بررسی روش‌های سنتی و مدرن تنازعات سایبری

علی مقدسی[۱]، علی محمدی[۲]

[۱] دانشجوی دکتری، دانشگاه جامع امام حسین(ع)

تهران، ایران

ali_moghaddasi@ihu.ac.ir

[۲] دانشکده و پژوهشکده مهندسی فاوا- دانشگاه جامع امام حسین (ع)

تهران، ایران

mohammadi@ihu.ac.ir

چکیده

این مقاله سعی دارد روشهای تنازعات و حملات سایبری در شبکه اینترنت را با دو دیدگاه سنتی و مدرن مورد بررسی قرار دهد و تفاوتهای آنها را مشخص کرده روشهایی نیز برای مقابله با آنها معرفی نماید. ابتدا اشاره‌ای به روند توسعه اینترنت صورت گرفته است و سپس روشهای حملات سایبری سنتی مرور گردیده است و پس از آن وارد بحث روشهای مدرن حملات سایبری شده و هر کدام را مورد بررسی قرار داده است. در ادامه روشهای شناخته شده را برای مقابله با حملات ذکر شده بیان نموده و پیشنهادهایی نیز ارایه گردیده است.

کلمات کلیدی:

ویروس، سرور، کلاینت، منع سرویس، نفوذ، شبکه اجتماعی، سیستم فرماندهی و کنترل

۱- مقدمه

از زمانی که شبکه‌ای از کامپیوترهای محلی توسط آژانس پروژه‌های تحقیقاتی پیشرفته دفاعی در اواسط دهه ۸۰ برقرار و به عنوان اولین عضو شبکه جهانی معرفی گردید رشد شبکه جهانی اینترنت به سرعت ادامه داشته و یکی از اصلی‌ترین عناصر عصر کنونی در بعد ارتباطات را ایجاد کرده است. به موازات رشد و گسترش بستر شبکه و فراهم نمودن امکانات و قابلیت‌های ارتباطی بسیار زیادی که اینترنت در ابعاد متعدد اقتصادی، علمی، رفاهی، اجتماعی، فرهنگی، تفریحی و ... به ارمغان آورده است اما نگرانی‌ها و خطراتی نیز در آن بوجود آمده و از زوایای مختلف فوق باعث ایجاد نا امنی‌هایی در همه ابعاد شده و امنیت جوامع را در ابعاد مختلف فرهنگی، اجتماعی، اقتصادی، اطلاعاتی، سیاسی و نظامی دچار چالش نموده است. نقطه اوج این خطرات در جایی بروز می‌کند که نزاع‌ها و اختلاف‌هایی در سطح دولتی یا بین‌المللی رخ می‌دهد. در این مقاله سعی بر آن است که این تنازعات در دو وضعیت سنتی و مدرن آن مورد تحقیق قرار گرفته و عوامل و شرایط آن بررسی گردد.

از آنجا که در ابتدای پیدایش اینترنت هنوز پروتکل‌های ارتباطی پیشرفت چندانی نداشته و بخصوص پروتکل وب توسعه نیافته بود بنابراین استفاده از اینترنت کمتر گسترش یافته و به شبکه‌هایی همچون UseNet و شبکه‌های خبری محدود بود. در چنین شبکه‌هایی تهدیدات موجود در شبکه تنها در غالب ویروسها و کرم‌های اینترنتی نمود و بروز داشتند و دو هدف عمده را تعقیب می‌کردند که شامل ۱) جمع‌آوری اطلاعات و ۲) تخریب اطلاعات بود. نمونه‌هایی از اینگونه حملات در ادامه یادآوری خواهند گردید.

با گسترش روز افزون و عمومی شدن استفاده از اینترنت بخصوص پس از پیدایش پروتکل جهانی وب، استفاده از این شبکه شکل جدیدتری به خود گرفت و به موازات آن مباحث امنیتی جدیدتری نیز در ابعاد بزرگتر از آنچه قبلا بود مطرح گردید. در ادامه روشهای حملات سایبری سنتی اشاره و مرور شده است و در قسمتهای بعدی مقاله به اهم روشهای جدید که در حملات سایبری مدرن مورد استفاده قرار می‌گیرند پرداخته شده است.

۲- متدولوژی بررسی

به منظور اینکه بررسی روشهای مورد نظر در دو بعد سنتی و مدرن منسجم‌تر صورت گیرد باید موضوعاتی که مبنای بررسی هستند مشخص شود. بر این اساس بررسی‌های خود را حول موضوعات زیر در نظر خواهیم گرفت:

معماری: نکاتی که در معماری سیستمها قابل ذکر هستند

بستر: پیشرفتهایی که در بستر شبکه ایجاد گردیده است

تکنولوژی: فناوریهای بکار رفته در هریک از ابعاد بحث

ابزار: وسایل و ابزاری که در طول دوره تبدیل استفاده گردیده است

تکنیک : روشهای تکنیکی مورد استفاده در هر کدام از دوره‌ها

۳- روشهای سایبری سنتی

در ابتدای پیدایش شبکه‌های کامپیوتری تنها چیزی که ذهن دانشمندان را به خود مشغول کرده بود امکان ایجاد بستری برای تبادل اطلاعات در شبکه به منظور اشتراک نظرات و مستندات و منابع بود و موضوعاتی که به امنیت داده‌ها مربوط می‌شد به ندرت مد نظر قرار داشت. حتی در طراحی پروتکل TCP/IP که بعدها به اصلی‌ترین پروتکل ارتباطی شبکه اینترنت تبدیل گردید نیز تمهیدات امنیتی در نظر گرفته نشده بود. مدت زیادی نگذشت که سوء استفاده از امکانی که شبکه در اختیار کاربران قرار داده بود در ذهن بعضی از افراد خطور کرد و دست به اقداماتی زدند که اکنون به عناوین مختلف مانند نفوذ یا حمله و یا سرقت اطلاعات نام برده می‌شود.

اولین کرم اینترنتی در سال ۱۹۸۸ به نام کرم موریس در اینترنت منتشر شد و حدود ۱۰ درصد کامپیوترهای متصل به اینترنت را آلوده نمود. ویروس‌های اینترنتی سابقه‌ای بیشتر از کرم اینترنتی دارند. در سال ۱۹۷۱ ویروس کریپر[1] در شبکه آرپانت پخش شد و کامپیوترهای DEC PDP-10 را آلوده کرد. در سال ۱۹۸۱ ویروس کلونر[2] برای سیستم عامل Apple DOS 3.3 نوشته و از طریق فلاپی دیسک منتشر شد البته ویروس‌ها سابقه‌ای حتی بیشتر از آنچه در اینجا ذکر گردید دارند.

خطوط تلفن نقش مهمی در برقرار ارتباطات شبکه ایفا می‌کرد و فراهم کردن خدمات شبکه نیز با اتصال کاربران با استفاده از مودم‌ها و از طریق خطوط تلفن انجام می‌گردید. بهمین دلیل روش حمله به خطوط تلفن[3] جزء روش‌های شناخته شده حملات سایبری سنتی به شمار می‌رود. در این روش یک مهاجم با استفاده از کامپیوتر و مودم

[1] creeper
[2] Cloner
[3] War Dialing

اقدام به گرفتن شماره‌های مختلف در یک لیست یا طی یک فرایند می‌کند تا سایر کامپیوترهایی که توسط مودم قابل دسترس هستند را پیدا کند و سپس علیه آنها اقداماتی انجام دهد. این حمله در روشهای تنازعات سایبری مدرن منسوخ شده است. می‌توان جایگزین این روش حمله در روشهای مدرن را روش حمله در حال رانندگی[1] برشمرد که در آن یک مهاجم در داخل خودروی در حال حرکت در جستجوی شبکه‌های بی‌سیم (wifi) می‌باشد تا بتواند از آنها سوء استفاده یا به آنها نفوذ کند.

حمله منع سرویس در روش‌های سنتی تهاجمات سایبری هنوز کاملا شناخته شده نبود و بخصوص موضوع حملات منع سرویس توزیع شده ناشناخته بوده و تا اوایل سال ۲۰۰۰ میلادی مطرح نشده بود.

به این ترتیب می‌توان ویژگی‌های تنازعات سایبری سنتی را در نکات زیر خلاصه نمود:

- دامنه حملات محدود
- روش‌های حمله مبتنی بر فناوری اولیه مانند جنگ تلفنها
- امنیت جریان داده‌ها مبتنی بر روش‌های قدیمی و رمزنگاری سنتی
- حملات به منظور جمع‌آوری اطلاعات بصورت محدود و موضعی
- استفاده از ویروس‌ها و کرم‌های ساده و قابلیت کشف و مهندسی معکوس آسان

بر این اساس ویژگیهای تنازعات سایبری سنتی را می‌توان در ابعاد متدولوژی انتخاب شده به این شرح بیان نمود:

معماری: سیستم‌های شبکه‌ای از معماری خاصی تبعیت نکرده و صرفا شبکه از کامپیوترهای متصل به هم را تشکیل داده‌اند، سرورها همگی بر اساس سخت‌افزارهای موجود شامل فضای ذخیره‌سازی و پروسسورهای نه چندان سریع می‌باشد، پراکندگی شبکه کم است و تهیه سرور برای گروه‌های عملیاتی سخت و پر هزینه است.

بستر: حملات روی شبکه‌های خبری و اشتراک داده‌ها انجام گرفته و هنوز شبکه وب ایجاد نشده است.

تکنولوژی: استفاده از روش‌های نیمه سخت‌افزاری مانند مودم‌ها، نیاز به دانش کافی روی سیستم‌های عامل و پروتکل‌ها

ابزار: زبان‌های برنامه‌نویسی برای انتخاب عملیات کنندگان محدود بوده و توسط متخصصین قابل استفاده است و ابزارهای مورد استفاده محدود و استفاده از آنها مشکل می‌باشد. بسیاری از ابزارها و تکنیک‌های قدیمی اکنون منسوخ شده و غیرقابل استفاده می‌باشد.

تکنیک: استفاده از تکنیک‌های ساده نفوذ و منع سرویس و روش‌هایی که در حال حاضر کارایی چندانی ندارد.

۴- روش‌های سایبری مدرن

با گسترش وسیع شبکه جهانی اینترنت و افزایش بسیار بالای تعداد سرورها و کلاینت‌های متصل به شبکه و همچنین افزایش پهنای باند ارتباطی هم در ستون فقرات شبکه[2] و هم در ارتباطات بین سرورها و همچنین افزایش پهنای باند اتصال کاربرن به اینترنت، فصل جدیدی از تنازعات سایبری شروع شد و استفاده از امکانات جدید برای طراحی حملات رونق گرفت. بدلیل گسترش شبکه و وابستگی بیش از پیش سیستم‌های اقتصادی- اجتماعی و تکنولوژیکی به شبکه اطلاعات، این سیستم‌ها در معرض تهدیدات بیشتری قرار گرفته‌اند. در اینجا به عناصر و موضوعات مرتبط با روش‌های سایبری مدرن اشاره می‌شود:

تکنولوژی وب

پس از گذشت دو دهه از تشکیل شبکه اینترنت و زمانی که هنوز اینترنت همگانی نشده بود زبان html معرفی و مقدمه گسترش فراگیر شبکه به صورت یک وب جهانی پیاده‌سازی گردید و همین امر باعث شد که اینترنت بسیار بیشتر از قبل عمومی شده و سرویس‌های فراوانی را ارائه نماید و به همین دلیل اطلاعات بیشماری نیز از طریق اینترنت در دسترس قرار گرفت که نسبت به گذشته قابل مقایسه نبود. از این دیدگاه حملات و عملیات سایبری پس از ارائه تکنولوژی وب فصل جدیدی از تاریخ خود را شروع کرد که در ادامه بیشتر به آن خواهیم پرداخت.

جمع‌آوری اطلاعات در حد وسیع

سرقت و دسترسی به اطلاعات در دوران اولیه تنازعات سایبری نیز وجود داشت ولی دسترسی به اطلاعات بی‌پایان که از آن به انفجار اطلاعات یاد می‌شود از ویژگی‌های نیمه دوم عمر اینترنت است. با همین دیدگاه روش‌های جمع‌آوری و سرقت اطلاعات پیشرفته‌تر و خودکار شده‌اند. از جمله منابع اطلاعاتی که بیشتر مورد توجه

[1] Wardriving

[2] Backbone

هستند می‌توان به پایگاه‌های علمی، متن و پیوست ایمیل‌ها، بانک‌ها، دیتابیس‌ها، اطلاعات نظامی و جریان ترافیک اینترنتی اشاره کرد و روش‌های مدرن جمع‌آوری نیز شامل تکنیکهای پیشرفته استراق سمع، روشهای نفوذ خود کار به تعداد زیادی از سرورهای اینترنتی، تکنیکهای پیشرفته و مدرن ویروس‌نویسی و روشهای نوین فرار از تشخیص توسط آنتی ویروس‌ها و دور زدن فایروالها می‌باشند.

حمله منع سرویس[1] توزیع شده[2]

با افزایش وابستگی زندگی روزمره انسانها به اینترنت بخصوص در ارایه خدمات شهری، اداری، مالی، دولتی و نظامی، یکی از حملاتی که در دنیای سایبری مدرن اهمیت ویژه‌ای پیدا کرده و تاثیر بسزایی دارد عملیات منع سرویس می‌باشد. روش‌های گوناگونی برای انجام عملیات منع سرویس پیشنهاد شده و این مساله از جمله موضوعات تحقیقاتی روز به شمار می‌رود. یکی از انواع روشها استفاده از تعداد زیادی عامل‌های نرم‌افزاری توزیع شده در نقاط مختلف شبکه در دنیا می‌باشد که طراحی آنها به نحوی است که همگی آماده انجام فرامین توسط فرمانده هستند و پس از دریافت فرمان بطور همزمان اقدام به انجام عملیات علیه یک هدف مشخص شده می‌نمایند و چون این حمله بصورت همزمان و با فشار شدید انجام می‌گیرد تاثیرات مخربی روی هدف بر جا می‌گذارد. این روش در زمره روش‌های نوین حملات سایبری بشمار می‌رود و اولین حمله شناخته شده در این زمینه به سال ۱۹۹۹ بر می‌گردد که سیستم کامپیوتری دانشگاه مینه سوتا مورد حمله قرار گرفت و بمدت دو روز از دسترس خارج شد[ ]2[]

سیستمهای فرماندهی و کنترل تحت شبکه

در تنازعات سایبری مدرن ایجاد سیستمهای فرماندهی و کنترل سایبری یکی از ارکان طراحی و بکارگیری سلاح‌های سایبری می‌باشد. در هر نوع حمله سایبری گروه حمله کننده برای ایجاد همزمانی و کنترل کامل روی حمله یک سیستم فرماندهی و کنترل را پیاده‌سازی می‌نماید. بطور مثال در انجام حملات منع سرویس توزیع شده لازم است روش‌هایی ابداع شوند که توسط آنها بتوان به عامل‌های نرم‌افزاری در اختیار بطور همزمان دستوراتی را صادر کرد و پس از اتمام عملیات بطور همزمان آنها را متوقف نمود. در ادامه به دو روش پیاده‌سازی سیستم فرماندهی و کنترل که قبلا مورد استفاده قرار گرفته‌اند اشاره خواهد شد. نکته مهم در هرگونه عملیات سایبری مخفی ماندن قبل و حین عملیات است. بدین منظور باید عملیات نصب عاملها، احضار آنها و انتقال فرامین به آنها به صورتی انجام پذیرد که حتی‌الامکان هیچگونه ردی از گروه‌های مهاجم بر جا نماند و عملیات قابل ردیابی به عقب[3] نباشد.

شبکه عامل‌های مبتنی بر سرور

یکی از روش‌های پیاده‌سازی حملات توزیع شده استفاده از شبکه عاملها یا بات[4]های نصب شده در سرورهای اینترنتی است. با توجه به اینکه معمولا سرورها از پهنای باند بسیار بالایی برخوردار هستند چنین شبکه‌ای از باتها می‌تواند به نحو موثری هدف خود را از پای درآورد. از ویژگی‌های این گونه شبکه‌ها می‌توان به پیاده‌سازی سریع و آسان، صدور سریع و بلافاصله فرامین شروع و پایان عملیات، قدرت بسیار بالا در تخریب، سادگی سیستم فرماندهی و کنترل و البته طول عمر کوتاه شبکه اشاره نمود. یک نمونه سیستم فرماندهی و کنترل در این گونه شبکه‌ها استفاده از سیستم گفت و گوی IRC[5] می‌باشد که در آن، همه عاملها خود را به سیستم چت معرفی می‌کنند و فرمانده از طریق خط فرمان به همه باتها هدف را معرفی کرده و فرمان را صادر می‌نماید.

شبکه عامل‌های مبتنی بر کلاینت

اینگونه شبکه‌ها از طریق پخش انبوه ویروس‌ها به کامپیوترهای کاربران شکل گرفته و روش موثری برای از کار انداختن اهداف در عملیات منع سرویس توزیع شده معرفی می‌نماید. معمولا برای اینکه انجام عملیات واقعا موثر باشد باید گسترش بات‌ها در این شبکه بسیار بالا و بیش از ده میلیون بات باشد. از ویژگی‌های این شبکه می‌توان به طول عمر زیاد شبکه، مدت زمان نسبتا طولانی گسترش آن، تاخیر در صدور فرامین شروع و پایان حمله، عدم امکان مقابله با آن از طریق فایروال‌ها، سیستم فرماندهی و کنترل نسبتا پیچیده و کارایی بالا اشاره کرد. یک نمونه سیستم فرماندهی و کنترل در این شبکه به این صورت است که باتها طی پریودهای زمانی مشخص به یک محل از قبل تعیین شده مراجعه کرده و فرامین را از آنجا

[1] Denial of Service
[2] Destributed Denial of Service
[3] Traceback
[4] Bot
[5] Internet Relay Chat

دریافت و اجرا می‌نمایند و فرمانده نیز فرامین خود را در همان محل (مانند یک تابلوی اعلانات) درج می‌نماید.

روش‌های پیچیده و ترکیبی

از ویژگی‌های تنازعات سایبری مدرن پیچیده بودن آن و استفاده از ترکیب انواع سلاح‌ها و تاکتیک‌ها می‌باشد. در این گونه حملات دشمن همزمان با نفوذ به سایتها و سرورهای حریف از یک جهت و انجام عملیات منع سرویس از طرف دیگر از شبکه‌های اجتماعی نیز بهره برده و به پیاده‌سازی جنگ نرم اقدام می‌نماید و بطور همزمان عملیات‌های دیگری نیز که ممکن است فیزیکی باشند اجرایی می‌کند.

مجازی‌سازی[1] و محاسبات ابری[2]

روش‌های مجازی‌سازی سیستم‌ها، فناوری‌ای است که در سالهای اخیر توسعه یافته و توسط شرکت‌هایی مانند vmware، sun-oracle و parallels رهبری می‌شود. این فناوری سرعت گسترش شبکه‌های اینترنتی را بسیار بالا برده بطوری که زمان نصب و آماده‌سازی یک سرور را از چندین ساعت به چندین ثانیه تقلیل داده است. روش‌های محاسبات ابری از همین ویژگی بهره برده و پیاده‌سازی شبکه‌های پردازش موازی یا خدمات‌رسانی مستقل از سخت‌افزار را به امری سهل‌الوصول و راحت تبدیل کرده‌اند. بنابراین این روش بستر مناسبی هم برای نفوذگران و مهاجمان سایبری و هم برای مدافعین و متخصصین امنیت سیستمها فراهم نموده است.

مهندسی اجتماعی[3]

روش‌های جدید همراه با افزایش تجربه نفوذگران برای فریب و جلب توجه اهداف مورد نظر پیشرفت قابل ملاحظه‌ای داشته است. این روشها بهمراه ابزارهای پیشرفته ترکیب فایل‌های سالم با ویروسها و ارسال آن به هدف، به همراه گسترش بیش از پیش استفاده از نامه‌های الکترونیکی و سیستم‌های پخش وسیع نامه‌ها مانند spamming باعث شده تا شیوه مهندسی اجتماعی یکی از موثرترین روشهای نفوذ به کامپیترها و سرورها در عصر کنونی باشد. همچنین استفاده از شبکه‌های اجتماعی مانند فیس بوک[4]، توییتر[5] و مای اسپیس[6] بستر مناسبی برای عملیات مهندسی اجتماعی است. یکی از روشهای رایج مهندسی اجتماعی فیشینگ[7] است که شخص مهاجم یک سایت مزین شده را بجای سایت اصلی جا زده و اهداف را قانع می‌کند که از آن برای وارد کردن اطلاعات خود استفاده نمایند. روش‌های مهندسی اجتماعی دارای خاصیتی هستند که هرگز کهنه نشده و همیشه یکی از راه‌ها و امیدهای نفوذ به اهداف از دیدگاه نفوذگران بشمار می‌روند.

شبکه‌های اجتماعی و عملیات روانی

از جمله تکنولوژی‌هایی که در شبکه‌های سایبری مدرن به وقوع پیوسته است ایجاد شبکه‌های اجتماعی است. در این خصوص در قسمت روش‌های دفاعی بیشتر صحبت خواهیم کرد اما لازم به ذکر است که شبکه‌های اجتماعی علیرغم ویژگیهای مثبت و موثری که دارد بستر مناسبی برای انحراف اذهان و مدیریت روانی و جنگ نرم است چنانکه این گونه عملیات در سالهای گذشته به کرات در کشورهای مختلف اتفاق افتاده و چنانچه کنترل علمی- فرهنگی همراه با تدبیر و روشن‌بینی روی آن صورت نگیرد می‌تواند تبعات سنگینی را با خود به همراه داشته باشد.

روشهای پردازش هوشمند

در دهه اخیر استفاده از روشهای پیشرفته‌تر داده کاوی[8] و ترکیب اطلاعات[9] اهمیت بیشتری پیدا کرده و هدف آن استفاده از انبوه داده‌های متراکم، نا همگون و بی‌ربط به منظور کشف واقعیتها و جریانهای خبری- اطلاعاتی مخفی در بین آنها است. در واقع بدون دسترسی به سیستمهای پیشرفته و هوشمند پردازش اطلاعات و روشهای مدرن و خودکار تصمیم‌گیری نمی‌توان از این همه داده‌های در دسترس استفاده مفید و موثری کرد و بهره مناسبی گرفت.

جنگ اطلاعاتی[10] یا جنگ سایبری[11]

از مجموع آنچه ذکر شد پدیده‌ای نوین در تنازعات سایبری مدرن ایجاد می‌شود که از آن به جنگ اطلاعاتی یاد می‌کنند. در [۱] جنگ

[1] Virtualization
[2] Cloud Computing
[3] Social Engineering
[4] Facebook
[5] Twitter
[6] MySpace
[7] Phishing
[8] Data Mining
[9] Information Fusion
[10] Information Warfare
[11] Cyber War

سایبری را تنازع نظامی با استفاده از فناوری اطلاعات تعریف کرده است. در واقع جنگ اطلاعاتی از وفور اطلاعات و اهمیت و تاثیر آن در صحنه نبرد به همراه ترکیب استراتژیها و تاکتیکهای متنوع سایبری با استفاده از فناوریهای مدرن و روشهای نوین بوقوع می‌پیوندد. بدلیل رشد سریع اینترنت هزینه نبردهای الکترونیکی و دیجیتالی کاهش یافته و آگاهی درباره اینکه چگونه از جنگهای اطلاعاتی استفاده شود در بین مردم در حال افزایش است. عبارتهای cyber war، cyber offensive، و cyber terrorism، cyber power، cyber strategy، cyber operations، اصطلاحات جدید در جنگهای مدرن هستند [۳].

انواع عملیات در جنگ سایبری شامل عملیات شبکه کامپیوتری (CNO)، جنگ الکترونیک (EW) و عملیات روانی (PsyOps) است. یکی از خاصیتهای جنگ سایبری نامتقارن بودن آن است[۴]:

- انجام یک حمله سایبری علیه یک سیستم حیاتی مانند SCADA[1] می‌تواند نسبتا سهل و ارزان باشد اما از طرف دیگر حفاظت چنین سیستمی در برابر حملات سخت و پرهزینه می‌باشد.
- وقتی حمله سایبری رخ می‌دهد حتی اگر کاملا هم موفق نباشد اطلاعاتی از هدف جمع‌آوری می‌شود که بعدا می‌تواند مورد استفاده باشد اما از طرف دیگر با عنایت به اینکه حمله کنندگان از روش‌های مخفی ماندن و فرار از شناسایی و ردیابی استفاده می‌کنند اطلاعاتی از مهاجمین و سیستمها و روشهای آنها بدست نمی‌آید.

یک شخص، یا یک گروه کوچک، یا یک ایالت، می‌تواند بالقوه خسارتی وارد کند که در سالهای گذشته فقط با پرتاب بمبها و انفجارت متعدد حاصل می‌شد.

بر این اساس ویژگیهای تنازعات سایبری مدرن را می‌توان در ابعاد متدولوژی انتخاب شده به این شرح بیان نمود:

معماری: استفاده از روشهای پیچیده و ترکیبی در تنازعات سایبری، سیستمهای فرماندهی و کنترل پیچیده و غیرقابل ردیابی، استفاده از سیستمهای محاسبات ابری

بستر: استفاده حداکثری از پروتکل وب، استفاده از زبانهای پیشرفته اسکریپتی مانند perl و php، امکانات پخش وسیع نامه‌های الکترونیکی، استفاده از شبکه‌های اجتماعی بمنظور عملیات روانی در سطح وسیع و پیاده‌سازی جنگ نرم

تکنولوژی: استفاده از روشهای نوین پردازش هوشمند داده‌ها، روشهای پیشرفته استراق سمع، رویکردهای جدید تحلیل و کشف رمز

ابزار: استفاده از روشهای مدرن برنامه‌نویسی ویروس‌ها، استفاده از شبکه عاملهای توزیع شده، ابزارهای مجازی‌سازی

تکنیک: روشهای مدرن فرار از آنتی ویروس و فایروالها، روشهای مخفی‌سازی و جلوگیری از تعقیب، پیاده‌سازی روشهای پیچیده‌تر نفوذ به سیستمها، روشهای مدرن مهندسی معکوس سیستمها و نرم‌افزارها، استفاده از شیوه‌های جدید مهندسی اجتماعی

۵- روشهای دفاع

در مقابل حملات سایبری که ممکن است علیه سایتها و شبکه‌ها انجام بگیرد لازم است روشهای تدافعی طراحی و پیاده‌سازی گردد. در میان روشها و تاکتیکهای مختلفی که وجود دارد در اینجا به موارد و نکاتی که مهمتر به نظر می‌رسد اشاره می‌گردد.

آنتی ویروس و فایروال

طبیعتا اولین سنگر دفاعی در دنیای سایبری استفاده از آنتی ویروس است. این ابزار هم در کلاینتها و هم در سرورها بخصوص در سرویس دهنده‌های ایمیل اهمیت دارد. بعضی از کاربران کامپیوتر این تصور را دارند که استفاده از آنتی‌ویروس امنیت کامپیوتر آنها را تضمین می‌کند در حالیکه این ایده غلطی است و وجود یک فایروال مناسب و انعطاف‌پذیر در کنار آنتی ویروس ضروری است. اما نکته مهمی که درباره آنتی ویروس لازم به تذکر است انتخاب آن است. در حال حاضر شرکتهای معروفی همچون نورتون، مک آفی و ای ست محصولات جامع امنیتی شامل آنتی ویروس و فایروال تجمیع شده را عرضه می‌کنند. ولی متاسفانه بدبینی‌هایی نسبت به صداقت کامل آنها در کشف و خنثی‌سازی خرابکاری‌های اینترنتی وجود دارد بخصوص که این نرم‌افزارهای امنیتی در کشف به هنگام کرم اینترنتی استاکس نت رفتار خوب و قابل دفاعی از خود بجا نگذاشتند.

[1] Supervisory Control And Data Acquisition System

سیستمهای کشف نفوذ[1] و جلوگیری از نفوذ[2]

اینگونه سیستمها معمولا نیاز به پردازش قوی و تکنولوژی پیشرفته دارند و بنابراین هزینه آنها بالا است و برای استفاده کلاینت‌ها مناسب نیست اما سرورهایی که برای حفظ امنیت خود اهمیت بیشتری قائل هستند با پرداخت این هزینه سیستم فوق را که معمولا بصورت سخت‌افزارهای آماده هستند در مسیر ترافیک نصب می نمایند. این سیستمها به دو روش عمل می‌کنند. روش اول کشف حملات در حال انجام از روی مشخصات و امضاء حمله[3] می‌باشد. روش دوم کشف حملات ناشناخته با بررسی رفتارهای غیر طبیعی در ترافیک است که از روشهای پیشرفته‌تر بدین منظور استفاده می‌کند. لازم به ذکر است که برای دفاع در مقالب حملات توزیع شده DDoS نیز سیستمهای تدافعی آماده در بازار وجود دارند که تا حدی می‌توانند جلوی این حملات را بگیرند اما اگر حمله مزبور به دقت طراحی شده و بطور موثری بکار رفته باشد در عمل جلوی آن را با هیچ روشی نمی‌توان بطور کامل گرفت.

آزمون نفوذپذیری[4]

حتی اگر مکانیزم‌های دفاعی برای سرورهای اینترنتی تدارک دیده شده باشد همیشه باید منتظر بود که روشهای نوین حمله و نفوذ به سرورها توسط نفوذگران ابداع و اجرا گردد بنابراین سرورهای مهمتر مانند بانکها و سازمانها معمولا آزمون نفوذپذیری را بطور منظم در دستور کار خود قرار داده و سالیانه بخشی از بودجه امنیتی خود را صرف این موضوع می‌نمایند.

سیستمهای محاسبات ابری[5]

وقتی سرورهای اینترنتی به دستگاه‌های خاص مانند CPU، هارد دیسک، مادر بورد، منبع تغذیه و کامپیوتر خاص وابسته باشند همیشه در معرض حذف و قطع سرویس‌دهی هستند چون یک اشکال فیزیکی در هر یک از این دستگاه‌ها (مانند سوختن منبع تغذیه یا شکسته شدن مادربورد) باعث از کار افتادن سرور خواهد شد. سیستمهای محاسبات ابری با جداکردن کامل سرویس‌ها از سخت‌افزارها خدمت ویژه‌ای را در عصر حاضر به سرویس‌های اینترنتی ارائه کرده‌اند. در این گونه سیستمها ارائه یک سرویس به هیچ دستگاه خاص مثل CPU یا هارد دیسک خاص و یا حتی یک محل فیزیکی خاص وابسته نیست و در هر لحظه می‌تواند محل فیزیکی آن تغییر کند بدون اینکه خللی در سرویس‌دهی ایجاد شود و البته لازم به ذکر است که این وظیفه را بکمک پیشرفتهای اخیر در مبحث مجازی‌سازی[6] پیاده‌سازی می‌نماید.

شبکه‌های اجتماعی[7]

شبکه‌های اجتماعی بستر مناسب و مدرنی برای ارتباطات بین افراد و گروه‌ها و حتی تمدن‌ها است و ارتباطات بین انسانها را از آنچه در گذشته از طریق مهاجرتها و مسافرتها و بندرت توسط افراد خاص انجام می‌شد به یک امر لحظه‌ای و دائمی در همه حوزه‌ها و توسط هر فرد علاقه‌مند تبدیل کرده است. اما این بستر خطراتی نیز در پی دارد که البته مشابه آن در سایر زمینه‌ها هم تجربه شده است که به حوزه اخلاق و عقاید مربوط می‌شود. همانطور که اگر عضوی از بدن انسان دچار عفونت و فساد شود از همان نقطه به سایر نقاط بدن هم گسترش می‌یابد و باید سریعا جلوی آن گرفته شود در موضوعات اخلاق و عقاید هم چنین مطلبی صحیح است و گاهی یک مفسده از طرف یک فرد فاسد – حال چه موضوع اخلاقی یا عقیدتی – ممکن است روی افراد بسیار زیادی تاثیر گذاشته و ذهن و روان آنها را تحت تاثیرات مخرب قرار دهد و حتما باید در مقابل آن واکنش نشان داد. در چنین شرایطی روشهای دفاعی سیستماتیک وجود ندارد هرچند از دیدگاه فنی روش فیلترینگ و سانسور ممکن است در کوتاه مدت با قصد دور نگه داشتن افراد از منبع فساد تاثیراتی داشته باشد اما افرادی که نسبت به انسان مطالعه و شناخت دارند اینگونه روش مقابله را به هیچ وجه توصیه و تشویق نمی‌نمایند بلکه باید برای مقابله با معضلات اجتماعی از این دست با ابزار علم و تفکر اقدام نمود.

۶- نتیجه

در این مقاله به معرفی اجمالی روشهای تنازعات و حملات سایبری در شبکه اینترنت پرداخته و با دو دیدگاه سنتی و مدرن

[1] IDS, Intrusion Detection System
[2] IPS, Intrusion Prevention System
[3] Signature
[4] Penetration Test
[5] Cloud Computing
[6] Virtualization
[7] Social Networks

مورد بررسی قرار گرفت و به بعضی از ویژگیها و عناصر مهم آنها را اشاره شد. همچنین روشهایی نیز برای مقابله و دفاع در مقابل حملات معرفی گردید.

مراجع

[1] Cyber war, Methods and Practice, K. Saalbach, 2011
[2] Defense Against Distrubuted Denial of Service Attacks, Gary C. Kessler, SANS/GIAC Security Essentials Certification, 2000
[3] First Battles in Cyberspace: New Paradigm for 21st Century Warfare?, Dr. Dan Kuehl, IRM College, National Defense University, IQPC Cyber Warfare, 2009
[4] Terrorism online and the change of modus operandi, Roland Heickerö, Swedish Defence Research Agency, FOI