Journal of North Khorasan University of Medical Sciences
No 53, Volume 14, Issue 1

Research Article

Risks, Limitations and the Need for Additional Measures Against Ransomware in the Health Information Technology Infrastructure

Mehran Garmehi[1,*]

[1]Assistant Professor University of Bojnord, University of Bojnord, Faculty of Engineering, Central Laboratories Building, APA-UBCERT LAB, Bojnord, Iran

***Corresponding author:** Mehran Garmehi, Assistant Professor University of Bojnord, University of Bojnord, Faculty of Engineering, Central Laboratories Building, APA-UBCERT LAB, Bojnord, Iran. E-mail: m.garme@ub.ac.ir

DOI: 10.52547/nkums.14.1.79

How to Cite this Article:
Garmehi M. Risks, Limitations and the Need for Additional Measures Against Ransomware in the Health Information Technology Infrastructure. *J North Khorasan Univ Med Sci*. 2022;**14**(1):79-85. DOI: 10.52547/nkums.14.1.79

Received: 30 May 2021
Accepted: 20 Feb 2022
Keywords:
Health Information System
Cyber Security
Economic Modelling
Ransomware Attack

Abstract

Introduction: Even before the Covid 19 pandemic, one of the lucrative targets for attackers behind ransomware attacks was Encroaching on the continuity of services in the field of health information technology. In this study, for the first time, while introducing, relying on statistics and modeling, it is shown that the prevention and counteraction of these attacks in the IT infrastructure of the healthcare sector are doubly essential compared to other areas and have a negative reciprocal effect so that this area requires different measures and actions.

Method: First, based on reviewing the statistics obtained from the rescue services in the country's field of countering ransomware attacks, the resulting economic parameters are mapped on the existing models in the issue area. Then, by applying the data obtained from the rescue services against ransomware attacks in the native environment of health information technology, in the created model, an estimate of the interaction of risks is presented.

Results: Economic-statistical analysis of quantitative results from modeling, methodological statistical-economic estimation, and data analysis indicate that the risks of ransomware in healthcare infrastructure can have fundamental differences and interactions with those in other areas of information technology application.

Conclusion: With the arguments and results presented in this study, it is possible to prove the need for different measures and tactics in the field of health information technology and indicate the need for investment and new prioritization for precautions and protective measures in this field.

مجله دانشگاه علوم پزشکی خراسان شمالی
دوره ۱۴، شماره ۱، بهار ۱۴۰۱

مقاله پژوهشی

مخاطرات، محدودیت‌ها و تمهیدات افزون در مقابله با باج افزارها در زیرساخت‌های فناوری اطلاعات حوزه سلامت

مهران گرمه‌ء[۱،*]

[۱]استادیار، گروه مهندسی کامپیوتر و رئیس آزمایشگاه تخصصی آپا، دانشکده فنی و مهندسی، دانشگاه بجنورد، بجنورد، ایران

[*]**نویسنده مسئول:** مهران گرمه‌ء، استادیار، گروه مهندسی کامپیوتر و رئیس آزمایشگاه تخصصی آپا، دانشکده فنی و مهندسی، دانشگاه بجنورد، بجنورد، ایران. ایمیل:m.garme@ub.ac.ir

DOI: 10.52547/nkums.14.1.79

تاریخ دریافت: ۱۴۰۰/۰۷/۲۸
تاریخ پذیرش: ۱۴۰۰/۱۲/۰۱

واژگان کلیدی:
زیرساخت‌های فناوری اطلاعات سلامت
امنیت اطلاعات
مدل‌سازی اقتصادی
حملات باج‌افزاری

چکیده

مقدمه: حتی قبل از پاندمی کووید ۱۹ یکی از اهداف پرمنفعت برای مهاجمین پشت حملات باج‌افزاری، دست‌اندازی به استمرار خدمات در حوزه فناوری اطلاعات سلامت بود. در این پژوهش برای اولین بار ضمن معرفی، با تکیه بر آمار و مدل‌سازی نشان داده می‌شود که پیشگیری و مقابله با این حملات در زیرساخت‌های فناوری اطلاعات حوزه سلامت، دارای اهمیت مضاعف در قیاس با سایر حوزه‌ها بوده، تأثیر منفی متقابل داشته و در این حوزه نیاز به تمهیدات و اقداماتی متفاوت وجود دارد.

روش کار: ابتدا با اتکا بر مرور آمارهای حاصل از ارائه خدمات امدادی در حوزه مقابله با حملات باج‌افزاری در سطح کشور، پارامترهای اقتصادی حاصل بر مدل‌های موجود در فضای مساله نگاشت می‌شود. پس از آن با اعمال داده‌های حاصل از ارائه خدمات امدادی در حوزه مقابله با حملات باج‌افزاری در فضای بومی فناوری اطلاعات سلامت، در مدل ایجاد شده، تخمینی از برهم‌کنش مخاطرات ارائه می‌گردد.

یافته‌ها: تحلیل اقتصادی-آماری نتایج کمی حاصل از مدلسازی، تخمین و تحلیل روش‌مند آماری-اقتصادی داده‌ها گواه بر آن است که مخاطرات ناشی از باج افزارها در زیرساخت‌های حوزه سلامت می‌تواند تفاوت‌هایی بنیادین و تاثیری متقابل با آنچه در سایر حوزه‌های کاربرد فناوری اطلاعات وجود دارد، داشته باشند.

نتیجه گیری: با استدلال‌ها و نتایج عرضه شده در این پژوهش می‌توان نیاز به تمهیدات و تدابیر متفاوت در زمینه فناوری اطلاعات حوزه بهداشت و درمان را به اثبات رساند و لزوم سرمایه‌گذاری و اولویت‌بندی جدید برای تمهیدات و اقدامات حفاظتی در این عرصه را نمایان نمود.

مقدمه

حوزه فناوری و فضای تبادل اطلاعات همواره در معرض تعرض‌های جدی بدخواهان با انگیزه‌های متفاوت بوده است، اما در سال‌های اخیر با رشد و توسعه فناوری‌های مرتبط با رمزنگاری و توسعه آن به تبادلات امن مالی و ارتباطات غیر قابل پیگرد در شبکه، بدافزارهایی که از آنها به عنوان باج افزار یاد می‌کنیم، متولد شدند. باج‌افزار اصطلاحی کلی برای توصیف خانواده‌ای از بدافزارها و حملات سایبری است که برای باج‌گیری از قربانیان خود در حوزه فناوری اطلاعات و مجبور کردن آنها به پرداخت مبلغی از ارزش، طراحی شده‌اند (۱) به طور کلی، این حملات را می‌توان به دو گروه تقسیم کرد. نوع اصلی از این حملات متکی بر گروهی از بدافزارها است که داده‌ها را رمزگذاری و ناخوانا کرده یا دسترسی به آنها را ناممکن می‌کنند. گروه دیگری از باج‌افزارها که امروزه کمتر شیوع دارند، دسترسی به سیستم عامل را محدود کرده یا کاربران را از دسترسی به سیستم‌های خود باز می‌دارند (۲).

امروزه روش انتقال ارزش و مطالبه پرداخت باج که اکثر مهاجمین پشت باج‌گیرهای دیجیتالی درخواست می‌کنند، مبتنی بر استفاده از پول رمز پایه بوده و معمولاً بیت‌کوین به این منظور به کار می‌رود (۲).

توسعه تکنولوژی در این خانواده از بدافزارها، ارائه کدهای متن باز از باج افزارهای آموزشی و موفقیت مهاجمین در استخراج منابع مالی چشمگیر از این حوزه، سبب شده تا امواج جدیدی از انواع حملات باج‌افزاری را شاهد باشیم (۳).

تنها با جمع شدن همزمان شرایطی به شرح زیر یک حمله باج افزاری می‌تواند به موفقیت تضمین شده یعنی دریافت باج نائل گردد: وجود راهی سهل برای انتقال و اجرای دستورات مهاجم در رایانه (های) قربانی، ارزشمند بودن داده‌ها یا خدمات، در دسترس بودن ابزارهای رمزگذاری قدرتمند، امکان انتقال ارزش و دریافت باج به صورت ناشناس، امکان دسترسی آسان قربانی به روش پرداخت باج، وجود کانال ارتباطی ناشناس بین مهاجم و قربانی و عدم وجود نسخ پشتیبان سالم از اطلاعات یا طرح بازگشت از فاجعه موفق و آزموده شده. طبیعی است

که برای به شکست کشاندن حمله کافی است تا حداقل یکی از این شرایط مثلاً در دسترس بودن ابزارهای رمزگذاری قدرتمند، نقض گردد. در مراجع گفته می‌شود که صنعت باج‌افزار، کسب و کاری بسیار سودآور با هزینه نزدیک به صفر یا قابل اغماض است که می‌تواند برای دنیای فناوری اطلاعات بسیار خطرناک باشد (۲). همچنین در مراجع سودآوری قابل توجه حملات باج‌افزاری را به عنوان دلیل رشد سرسام‌آور رخداد این حملات می‌شناسند (۴).

از منظر اقتصادی و با دقت در اقتصاد مساله، هزینه راه‌اندازی یک حمله باج‌افزاری می‌تواند در مقایسه با درآمدهای ناشی از آن بسیار ناچیز باشد، چرا که برای انجام حمله از چند روش مختلف استفاده می‌شود که در تمامی آنها هزینه راه اندازی حمله در عمل بسیار کوچک بوده و منجر به ایجاد درآمدهای درشت می‌شود (۵).

مدلسازی حملات باج‌افزاری، موضوعی جذاب در بین پژوهشگران این حوزه بوده است (۶). در مسیر مدلسازی حملات باج افزاری مشاهده می‌گردد که انگیزه‌های اقتصادی مهاجمین و ارزش بستر به گروگان گرفته شده در سمت قربانیان در یک برهم‌کنش استراتژیک، تصمیم مهاجم برای تعیین مبلغ مطالبه شده به عنوان باج و رویکرد استراتژیک قربانی در پذیرش پرداخت باج یا رد درخواست و تحمل خسارات ناشی از حمله را می‌سازد. روش مدلسازی اقتصادی و طراحی سازوکار، در گذشته و در سایر زمینه‌های علوم کامپیوتر، با دست آوردهای چشمگیر کاربرد داشته (۷) و این زمینه در مدلسازی تعامل بین مهاجم و قربانی، به نظر یک رویکرد مناسب به نظر می‌رسد.

در مراجع علاوه بر این که اذعان بر عدم توجه کافی بر حوزه مخاطرات ناشی از باج افزارها در زیرساخت‌های حوزه سلامت، مشاهده می‌گردد (۸)، گزارشات آماری نگران کننده‌ای نیز از خسارات ناشی از این حملات در این زیرساخت‌ها و روند کلی تغییرات در این حوزه نیز به چشم می‌آید (۹). اگرچه در مورد حمله باج افزاری معروف واناکرای، به طور قاطع ادعای رخداد از دست رفتن جان انسانها در اثر حمله سایبری اثبات نشد، اما گزارش‌هایی مستند از این رخداد در حملات بعدی در رسانه‌ها وجود دارد (۱۰). اتفاقاتی متداول و به سادگی آن چه در یک حمله کوچک چون آنچه در (۱۱, ۱۲) گزارش شده، هزاران دلار باج را به این بازار زیرزمینی و خلاف تزریق کرده، خسارات اقتصادی جدی با از کار انداختن روند ارائه خدمات در این حوزه ایجاد نموده و سبب شده است که در این خصوص حتی تمهیداتی فنی در خصوص روش‌ها و رویکردهای اختصاصی برای مقابله با این مخاطرات در حوزه سلامت نیز ارائه شود (۱۳). در همین گزارش (۱۳)، افزون بودن اهمیت و حساسیت امنیت اطلاعات در حوزه سلامت با ارائه آمارهایی کلی و مقایسه بین میزان خسارات ناشی از رخدادها در این حوزه در قیاس با حوزه عمومی امنیت اطلاعات گزارش شده است. همچنین در همین مرجع، نسبت رشد نگران کننده فراوانی رخدادها در حوزه سلامت نیز گزارش شده است.

با مرور منابع و تا جایی که می‌دانیم نه تنها مطالعه برهم‌کنش اقتصادی حملات باج‌افزاری در حوزه سلامت و خارج از آن در سطح جهان هنوز مورد مطالعه قرار نگرفته است، که در سطح ملی نیز این یک مطالعه جدید است. در این پژوهش نتایج حاصل از ارائه خدمات امدادی در حوزه باج افزارها در سطح ملی در یک بازه ۳ ساله با تفکیک حوزه سلامت، بر مدل اقتصادی مساله اعمال می‌گردند، تا بتوان در مورد دو موضوع مهم به قضاوت رسید، اول این که میزان خسارات ناشی از حملات باج‌افزاری در این حوزه چه تفاوتی با حوزه عمومی فناوری اطلاعات دارد و دیگری این که تأثیر رخداد حملات موفق در این حوزه بر خسارات ناشی از حملات باج افزاری در کل جامعه چگونه است.

روش کار

با توجه به ساختار و شرایط حملات باج‌افزاری معمول که به تجربه مشاهده شده است، مهاجم با تعیین و بهینه‌سازی میزان باج مطالبه شده به دنبال بیشینه کردن درآمد و به تبع سود خود می‌باشد (۱۴). بر اساس سوابق، در حملات باج‌افزاری معمولاً مهاجمین برای انجام این نوع از نفوذ، هزینه‌های قابل توجهی متحمل نمی‌شوند (۱۴). به این ترتیب می‌توان سمت هزینه در تابع سود مهاجم را به تقریب، صفر دانست.

در مراجع حوزه طراحی سازوکارهای اقتصادی (۱۵)، به عنوان سازوکارهای بیشینه‌کننده سود، به دو گروه از حراجها اشاره می‌شود. گروه اول از حراجهای بیشینه‌کننده سود، بر اطلاعات و دانش پیشین از میزان ارزش اطلاعات تکیه نمی‌کند، بلکه طرف فروشنده (مهاجم) در یک سازوکار راستگو از خریداران (قربانیان) می‌خواهد که برای دریافت خدمت یا محصول (بازگشایی اطلاعات) پیشنهاد قیمت دهند (۱۶). پس از آن با انجام یک بهینه‌سازی ساده، قیمت بهینه و بیشینه‌کننده سود تعیین می‌شود. به طور طبیعی و با توجه به ساختار حمله باج‌افزاری که در آن معمولاً مهاجم بدون سؤال از قربانی قیمت باج را تعیین می‌نماید، می‌توان این رویکرد را در این مساله رد شده دانست. رویکرد دیگر که روش مبتنی بر اطلاعات پیشین نام دارد، با توجه به ساختار اقتصادی موضوع، منطبق بر این مساله می‌باشد. از میان سازوکارهای بیشینه کننده سود آن دسته که در آنها هزینه تولید یا ارائه خدمات، قابل اغماض می‌باشد، در گروه حراجهای بیشینه کننده سود محصولات و خدمات دیجیتال دسته‌بندی می‌شوند (۱۷). در مراجع برای تعیین قیمت بهینه در این سازوکارها، اثبات شده است که می‌توان بر روش Myerson تحت شرایط مزایده محصولات دیجیتال متکی بود (۱۸).

در (۶) با مدلسازی ریاضیات حاکم بر اقتصاد مساله و با اتکا بر سازوکارهای بیشینه‌کننده سود در بازار محصولات دیجیتال، تاثیرات متقابل مداخلات در بازار رمز ارز بر اقتصاد، انگیزه‌ها و عوارض حملات باج افزاری بررسی شده است.

در (۶) برای مدل کردن مساله از متغیرهایی برای معرفی مجموعه‌های مختلفی از قربانیان درگیر در حمله استفاده شده است. با در پیش گرفتن همین رویکرد، با اغماض از جزییات می‌توان قربانیانی که از حمله آسیب دیده‌اند و در آنها جمیع شرایط موفقیت حمله باج‌افزاری برقرار است، از جمله ارزشمندی خدمات و اطلاعات و در اختیار نداشتن نسخ پشتیبان یا طرح جامع بازگشت از فاجعه، را با VCM معرفی نمود. مدیران این زیرساختهای قربانی خود را در شرایطی خواهند یافت که مجبورند بین دو گزینه پرداخت باج و احتمالاً بازپس گرفتن دارایی‌های الکترونیکی خود یا رد کردن تقاضای پرداخت باج و تحمل کردن خسارات ناشی از حمله، انتخاب کنند. به این ترتیب مجموعه VCM به دو مجموعه RPV و LDV افراز می‌شوند. این افراز با تصمیم استراتژیک قربانیان در مقابل مطالبه مبلغ باج که از سوی مهاجم اتفاق

می‌افتد جامه عمل می‌پوشد. به بیان ساده، مهاجم (ها) از هریک از قربانیان حمله یعنی $v \in VCM$ عددی چون r_v را به عنوان باج مطالبه می‌کنند. جدول ۱ متغیرهای مورد استفاده در این فرآیند مدلسازی را معرفی می‌کند.

در یک حمله باج‌افزاری، تعداد قربانیان معمولاً (و نه البته همواره) بیش از آن است که مهاجم فرصت لازم برای کسب شناخت از زیرساخت‌های آنها را داشته باشد. بنابراین مهاجم معمولاً نمی‌تواند میزان بهینه باج بر اساس ارزش دارایی‌های به گروگان گرفته را تعیین کند. از این رو، معمولاً عدد یکسان و ثابتی به عنوان مبلغ باج درخواستی، برای تمام قربانیان تعیین و مطالبه می‌شود. برای این موضوع اگر چه به ندرت مثال‌های نقض نیز یافت می‌شود، اما در محاسبات می‌توان موارد نقض را برای رسیدن به یک مدل قابل اتکا نادیده گرفت.

جدول ۱. معرفی متغیرهای استفاده شده در مدل‌سازی اقتصادی حملات باج‌افزاری

نام متغیر	مفهوم
VCM	مجموعه رایانه‌های قربانی حمله (ViCtiM)
RPV	مجموعه رایانه‌های قربانی حمله که باج را پرداخت می‌کنند (Ransom Paying Victims)
LDV	مجموعه رایانه‌های قربانی حمله که باج را پرداخت نمی‌کنند. (Lost Data Victims)
V	یکی از قربانیان حمله (عضو VCM)
r_v	میزان باج مطالبه شده(Ramsom) از قربانی v در حمله
SEV_v	میزان تخمین قربانی v از ارزش دارایی‌های به گروگان گرفته شده از سوی مهاجم (Self-Estimated Value)
RVN_{RWA}	درآمد حاصل از حمله RWA (ReVeNue)
PRF_{RWA}	سود خالص حاصل از حمله RWA (PRoFit)
CST_{RWA}	هزینه صرف شده برای حمله RWA (CoST)
TLD_{RWA}	خسارت تحمیل شده به اعضای مجموعه VCM در حمله RWA (Total Loss Damage) که باج را نپرداختند.
TVS_{RWA}	کل خسارت ایجاد شده در اثر خرابکاری ناشی از حمله RWA (Total Value of Sabotage)

در افراز مجموعه VCM به RPV و LDV، متغیر r که میزان باج مطالبه شده از سوی مهاجم می‌باشد و میزان ارزش دارایی‌های به گروگان گرفته شده از سوی مهاجم که توسط قربانی تخمین زده می‌شود و با SEV_v نشان داده شده است، نقش کلیدی را بر عهده دارند.

$$RPV = \{v \in VCM | SEV_v \geq r\}$$ رابطه ۱

بنابراین؛

$$LDV = VCM - RPV$$ رابطه ۲

به عبارت دیگر، مهاجم با تعیین مبلغ باج مطالبه شده، سبب تقسیم مجموعه قربانیان به این دو مجموعه می‌شود. قربانیان با رفتاری استراتژیک، در صورتی که ارزش اطلاعات خود را بیش از مبلغ باج مطالبه شده بدانند، پرداخت باج را یک سیاست غالب اقتصادی خواهند یافت، در این صورت در مجموعه RPV قرار گرفته و مبلغ باج برابر با r را خواهند پرداخت و در غیر این صورت در مجموعه LDV قرار گرفته و متحمل خسارت مساوی با ارزش اطلاعات و خدمات از دست رفته خود می‌شوند.

در تعیین r، مهاجم به دنبال بیشینه کردن سود خود می‌باشد. بر اساس سوابق، در حملات باج‌افزاری معمولاً آسیب‌پذیری‌های روز صفر که تهیه آن‌ها هزینه‌های قابل توجه در بر دارد، استفاده نمی‌شود (۲)، بلکه از آسیب‌پذیری‌های شناخته شده که برای آن‌ها روش‌های پیشگیری مناسب و به‌روزرسانی مؤثر منتشر شده است و البته برخی از کاربران با سهل‌انگاری، آن وصله‌ها و به‌روزرسانی‌ها را نادیده گرفته‌اند، یا روش‌های دیگری چون شنود یا کشف رمز ورود به سامانه‌های دارای قابلیت دسترسی از راه دور یا مهندسی اجتماعی و فریفتن کاربران برای نصب تکه برنامه‌های مخرب پیوست شده به هرزنامه‌ها، استفاده می‌شود. انجام این نوع از نفوذ هزینه‌های قابل توجهی در بر ندارد. سایر مراحل حمله نیز با اتکا به امکانات نرم‌افزاری و سخت‌افزاری قربانی انجام می‌گیرد. معمولاً رمزگذاری اطلاعات با اتکا بر امکانات استاندارد رمزنگاری موجود در سامانه قربانی انجام می‌شود. در پردازش رمزکردن اطلاعات از بستر سخت‌افزار قربانی و در صورت نیاز، در تبادل اطلاعات با سرورهای کنترل و مدیریت حمله، از دسترسی شبکه سامانه قربانی سوء استفاده می‌شود. به این ترتیب می‌توان سمت هزینه در تابع سود مهاجم را به تقریب، صفر دانست. به این ترتیب اگر درآمد حاصل از حمله RWA را با RVN_{RWA} نشان دهیم و از نماد PRF_{RWA} برای نشان دادن سود و از نماد CST_{RWA} برای نشان دادن هزینه حمله RWA استفاده کنیم، داریم؛

$$PRF_{RWA} = RVN_{RWA} - CST_{RWA} \text{ and } CST_{RWA_a} \simeq 0 \rightarrow PRF_{RWA} \simeq RVN_{RWA}$$ رابطه ۳

در مراجع، به عنوان سازوکارهای بیشینه‌کننده سود، به دو گروه از حراج‌ها اشاره می‌شود. در (۶) با استدلال کافی بر روشی مبتنی بر اطلاعات پیشین که، با توجه به ساختار اقتصادی موضوع، منطبق بر این مساله می‌باشد، تکیه شده است. از میان سازوکارهای بیشینه‌کننده سود آن دسته که در آنها هزینه تولید یا ارائه خدمات، قابل اغماض می‌باشد، در گروه حراج‌های بیشینه‌کننده سود محصولات و خدمات دیجیتال دسته‌بندی می‌شوند (۱۷). در مراجع برای تعیین قیمت بهینه در این سازوکارها، اثبات شده است که می‌توان بر روش Myerson تحت شرایط مزایده محصولات دیجیتال متکی بود (۱۸)؛

$$\phi(r) = r - \frac{1-CDF(r)}{pdf(r)} \rightarrow Opt(r) = \phi^{-1}(0)$$ رابطه۴

که در این رابطه r مقدار بهینه پیشنهاد شده از سوی مهاجم را نشان می‌دهد. توابع CDF و pdf به ترتیب معرف تابع توزیع تجمعی و تابع توزیع احتمال متغیر r هستند. در نتیجه، بر اساس (۱۸) با یافتن نقطه صفر در معکوس تابع Myerson که با $\phi^{-1}(0)$ نشان داده شده، می‌توان به مقدار بهینه r در این مزایده دست یافت.

بر اساس مشاهدات می‌توان گفت که مهاجمین با تکیه بر تجارب گذشته و سعی و خطا در تغییر دادن مقدار باج در حملات متوالی به دنبال بیشینه کردن سود (درآمد) خود خواهند بود (۱۴). با تعیین و مشخص شدن مقدار باج r، آن دسته از قربانیان که در مجموعه RPV قرار می‌گیرند، در مجموع به اندازه

$$PRF_{RWA} \simeq RVN_{RWA} = r.|RPV|$$ رابطه ۵

به مهاجم می‌پردازند و احتمالاً (۲) اطلاعات به گروگان گرفته شده خود را باز پس می‌گیرند. اعضای مجموعه LDV نیز به اندازه

$$TLD_{RWA} = \sum_{v \in LDV} CEV_v$$ رابطه ۶

متحمل خسارت می‌شوند. در این رابطه TLD_{RWA} نشان‌دهنده خسارت ناشی از از دست رفتن اطلاعات و تنظیمات آن دسته از قربانیان است که باج را پرداخت نکرده‌اند. همچنین به میزان ارزش واقعی اطلاعات قربانیانی که باج را پرداخته‌اند از بروز خسارت جلوگیری شده است.

مهاجم از یک سو موفق به دریافت مبلغ RVN_{RWA} از قربانیان و ایجاد سود تقریباً برابر با همین مبلغ برای خود می‌شود و از سوی دیگر سبب ایجاد خسارتی برابر با مجموع خسارت وارد شده به سیستم‌های آسیب‌دیده شامل خسارت عدم پرداخت باج، منهای ارزش کل اطلاعات قربانیانی که باج را پرداخته‌اند به علاوه مجموع باج دریافت شده، در سطح اقتصاد کلان خواهد شد که با TVS_{RWA} نشان داده شده است:

$$TVS_{RWA} = RVN_{RWA} + TDG_{RWA} - \sum_{v \in RPV} CEV_v$$ رابطه ۷

یافته‌ها

بر اساس داده‌های ارائه شده در جدول (۲) برای ۲۳۷ مورد مشاهده در فرآیند امداد باج افزاری، ۳۹ مورد متعلق به حوزه سلامت بوده است. در جدول (۲) جزییات موضوع به تفکیک ارائه شده است. در این پژوهش برای به دست آوردن دو تابع CDF و pdf در هریک از گروههای رخدادها با دسته بندی کلی، منحصر به حوزه سلامت و غیر آن، با دقت کافی از رگرسیون چندجمله‌ای درجه ۵ استفاده شده است تا بتوان با مدل کردن رفتار مهاجمین پس از کسب تجربه یا آگاهی از ارزش اطلاعات قربانیان بعدی، به تخمین و پیشبینی نتایج حاصل از رخداد حملات آتی پرداخت. نتایج حاصل از این اقدام و محاسبات مرتبط با آن در دو سطر پایانی این جدول گزارش شده‌اند. در این گزارش داده‌های ۲۳۷ مورد از حملات باج‌افزاری که در بازه ۱۳۹۶/۱/۱ تا ۱۳۹۹/۱۲/۳۰ برای ارائه خدمات امدادی به یکی از مراکز آپا فعال در یکی از دانشگاههای کشور ارجاع شده، گزارش شده است. از این میان ۳۹ مورد از قربانیان بیمارستان‌ها، حوزه درمان دانشگاههای علوم پزشکی، کلینیک‌های خصوصی، سامانه‌های مدیریت اطلاعات سلامت و سایر سامانه‌های مرتبط بوده‌اند. در فرآیند امدادی یکی از اولین داده‌های مورد نیاز، ارزش بستر مورد حمله و خسارات ناشی از رخداد امنیتی به صورت تخمینی بوده است که در جدول (۲) به صورت تجمعی و میانگین، گزارش شده است. همچنین با بررسی شواهد و پیام‌ها در سامانه قربانی، اجرای کدهای مهاجم در بستر آزمایشگاهی یا با اتکا بر دانش قبلی، مبلغ باج مطالبه‌شده در مورد هر حمله استخراج شده و به دلیل شناور بودن قیمت بیت‌کوین و سایر رمزارزها در گذر زمان و همچنین تغییرات معمول در تغییر ارزش ریال، برحسب دلار امریکا در زمان حمله ثبت و گزارش گردیده است.

جدول ۲. گزارش داده‌ها و نتایج حاصل از مدل‌سازی آماری حملات باج‌افزاری

ردیف		کلیه موارد امدادی	حوزه سلامت	غیر حوزه سلامت
۱	تعداد رویدادهایی که خدمات امدادی دریافت نموده‌اند.	۲۳۷	۳۹	۱۹۸
۲	درصد از کل رویدادها	۱۰۰	۱۶	۸۴
۳	میانگین باج مطالبه شده (دلار امریکا در روز رخداد)	۱۰۵۷	۱۷۷۴	۹۱۶
۴	مجموع خسارت (دلار امریکا در روز هر رخداد)	۲۲۳۴۷۴	۶۵۸۴۷	۱۵۷۶۲۷
۵	میانگین خسارت (دلار امریکا در روز هر رخداد)	۹۴۲	۱۶۸۸	۷۹۶
۶	مجموع درآمد مهاجم (دلار امریکا در روز رخداد)	۱۹۱۶۰۰	۴۶۲۰۰	۱۴۵۴۰۰
۷	میانگین درآمد مهاجم از کل حملات (دلار امریکا در روز رخداد)	۸۰۸	۱۱۸۴	۷۳۴
۸	مجموع خسارت در عدم پرداخت باج (دلار امریکا در روز رخداد)	۳۱۸۷۴	۱۹۶۴۷	۱۲۲۲۷
۹	میانگین خسارت در شرایط عدم پرداخت باج (دلار امریکا در روز رخداد)	۳۷۲	۵۰۳	۶۱
۱۰	میانگین ارزش بستر به گروگان گرفته شده (هزار دلار امریکا در روز رخداد)	۴۱۵۲	۲۲۰۲۷	۶۳۲
۱۱	مقدار بهینه برای باج مطالبه شده	۱۷۹۵	۴۰۳۶	۸۲۳
۱۲	درصد تغییر مجموع خسارت در صورت اعمال مقدار بهینه باج	۵۴	۱۴۷	-۱۹
۱۳	درصد تغییر درآمد مهاجمین در صورت اعمال مقدار بهینه باج	۳۲	۱۳۴	۹

دیگر نکته مهم و شایان ذکر در خصوص داده‌های ارائه شده، اطمینان از وجود موارد گزارش نشده یا رخدادهای ارجاع نشده برای ارائه خدمات امدادی است که ساده‌ترین دلیل آن به تجربه، پنهان کردن موضوع از نهادهای ناظر بر امنیت اطلاعات به قیمت محروم شدن از خدمات امدادی بوده است.

عموماً این موضوع که قربانیان مبلغ باج مطالبه شده را در نهایت پرداخت می‌نمایند یا نه، بر تیم امداد فاش نمی‌شود اما شواهد نشان از آن دارد که اگرچه پرداخت باج احتمالاً عملی دارای ابعاد حقوقی منفی بوده و تضمینی بر بازگشت گروگان پس از آن وجود ندارد، رخداد نادری نیست. به این دلیل، در ارائه اطلاعات آماری در این حوزه به بررسی اقتصادی بودن پرداخت باج در سمت قربانی تکافو شده و با اتکا بر استنتاج و در نظر داشتن مبلغ مطالبه شده و ارزش زیرساخت گرو گرفته شده، تصمیم استراتژیک قربانیان بازسازی شده و آنها را به دو مجموعه پرداخت کننده باج یا رد کننده پیشنهاد مهاجم دسته بندی کرده‌ایم. این رویکرد، راه محاسبه درآمد مهاجمین و خسارات مجموعه قربانیانی را که باج را پرداخت نمی‌کنند نیز هموار می‌سازد.

در دو سطر پایانی جدول، با اتکا بر داده‌ها و مدل، نتایج حاصل از بهینه سازی فرضی مبلغ باج مطالبه شده در یک سازوکار اقتصادی شفاف در سمت مهاجم، آورده شده است.

بحث

با اتکا بر آمار ارائه شده می‌توان مشاهده نمود که حوزه سلامت کسر قابل اعتنایی از قربانینان حملات باج افزاری را به خود اختصاص داده

است. همچنین با توجه به آمارها در سطر ۳ جدول می‌توان مشاهده کرد که میانگین باج مطالبه شده در مورد قربانیان حوزه سلامت ۹۳ درصد بیشتر از میانگین بوده است. با توجه به همین آمارها در سطر ۴ میزان خسارت ایجاد شده در این حوزه اگرچه تنها ۱۶ درصد قربانیان را تشکیل می‌دهند اما ۲۹ درصد از خسارت کل را می‌سازد. این موضوع نشان از آن دارد که اگرچه نه به کمال اما مهاجمین حداقل در قسمت قابل توجهی از حملات به زیرساخت‌های حوزه سلامت، آگاهی و شناخت ز مجموعه قربانی را دارا می‌باشد. در ادامه می‌توان مشاهده کرد که میانگین خسارت در حوزه سلامت تقریباً ۷۹ درصد بیش از سایر حوزه‌ها است. به سادگی می‌توان مشاهده کرد که این به دلیل ارزش و حساسیت بالاتر خدمات و داده‌ها در این حوزه است.

نگاهی بر سطر ۶ نشانگر این است که مهاجمین ۲۴ درصد درآمد خود را از حوزه درمان که تنها ۱۶ درصد قربانیان را تشکیل می‌دهند به دست آورده‌اند. همچمنین با نگاهی به سطر بعد می‌توان دید که میانگین درآمد مهاجمین از این حوزه ۶۱ درصد بیشتر از میانگین سایر قربانیان است. سطر بعد جدول که مجموع خسارت در عدم پرداخت باج را معرفی می‌کند نشان می‌دهد که قربانیانی که به طور استراتژیک تصمیم به عدم پرداخت باج می‌گیرند در حوزه سلامت بیش از ۶۰ درصد نسبت به سایرین متحمل خسارت بیشتر می‌شوند. علاوه بر این نگاهی به سطر بعد که میانگین خسارت در شرایط عدم پرداخت باج را نمایش می‌دهد عمق این مشاهده را با وضوح بیشتر به شکل نسبت بیش از ۸ برابر خسارت میانگین در عدم پرداخت باج در حوزه سلامت به نسبت سایر قربانیان نشان می‌دهد.

این مشاهدات به این نتیجه گیری اولیه می‌رسند که اهمیت دفاع در برابر باج افزارها و ارائه خدمات امدادی در پس رخداد هر حمله در حوزه سلامت بسیار بیشتر از سایر حوزه‌های کاربرد فناوری اطلاعات است.

این نتیجه گیری با توجه به تخمین ارائه شده در خصوص میانگین ارزش بستر به گروگان گرفته شده که نشان از ارزش ۳۴ برابری زیرساخت‌های در معرض حمله در حوزه سلامت در قیاس با میانگین سایر حوزه‌ها دارد قابل درک است.

نتیجه‌گیری

با اعمال نتایج حاصل از مدلسازی اقتصادی حمله، مقدار بهینه برای باج مطالبه شده، درصد رشد مجموع خسارت در صورت اعمال مقدار بهینه باج و درصد رشد درآمد مهاجمین در صورت اعمال مقدار بهینه باج محاسبه شده است. نگاهی گذرا بر این مقادیر گواه از آن است که اگر مهاجمین بتوانند به هر طریق ممکن با به دست آوردن دانش یا بینش کافی یا در اثر بی احتیاطی قربانیان در زمان مذاکره، به ارزش بستر مورد حمله پی ببرند و میزان بهینه‌ای از باج را مطالبه کنند چه اتفاقاتی رخ خواهد داد. در ابتدا می‌توان دید که مقدار میانگین بهینه برای باج مطالبه شده رشد حدود ۷۰ درصدی از ۱۰۵۷ دلار به ۱۷۹۵ خواهد داشت. این موضوع در خصوص حوزه سلامت از ۱۷۷۴ به ۴۰۳۶ دلار یعنی به بیش از ۱۲۷ درصد رشد می‌رسد. ساده‌ترین نتیجه نامیمون ناشی از این موضوع می‌تواند افزایش تلاش مهاجمان برای نفوذ به این زیرساخت‌ها باشد.

در این شرایط اما در حوزه خارج از خدمات سلامت شاهد کاهش میزان باج مطالبه شده از ۹۱۶ دلار به ۸۲۳ هستیم. در درصد تغییرات مجموع خسارت در صورت اعمال مقدار بهینه باج موضوع با مشاهده ۵۴ درصد در حالت کلی، ۱۴۷ درصد رشد در حوزه سلامت و ۱۹ درصد کاهش در غیر حوزه سلامت مواجه می‌شویم. این مشاهده و در نظر گرفتن درصد تغییرات مجموع درآمد مهاجمین در صورت اعمال مقدار بهینه باج که رشد ۳۲ درصدی درکل و ۱۳۴ درصدی در حوزه سلامت و ۹ درصدی در سایر قربانیان را نشان می‌دهد نتایج قابل توجه و ارزشمندی به شرح زیر را در مقابل حوزه پدافند سایبری قرار می‌دهد:

الف: ضرورت دقت جدی در حوزه سلامت در زمان مقابله با رخداد برای عدم اطلاع یافتن مهاجم از ارزش بستر به گروگان گرفته شده.

ب: دقت در حوزه سلامت و توجه به کاهش رخداد و سود حملات با سرمایه گذاری در حوزه درمان

ج: وجود انگیزه اقتصادی در مهاجم برای کاهش دادن مبلغ باج به رغم افزایش درآمد و کاهش خسارت در اثر خروج قربانیان حوزه سلامت از مجموعه قربانیان.

جمع بندی نتایج حاصل از این مطالعه را می‌توان در یک عبارت خلاصه کرد: " در حوزه سلامت باید برای مقابله با حملات باج‌افزاری سرمایه گذاری مضاعف انجام داد. این سرمایه‌گذاری نه تنها برای پیشگیری از رخداد خسارات سنگین در این حوزه ضروری است که از آسیب ناشی از افزایش درآمد مهاجمان باج افزاری و افزایش خسارات در خارج این حوزه نیز تأثیر جدی دارد."

References

1. Gazet A. Comparative analysis of various ransomware virii. *J Comput Virol.* 2010;**6**(1):77-90. **DOI:** 10.1007/s11416-008-0092-2
2. Liska A, Gallo T. Ransomware: Defending Against Digital Extortion. 1st ed. O'Reilly Mecia Inc2016.
3. Kharaz A, Arshad S, Mulliner C, Robertson W, Kirda E. {UNVEIL}: A large-scale, automated approach to detecting ransomware. In: 25th {USENIX} Security Symposium ({USENIX} Security 16). 2016:757-772.
4. Laszka A, Farhang S, Grossklags J. On the economics of ransomware. In: International Conference on Decision and Game Theory for Security. Springer. 2017:397-417. **DOI:** 10.1007/978-3-319-68711-7_21
5. Kharraz A, Robertson W, Balzarotti D, Bilge L, Kirda E. Cutting the gordian knot: A look under the hood of ransomware attacks. In: International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment. Springer. 2015:3-24. **DOI:** 10.1007/978-3-319-20550-2_1
6. Garmehi M, Rahimi Devin S. Economic Modeling of Restricting the cryptocurrency market on ransomware attacks. Persian. *Econ Model.* 2020;**14**(51):16-38.
7. Garmehi M, Analoui M, Pathan M, Buyya R. An economic replica placement mechanism for streaming content distribution in Hybrid CDN-P2P networks. *Comput Commun.* 2014;**52**:60-70. **DOI:** 10.1016/j.comcom.2014.06.007
8. Kruse CS, Frederick B, Jacobson T, Monticone DK. Cybersecurity in healthcare: A systematic review of modern threats and trends. *Technol Health Care.* 2017;**25**(1):1-10. **DOI:** 10.3233/THC-161263 **PMID:** 27689562
9. Zimba A, Chishimba M. On the economic impact of crypto-ransomware attacks: the state of the art on enterprise systems. *Eur J Secur Res.* 2019;**4**(1):3-31. **DOI:** 10.1007/s41125-019-00039-8
10. Eddy M, Perlroth N. Cyber Attack Suspected in German Woman's Death. The New York Times [Internet]. [cited 2021 Aug 30] 2020 Available from:

https://www.nytimes.com/2020/09/18/world/europe/cyber-attack-germany-ransomeware-death.html.
11. Snell E. Patient Data Unaffected in Hancock Health Ransomware Attack [Internet]. HealthITSecurity- Xtelligent Healthcare Media. [cited 2021 Aug 30] 2018. Available from: https://healthitsecurity.com/news/patient-data-unaffected-in-hancock-health-ransomware-attack.
12. Farringer DR. Send us the Bitcoin or patients will die: addressing the risks of ransomware attacks on hospitals. *Seattle UL Rev*. 2016;**40**:937.
13. Abraham C, Chatterjee D, Sims RR. Muddling through cybersecurity: Insights from the US healthcare industry. *Bus Horiz*. 2019;**62**(4):539-548. **DOI:** 10.1016/j.bushor.2019.03.010
14. Hernandez-Castro J, Cartwright A, Cartwright E. An economic analysis of ransomware and its welfare consequences. *R Soc Open Sci*. 2020;**7**(3):190023. **DOI:** 10.1098/rsos.190023 **PMID:** 32269778
15. Ory MG, Yuma PJ, Hurwicz ML, Jarvis C, Barron KL, Tai-Seale T, et al. Prevalence and correlates of doctor-geriatric patient lifestyle discussions: analysis of ADEPT videotapes. *Prev Med*. 2006;**43**(6):494-497. **DOI:** 10.1016/j.ypmed.2006.06.015 **PMID:** 16901534
16. Guruswami V, Hartline JD, Karlin AR, Kempe D, Kenyon C, McSherry F. On profit-maximizing envy-free pricing. In: SODA. 2005:1164-1173.
17. Goldberg AV, Hartline JD. Envy-free auctions for digital goods. In: Proceedings of the 4th ACM conference on Electronic commerce. 2003:29-35. **DOI:** 10.1145/779928.779932
18. Nisan N, Roughgarden T, Tardos E, Vazirani V. Algorithmic Game Theory [Internet]. Cambridge: Cambridge University Press 2007. Available from: https://www.cambridge.org/core/books/algorithmic-game-theory/0092C07CA8B724E1B1BE2238DDD66B38.