مجله علمی- پژوهشی "پدافند الکترونیکی و سایبری"
ویژه نامه کنفرانس ترکیبیات، رمزنگاری و محاسبات، ص ۱۳۸-۱۵۲

ارائه چارچوبی برای دفاع سایبری فعال در برابر حملات سایبری پیشرفته

رحیم اصغری[۱]، حسین باقری[۲]، محمدعلی میرزازاده[۳]

۱- استادیار، ۲- دانشجوی کارشناسی ارشد، دانشگاه صنعتی مالک اشتر ۳- استادیار، دانشکده فنی مهندسی شرق گیلان، دانشگاه گیلان
(دریافت: ۹۸/۹/۱۰، پذیرش: ۹۹/۰۲/۱۵)

چکیده

به همراه رشد تهدیدات سایبری، تکنیک‌های امنیتی جهت مقابله با آن‌ها هم رشد می‌کنند. راه‌حل‌های مختلف دفاعی برای مقابله با حملات سایبری پیشرفته و نوظهور وجود دارند. هدف از ایجاد مفهوم دفاع سایبری فعال و به‌کارگیری تکنیک های برخاسته از این مفهوم، پدافند سایبری کشور را در برابر حملات پیشرفته سایبری علیه زیرساخت‌های ملی ارتقاء می‌دهد. در این مقاله، بر آنیم که مفهوم دفاع سایبری فعال و مؤلفه‌های آن ارائه شود. هم‌چنین، مقدمات لازم برای اجرای دفاع سایبری فعال به همراه گام‌های اولیه برای رسیدن به آمادگی، جهت هدایت مأموریت‌های دفاع سایبری فعال ارائه شد. برای اولین بار در حوزه دفاع سایبری، مأموریت‌های دفاع سایبری فعال دسته‌بندی و انواع آن بیان‌شده است که چارچوبی برای دفاع سایبری فعال خواهند بود. با توجه به مورد کاوی انجام‌شده، نتایج حاصل از به‌کارگیری مدل‌ها، روش‌ها، چارچوب و تکنیک دفاع سایبری فعال حاکی از بهبود پدافند سایبری خواهد شد.

واژه‌های کلیدی: امنیت سایبری، دفاع سایبری فعال، تهدیدات سایبری، حملات سایبری، دارایی‌های سایبری

۱- مقدمه

متخصصان امنیت و دفاع سایبری با پیگیری و مشاهده مستمر سرخط گزارش‌های مربوط به حملات سایبری به این نتیجه رسیده‌اند که حملات سایبری هرروز پیچیده‌تر و مخرب‌تر می‌شوند. با بررسی و تحلیل روند توسعه جهانی درزمینه امنیت سایبری، به‌وضوح دیده می‌شود که اکثر سازمان‌ها در حال تلاش برای توسعه و ارتقای امنیت قلمرو سایبری خود هستند. بر اساس تحقیقاتی که در سال ۲۰۱۴ در اروپا انجام‌شده است، ۴۹ درصد مردم انتظار داشتند که بودجه‌های امنیتی آن‌ها حداقل"نسبت به سال قبل" همان مقدار باقی بماند و کاهش نداشته باشد. اگرچه نتایج نظرسنجی در سال ۲۰۱۵، کاهش این مقدار بودجه به۳۹٪ را نشان می‌دهد ولی ۵ درصد سازمان‌ها، بودجه‌های امنیتی خود را بین ۵٪ تا ۲۵٪ افزایش داده اندو بقیه سازمان‌ها هم بودجه امنیتی خود را ثابت نگه‌داشته‌اند. از طرف دیگر توانمندی به‌کارگیری مؤثر منابع امنیتی اختصاص داده‌شده، از چالش‌های مهم سازمان‌ها به شمار می‌رود. در یک نظرسنجی صورت گرفته در اروپا، هفتادویک درصد از پاسخ‌دهندگان بیان کردند، احتمال این‌که سازمان آن‌ها بتواند یک حمله پیچیده سایبری را تشخیص دهند کمتر از ۵۰٪ است.

هم‌چنین، ۶۲ درصد پاسخ‌دهندگان شایع‌ترین موانع برای کارایی برنامه امنیتی را، "محدودیت بودجه" و۵۷ درصد آن‌ها بزرگ‌ترین مانع را " فقدان توانمندی و مهارت لازم" دانستند. طی بررسی‌های صورت گرفته در سال ۲۰۱۵، میانگین زمان سپری‌شده برای کشف یک حمله سایبری ۲۰۵ روز بوده است که نشان از پایین بودن سرعت تشخیص حملات سایبری دارد. سؤال مهم و اساسی که مطرح می‌شود و باید به آن پاسخ داده شود این است که برای بهبود امنیت قلمرو سایبری چه ابزاری لازم است؟ متخصصان حوزه سایبر معتقدند که پاسخ این سؤال دفاع سایبری فعال هست[1, 2, 3]. در حال حاضر دفاع سایبری فعال یکی از مهم‌ترین روش‌های مبارزه با حملات سایبری است که برخلاف روش‌های دفاعی متعارف نظیر فیلترسازی مبتنی بر دیواره آتش و ابزارهای ضد بدافزاری، دفاع سایبری فعال می‌تواند از طریق تولید و انتشار حملات سفید و خوش‌خیم به مبارزه با بدافزارهای مهاجمان بپردازد[4, 5, 6].

در گزارش انجمن تحقیقات ملی(NCR) تحت عنوان « سیاست، قانون و اصول اخلاقی فناوری»، نویسندگان به‌طور خلاصه بر روش‌های دفاع سایبری فعال نظیر جمع‌آوری اطلاعات غیر مشارکتی، ضد حمله و دفاع پیش‌دستانه دست گذاشته‌اند[7]. جمع‌آوری اطلاعات غیر مشارکتی به مفهوم جمع‌آوری اطلاعات در موردحمله و حمله‌کننده از طریق استفاده از هر نوع ابزار یا وسیله‌ای می‌باشد. ضد حمله(حمله متقابل) به معنای هک کردن متقابل سیستم یک حمله‌کننده است. دفاع

[۱] رایانامه نویسنده مسئول: meisam.mathhome@gmail.com

پیش‌دستانه به معنای هدایت یک حمله به سیستم یا شبکه دشمن است و این‌زمانی رخ می‌دهد که هدایت یک حمله حتمی توسط دشمن بر روی سیستم قربانی، پیش‌بینی‌شده باشد. باوجوداینکه این اقدامات به‌ویژه ازنظر قانونی بودن و مشروعیت آن‌ها خیلی بحث‌انگیز است، ممکن است این اقدامات به نوآوری و ارائه چیز جدیدی در کل وضعیت دفاع سایبری منجر شود [9, 10, 11].

تاکنون تحقیقات مختلفی در زمینه مدل‌های ریاضی بدافزارهای رایانه‌ای انجام‌شده است. این مدل‌ها از مدل‌های ریاضی که در ابتدا برای مطالعه انتشار ویروس رایانه‌ای در دهه 1990 ایجاد شدند نشاءت می‌گیرند. همه این مدل‌ها این فرض همگن را تشکیل دادند که هر فرد(نظیر رایانه) در یک جمعیت دارای اثر آلودگی برابری نسبت به دیگر افراد حاضر در آن جمعیت است و فرض این است که افراد آلوده‌شده به دلیل دفاع واکنشی بهبود می‌یابند (نظیر ابزار ضد بدافزار)[13, 15, 16].

در دهه اخیر، مطالعات زیادی بر روی ترکیب آشکار ساختارهای شبکه‌ای ناهمگن صورت گرفته باهدف حذف کردن فرض ناهمگن بودن انجام‌گرفته است [17, 18, 19, 20, 21]. ابزارهای ریاضی استفاده‌شده در این مطالعات، سامانه‌ها دینامیکی هستند. این تحقیقات اثبات نمودند که اثر حمله انتشار بدافزار در برابر دفاع واکنشی به‌طور خودکار توسط مقدار مشخصه ماتریس هم‌جواری تقویت می‌گردد که بیانگر ساختار شبکه‌ای پیچیده پنهان است. این پدیده عدم تقارن حمله و دفاع نامیده می‌شود. پدیده عدم تقارن حمله و دفاع، انگیزه‌ای برای مطالعه مدل‌های ریاضی دفاع سایبری فعال‌شده است که یکی از زمینه‌های نسبتاً جدید در امنیت سایبری محسوب می‌شود چراکه کاوش‌های قبلی عمدتاً در جهت مباحث حقوقی و سیاستی انجام می‌شدند.

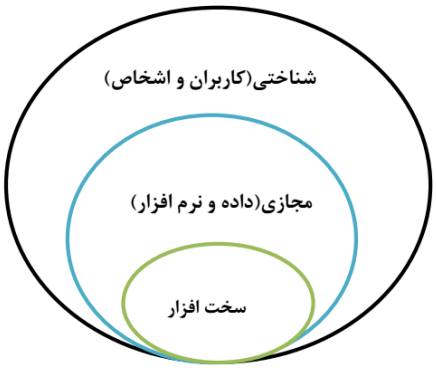
درزمینه به‌کارگیری نظریه کنترل و نظریه بازی‌ها در درک مباحث مختلف مرتبط با انتشار بدافزار رایانه‌ای تحقیقات زیادی شده است[22, 23, 24]. مطالعه ما تا حدودی از مدل دفاع سایبری فعال که موردبررسی قرارگرفته است، الهام می‌گیرد. برای کسب اطلاعات کلی درزمینه به‌کارگیری نظریه کنترل و نظریه بازی‌ها در امنیت سایبری می‌توان به مراجع [1, 2, 6] مراجعه نمود. در این مقاله به دنبال تشریح اهداف، ابزارها و مأموریت‌های دفاع سایبری فعال هستیم.

این مقاله در ۸ بخش ارائه‌شده است. در بخش دوم دفاع سایبری فعال معرفی شد. در بخش سوم نقش دفاع سایبری فعال در ارتقای امنیت سایبری کشور معرفی گردید. در بخش چهارم موارد لازم برای آمادگی ارائه یک دفاع سایبری فعال تعیین شدند. در بخش پنجم، گام‌های لازم برای هدایت دفاع سایبری فعال و در بخش ششم، نحوه هدایت دفاع سایبری فعال مطرح گردیدند. در بخش هفتم، مؤلفه‌ها و در بخش هشتم مأموریت‌های دفاع سایبری فعال مشخص شدند.

۲- مفاهیم پایه برای ارائه چارچوب در دفـاع سایبری فعال

در این بخش مروری بر مفاهیم پایه برای ایجاد چارچوبی به دفاع سایبری فعال خواهیم داشت. که لزوماً این مفاهیم دارای جامعیت نخواهد بود و فراخور تحقیق این مفاهیم اضافه خواهد شد.

فضای سایبری[۱] به مجموعه‌ای اطلاق می‌گردد که شامل زیرساخت‌های فناوری اطلاعات، شبکه‌های ارتباطی آن و سامانه‌های رایانه‌ای است. فضای سایبری یا فضای مجازی ترکیبی از ده‌ها هزار رایانه‌ی به‌هم‌پیوسته، سرویس‌دهنده‌ها، شبکه‌های ارتباطی، سوییچ‌ها و کابل‌های فیبر نوری است که امکان ایجاد ارتباطات را در یک سامانه جامع فراهم می‌آورد. فضای سایبری از تعامل سه مؤلفه مختلف سخت‌افزاری، مجازی و شناختی ایجادشده است. در شکل ۱، مؤلفه‌های فضای سایبری و نحوه تعامل آن‌ها به‌طور مشخص نشان داده می‌شوند.

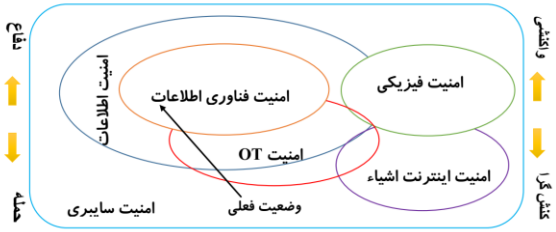


شکل (۱): مؤلفه‌های فضای سایبری

به‌تمامی داده‌ها و اجزای سامانه‌های سایبری که در یک ساختار وجود دارند سرمایه سایبری[۲] اطلاق می‌شود. شامل زیرساخت‌ها و اطلاعات در شبکه‌های اطلاعاتی و نیز ساختارهای اداری در یک نظام اقتصادی می‌شود. حمله سایبری[۳]، مجموعه اعمالی است که برای ایجاد اختلال، قطعی،

[۱] Cyber Space
[۲] Cyber Capital
[3] Cyber Attack

کاهش کیفیت یا نابودی اطلاعات مقیم در رایانه‌های موجود در فضای سایبری انجام می‌شود. اما تهدید سایبری برخلاف حملات سایبری، حاصل مخاطرات موجود در فضای سایبری است. چراکه تهدید سایبری یک عامل بالقوه (پتانسیل) برای نقض امنیت در فضای سایبری محسوب می‌گردد. یعنی تهدید سایبری در صورتی وجود خواهد داشت که یک پیشامد، قابلیت، کنش، یا رخداد که می‌تواند در امنیت سایبری رخنه ایجاد نموده، منجر به صدمه شود به وجود بیاید. این بدان معنی است که یک تهدید سایبری، یک خطر بالقوه است که ممکن است منجر به بهره‌برداری از یک آسیب‌پذیری امنیتی شود. پدافند غیرعامل سایبری[1] شامل کلیه اقدامات به‌منظور حفظ امنیت، ایمنی و پایداری شبکه و تجهیزات وابسته به شبکه می‌باشد. پدافند عامل سایبری[2]، شامل اقداماتی در جریان حمله یا قبل از حمله‌ی دشمن است که می‌تواند موجب بهبود تشخیص، جلوگیری و پاسخگویی به حملات سایبری دشمن می‌شود[4, 5, 25]. با توجه به تعریف‌های انجام‌شده از تهدید سایبری و حمله سایبری عملیات فضای سایبری، به‌کارگیری قابلیت‌های سایبری[3] به‌گونه‌ای که مقصود اصلی از آن رسیدن به اهداف در فضای سایبری و یا از طریق فضای سایبری باشد را عملیات فضای سایبری[4] می‌نامند. چنین عملیاتی شامل فعالیت‌ها و عملیات شبکه‌های رایانه‌ای است تا با آن شبکه‌ی اطلاعات سراسری را عمل کرده و از آن دفاع کند. برای ارائه یک چارچوب دفاع سایبری فعال دو مفهوم امنیت اطلاعات و امنیت سایبری حائز اهمیت است برخلاف آنچه که تصور می‌شود امنیت اطلاعات و امنیت سایبری یکسان نیست گارتنر به‌عنوان یک متخصص برجسته امنیت سایبری تفاوت این دو مؤلفه را این‌گونه بیان کرده است. از دیدگاه گارتنر[5] ، امنیت سایبری شامل امنیت اطلاعات[6]، امنیت فناوری اطلاعات[7]، امنیت فیزیکی[8]، امنیت فناوری عملیات[9] و امنیت اینترنت اشیاء[10] است. در دیدگاه گارتنر، امنیت سایبری وسیع‌تر از امنیت اطلاعات است درحالی‌که امنیت اطلاعات بیشتر دفاعی و واکنشی است و امنیت سایبری معیارها یا نگرش‌های کنش گرا و تهاجمی بیشتری دارد. در شکل۲، برای وضوح بیشتر با کمک نمودار، دیدگاه گارتنر را با وضوح بیشتری نمایش می‌دهیم.



شکل (۲): دیدگاه گارتنر در مورد امنیت سایبری

یوشنکو و راشر طی مقاله‌ای در سال ۲۰۱۱ دفاع سایبری را به‌صورت زیر تعریف نمودند: " قابلیت‌های سازمان‌یافته برای محافظت در مقابل، یا کاهش و بازیابی. سریع اثرات حمله سایبری است.

انواع دفاع سایبری را می‌توان به سه دسته تقسیم‌بندی کرد که عبارت‌اند از[26, 27]:

۱. دفاع غیر فعالانه[11] (واکنشی[12])

۲. دفاع فعالانه[13] (کنش‌گرایانه[14])

۳. دفاع پیش‌گویانه[15]

تعریف دیگری که رابرات دوار و همکاران در [27] از این مفهوم ارائه کردند. در این تعریف برای دفاع فعالانه سایبری دو خصیصه برشمرده شده است:

۱. تشخیص بی‌درنگ و کاهش تهدیدات در شبکه‌های مدافع

۲. داشتن توانایی انجام اعمال متقابل افندی ، تهاجمی به سمت بیرون

تعریف این مقاله از دفاع سایبری عبارت است از یک راهکار برای رسیدن به امنیت سایبری مبتنی بر توسعه معیارهایی برای شناسایی، تحلیل، تشخیص و کاهش تهدیدات در سامانه‌ها و شبکه‌های ارتباطی به‌صورت بی‌درنگ که باقابلیت و منابعی برای انجام اعمال کنش گرایانه یا آفندگونه در مقابل تهدیدات و موجودیت‌های تهدیدکننده شامل اعمال موجودیت‌های شبکه‌های خانگی ترکیب می‌شود.

[1] Non-passive Cyber Defense
[2] Passive Cyber Defense
[3] Cyberspace Capabilities
[4] Cyberspace Operations
[5] Gartner
[6] Information Security
[7] IT Security
[8] Physical Security
[9] Operation Technology Security (OT)
[10] Internet of Things(IOT) Security
[11] Non-Active Cyber Defense
[12] Reactive Defense
[13] Active Cyber Defense
[14] Proactive Defense
[15] Predictive Defense

۳- جایگاه دفاع سایبری فعال در پدافند سایبری

برای تبیین جایگاه دفاع سایبری فعال می‌توان با آن را با جایگاه عملیات امنیتی در پلیس شبکه مقایسه نمود. نظارت امنیتی بر شبکه‌ها و ابزارهای انتهایی، کاری مشابه فرستادن افسرها به سطح شهرها جهت اعمال محدودیت‌های لازم و مراقبت از وقوع جرم است. در دنیای واقعی، نیروهای گشت زنی در جلوگیری و غلبه بر جنایتکارانی که می‌توانند دیده شوند، مؤثر هستند. ولی برای مقابله با جنایات پیچیده‌ای که در پشت درهای بسته که مورد گشت زنی قرار نمی‌گیرند انجام شود، به‌تنهایی مؤثر نیستند. برای این‌گونه جنایتکاران حرفه‌ای، شهرها نیاز به استفاده از کارآگاه‌های ماهر دارد. کارآگاهان به‌جای گشت زنی و نظارت در سطح شبکه، اطلاعات را جمع‌آوری، بررسی و شواهد را تجزیه‌وتحلیل نموده و به‌طور فعالانه و هوشمند مظنونین را کشف می‌کنند. دفاع سایبری فعال در سطح فضای سایبر، عملکردی مشابه عملکرد کارآگاهان دارد. اکثر گروه‌های عملیات امنیتی فاقد قابلیت "کارآگاهی" هستند و این‌جایی است که دفاع سایبری فعال می‌تواند اثربخشی سازمانی را افزایش دهد. مراکز حساس برای اینکه توانایی شناسایی و ریشه‌کن کردن مهاجمان پنهان‌شده در شبکه‌ها را داشته باشند، سازمانی را ایجاد و تجهیز می‌کنند که با بهره‌مندی از یک چرخه عملیاتی مؤثری که شامل برنامه‌ریزی، بررسی فعالیت‌های اطلاعاتی جهت هدایت یک عملیات هدفمند، اجرای یک اقدام متقابل، ایجاد یک دفاع سایبری مستحکم در برابر مزاحمان سایبری و استفاده از متخصصان دفاع فعال می‌باشد، کارا باشد[28, 29].

۴- آماده‌سازی برای اجرای یک دفاع سایبری فعال

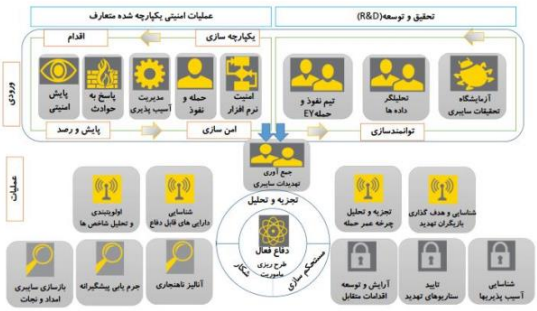
دفاع سایبری فعال جایگزینی برای فعالیت‌های امنیت سایبری سنتی نیست بلکه هدف آن سازمان‌دهی و ارتقای برنامه‌های امنیت سایبری موجود است. انجام یک دفاع فعال مستلزم آماده‌سازی لازم برای دستیابی به حداکثر اثربخشی است.

اولاً، مدافعان سایبری باید اطمینان حاصل کنند که آن‌ها درک درستی از دارایی‌های سایبری که اغلب مورد طمع مهاجمان قرار می‌گیرند، دارند. بر اساس تحقیقاتی که در سال ۲۰۱۵ انجام شد، ۷۷ درصد سازمان‌ها اعلام کردند که مرکز عملیات امنیت سایبری آن‌ها "با کسب‌وکارها ارتباط برقرار نمی‌کنند" و تنها ۲۳ درصد آن‌ها گزارش دادند که مرکز عملیات امنیت آن‌ها "به‌شدت یکپارچه‌شده است و برای درک درست از کسب‌وکارها و ایجاد آگاهی از نگرانی‌ها و خطراتی که آن‌ها را تهدید می‌کند ملاقات با مدیران تجاری را به‌طور منظم انجام می‌دهند". وجود این تعامل یک نکته کلیدی بوده و متأسفانه در بسیاری از برنامه‌های امنیتی مفقود است.

گفتگوهای مستمر و آگاهانه میان متخصصان دفاع سایبری و مدیران شاغل درنهایت منجر به تهیه فهرستی شامل دارایی‌های سایبری که باید از آن‌ها حمایت گردد، می‌شود. این دارایی‌ها، آن‌هایی هستند که در معرض خطرات جدی مانند سرقت اینترنتی، جمع‌آوری آفلاین و... قرار دارند مانند مالکیت معنوی، حمایت از تحقیقاتی که منجر به ابداعات آینده می‌شوند، اطلاعات شناسایی شخصی مشتریان و کارمندان، اطلاعات کارت پرداخت مشتریان و سیستم‌های کنترل صنعتی که از مشاغل حیاتی حمایت می‌کند، نام برد[30, 31].

۴-۱ اطلاعات لازم از سازمان خود برای ارائه دفاع سایبری فعال

در ابتدا مدافعان باید درک درستی از مفهوم نرمال بودن ترافیک شبکه داشته باشند که این مفهوم یک مبنا در زمینه امنیت فضای سایبری است. بااین‌حال، بسیاری از کارمندان فناوری اطلاعات، از این مفهوم در ابزارهای نظارت بر شبکه استفاده می‌کند. این مفهوم برای ارتقای عملکرد عملیات سایبری مهم است، زیرا دفاع فعال شامل تجزیه‌وتحلیل ناهنجاری‌های شدید در شبکه است. بسیاری از فعالیت‌های انجام‌شده توسط مهاجمین به دلیل عدم سازگاری آن‌ها با روال‌های معمول یک ناهنجاری بشمار رفته و توسط ابزارهای نظارت خودکار امنیتی از انجامشان جلوگیری می‌گردد مانند ورودی‌ها یا مدل امضا مربوط به حملات شناخته‌شده. در عوض، مهاجمین از اعتبارات محرمانه یا حساب‌های غیرقانونی استفاده کرده و با رفتار کاربرهای معمولی و عادی ترکیب می‌شوند تا شناخته نشوند. درهرصورت، تحلیلگران امنیتی باتجربه قادرند در بعضی موارد(نه همیشه)، فعالیت‌های مخرب و غیرعادی در شبکه که به‌صورت یک رفتار عادی دیده می‌شود را شناسایی کنند [31].



شکل(۳): ورودی‌ها و عملیات‌ها در دفاع سایبری فعال

۴-۲ اطلاعات لازم از مهاجمان برای ارائه یک دفاع سایبری فعال

لازم است مدافعان سایبری درک مناسبی از بازیگران اصلی تهدیدات سایبری که به‌احتمال‌زیاد مورد هدف آن‌ها خواهند بود، داشته باشند. بسیاری از گروه‌های امنیتی به‌سادگی فرض می‌کنند که توسط سه گروه بزرگ که شامل کشورهای دشمن، گروه‌های جنایی سازمان‌یافته و هکرهاست، مورد هدف قرار می‌گیرند. اگرچه ممکن است این حرف درست باشد، اما برای ایجاد یک دفاع سایبری فعال لازم است که بینشی وسیع‌تر داشته باشیم. در هر گروهی افراد متخصص سایبری باانگیزه‌های متفاوت و توانایی‌های مختلف وجود دارند. مدافعین سایبری با نزدیک شدن به طراحان تهدیدات سایبری، باید بسیار هوشمندانه عمل کنند تا با یک نگاه دقیق جزئیات کامل یک تهدید را به تصویر بکشند. در صورت امکان، باید بازیگران تهدید سایبری را شناسایی و آن‌ها را تجزیه‌وتحلیل کنند تا بتوانند با یک بینش دقیق و مناسب، فعالیت‌های دفاع سایبری خود را با حداکثر بازدهی انجام دهند[32, 33].

۵ گام‌های رسیدن به آمادگی جهت هدایت مأموریت‌های دفاع سایبری فعال

در این بخش گام‌های لازم برای کسب آمادگی جهت هدایت نمودن مأموریت‌های دفاع سایبری فعال معرفی می‌شود که شامل ۴ گام اساسی زیر است. در مسیر ایجاد یک دفاع سایبری فعال، در ابتدا باید گام‌های اول، دوم و سوم طی شوند تا بتوانیم به توانایی هدایت یک دفاع سایبری فعال که گام آخر در اجرای دفاع سایبری فعال است برسیم.

گام اول: شناسایی دارایی‌های سایبری حیاتی سازمان خود
گام دوم: بهبود و توسعه زمینه‌های محیطی (توسعه شبکه و خطوط اصلی فعال)
گام سوم: شناسایی و شناخت مشخصات بازیگران اصلی تهدیدات سایبری
گام چهارم: هدایت مأموریت‌های دفاع سایبری فعال

در شکل ۴ گام‌های مرتبط با اجرای یک دفاع سایبری فعال که در ۴ گام خلاصه‌شده است، نشان داده می‌شود.

شکل(۴): گام‌های دفاع سایبری فعال

۶- هدایت مأموریت‌های دفاع سایبری فعال

دفاع سایبری فعال شامل طرح عملیات دفاع سایبری هدفمند است که آن‌ها را "مأموریت" می‌نامیم. هریک از مأموریت‌ها به دنبال انجام فعالیت‌هایی هستند که برای کسب یادگیری‌ها و ارتقای بینش سایبری سازمان‌ها طراحی‌شده است. این مأموریت‌ها شامل یک یا چند موضوع خاص شده و ممکن است بین یک روز تا چند هفته به طول انجامد. اهداف مأموریت معمولاً شامل اجرای یک یا چند اقدام متقابل هدفمند برای شکست دادن سناریوهای یک تهدید سایبری خاص و یا انجام فعالیت‌های از قبل برنامه‌ریزی‌شده برای شناسایی مهاجمین مخرب است. برنامه‌های دفاع سایبری فعال به‌صورت یک دوره عملیاتی تکراری که چرخه عملیات سایبری می‌نامیم، اجرا می‌شود. هر چرخه ممکن است شامل یک یا چند مأموریت باشد و بر روی دفاع از یک یا گروهی از دارایی‌های سایبری خاص تمرکز می‌کند. هر چرخه عملیاتی شامل مراحل برنامه‌ریزی، اجرای مأموریت‌ها (از یک یا چند مأموریت) و بررسی چرخه است. همچنین هر مأموریت در یک چرخه عملیاتی می‌تواند شامل مراحل برنامه‌ریزی، اجرا و مرور مجدد باشد. در شکل۵، گام‌های هر مأموریت که بر اساس طرح‌های هدفمند و مأموریت‌های متمرکزشده است، نمایش داده می‌شود.

۷- مؤلفه‌های دفاع سایبری فعال

فهم حمله سایبری کمک می‌کند تا زمینه‌ای برای هدایت دفاع فعال در طول عملیات فراهم شود. هنگامی‌که مهاجمان سایبری شناسایی‌شده‌اند، مدافعین بافهم رفتار آن‌ها، از طریق تجزیه‌وتحلیل زنجیره قتل سایبری به شناسایی تاکتیک‌های خاص آن‌ها می‌پردازند. علاوه بر تاکتیک‌های حملات شناخته‌شده، باید برای هدایت یک دفاع سایبری فعال موفق، به جمع‌آوری اطلاعات

اضافه‌تر، ترسیم آن‌ها و شناسایی بازیگران اصلی حمله سایبری بپردازیم که این اطلاعات مهم شامل موارد زیر می‌شوند:

- محدوده IP مورداستفاده حمله‌کنندگان
- داده‌های مخرب
- سخت‌افزار یا نرم‌افزارهای بکار گرفته‌شده توسط حمله‌کنندگان
- سخت‌افزار یا نرم‌افزارهای مورد هدف توسط حمله‌کنندگان
- زمان‌های معمول جهت انجام عملیات فرد مهاجم

مدافعان همچنین برای هر حمله سایبری که در مقابل آن دفاع می‌کنند به جمع‌آوری اطلاعات زیر می‌پردازند:

- سخت‌افزار یا نرم‌افزار مورداستفاده برای دسترسی به اطلاعات حساس و فرآیندهای کسب‌وکار
- وصله‌های سخت‌افزار و نرم‌افزار شناسایی‌شده
- اطلاعات حملات قبلی
- هویت دقیق و اطلاعات دسترسی به منابع مرتبط

این اطلاعات در مورد رویدادهای جاری صنعت بوده که با هوشمندی جمع‌آوری می‌شود و برای تعیین اینکه چه کسی و با چه هدفی حمله کرده است، مورداستفاده قرار می‌گیرد. همکاران صنعت منبع خوبی برای رشد و توسعه دیدگاه‌های متخصصان دفاع سایبری درباره آخرین ابزارها، تاکتیک‌ها و روش‌های استفاده‌شده توسط مهاجمان سایبری هستند.

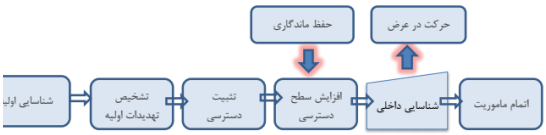
شکل (۵): گام‌های هر مأموریت در دفاع سایبری فعال

۷-۱ ساختار زنجیره انهدام مهاجم سایبری

علی‌رغم فنّاوری‌های دفاعی پیشرفته مانند آنتی‌ویروس، دیواره آتش و ... مهاجمان همیشه با تحلیل جنبه‌ی انسانی نهادهای هدف و پیاده‌سازی فیشینگ، آسیب‌پذیری‌های یک سیستم یا شبکه خاص را شناسایی و از اقدامات امنیت موجود عبور می‌کنند. سپس مهاجمان سایبری با ادامه‌ی این فرآیند می‌توانند آلودگی‌های جانبی را روی شبکه قربانی پیاده‌سازی کنند. این مسیر حمله، به نام "زنجیره انهدام مهاجم سایبری" شناخته‌شده است که می‌تواند موجب کسب اطلاعات حیاتی مهاجم و آسیب‌رسانی حداکثری به قربانی می‌گردد. بر اساس زنجیره انهدام سایبری، مهاجمان مراحل زیر را دنبال می‌کنند:

- شناسایی اولیه
- تشخیص تهدیدات اولیه
- تثبیت دسترسی
- افزایش سطح دسترسی
- شناسایی داخلی
- حرکت جانبی
- حفظ ماندگاری
- تکمیل مأموریت و یا تکرار افزایش دسترسی‌ها برای رسیدن به اهداف حمله

در شکل۶، ساختار زنجیره انهدام مهاجم سایبری که مطابق گزارش تحقیقات جاسوسی سایبری ارائه‌شده، نشان داده می‌شود.



شکل (۶): نمودار ساختار زنجیره انهدام مهاجم سایبری

۸ مأموریت یک دفاع سایبری فعال

یک جنبه کلیدی دفاع سایبری فعال، افزایش تمرکز عملیاتی از طریق برنامه‌ریزی هدفمنداست که سبب افزایش اثربخشی مأموریت‌های دفاع سایبری فعال می‌شود. گروه‌های امنیتی، بر پایه ادهاک (ساختارهای اقتضائی) ساختار دفاع سایبری خود را به‌طور متناوب سخت‌تر می‌کنند تا بتوانند در زمان‌های مقتضی در واکنش به اعلان آسیب‌پذیری‌های سطح بالا بهترین تاکتیک‌های ممکن را پیاده‌سازی نمایند. مأموریت‌های دفاع سایبری فعال به‌طور مستمر طرح‌ریزی و اجرا می‌شوند تا سناریوهای تهدید سایبری را شکست دهند و مهاجمان سایبری پنهانی را در شبکه کشف کنند. این بدان معنی است که وقت مدافعان سایبری، صرف شناسایی مهاجمان مخرب یا

غیرقابل‌شناسایی و جلوگیری از نفوذ و شکست دادن آن‌ها می شود.

۸-۱ دسته‌بندی مأموریت‌ها در هدایت دفاع سایبری فعال

استفاده از اصطلاح "مأموریت" این واقعیت را بیان می‌کند که به‌منظور دستیابی به حداکثر اثربخشی در انجام اهداف امنیتی سازمان‌ها، فرآیند عملیات سایبری با یک نظم خاص و با دقت قابل‌توجه در انجام تحلیل‌ها، ادامه دارد. مأموریت‌ها در پاسخ به فهم تهدید خاص در سازمان‌های دفاعی، برنامه‌ریزی‌شده و با تمرکز بر تهدیدات کسب‌وکار و مطابق با سناریوهای واقعی در جهان، طراحی می‌شوند. به‌منظور دست‌یابی به حداکثر توانمندی های دفاعی، متخصصان حوزه دفاع سایبری فعال می‌توانند توانمندی‌های دفاعی خود را به بالاترین حد ممکن برسانند. اگرچه دفاع فعالانه ذاتاً متمرکز بر روی مهاجمان است، اما گاها با اهداف خاص نیز طراحی می‌شود ازجمله حمایت از دارایی‌های ارزشمند سایبری که باید از آن‌ها محافظت شود. این دارایی‌ها شامل ارزشمندترین داده‌های سازمان‌ها و سیستم‌های کسب‌وکار می‌شوند. مأموریت دفاع سایبری فعال می‌تواند شامل هر نوع فعالیت و عملیاتی بشود که درنهایت از این دارایی‌های سایبری به‌درستی مراقبت شود. در ادامه مأموریت‌های دفاع سایبری فعال طبق دسته‌بندی‌های زیر تقسیم‌بندی می‌شوند.

۸-۱-۱ استحکام و غنی‌سازی

دسته اول از مأموریت‌های دفاع سایبری فعال شامل فعالیت‌هایی است که به بهبود کار دفاعی در برابر تاکتیک‌های خاص می انجامد که ممکن است توسط مهاجمان حرفه‌ای مورداستفاده قرار گیرد. مهم‌ترین هدف این مأموریت‌ها، شناسایی و اعتبار سنجی آسیب‌پذیری‌های پیچیده و سناریوهای تهدید و توسعه بخشیدن به آگاهی وضعیتی از شبکه برای تصمیم‌گیرندگان دفاع سایبری است. این دسته از مأموریت‌ها به دو زیر بخش که شامل شناسایی شبکه و اقدامات متقابل هدفمند است، تقسیم‌بندی می‌شود.

۸-۱-۱-۱ شناسایی شبکه

مأموریت شناسایی شبکه، فهم سازمان از سطح توانمندی خود برای مقابله با سناریوهای تهدید را توسعه می‌دهد. مأموریت‌هایی از این نوع، معمولاً پیچیده‌تر از اسکن آسیب‌پذیری رایج هستند و ممکن است شامل حملات فریبنده بشوند. به‌عنوان نمونه، مأموریت جمع‌آوری اطلاعات، یک آزمایش چندروزه است که تعیین می‌کند آیا ابزارهای نظارت امنیتی موجود قادر به شناسایی استفاده از یک تهدید مخرب خاص در شبکه هستند یا خیر.

۸-۱-۱-۲ اقدامات متقابل هدفمند

مقابله با اقدامات متداول اغلب بر روی شبکه تمرکز می‌کند و تلاش آن برای جلوگیری، تضعیف یا شکست دادن تاکتیک‌های خاص مهاجمان است. فعالیت‌های دفاع سایبری فعال متفاوت از فعالیت‌هایی است که توسط گروه‌های عملیات امنیتی سنتی اجرا می‌شود، زیرا آن‌ها به‌صورت عمدی در پاسخ به‌موقع به یک تهدید یا یک فرد مهاجم به اجرا درمی‌آیند. مهم‌ترین هدف این بخش از مأموریت‌ها شامل فهم و آگاهی از میزان قدرت نفوذ هوشمند است. این نفوذها برای طراحی و پیاده‌سازی اقدامات متقابلی بکار می‌رود که در جهت شکست دادن سناریوهای حملات مخرب است.

۸-۱-۲ شکار کردن مهاجمان پنهان

مأموریت‌های شکار مهاجمان سایبری، تلاش می‌کنند تا مهاجمان پنهان‌شده اما فعال در شبکه را با کمک مدارک ناشناخته از حملات گذشته کشف کنند. متخصصان دفاع سایبری فعال با پیشگامی و ابتکار عمل علیه مهاجمان که به‌صورت شناسایی و جلوگیری از فعالیت آن‌ها (ریشه‌کن کردن آن‌ها) است، سبب کاهش زمان فعالیت مهاجمان سایبری درون شبکه می‌شود. مأموریت‌های شکار معمولاً به دودسته تله گذاری و اجبار و تحلیل ناهنجاری‌ها تقسیم می‌شوند.

۸-۱-۲-۱ تحلیل ناهنجاری‌ها

در این مأموریت جهت شناسایی فعالیت‌های مخرب، داده‌هایی را که بر روی میزبان‌های خاص قرار دارند با الگوهای ترافیک شبکه تطبیق می‌دهند. اگرچه سازمان ممکن است یک حسگر جامع و پیچیده برای نظارت بر امنیت شبکه‌ها(بخش‌بندی ترافیک‌ها) و نقاط پایانی به‌کارگیری کنند، اما اشکال بسیاری از این حسگرها این است که بسیاری از این فعالیت‌های مخرب وجود دارند که تشخیص خودکار را خنثی می‌کنند (دور می‌زنند) درحالی‌که این فعالیت‌های مخرب توسط تحلیلگران انسانی به‌طور کاملاً واضح شناسایی می‌شوند. همان‌طور که پیش‌ازاین بحث شده است، توانایی شناسایی فعالیت‌های غیرعادی(ناهنجاری) یکی از ابزارهای مهم دفاع فعال بوده و برای انجام مأموریت‌های شکار حیاتی است. فعالیت غیرمعمول(غیر نرمال)، فعالیتی است که نرمال نبوده و با ترافیک عادی شبکه هم‌خوانی ندارد و به عبارتی به زمینه‌ای که در آن دیده می‌شود تعلق ندارد. مدافعان علاوه برشکار فعالیت غیرمعمول در جریان رویدادهای جدید، باید

اطمینان حاصل کنند کـه داده‌هـا و فعالیت‌هـای قبـل را نیـز در بایگانی‌ها به‌خوبی جستجو می‌کنند. زمـانی کـه مـدافعان از یـک رفتار مخرب خاص آگاهی می‌یابند، همیشه بایستی به‌محض آنکه مهاجمان شروع به استفاده از آن می‌کنند، جستجو را آغاز نمایند و حتماً باید سری به بایگانی‌ها بزنند تا اطمینان حاصل شـود کـه سـازش و مصـالحه‌ای از قبـل رخ نـداده اسـت. تجزیـه‌وتحلیل ناهنجاری‌ها می‌تواند به شناسـایی فضـای سـایبر و جلـوگیری یـا شکست فشرده‌سازی اطلاعات حساس بیانجامد. مهاجمان اغلـب درجایی از شبکه ساکن هستند که یـک حملـه مـی‌توانـد شـکل بگیرد که به آن Beachhead می‌گویند. این می‌تواند میزبانی باشد که از آن برای آغاز کـردن حمـلات بـه میزبان‌هـای دیگـری کـه داده‌های ربوده‌شده در آن‌ها ذخیره می‌شود استفاده می‌کند. اغلب این داده‌ها فشرده، مبهم و یـا حتـی رمزگـذاری شـده مـی‌شـوند به‌طوری‌که به نظر می‌رسد چیزی در آن‌ها نیست. برای شناسـایی مکان‌های استقرار، مدافعان سایبری احتمالاً موقعیت‌های نزدیـک بـه منـاطق حسـاس را کـه ابزارهـای ذخیره‌سـازی و اطلاعـات دزدیده‌شده در آن‌ها هستند را جستجو می‌کنند. در شـرکت‌هایی که بر روی مکان ذخیره‌سازی داده‌های کاربران تأکیـد مـی‌کننـد، مانند کسانی که نیاز به ذخیره تمام فرایندهای شخصی در پوشـه مشترک شبکه‌دارند، این جستجو می‌تواند ساده باشد. جستجو نیز ممکن است از طریق برنامه‌های نام‌گذاری فایل سازمانی پشتیبانی شود. این‌ها اغلب برای بیگانه‌ها آشکار نیستند، بنابراین مهاجمـان ممکن است سهواً نام‌های فایلی ایجاد کنند که بلافاصله غیرعادی تلقی شود. مهم‌ترین هدف این بخش شامل، بازجویی‌های متمرکز با ابزارهای نظارت خودکار امنیتی بر روی فعالیت‌های غیرمعمـول و مخربی که قابل‌شناسایی نیست، می‌شود.

۸-۱-۲-۲ فریب سایبری

این مأموریت‌ها تلاش می‌کنند تا مهاجمـان پنهـان را مجبـور بـه انجام فعالیت‌هایی کنند که باعـث مـی‌شـود آن‌هـا کشـف شـوند. هنگامی‌کـه یـک مهـاجم بـه شـبکه دسترسـی یافتـه و در آنجـا مستقرشـده و پایـدارمی شـوند، بعیـد اسـت کـه ناگهـان وارد موقعیت‌های دیگری شده و در فعالیت‌های مخرب دیگری شرکت کنند. این به این دلیل است که آن‌ها به‌احتمال‌زیاد دسترسـی بـه اعتبار حساب‌های قانونی را به دست آورده‌انـد و یـا امکـان نصـب نرم‌افزارهـای مخـرب بـرای آن‌هـا فراهم‌شـده اسـت و قادرنـد فعالیت‌های خود را پنهان یا حذف کنند. با تغییر شـرایط شـبکه، مدافعان سایبری می‌توانند شرایط مخفی شدن را برای مهاجمـان حرفه‌ای سخت نمایند. مهم‌ترین هدف این بخش، تغییر شـبکه و شرایط نقطه پایان برای تحریک کردن یک مهاجم پنهـان جهـت انجام فعالیت‌های مخرب جدیدی است که این فعالیت‌ها از طریق انجام نظارت‌های هدفمندی که به‌صورت فشرده و مستمر انجام می‌شود، توسط مدافعان سایبری قابل‌شناسایی هستند.

۸-۱-۳ ضربات پیش‌دستانه

ضربت پیش‌دستانه، عبارت است از توسل به‌زور در برابر حملـه‌ای است که به قریب‌الوقوع بودن آن ایمان‌داریم. بر اساس شـواهدی مبنی بر اینکه یک فعالیت خصمانه شروع‌شده یا در شـرف وقـوع است. همانند حملـه متقابـل، ضـربه پیش‌دسـتانه نیـز در ارتـش دیده‌شده است. برای مثال، در سال ۱۹۶۷، زمانی که مصـر قـوای جنگی خود را در مرزهای اسرائیل متمرکـز کـرده بـود، اسـرائیل اعتقاد داشت که در حال راه‌اندازی یک جنگ پیش‌دسـتانه علیـه مصر است در قلمرو فضـای سـایبری، یـک ضـربت پیش‌دسـتانه ممکن است به‌عنوان هدایت یک حمله سایبری بـر روی سیسـتم یا شبکه‌ای که ممکن است حمله‌ای توسط آن سیستم یا شبکه به سیستم خودمان هدایت گردد، تعریف شود. سـناریویی را فـرض کنید که کشور(آبی) اطلاعاتی جمع‌آوری نموده اسـت کـه نشـان می‌دهد کشور متخاصم (سرخ) برنامه‌هایی برای اجرای یک حمله سایبری علیه آن کشور دارد، کشـور آبـی ممکـن اسـت عملیـات سایبری پیش‌دستانه‌ای را علیه کشور قرمز راه‌اندازی کنـد. انجـام این کار می‌تواند در دستیابی به موارد زیر کمک‌کننده باشد.

۸-۱-۳-۱ فلج کردن قابلیت حمله دشمن

در مورد جنگ شش‌روزه در ۱۹۶۷، بلافاصله زمانی که اسـرائیل دریافت که مصر در حال سازمان‌دهی نیروهای خـود در مرزهـای اسرائیل است، اسرائیل حمله‌ای علیه کشورهای عربـی راه‌انـدازی نمود. حمله پیش‌دستانه انجام‌شده توسط نیروهای اسرائیل، تقریباً چهارصـد هواپیمـای نظـامی مسـتقر در مصـر را نـابود کـرد. در عملیات سایبری ذکرشده فوق، بر پایه نفوذ در شبکه‌های کشـور سرخ، کشور آبی می‌توانـد از طریـق قطـع شـبکه کشـور سـرخ، قابلیت حمله سایبری کشور سرخ را فلج کند.

۸-۱-۳-۲ بازدارندگی

کشور آبی به‌محض نفوذ در شبکه کشور سرخ، می‌تواند با زیرکـی حضور خود را نشان داده و به‌موجب آن به کشـور سـرخ هشـدار دهد که شبکه‌اش به خطر افتاده است. انجام این کار ممکن است سرخ‌ها را از شروع حمله علیه آبی‌ها بازدارد. ایـن موضـوع توسـط دابلیو. اِرل بوبرت در گزارش NRC به این صـورت توصیف‌شـده است که « آگاهیِ مهاجمان احتمالی از اینکه چنـین «پاسـداری سایبری» در حال انجام است ، به‌خودی‌خود بـه‌عنوان یـک عامـل بازدارنده عمل خواهد کرد. زیرا آن‌هـا ممکـن اسـت بـا اقـدامات

امنیتی دیگر و نیز تا درجه‌ای از عدم اطمینان مواجه شوند که ممکن است خودشان مورد نفوذ قرارگرفته و به خطر بیافتند.

۸-۱-۴ ضربات پیشگیرانه

درحالی‌که ازنظر مفهومی یک ضربت پیش‌بینی کننده ممکن است مشابه یک ضربت پیشدستانه به نظر برسد، یک تمایز مهم بین این دو وجود دارد. همان‌طور که آبراهام سوفائر توصیف نمود، یک ضربت پیش‌دستانه توسل به‌زور در برابر یک حمله پیش‌بینی‌شده مبتنی بر این باور است که مهاجم از روش‌های موجود یا روش‌های بالقوه برای حمله در آینده یا برای ایجاد سایر انواع صدمات شامل برای مثال صدمه به گروگان‌ها، حمله توسط عوامل غیردولتی یا بدرفتاری یک دولت نسبت به شهروندان خود استفاده خواهد کرد. این به معنای آن است که چنین حمله‌ای قبل از هر حمله یا تهدید غیر حتمی که طبق قوانین بین‌المللی به‌عنوان یک حمله به‌حساب نمی‌آید، شروع گردد. به دلایلی مشابه، یک حمله سایبری پیشگیری‌کننده می تواند در برابر یک عامل متخاصم (چه دولتی و چه غیردولتی) برای بازداشتن مهاجم از دستیابی به هر نوع قابلیت آفندی سایبری راه‌اندازی گردد. همچنین این نوع حمله می‌تواند به اثر بازدارندگی مشابه با حمله پیش‌دستانه ذکرشده در بالادست یابد. یعنی، وقتی عامل متخاصم دریابد که شبکه‌اش به خطر افتاده است، ممکن است در مورد ادامه حمله سایبری تجدیدنظر کند. هرچند، یک حمله سایبری پیشگیرانه همچنین می‌تواند به یک قابلیت آفندی غیر سایبری نیز توسعه یابد. مثالی خوب از این موضوع استاکس نت ، اولین کرم کامپیوتری که باهدف سیستم‌های صنعتی یا به‌طور خاص‌تر تأسیسات هسته‌ای ایجاد گردید می‌باشد. درحالی‌که استاکس نت به رایانه‌های سراسر جهان گسترش پیدا کرد، آلودگی عمدتاً در ایران متمرکزشده بود. به نظر می‌رسد که خالق استاکس نت قصد داشته از این کرم برای جلوگیری از قابلیت ساخت سلاح‌های هسته‌ای در ایران استفاده کند.

۸-۱-۵ بهره‌کشی سایبری

این نوع حمله به مفهوم بهره‌برداری از سیستم‌های رایانه‌ای دخیل در یک حمله سایبری به‌منظور بدست‌آوردن اطلاعات حساسی است که به تحلیل حمله و تعیین مقصر این حمله کمک می‌کند. در طول یک حمله سایبری یا بعدازآن، دفاع‌های غیرفعال از قبیل روش‌های علمی بررسی جرائم و بازبینی لاگ‌ها (واقعه‌نگارها) تنها قادر به آشکار نمودن آدرس‌های آی پی منابع بلا واسطه حملات هستند. هرچند، همان‌طور که پیش‌تر بحث شد، بسیاری از حملات از طریق پرش‌های چندگانه و با استفاده از رایانه‌های هک شده متعدد آغاز می‌شوند. درنتیجه، برای تعیین منشأ واقعی یک حمله، به روشی اثربخش جهت ردگیری مسیر حمله اتخاذشده توسط مهاجم نیاز است. یکی از روش‌هایی که به‌طور گسترده موردتحقیق قرارگرفته است و نیاز به هیچ‌گونه بهره‌کشی از رایانه‌های حمله‌کننده ندارد، ردیابی معکوس آی پی است. هرچند این روش هنوز به بلوغ نرسیده و منجر به مسائل سازگاری و عملکردی می‌گردد. همچنین، سیستم‌های انتساب حمله که بر اساس روش‌هایی نظیر ردیابی معکوس آی پی ساخته‌شده‌اند برای اینکه بتوانند نتایج دقیق و درستی ارائه دهند، می‌بایست در تعداد هر چه بیشتری از ارائه‌دهندگان سرویس اینترنت پیاده‌سازی شوند. این روش هزینه بالایی در بردارد. بدون هیچ‌گونه صرفه مالی، انگیزه اندکی برای ISP ها برای پیاده‌سازی سامانه‌های انتساب حمله وجود خواهد داشت حتی اگر این سامانه‌ها عملکرد بی‌نقص داشته باشند. به‌علاوه، قابل‌اعتماد بودن اطلاعات ممکن است با دخیل شدن یک کشور غیردوستانه زیر سؤال برود. برای مثال، فرض کنید ترافیک شبکه‌ای وجود داشته باشد که از ایالات‌متحده به روسیه روی شبکه‌ای انتقال پیدا می‌کند که تا کره شمالی ادامه دارد. کره شمالی‌ها تا چه حد مایل خواهند بود تا در انتشار اطلاعات انتساب حمله همکاری کنند؟ و حتی اگر مایل به انتشار اطلاعات باشند، آیا این اطلاعات قابل‌اطمینان خواهد بود؟ از طریق بهره‌کشی سایبری، از این مباحث ممکن است اجتناب شود. بعد از به دست آوردن آدرس آی پی آخرین رایانه استفاده‌شده توسط مهاجم (بر اساس نتایج حاصل از کشف جرم و بازبینی وقایع‌نگار) ، این رایانه ممکن است مورد بهره‌کشی قرارگرفته یا به‌طور معکوس هک شود. بعد از دسترسی به این رایانه، تحلیل عمیق این سیستم ممکن است سیستم بعدی در زنجیره را مشخص کند. با تکرار این فرایند، مسیر حمله قابل‌شناسایی بوده و درنهایت منجر به کشف رایانه‌ای می‌گردد که عامل اصلی حمله بوده است. زمانی که این نتیجه حاصل شد، روش‌های کشف جرم باید بر روی این رایانه انجام گردد تا صاحب آن را مشخص کند. با بررسی اسناد ذخیره‌شده در این رایانه، تاریخچه وب‌گردی و فایل‌های نهان شده، نامه‌های الکترونیکی و غیره ، مالک یا کاربر آن رایانه قابل‌شناسایی خواهد بود. اطلاعات بازیابی شده از این بررسی، ممکن است سرنخ‌هایی نظیر اینکه مغز متفکر اصلی چه کسی است و آیا پای یک دولت/کشور در میان است ارائه دهد. برای مثال، ممکن است مکالمه ایمیلی یا سندی حاوی دستوراتی از جانب برخی مقامات دولتی وجود داشته باشد. هرچند، این دلیل قاطعی علیه دولت موردنظر نخواهد بود زیرا آن مقام رسمی ممکن است به‌دلخواه خود اقدام به این کارنکرده باشد(برای مثال

ممکن است سیستم او هک شده باشد). بسیاری از مهاجمان از همان معماری اینترنت برای پوشاندن رد خود بهره می‌برند. در انجام این کار، آن‌ها می‌توانند حملات خود را بدون هیچ‌گونه ترسی از شناسایی شدن یا مواجه‌شدن با پیامدهای دیگر اجرا کنند. آن‌ها مجموعه‌ای از رایانه‌های آسیب‌پذیری که هک شده‌اند را جمع‌آوری می‌کنند و متعاقباً از طریق مجموعه‌ای از این رایانه‌های هک شده قبل از راه‌اندازی حمله، به سیستم ورود پیدا می‌کنند. آن‌ها ممکن است به‌عنوان جایگزین از طریق پراکسی سرورهای بی‌نام یا TOR برای اتوکشی ترافیک خود متصل شوند. درحالی‌که ممکن است حمله متقابل به مهاجم تا تعیین محل واقعی آن امکان‌پذیر نباشد، این روش همچنان سودمند است. همان‌طور که قبلاً بحث شد، بهره‌کشی از رایانه‌های هک شده مختلف امکان بازسازی مسیر حمله را خواهد داد که به‌نوبه خود محل حمله‌کننده را آشکار خواهد ساخت. زمانی که این مکان به دست آمد، اقداماتی برای از کار انداختن سیستم حمله‌کننده قابل انجام خواهد بود. مهاجم با دانستن اینکه دیگر در سایه اینترنت پنهان نبوده و سیستم‌های او ممکن است موردحمله قرار گیرند، احتمالاً از ادامه حمله منع خواهد شد.

۹ مدل‌سازی ریاضی دفاع سایبری فعال

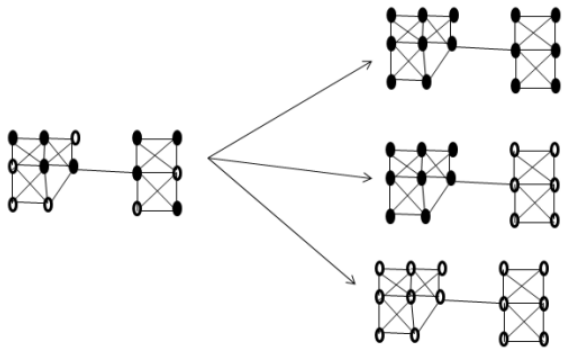
باوجوداینکه در سال‌های اخیر، مفاهیم دفاع سایبری فعال در ادبیات دفاع سایبری واردشده است ولی مدل ریاضی برای مشخص کردن میزان اثربخشی دفاع سایبری فعال وجود ندارد. در این بخش می‌خواهیم یک مدل فرآیند مارکوفی که برای تعامل بین حمله سایبری و دفاع سایبری فعال است معرفی نماییم. نکته قابل‌ذکر این است که مدل فرآیند مارکوفی معرفی‌شده با روش‌های ریاضی که ما می‌شناسیم، حل نمی‌شود. بنابراین، از طریق تقریب میانگین، مدل فرایند مارکوفی ساده می‌شود و این به ما اجازه می‌دهد مجموعه‌ای از نتایج تحلیلی ارزشمندی که اثربخشی دفاع فعال سایبری را مشخص می‌کند، به دست آوریم. مدل مارکوفی شرایطی را فراهم می‌کند که تحت آن دفاع سایبری مؤثر بوده و منجر به بینش عملی شود که می‌تواند برای تصمیم‌گیری و سیاست‌گذاری در زندگی واقعی اتخاذ شود.

یک رایانه دارای دو حالت است: آسیب‌پذیر و امن (آسیب‌پذیر اما بدون خطر). مهاجم می‌تواند از آسیب‌پذیری‌های رایانه (رخنه روز صفر) بهره‌برداری کند. این حملات به‌نوعی بدافزار هستند، به این معنی که رایانه‌های خطرناک می‌توانند در یک به رایانه‌های آسیب‌پذیر حمله کنند. با دفاع فعال سایبری، مدافع می‌تواند "کرم خوب" را برای شناسایی و پاک‌سازی رایانه‌های خطرناک گسترش دهد. تقابل بین حمله سایبری و دفاع سایبری فعال، به ایجاد یک ساختار تقابلی دفاع – حمله منجر می‌شود. گراف زیر یک توپولوژی ارائه داده که نشان می‌دهد، چگونه گره‌های آسیب‌دیده به گره‌های امن حمله می‌کنند و چگونه گره‌های امن با استفاده از دفاع سایبری فعال به اصلاح گره‌های آسیب‌دیده می‌پردازد.

می‌گوییم یک مدافع (مهاجم) استراتژیک است اگر در ابتدا گره‌های با درجه بزرگ، را در گراف با احتمال بیشتری اشغال کند. فعل‌وانفعال میان دفاع و حمله، منجر به ایجاد تحول امنیت سایبری در کل سیستم سایبری می‌شود. در گراف زیر گره‌های توپر نشان‌دهنده گره‌های امن و گره‌های توخالی نشان‌دهنده گره‌های آسیب‌پذیر می‌باشد.

همان‌طور که در شکل ۸ نشان داده‌شده، تحول حالت‌ها می‌تواند وجود چندین نوع موازنه را نشان دهد. در سطوح بالا، هدف مشخص کردن چگونگی حالت اولیه، توپولوژی گراف، پارامترها و استراتژی‌های فرد مهاجم یا مدافع اداره می‌شود. این ویژگی به ما اجازه می‌دهد تا به برخی از سؤالات اساسی پاسخ دهیم مانند اینکه در چه شرایطی امنیت سایبری در جهت تحول حرکت می‌کند. در شکل۷، تصویری از تحولات امنیت سایبری تحت دفاع سایبری فعال را نشان می‌دهد، به‌طوری‌که حالت اولیه در شرایط یکسان ممکن است به سمت یکی از سه حالت مختلف زیر پیش برود:

- همه گره‌ها امن هستند (حلقه‌های پرشده)
- تمام گره‌ها در معرض خطر قرار دارند
- برخی از گره‌ها امن هستند.



شکل(۷): تصویری از تحولات امنیت سایبری تحت دفاع سایبری فعال

۹-۱ ارائه یک مدل مارکوفی برای دفاع سایبری فعال

ساختار دفاع- حمله با کمک یک گراف متناهی $G=(V,E)$ نمایش داده می‌شود که در آن مجموعه

$V=\{v_1,v_2,...,v_n\}$ رأس‌های گراف بوده که رایانه‌ها هستند و مجموعه E یال‌های گراف می‌باشد که شامل حلقه نیست.

در هرلحظه یک رأس می‌تواند دارای دو حالت باشد:

- امن(آسیب‌پذیر است اما توسط مهاجم به خطر نمی‌افتد)
- آسیب‌پذیر(توسط مهاجم به خطر می‌افتد)

رأس v تغییر حالت می‌دهد اگر رأس uای داشته باشیم که: $(u,v)\in E$

در این گراف، رابطه $(u,u)\notin E$ نداریم زیرا هیچ رایانه امنی خود را امن نمی‌کند و هم‌چنین هیچ رایانه پرخطری به خودش حمله نخواهد کرد. این گراف‌ها می‌توانند جهت‌دار یا غیر جهت‌دار باشند ولی تمرکز ما صرفاً بر روی گراف‌های غیر جهت‌دار است. در گراف مطرح‌شده، هیچ محدودیت خاصی نداریم زیرا در دنیای واقعی گراف $G=(V,E)$ می‌تواند هر توپولوژی داشته باشد.

حالت رأس v در لحظه t یک متغیر تصادفی $\xi_v(t)\in\{0,1\}$ است به‌طوری‌که:

$$\xi_v(t)\in\begin{cases}1 & v\,is\,\text{secure}\quad at\,time\,t\\ 0 & v\,is\,\text{compromised}\,at\,time\,t\end{cases}$$

مطابق رابطه بالا روابط زیر را تعریف می‌نماییم:

$$B_v(t)=P(\xi_v(t)=1)\quad,\quad R_v(t)=P(\xi_v(t)=0)$$

متغیر تصادفی $\tilde{\theta}_{v,BR}(t)$ نیز میزان تغییرات حالت v در لحظه t از حالت امن به حالت آسیب‌پذیر را نشان می‌دهد که مقدارش وابسته به حالات رئوس مجاورش دارد و به‌طور مشابه، متغیر تصادفی $\tilde{\theta}_{v,RB}(t)$ می‌تواند میزان تغییرات حالت v در لحظه t از حالت امن به حالت آسیب‌پذیر را نشان دهد.

$$P(\xi_v(t+\Delta t)=1\,|\,\xi_v(t))=\begin{cases}\Delta t.\tilde{\theta}_{v,BR}(t)+o(\Delta t), & \xi_v(t)=0\\ 1-\Delta t.\tilde{\theta}_{v,BR}(t)+o(\Delta t), & \xi_v(t)=1\end{cases}$$

تغییر حالات v را می‌توان با مدل مارکوفی زیر نمایش داد:

(۱)

$$P(\xi_v(t+\Delta t)=0\,|\,\xi_v(t))=\begin{cases}\Delta t.\tilde{\theta}_{v,BR}(t)+o(\Delta t), & \xi_v(t)=1\\ 1-\Delta t.\tilde{\theta}_{v,BR}(t)+o(\Delta t), & \xi_v(t)=0\end{cases}$$

,

(۲)

که در آن رابطه $\Delta t\to 0$ برقرار است.

از طرفی مجموعه زیر نشان‌دهنده تمام همسایگی‌های رأس v است:

$$N_v=\{u\in V,(u,v)\in E\}$$

ازآنجایی‌که مقدار متغیرهای تصادفی $\tilde{\theta}_{v,BR}(t)$ و $\tilde{\theta}_{v,RB}(t)$ به کمک حالات تصادفی رئوس همسایه v تعیین می‌شود از توابع غیرخطی و قطعی زیر برای انجام محاسبات آن استفاده می‌کنیم:

$$f_{RB}(.):R\to[0,1]\quad,\quad f_{BR}(.):R\to[0,1]$$

به‌طوری‌که :

$$\tilde{\theta}_{v,BR}(t)=f_{BR}\Big(\frac{1}{\deg(v)}\sum_{u\in N_v}(1-\xi_u(t))\Big)$$

$$\tilde{\theta}_{v,RB}(t)=f_{RB}\Big(\frac{1}{\deg(v)}\sum_{u\in N_v}(\xi_u(t))\Big)$$

با توجه به اینکه این توابع توانمندی‌های نبرد سایبری حمله‌کننده و دفاع کننده را نشان می‌دهد، به آن‌ها توابع توان نبرد[۱] می‌گوییم.

این مدل‌ها معمولاً یک فرآیند مارکوفی پوآسن با نرخ ثابت بوده و می‌تواند به یک فرایند دوگانی تبدیل شوند که در زمان به عقب برگشته و به فرآیند قدم زدن تصادفی تبدیل شود که باعث می‌شود قابل‌ردیابی باشد. اما در مدل ما، یک گره حالت خود را با توجه به نرخی که ثابت نشده است تغییر می‌دهد و به‌طور غیرخطی به حالت‌های همسایگان خود وابسته است. این غیرخطی مانع از تبدیل مدل فرایند مارکوف مطرح‌شده به مدل قدم زدن تصادفی می‌شود.

مشکلات ناشی از غیرخطی بودن به ما پیشنهاد می‌دهد که ما باید این مدل فرایند مارکوف را به‌عنوان یک مدل سیستم دینامیکی قابل‌ردیابی تقریب بزنیم.

۹-۱ ساده‌سازی مدل فرایند مارکوفی به‌عنوان یک مدل سیستم دینامیکی

اکنون ما نشان می‌دهیم که چگونه می‌توان مدل فرایند مارکوفی را به یک مدل سیستم دینامیکی قابل‌ردیابی با استفاده از تقریب متوسط میدان[۲] به دست آورد.

طبق معادله(۱) و برای $v\in V$ داریم:

$$B_v(t+\Delta t)=\Delta t.\tilde{\theta}_{v,BR}(t).R_v(t)+(1-\Delta t.\tilde{\theta}_{v,RB}(t))B_v(t)+o(\Delta t),$$

[۱] Combat Power

[۲] Mean-field Approximation

که می‌تواند به‌صورت زیر نوشته شود:

$$\frac{B_v(t+\Delta t)-B_v(t)}{\Delta t}=\tilde{\theta}_{v,RB}(t).R_v(t)-\tilde{\theta}_{v,BR}(t))B_v(t)+o(\Delta t).$$

و به‌طور مشابه از معادله (۲) و برای $v\in V$ داریم:

$$\frac{R_v(t+\Delta t)-R_v(t)}{\Delta t}=\tilde{\theta}_{v,BR}(t).B_v(t)-\tilde{\theta}_{v,RB}(t))R_v(t)+o(\Delta t).$$

می‌توان نوشت:

$$E(\tilde{\theta}_{v,RB}(t))=E(f_{RB}(\frac{1}{\deg(v)}\sum_{u\in N_v}(\xi_u(t))).$$

با کمک تقریب میدان متوسط، می‌توانیم امید ریاضی را به داخل تابع توان نیرو برده که رابطه زیر را خواهیم داشت:

$$f_{RB}(\frac{1}{\deg(v)}\sum_{u\in N_v}E[\xi_u(t)])=f_{RB}(\frac{1}{\deg(v)}\sum_{u\in N_v}B_u(t)).$$

هم‌چنین احتمال انتقال حالت‌های $\theta_{v,RB}(t)$ و $\theta_{v,BR}(t)$ را به‌صورت زیر می‌نویسیم:

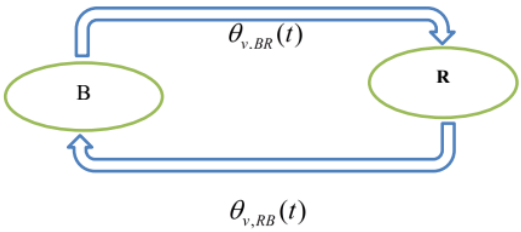
$$\theta_{v,BR}(t)=f_{BR}(\frac{1}{\deg(v)}\sum_{u\in N_v}(R_u(t))$$

بنابراین، برای هر $v\in V$، معادله (۳) می‌تواند به مدل سیستم دینامیکی زیر تبدیل گردد:

$$\begin{cases}\frac{d}{dt}B_v(t)=\theta_{v,RB}(t).R_v(t)-\theta_{v,BR}(t))B_v(t)\\ \frac{d}{dt}R_v(t)=\theta_{v,BR}(t).B_v(t)-\theta_{v,RB}(t))R_v(t)\end{cases}\qquad(۴)$$

توجه داشته باشید که مدل سیستم دینامیکی، برای هر $v\in V$ و به ازای پارامترهای $\theta_{v,RB}(t)$ و $\theta_{v,BR}(t)$ توپولوژی گراف را کدگذاری می‌نماید که این کدگذاری شامل اطلاعات تمام حالات همسایگی‌های رأس v است. نمودار مربوط به انتقال حالت برای هر رأس $v\in V$ در شکل ۸ نشان داده‌شده است.

$$\begin{cases}\frac{d}{dt}B_v(t)=\tilde{\theta}_{v,RB}(t).R_v(t)-\tilde{\theta}_{v,BR}(t))B_v(t)\\ \frac{d}{dt}R_v(t)=\tilde{\theta}_{v,BR}(t).B_v(t)-\tilde{\theta}_{v,RB}(t))R_v(t)\end{cases}$$



شکل(۸): نمودار انتقال حالت رأس $v\in V$

۹-۲نمونه‌سازی مدل سیستم دینامیکی از طریق توابع توان نبرد خاص

تابع توان نبرد $f_{RB}(.)$ توان یک مدافع در برابر یک مهاجم را به‌طور خلاصه‌شده نشان می‌دهد به‌طوری‌که دارای ۳ ویژگی زیر است:

I. $f_{RB}(0)=0$

II. $f_{RB}(1)=1$

III. $f_{RB}(.)$ is increases monotonically

این قابل‌درک است چون بیشتر رأس‌های B توسط رأس‌های R احاطه‌شده‌اند بیشترین احتمال برای رأس R این است که به رأس B برود(چراکه دفاع سایبری فعال از رأس‌های B شروع می‌کند). انواع مختلفی از توابع توان نبرد را می‌توان در نظر گرفت که به‌طور نمونه در ادامه به دو مورداشاره می‌نمایم.

- **نوع اول**

برای مقدار آستانه $\sigma\in(0,1)$ تعریف می‌نماییم:

$$f_{RB}(\frac{1}{\deg(v)}\sum_{u\in N_v}B_u(t))=\begin{cases}1 & \frac{1}{\deg(v)}\sum_{u\in N_v}B_u(t)\succ\sigma\\ 0 & \frac{1}{\deg(v)}\sum_{u\in N_v}B_u(t)\prec\sigma\\ \frac{1}{2} & otherwise\end{cases}$$

اگر $\sigma\prec\frac{1}{2}$ باشد، مدافع توانمندتر از مهاجم است. اگر $\sigma=\frac{1}{2}$ باشد، مهاجم قوی‌تر از مدافع بوده و اگر $\sigma\succ\frac{1}{2}$ باشد توان نبرد برابری دارند.

- **نوع دوم**

اگر تابع توان نبرد در بازه $[0,1]$ مقعر، پیوسته و صعودی باشد. هم‌چنین داشته باشیم:

I. $f_{RB}(0)=0$

II. $f_{RB}(1)=1$

III. $f_{RB}(x)\succ x \quad x\in(0,1)$

در این حالت مدافع پیشرفته‌تر از مهاجم است.

۹-۳ اعتبار سنجی مدل سیستم دینامیکی از طریق شبیه‌سازی

روش اعتبار سنجی ما متمرکز بر بررسی دقت دینامیک و دقت آستانه مدل سیستم دینامیکی است. برای بررسی دقت دینامیک، ما متوسط احتمال وقوع B را در مدل سیستم دینامیکی مقایسه می‌کنیم که با رابطه زیر محاسبه می‌شود:

$$\langle B_v(t)\rangle=\frac{1}{|V|}\sum_{v\in V}B_v(t)$$

کسر میانگین شبیه‌سازی‌شده مربوط به رأس‌های B در مدل فرآیند مارکوفی نیز طبق رابطه زیر حاصل می‌شود:

$$\langle \xi_v(t)\rangle=\frac{1}{|V|}\sum_{v\in V}\xi_v(t)$$

اگر $\langle B_v(t)\rangle$ و $\langle \xi_v(t)\rangle$ مشابه باشند. در این صورت اگر دقیقاً یکسان نباشند، از رفتار دینامیکی، نتیجه‌گیری می‌کنیم که نتایج تحلیلی حاصل از مدل سیستم دینامیکی طبیعتاً همان مدل فرایند مارکوفی هستند.

I. شبیه‌سازی مدل مارکوفی بر اساس معادله(۱) به‌صورت زیر است:

$$P(\xi_v(t+\Delta t)=1|\xi_v(t),v\in N)=\begin{cases}\Delta t.\tilde{\theta}_{v,RB}(t) & \xi_v(t)=0\\ 1-\Delta t.\tilde{\theta}_{v,BR}(t) & \xi_v(t)=1\end{cases}$$

که نرخ تصادفی $\tilde{\theta}_{v,RB}(t)$ با میانگین اش $\theta_{v,RB}(t)$ جایگزین می‌گردد. نتایج شبیه‌سازی‌ها بر اساس میانگین ۵۰ بار اجرای شبیه‌سازی می‌باشند.

II. محاسبات عددی در مدل سیستم دینامیکی، با معادله زیر انجام می‌گردد:

$$B_v(t+\Delta t)=B_v(t)+[\theta_{v,RB}(t)-B_v(t)]\Delta t.$$

در هر دو حالت مقدار $\Delta t=0.01$ را قرار می‌دهیم.

با انجام شبیه‌سازی‌ها در گرافER به ازای ۲۰۰۰ رأس و اتصال‌های مستقل با احتمال P=0.02 نتایج زیر حاصل شد.

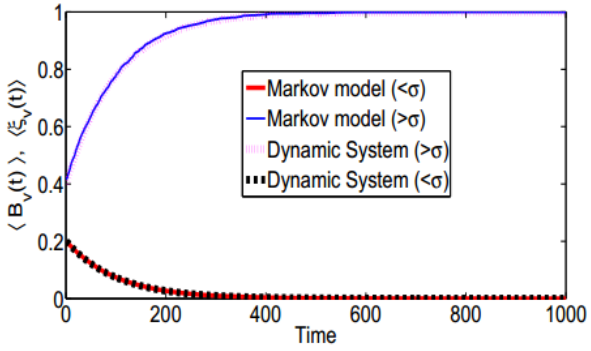
اگر تابع توان نبرد نوع اول را در نظر بگیریم که مدافعان غیراستراتژیک با احتمال تصرف اولیه $B_v(0)$ باشد. ثابت می‌شود که مدل سیستم دینامیک طبیعتاً همان مدل فرآیند مارکوفی است. به‌طور خاص، در مدل سیستم دینامیکی برای مقدارهای $\langle B_v(t)\rangle$،

$B_v(0)=0.4\succ\sigma=\frac{1}{3}$ همگرا به عدد یک و

$B_v(0)=0.2\prec\sigma=\frac{1}{3}$ همگرا به عدد صفر هستند.

در مدل‌های مارکوفی، برای مقدارهای $\langle\xi_v(t)\rangle$، که در رابطه $P\{\xi_v(0)=1\}=0.2$ صدق می‌کنند همگرا به عدد صفر و آن‌هایی که در رابطه $P\{\xi_v(0)=1\}=0.4$ صدق می‌کنند همگرا به عدد یک می‌باشند.

بنابراین رفتارهای دینامیکی منطبق با مدل مارکوفی مدنظر ماست.



شکل ۱۰.مقادیر $\langle \xi_v(t) \rangle$ در مقابل $\langle B_v(t) \rangle$ در دینامیک نوع اول با مدافع غیراستراتژیک و $\sigma = \frac{1}{3}$

۱۰ نتیجه‌گیری

در این مقاله، ابتدا مفهوم دفاع سایبری فعال و مؤلفه‌های آن مطرح شد. هم‌چنین اطلاعات اولیه ضروری برای اجرای دفاع سایبری فعال و گام‌های لازم برای هدایت مأموریت‌های دفاع سایبری فعال معرفی شدند. در ادامه با ارائه یک دسته‌بندی، انواع مأموریت‌های دفاع سایبری فعال و اهداف هریک از آن‌ها معرفی شدند که به‌عنوان یک چارچوب برای دفاع سایبری فعال خواهند بود. در پایان یک مدل مارکوفی برای مدل‌سازی دفاع سایبری فعال معرفی و اعتبار آن با کمک شبیه‌سازی سنجش گردید. با انجام شبیه‌سازی‌ها در گرافER به ازای ۲۰۰۰ رأس و اتصال‌های مستقل با احتمال P=0.02 نتایج زیر حاصل شد. اگر تابع توان نبرد نوع اول را در نظر بگیریم که مدافعان غیراستراتژیک با احتمال تصرف اولیه $B_v(0)$ باشد. ثابت می‌شود که مدل سیستم دینامیک طبیعتاً همان مدل فرآیند مارکوفی است. به‌طور خاص، در مدل سیستم دینامیکی برای مقدارهای $\langle B_v(t) \rangle$، $B_v(0) = 0.4 \succ \sigma = \frac{1}{3}$ همگرا به عدد یک و $B_v(0) = 0.2 \prec \sigma = \frac{1}{3}$ همگرا به عدد صفر هستند.

در مدل‌های مارکوفی، برای مقدارهای $\langle \xi_v(t) \rangle$، که در رابطه $P\{\xi_v(0) = 1\} = 0.2$ صدق می‌کنند همگرا به عدد صفر و آن‌هایی که در رابطه $P\{\xi_v(0) = 1\} = 0.4$ صدق می‌کنند همگرا به عدد یک می‌باشند. بنابراین رفتارهای دینامیکی منطبق با مدل مارکوفی مدنظر ماست.

۱۱- مراجع

[1] T. Alpcan and T. Basra, “Network Security: A Decision and Game Theoretic Approach”, Cambridge University Press, 2013.

[2] A. Bensoussan, M. Kantarcioglu and S. Hoe, “A game-theoretical approach for finding optimal strategies in a botnet defense model”, In Proc. GameSec’10, pages 135–148, 2010.

[3] M. Collins, “Cost-based mechanism for evaluating the effectiveness of moving target defenses. In Proc. GameSec’12, pages 221–233, 2012.

[4] M. Khouzani, S. Sarkar and E. Altman, “A dynamic game solution to malware attack”, In Proc. IEEE INFOCOM, pages 2138–2146, 2016.

[5] M. Khouzani, S. Sarkar and E. Altman, ”Saddle-point strategies in malware attack”, IEEE Journal on Selected Areas in Communications, 30(1):31–43, 2017.

[6] R. P´ıbil, V. Lis´y, C. Kiekintveld, B. Bosons’ and M. Pechoucek, “Game theoretic model of strategic honeypot selection in computer networks”, In Proc. GameSec’12, pages 201–220, 2017.

[7] L. Shaughnessy, “The internet: Frontline of the next war? “, November 7, 2015.

[8] George Theodorakopoulos, Jean-Yves Le Boudec and John S. Baras, “Selfish response to epidemic propagation”, IEEE Trans. Aut. Contr., 58(2):363–376, 2013.

[9] M. Vojnovic and A. Ganesh, “On the race of worms, alerts, and patches”, IEEE/ACM Trans. Netw., 16:1066–1079, October 2014.

[6] D. Chakrabarti, Y. Wang, C. Wang, J. Leskovec, and C. Faloutsos, “Epidemic thresholds in real networks”, ACM Trans. Inf. Syst. Secure., 10(4):1–26, 2008.

[22] R. P´ıbil, V. Lis´y, C. Kiekintveld, B. Bosansk´y, and M. Pechoucek, “Game theoretic model of strategic honeypot selection in computer networks”, In Proc. GameSec’12, pages 201–220, 2012.

[23] B. Schneider, “Benevolent worms”, http://www.schneier.com/blog/archives/2008/02/benevolent_worm_1.html, February 19, 2008.

[24] L. Shaughnessy. The internet: Frontline of the next war? http://www.cnn.com/2011/11/07/us/darpa/, November 7, 2011.

[25] G. Theodorakopoulos, Jean-Yves Le Boudec, and John S. Baras, “Selfish response to epidemic propagation. IEEE Trans. Aut. Contr., 58(2):363–376, 2013.

[26] P. Van Mieghem, J. Omic, and R. Kooij, “Virus spread in networks”, IEEE/ACM Trans. Netw., 17(1):1–14, February 2009.

[27] M. Vojnovic and A. Ganesh, “On the race of worms, alerts, and patches”, IEEE/ACM Trans. Netw., 16:1066–1079, October 2008.

[28] Y. Wang, D. Chakrabarti, C. Wang, and C. Faloutsos. Epidemic spreading in real networks: An eigenvalue viewpoint. In Proc. IEEE SRDS’03, pages 25–34, 2003.

[29] N. Weaver and D. Ellis, “White worms don’t work”, Login: The USENIX Magazine, 31(6):33–38, 2006.

[30] Homeland Security News Wire. Active cyber-defense strategy best de active-cyber-defense-strategy-best-deterrent-against-cyber-attacks, 28 June 2011.

[31]S. Xu, W. Lu, and L. Xu, “Push- and pull-based epidemic spreading in arbitrary networks: Thresholds and deeper insights. ACM Transactions on Autonomous and Adaptive Systems (ACM TAAS), 7(3):32:1–32:26, 2012.

[32] S. Xu, W. Lu, L. Xu, and Z. Zhan, “Adaptive epidemic dynamics in networks: Thresholds and control”, ACM Transactions on Autonomous and Adaptive Systems (ACM TAAS), to appear.

[33] S. Xu, W. Lu, and Z. Zhan. A stochastic model of

multivirus dynamics. IEEE Trans. Dependable Sec. Compute., 9(1):30–45, 2012.