تاریخ دریافت:۹۵/۱۱/۹
تاریخ پذیرش نهایی:۹۶/۲/۳

فصلنامه دانش امنیتی
سال اول/شماره یکم/ بهار ۱۳۹۶

راهبردهای پدافند غیرعامل در برابر تهدیدهای پایدار پیشرفته در محیط سایبری

سعید کافی[۱]

چکیده

امروزه تهدیدهای پایدار پیشرفته یکی از دغدغه‌های مهم جوامع بشری است. با گسترش فناوری اطلاعات و سرعت شتابان آن در وابستگی ابعاد مختلف جامعه به خود، زمینه‌های تهدیدهای جدیدی نیز در این حوزه شکل گرفته است. تهدید پایدار پیشرفته سازمان‌های خاصی را به منظور سرقت اطلاعات یا وارد آوردن خسارت به اموال و دارایی‌ها هدف قرار می‌دهد. بنابراین هر سازمانی که اطلاعات ارزشمندی دارد، در برابر تکنیک‌های تهدید پایدار پیشرفته آسیب‌پذیر است. از طرف دیگر، هر چه اطلاعات سازمان از ارزش بیشتری برخوردار باشد، احتمال مورد تهدید قرار گرفتن سازمان بیشتر است. در این تحقیق با استفاده از روش تحقیق توصیفی- تحلیلی- پیمایشی راهبردهای پدافند غیرعامل در برابر تهدیدهای پایدار پیشرفته در محیط سایبری ارائه شده است.

واژگان کلیدی

راهبردهای پدافند غیرعامل، تهدیدهای پایدار پیشرفته، فضای سایبری

۱ . استادیار دانشگاه امام حسین (ع)

مقدمه

تهدیدهای پایدار پیشرفته[1] نگرانی بزرگ جامعه فناوری اطلاعات در عصر حاضر به شمار می‌آید. حملات اخیر به دولت‌های کانادا و فرانسه و اتحادیه 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؟ مقاله حاضر ماهیت تهدیدهای پایدار پیشرفته را توصیف می‌کند و راهبردهایی درباره محافظت سازمان‌ها در برابر این تهدید ارائه می‌دهد.

اکثر پژوهشگران حوزه امنیتی بر این باورند که نخستین بار واژه «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) به کار برده است.

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

اینکه واژه تهدید پایدار پیشرفته برای اشاره به فعالیت مجرمان سایبری با هدف سرقت اطلاعات سازمان‌ها به کار می‌رود یا خیر موضوع معناشناسی است؛ اما آنچه برای کارشناسان امنیتی اهمیت دارد اطلاع از این واقعیت است که مجرمان سایبری از همان تکنیک‌های تهدید پایدار پیشرفته استفاده می‌کنند که کشورها برای بهره‌برداری راهبردی به کار می‌گیرند و هدف آنها از استفاده نیز سرقت اطلاعات از سازمان‌هاست. بنابراین، سازمان‌های دولتی و خصوصی نیازمند شناخت این تهدید و تکنیک‌های آن به منظور محافظت از خود در برابر آن هستند. بدین منظور خصوصیات تهدید پایدار پیشرفته، فرایند آن و سیکل زمانی فعالیت بدافزار بر اساس شیوه‌های جدید به کارگیری بررسی می‌شود. راهبردها و تاکتیک‌های پیشنهادی برای مقابله با این تهدید نیز بر اساس شیوه عملکرد آن ارائه می‌شود.

1 . Advanced Persistent Threats (APT)

۱. بیان مسئله

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 جبران‌ناپذیری برای تداوم فعالیت جوامع بشری به دنبال خواهد داشت. بنابراین، در صورت فقدان راهبرد مشخص برای مقابله با این تهدیدها، خسارات سنگینی وارد خواهد شد تا جایی که امکان جبران آن به راحتی میسر نیست. این تحقیق به ارائه راهبردهای پدافند غیرعامل در برابر تهدیدهای پایدار پیشرفته می‌پردازد.

۲ . ضرورت و اهمیت تحقیق

با توجه به وابستگی 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 زیادی برخوردار است.

۳. 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.

۴. 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؟

۵. نوع و روش تحقیق

تحقیق حاضر از نوع کاربردی است و به روش توصیفی- تحلیلی ـ پیمایشی انجام گرفته است. این روش تحقیق برای توصیف عینی و کیفی محتوای مفاهیم مبتنی بر یک روش نظام‌مند به کار می‌رود. در واقع، قلمرو این روشِ تحقیق را اسناد مکتوب،

شفاهی و تصویری نظیر کتاب‌ها، مقاله‌ها، روزنامه‌ها، مجله‌ها، مطالب نوار و فیلم، سخنرانی‌ها و... درباره موضوعی خاص تشکیل می‌دهد. برلسون روش تحلیلی را ابزاری برای توصیف عینی، سیستماتیک و کمّی محتوای مطالب تعریف کرده است (Chandrashekar, 2008: 11).

۶. روش و ابزار گردآوری اطلاعات

در تحقیق حاضر برای تدوین ادبیات و چارچوب نظری از مطالعه اسنادی و کتابخانه تخصصی و نیز مصاحبه استفاده شده است.

ادبیات تحقیق

۱. تهدیدها، مفاهیم و کارکردها

هدف از تهدیدها تأثیرگذاری بر اراده، اعتقادات، افکار و احساسات مخاطبین به منظور انهدام یا تسلیم کردن جامعه هدف است. وجه اشتراک تمام تهدیدها، تحمیل اراده به دشمن است؛ همان‌طور که هدف از جنگ نیز همین است. بشر همواره در معرض تهدید قرار داشته است. برخی تهدیدها طبیعی (مانند زلزله، سیل و 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 یا مجموعه‌ای از کشورها علیه افراد یا گروه‌ها یا کشور یا کشورهای دیگر است. از طرفی، تهدید همیشه در مقابل امنیت طرح می‌شود و مبتنی بر تصورات ذهنی است. «تهدید» ادراکی ذهنی و نقطه 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 ارائه تعریف از مفهوم تهدید، با توجه به درونمایه بحث تهدیدها و ذهنی بودن آن، نمی‌توان از یک نقطه ساکن برای توضیح درباره 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 علایق و مقاصد امنیت ملی یا مداخله به نحوی که نیل به علایق 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 (Lipinski, 2015: 21). به بیان دیگر، وضعیت فوری محرک که نتیجه‌اش تهدید است، تنها خبر از آسیبی می‌دهد که در قبال منافع و ارزش‌ها در راه است. ظهور علایم نگران‌کننده براساس دگرگونی در محیط، موضع‌گیری، رخدادهای سیاسی- امنیتی و پاره‌ای از عوامل دیگر واقعیات جدیدی را شکل می‌دهد که به منزله «پیدایش وضعیت» جدید است. ادراک تهدید متأثر از ظهور واقعیات جدید است که در تعامل با ادراک ذهنی مفهوم تهدید و کنش و واکنش‌ها را تشکیل می‌دهد.

در ادبیات سیاسی کنونی تهدیدها را به سه نوع تقسیم کرده‌اند: تهدیدهای سخت (جنگ نظامی)، تهدیدهای نیمه سخت (اقدامات اطلاعاتی و امنیتی) و تهدیدهای نرم (اقدامات فرهنگی، سیاسی، اجتماعی، اقتصادی، رسانه‌ای، سایبری و...). عرصه تهدیدهای نرم ممکن است متنوع و وسیع باشد، اما برای جلوگیری از بسط مطلب سعی شده است در دسته‌بندی محدودتری ارائه شود. با این توضیح، عرصه‌های تهدیدهای نرم را می‌توان به شش دسته تقسیم کرد:

۱. حوزه تهدیدهای سیاسی؛
۲. حوزه تهدیدهای اقتصادی؛
۳. حوزه تهدیدهای فرهنگی؛
۴. حوزه تهدیدهای اجتماعی؛
۵. حوزه تهدیدهای فناوری اطلاعات و ارتباطات اجتماعی؛
۶. حوزه تهدیدهای علمی و اندیشه‌ای.

پرداختن به تمام انواع تهدیدها خارج از موضوع و حوصله تحقیق حاضر است؛ بنابراین، تنها به تهدیدهای فناوری اطلاعات و ارتباطات اجتماعی پرداخته می‌شود که فضای به وجود آمده از تهدیدهای ارتباطی مربوط به پدیده عصر حاضر یعنی عصر ارتباطات یا اطلاعات و همچنین عصر انفجار اطلاعات است. در محیط این تهدید، مخاطب با هزاران طول موج رادیویی، امواج دیجیتالی، فیبر نوری، سیگنال‌های مختلف،

فناوری‌ها، جامعه 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،[1] لیزری، خواب رادیویی،[2] امواج کوتاه الکتریکی تنش‌ساز[3] و فناوری‌های نوین در عملیات روانی مانند هواپیماهای بدون سرنشین کومندو سولو[4] و... مواجه است (Zurich, 2009: 88).

۲. خصوصیات تهدید پایدار پیشرفته

تهدید پایدار پیشرفته سازمان‌های خاصی را به منظور سرقت اطلاعات خاص یا وارد آوردن خسارت به اموال و دارایی‌ها هدف قرار می‌دهد. این شیوه عملکرد مقابل اکثر نرم‌افزارهای با محتوای مخرب که در هر سامانه آلوده به صورت تصادفی عمل می‌کنند، قرار می‌گیرد. حملاتی که در سال‌های اخیر به برخی سازمان‌ها در دنیا انجام گرفت، حملات فرصت‌طلبانه با هدف قربانی کردن هر سازمانی در هر سطح ممکن نبوده است، بلکه این حملات با سرمایه‌گذاری مالی و زمانی به منظور بهره‌برداری از اهداف مشخص انجام گرفته است. دو نتیجه از این شرایط می‌توان گرفت: نخست آنکه هر سازمانی که دارای اطلاعات ارزشمند است، در برابر تکنیک‌های تهدید پایدار پیشرفته آسیب‌پذیر است. دوم آنکه هر چه اطلاعات سازمان از ارزش بیشتری برخوردار باشد، احتمال مورد تهدید قرار گرفتن سازمان نیز بیشتر است. اقتصاد جرایم سایبری با استخدام هکرهای حرفه‌ای به خوبی سازمان یافته و دایر شده است (Zurich, 2009: 23).

۳. پایداری

تهدید پایدار پیشرفته در مراحل مختلف در طول زمان شکل می‌گیرد. مهاجم پیش از حمله واقعی تنها اطلاعاتی از سازمان مورد هدف و اهداف خود دارد. آنها نمی‌دانند داده‌های ارزشمند سازمان مورد هدف کجا قرار دارد، چه کنترل‌های امنیتی وجود دارد یا چه آسیب‌هایی در سازمان برای بهره‌برداری در دسترس است. مهاجم برای سرقت اطلاعات آسیب‌پذیری‌ها را شناسایی و کنترل‌های امنیتی موجود را ارزیابی می‌کند، به

1 . Psychotropic
2 . Radiosleep Radioson
3 . Pulsed Microwaves
4 . Commando Solo

میزبان‌ها در محدوده شبکه هدف دسترسی می‌یابد، اطلاعات هدف را پیدا و سرانجام اطلاعات را از شبکه استخراج می‌کند. کل این فرایند ماه‌ها یا حتی سال‌ها طول می‌کشد؛ بنابراین، کشف این تهدید تنها با تکیه بر مشاهده هر اتفاقی ممکن نیست، بلکه باید به دنبال مجموعه رویدادهایی بود که ویژگی متدولوژی‌های تهدیدهای پایدار پیشرفته است (Eeten, 2006: 2).

تهدیدهای پایدار پیشرفته به طور سیستماتیک با هدف فرار از دام محصولات امنیتی سنتی که اکثر سازمان‌ها سال‌ها به آنها تکیه می‌کنند، طراحی شده است. برای مثال، به موارد زیر اشاره می‌شود:

مهاجم برای دستیابی به میزبان‌های درون شبکه هدف، ضمن پرهیز از فایروال‌های شبکه، تهدیدهایی را درون محتوای پروتکل‌های معمول (http, https, smtp , etc) ارائه می‌دهد. مهاجم برای نصب بدافزارها در شبکه میزبان ضمن پرهیز از برنامه‌های ضد ویروس، کدهایی را برای محیط هدف معین می‌نویسد. این کدها پیش از به کارگیری در جایی مشاهده نشده‌اند و به همین دلیل هیچ برنامه ضد ویروسی برای محافظت در برابر آن وجود ندارد. مهاجم برای ارسال اطلاعات به خارج از شبکه هدف ضمن پرهیز از فایروال‌ها از رمزگذاری متداول استفاده و محتوا را از طریق پروتکل‌های مجاز از نظر فایروال‌ها خارج می‌کند (Dunn, 2005: 11).

۴. پیچیدگی تهدیدهای پایدار پیشرفته

تهدیدهای پایدار پیشرفته ترکیبی پیچیده از روش‌های حمله را با هدف‌گیری آسیب‌های چندگانه شناسایی‌شده در سازمان مورد استفاده قرار می‌دهند. یک تهدید پایدار پیشرفته مشخص گام‌های زیر را طی می‌کند (Dunn, 2005: 19):

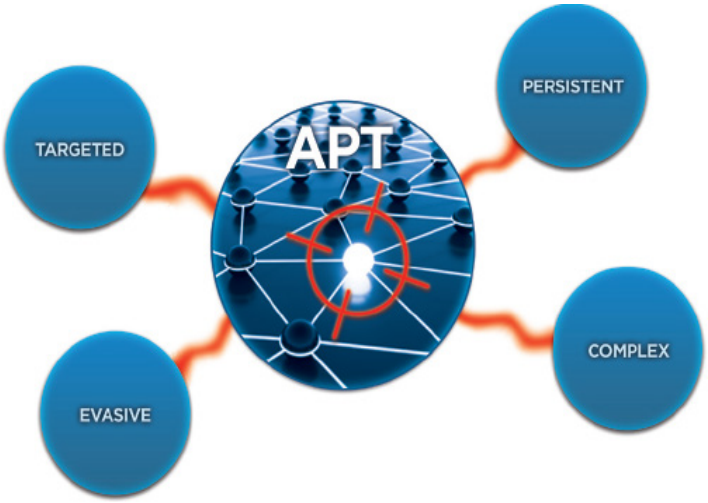
ـ استفاده از مهندسی اجتماعی مبتنی بر شبکه تلفن به منظور شناسایی اشخاص کلیدی درون سازمان؛

ـ شکار نامه‌های الکترونیکی ارسالی به اشخاص کلیدی در سازمان از طریق اتصال به وب‌سایتی که کدهای جاوا اسکریپت را به منظور نصب ابزار دسترسی از راه دور اجرا می‌کند.

ـ استفاده از کدهای فرماندهی و کنترل باینری (کدهای متعارف یا کدهای تولیدی با استفاده از کیت‌های بدافزاری موجود متداول)؛

ـ استفاده از فناوری رمزگذاری متعارف.

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



شکل ۱ــ ویژگی‌های تهدید پایدار پیشرفته

۵. فرایند تهدید پایدار پیشرفته

فرایند تهدید پایدار پیشرفته سه مرحله مهم را دربرمی‌گیرد که در طول چند ماه رخ می‌دهد. در ادامه به توضیح این مراحل می‌پردازیم: (MIT, 2008: 15)

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

روش‌های متداول در این خصوص عبارت است از: (DOT, 2008: 12)

ـ نامه‌های الکترونیکی جذاب با لینک‌هایی که ارتباط با وب‌سایت‌های حامل بدافزارها را فراهم می‌کند.

ـ نامه‌های الکترونیکی با فایل‌های پیوست در فرمت‌های متداول مانند آفیس و پی‌دی‌اف؛ این پیوست‌ها شامل کدهای حمله با استفاده از بدافزارهای ناشناخته‌ای می‌شود که هدف از به کارگیری آنها حمله به آسیب‌هایی است که قبلاً شناخته شده نبودند.

ـ استفاده از وب‌سایت‌های آلوده که افراد هدف به آنها علاقه دارند. این افراد از طریق پروفایل‌های رسانه‌های اجتماعی شناسایی می‌شوند.

ـ مهندسی اجتماعی به منظور کسب اطلاعات درباره توانایی‌های فردی کاربران مورد هدف.

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

مرحله دوم، کنترل، روزآمدسازی، کشف و پایداری: مهاجم در این مرحله میزبان‌های آلوده را کنترل و کد را روزآمد می‌کند، 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. هر چند در مواردی این سرویس در میزبان درون شبکه هدف قرار داشته، اما مواردی نیز مشاهده شده است که سرویس فرماندهی و کنترل را از طریق اینترنت در اختیار قرار گرفته است. سرویس فرماندهی و کنترل به مهاجم این امکان را می‌دهد تا از راه دور بدافزار را به‌روز کند و بدافزارهای جدید را اضافه و فرامینی را به میزبان ارسال کند (EU, 2013: 15).

در این مرحله اجزای اضافی با توانایی کشف اطلاعات هدف در میزبان‌های آلوده پیاده می‌شود. اهداف کلیدی شامل سرورهای PKI و دایرکتوری‌های فعال برای دسترسی به اطلاعات محرمانه می‌شود. نظارت بر اطلاعات مورد استفاده 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 شبکه هدف به دست 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 شبکه ابزارهای استاندارد شبکه مانند Gsecdump، Cain & Abe، SSH، RDP است (E- Government, 2009: 32).

مرحله سوم، حمله ـ استخراج اطلاعات و اقدام به حمله: مهاجم در این مرحله اطلاعات را از شبکه هدف استخراج می‌کند و اقدامات لازم را انجام می‌دهد. (اطلاعات را خارج می‌کند.) مهاجم در این مرحله کنترل یک یا چند میزبان را درون شبکه هدف در دست گرفته است و اقدامات لازم را برای گسترش دسترسی و شناسایی اطلاعات هدف انجام می‌دهد (Alperovitch, 2011: 12).

تنها اقدامی که در این مرحله باقی می‌ماند ارسال اطلاعات به خارج از شبکه است. دریافت‌کننده اطلاعات می‌تواند سرور فرماندهی و کنترل یا سروری باشد که پیش از این به کار گرفته نمی‌شد (Drew, D.M.Snow, 2012: 21).

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

ـ فروش شیوه‌های حمله: در صورتی که قربانی قادر به خنثی‌سازی حمله نباشد، روش‌های حمله به سایر مهاجمان فروخته می‌شود تا از همان شیوه برای حمله به قربانی استفاده شود.

ـ فروش اطلاعات: در صورتی که اطلاعات ذی‌قیمتی به سرقت رفته باشد، مهاجم اطلاعات را به مخاطبین اطلاعات سرقت‌رفته می‌فروشد.

ـ افشای رسانه‌ای: اطلاعات به سرقت‌رفته ممکن است در اختیار رسانه‌ها قرار گیرد تا برای مقاصد سیاسی و وارد آوردن فشار افکار عمومی بر مخاطبین مورد استفاده قرار گیرد.

۶. چرخه عمر به کارگیری بدافزار

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

در این حالت، چرخه عمر تهدیدهای پایدار پیشرفته تا سال‌ها بیش از میزان عمر

اولیه آن ادامه خواهد داشت و صدها قربانی دیگر را علاوه بر قربانی اولیه آن هدف قرار می‌دهد (DHS, 2008: 33).

۷. ضرورت‌های به کارگیری اقدامات پدافند غیرعامل در برابر تهدیدهای پایدار پیشرفته

با تحلیل خصوصیات تهدیدهای پایدار پیشرفته که پیش از این شرح داده شد، می‌توان ضرورت‌های مهم راهبرد امنیتی مؤثر را تشریح کرد.

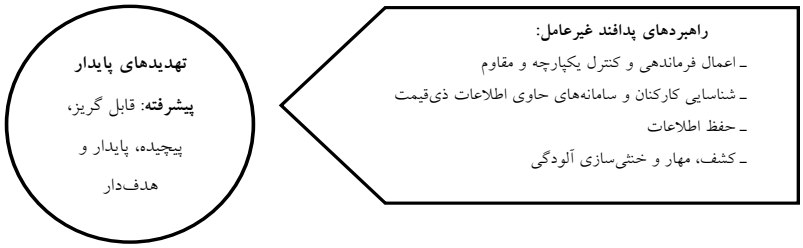
شناخت محتوایی: از آنجا که تهدیدهای پایدار پیشرفته با بهره‌برداری از پروتکل‌های مجاز متداول به پدافند فایروال شبکه نفوذ می‌کند، تدوین راهبردهای تهدیدهای پایدار پیشرفته نیازمند شناخت عمیق از محتوای تهدید است.

شناخت مجموعه علایم تهدید: بیشتر تهدیدهای پایدار پیشرفته از کدهای متعارف و آسیب‌های هدف استفاده می‌کنند، بنابراین با استفاده از یک IPS و ضد بدافزار نمی‌توان تهدید را شناسایی کرد. بدون وجود علایم قابل تعریف حمله باید به مشخصه‌های کمتری تکیه کرد. هر چند یک مشخصه 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: 23) .

شناخت موقعیت زمانی: با اینکه سازمان‌ها ممکن است اطلاع دقیقی از چگونگی تهدیدهای پایدار پیشرفته نداشته باشند، اما بیشتر سازمان‌ها می‌توانند اهمیت موقعیت زمانی سازمان خود را شناسایی کنند. بنابراین، فناوری ممانعت از سرقت اطلاعات به عنوان یک لایه دفاعی برای شناسایی تاریخ‌های مهم و جلوگیری از سرقت اطلاعات قابل ایجاد است. شناسایی کاربرد کدها در ترافیک شبکه در دفاع تهدید پایدار پیشرفته حایز اهمیت است (Chaturvedi, 2007: 43).

مدل مفهومی تحقیق

مدل مفهومی تحقیق روابط بین متغیرها را نشان می‌دهد.



تجزیه و تحلیل داده‌ها و یافته‌های تحقیق

تحلیل توصیفی پاسخ‌دهندگان

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

براساس جدول فوق، از کل پاسخ‌دهندگان بیشترین تعداد یعنی ۷۰ درصد دارای مدرک کارشناسی و کارشناسی ارشد و کمترین تعداد معادل ۳۰ درصد دارای مدرک دکتری تخصصی هستند.

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

نتایج حاصل از میانگین و انحراف استاندارد راهبردهای پدافند غیرعامل

شاخص	تعداد سؤال	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
هدف دار	۱۰	۱,۲۳	۰,۴۷۵	۰,۰۴۸
قابل گریز	۱۰	۱,۲۱	۰,۲۳۵	۰,۰۴۷

جدول‌های تحلیلی فوق نشان می‌دهد که اعداد «تی» حاصل از آزمون تک‌متغیره تی درباره شاخص‌ها همگی بالاتر از از اعداد جدول آزمون تی است؛ بنابراین، شاخص‌ها با درجه اطمینان ۹۵ درصد 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 (به درصد)	رتبه
اعمال فرماندهی و کنترل یکپارچه و مقاوم	۱,۵۷	۱
شناسایی کارکنان و سامانه‌های حاوی اطلاعات ذی‌قیمت	۱,۴۱	۲
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 (به درصد)	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 ضد بدفزاز، فایروال‌ها و IDS/IPS می‌شود؛ اما مهاجمین 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 قربانی کردن 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 علایم تهدید و موقعیت زمانی دارد. لایه‌های دفاعی باید بر ارتباطات برای کشف رفتارهای مشکوک نظارت کنند.

شبکه‌های مجهز به فایروال، IDS/IPS و ضد بدافزار 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 ضد بدافزارها ضروری است، زیرا بدافزارهای تهدیدآمیز را مسدود می‌کنند. اما این موارد کافی نیست و باید محدودیت‌های آنها در برابر تکنیک‌های تهدیدهای پایدار پیشرفته و حملات هدف‌دار شناسایی شود.

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

در گام نخست باید از درگاه امن پست الکترونیکی 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

ضد بدافزاری سنتی برخوردار است. راهبرد مؤثر استفاده از تحلیل تهدیدها در زمان حقیقی به منظور شناسایی بدافزارهای بدون سابقه قبلی و غیربایتری مانند جاوا اسکریپتس است. سوم آنکه راهبرد باید از توانایی کشف بدافزارهای سارق اطلاعات در فرایند برخوردار باشد. راهبرد اتخاذی باید از توانایی‌های DLP استفاده کند تا سازمان متوجه زمان خروج اطلاعات شود.

به طور خلاصه توصیه می‌شود از راهبرد یکپارچه که توانایی تحلیل محتوای تهدید، مجموعه علایم تهدید و موقعیت زمانی ترافیک اطلاعات را در خصوص ترافیک ورودی و خروجی اطلاعات در امتداد ورودی‌های پست الکترونیکی 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 ۱ـ راهبردهای پدافند غیرعامل در برابر تهدیدهای پایدار پیشرفته در محیط سایبری

پیش از طراحی یک سامانه 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 طبقه بندی 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 پست الکترونیک و شبکه.

مهاجمان همان‌طور که پیش از این بیان شد، کارکنان با اطلاعات ذی‌قیمت

و متخصصین فناوری اطلاعات را که دارای مجوز دسترسی به اطلاعات هستند، با استفاده از شیوه‌های مختلف از جمله مهندسی اجتماعی هدف قرار می‌دهند.

یکی از اقدامات متداول مهاجمان استفاده ترکیبی از روش‌های شبکه‌ای و پست الکترونیک است. اکثر این اقدامات ترکیبی با ارسال نامه الکترونیکی به شخص هدف آغاز می‌شود. در اکثر مواقع این نامه دارای ظاهری فریبنده است به گونه‌ای که فرستنده آن را یک شخص مطمئن نشان می‌دهد.

برای مقابله با این اقدامات باید بررسی‌های اولیه در خصوص هویت و بررسی آنتی‌اسپم مکان نامه ارسالی صورت گیرد؛ سپس تحلیل ضد بدافزار در خصوص پیوست با استفاده از موتورهای ضد بدافزار چندگانه انجام شود. سرانجام طبقه‌بندی امنیتی باید در زمان حقیقی با تحلیل محتوای تهدید و علایم آن و بر اساس ترافیک زمانی اطلاعات صورت گیرد.

پاسخ به سؤال‌های 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 جدول‌ها عبارت‌اند 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 ذی‌قیمت	۲۲	۷۸
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 به عنوان 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

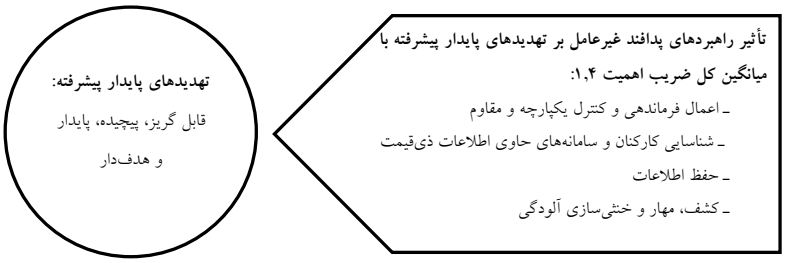
تهدیدهای پایدار پیشرفته داشته است.

سؤال فرعی: شاخص‌های تهدیدهای پایدار پیشرفته کدام است؟

با توجه به نتایج حاصل از جدول‌های شاخص‌های تهدیدهای پایدار پیشرفته عبارت‌اند از:

نتایج حاصل از ضریب اهمیت شاخص‌های تهدیدهای پایدار پیشرفته

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



نمودار ۲ـ مدل عملیاتی راهبردهای پدافند غیرعامل در برابر تهدیدهای پایدار پیشرفته در محیط سایبری

نتیجه‌گیری

براساس نتایج تحقیق، ۷۵,۵ درصد از پاسخ‌دهندگان تأثیر خیلی زیاد را برای شاخص‌های تهدیدهای پایدار پیشرفته قائل‌اند 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 و قابل گریز. راهبردهای مؤثر در برابر تهدیدهای پایدار پیشرفته با شاخص‌های مربوط نیز عبارت‌اند از: اعمال فرماندهی و کنترل یکپارچه و مقاوم، شناسایی کارکنان و سامانه‌های حاوی اطلاعات ذی‌قیمت، حفظ اطلاعات و کشف، مهار و خنثی‌سازی آلودگی.

منابع لاتین

- Alperovitch, D. (2011), “Revealed: Operation Shady RAT”, McAfee Corporation Santa Clara, CA.

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

- Chandrashekar ,C.P.(2008), “In Search of Causes”, ***Frontline***, Vol. 2, 25th October-7th November.

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

- Complexity and Organizational Surprises”, in M. Dunn and V. Mayer (eds),(2011), International CIIP Handbook Cyber Security.

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

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

- Drew, D.M. Snow (2012), ***Making Twenty-first Century Strategy: An Iintroduction to Modern National Security Process and Problems***, Air University Press.

- Dunn, Myriam (2005), “A Comparative Analysis of Cyber Security Initiatives Worldwide”, ***Center for Security***.

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

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

- EU (2013), memo/10/463: Proposal for a Directed on Attacks against Information Systems, Repealing Framework Decision 2005/222/JHS, European Union (EU), Brussels.

- IETF (Ed.)(2014), rfc 2196: Site Security Handbook, Internet Engineering Task Force (IETF). Lipinski, D ,.et al .(2015),» H.R. 4061: Cybersecurity Enhancement Act of 2010”, in111 th Congress 2009-2010, Washington, DC, United States House of Representatives.

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

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

- Technology Infrastructure Vulnerabilities in Indian Context”, In J. Bhattacharya (Ed),***Towards Next Generation***.

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