فصلنامهٔ مطالعات راهبردی سیاست‌گذاری‌عمومی، دورهٔ ۷، شمارهٔ ۲۳، تابستان ۹۶

مدل‌سازی و تحلیل راهبردی مناقشهٔ نویسندگان بدافزار و تحلیل‌گران سامانه‌های امنیتی با استفاده از نظریهٔ بازی

مصطفی عباسی،[۱] مجید شیخ محمدی،[۲] مجید غیوری ثالث[۳]

چکیده

با توجه به گسترش روزافزون فضای سایبر و بروز حملات سایبری به‌خصوص از طریق بدافزارها، فضای رقابتی بین نویسندگان بدافزارها و طراحان سامانه‌های امنیتی دفاعی، به وجود آمده است. با مدلسازی مبتنی بر نظریهٔ بازی، علاوه بر تبیین و تشریح مسائل، مناقشه‌ها و فضاهای رقابتی، می‌توان به کشف راه‌حل‌هایی سازنده برای حل بهتر آن‌ها رسید و شرایط مؤثر بر تصمیم‌گیری بازیگران و رفتار آن‌ها را مدل، تحلیل و پیش‌بینی کرد. در این مقاله، رقابت بین نویسندگان بدافزار و تحلیل‌گران سامانه‌های امنیتی با استفاده نظریهٔ بازی مدل‌سازی و تحلیل شده است. در این مدل‌سازی از بین ۱۲۸ ترکیب انتزاعی راهبردهای بازیگران، با اعمال محدودیت‌هایی، پانزده حالت ممکن رقابت، تحلیل و در نهایت دو حالت به‌عنوان وضعیت‌های تعادل بازی، معرفی می‌گردد که براساس آن می‌توان رفتارهای بازیگران را پیش‌بینی کرد. توجه به وضعیت‌های پایداری، بیان می‌کند که نویسندگان بدافزار جهت اطمینان از اجرای اهداف خود، برای تولید بدافزار از فناوری‌های خود محافظتی و شناسایی محیط، استفاده می‌کنند و نیز تحلیل‌گران سامانه‌های امنیتی با توجه به راهبردهای محتمل نویسندگان بدافزار، ایمن‌ترین

۱. دانشجوی دکتری دانشگاه جامع امام حسین (ع)؛ رایانامه: moabbasi@ihu.ac.ir
۲.استادیاردانشکدهٔمهندسی‌صنایع‌وسیستم‌هادردانشگاه‌تربیت‌مدرس(نویسندهٔمسئول)؛رایانامه:msheikhm@modares.ac.ir
۳. استادیار دانشگاه جامع امام حسین (ع)؛ رایانامه: ghayoori@ihu.ac.ir

و مناسب‌ترین راهبردها را یعنی بهره‌برداری از تمامی قابلیت‌های دفاعی، جهت مقابله با رقیب استفاده می‌کنند. بررسی رفتارهای اخیر بدافزارها و سامانه‌های دفاعی، تأییدی بر نتایج این پژوهش است.

کلیدواژه‌ها: نظریهٔ بازی، وضعیت تعادل، بدافزار، سامانه‌های امنیتی، راهبرد.

۱. مقدمه

نظریهٔ بازی[۴] شاخه‌ای از ریاضیات کاربردی است که در علوم اجتماعی و به‌ویژه در اقتصاد، زیست‌شناسی، مهندسی، علوم سیاسی، روابط بین‌الملل، علوم رایانه، بازاریابی و فلسفه از آن استفاده شده است. نظریهٔ بازی تلاش می‌کند رفتار ریاضی حاکم بر یک موقعیت راهبردی (تضاد منافع) را مدل‌سازی کند. این موقعیت زمانی پدید می‌آید که موفقیت یک فرد وابسته به راهبردهایی است که دیگران انتخاب می‌کنند. هدف نهایی این دانش، یافتن راهبرد بهینه برای بازیکنان است.

یکی از موضوعات مهم که با گسترش فضای مجازی، امنیت این فضا را به‌شدت تحت تأثیر خود قرار داده، گسترش بدافزارها و حملات سایبری از طریق آن‌ها است؛ به‌نحوی‌که در کسری از ثانیه یک بدافزار تولید می‌گردد (جواهری و پارسا، ۲۰۱۵) که می‌تواند هزینه‌های جبران‌ناپذیری برای کشورها و سازمان‌ها در فضای سایبری داشته باشد. برای تهیه و طراحی و اجرای موفقیت‌آمیز مأموریت‌های یک بدافزار، شرایط و بازیگران مختلفی با هم تعامل و رقابت دارند. بازیگران درگیر در این رقابت نویسندگان و تحلیلگران سامانه‌های امنیتی-دفاعی[۵] به‌عنوان نمایندهٔ سامانه‌های امنیتی-دفاعی و نویسندگان بدافزارها[۶] به‌عنوان نماینده نفوذگران و حملات سایبری هستند. در این رقابت، هدف بدافزارها حداکثر کردن تخریب و تأثیر در سامانه‌های هدف است و سامانه‌های دفاعی، تلاش می‌کنند بتوانند با حداقل خسارت‌ها، بدافزارها را شناسایی و مانع اقدامات مخرب آن‌ها گردند. بنابراین، بررسی، تعیین و تحلیل راهبردهای محتمل بازیگران رقابت از نیازمندی‌های ضروری است.

مسئلهٔ اصلی این مقاله عبارت است از تحلیل و مدل‌سازی راهبردهای بدافزارها و سامانه‌های دفاعی سایبری با بهره‌گیری از قابلیت‌های نظریهٔ بازی، تا ضمن استخراج نقاط تعادل[۷] و ائتلافی[۸] رقابت با توجه به فرضیات و میزان خطرپذیری بازیگران، براساس آن پیش‌بینی و تخمینی از شرایط پیش رو به دست آوریم.

بنابراین، در این تحقیق راهبردهای سامانه‌های دفاعی و حملات سایبری با توجه به ویژگی‌های بازی و شرایط رقابت فضای سایبری استخراج می‌گردد و رقابت براساس مدل گراف برای تحلیل مناقشه،[۹] مدل‌سازی و تحلیل می‌شود و در پایان، مناسب‌ترین پیش‌بینی‌ها و پیشنهاد در خصوص آینده این رقابت براساس نقاط تعادلی به بازیگران، ارائه می‌گردد و نتایج تحلیل مدل‌سازی جهت پیش‌بینی

4. game theory
5. security Analysts
6. malware authors
7. equilibrium
8. coalition
9. graph model for conflict resolution

روندهای آینده تهدیدات این فضا، مورداستفاده و بهره‌برداری بازیگران قرار می‌گیرد.

بر این اساس، در بخش دوم این مقاله، پیشینه و ویژگی‌های تحقیق بیان می‌شود. بخش سوم مفاهیم اساسی و پایه‌ای نظریهٔ بازی و بدافزار متناسب با نیاز پژوهش را عرضه می‌کند و ضمن آن، نقاط تعادل بازی مطابق با تعریف‌های مختلف صاحب‌نظران بیان‌شده است. در بخش چهارم، مدل‌سازی بازی با توجه به نوع بازی، بازیگران و راهبرد و ترجیحات آن‌ها ارائه و سپس به تحلیل نتایج بازی براساس وضعیت‌های تعادل پرداخته می‌شود. نتایج و پیشنهادها در بخش پنجم آمده است.

۲. پیشینهٔ تحقیق

تحقیقات متعددی در خصوص به‌کارگیری نظریهٔ بازی در امنیت سایبری و شبکه‌های کامپیوتری صورت گرفته است ولی تحقیقی که به‌طور مشخص، رفتار بدافزارها و سامانه‌های دفاعی را از دید رفتارهای کلان و راهبردی[10] آن‌ها بررسی کند تاکنون گزارش نشده است. یکی از ویژگی‌های این پژوهش نسبت به سایر پژوهش‌ها، نگاه کلان نگر به رقابت بازیگران حوزهٔ بدافزار و راهبردهای آن‌ها است که می‌تواند برای تصمیم‌گیری‌های کلان تصمیم سازان متناسب با میزان عقلانیت[11] و خطرپذیری آن‌ها، در قالب یک مدل تصمیم‌یار به‌کارگیری شود. در ادامه، به برخی از تحقیقات مرتبط به موضوع پژوهش و به‌کارگیری نظریهٔ بازی در امنیت سایبری اشاره می‌شود.

در ۲۰۰۷ م، اسمیت[12] و همکاران روشی با رویکرد نظریهٔ بازی، برای شناسایی بدافزارها و آشکارسازی مشکلات امنیتی در امنیت شبکه ارائه کردند. هدف اصلی آن‌ها توسعهٔ یک الگوریتم آشکارساز بهینه با توجه به راهبردها و اقدامات[13] مهاجم بوده است. در این مدل‌سازی، مهاجم منطقی و هوشمند در نظر گرفته شده و بازی دونفره و غیرهمکارانه بوده است. همچنین، از مدل‌های رسمی و ویژگی‌های نظریهٔ بازی برای مدل‌سازی، آزمون و ارزیابی الگوریتم در بستر شبکه برای رقابت بین مهاجم و سامانهٔ تشخیص نفوذ استفاده شده است و در پایان روش بهینهٔ توسعهٔ شناسایی بدافزار در محیط شبکه ارائه شده است (Schmidt et al, 2007).

در ۲۰۱۰ م، سینگ[14] و همکاران مفاهیم پایه‌ای نظریهٔ بازی و برخی ویژگی‌های موردنیاز برای تحلیل بازی ضد بدافزارها و بدافزارها را مرور کرده‌اند. در این پژوهش، به‌صورت محدود راهبردهای بازیگران بیان شده، اما جزئیاتی از مدل‌سازی و شبیه‌سازی بازی و نتایج آن نیامده است و تنها نوشته‌اند که از این مدل می‌توان در تحلیل وضعیت رفتار بدافزارها استفاده کرد (Singh et al, 2010).

در ۲۰۱۱ م، خوزانی[15] و همکاران از راه‌حل نظریهٔ بازی پویا[16] برای تشخیص بدافزار استفاده کردند. در این روش، با توجه به تغییر رفتارهای بدافزارها در سامانه‌های آلوده‌شده، به تغییر

10. strategy
11. rationality
12. Schmidt
13. strategies & actions
14. Singh
15. Khouzani
16. Dynamic Game Theory

راهکارهای دفاعی توسط سامانه‌های امنیتی و دفاعی نیاز هست. در این مدل‌سازی، از ویژگی‌های بازی غیرهمکارانه و مجموع صفر با مدل بازی‌های پویا روشی جهت تشخیص بدافزارها ارائه شده و با درجهٔ تشخیص مناسبی بدافزارهای هدف شناسایی شده است (Khouzani et al, 2011).

در ۲۰۱۲ م، خوزانی و همکاران با رویکرد نظریهٔ بازی، مدل‌سازی تشخیص نفوذ در شبکه‌های موبایلی را ارائه کرده‌اند. در این بازی که برای تعاملات بین گره‌ها از نظریهٔ بازی استفاده شده، برای مدل‌سازی بازی، فرض شده است که مهاجم به‌عنوان یک گره تمایل دارد به یکی از گره‌های شبکه نفوذ کند؛ بنابراین، یک بازیِ دونفره غیرهمکارانه است. در پایان، این پژوهشگران نتایج مختلف بازی را مطابق با سناریوهای مختلفِ عرضه کرده‌اند (Khouzani et al, 2012 a).

در ۲۰۱۲ م، خوزانی و همکاران به منظورِ بررسی نقطهٔ زینی[17] در حملات بدافزارها بر مبنای نظریهٔ بازی، پژوهشی انجام داده‌اند که با توجه به رفتارهای متغیر بدافزارها در شرایط مختلف نیاز است تغییرات پویایی در سامانه‌های دفاعی جهت مقابله با آن‌ها، بدون تغییر در کارایی سامانه‌های شبکه صورت گیرد. در این مدل‌سازی، بازی به‌صورت غیرهمکارانه، مجموع صفر و پویا است و در پایان نشان داده می‌شود که راهبردهای نقطهٔ زینی، همان سیاست‌های مبتنی بر آستانه است؛ بنابراین، دفاع پویا قوی‌تر و قابل پیش‌بینی‌تر است (Khouzani et al, 2012 b).

در ۲۰۱۳ م زولیتکین[18] و هامیلتن[19] روش نوینی را جهت شناسایی و طبقه‌بندی[20] نرم‌افزارهای مخرب با کمک رویکرد یادگیری ماشینی تحت نظارت[21] ارائه کردند. در این پژوهش، از نظریهٔ بازی برای ترکیب نتایج طبقه‌بندهای مختلف استفاده‌شده است؛ که نهایتاً مدل طبقه‌بندی براساس ماشین بردار پشتیبانی[22] با بهره‌گیری از روش بررسی کُدهای باینری و ترکیب با الگوریتم ژنتیک، بهترین نرخ تشخیص نرم‌افزارهای مخرب و دقت طبقه‌بندی را نسبت به سایر ترکیب‌ها داشته است (Zolotukhin & Hamalainen, 2013).

در ۲۰۱۴ م، پنگ[23] و همکاران مدلی جهت شناسایی و فیلتر بدافزارها، بات نت‌ها[24] و ایمیل‌های مخرب در شبکه‌های تحمل‌پذیر تأخیر[25] با بهره‌گیری از قابلیت‌های نظریهٔ بازی‌ها و مدل بیز ساده عرضه کردند. در این تحقیق، متناسب با ویژگی‌های شبکه‌های سیار، در ابتدا مجموعهٔ رفتارهای عمومی بر مبنای مدل بیز ساده ارائه و سپس مدل موردنظر در شبکهٔ غیرقابل تحمل‌پذیر تأخیری با موفقیت آزمایش‌شده است. آنان در روش ارائه‌شده، چالش‌های نبود شواهد کافی و نحوهٔ فیلتر کردن شواهد نادرست به صورت پیوسته و توزیع‌شده را با رویکرد نگاه به آینده مرتفع نموده‌اند؛ و در پایان روش تشخیص را با شبکهٔ موبایلی واقعی آزمایش و نتیجهٔ آن را بیان کرده‌اند (Peng et al, 2012).

17. saddle-point
18. Zolotukhin
19. Hamalainen
20. clasifier
21. supervised machine learning
22. support vector machine
23. Peng
24. botnets
25. Delay-tolerant networks

در ۲۰۱۵ م، رشیدی[۲۶] و همکاران پژوهشی در خصوص بررسی و تحلیل کاربران قانونی و مخرب سامانهٔ کنترل دسترسی گوشی‌های هوشمند اندروید ارائه کردند و برای بررسی این چالش از راهکارهای نظریهٔ بازی و الگوریتم‌های بیزین[۲۷] برای تحلیل تعاملات بین کاربران و سامانهٔ هوشمند کنترل دسترسی بهره‌برداری شده است. در این بازی، دو بازیگر بهترین راهبرد پاسخ برای کاهش ضرر در تعاملات را به‌کار می‌گیرند و براساس راهکارهای نظریهٔ بازی متناسب با سناریوهای مختلف نقاط تعادل نش را در راهبردهای خالص و ترکیبی[۲۸] استخراج می‌کنند (Rashidi et al, 2015).

در ۲۰۱۵ م، سندهوم[۲۹] و همکاران مدلی برای حل بازی‌های با اطلاعات ناقص و بزرگ عرضه کردند. در این مدل، ابتدا بازی‌های پیچیده به بازی انتزاع‌یافته تبدیل می‌شود؛ سپس بازی انتزاع‌یافته تحلیل و نقاط تعادلی آن استخراج می‌گردد؛ سرانجام، با مدل معکوسی این نقطهٔ تعادلی به بازی پیچیدهٔ اصلی نگاشت[۳۰] می‌گردد (Sandholm et al, 2015).

هدف از این مقاله بررسی تقابل رقابت بین نویسندگان بدافزار و سامانه‌های امنیتی است. می‌خواهیم نشان دهیم هر کدام از بازیگران، راهبردهایی دارند که اجرای این راهبردها براساس میزان هزینه، شرایط اجرایی، راهکارهای مقابله‌ای رقیب و سایر مؤلفه‌های مرتبط دارای اولویت‌های متفاوتی است. پس، بازیگر علاوه بر اولویت‌گذاری راهبردهای خود، وضعیت راهبردهای رقیب را در رقابت، مدنظر قرار می‌دهد و متناسب با راهبردهای محتمل و میزان خطرپذیری خود و رقیب، راهبردهای آتی را تعیین می‌کند تا بتوان قبل از اجرای راهبردهای رقیب، چالش‌ها و اقدامات احتمالی آن‌ها را پیش‌بینی کرد و اینکه باید دریافت که بازیگران ـبا توجه به وضع موجود، راهبردهای بازیگران و اولویت‌های آنان، متناسب با میزان عقلانیت بازیگرانـ کدام راهبردها را اجرا می‌کنند.

۳. مفاهیم اساسی و پایه تحقیق

برای تحلیل و بررسی رقابت بین بازیگران از نظریهٔ بازی و قابلیت‌های آن استفاده شده است. بنابراین متناسب با نیاز تحقیق، در این بخش مفاهیم پایه‌ای و ضروری نظریهٔ بازی و مجموعه اقدامات چند نمونه بدافزار مهم و راهکارهای دفاعی آن‌ها ارائه می‌گردد تا براساس آن‌ها رقابت بازیگران مدل‌سازی و تحلیل گردد.

۳. ۱. مفاهیم پایه‌ای نظریهٔ بازی

در این بخش متناسب با نیاز مسئله، مفاهیم نظریهٔ بازی ـشامل ویژگی‌های بازی، روش‌های بررسی نقاط تعادل و بررسی مفهوم‌های مختلف تعادل مطابق با عقلانیت بازیگرانـ بیان می‌گردد.

26. Rashidi
27. bayesian algorithm
28. pure and mixed strategies
29. Sandholm
30. Map

۳. ۱. ۱. مؤلفه‌های بازی و دسته‌بندی آن‌ها

به‌طورکلی هر بازی یا یک مناقشه در نظریهٔ بازی شامل موارد زیر است:

بازیگران.[۳۱] یک فرد یا گروهی از افراد که در یک بازی به‌عنوان یک بازیگر می‌توانند نقش ایفا کنند.

اقدامات.[۳۲] مجموعه‌ای از حرکت‌ها و یا تصمیم‌ها که بازیگر می‌تواند در یک رقابت انجام دهد.

راهبرد.[۳۳] مجموعهٔ اقداماتی که بازیگر تصمیم می‌گیرد در مواجهه با رقبا و در راستای کسب منافع خود انجام دهد.

مناقشهٔ راهبردی.[۳۴] نتیجهٔ رویکرد غیر همکارانهٔ بازیگران در تعارضات دنیای واقعی است.

پیامدها.[۳۵] هرگونه ترکیبی از راهبردها که برای هر بازیگر عایدی و منفعتی دارد.

ترجیحات.[۳۶] مرتب‌سازی پیامدها از سوی هر بازیگر متناسب با عایدی‌های کسب‌شده از هر پیامد.

دسته‌بندی بازی‌ها. در نظریهٔ بازی برای نمایش وضعیت‌های مختلف می‌توان از حالت نرمال[۳۷] یا حالت راهبردی، نمایش گسترده،[۳۸] حالت گزینه‌ای[۳۹] و نمایش گراف استفاده کرد که هرکدام مزیت‌ها و محدودیت‌هایی دارند.

با توجه به حالت همکاری بازیگران با یکدیگر، بازی‌های همکارانه یا غیر همکارانه داریم که در حالت غیر همکارانه هر بازیگر به منفعت خود می‌اندیشد و با رقبا همکاری نمی‌کند و اینکه پیامدها و عایدی‌های بازی به چه صورت تقسیم شود به بازی‌های مجموع 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 در صورتی که بازیگران از مجموعهٔ راهبردها و پیامدهای رقیب مطلع باشند بازی به بازی با اطلاع کامل، وگرنه، به بازی با اطلاع ناقص تقسیم‌بندی می‌شود.

۳. ۱. ۲. روش‌های مختلف بررسی وضعیت تعادل بازی

با توجه به ماهیت و اهداف نظریهٔ بازی، جهت بررسی وضعیت و سناریوهای مختلف بازی و نهایتاً استخراج نقاط تعادل، در ادامه، راهحلهای مختلف استخراج نقاط تعادل بیان‌شده است:

وضعیت تعادل.[۴۰] در یک بازی، تعادل به وضعیتی گفته می‌شود که در آن هیچ‌یک از بازیگران تمایلی به خروج از آن وضعیت نداشته باشند. اینکه یک بازیگر در یک وضعیت باقی می‌ماند یا

31. players
32. actions
33. strategies
34. strategic conflict
35. outcomes
36. preferences
37. normal form
38. extensive form
39. option form
40. equilibrium state

به‌صورت یک‌جانبه آنجا را ترک می‌کند، به عوامل مختلفی همچون خطرپذیری یا خطر گریزی فرد، عمق بینش و درک او از رقیب بستگی دارد.

بر این مبنا، برای تعریف پایداری فردی،[41] راه‌حل‌های مختلفی ارائه شده است که مهم‌ترینِ آن‌ها به شرح زیر است:

پایداری نش.[42] معرّف وضعیتی است که یک بازیگر خاص نمی‌تواند با حرکتی یک‌جانبه (با فرض ثابت بودن راهبرد سایر بازیگران)، به موقعیت بهتری دست یابد (Nash, 1951).

ماورای عقلانیت عمومی.[43] در این روش، بازیگر علاوه بر بررسی وضعیت‌های بهبود یک‌طرفهٔ[44] خود، رقیب را هم به حساب می‌آورد و تنها در صورتی تصمیم می‌گیرد که تغییر وضعیت دهد که بعد از حرکت خود، رقیب نتواند او را به وضعیت بدتری منتقل نماید (Howard , 1971).

ماورای عقلانیت متقارن.[45] در اینجا فرض بر این است که بازیگر پس از پاسخ رقبا می‌تواند حرکت دیگری هم داشته باشد. پایداری با مفهوم ماورای عقلانیت متقارن معرّف شرایطی است که یک بازیگر از هیچ‌یک از بهبودهای یک‌جانبهٔ خود بهره‌مند نمی‌شود؛ زیرا تمام حرکت‌های او توسط رقبا مورد مجازات[46] قرار می‌گیرد و حرکت ثانویهٔ او نیز شرایط را برای او بهتر نمی‌کند (Howard, 1971).

پایداری متوالی.[47] در این تعریف، بازیگر در زمان تغییر وضعیت، علاوه بر بررسی بهبود یک‌طرفهٔ خود، رقیب را هم به‌عنوان یک بازیگر عاقل در نظر می‌گیرد. پایداری متوالی معرف وضعیتی است که در آن تمام بهبودهای یک‌جانبهٔ فرد به‌وسیله حداقل یکی از بهبودهای یک‌جانبهٔ سایر رقبا مجازات می‌شود (Fraser & Hipel, 1984).

پایداری حرکت محدود.[48] یک بازیگر به‌اندازه h قدم جلوتر از خود را می‌بیند. پارامتر h متغیر است (Zagare, 1984).

پایداری غیر کوته‌نظرانه.[49] حالت خاصی از پایداری حرکت محدود است که در آن پارامتر h به سمت بی‌نهایت میل می‌کند. درواقع، بازیگری که با مفهوم پایداری غیر کوته‌نظرانه تصمیم می‌گیرد، دارای افق دید بسیار وسیع است (Brams & Wittman, 1981).

در جدول ۱ مقایسهٔ کیفی تعریف پایداری و سایر مشخصات آن آمده است.

41. individual stability
42. nash stability
43. general meta-rationality (GMR)
44. unilateral improvement(UI)
45. symmetric meta-rationality (SMR)
46. sanction
47. sequential stability (SEQ)
48. limited move stability
49. non- myopic stability

جدول ۱. مقایسهٔ کیفی پایداری غیر همکارانه

مفاهیم راه‌حل	ارائه‌دهندهٔ ایده	دوراندیش	تنزل راهبردی[50]
(R) پایداری نش	(Nash, 1951)	کم	هرگز
(GMR) ماورای عقلانیت عمومی	(Howard , 1971)	متوسط	فقط برای رقبا
(SMR) ماورای عقلانیت متقارن	(Howard , 1971)	متوسط	فقط برای رقبا
(SEQ) پایداری متوالی	(Fraser & Hipel, 1984)	متوسط	هرگز
(Lh) پایداری حرکت محدود	(Zagare, 1984)	متغیر	راهبردی
(NM) پایداری غیرکوته‌نظرانه	(Brams & Wittman, 1981)	بالا	راهبردی

یک مناقشهٔ راهبردی به فعل‌وانفعال متقابل دو یا چند بازیگر گفته می‌شود. هر کدام تصمیماتی را اتخاذ می‌کنند که روی‌هم‌رفته مشخص می‌کند حالت مناقشه چگونه از کار درمی‌آید و نیز هر کدام، برای خود ترجیحاتی در میان حالت‌های ممکن (به‌عنوان راه‌حل نهایی) دارند. لذا، یک مناقشهٔ راهبردی، یک مسئله و مشکل تصمیم تعاملی است که در آن دو یا چند تصمیم‌ساز وجود دارند، هر بازیگر انتخابی دارد (دو یا چند گزینه) و برای هر تصمیم‌ساز، اصالتاً انتخاب‌های دیگران دارای اهمیت است (Fang et al, 1993). به‌طور دقیق‌تر، هر بازیگر از تصمیمات سایر بازیگران، منتفع یا متضرر می‌شود. واضح است که مناقشات راهبردی در تعاملات فی‌مابینی و در همهٔ سطوح از قبیل شخصی، خانوادگی، شغلی، ملیتی و بین‌المللی، بسیار معمول و رایج است.

فنگ[51] و همکاران در ۱۹۹۳ م مدل گراف برای حل مناقشه را ارائه کردند و یک متدولوژی منعطف و توانمند برای مطالعهٔ مناقشات راهبردی در دنیای واقعی است. کارایی این مدل که از فن‌های نظریهٔ بازی در حالت غیر همکارانه است، زمانی بیشتر خود را نشان می‌دهد که بیان مطلوبیت بازیگران با اعداد کمّی و مقداری ممکن نباشد (Fang et al, 1993). مدل گراف برای تجزیه‌وتحلیل مناقشات نسبت به مدل‌های کلاسیک نظریهٔ بازی دارای مزایایی به شرح زیر است:

ـ نمایش بازی‌هایی که تعداد بازیگران آن بیش از دو نفر باشد به‌راحتی و به‌فرم گزینه‌ای صورت می‌گیرد.

ـ هر بازیگر می‌تواند هر تعداد از گزینه‌های خود را هم‌زمان انتخاب کند (راهبرد هر بازیگر منحصر به یک اقدام نیست).

ـ وضعیت‌های نشدنی[52] در مسائل دنیای واقعی به‌راحتی از وضعیت‌های ممکن متمایز شده حذف

50. strategic dis-improvement
51. Fang
52. infeasible state

می‌گردند.

ـ تعیین ارزش‌های عددی[53] به‌عنوان مطلوبیت بازیگران در وضعیت‌های مختلف ضرورتی ندارد (تنها بیان ترجیحات هر بازیگر روی وضعیت‌های مختلف به‌صورت ترتیبی کفایت می‌کند).

ـ حرکت‌های برگشت‌ناپذیر[54] و ترجیحات غیر متعددی[55] را لحاظ می‌کند.

ـ از مفاهیم حل[56] متفاوت برای تعیین پایداری فردی[57] و وضعیت‌های تعادل استفاده می‌کند.

این مدل دارای چهار مؤلفه به شرح زیر است:

۱. مجموعهٔ تصمیم‌گیرندگان که با N=[1,2,...,n] نشان داده می‌شود و $2 \leq |N| < \infty$

۲. مجموعهٔ وضعیت‌های شدنی با S نشان داده می‌شود $2 \leq |S| < \infty$

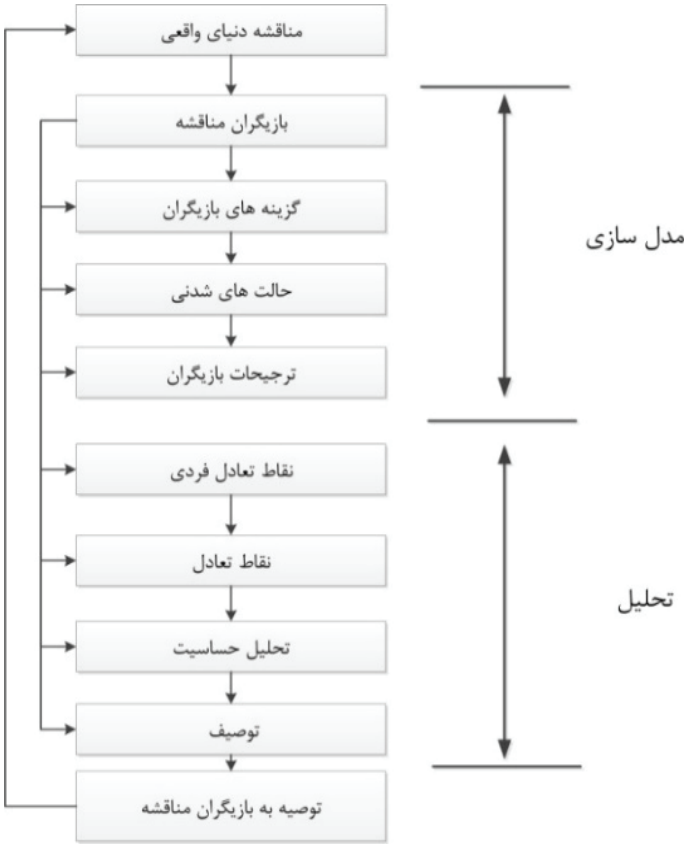
۳. هر بازیگر دارای یک گراف است. رئوس این گراف معرّف وضعیت‌های شدنی مختلف و کمان‌های جهت‌دار بین برخی از رئوس معرّف این است که آن بازیگر می‌تواند به‌صورت یک‌جانبه مناقشه را از یک وضعیت به وضعیت دیگر سوق دهد.

۴. ترجیحات هر تصمیم‌گیرنده روی وضعیت‌های شدنی مختلف به‌صورت ترتیبی[58] مشخص است.

مدل گراف برای حل مناقشات، یک متدولوژی مدل‌سازی و تحلیل مناقشات راهبردی ارائه می‌کند و به‌آسانی قابل‌استفاده و منعطف است و درک خوبی برای تصمیم سازان دربارهٔ اینکه چگونه آنچه باید انجام دهند را انتخاب کنند، فراهم می‌کند. البته سامانه‌های جایگزین برای مدل‌سازی و تحلیل مناقشات راهبردی که مجزا و متمایز از «تئوری بازی غیر همکارانه» باشند، وجود دارد که از آن جمله می‌توان روش‌های تحلیل متاگیم توسط هاوارد در سال‌های ۱۹۷۱ و ۱۹۸۷ م (Howard, 1971& 1987)، تحلیل مناقشه توسط فریزر و هایپل در ۱۹۸۴ م (Fraser & Hipel, 1984)، بازی خردآگاه[59] توسط تاکاهاشی[60] و همکاران در ۱۹۸۴ (Takahashi et al, 1984)، تئوری درام[61] توسط هاوارد در سال ۱۹۹۴ (Howard, 1994)، تئوری حرکات[62] توسط برامز[63] و متلی[64] در ۱۹۹۳ م (Brams & Mattli, 1993) و تئوری حرکات فازی را نام برد. تمرکز اصلی و مشخص این مقاله استفاده از مدل گراف برای حل مناقشات است. باورمان این است که مدل مذکور منعطف‌تر، دارای حوزهٔ وسیع‌تر و کاربرد آسان‌تر نسبت به روش‌های جایگزین خود است. این مدل هنر خود را در تحلیل مسائل پیچیدهٔ دنیای واقعی به‌خوبی نشان داده است (Fang et al, 1993). به‌عنوان نمونه، این

53. cardinal values
54. irreversible moves
55. intransitive preferences
56. solution concepts
57. individual stability
58. ordinal
59. hyper game
60. Takahashi
61. drama theory
62. theory of moves
63. Brams
64. Mattli

مدل به‌منظور پیش‌بینی محتمل‌ترین نتایج مورد انتظار در مناقشهٔ هسته‌ای ایران توسط شیخ محمدی و همکاران در ۲۰۰۹ م (Sheikhmohammady et al, 2009) و منازعهٔ قدرت‌های منطقه‌ای و بین‌المللی در سوریه مجدداً توسط شیخ محمدی و همکاران در ۲۰۱۳ م (Sheikhmohammady et al, 2013) به کار گرفته‌شده است. شکل ۱ فرایند به‌کارگیری مدل گراف برای حل مناقشه را برای مدل‌سازی و



تحلیل مناقشات پیچیدهٔ دنیای واقعی به‌خوبی نمایش می‌دهد.

شکل ۱. مدل گراف برای حل مناقشه

مأخذ: Fang et al, 1993

۳. ۲. معرفی چند بدافزار معروف و راهکارهای مقابله

از آنجا که بدافزار به‌عنوان نمایندهٔ بازیگران عرصهٔ بازی است، در ادامه، به برخی از ویژگی‌ها و قابلیت‌های سه نوع از بدافزارهای مهم و راهکارهای مقابله با آن‌ها پرداخته خواهد شد تا براساس آن‌ها راهبردهای بازیگران و مفروضات بازی استخراج گردد.

۳. ۲. ۱. دینو[۶۵]

این نوع بدافزار از نوع جاسوس‌افزارها[۶۶] و درب پشتی[۶۷] است که برای جاسوسی از سازمان‌های خاصی طراحی شده است و حملات هدفمند را پی‌ریزی می‌کنند و آسیب رساندن به منابع اطلاعاتی مراکز حساس کشور، نیز می‌تواند یکی از اهداف این بدافزار باشد.

در بین نوآوری‌های فنی این جاسوس‌افزار، فایل‌های سیستمی به چشم می‌خورد که دستورات را به‌صورت مخفیانه اجرا می‌کند. افزون بر مطالب گفته‌شده، این جاسوس‌افزار محتوی حجم بالایی از پیام‌های خطای طولانی است که اجازه نمی‌دهد نحوهٔ جمله‌بندی و ساختار برنامه‌نویسی دینو مهندسی معکوس شود(Calvet, 2015).

ویژگی‌ها و قابلیت‌ها:

- توانایی اجرای دستورات در سطح سیستم‌عامل؛
- بهره‌برداری از سامانه فرماندهی و کنترل جهت تعامل با جاسوس‌افزار؛
- توانایی شناسایی محیط.

روش‌های شناسایی و مقابله با آن:

- بهره‌برداری از روش‌های تشخیص ناهنجاری[۶۸]؛
- بهره‌برداری از ابزارهای دیده‌بانی[۶۹]؛
- بهره‌برداری از روش‌های و ابزارهای تقلید و شبیه‌سازی؛
- بروز رسانی سامانه‌های دفاعی و امنیتی و قوانین و سطوح دسترسی متناسب باقابلیت‌های جاسوس‌افزار؛
- پاک‌سازی و قطع ارتباط سامانه‌های آلوده از شبکه.

۳. ۲. ۲. دوکو[۷۰]

نام کرمی است که در ۲۰۱۱ م برای اولین بار کشف شد و بعدها نه ازلحاظ دسته‌بندی بلکه ازلحاظ فارنسیکی[۷۱] به حملات استاکس‌نت مرتبط شد. در این حملهٔ پیچیدهٔ سطح بالا از سه آسیب‌پذیری اصلاح‌نشده استفاده شده است. برای پنهان ماندن این حمله، بدافزار تنها در هستهٔ سیستم‌عامل مقیم شده است درنتیجه راه‌حل‌های ضد بدافزاری قادر به تشخیص آن نیستند. این بدافزار برای گرفتن دستورات مستقیماً به یک سرور فرماندهی و کنترل[۷۲] متصل نشده است بلکه مهاجم فایروال‌ها و دروازه‌های ورودی شبکه را با نصب درایوهای مخرب آلوده کرده و درنتیجه تمام ترافیک شبکهٔ خارجی به

65. Dino
66. spyware
67. backdoor
68. anomaly detection
69. Monitoring Tools
70. Duqu
71. Forensics
72. command and control

سرورهای فرماندهی و کنترل مهاجم از طریق پروکسی منتقل‌شده است.

شرکت سیمانتک اعلام کرد که دوکو نسخهٔ ۲٫۰ یک ابزار سرقت اطلاعات با ویژگی‌های کامل است که برای استفاده در درازمدت طراحی‌شده است. به احتمال زیاد، سازندگان این بدافزار از آن به‌عنوان یکی از ابزارهای اصلی خود در کمپین‌های هوشمند جمع‌آوری اطلاعات استفاده می‌کنند (Bencsáth et al, 2012).

ویژگی‌ها و قابلیت‌ها:

- مقیم شدن در هستهٔ سیستم‌عامل و بهره‌برداری از امکانات ریشه؛
- سرقت امضاهای امنیتی شرکت‌های مشهور؛
- بهره‌برداری از آسیب‌پذیری‌های شناخته‌شده و ناشناخته؛
- شناسایی محیط و قابلیت تعامل با سخت‌افزارها.

روش‌های شناسایی و مقابله با آن:

- بهره‌برداری از روش‌های تشخیص ناهنجاری؛
- بهره‌برداری از ابزارهای دیده‌بانی؛
- بهره‌برداری از روش‌ها و ابزارهای تقلید و شبیه‌سازی؛
- به‌روزرسانی سامانه‌های دفاعی و امنیتی متناسب با ویژگی‌های بدافزار؛
- پاک‌سازی و قطع ارتباط سامانه‌های آلوده از شبکه.

۳. ۲. ۳. استاکس‌نت[۷۳]

این بدافزار کرم کامپیوتری مبتنی بر سیستم‌عامل ویندوز است که در اواسط ژوئیهٔ ۲۰۱۰ م نخستین بار توسط کارشناسان کامپیوتری بلاروسی کشف شد که هدف آن سامانه‌های هدایتگر تأسیسات صنعتی با سیستم‌عامل ویندوز است. با بررسی‌های انجام‌شده مشخص گردید توسعه‌دهندگان استاکس‌نت یک منطقهٔ جغرافیایی ویژه‌ای را در نظر داشته‌اند و هدف از طراحی این بدافزار دستیابی به اطلاعات حساس صنعتی ایران بوده است. استاکس‌نت برای مشروع‌سازی خود و جلوگیری از شناسایی شدن، از امضای دیجیتال به‌سرقت‌رفتهٔ شرکت ریلتک[۷۴] استفاده کرده و از طریق یک حفرهٔ امنیتی، در ویندوز و سامانه کنترل صنعتی[۷۵] نفوذ و گسترش پیدا می‌کند و به دنبال سامانه‌هایی است که نرم‌افزار WinCC SCADA، متعلق به شرکت زیمنس بر روی آن‌ها نصب باشد (Falliere et al, 2010).

ویژگی‌ها و قابلیت‌ها:

- انتشار از طریق پست الکترونیکی و حافظه‌های قابل‌حمل؛
- توانایی شناسایی و تشخیص محیط و اهداف موردنظر؛

73. Staxnet
74. Realtek
75. SCADA

- بهره‌برداری از ویژگی‌های چندریختی و فشرده‌سازی؛
- توانایی دور زدن سامانه‌های امنیتی و مخفی‌سازی؛
- بهره‌برداری از آسیب‌پذیری‌های سامانه‌ها.

روش‌های شناسایی و مقابله با آن:
- بهره‌برداری از روش‌های تشخیص ناهنجاری؛
- بهره‌برداری از ابزارهای دیده‌بانی؛
- بهره‌برداری از روش‌ها و ابزارهای تقلید و شبیه‌سازی؛
- به‌روزرسانی سامانه‌های دفاعی و امنیتی؛
- پاک‌سازی و قطع ارتباط سامانه‌های آلوده از شبکه.

در شکل ۲ برخی از روش‌های دفاعی جهت شناسایی و جلوگیری از اقدامات بدافزارها معرفی شده است. مطابق شکل ۲، روش‌های پویش فایل‌ها، مجازی‌سازی، دیده‌بانی و جستجو برای رفتارهای غیرعادی از مؤلفه‌های فنی شناسایی بدافزارها است؛ این روش‌ها از لحاظ سطح بررسی جزئیات متفاوت است و در بخش‌های بعدی در راستای تعریف راهبردهای سامانه‌های دفاعی در مقابل بدافزارها از آن‌ها استفاده می‌گردد (Falliere et al, 2010).

٤. مدل‌سازی رقابت و تحلیل نتایج

مطابق تعاریف و مفاهیم بیان‌شده در بخش قبل، فضای رقابتی بین نویسندگان بدافزار و تحلیل‌گران امنیتی به‌عنوان یک بازی، مدل‌سازی می‌گردد. در این بازی، بنابر بررسی گزارش‌های چند نمونه بدافزار پیشرفته و معروف و راهکارهای دفاعی برای شناسایی و تحلیل آن‌ها، مفروضات و اقدامات بازیگران بیان و ویژگی‌ها و شرایط بازی متناسب با عدم قطعیتهای فضای سایبری و حوزه بدافزار تشریح می‌گردد.

٤. ١. مفروضات مسئله

برای مدل‌سازی و تحلیل هر مناقشه، علاوه بر شناخت بازیگران و راهبردهای آن‌ها باید مفروضاتی نیز برای مسئله در نظر گرفت. مفروضاتی که برای این چالش فنی و امنیتی، رقابت بین نویسندگان بدافزارها و سامانه‌های امنیتی و دفاعی، در نظر گرفته‌شده است به شرح زیر است:

۱. هرکدام از بازیگران باید حداقل از یکی از راهبردهای خود استفاده کنند.

۲. با توجه به سوابق قبلی بدافزارها برای برخی از راهبردها و عملکردهای آن‌ها راه‌حل‌های دفاعی وجود دارد، مثل

-برای تحلیل و شناسایی بدافزارهایی که فشرده‌شده[۷۶] باشند، می‌توان از روش‌های بررسی امضا،[۷۷]

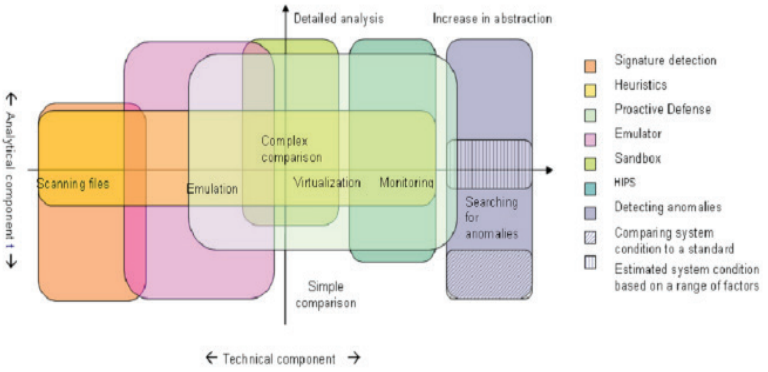
76. pack
77. signature

تقلید و مجازی‌سازی[۷۸] و سند باکس‌ها[۷۹] استفاده کرد.

ـ برای بدافزارهای جاسوسافزار[۸۰] که در سطح هستهٔ سیستم‌عامل فعالیت دارند می‌توان از ابزارهای دیده‌بانی و تشخیص ناهنجاری[۸۱] استفاده کرد.

ـ برای بدافزارهای چند ریخت[۸۲] از روش‌های دیده‌بانی و سند باکس و تشخیص ناهنجاری استفاده کرد.

شکل ۲. مدل ارزیابی روش‌های تشخیص کُدهای مخرب



مأخذ: Shevchenko, 2008

ـ برای بدافزارهای که قابلیت شناسایی محیط را دارند می‌توان از روش‌های بررسی امضا، تشخیص ناهنجاری و ابزارهای دیده‌بانی بهره برد.

۳. بدافزار نویس‌ها به‌طور کامل از وضعیت سامانه‌های دفاعی و امنیتی هدف مطلع نیستند.

۴. نویسندگان سامانه‌های دفاعی و امنیتی نیز به‌طور کامل از روش‌ها و راه‌حل‌های به‌کارگرفته‌شده توسط نویسندگان بدافزار و اهداف آن‌ها مطلع نیستند و پس از تحلیل و مهندسی معکوس می‌توانند ویژگی‌ها و قابلیت‌های آن‌ها را استخراج کنند.

۵. اهداف اصلی نویسندگان بدافزارها تخریب اطلاعات، از کار انداختن، دزدی و جاسوسی اطلاعات، بهره‌برداری از منابع سیستم و سایر اهداف مرتبط است.

۶. اهداف اصلی سامانه‌های دفاعی امنیتی حفاظت از زیرساخت‌های سایبری هدف و حفظ امنیت، یکپارچگی و دسترسی آن است.

78. virtualization
79. sandbox
80. stealth
81. anomaly detection
82. polymorphism

٤. ٢. ویژگی‌ها و شرایط بازی

در این بازی، با توجه به تعداد بازیگران و راهبردهای مختلف هر کدام، نمایش وضعیت‌های بازی را از طریق حالت‌های گراف و حالت انتخابی نمایش می‌دهیم و با توجه به نوع تعاملات بازیگران، انتخاب و تغییر راهبردها، به‌صورت متوالی و انتخابی است. با توجه به اینکه هر کدام از بازیگران تمایل به ضربه زدن به رقیب دارند و تمایل دارند موفقیت بیشتری در راستای اهداف خود داشته باشند، بازی غیر همکارانه است. همان‌طور که دیده شده است، ابتدا نویسندگان بدافزار به‌وسیلهٔ یک بدافزار در راستای اهداف تعیین‌شده شروع کنندهٔ بازی هستند و پس‌از آن، تحلیل گران امنیتی با روش‌های شناسایی سعی در مقابله با بدافزار موردنظر می‌نمایند؛ بنابراین مدل‌سازی تعاملات به‌صورت متوالی و انتخابی، گزینه مناسبی برای این بازی است.

به‌طور کلی، این بازی با توجه به اهداف بازیگران در همه پیامدها یک بازی مجموع غیر صفر است. برای مثال، وقتی یک بدافزار به‌آسانی تحلیل گردد اما به دلیل تنوع زیاد آن شناسایی نشود، هر دو بازیگر پیامد مثبتی از عایدی‌های به دست خواهند آورد؛ چراکه هم تحلیل‌شده و هم به‌طور کامل شناسایی نشده است.

تحلیل گران سامانه‌های امنیتی، قبل از اجرای راهبردهای خود، راهبرد رقیب را رصد و متناسب با نوع اقدام آن، عمل می‌کنند و با توجه به اینکه تحلیل گران سامانه‌های امنیتی از اقدامات و راهبردهای قبلی بدافزارنویسان به‌طور کامل مطلع نیستند، این بازی از نوع بازی ناقص[۸۳] است و به علت اینکه واقعاً اطلاعات در خصوص مجموعه فعالیت‌ها و منفعت بازیگران به‌طور کامل مشخص نیست، این بازی یک بازی با اطلاعات ناقص[۸۴] است (Bedi & Shiva, 2012).

٤. ٣. بازیگران و راهبردهای آنان

ابزارهایی که بدافزارنویسان جهت تخریب و بهره‌برداری از اهداف خود استفاده می‌کنند، شامل تروجان، کرم، ویروس و... است و برنامه کاربردی که به‌وسیلهٔ این کُد آلوده شده است، نیز می‌تواند به‌عنوان نماینده‌ای از اقدامات بدافزار نویسان قلمداد شود. در ضمن، اگر سیستم‌عامل نیز توسط این کُد مخرب آلوده شده باشد، کلّ ماشین نیز می‌تواند به‌عنوان نماینده‌ای از بدافزارنویسان جهت اقدامات بعدی قلمداد شود و در سطوح پیچیده‌تر شبکه، ماشین آلوده‌شده نیز می‌تواند به‌عنوان نماینده خوبی برای بدافزار نویسان در نظر گرفته شود.

نمایندهٔ تحلیل گران سامانه‌های امنیتی در این بازی، شرکت‌های ضدبدافزار هستند که با به‌روزرسانی بانک‌های اطلاعاتی خود، قصد دفاع در برابر تهاجم بدافزارها دارند و به‌طور خاص‌تر می‌توانند آزمایشگاه‌های تحلیل بدافزار شرکت‌های ضد بدافزار باشد که بدافزارها را به‌صورت تخصصی‌تر تجزیه‌وتحلیل می‌کنند و این ضدبدافزارها شخصاً می‌توانند نماینده‌ای از طرف سامانه‌های امنیتی باشند که با روش‌های مختلف سعی دارند بدافزارها را شناسایی کنند. پس، این بازی دو بازیگر دارد که عبارت‌اند از نویسندگان بدافزارها با نمایندگی بدافزارها و تحلیل گران سامانه‌های امنیتی و یا نمایندگی

83. imperfect information
84. incomplete information

ضد بدافزارها و هر کدام از بازیگران جهت مغلوب کردن رقیب خود متناسب با شرایط و اهداف بازی از راهبردهای متنوعی استفاده می کنند (Singh et al, 2010). از آنجا که در این رقابت، هدف انتخاب و اجرای راهبردها قبل از طراحی و تولید بدافزار است، راهبردها متناسب با مأموریت‌های بدافزار و راهکارهای دفاعی تعیین‌شدهٔ طراحان، انتخاب می گردند؛ بنابراین، در این رقابت خود نویسندگان و طراحان بدافزار و سامانه‌های امنیتی را به‌عنوان بازیگران، مدنظر قرار گرفته است.

گزینه‌های بازیگران، با توجه به ماهیت و اهداف آن‌ها در گذشته و ویژگی‌های خودمحافظتی بدافزارها و...، قابل تعریف است. به علت اینکه تحلیل گران سامانه‌های امنیتی و ضد بدافزارها باید به‌طور خودکار و همانند یک سامانهٔ یادگیرنده عمل کنند تا بدافزارهای قدیمی و نوین را شناسایی کنند و مانع رفتارهای بداندیش آن‌ها شوند، راهبردهای متنوعی دارند و در مقاطع زمانی مختلف راهبردهای نوینی را به مجموعه راهبردهای خود اضافه می کنند. برای هر بازیگر، اقداماتی به شرح جدول ۲ قابل تعریف است؛ در این بازی، بدافزارها سعی دارند ضمن اجرای مأموریت خود، با توجه به تعاریف مختلف پایداری فردی مندرج در جدول ۱، از خود محافظت کنند تا ضد بدافزارها آن‌ها را شناسایی نکنند و، در ضمن، ضد بدافزارها سعی دارند، ضمن شناسایی بدافزارها، جلو اهداف بداندیش آن‌ها را بگیرند (Shevchenko, 2008).

جدول ۲. اقدامات ممکن برای بازیگران رقابت

Players	ID	Strategy	Summarized
malware authors (MA)	1	Code Morphism: e.g. Polymorphism	Polymorphism
	2	Stealth: e.g. Rootkits.	Rootkit
	3	Environment Diagnostics: e.g. VM detection, debugger detection, emulator detection, AV software detection and disabling.	Diagnostic
security analysts (SA)	1	File scanning	Scanning
	2	System event monitoring	Monitoring
	3	Global system state anomaly detection	Anomaly
	4	Emulation	Emulation

مأخذ: Shevchenko, 2008

٤. ٤. حالت‌های شدنی بازی

راهبرد هر بازیگر، یک انتخاب از بین تمام اقداماتِ ممکنِ آن بازیگر است. براساس اطلاعات مندرج در جدول ۲، بازیگران این بازی جمعاً ۷ اقدام بالقوه دارندَ که در راهبرد انتخابی خود می‌توانند آن‌ها را اختیار کنند یا نکنند؛ بنابراین، تعداد ترکیب‌های این بازی به لحاظ نظری، ۲ به توان ۷ یا ۱۲۸ حالت است، ولی با اعمال محدودیت‌ها و حذف ترکیب‌های ناممکن، تعداد وضعیت‌های ممکن به ۱۵ وضعیت تقلیل می‌یابد. حالت‌های نشدنی متأثر از قیدها و محدودیت‌هایی است که باید به این بازی اعمال کرد که عبارت‌اند از:

ـ وجود حداقل یک گزینه:[85] این محدودیت بیان می‌کند که بازیگر باید حداقل یکی از اقدامات ممکن هر بازیگر را انتخاب کند.

ـ گزینه‌های دوبه‌دو ناسازگار:[86] پس از اعمال این قید، ترکیب‌هایی که در آن گزینه‌ها نمی‌توانند در کنار هم قرار گیرند، از ترکیب‌های بالقوه حذف می‌شوند.

ـ وابستگی بین گزینه‌ها:[87] با اعمال این قید، رخداد یا عدم رخداد یک گزینه را مشروط به رخداد یا عدم رخداد گزینه‌های دیگر می‌کنیم.

لذا محدودیت‌هایی به شرح زیر برای بازیگران اعمال می‌گردد:

ـ وجود حداقل یک گزینه: بدافزارنویسان برای نوشتن بدافزار، باید حداقل از یکی از سه راهبرد تعریف‌شده استفاده کنند تا شناسایی آن‌ها از طریق سامانه‌های امنیتی به حداقل ممکن برسد و ضمن حفاظت از خود، بتواند به اهداف موردنظر دسترسی یابد. تحلیل‌گران سامانه‌های امنیتی نیز برای مقابله با این بدافزار حداقل باید از یکی از راهکارهای امنیتی خود جهت مقابله با بدافزارها استفاده کنند.

ـ وابستگی بین گزینه‌ها: تحلیل‌گران سامانه‌های امنیتی برای مقابله با ویژگی‌های استفاده‌شده توسط بدافزارنویسان، باید از روش‌های مقابله مربوطه استفاده کنند. برای مثال، برای بدافزاری که فشرده‌شده است، باید از راهکارهای بررسی رفتار فایل و ابزارهای دیده‌بانی استفاده شود.

جدول ۳. حالت‌های نشدنی بازی متناسب با محدودیت‌های مختلف

Players	ID	Strategy	At least one option		Option dependence				
			1	2	1	2	3	4	5
MA	1	Polymorphism	Y	-	Y	-	-	Y	Y
	2	Rootkit	Y	-	-	Y	-	N	Y
	3	Diagnostic	Y	-	-	-	Y	N	Y
SA	1	Scanning	-	Y	N	-	-	N	Y
	2	monitoring	-	Y	Y	Y	-	Y	Y
	3	Anomaly	-	Y	Y	Y	Y	Y	Y
	4	Emulation	-	Y	-	-	Y	-	Y

مطابق جدول ۳ و پس از حذف حالت‌های نشدنی از ۱۲۸ ترکیب بالقوه، تنها ۱۵ وضعیت ممکن است اتفاق بیفتد. حالت‌های ممکن این بازی که به فرم گزینه‌ای[88] ارائه شده است در جدول ۴ نمایش داده شده‌اند.

85. at least one option
86. mutually exclusive options
87. option dependence
88. option form

جدول ٤. حالت‌های ممکن بازی پس از اعمال محدودیت‌های بازی

DMs	Options	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
MA	Polymorphism	Y	N	Y	N	N	N	N	Y	N	Y	N	Y	N	N	N
	Rootkit	N	Y	Y	Y	N	N	Y	Y	N	N	Y	Y	Y	N	Y
	Diagnostic	N	N	N	N	Y	Y	N	N	Y	Y	Y	Y	N	Y	Y
SA	Scanning	N	N	N	Y	N	Y	N	N	N	N	N	N	Y	Y	Y
	Monitoring	Y	Y	Y	Y	N	N	Y	Y	Y	Y	Y	Y	Y	Y	Y
	Anomaly	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
	Emulation	N	N	N	N	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y

در هر وضعیت، انتخاب گزینه‌ها به‌صورت Y یا N مشخص شده است. مثلاً، وضعیت ۳ بیان کنندهٔ این حالت است که اگر بدافزارنویسان از ویژگی‌های چندریختی و اجرا در سطح هستهٔ سیستم‌عامل در بدافزار خود استفاده کنند، تحلیل‌گران سامانه‌های امنیتی جهت تشخیص و مقابله با آن، از راهبردهای رصد و سامانه کشف ناهنجاری استفاده می‌کنند.

٤. ٥. ترجیحات بازیگران

برای تعیین ترجیحات بازیگران در نظریهٔ بازی، روش‌های مختلفی شامل ترجیح مستقیم، اولویت‌بندی راهبردها و وزن‌دهی به راهبردها وجود دارد. در این بازی هم از روش وزن‌دهی به راهبردها مطابق نظر بازیگران و هم از روش اولویت‌بندی مستقیم ترجیحات بهره‌برداری شده است. پس از وزن ده‌دهی به راهبردها، ترجیحات بازیگران و اولویت‌گذاری مستقیم، براساس آن پیامدهای بازی مشخص می‌شود. همان‌طور که در جدول ۵، ترجیحات نویسندگان بدافزار و سامانه‌های امنیتی مشخص‌شده است (اهمیت ترجیحات از سمت چپ به راست کاهش می‌یابد) برای بدافزارنویسان وضعیت ۱ بالاترین اولویت و وضعیت ۱۳ کمترین اولویت را دارد. لازم به ذکر است برای تعیین این ترجیحات، ضمن استفاده از نظرهای خبرگان حوزهٔ بدافزار، از نتایج گزارش‌های تحلیلی آزمایشگاه‌های معتبر نیز استفاده‌شده است.

جدول ۵. ترجیحات ترتیبی بازیگران روی پیامدهای مختلف

DMs	Preferences: High Priority to Low Priority														
MA	1	2	4	3	6	5	7	9	14	11	10	12	8	15	13
SA	14	13	15	10	9	12	11	7	8	5	6	2	4	1	3

بدافزارنویس‌ها، متناسب با فناوری، نقاط ضعف سامانه‌های امنیتی، بودجه‌های موردنیاز، سعی دارند از حداقل بودجه حداکثر بهره‌وری را داشته باشند تا بتوانند حداکثر اهداف خود را به اجرا بگذارند. در ضمن، نویسندگانِ سامانه‌های امنیتی متناسب بااهمیت نوع زیرساخت، سعی دارند با اجرای راهبردهای مختلف از اجرای اَهداف بدافزارها جلوگیری کنند.

٤. ٦. شبیه‌سازی و تحلیل نتایج بازی

نتایج حاصل از مدل‌سازی رقابت بازیگران براساس منطقه‌ای مختلف بررسی و وضعیت‌های تعادلی بازی ارائه می‌شود. برای مدل‌سازی و شبیه‌سازی این بازی، مدل گراف برای حل مناقشه به‌عنوان روش مدل‌سازی و برای شبیه‌سازی و تحلیل بازی از نرم‌افزار GMCR II استفاده شده است. این ابزار، ضمن تعریف بازیگران و راهبردهای آن‌ها، بازی را ازلحاظ بررسی نقاط تعادل و ائتلافی از دیدگاه‌های مختلف بررسی و نتایج را ارائه می‌کند.

٤. ٧. تحلیل بازی

برای به دست آوردن وضعیت تعادل بازی، ابتدا باید وضعیت‌های پایدار[89] برای هر بازیگر را به دست آورد. وضعیت پایدار یعنی وضعیتی که بازیگر تمایلی برای خروج از آن حالت نداشته باشد. اگر همهٔ بازیگران در یک وضعیت پایدار باشند، آن را وضعیت تعادل می‌گویند. بنابراین وضعیت‌های ۱، ۴، ۵، ۶، ۷، ۹، ۱۱ و ۱۴ از نظر نویسندگان بدافزارها و وضعیت‌های ۱، ۸، ۱۰، ۱۲، ۱۳، ۱۴ و ۱۵ از نظر تحلیل‌گران سامانه‌های امنیتی از جدول ۴ مطابق منطق‌های بیان‌شده در جدول ۱، وضعیت‌های پایداری است و ماندن در این وضعیت برای این بازیگر مناسب‌تر از انتقال به سایر وضعیت‌های دیگر است و این نشانی از احتمال وجود وضعیت تعادل در بازی است که با مقایسه آن با وضعیت پایداری رقیب می‌توان وضعیت‌های تعادلی بازی را بیان کرد.

٤. ٨. وضعیت‌های تعادل و ائتلافی بازی

وضعیت‌های تعادل و تفسیر آن‌ها:

پس از اعمال روش‌های گوناگون محاسبهٔ وضعیت تعادل، براساس منطق‌های مختلف، مطابق جدول ۶، وضعیت‌های تعادل بازی مشخص می‌شود. در ادامه، وضعیت‌های تعادل بازی تفسیر می‌گردد.

جدول ٦. وضعیت‌های تعادل بازی

ردیف	نوع تحلیل	وضعیت‌های تعادل	
		۱	۱۴
۱	R	✓	✓
۲	GMR	✓	✓
۳	SMR	✓	✓
۴	SEQ	✓	✓
۵	NM	✓	✓

89. stable states

وضعیت ۱:

براساس جدول ۴ که در آن وضعیت‌های بازی فهرست شده‌اند، در وضعیت ۱، بدافزارنویسان سعی می کنند با توجه به هزینهٔ تولید بدافزار و همچنین مکانیسم‌های دفاعی نسبت به سایر وضعیت‌ها، از فنّاوری‌های چندریختی جهت اعمال مکانیسم خودمحافظتی از بدافزار در مقابل سامانه‌های امنیتی استفاده کنند و تحلیل گران سامانه‌های امنیتی جهت تشخیص و تحلیل این نوع از بدافزارها از روش‌های دیده‌بانی رفتار بدافزار و تشخیص ناهنجاری استفاده خواهند کرد. درصورتی که بازیگران تمایل داشته باشند از این وضعیت تغییر حالت دهند، امکان شناسایی بدافزار، مغلوب شدن سامانه‌های دفاعی و یا سایر پیامدهای غیر مطلوب بازیگران ایجاد خواهد شد، بنابراین، بازیگران تمایلی به تغیر وضعیت ندارند و در این حالت پایدار خواهند ماند.

وضعیت ۱۴:

با توجه به ویژگی‌های راهبرد شناسایی محیط توسط بدافزارها، به‌خصوص محیط‌های تحلیل گر، بدافزارنویسان از این راهبرد، جهت مخفی ماندن از سامانه‌های دفاعی و خودمحافظتی بدافزار استفاده می کنند و از آنجا که سامانه‌های دفاعی باید توانایی مقابله با هر نوع بدافزاری را داشته باشند از تمامی قابلیت‌های خود بهره می‌برند؛ درصورتی که غیر از این باشد، بدافزارها با استفاده از سست‌ترین حلقهٔ امنیتی سامانه‌های دفاعی، اهداف مدّنظر طراحان را اجرا و سامانه‌های دفاعی را مغلوب می کنند.

٤. ٩. تحلیل حساسیت

یکی از روش‌های تعیین قابل‌اعتماد بودن نتایج کسب‌شده از حل مسئله، تحلیل حساسیت بازی است؛ بدین‌صورت که با تغییر جزئی اولویت‌های بازیگران نباید نتایج مدل‌سازی و وضعیت‌های تعامل به‌صورت گسترده‌ای تغییر کند. پس، در این بازی، اولویت‌های بازیگران به‌صورت محدود تغییر داده شده ولی نتایج مدل‌سازی همان نتایج اولیه، یعنی نقاط تعادل و ائتلاف، باقی ماند. می توان نتیجه گرفت که نقاطِ تعادل به‌دست‌آمده نقاطِ تعادل پایدار و قابل‌اعتمادی هستند.

٤. ١٠. تحلیل و ارزیابی نتایج بازی

با توجه به نتایج به‌دست‌آمده از بازی و وضعیت‌های تعادلی بر مبنای عقلانیت‌های مختلف، می‌توان موارد زیر را در خصوص این مناقشه بیان کرد:

ـ یکی از راهبردهایی که بدافزارنویسان از آن نهایتِ استفاده را، جهت شناسایی نشدن از طریق سامانه‌های دفاعی و امنیتی، می کنند، چندریختی است که راهکارهای مقابله با آن، استفاده از ابزارهای دیده‌بانی و تشخیص ناهنجاری در سامانه‌ها است. بنابراین، لازم است سامانه‌ها و ابزارهایی بروز این حوزه جهت محافظت از زیرساخت‌ها حساس، به‌کار گرفته شود.

ـ یکی دیگر از راهبردهای بدافزارها شناسایی و تشخیص سامانه‌های دفاعی ـ امنیتی و دور زدن آن‌ها است. پس، باید در سامانه‌های هدف، از قابلیت‌های مختلف نظیر شناسایی براساس امضا،

سامانه‌های نظارتی و رصد رفتارها، سامانه‌های تشخیص ناهنجاری و... جهت مراقبت از زیرساخت‌ها و مقابله با این فن استفاده کرد.

ـ بدافزارهای اساسیِ تولیدی سعی می‌کنند متناسب با اهداف خود، از دانش‌ها و فناوری‌های خاص و ناشناخته متناسبَ با زیرساخت اهداف بهره‌برداری کنند.

ـ تحلیل گران سامانه‌های امنیتی در برابر آثارِ تخریبی بدافزارها ریسک نمی‌کنند و از همهٔ قابلیت‌ها و دانش‌های حوزهٔ امنیت جهت مقابله با بدافزارها، استفاده می‌کنند.

ـ نمونه‌های اخیر بدافزارها بیانگر مطالب فوق است که بدافزار تولیدی از دانش‌های خاص‌منظوره حوزهٔ بدافزار استفاده می‌کنند.

ـ با توجه به اهمیت زیرساخت‌های سایبری، تحلیل گران سامانه‌های امنیتی متناسب با زیرساخت‌ها و بدون توجه به هزینه‌های تولید سامانه‌های دفاعی، از تمامی دانش‌ها و فناوری‌های حوزه امنیت و ضد بدافزار استفاده می‌کنند.

ـ با توجه به تأثیرات بدافزارها در زیرساخت‌های اساسی کشور، مثل مجموعهٔ اقدامات بدافزار استاکس‌نت، توجه مسئولین و متخصصان حوزهٔ امنیت فضای سایبری، نسبت به سال‌های گذشته تغییریافته و پیشرفت‌های مطلوبی در این زمینه صورت گرفته است که نتایج تحقیق تأییدی بر این موضوع است.

۵. نتیجه

در این مقاله، یکی از چالش‌های حوزهٔ فضای سایبری یعنی رقابت بین نویسندگان بدافزارها و تحلیل گران سامانه‌های امنیتی با استفاده از نظریهٔ بازی و براساس مدل گراف برای تحلیل مناقشات مدل‌سازی شده است. نتایج متأثر از تحلیلِ مدل دو وضعیت را به‌عنوان نقاط تعادل بازی نشان می‌دهد. در وضعیت اول، بدافزارنویسان از راهبرد چندریختی و سامانه‌های دفاعی از راهبرد مقابله‌ای دیده‌بانی و تشخیص ناهنجاری استفاده می‌کنند و در وضعیت دوم، بدافزارنویسان از راهبرد تشخیص محیط و سامانه‌های دفاعی از همهٔ راهبردهای دفاعی، جهت مقابله با آن، بهره‌برداری می‌کنند. با توجه به نتایج تحلیلی بازی و گزارش‌ها و عملکردهای سامانه‌های امنیتی و بدافزارها موارد زیر قابل پیش‌بینی هست:

ـ بدافزارنویسان متناسب با اهداف، بدافزارهای خاص‌منظوره تولید می‌کنند و سعی در بهره‌برداری از آسیب‌پذیری‌های ناشناخته خواهند داشت.

ـ با توجه به تعیین محتمل‌ترین سناریوی بدافزارنویسان، سامانه‌های دفاعی جهت مقابله، باید بهترین و ایمن‌ترین راهبردهای دفاعی را انتخاب کنند؛ بنابراین، سعی می‌کنند از همهٔ قابلیت‌های دفاعی بهره‌برداری کنند.

نتایج حاصل از مدل‌سازی این بازی نیز نتایج بیان‌شده را به‌صورت مشهود ارائه کرده است. تحلیل حساسیت صورت‌گرفته بر روی مدل نشان می‌دهد که تغییر جزئی اولویت‌های بازیگران اثری بر خروجی‌های مدل یعنی وضعیت‌های تعادل ندارد.

در پایان، پیشنهاد می‌کنیم که با توجه به شرایط فضای سایبر و وجود عدم قطعیت‌ها در خصوص شناخت کامل مهاجم و مدافع از رفتارهای یکدیگر، براساس نتایج تحقیق و توسعهٔ آن، سامانه‌های پیش‌فعال و تخمین‌گری تهیه کرد که قبل از اجرای اقدامات مهاجم، راهبردها و اهداف مدّنظر وی مشخص شود تا سناریوهای دفاعی متناسب، شناسایی و پیاده‌سازی گردد؛ همچنین می‌توان با شناخت دقیق‌تر و کامل‌تر رفتار بازیگران، براساس نوع اقدامات و راهبردهای به‌کارگرفته‌شدهٔ آن‌ها در گذشته، در یک مدل یادگیر با بهره‌گیری از راهبردهای گذشته، رفتارها و راهبردهای آینده را تخمین زد.

کتابنامه

Bedi, H. S. & Shiva, S. 2012. "Securing cloud infrastructure against co-resident DoS attacks using game theoretic defense mechanisms". Paper presented at the Proceedings of the International Conference on Advances in Computing, Communications and Informatics, Chennai, India.

Bencsáth, B., Pék, G., Buttyán, L. & Félegyházi, M. 2012. "Duqu: Analysis, detection, and lessons learned". Paper presented at the ACM European Workshop on System Security (EuroSec).

Brams, S. J., & Mattli, W. 1993. "Theory of moves: overview and examples". *Conflict Management and Peace Science*. 12 (2). pp 1-39.

Brams, S. J., & Wittman, D. 1981. "Nonmyopic equilibria in 2× 2 games". *Conflict Management and Peace Science*. 6 (1). pp 39-62.

Calvet, J. 2015. "Dino – the latest spying malware from an allegedly French espionage group analyzed". Retrieved from http://www.welivesecurity.com/2015/06/30/dino-spying-malware-analyzed/

Daniel, J. & saeed, P. 2015. "Provide a safe environment for malware analysis". *Electronic and cyber defense Journal*. 5 (3). pp 65-73.

Falliere, N., Murchu, L. O., & Chien, E. 2010. "W32. Stuxnet dossier". White paper, Symantec Corp. Security Response. 5.

Fang, L., Hipel, K. W., & Kilgour, D. M. 1993. *Interactive decision making: The graph model for conflict resolution* (Vol. 3): John Wiley & Sons.

Fraser, N. M. & Hipel, K. W. 1984. *Conflict analysis: models and resolutions*. Vol. 11. North-Holland.

Howard, N. 1971. "Paradoxes of Rationality: Theory of Metagames and Political Behavior". MIT Press.

Howard, N. 1987. "The present and future of metagame analysis". *European Journal of Operational Research*. 32 (1). pp 1-25.

Howard, N. 1994. "Drama theory and its relation to game theory". *Part 1: dramatic resolution vs. rational solution. Group Decision and Negotiation*. 3 (2). pp 187-206.

Khouzani, M. H. R., Sarkar, S., & Altman, E. 2011. "A dynamic game solution to malware attack". Paper presented at the INFOCOM, 2011 Proceedings IEEE.

Khouzani, M., Sarkar, S., & Altman, E. 2012 a. "Maximum damage malware attack in mobile wireless networks". Networking, *IEEE/ACM Transactions on*, 20 (5). pp 1347-1360.

Khouzani, M. H. R, Sarkar, S., & Altman, E. 2012 b. "Saddle-Point Strategies in Malware Attack". *IEEE Journal on Selected Areas in Communications*, 30(1), 31-43. doi:10.1109/JSAC.2012.120104

Nash, J. 1951. "Non-cooperative games. Annals of mathematics". pp 286-295.

Peng, W., Li, F., Zou, X., & Wu, J. 2014. "Behavioral malware detection in delay tolerant networks". *Parallel and Distributed Systems, IEEE Transactions on,* 25(1). pp 53-63.

Rashidi, B., & Fung, C. 2015. "Disincentivizing Malicious Users in RecDroid Using Bayesian Game Model". *Journal of Internet Services and Information Security (JISIS)*. 5 (2). pp 33-46.

Sandholm, T. 2015. "Abstraction for Solving Large Incomplete-Information Games". Paper presented at the AAAI.

Schmidt, S., Alpcan, T., Albayrak, Ş., Başar, T. & Mueller, A. 2007. "A malware detector placement game for intrusion detection Critical Information Infrastructures Security". pp 311-326. Springer.

Sheikhmohammady, M., Bitalebi, H., Moatti, A., & Hipel, K. W. 2013, "Formal Strategic Analysis of the Conflict over Syria". Paper presented at the 2013 IEEE International Conference on Systems, Man, and Cybernetics.

Sheikhmohammady, M., Hipel, K. W., Asilahijani, H., & Kilgour, D. M. 2009. "Strategic analysis of the conflict over Iran's nuclear program". Paper presented at the Systems, Man and Cybernetics, 2009. SMC 2009. IEEE International Conference on.

Shevchenko, A. 2008. "Malicious Code Detection Technologies. Kaspersky Lab".

Singh, A., Lakhotia, A. & Walenstein, A. 2010. "Malware antimalware games". Paper presented at the International Conference on Information Warfare and Security.

Takahashi, M. A., Fraser, N. M. & Hipel, K. W. 1984. "A procedure for analyzing hypergames". *European Journal of Operational Research*, 18 (1). pp. 111-122.

Zagare, F. C. 1984. "Limited-move equilibria in 2× 2 games". *Theory and Decision*, 16 (1). pp 1-19.

Zolotukhin, M., & Hamalainen, T. 2013. "Support vector machine integrated with game-theoretic approach and genetic algorithm for the detection and classification of malware". Paper presented at the Globecom Workshops (GC Wkshps). 2013 IEEE.