فصلنامه مدلسازی اقتصادی (سال چهاردهم، شماره ۳ «پیاپی ۵۱» پاییز ۱۳۹۹، صفحه‌های ۳۸-۱۷)

مدل‌سازی اقتصادی تاثیر محدودسازی بازار رمز ارز بر حملات باج‌افزاری

مهران گرمه‌ء[*]، سارا رحیمی دوین[**]

تاریخ دریافت: ۹۹/۰۵/۲۵ تاریخ پذیرش: ۹۹/۱۱/۲۰

چکیده

هدف این مقاله تبیین اقتصادی حملات باج‌افزاری و ارزیابی تاثیر متغیرهای اقتصادی بر خسارات ناشی از آن‌هاست. نتایج رویکرد میدانی نشان داد رابطه میان سود گروه مهاجم و خسارات ناشی از حمله، غیرخطی و دارای بیشینه و کمینه‌هایی محلی بوده و هرگونه اقدام متقابل در پاسخ به این حملات باید با دقت کافی در عواقب آن از منظر اقتصادی صورت گیرد؛ به بیان روشن‌تر، اگرچه تابع خسارت ناشی از باج‌افزار، نسبت به مبلغ باج کاملا صعودی است؛ اما، تابع سود مهاجم، رفتاری غیریک‌نوا داشته و به این ترتیب، به ازای هر میزان سود، ممکن است، مهاجم با مطالبه مبالغ متفاوتی از باج به هدف خود برسد. بدین ترتیب، نشان داده شده است که عدم اتخاذ سیاست‌های کلان که ممکن است مهاجم را به سمت مطالبه مبالغ باج خسارت‌بارتر سوق دهد، از حساسیت تصمیم‌گیری بیش‌تر و پیامدهای مهم‌تری برخوردار خواهد بود.

طبقه‌بندی JEL: E42, E41, C51

واژگان کلیدی: باج‌افزار، حمله سایبری، ارز رمزپایه، مدل‌سازی اقتصادی، ساز و کار اقتصادی.

[*] استادیار گروه مهندسی کامپیوتر، دانشگاه بجنورد، بجنورد، ایران (نویسنده مسئول)، پست الکترونیکی: m.garme@ub.ac.ir

[**] کارشناس فناوری اطلاعات، بجنورد، ایران، پست الکترونیکی: srahimi386@gmail.com

۱. مقدمه

حملات سایبری و گروه‌های تبهکار در فضای تبادل اطلاعات سابقه‌ای طولانی دارند؛ اما در سال‌های اخیر با رشد و توسعه فناوری‌های مرتبط با حوزه رمزنگاری و توسعه آن به تبادلات امن مالی و ارتباطات غیرقابل پیگرد در شبکه، بدافزارهایی که از آنها به عنوان باج‌افزار یاد می‌کنیم، متولد شدند. «باج‌افزار[1]» اصطلاحی کلی برای توصیف نوعی بدافزار است که برای باج‌گیری دیجیتالی از قربانیان و مجبور کردن ایشان به پرداخت مبلغ مشخصی پول و به ندرت انجام کاری ناخواسته، طراحی شده‌است (گازت[2]، ۲۰۱۰).

به طور کلی، این شکل از باج‌گیری دیجیتال را می‌توان به دو گروه تقسیم کرد؛ نوع اصلی باج‌افزارها شامل گروهی از بدافزارهاست که فایل‌ها 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 می‌کند یا کاربران را از دسترسی به سیستم‌های خود باز می‌دارند (لیسکا و گالو، ۱۳۹۶).

روش انتقال ارزش و پرداخت باج که امروزه اکثر باج‌گیرهای دیجیتالی درخواست می‌کنند، مبتنی بر استفاده از پول رمزپایه است و معمولا بیت کوین به این منظور به کار می‌رود. البته شایان ذکر است که این تنها روش درخواست پول نیست و هر روش انتقال ارزش که هویت دریافت‌کننده را مخفی نگاه دارد، در این حملات می‌تواند به کار گرفته شود (همان).

برخلاف گذشته، باج‌افزارهای امروزی دیگر متکی بر روش‌های رمزنگاری قابل شکست نیستند. در گذشته، در حملات باج‌افزاری برای رمزگذاری از روش کلید متقارن استفاده می‌شد و متخصصان فرصت دست پیدا کردن به کلید و شکست دادن مهاجم را می‌یافتند (لو و لیائو[3]، ۲۰۰۷).

برخی از باج‌افزارها، پس از رمزدار کردن فایل‌ها، نسخه فایل رمزدار نشده را به طور معمول و قابل بازگشت، پاک می‌کردند؛ اما، امروزه دیگر تقریبا تمام باج‌افزارها از روش‌های پیشرفته رمزنگاری نامتقارن و ترکیبی استفاده می‌کنند و هیچ ردپایی از اطلاعات رمزدار نشده یا برجای گذاشتن کلید رمز باقی نمی‌گذارند (لیسکا و همکاران، ۱۳۹۶).

---

[1] Ransomware
[2] Gazet
[3] Luo & Liao

رشد و توسعه این خانواده از بدافزارها و موفقیت مهاجمان در استخراج منابع مالی چشم‌گیر از این حوزه، سبب شده تا امواج جدیدی از انواع حملات باج‌افزاری را شاهد باشیم (خراز، ارشد، مولینر، روبرتسون و کردا[1]، ۲۰۱۶).

روند نامیمون دیگری که در سایه حملات باج‌افزاری مشاهده می‌شود، انجام حملات با نیت‌های غیرباج‌خواهانه در پوشش حملات باج‌افزاری است. شاهدهایی از این موضوع، باج‌افزارهای واناکرای و پتیای جدید هستند که در سال‌های اخیر سبب ایجاد خساراتی گسترده شده و در واقع، حملاتی با نیت‌های سیاسی در پوشش باج‌افزار هستند (لازکا، فرهنگ و گراسکلگس[2]، ۲۰۱۷).

دلیل این که حملاتی با سایر مقصودها در پوشش حملات باج‌افزاری پنهان می‌شوند، ذات و ماهیت حملات باج‌افزاری است که با اتکا به رمزنگاری، تعقیب و تشخیص مبدا و منشاء حملات را ناممکن یا حداقل دشوار می‌کند. مشاهده روند فزاینده انجام حملات موفق، این نگرانی را تقویت می‌کند که در آینده شاهد حملاتی بسیار گسترده و خسارت‌بار در سطح جهان باشیم (آی‌بی‌ام[3]، ۲۰۱۶).

برای موفقیت یک حمله باج‌افزاری نیاز است تا شرایطی به شرح زیر به صورت هم‌زمان رخ دهند: ارزشمندی داده‌ها یا سرویس‌ها، وجود و امکان استفاده از روش‌های 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.

طبیعی است که برای به شکست کشاندن حمله، کافی است تا حداقل یکی از این شرایط نقض گردد (مثلا، امکان انتقال ناشناس ارزش). از آنجا که اخیرا در رسانه‌ها و حتی مجامع فنی، بحث‌هایی در مورد ایجاد منع قانونی در تبادل ارزهای رمزپایه در سطح کشورهای مختلف صورت گرفته است (کتابخانه حقوقی کنگره[4]، ۲۰۱۸) این نوشتار برآن است تا با تکیه بر تجارب و داده‌های حاصل از فرآیندهای امدادی در مقابله با حملات باج‌افزاری، به

[1] Kharraz, Arshad, Mulliner, Robertson & Kirda
[2] Laszka, Farhang & Grossklags
[3] IBM
[4] The Law Library of Congress

مدل‌سازی اقتصادی انواع حملات باج‌افزاری بپردازد و از این طریق بتواند مسیر مقابله با این حملات از منظر مدیریت بازار رمز ارزها را روشن نماید. در این مسیر، در وهله نخست، مختصری از تاریخچه موضوع ارایه شده است. پس از آن با بررسی و دسته‌بندی گام‌های این حملات، به معرفی مدل اقتصادی حملات باج‌افزاری پرداخته شده است. در ادامه با تکیه بر اطلاعات به دست آمده در فرایندهای امدادی و آموزشی، مدل‌های معرفی شده به کار گرفته شده‌اند. پس از این مرحله، نتایج به دست آمده تحلیل شده‌اند و دست‌آوردهای عملی پژوهش معرفی شده‌اند. در انتها با ارایه خلاصه‌ای از پژوهش، به جمع‌بندی و ترسیم مسیر آینده این مطالعه پرداخته شده است.

۲. مروری بر ادبیات

از لحاظ تاریخی، تولد مفهوم باج‌افزار به تولد قطعه کدی مخرب به نام AIDS برمی‌گردد که در سال ۱۹۸۹ توسط جوزف پاپ نوشته شد. با بررسی‌های بیش‌تر این بدافزار توسط متخصصان امنیت، آشکار شد که در سیستم‌های آلوده، صرفا نام فایل‌ها با استفاده از رمزگذاری با کلید متقارن تغییر یافته است که سرانجام، با مساعی متخصصان، الگوریتم ناقص رمزنگاری و آلودگی ایجاد شده، شکسته و محو شد (لیسکا و همکاران، ۱۳۹۶).

با شکست این حمله و عدم دست‌یابی به منابع حاصل از آن (که بر فرض محدودیت فنی و تکنولوژیکی تاکید داشت) تا سال ۲۰۰۵ اثری از این حملات نبود. در دسترس قرار گرفتن روش‌های رمزگذاری پیچیده‌تر به همراه افزایش قدرت محاسباتی سیستم‌ها، امکانات لازم را برای استفاده از باج‌افزارها توسط مهاجمان ایجاد کرد و سبب رشد فزاینده آن‌ها گردید (لیائو، ژائو، دوپه و آن[1]، ۲۰۱۶). در سال ۲۰۱۶ باج‌افزارها با تکیه بر حداقل آسیب‌پذیری‌ها و کم‌ترین ارتباط با هدف، به عنوان یکی از متداول‌ترین روش‌های حمله به سیستم‌های کامپیوتری مطرح شدند (لازکا و همکاران، ۲۰۱۷).

[1] Liao, Zhao, Doup´e & Ahn

یکی از شناخته شده‌ترین نمونه باج‌افزارها، کریپتووال[1] می‌باشد. این باج‌افزار در حال حاضر منسوخ شده است؛ اما، بنابر گزارش‌ها، تا اواسط ژوئن ۲۰۱۵ به طور برآوردی، درآمدی در حدود ۱۸ میلیون دلار در برداشته است (لیسکا و همکاران، ۱۳۹٦).

باج‌افزارهای واناکرای (ویکی‌پدیا[2]، ۲۰۱۷) و پتیای جدید (فایی[3]، ۲۰۱۸) در سال‌های اخیر، آسیب‌هایی جدی و خساراتی شدید در سطح جهان ایجاد کردند و حتی سبب به خطر افتادن جان انسان‌ها، وقفه در خدماتِ درمانی، خسارت‌های اقتصادی هنگفت، قطع خدمات عمومی انرژی و حمل و نقل و بحران‌های غیرقابل پیش‌بینی شده و موجب افزایش سطح نگرانی‌ها از امنیت دنیای سایبری شده‌اند. البته این دو باج‌افزار برخلاف سایر باج‌افزارها به نظر می‌رسد که با نیت‌هایی غیر از باج‌خواهی طراحی و منتشر شده باشند. هم‌چنین، میزان پیچیدگی این دو، بیش‌تر از توان فنی بدافزارنویسان معمولی به نظر می‌رسد (لازکا و همکاران، ۲۰۱۷).

تصور رایج در مورد صنعت باج‌افزار، آن را صنعتی بسیار سودآور با هزینه نزدیک به صفر و قابل اغماض می‌دانند که می‌تواند برای دنیای فناوری اطلاعات بسیار خطرناک باشد (لیسکا و همکاران، ۱۳۹٦). هم‌چنین، در برخی منابع، سودآوری زیاد این حملات را دلیل رشد سرسام‌آور این حملات معرفی می‌کنند (لازکا و همکاران، ۲۰۱۷).

هزینه یک حمله باج‌افزاری می‌تواند در مقایسه با درآمدهای ناشی از آن بسیار ناچیز باشد؛ زیرا برای انجام حمله از چند روش مختلف استفاده می‌شود که در تمامی آنها هزینه حمله در عمل بسیار اندک بوده و منجر به ایجاد درآمدهای زیاد می‌شود (خراز، روبرتسون، بالزاروتی، بلج و کردا[4]، ۲۰۱۵).

در روش استفاده از هرزنامه برای توزیع باج‌افزار، با هزینه کم‌تر از چند دلار، مهاجمان می‌توانند میلیون‌ها پیام فریبنده و آلوده بفرستند و کافی است که فقط حتی یک درصد از افراد این ایمیل‌های آلوده را دریافت و فایل مخرب پیوست را اجرا کنند تا مهاجم به درآمد چندین هزار دلاری برسد. در روش آلوده کردن وب‌سایت‌های قانونی به بدافزار منتشرکننده باج‌افزار، انتشار باج‌افزار با اتکا بر زیرساخت وب‌سایت‌های پرمخاطب که مورد نفوذ مهاجمان قرار

[1] CrytpoWall
[2] Wikipedia
[3] Fayi
[4] Kharraz, Robertson, Balzarotti, Bilge & Kirda

گرفته‌اند، انجام می‌گیرد و می‌توان اطمینان داشت که در عمل، مهاجمان هزینه‌ای مستقیم برای به دست آوردن سود ناشی از حمله متحمل نمی‌شوند. در مورد حملات متکی بر توزیع خودکار از طریق آسیب‌پذیری سیستم عامل، مثل واناکرای، مهاجم عملا هیچ هزینه‌ای برای توزیع باج‌افزار نمی‌پردازند؛ با اتکا بر روش انتشار کرم‌گونه، توزیع بدافزار توسط رایانه‌هایی که مورد تسخیر و آلودگی قرار گرفته‌اند، انجام می‌پذیرد (لیسکا و همکاران، ۱۳۹۶).

در این پژوهش، برای مدل‌سازی خسارات و تهدیدهای ناشی از حملات باج‌افزاری، از نظریه «طراحی ساز و کارهای اقتصادی[1]» استفاده شده است (هورویکز و ریتر[2]، ۲۰۰۶). به بیان دقیق‌تر، با تطبیق دادن شرایط مساله با ساز و کارهای شناخته شده، به ارایه مدل اقتصادی حملات پرداخته شده است (گوروسوامی و همکاران[3]، ۲۰۰۵). کاربرد این نظریه، طیف کاملی از مسایل از اقتصاد خرد تا اقتصاد کلان را شامل می‌شود و مثال‌های فراوانی از این کاربردها در منابع علمی گزارش شده است (ویکی‌پدیا، ۲۰۱۹).

با توجه به ساختار و شرایط حملات باج‌افزاری، مهاجم با تعیین و بهینه‌سازی میزان باج مطالبه شده به دنبال بیشینه کردن درآمد و سود خود می‌باشد (هرناندز کاسترو، کارترایت و کارترایت[4]، ۲۰۲۰). بر اساس سوابق، در حملات باج‌افزاری معمولا مهاجمان برای انجام این نوع از نفوذ، هزینه‌های قابل توجهی متحمل نمی‌شوند (هرناندز کاسترو و همکاران، ۲۰۲۰). به این ترتیب، می‌توان سمت هزینه در تابع سود مهاجم را به طور تقریبی، صفر دانست.

در مراجع، به عنوان ساز و کارهای بیشینه‌کننده سود، به دو گروه از حراج‌ها اشاره می‌شود. گروه اول از حراج‌های بیشینه‌کننده سود[5]، بر اطلاعات و دانش پیشین از میزان ارزش اطلاعات تکیه نمی‌کند[6]؛ بلکه طرف فروشنده (مهاجم) در یک ساز و کار راستگو[1] از خریداران

---

[1] Mechanism Design Theory: در اقتصاد و تئوری بازی‌ها، طراحی ساز و کار یا طراحی مکانیسم، مطالعه طراحی قواعد یک بازی یا سیستم است. لئونید هورویچ (اقتصاددان و ریاضیدان لهستانی یا لهستانی – آمریکایی) را مبدع این نظریه دانسته‌اند. وی (به دلیل ابداع این نظریه) به همراه دو هم وطن دیگر خود به نام‌های اریک مسکین و راجر مایرسون (به دلیل کاربردی کردن این نظریه) جایزه نوبل اقتصاد را در سال ۲۰۰۷ از آنِ خود کردند. بنیان نظریه طراحی مکانیسم، عینی‌تر و دقیق‌تر کردن اطلاعات کنشگران اقتصادی از بازار است.

[2] Hurwicz & Reiter
[3] Guruswami et al.
[4] Hernandez-Castro, Cartwright and Cartwright
[5] Profit-Maximizing Auctions
[6] Without a Priori

(قربانیان) می‌خواهد که برای دریافت خدمت یا محصول (بازگشایی اطلاعات) قیمتی را پیشنهاد دهند (گوروسوامی و همکاران، ۲۰۰۵). پس از آن با انجام یک بهینه‌سازی ساده، قیمت بهینه و بیشینه‌کننده سود تعیین می‌شود.

اما، به طور طبیعی و با توجه به ساختار حمله باج‌افزاری که در آن، مهاجم بدون سوال از قربانی، قیمت باج را تعیین می‌نماید، می‌توان این رویکرد را با مکانیسم حراج نخستین در تضاد دانست.

رویکرد دیگر که «روش مبتنی بر اطلاعات پیشین» نام دارد؛ با توجه به ساختار اقتصادی موضوع، منطبق با مکانیسم حراج یاد شده است. از میان ساز و کارهای بیشینه‌کننده سود، آن دسته که در آنها، هزینه تولید یا ارایه خدمات، قابل اغماض می‌باشد، در گروه حراج‌های بیشینه‌کننده سود محصولات و خدمات دیجیتال[۲] دسته‌بندی می‌شوند (گلدبرگ و هارتلاین[۳]، ۲۰۰۳). در مراجع برای تعیین قیمت بهینه در این ساز و کارها، اثبات شده است که می‌توان بر روش «میرسون[٤]» تحت شرایط مزایده محصولات دیجیتال تکیه نمود (نوام، رافگاردن و تاردوس[٥]، ۲۰۰۷).

در این پژوهش، با مدل‌سازی ریاضیات حاکم بر اقتصاد مساله پیشِ رو و با اتکا بر سازوکارهای بیشینه‌کننده سود در بازار محصولات دیجیتال و نیز با ارزیابی مدل‌های ارایه شده با اتکا بر داده‌های حاصل از پژوهش‌های میدانی، تاثیر اعمال ممنوعیت در انتقال و تبادل ارزهای رمزپایه، مورد بررسی قرار گرفته و نشان داده شده است که اگرچه یک پیش‌نیاز اساسی در موفقیت حملات باج‌افزاری، وجود راهی برای تبادل ناشناس ارزش می‌باشد؛ اما این سیاست می‌تواند در شرایطی برعکس عمل کند و سبب افزایش خسارت کلی حمله و دیگر عواقب نامطلوب شود. نوآوری این پژوهش این است که تاکنون هیچ مطالعه مستندی در این حوزه، در ایران، به انجام نرسیده است.

---

[1] Truthful
[2] Profit-Maximizing Auctions for Digital Goods
[3] Goldberg & Hartline
[4] Myerson
[5] Noam, Roughgarden & Tardos

۳. روش پژوهش

در این پژوهش برای مدل‌سازی یک حمله باج‌افزاری (مانند RWA) از متغیرهای جدول (۱) استفاده شده است. در یک حمله باج‌افزاری، مهاجم یا گروه تبهکار سایبری، با روشی مثل ارسال هرزنامه حاوی پیوست یا پیوند مخرب، آلوده کردن وب‌سایت‌های پر مراجعه به کد مهاجم، انتشار کدهای دارای توان نفوذ با اتکا بر نقاط ضعف قبلا شناخته شده سیستم‌عامل‌ها و نرم‌افزارها، گروهی مانند THR از رایانه‌ها را در معرض حمله قرار می‌دهد. زیرمجموعه‌ای از THR چون EDG به دلیل کاستی خود یا کاربران در پیشگیری از حمله، در معرض خطر قرار می‌گیرند و زیرمجموعه‌ای چون DMG از آنها، با موفقیت نفوذ، آسیب می‌بینند و فایل‌های موجود در آنها رمزگذاری شده و از مالکان آنها باج مطالبه می‌شود.

از مجموعه DMG زیرمجموعه‌ای چون VCM از سامانه‌هایی که در آنها تمامی شرایط موفقیت حمله باج‌افزاری برقرار است، از جمله ارزش‌مندی خدمات و اطلاعات و در اختیار نداشتن نسخ پشتیبان یا طرح جامع بازگشت از تخریب، خود را در شرایطی خواهند یافت که مجبورند بین دو گزینه پرداخت باج و احتمالا، بازپس گرفتن دارایی‌های الکترونیکی خود یا رد کردن تقاضای پرداخت باج و تحمل کردن خسارات ناشی از حمله، دست به انتخاب بزنند. این دو مجموعه با نمادهای RPV و LDV نشان داده شده‌اند. مهاجم(ها) از هریک از قربانیان حمله یعنی $v\epsilon VCM$ عددی چون r_v را به عنوان باج مطالبه می‌کنند.

جدول ۱. متغیرهای استفاده شده در مدل‌سازی اقتصادی حملات باج‌افزاری

متغیر	مفهوم
RWA	یک حمله باج‌افزاری (RansomWare Attack)
THR	مجموعه رایانه‌های در معرض تهدید قرار گرفته در حمله (THReatened)
EDG	مجموعه رایانه‌های مورد نفوذ قرار گرفته در حمله (EnDanGered).
DMG	مجموعه رایانه‌های آسیب دیده از حمله (DaMaGed)
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 از قربانی v در حمله
r	میزان باج مطالبه شده از قربانیان حمله (Ransom)
SEV_v	میزان ارزش دارایی‌های به گروگان گرفته شده از سوی مهاجم که توسط قربانی فرضی تخمین زده می‌شود.
CEV_v	میزان ارزش دارایی‌های به گروگان گرفته شده از سوی مهاجم که با پردازش اطلاعات ارایه شده از سوی قربانی فرضی محاسبه می‌شود.
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)
TDG_{RWA}	خسارت کل تحمیل شده به اعضای مجموعه DMG در حمله RWA (Total DamaGe)
TLD_{RWA}	خسارت تحمیل شده به اعضای مجموعه VCM در حمله RWA که باج را نپرداختند. (Total Loss Damage)
TVS_{RWA}	کل خسارت ایجاد شده در اثر خرابکاری ناشی از حمله RWA (Total Value of Sabotage)

منبع: گردآوری محقق

در یک حمله باج‌افزاری، تعداد قربانیان معمولا بیش از آن است که مهاجم فرصت لازم برای کسب شناخت از زیرساخت‌های آنها را داشته باشد؛ بنابراین، مهاجم نمی‌تواند میزان بهینه باج بر اساس ارزش دارایی‌های به گروگان گرفته شده را تعیین کند. هم‌چنین، مهاجم معمولا به منظور حداقل کردن احتمال شناسایی و تعقیب قضایی، تمایل چندانی به برقراری ارتباط خارج از چارچوب حمله یا حتی مذاکره با قربانی بر سر موضوع تعیین میزان باج ندارد؛ از این‌رو، معمولا عدد یکسان و ثابتی به عنوان مبلغ باج درخواستی، برای تمام قربانیان تعیین و

مطالبه می‌شود. برای این موضوع اگرچه، به ندرت، مثال‌های نقض یافت می‌شود؛ اما، در محاسبات می‌توان موارد نقض را برای رسیدن به یک مدل قابل اتکا نادیده گرفت.

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.

$$RPV = \{v \in VCM | SEV_v \geq r\} \quad (۱)$$

بنابراین؛

$$LDV = VCM - RPV \quad (۲)$$

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.

نکته کلیدی که در فرایندهای امدادی مشاهده می‌شود؛ این است که الزاما، قیمت مورد تصور قربانیان برای ارزش اطلاعات و تنظیمات سامانه‌ها، مساوی با ارزش واقعی این دارایی‌ها نمی‌باشد؛ به بیان دیگر، می‌توان نمونه‌هایی را مشاهده کرد که قربانیان با وجود آن که خسارات وارد شده به ایشان بیش از مبلغ باج مطالبه شده است؛ اما، درخواست پرداخت باج را نپذیرفته و متحمل خساراتی درشت‌تر از باج مطالبه شده می‌شوند. این مشاهده می‌تواند در اثر این واقعیت رخ دهد که پس از وقوع حمله، دیگر برای بسیاری از قربانیان، امکان تعیین قیمت واقعی آنچه که از دسترس خارج شده است، وجود ندارد. این مقدار برای هر قربانی مفروض با متغیر CEV_v نشان داده شده است. بنابراین، کل خسارت وارده در حمله RWA برابر با مجموع ارزش واقعی پذیرفتن آسیب یا پرداخت باج به ازای تمامی رایانه‌های آسیب دیده از حمله (DMG) می‌باشد که با نماد TDG_{RWA} نشان داده می‌شود.

در تعیین r، مهاجم به دنبال بیشینه کردن سود خود می‌باشد. بر اساس سوابق، در حملات باج‌افزاری معمولا برای به دست آوردن راه نفوذ به سامانه قربانی از روش‌های نو در نفوذ یا به

عبارتی، آسیب‌پذیری‌های روز صفر که تهیه آن‌ها هزینه‌های قابل توجه دربر دارد، استفاده نمی‌شود (لیسکا و همکاران، ۱۳۹۶)؛ بلکه از آسیب‌پذیری‌های شناخته شده که برای آن‌ها روش‌های پیشگیری مناسب و به‌روزرسانی موثر 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. معمولا، رمزگذاری اطلاعات با اتکا بر توابع شناخته شده رمزنگاری موجود در سامانه قربانی انجام می‌شود. در پردازش رمزکردن اطلاعات از سخت‌افزار قربانی و در صورت نیاز، در تبادل اطلاعات با سرورهای فرماندهی، از پهنای باند سامانه قربانی سوء استفاده می‌شود. به این ترتیب، می‌توان سمت هزینه در تابع سود مهاجم را به طور تقریبی، 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؛

$$PRF_{RWA} = RVN_{RWA} - CST_{RWA} \quad (۳)$$
$$and\ CST_{RWA_a} \simeq 0$$
$$\rightarrow PRF_{RWA} \simeq RVN_{RWA}$$

همان طور که در مورد ساز و کارهای بیشینه‌کننده سود به حراج‌ها اشاره شد؛ در رویکرد نخست، مهاجم، خود را بی‌نیاز از میزان ارزش اطلاعات می‌بیند و در رویکرد دوم، مهاجم بر روش مبتنی بر اطلاعات پیشین تکیه می‌کند. در رویکرد دوم، برای تعیین قیمت بهینه در این سازوکارها، از روش Myerson تحت شرایط مزایده محصولات دیجیتال استفاده می‌شود؛

$$\phi(r) = r - \frac{1-CDF(r)}{pdf(r)} \rightarrow Opt(r) = \phi^{-1}(0) \quad (٤)$$

که در رابطه (٤)، 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 متغیرr هستند. در نتیجه، بر اساس مطالعه نوام و همکارن (۲۰۰۷) با یافتن نقطه صفر در معکوس تابع «میرسون» که با $\phi^{-1}(0)$ نشان داده شده، می‌توان به مقدار بهینه r در این مزایده دست یافت.

روشن است که در این مدل، مهاجم نیاز به دانستن توزیع آماری ارزش اطلاعات برای کاربران دارد. دست یافتن به این توزیع آماری، امری چالش‌برانگیز بوده و بعید به نظر می‌رسد که مهاجم بتواند منابع فنی و زمانی مورد نیاز برای رسیدن به این دانش را به دست بیاورد؛ در عوض، بر اساس مشاهدات می‌توان گفت که مهاجمان با تکیه بر تجارب گذشته و سعی و خطا در تغییر دادن مقدار باج در حملات متوالی به دنبال بیشینه کردن سود (درآمد) خود خواهد بود.

با تعیین و مشخص شدن مقدار باج r، آن دسته از قربانیان که در مجموعه RPV قرار می‌گیرند، در مجموع به اندازه رابطه (۵) به مهاجم می‌پردازند و احتمالا اطلاعات به گروگان گرفته شده خود را باز پس می‌گیرند. رابطه (۵) عبارت است از:

$$\mathrm{PRF_{RWA}} \simeq \mathrm{RVN_{RWA}} = \mathrm{r}.|\mathrm{RPV}| \qquad (۵)$$

اعضای مجموعه LDV نیز به اندازه رابطه (٦) متحمل خسارت می‌شوند. رابطه (٦) در زیر آورده شده است.

$$\mathrm{TLD_{RWA}} = \sum_{\mathrm{v}\in\mathrm{LDV}} \mathrm{CEV_v} \qquad (٦)$$

در رابطه (٦)، $\mathrm{TLD_{RWA}}$ 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 یک‌سو، موفق به دریافت مبلغ $\mathrm{RVN_{RWA}}$ از قربانیان و ایجاد سود تقریبا 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؛ علاوه بر مجموع باج دریافت شده، در سطح اقتصاد کلان خواهد شد که در رابطه (۷) با $\mathrm{TVS_{RWA}}$ نشان داده شده است.

$$\mathrm{TVS_{RWA}} = \mathrm{RVN_{RWA}} + \mathrm{TDG_{RWA}} - \sum_{\mathrm{v}\in\mathrm{RPV}} \mathrm{CEV_v} \qquad (۷)$$

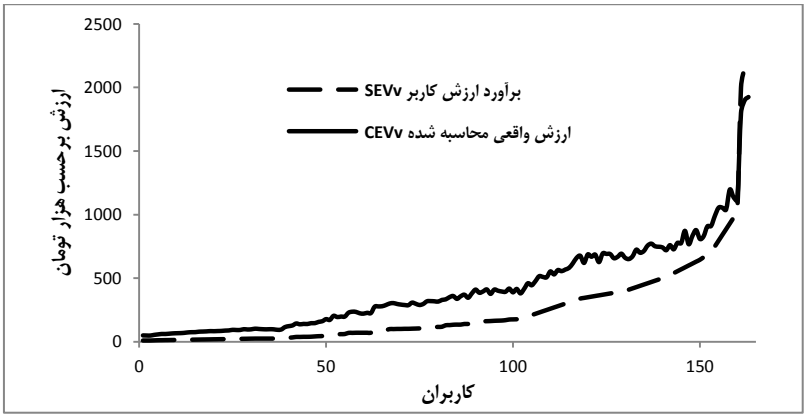
٤. برآورد مدل و تجزیه و تحلیل آن

برای تعمق بیش‌تر در موضوع و بررسی رفتاری این توابع از یک مجموعه داده‌های واقعی استفاده شده است. به منظور به دست آوردن ارزش اطلاعات کاربران، از دو روش مستقل استفاده شده و دو مجموعه داده‌های واقعی با تعداد ١٦٣ زوج نمونه قابل استفاده از داده‌ها ایجاد شده است. این داده‌ها با همکاری ١٦٣ تن از شرکت‌کنندگان در کارگاه‌های آموزشی مقابله با باج‌افزارها به دست آمده است. در مجموعه اول از داده‌ها، هر مخاطب همکاری‌کننده در طرح، خود به اظهار ارزش اطلاعات و هزینه زحمت نصب نرم‌افزارها و انجام تنظیمات موجود روی سامانه خود پرداخته است. در مجموعه دوم از اطلاعات، هر یک از ١٦٣ تن از شرکت‌کنندگان، به ارایه جزییات ابزارها، سیستم عامل و فایل‌های موجود روی سامانه خود پرداخته‌اند. این جزییات شامل تعداد، اندازه میانگین و شیوه به‌دست آوردن (دانلود، ایجاد، کپی و ...) هر یک از انواع محدود فایل‌هایی است که روی سامانه قربانی فرضی موجود می‌باشد و معمولا، هدف باج‌افزارها هستند (از قبیل PDF، اسناد Office، تصاویر، ویدیوها، فایل‌های پایگاه‌داده و ...).

هم‌چنین، از هر یک از مخاطبان اطلاعات تنظیمات نرم‌افزارها و سیستم عامل نیز مورد پرسش قرار گرفته است. نتایج این دو مطالعه به عنوان ورودی مدل استفاده شده و در شکل (١) نشان داده شده است. از آنجا که نشان دادن تعداد قابل توجه از اعداد جز به صورت نموداری، ملموس نخواهد بود، با مرتب کردن داده‌های زوج‌های مرتب بر اساس ارزش اظهار شده، نمودار مشخص شده در شکل (١) ترسیم شده است. طبیعی است که روند صعودی ناشی از مرتب‌سازی بوده و مفهوم دیگری را جز الگوی پراکندگی و روند تعییرات ارزش، منتقل نمی‌کند.

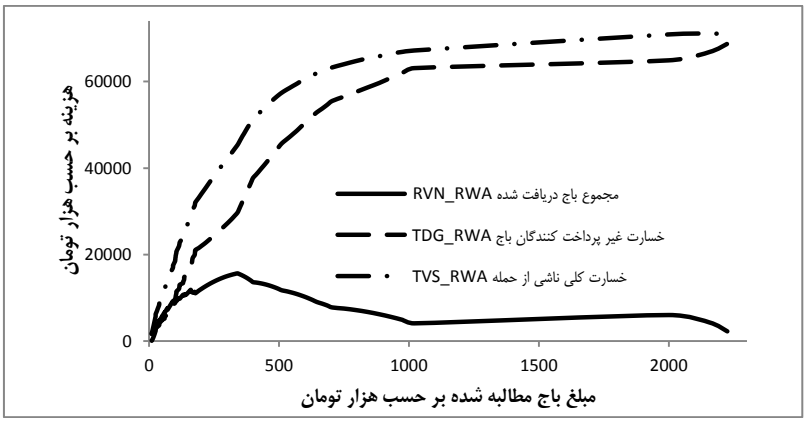
در خصوص این دو منحنی می‌توان گفت که نمودار اول (بدون خط چین)، نشان‌دهنده ارزش‌گذاری شخصی افراد برای اطلاعات خود بوده که در کمال تعجب همواره کم‌تر از نمودار دوم (خط چین) که نشان‌دهنده تخمین واقعی از ارزش اطلاعات ایشان است، می‌باشد. اگر چه بین این دو نمودار شباهت‌های قابل توجه وجود دارد؛ اما، منحنی اول معیار تصمیم‌گیری کاربران و منحنی دوم، واقعیت اقتصادی برای خسارات ناشی از تلف شدن اطلاعات و تنظیمات سامانه‌های قربانی را منعکس می‌کند.

شکل ۱. نمودارهای ارزش برآورد شده اطلاعات و تنظیمات سامانه قربانی توسط کاربر و تخمین واقع‌گرایانه آن در مطالعه



منبع: یافته‌های پژوهش

شکل ۲. نمودارهای میزان سود مهاجم، خسارات وارد شده به قربانیان غیرپرداخت‌کننده باج و مجموع خسارت ناشی از حمله



منبع: یافته‌های پژوهش

همان طور که در نمودار ارایه شده در شکل (۲) دیده می‌شود، در این بررسی برای مهاجم میزان باج مطالبه شده تقریبا برابر با ۳٤۰ هزار تومان مطلوب است. گفتنی است که این مبلغ مربوط به ٦ ماهه منتهی به اسفند ۹٦ می‌باشد و مهم‌ترین دلیل تاخیر در ارایه این پژوهش

رعایت ملاحظات امنیتی و اطمینان یافتن از عدم افشای اطلاعات حساس در مورد ارزش دارایی‌های مخاطبان است. نکته کلیدی آن جاست که اگر چه میزان باج مطالبه شده کاملا به مجموعه آماری تحت مطالعه وابسته است؛ اما، این مقدار از باج مطالبه شده با مشاهدات در روندهای ارایه امداد نیز هم‌خوانی دارد. توجه بیش‌تر به نمودار نشان می‌دهد که همان طور که انتظار می‌رود، تابع خسارت کلی حمله، یک تابع اکیدا صعودی بر حسب باج مطالبه شده است. تابع خسارت مربوط به افرادی که قطعا اطلاعات خود را از دست می‌دهند، نیز نسبت به میزان باج مطالبه شده، صعودی است.

یک نکته قابل توجه دیگر، مربوط به در خصوص میزان سود خالص مهاجم مشاهده می‌شود. بر اساس شکل (۲) رفتار این تابع الزاما یکنوا نبوده و دارای بیش از یک ماکزیمم محلی است. به دلیل وجود چند ماکزیمم محلی در تابع سود مهاجم، توجه به شیوه مهاجم برای میل دادن این میزان به سمت نقطه بهینه سود، اهمیت دارد. پر واضح است که انگیزه پنهان نگه داشتن هویت مهاجم، ایشان را از انجام مطالبه روی گروه‌های قربانیان احتمالی باز می‌دارد. بنابراین می‌توان نتیجه گرفت که در عمل مجریان حملات باج‌افزاری از روش تجربی برای بیشینه کردن سود خود استفاده می‌کنند.

۵. تحلیل و مدل‌سازی مداخله اقتصادی

برای مقابله با حملات باج‌افزاری رویکردهای مختلفی را می‌توان در پیش گرفت. مهم‌ترین رویکرد کلان در مقابل این حملات می‌تواند پایش و ممنوعیت گسترده زیرساخت‌های اقتصادی انتقال ناشناس ارزش چون ارزهای رمزپایه مثل بیت‌کوین[1] یا کوپن‌های پیش‌پرداخت چون وب‌مانی[2] باشد. در صورتی که این زیرساخت‌های انتقال ارزش در دسترس مهاجمان و قربانیان نباشند، بدیهی است که در کل، بازاری برای حملات باج‌افزاری شکل نخواهد گرفت.

اما، در صورت وجود و در دسترس بودن این ابزارهای انتقال ارزش و در عین حال در صورت آغاز مداخله مانند ایجاد منع قانونی در دسترسی قربانیان احتمالی به ابزارهای پرداخت و تبادل ارزهای رمزپایه، به طور طبیعی تمایل کاربران برای پرداخت باج کاهش می‌یابد. بدیهی

[1] Bitcoin
[2] Webmoney

است که با ممنوع کردن هر بازاری قیمت تمام شده خریدار در آن بازار رشد خواهد کرد؛ زیرا فروشنده افزون بر قیمت محصول یا خدمت، هزینه ریسک برخورد پلیس یا مراجع قانونی با معامله موضوع ممنوع را نیز روی قیمت تمام شده اضافه خواهد کرد. این مساله سبب می‌شود نمودار برآورد ارزش قربانیان، از نمودار ارزش واقعی اطلاعات ایشان فاصله بیش‌تری بگیرد و به طور قابل توجهی کم‌تر از آن شود. نتیجه این رخداد با توجه به ساختار غیرخطی مساله می‌تواند به مثابه افزایش مجازی مبلغ باج مطالبه شده باشد. به بیان دیگر، این رویکرد سبب می‌شود خروجی مساله به سمت شرایطی شبیه به ثابت ماندن نمودار خسارت کاربران غیرپرداخت‌کننده باج در شکل (۲) و حرکت نمودار درآمد مهاجم به سمت راست، میل کند. اگرچه این یک حالت جدید و پاسخی جدید برای مساله خواهد بود؛ اما بدیهی است که در این حالت، به دلیل افزایش نسبت کاربرانی که تمایل یا امکان پرداخت باج را نداشته و اطلاعات خود را از دست داده‌اند، میزان مجموع خسارت ایجاد شده افزایش می‌یابد.

برای ایجاد درک عمیق‌تر از موضوع با در نظر گرفتن r به عنوان میزان باج مطالبه شده، در شکل (۳) پارامترهای اقتصادی ناشی از یک حمله باج‌افزاری به شکل سطح زیر نمودارها ترسیم شده است.

در صورت انجام مداخله‌های پیشگیرانه در تبدیل و انتقال ارزش از قربانی به مهاجم به شکل ارزهای رمزپایه یا غیرقابل پیگرد، دو پدیده کلی در روند پرداخت رخ خواهند داد.

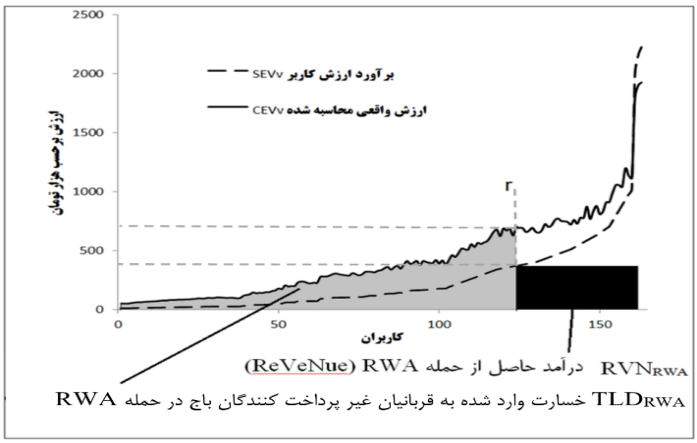
الف: قربانی برای پرداخت هر مقدار از باج مطالبه شده r به شکل ارز ممنوع نیاز به صرف کردن یک هزینه ثابت چون r_0 دارد. این عدد را می‌توان به عنوان هزینه اولیه انجام هر تراکنش دید؛

ب: تبدیل ارز رایج در جغرافیای قربانی به ارز مطالبه شده هزینه‌ای سربار چون α نیز در بر خواهد داشت؛ به بیان ساده‌تر، قربانی به ناچار برای تامین r باید متحمل هزینه‌ای $(1+\alpha)$ برابر r شود.

در اثر اعمال این محدودیت، قربانی در عمل در مواجه شدن با مطالبه مبلغ r بـه شـکل ارز رمزپایه فقط در صورتی پرداخت باج را قبول خواهد کرد که مبلغ هزینـه کلـی پرداخـت بـاج یعنی r' که از ارزش برآورد شده از سوی او برای اطلاعات یعنی SEV_v کمتر باشد. در شکل ٤ می‌توان نتیجه اقتصادی این تغییر را مشاهده نمود.

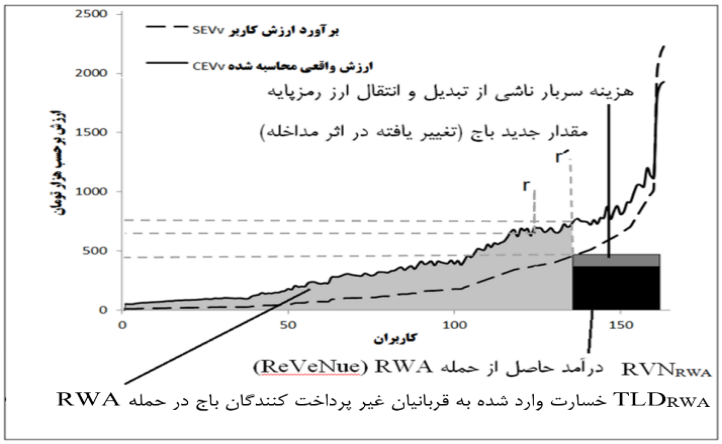
$$r' = (1 + \alpha).r + r_0 \quad (۸)$$

شکل ۳. میزان سود مهاجم، خسارات وارد شده به قربانیان غیرپرداخت‌کننده باج ناشی از حمله



منبع: یافته‌های پژوهش

شکل ٤. میزان سود مهاجم، خسارات وارد شده به قربانیان غیرپرداخت‌کننده باج و هزینه‌های انتقال ارز در حمله



منبع: یافته‌های پژوهش

همان طور که در شکل (٤) در مقایسه با شکل (۳) دیده می‌شود، مساحت مستطیل نشان‌دهنده میزان باج دریافت شده توسط مهاجم در شرایط مساوی، کوچک‌تر شده است و در عوض، با جابه‌جا شدن نقطه افراز مجموعه قربانیان، دو رخداد نامطلوب به وقوع پیوسته است؛

اول اینکه به اندازه مساحت مستطیل هزینه سربار ناشی از تبدیل و انتقال ارز رمزپایه، به بازار زیرزمینی (در اثر ممنوعیت انتقال ارز رمزپایه) ارزش وارد شده است که این موضوع خود می‌تواند مسبب مشکلات بعدی باشد و دوم اینکه به اندازه تفاضل r و r' نقطه افراز مجموعه قربانیان پرداخت‌کننده باج و تحمل‌کننده خسارت از دست رفتن اطلاعات، به سمت خسارت بیش‌تر حرکت کرده است. با توجه به شکل‌های (۳ و ٤) و در نظر گرفتن مجموع مساحت زیر نمودارها می‌توان نتیجه گرفت که اتخاذ این سیاست، مسبب افزایش مجموع خسارات ایجاد شده برای جامعه یعنی TVS_{RWA} نیز شده است.

٦. نتیجه‌گیری

در این پژوهش بیان شد که با مدل‌سازی حملات سنتی باج‌افزاری و با تکیه بر یک مجموعه داده تجربی می‌توان دریافت که در مقابله با حملات باج‌افزاری و بازار پرسود این حملات برای مجرمان سایبری باید دقت فراوان به خرج داد.

اگرچه تابع خسارت ناشی از باج‌افزار، نسبت به مبلغ باج کاملا صعودی است؛ اما، تابع سود مهاجم رفتاری غیریکنوا داشته و به این ترتیب، به ازای هر میزان از سود ممکن است مهاجم با مطالبه مبالغ متفاوتی از باج به هدف خود برسد. هم‌چنین، چگونگی و روش به دست آوردن مبلغ بهینه باج برای مهاجم نیز ارائه شد.

هم‌چنین، بیان شد که ایجاد محدودیت در دسترسی به ارزهای رمزپایه یا دیگر روش‌های ناشناس انتقال ارزش می‌تواند همچون شمشیری دو لبه عمل کند که در صورت مسدودسازی کامل دسترسی به این ارزها، سبب حذف امکان حملات و در صورت اعمال ناقص سیاست‌ها، خسارت‌های کلی بیش‌تری برای مجموعه قربانیان به وجود خواهد آمد.

با توجه به شرایط حاکم بر زیرساخت‌های مرتبط با ارزهای رمزپایه امروزی و ناممکن بودن مسدودسازی کامل این زیرساخت‌ها، این پژوهش می‌تواند برای سیاست‌گذاران اقتصاد کلان نتایج حاصل از اعمال محدودیت‌های انتقال و تبدیل ارز رمزپایه بر بازار زیرزمینی حملات باج‌افزاری را روشن نماید.

منابع

- لیسکا، آلن، گالو، تیموتی (۱۳۹۶). باج‌افزار و روش‌های دفاع در برابر باج‌گیری دیجیتال، ویرایش دوم. ترجمه مهران گرمه‌ء، میلاد حضرتی و سارا رحیمی دوین. گسترش علوم پایه. تهران.
- Fayi, S. Y. A. (2018). What Petya/NotPetya ransomware is and what its remidiations are. In Information Technology-New Generations. *Springer*, Cham: 93-100.
- Gazet, A. (2010). Comparative analysis of various ransom ware vii. *Journal in Computer Virology*, 6(1):77–90.
- Goldberg, A. V., & Hartline, J. D. (2003). Envy-free auctions for digital goods. In Proceedings of the 4th ACM conference on Electronic commerce (pp. 29-35).
- Guruswami, V. (2005).On profit-maximizing envy-free pricing, in sixteenth annual ACM-SIAM symposium on Discrete algorithms Society for Industrial and Applied Mathematics: 1164-1173.
- Hernandez-Castro, J., Cartwright, A., & Cartwright, E. (2020). An economic analysis of ransom ware and its welfare consequences. *Royal Society Opens Science*, 7(3): 190023.
- Hurwicz L. & Reiter, S., (2006). Designing economic mechanisms. New York, US: Cambridge University Press.
- IBM. (2016). Businesses more likely to pay ransom ware than consumers. Industry report. Available at: www-03. ibm. Com/ press/us/ en/ pressrelease/51230.
- Kharraz, A. Arshad, S. Mulliner, C. Robertson, W. & Kirda, E. (2016). UNVEIL: A large-scale, automated approach to detecting ransom ware. In Proceedings of the 25th USENIX Security Symposium (USENIX Security): 757–772.
- Kharraz, A. Robertson, W. Balzarotti, D. Bilge, L. & Kirda, E. (2015). Cutting the gordian knot: A look under the hood of ransomware attacks. In Proceedings of the 12th International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment (DIMVA), *Springer*: 3–24.
- Laszka A., Farhang S., Grossklags J. (2017). On the economics of ransomware. In: Rass S., An B., Kiekintveld C., Fang F., Schauer S. (eds) Decision and Game Theory for Security. GameSec Lecture Notes in Computer Science, 10575. *Springer*, Cham.
- Liao, K. Zhao, Z. Doup´e, A. & Ahn, Gail-Joon. (2016). Behind closed doors: Measurement and analysis of CryptoLocker ransoms in Bitcoin. In Proceedings of the 2016 APWG Symposium on Electronic Crime Research (eCrime).
- Luo, X. & Liao, Q. (2007). Awareness education as the key to ransom ware prevention. *Information Systems Security*, 16(4):195–202.

- Noam, N. Roughgarden, T., & Tardos, E. (2007). Algorithmic Game Theory. Cambridge University Press.
- The Law Library of Congress, Global Legal Research Center. (June 2018). Regulation of Cryptocurrency around the World, Report. Available at: https://www.loc.gov/law/help/cryptocurrency/cryptocurrency-world-survey. pdf
- Wikipedia (2019). Mechanism design, January, Available at: https://en.wikipedia.org/wiki/Mechanism_design
- Wikipedia. (2017). WannaCry ransomware attack. Available at: https://en.wikipedia.org/wiki/WannaCry_ransomware_attack.