Journal of Electronical & Cyber Defence
Vol. 10, No. 1, Spring 2022, Serial No. 37

A Framework for Evaluating Malware and Countermeasures with an Analytical Approach based on the Game Theory Case Study: Actors' Actions Based on Environmental Evidence

M. Abbasi, M. Bayat, M. Ghayoori*

* Assistant Professor, Faculty of Computer and Cyber Power, Imam Hossein University (AS), Tehran, Iran

(Received: 03/05/2021, Accepted: 13/12/2021)

ABSTRACT

One of the most serious threats to the cyberspace is malware, with multiple actors and diverse targets. Among the most important challenges in malware analysis systems, are the extent of malware and counter-measure actions, action evaluation of the actors, and extraction of the effective actions of actors. In this paper, a four-layer framework for extracting the effective actions of malware actors with a game theory approach is presented. In the first layer, based on environmental evidence, the actions of the attacker and the defender and their parameters are defined and determined; in the second layer, the activities of the actors are extracted based on the abstraction techniques implemented on the actions. In the third and fourth layers, the activities of the actors are modeled and analyzed in a scenario-centric approach based on the game theory. The effective options of the actors and the optimal equilibrium states of the games are extracted based on 13 defined measures. The proposed framework is modeled and evaluated based on a case study involving 12 offensive and 12 defensive activities in three games; the activities of the actors are extracted from their actions. The results show the effective activities of the attacker and the defender to be 3 and 2 activities, respectively, while the participation rate of these activities in the basic and optimal equilibrium states are 83% and 100%, respectively. Reducing the game space, evaluating actions, and extracting effective actions and optimal equilibrium states of the actors are some of the benefits of the proposed framework.

Keywords: Malware Analysis, Countermeasure Actions, Action Abstraction, Environmental Evidence, Game Theory, Graph Model.

* Corresponding Author Email: ghayoori@ihu.ac.ir

نشریه علمی "پدافند الکترونیکی و سایبری"
سال دهم، شماره ۱، بهار ۱۴۰۱، ص ۷۱-۴۷

علمی-پژوهشی

چارچوب ارزش‌گذاری اقدامات بدافزارها و مقابله‌کنندگان با رویکرد تحلیل مبتنی بر نظریه‌ی بازی مطالعه‌ی موردی: اقدامات بازیگران بر اساس شواهد محیطی

مصطفی عباسی[1*]، مجید غیوری ثالث[2]

۱- مربی، ۲- استادیار، دانشکده کامپیوتر و قدرت سایبری، دانشگاه جامع امام حسین(ع)، تهران، ایران

(دریافت: ۱۴۰۰/۰۲/۱۳، پذیرش: ۱۴۰۰/۰۹/۲۲)

چکیده

یکی از تهدیدهای جدی فضای سایبری، بدافزارها، با بازیگران متعدد و اهداف متنوع هستند. در سامانه‌های تحلیلی بدافزاری، گستردگی اقدامات بدافزارها و مقابله‌کنندگان، ارزش‌گذاری اقدامات بازیگران و استخراج اقدامات اثرگذار بازیگران از چالش‌های مهم است. در این مقاله، چارچوبی چهار لایه جهت استخراج اقدامات اثرگذار بازیگران حوزه‌ی بدافزار با رویکرد نظریه‌ی بازی ارائه شده است. در لایه‌ی اول بر اساس شواهد محیطی، اقدامات مهاجم و مدافع و پارامترهای آن‌ها تعریف و تعیین گردید؛ در لایه‌ی دوم، فعالیت‌های بازیگران مبتنی بر تکنیک‌های انتزاع‌سازی بر اساس اقدامات استخراج شد. در لایه‌ی سوم و چهارم مبتنی بر نظریه‌ی بازی، فعالیت‌های بازیگران به‌صورت سناریومحور، مدل‌سازی و تحلیل شد و گزینه‌های تأثیرگذار بازیگران و وضعیت‌های تعادلی مطلوب بازی‌ها بر اساس ۱۳ معیار تعریف‌شده، استخراج گردید. چارچوب پیشنهادی، بر اساس یک مطالعه موردی شامل ۱۲ فعالیت مهاجم و ۱۲ فعالیت مدافع در قالب سه بازی، مدل‌سازی و ارزیابی شد؛ فعالیت‌های بازیگران از اقدامات آن‌ها استخراج شده است. نتایج نشان داد فعالیت‌های تأثیرگذار مهاجم و مدافع به ترتیب ۳ و ۲ فعالیت هستند و میزان مشارکت این فعالیت‌ها در وضعیت‌های تعادلی پایه و مطلوب به ترتیب ۸۳ و ۱۰۰ درصد بوده است. کاهش فضای حالت بازی، ارزش‌گذاری اقدامات و استخراج اقدامات مؤثر و وضعیت‌های تعادلی مطلوب بازیگران از مزایای چارچوب پیشنهادی است.

کلیدواژه‌ها: تحلیل بدافزار، اقدامات مقابله‌ای، انتزاع‌سازی اقدامات، شواهد محیطی، نظریه‌ی بازی، مدل گراف

۱- مقدمه

حملات سایبری به سازمان‌ها از تهدیدات جدی سال‌های اخیر بوده است و بدافزارها از ابزارها و سلاح‌های مهم، حملات سایبری هستند [۱-۲]. راهکارهای متنوعی جهت شناسایی و مقابله با بدافزارها وجود دارد و این راهکارها عموماً در سامانه‌های دفاعی و امنیتی تعبیه شده‌اند. برای تهیه، طراحی و اجرای موفقیت‌آمیز یک بدافزار، بازیگران این حوزه در شرایط مختلف، باهم تعامل و رقابت دارند. با توجه به وجود رقابت همیشگی بین بدافزارها و سامانه‌های امنیتی، این رقابت یک مناقشه‌ی راهبردی و یکی از روش‌های مدل‌سازی و تحلیل آن نظریه‌ی بازی است [۳].

در یک مدل تصمیم‌یار مبتنی بر مدل گراف حل مناقشه، با افزایش رفتارهای بازیگران بازی، انفجار فضای حالتی با تعداد وضعیت‌هایی به‌صورت دو به توان مجموع تعداد رفتار بازیگران به وجود می‌آید [۳-۵]. تحلیل فضای گسترده و استخراج رفتارهای محتمل بازیگران، نیاز به سیستم‌های پردازشی قوی با حجم فضای حافظه‌ی بالا است [۶-۹]. با توجه به گستردگی رفتارهای بدافزارها و راهکارهای مقابله‌ای، یکی از مهم‌ترین اقدامات برای تحلیل رفتار بدافزارها و مقابله‌کنندگان مبتنی بر نظریه‌ی بازی، تبدیل داده‌های فنی به داده‌های سطوح بالاتر با جزئیات کمتر با رویکرد انتزاع‌سازی است [۱۰-۱۲]. یکی دیگر از نیازمندی‌های تحلیل رفتارهای بازیگران حوزه‌ی بدافزار مبتنی بر نظریه‌ی بازی، سیستم ارزش‌گذاری رفتارهای بازیگران است [۱۳-۱۵]. برای حل این مشکل نیاز است مجموعه پارامترهایی متناسب با رفتارهای بازیگران تعریف و مقداردهی گردد تا بر اساس آن پارامترها، ضمن تعریف تابع پاداش‌دهی برای رفتارهای بازیگران، بتوان بازی را در وضعیت‌ها و شرایط متنوع، بررسی و تحلیل کرد [۱۳].

هدف از انجام این مقاله ارائه‌ی چارچوبی است که ضمن انتزاع‌سازی اقدامات و پارامترهای آن‌ها در سطوح مختلف، اقدامات بازیگران را ارزش‌گذاری نماید و با بهره‌گیری از مدل‌های نظریه‌ی بازی، اقدامات بازیگران بازی را تحلیل و تأثیرگذارترین اقدامات را استخراج کند.

بنابراین با توجه به موضوع تحقیق، در بخش ۲ این مقاله، ادبیات موضوع شامل روش‌های شناسایی بدافزار، روش‌های تحلیل مسئله با استفاده از نظریه‌ی بازی و کارهای مرتبط با تحقیق بیان شده است. در بخش ۳، چارچوب پیشنهادی برای ارزش‌گذاری اقدامات بدافزارها و مقابله‌کنندگان و پارامترهای

* رایانامه نویسنده مسئول: ghayoori@ihu.ac.ir

ناشر: دانشگاه جامع امام حسین (ع)

آن‌ها و انتزاع تشریح می‌گردد. معیارهای استخراج اقدامات تأثیرگذار بازیگران در این بخش تعریف می‌شود. در ادامه، ارزیابی چارچوب ارائه‌شده بر اساس رفتارها و شواهد محیطی بازیگران و پارامترهای آن‌ها در بخش ۴ بیان گردیده است و در پایان نتیجه‌گیری مقاله مطرح می‌شود.

۲- ادبیات موضوع و پیشینه‌ی تحقیق

با توجه به موضوع مقاله، در این بخش مفاهیم مرتبط با این تحقیق و کارهای مرتبط تشریح می‌گردد.

۲-۱- روش‌های عمده‌ی شناسایی و تحلیل بدافزارها

روش‌های شناسایی بدافزارها ایستا (ساختاری)، پویا (رفتار) یا ترکیبی از آن دو است که در ادامه توضیح داده می‌شوند.

۲-۱-۱- شناسایی و تحلیل ایستا

تجزیه و تحلیل ایستا و ساختاری یکی از روش‌های شناسایی بدافزارها بر اساس ساختار فایل است که در آن بر اساس ساختار و ویژگی فایل‌های اجرایی، فایل موردنظر تجزیه و تحلیل می‌شود. بر اساس ویژگی‌ها و ساختار استخراج‌شده و تطابق آن با ویژگی‌های بدافزارها میزان مخرب بودن آن شناسایی و در دسته‌بندی‌های مختلف بدافزاری قرار می‌گیرد. از مزایای این روش سرعت شناسایی و از معایب آن عدم شناسایی بدافزارهای نوین، چندریختی و فشرده شده است. ابزارهایی که در این روش از آن‌ها برای شناسایی و تحلیل بدافزارها استفاده می‌گردد عبارت است از Explorer PE Debuger, Olly Pro, IDA و سایر نرم‌افزارهای مرتبط است [۱۳-۱۶]. یکی از ابزارهای تحلیل و بررسی فایل‌های اجرایی بخصوص بدافزارها، اشکال‌زداها[1] هستند. اشکال‌زدا قسمتی از نرم‌افزار یا سخت‌افزار است که برای ارزیابی یا بررسی فرایند اجرای برنامه‌ی دیگر به کار می‌رود [۱۶]. اشکال‌زداها در سطوح مختلفی از سیستم‌عامل و سخت‌افزار پیاده‌سازی می‌گردند؛ در جدول (۱) مقایسه سطوح مختلف اشکال‌زداها ارائه شده است [۱۳] و [۱۷].

جدول (۱): مقایسه‌ی سطوح مختلف اشکال‌زداها

ردیف	سطح اشکال‌زدا	نمونه اشکال‌زدا	شفافیت
۱	سطح کاربری سیستم‌عامل[2]	OllyDbg OllyICE,	↓ افزایش شفافیت
۲	سطح هسته سیستم‌عامل F۳[3]	KD WinDbg,	
۳	دیباگرهای مبتنی بر مجازی‌سازی F۴[4]	BOCHS, Ether, HyperDBG	
۴	دیباگرهای مبتنی بر فلز لخت F۵[5]	MALT	

[1] Debugger
[2] User-Mode Debuggers (UD)
[3] Kernel Debuggers (KD)
[4] Virtualization-Based Debuggers (VD)
[5] Bare-Metal Debuggers (BD)

منظور از شفافیت در جدول (۱)، میزان اطلاعاتی است که اشکال‌زدا می‌تواند از نرم‌افزار یا بدافزار در حال تحلیل، جمع‌آوری نماید. شناسایی محیط اشکال‌زدا، اجرا نشدن کدهای اصلی بدافزاری در محیط اشکال‌زدا، غیرفعال کردن محیط اشکال‌زدا و سایر رفتارهای مشابه از سوی بدافزارها، از چالش‌های محیط اشکال‌زدا در مواجه با بدافزارها است [۱۳]؛ بدافزارها از روش‌های متعددی مانند بررسی پردازه‌های در حال اجرا، کلیدهای رجیستری سیستم‌عامل، بررسی زمان اجرای دستورات خاص و کارهایی ازاین‌دست جهت شناسایی محیط هدف استفاده می‌نماید [۱۸]. به‌طورکلی روش‌های فریب محیط‌های اشکال‌زدا از طریق بدافزارها شامل روش‌های فریب وابسته به عوامل محیطی (مانند جمع‌آوری نشانه‌ها از محیط اشکال‌زدا (نقاط شکست، پردازش بلوک پردازنده، پردازش توابع مرتبط با زمان اجرا)، بررسی نتایج فراخوانی وقفه‌ها، شناسایی نشانه‌های هدفمند مرتبط با محیط اشکال‌زدا) و غیر وابسته به عوامل محیطی (دست‌کاری کنترل جریان پردازه‌های مرتبط، قفل‌کردن محیط اجرایی، حملات مبتنی بر تکنیک‌های بدون فایل) است [۱۹-۲۰].

۲-۱-۲- شناسایی و تحلیل پویا

یکی دیگر از روش‌های شناسایی بدافزارها، تحلیل رفتارهای بدافزارهای در زمان اجرا است. برای این منظور بدافزارهای در محیط‌های مجازی و کنترل‌شده اجرا می‌گردد و با استفاده از ابزارهای رصد و پایش، مجموعه اقدامات آن‌ها شناسایی و کنترل می‌گردد؛ سپس با تحلیل رفتارهای آن‌ها میزان مخرب بودن و اهداف آن‌ها استخراج می‌شود. با توجه به اینکه رفتارهای بدافزار در زمان اجرا بررسی و تحلیل می‌گردد، شناسایی بدافزارهای نوین از مزیت‌های این روش است. اما سرعت شناسایی پایین و شناسایی محیط‌های تحلیل و مجازی از سوی بدافزارها از معایب این روش است. جعبه‌ی شن و سایر ابزارهای رصد رفتارهای تغییرات فایل‌ها، رجیستری، ارتباطات شبکه‌ای از ابزارهای شناسایی بدافزارها بر اساس رفتار است [۱۳]. جعبه‌ی شن محیطی است که برای کنترل اثرات ناخواسته‌ی نرم‌افزارهای ناشناخته، توسعه داده شده است [۲۱] و محیطی کاملاً کنترل‌شده و جدا شده است که برای ارزیابی برنامه‌های تأیید نشده به کار گرفته می‌شود. جعبه‌ی شن‌ها محیط‌های اجرایی هستند که با شبیه‌سازی، مجازی‌سازی و مخفی‌سازی امکانات سیستم‌عامل، محیط ایمنی را برای اجرای تحت‌کنترل بدافزارها فراهم می‌کنند. جعبه‌ی شن به روش‌های مختلفی ایجاد می‌شود [۲۲]؛ در جدول (۲)، مروری بر انواع سطوح پیاده‌سازی جعبه‌ی شن ارائه شده است.

جدول (۲): بررسی و مقایسه انواع جعبه شن

ردیف	سطح جعبه شن	نمونه جعبه شن	شفافیت
۱	مبتنی بر مجازی‌سازی F۶[1]	Norman,CW,Cuckoo	↓ افزایش شفافیت
۲	مبتنی بر تقلید۷[2]	QEMU, Anubis	
۳	مبتنی بر فلز لخت۸[3]	Barebox, Bare cloud	

نام پردازه‌های مرتبط با جعبه‌ی شن، علائم و نشانه‌های مرتبط با محیط‌های مجازی، ویژگی‌هایی مانند مقدار فضای حافظه و زمان اجرای دستورات مشخص، بررسی ارتباطات شبکه‌ای ثابت، ارزیابی نتایج تعامل با کاربر، از روش‌های شناسایی محیط‌های جعبه‌ی شن است که بدافزارها بر اساس آن‌ها اجرای دستورات اصلی بدافزاری را به تأخیر انداخته یا اصلاً دستورات هدف را اجرا نمی‌کنند [۲۳]؛ بر همین اساس طراحان محیط‌های جعبه‌ی شن نیز مجموعه اقداماتی جهت مخفی نگه‌داشتن نشانه‌های جعبه‌ی شن و فریب بدافزارها جهت اجرای کامل دستورات آن‌ها، به کار می‌گیرند [۲۴]. به‌طورکلی روش‌های فریب جعبه شن‌ها از طریق بدافزارها شامل روش‌های فریب وابسته به عوامل محیطی (مانند جمع‌آوری نشانه‌ها (سخت‌افزاری، محیط اجرایی، برنامه‌های کاربردی، شبکه)، بررسی تعامل‌ها و داده‌های ورودی کاربری، شناسایی نشانه‌های هدفمند در محیط اجرایی و غیر وابسته به عوامل محیطی، به تعویق انداختن اجرای دستورات اصلی بدافزاری، فعال‌سازی بدافزار مبتنی بر فعال‌ساز محیطی، حملات مبتنی بر تکنیک‌های بدون فایل) است [۲۵-۲۶].

۲-۱-۳- شناسایی و تحلیل ترکیبی

در این روش که اکثر سامانه‌های دفاعی و آنتی‌ویروس‌ها از آن استفاده می‌کنند، بدافزارها و فایل‌های مشکوک از لحاظ ساختاری و رفتاری تحلیل می‌شوند تا ضمن بهره‌برداری از مزایای هر دو روش بتوانند حداقل معایب و کاستی را داشته باشند [۲۷].

یکی از چالش ها و نیازمندهای بررسی اقدامات بدافزارها در مدل‌های تحلیلی شبیه به نظریه‌ی بازی، نحوه‌ی ارزش‌گذاری کمّی اقدامات بدافزارها است. تعریف پارامترهایی متناسب با سطح اجرای اقدامات و سطوح امنیتی سیستم‌عامل و شرایط به‌کارگیری برای ارزش گذاری از اقدامات ضروری است. هرچند در برخی از پژوهش‌های مرتبط به‌خصوص افنانیان و همکاران برخی از اقدامات بدافزارها و راهکارهای مقابله‌ای و پارامترهای آن‌ها به‌صورت محدود تعریف شده، اما برای به‌کارگیری در مدل‌های نظریه‌ی بازی در حوزه‌ی بدافزار، نیاز به تعریف و ارزش‌گذاری دقیق تر اقدامات بدافزارها و راهکارهای مقابله نسبت به تحقیقات پیشین است.

۲-۲- روش‌های تحلیل مسئله مبتنی بر نظریه‌ی بازی

نظریه بازی یک ابزار بالقوه و مناسب برای مدل‌سازی و تجزیه‌وتحلیل اقدامات بازیگران یک فضای بزرگ و پیچیده مانند فضای سایبر است. نظریه بازی می‌تواند رفتارهای ذاتاً خودخواهانه و رقابتی از مهاجم، مدافع و محیط را مدل و تجزیه و تحلیل نماید. علاوه بر این، نظریه بازی این قابلیت را دارد که سناریوهای مختلف را قبل از اجرا در سیستم واقعی، مدل و اجرا کرده و نتایج را بر اساس راهبردها و ترجیحات بازیگران ارائه نماید.

نظریه بازی علاوه بر اینکه موقعیت‌های مختلف راهبردی را به‌صورت یک بازی مدل می‌کند؛ می‌تواند حملات انجام‌گرفته را تحلیل و ابعاد آن را مورد بررسی قرار دهد یا حتی احتمال وقوع یک حمله و حتی نوع آن را پیش‌بینی کند. با توجه به پیچیدگی‌های فضای سایبر و نبود اطلاعات کافی در خصوص رفتارهای مختلف بازیگران این فضا، بخصوص رقابت بازیگران حوزه بدافزار، قابلیت‌های نظریه بازی امکانات مناسبی برای مدل‌سازی و تحلیل سناریوهای مختلف، مدنظر بازیگران ارائه می‌نماید. در این بخش ضمن بیان مؤلفه‌ها و ویژگی‌های ضروری نظریه بازی‌ها، دسته‌بندی انواع بازی بیان می‌گردد.

۲-۲-۱- دسته‌بندی بازی‌ها

در نظریه بازی برای نمایش وضعیت‌های مختلف می‌توان از حالت نرمال[4] یا راهبردی، نمایش گسترده[5]، حالت گزینه‌ای[6] و نمایش گراف استفاده کرد که هرکدام مزیت‌ها و محدودیت‌هایی دارند. با توجه به حالت همکاری بازیگران با یکدیگر بازی‌های همکارانه یا غیر همکارانه وجود دارد. در حالت غیرهمکارانه هر بازیگر به منفعت خود می‌اندیشد و با رقبا همکاری نمی‌کند. پیامدها و عایدی‌های بازی به‌صورت صفر و غیر صفر تقسیم می‌شود. بازی‌ها با توجه به میزان دسترسی بازیگران به حرکات قبلی بازیگران به بازی با اطلاع کامل و ناقص تقسیم می‌شود و همچنین درصورتی‌که بازیگران از مجموعه راهبردها و پیامدهای رقیب مطلع باشند بازی با اطلاع کامل در غیر این‌صورت بازی با اطلاع ناقص تقسیم‌بندی می‌شود [۲۸].

۲-۳- مدل گراف تحلیل مناقشه و کاربردها

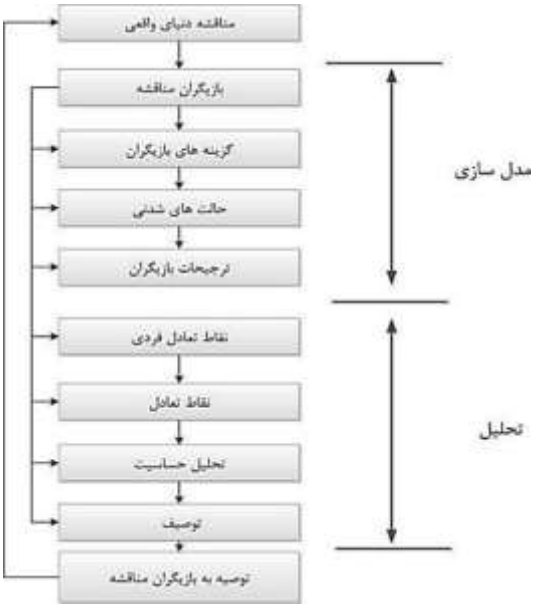
مدل گراف تحلیل مناقشه، یک متدولوژی مدل‌سازی و تحلیل مناقشه‌ی راهبردی مبتنی بر روش تحقیق

[1] Virtualization-Based Sandboxes(VS)
[2] Emulation-Based Sandboxes(ES)
[3] Bare-Metal Sandboxes(BS)
[4] Normal Form
[5] Extensive Form
[6] Option Form

توصیفی- تحلیلی، ارائه می‌کند. این مدل، به‌آسانی قابل‌استفاده و منعطف است. در آن مدل تصمیم سازان درک خوبی درباره‌ی اینکه چگونه آنچه باید انجام دهند را انتخاب کنند، دارند. البته سیستم‌های جایگزین برای مدل‌سازی و تحلیل مناقشات راهبردی که مجزا و متمایز از «نظریه بازی غیر همکارانه» باشند وجود دارد که از آن جمله می‌توان روش تحلیل متاگیم از سوی هوارد[1] [۲۹-۳۰]، در سال ۱۹۷۱ و ۱۹۸۷، تحلیل مناقشه از سوی فریزر[2] و هایپل [۳۱] در سال ۱۹۸۴، بازی خرد آگاه[3] از سوی تاکاهاشی و همکاران [۳۲] در سال ۱۹۸۴، نظریه‌ی درام[4] از سوی هوارد [۳۳] در سال ۱۹۹۴، تئوری حرکات[5] از سوی برمز[6] [۳۴] در سال ۱۹۹۳ و تئوری حرکات فازی را نام برد. این مدل هنر خود را در تحلیل مسائل پیچیده‌ی دنیای واقعی به‌خوبی نشان داده است. به‌عنوان مثال، به‌منظور پیش‌بینی محتمل‌ترین نتایج مورد انتظار در مناقشه‌ی هسته‌ای ایران از سوی شیخ محمدی، هایپل[7]، عاصی لاهیجانی و کیلگور[8] [۴] در سال ۲۰۰۹ و منازعه‌ی قدرت‌های منطقه‌ای و بین‌المللی در سوریه از سوی شیخ محمدی، بی طالبی، معطی و هایپل [۲۰] در سال ۲۰۱۳، این مدل به کار گرفته شده است. در پژوهشی در سال ۲۰۱۶، شیخ محمدی و عباسی [۵]، چالش اجتماعی تقسیم ارث زوجین مرحوم را با استفاده از قابلیت‌های نظریه‌ی بازی مدل‌سازی و تحلیل نموده‌اند و نتایج کسب‌شده از مدل‌سازی و تحلیل بازی با نتایج واقعی، یکسان بوده است. در سال ۲۰۱۷ عباسی و همکاران مدل‌سازی و تحلیل راهبردی مناقشه‌ی نویسندگان بدافزار و تحلیلگران سامانه‌های امنیتی با استفاده از نظریه بازی را ارائه نمودند [۳].

شکل (۱)، طرح به‌کارگیری مدل گراف حل مناقشه را در مدل‌سازی و تحلیل مناقشات پیچیده‌ی دنیای واقعی، نمایش می‌دهد. این مدل علاوه‌بر احصاء وضعیت تعادلی نش[9]، وضعیت‌های تعادلی SEQ[10]، GMR[11] و SMR[12] را نیز محاسبه و ارائه می‌نماید.

[1] Howard
[2] Fraser
[3] Hyper Game
[4] Drama Theory
[5] Theory of Moves
[6] Brams
[7] Hipel
[8] Kilgour
[9] Nash Equilibrium
[10] Sequential Stability
[11] General Meta-rationality
[12] Mymmetric Meta-rationality



شکل (۱): مدل گراف حل مناقشه [۳]

در مدل GMCR، به ارزش‌گذاری هر ترکیب ممکن از اقدامات بازیگران (وضعیت‌های ممکن بازی[13])، پیامد[14] گفته می‌شود؛ ترجیح‌گذاری پیامدها بر اساس مرتب‌سازی ترتیبی[15] پیامدها از طریق هر بازیگر برمبنای عایدی‌های کسب شده از هر پیامد، انجام می‌گیرد [۵]. ارزش‌گذاری کمّی پیامدها، یکی از چالش‌های به‌کارگیری مدل GMCR است و توسعه و بهره‌گیری این مدل در حوزه‌های جدید به خصوص بدافزار، با این چالش مواجه خواهد. با افزایش گزینه های بازیگران در مدل GMCR، تعداد وضعیت‌های بازی و مبتنی بر اساس وضعیت‌های تعادلی افزایش می‌یابد؛ بنابراین برای استخراج گزینه‌های تأثیرگذار بازیگران و محدودسازی و انتخاب وضعیت‌های تعادلی هدف در بازی نیاز به تعریف مجموعه معیارهایی هست. با توجه به گستردگی رفتارهای بدافزارها و راهکارهای مقابله ای، تعریف معیارهای استخراج گزینه‌های تأثیرگذار بازیگران از ضرورت‌ها و چالش‌های به کارگیری مدل گراف تحلیل مناقشه در حوزه بدافزار است.

۲-۴- انتزاع‌سازی فضای بازی و کاربردها

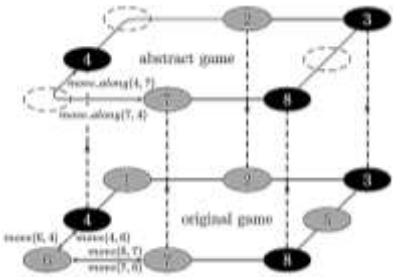
مفهوم انتزاع‌سازی فرآیند اختصار، فشرده‌سازی و تلخیص اطلاعات از طریق شناسایی، استخراج و سپس، جداسازی و پنهان‌سازی جزئیات از کلیات است. انتزاع فرآیند یا نتیجه تعمیم بخشیدن با کاهش محتوای اطلاعاتی یک مفهوم یا یک پدیده‌ی قابل مشاهده، جهت حفظ اطلاعات برای منظور خاص است. با توجه به ماهیت این پژوهش، انتزاع‌سازی در دانش رایانه و

[13] Feasible States
[14] Outcomes
[15] Ordinal Sort

مهندسی نرم‌افزار به معنای تفکیک مباحث مربوط به هم و نگریستن به موضوع جدای از مباحث وابسته به آن است [۱۱]. مزیت این کار در مهندسی نرم‌افزار کمک به مدیریت پیچیدگی و پیشگیری از وابستگی[1] اجزای سیستم به یکدیگر است که باید در سامانه‌های نرم‌افزاری تا حد امکان از آن کاسته شود. از انتزاع‌سازی در علوم کامپیوتر می‌توان مدل لایه‌ای شبکه‌ی OSI[2] و TCP/IP را بیان کرد.

اکثر بازی‌های جهان واقعی بازی با اطلاعات ناقص است و در سال‌های اخیر انتزاع‌سازی[3] به یکی از قابلیت‌های مهم برای حل بازی‌های بزرگ با اطلاعات ناقص تبدیل‌شده است. در این روش ابتدا بازی اصلی به بازی انتزاعی و کوچک‌تر تبدیل می‌گردد و از نگاه کلان و راهبردی بازی انتزاعی چکیده‌ای از بازی اصلی است. تعادل نش تقریبی در بازی انتزاعی تعیین و راهبردهای انتخاب‌شده از بازی انتزاعی با روش معکوس به بازی اصلی نگاشت می‌گردد [۶]. پیچیدگی نحوه‌ی تعیین تعادل نش در بازی‌های پیچیده و کارایی نداشتن روش‌های فعلی تعیین وضعیت تعادل و مدل‌سازی بازی‌های بزرگ با جزئیات گسترده، دلایلی بود که پژوهشگران روش انتزاع‌سازی بازی‌های بزرگ و پیچیده را پیشنهاد دادند. استراتژی‌های جدید بازیگران و نبودن دانشی از آن‌ها، همچنین از دست رفتن برخی از داده‌هایی که ممکن است در آینده باز هم نیاز باشد برخی از چالش‌های انتزاع‌سازی است.

بازی انتزاعی محدودیت‌هایی برای بازیگران و فضای راهبردهای آن‌ها لحاظ می‌نماید و یکی از نمونه‌های آن انتزاع‌سازی اطلاعات[4] است که در آن حالت‌های اطلاعات به یکدیگر بسته‌بندی می‌شوند. نوع دیگر انتزاع‌سازی، انتزاع‌سازی اقدامات[5] (شکل ۲) است که در آن فرض بر این است که برخی از اقدامات در بازی‌های اصلی کاربردی نبوده و فعلاً می‌توان از آن‌ها صرف‌نظر کرد [۳۵-۳۷].



شکل (۲): نمونه‌ی از انتزاع‌سازی اقدامات [۱۲]

با توجه به مبانی نظری و کاربردهای انتزاع‌سازی، یکی از راه‌کارهای کاهش فضای حالت مسئله و وضعیت‌های بازی در به‌کارگیری مدل GMCR، انتزاع‌سازی اقدامات بازیگران و تبدیل بازی اصلی مسئله به بازی انتزاع‌یافته است. نحوه‌ی انتزاع‌سازی اقدامات بدافزارها و پارامترهای آن‌ها و استخراج ارتباط بین نتایج بازی انتزاع‌یافته و بازی اصلی، یکی از چالش‌های مرتبط با تحلیل اقدامات بدافزارها است.

۲-۵- کارهای مرتبط

در سال ۲۰۱۲ سندلم و همکاران [۳۸]، زیرساخت عمومی برای انتزاع‌سازی مسئله‌ی دارای اتلاف و محدودیت را برای مدل تصادفی ارائه نمودند؛ در مدل پیشنهادی، با مدیریت هم‌زمان انتزاع‌سازی حالت‌ها و اقدامات، کیفیت راه‌حل ارائه شده، با اطمینان مناسبی تأیید می‌گردد. در سال ۲۰۱۱، باسیکو وگاتی در پژوهشی [۱۲]، محدودیت‌هایی برای بازی‌های امنیتی گشت‌زنی با قرار دادن محدودیت‌ها و مرزهایی ارائه دادند تا با استفاده از این روش، اقدامات را به حداقل تبدیل کنند؛ انتزاع بهینه متناسب با نوع سناریو به‌عنوان یکی از چالش‌های اصلی این پژوهش عنوان شده است. در شکل (۲)، روش محدود نمودن اقدامات برای بازی امنیتی گشت‌زنی با حذف موقعیت‌های ۱، ۵ و ۶ به دلیل نوع وابستگی آن‌ها ارائه شده است.

در سال ۲۰۱۴ در پژوهش کورر و سندهوم [۷]، چارچوب ریاضی برای استفاده در محدودسازی کیفیت راه‌حل بازی فرم گسترده یادآوری کامل[6] ارائه شده است. این چارچوب دارای مدل مفهومی جدیدی برای نگاشت رفتارها در بازی انتزاعی به بازی اصلی و تحلیل و بررسی آن‌ها است؛ همچنین آن‌ها در پژوهش دیگری در سال ۲۰۱۴، مدلی برای انتزاع‌سازی مبتنی بر خوشه‌بندی ارائه نموده‌اند که از الگوریتم‌های برنامه‌ریزی عدد صحیح[7] مقیاس‌پذیرتر بوده است [۸]. در پژوهش فرانتز [۹]، طبقه‌بندی جامعی از روش‌های انتزاع‌سازی ارائه شده است؛ بر اساس این طبقه‌بندی، تکنیک‌های انتزاع‌سازی در سه دسته کلی تغییر و اصلاح مدل مرزی[8]، تغییر و اصلاح رفتارها[9] و تغییر و اصلاح فرم مدل[10]، قابل تعریف هستند. با توجه به شرایط مسائل حوزه‌ی امنیت و جنگ اطلاعات با ترکیبی از تکنیک‌های ارائه‌شده مسائل را مدل کرد. در سال ۲۰۱۰ در پژوهش بیوکمپس و همکاران [۱۰]، روشی برای شناسایی الگوهای رفتارهای بدافزارهای به‌صورت پیش‌کنشانه ارائه شده که در آن برخی از اقدامات و فعالیت‌های بدافزار در سطح پایین استخراج

[1]. Tight Coupling
[2] .Open Systems Interconnection model
[3] .Abstraction
[4]. Information Abstraction
[5] .Action Abstraction

[6]. Perfect-recall
[7] Integer Programming Algorithms
[8] Model Boundary Modification
3.Behaviors of Modification
4.Form Model of Modification

گردیده و بر اساس مدل‌سازی رسمی و تعریف الگوهای رفتاری بدافزار، ضمن کاهش فضای مسئله تحلیل، رفتارهای مخرب آن را نیز شناسایی می‌نماید.

در مقاله‌ی بلوچیان و ایزدی‌پور [۳۹]، اهمیت نظریه‌ی بازی در مدل‌سازی و حل مسئله‌ی تخصیص در فرماندهی و کنترل شبکه‌ی محور بررسی شده است. این مقاله با در نظر گرفتن هوشمندی اهداف به دنبال حل مسئله‌ی تخصیص است. در نظر گرفتن رفتار دشمن در مسئله‌ی تخصیص سلاح ضروری است که در مقاله‌ی مذکور مدل‌سازی ریاضی مسئله‌ی تخصیص سلاح با تعیین زمان شلیک به اهداف و حل آن بر اساس نظریه‌ی بازی ارائه گردیده است

در سال ۲۰۱۴ در پژوهش کورر و سندهوم [۴۰]، چارچوب ریاضی برای استفاده در محدودسازی کیفیت راه‌حل بازی فرم گسترده یادآوری کامل[1] ارائه شده است. این چارچوب دارای مدل مفهومی جدیدی برای نگاشت رفتارها در بازی انتزاعی به بازی اصلی و تحلیل و بررسی آن‌ها است؛ همچنین آن‌ها در پژوهش دیگری در سال ۲۰۱۴، مدلی برای انتزاع‌سازی مبتنی بر خوشه‌بندی ارائه نموده‌اند که از الگوریتم‌های برنامه‌ریزی عدد صحیح[2] مقیاس‌پذیرتر بوده است [۴۱]. در پژوهش فرانتز [۴۲]، طبقه‌بندی جامعی از روش‌های انتزاع‌سازی ارائه شده است؛ بر اساس این طبقه‌بندی، تکنیک‌های انتزاع‌سازی در سه دسته‌ی کلی تغییر و اصلاح مدل مرزی[3]، تغییر و اصلاح رفتارها[4] و تغییر و اصلاح فرم مدل[5]، قابل تعریف هستند. با توجه به شرایط مسائل حوزه‌ی امنیت و جنگ اطلاعات با ترکیبی از تکنیک‌های ارائه‌شده مسائل را مدل کرد. در سال ۲۰۱۰ در پژوهش بیوکمپس و همکاران [۱۰]، روشی برای شناسایی الگوهای رفتارهای بدافزارهای به‌صورت پیش‌کنشانه ارائه شده که در آن برخی از اقدامات و فعالیت‌های بدافزار در سطح پایین استخراج گردیده است و بر اساس مدل‌سازی رسمی و تعریف الگوهای رفتاری بدافزار، ضمن کاهش فضای مسئله‌ی تحلیل، رفتارهای مخرب آن نیز شناسایی می‌شود.

به‌منظور آشکارسازی نفوذ در شبکه، یک معماری ترکیبی از پارسا و اعرابی ارائه شده است؛ [۴۳] این معماری مبتنی بر روش آشکارسازی ترکیبی، ساختاری چهار لایه دارد. لایه‌ی اول از واحد تحلیلگر جریان داده‌ها و واحد طبقه‌بندی تشکیل گردیده است. لایه‌ی تشخیص نفوذ (لایه‌ی دوم)، یک واحد آشکارساز مبتنی بر امضاء و واحدهای آشکارساز مبتنی بر ناهنجاری دارد و به شکل ترکیبی پیاده‌سازی شده‌اند. لایه‌ی سوم و چهارم به ترتیب لایه‌ی تصمیم‌گیری و مدیریت وقایع هستند. نتایج حاصل از ارزیابی حاکی از تشخیص ۸۱/۹۹ درصد از نفوذها است که کاهش میزان نرخ مثبت کاذب را نشان می‌دهد.

۲-۶- جمع‌بندی و نتیجه‌گیری

با توجه به بین‌رشته‌ای بودن مقاله‌ی حاضر، نیاز است تا مبانی نظری چارچوب پیشنهادی و کاربرد آن‌ها بیان گردد. هرچند کارهای انجام‌شده‌ی قبلی که در مبانی نظری و کارهای مرتبط عنوان شد تا اندازه‌ای به حل مسئله کمک کرده اند؛ ولی در مسئله‌ی به‌کارگیری مدل گراف تحلیل مناقشه در حوزه‌ی تحلیل بدافزارها هنوز چالش‌هایی وجود دارد. چارچوب ارزش‌گذاری رفتارها، مدل نظریه‌ی بازی مناسب تحلیل رفتارهای بازیگران حوزه‌ی بدافزار، معیارهای استخراج وضعیت‌های تعادلی مناسب، نحوه ی اعمال عدم قطعیت اطلاعات در بازی و روش انتزاع‌سازی اقدامات بازیگران از چالش‌های موجود، کارهای مرتبط با این مقاله بوده و هدف این مقاله ارائه ی چارچوبی جهت رفع چالش‌های عنوان شده است.

۱- ۳- چارچوب پیشنهادی

نمای کلی چارچوب پیشنهادی در شکل (۳) ارائه شده است؛ در این چارچوب چهار لایه‌ی پردازشی شامل ۱) جمع‌آوری اقدامات بازیگران و پارامترهای آن‌ها ۲) تبدیل اقدامات فنی و تکنیکی به فعالیت ۳) مدل‌سازی و تحلیل بازی ۴) لایه‌ی پیش‌بینی و استخراج محتمل‌ترین رفتار بازیگران، وجود دارد. در این مقاله، بدافزارها (مهاجم) و مقابله کنندگان (مدافع) به‌عنوان دو بازیگر مفروض در نظر گرفته شده‌اند.

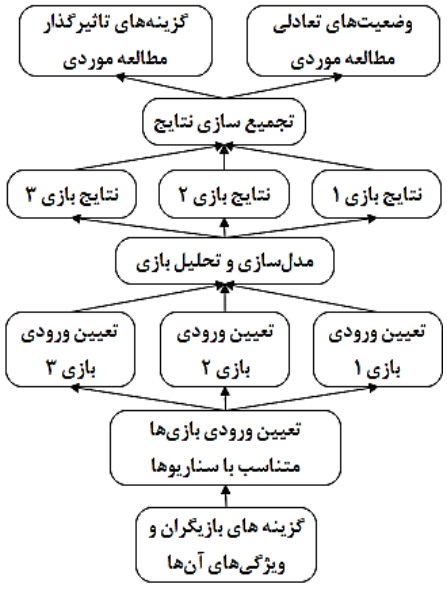
شکل (۳): طرح کلی تعامل لایه‌های چارچوب پیشنهادی

[1]. Perfect-recall
[2]. Integer Programming Algorithms
[3] .Model Boundary Modification
[4] .Modification of Behaviors
[5] .Modification of Model Form

به‌منظور تحلیل فعالیت‌های بدافزارها و مقابله‌کنندگان مبتنی بر نظریه‌ی بازی، ضمن تعریف و استخراج ارتباط بین اقدامات و فعالیت‌های بازیگران، نیازمند یک سیستم ارزش‌گذاری سلسله‌مراتبی فعالیت‌های بازیگران است. برای این منظور ابتدا پارامترهای ارزش‌گذاری اقدامات و فعالیت‌های بازیگران تعریف و مقداردهی می‌گردد؛ سپس روابط بین اقدامات و فعالیت‌ها و نحوه‌ی انتزاع‌سازی اقدامات به فعالیت‌ها بیان می‌گردد.

در این چارچوب لایه‌هایی جهت جمع‌آوری و انتزاع‌سازی اقدامات بازیگران و استخراج پارامترهای مرتبط با اقدامات و فعالیت‌ها ارائه گردیده است. در لایه‌ی مدل‌سازی و تحلیل، «مدل گراف تحلیل مناقشه» به‌عنوان روش تحلیل مبتنی بر نظریه‌ی بازی انتخاب شده است. تکنیک‌های بر مبنای پارامترهای ورودی به این لایه و منطق های تعادلی، بازی مدل سازی و تحلیل می‌گردد. در لایه‌ی پیش‌بینی و استخراج محتمل‌ترین رفتارها، بر اساس نتایج بازی و معیارهای ارزیابی رفتارهای تأثیرگذار بازیگران، وضعیت های تعادلی مطلوب استخراج و مبتنی بر آن پیشنهادها و تصمیم‌سازی مناسب به بازیگران ارائه می‌گردد.

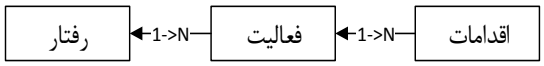
با توجه به گستردگی فعالیت‌های بازیگران، معیارهای استخراج گزینه‌های تأثیرگذار بازیگران و وضعیت‌های تعادلی بازی تعریف می‌شود. متناسب با سناریوهای تعریف‌شده، با تغییر در پارامترهای اقدامات و فعالیت‌های بازیگران و میزان شناخت بازیگران از شرایط مطالعه‌ی موردی، بازی‌های متنوع ایجاد می‌گردد. نتایج بازی‌ها بر اساس معیارهای استخراج گزینه‌های تأثیرگذار، بررسی و مؤثرترین گزینه‌های بازیگران در ایجاد شرایط تعادلی استخراج می‌گردد (شکل (۴)).



شکل (۴): طرح سناریو محور استخراج گزینه‌های تأثیرگذار بازیگران

۳-۱- تعریف اقدام و فعالیت بازیگران

اقدام شامل توابع سیستمی که در لایه‌های مختلفی از سیستم‌عامل از قبل پیاده‌سازی شده و موجب تسهیل در تعامل با سخت‌افزار یا سیستم‌عامل می‌شوند. یک نمونه اقدام می‌توان به «بررسی پرچم NtGlobalFlag برای تشخیص اشکال‌زدا» اشاره کرد.

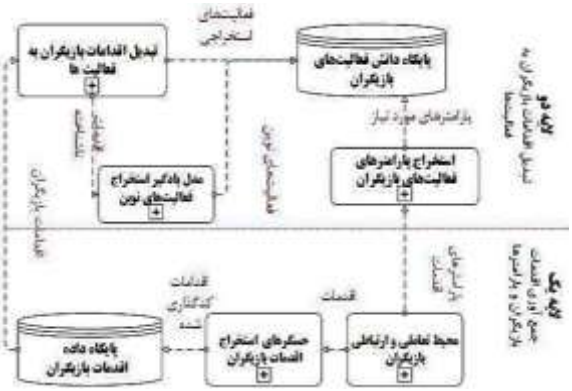


شکل (۵): رابطه‌ی بین اقدام، فعالیت و رفتار بازیگران

همان‌طور که در شکل (۵)، نشان داده شده رابطه‌ی بین فعالیت و اقدام رابطه‌ی یک به چند است؛ یعنی یک فعالیت حداقل شامل یک اقدام و بیشتر است. در سطوح بالاتر چند فعالیت تشکیل‌دهنده‌ی یک رفتار برای بازیگران است. بنابراین در چارچوب پیشنهادی این مقاله، ابتدا اقدامات بازیگران و پارامترهای آن‌ها در پایین‌ترین سطح استخراج می‌گردد و سپس فعالیت‌ها بازیگران و پارامترهای بر اساس اقدامات تشکیل می‌شود (شکل (۶)).

۳-۲- جمع آوری اقدامات بازیگران و پارامترهای آن‌ها و تبدیل اقدامات به فعالیت‌ها

در لایه‌ی یک شکل (۶)، ابتدا مجموعه اقدامات دریافتی از حسگرهای مختلف موجود در محیط تعاملی بازیگران (بخصوص بدافزارها) در پایگاه داده مربوطه ذخیره می‌گردد. محیط تعاملی بازیگران در پایین‌ترین سطح، سیستم‌عامل و برنامه‌های کاربردی و محیط شبکه است که در آن‌ها، بدافزارها عملیات ایجاد، تغییر، حذف و جست‌وجو در سطح فایل‌ها، پردازه‌ها، رجیستری و اقدامات مشابهی در سطح شبکه و سایر مؤلفه‌های مرتبط با سیستم‌عامل را انجام می‌دهند. اقدامات بدافزارها یا هرگونه فایل‌های مشکوک، به‌وسیله‌ی ابزارهای تحلیل مبتنی بر تحلیل ساختار، رفتار و ترکیبی بررسی و نتایج تحلیل جهت بهره‌برداری‌های آتی، در پایگاه داده ذخیره می‌گردد.



شکل (۶): طرح انتزاع‌سازی اقدامات بازیگران

در لایه‌ی دو شکل (۶)، طرح تبدیل اقدام به فعالیت، اقدامات موجود در پایگاه داده‌ی اقدامات بازیگران به‌وسیله الگوریتم‌های استخراج ویژگی و الگو و مدل‌های انتزاع‌سازی، به فعالیت‌های مدنظر تبدیل می‌شوند. فعالیت‌ها در پایگاه دانش فعالیت‌های بازیگران ذخیره می‌شود. متناسب با شرایط اقدامات و فعالیت‌های بدافزارها و مقابله‌کنندگان، از تکنیک‌های محدودیت فضای ورودی، انتزاع‌سازی تابعی و موجودیتی و تجمیع، برای تبدیل اقدامات به فعالیت‌ها در این لایه بهره‌برداری شده است.

در روابط (۱) الی (۵) تعاریف اقدامات و فعالیت‌های بازیگران و روابط بین آن‌ها، بیان شده است. در رابطه‌ی (۱)، مجموعه‌ی A معرف کل اقدامات بازیگران و مجموعه‌های A_{At} و A_f به ترتیب بیانگر اقدامات مهاجم و مدافع است؛ به‌نحوی‌که مجموعه اقدامات مهاجم و مدافع باهم اشتراکی ندارد و اجتماع آن‌ها مجموعه M را ایجاد می‌کند. مجموعه اقدامات یک بازیگر، حداقل شامل یک اقدام و هر اقدام حداقل دارای یک پارامتر و هر پارامتر از یک سه‌تایی مرتب شامل نام، مقدار و وزن تشکیل شده است. در رابطه‌ی (۱) مفهوم نمادها به شرح زیر است:

- ✓ $N_{At}^{A}(i,j)$ و $N_{Df}^{A}(i,j)$ به ترتیب نام پارامتر i ام اقدامات j ام مهاجم و مدافع؛
- ✓ $V_{At}^{A}(i,j)$ و $V_{Df}^{A}(i,j)$ به ترتیب ارزش پارامتر i ام و j ام مهاجم و مدافع؛
- ✓ $W_{At}^{A}(i,j)$ و $W_{Df}^{A}(i,j)$ به ترتیب وزن پارامتر i ام اقدامات j ام مهاجم و مدافع؛
- ✓ $\propto$ یعنی وابستگی و ارتباط اعضای دو مجموعه
- ✓ $^{+}$بیان‌کننده‌ی حداقل یک تکرار عضو (عمل) موردنظر
- ✓ $sizeof$ بیان‌کننده تعداد عناصر یک مجموعه

بر اساس تعاریف رابطه (۱)، رابطه‌ی $A_{At} \propto A_{Df}$ بیان می‌کند که برخی از اعضای مجموعه A_{At} با عناصر مجموعه A_{Df} رابطه دارد؛ یعنی اینکه، مهاجم از برخی از اقدامات خود برای مقابله با اقدامات مدافع استفاده می‌کند و برعکس برای مدافع نیز اقداماتی برای مقابله با اقدامات مهاجم نیز در نظر گرفته می‌شود. ارتباط بین اعضای مهاجم و مدافع یک ارتباط یک به چند است و این موضوع برای ارتباط مدافع و مهاجم نیز صدق می‌نماید.

$$\begin{matrix} \left\{\begin{matrix} A = A_{At} \cup A_{Df}\ ;\ A_{At} \cap A_{Df} = \emptyset; \\ A_{At} \propto A_{Df};\ A_{Df} \propto A_{At}; \end{matrix}\right\} \\ A_{At} = \left\{\begin{matrix} (a_{At}(i), (N_{At}^{A}(i,j), V_{At}^{A}(i,j), W_{At}^{A}(i,j))^{+})^{+} \mid i = 1,2,..,n; \\ j = 1,2,..,m;\ n,m \in N;\ V_{A}^{M}(i,j), W_{A}^{M}(i,j) \in R \end{matrix}\right\} \\ A_{Df} = \left\{\begin{matrix} \left(a_{Df}(i), \left(N_{Df}^{A}(i,j), V_{Df}^{A}(i,j), W_{Df}^{A}(i,j)\right)^{+}\right)^{+} \mid i = 1,2,..,n; \\ j = 1,2,..,m;\ n,m \in N;\ V_{Df}^{A}(i,j), W_{Df}^{A}(i,j) \in R \end{matrix}\right\} \end{matrix} \quad (۱)$$

توابع $F_{At}^{A}(i)$ و $F_{D}^{A}(i)$، مقدار ارزش یک اقدام برای بازیگران را بر اساس میانگین حسابی پارامترهای آن، طبق رابطه (۲)، محاسبه می‌نمایند. از این مقادیر در ارزش‌گذاری وضعیت‌های بازی‌ها استفاده می‌گردد.

$$\begin{aligned} F_{At}^{A}(i) &= \frac{\sum_{j=1}^{N} V_{At}^{A}(i,j) \ * \ W_{At}^{A}(i,j)}{\sum_{j=1}^{N} W_{At}^{A}(i,j)} \\ F_{Df}^{A}(i) &= \frac{\sum_{j=1}^{N} V_{Df}^{A}(i,j) \ * \ W_{Df}^{A}(i,j)}{\sum_{j=1}^{N} W_{Df}^{A}(i,j)} \end{aligned} \quad (۲)$$

در رابطه (۲)، $V_{At}^{A}(i,j)$ و $W_{At}^{A}(i,j)$ اعضای پارامترهای مجموعه اقدامات مهاجم و $V_{Df}^{A}(i,j)$ و $W_{Df}^{A}(i,j)$ اعضای پارامترهای مجموعه اقدامات مدافع است. مقدار عایدی یک اقدام برای یک بازیگر مشخص بر اساس توابع $U_{At}^{A}(i)$ و $U_{Df}^{A}(i)$ مطابق با رابطه (۳)، محاسبه می‌گردد. مطابق رابطه (۳)، عایدی بازیگر برای یک اقدام مشخص، از کسر مقادیر ارزش راهکارهای مقابله‌ای رقیب از ارزش اقدام بازیگر محاسبه می گردد؛ بنابراین هرچه ارزش راهکارهای مقابله‌ای رقیب در برابر اقدام بازیگر کمتر باشد یا رقیب شناخت کمتری نسبت به اقدام بازیگر، داشته باشد، ارزش بهره‌برداری از آن اقدام در وضعیت‌های مختلف بازی بیشتر خواهد بود. در مدل سازی و تحلیل بازی مبتنی بر GMCR، ترجیح‌گذاری وضعیت‌های ممکن بازی، با مرتب‌سازی ترتیبی وضعیت‌ها مبتنی بر ارزش آن‌ها، صورت می‌گیرد؛ بنابراین منفی‌شدن ارزش برخی از اقدامات و وضعیت‌ها، مشکلی در مدل‌سازی و تحلیل بازی به‌وجود نمی‌آورد.

$$\begin{aligned} U_{At}^{A}(i) &= F_{At}^{A}(i) - \sum_{j=1}^{N} F_{Df}^{A}(j) \\ U_{Df}^{A}(i) &= F_{Df}^{A}(i) - \sum_{j=1}^{N} F_{At}^{A}(j) \end{aligned} \quad (۳)$$

در رابطه (۴) مجموعه B به‌عنوان فضای حالت کل فعالیت‌های بازیگران، شامل دو مجموعه B_{At} و B است که این دو مجموعه اشتراکی ندارند. اعضای مجموعه‌های B_{At} و B_{Df} با یکدیگر ارتباطاتی دارند. به‌عنوان نمونه ممکن است یک عضو مجموعه B_{Df} (که یک رفتار دفاعی است) بتوانند با چند عضو مجموعه B_{At} (شامل چند رفتار بدافزاری است) مقابله کند (رابطه‌ی ۴).

$$\left\{\begin{matrix} B = B_{At} \cup B_{Df} \\ B_{At} \cap B_{Df} = \emptyset \\ B_{At} \propto B_{Df};\ B_{Df} \propto B_{At} \\ B_{At} \propto A_{At};\ B_{Df} \propto A_{Df} \end{matrix}\right\} \quad (۴)$$

مجموعه فعالیت‌های بازیگران نیز با مجموعه اقدامات بازیگران ارتباط دارند و پارامترهای مرتبط با فعالیت‌ها بر اساس پارامترهای اقدامات منتسب به فعالیت‌ها، محاسبه می‌گردد. قالب کلی تعریف فعالیت‌ها شبیه به قالب تعریف اقدامات بوده و روابط

حاکم بر محاسبات فعالیت‌ها، شبیه به محاسبات اقدامات است. در رابطه‌ی (۵) نحوه‌ی استخراج پارامترهای فعالیت‌های مهاجم بر اساس اقدامات مهاجم ارائه شده و $W_{At}^{B}(i,j)$ و $W_f\ \ (i,j)$ به ترتیب بیان‌کننده وزن پارامتر i ام فعالیت j ام مهاجم و مدافع است.

$$\begin{gathered} V_{At}^{B}(i,j), W_{At}^{B}(i,j) \epsilon B_{At} \\ V_{At}^{A}(m,n), W_{At}^{A}(m,n) \in A_{At} \\ V_{At}^{B}(i,j) = \frac{\sum_{m\epsilon M, n\epsilon N} V_{At}^{A}(m,n) * W_{At}^{A}(m,n)}{\sum_{m\epsilon M, n\epsilon N} W_{At}^{A}(m,n)} \\ W_{At}^{B}(i,j) = \frac{\sum_{m\epsilon M, n\epsilon N} W_{At}^{A}(m,n)}{sizeof(W_{At}^{A}(m,n))} \end{gathered} \quad (۵)$$

۳-۳- پارامترهای اقدامات بازیگران

پارامترهای اقدامات بازیگران و مقادیر آن‌ها، متناسب با ویژگی‌های اقدامات، تعیین می‌شود. بر اساس روابط بین اقدام، فعالیت و رفتار، ارزش‌گذاری و اولویت‌گذاری بازیگران نسبت به رفتارها و فعالیت و اقدامات خود و رقیب، تعیین می‌گردد. در پژوهش افنانیان و همکاران [۱۳]، پارامترهای پیچیدگی[1]، تاب‌آوری[2]، سطح اثربخشی[3] و فراوانی[4] به‌عنوان پارامترهای اقدامات بدافزارها به‌صورت کیفی معرفی تشریح شده است. در این مقاله، پارامترها به دو دسته ی کلیِ پارامترهای وابسته به اقدامات و وابسته به بهره‌بردار اقدامات، تقسیم می‌شوند. بازه‌ی مقادیر پارامترهای اقدامات با الگوبرداری از بازه ی تقسیم بندی طیف لیکرت[5] و سیستم امتیازدهی آسیب‌پذیری‌ها مشترک[6] [۱۴-۱۵]، طیف اعداد ۰ تا ۱۰، تعیین شده است. در این مقاله، علاوه بر کمی و کیفی‌سازی پارامترهای ارائه شده در پژوهش افنانیان و توسعه‌ی آن‌ها، دسته‌بندی جدیدی از پارامترهای مقابله‌کنندگان بدافزارها نیز ارائه شده است. پارامترهای پیچیدگی، تاب‌آوری، سطح اثربخشی و فراوانی به‌عنوان پارامترهای وابسته به اقدامات بازیگران و پارامتر قابلیت بهره‌برداری وابسته به بهره‌بردار لحاظ می‌گردد. پارامترهای اقدامات بازیگران در سطح فعالیت بر اساس پارامترهای سطح اقدامِ بازیگران تعیین می‌شود. بر مبنای نظر خبرگان و مطالعه‌ی پژوهش‌های مرتبط با شرایط بازیگران، مقادیر توصیفی پارامترها و طیف مقادیر عددی آن‌ها، برای مهاجم و مدافع به ترتیب جدول (۳) و (۴)، از پیوست ارائه شده است. در ادامه، تشریح پارامترها ارائه می‌گردد.

۳-۳-۱- پیچیدگی پیاده‌سازی

منظور از پیچیدگی پیاده‌سازی، تعداد خط کدهایی موردنیاز برای پیاده‌سازی و اجرای اقدام مدنظر و سطح پیاده‌سازی کدها متناسب با لایه‌بندی امنیتی سیستم‌عامل است. این سطح امنیتی از کدنویسی و پیاده‌سازی در سطح کاربری سیستم‌عامل تا سطح ثابت‌افزار، قابل تقسیم‌بندی و مقداردهی است.

۳-۳-۲- تاب‌آوری

این پارامتر، میزان سختی مقابله با اقدام بازیگر توسط رقیب را نمایش می‌دهد؛ هرچه راهکارهای مقابله‌ای رقیب از سمت ثابت‌افزار به سمت سطح کاربری سیستم‌عامل تمایل بیشتری داشته باشد میزان تاب‌آوری اقدام موردنظر و ارزش آن، کمتر و راهکارهای دور زدن آن بیشتر است.

۳-۳-۳- سطح اثربخشی

این پارامتر میزان اثربخشی اقدام بازیگر بر راهکارهای مقابله‌ای رقیب را بر اساس سطوح امنیتی سیستم‌عامل، نشان می‌دهد. هرچه سطح اثرگذاری اقدام بازیگر به سطح ثابت‌افزار و سخت‌افزار نزدیک‌تر باشد میزان اثربخشی و ارزش آن بیشتر و راهکارهای مقابله‌ای با آن سخت‌تر است.

۳-۳-۴- فراوانی به‌کارگیری

این پارامتر میزان فراوانی استفاده از اقدام بازیگر بر اساس تاریخچه و سوابق را، نشان می‌دهد. مقادیر این پارامتر بر اساس منابع مرتبط و نظر خبرگان مقداردهی شده است. تمایل این پارامتر به سمت یک، نشان‌دهنده عمومی‌تر بودن و تمایل به سمت ده، نشانه جدید و ناشناخته بودن اقدام بازیگر را بیان می‌کند.

۳-۳-۵- قابلیت بهره‌برداری

این پارامتر، میزان توانمندی‌های بازیگران برای بهره‌برداری از اقدام مدنظر را بیان می‌دارد. هرچه منابع مالی، نیروی انسانی متخصص، سامانه‌های نرم‌افزاری پایه بومی، تجهیزات زیرساختی بومی و دسترسی به دانش و فناوری بازیگران مناسب‌تر باشد قابلیت بهره‌برداری از اقدام بیشتر است، مقدار این پارامتر به سمت عدد ده میل می‌کند.

ضریب پارامترها میزان اهمیت آن پارامتر نسبت به سایر پارامترهای اقدامات را بیان می‌کند؛ جهت ساده‌سازی و به‌صورت مفروض در این مقاله، مقدار ضریب پارامترها ثابت و یک در نظر گرفته شده است.

۳-۴- نحوه محاسبه ظرفیت و توانمندی اجرای گزینه‌ها از سوی بازیگر

ظرفیت و توانمندی اجرای اقدام از سوی بازیگر، بر اساس شرایط

[1] Complexity
[2] Resistance
[3] Efficacy-Level
[4] Pervasiveness
[5] Likert Spectrum
[6] Common Vulnerability Scoring System (CVSS)

بازیگر (شامل منابع مالی، نیروی انسانی متخصص، سامانه‌های نرم‌افزاری پایه بومی، تجهیزات زیرساختی بومی و دسترسی به دانش و فناوری) و پارامترهای مرتبط با اقدام آن (شامل پیچیدگی پیاده‌سازی، تاب‌آوری، سطح اثربخشی و فراوانی به‌کارگیری) طبق رابطه‌ی (۶) محاسبه می‌گردد. مقدار کمی و کیفی هر یک از شرایط بازیگران شامل یکی از موارد: ۵-خیلی خوب ۴- خوب ۳-متوسط ۲ –ضعیف ۱- خیلی ضعیف است.

$$Ex_k^p = \left(\sum_{i=1..I, j=1..J, k=1..K} (x_{ki} * S_{ki}^p + y_{kj} * P_{kj}^p) \right) / 60 \qquad (۶)$$

در رابطه (۶)، Ex_k^p نشان‌دهنده، توانمندی بهره‌برداری بازیگر p (مهاجم یا مدافع) از اقدام k است. x_{ki} ضریب ثابت شرایط بازیگر و S_{ki}^p مقدار شرایط iام بازیگر p در اقدام k است؛ y_{kj} ضریب ثابت پارامترهای اقدام بازیگر و P_{kj}^p مقدار پارامتر jام بازیگر p در اقدام k است. ضریب ثابت شرایط بازیگر شامل منابع مالی، نیروی انسانی متخصص، سامانه‌های نرم‌افزاری پایه بومی، تجهیزات زیرساختی بومی و دسترسی به دانش و فناوری به ترتیب ۱,۲۵، ۱,۲۵، ۰/۷۵، ۰/۷۵ و ۱ و ضریب ثابت پارامترهای اقدام بازیگر شامل پیچیدگی پیاده‌سازی،

اقدام تاب‌آوری، سطح اثربخشی و فراوانی به‌کارگیری به ترتیب ۳، ۳، ۳ و ۱ هست.

در جدول (۵) از پیوست مقاله، ضریب ثابت پارامترهای اقدام و شرایط بازیگر ارائه شده است. در جدول (۵)، مثالی از یک اقدام بازیگر که همه‌ی شرایط بازیگر ۵ و همه‌ی پارامترهای ۱۰ است ارائه‌شده که نتیجه‌ی آن ظرفیت و توانمندی اجرای اقدام از سوی بازیگر به‌صورت ۱۰ یا ۱۰۰ درصد است و علت تقسیم نتایج بر ۶۰، نرمال‌سازی جواب به عدد ۱۰ یعنی حداکثر مقدار پارامترهای اقدام بازیگر است.

۳-۵- معیارهای استخراج گزینه‌های تأثیرگذار

در مدل گراف تحلیل مناقشه، تعداد وضعیت‌های ممکن بازی، توانی از تعداد گزینه‌های بازیگران است؛ با افزایش تعداد گزینه‌های بازیگران تعداد وضعیت‌های ممکن بازی و به همان نسبت وضعیت‌های تعادلی افزایش می‌یابد. برای تعیین و انتخاب وضعیت های تعادلی مطلوب، نیاز به معیارهایی جهت توسعه ی مدل GMCR است تا بر اساس آن ها، گزینه های تأثیرگذار و وضعیت‌های تعادلی مطلوب بازی انتخاب گردد. در ادامه معیارهای استخراج گزینه‌های تأثیرگذار، ارائه می‌شود.

معیار (۱) – کیفیت ارزش گزینه‌ی بازیگر: برابر است با تقسیم ارزش گزینه‌ی بازیگر به مجموع ارزش سایر گزینه‌های بازیگر ضرب‌در ۱۰۰.

معیار (۲) – کیفیت شناخت گزینه‌ی بازیگر: برابر است با تقسیم تعداد الگوهای حذف وضعیت‌های غیرممکن بازی شامل گزینه بازیگر به تعداد کل الگوهای حذف وضعیت‌های غیرممکن بازی ضرب‌در صد

معیار (۳) – کیفیت مشارکت گزینه‌ی بازیگر: برابر است با تقسیم تعداد وضعیت‌های ممکن بازی شامل گزینه‌ی بازیگر به‌کل وضعیت‌های ممکن بازی، ضرب‌در صد.

معیار (۴) – کیفیت شکست گزینه‌ی بازیگر: برابر است با تقسیم تعداد وضعیت‌های ممکن بازی شامل گزینه‌ی بازیگر و با عایدی کمتر نسبت به رقیب به‌کل وضعیت‌های ممکن بازی با عایدی کمتر بازیگر، ضرب‌در صد

معیار (۵) – کیفیت برابری گزینه‌ی بازیگر: برابر است با تقسیم تعداد وضعیت‌های ممکن بازی شامل گزینه‌ی بازیگر و با عایدی برابر با رقیب به‌کل وضعیت‌های ممکن بازی با عایدی برابر بازیگران، ضرب‌در صد

معیار (۶) – کیفیت برتری گزینه‌ی بازیگر: برابر است با تقسیم تعداد وضعیت‌های ممکن بازی شامل گزینه‌ی بازیگر و با عایدی بیشتر نسبت به رقیب به‌کل وضعیت‌های ممکن بازی با عایدی بیشتر بازیگر، ضرب‌در صد

معیار (۷) – کیفیت پایداری گزینه‌ی بازیگر: برابر است با تقسیم تعداد وضعیت‌های پایداری شامل گزینه‌ی بازیگر نسبت به‌کل وضعیت‌های پایداری بازیگر، ضرب‌در صد

معیار (۸) – کیفیت تعادل Nash گزینه‌ی بازیگر: برابر است با تقسیم تعداد وضعیت‌های تعادل Nash شامل گزینه‌ی بازیگر نسبت به‌کل وضعیت‌های تعادلی نش بازی، ضرب‌در صد

معیار (۹) – کیفیت تعادل SEQ گزینه‌ی بازیگر: برابر است با تقسیم تعداد وضعیت‌های تعادل SEQ شامل گزینه‌ی بازیگر نسبت به‌کل وضعیت‌های تعادلی SEQ بازی، ضرب‌در صد

معیار (۱۰) – کیفیت تعادل GMR گزینه‌ی بازیگر: برابر است با تقسیم تعداد وضعیت‌های تعادل GMR شامل گزینه‌ی بازیگر نسبت به‌کل وضعیت‌های تعادلی GMR بازی، ضرب‌در صد

معیار (۱۱) – کیفیت تعادل SMR گزینه‌ی بازیگر: برابر است با تقسیم تعداد وضعیت‌های تعادل SMR شامل گزینه‌ی بازیگر نسبت به‌کل وضعیت‌های تعادلی SMR بازی، ضرب‌در صد

معیار (۱۲) - کیفیت تعادلی پایه گزینه‌ی بازیگر: برابر است با میانگین معیارهای ۸ تا ۱۱

معیار (۱۳) - کیفیت تعادلی مطلوب (BestEQ) گزینه‌ی بازیگر: برابر است با تقسیم تعداد وضعیت‌های تعادلی مطلوب شامل گزینه‌ی بازیگر نسبت به‌کل وضعیت‌های تعادلی مطلوب ضرب‌در صد

وضعیت‌های تعادلی مطلوب در این مقاله با توجه به ویژگی‌های بدافزارها و فضای سایبری، وضعیت‌هایی است که دارای شرایط وضعیت‌های تعادلی GMR و SMR و از گزینه‌های تأثیرگذار در آن استفاده شده باشد. در معیارهای بیان شده در این مقاله، ابتدا مقادیر معیارها برای هرکدام از گزینه‌های بازیگران محاسبه شده و سپس حداکثر مقدار هر معیار بین همه‌ی گزینه‌های هر بازیگر، استخراج می‌گردد؛ گزینه‌هایی از هر بازیگر که مقدار معیار مدنظر برای آن گزینه از نودوپنج درصد حداکثر مقدار آن معیار بیشتر باشد به‌عنوان گزینه‌های برتر آن معیار برای بازیگر انتخاب می‌شوند. حد آستانه‌ی نودوپنج درصد، بر اساس نتایج مدل‌سازی و شبیه‌سازی متنوع در این مقاله، به‌عنوان حد آستانه‌ی مناسب تعیین شده و با این حد آستانه، درصد قابل قبولی از گزینه‌های بازیگران به‌عنوان گزینه‌های تأثیرگذار انتخاب می‌شوند و بر مبنای آن‌ها، تعداد مناسبی وضعیت‌های تعادلی مطلوب استخراج می‌شود. درصورتی‌که حد آستانه‌ی صددرصدی (حداکثر مقدار معیار) مدنظر باشد؛ برای هر بازیگر در هر معیار فقط یک گزینه به‌عنوان گزینه‌ی تأثیرگذار لحاظ می‌گردد و سایر گزینه‌های مشابه به گزینه‌ی تأثیرگذار حذف می‌شوند. اگر حد آستانه‌ی کمتر در نظر گرفته شود (مثلاً ۷۰٪) و ویژگی‌های پارامتری و شناخت بازیگران از گزینه‌ها شبیه به هم باشند؛ گزینه‌های تأثیرگذار زیاد شده واگرایی نتایج به وجود می‌آید و گزینه‌های تأثیرگذار واقعی به‌صورت مناسب استخراج نمی‌شود.

۳- ارزیابی چارچوب پیشنهادی

در این بخش مشخصات بازی، مدل‌سازی و شبیه‌سازی و تحلیل مطالعه موردی ارائه می‌گردد.

۳-۱- گزینه‌های بازیگران و شرایط بهره‌برداری آن‌ها

در فرآیند مدل‌سازی و تحلیل بازی‌ها، جهت تکرار کمتر واژه‌های اقدامات و فعالیت‌های بازیگران، از عنوان گزینه‌های بازیگران، استفاده می‌شود. در این بخش گزینه‌های بازیگران در سطح اقدام و فعالیت و مقادیر پارامترهای آن‌ها ارائه می‌گردد. شرایط بهره‌برداری بازیگران در این ارزیابی به‌صورت مفروض در نظر گرفته شده و ظرفیت و توانمندی بازیگران جهت اجرای گزینه‌ها بر مبنای شرایط بهره‌برداری بازیگران محاسبه می‌گردد.

۳-۱-۱- شرایط بازیگران جهت بهره‌برداری از گزینه‌ها

قابلیت و توانمندی بهره‌برداری بازیگران جهت اجرای گزینه‌ها در بازی‌های این مطالعه موردی که به‌صورت مفروض در نظر گرفته‌شده، به شرح زیر است:

- مهاجم: منابع مالی (متوسط)، نیروی انسانی متخصص (خوب)، سامانه‌های نرم‌افزاری پایه بومی (خوب)، تجهیزات زیرساختی بومی (متوسط)، دسترسی به دانش و فناوری (خوب)
- مدافع: منابع مالی (متوسط)، نیروی انسانی متخصص (خوب)، سامانه‌های نرم‌افزاری پایه بومی (خوب)، تجهیزات زیرساختی بومی (ضعیف)، دسترسی به دانش و فناوری (متوسط)

با بهره‌گیری از شرایط بازیگران و پارامترهای گزینه‌های آن‌ها، ظرفیت بهره‌برداری از هر گزینه برای هر بازیگر و ارزش آن‌ها در هر بازی بر اساس رابطه‌ی (۶) محاسبه می‌گردد.

۳-۱-۲- گزینه‌های بازیگران در سطح اقدام

گزینه‌های مهاجم و مدافع در سطح اقدام و مقادیر پارامترهای مرتبط به آن‌ها، مطابق با جدول (۶) و (۷) از پیوست مقاله، ارائه شده است. در جدول (۶)، شناسه‌ی راهکارهای و اقدامات دفاعی (گزینه‌های مدافع در سطح) مرتبط با هر اقدام تهاجمی نیز تعیین گردیده است. اقدامات و پارامترهای بازیگران، با روش تحقیقی و اکتشافی از منابع علمی شامل گزارش های امنیتی، مقالات، بررسی مجموعه داده و تحلیل بدافزارهای مرتبط و نتایج تجربی و آزمایشگاهی محققان و خبرگان حوزه ی بدافزار، مبتنی بر جداول (۳) و (۴)، استخراج گردیده‌اند. علاوه‌بر اینکه اقدامات و فعالیت های بازیگران و پارامترهای آن ها از منابع علمی معتبر تهیه و تدوین شده اند؛ جمعی از پژوهشگران و خبرگان حوزه ی بدافزار به‌صورت خبره‌سنجی ارزیابی و تأیید کرده‌اند. نحوه‌ی خبره‌سنجی به این صورت بود که ابتدا گزینه‌های بازیگران و مقادیر پارامترهای آن ها از منابع علمی استخراج شد و سپس نتایج در اختیار خبرگان قرار گرفت. جمع‌بندی نتایج خبره‌سنجی در قالب جدول این مقاله ارائه (جداول (۳) و (۴)) شد. تجمیع سازی و انتزاع‌سازی اقدامات و تبدیل آن‌ها به فعالیت‌ها بر اساس رابطه (۵)، انجام شده است. در این مطالعه‌ی موردی، تعداد اقدامات مهاجم و مدافع به ترتیب ۲۵ و ۲۷ مورد، در نظر گرفته شده‌است. برای مدافع و مهاجم هرکدام ۵ پارامتر لحاظ شد. از بین پارامترها، چهار پارامترِ پیچیدگی، تاب‌آوری، سطح اثربخشی و فراوانی به‌کارگیری، مربوط به اقدام و قابلیت بهره‌برداری به شرایط بهره‌بردار (مهاجم و مدافع) وابسته است.

۳-۱-۳- گزینه‌های بازیگران در سطح فعالیت

در این مطالعه‌ی موردی، گزینه‌های مهاجم (جدول (۸)) و مدافع (جدول (۹)) به‌ترتیب ۱۲ و ۱۲ مورد، در نظر گرفته شده و پارامترهای آن‌ها شبیه به پارامترهای گزینه‌ها در سطح اقدام است. پارامترهای گزینه‌ها در سطح فعالیت بر اساس پارامترهای گزینه‌های بازیگران در سطح اقدام مطابق با رابطه (۵) محاسبه می‌شوند.

جدول (۸): گزینه‌های مهاجم و ویژگی‌های آن‌ها در مطالعه موردی

ردیف	عنوان گزینه
۱	پردازش بلوک اطلاعات پردازنده‌ها PEB جهت تشخیص اشکال‌زدا
۲	جست‌وجو و تشخیص نقاط شکست سخت‌افزاری و نرم‌افزار
۳	استخراج شواهد محیط اشکال‌زدا با بهره‌گیری از مصنوعات سیستمی
۴	کاوش شیء NTQuery جهت استخراج شواهد اشکال‌زدا
۵	کنترل والد پردازه‌ها با بررسی شناسه‌ی پردازه و ارتباط با پردازه‌های شناخته‌شده‌ی سیستم‌عامل و اشکال‌زداها
۶	تشخیص محیط اشکال‌زدا مبتنی بر زمان
۷	تله‌گذاری (دستوراتی که باعث فراخوانی اشکال‌زدا شده و اجرای آن در پردازنده واقعی و محیط اشکال‌زدا متفاوت است)
۸	بهره‌گیری از آسیب‌پذیری اشکال‌زداهای خاص
۹	شناسایی محیط‌های جعبه‌ی شن و نظارتی با جمع‌آوری نشانه‌ها
۱۰	شناسایی محیط‌های جعبه‌ی شن و نظارتی با بررسی آزمون تورینگ معکوس
۱۱	جست‌وجو و تشخیص هدفمند محیط‌های تحلیل پویایی هدف
۱۲	تشخیص هدفمند محیط اشکال‌زدا و فعال‌سازی کد مخرب متناسب با شرایط و نشانه‌های محیطی

گزینه‌های مهاجم، متناسب با راهکارهای تشخیص محیط‌های تحلیل و اشکال‌زدایی هدف بر اساس شواهد شناسایی‌شده وابسته به محیط تعریف شده است. گزینه‌های مدافع متناسب با گزینه‌های مهاجم و بر اساس راهکارهای مخفی‌سازی شواهد محیط‌های تحلیلگر و اشکال‌زدا، تعیین گردیده است.

جدول (۹): گزینه‌های مدافع و ویژگی‌های آن‌ها در مطالعه موردی

ردیف	عنوان گزینه
۱	مخفی کردن شواهد محیط اشکال‌زدا با تنظیم PEB اشکال‌زدا
۲	تنظیم نقطه‌های شکست در اشکال‌زدا در مراحل اجرای فرآیند تحلیل
۳	تصادفی‌سازی متغیرها و عنوان‌های برنامه‌ها جهت پنهان‌سازی شواهد
۴	تغییر وضعیت پردازه‌ها بعد از فراخوانی توابع مرتبط یا جلوگیری از اجرای توابع کاویدن اشیاء
۵	انسداد پیمایش (پردازنده) جهت عدم شناسایی والد محیط اشکال‌زدا
۶	جلوگیری از تشخیص محیط اشکال‌زدا مبتنی بر زمان اجرای حمله - نصب افزونه‌های هسته برای جلوگیری از افزایش سطح دسترسی
۷	جلوگیری از تله‌گذاری با استفاده از تنظیم نقطه‌ی دست‌یابی کنترل‌کننده‌های استثناها و تبدیل نقطه‌ی دست‌یابی تک‌مرحله‌ای به حالت خودکار
۸	جلوگیری از شناسایی اشکال‌زداهای مشهور با بهره‌گیری از تکنیک‌های وصله‌ی آسیب‌پذیری و تنظیم نقطه‌ی شکست
۹	جلوگیری از شناسایی محیط‌های جعبه‌ی شن با جمع‌آوری نشانه‌ها
۱۰	جلوگیری از شناسایی محیط‌های جعبه‌ی شن با بهره‌گیری از تکنیک آزمون تورینگ معکوس
۱۱	جلوگیری از شناسایی هدفمند محیط‌های جعبه‌ی شن
۱۲	جلوگیری از شناسایی هدفمند محیط‌های اشکال‌زدا

۳-۲- مشخصات بازی‌های مطالعه‌ی موردی

در جدول (۱۰)، مشخصات بازی‌های مطالعه‌ی موردی ارائه شده و بازی (۱) به‌عنوان بازی پایه این مطالعه موردی قرار داده شد. شناخت بازیگران نسبت به اقدامات یکدیگر در همه‌ی بازی‌ها، در قالب ستون «گزینه مقابله‌ای» لحاظ شده است.

جدول (۱۰): مشخصات بازی‌های مطالعه‌ی موردی

شماره گزینه	بازی ۱			بازی ۲			بازی ۳			
	مهاجم		مدافع	مهاجم		مدافع	مهاجم		مدافع	
	ارزش گزینه	گزینه مقابله‌ای	ارزش گزینه	ارزش گزینه	گزینه مقابله‌ای	ارزش گزینه	گزینه مقابله‌ای	ارزش گزینه	ارزش گزینه	گزینه مقابله‌ای
۱	۲۳	۱	۱۹	۱۹	۱	۲۲	۱	۱۹	۲۲	۱
۲	۳۱	۲	۲۸	۳۱	۲	۱۸	۲	۳۱	۱۸	
۳	۲۱	۹ ،۳	۲۰	۱۶	۳	۲۷	۳	۱۶	۲۷	۳
۴	۱۶	۴	۱۷	۲۱	۴	۲۴	۴	۲۱	۲۴	
۵	۲۶		۱۹	۲۱		۲۷		۲۱	۲۷	
۶	۲۸	۶	۳۰	۲۳	۶	۲۰	۶	۲۳	۲۰	۵
۷	۲۴	۷ ،۳	۲۶	۲۴	۷	۲۱	۷	۲۴	۲۱	۷
۸	۱۹	۸	۲۰	۲۷		۲۸	۸	۲۷	۲۸	
۹	۲۰	۱۰ ،۹	۱۹	۲۸	۸ ،۳	۳۰	۹	۲۸	۳۰	۹ ،۳
۱۰	۲۸	۱۱ ،۱۰	۲۷	۲۲		۲۹	۱۰	۲۲	۲۹	
۱۱	۲۳	۱۲ ،۱۱	۲۶	۲۸	۱۲ ،۱۱	۱۵	۱۱	۲۸	۱۵	۱۱
۱۲	۲۸	۱۲	۲۵	۳۴		۲۶	۱۲	۳۴	۲۶	۱۲

در جدول (۱۰)، تغییرات بازی (۲) نسبت به بازی (۱)، تغییر در مقادیر پارامترهای گزینه‌های بازیگران و متناسب با آن تغییر ارزش گزینه‌ی بازیگران است. در بازی (۳)، در میزان شناخت اقدام مقابله‌ای رقیب، نسبت به بازی (۲)، تغییر ایجاد شده است. هدف از تغییر در پارامترهای گزینه‌های بازیگران و شناخت آن‌ها و ایجاد بازی‌های متنوع، فراهم شرایط عدم قطعیت به‌دلیل کامل نبودن اطلاعات بازیگران به شرایط بازی و ارزیابی مطالعه موردی به‌صورت سناریومحور است. ارزش گزینه بازیگر از رابطه (۳) محاسبه می‌گردد.

الگوهای حذف وضعیت‌های غیرممکن بازی‌ها مطابق با جدول (۱۱)، بر اساس محدودیت‌های «استفاده از حداقل یکی از اقدامات»، «وابستگی اقدام بازیگران» و «نبود قابلیت پیاده‌سازی و اجرا از طریق بازیگر» تعیین شده است. در هیچ‌کدام از بازی‌ها الگویی مبتنی بر «نبود قابلیت و پیاده‌سازی اجرای گزینه» نبوده یعنی اینکه همه گزینه‌ها شرایط اجراشدن از طریق بازیگران را دارند.

جدول (۱۱): الگوهای حذف وضعیت‌های غیرممکن بازی‌ها

ردیف	بازی / عنوان الگو	بازی ۱		بازی ۲		بازی ۳	
		مهاجم	مدافع	مهاجم	مدافع	مهاجم	مدافع
۱	استفاده از حداقل یکی از گزینه‌ها	۱	۱	۱	۱	۱	۱
۲	وابستگی گزینه‌ها	۱۶	۹	۹	۹	۹	۸

در جدول (۱۲)، خلاصه مشخصات بازیگران در بازی‌های این مطالعه‌ی موردی، بیان گردیده است؛ تعداد اقدامات بازیگران و پارامترهای آن‌ها، وابستگی اقدام و الگوهای حذف وضعیت غیرممکن بازی، وضعیت‌های ممکن بازی‌ها از مشخصاتی است که بر اساس مراحل مدل‌سازی، ارائه شده است. در جدول (۱۲) عنوان ویژگی مرتبط با شماره‌ی ویژگی، شامل (۱) تعداد گزینه‌های بازیگر، (۲) تعداد پارامترهای گزینه‌ها، (۳) میانگین پارامترهای گزینه‌ها، (۴) تعداد پارامترهای بهره‌بردار، (۵) میانگین

پارامترهای بهره‌بردار (۶) تعداد الگوهای حذف وضعیت‌های غیرممکن، (۷) تعداد کل وضعیت‌های بازی‌ها، (۸) تعداد وضعیت‌های غیرممکن بازی‌ها، (۹) تعداد وضعیت‌های ممکن بازی‌ها، (۱۰) درصد کاهش تعداد وضعیت‌های بازی، (۱۱) تعداد تعادل SEQ، (۱۲) تعداد تعادل GMR، (۱۳) تعداد تعادل SMR، (۱۴) تعداد تعادل Best هستند. در جدول (۱۲)، ویژگی‌های شماره (۱۱) تا (۱۵) بیان‌کننده‌ی وضعیت‌های تعادلی سه بازی مطالعه‌ی موردی به تفکیک است. حداقل تعداد وضعیت‌های تعادلی مربوط به بازی شماره (۳) و وضعیت‌های تعادلی SMR و BestEQ است. با اعمال محدودیت‌های بیشتری به بازی‌ها، ضمن کاهش تعداد وضعیت‌های ممکن بازی، تعداد وضعیت‌های تعادلی نیز کاهش می‌یابد.

جدول (۱۲): مشخصات و شرایط مدل‌سازی بازی‌های مطالعه موردی

بازی‌ها / ویژگی	بازی ۱		بازی ۲		بازی ۳	
	مهاجم	مدافع	مهاجم	مدافع	مهاجم	مدافع
۱	۱۲	۱۲	۱۲	۱۲	۱۲	۱۲
۲	۴	۴	۴	۴	۴	۴
۳	۴/۷۲	۴/۵۵	۴/۸۱	۴/۷	۴/۸۱	۴/۷
۴	۱	۱	۱	۱	۱	۱
۵	۵/۰۴	۴/۸۲	۵/۱۶	۵/۰۴	۵/۱۶	۵/۰۴
۶	۱۷	۱۰	۱۰	۱۰	۱۰	۹
۷	۱۶،۷۷۷،۲۱۶		۱۶،۷۷۷،۲۱۶		۱۶،۷۷۷،۲۱۶	
۸	۱،۷۶۹،۱۸۴		۱۶،۷۳۵،۷۹۰		۱۶،۷۱۵،۰۸۶	
۹	۸۰۳۲		۴۱۴۲۶		۶۲۱۳۰	
۱۰	۹۹/۹۵		۹۹/۷۶		۹۹/۶۳	
۱۱	۵۳		۱۱۶		۳۲	
۱۲	۳۸۴۸		۳۵۵۲۸		۵۹۵۲۵	
۱۳	۲۷۹		۱۱۹۱		۲۳۶۹	
۱۴	۶۶		۱۴۰		۳۲	
۱۵	۶۳		۱۴۰		۳۲	

۳-۳- بحث و نتایج

جدول (۱۳) و (۱۴)، به ترتیب نتایج تحلیل سه بازی مطالعه‌ی موردی جهت استخراج گزینه‌های تأثیرگذار مهاجم و مدافع را نشان می‌دهد. هر خانه از جداول (۱۳) و (۱۴) بیان‌کننده، تعداد بار انتخاب یک گزینه از طریق یک معیار به‌عنوان گزینه‌ی تأثیرگذار در هر سه بازی بوده است.

در معیار (۱۱) جدول (۱۴)، در سه بار بازی این مطالعه‌ی موردی، یک‌بار گزینه‌ی (۵) و دو بار گزینه‌ی (۹) به‌عنوان گزینه‌های تأثیرگذار مدافع انتخاب شده‌اند. بر اساس جدول (۱۳)، گزینه (۲)، (۵) و (۸) مهاجم و مطابق با جدول (۱۴) گزینه (۶) و (۱۰) مدافع به‌عنوان گزینه‌های تأثیرگذار مطالعه موردی معرفی شده است. بر اساس معیار شماره (۱۳)، جداول (۱۳) و (۱۴)، گزینه‌های تأثیرگذار مهاجم تمرکز بر گزینه‌ی مشخصی نبوده اما در گزینه‌های مدافع، تمرکز بیشتر بر گزینه شماره (۱۰) است. گزینه‌های تأثیرگذار بازی (۱) شامل گزینه (۵) مهاجم و گزینه (۶) مدافع، گزینه‌های تأثیرگذار بازی (۲) شامل گزینه (۸) مهاجم و گزینه (۱۰) مدافع و گزینه‌های تأثیرگذار بازی (۳) شامل گزینه‌ی (۲) مهاجم و گزینه‌ی (۱۰) مدافع بوده و در جدول (۱۵) معیارهای مؤثر در انتخاب گزینه‌های تأثیرگذار بازی‌ها به تفکیک ارائه شده است.

جدول (۱۳): نتایج بازی‌ها در استخراج گزینه‌های تأثیرگذار مهاجم

معیارها	گزینه‌های مهاجم												میانگین مشارکت (درصد)
	۱	۲	۳	۴	۵	۶	۷	۸	۹	۱۰	۱۱	۱۲	
۱	۰	۲	۰	۰	۰	۰	۰	۰	۰	۰	۰	۲	۱۷
۲	۰	۰	۳	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰
۳	۰	۱	۱	۰	۱	۰	۱	۰	۰	۰	۰	۱	۶۷
۴	۰	۰	۲	۱	۰	۰	۰	۰	۰	۰	۰	۰	۰
۵	۰	۱	۲	۱	۱	۰	۱	۰	۰	۰	۰	۱	۶۷
۶	۱	۲	۰	۰	۰	۰	۰	۰	۰	۰	۲	۱	۱۷
۷	۰	۱	۰	۰	۱	۰	۰	۱	۰	۰	۰	۰	۱۰۰
۸	۰	۱	۰	۰	۰	۱	۰	۱	۰	۰	۰	۰	۶۷
۹	۰	۰	۱	۰	۱	۰	۲	۱	۰	۰	۰	۰	۶۷
۱۰	۰	۱	۰	۰	۱	۰	۱	۰	۰	۰	۰	۰	۶۷
۱۱	۰	۱	۰	۰	۰	۱	۰	۱	۰	۰	۰	۰	۶۷
۱۲	۰	۱	۱	۰	۱	۰	۱	۱	۰	۰	۰	۰	۱۰۰
۱۳	۰	۱	۰	۰	۱	۰	۰	۱	۰	۰	۰	۰	۵۰

جدول (۱۴): نتایج بازی‌ها در استخراج گزینه‌های تأثیرگذار در یک نگاه

معیارها	گزینه‌های مدافع													میانگین مشارکت گزینه‌های بازیگران (درصد)
	۱	۲	۳	۴	۵	۶	۷	۸	۹	۱۰	۱۱	۱۲	میانگین مشارکت	
۱	۰	۰	۰	۰	۰	۱	۰	۰	۲	۰	۰	۰	۵۰	۳۳
۲	۳	۲	۳	۲	۰	۲	۰	۱	۳	۳	۳	۳	۵۸	۲۹
۳	۰	۱	۲	۱	۰	۱	۰	۱	۰	۳	۰	۱	۸۳	۷۵
۴	۱	۲	۰	۰	۰	۰	۰	۰	۰	۰	۲	۱	۰	۰
۵	۰	۱	۱	۰	۰	۱۰۰	۰	۱	۰	۲	۰	۱	۱۰۰	۸۳
۶	۰	۰	۲	۰	۰	۱	۰	۰	۰	۱	۰	۰	۱۰۰	۵۸
۷	۰	۰	۰	۰	۰	۱	۰	۰	۰	۲	۰	۰	۱۰۰	۱۰۰
۸	۰	۰	۰	۰	۰	۱	۰	۰	۰	۲	۰	۰	۱۰۰	۸۳
۹	۰	۱	۱	۱	۰	۱	۰	۲	۰	۲	۰	۱	۱۰۰	۸۳
۱۰	۰	۰	۱	۰	۰	۱	۲	۰	۰	۱	۰	۰	۱۰۰	۸۳
۱۱	۰	۰	۰	۰	۰	۱	۰	۰	۰	۲	۰	۰	۱۰۰	۸۳
۱۲	۰	۰	۱	۰	۰	۰	۰	۰	۰	۳	۰	۰	۳۳	۶۷
۱۳	۰	۰	۰	۰	۰	۱	۰	۰	۰	۲	۰	۰	۷۱	۶۰

در جدول (۱۵)، خانه‌های مرتبط با معیار (۱۲) و ستون‌های مهاجم و مدافع و تجمیعی بازی (۳) بیان‌کننده این موضوع است که گزینه‌های تأثیرگذاری استخراجی مهاجم ۱۰۰ درصد در گزینه‌های نهایی استخراج‌شده برای مهاجم تأثیرگذار بوده است؛ این شرایط برای مدافع ۵۰ درصد بوده یعنی ۵۰ درصد گزینه‌های انتخابی از سوی این معیار در گزینه‌های تأثیرگذار نهایی مدافع نقش داشته‌اند و تجمیعی مهاجم و مدافع با در نظر گرفتن همه‌ی گزینه‌ها، ۶۷ درصد محاسبه شده است.

جدول (۱۵): معیارهای مؤثر در گزینه‌های تأثیرگذار بازی‌ها

معیارها	بازی ۱			بازی ۲			بازی ۳		
	مهاجم	مدافع	تجمیعی	مهاجم	مدافع	تجمیعی	مهاجم	مدافع	تجمیعی
۱	۰	۱۰۰	۵۰	۰	۰	۰	۰	۰	۰
۲	۰	۰	۰	۰	۱۱	۱۰	۰	۱۱	۱۰
۳	۰	۰	۰	۰	۳۳	۲۰	۰	۲۵	۲۰
۴	۰	۰	۰	۰	۰	۰	۰	۰	۰
۵	۰	۳۳	۱۷	۰	۱۰۰	۳۳	۰	۰	۰
۶	۰	۵۰	۲۵	۰	۰	۰	۰	۰	۰
۷	۱۰۰	۱۰۰	۱۰۰	۱۰۰	۱۰۰	۱۰۰	۱۰۰	۱۰۰	۱۰۰
۸	۰	۱۰۰	۵۰	۱۰۰	۱۰۰	۱۰۰	۱۰۰	۱۰۰	۱۰۰
۹	۰	۰	۰	۰	۰	۰	۰	۲۵	۱۷
۱۰	۱۰۰	۰	۵۰	۰	۰	۰	۱۰۰	۰	۲۵
۱۱	۰	۱۰۰	۵۰	۱۰۰	۱۰۰	۱۰۰	۱۰۰	۱۰۰	۱۰۰
۱۲	۱۰۰	۰	۵۰	۳۳	۱۰۰	۵۰	۱۰۰	۵۰	۶۷
۱۳	۱۰۰	۱۰۰	۱۰۰	۱۰۰	۱۰۰	۱۰۰	۱۰۰	۱۰۰	۱۰۰

مطابق با جداول (۱۳)، (۱۴) و (۱۵)، تحلیل میزان مشارکت گزینه‌های بازیگران بر اساس پارامترهای مؤثر در استخراج گزینه‌های تأثیرگذار بازیگران، به شرح زیر است:

- معیار شماره (۱) و (۲) مرتبط با ارزش و میزان شناخت گزینه‌های بازیگران، به ترتیب مشارکت ۳۳ و ۲۷ درصدی داشته‌اند و این میزان مشارکت، نشان‌دهنده‌ی قوی و قابل قبول بودن معیارها نیست.
- معیار شماره‌ی (۳) مرتبط با مشارکت گزینه‌های بازیگران در بازی، مشارکت ۷۵ درصدی در استخراج گزینه‌های تأثیرگذار بازی‌ها داشته است.
- معیار (۴) مرتبط با کیفیت مشارکت گزینه‌های بازیگر در وضعیت‌های بازی با عایدی کمتر بازیگران، تأثیری در استخراج گزینه‌های تأثیرگذار نداشته و این موضوع به دلیل عدم تمایل بازیگران به حضور در وضعیت شکست و ناپایدار بودن در چنین وضعیت‌هایی، منطقی و قابل پیش‌بینی بوده است.
- معیار (۵) مرتبط با کیفیت مشارکت گزینه‌های بازیگر در وضعیت‌های بازی با عایدی برابر بازیگران، تأثیر ۸۳ درصدی در استخراج گزینه‌های تأثیرگذار بازی‌ها داشته و این موضوع با منطق پایداری و تعادل بازیگران در وضعیت‌های بازی همخوانی دارد.
- معیار (۶) مرتبط با کیفیت مشارکت گزینه‌های بازیگر در وضعیت‌های بازی با عایدی بیشتر بازیگران، تأثیر ۵۸

درصدی در استخراج گزینه‌های تأثیرگذار بازی‌ها داشته و مقدار این معیار در اقدام بازیگر مدافع ۱۰۰ درصد بوده است.

- معیار (۷) مرتبط با کیفیت پایداری گزینه‌های بازیگر، مشارکت ۱۰۰ درصدی در تعیین اقدام تأثیرگذار داشته‌اند که بیان‌کننده‌ی موضوع است که همه‌ی وضعیت‌های شامل گزینه‌های تأثیرگذاری بازیگران مطابق با منطق نش، وضعیت تعادل بوده‌اند.
- میانگین معیارهای مرتبط با وضعیت تعادلی شامل معیارهای (۷) تا (۱۲) تأثیر ۸۹ درصدی داشته و نشان‌دهنده‌ی این است که گزینه‌های تأثیرگذار استخراجی بازی به‌طور میانگین در ۸۹ درصد وضعیت‌های مرتبط با تعادلی پایه مشارکت داشته‌اند.
- معیار (۱۳) مرتبط با کیفیت تعادل مطلوب تأثیر ۱۰۰ درصدی در استخراج گزینه‌های تأثیرگذار بازی داشته است.

بر اساس نتایج مطالعه‌ی موردی و ارتباط بین گزینه‌های بازیگران در سطح فعالیت و اقدام، گزینه‌های تأثیرگذار بازیگران در سطح فعالیت و اقدام در ادامه تشریح می‌شود.

گزینه‌های مهاجم در سطح فعالیت و اقدام:

✓ **فعالیت (۲)**- جست‌وجو و تشخیص نقاط شکست سخت‌افزاری و نرم‌افزار

- **اقدام**- بررسی وجود نقاط شکست نرم‌افزاری Self-integrity-check instruction, 3 INT spot to Self-scan
- **اقدام**- تشخیص اجرا در محیط اشکال‌زدا با بررسی رجیستر DR پردازنده به‌وسیله تابع مربوطه جهت تشخیص نقاط شکست سخت‌افزاری

✓ **فعالیت (۵)**- کنترل والد پردازه‌ها با بررسی شناسه‌ی پردازه و ارتباط با پردازه‌های شناخته‌شده سیستم‌عامل و اشکال‌زداها

- **اقدام** – توابع مربوط به بررسی و ارزیابی شناسه پردازه والد GetCurrentProcessId(),CreateToolhelp32Snapshot(), Process32First()+Process32Next()

فعالیت (۸)-بهره‌گیری از آسیب‌پذیری اشکال‌زداهای خاص

- **اقدام** – بهره‌گیری از آسیب‌پذیری اشکال‌زدا OllyDBG با استفاده از خطای قالب‌بندی رشته
- **اقدام** – بهره‌گیری از آسیب‌پذیری اشکال‌زدا در برابر حمله‌ی منع خدمت مبتنی بر توابع مربوط 09 و 0x83

گزینه‌های مدافع در سطح فعالیت و اقدام:

فعالیت (۶)-جلوگیری از تشخیص محیط اشکال‌زدا مبتنی بر زمان اجرای حمله - نصب افزونه‌های هسته برای جلوگیری از افزایش سطح دسترسی

- **اقدام –** وصله‌ی هسته سیستم‌عامل برای جلوگیری از دسترسی به ساختمان داده rdtsc خارج از سطح دسترسی
- **اقدام** – حفظ و مدیریت منبع زمان وفاداری بالا Maintain source time high-fidelity
- **اقدام –** قلاب‌اندازی یا مسدودسازی فراخوانی توابع سیستمی مرتبط با بررسی زمان (time-checking APIs)
- NTP) (e.g. source time external Query

فعالیت (۱۰)-جلوگیری از شناسایی محیط‌های جعبه‌ی شن با بهره‌گیری از تکنیک آزمون تورینگ معکوس توسط مهاجم

- **اقدام** – شبیه‌سازی رفتارهای تعاملی کاربر با محیط تحلیل به‌وسیله‌ی تنظیم دستگاه‌های ورودی Simulation Digital
- **اقدام** – تشخیص و غیرفعال کردن دستورات شناسایی تعاملات کاربر توسط بدافزار با استفاده از تکنیک‌های اکتشاف مسیر exploration path

هرکدام از وضعیت‌های تعادلی و غیرتعادلی بازی‌های این مطالعه‌ی موردی، متناسب با بهره‌گیری بازیگران از گزینه‌های خود در آن وضعیت، قابل تفسیر است. به‌عنوان نمونه، وضعیت شماره (۸۳۶) بازی (۱) مطالعه موردی، بر اساس منطق تعادل Nash، وضعیت تعادلی نبوده ولی بر اساس منطق‌های SEQ، GMR، SMR و BestEQ به دلیل مجازات مدافع از طریق مهاجم وضعیت تعادلی است. در این وضعیت مهاجم از اقدام (۲)، (۵) و (۸) مدافع از اقدام (۲)، (۴)، (۵)، (۸) و (۱۰) خود استفاده می‌نماید.

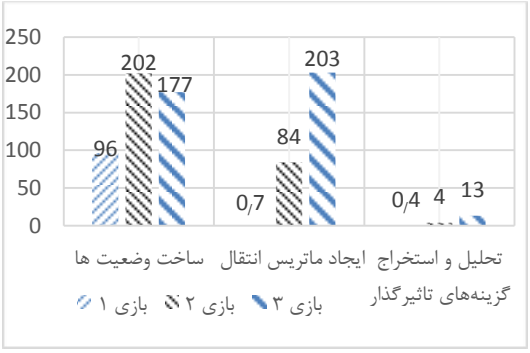
۳-۴- تحلیل حساسیت بازی

یکی از روش‌های تعیین قابل‌اعتماد بودن نتایج، تحلیل حساسیت بازی است؛ بدین‌صورت که با تغییر جزئی اولویت‌های بازیگران نباید نتایج مدل‌سازی و وضعیت‌های تعادل به‌صورت گسترده‌ای تغییر کند. در این مقاله با تغییرات مناسب در پارامترهای گزینه‌های بازیگران و شناخت بازیگر از گزینه‌های مقابله‌ای رقیب، علاوه بر بازی پایه، دو بازی جدید و وابسته به بازی پایه ایجاد شد. هرکدام از بازی‌ها به تفکیک، مدل‌سازی و تحلیل شد و گزینه‌های تأثیرگذار و وضعیت تعادلی مطلوب بازی‌ها استخراج گردید و سپس با تجمیع نتایج بازی‌ها،

گزینه‌های تأثیرگذار نهایی بازیگران تعیین شد. علاوه بر سه بازی، بازی‌هایی با تغییرات جزئی نیز مدل‌سازی و شبیه‌سازی شد، اما به دلیل این‌که تأثیراتی خاصی در گزینه‌های تأثیرگذار نهایی و وضعیت تعادلی مطلوب نداشتند، نتایج آن‌ها در مقاله ارائه نگردید. با توضیحات عنوان‌شده، به دلیل این‌که گزینه‌های تأثیرگذار استخراجی و وضعیت‌های تعادلی مطالعه‌ی موردی، برمبنای سه بازی متفاوت و مرتبط است و وضعیت‌های تعادلی بر اساس ۵ منطق تعادلی (BestEQ SMR, GMR, SEQ, Nash,) است، نتایج قابل اعتماد و پایداری هستند.

۳-۵- زمان شبیه‌سازی و تحلیل بازی‌ها

در شکل (۵)، نمودار زمان مدل‌سازی و شبیه‌سازی بازی‌های مطالعه موردی برحسب ثانیه، در سه بخش، ارائه شده است.



شکل (۵): نمودار زمان مدل‌سازی و تحلیل بازی‌ها

۱- زمان ساخت وضعیت‌های ممکن بازی و ویژگی‌های آن شامل استخراج حالت گزینه‌ای وضعیت‌ها (گزینه‌های به‌کارگرفته‌شده در وضعیت)، عایدی و ترجیحات بازیگران در وضعیت‌های ممکن بازی محاسبه و ارائه شده است.

۲- زمان محاسبه‌ی ماتریس انتقال بازیگران شامل استخراج بهبود و حرکت‌های یک‌جانبه‌ی بازیگران در وضعیت‌های ممکن بازی، ارائه شده است. این زمان با تعداد وضعیت‌های ممکن بازی و ارتباط مستقیم دارد و هرچه تعداد وضعیت‌ها بیشتر باشد زمان محاسبه نیز افزایش خواهد یافت.

۳- زمان تحلیل بازی شامل استخراج پایداری فردی و تعادلی بازیگران بر مبنای منطق‌های *SMR GMR, SEQ, Nash,* و *BestEQ* و محاسبه‌ی مقادیر معیارهای مؤثر در تعیین گزینه‌های اثرگذار بازیگران است.

۴- نتیجه‌گیری

در این مقاله، گزینه‌های بدافزارها و مقابله‌کنندگان شامل اقدامات و فعالیت‌ها، مبتنی بر مدل گراف تحلیل مناقشه، مطابق با چارچوب چهار لایه‌ی پیشنهادی، استخراج و تحلیل شد. برای ارزش‌گذاری گزینه‌های بازیگران در این چارچوب پیشنهادی، چهار پارامتر وابسته به گزینه‌ها و یک پارامتر وابسته به بازیگران تعریف و گزینه‌های بازیگران مبتنی بر آن‌ها ارزش‌گذاری گردید. به توجه به فراوانی گزینه‌های بازیگران و کثرت وضعیت‌های تعادلی، ضمن بهره‌گیری از تکنیک‌های انتزاع‌سازی بازی‌ها، سیزده معیار جهت استخراج وضعیت‌های تعادلی مطلوب بازیگران تعریف شد. با مدل‌سازی و تحلیل سه بازی چارچوب پیشنهادی مقاله به‌صورت سناریو محور ارزیابی گردید. نتایج حاصل از ارزیابی نشان می‌دهد گزینه‌ی (۲)، (۵) و (۸) مهاجم و گزینه‌ی (۶) و (۱۰) مدافع با میزان مشارکت ۸۹ درصدی گزینه‌های بازیگران بر اساس معیارهای استخراج گزینه‌های تأثیرگذار، به‌عنوان گزینه‌های تأثیرگذار در ایجاد وضعیت‌های تعادلی این مطالعه‌ی موردی، معرفی گردیده است. نتایج حاصل از ارزیابی نشان داد که انتزاع‌سازی بازی‌ها و محدودیت‌های اعمالی فضای حالت مسئله را به‌نحو بسیار مطلوبی کاهش می‌دهد و پارامترهای استخراج‌شده برای گزینه‌ها و بازیگران قابلیت به‌کارگیری در مدل‌های مختلف تصمیم‌گیری را دارد. اقدامات بازیگران و پارامترهای آن‌ها، معیارهای تعریف‌شده جهت استخراج وضعیت‌های تعادلی مطلوب بازی و گزینه‌های تأثیرگذار بازیگران و سناریوسازی و انتزاع‌سازی بازی‌ها در حوزه‌ی بدافزار از نوآوری‌های این مقاله است و کارکرد آن‌ها در مطالعه‌ی موردی بررسی شد و نتایج قابل قبولی به‌دست آمد. استخراج خودکار پارامترهای گزینه‌های بازیگران و مقادیر و ضرایب آن‌ها، بهبود مدل گراف تحلیل مناقشه مبتنی بر تحلیل آماری وضعیت‌های بازی جهت استخراج گزینه‌های تأثیرگذار بازیگران و به‌کارگیری چارچوب پیشنهادی در سایر فعالیت‌های بدافزارها و حملات سایبری از فعالیت‌های آتی و پیشنهادی این مقاله است.

۵- مراجع

[1] S. Parsa and A. Gooran Oorimi, "An Optimal and Transparent Framework for Automatic Analysis of Malware," ADST J., vol. 7, pp. 71–80, 2016. (In Persian)

[2] S. Parsa, H. Saifi, and M. H. Alaeian, "Providing a New Approach to Discovering Malware Behavioral Patterns Based on the Dependency Graph Between System Calls," J. Electron. CYBER Def., vol. 4, no. 3 (15), pp. 47–59, 2016. (In Persian)

[3] M. Abbasi, M.S Mohammadi, and M Ghayoori, "Modeling and analysis of competition between malware authors and security analysis, using game theory" , SPP, vol. 7, no. 23, 2017 .(In Persian)

[4] M. Sheikhmohammady, K. W. Hipel, H. Asilahijani, and D. Marc Kilgour, "Strategic analysis of the conflict over Iran's nuclear program," in Conference Proceedings - IEEE International Conference on Systems, Man and Cybernetics, 2009, pp. 1911–1916, doi: 10.1109/ICSMC.2009.5346148.

[5] M. Abbasi and M. Sheikhmohamadi, "An approach based on game theory in modeling and analysis of inheritance of the deceased couple," J. Res. Econ. Model, vol. 10, pp. 23-48 2016 .(In Persian)

[6] T. Sandholm, "Abstraction for solving large incomplete-information games," in Proceedings of the National Conference on Artificial Intelligence, vol. 6, pp. 4127–4131, 2015.

[7] Kroer and T. Sandholm, "Extensive-form game abstraction with bounds," in Proceedings of the fifteenth ACM conference on Economics and computation, pp. 621–638, 2014.

[8] Kroer and T. Sandholm, "Extensive-form game imperfect-recall abstractions with bounds," arXiv Prepr. http//arxiv. org/abs/1409.3302, 2014.

[9] F. K. Frantz, "A taxonomy of model abstraction techniques," in Proceedings of the 27th conference on Winter simulation, pp. 1413–1420, 1995.

[10]P. Beaucamps, I. Gnaedig, and J. Y. Marion, "Behavior abstraction in malware analysis," in Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), vol. 6418 LNCS, pp. 168–182, 2010.

[11]T. Colburn and G. Shute, "Abstraction in computer science," Minds Mach., vol. 17, no. 2, pp. 169–184, 2007.

[12]N. Basilico and N. Gatti, "Automated abstractions for patrolling security games," in Proceedings of the National Conference on Artificial Intelligence, vol. 2, pp. 1096–1101, 2011.

[13]Afianian, S. Niksefat, B. Sadeghiyan, and D. Baptiste, "Malware Dynamic Analysis Evasion Techniques: A Survey," CoRR, vol. abs/1811.0, 2018.

[14]P. Mell, K. Scarfone, and S. Romanosky, "Common vulnerability scoring system," IEEE Secur. Priv., vol. 4, no. 6, pp. 85–89, 2006.

[15]Common Vulnerability Scoring System SIG." https://www.first.org/cvss/ (accessed Nov. 03, 2020).

[16]T. Shields, "Anti-debugging–a developers view," Veracode Inc., USA, 2010.

[17]S. Gao and Q. Lin, "Debugging classification and anti-debugging strategies," in Fourth International Conference on Machine Vision (ICMV 2011): Computer Vision and Image Analysis; Pattern Recognition and Basic Technologies, vol. 8350, p. 83503C, 2012.

[18]R. Rubira Branco, G. Negreira Barbosa, P. Drimel Neto, R. R. Branco, G. N. Barbosa, and P. D. Neto, "Scientific but Not Academical Overview of Malware Anti-Debugging, Anti-Disassembly and Anti- VM Technologies," Black Hat, 2012.

[19]Bulazel and B. Yener, "A survey on automated dynamic malware analysis evasion and counter-evasion: PC, Mobile, and Web," ACM Int. Conf. Proceeding Ser., pp. 1–21, 2017.

[20]M. Botacin et al., "Analysis, Anti-Analysis, Anti-Anti-Analysis: An Overview of the Evasive Malware Scenario," no. Ic, pp. 1–38, 2017.

[21]Goldberg, D. Wagner, R. Thomas, and E. A. Brewer, "A secure environment for untrusted helper applications: Confining the wily hacker," in Proceedings of the 6th conference on USENIX Security Symposium, Focusing on Applications of Cryptography, 1996, vol. 6, p. 1.

[22]X. Chen et al., "Towards an understanding of anti-virtualization and anti-debugging behavior in modern malware," in 2008 IEEE International Conference on Dependable Systems and Networks With FTCS and DCC (DSN), 2008, pp. 177–186.

[23]M. Mehra and D. Pandey, "Event triggered malware: A new challenge to sandboxing," in 12th IEEE International Conference Electronics, Energy, Environment, Communication, Computer, Control: (E3-C3), INDICON 2015, 2016.

[24]S. Reeves, "Detecting Malware and Sandbox Evasion Techniques," Inf. Secur., p. 9, 2016.

[25]N. Miramirkhani, M. P. Appini, N. Nikiforakis, and M. Polychronakis, "Spotless Sandboxes: Evading Malware Analysis Systems Using Wear-and-Tear Artifacts," in Proceedings - IEEE Symposium on Security and Privacy, 2017, pp. 1009–1024.

[26] "Evolution of Malware Sandbox Evasion Tactics – A Retrospective Study | McAfee Blogs." [Online]. Available: https://securingtomorrow.mcafee.com/other-blogs/mcafee-labs/evolution-of-malware-sandbox-evasion-tactics-a-retrospective-study/. [Accessed: 29-Oct-2019].

[27]R. Sihwail, K. Omar, and K. A. Z. Ariffin, "A survey on malware analysis techniques: Static, dynamic, hybrid and memory analysis," Int. J. Adv. Sci. Eng. Inf. Technol., vol. 8, no. 4–2, pp. 1662–1671, 2018.

[40]Kroer and T. Sandholm, "Extensive-form game abstraction with bounds," in Proceedings of the fifteenth ACM conference on Economics and computation, pp. 621–638, 2014.

[41]C. Kroer and T. Sandholm, "Extensive-form game imperfect-recall abstractions with bounds," arXiv Prepr. http//arxiv. org/abs/1409.3302, 2014.

[42]K. Frantz, "A taxonomy of model abstraction techniques," in Proceedings of the 27th conference on Winter simulation, pp. 1413–1420, 1995.

[43]S. Parsa and S. H. R. Aarabi, "A New Approach to Network Intrusion Detection Based on Hybrid Methods," J. Electron. CYBER Def., vol. 5, no. 3 (19), pp. 79–93, 2017. (In Persian)

[44]The Cylance Threat Research Team, "threat-spotlight-satan-raas," 2017. [Online]. Available: https://threatvector.cylance.com/en_us/home/threat-spotlight-satan-raas.html.

[45]P. Ferrie, "The ultimate anti-debugging reference,", [Online]. Available: internal-pdf://251.172.174.167/The_Ultimate_Anti-Reversing_Reference.pdf, 2011.

[46]Kulchytskyi Oleg, "Anti-Debug Protection Techniques: Implementation and Neutralization," www.codeproject.com, https://www.codeproject.com/Articles/1090943/Anti-Debug-Protection-Techniques-Implementation-an, 2016.

[47]T. Shields, "Anti-debugging–a developers view," Veracode Inc., USA, 2010

[48]M. Sikorski, A. Honig, A. Mylonas, and D. Gritzalis, Practical malware analysis: the hands-on guide to dissecting malicious software, vol. 31, no. 6. no starch press, 2012.

[49] "Inkasso trojaner - part 3," Curesec Security Research, 2013. https://curesec.com/blog/article/blog/Inkasso-Trojaner--Part-3-24.html.

[50]H. Shi and J. Mirkovic, "Hiding debuggers from malware with apate," in Proceedings of the ACM Symposium on Applied Computing, vol. Part F1280, pp. 1703–1710, doi: 10.1145/3019612.3019791, 2017.

[51]Microsoft, "Acquiring high-resolution time stamps," https://docs.microsoft.com/en-us/windows/win32/sysinfo/acquiring-high-resolution-time-stamps, 2018. (accessed Jan. 01, 2019)

[28]M. J. Osborne, An introduction to game theory, vol. 3. Oxford University Press New York, 2004.

[29]D. S. Lutz and N. Howard, "Paradoxes of Rationality: Theory of Metagames and Political Behavior," Technometrics, vol. 15, no. 3, p. 652, 1973, doi: 10.2307/1266876.

[30]N. Howard, "The present and future of metagame analysis," Eur. J. Oper. Res., vol. 32, no. 1, pp. 1–25, 1987, doi: 10.1016/0377-2217(87)90267-0.

[31]N. M. Fraser and K. W. L. B. Hipel, Conflict analysis: models and resolutions, vol. 11. North-Holland, 1984.

[32]M. A. Takahashi, N. M. Fraser, and K. W. Hipel, "A procedure for analyzing hypergames," Eur. J. Oper. Res., vol. 18, no. 1, pp. 111–122, 1984, doi: 10.1016/0377-2217(84)90268-6.

[33]N. Howard, "Drama theory and its relation to game theory. Part 1: dramatic resolution vs. rational solution," Gr. Decis. Negot., vol. 3, no. 2, pp. 187–206, 1994.

[34]S. J. Brams and W. Mattli, "Theory of moves: Overview and examples," Confl. Manag. Peace Sci., vol. 12, no. 2, pp. 1–39, 1993, doi: 10.1177/073889429301200201.

[35]Gilpin and T. Sandholm, "Lossless abstraction of imperfect information games," J. ACM, vol. 54, no. 5, p. 25, 2007.

[36]Gilpin, T. Sandholm, and T. B. Sørensen, "Potential-aware automated abstraction of sequential games, and holistic equilibrium analysis of Texas Hold'em poker," in Proceedings of the National Conference on Artificial Intelligence, 2007, vol. 1, pp. 50–57.

[37]Waugh, D. Schnizlein, M. Bowling, and D. Szafron, "Abstraction pathologies in extensive games," in Proceedings of the International Joint Conference on Autonomous Agents and Multiagent Systems, AAMAS, 2009, vol. 2, pp. 870–877.

[38]T. Sandholm and S. Singh, "Lossy stochastic game abstraction with bounds," in Proceedings of the 13th ACM Conference on Electronic Commerce, 2012, pp. 880–897, doi: 10.1145/2229012.2229079.

[39] S. Balochian, and A. Izadipour, "Importance of Game Theory in Modelling and Solution of Network Centric Weapon Target Assignment with consideration to Target Intelligence". C4I In Anais do SBSeg'17, XVII Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais, pp. 250-263, 2019.

[52]M. V. Yason and Ncent, "The Art of Unpacking," Black Hat 2007,https://wikileaks.org/hbgary-emails//fileid/21224/6926, 2007.

[53]P. Ferrie, "Anti-unpacker tricks - part one," Virus Bull. December, vol. 4, p. 4, doi: 10.1016/j.critrevonc.2016.03.005, 2008.

[54]T. Raffetseder, C. Kruegel, and E. Kirda, "Detecting system emulators," in Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), vol. 4779 LNCS, pp. 1–18, doi: 10.1007/978-3-540-75496-1_1, 2007.

[55]Blackthorne, A. Bulazel, A. Fasano, P. Biernat, and B. Yener, "AVLeak: fingerprinting antivirus emulators through black-box testing," in 10th {USENIX} Workshop on Offensive Technologies ({WOOT} 16), 2016.

[56]Pék, B. Bencsáth, L. Buttyán, G. Pek, B. Bencsath, and L. Buttyan, "nEther: In-guest Detection of Out-of-the-guest Malware Analyzers," in Proceedings of the Fourth European Workshop on System Security, pp. 1-6 , 2011.

[57]C. Spensky, H. Hu, and K. Leach, "LO-PHI: Low-Observable Physical Host Instrumentation for Malware Analysis," in NDSS, 2017.

[58]T. Garfinkel, K. Adams, A. Warfield, and J. Franklin, "Compatibility is Not Transparency: VMM Detection Myths and Realities," 2007.

[59]J. A. P. Marpaung, M. Sain, and H.-J. Lee, "Survey on malware evasion techniques: State of the art and challenges," in 2012 14th International Conference on Advanced Communication Technology (ICACT), pp. 744–749, 2012.

[60]McAfee, "McAfee Labs Threats Report," https://www.mcafee.com/enterprise/en-us/assets/reports/rp-quarterly-threats-jun-2017.pdf, 2017. (accessed Jan. 01, 2019).

[61]A. Kapravelos, M. Cova, C. Kruegel, and G. Vigna, "Escape from monkey island: Evading high-interaction honeyclients," in International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment, pp. 124–143, 2011.

[62]T. Morrow and J. Pitts, "Genetic Malware: Designing Payloads for Specific Targets," Infiltrate, [Online]. Available: https://infiltratecon.com/archives/Genetic_Malware_Travis_Morrow_Josh_Pitts.pdf, 2016.

[63]D. Kirat, J. Jang, and M. P. Stoecklin, "DeepLocker Concealing Targeted Attacks with AI Locksmithing," 2018.

[64]B. Bencsáth, G. Pék, L. Buttyán, and M. Felegyhazi, "The cousins of stuxnet: Duqu, flame, and gauss," Futur. Internet, vol. 4, no. 4, pp. 971–1003, 2012.

پیوست :

جدول (۳): پارامترهای تأثیرگذار بر اقدام، فعالیت، رفتار مهاجم

ردیف	نام پارامتر	ضریب پارامتر	مقادیر توصیفی پارامتر		طیف مقادیر عددی
۱	پیچیدگی پیاده‌سازی	۱	فراخوانی یک تابع API در سطح کاربری سیستم عامل و پردازش خروجی تابع هدف		۲-۰
			فراخوانی چندین تابع API و پردازش نتایج خروجی توابع در سطح کاربری سیستم عامل		۴-۲
			فراخوانی چندین تابع API و پردازش نتایج خروجی توابع در سطح هسته‌ی سیستم عامل		۶-۴
			بهره‌گیری از تکنیک‌ها و توابع خاص و منتشرنشده سیستم عامل و آسیب‌پذیری‌های سطح بالا در سطح هسته‌ی سیستم عامل		۸-۶
			بهره‌گیری از تکنیک‌های خاص‌منظوره جهت پیاده‌سازی در سطح ثابت‌افزار و تقلیدسازی		۱۰-۸
۲	تاب‌آوری	۱	قابل دفاع بودن عمل بدافزاری با تغییر برخی از اطلاعات سیستم هدف (تغییر تصادفی کلید رجیستری، تغییر در ساختمان داده PEB)		۲-۰
			قابل دفاع بودن عمل بدافزاری با قلاب‌اندازی به توابع و تزریق کد در سطح کاربری		۴-۲
			قابل دفاع بودن عمل بدافزاری با قلاب‌اندازی به توابع و تزریق کد در سطح هسته سیستم عامل		۶-۴
			قابل دفاع بودن عمل بدافزاری در سطح مجازی‌سازی و تقلیدسازی		۸-۶
			نبود راهکار مقابله با عمل بدافزاری یا نبود زیرساخت‌های لازم برای پیاده‌سازی راهکار دفاعی		۱۰-۸
۳	سطح اثربخشی	۱	اثربخشی تا سطح سطح کاربری سیستم‌عامل		۲-۰
			اثربخشی تا سطح هسته سیستم‌عامل		۴-۲
			اثربخشی تا سطح مجازی سازی و تقلید		۶-۴
			اثربخشی تا سطح فلز گداخته		۸-۶
			اثربخشی تا ثابت‌افزار		۱۰-۸
۴	فراوانی به‌کارگیری	۱	استفاده‌ی فراوان در بدافزارهای مختلف و انتشار عمومی تکنیک‌های پیاده‌سازی		۲-۰
			استفاده در بدافزارهای خاص منظوره و انتشار عمومی و راهکار دفاعی محدود در سطح کاربری		۴-۲
			استفاده محدود در بدافزارهای خاص‌منظوره و انتشار عمومی و راهکار دفاعی محدود در سطح هسته		۶-۴
			استفاده محدود در بدافزارهای خاص‌منظوره و انتشار عمومی و راهکار دفاعی محدود در سطح مجازی‌سازی و تقلیدسازی		۸-۶
			استفاده بسیار محدود و قابلیت شناسایی بسیار پایین با اثرگذاری بر سطح فلز گداخته و ثابت‌افزار		۱۰-۸
۵	قابلیت بهره‌برداری	۱	شرایط منابع مالی، نیروی انسانی، سامانه‌های نرم افزاری، تجهیزات زیرساختی و منابع علمی بهره‌بردار	شرایط بهره‌بردار(شامل منابع مالی، نیروی انسانی متخصص و غیره) خیلی ضعیف	۲-۰
				شرایط بهره‌بردار (شامل منابع مالی، نیروی انسانی متخصص و غیره) ضعیف	۴-۲
				شرایط بهره‌بردار (شامل منابع مالی، نیروی انسانی متخصص و غیره) متوسط	۶-۴
				شرایط بهره‌بردار (شامل منابع مالی، نیروی انسانی متخصص و غیره) خوب	۸-۶
				شرایط بهره‌بردار (شامل منابع مالی، نیروی انسانی متخصص و غیره) خیلی خوب	۱۰-۸

جدول (۴): پارامترهای تأثیرگذار بر اقدامات مقابله‌کنندگان(مدافع)

ردیف	پارامتر	ضریب پارامتر	مقادیر توصیفی پارامتر		طیف مقادیر عددی
۱	پیچیدگی پیاده‌سازی	۱	قابلیت پیاده‌سازی در سطح کاربری با بهره‌گیری از توابع سیستمی		۲-۰
			قابلیت پیاده‌سازی در سطح هسته با بهره‌گیری از توابع سیستمی		۴-۲
			قابلیت پیاده‌سازی با استفاده از مجازی‌سازی و تقلید		۶-۴
			قابلیت پیاده‌سازی با استفاده از فلز گداخته		۸-۶
			قابلیت پیاده‌سازی با استفاده از ثابت‌افزار و سخت‌افزار		۱۰-۸
۲	تاب‌آوری	۱	قابلیت تشخیص و دورزدن فن از طریق بدافزار و با کدنویسی چند تابع سیستمی در سطح کاربری سیستم‌عامل و با تغییر برخی از مشخصه‌های عمومی		۲-۰
			قابلیت تشخیص و دور زدن فن از طریق بدافزار در سطح کاربری سیستم‌عامل با استفاده از توابع سیستمی		۴-۲
			قابلیت تشخیص و دور زدن فن از طریق بدافزار در سطح هسته سیستم عامل		۶-۴
			قابلیت تشخیص و دور زدن فن از طریق بدافزار در سطح ثابت‌افزار و سخت‌افزار		۸-۶
			غیر قابل تشخیص و مقابله با توجه به فن‌های موجود		۱۰-۸
۳	سطح اثر بخشی	۱	شناسایی بدافزارها در سطح کاربری سیستم عامل		۲-۰
			شناسایی بدافزارها در سطح هسته سیستم‌عامل		۴-۲
			شناسایی بدافزارها در سطح مجازی‌سازی و تقلید		۶-۴
			شناسایی بدافزارها در سطح فلز گداخته		۸-۶
			شناسایی بدافزارها در سطح ثابت افزار		۱۰-۸
۴	فراوانی	۱	قابلیت پیاده‌سازی در سطح کاربری و با فراخوانی چند تابع سیستمی و انتشار عمومی فن		۲-۰
			قابلیت پیاده‌سازی در سطح کاربری و با فراخوانی تابع سیستمی و انتشار عمومی فن		۴-۲
			قابلیت پیاده‌سازی در سطح هسته‌ی سیستم عامل و با استفاده از تکنیک‌های قلاب‌اندازی		۶-۴
			قابلیت بهره‌گیری در تکنیک‌های مجازی‌سازی و تقلید		۸-۶
			قابلیت بهره‌گیری به‌وسیله‌ی تکنیک‌های فلز گداخته و تحلیل ناهمگن[1]		۱۰-۸
۵	قابلیت بهره‌برداری	۲	شرایط منابع مالی، نیروی انسانی متخصص، سامانه‌های نرم‌افزاری، تجهیزات زیرساختی و منابع علمی بهره‌بردار	شرایط بهره‌بردار(شامل منابع مالی، نیروی انسانی متخصص و غیره) خیلی ضعیف	۲-۰
				شرایط بهره‌بردار (شامل منابع مالی، نیروی انسانی متخصص و غیره) ضعیف	۴-۲
				شرایط بهره‌بردار (شامل منابع مالی، نیروی انسانی متخصص و غیره) متوسط	۶-۴
				شرایط بهره‌بردار (شامل منابع مالی، نیروی انسانی متخصص و غیره) خوب	۸-۶
				شرایط بهره‌بردار (شامل منابع مالی، نیروی انسانی متخصص و غیره) خیلی خوب	۱۰-۸

[1] Heterogeneous Analysis

جدول (۵): محاسبه‌ی ظرفیت و توانمندی اجرای اقدام از طریق بازیگر

ظرفیت و توانمندی اجرای اقدام توسط بازیگر		پارامتر اقدام	پیچیدگی پیاده‌سازی	تاب‌آوری	سطح اثربخشی	فراوانی به‌کارگیری
		ضریب ثابت پارامترها	۳	۳	۳	۱
شرایط بازیگر	ضریب ثابت شرایط بازیگر	شرایط بازیگر/ پارامتر اقدام	۱۰	۱۰	۱۰	۱۰
منابع مالی	۱,۲۵	۵	۳۶,۲۵	۳۶,۲۵	۳۶,۲۵	۱۶,۲۵
نیروی انسانی متخصص	۱,۲۵	۵	۳۶,۲۵	۳۶,۲۵	۳۶,۲۵	۱۶,۲۵
سامانه‌های نرم‌افزاری پایه بومی	۰,۷۵	۵	۳۳,۷۵	۳۳,۷۵	۳۳,۷۵	۱۳,۷۵
تجهیزات زیرساختی بومی	۰,۷۵	۵	۳۳,۷۵	۳۳,۷۵	۳۳,۷۵	۱۳,۷۵
دسترسی به دانش و فناوری	۱	۵	۳۵	۳۵	۳۵	۱۵

جدول (۶): گزینه‌های مهاجم در سطح اقدام و پارامترهای مرتبط

شناسه فعالیت	شناسه اقدام	عنوان گزینه‌های مهاجم	پارامترهای وابسته به اقدامات				شناسه راهکار دفاعی
			پیچیدگی	تاب‌آوری	سطح اثر	فراوانی	
۱-۱ [۳۵] [۴۴] [۳۷]	۱-۱-۱	تشخیص وجود اشکال‌زدا با توابع مربوطه IsDebuggerPresent() و CheckRemoteDebuggerPresent()	۲	۲	۵	۳	۱-۱-۱ ۲-۱-۱
	۲-۱-۱	بررسی پرچم NtGlobalFlag برای تشخیص اشکال‌زدا NtGlobalFlags()	۲	۳	۶	۴	۳-۱-۱ ۴-۱-۱
۲-۱ [۳۵] [۴۵] [۴۶]	۱-۲-۱	بررسی وجود نقاط شکست نرم‌افزاری Self-scan to spot INT 3 instruction Self-integrity-check	۳	۴	۶	۷	۱-۲-۱
	۲-۲-۱	تشخیص اجرا در محیط اشکال‌زدا با بررسی رجیستر DR پردازنده به‌وسیله‌ی تابع مربوطه جهت تشخیص نقاط شکست سخت‌افزاری GetThreadContext()	۶	۷	۷	۷	۲-۲-۱
۳-۱ [۴۷] [۴۸]	۱-۳-۱	جست‌وجوی نام پردازه‌های مشهور اشکال‌زداها و بررسی عنوان پنجره‌ی برنامه‌های مرتبط FindWindow(), FindProcess(), FindFirstFile()	۲	۴	۴	۲	۱-۳-۱ ۲-۳-۱
۴-۱ [۴۵] [۴۹]	۱-۴-۱	کاوش درآثار و شواهد محیط اشکال‌زدا به‌وسیله‌ی توابع مرتبط ProcessDebugObjectHandle(), ProcessDebugFlags(), ProcessBasicInformation()	۴	۴	۵	۳	۱-۴-۱ ۲-۴-۱
۵-۱ [۳۵] [۵۰] [۴۵]	۱-۵-۱	توابع مربوط به بررسی و ارزیابی شناسه‌ی پردازه والد GetCurrentProcessId() + CreateToolhelp32Snapshot()+ Process32First()+Process32Next()	۴	۶	۴	۲	۱-۵-۱ ۲-۵-۱
۶-۱ [۵۱]	۱-۶-۱	توابع مرتبط با بررسی ساختمان داده پردازنده، مدت زمان اجرای کد Local Resource: RDTSC, timeGetTime(), GetTickCount(), QueryPerformanceCounter(), GetLocalTime() , GetSystemTime()	۳	۵	۵	۴	۱-۶-۱ ۲-۶-۱ ۳-۶-۱
	۲-۶-۱	بررسی و تحلیل زمان پاسخ‌گویی منابع بیرونی از طریق شبکه source time external Query	۲	۴	۴	۵	۴-۶-۱
۷-۱	۱-۷-۱	Instruction Prefix (Rep)	۲	۶	۵	۶	۱-۷-۱

شناسه فعالیت	شناسه اقدام	عنوان گزینه‌های مهاجم	پارامترهای وابسته به اقدامات				شناسه راهکار دفاعی
			پیچیدگی	تاب‌آوری	سطح اثر	فراوانی	
[۳۵]	۱-۷-۲	قرار دادن دستور فعال‌سازی وقفه 2dh int در کد بدافزاری و مدیریت اجرای استثناها برای تشخیص وجود اشکال‌زدا(0x2D 3, Interrupt)	۲	۶	۵	۶	۱-۷-۱
	۱-۷-۳	فراخوانی وقفه 0x41 جهت تشخیص اشکال‌زدای سطح هسته با بررسی مقدار DPL (DPL در فراخوانی در محیط اشکال‌زدا مقدار سه دارد و در حالت عادی مقدار صفر)0x41 Interrupt	۳	۶	۶	۷	۱-۷-۱
۸-۱ [۵۲] [۵۳]	۱-۸-۱	بهره‌گیری از آسیب‌پذیری اشکال‌زدا OllyDBG با استفاده از خطای قالب‌بندی رشته مبتنی بر توابع InputDebugString(), OutPutDebugString()	۴	۶	۶	۸	۱-۸-۱
	۱-۸-۲	بهره‌گیری از آسیب‌پذیری اشکال‌زدا SoftICE در برابر حمله‌ی منع خدمت مبتنی بر توابع مربوط 09 و 0x83	۳	۲	۵	۸	۱-۸-۲
۹-۱ [۶] [۳۶] -۵۴] [۶۰	۱-۹-۱	آثار سخت‌افزار: شناسایی درایور و سخت‌افزارهای شناخته شده و مرتبط با محیط‌های تحلیل مجازی (Vmmouse.sys, vm3dgl.dll, VMToolsHook.dl)	۶	۵	۷	۶	۱-۹-۱ ۲-۹-۱
	۱-۹-۲	آثار محیط اجرایی: بررسی و مقایسه مقادیر مؤلفه‌های محیط اجرایی با مقدار نسبی آن‌ها (مقدار فضای حافظه‌ی هسته، بررسی وجود کانال ارتباطی بین میزان و محیط مجازی(ComCHannel))	۶	۷	۵	۵	۱-۹-۱ ۲-۹-۱
	۱-۹-۳	آثار برنامه‌ی کاربردی: بررسی و شناسایی نشانه‌ها و آثار نصب و اجرایی بودن برنامه‌ی کاربردی یا محیط تحلیلی مدنظر (مثل)VMtools.exe, Vmwareuser.exe or vboxservice.exe.	۶	۵	۵	۲	۱-۹-۱ ۲-۹-۱
	۱-۹-۴	آثار رفتاری: بررسی نتایج حملات زمان‌بندی جهت تشخیص اجرای دستورات در سخت‌افزار واقعی از سخت‌افزار شبیه‌سازی شده، آزمون قرص قرمز[1]	۷	۶	۶	۳	۱-۹-۱ ۲-۹-۱
	۱-۹-۵	آثار شبکه‌ای: پویش شبکه برای شناسایی آدرس‌های IP ثبات و شناخته شده و یا تقلید و شبیه‌سازی دسترسی اینترنت	۶	۸	۶	۴	۱-۹-۱ ۲-۹-۱
۱۰-۱ [۶۱]	۱-۱۰-۱	بررسی تاریخچه‌ی تعامل کاربر با محیط GetTickCount(), GetLastInputInfo(), GetCursorPos()	۴	۳	۵	۵	۱-۱۰-۱ ۲-۱۰-۱
۱۱-۱ [۲۳] [۶۲]	۱-۱۱-۱	فعال شدن با شناسایی اهداف محیطی مدنظر[2] (مثل جست‌وجوی سیستم کنترل صنعتی خاص مد نظر بدافزار استاکس‌نت)	۶	۴	۶	۷	۱-۱۱-۱
	۱-۱۱-۲	جست‌وجو و گسترش تا شناسایی محیط هدف[3] بدافزار (مثل گسترش بدافزار استاکس‌نت در شبکه تا رسیدن به مقصد)	۶	۵	۶	۶	۱-۱۱-۱
	۱-۱۱-۳	رمزنگاری و رمزگشایی کد مخرب مبتنی بر یکی از ویژگی‌های تعریف‌شده‌ی سیستم قربانی[4]	۵	۵	۶	۳	۱-۱۱-۱
۱۲-۱ [۶۳] [۶۴]	۱-۱۲-۱	رمز نگاری کدمخرب با کلید قابل استخراج از سیستم هدف برای جلوگیری از تحلیل (شماره‌ی سریال سخت‌افزار خاص، کلید ریجیستری خاص و غیره) Stuxnet: RegKeyExists("HKLM\SOFTWARE\ SIEMENS\STEP7")	۴	۷	۶	۴	۱-۱۲-۱ ۲-۱۲-۱
	۱-۱۲-۲	قفل‌سازی مبتنی بر هوش مصنوعی[5] برای رمزنگاری کد مخرب و فعال‌سازی آن در شرایط هدف	۷	۸	۷	۷	۳-۱۲-۱

[1] Red pill tests
[2] Environmentally-targeted
[3] Individually Targeted
[4] Environment-dependent Encryption
[5] AI Locksmithing

جدول (۷): گزینه‌های مدافع در سطح اقدام و پارامترهای آن

شناسه فعالیت	شناسه اقدام	عنوان گزینه‌ها	پارامترهای وابسته به اقدامات			
			پیچیدگی	تاب‌آوری	سطح اثربخشی	فراوانی
۱-۱	۱-۱-۱	تنظیم پرچم Beingdebugged با مقدار صفر	۲	۴	۴	۵
	۱-۱-۲	فعال‌سازی flag heap_groawable و تنظیم پرچم forceflags با مقدار صفر	۴	۵	۴	۵
	۱-۱-۳	اجرای اشکال‌زدا بعد از ایجاد پردازه creation, process after debugger Attach	۴	۵	۵	۴
	۱-۱-۴	قلاب توابع API مربوط به بررسی توابع مرتبط با ساختمان داده PEB	۴	۶	۶	۳
۱-۲	۱-۲-۱	تنظیم نقطه‌ی شکست بر روی بایت اول نخ اجرایی	۲	۵	۳	۴
	۱-۲-۲	ریست‌کردن پرچم context_debug_registers در contextflags قبل/بعد از فراخوانی تابع ntgetcontextthread()	۲	۴	۲	۴
۱-۳	۱-۳-۱	تصادفی‌سازی مقدار و نام متغیرها و عنوان برنامه‌ها achieve more transparency SetWindowTextA, SetWindowText, SetWindowTextW	۵	۶	۶	۳
	۱-۳-۲	تغییر نتایج حاصل از پرس‌وجوها با قلاب‌اندازی به توابع مرتبط	۶	۶	۴	۴
۱-۴	۱-۴-۱	تغییر حالات فرآیندها پس از فراخوانی	۵	۴	۴	۳
	۱-۴-۲	مسدودسازی توابع مرتبط با کاویدن اشیاء skipping related API CreateToolhelp32Snapshot, Process32First, Process32Next, FindFirstFileA, FindFirstFile, FindFirstFileW, FindNextFileA, FindFirstFile, FindFirstFileW	۶	۶	۵	۳
۱-۵	۱-۵-۱	قلاب‌اندازی به توابع مرتبط با پیمایش والد پردازه و مسدودسازی فراخوانی آن‌ها	۵	۶	۵	۴
	۱-۵-۲	تغییر و تصادفی‌سازی نام پردازه‌های مرتبط با اشکال‌زدا	۴	۵	۶	۴
۱-۶	۱-۶-۱	وصله‌ی هسته سیستم‌عامل F۴۸[1] برای جلوگیری از دسترسی به ساختمان داده rdtsc خارج از سطح دسترسی	۳	۶	۵	۶
	۱-۶-۲	حفظ و مدیریت منبع زمان وفاداری بالا source time high-fidelity Maintain	۳	۵	۲	۴
	۱-۶-۳	قلاب‌اندازی یا مسدودسازی فراخوانی توابع سیستمی مرتبط با بررسی زمان (time-checking APIs) CompareFileTime, DosDateTimeToFileTime, FileTimeToDosDateTime, FileTimeToLocalFileTime FileTimeToSystemTime, GetFileTime, GetLocalTime GetSystemTime, GetSystemTimeAdjustment, GetSystemTimeAsFileTime, GetTickCount GetTimeZoneInformation, LocalFileTimeToFileTime SetFileTime, SetLocalTime, SetSystemTime, SetSystemTimeAdjustment, SetTimeZoneInformation SystemTimeToFileTime, SystemTimeToTzSpecificLocalTime	۵	۶	۴	۴
	۱-۶-۴	Query external time source (e.g. NTP), InternetOpen, InternetOpenUrl, CreateFile, InternetReadFile, WriteFile, InternetCloseHandle	۳	۳	۲	۲
۱-۷	۱-۷-۱	Set breakpoint on exception handler, Allow single-step/breakpoint exceptions to be automatically passed to the exception handler	۵	۴	۴	۳
۱-۸	۱-۸-۱	وصله‌ی پارامترهای ورودی تابع outputdebugstring() و کنترل داده‌های ورودی مرتبط به کتابخانه kernel32	۶	۵	۴	۴
	۱-۸-۲	قراردادن نقطه‌ی شکست در ورودی تابع createfilefilew() kernel32! createfilefilew() kernel32! createfilefilew() kernel32!	۶	۵	۵	۷
۱-۹	۱-۹-۱	بهره‌گیری از تکنیک‌های تحلیل نامتجانس F۴۹[2] جهت مقابله با تکنیک‌های خودمحافظتی و هوشمندی بدافزار در شناسایی مؤلفه‌های محیطی هدف analysis heterogeneous Using	۵	۵	۷	۶
	۱-۹-۲	تصادفی‌سازی مقادیر شواهد محیطی جهت مخفی‌سازی آن‌ها Randomization Artifact	۶	۵	۶	۵
۱-۱۰	۱-۱۰-۱	شبیه‌سازی رفتارهای تعاملی کاربر با محیط تحلیل به‌وسیله‌ی تنظیم دستگاه‌های ورودی Simulation Digital	۸	۷	۹	۷
	۱-۱۰-۲	تشخیص و غیرفعال کردن دستورات شناسایی تعاملات کاربر از طریق بدافزار با استفاده از تکنیک‌های اکتشاف مسیر exploration path	۳	۳	۲	۴
۱-۱۱	۱-۱۱-۱	تشخیص و غیرفعال کردن دستورات شناسایی شواهد محیطی بدافزار با استفاده از تکنیک‌های اکتشاف مسیر exploration Path	۳	۳	۲	۴
۱-۱۲	۱-۱۲-۱	شمارش جامع ۵۰[3] شرایط مرتبط محیطی با سیستم هدف جهت تحلیل نامتجانس ۵۱[4]	۵	۵	۴	۶
	۱-۱۲-۲	کشف شرایط و ویژگی‌های هدف‌گرای نهفته‌ی بدافزار با استفاده از تکنیک‌های اکتشاف مسیر ۵۲[5]	۴	۴	۵	۵
	۱-۱۲-۳	AI Locksmithing, *	۵	۵	۴	۶

[1] Kernel patch
[2] Heterogeneous analysis
[3] Exhaustive Enumeration
[4] Heterogeneous analysis
[5] Path exploration