررسی برنامه‌های شخص ثالث و آموزش کاربران است، در نتیجه آنها را قادر می‌سازد تا منابع قابل اعتماد یا معتبر (مانند سازمان‌های دولتی یا مؤسسات تحقیقاتی و بهداشتی معتبر) را شناسایی کنند. رتبه بندی برنامه ها همچنین می تواند نشانه دیگری باشد که آیا برنامه ها قابل اعتماد هستند یا خیر. با این حال، این رویکرد برای برنامه های جدید، به ویژه در موقعیت های همه گیر، کارکرد مؤثری نخواهد کرد.

۷-۲. شناسایی و مسدود کردن تماس های کلاهبرداری

ارائه دهندگان خدمات VoIP[۱۷] می توانند نقش موثری در کاهش تهدیدات تماس کلاهبرداری ایفا کنند، مانند کمک به افزایش آگاهی کاربر و شناسایی فعال و مسدود کردن تماس گیرندگان بالقوه کلاهبردار (به عنوان مثال، بر اساس شاخص های پرچم قرمز، مانند تماس های ربات). اگرچه همه کاربران از فضای سایبری آگاه نیستند، کمپین های آموزشی رایگان، مانند عدم به اشتراک گذاشتن اطلاعات شخصی از طریق تماس های صوتی و نادیده گرفتن پیشنهادهای آنلاین که بیش از حد خوب هستند (مانند آزمایش های پزشکی رایگان)، ممکن است در طول همه‌گیری تشدید شوند.

استراتژی کاهش احتمالی دیگر شامل طراحی و توسعه آشکارسازهای ضد هرزنامه مبتنی بر هوش مصنوعی است. با استفاده از داده‌های پاندمی‌های قبلی، می‌توان یک ربات مبتنی بر هوش مصنوعی ایجاد کرد تا به تماس‌ها (به جای کاربران) پاسخ دهد و تأیید کند که آیا تماس ورودی اسپم است یا خیر.

[16] Corona Relief Tiger Force (CRTF)

[۱۷] یک روش برای تبدیل سیگنال های آنالوگ صوت به داده های دیجیتال است که از طریق اینترنت منتقل می شوند

۷-۳. همکاری بین المللی

بدیهی است که ما به تلاش جمعی از کشورها و دولت‌های مختلف در طول همه‌گیری‌ها، مانند وضعیت اضطراری فعلی کووید-۱۹ ، نیاز داریم. برای مبارزه با تهدیدات سایبری با مضمون همه گیری، تلاش و اقدامات متقابل از سوی جامعه بین المللی مورد نیاز است، از جمله ایجاد یک کارگروه بین المللی برای تسهیل اشتراک گذاری اطلاعات فعلی تهدیدات سایبری (به عنوان مثال، بردارهای تهدید و تکنیک ها).

اهمیت حمایت مالی را نمی توان در فعالیت های همکاری بین المللی دست کم گرفت (به عنوان مثال، آموزش بهداشت سایبری). با این حال، بسیاری از اولویت های رقابتی دیگر در طول همه گیری ها وجود دارند. از این رو، حمایت جامعه و سازمان‌های بین‌المللی باید برای تأمین بودجه طرح‌های کاهش اثر باشد. برای مثال، حمایت مالی از سوی سازمان‌هایی مانند صندوق بین‌المللی پول می‌تواند برای توسعه ابزارها و مهارت‌هایی برای کاهش تهدیدات سایبری استفاده شود.(نجفی ابرندآبادی، ۱۳۹۲: ۱۴۰-۱۳۹)

۷-۴. مقابله با کمپین های اطلاعاتی

برای مقابله با کمپین‌های اطلاعاتی، ما به حمایت و مشارکت طیف وسیعی از سهامداران، مانند پلتفرم‌های رسانه‌های اجتماعی، نیاز داریم. با این حال، تعیین جعلی بودن مطالب ارسال شده می تواند چالش برانگیز باشد، به ویژه در مواردی که به بیماری های همه گیر در حال انجام مربوط می شود. از این رو، دانشمندان رایانه و علوم اجتماعی و متخصصان مراقبت های بهداشتی در همکاری و طراحی رویکردهایی (به عنوان مثال، بر اساس تکنیک های یادگیری ماشینی انسان در حلقه) برای شناسایی و طبقه بندی اخبار جعلی یا گمراه کننده به میزان قابل توجهی نقش دارند.(آرمان،۱۳۸۶: ۱۲۴)

۷-۵. سیستم‌های امن و به روز شده

با توجه به افزایش استفاده از سیستم ها در خانه ها به دلیل اقدامات فاصله گذاری اجتماعی، باید تلاش کرد تا اطمینان حاصل شود که سیستم های خانه متصل و ایمن هستند. برای مثال، اصلاح سیستم‌های عامل و برنامه‌ها یکی از استراتژی‌های کاهش سایبری کلیدی است که توسط مرکز امنیت سایبری استرالیا اداره سیگنال‌های استرالیا توصیه می‌شود. سازمان‌های امنیتی نیز می‌توانند نقشی را ایفا کنند، مانند عدم دریافت هزینه اشتراک برای محصولات امنیتی خود (مانند نرم‌افزار ضد بدافزار) در طول همه‌گیری.

۷-۶. چارچوب های مدیریت ریسک

چارچوب مدیریت ریسک روشی موثر برای دسترسی، کاهش و ارزیابی ریسک های مرتبط با تهدید است. چندین چارچوب مدیریت ریسک مانند سیستم‌های اسکادا ، خدمات آنلاین و سیستم‌های فیزیکی سایبری در دسترس هستند. (آرمان،۱۳۸۶: ۱۰۵) بر این اساس، یک بیماری همه گیر مانند کووید-۱۹ چارچوب جدید و سریعی را تضمین می کند که می تواند بلافاصله اجرا شود. چنین چارچوبی باید قوی، مقیاس پذیر، زمان کارآمد و دقیق باشد که می تواند به راحتی توسط متخصصان، چه فنیچه غیر فنی کامپیوتر در محیط های پویا، چه در محیط های خانگی و چه در محیط های اداری،دنبال شود.

۷-۷. چند روش ابتدایی و ساده اما مهم

۵-۷-۱. آگاهی و دانش کاربران را افزایش دهید. برخی botnet ها در اینترنت به دنبال سیستمهای آسیب پذیر میگردند تا به آنها آسیب برسانند. یک تاکتیک دیگر مورد استفاده botnet ها مهندسی اجتماعی است که به وسیله آن، قربانی خود را برای باز کردن یک فایل یا کلیک کردن روی یک لینک فریب میدهند .این Botnet ها تا زمانیکه کاربر فریب آنها را نخورده باشد نمیتوانند کاری از پیش ببرند .در گذشته مهاجمان فایلهای اجرایی خرابکار را بعنوان پیوست یک ایمیل ارسال میکردند. اما اکنون بیشتر فعالیتها مبتنی بر وب است. ایمیلهای خرابکار که قبلا پیوست داشتند، اکنون شامل لینکی به یک سایت خرابکار هستند. این وظیفه شماست که این مساله را

فصلنامه علمی
مطالعات حقوقی فضای مجازی
سال اول | شماره دوم | تابستان ۱۴۰۱

برای کاربران خود به روشی که آنها کاملا متوجه شوند توضیح دهید. به آنها بگویید که پیوستهای ناشناس یا ناخواسته را باز نکنند، روی لینکهای داخل ایمیلها کلیک نکنند، و به هر لینک غیر عادی که میبینند فکر کنند.

۷-۷-۲. جاوا اسکریپت را مسدود کنید. تنظیم مرورگر به صورتی که قبل از اجرای جاوا اسکریپت به کاربر هشدار دهد، بسیاری از مشکلات را حذف خواهد کرد.

۷-۷-۳. از دفاع لایه ای استفاده نمایید. هیچیک از ابزارهای امنیتی قادر نیستند بطور کامل از سیستم شما محافظت نمایند. اما استفاده از چند ابزار مختلف میزان امنیت سیستم شما را افزایش میدهد. برای مثال اگر دو ابزار امنیتی داشته باشید که هریک ۵۰ درصد از خطراتی را که با آن مواجه میشوند را پوشش دهند، در صورت نصب هر دو ابزار، تقریبا می‌توانید با ۷۵ درصد از خطرات امنیتی مقابله نمایید.

۷-۷-۴. وضعیت امنیت خود را ارزیابی کنید. بسیاری از تولیدکنندگان مهم نرم افزارها، ابزارهای رایگان یا نسخه های آزمایشی رایگانی برای ارزیابی امنیت سیستم شما ارائه میدهند. این ابزارها قادرند گستره ای از تهدیدات، ترافیک، و نقاط ضعف امنیتی سیستمها را به شما گزارش دهند. این کار به شما کمک میکند که در مورد سیاستهای امنیتی خود تصمیم گیری مناسبی انجام دهید.

۷-۷-۵. توصیه های معمول امنیتی را جدی بگیرید. استفاده از آنتی ویروسهای به روز، نصب فایروال، استفاده از کلمات عبور مناسب، به روز نگه داشتن نرم افزارها، و رعایت جوانب احتیاط در هنگام استفاده از ایمیل و مرورگرهای وب، از این دسته توصیه های امنیتی هستند. متاسفانه اگر یک فرد مهاجم در حال استفاده از سیستم شما در یک botnet باشد، ممکن است شما اصلا متوجه این موضوع نشوید. حتی اگر به این موضوع پی ببرید که قربانی خرابکاران شده اید، باز هم رهایی از این وضعیت برای یک کاربر عادی کار مشکلی خواهد بود. ممکن است فرد مهاجم فایلها را روی سیستم شما تغییر داده باشد، بنابراین صرفا پاک کردن فایلهای خرابکار ممکن است مساله را حل نکند. از این گذشته ممکن است شما نتوانید به این سادگی به نسخه اولیه فایل اعتماد کنید. اگر فکر میکنید که قربانی افراد خرابکار شده اید، باید با یک فرد آموزش دیده و مسلط تماس بگیرید.

۷-۷-۶. روی لینک ها یا تصاویر ایمیل هایی که از واقعی بودن آن ها اطمینان ندارید، کلیک نکنید.اگر از شرکتی که با آن کار می کنید، نامه ای دریافت کردید، مستقیماً به سایت آن شرکت بروید و به حسابتان داخل شوید .در غیراین صورت بهتر است با آن ها تماس تلفنی بگیرید.

۷-۷-۷. از برنامه های ضد اسپم مناسب استفاده کنید .به این طریق بسیاری از ایمیل های فریبکارانه هرگز به صندوق پستی شما وارد نخواهند شد.

۷-۷-۵۷-۸. نرم افزارهای جاسوس یاب روی کامپیوترتان نصب کنید. استفاده از برنامه هایی مانند: Lavasoft Ad-Aware و spybot search Destroy دو نمونه خوب از چنین برنامه هایی هستند.

۷-۷-۵-۹. اگر نسبت به پیغامی شک دارید آنرا تائید نکنید و از پیوندهای های ارسالی آن استفاده نکنید .در عوض به شرکت تلفن زده و یا مستقیما به سایت آنها بروید.

۷-۷-۱۰. از پر کردن فرمهایی که توسط نامه برای شما رسیده و اطلاعات اعتباری و شخصی شما را می‌خواهند اجتناب کنید و برای اطمینان از واقعی بودن سایت، آدرس داده شده بصورت پیوند را جداگانه و در یک مرورگر با پیشوند "https//:" .یا"http//:" امتحان کنید.(آرمان، ۱۳۹۶، ۱۲۷)

۷- نتیجه‌گیری

بارزترین تأثیر کووید-۱۹ تغییر چشم انداز امنیت سایبری از یک شرکت به یک محیط خانه است. این تغییر اتفاقی فرصت های جدیدی را برای هکرها و مجرمان سایبری فراهم کرده است و در نتیجه منجر به افزایش خطر سوء استفاده از آسیب‌پذیری می‌شود. در طول همه گیری کووید-۱۹ ، موج جدیدی از حملات سایبری ثبت شد. دورکاری به دلایل مختلف خطر حملات سایبری را افزایش داده است. در محیط سازمانی یا شرکتی، امنیت کلیه دارایی ها (سخت افزار و نرم افزار) به درستی توسط کارکنان پشتیبانی فناوری اطلاعات و دسترسی به سیستم ها مدیریت می‌شود. و اینترنت تحت سیاست‌های سختگیرانه امنیت سایبری و SOP ها اداره می‌شود. دارایی‌های مرتبط با فناوری اطلاعات مرتباً اصلاح و به روز می شوند. با این حال، کار از خانه با استفاده از دستگاه های خود کارمندان با شبکه‌های ناامن آنها فرصت‌های تهدیدات سایبری را افزایش می‌دهد. بر این اساس، کار با این کانال های ارتباطی محافظت نشده و ناامن از خانه، نقطه ورود هکرها را فراهم می‌کند.

همانطور که جهان در حال پیشرفت است و استفاده از محاسبات همه جا به صورت روزانه در حال افزایش است، با همین نسبت نیز، تهدیدات امنیت سایبری و مسائل مربوط به حریم خصوصی افزایش یافته است. با شیوع اخیر همه‌گیری ویروس کرونا، تعداد کاربرانی که به صورت آنلاین با یکدیگر تعامل دارند، افزایش یافته است. با استفاده از موقعیت، بازیگران بد برای هک و حمله به پلتفرم های مختلف فعال تر شدند. برای برخی منافع مالی و سایر منافع. افزایش قابل توجهی در ثبت دامنه های مخرب، وب سایت ها و ایمیل های اسپم مشاهده شده است. متجاوزان افراد، مقامات دولتی و حتی پزشکی و بهداشت را هدف قرار می دهند.
سیستم های مراقبت این مقاله تهدیداتی را ارائه می کند که اجتناب از آنها در این وضعیت همه‌گیری ضروری است. این تهدیدات امنیت سایبری منجر به برخی مسائل و نگرانی های جدی در خصوص حریم خصوصی شده است. فعالییهای آینده بر تهدیدات جدید و مسائل مربوط به حریم خصوصی که به دلیل همه‌گیری کووید-۱۹ پدیدار شده‌اند، تمرکز خواهد کرد.

منابع و مراجع:

الف: منابع فارسی

- آرمان ، علی، جعفری،محمدجواد، وروایی اکبر،(۱۳۹۷)*ابعاد اخلاقی مقررات حفاظت اطلاعات عمومی* (GDPR) وتأثیر آن بر قوانین وحقوق شهروندی ایران در فضای سایبر مجله اخلاق زیستی دانشگاه شهید بهشتی دوره۸ شماره ۳۰
- آرمان ، علی، (۱۳۸۶)،*جرائم سایبری علیه اموال و مالکیت و چارچوب قانونی پیشگیری از آن*، رساله دکتری

- آیکاو، دیوید، کارل، سیگر، وان اِستروچ، ویلیام (۱۳۸۳)*راهکارهای پیشگیری و مقابله با جرایم رایانه ای*، ترجمه اکبر استرکی و محمد صادق روزبهانی و تورج ر یحانی و راحله الیاسی، انتشارات دانشگاه علوم انتظامی
- ایازی ، سید فیروز ، (۱۳۸۴)*نرم افزارهای آنتی فیشینگ* ، نشریه الکترونیکی رایانه خبر، شماره۳۲
- نجفی ابرندآبادی، علی‌حسین،(۱۳۹۲)*پیشگیری عادلانه از جرم، علوم جنایی*، مجموعه مقالات در تجلیل از استاد آشوری، انتشارات سمت،

ب: منابع لاتین:

- Cook, "COVID-19: Companies and Verticals at Risk for CyberAttacks," 2020. [Online]. Available: https://www.digitalshadows.com/blog-and-research/covid-19-companies-and-verticals-at-risk-for-cyber-attacks/. [Accessed: 04-May-2020].
- Ren, C. Liang, I. Hyug, S. Broh, and N. Z. Jhanjhi, "A ThreeLevel Ransomware Detection and Prevention Mechanism," *EAI Endorsed Trans. Energy Web*, vol. 7, no. 26, 2020.

- St. John, “It’s Not Just Zoom. Google Meet, Microsoft Teams, and Webex Have Privacy Issues, Too.,” 2020. [Online]. Available: https://www.consumerreports.org/video-conferencingservices/videoconferencing-privacy-issues-google-microsoftwebex/. [Accessed: 04-May-2020].
Accenture, “COVID-19: Managing the human and business impact of coronavirus,” 2020. [Online]. Available: https://www.accenture.com/my-en/about/company/coronavirusbusiness-economic-impact. [Accessed: 04-May-2020].
- Vigliarolo, “Who has banned Zoom? Google, NASA, and more, 2020. [Online]. Available: https://www.techrepublic.com/article/who-has-banned-zoomgoogle-nasa-and-more/. [Accessed: 04-May-2020]
- brian grow and Jason bush , "hacker hunters" businessweek online (june 8,2005) , available online at http ://biz.yahoo.com/special/hacker05 – atticle1.html (accessed February 2008)coronavirus-(2019-ncov).[Accessed: 04-May-2020].
- Frank Rauch CP, “Update: Coronavirus-themed domains 50% more likely to be malicious than other domains,” 2020. [Online].
Available:https://blog.checkpoint.com/2020/03/05/update-coronavirusthemed-domains-50-more-likely-to-be-malicious-than-otherdomains/. [Accessed: 04-May-2020].
- GoldSparrow, “Oski Stealer,” 2020. [Online].
Available:https://www.enigmasoftware.com/oskistealer-removal/. [Accessed:05-May-2020].
- H. Saeed, “Personal Data of Thousands of Tiger Force Members Leaks,” 2020. [Online]. Available: https://propakistani.pk/2020/05/04/personal-data-of-thousands-oftiger-force-members-leaks/. [Accessed: 04-May-2020].
- Hakak, S., Khan, W. Z., Imran, M., Choo, K.-K. R., & Shoaib, M. (2020). Have You Been a Victim of COVID-19-Related Cyber Incidents? Survey, Taxonomy, and Mitigation Strategies. IEEE Access, 8, 124134–124144.
- https://doi.org/10.1109/ACCESS.2020.3006172 https://tcrn.ch/3buz3gW
- https://www.esafety.gov.au/key-issues/image-based-abuse/take-action/deal-with-sextortion https://www.trendmicro.com/vinfo/us/security/definition/business-email-compromise-(bec)
- https://www.who.int/news room/commentaries/detail/modes-of-transmission-of-virus-causingcovid-19- implications-for-ipc-precaution-recommendations.[Accessed: 04-May-2020]
- Interpol, “COVID-19 cyberthreats,” 2020. [Online].
Available:https://www.interpol.int/en/Crimes/Cybercrime/COVID-19- cyberthreats.
[Accessed: 04-May-2020].
- JHU, “Coronavirus COVID-19 Global Cases by the Center for Systems Science and Engineering (CSSE) at Johns Hopkins University (JHU)”,” 2020. [Online]. Available: https://coronavirus.jhu.edu/map.html. [Accessed: 04-May-2020].
- J. W. Han, O. J. Hoe, J. S. Wing, and S. N. Brohi, “A conceptual security approach with awareness strategy and implementation policy to eliminate ransomware,” in *Proceedings of the 2017 International Conference on Computer Science and Artificial Intelligence*, 2017,.
- Jayakumar, Priyanka; Brohi, Sarfraz Nawaz; Zaman, Noor (2020):Top 7 Lessons Learned from COVID-19 Pandemic. TechRxiv. Preprint.
https://doi.org/10.36227/techrxiv.12264722.v1
- K. L. Bajema *et al.*, “Persons evaluated for 2019 novel coronavirus—United States, January 2020,”
- Kumar,., & K. R. Nayar, (2020). COVID 19 and its Mental Health Consequences. Journal of Mental Health, 1–https://doi.org/10.1080/09638237.2020.1757052
- M. Humayun, M. Niazi, N. Z. Jhanjhi, M. Alshayeb, and S. Mahmood, “Cyber Security Threats and Vulnerabilities: A Systematic Mapping Study,” *Arab. J. Sci. Eng.*, 2020.
- M. Security, “Sophisticated COVID-19–Based Phishing Attacks Leverage PDF Attachments and SaaS to Bypass Defenses,” *2020*.[Online]. Available:
https://www.menlosecurity.com/blog/sophisticated-covid-19-basedphishing-attacks-leverage-pdf-attachments-and-saas-to-bypassdefenses. [Accessed: 05-May-2020].
- MalwareBytes, “Fake ‘Corona Antivirus’ distributes BlackNET remote administration tool.” [Online]. Available: https://blog.malwarebytes.com/threat-analysis/2020/03/fake-coronaantivirus-distributes-blacknet-remote-administration-tool/.[Accessed: 04-May-2020].
- MalwareBytes,“SMS Trojan,” 2016. [Online].
Available:https://blog.malwarebytes.com/threats/sms-trojan/. [Accessed: 05- May-2020].
- M. luehlfing , Cynthia daily , Thomas Phillips , jr., and L.Murphy smith, "cyber crimes, intusion detetion, and computer forensics , " internal auditing 18 , no , 5 (September / October 2003)
- N. A. Khan, S. N. Brohi, and Jhanjhi. NZ, “UAV’s Applications Architecture Security issues and Attack Scenarios: A Survey,” in *1st International Conference on Technology Innovation and Data Sciences (ICTIDS) 2019*.
- R. Naidoo,. (2020). A Multi-Level Influence Model of COVID-19 Themed Cybercrime.European Journal of Information Systems, 29(3), 306–321.
https://doi.org/10.1080/0960085X.2020.1771222
- P. Boyden, “COVID-19 and privacy. Do we still have our privacy?,” 2020. [Online]. Available: https://fraudwatchinternational.com/all/covid-19-and-privacy-dowe-still-have-it/. [Accessed: 04-May-2020].
- P. Peterson, “Business Email Compromise (BEC): Coronavirus a Costly New Strain of Email Attack,” 2020. [Online]. Available: https://www.agari.com/email-security-blog/business-emailcompromise-bec-coronavirus-covid-19/. [Accessed: 04-May-2020].
- P. Stevens, “Oil plunges 24% for worst day since 1991, hits multiyear low after OPEC deal failure sparks price war,” 2020. [Online].Available: https://www.cnbc.com/2020/03/08/oil-plummets-30percent-as-opec-deal-failure-sparks-price-war-fears.html. [Accessed: 05-May-2020].
- S. Burgess and H. H. Sievertsen, “Schools, skills, and learning: The impact of COVID-19 on education,” *VoxEu. org*, vol. 1, 2020

- S. N. Brohi, N. Z. Jhanjhi, N. N. Brohi, and M. N. Brohi, "Key Applications of State-of-the-Art Technologies to Mitigate and Eliminate COVID-19," 2020
- S. P. Berman and J. W. Gately, "COVID-19 and Its Impact on Data Privacy and Security," 2020. [Online]. Available:https://www.lexology.com/library/detail.aspx?g=dec8ccab-d74a- 4bc1-9e4a-9b1e5626e936. [Accessed: 04-May-2020].
- S. Perez, "Videoconferencing apps saw a record 62M downloads during one week in March," 2020. [Online]. Available:https://techcrunch.com/2020/03/30/video-conferencing-apps-saw-arecord-62m-downloads-during-one-week-in-march/. [Accessed: 05-May-2020]
- S. Stein and J. Jacobs, "Cyber-Attack Hits U.S. Health Agency Amid Covid-19 Outbreak," 2020. [Online]. Available:https://www.bloomberg.com/news/articles/2020-03-16/u-s-healthagency-suffers-cyber-attack-during-covid-19-response. [Accessed:04-May-2020].
- T. Warren, "Zoom faces a privacy and security backlash as it surges in popularity," 2020. [Online]. Available: https://www.theverge.com/2020/4/1/21202584/zoom-securityprivacy-issues-video-conferencing-software-coronavirus-demandresponse. [Accessed: 04-May-2020].
- TM, "Developing Story: COVID-19 Used in Malicious Campaigns," 2020. [Online]. Available: https://www.trendmicro.com/vinfo/us/security/news/cybercrimeand-digital-threats/coronavirus-used-in-spam-malware-file-names and-malicious-domains. [Accessed: 04-May-2020].
- University (JHU)"," 2020. [Online]. Available:https://coronavirus.jhu.edu/map.html. [Accessed: 04-May-2020].
- WHO (World Health Organization), "Statement on the second meeting of the International Health Regulations (2005) Emergency Committee regarding the outbreak of novel coronavirus (2019- nCoV)," 2020. [Online]. Available: https://www.who.int/newsroom/detail/30-01-2020-statement-on-the-second-meeting-of-theinternational-health-regulations-(2005)-emergency-committeeregarding-the-outbreak-of-novel-
- WHO, "Beware of criminals pretending to be WHO," 2020. [Online]. Available: https://www.who.int/about/communications/cyber security. [Accessed: 04-May-2020]. "Agari Cyber Intelligence Division (ACID)," 2020. [Online]. Available: https://acid.agari.com/. [Accessed: 04-May-2020].
- WHO, "Modes of transmission of virus causing COVID-19:implications for IPC precaution recommendations," 2020.
- Worldometers, "Reported Cases and Deaths by Country, Territory or Conveyance https://www.worldometers.info/coronavirus/#countries. [Accessed: 04-May-2020]
- Y. Dion and S. N. Brohi, "An Experimental Study to Evaluate the Performance of Machine Learning Alogrithms in Ransomware Detection," *J. Eng. Sci. Technol.*, vol. 15, no. 2, 2020.