تجزیه و تحلیل جرایم سایبری و حملات سایبری در طی همه‌گیری COVID-19

الناز کتانچی[1] و بابک پورقهرمانی*[2]

[1]دانشجوی دکتری تخصصی حقوق بین‌الملل عمومی، واحد مراغه، دانشگاه آزاد اسلامی، مراغه، ایران
e.katanchi20@gmail.com

[2]استادیار گروه حقوق جزا و جرم‌شناسی، واحد مراغه، دانشگاه آزاد اسلامی، مراغه، ایران
b.pourghahramani@yahoo.com

چکیده

همه‌گیری COVID-19 یک رویداد قابل توجه و بی‌سابقه بود که زندگی میلیاردها شهروند را در سطح جهان تغییر داد و نتیجهٔ آن چیزی بود که از نظر هنجارهای اجتماعی و نحوه زندگی و کار با عنوان جدید شناخته می‌شود. گذشته از تأثیر شگفت‌انگیز بر جامعه و تجارت به طور کلی، این همه‌گیری مجموعه‌ای از شرایط منحصر به فرد مربوط به جرایم اینترنتی را ایجاد کرد که جامعه و تجارت را نیز تحت تأثیر قرار داد. افزایش اضطراب ناشی از این بیماری همه گیر، احتمال موفقیت حملات سایبری را با افزایش تعداد و دامنه حملات سایبری افزایش می‌دهد. این مقاله، همه گیری COVID-19 را از منظر جرایم اینترنتی تجزیه و تحلیل کرده و طیف وسیعی از حملات سایبری را که در سطح جهانی در طی همه‌گیری تجربه کرده‌اند، برجسته می‌کند. حملات سایبری در چارچوب رویدادهای مهم جهانی تجزیه و تحلیل می‌شوند تا شیوه عمل حملات سایبری را آشکار سازند. این تحلیل نشان می‌دهد که چگونه به دنبال چیزی که به نظر می‌رسد فاصله زیادی بین شیوع ابتلا به همه‌گیری در چین و نخستین حمله سایبری مرتبط با COVID-19 وجود دارد، حملات به‌طور پیوسته، شیوع بیشتری پیدا می‌کنند تا جایی که در بعضی از روزها، ۳ یا ۴ حمله سایبری منحصر به فرد گزارش می‌شد. این تحلیل با استفاده از بررسی‌ها در کشور انگلستان به‌عنوان یک مطالعه موردی نشان می‌دهد که چگونه مجرمان اینترنتی از وقایع مهم و اطلاعیه‌های دولتی برای ساخت و طراحی دقیق کمپین‌های جرایم اینترنتی استفاده می‌کنند.

واژگان کلیدی: امنیت سایبری، حملات سایبری، جرایم سایبری، همه گیری، COVID-19

۱- مقدمه

ویروس کرونا که از سال ۲۰۱۹ آغاز شد، به‌سرعت به یک بحران جهانی تبدیل و در نتیجه قرنطینه گسترده صدمیلیون شهروند در سراسر جهان ایجاد شد. هم‌زمان با گسترش ویروس کرونا در جهان، این امر همچنین منجر به تهدید ثانویهٔ قابل توجه برای جامعه مبتنی بر فناوری می‌شود. به‌عنوان مثال، یک سری حملات سایبری بی‌هدف و همچنین حملات سایبری و جرایم سایبری. از زمان شیوع، گزارش‌هایی درباره کلاه‌برداری‌هایی ارائه شده است که سازمان‌ها (به عنوان مثال: سازمان بهداشت جهانی) و مکان‌های عمومی (به‌عنوان مثال: سوپرمارکت‌ها و خطوط هوایی) را جعل می‌کنند، سیستم عامل‌های پشتیبانی را هدف قرار می‌دهند [۱]، اقدام به کلاه‌برداری در تجهیزات حفاظت شخصی[1] [۳] و ارائه درمان بیماری کرونا [۴] می‌کنند. این کلاه‌برداری‌ها به‌طورعمومی مردم و همچنین میلیون‌ها نفری را که در خانه کار می‌کنند هدف قرار می‌دهند. کار در خانه به‌طور دسته‌جمعی باعث شده است که سطحی از نگرانی‌های امنیتی سایبری و چالش‌هایی که پیش از این صنعت و شهروندان با آن مواجه نشده‌اند، به وجود آید. مجرمان اینترنتی با استفاده از نیرنگ‌های سنتی به‌عنوان فرصت؛ برای گسترش حملات خود استفاده کرده‌اند، همچنین از استرس، اضطراب و نگرانی بیشتر افراد بهره می‌برند. علاوه‌براین، تجارب کار در خانه، سطح عمومی عدم آمادگی فروشندگان نرم‌افزار، به‌ویژه در مورد امنیت محصولاتشان را نشان داد. حملات سایبری همچنین زیرساخت‌های حیاتی مانند خدمات بهداشتی و درمانی را هدف قرار داده است [۵]. در پاسخ به این حملات، در تاریخ ۸ آوریل ۲۰۲۰، مرکز امنیت سایبری ملی انگلستان[2] و آژانس امنیت سایبری و زیرساخت آمریکا[3]، وزارت امنیت داخلی

[1] Personal Protection Equipment (PPE)

[2] National Cyber Security Center (NCSC)
[3] Department of Homeland Security (DHS)

*نویسندهٔ عهده‌دار مکاتبات: بابک پورقهرمانی

ایالات متحده[1] یک مشاوره مشترک در مورد جرایم اینترنتی منتشر کردند که چگونه با تهدیدهای پیشرفته مداوم، این گروه‌ها از بیماری همه گیر COVID- 19 بهره برداری می‌کنند [۶]. این گفتگوی مشورتی درخصوص مصالحه مسائلی نظیر فیشینگ، بدافزار و بستر ارتباطی (به‌عنوان مثال: تیم‌های مایکروسافت) بحث می‌کند. آنچه که در اینجا و در تحقیقات بحث نشده است، ارزیابی گسترده‌تری از طیف وسیعی از حملات مربوط به بیماری همه گیر است. وضعیت کنونی حملات بسیار پراکنده است، حملاتی که از سوی دولت‌ها، رسانه‌ها، سازمان‌های امنیتی و تیم‌های حادثه‌ای گزارش شده است. بنابراین تهیه اقدامات حفاظتی و پاسخگویی مناسب با توجه به فضای پویا برای سازمان‌ها بسیار چالش برانگیز است.

جرم سایبری، به عنوان جرم سنتی، اغلب با مثلث جرم توصیف می‌شود [۷]، که مشخص می‌کند برای وقوع جرم سایبری، سه عامل باید وجود داشته باشد: قربانی، انگیزه و فرصت. قربانی هدف حمله است، انگیزه جنبه‌ای است که مجرم را به سمت حمله سوق می‌دهد و فرصت؛ فرصتی برای ارتکاب جرم است (این فرصت به‌عنوان مثال می‌تواند یک آسیب پذیری ذاتی در سیستم یا یک دستگاه محافظت نشده باشد). سایر مدل‌های جرم شناسی، مانند نظریه فعالیت‌های معمولی[2] [۸] و مثلث کلاه‌برداری [۹] از عوامل مشابهی برای توصیف جرایم استفاده می‌کنند، بعضی از آنها قربانی را با استفاده از مهاجم جایگزین می‌کنند، که در غیر این صورت می‌تواند بخشی از آن فرصت تلقی شود.

درحالی‌که امروزه حملات بسته به انگیزه مهاجم پیچیده‌تر و هدفمند هستند و قربانیان خاص را شامل می‌شوند، به عنوان مثال برای سود مالی، جاسوسی، زورگویی یا انتقام. حملات فرصت طلبانه هدفمند نیز بسیار شایع است. «حملات فرصت طلبانه» حملاتی هستند که قربانیان را براساس حساسیت آنها برای حمله انتخاب می‌کند [۱۰]. مهاجمان فرصت طلب قربانیانی را هدف قرار می‌دهند که آسیب‌پذیری خاصی دارند یا از قلاب‌هایی استفاده می‌کنند که معمولاً به صورت مهندسی اجتماعی هستند و این آسیب‌پذیری‌ها را ایجاد می‌کنند. بنابراین، هر مکانیسم مورد استفاده به‌منظور گمراه‌کردن قربانی برای واقع‌شدن در یک حمله را به‌عنوان «قلاب» تعریف می‌کنیم. این قلاب‌ها از مزاحمت، محدودیت زمانی، وحشت و سایر عوامل انسانی استفاده می‌کنند تا مؤثر واقع شوند. [۱۱] وقتی قربانیان از آنچه توجه آنها را به خود جلب می‌کند یا وقتی وحشت می‌کنند، حواسشان پرت می‌شود، بیشتر فریب می‌خورند. به همین ترتیب، محدودیت‌های زمانی، قربانیان را تحت فشار بیشتری قرار می‌دهد که می‌تواند منجر به اشتباه شود و احتمال قربانی شدن از طریق کلاه‌برداری و حملات را افزایش دهد. مثال‌های دیگر شامل فشار کاری، تغییر وضعیت شخصی، مسائل پزشکی یا حوادثی است که به طور کلی تأثیرات عمیق و آسیب زایی را در کل جامعه ایجاد می‌کند مانند مرگ و میرها و فاجعه‌ها. مهاجمان فرصت طلب همیشه به دنبال به حداکثر رساندن سود خود هستند و بنابراین منتظر بهترین زمان برای حمله به جایی هستند که شرایط متناسب با موارد ذکر شده در بالا باشد.

با توجه به انواع کلاه‌برداری‌ها و حملات سایبری، تعجب آور نیست که حملات مشابهی در طی بیماری همه گیر COVID-19 ظاهر شده باشد. این شیوع باعث ایجاد اختلال گسترده در سراسر جهان شده است، به طوری که افراد مجبورند کارهای روزمره خود را با واقعیت جدیدی مطابقت دهند: کار در خانه، فقدان تعاملات اجتماعی و فعالیت فیزیکی و ترس از عدم آمادگی [۱۲]. این شرایط می‌تواند در بسیاری از افراد باشد و باعث ایجاد استرس و اضطراب شود که می‌تواند شانس قربانی‌شدن در یک حمله را افزایش دهد. همچنین، تغییر ناگهانی زمینه‌های کار، به این معنی بوده است که شرکت‌ها مجبور شده‌اند ساختارهای کاری جدید را تعبیه کرده و به‌طور بالقوه دارایی‌های شرکت را به‌دلیل قابلیت همکاری کمتر محافظت کنند. از زمان شروع COVID-19، تعداد کلاه‌برداری‌ها و حملات بدافزار به‌طور قابل توجهی افزایش یافته است [۱۳] و گزارش شده که فیشینگ در مارس ۲۰۲۰، ۶۰۰٪ افزایش یافته است [۱۴]. طی آوریل ۲۰۲۰، گوگل روزانه ۱۸ میلیون بدافزار و ایمیل فیشینگ مربوط به ویروس را مسدود کرد [۱۵]. برای افزایش احتمال موفقیت، این حملات، فروش کالاهای با تقاضای زیاد (به‌عنوان مثال تجهیزات حفاظت شخصی و کیت‌ها و داروهای آزمایش ویروس کرونا)، سرمایه‌گذاری‌های بالقوه سودآور در سهام مربوط به COVID-19 و جعل هویت نمایندگان مردم را هدف قرار می‌دهد. مانند جعل هویت مقامات سازمان بهداشت جهانی و کلاه‌برداری از طریق کمک‌رسانی [۱۶]. حملات بی‌رحمانه به سیستم‌های

[1] Cybersecurity and Infrastructure Security Agency (CISA)
[2] RAT

دسک تاپ از راه دور مایکروسافت[1] نیز افزایش یافته است [۱۷]، که نشانه حملات به فناوری است، نه تنها به جنبه‌های انسانی. بنابراین روشن است که مهاجمان در تلاشند تا از اختلالات ناشی از بیماری همه گیرانه حداکثر استفاده را ببرند، به خصوص با توجه به ادامه آن. در نتیجه، چندین دستورالعمل و توصیه نیز برای محافظت در برابر حملات منتشر شده است. این دستورالعمل‌ها برای کاهش تهدیدهای فزاینده ضروری هستند، اما برای تقویت مبانی آنها، ابتدا باید درک اساسی از حملات سایبری در حال انجام باشد. این مقاله می‌کوشد تا با تعیین یک جدول زمانی از حملات سایبری و در نظر گرفتن چگونگی تأثیر آنها بر شهروندان و نیروی کار، به این شکاف در تحقیق و عمل بپردازد.

۲- جدول زمانی حملات سایبری مرتبط با COVID-19

حوادث جرم سایبری برآمده از بیماری همه گیر COVID-19 تهدیدهای جدی‌ای را متوجه امنیت و اقتصاد جهانی در سراسر جهان نمود، از این رو درک مکانیسم‌های آنها و همچنین انتشار و دستیابی به این تهدیدات ضروری است. برای تحلیل چگونگی وقوع چنین رویدادهایی از تعاریف رسمی گرفته تا رویکردهای سیستماتیک بررسی ماهیت تهدیدها، راه حل‌های زیادی در ادبیات ارائه شده است [۱۸]. گرچه این رویکردها دسته بندی حمله را امکان پذیر می‌کنند، اما اغلب فاقد توانایی جانمایی وقایع بزرگتر و توزیع شده همانند موارد ارائه شده در این نوشته هستند، آنجاکه وقایع زیادی از همه گیری ناشی می‌شود، حال آنکه ارتباطی با آن ندارد. برای این منظور، ما به طور موقت تجسم زمانی را انتخاب کردیم تا بتوانیم وقایع را بدون به خطر انداختن روایت ترسیم کنیم [۱۹]. بعلاوه، این نوع تجسم در حوزه امنیت سایبری برای نشان دادن حملات سایبری متعاقب آن استفاده می‌شود [۲۰].

الف. رویکرد ایجاد جدول زمانی

در این بخش، ما روش مورد استفاده برای ایجاد جدول زمانی را بیان می‌کنیم. ما عبارات جستجوی مورد استفاده برای جمع آوری اطلاعات مربوط به حمله سایبری COVID-19، منابع داده (موتورهای جستجو) مورد استفاده، منابع اطلاعاتی را که برای تمرکز انتخاب کردیم و انواع حمله را توضیح می‌دهیم. همچنین محدودیت‌های بالقوه کار را مورد تأکید قرار می‌دهیم.

۲-۱- نامگذاری

ما طیف وسیعی از حملات سایبری که در طی همه گیری بیماری COVID-19 اتفاق افتاده است را کشف می‌کنیم. ویروس کرونا در زبان انگلیسی با اصطلاحات مختلفی از جمله Coronavirus، Covid19، COVID-19، 2019-nCoV و SARS-CoV-2 مورد اشاره قرار گرفته است. ما از واژه COVID-19 برای اشاره به ویروس استفاده می‌کنیم، که مطابق با اصطلاحاتی است که توسط سازمان بهداشت جهانی استفاده می‌شود [۲۱].

۲-۲- ساخت جدول زمانی

برای کمک به ساخت جدول زمانی، در ابتدا تعدادی جستجو برای شناسایی حملات سایبری مرتبط با این همه‌گیری انجام دادیم. این حملات سایبری براساس نوع حمله و روش تحویل طبقه بندی شده و براساس تاریخ آنها ترتیب داده شده است. اطلاعات جمع آوری شده و در شکل (۲) ارائه شده است که مبنایی برای ایجاد جدول (۱) است.

اطلاعات ارائه شده در جدول زمانی شامل تاریخ هشدار چین به سازمان بهداشت جهانی در مورد ویروس، تاریخ اعلام رسمی همه گیری و حملات سایبری است که به طور خاص مربوط به بیمارستان‌ها یا دارو است. علاوه بر این، کشورهای مهم درگیر در همه گیری شناسایی شدند و اولین مورد شناسایی شده، قفل زمانی ایجاد شده و اولین حمله سایبری را که متحمل شدند؛ به آنها ارائه شد. این جدول به بررسی زیر مجموعه‌ای از اطلاعات جدول زمانی می پردازد.

علاوه بر این، تعدادی از منابع ارائه دهنده گزارش حملات انتخاب شده‌اند. این منابع ترکیبی از رسانه‌های خبری معتبر (مانند رویترز و بی بی سی)، مقالات وبلاگ، گزارش شرکت‌های امنیتی و پست‌های رسانه‌های اجتماعی است. اگرچه مقالات وبلاگ‌ها و پست‌های رسانه‌های اجتماعی به عنوان منبع آکادمیک در نظر گرفته نمی‌شوند، اما در متن این تحقیق که در حال بررسی یک تهدید در حال ظهور هستیم، آنها اطلاعات مهمی در مورد روند حملات سایبری ارائه می‌دهند. همچنین توجه به این نکته مهم است که حملات سایبری ممکن است ابتدا در این حوزه‌ها ارائه شود، قبل از اینکه توسط رسانه‌های اصلی برجسته شود. با توجه به درج گزارش‌های خبری در جدول حملات و جدول زمانی بعدی، باید اذعان کرد که این حملات از طریق لنز روزنامه

[1] RDP

نگاری ارائه شده و به همین دلیل ممکن است تلاشی برای برجسته سازی موضوع باشد. با این وجود، این حملات سایبری گزارش شده هنوز تهدیدی ملموس برای عموم مردم در طی بیماری همه گیر COVID-19 است. این جدول زمانی به دنبال ارائه یک نمای کلی از حملاتی است که رخ داده است.

بررسی وضعیت گزارشات از اواسط مارس تا اواسط ماه مه سال ۲۰۲۰ انجام شد. این جدول زمانی حملات سایبری را به افرادی که تا ۳۱ مارس تجربه کرده‌اند، محدود می‌کند. دلیل این امر آنست که ما به آنچه که اعتقاد داشتیم رسیدیم و آن یک نقطه اشباع شامل تعداد کافی حملات سایبری برای نمایندگی بود. پس از پایان جستجو، اولین حمله گزارش شده در ۶ ژانویه ۲۰۲۰ بود [۲۳]، در حالی که آخرین حمله ذکر شده در جدول زمانی ۳۱ مارس ۲۰۲۰ بود [۲۴]. آخرین حمله ذکر شده در جدول ۱۳ ماه مه سال ۲۰۲۰ بود [۲۵]. این جدول دوره زمانی را کمی جلوتر می‌برد، زیرا قصد دارد جزئیات بیشتری را در مورد حملات سایبری تجربه شده در این مدت ارائه دهد. منابع از تعدادی مکان جمع شده بودند. معیارهای مورد استفاده برای یافتن گزارش‌ها در زیر تعریف شده‌اند و به روشی مشابه با بررسی‌های موجود در ادبیات امنیت سایبری ارائه شده‌اند [۲۶]. ساختار جدول زمانی با جزئیات بیشتر در بخش سوم شرح داده شده است.

الف: موتورهای جستجو

در ایجاد جدول زمانی از چندین موتور جستجو استفاده شده است. اینها عبارتند از: Google1 (مستقر در ایالات متحده و مسلط بر سهم بازار موتور جستجو)، Baidu2 (ارائه دهنده جستجوی مستقر در چین)، Qwant3 (موتور جستجوی مستقر در فرانسه با تمرکز بر حریم خصوصی) و DuckDuckGo4 (موتور جستجوی مستقر در ایالات متحده با تمرکز بر روی حریم خصوصی).

ب: کلمات کلیدی مورد استفاده

هنگام جمع‌آوری گزارش حملات سایبری، از کلمات کلیدی متنوعی استفاده شد. اصطلاحات غیر انگلیسی با استفاده از سرویس Google Translate [۲۷] ترجمه شدند و منابع مستقل دیگری نیز به‌عنوان ابزاری برای تأیید ترجمه استفاده شدند. هنگام تمرکز بر روی خود ویروس، از کلمات کلیدی زیر استفاده می‌شود: ترجمه چینی برای کرونا ویروس[۱] و ترجمه ژاپنی برای کرونا ویروس[۲] تأیید شده توسط وزارت بهداشت، کار و رفاه ژاپن [۲۸]). هنگام جستجو برای حملات سایبری، از عبارات کلیدی زیر استفاده شد: در ترجمه چینی به معنای حمله به شبکه [۲۹] یا حملات سایبری[۳] [۳۰]، در ترجمه ژاپنی برای حملات سایبری یا حملات هک[۴] [۳۱] در ترجمه فرانسوی برای حملات کامپیوتری[۵] [۳۲]، در ترجمه ایتالیایی برای حملات سایبری[۶] [۳۳].

ج: دامنه زمانی

ما سعی کردیم اولین حمله سایبری گزارش شده را که با بیماری همه گیر COVID-19 همراه بود پیدا کنیم. برای امکان توسعه جدول زمانی و تجزیه و تحلیل یافته‌ها، اواسط ماه مه سال ۲۰۲۰ به عنوان نقطه برش تعریف شد و آخرین مقاله خبری مربوط به تاریخ ۱۳ مه ۲۰۲۰ است.

د: معیارهای خروج

اگرچه یک جدول جامع زمانی ایجاد کرده‌ایم، اما تعدادی از نتایج از تحقیق خارج شدند. اینها شامل نتایجی بود که: الف) پشت دیوار پرداخت بودند، ب) ایجاد حساب مورد نیاز قبل از نمایش کامل مقاله، ج) کپی از گزارش‌های خبری موجود و د) قابل ترجمه نبودند.

۳- انواع حملات سایبری

برای هدایت تجزیه و تحلیل و ایجاد جدول زمانی حملات سایبری مربوط به COVID-19، تصمیم گرفتیم حملات را بر اساس انواع آنها تعریف کنیم. این به ما اجازه می‌دهد تا برجستگی را در انواع خاصی از حملات بررسی کنیم. اگرچه طبقه‌بندی‌های متعددی در رابطه با حملات و جرایم اینترنتی وجود دارد، اما هیچ الگوی پذیرفته شده جهانی وجود ندارد [۳۴]. بنابراین، در این کار، ما به طبقه‌بندی که سرویس دادستانی سلطنتی بریتانیا از جرم سایبری[۷] ارائه کرده است، اعتماد کردیم. این تعریف به طور پیش فرض شامل امنیت سایبری است و بسیاری از تعاریف بین‌المللی از جرایم اینترنتی از آن الهام گرفته است.

سرویس دادستانی سلطنتی بریتانیا جرایم سایبری را به دو دسته گسترده تقسیم می‌کند: جرایم وابسته به سایبر و جرایم سایبری [۲۲]. جرم وابسته به فضای

[1] . sarscov-2, Covid, Covid19, Coronavirus, 冠状病毒

[2] . コロナウイルス

[3] . 网络攻击

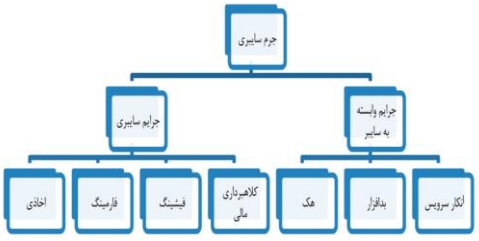
[4] . サイバ 攻

[5] . Attaque Informatique

[6] . Attacco Informatico

[7] . UK Crown Prosecution Service (CPS)

سایبری یک جرم است، که فقط با استفاده از رایانه، شبکه‌های رایانه‌ای یا شکل دیگری از فناوری ارتباطات و اطلاعات قابل ارتکاب است [۳۵]. جرایم وابسته به سایبر عبارتند از: جرایم سنتی، که می‌توانند با استفاده از رایانه، شبکه‌های رایانه‌ای یا سایر اشکال فناوری ارتباطات و اطلاعاتی در مقیاس یا دامنه خود افزایش یابند [۳۶]. این دسته‌ها و همچنین نمونه‌هایی از زیر مجموعه‌های آنها در شکل ۱ دیده می‌شود. برخی از عناصر توصیف شده توسط سرویس دادستانی سلطنتی بریتانیا اغلب در یک حمله سایبری به هم پیوند می‌خورند. به عنوان مثال، ممکن است از یک ایمیل یا پیام متن فیشینگ (به عنوان مثال پیام کوتاه یا واتس آپ) برای جلب قربانی به سمت یک وب سایت تقلبی استفاده شود. وب سایت ممکن است داده‌های شخصی را که برای ارتکاب کلاهبرداری مالی استفاده می‌شود، جمع آوری کند یا ممکن است بدافزار (به طور خاص، باج افزار) را نصب کند که سپس برای اخاذی استفاده می‌شود. این مفهوم از توالی‌های حمله سایبری با جزئیات بیشتر در بخش سوم توضیح داده شده است.



(شکل-۱): جرایم وابسته به سایبر و جرایم سایبری

به همین نحو، حملات انکار سرویس[1] به طور فزاینده‌ای توسط مجرمان اینترنتی برای حواس پرتی در طول تلاش برای هک کردن مورد استفاده قرار می‌گیرد [۴۰]. در ادامه، انواع این حملات را در نظر می‌گیریم و نحوه راه‌اندازی آنها را منعکس می‌کنیم، از جمله عوامل انسانی یا جنبه‌های فنی (به عنوان مثال آسیب پذیری‌ها) که آنها می‌خواهند از آن استفاده کنند.

فیشینگ یا مهندسی اجتماعی به طور گسترده‌تر، شامل تلاش غیرقانونی گروه‌ها برای ترغیب افراد به انجام عملی (به عنوان مثال: به اشتراک گذاشتن اطلاعات یا بازدید از یک وب سایت) به این بهانه است که آنها با یک گروه قانونی درگیر هستند. اغلب اوقات از پیام‌های ایمیل استفاده می‌شود، گاهی اوقات از پیامک یا پیام واتس آپ استفاده می‌شود (که به آن smishing گفته می‌شود). مهندسی اجتماعی مشابه فیشینگ است اما مهاجمان به جای فریب کاربران برای بازدید از سایت‌های مخرب، به سیستم‌های خطرناک (به عنوان مثال دستگاه کاربر یا سرورهای DNS[2] برای هدایت افراد به سایت‌های غیرقانونی استفاده می‌کنند. این نوع حمله به طور کلی کمتر رایج است، زیرا نیاز به دسترسی بیشتر به قابلیت‌های فنی دارد. کلاهبرداری مالی به طور کلی شامل فریب افراد یا سازمان‌ها است که برای سود مالی مهاجم یا مجرم استفاده می‌کنند. اخاذی به اعمالی گفته می‌شود که افراد را تهدید یا مجبور به انجام برخی اقدامات، معمولاً امور مالی می‌کند.

حملات هک، بدافزار و انکار سرویس نوعی جرم است که بیشتر مورد توجه مهاجمان فنی قرار می‌گیرد. هک کردن به معنای به خطر انداختن یکپارچگی یک سیستم است و به مهارت کافی نیاز دارد. تکنیک‌های آن می‌تواند شامل سو استفاده از آسیب پذیری‌های سیستم برای ورود به سیستم‌ها باشد. بدافزار به نرم افزار مخربی اطلاق می‌شود که می‌تواند برای ایجاد اختلال در خدمات، استخراج داده و طیف وسیعی از حملات دیگر مورد استفاده قرار گیرد. Ransomware (نوعی باج افزار) یکی از رایج‌ترین نوع بدافزارهای امروزی است [۴۱] و بدافزار را با تلاش برای اخاذی ترکیب می‌کند. حملات انکار سرویس با هجمه به سرویس‌های اصلی و با درخواست‌های نامشروع، در دسترس بودن و فعالیت سیستم را هدف قرار می‌دهد. هدف در اینجا مصرف پهنای باند مورد استفاده برای درخواست‌های مجاز سرور و نهایتاً مجبور کردن سرور آفلاین است.

این نوع از حملات، مبنایی برای تجزیه و تحلیل ما در این جدول زمانی و چگونگی رویکرد ما به بحث خود را در بخش بعدی این تحقیق فراهم می‌نماید.

۴- محدودیت‌های جدول

در جدول (۱)، دو ستون که مربوط به تاریخ هاست ارائه شده است. ستون اول «تاریخ مقاله» به تاریخ انتشار اولیه مرجع اشاره دارد. ما اذعان می‌کنیم که در برخی موارد، صفحات وب مرتبط با منابع، با اطلاعات بعدی، پس از درج آن در مقاله، به روز شد. این جدول توسط «تاریخ مقاله» ترتیب داده شده است تا نمایش زمانی منسجمی از وقایع ارائه دهد. ما همچنین ستون دوم، «تاریخ حمله» را ارائه داده‌ایم. هنگام بررسی هر مرجع، اگر تاریخ مشخصی برای

[1] Denial of Service (DoS)

[2] Domain Name System (DNS)

زمان اجرای حمله در نظر گرفته شده باشد، آن ذکر شده است. دلیل منطقی درج تاریخ حمله و تاریخ گزارش این است که حمله ممکن است تا چند روز پس از اجرای آن ظاهر نشود.

۵- محدودیت‌های جدول زمانی

دو نوع گزارش حمله سایبری در این دست نوشته در نظر گرفته شده است، مواردی که حملات سایبری را بدون ارائه تاریخ حمله توصیف می‌کنند و مواردی که حملات سایبری را توصیف می‌کنند و تاریخ ارتکاب آن را شامل می‌شوند. وقتی تاریخ حمله درج نشده باشد، تاریخ ارائه شده در جدول زمانی به تاریخ انتشار اشاره دارد. منطق گنجاندن هر دو نوع گزارش بر اساس ارائه یک تقویم زمانی از وقایع است. علاوه بر این، در حالی که این جدول مروری گسترده از چشم انداز تهدید را ارائه می‌دهد، اما به هیچ وجه لیستی جامع از تمام حملاتی نیست که در رابطه با بیماری همه گیر انجام شده است، زیرا جمع آوری چنین اطلاعاتی در این زمینه به دلیل عدم وجود و کیفیت گزارش دهی، تعداد حوادث هدفمند، تعداد حوادث مورد هدف عموم مردم، پوشش جهانی همه گیر و تعداد بازیگران مخربی که این حملات را انجام می‌دهند، امکان ندارد. با این وجود، علی رغم این محدودیت‌ها، ما تمام منابع موجود را برای تجسم دقیق‌تر از تهدیدات بررسی کرده‌ایم.

ب. جدول زمانی

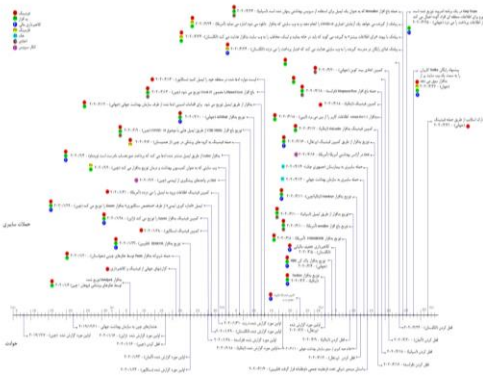
در این بخش، حملات سایبری را با جزئیات بیشتر بررسی می‌کنیم. شکل (۲) نمایشی دقیق از زنجیرهٔ حملات سایبری کلیدی ناشی از همه گیری COVID-19 را ارائه می‌دهد. این جدول زمانی شامل اولین موارد گزارش شده در چین، ژاپن، آلمان، سنگاپور، اسپانیا، انگلستان، فرانسه، ایتالیا و پرتغال و سپس آگهی‌های قفل بعدی است. این جدول زمانی ۴۳ حمله سایبری را دسته‌بندی می‌کند که با استفاده از طبقه‌بندی سرویس دادستانی سلطنتی بریتانیا شرح داده شده در بخش سوم طبقه بندی می‌شوند و به اختصار عنوان می‌شوند: P: فیشینگ، M: بدافزار، Ph: فارمینگ، E: اخاذی، H: هک، D: انکار خدمات و F: کلاه‌برداری مالی. وقایع مربوط به بحران برای اطمینان از تولید دقیق زمانی در سازمان بهداشت جهانی تائید شدند. جدول۱ تعدادی از حملات سایبری را با جزئیات بیشتر شرح می‌دهد. در داخل جدول، حملات سایبری براساس تاریخ حمله سازمان یافته‌اند. اگر تاریخ حمله در مرجع موجود نبود، از تاریخ مقاله استفاده شده است. کشور هدف هر سایبر همراه با شرح مختصری از روش‌های اتخاذ شده ذکر شده است. سرانجام، نوع حمله نیز طبق طبقه بندی سرویس دادستانی سلطنتی بریتانیا که قبلاً توضیح داده شد طبقه بندی شده است، جایی که در مرجع ذکر شده است. هر دو شکل و جدول حملات و حوادث خاص سایبری را نشان می‌دهد و موارد زیر را شامل نمی‌شود: مشاوره‌های عمومی (به‌عنوان مثال از ادارات دولتی)، بحث‌های کلی و خلاصه‌ای از حملات و توضیحات دقیق تکنیک‌ها و روش‌های استفاده شده توسط مهاجمان.

ج. حملات سایبری COVID-19 در انگلستان

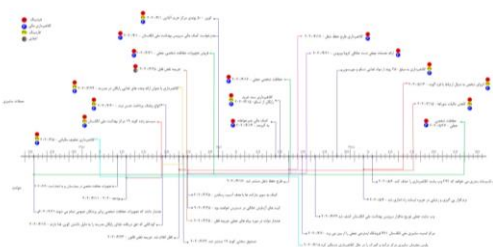
میزان مشکلات مربوط به امنیت سایبری بسیار استثنایی بود و در این بخش ما از انگلستان به‌عنوان یک مطالعه موردی برای تجزیه و تحلیل جرایم سایبری مرتبط با COVID-19 استفاده می‌کنیم. بحث در اینجا نشان می‌دهد همانطور که انتظار می‌رفت و در بالا توضیح داده شد، یک ارتباط ضعیف بین اعلامیه‌های سیاسی / اخبار و کمپین‌های مرتبط با جرایم اینترنتی وجود داشت. تجزیه و تحلیل ارائه شده در اینجا فقط به وقایع جرایم سایبری مخصوص انگلیس متمرکز است. بنابراین، اگرچه بسیاری از حوادث شناسایی شده در بخش قبلی و به ویژه در [۷۰] حملات سایبری جهانی هستند، اما بحث در اینجا این موارد را نادیده می‌گیرد. در نتیجه، بیانیه‌های متعددی که گویا از طرف سازمان‌های معتبری مانند سازمان بهداشت جهانی و بسیاری از بدافزارها که به شهروندان انگلیس رسیده است، نادیده گرفته می‌شوند، زیرا این موارد خاص انگلستان نبود. نشانه‌هایی از میزان حادثه جرایم سایبری انگلستان که در طی همه گیری تجربه شده است، توسط سطح گزارش شده از ایمیل‌های مشکوک و تقلب گزارش شده است. در اوایل ماه مه ۲۰۲۰، بیش از ۱۶۰۰۰۰، نامه الکترونیکی «مشکوک» به مرکز امنیت سایبری ملی انگلستان [۷۱] گزارش شده بود و در پایان ماه مه ۲۰۲۰، ۴/۶ میلیون پوند خسارت کلاه‌برداری‌های مرتبط با COVID-19 با حدود ۱۱۲۰۶ قربانی کمپین‌های فیشینگ و یا دزدی سایبری (smishing) بوده است [۷۲]. در واکنش، مرکز امنیت سایبری ملی انگلستان؛ ۴۷۱ فروشگاه آنلاین جعلی [۷۳] و مرکز فرهنگ و درآمد باشکوه[1] و ۲۹۲ وب سایت جعلی را بست. [۷۴]. جدول زمانی در شکل (۳) مجموعه‌ای از وقایع خاص انگلیس و حوادث جرایم سایبری را نشان می‌دهد. جدول زمانی همبستگی مستقیم و معکوس بین اعلامیه‌ها و حوادث را نشان می‌دهد.

[1] . Her Majesty's Revenue and Customs (HMRC)

همبستگی مستقیم مواردی است که به نظر می‌رسد مرتکبین اعلامیه‌ها یا رویدادها را دنبال می‌کنند، ممکن است این رویدادها را مورد توجه قرار داده و حملات سایبری را به دقت در چارچوب سیاست تنظیم کرده‌اند. اینها در شکل با یک پیکان اتصال رنگی ثابت نشان داده شده است. همبستگی معکوس مواردی است که یک حادثه ارتباط مشخصی با یک رویداد یا اعلامیه ندارد. اگرچه ارتباط مستقیم همبستگی معکوس به نظر نمی‌رسد؛ اما ممکن است وجود داشته باشد زیرا تعدادی از وقایع به طور فعال در رسانه‌ها برجسته شده‌اند. به‌عنوان مثال، موضوع تجهیزات حفاظت شخصی قبل از توجه دولت انگلستان، به‌عنوان بحث مهم بود. به همین ترتیب، احتمال طرح تخفیف مالیاتی در اوایل ماه مارس قبل از اعلام بودجه در تاریخ ۱۱-۰۳-۲۰ در حال بررسی بود. اولین کمپین‌های فیشینگ تخفیف مالیاتی قبل از اعلام بودجه در گردش فعال بودند. در هر دو مورد، باید تأکید کنیم که این همبستگی‌ها سست هستند و باید کار بیشتری در این زمینه انجام شود که آیا می‌توان با استفاده از این داده‌ها در سراسر جهان به‌عنوان نمونه، مدل پیش‌بینی ساخت.



(شکل-۲): جدول زمانی وقایع کلیدی مربوط به حملات سایبری و بیماری همه گیر covid – 19



(شکل-۳) : جدول زمانی انگلستان

در یازدهم مارس ۲۰۲۰، دولت انگلیس تعدادی از اعلامیه‌های مهم بودجه [۷۵] را صادر کرد که شامل: صندوق واکنش اضطراری ۵ میلیارد پوندی برای حمایت از سرویس بهداشت ملی و سایر خدمات عمومی در انگلیس بود. استحقاق پرداخت قانونی حقوق بیمار برای افرادی که به قرنطینه شدن توصیه می‌شوند؛ صندوق ۵۰۰ میلیون پوندی سختی مشاغل آزاد برای شوراها به منظور کمک به آسیب پذیرترین افراد در مناطق خود؛ وام تعطیلی کسب و کار در اثر COVID 19 برای شرکت‌های کوچک؛ و لغو تعرفه تجارت برای شرکت‌های معین.

اندکی بعد، دولت همچنان به صدور اطلاعیه‌هایی برای حمایت از شهروندی و اقتصاد ادامه داد. این اطلاعیه‌ها شامل: طرحی برای حمایت از کودکانی که حق دریافت وعده‌های غذایی رایگان در مدرسه را دارند (۱۹-۰۳-۲۰). صندوق سختی (۲۴-۰۳-۲۰) کمک به سوپرمارکت‌ها، برای افراد آسیب پذیر (۲۵-۰۳-۲۰) احتمال دسترسی کیت‌های تست خانگی (۲۵-۰۳-۲۰) طرح حفظ شغل (۱۷-۰۴-۲۰) و راه اندازی برنامه ردیابی[1] با بیشترین متقاضی (۰۴-۰۵-۲۰).

ردیف	منبع	کشور	نوع حملات	شرح	تاریخ حمله	تاریخ حمله
۱	۲۳	چین	P.M	ویندم منهم به راه اندازی کمپین فیشینگ METALJACK علیه دفاتر منطقه ویغل شد.	۲۰۲۰/۲/۲۲	۲۰۲۰/۲/۱۶
۲	۲۴	جهانی	P.M	گزارش‌های بین‌المللی نشان می‌دهد که هر دو کمپین فیشینگ و کلاهبرداری در حال انجام است.	۲۰۲۰/۱/۱۸	-
۳	۲۳	چین، مغولستان	P.M	هکرهای چینی منهم به توزیع بدافزار Vicious Panda به مغولستان از طریق ایمیل هایی که ادعا می شود از وزارت امور مغولستان است.	۲۰۲۰/۲/۱۲	۲۰۲۰/۱/۲۰
۴	۲۴	فیلیپین	P.M.F	بدافزار REMCOS به شهروندان فیلیپینی توزیع شده است.	۲۰۲۰/۲/۱۳	۲۰۲۰/۱/۲۲
۵	۲۵	سنگاپور	P	کمپین فیشینگ اعتبار ورود به سیستم ایمیل را می‌دزدند.	۲۰۲۰/۲/۱۸	-
۶	۲۶	ژاپن	P.M.F	کمپین فیشینگ اقدامات ایمنی بدافزار Emotet را توزیع می‌کند.	۲۰۲۰/۲/۱۸	۲۰۲۰/۱/۲۸
۷	۲۷	چین	P.M.F	ایمیل «اتیاره گیری ایمنی» از سوی «متخصص سنگاپوری» بدافزار Emotet را توزیع می‌کند.	۲۰۲۰/۲/۱۶	۲۰۲۰/۱/۲۹
۸	۲۵	آمریکا	P	لیست ادعای ایمیل موارد COVID-19 در شهر فریلی، کارپ را به وب سایتی می‌برد که اطلاعات را می‌دزدند.	۲۰۲۰/۲/۱۱	۲۰۲۰/۱/۳۱
۹	۲۸	چین	H	DoS در واحدهای پیشگیری از اپیدمی	۲۰۲۰/۲/۱۹	۲۰۲۰/۲/۲
۱۰	۲۸	چین	P	کمپین فیشینگ اعتبار ورود به سیستم ایمیل را می‌دزدند.	۲۰۲۰/۲/۱۹	۲۰۲۰/۲/۲
۱۱	۲۹	جهان	P.M.F	اولین موارد بدافزار سرقت داده AZORult	۲۰۲۰/۲/۱۰	-
۱۲	۵۰	چین	P.M	اقدامات ایمنی تخصصی از طرف WHO خواستار بازگیری بدافزار هستند.	۲۰۲۰/۲/۱۲	-
۱۳	۲۴	ویندم	P.M	بدافزار LOKIBOT از طریق ایمیل منتشر شده و ادعا می کند پرداخت فاکتور نادرست است.	۲۰۲۰/۲/۱۳	۲۰۲۰/۲/۳
۱۴	۵۱	چین	P.Ph	حمله فیشینگ به گروه‌های پزشکی در چین (از هند)	۲۰۲۰/۲/۱۶	۲۰۲۰/۲/۶
۱۵	۵۲	چین	P.M.E	توزیع باج افزار CXK-NMSL از طریق ایمیل‌های مضمون COVID-19	۲۰۲۰/۲/۱۸	۲۰۲۰/۲/۹
۱۶	۵۲	چین	P.M.E	توزیع باج افزار Dharma / Crysis از طریق ایمیل‌های مضمون COVID-19	۲۰۲۰/۲/۱۸	۲۰۲۰/۲/۱۳
۱۷	۲۴	ایتالیا	P.M	بدافزار Trickbot از طریق ایمیل توزیع می‌شود.	۲۰۲۰/۲/۱۳	۲۰۲۰/۲/۳
۱۸	۵۳	جهانی	P.M.F	بدافزار باگ کن MBR که به عنوان اطلاعات رتبابی تعلی میدل شده است.	۲۰۲۰/۲/۱۴	-
۱۹	۲۴	آمریکا	P.M	بدافزار FORMBOOK توزیع شده از طریق ایمیل متناوره حمل بسته	۲۰۲۰/۲/۱۳	۲۰۲۰/۲/۸
۲۰	۵۲	آمریکا	M	سیستم‌های بهداشتی در ناحیه بهداشت عمومی (ایلینوی) تحت تأثیر باج افزار netwalker قرار دارند.	۲۰۲۰/۲/۱۳	۲۰۲۰/۲/۱۰
۲۱	۲۴	اسپانیا	P.M	ایمیل ادعا می کند که درمان COVID-19 هماطیور است که دانشمندان اسرائیلی روزها قبل از آن صحبت کرده‌اند.	۲۰۲۰/۲/۱۳	۲۰۲۰/۲/۱۰
۲۲	۵۵	چک	H	حمله سایبری به بیمارستان چک	۲۰۲۰/۲/۱۳	۲۰۲۰/۲/۱۲
۲۳	۵۶	آمریکا	H	ارگار خدمات در آژانس بهداشتی ایالات متحده	۲۰۲۰/۲/۱۶	-
۲۴	۵۷	لیبی	P.M	Corona live 1.1 یک بدافزار SpyMax است که در این مورد یک برنامه ترجمان شده است که اطلاعات کاربر را از بین می‌برد.	۲۰۲۰/۲/۱۸	-
۲۵	۵۸	جهان	P.M	پیشنهاد مالیک کرونا چیزی را غصب می کند که به نظر می رسد یک بدافزار بی ضرر است و یک پیام کوتاه را به تمام مخاطبین توزیع می کرد. احتمالاً با به روزرسانی برنامه بدافزار را مسیح می کند.	۲۰۲۰/۲/۱۹	-
۲۶	۵۹	جهانی	P.E	کمپین اخاذی تهدید می کند که گیرنده را با COVID-19 آلوده می کند مگر اینکه پرداخت ۲۰۰۰ دلار بیت کوین انجام شود.	۲۰۲۰/۲/۲۰	۲۰۲۰/۲/۲۰
۲۷	۶۰	اسپانیا	P.M	حمله باج افزار Netwalker که به عنوان یک ایمیل در مورد استفاده از سرویس بهداشتی پنهان شده است.	۲۰۲۰/۲/۲۲	-
۲۸	۶۱	آمریکا	P.M	پیامک از گیرنده می خواهد یک آزمایش اجرای آماده سازی COVID-19 انجام دهد و به وب سایتی که بدافزار را ربا گیری می کند اشاره دارد.	۲۰۲۰/۲/۲۲	۲۰۲۰/۲/۲۲
۲۹	۶۲	انگلستان	P.M	پیامک با پیوند برای اطلاعات بیشتر به گیرنده می گوید که در خانه بمانید. پیوند، گیرنده را به یک وب سایت آلوده به بدافزار هدایت می کند.	۲۰۲۰/۲/۲۲	-
۳۰	۶۳	انگلستان	P.Ph.F	پیامک غذای رایگان مدرسه، گیرنده را به وب سایتی هدایت می کند که اعتبار پرداخت را می‌دزدند.	۲۰۲۰/۲/۲۳	۲۰۲۰/۲/۲۲
۳۱	۶۴	جهان	M.F	Gimp Trojan در یک برنامه تقویه توزیع شده است. برنامه برای کسب اطلاعات در مورد افراد آلوده در منطقه گیرنده ۰۷۵. است. در واقع این اطلاعات پرداخت را سرقت می کند.	۲۰۲۰/۲/۲۵	-
۳۲	۲۴	جهانی	P	گواهینامه‌های اسکلیب که از طریق یک کار فیشینگ سانحگی به سرقت رفته است.	۲۰۲۰/۲/۲۲	۲۰۲۰/۲/۲۱
۳۳	۶۵	جهان	P.Ph.M.F	پیشنهاد رایگان Netflix کاربران را به سمت یک وب سایت پر از بدافزار سوق می دهد.	۲۰۲۰/۲/۲۲	-
۳۴	۶۶	انگلستان	M	وب سایت جعلی NHS اطلاعات کاربری را جمع آوری می کند.	۲۰۲۰/۲/۲۵	-
۳۵	۶۷	انگلستان	P.M	ایمیل پیشنهاد می کند که طبق آخرین اطلاعیه دولت انگلیس، پرداخت شغل خود را ارگ دهید.	۲۰۲۰/۲/۲۰	۲۰۲۰/۲/۱۹
۳۶	۶۸	جهانی	M	Coronalocker رایانه را قفل می کند و به نظر می‌رسد پیش از آسیب واقعی باعث ارز و اذیت می‌شود.	۲۰۲۰/۲/۲۱	-
۳۷	۶۹	جهانی	P.M	گیرندگان Docusign به وب سایت جعلی با ارگ اطلاعات COVID-19 هدایت می‌شوند.	۲۰۲۰/۲/۱۸	-
۳۸	۲	انگلستان	P.M	گیرندگان به یک وب سایت رهگیری و ردیابی جعلی هدایت می شوند که اطلاعات کاربری کارپ را جمع آوری می‌کند.	۲۰۲۰/۱/۲۲	-

(جدول-۱): توصیف حملات سایبری مرتبط با COVID 19

[1] . track and trace

تاریخ رویداد	رویداد	تاریخ حادثه	نوع	حادثه
۲۰۲۰/۲/۲۱ ۲۰۲۰/۳/۹	هشدار پزشکان به اتمام تجهیزات حفاظت شخصی در بیمارستان‌ها	۲۰۲۰/۴/۱۷ ۲۰۲۰/۵/۲۷	P, Ph,F P, Ph,F	پیشنهادات جعلی تجهیزات حفاظت شخصی از طریق ایمیل و پیوند به URL هایی که کارت اعتباری و سایر جزئیات را ضبط می‌کنند.
۲۰۲۰/۳/۱۱	اعلام دولت به طیف وسیعی از بسته‌های کمک مالی در بودجه	۲۰۲۰/۳/۲۰	P Ph F	کمپین Smishing که نوید پرداخت کمک مالی COVID-19 را می‌دهد. پاسخ دهندگان به یک وب سایت جعلی gov.uk هدایت می شوند که جزئیات کارت اعتباری را درخواست می‌کند.
۲۰۲۰/۳/۱۹	دولت طرحی را اعلام می کند که به کودکانی که واجد یک وعده غذایی رایگان در مدرسه هستند، در صورت عدم توانایی ادامه تحصیل در مدرسه، از یک کوپن غذا استفاده می‌کند.	۲۰۲۰/۳/۲۴	P Ph F	یک کارزار کلاهبرداری که والدین را با قول کمک به وعده های غذایی رایگان مدرسه در ازای دریافت اطلاعات بانکی هدف قرار داد. جزئیات بانکی کلاهبرداری می‌شود.
۲۰۲۰/۳/۲۳	افزایش جریمه نقض تخلف ۶۰ پوندی، بعداً (۱۰-۵-۲۰۰۰) به ۱۰۰ پوند.	۲۰۲۰/۳/۲۷	P E	پیامک خلاف قفل
۲۰۲۰/۳/۲۴	صندوق سختی COVID-19 به شوراها امکان می دهد صورتحساب مالیاتی شوراها را برای ۱۵۰ ٪ برای ساکنان در سن کار و با پرداخت جایزه شورای پول، کاهش دهند.	۲۰۲۰/۵/۱۵	P Ph F	کلاهبرداری تخفیف مالیاتی شورای
۲۰۲۰/۳/۲۵	دسترسی به کیت‌های آزمایش خانگی از سوی دولت	۲۰۲۰/۳/۳۱ ۲۰۲۰/۴/۱۷ ۲۰۲۰/۵/۲۷	P F	اقدامات فیشینگ در انگلیس و اسکاتلند قربانیان را به سمت وب سایت های جعلی سوق می‌دهد که ادعا می کنند تجهیزات حفاظت شخصی را می‌فروشند.
۲۰۲۰/۴/۱۷	اعلام طرح حفظ شغل از سوی دولت	۲۰۲۰/۴/۱۹	P F	کمپین فیشینگ طرح حفظ شغل جعلی.

(جدول-۲): همبستگی‌های انتخاب شده بین رویدادها و کارزارهای مجرمانه سایبری

رویدادهایی از این دست احتمال واکنش مثبت به کارزار مجرمانه اینترنتی را افزایش می‌دهد و عاملان آن احتمالاً درگیر حوادث می‌شوند. اگرچه به نظر می‌رسد بین برخی از وقایع و حوادث ارتباط وجود دارد، اما تعدادی از کلاهبرداری‌ها را نمی‌توان به راحتی در یک رویداد یا اعلامیه جستجو کرد. از جمله این موارد می‌توان به پرداخت ۲۵۰ پوند از روی حسن نیت (۲۰-۰۳-۲۱)، درخواست کمک مالی (۰۲-۰۴-۲۰)، هزینه سوپرمارکت‌های انگلیس (۰۲-۰۴-۲۰، ۱۵-۰۴-۲۰، ۲۸-۰۴-۲۰) و یک کمک خیرخواهانه به گیرنده اشاره کرد. هیچ یک از این رویدادها با اطلاعیه‌های دولتی یا حتی گمانه‌زنی‌های عمومی همراه نبوده است.

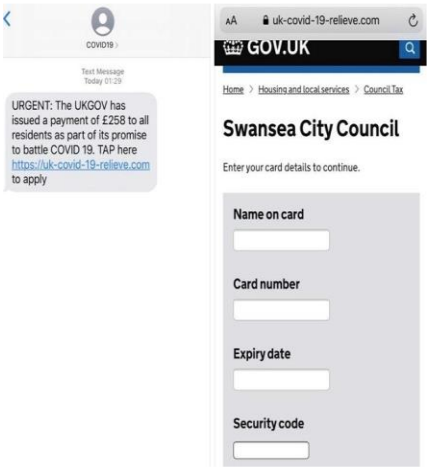
نمونه‌هایی از مفهوم همبستگی بین رویدادها و فعالیت‌های امنیتی سایبری در جدول (۲) ارائه شده است و در شکل (۳) نشان داده شده است. این نمونه‌ها نشان دهنده ارتباط بین رویدادها و کمپین‌های جرایم اینترنتی است. بسیاری از موارد ذکر شده در جدول (۲) و شکل (۳) بسیار ساده بودند. به قربانیان احتمالی URL از طریق ایمیل، پیام کوتاه یا واتس آپ ارائه شده است. نمونه‌ای از این در شکل (۴) ارائه شده است. در این حالت، URL به یک وب سایت سازمانی جعلی اشاره می‌کند که جزئیات کارت اعتباری را درخواست می‌کند. اگرچه عناصری در این فرآیند وجود دارد که برای یک کاربر با تجربه رایانه مشکوک است، به‌عنوان مثال: اشتباهات املایی (بکار بردن واژه تسکین به جای امداد در کلاهبرداری COVID-19)، پاسخ مشکوک به آدرس‌های ایمیل و URL های کاملاً نادرست، اینها بلافاصله برای بسیاری از کاربران مشخص نمی‌شد.

د. تجزیه و تحلیل حملات سایبری و خطرات مرتبط با آن

جدول زمانی نشان داده شده در شکل (۲) و مطالعه موردی انگلستان در بالا یک بستر ایده آل ایجاد می‌کند که از طریق آن می‌توان حملات سایبری را که در پرتو همه‌گیری اتفاق افتاده است، تجزیه و تحلیل کرد. از آنجا که اولین مورد در چین اعلام شد (۱۹-۱۲-۱۹)، اولین حمله سایبری الهام گرفته شده از COVID-19 ۳۰ روز طول کشید. حمله سایبری بعدی گزارش شده ۱۴ روز بود (۱۹-۰۱-۲۰). از این مرحله به بعد مشخص است که بازه زمانی بین وقایع و حملات سایبری به طرز چشم‌گیری کاهش می‌یابد.

۴۳ حمله سایبری ارائه شده در جدول زمانی می‌تواند باشد که بعداً به شرح زیر طبقه‌بندی می‌شود:

- ۳۷ (۸۶٪) شامل فیشینگ می‌شود.
- ۲ (۵٪) شامل هک می‌شود.
- ۲ (۵٪) شامل انکار خدمات می‌شود.
- ۲۸ (۶۵٪) شامل بدافزار بودند.
- ۱۵ (۳۴٪) شامل کلاهبرداری مالی بود.
- ۶ نفر (۱۳٪) داروسازی داشتند.
- ۶ (۱۵٪) شامل اخاذی بود.



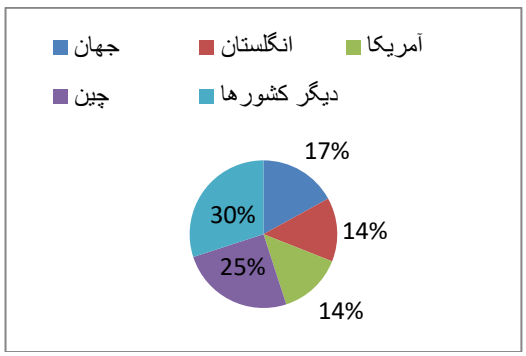
(شکل-۴): کلاهبرداری تخفیف کووید ۱۹ [۷۶]

در حالی که این تجزیه و تحلیل مفید است، توالی وقایع در حمله کامل همچنین می‌تواند بینش اصلی حمله را فراهم کند. جدول زمانی این توالی‌ها را نشان می‌دهد و

کمپین کاملی را شامل می‌شود، به عنوان مثال: توزیع بدافزار (متر) از طریق فیشینگ که اعتبار پرداختی را که برای کلاه‌برداری مالی مورد استفاده قرار می‌گیرد، سرقت می‌کند. می‌توانیم این توالی حمله سایبری را به‌صورت فیشینگ (p)، بدافزار (m)، کلاه‌برداری مالی (f)، فارمینگ (ph)، اخاذی (e)، توصیف کنیم. تجزیه و تحلیل حملات سایبری از این طریق مهم است. زیرا این نشان دهنده چندین نقطه در یک حمله سایبری است که در آن می‌توان از حمایت‌ها استفاده کرد. جدول زمانی توالی‌های حمله سایبری زیر را نشان می‌دهد:

p، m: n = 8، ٪19
p، m، f: n = 10، ٪23
ph، m: n = 1، ٪2
p، ph: n = 1، ٪2
p، p.m.e: n = 5، ٪12
p، ph، m: n = 2، ٪5
p، ph، f: n = 1، ٪2
p، e: n = 1، ٪2
p، ph، m، f: n = 1، 2

این تجزیه و تحلیل شامل توالی رویدادهایی است که در دو حادثه هک و دو واقعه انکار خدمات رخ داده است. لازم به ذکر است که اگرچه کلاه‌برداری مالی محتمل ترین هدف در بیشتر حملات سایبری مندرج در جدول زمانی است، اما کلاه‌برداری مالی تنها آنجا که گزارش‌ها به وضوح نشان می‌دهد که این نتیجه یک حمله سایبری است؛ در جدول زمانی ثبت شده است. درواقع موارد p، m و f، ph و p به احتمال زیاد بیشتر است.



(شکل-۵): توزیع حمله سایبری در سراسر کشورها

در شکل (۵) به برخی از کشورهایی که در طی همه گیری هدف حملات سایبری اولیه قرار گرفتند، بر اساس تاریخ حمله ارائه شده است. همانطور که نشان داده شده است، چین و ایالات متحده آمریکا ٪۳۹ از حملات گزارش شده را تشکیل می‌دهند. همچنین از جدول شماره ۱ مشخص است که هر دو این کشورها از ابتدای ابتلا به بیماری همه گیر هدف اصلی بودند. این حملات سپس به انگلستان و سایر کشورها گسترش یافت. با این حال، تا مارس ۲۰۲۰، اکثریت قریب به اتفاق حملات در کل جهان انجام می‌شود، یادآوری حملاتی که به طور خاص در حوادث یک کشور منفرد متمرکز شده است، مانند تخفیف مالیاتی ناشی از COVID-19، یا پیام‌های فیشینگ ردیابی تماس.

توجه به این موضوع در خصوص حملات سایبری خاص انگلستان مفید است. این بررسی نشان می‌دهد که فیشینگ ترکیبی از تمامی حملات سایبری مورد تجزیه و تحلیل بود. یک مورد اخاذی به عنوان هدف نهایی، شانزده مورد دیگر شامل کلاه‌برداری مالی، نه حمله سایبری متشکل از توالی: p، ph، f، هفت متشکل از توالی p، f ، بقیه شامل p، e.

قابل توجه است که اگرچه یک وب سایت توزیع بدافزار از طریق سرویس بهداشت ملی انگلستان در تاریخ ۲۳ تا ۰۴ کشف و حذف شد، اما هیچ یک از حملات سایبری که ما تجزیه و تحلیل کردیم، به همان روشی که تجزیه و تحلیل جهانی نشان می‌دهد، شامل بدافزار نیست. این ممکن است دلایل مختلفی داشته باشد. راه‌اندازی یک کمپین متصل به بدافزار به پیچیدگی و زمان بیشتری نیاز دارد. ممکن است فرصت کمتری برای اتصال مستقیم آن به یک رویداد یا اعلامیه خاص وجود داشته باشد. تأخیر زمانی بین برخی از اعلامیه‌ها و کمپین‌های مرتبط به طرز چشمگیری کوتاه بود. به عنوان مثال، تاخیر زمانی بین آگهی پلمپ (۲۳-۰۳-۲۰) و «جریمه نقض پلمپ» (۲۵-۰۳-۲۰) ۲ روز بود و تاخیر زمانی بین اطلاعیه طرح حفظ شغل (۱۷-۰۴- ۲۰) و کلاه‌برداری حفظ شغل (۱۹-۰۴-۲۰) نیز ۲ روز بود.

برای تعمق بیشتر در مورد حملات سایبری کشف شده، می‌توانیم ببینیم که فیشینگ (از جمله smishing) با توجه به تجزیه و تحلیل ما، شایع ترین بوده است. در کل، در ٪۸۶ از حملات جهانی نقش داشته است. اما این تعجب آور نیست، زیرا تلاش‌های فیشینگ هزینه کمی دارند و از موفقیت خوبی برخوردار هستند. در مورد COVID-19، این موارد شامل تلاش برای جعل هویت از سازمان‌های دولتی، سازمان جهانی بهداشت، سرویس بهداشت ملی انگلستان، خطوط هوایی، سوپرمارکت‌ها و ارائه دهندگان فناوری ارتباطات است. زمینه خاص حملات می‌تواند کمی متفاوت باشد اما تکنیک‌های اساسی و هدف نهایی یکسان است. به‌عنوان مثال، در یک ایمیل

که هویت سازمان جهانی بهداشت را نشان می‌دهد، مهاجمان یک فایل zip را ضمیمه می‌کنند که ادعا می‌کنند حاوی یک کتاب الکترونیکی است که «تحقیق / منشا کامل ویروس کرونا و راهنمای توصیه شده برای محافظت از خود و دیگران» را ارائه می‌دهد [۷۷]. علاوه بر این، آنها اظهار می‌کنند: «شما اکنون این ایمیل را دریافت می‌کنید زیرا زندگی شما همانطور که همه زندگی می‌کنند، محاسبه می‌شود». در اینجا، مهاجمان، آرم سازمان جهانی بهداشت را با القاء کمک (مابقی ایمیل، حاوی دستورالعمل قانونی است)، استفاده می‌کنند و احساسات مردم را در ساخت ایمیل حمله خود جلب می‌نمایند [۷۸]. تکنیک‌های مشابه را می‌توان در یک وب سایت جعلی سرویس بهداشت ملی انگلستان که توسط مجرمان شناسایی شدهِ در اینترنت ایجاد شده است، مشاهده کرد که دارای مارک تجاری یکسان است اما با بدافزار پر شده است [۷۹] و وب سایتی مخرب حاوی بدافزار است که داشبورد قانونی COVID-19 دانشگاه جان هاپکینز را نیز ارائه می‌دهد. قابل توجه است که ایمیل جعلی سازمان جهانی بهداشت حاوی اشتباهات املایی / دستوری است. بحث در بخش سوم مثال‌های مشخص دیگری از این مورد را ارائه می‌دهد.

برای افزایش بیشتر موفقیت احتمالی حملات فیشینگ، مجرمان اینترنتی در ثبت تعداد زیادی دامنه وب سایت حاوی کلمات «covid» و «ویروس کرونا» شناسایی شده‌اند [۸۰]. چنین دامنه‌هایی احتمالاً باورپذیر است و به همین دلیل به آنها دسترسی پیدا می‌شود، خصوصاً اگر با عبارت‌های معتبری مانند سازمان جهانی بهداشت یا مراکز کنترل و پیشگیری از بیماری[1] یا کلمات کلیدی مثلا (Coronavirusapps.com، anticovid19-pharmacy.com)، به‌عنوان مورد استفاده برجسته شده است [۸۱]. سیستم عامل‌های ارتباطی مانند زوم، مایکروسافت و گوگل نیز جعل هویت شده‌اند، هم از طریق ایمیل و هم از طریق نام دامنه. این نکته با توجه به این واقعیت قابل توجه است که اینها فناوری‌های اصلی هستند که میلیون‌ها نفر در سراسر دنیا از آنها برای برقراری ارتباط استفاده می‌کنند، هم برای کار و هم برای تفریح. این حقایق، در ترکیب با ایمیل‌های متقاعد کننده مهندسی اجتماعی، پیامک‌ها و پیوندها، چندین راه قابل توجه برای حمله مجرمان را فراهم می‌کند. حملات داروسازی بسیار کمتر شایع بوده اما در ۱۳٪ موارد رخ داده است. همانطور که در جدول ۱ مشاهده می‌شود، این موارد اغلب در کنار حملات دیگر اتفاق می‌افتد.

تقلب الهام گرفته از COVID-19 از اطلاعیه‌های دولتی / علمی برای بهره‌برداری از اضطراب‌های کاربران و جستجوی سود مالی استفاده کرده است. از تجزیه و تحلیل ما، کلاه‌برداری معمولاً از طریق حملات فیشینگ و ایمیل انجام شده است - ما همچنین می‌توانیم این مورد را در توالی بالا مشاهده کنیم. در یک مورد، مجرمان به عنوان مرکز کنترل و پیشگیری از بیماری در نامه الکترونیکی ظاهر شده و مودبانه درخواست کمک برای تولید واکسن کردند و اینکه هرگونه پرداختی نیز می بایست به بیت کوین انجام شود [۷۳]. نمونه درخواست‌های متضمن پول: «سرمایه گذاری در پروژه فوق، هزینه بسیار زیادی دارد و ما خواستار اهداء حسن نیت شما هستیم، همه چیز خیلی کوچک است». نکته قابل توجه در مورد این حمله خاص این است که از گیرندگان نیز می‌خواهد پیام را با بیشترین تعداد ممکن به اشتراک بگذارند. این مسئله نگران کننده است، زیرا احتمال اعتماد افراد به ایمیل‌هایی که توسط افراد نزدیک آنها تأیید شده است زیاد است.

طیف دیگری از اقدامات کلاه‌برداری نیز وجود داشت که عمدتاً مبتنی بر تهدید یا درخواست تجدیدنظر بود. به عنوان مثال، تجزیه و تحلیل ما پیشنهادات سرمایه گذاری در شرکت‌های ادعای جلوگیری، شناسایی یا درمان COVID-19 و سرمایه گذاری در طرح ها و گزینه‌های معاملاتی را نشان می‌دهد که کاربران را قادر می‌سازد تا از رکود اقتصادی احتمالی COVID-19 استفاده کنند [۸۲]. پیشنهاداتی برای درمان، واکسن و مشاوره در مورد درمان‌های موثر برای ویروس وجود داشت. سازمان غذا و دارو[2] نامه هشدار دهنده از ۶ مارس تا ۱ آوریل ۲۰۲۰ به شرکت‌ها «برای فروش محصولات متقلبانه با ادعاهای جلوگیری، معالجه، کاهش، تشخیص یا درمان COVID 19 » صادر کرده است [۸۳]. دفتر مبارزه با کلاه‌برداری اروپا با باز کردن پرسشی درباره واردات محصولات جعلی به دلیل بیماری همه گیر COVID-19 [۸۴] و در انگلیس، سازمان تنظیم مقررات محصولات پزشکی و بهداشتی به سیل محصولات جعلی به صورت آنلاین پاسخ داده است. شروع به تحقیق در مورد تجهیزات پزشکی جعلی یا غیرمجاز کرده است که هم اکنون از طریق وب سایت‌های غیرمجاز و غیرقانونی معامله می‌شوند [۸۵].

حملات اخاذی در تجزیه و تحلیل ما مشاهده شده

[1] Centers for Disease Control and Prevention (CDC)

[2] Food and Drug Administration (FDA)

است اما در مقایسه با بقیه موارد شیوع کمتری داشته است (فقط در ۱۳٪ موارد ظاهر می‌شود). برجسته‌ترین مورد این حمله یک ایمیل اخاذی بود که تهدید می‌کند گیرنده و اعضای خانواده آنها را با COVID-19 آلوده کند مگر اینکه پرداخت بیت کوین انجام شود [۸۶]. برای افزایش باورپذیری پیام، نام فرد و یکی از رمزهای عبور وی (که احتمالاً از نقض رمز عبور قبلی جمع شده است) در آن وجود داشت. با مطالبه پول، این پیام ادامه می‌یابد: «اگر مبلغی را دریافت نکنم، همه اعضا خانواده شما را با ویروس کرونا آلوده می‌کنم». این تلاش برای استفاده از ترس برای ایجاد انگیزه در افراد برای پرداخت و استفاده از رمزهای عبور (به عنوان مثال، موارد شخصی) برای ساختن پیام مجرم است.

بدافزارهای مرتبط با COVID-19 در طی همه گیر شدن، بر میزان برجستگی افراد و سازمان‌ها در سرتاسر جهان افزوده‌اند. همانطور که در بالا نشان داده شد، این دومین نوع حمله سایبری بود که در ۶۵٪ موارد ظاهر شد. پاندای شرور و MBR Loader تنها بدافزار جدید کشف شده در این دوره بود. حملات باقیمانده بدافزارها انواع بدافزارهای موجود بود و شامل Metaljack، REMCOS، Emotet، LOKIBOT، CXK-NMSL، Dharma، Crysis، Netwalker، Mespinoza / Pysa، SpyMax مبدل به برنامه GuLoader، Corona live (1.1)، Hawkeye، FORMBOOK، Trickbot به ویژه Ransomware تهدید قابل توجهی بود و نمونه آن COVIDLock بود، برنامه اندرویدی که به عنوان نقشه حرارتی مبدل می‌شود و به‌عنوان باج افزار عمل می‌کند. اساساً صفحه کاربر قفل می‌شود مگر اینکه مبلغی «به عنوان باج» پرداخت شود [۸۷].

در سطح سازمانی، باج افزار به طور قابل توجهی بر خدمات مراقبت‌های بهداشتی تأثیر گذاشته است - مسلماً در این زمان شکننده‌ترین مولفه زیرساخت‌های مهم ملی یک کشور است. حملات در ایالات متحده، فرانسه، اسپانیا و جمهوری چک و با استفاده از باج افزارهایی مانند Netwalker گزارش شده است [۵]. اگر تصور کنیم که بازیگران مخرب مناطقی را هدف قرار می‌دهند که معتقدند برای استفاده از حملات خود ایستادگی می‌کنند، چنین حملاتی متناسب با عملکرد جنایی است. به عنوان مثال، ممکن است سازمان‌های بهداشتی جهت جلوگیری برای از دست دادن جان بیمار، باج بدهند. جالب است که از آن زمان قول‌هایی از طرف باندهای جرایم اینترنتی داده شده است که آنها هدف قرار دادن خدمات مراقبت‌های بهداشتی را نخواهند گرفت (یا متوقف نمی‌کنند). در یک گزارش، اپراتورهای پشت CLOP Ransomware، DoppelPaymer Ransomware، Maze Ransomware و Nefilim Ransomware تأکید کردند که آنها (به طور معمول) بیمارستان‌ها را هدف قرار نمی‌دهند یا تا ثبات ویروس تمام فعالیت‌ها را علیه خدمات بهداشتی متوقف می‌کنند [۸۸]. سایر نمونه‌های برجسته بدافزار در طی همه گیر شدن شامل: Trickbot، یک تروجان است که به طور معمول به عنوان بستر نصب سایر بدافزارها بر روی دستگاه‌های قربانیان استفاده می‌شود - طبق گفته مایکروسافت، Trickbot پرکارترین عملیات بدافزار است که از فریب‌های مضمون COVID-19 برای حملات آن استفاده می‌کند [۸۹]؛ یک بدافزار بازنویسی[1] که دیسک‌های دستگاه را پاک کرده و بدافزار بازنویسی را رونویسی می‌کند تا دیگر قابل استفاده نباشد [۹۰] و Corona Live 1.1، برنامه‌ای که از یک ردیاب قانونی COVID-19 منتشر شده توسط دانشگاه جان هاپکینز استفاده می‌کند و به عکس‌ها، فیلم‌ها، داده‌های مکان و دوربین دسترسی پیدا می‌کند [۲۵]. با ادامه بیماری همه گیر، احتمالاً ویروس‌های مخرب بیشتری وجود دارد که انواع مختلفی از آسیب‌ها را هدف قرار می‌دهد، به‌عنوان مثال: جسمی، مالی، روانی، اعتبار (برای مشاغل) و اجتماعی [۹۱]. در طی بیماری همه‌گیر COVID-19، تجزیه و تحلیل ما فقط مقدار بسیار کمی (۵٪) حملات انکار سرویس را شناسایی کرد، اما چندین گزارش از هک گزارش شده است. این گزارش‌ها حاکی از آن است که هک کردن بی هدف نبوده بلکه هدف آن موسساتی بوده است که در زمینه ویروس کرونا تحقیق کرده‌اند.

در یک گزارش، معاون دستیار اداره تحقیقات فدرال آمریکا اظهار داشت: «ما مطمئناً فعالیت شناسایی و برخی از دخالت‌ها را در برخی از این موسسات مشاهده کرده‌ایم، خصوصاً موسساتی که به طور علنی خود را به عنوان کار در تحقیقات مرتبط با COVID معرفی کرده‌اند» [۹۲]. این موضوع یک ماه بعد توسط مرکز امنیت سایبری ملی انگلیس و آژانس امنیت سایبری و زیرساخت ایالات متحده مورد حمایت قرار گرفت. در این مشاوره مشخص شد که گروه‌های تهدید پایدار پیشرفته - برخی از آنها ممکن است با دولت‌های ملی همسو شوند - شرکت‌های دارویی، سازمان‌های تحقیقات پزشکی و دانشگاه‌های درگیر در پاسخ COVID-19 را هدف قرار

[1] Master Boot Record (MBR)

می‌دهند. هدف لزوماً اخلال در فعالیت‌های آنها نبود (مانند پرونده باج افزار)، بلکه سرقت اطلاعات حساس تحقیقاتی یا دارایی معنوی (مثلاً در مورد واکسن‌ها، روش‌های درمانی) بود.

در حالی که هنوز تجزیه و تحلیل دقیق این حملات ظاهر نشده است، با شش رمز عبور (حمله بی‌رحمانه که با استفاده از رمزهای عبور معمول در تلاش برای ورود به سیستم حساب‌ها) و استفاده از آسیب پذیری‌ها در شبکه خصوصی مجازی (VPN) علامت‌گذاری شده است [۹۳]. انتساب، یکی دیگر از موارد مهم در چنین حملاتی است. تعیین منشأ واقعی حملات سایبری همیشه دشوار بوده است، با این حال، در پاسخ به این تهدیدات مربوط به COVID-19، ایالات متحده علناً جمهوری خلق چین را در اعلامیه مشترک اداره تحقیقات فدرال آمریکا و آژانس امنیت سایبری و زیر ساخت آمریکا به‌عنوان عامل عنوان کرد [۹۴].

۳- تأثیر حملات بر کار

اثرات همه گیری، قرنطینه انبوه کارکنان و اقدامات انجام شده برای تسهیل کار از راه دور و مقاوم‌سازی زیرساخت‌های سایبری موجود، در برابر حملات و جدول زمانی که قبلاً شرح داده شد، تأثیر زیادی بر نیروی کار - افراد درگیر یا موجود برای کار داشته است. این همه گیری همچنین بر مقاومت در برابر فناوری، ساختارهای اقتصادی - اجتماعی تأثیر داشته و تا حدی شیوه زندگی و ارتباط مردم را تهدید می‌کند. شکل (۶) تأثیر COVID-19 بر نیروی کار را در هشت گروه مختلف نشان می‌دهد. به نظر می‌رسد همه دسته‌ها با دارایی‌ها و ابزارهای سایبری تلفیق می‌شوند و دسته‌های مختلف تحت تأثیر متفاوت قرار می‌گیرند. این همه‌گیری باعث ایجاد درگیری‌های خطرناک می‌شود، به‌عنوان مثال: رعایت دقیق استانداردهای امنیتی که باعث دلسردشدن اشتراک داده‌ها می‌شود، می‌تواند مضرتر از به اشتراک‌گذاری داده‌ها باشد. بنابراین، در حالیکه ممکن است الزامات سختگیرانه‌ای برای عدم دسترسی پزشکان عمومی در خانه به داده‌های بیمار (پزشکان عمومی) وجود داشته باشد، این امر آسیب بیشتری در حین قرنطینه نسبت به امکان دسترسی پزشکان عمومی به داده‌های بیمار ایجاد می‌کند. همچنین، روش پردازش اطلاعات محرمانه بیمار، نیاز به ارزیابی تأثیر حفاظت از داده‌ها دارد تا در صورت لزوم، پشتیبانی بیشتر سرویس بهداشت ملی انگلیس را فعال کند. این می‌تواند از نظر ارائه به موقع مداخلات پزشکی در پاسخ به COVID-19 تأثیرگذار باشد.

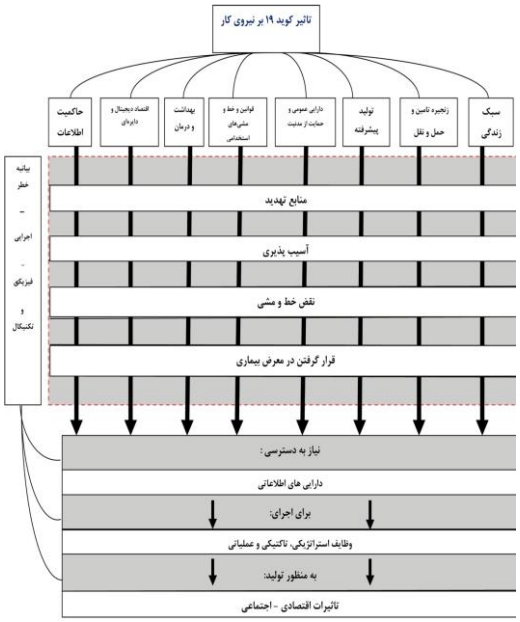
در طبقه بندی خطر سنتی، عناصری مانند ثبت و ارزیابی دارایی، دفعات تهدید و احتمال آسیب پذیری بیشتر در معرض خطر تهدیدات سایبری هستند. بنابراین، پیش بینی می‌کنیم تغییراتی در نحوه دسترسی نیروی کار به این دارایی‌های اطلاعاتی و نحوه اجرای وظایف استراتژیک، تاکتیکی و عملیاتی برای تولید بازده اقتصادی - اجتماعی پیش بینی شود. این تغییرات را می‌توان با تهیه و آزمایش اظهارات ریسک گرفتن ۱) عوامل تهدید، ۲) آسیب پذیری‌ها، ۳) نقض سیاست / روند و ۴) قرار گرفتن در معرض دارایی کلی در تمام مناظر تهدید در حال ظهور، همانطور که در شکل (۶) نشان داده شده است. تغییرات بیشتر در مناظر تهدید مرتبط با فعالیت‌های نیروی کار از راه دور و افزایش دفعات خطوط حمله مسلحانه مربوط به انتشار ویروس کرونا. با توجه به شرایط فعلی، پیش بینی اینکه این تغییرات تأثیری طولانی مدت بر نیروی کار داشته باشند دشوار است، اما اهمیت آنها قبلاً ثبت شده است [۹۵]. بنابراین، با توجه به افزایش حملات سایبری به زیرساخت‌های مهم، از اهمیت بالاتری برخوردار است که کنترل اطلاعات (ذخیره‌سازی، پردازش، انتقال) از اهمیت بالایی برخوردار باشد.

دولت‌ها، بخش‌های خصوصی و دولتی در سراسر اروپا در حال حاضر اقداماتی را برای محدود کردن و کاهش تأثیر COVID-19 بر ساختارهای داده موجود و چارچوب‌های حاکمیت اطلاعات در نظر می‌گیرند.

[۹۶]. به‌عنوان مثال: تأکید ویژه‌ای بر پیامدهای همه گیری در پردازش داده‌های شخصی داده شده است. قانون مقررات عمومی حفاظت از داده‌ها[1] در انگلستان حکم می‌کند که داده‌های شخصی باید فقط برای اهداف مشخصی که برای آنها بدست آمده پردازش شوند [۹۷]. علاوه بر این، افراد داده باید همیشه اطلاعات صریح و شفاف را با توجه به فعالیت‌های پردازشی انجام شده، از جمله ویژگی‌ها و ماهیت فعالیت، دوره نگهداری و هدف از پردازش، دریافت کنند. چالش‌های مربوط به زمینه انطباق قانونی و نظارتی حاکمیت از نظر انطباق در مقابل دسترسی سریع و پردازش داده‌ها توسط نهادهای مختلف وجود دارد. این در مواردی که مقامات دولتی به دنبال دستیابی به PII برای کاهش شیوع COVID-19 هستند کاملاً مشهود است. نمونه‌های معمول نیز شامل برنامه‌های

[1] General Data Protection Regulation (GDPR)

ردیابی تماس و سیستم عامل‌هایی است که داده‌ها به‌صورت آنلاین برای پردازش جمع می‌شوند [۹۸]. اقدامات قانونی خاص برای حفظ امنیت عمومی ضمن حفظ حریم خصوصی باید مجدداً به کار گرفته یا معرفی شود، در حالی که اصول قانونی و نظارتی همچنان حفظ می‌شوند [۹۹].



(شکل-۶): تأثیر COVID-19 بر نیروی کار

با افزایش سریع علائم COVID-19، دولت‌ها مجبور شدند طرحی تهیه کنند که به آنها امکان درک بیشتر داده‌های اپیدمیولوژیک و شناسایی مداخلات مثبت برای مهار و کاهش تأثیر همه‌گیری را بدهد. تحقیقات نشان می‌دهد بین استفاده از داده‌های بزرگ که شامل اطلاعات قابل شناسایی خصوصی در اثربخشی این تحقیقات اپیدمیولوژیک است، همبستگی زیادی وجود دارد [۱۰۰]. این بدان معنا بود که در بیشتر موارد، شهروندان مجبور بودند این اطلاعات را داوطلبانه ارائه دهند و این به سرعت منجر به بحث و گفتگو در مورد مبادلات بین امنیت عمومی در برابر حریم شخصی شد [۱۰۱]. این اطلاعات همچنین از طریق فناوری ارتباطات اینترنتی بدست آمده است. تجهیزات آزمایش پزشکی و آزمایش ویروس کرونا در مقیاس وسیع به عنوان ابزاری برای جمع آوری داده‌ها در مبارزه برای کاهش میزان مرگ و میر استفاده شد. چارچوب‌های انطباق قانونی و نظارتی بین کشورها متفاوت است. بنابراین، مدیریت اطلاعات شخصی منوط به اقدامات مختلف محافظت از حریم خصوصی بود.

شناسایی نکردن اطلاعات شخصی یکی دیگر از مولفه‌هایی بود که دولت‌ها مجبور شدند برای برآوردن شرایط حریم خصوصی شخصی و افزایش اعتماد شرکت کنندگان انسانی در طول تحقیقات اپیدمیولوژیک استفاده کنند. روند جمع‌آوری و پردازش استفاده از اطلاعات شخصی با استفاده از فناوری‌های شناسایی غیرمشخص، چالش‌های فنی را در رابطه با دقت و رضایت، دفع اطلاعات دفاعی ایمن و قانونی و استحکام سیاست‌های مرتبط پردازش و مدیریت داده‌ها برای تحقیقات اپیدمیولوژیک ایجاد کرده است. فوریت وضعیت و سرعت دستیابی و پردازش داده ها، باعث ایجاد بی اعتمادی در بین شهروندان شده و کارآیی فرآیندهای موجود را به چالش می‌کشد [۱۰۱]. همچنین دوره‌های طولانی پلمپ که در بسیاری از کشورها معرفی شده است (در بخش سوم شرح داده شده است) توانایی آنها را در استقرار استراتژی‌های بهبود تجارت پس از این دوره‌ها بررسی کرده است. این استراتژی‌ها باید از بهبودی نرم و تدریجی در یک بیماری همه گیر در حال انجام اطمینان حاصل کنند، که اثبات شده یک کار چالش برانگیز است. با این حال، یک سرعت و مقیاس بی‌سابقه در فعالیت‌های تحقیق و توسعه در پاسخ به شیوع COVID-19 وجود دارد که همکاری‌های چند جانبه بین سازمانی را مجبور می‌کند [۱۰۲].

در حال حاضر در اروپا چالشی برای سازماندهی به موقع و دقیق اشتراک اطلاعات وجود دارد زیرا به نظر می‌رسد حتی منابع جریان اصلی رسانه‌ها اطلاعات نادرست را تبلیغ کرده‌اند [۱۰۳]. افزایش هر دو فرکانس و تأثیر این حملات، توانایی نظارت و ممیزی موجود، کنترل دسترسی منطقی و فیزیکی، طرح‌های تأیید اعتبار را که در حال حاضر استفاده شده است، بیشتر آزمایش می‌کند. همچنین، به عنوان بخشی از مدیریت ریسک سازمانی در حال حاضر، به روشی که سازمان‌ها برای پاکسازی گزارشات حادثه استفاده می‌کنند، دفع رسانه‌ها و تخریب و به اشتراک گذاری داده‌ها نیز در کنار اصول عمیق دفاعی که در حال حاضر به‌صورت واقعی انجام می‌شود، آزمایش خواهد شد. بخش مالی نیز تحت تأثیر قرار می‌گیرد، زیرا رکود اقتصادی پیش بینی شده از پیشرفت و مقیاس حملات هدفمند به دلیل رشد توانایی‌های بازیگران به‌عنوان تهدید استفاده می‌کند [۱۰۴].

۴- نتیجه‌گیری

همه‌گیری COVID-19 شرایط اجتماعی و اقتصادی قابل توجه و منحصر به فردی را ایجاد کرده است که توسط

مجرمان سایبری اعمال شده است. تجزیه و تحلیل ما از وقایع مانند اطلاعیه‌ها و داستان‌های رسانه‌ای نشان داده است که به نظر می‌رسد ارتباط بین اعلامیه و یک حمله سایبری مربوطه وجود دارد که از این رویداد به عنوان یک قلاب استفاده می‌کند و در نتیجه احتمال موفقیت را افزایش می‌دهد. بیماری همه‌گیری COVID-19 و افزایش نرخ حملات سایبری که به آن متوسل شده است، پیامدهای گسترده‌تری دارد که فراتر از اهداف چنین حملاتی است. تغییر در شیوه‌های کار و معاشرت به معنای این است که مردم اکنون دوره‌های بیشتری را به صورت آنلاین می‌گذرانند. علاوه بر این، نرخ بیکاری نیز افزایش یافته است، به این معنی که افراد بیشتری در خانه نشسته‌اند. به احتمال زیاد برخی از این افراد برای تأمین هزینه زندگی خود به جرایم اینترنتی روی می‌آورند. ترکیبی از افزایش سطح حملات سایبری و ابزارهای جرایم اینترنتی ترکیبی از افزایش سطح حملات سایبری و جرایم سایبری به این معنی است که ممکن است عواقبی برای پلیس در اجرای قانون جهانی داشته باشد، باید اطمینان حاصل کند که توانایی برخورد با جرایم سایبری را دارد.

تجزیه و تحلیل ارائه شده در این مقاله عملکرد رایج بسیاری از حملات سایبری را در این دوره برجسته کرده است. بسیاری از حملات سایبری با یک کمپین فیشینگ آغاز می‌شود که قربانیان را به بارگیری پرونده یا دسترسی به URL هدایت می‌کند. پرونده یا URL به عنوان حامل بدافزار عمل می‌کند که هنگام نصب، به عنوان وسیله‌ای برای کلاه‌برداری مالی عمل می‌کند. تجزیه و تحلیل همچنین نشان داده است که برای افزایش احتمال موفقیت، کمپین فیشینگ از اعلامیه‌های رسانه‌ای و دولتی استفاده می‌کند. اگرچه این تجزیه و تحلیل لزوماً جدید نیست، اما ما معتقدیم این اولین بار است که با زمینه‌ای از وقایع زنده واقعی پشتیبانی می‌شود. این تجزیه و تحلیل این توصیه را ایجاد می‌کند که دولت‌ها، رسانه‌ها و سایر نهادها باید آگاه باشند که اعلامیه‌ها و انتشار داستان‌ها احتمالاً باعث ارتکاب فعالیت‌های حملات سایبری مرتبط با این حوادث می‌شود. این رویدادها باید با یک یادداشت سلب مسئولیت همراه باشد که در آن نحوه انتقال اطلاعات مربوط به اعلامیه توضیح داده شده است.

این پژوهش نشان داده است که چه چیزی می تواند به‌عنوان یک ارتباط مستقیم و معکوس سست بین حوادث و حملات سایبری توصیف گردد. تحقیقات بیشتر باید این پدیده را بررسی کند و مشخص کند آیا می‌توان از یک مدل پیش بینی برای تأیید این ارتباط استفاده کرد. مطالعات موردی مربوط به حملات سایبری در مورد کشورهای جهان به وفور یافت می‌شود و تحلیل گسترده‌تری از این مسأله می‌تواند به تأیید این پدیده کمک کند.

۵- مراجع

[1] Krebs on Security, “Live Coronavirus Map Used to Spread Malware,” 2020, https://krebsonsecurity.com/2020/03/live-coronavirusmap- used-to-spread-malware/ (Accessed 15 June 2020).

[2] R. Smithers, “Fraudsters use bogus nhs contact-tracing app in phishing scam,” 2020, https://www.theguardian.com/world/2020/may/13/ fraudsters-use-bogus-nhs-contact-tracing-app-inphishing- scam (Accessed 30 May 2020).

[3] Europol, “Pandemic Profiteering: How Criminals Exploit COVID-19 Crisis,” 2020, https://www.europol.europa.eu/publicationsdocuments/ pandemic-profiteering-how-criminalsexploit- covid-19 crisis (Accessed 15 June 2020).

[4] Norton, “Coronavirus Phishing Emails: How to Protect against COVID-19 Scams,” 2020, https://us.norton.com/internetsecurity-online-scamscoronavirus- phishing-scams.html (Accessed 15 June 2020).

[5] Wired, “Hackers Are Targeting Hospitals Crippled by Coronavirus,” 2020, https://www.wired.co.uk/article/coronavirus-hackerscybercrime- phishing (Accessed 15 June 2020).

[6] UK’s National Cyber Security Centre (NCSC) and the US’ Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA), “Advisory: COVID-19 Exploited by Malicious Cyber Actors,” 2020, https://www.ncsc.gov.uk/news/covid-19-exploited-by-cyber-actors-advisory (Accessed 15 June2020).

[7] M. Cross and D. L. Shinder, Scene of the cybercrime. Syngress Pub., 2008.

[8] M. Yar, “The novelty of ’cybercrime’ an assessment in light of routine activity theory,” European Journal of Criminology, vol. 2, no. 4, pp. 407–427, 2005.

[9] D. R. Cressey, Other people’s money; a study of the social psychology of embezzlement. Free Press, 1953.

[10] N. Dhanjani, B. Rios, and B. Hardin, Hacking: The Next Generation: The Next Generation. O’Reilly Media, Inc., 2009.

[11] K. Shoshian, A.J. Rashidi, A.R. Mirghadri,

“Probabilistic Modeling of Obfuscated Multi – Stage cyber Attacks,” Journal of Electronical & Cyber Defence, vol. 8, no. 2, pp. 61-73, 2020. (In Persion)

[12] NHS, “10 tips to help if you are worried about coronavirus,” 2020, https://www.nhs.uk/oneyou/every mindmatters/ coronavirus-covid-19-anxiety-tips (Accessed 9 May 2020).

[13] S. Gallagher and A. Brandt, “Facing down the myriad threats tied to covid- 19,” 2020, https://news.sophos.com/enus/ 2020/04/14/covidmalware (Accessed 9 May 2020).

[14] F. Shi, “Threat spotlight: Coronavirus-related phishing,” 2020, https://blog.barracuda.com/2020/03/26/threats potlight- coronavirus-related-phishing (Accessed 9 May 2020).

[15] N. Kumaran and S. Lugani, “Protecting businesses against cyber threats during covid-19 and beyond,” 2020, https://cloud.google.com/blog/products/identit ysecurity/ protecting-against-cyber-threats-during-covid- 19-and-beyond (Accessed 17 June 2020).

[16] T. L. O’Brien, “Covid aid scams and dodgydeals could have been avoided,” 2020, https://www.bloomberg.com/opinion/articles/ 2020- 05-01/coronavirus-trillions-in-aid-draws-scams-anddodgy- deals (Accessed 9 May 2020).

[17] D. Galov, “Remote spring: the rise of rdp bruteforce attacks,” 2020, https://securelist.com/remote-spring-therise-of-rdp-bruteforce-attacks/96820 (Accessed 9 May 2020).

[18] G. Tsakalidis and K. Vergidis, “A systematic approach toward description and classification of cybercrime incidents,” IEEE Transactions on Systems, Man, and Cybernetics: Systems, vol. 49, no. 4, pp. 710–729, 2017.

[19] O. Kolomiyets, S. Bethard, and M.-F. Moens, “Extracting narrative timelines as temporal dependency structures,” in Proceedings of the 50th Annual Meeting of the Association for Computational Linguistics: Long Papers-Volume 1. Association for Computational Linguistics, 2012, pp. 88–97.

[20] R. Van Heerden, S. Von Soms, and R. Mooi, “Classification of cyber attacks in south africa,” in 2016 IST Africa Week Conference. IEEE, 2016, pp. 1–16.

[21] World Health Organisation (WHO), “Naming the coronavirus disease (COVID-19) and the virus that causes it,” 2020, https://www.who.int/emergencies/diseases/no velcoronavirus- 2019/technical-guidance/naming thecoronavirus- disease-(covid-2019)-and-the-virus-thatcauses- it (Accessed 15 June 2020).

[22] CPS, “Cybercrime - prosecution guidance,” The Crown Prosecution Service (CPS), Tech. Rep., 2019, https://www.cps.gov.uk/legal-guidance/cybercrimeprosecution- guidance (Accessed 17 June 2020).

[23] S. Henderson, G. Roncone, S. Jones, J. Hultquist, and B. Read, “Vietnamese threat actors apt32 targeting wuhan government and chinese ministry of emergency management in latest example of covid-19 relatedespionage,” 2020, https://www.fireeye.com/blog/threatresearch/ 2020/04/apt32-targeting-chinese governmentin- covid-19-related-espionage.html (Accessed 17 June 2020).

[24] L. O’Donnell, “Skype phishing attack targets remote workers’ passwords,” 2020, https://threatpost.com/skype-phishing-attack-targetsremote- workers-passwords/155068/ (Accessed 30 May 2020).

[25] CNET, “Fake Coronavirus Tracking Apps Are Really Malware That Stalks You,” 2020, https://www.cnet.com/news/fake-coronavirus-trackingapps- are-really-malware-that-stalks-its-users/ (Accessed 15 June 2020).

[26] S. Chockalingam, W. Pieters, A. Teixeira, and P. van Gelder, “Bayesian network models in cyber security: a systematic review,” in Nordic Conference on Secure IT Systems. Springer, 2017, pp. 105–122.

[27] Google, “Google Translate,” 2020, https://translate.google.co.uk/ (Accessed 30 May 2020).

[28] The Ministry of Health, Labour and Welfare, “Latest information on Coronavirus disease 2019 (COVID-19).” 2020, https://www.mhlw.go.jp/stf/seisakunitsuite/bunya/ 0000164708 00001.html (Accessed 30 May 2020).

[29] G.-y. Wang, H.-m. Wang, Z.-j. Chen, and M. Xian, “Research on computer network attack modeling based on attack graph [j],” Journal of National University of Defense Technology, vol. 4, 2009.

[30] World Health Organisation (WHO), “Who reports fivefold increase in cyber attacks, urges vigilance,” 2020, https://www.who.int/zh/news-room/detail/23-04- 2020-who-reports-fivefold-increase-in-cyber-attacksurges- vigilance (Accessed 18 June 2020).

[31] Jisho, “Cyber attack,” 2020, https://jisho.org/search (Accessed 30 May 2020).

[32] Le Parisien, “Municipal: “massive” computer attack at the town hall of marseille,” 2020, http://www.leparisien.fr/elections/municipales

https://www.kaspersky.com/blog/coronavirusphishing/ 32395/ (Accessed 30 May 2020).

[46] J. Walter, "Threat Intel:Cyber Attacks Leveraging the COVID-19/CoronaVirus Pandemic," 2020, https://labs.sentinelone.com/threat-intel-update-cyberattacks- leveraging-the-covid-19-coronavirus-pandemic/, (Accessed 10 June 2020).

[47] smzdm.com, "Hackers are using the "coronavirus" fear for phishing, please pay attention to prevention!" 2020, https://post.smzdm.com/p/a07ol5x0/ (Accessed 30 May 2020).

[48] CSDN, "Take advantage of the fire! "the epidemic is a bait" cyber attack," 2020, https://blog.csdn.net/weixin 43634380/article/details/ 104237121 (Accessed 30 May 2020).

[49] TechRepublic, "Global shipping industry attacked by coronavirus-themed malware," 2020, https://www.techrepublic.com/article/global-shippingindustry- attacked-by-coronavirus-themed-malware/ (Accessed 30 May 2020).

[50] cqgbxa.com, "Fighting the spread of coronaviruses who faces severe cybersecurity threats," 2020, www.cqgbxa.com/newshy/67936.html (Accessed 30 May 2020).

[51] S. Patranobis, "Indian Hackers Targeting Chinese Medical Institutes Amid Coronavirus Outbreak, Says Report," 2020, https://www.hindustantimes.com/worldnews/ indian-hackers-targetting-chinese-medicalinstitutes- amid-coronavirus-outbreak-says-report/storypiDHQeY4UfTVy8BWa2GG3O.html, (Accessed on 12 June 2020).

[52] freebuf.com, "Analysis and suggestions on several types of network security threats during the epidemic prevention and control period," 2020, https://www.freebuf.com/companyinformation / 227585.html (Accessed 30 May 2020).

[53] Stonefly, "Coronavirus and ransomware infection - what's the connection?" 2020, https://stonefly.com/blog/coronavirus-ransomwareinfection- whats-the-connection (Accessed 12 June 2020).

[54] The Register, "Fresh virus misery for illinois: Public health agency taken down by... web ransomware. great timing, scumbags," 2020, https://www.theregister.co.uk/2020/03/12/ ransomware illinois health/ (Accessed 30 May 2020).

[55] R. Millman, "Coronavirus test results delayed by cyber-attack on czech hospital," 2020, https://www.scmagazineuk.com/coronaviruste /municipalesattaque- informatique-massive-a-la-mairie-de-marseille 15-03-2020-8280114.php (Accessed 30 May 2020).

[33] la Repubblica, "Cyber attack on easyjet, compromised the data of nine million customers," 2020, https://www.repubblica.it/tecnologia/sicurezza /2020/05/19/ news/attacco informatico a easyjet compromessi i dati di nove milioni di clienti- 257099879/ (Accessed 30 May 2020).

[34] H. Hindy, D. Brosset, E. Bayne, A. Seeam, C. Tachtatzis, R. Atkinson, and X. Bellekens, "A taxonomy of network threats and the effect of current datasets on intrusion detection systems," IEEE Access, pp. 1–1, 2020.

[35] M. McGuire and S. Dowling, "Chapter 1: Cyberdependent crimes," Home Office, Tech. Rep., 2013, https://assets.publishing.service.gov.uk/government /uploads/system/uploads/attachment data/ file/246751/horr75-chap1.pdf (Accessed 18 June 2020).

[36] ——, "Chapter 2: Cyber-enabled crimes – fraud and theft," Home Office, Tech. Rep., 2013, https://assets.publishing.service.gov.uk/government/uploads /system/uploads/attachment data/file /248621/horr75 chap2.pdf (Accessed 18 June 2020).

[40] X. Bellekens, G. Jayasekara, H. Hindy, M. Bures, D. Brosset, C. Tachtatzis, and R. Atkinson, "From cybersecurity deception to manipulation and gratification through gamification," in International Conference on Human-Computer Interaction. Springer, 2019, pp. 99– 114.

[41] Malwarebytes, "2020 state of malware report," 2020, https://resources.malwarebytes.com/files/2020 /02 /2020 State-of-Malware-Report.pdf (Accessed 30 May 2020).

[42] AON, "Social engineering attacks and covid-19," 2020, https://www.aon.com/cyber solutions/thinking/socialengineering- attacks-and-covid-19/ (Accessed 17 June 2020).

[43] Forbes, "Chinese hackers 'weaponize' coronavirus data for new cyber attack: Here's what they did," 2020, https://www.forbes.com/sites/zakdoffman/2020/03/12/ chinese-hackers-weaponized-coronavirus-datato- launch this-new-cyber-attack/#196851b03861 (Accessed 30 May 2020).

[44] F-Secure, "Coronavirus email attacks evolving as outbreak spreads," 2020, https://blog.fsecure. com/coronavirus-email-attacks-evolving-asoutbreak- spreads/ (Accessed 30 May 2020).

[45] Kaspersky, "Coronavirus phishing," 2020,

st- results-delayed-cyber-attack-czechhospital/ article/1677194 (Accessed 30 May 2020).

[56] S. Stein and J. Jacobs, "Cyber-attack hits u.s. health agency amid covid-19 outbreak," 2020, https://www.bloomberg.com/news/articles/20 20-03- 16/u-s-health-agency-suffers-cyber-attack-during-covid- 19 response (Accessed 30 May 2020).

[57] K. D. Rosso, "New threat discovery shows commercial surveillanceware operators latest to exploit covid- 19," 2020, https://blog.lookout.com/commercialsurveilla nceware- operators-latest-to-take-advantage-ofcovid- 19 (Accessed 30 May 2020).

[58] S. Desai, "New android app offers coronavirus safety mask but delivers sms trojan," 2020, https://www.zscaler.com/blogs/research/new-androidapp- offers-coronavirus-safety-mask-delivers-sms-trojan (Accessed 30 May 2020).

[59] N. FitzGerald, "Scams, lies, and coronavirus," 2020, https://www.welivesecurity.com/2020/04/17/s cams liescoronavirus/ (Accessed 30 May 2020).

[60] Murica Today, "Cyber-attack threatens spanish hospital computer systems," 2020, https://murciatoday.com/cyber attack threatens spanish hospital computer systems 1367723-a.html (Accessed 30 May 2020).

[61] B. Koenig, "Covid sms phishing attempt," 2020, https://twitter.com/BigBenKoenig/status/ 1242503232527589376 (Accessed 30 May 2020).

[62] Glos Safe Cyber, "Our @glospolice fcr have had calls asking if covid-19 texts like the below are genuine," 2020, https://twitter.com/GlosSaferCyber/status /1242525105508532225 (Accessed 30 May 2020).

[63] J. Rodger, "The school meals coronavirus text scam which could trick parents out of thousands," 2020, https://www.birminghammail.co.uk/news/mid landsnews/ school-meals-coronavirus-text-scam-17975311 (Accessed 30 May 2020).

[64] P. Muncaster, "Android malware takes payment for 'coronavirus finder' map," 2020, https://www.infosecurity magazine.com/news/androidmalware-payment/ (Accessed 30 May 2020).

[65] G. Strawbridge, "Warning over coronavirus netflix scam," 2020, https://www.metacompliance.com/blog/warning-overcoronavirus- netflix-scam/ (Accessed 30 May 2020).

[66] J. Chadwick, "Cyber criminals create a spoof copy of the nhs website in the midst of the coronavirus pandemic to trick users into downloading dangerous malware that can steal their passwords and credit card data," 2020, https://www.dailymail.co.uk/sciencetech/articl e- 8250737/Kaspersky-detects-fake-NHS-site-steals-creditcard- data.html (Accessed 30 May 2020).

[67] D. C. R. Magazine, "Hackers exploit hmrc coronavirus job retention scheme with phishing email scam," 2020, https://datacentrereview.com/news/1680-hackersexploit- hmrc-coronavirus-job-retention-scheme-withphishing- email-scam (Accessed 30 May 2020).

[68] L. Abrams, "New coronavirus screenlocker malware is extremely annoying," 2020, https://www.bleepingcomputer.com/news/sec urity/newcoronavirus- screenlocker-malware-is-extremelyannoying/ (Accessed 30 May 2020).

[69] Dark Reading, "Docusign phishing campaign uses covid-19 as bait," 2020, https://www.darkreading.com/attacksbreaches / docusign-phishing-campaign-uses-covid- 19-as-bait/d/d-id/1337776 (Accessed 30 May 2020).

[70] Mimecast, "New Threat Intelligence Report: 100 Days of Coronavirus," 2020, https://www.mimecast.com/blog/2020/05/100-daysof- coronavirus/, (Accessed 15 June 2020).

[71] NCSC, "NCSC Shines Light on Scams Being Foiled via Pioneering New Reporting Service," 2020, https://www.actionfraud.police.uk/news/cyber -expertsshine- light-on-online-scams-as-british-public-flag-over- 160000-suspect-emails, (Accessed 7 May 2020).

[72] Sky News, "Coronavirus: Fraud victims have lost more than £4.6m to virus-related scams," 2020, https://news.sky.com/story/coronavirus-fraud-victimshave- lost-more-than-4-6m-to-virus-related-scams- 11996721, (Accessed 10 June 2020).

[73] J. Tidy, "Coronavirus: Israel enables emergency spy powers," 2020, https://www.bbc.co.uk/news/technology-51930681 (Accessed 30 May 2020).

[74] M. Hill, "HMRC Shuts Down Almost 300 COVID19 Phishing Scam Sites," 2020, https://www.infosecurity magazineinfosecuritymagazine. com/news/hmrc-covid19-phishing-scams/, (Accessed 10 June 2020).

[75] U. Government, "Budget 2020: What You Need to Know," 2020, https://www.gov.uk/government/news/budget-2020- what-you-need-to-know, (Accessed 10 June 2020).

[76] Swansea Council, “Coronavirus Scams,” 2020, https://www.swansea.gov.uk/coronavirusscam , (Accessed 10 June 2020).

[77] X. Bellekens, A. Hamilton, P. Seeam, K. Nieradzinska, Q. Franssen, and A. Seeam, “Pervasive ehealth services a security and privacy risk awareness survey,” in 2016 International Conference On Cyber Situational Awareness, Data Analytics And Assessment (CyberSA). IEEE, 2016, pp. 1–4.

[78] C. Iuga, J. R. C. Nurse, and A. Erola, “Baiting the hook: factors impacting susceptibility to phishing attacks,” Human-centric Computing and Information Sciences, vol. 6, no. 1, p. 8, 2016.

[79] Daily Mail, “Cyber Criminals Create a Spoof Copy of the NHS Website in the Midst of the Coronavirus Pandemic to Trick Users Into Downloading Dangerous Malware That Can Steal Their Passwords and Credit Card Data,” 2020, https://www.dailymail.co.uk/sciencetech/articl e- 8250737/Kaspersky-detects-fake-NHS-site-stealscredit- card-data.html (Accessed 15 June 2020).

[80] Check Point, “Coronavirus Cyber-attacks Update: Beware of the Phish,” 2020, https://blog.checkpoint.com/2020/05/12/coron aviruscyber- attacks-update-beware-of-the-phish/ (Accessed 17 May 2020).

[81] Forbes, “There Are Now More Than 40,000 ’High- Risk’ COVID-19 Threats On The Web,” 2020, https://www.forbes.com/sites/thomasbrewster/ 2020/04/22/ there-are-now-more-than-40000-high-risk-covid-19– threats-on-the-web/ (Accessed 17 May 2020).

[82] US Department of Justice (DOJ), “Covid-19 fraud,” 2020, https://www.justice.gov/usao-edky/covid-19- fraud-1 (Accessed 15 June 2020).

[83] Food and Drugs Administration (FDA), “Fraudulent coronavirus disease 2019 (covid-19) products,” 2020, https://www.fda.gov/consumers/health-fraudscams/ fraudulent-coronavirus-disease-2019-covid-19- products (Accessed 15 June 2020).

[84] European Anti-Fraud Office (OLAF), “OLAF Launches Enquiry into Fake COVID-19 Related Products,” 2020, https://ec.europa.eu/anti-fraud/media-corner/news/20- 03-2020/olaf-launches-enquiry-fake-covid-19 relatedproducts en (Accessed 17 May 2020).

[85] UK Government, “UK Medicines and Medical Devices Regulator Investigating 14 Cases of Fake or Unlicensed COVID-19 Medical Products,” 2020, https://www.gov.uk/government/news/uk-medicinesand- medical-devices-regulator-investigating-14-casesof- fake-or-unlicensed-covid-19-medical-products (Accessed 17 May 2020).

[86] Sophos, “Dirty little secret extortion email threatens to give your family coronavirus,” 2020, https://nakedsecurity.sophos.com/2020/03/19/ dirtylittle- secret-extortion-email-threatens-to-give-yourfamily- coronavirus/ (Accessed 15 June 2020).

[87] Domain Tools, “Covidlock update: Deeper analysis of coronavirus android ransomware,” 2020, https://www.domaintools.com/resources/blog/ covidlockupdate- coronavirus-ransomware (Accessed 15 June 2020).

[88] BleepingComputer, “Ransomware Gangs to Stop Attacking Health Orgs During Pandemic,” 2020, https://www.bleepingcomputer.com/news/security /ransomware-gangs-to-stop-attacking-health-orgsduring- pandemic/ (Accessed 15 June 2020).

[89] InfoSecurity, “Trickbot Named Most Prolific #COVID19 Malware,” 2020, https://www.infosecuritymagazine. com/news/trickbot-named-most-prolific/ (Accessed 15 June 2020).

[90] SonicWall, “Coronavirus Trojan Overwriting The MBR,” 2020, https://securitynews.sonicwall.com/xmlpost/coronavirustrojan- overwriting-the-mbr/ (Accessed 15 June 2020).

[91] 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,” Journal of Cybersecurity, vol. 4, no. 1, 2018.

[92] Reuters, “FBI official says foreign hackers have targeted COVID-19 research,” 2020, https://uk.reuters.com/article/us-health-coronaviruscyber/ foreign-state-hackers-target-u-s-coronavirustreatment- research-fbi-official-idUKKBN21Y3GL (Accessed 15 June 2020).

[93] UK’s National Cyber Security Centre (NCSC) and the US’ Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA), “Advisory: APT groups target healthcare and essential services,” 2020, https://www.ncsc.gov.uk/news/apt-groupstarget- healthcare-essential-services-advisory (Accessed 15 June 2020).

[94] The Federal Bureau of Investigation (FBI), “People’s Republic of China (PRC) Targeting

of COVID-19 Research Organizations," 2020, https://www.fbi.gov/news/pressrel/pressreleases/ peoples-republic-of-china-prc-targeting-ofcovid- 19-research-organizations (Accessed 15 June 2020).

[95] A. Pipikaite and N. Davis, "Why cybersecurity matters more than ever during the coronavirus pandemic," 2020, https://www.weforum.org/agenda/2020/03/coronaviruspandemic- cybersecurity/ (Accessed 18 June 2020).

[96] Data Protection Commission, "Data Protection and COVID-19," 2020, https://dataprotection.ie/en/newsmedia/ blogs/data-protection-and-covid-19 (Accessed on 20 June 2020).

[97] The Information Commissioner's Office, "General data protection regulation (gdpr): Principle (b): Purpose limitation," 2020, https://ico.org.uk/for-organisations/guideto-data-protection/guide-to-the-general-data-protectionregulation- gdpr/principles/purpose-limitation/(Accessed 19 June 2020).

[98] A. Downey, "NHS contact-tracing app 'falls short of data protection law'," 2020, https://www.digitalhealth.net/2020/05/nhs-contacttracing- app-falls-short-of-data-protection-law/ (Accessed on 20 June 2020).

[99] NHSXIG Team, "Covid-19 information governance advice for ig professionals," 2020, https://www.nhsx.nhs.uk/covid-19-response/data-andinformation-governance/information-governance/covid-19-information-governance-advice-ig-professionals/ (Accessed 18 June 2020).

[100] W. Price and I. Cohen, "Privacy in the age of medical big data," Nature Medicine, vol. 25, 01 2019.

[101] N.-Y. Ahn, J. E. Park, D. H. Lee, and P. C. Hong, "Balancing personal privacy and public safety in covid- 19: Case of korea and france," 2020.

[102] A. Downey, "COVID-19: Collaboration is the Engine of Global Science – Especially for Developing Countries," 2020, https://www.weforum.org/agenda/2020/05/globalscience- collaboration-open-source-covid-19/ (Accessed on 20 June 2020).

[103] M. Gagne, "The danger of mainstream media infections with viral and fake information," 2020, https://alibi.com/news/60740/The-Danger-of- Mainstream-Media-Infections-with-Vir.html (Accessed 18 June 2020).

[104] A. Cook, "Covid-19: Companies and verticals at risk for cyber attacks," 2020, https://www.digitalshadows.com/blog-andresearch/ covid-19-companies-and-verticals-at-riskfor- cyber-attacks/ (Accessed 17 June 2020).