مجله‌ی سیاست دفاعی
سال بیست و چهارم، شماره‌ی ۹۳، زمستان ۱۳۹۴

راهبردهای پدافند غیرعامل در برابر تهدیدهای پایدار پیشرفته در محیط سایبری

سعید کافی [۱]

تاریخ دریافت مقاله: ۱۳۹۴/۰۳/۱۰
تاریخ تأیید مقاله: ۱۳۹۴/۰۶/۱۹
صفحات مقاله: ۷۱ - ۵۱

چکیده:

با توجه به گسترش فناوری اطلاعات و وابستگی روزافزون جوامع بشری به این فناوری حوزه‌های جدید تهدید نیز شکل گرفته است. یکی از این تهدیدها به نام تهدیدهای پایدار پیشرفته شناخته می‌شود و بی‌توجهی به آن آثار و عواقب جبران ناپذیری را برای تداوم فعالیت جوامع بشری به‌دنبال خواهد داشت. تهدیدهای پایدار پیشرفته، یکی از دغدغه‌های مهم جوامع امروز بشری است. تهدید پایدار پیشرفته‌ی سازمان‌های خاصی را به‌منظور سرقت اطلاعات و یا واردآوردن خسارت به اموال و دارایی‌ها مورد هدف قرار می‌دهد.

مقاله‌ی حاضر از نوع کاربردی و به روش توصیفی تحلیلی - پیمایشی صورت گرفته است. این روش تحقیق برای توصیف عینی و کیفی محتوای مفاهیم مبتنی بر یک روش نظامند برای تبیین راهبردهای پدافند غیرعامل در برابر تهدیدهای پایدار پیشرفته در محیط سایبری ارائه شده است، به‌کار می‌رود. بنابراین، سؤال اصلی پژوهش، راهبردهای پدافند غیرعامل در برابر تهدیدهای پایدار پیشرفته در محیط سایبری چیست؟ و سؤال فرعی آن شاخص‌های تهدیدهای پایدار پیشرفته کدام است؟، می‌باشد. در تحقیق حاضر برای تدوین ادبیات و چارچوب نظری از مطالعه‌ی اسنادی و کتابخانه‌ی تخصصی و نیز مصاحبه استفاده شده است. در نهایت نتیجه‌گیری شد که هر سازمانی که دارای اطلاعات ارزشمند است، در برابر تکنیک‌های تهدید پایدار پیشرفته آسیب‌پذیر است. از طرفی دیگر، هر چه اطلاعات سازمان از ارزش بیش‌تری برخوردار باشد، احتمال مورد تهدید قرارگرفتن سازمان نیز بیش‌تر است.

* * * * *

واژگان کلیدی

فناوری اطلاعات، حوزه‌های جدید تهدید، تهدیدهای پایدار پیشرفته، راهبردهای پدافند غیرعامل، فضای سایبری.

---

۱ - استادیار دانشگاه جامع امام حسین(ع)

مقدمه

تهدیدهای پایدار پیشرفته[۱]، نگرانی بزرگ جامعه‌ی فناوری اطلاعات در عصر حاضر به‌شمار می‌آید. حملات اخیر به دولت‌های کانادا، فرانسه، اتحادیه‌ی اروپا و سایر کشورها ناشی از تهدیدهای پایدار پیشرفته بوده است، اما تهدید پایدار پیشرفته چیست؟ سازمان‌ها و نهادهای دولتی و خصوصی تا چه میزان در معرض این تهدید قرار دارند؟ مقاله‌ی حاضر، ماهیت تهدیدهای پایدار پیشرفته را توصیف کرده و راهبردهایی در خصوص محافظت سازمان‌ها در برابر این تهدید ارائه می‌دهد.

بیش‌تر پژوهش‌گرهای حوزه‌ی امنیتی بر این باورند که نخستین‌بار واژه‌ی "تهدید پایدار پیشرفته" را نیروی هوایی ارتش آمریکا در سال ۲۰۰۶ برای توصیف حملات سایبری پیچیده (پیشرفته) در برابر اهداف خاص در مدت زمان طولانی (منظور پایداری آن است) به‌کار برده است.

در ابتدا این واژه برای بیان سرقت اطلاعات از یک کشور و یا وارد آوردن خسارت به کشورها با هدف بهره‌برداری راهبردی مورد استفاده قرار می‌گرفت، اما بتدریج معنای آن گسترش یافت و کارشناسان امنیتی و رسانه‌ای برای اشاره به حملات سایبری که از سوی مجرمان سایبری با هدف سرقت اطلاعات از سازمان‌ها صورت می‌گرفت، از آن استفاده کردند.

حال این که واژه‌ی تهدید پایدار پیشرفته برای اشاره به فعالیت مجرمان سایبری با هدف سرقت اطلاعات سازمان‌ها مورد استفاده قرار می‌گیرد یا خیر، موضوع معناشناسی است، اما آنچه که برای کارشناسان امنیتی حائز اهمیت است، اطلاع از این واقعیت است که همان تکنیک‌های تهدید پایدار پیشرفته‌ی مورد استفاده‌ی کشورها برای بهره‌برداری راهبردی از سوی مجرمان سایبری استفاده می‌شود و هدف از استفاده نیز سرقت اطلاعات از سازمان‌هاست. بنابراین، سازمان‌های دولتی و خصوصی نیازمند شناخت این تهدید و تکنیک‌های آن به‌منظور محافظت از خود در برابر آن هستند. برای این منظور، خصوصیات تهدید پایدار پیشرفته، فرآیند آن، سیکل زمانی فعالیت بدافزار بر اساس شیوه‌های جدید به‌کارگیری مورد بررسی قرار

۱ - Advanced Persistent Threats (APT)

می‌گیرد. راهبردها و تاکتیک‌های پیشنهادی برای مقابله با این تهدید نیز بر اساس شیوه‌ی عملکرد آن ارائه می‌شود.

بیان مسأله

با توجه به گسترش فناوری اطلاعات و وابستگی روزافزون جوامع بشری به این فناوری حوزه‌های جدید تهدید نیز شکل گرفته است. یکی از این تهدیدها به نام تهدیدهای پایدار پیشرفته شناخته می‌شود و بیرتوجهی به آن آثار و عواقب جبرانرناپذیری را برای تداوم فعالیت جوامع بشری بهردنبال خواهد داشت. بنابراین، در صورت فقدان راهبرد مشخص برای مقابله با این تهدیدها خسارات سنگینی وارد خواهد شد تا جایی که امکان جبران آن به‌راحتی وجود نخواهد داشت. این تحقیق به‌عنوان مسأله‌ی خود به ارائه‌ی راهبردهای پدافند غیرعامل در برابر تهدیدهای پایدار پیشرفته می‌پردازد.

ضرورت و اهمیت تحقیق

با توجه به وابستگی هر چه بیش‌تر و روزافزون ابعاد مختلف جوامع بشری به فناوری اطلاعات و لزوم تداوم فعالیت‌های بشری بدون وجود اختلال در کارکرد آنها و نیز امنیت اطلاعاتی در این حوزه انجام این تحقیق برای یافتن راهبردهای پدافند غیرعامل در برابر تهدیدهای پایدار پیشرفته از ضرورت و اهمیت بالایی برخوردار خواهد بود.

هدف اصلی و فرعی تحقیق

هدف اصلی: تبیین راهبردهای پدافند غیرعامل در برابر تهدیدهای پایدار پیشرفته در محیط سایبری

هدف فرعی: تبیین شاخص‌های تهدیدهای پایدار پیشرفته

سؤال اصلی و فرعی تحقیق

سؤال اصلی: راهبردهای پدافند غیرعامل در برابر تهدیدهای پایدار پیشرفته در محیط سایبری چیست؟

سؤال فرعی: شاخص‌های تهدیدهای پایدار پیشرفته کدام است؟

نوع و روش تحقیق

تحقیق حاضر از نوع کاربردی و به روش توصیفی تحلیلی- پیمایشی صورت گرفته است. این روش تحقیق برای توصیف عینی و کیفی محتوای مفاهیم مبتنی بر یک روش نظامند به‌کار می‌رود. در واقع، قلمرو این روش تحقیق را اسناد مکتوب، شفاهی و تصویری نظیر کتاب‌ها، مقاله‌ها، روزنامه‌ها، مجله‌ها، مطالب نوار و فیلم، سخنرانی‌ها... درباره‌ی موضوعی خاص تشکیل می‌دهد. برلسون روش تحلیلی را ابزاری برای توصیف عینی، سیستماتیک و کمّی محتوای مطالب تعریف کرده است. (Chandrashekar, 2008: 11)

روش و ابزار گردآوری اطلاعات

در تحقیق حاضر، برای تدوین ادبیات و چارچوب نظری از مطالعه‌ی اسنادی و کتابخانه‌ی تخصصی و نیز مصاحبه استفاده شده است.

ادبیات تحقیق

تهدیدها: مفاهیم و کارکردها

هدف از تهدیدها تأثیرگذاری بر اراده، اعتقادات، افکار و احساسات مخاطبان به‌منظور انهدام یا به تسلیم کشاندن جامعه‌ی هدف است. وجه اشتراک تمام تهدیدها، تحمیل اراده به دشمن است، همان‌طور که هدف از جنگ این‌گونه است. بشر همواره در معرض تهدید قرار داشته است. برخی از تهدیدها طبیعی (مانند زلزله، سیل، طوفان) و برخی دیگر از تهدیدها غیرطبیعی است. تهدیدهای غیرطبیعی خود به دو نوع (بدون برنامه‌ریزی مانند نزاع‌های انفرادی، تصادفات، سهل‌انگاری‌ها و ...، و برنامه‌ریزی‌شده توسط فرد یا گروه یا کشور و یا مجموعه‌ای از کشورها علیه افراد یا گروها یا کشور یا کشورهای دیگر) است. از طرفی تهدید همیشه در مقابل امنیت قابل طرح است، و آن نیز مبتنی بر تصورات ذهنی است. «تهدید» ادراکی ذهنی و نقطه‌ی آغاز شکل‌گیری نگرانی از مخاطرات و پیامدهای تحقق تهدید نسبت به منافع و ارزش‌هاست. مفهوم تهدید همانند سایر مفاهیم علوم اجتماعی با تغییر و تداوم همراه

است. تنها نام تهدید ثابت است، اما مفهوم آن پدیده‌ای پویا و در حال رشد و توسعه و تکامل است که در موقعیت‌های مختلف معانی متفاوتی دارد. برای ارائه‌ی تعریف از مفهوم تهدید با توجه به درون‌مایه‌ی بحث تهدیدات و ذهنی بودن آن نمی‌توان از یک نقطه‌ی ساکن برای توضیح درباره‌ی ادراکات ذهنی نسبت به تهدید شروع کرد، بلکه نوعی پیوستگی و تعامل عمیق میان تهدید و ادراک ذهنی از تهدیدها در سطوح و زمان‌های مختلف وجود دارد و اساساً پویایی و گسترش و تعمیق مفهوم تهدید و تعریف از تهدیدها، حاصل همین پیوستگی مفهوم با وقایع و رخدادهاست. مفهوم تهدید در ادبیات سیاسی– امنیتی به معنای توانایی‌ها، نیات و اقدامات دشمن بالفعل و بالقوه برای ممانعت از دستیابی موفقیت‌آمیز خودی به علائق و مقاصد امنیت ملی یا مداخله به نحوی که نیل به علائق و مقاصد به خطر بیفتد، تعریف شده است. (Lipinski, 2015)تهدید به گمان لازاروس (۱۹۶۸) انتظار نوعی خسارت و ضرر و زیانی است که هنوز پیش نیامده، اما مورد انتظار است. تهدید ممکن است نسبت به ارزش‌های کسی فعال یا منفعل، قوی یا ضعیف و مرکزی یا حاشیه‌ای باشد. (ibid, P.21) به بیان دیگر، وضعیت فوری محرک که نتیجه‌اش تهدید است، تنها خبر از آسیبی می‌دهد که نسبت به منافع و ارزش‌ها در راه است. ظهورعلائم نگران‌کننده بر اساس دگرگونی در محیط، موضع‌گیری، رخدادهای سیاسی– امنیتی و پاره‌ای از عوامل دیگر واقعیات جدیدی را شکل می‌دهد، که به منزله‌ی "پیدایش وضعیت" جدید است. ادراک تهدید متأثر از ظهور واقعبات جدید است که در تعامل با ادراک ذهنی مفهوم تهدید و کنش و واکنش‌ها را تشکیل می‌دهد. در ادبیات سیاسی کنونی تهدیدات را به سه نوع تقسیم کرده‌اند: تهدیدات سخت (جنگ نظامی)، تهدیدات نیمه‌سخت (اقدامات اطلاعاتی و امنیتی)، تهدیدات‌نرم (اقدامات فرهنگی، سیاسی، اجتماعی، اقتصادی، رسانه‌ای، سایبری و...). عرصه‌ی تهدیدهای نرم می‌تواند متنوع و وسیع باشد، اما برای جلوگیری از بسط مطلب سعی خواهد شد، آن را در دسته‌بندی محدودتری ارائه نمود. با این توضیح، عرصه‌های تهدیدهای نرم را می‌توان در شش دسته تقسیم نمود: ۱) حوزه‌ی تهدیدها سیاسی؛ ۲) حوزه‌ی تهدیدها اقتصادی؛ ۳) حوزه‌ی تهدیدها فرهنگی؛ ۴) حوزه‌ی تهدیدات اجتماعی؛ ۵) حوزه‌ی تهدیدها فناوری اطلاعات و ارتباطات اجتماعی؛ ۶) حوزه‌ی تهدیدها

علمی و اندیشه‌ای. پرداختن به تمام انواع تهدیدها خارج از موضوع و حوصله‌ی تحقیق حاضر است. بنابراین، تنها به تهدیدهای فناوری اطلاعات و ارتباطات اجتماعی پرداخته می‌شود: فضای به‌وجود آمده از تهدیدهای ارتباطی مربوط به پدیده‌ی عصر حاضر یعنی عصر ارتباطات یا اطلاعات و هم‌چنین عصر انفجار اطلاعات است. در محیط این تهدید مخاطب با هزاران طول موج‌های رادیویی، امواج دیجیتالی، فیبر نوری، سیگنال‌های مختلف، فناوری‌ها، جامعه‌ی شبکه‌ای و چندرسانه‌ای، تلفن‌های همراه و نسل اول و دوم تلفن‌های سلولی، اینترنت و امواج ماهواره‌ای دیجیتالی، فرستنده‌های مینیاتوری، ماکرویوهای با توان بالا و ابزارهای نوین در عملیات روانی مانند اشعه‌های الکترومغناطیس، سایکو تروپیک[۱]، لیزری، خواب رادیویی[۲]، امواج کوتاه الکتریکی تنش‌ساز[۳] و فناوری‌های نوین در عملیات روانی مانند هواپیماهای بدون سرنشینِ کومندو سولو [۴]، و... مواجه است. (Zurich, 2009, P.88)

خصوصیات تهدید پایدار پیشرفته

تهدید پایدار پیشرفته، سازمان‌های خاصی را به‌منظور سرقت اطلاعات خاص و یا وارد آوردن خسارت به اموال و دارایی‌ها مورد هدف قرار می‌دهد. این شیوه عملکرد مقابل بیش‌تر نرم‌افزارهای با محتوای مخرب که در هر سامانه‌ی آلوده به‌صورت تصادفی عمل می‌کنند، قرار می‌گیرد. حملاتی که در سال‌های اخیر به برخی از سازمان‌ها در دنیا صورت گرفت، حملات فرصت‌طلبانه با هدف قربانی کردن هر سازمانی در هر سطح ممکن نبوده است، بلکه این حملات با سرمایه‌گذاری مالی و زمانی به‌منظور بهره‌برداری از اهداف مشخص صورت گرفته است. دو نتیجه از این شرایط می‌توان گرفت: نخست آن‌که هر سازمانی که دارای اطلاعات ارزشمند است و در برابر تکنیک‌های تهدید پایدار پیشرفته آسیب‌پذیر است. دوم آن‌که هرقدر اطلاعات سازمان از ارزش بیش‌تری برخوردار باشد، احتمال مورد تهدید قرار گرفتن سازمان

۱ - Psychotropic
۲ - Radiosleep radioson
۳ - Pulsed microwaves
۴ - Commando solo

نیز بیش‌تر است. اقتصاد جرائم سایبری با استخدام هکرهای حرفه‌ای به خوبی سازمان یافتـه و دایر شده است. (ibid, p.23)

پایداری

تهدید پایدار پیشرفته در مراحل مختلف در طول زمان شکل می‌گیرد. مهاجم پیش از حملـه‌ی واقعی تنها اطلاعاتی از سازمان مورد هدف و اهداف خـود دارد. آنهـا نمی‌داننـد داده‌هـای ارزشـمند سازمان موردهدف در کجا قرار دارند، چه کنترل‌هـای امنیتـی وجـود دارد و یـا چـه آسـیب‌هایی در سازمان برای بهره‌برداری قابل دسترس است. مهاجم برای سرقت اطلاعات آسـیب‌پذیری‌ها را مـورد شناسایی قرار داده، کنترل‌های امنیتی موجود را ارزیابی می‌کند، بـه میزبان‌هـا در محـدوده‌ی شـبکه‌ی هدف دسترسی پیدا می‌نماید، اطلاعـات هـدف را پیـدا می‌کنـد و سـرانجام اطلاعـات را از شـبکه استخراج می‌نماید. کل این فرآیند ماه‌ها و یا حتی سال‌ها طول می‌کشد. بنابراین، کشـف ایـن تهدیـد تنها با تکیه بر مشاهده‌ی هر اتفاقی ممکن نیست، بلکه باید به‌دنبـال مجموعـه رویـدادهایی بـود کـه ویژگی متدولوژی‌های تهدیدهای پایدار پیشرفته است. (Eeten, 2006, P.2)

تهدیدهای پایدار پیشرفته به‌طور سیستماتیک با هدف فرار از دام محصولات امنیتی سنتی که بیش‌تر سازمان‌ها سال‌ها به آنها تکیه می‌کنند، طراحی شده است. برای مثال، بـه مـوارد زیـر اشاره می‌شود:

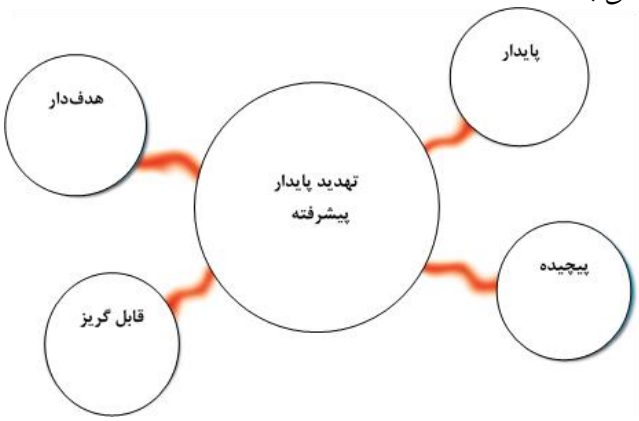
مهاجم برای دستیابی به میزبان‌های درون شـبکه‌ی هـدف ضـمن پرهیـز از فایروال‌هـای شبکه، تهدیدهایی را درون محتوای پروتکل‌های معمول (http, https, smtp , etc) ارائه می‌دهد. مهاجم برای نصب بدافزارها در شبکه‌ی میزبان ضمن پرهیز از برنامه‌های ضدویروس کـدهایی را برای محیط هدف معین می‌نویسد. ایـن کـدها تـا پـیش از بـه‌کـارگیری در جـایی مشـاهده نشده‌اند و به همین دلیل، هیچ برنامه‌ی ضدویروسی برای ایجاد محافظـت در برابـر آن وجـود ندارد. مهاجم برای ارسال اطلاعات به خارج از شبکه‌ی هـدف ضـمن پرهیـز از فایروال‌هـا از رمزگذاری متداول استفاده کرده و محتواهای را از طریق پروتکل‌های مجـاز از نظـر فایروال‌هـا خارج می‌کند. (Dunn, 2005, P.11)

پیچیدگی تهدیدهای پایدار پیشرفته

تهدیدهای پایدار پیشرفته، ترکیب پیچیده‌ای از روش‌های حمله را با هدف‌گیری آسیب‌های چندگانه‌ی شناسایی‌شده در سازمان مورد استفاده قرار می‌دهند. یک تهدید پایدار پیشرفته‌ی مشخص گام‌های زیرا به‌عمل می‌آورد: (ibid, p19)

- استفاده از مهندسی اجتماعی مبتنی بر شبکه‌ی تلفن به‌منظور شناسایی اشخاص کلیدی درون سازمان؛
- شکار نامه‌های الکترونیکی ارسالی به اشخاص کلیدی در سازمان از طریق اتصال به وب‌سایتی که کدهای جاوا اسکریپت را به‌منظور نصب ابزار دسترسی از راه‌دور اجرا می‌کند؛
- استفاده از کدهای فرماندهی و کنترل باینری (کدهای متعارف و یا کدهای تولیدی با استفاده از کیت‌های بدافزاری موجود متداول)؛
- استفاده از فناوری رمزگذاری متعارف.

بی‌تردید، اتخاذ تنها یک اقدام امنیتی نمی‌تواند پوششی را برابر تمام اقدام‌های تهدیدآمیز فراهم کند. راهبردهای موفقیت‌آمیز پدافند غیرعامل در برابر تهدیدهای پایدار پیشرفته باید چندلایه و مبتنی بر مکانیزم‌های دفاعی چندگانه همراه با شناسایی الگوهای پیچیده‌ی فرار از دام شبکه‌ی دفاعی باشد.



تصویر شماره‌ی ۱ – ویژگی‌های تهدید پایدار پیشرفته

فرآیند تهدید پایدار پیشرفته

فرآیند تهدید پایدار پیشرفته سه مرحله‌ی مهم را دربر می‌گیرد که در طول چند ماه رخ می‌دهد. این مراحل شامل موارد زیر می‌شود:(MIT, 2008, p15)

- مرحله‌ی اول: شناسایی، آغاز حمله و آلوده‌سازی: مهاجم در این مرحله، هدف را شناسایی کرده و آسیب‌های آن را مشخص می‌کند، حمله را آغاز می‌نماید و میزبان‌های هدف را آلوده می‌کند. مهاجم در این مرحله نقاط رخنه، آسیب‌ها، اشخاص مهم و تجهیزات کلیدی را جستجو می‌کند. این موارد می‌تواند شامل مجریان رده‌ی بالا، گردانندگان فناوری اطلاعات و میزبان‌هایی شود که امکان دسترسی به منابع هدف را در سازمان فراهم می‌کنند. این مرحله شامل به‌کارگیری یک یا چند روش می‌شود که با هدف دسترسی به میزبان صورت می‌گیرد. در این مرحله، حملات هدفمند و شکار اطلاعات به‌منظور جلوگیری از کشف حمله از شدت کمی برخوردار است. (IETF, 2014, P.51)

روش‌های متداول در این خصوص شامل موارد زیر می‌شود: (DOT ,2008, p12)

- نامه‌های الکترونیکی جذاب با لینک‌هایی که ارتباط با وب‌سایت‌های حامل بدافزارها را فراهم می‌کند؛
- نامه‌های الکترونیکی با فایل‌های پیوست در فرمت‌های متداول مانند آفیس و پی.دی.اف. این پیوست‌ها شامل کدهای حمله با استفاده از بدافزارهای ناشناخته‌ای می‌شود که هدف از به‌کارگیری آنها حمله به آسیب‌هایی است که قبلاً شناخته نشده بودند؛
- استفاده از وب‌سایت‌های آلوده که مورد علاقه‌ی افراد موردهدف هستند. این افراد از طریق پروفایل‌های رسانه‌های اجتماعی شناسایی می‌شوند؛
- مهندسی اجتماعی به‌منظور کسب اطلاعات در خصوص توانایی‌های فردی کاربران مورد هدف.

کد متعارف برای آلوده‌سازی در شبکه میزبان نصب می‌شود. این کد گزارش‌های مربوطه را با استفاده از شبکه و سایر اطلاعات که مهاجم را در مرحله‌ی دوم کمک می‌کند، به مرکز فرماندهی و کنترل ارائه می‌دهد.

- مرحله‌ی دوم: کنترل، روزآمدسازی، کشف و پایداری: مهاجم در این مرحله میزبان‌های آلوده را کنترل می‌کند، کد را روزآمد می‌نماید، آلودگی را گسترش می‌دهد و اطلاعات هدف را کشف و جمع‌آوری می‌کند. مهاجم از راه دور کنترل میزبان‌های آلوده را با استفاده از سرویس فرماندهی و کنترل در دست می‌گیرد. هرچند که در مواردی این سرویس در میزبان درون شبکه هدف قرار داشته است، اما مواردی نیز مشاهده شده است که سرویس فرماندهی و کنترل از طریق اینترنت در اختیار قرار گرفته است. سرویس فرماندهی و کنترل به مهاجم این امکان را می‌دهد تا از راه دور بدافزار را به روز کند و بدافزارهای جدید را اضافه نماید و فرامینی را به میزبان ارسال نماید. (EU, 2013, P.15)

در این مرحله، اجزای اضافی با توانایی کشف اطلاعات هدف در میزبان‌های آلوده پیاده می‌شود. اهداف کلیدی شامل سرورهای "PKI" و دیرکتوری‌های فعال برای دسترسی به اطلاعات محرمانه می‌شود. نظارت بر اطلاعات مورد استفاده‌ی کاربران و رخنه به سیستم‌هایی که کاربران مجوز ورود به آنها را دارند، یکی از روش‌های کشف اطلاعات است. مهاجم با کشف میزبان‌های بیش‌تر کنترل بیش‌تری را در شبکه‌ی هدف به‌دست می‌آورد و از آسیب‌های شبکه و سایر آسیب‌های در سطح سیستم برای آلوده‌سازی سایر میزبان‌ها استفاده می‌کند. ابزارهای مورد استفاده برای اعمال کنترل بیش‌تر در شبکه‌ی ابزارهای استاندارد شبکه مانند "Gsecdump" ، "Cain & Abe" ، "SSH" ، "RDP" است. (E- government, 2009, P.32)

- مرحله‌ی سوم حمله: استخراج اطلاعات و اقدام به حمله: مهاجم در این مرحله، اطلاعات را از شبکه‌ی هدف استخراج می‌کند و اقدامات لازم را به‌عمل می‌آورد (اطلاعات را خارج می‌کند). مهاجم در این مرحله، کنترل یک یا چند میزبان را درون

شبکه‌ی هدف در دست گرفته است و اقدامات لازم را برای گسترش دسترسی و شناسایی اطلاعات هدف به‌عمل می‌آورد. (Alperovitch, 2011, P.12)

تنها اقدامی که در این مرحله باقی می‌ماند، ارسال اطلاعات به خارج از شبکه است. دریافت‌کننده‌ی اطلاعات می‌تواند سرور فرماندهی و کنترل و یا سروری که پیش از این از آن استفاده نمی‌شد، باشد. (Drew, D.M.Snow, 2012, p.21)

این سرور یا در محل استقرار مهاجم و یا در کشور دیگری قرار دارد. حمله تا زمانی که مهاجم به اطلاعات موردنیاز خود دسترسی پیدا کند، ادامه خواهد داشت و پس از آن و یا در صورت اطلاع قربانی و اقدام به قطع ارتباط متوقف خواهد شد. در این مرحله چند اتفاق روی خواهد داد. (CCRA,2009, P.15)

- فروش شیوه‌های حمله: در صورتی که قربانی توانایی خنثی‌سازی حمله را نداشته باشد، روش‌های حمله به سایر مهاجمان فروخته می‌شود تا از همان شیوه برای حمله به قربانی استفاده گردد؛
- فروش اطلاعات: در صورتی که اطلاعات ذی‌قیمتی به سرقت رفته باشد، مهاجم اطلاعات را به مخاطبان اطلاعات سرقت رفته می‌فروشد؛
- افشای رسانه‌ای: اطلاعات به سرقت‌رفته ممکن است در اختیار رسانه‌ها قرار گیرد تا برای مقاصد سیاسی و وارد آوردن فشار افکار عمومی بر مخاطبان مورد استفاده قرار گیرد.

چرخه‌ی عمر به‌کارگیری بدافزار

روش‌های مورد استفاده در تهدیدهای پایدار پیشرفته همواره به یک حمله ختم نمی‌شود. این تکنیک‌ها کپی شده و مورد استفاده‌ی سایر نفوذگرها برای نفوذ به سازمان‌های دیگر قرار می‌گیرد. حتی بتدریج احتمال شکل‌گیری کیت‌های بدافزار برای استفاده‌ی عموم هکرها به بهای مشخصی وجود دارد. (Chandrashekar, 2008, P.11)

در این حالت، چرخه‌ی عمر تهدیدهای پایدار پیشرفته تا سال‌ها بیش از میزان عمر اولیه‌ی آن ادامه خواهد داشت و صدها قربانی دیگر را جدای از قربانی اولیه‌ی آن مورد هدف قرار می‌دهد. (DHS, 2008, P.33)

ضرورت‌های به‌کارگیری اقدامات پدافند غیرعامل در برابر تهدیدهای پایدار پیشرفته

با تحلیل خصوصیات تهدیدهای پایدار پیشرفته که پیش از این شرح داده شد، ضرورت‌های مهم راهبرد امنیتی مؤثر قابل تشریح است:

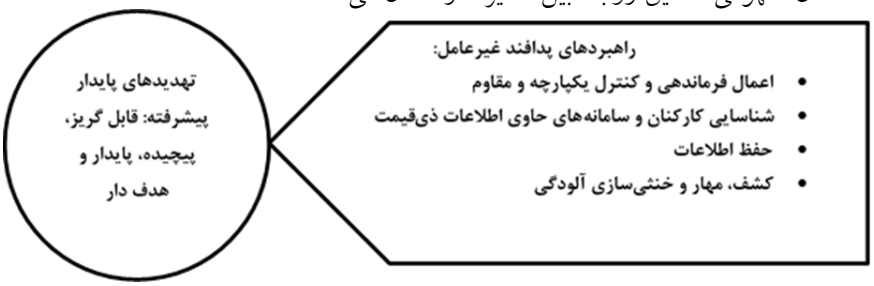
شناخت محتوایی: از آنجایی که تهدیدهای پایدار پیشرفته با بهره‌برداری از پروتکل‌های مجاز متداول به پدافند فایروال شبکه نفوذ می‌کند، تدوین راهبردهای تهدیدهای پایدار پیشرفته، نیازمند شناخت عمیق از محتوای تهدید است.

شناخت مجموعه علائم تهدید: از آنجایی که بیش‌تر تهدیدهای پایدار پیشرفته از کدهای متعارف و آسیب‌های هدف استفاده می‌کنند، با استفاده از یک "IPS" و ضدبدافزار نمی‌توان تهدید را شناسایی کرد. بدون وجود علائم قابل تعریف حمله باید به مشخصه‌های کم‌تری تکیه کرد. هرچند که یک مشخصه‌ی مشکوک برای شناسایی حمله کافی نیست، اما در صورت ارزیابی هر یک از مشخصه‌های مشکوک در کنار سایر مشخصه‌ها امکان جمع‌آوری شواهد کافی قابل اطمینان برای تشخیص فعالیت بدافزارها وجود دارد. (Complexity and Organizational Surprises, 2011, P.23)

شناخت موقعیت زمانی: هر چند که سازمان‌ها ممکن است اطلاع دقیقی از چگونگی تهدیدهای پایدار پیشرفته نداشته باشند، اما اکثر سازمان‌ها می‌توانند اهمیت موقعیت زمانی سازمان خود را شناسایی کنند. بنابراین، فناوری ممانعت از سرقت اطلاعات به‌عنوان یک لایه‌ی دفاعی برای شناسایی تاریخ‌های مهم و جلوگیری از سرقت اطلاعات قابل ایجاد است. شناسایی کاربرد کدها در ترافیک شبکه در دفاع تهدید پایدار پیشرفته حائز اهمیت است. (Chaturvedi, 2007, P.43)

مدل مفهومی تحقیق

مدل مفهومی تحقیق روابط بین متغیرها را نشان می‌دهد.



تجزیه و تحلیل داده‌ها و یافته‌های تحقیق

تحلیل توصیفی پاسخ دهندگان

مدرک تحصیلی	فراوانی	درصد	درصد تجمعی
کارشناس و کارشناس ارشد	۲۸	۷۰	۷۰
دکترای	۱۲	۳۰	۱۰۰
کل	۴۰	۱۰۰	۱۰۰

بر اساس جدول فوق از کل پاسخ‌دهندگان بیش‌ترین تعداد (۷۰ درصد) دارای مدرک کارشناسی و کارشناسی ارشد و کم‌ترین تعداد معادل ۳۰ درصد دارای مدرک دکترای تخصصی هستند.

سابقه شغلی مرتبط	فراوانی	درصد	درصد تجمعی
۱۵-۵ سال	۱۵	۳۷,۵	۳۷,۵
۲۵-۱۵ سال	۱۲	۳۰	۶۷,۵
۳۵-۲۵ سال	۱۳	۳۲,۵	۱۰۰
کل	۴۰	۱۰۰	۱۰۰

نتایج حاصل از میانگین و انحراف استاندارد راهبردهای پدافند غیرعامل

شاخص	تعداد سوال	میانگین کل	انحراف استاندارد	میانگین خطای استاندارد
اعمال فرماندهی و کنترل یکپارچه و مقاوم	۱۰	۱,۱۴	۰,۸۴۲	۰,۱۱۹
شناسایی کارکنان و سامانه‌های حاوی اطلاعات	۱۰	۱,۱۹	۰,۵۷۴	۰,۰۸۲
ذی‌قیمت حفظ اطلاعات	۱۰	۱,۲۳	۰,۴۷۵	۰,۰۴۸
کشف، مهار و خنثی‌سازی آلودگی	۱۰	۱,۱۸	۰,۴۴۵	۰,۱۱۸

نتایج حاصل از میانگین و انحراف استاندارد شاخص‌های تهدیدهای پایدار پیشرفته

شاخص	تعداد سؤال	میانگین کل	انحراف استاندارد	میانگین خطای استاندارد
پایدار	۱۰	۱,۱۴	۰,۸۴۲	۰,۱۱۹
پیچیده	۱۰	۱,۱۹	۰,۵۷۴	۰,۰۸۲
هدف‌دار	۱۰	۱,۲۳	۰,۴۷۵	۰,۰۴۸
قابل گریز	۱۰	۱,۲۱	۰,۲۳۵	۰,۰۴۷

جداول تحلیلی فوق نشان‌دهنده‌ی آن است که اعداد "تی" حاصل از آزمون تک متغیره "تی" در مورد شاخص‌ها همگی بالاتر از از اعداد جدول آزمون "تی" است. بنابراین، شاخص‌ها با درجه‌ی اطمینان ۹۵٪ مورد تأیید قرار می‌گیرد. نتایج حاصل از میانگین شاخص‌ها در جدول فوق نشان داده شده است.

نتایج حاصل از ضریب اهمیت راهبردهای پدافند غیرعامل

شاخص	میانگین کل/ ضریب اهمیت(٪)	رتبه
اعمال فرماندهی و کنترل یکپارچه و مقاوم	۱,۵۷	۱
شناسایی کارکنان و سامانه‌های حاوی اطلاعات	۱,۴۱	۲
ذی‌قیمت حفظ اطلاعات	۱,۳۵	۳
کشف، مهار و خنثی‌سازی آلودگی	۱,۲۷	۴

نتایج حاصل از ضریب اهمیت شاخص‌های تهدیدهای پایدار پیشرفته

شاخص	میانگین کل/ضریب اهمیت(٪)	رتبه
پایدار	۱,۴۱	۱
پیچیده	۱,۳۱	۲
هدف‌دار	۱,۲۷	۳
قابل گریز	۱,۲۱	۴

نتایج و یافته‌ها

امروزه بخش زیادی از بودجه‌های امنیت فناوری اطلاعات در سازمان‌ها صرف محصولات ضدبدفزاز، فایروال‌ها و "IDS/IPS" می‌شود، اما مهاجمان با عبور از این موانع هم‌چنان به سازمان‌ها حمله می‌کنند. اقدامات امنیتی سنتی جوابگوی تهدیدهای امروزی نیست. بسیاری از حملات با استفاده از تکنیک‌های تهدیدهای پایدار پیشرفته بدون وجود وضعیت امنیتی جدید در قربانی‌کردن اهداف خود موفق می‌شوند.

ایجاد پدافند مناسب در برابر تکنیک‌های تهدیدهای پایدار پیشرفته نیاز به نظارت در ترافیک داخلی و خارجی در خصوص محتوای تهدید، مجموعه علائم تهدید و موقعیت زمانی دارد. لایه‌های دفاعی باید بر ارتباطات برای کشف رفتارهای مشکوک نظارت کنند.

شبکه‌های مجهز به فایروال، "IDS/IPS" و ضدبدافزار بر محافظت در برابر تهدید داخلی با استفاده از تحلیل‌های دفاعی تمرکز دارند و ارتباطات خارجی را نادیده می‌گیرند. وجود

پدافندهای سنتی مانند فایروال‌ها و ضدبدافزارها ضروری است، زیرا بدافزارهای تهدیدآمیز را مسدود می‌کنند، اما این موارد کافی نبوده و باید محدودیت‌های آنها در برابر تکنیک‌های تهدیدهای پایدار پیشرفته و حملات هدف‌دار شناسایی شود.

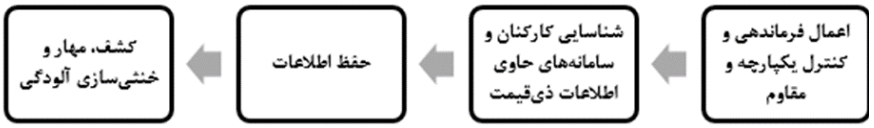
درگاه‌های امن شبکه، یک‌لایه‌ی دفاعی دیگری را با وجود اسکن ضدبدافزار و فیلترینگ "URL" از جمله توانایی تحلیل ترافیک "SSL" اضافه می‌کند. برای محافظت از سازمان در محیط خصمانه توصیه می‌شود از یک راه‌حل دفاعی چندلایه برای محافظت داخلی و ممانعت از سرقت اطلاعات از خارج از سازمان استفاده شود.

در گام نخست باید از درگاه امن پست‌الکترونیکی استفاده کرد که توانایی بازرسی شبکه را در خصوص شبکه‌های بدافزاری برای جلوگیری از آلوده‌سازی اولیه دارد. دوم آن‌که باید درگاه امن شبکه‌ای را انتخاب کرد که از توانایی بیش از فیلترینگ "URL" و ضدبدافزاری سنتی برخوردار است. راهبرد مؤثر استفاده از تحلیل تهدیدها در زمان حقیقی به‌منظور شناسایی بدافزارهای بدون سابقه‌ی قبلی و غیربااینری مانند جاوا اسکریپتس است. سوم آن‌که راهبرد باید از توانایی کشف بدافزارهای سارق اطلاعات در فرآیند برخوردار باشد. راهبرد اتخاذی باید از توانایی‌های "DLP" استفاده کند تا سازمان متوجه زمان خروج اطلاعات شود.

به‌طور خلاصه توصیه می‌شود: از راهبرد یکپارچه که توانایی تحلیل محتوای تهدید، مجموعه علائم تهدید و موقعیت زمانی ترافیک اطلاعات را در خصوص ترافیک ورودی و خروجی اطلاعات در امتداد ورودی‌های پست‌الکترونیکی دارد، استفاده شود.

راهبردهای پدافند غیرعامل در برابر تهدیدهای پایدار پیشرفته در محیط سایبری به قرار زیر خلاصه می‌شود:

- اعمال فرماندهی و کنترل یکپارچه و مقاوم؛
- شناسایی کارکنان و سامانه‌های حاوی اطلاعات ذی‌قیمت؛
- حفظ اطلاعات؛
- کشف، مهار و خنثی‌سازی آلودگی.



نمودار شماره‌ی ۱ - راهبردهای پدافند غیرعامل در برابر تهدیدهای پایدار پیشرفته در محیط سایبری

پیش از طراحی یک سامانه‌ی کنترل امنیتی برای دفاع در برابر تهدیدهای پایدار پیشرفته نیاز به شناسایی اطلاعات حساس و محل قرارگیری آنهاست. سامانه‌های حس‌گر سرقت اطلاعات با اسکن شبکه می‌توانند اطلاعات حساس را شناسایی و طبقه‌بندی کنند. به محض شناسایی مکان اطلاعات حساس امکان کاهش مخاطرات به چند شیوه وجود دارد:

- حذف اطلاعات از مکان‌های ناامن و غیرضروری؛
- حصول اطمینان از وجود سامانه‌های محافظت در برابر دسترسی‌های غیرمجاز در مناطق وجود اطلاعات مهم؛
- نظارت و ممانعت از سرقت اطلاعات در درگاه‌های پست‌الکترونیک و شبکه؛

مهاجمان همان‌طور که پیش از بیان شد، کارکنان با اطلاعات ذی‌قیمت و متخصصان فناوری اطلاعات را که دارای مجوز دسترسی به اطلاعات هستند، با استفاده از شیوه‌های مختلف از جمله مهندسی اجتماعی موردهدف قرار می‌دهند.

یکی از اقدامات متداول مهاجمان استفاده‌ی ترکیبی از روش‌های شبکه‌ای و پست‌الکترونیک است. بیش‌تر این اقدامات ترکیبی با ارسال نامه‌ی الکترونیکی به شخص هدف آغاز می‌شود. در بیش‌تر مواقع این نامه دارای ظاهری فریبنده است، به‌گونه‌ای که فرستنده‌ی آن را یک شخص مطمئن نشان می‌دهد.

برای مقابله با این اقدامات باید بررسی‌های اولیه در خصوص هویت و بررسی آنتی‌اسپم مکان نامه‌ی ارسالی صورت گیرد. سپس تحلیل ضدبدافزار در خصوص پیوست با استفاده از موتورهای ضدبدافزار چندگانه انجام شود.

سرانجام طبقه‌بندی امنیتی باید در زمان حقیقی با تحلیل محتوای تهدید و علائم آن و بر اساس ترافیک زمانی اطلاعات صورت گیرد.

پاسخ به سؤالات اصلی و فرعی تحقیق

سؤال اصلی: راهبردهای پدافند غیرعامل در برابر تهدیدهای پایدار پیشرفته در محیط سایبری چیست؟

راهبردهای پدافند غیرعامل در برابر تهدیدهای پایدار پیشرفته با توجه به نتایج حاصل از جداول عبارتند از:

نتایج حاصل از ضریب اهمیت شاخص‌های تهدیدهای پایدار پیشرفته

شاخص	تأثیر کم	خیلی مؤثر
اعمال فرماندهی و کنترل یکپارچه و مقاوم	۱۰	۹۰
شناسایی کارکنان و سامانه‌های حاوی اطلاعات	۲۲	۷۸
ذی‌قیمت حفظ اطلاعات	۳۱	۶۹
کشف، مهار و خنثی‌سازی آلودگی	۳۵	۶۵
کل	۲۴,۵	۷۵,۵

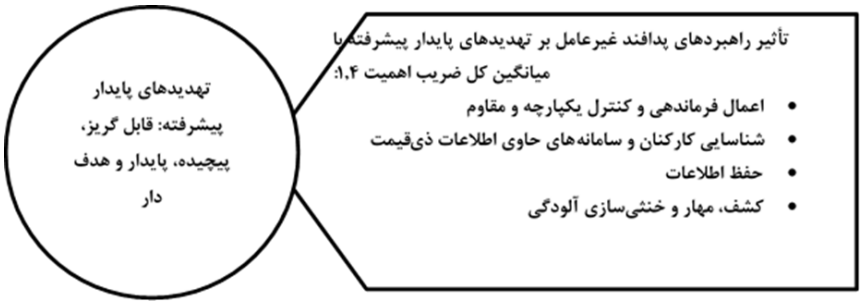
شاخص‌های فوق نشان می‌دهد که راهبردهای پدافند غیرعامل شامل موارد فوق به‌عنوان متغیر مستقل بر شاخص‌های تهدیدهای پایدار پیشرفته تأثیرگذار است. علاوه بر این، به موجب نتایج حاصل از تحقیق راهبردهای پدافند غیرعامل در برابر تهدیدهای پایدار پیشرفته در محیط سایبری با ۷۵,۵ درصد تأثیر بسیاری بر کاهش تهدیدهای پایدار پیشرفته داشته است.

سؤال فرعی: شاخص‌های تهدیدهای پایدار پیشرفته کدام است؟

با توجه به نتایج حاصل از جداول شاخص‌های تهدیدهای پایدار پیشرفته عبارتند از:

نتایج حاصل از ضریب اهمیت شاخص‌های تهدیدهای پایدار پیشرفته

شاخص	میانگین کل/ ضریب اهمیت (٪)	رتبه
پایدار	۱,۴۱	۱
پیچیده	۱,۳۱	۲
هدف دار	۱,۲۷	۳
قابل گریز	۱,۲۱	۴
میانگین کل	۱,۳	



نتیجه‌گیری

بر اساس نتایج تحقیق ۷۵,۵ درصد از پاسخ‌دهندگان تأثیر خیلی‌زیاد را برای شاخص‌های تهدیدهای پایدار پیشرفته قائلند و تنها ۲۴,۵ درصد از آنها تأثیر این شاخص‌ها را کم می‌دانند. میانگین کل ضریب اهمیت شاخص‌های تهدیدهای پایدار پیشرفته ۱,۳ است. رتبه‌بندی شاخص‌های تهدیدهای پایدار پیشرفته به ترتیب عبارت است از: پایدار، پیچیده، هدف‌دار، قابل گریز. راهبردهای مؤثر در برابر تهدیدهای پایدار پیشرفته با شاخص‌های مربوطه نیز عبارتند از: اعمال فرماندهی و کنترل یکپارچه و مقاوم، شناسایی کارکنان و سامانه‌های حاوی اطلاعات ذی‌قیمت، حفظ اطلاعات و کشف، مهار و خنثی‌سازی آلودگی.

منابع

انگلیسی

1- Chandrashekar ,C.P.(2008) ,"In Search of Causes", Frontline, Vol. 2, 25th October-7th November 2008, P.11.

2- Chaturvedi M.M.,Gupta M.P., Bhattacharya J.(2007),"Analysis of Information and Communication, P.43.

3- Complexity and Organizational Surprises", in M. Dunn and V. Mayer (eds),(2011), International CIIP Handbook Cyber security, P21.

4- DHS(2008),Department of Homeland Security website, www.dhs.gov/nipp, Retrieved October 7, 2008, P.33.

5- DOT(2008), Retrieved August, 2008 from http://www.dot.gov.in

6- Dunn Myriam(2005), "A Comparative Analysis of Cyber security Initiatives Worldwide", Center for Security, P.11

7- E- government (2009) India: Gift Publishing, P.32

8- Eeten, M.J.G. van, Roe, E.M., Schulman, P , Bruijne, M.L.C. de,(2006), "The Enemy Within: System, P.2

9- ITU (2007), Retrieved September 22, 2007 from http://www.itu.int/ITU-D/cyb/events/2007/hanoi

10- ITU/WSIS(2002), World Summit on the Information Society,www.itu.int/wsis/INDEX.HTML

11- Technology Infrastructure vulnerabilities in Indian context" In J. Bhattacharya(Ed),Towards next generation

12- Zurich,(2009)at<www.crn.ethz.ch/publications/crn_team/detail.cfm?id=16157>, Retrieved October 7.P.89

13- Alperovitch, D. (2011) "Revealed: Operation Shady RAT" McAfee Corporation Santa Clara, CA. P.12

14- CCRA (2009) Common Criteria for Information Technology Security Evaluation, Common Criteria Recognition Agreement (CCRA), CCMB-2009-07-001, P.23

15- Drew, D.M.Snow (2012), making twenty-first century strategy: an introduction to modern national security process and problems, air university press, p.21

16- EU (2013), memo/10/463: Proposal for a Directed on attacks against information systems, repealing Framework Decision 2005/222/JHS, European Union (EU), Brussels, p.15

17- IETF (Ed.)(2014), rfc 2196: Site Security Handbook, Internet Engineering Task Force (IETF). P.51

18- Lipinski, D ,.et al .(2015)" H.R. 4061: Cybersecurity Enhancement Act of 2010". in 111th Congress 2009-2010, Washington, DC, United States House of Representatives.