تاریخ دریافت: ۹٤/۷/۱۰
تاریخ تأیید: ۹٤/۹/۲۵

راه‌کارهای پدافند غیرعامل برای مقابله با جاسوسی در فضای مجازی ناجا

بهزاد وثوقی[۱]
سعید کوچی[۲]

چکیده

توسعه‌ی فضای مجازی در بخش اینترنت کمک شایانی به جاسوسان و راهبرد و هدایت آنان نموده است؛ امروزه شاید کمتر سازمان و اداره‌ای باشد که در فضای مجازی حضور نداشته و در این فضا از رایانه و شبکه‌های رایانه‌ای استفاده نکند. استفاده از رایانه به‌حدی مورد توجه قرار گرفته که یکی از شاخص‌های برخورداری از سواد در قرن حاضر را فراگیری علوم رایانه‌ای می‌دانند. همزمان با گسترش استفاده از رایانه و نرم‌افزارهای رایانه‌ای بین سطوح مختلف افراد جامعه، نرم‌افزارهای جاسوسی و ویروس‌های مخرب نیز گسترش یافته است. بنابراین پژوهش حاضر با اشاره به تعاریف کارامد، به تغییر شیوه‌های جمع‌آوری اطلاعات و پیشرفت آنها و از طرفی ایجاد شیوه‌های ارتباطی در فضای مجازی پرداخته و به این سؤال پاسخ خواهد داد: آیا می‌توان با اقدام‌های پدافند غیرعامل از جاسوسی در فضای مجازی ناجا جلوگیری به‌عمل آورد؟

برای پاسخگویی به این مهم، از روش کاربردی و ابزار گردآوری داده‌ها به‌صورت مطالعه‌ی کتاب، مقاله‌ها و مستندات قانونی موجود به‌صورت اسنادی و کتابخانه‌ای استفاده شده است. نتایج به‌دست آمده، گویای به‌کارگیری هدفمند اقدام‌های پدافند غیرعامل برای مقابله با جاسوسان در فضای مجازی ناجا بوده و در این خصوص محقق پیشنهادهای کارسازی را ارائه نموده است.

کلید واژه

پدافند غیرعامل، تهدید، جاسوس، فضای مجازی، ناجا.

---

۱. کارشناس ارشد علوم دفاعی – دانشگاه امام حسین (ع).
۲. کارشناس ارشد پدافند غیر عامل- امنیت ملی، دانشگاه فارابی .

مقدمه

امروزه کارشناسان اطلاعاتی بدون آشنایی با فناوری‌های نوین و روند تغییر این فناوری‌ها نمی‌توانند وظایف خود را به‌خوبی انجام دهند. با نگاهی به سیر تحول ابزارهای جاسوسی، این واقعیت به‌خوبی احساس می‌شود که ابزارهای جاسوسی به‌دلیل پیشرفت‌های صورت گرفته، نسبت به قبل دچار تغییرات بنیادی شده‌اند. در این پژوهش سعی شده با در نظر گرفتن این فرض که فضای مجازی و شیوه‌های ارتباطی نوین در آن بر اقدام‌های جاسوسی و ضدجاسوسی تأثیر گذاشته است، با ذکر مصداق‌هایی به بیان کاربردهای آنها در روش‌های جمع‌آوری اطلاعات پنهان و روش‌های برقراری ارتباط به‌عنوان مؤلفه از جاسوسی و مراحل ضدجاسوسی به‌عنوان مهم‌ترین قسمت ضدجاسوسی پرداخته شود.

یکی از ابزارهای مهم در فضای مجازی، اینترنت است. این پدیده هر چند عمرش از پنج دهه تجاوز نمی‌کند ولی از ابزار تأثیرگذار در حوزه‌ی اطلاعات محسوب می‌شود. امروزه این دریای بی‌کران، فضایی برای تأثیرگذاری در حوزه‌ی اطلاعات در یک گستره‌ی جهانی را در اختیار کاربران قرار داده است.

به‌یقین هر چه میزان آگاهی از این عرصه بیشتر باشد، بهتر و بیشتر می‌توان از این اطلاعات استفاده نمود و از آسیب‌های آن در امان ماند.

کلیات

بیان مسئله

استفاده از فضای مجازی با افزایش سطح آن در دولت و عموم، موجب شده تا جامعه به‌طور فزاینده‌ای به‌سمت شبکه‌ای شدن پیش رود. به هر صورت، این رشد، موجب وابستگی می‌شود؛ در نتیجه سطح آسیب‌پذیری و ظهور بخشی از تهدیدهای امنیت ملی که در تماس با فضای مجازی است افزایش می‌یابد. به‌عنوان نمونه چنانچه زیرساخت‌های اطلاعات ملی کشور مورد آسیب قرار گیرد، تأمین انرژی برق، توزیع غذا، تأمین آب و تصفیه‌ی آن، ارائه‌ی خدمات مالی، تبلیغات، حمل و نقل، بهداشت و سلامتی، خدمات اضطراری و خدمات دفاعی و دولتی همگی

آسیب خواهند دید. مطابق قانون برنامه‌ی چهارم توسعه، یکی از محورهـای اساسـی موضوع امنیت ملی، بحث امنیت فضای مجازی است. از این‌رو ضرورت عقلی دفاع، به‌طور کامل مشهود است. آمار و سوابق جنگ‌های گذشته نشان می‌دهد کـه پدافنـد غیرعامل در حال حاضر یکی از مهم‌ترین اقـدام‌هـا بـرای کـاهش آسـیب‌پـذیری در حوزه‌ی مجازی است؛ بنابراین، به‌کارگیری اصول و معیارهای امنیتی در ایـن حـوزه، می‌تواند به تکمیل زنجیره‌ی دفاعی، کمک مؤثر و قابل تـوجهی نمایـد کـه ایـن امـر به‌طور شایسته‌ای از جانب مقام معظم رهبری(مدظله‌العالی) نیز مورد تأکید قرار گرفتـه است. ضروری است این مسئله مورد اهتمام جدی‌تری در ناجا قـرار گیـرد (کـوچی، ۱۳۹۳ :۱۳۸).

اهمیت و ضرورت تحقیق

در فضای مجازی، زمانی می‌توان عملکرد مؤثری داشت که این فضا امن باشد. هر دولتی برای کسب موفقیت بیشتر باید اقدام‌هایی انجام دهد تا از فرصت‌های موجـود در فضای مجازی به بهترین وجه بهره‌بـرداری نمایـد. هرچـه وابسـتگی بـه فضـای مجازی افزایش یابد، به همان میزان امنیت فضای مجازی به موضوعی بـا اهمیـت‌تـر تبدیل می‌شود. فضای مجازی از میان تمامی تهدیدها و مؤلفه‌هایی که در امنیت ملی قرار دارند، عبور می‌کند؛ به‌عبارت دیگر این فضا با توجه به نوع خدمات‌رسانی ناجـا در اینترنت و شبکه‌ی داخلی خود (اینترانت) از تمامی مرزهای بین کشور می‌گـذرد و به شکلی ناشناخته و بی‌نام عمل می‌کند و فنـاوری‌ای کـه از سـوی ایـن فضـا بـه خدمت گرفته می‌شود با سرعت به توسعه‌ی خود ادامه می‌دهد.

در این حوزه، صحبت از تهدید کسانی است که فضای مجازی را گستره‌ای عظـیم از کار، از ماهی‌گیری گرفته تا فعال‌سـازی و سـوءاسـتفاده از کـارت‌هـای اعتبـاری، به‌خدمت می‌گیرند تا با استفاده از آن، در یک عملیات جاسوسـی مشـارکت نماینـد؛ پس نیاز راهبردی و امنیتی است تا بر اساس آن، امنیت فضای مجازی را تأمین نمود. (همان)

نرم‌افزارهای جاسوسی، درست مانند علف‌های هرز که بدون سروصدا هنگام قـدم زدن در جنگل به جوراب می‌چسبند، هنگامی که فردی مشـغول گشـت و گـذار در

اینترنت است، نرم‌افزار جاسوسی خودش را مانند یک مسافر قاچاقی به رایانه می‌چسباند اما قبل از اینکه برنامه‌ای بتواند روی رایانه نصب شود، باید روی چیزی کلیک یا برنامه‌ای را باز کرد.

هدف‌های تحقیق

هدف اصلی

- ارائه‌ی راه‌کارهای پدافند غیرعامل برای مقابله با جاسوسی در فضای ناجا.

هدف‌های فرعی

- شناخت فضای مجازی و جمع‌آوری پنهان در این فضا
- آشنایی با جمع‌آوری اطلاعات فنی در فضای مجازی
- شناخت راهبری و هدایت جاسوسان در فضای مجازی
- آشنایی با روش‌های نوین انتقال اطلاعات در فضای مجازی
- شناخت ضدجاسوسی در فضای مجازی
- آشنایی با راه‌کارهای پدافند غیرعامل برای مقابله با نرم‌افزارهای جاسوسی
- شناخت راه‌کارهای پدافند غیرعامل با رویکرد پیشگیرانه برای حفاظت فضای مجازی

سؤال‌های تحقیق

سؤال اصلی

- آیا می‌توان با اقدام‌های پدافند غیرعامل از جاسوسی در فضای مجازی ناجا جلوگیری به‌عمل آورد؟

سؤال‌های فرعی

- روش‌های جمع‌آوری اطلاعات در فضای مجازی چگونه است؟
- چگونه می‌توان از اطلاعات ناجا در فضای مجازی حراست نمود؟
- ضدجاسوسی در فضای مجازی چیست؟

روش تحقیق

روش تحقیق از لحاظ هدف؛ کاربردی و از نظر روش؛ توصیفی- تحلیلی است. روش گردآوری داده‌ها در این مقاله، به‌صورت مطالعه‌ی کتاب‌ها، مقاله‌ها و مستندات قانونی موجود به‌صورت اسنادی و کتابخانه‌ای است.

ادبیات نظری

فضای مجازی

فضای مجازی به فضای تبادل اطلاعات الکترونیکی اطلاق می‌شود و تمامی اشکال تبادل اطلاعات الکترونیکی به‌صورت دیجیتال و شبکه‌ای را دربر می‌گیرد و این موضوع شامل مفاهیم و عملکردهایی که از طریق شبکه‌های دیجیتالی هدایت می‌شوند نیز می‌گردد.

زیرساخت اصلی فضای مجازی، فناوری اطلاعات و ارتباطات است که در پنجاه سال گذشته پیشرفت زیادی پیدا کرده است. پایه‌های فیزیکی ساختمان فضای مجازی در واقع رایانه‌های شخصی و سامانه‌های ارتباطی هستند. هر کدام از این عناصر فنی ناپیوسته، بسیاری از فعالیت‌های روزانه‌ی شهروندان را چه در محیط کار و چه در محیط شخصی زندگی و همچنین به‌طور اساسی از بسیاری از زیرساخت‌های ارتباطی و اطلاعات ملی پشتیبانی می‌کنند (کوچی،۱۳۹۳ :۸۹).

جاسوسی

جاسوسی به هرگونه اقدام پنهان و غیرقانونی گفته می‌شود که توسط سازمان‌های اطلاعاتی کشورها و یا سازمان‌های مستقل طرح‌ریزی، هدایت و اجرا می‌شود تا به اطلاعات حساس و غیرعلنی دسترسی یابند. بر اساس این تعریف، اقدام پنهان و غیرقانونی جزء یکی از ویژگی‌های اصلی جاسوسی محسوب می‌شود. انجام این امور همان‌طور که از نامش پیداست، نیاز به انجام اقدام‌ها به‌صورت مخفیانه و به‌دور از انظار عموم مردم و سازمان‌های ضداطلاعاتی دارد. تأمین این امر (مخفی‌کاری و پنهان‌کاری) نیاز به ابزارها و شیوه‌هایی دارد که به‌گونه‌ای طراحی شده باشند که موجب جلب توجه نشوند و یا حداقل برای مردم آشنا نباشند. سازمان‌های اطلاعاتی برای دستیابی به این ابزارها و شیوه‌ها، چاره‌ای جز استفاده از فناوری‌ها و علوم نوین در فضای مجازی ندارند. از طرفی ضدجاسوسی که وظیفه‌ی جلوگیری از نفوذ و رخنه‌ی عوامل دشمن در تشکیلات خودی را دارد باید با روش‌های مورد استفاده‌ی جاسوسان، آشنا و از ابزارهایی برخوردار باشد که بتواند از انجام این‌گونه اقدام‌ها از جانب آنها جلوگیری نماید. بنابراین می‌توان گفت تنها راه برای رسیدن سازمان‌های

اطلاعاتی و ضداطلاعاتی به هدف‌هایشان، شناسایی فناوری‌ها و ابزارهای نوین و استفاده از آنها در راستای اقداماتشان است (واحدی، ۱۳۹۱ :۱٤۹).

پدافند غیرعامل

در بند اول از سیاست‌های کلی پدافند غیرعامل؛ ابلاغی مقام معظم رهبری(مدظله‌العالی) که در تاریخ ۱۳۸٦/۰۸/۱۲ به‌تصویب مجمع تشخیص مصلحت نظام رسید، پدافند غیرعامل عبارت است از: مجموعه اقدام‌های غیرمسلحانه‌ای که موجب افزایش بازدارندگی، کاهش آسیب‌پذیری، تداوم فعالیت‌های ضروری، ارتقای پایداری ملی و تسهیل مدیریت بحران در مقابل تهدیدها و اقدام‌های نظامی دشمن می‌شود؛ به‌عبارت دیگر می‌توان گفت پدافند غیرعامل، مجموعه اقدام‌های پایدار کننده‌ی نظام در حوزه‌ی نظم و امنیت داخلی، با انجام اقدام‌های غیرنظامی و غیرمسلحانه‌ای است که به‌کارگیری آنها باعث تولید بازدارندگی دفاعی، افزایش پایداری ملی، کاهش آسیب‌پذیری‌های انتظامی، تسهیل مدیریت بحران در حوزه‌ی نظم و امنیت و تداوم خدمات انتظامی کشور در برابر تهدیدها و اقدام‌های نظامی دشمن شود. (سروری،۱۳۹۲ :۲)

فضای مجازی و جمع‌آوری پنهان

در گذشته کارشناسان اطلاعاتی، جمع‌آوری اطلاعات به‌صورت پنهانی را به سه دسته‌ی اطلاعات تصویری، فنی و انسانی تقسیم می‌کردند اما امروزه با پوشش گسترده‌ی فضای مجازی، جمع‌آوری اطلاعات از سامانه‌های موجود در این فضا به‌ویژه رایانه، اهمیت روزافزونی برای سازمان‌های اطلاعاتی یافته است.

با ظهور فضای مجازی و استفاده‌ی روزافزون از آن، سازمان‌های اطلاعاتی درصدد دستیابی به روش‌هایی برای دسترسی به اطلاعات موجود در این فضا برآمده‌اند. در زیر به تشریح مصداق‌هایی از فناوری‌های پیشرفته در هر یک از روش‌های جمع‌آوری پنهان پرداخته می‌شود.

جمع‌آوری اطلاعات تصویری در فضای مجازی

در گذشته‌ی بسیار دور، اطلاعات تصویری فقط از طریق اتکا به قوای جسمانی به‌دست می‌آمد. با پیشرفت فناوری و اختراع دوربین، از این وسیله استفاده شد. با

شروع قرن بیستم و همزمان با جنگ جهانی اول و دوم، میزان فعالیت‌های اطلاعـاتی گسترش یافت و کشورها به‌سمت اسـتفاده از ابزارهـای جدیـد جاسوسـی حرکـت کردند. در سال ۱۹٦۰ امریکایی‌ها، فناوری جاسوسی تازه‌ای (استفاده از هواپیماهـای جاسوسی) را به‌کار گرفتند و بارها از طریق مأموریت‌های هواپیماهای «یو۲» که قادر بود در ارتفاع ۱٦۰۰۰ متری پرواز کند، از قلمـروی کشـور شـوروی عکـس‌بـرداری کردند. اما یکی از این هواپیماها در روز اول ماه مه سال ۱۹٦۰ سرنگون شد. پیش از این شکست، ماهواره‌های جاسوسـی سـاخته شـدند کـه بـه جمع‌آوری اطلاعـات تصویری می‌پرداختند (پیرآلمژان، ۱۳٦۹ :۱۵).

در جنگ سلطه (جنگ عراق) نیروهـای ائـتلاف بـیش از ۸۰ هواپیمـای شناسـایی داشتند و بیش از ۱۰۰۰ پرواز شناسایی را انجـام دادنـد و طـی آن ٤۲۰۰۰ عکـس از مناطق مورد نظر برای جنگ با عراق تهیه شد. علاوه بـر آن ۲٤۰۰ سـاعت پوشـش، ۳۲۰۰ ساعت نوار ویدئویی و ۱۷۰۰ ساعت فیلم از نشانگرهای هدف‌هـای متحـرک تهیه شده بود (یحیایی، حیدری، اشراقی،۱۳۸۲ :٤۱۷).

هواپیماها و ماهواره‌های جاسوسی از جمله ابزارهای جاسوسی پرکاربردی هستند که با استفاده از فناوری‌های پیشرفته ساخته شده‌اند و مورد اسـتفاده‌ی سـازمان‌هـای اطلاعاتی قرار می‌گیرند.

یکـی از مـاهواره‌هـایی کـه رژیـم صهیونیسـتی از آن بـرای جاسوسـی اسـتفاده می‌کند، ماهواره‌ی «افـک-۷» اسـت. «افـک-۷» نـام هفتمـین نسـل از مـاهواره‌هـای جاسوسی ارتش رژیم صهیونیستی است که توسط سازمان تحقیقـات فضـایی رژیـم صهیونیستی در تاریخ ۱۱ ژوئن ۲۰۰۷ میلادی (۲۱ خرداد ۱۳۸٦ خورشـیدی) بـرای جاسوسی نظامی از کشورهایی چون ایران و سوریه و بـا قابلیـت عکـس‌بـرداری در تمام نقاط منطقه‌ی خاورمیانه از پایگـاه هـوایی «پـالم ایچـیم» کـه در ده کیلـومتری جنوب «تل‌آویو» قرار دارد، با موفقیت به فضا پرتاب شد. به ادعای وزیر دفاع رژیـم صهیونیستی، این ماهواره‌ی جاسوسی باعث افزایش توانایی‌های نظامی ارتـش رژیـم صهیونیستی و مورد استفاده‌ی راهبردی در صورت حمله رژیم صهیونیستی به مراکـز اتمی ایران خواهد بود. رادیو ارتش رژیـم صهیونیسـتی از قـول مقامـات اطلاعـاتی

ارتش اعلام کرد که دوربین‌های عکس‌برداری ماهواره‌ی «افک-۷» قادرند اشیایی به اندازه‌ی ۷۰ سانتی‌متر را از سطح زمین شناسایی و عکس‌برداری کنند. ماهواره‌های جاسوسی به‌راحتی و بدون آگاهی نیروهای دشمن می‌توانند هدف‌های مورد نظر را از فضایی بسیار دورتر از آنچه که در دسترس نیروهای دشمن باشد مورد مراقبت قرار دهند. امروزه دستیابی به اطلاعات تصویری ماهواره‌های جاسوسی برای افراد غیراطلاعاتی نیز از طریق شبکه‌ی جهانی اینترنت ممکن است. هم اکنون کاربران اینترنت می‌توانند از طریق سایت‌هایی مانند گوگل ارث، دیجیتال گلاب، تراسرور و... به تصاویر ماهواره‌ای مناطق مختلف دست یابند (همان: ۱۵۱).

جمع‌آوری اطلاعات فنی در فضای مجازی

یکی از سامانه‌های شناخته شده، سامانه اشلون (Echelon) است. این سامانه هم‌اکنون توسط امریکا، انگلیس، کانادا و نیوزلند استفاده می‌شود. سامانه اشلون از طریق ماهواره‌ها و ایستگاه‌های زمینی، اطلاعات ارتباطی پخش شده در فضای مجازی را جمع‌آوری می‌کند. طبق گزارش‌ها، سامانه‌ی اشلون می‌تواند در هر نیم ساعت، یک میلیون مورد ارتباط را در سراسر جهان رهگیری و شنود کند (فریدل، ۱۳۸۲: ۱۸۹)

جمع‌آوری انسانی در فضای مجازی

هر چند پس از گذشت قرن‌ها از تاریخ جاسوسی، هنوز استفاده از عوامل انسانی به‌عنوان بهترین شیوه‌ی جمع‌آوری مطرح است ولی از این حقیقت نباید گذشت که با دستیابی سازمان‌های اطلاعاتی به فناوری‌های نوین، این سازمان‌ها توانسته‌اند برخی از اطلاعات مورد نیاز خود را از طریق این ابزارها به‌دست آورند و وابستگی خود را به عوامل انسانی کمتر نمایند.

حضور در فضای مجازی، وابستگی سازمان‌های اطلاعاتی را به عوامل انسانی از لحاظ کمی، کم نموده ولی وابستگی به نیروی انسانی کیفی فن‌مدار را افزایش داده است. به‌عبارتی عوامل انسانی امروزه با استفاده از امکاناتی که فضای مجازی در اختیار آنها قرار داده است توانسته‌اند از دیدگاه‌های مختلف در امر جمع‌آوری اطلاعات، بهتر عمل کنند. فضای مجازی به آنها اجازه می‌دهد راحت‌تر،

غیرمحسوس‌تر و با ضریب امنیتی بالاتری به هدف‌های خود دسترسی پیدا کنند و به خطر افتادن را کاهش دهند.

جمع‌آوری اطلاعات رایانه‌ای در فضای مجازی

امروزه شاید کمتر سازمان و اداره‌ای باشد که در فضای مجازی حضور نداشته و در این فضا از رایانه و شبکه‌های رایانه‌ای استفاده نکند. استفاده از رایانه به‌حدی مورد توجه قرار گرفته که یکی از شاخص‌های برخورداری از سواد در قرن حاضر را فراگیری علوم رایانه‌ای می‌دانند. همزمان با گسترش استفاده از رایانه و نرم‌افزارهای رایانه‌ای بین سطوح مختلف افراد جامعه، نرم‌افزارهای جاسوسی و ویروس‌های مخرب نیز گسترش یافته است؛ این نرم‌افزارها با انگیزه‌های متفاوتی ساخته می‌شوند و مورد استفاده قرار می‌گیرند. یکی از کاربردهای ویروس‌های رایانه‌ای و نرم‌افزارهای جاسوسی، استفاده از آنها در امور اطلاعاتی است. سازمان‌های اطلاعاتی با استفاده از نرم‌افزارهای جاسوسی مانند: تروجان‌ها، بک‌اوریفیس، اسپای‌ورها و... به رایانه‌های افراد نفوذ کرده و اطلاعات آنها را جمع‌آوری می‌نمایند. به‌عنوان مثال تروجان‌ها به‌عنوان یکی از ابزارهای جاسوسی رایانه‌ای، کاربردهای زیر را دارند: (سی.بونی، ال.کواسیچ ،۱۳۸۲ : ۱۸۲)

- برنامه‌هایی را که در سامانه‌ی رایانه‌ای قرار دارد از راه دور و بدون اینکه کاربر متوجه شود اجرا می‌نمایند
- فشار بر صفحه کلید را دریافت می‌کنند
- تصاویر صفحه نمایش را دریافت می‌کنند
- وب‌کم را خاموش و روشن می‌کنند
- برنامه‌ها را در رایانه هدف و بدون اطلاع کاربر نصب و اجرا می‌کنند
- می‌توانند میکروفن، دوربین، مودم و دیگر دستگاه‌های جانبی را متصل به رایانه را روشن و اطلاعات را استخراج کنند
- می‌توانند رایانه را از راه دور روشن کنند و محتوای آن را ذخیره و دوباره رایانه را خاموش کنند

همان‌طور که مشاهده می‌شود، پیشرفت فناوری، دسترسی غیرمحسوس و مؤثر

سازمان‌های اطلاعاتی دشمن را به اطلاعات رایانه‌ها ممکن کـرده اسـت. اسـتفاده از روش جمع‌آوری رایانه‌ای به‌گونه‌ای است که بدون داشتن کوچک‌ترین خطری برای سازمان‌های اطلاعاتی، آنها را به مقصودشان می‌رساند.

یکی دیگر از کارکردهایی که اینترنـت بـه‌عنـوان یـک فنـاوری جدیـد در اختیـار سازمان‌های اطلاعاتی دشمن قرار داده است، جمـع‌آوری اطلاعـات افـراد داوطلـب استخدام در این سازمان‌ها از طریق فرم‌های اینترنتـی ثبـت‌نـام اسـت، سـازمان‌هـای اطلاعاتی مانند: سـیا، موسـاد، آژانـس امنیـت ملـی، ام.آی۵ و... اقـدام بـه دریافـت اطلاعات از این طریق می‌کنند. در این روش، سازمان‌های اطلاعاتی با قرار دادن یک لینک با عنوان ارتباط با ما و الفاظ مشابه آن، اطلاعاتی را از فرد ماننـد: نـام و نشـان، آدرس کامل، شماره تلفن و آدرس پست الکترونیکی دریافت می‌کنند.

راهبری و هدایت جاسوسان در فضای مجازی

در گذشته، سازمان‌های اطلاعاتی با توجه به میزان توانایی علمی و فنی که داشتند از شیوه‌های مختلفی برای انتقال اطلاعات اسـتفاده مـی‌کردنـد. در اوایـل از جاسـازی، نامرئی‌نویسی و ناقل‌گذاری و سپس با پیشرفت فناوری، از دستگاه‌هـای رمزکننـده‌ی رادیویی و در نهایت از هواپیماها و با گسترش اینترنت از آن استفاده کردند.

امروزه توسعه‌ی فضای مجازی در بخش اینترنـت، کمـک شـایانی بـه ارتباطـات جاسوسی و راهبرد و هدایت آنان نموده است که نمونـه‌ای از ایـن نـوع جاسوسـی، قرارداد جاسوسی گوگل برای سازمان اطلاعات امریکا است. بر اساس مطالب منتشر شده در روزنامه‌ی واشنگتن پست، به‌نظر می‌رسد گوگل قراردادهای محرمانـه‌ای بـا دولت امریکا منعقد کرده تا خدمات جست‌وجو و یافتن اطلاعات در فضای مجازی را به این دولت ارائه کند. این نگرانی‌ها با توجه به رابطـه‌ی نزدیـک میـان گوگـل و تشکیلات امنیت ملی امریکا، به‌شدت افزایش می‌یابد.

واشنگتن پست افشا کرده که گوگل دارای یک مشتری خیلـی محرمانـه از دولـت امریکاست. به نوشته‌ی این روزنامه، بخش «اینترپرایـز سولوشـن» گوگـل، خـدمات جست‌وجو و محصولات مکان‌یابی مانند گوگل ارث و سازمان نقشـه گوگـل را در اختیار دولت فدرال و از جمله ارتش و جامعه‌ی اطلاعاتی امریکا قرار می‌دهد.

روش‌های نوین انتقال اطلاعات در فضای مجازی

ارتباطات ماهواره‌ای

ارتباطات ماهواره‌ای به‌گونه‌ای است که به جاسوسان اجازه می‌دهد در هر جایی و با هر کسی که بخواهند ارتباط برقرار کنند. به‌عبارتی ارتباطات اپتیکال ماهواره‌ای، مشکلات ناشی از ارتباطات باسیم و بیسیم کوته‌برد را رفع نموده و از طرفی امکان برقراری ارتباط با امنیت بالا را ایجاد کرده است و برخورداری از این نوع از ارتباطات برای نیروهای نظامی و انتظامی، افزایش میزان تبادل اطلاعات را در پی داشته است. به‌عنوان مثال: میزان تبادل اطلاعات در سال ۱۹۸۵ ، ١٦بیت در ثانیه بوده است اما میزان تبادل اطلاعات در جنگ عراق در سال ۲۰۰۱ در یگان‌های نظامی ۱/۵ مگابایت در ثانیه بوده است.

یکی از روش‌های قبلی انتقال اطلاعات و ارتباطات جاسوسی، استفاده از ناقل‌گذاری است که در این روش از ناقل‌های با روح و بی‌روح برای جاسازی و برداشت اطلاعات استفاده می‌شد. امروزه این روش با استفاده از فناوری‌های جدید صورت می‌گیرد. به‌عنوان مثال برای ارسال اطلاعات از روش ناقل‌گذاری بر اساس فناوری‌های نوین، این‌گونه عمل می‌شود: «جاسوس اطلاعات را در دستگاه فرستنده‌ی خود ذخیره کرده و به او گفته می‌شود در طول یک خیابان که از قبل برای او مشخص شده است مانند یک عابر به‌گونه‌ای که جلب توجه نکند قدم بزند و همزمان دستگاه فرستنده‌ی همراه خود را روشن کند. ناقل که در واقع یک دستگاه گیرنده و فرستنده‌ی رادیویی است، اطلاعات را از دستگاه فرستنده‌ی جاسوس دریافت نموده و اقدام به ارسال آن برای ماهواره‌ی جاسوسی می‌کند» این دستگاه می‌تواند در صندوق عقب یک ماشین پارک شده در خیابان و یا هر چیز دیگری قرار گیرد.

ارتباطات اینترنتی

ارتباطات اینترنتی یکی از شیوه‌های جدید ارتباطی است که در چند دهه‌ی اخیر مورد استفاده‌ی سازمان‌های اطلاعاتی قرار گرفته است. یکی از مزایای این نوع

ارتباط، سهولت و نیاز کم به امکانات است. در این روش، سازمان اطلاعاتی برای جاسوس، سامانه‌ای را طراحی می‌کند که وی می‌تواند از طریق آن سامانه، اطلاعات خود را به‌صورت آنلاین ارسال و همچنین پیام‌های سازمان اطلاعاتی را دریافت نماید. بدین ترتیب سازمان‌های اطلاعاتی بدون ارتباط حضوری و صرف هزینه‌های متداول برای انجام قرارهای اطلاعاتی، می‌توانند اطلاعات را دریافت و ارسال نمایند.

از دیگر کاربردهای ارتباطات اینترنتی که کمتر به آن پرداخته شده است، امکان ارتباط چهره‌به‌چهره بین رابط و جاسوس است. ابزارهای چت در اینترنت و استفاده از وب‌کم برای ملاقات دیداری از دور، این امکان را به رابط می‌دهد که بتواند جاسوس را از راه دور مورد روان‌کاوی قرار دهد و نوعی ارتباط حضوری با وی برقرار کند؛ این امر که با پیشرفت فناوری به‌دست آمده است، موجب جلوگیری از ایجاد فضایی عاطفی در برقراری ارتباط از راه دور می‌شود.

ارتباطات با استفاده از شیوه‌های مبتنی بر رمزنگاری و پوشیده‌نگاری

رمزنگاری دانش سری نوشتن است که به اصطلاح به آن «سایپوتوگرافی» گفته می‌شود. سامانه‌های رمزنگاری بسیار متنوع هستند و دلیل این نوع تنوع، پیشرفت فناوری است.

در واقع این سامانه‌ها به مرور زمان و با پدید آمدن روش‌های علمی و فناوری جدید، دچار تغییر شده‌اند و در نتیجه تنوع فراوانی در روش‌های رمزنگاری به‌وجود آمده است. روش‌های رمزنگاری قدیمی بر این اساس پایه‌گذاری شده بودند که اطلاعات برای فرد غیرمجاز (فردی که دسترسی به کلید رمز ندارد) غیرقابل فهم باشند اما با پدید آمدن رایانه‌ها و استفاده از امکانات آن، روش‌های پوشیده‌نگاری به‌وجود آمد که در آن موجودیت پیام رمز، مخفی نگه داشته می‌شود.

«استانوگرافی» فن ذخیره‌سازی و مبادله‌ی پنهانی اطلاعات است. در این روش، اطلاعات جاسوسی در قالب فایل‌های صوتی و تصویری رایانه‌ای مبادله می‌شود. با استفاده از این روش، اطلاعات را می‌توان با کدگذاری و جاگذاری در پیکسل‌های

تصویری به‌سهولت و با ایمنی بسیار بالا، از طریق اینترنت یا به روش‌های دیگر ذخیره‌سازی و منتقل کرد و آنها را با استفاده از برنامه‌های کدگشا، بازیابی و استخراج نمود (عباسی، ۱۳۸٤ :۸٤-۷۱). درباره‌ی اساس علمی این شیوه، می‌توان گفت که تمامی تصاویر از ترکیب سه رنگ اصلی قرمز، آبی و سبز ساخته شده‌اند. در این روش، ابتدا توسط برنامه‌ی کدگذار، اطلاعات از درون یک فایل ورودی به‌صورت بایت بایت خوانده می‌شود و سپس یک بیت از اطلاعات در رنگ سبز، یک بیت در رنگ قرمز و دو بیت در رنگ آبی جاگذاری می‌شود. به این ترتیب با توجه به این که هر بایت اطلاعات شامل هشت بیت است، در هر رنگ یک بایت اطلاعات ذخیره می‌شود. برای کدگشایی تصاویر نیز برنامه‌ای در نظر گرفته شده است که با توجه به الگوریتم کدگذاری، پیکسل‌های کد شده را شناسایی می‌کند و با استخراج و کنار هم گذاشتن بیت‌های مورد نظر، محل‌های اطلاعات رمز شده را استخراج می‌کند و از این روش می‌توان برای قرار دادن اطلاعاتی نظیر نامه‌های محرمانه، نتایج آزمون‌ها و اطلاعات شخصی روی اینترنت استفاده کرد. از مزایای این روش، تازگی، تنوع در به‌کارگیری و غیرمحسوس بودن اطلاعات، استفاده چندباره از یک تصویر برای مبادله‌ی اطلاعات و سادگی عمل است. با توجه به وجود میلیون‌ها تصویر در شبکه‌ی اینترنت، احتمال شناسایی تصویر حاوی اطلاعات توسط هکرها و سارقان اینترنتی بسیار ضعیف است؛ حتی اگر موفق به یافتن آن شوند تا زمانی که رمز آن را نداشته باشند قادر به بازیابی اطلاعات پوشیده‌نگاری شده، نخواهند شد (واحدی، نصر اصفهانی ،۱۳۹۱ : ۱۵۸).

یکی دیگر از تغییراتی که در شیوه‌های ارتباطی نامرئی‌نگاری ایجاد شده است، استفاده از کاربن‌های نامرئی‌نویسی است که مشکلات ناشی نامرئی‌نویسی گذشته از جمله بر جا ماندن رد قلم را از بین برده است.

تبادل اطلاعات و فضای مجازی

یکی از شاخص‌های موفقیت در سرنخ‌یابی، تبادل اطلاعات بین سازمان‌های اطلاعاتی است. سازمان‌های اطلاعاتی برای اینکه بتوانند از اطلاعات یکدیگر در

موضوع‌های مشترک استفاده کنند، می‌بایست بـه مثابـه‌ی یـک جامعـه‌ی یکپارچـه‌ی اطلاعاتی عمل کنند و این موضوع، برای ارتباطات سازمانی می‌تواند بسیار پرکـاربرد باشد.

به‌کارگیری ارتباطات و فناوری اطلاعات در فضای سایبر می‌تواند فضایی را برای سازمان‌های اطلاعاتی و ضداطلاعاتی ایجاد کند که در کمترین زمـان، بـه اطلاعـات یکدیگر دسترسی یابند. به‌وجود آمدن شـبکه‌هـای رایانـه‌ای و امکـان ارتبـاط و بـه اشتراک گذاشتن اطلاعات در نقاط مختلف، یکی از ابزارهـایی اسـت کـه مـی‌توانـد سازمان‌های اطلاعاتی را در دسترسی به این امر، یاری رساند. تبادل اطلاعات بـدین شکل قدرت تحرک سازمان‌های اطلاعاتی را در نقاطی که نیاز به اطلاعات تکمیلـی در آن ضروری است، بیشتر خواهد کرد (همان : ۱۵۹).

واپایش مظنونین و فضای مجازی

تغییر شیوه‌های جمع‌آوری اطلاعات و پیشرفت آنهـا و از طرفـی ایجـاد شـیوه‌هـای ارتباطی در فضای مجازی، تا حدودی باعث تغییر چهره‌ی مظنونین و به‌تبع آن تغییر شاخص‌های مظنونیـت شـده اسـت. امـروزه گسـترش ارتباطـات جاسوسـی ماننـد ارتباطات اینترنتی، ماهواره‌ای و ... فضایی جدید را در مقابل سازمان‌های جاسوسـی قرار داده است؛ شیوه‌های نوین ارتباطی در این فضا، از این‌رو می‌تواند یـک تهدیـد محسوب شود اما اگر از همـین شـیوه‌هـا بـرای تشـخیص مظنـونین اسـتفاده شـود، می‌تواند به‌عنوان یک فرصت نیز به‌کار آید. به‌عنوان مثال: FBI سازمان ضـداطلاعاتی امریکا اقدام به طراحی و راه‌اندازی سامانه‌ای به نـام «کـارنیوور» نمـوده اسـت؛ ایـن سامانه دارای یک برنامه‌ی نرم‌افزاری پیشرفته است کـه مـی‌توانـد حجـم عظیمـی از ارتباطات الکترونیکی را شنود کند. وقتی «کـارنیوور» روی یـک «آی‌اس‌پـی» نصـب مـی‌شـود، تمـام پسـت‌هـای الکترونیکـی ورودی و خروجـی را عکـس‌بـرداری و نشانی‌های پست الکترونیکی را بررسی می‌کند. بدین طریق FBI بـا اسـتفاده از ایـن سامانه می‌تواند مظنونین احتمالی را شناسایی کند (فریدل، ۱۳۸۲ : ۱۸۲).

تعقیب و مراقبت در فضای مجازی

بسیاری از شیوه‌های تعقیب و مراقبت قدیمی هنوز پرکاربرد است اما فضای مجازی

به کمک این شیوه‌ها آمده است. به‌عنوان مثال برای تعقیب یک خودرو علاوه بر استفاده از شیوه‌های قدیمی، می‌توان از یک فرستنده‌ی رادیویی یا سامانه‌ی GPS استفاده نمود. این امکانات جدید، باعث می‌شود کفایت عملیات بیشتر شود (واحدی، نصر اصفهانی، ۱۳۹۱ : ۱۶۰).

نرم‌افزارهای جاسوسی و راه‌کارهای پدافند غیرعامل برای مقابله با آنها

برخی اوقات که کاربران با اینترنت در حال کار هستند، ناگهان پنجره‌های مختلف بدون خواست کاربران باز می‌شود که در اصطلاح «پاپ ویندوز» نام دارند و کاربر باید وقت زیادی را برای بستن آنها صرف کند. نرم‌افزار جاسوسی هر نوع فناوری یا برنامه روی رایانه است که اطلاعات را به‌طور پنهانی جمع‌آوری می‌کند و سپس این داده‌ها به متقاضیان فروخته می‌شود. نوع اطلاعاتی که از رایانه‌های شخصی و یا کشور هدف جمع‌آوری می‌شود متفاوت است. بعضی نرم‌افزارهای جاسوسی، فقط اطلاعات خاصی از سامانه‌ها مانند نوع اتصال به اینترنت و سیستم‌عامل رایانه را ردیابی می‌کنند. برخی دیگر از نرم‌افزارهای جاسوسی، اطلاعات فردی را جمع‌آوری می‌کنند؛ مانند: ردگیری عادات و علائق فردی در هنگام کار با اینترنت. نرم‌افزارهای جاسوسی بدون رضایت و اجازه‌ی کاربر، نصب می‌شود؛ چنانچه به یک شرکت، اجازه‌ی جمع‌آوری داده را بدهید، دیگر نام این عمل جاسوسی نیست. بنابراین همیشه قبل از اجازه دادن، موارد افشای داده به‌صورت آنلاین را با دقت بخوانید. بعضی افراد به جاسوسی عمومی که گرایش‌های اینترنتی و نرم‌افزاری را ردگیری می‌کند تا جایی که اطلاعات مشخصه‌ی فردی را شامل نشود، اعتراضی ندارند اما بقیه به هر نوع داده‌ای که بدون اجازه از رایانه‌شان برداشته می‌شود معترض هستند. به هر حال، نرم‌افزار یا ابزاری که این اطلاعات را جمع‌آوری می‌کند، نرم‌افزار جاسوسی نامیده می‌شود.

نصب نرم‌افزار جاسوسی روی رایانه می‌تواند با مشاهده‌ی یک وب‌گاه، دیدن یک پست الکترونیکی به فرمت HTML یا با کلیک کردن یک پنجره باز شونده آغاز شود. از آنجا که روند دانلود اطلاع داده نمی‌شود؛ بنابراین کاربر از اینکه رایانه پذیرای یک نرم‌افزار جاسوسی شده است بی‌اطلاع خواهد ماند (واحدی، نصراصفهانی، ۱۳۹۱ :۱۶۰).

نرم‌افزارهای جاسوسی در فضای مجازی

قبل از ظهور نرم‌افزارهای جاسوسی، تبلیغ اینترنتی از طریق قرار دادن نشان‌هایی بود که در صفحات وب قابل مشاهده بود و کاربران با کلیک کردن روی آنها از اطلاعات یا خدمات ارائه شده، به دلخواه آگاهی می‌یافتند اما به‌تدریج کاربران از این نحو تبلیغ خسته شدند و به این ترتیب تبلیغ‌کنندگان در حال ورشکستگی بودند؛ زیرا میزان درآمد آنها با میزان کلیک از طرف بازدیدکنندگان بر تبلیغاتی بود که روی وب‌گاه خود قرار می‌دادند. (همان)

تبلیغ‌کنندگان دریافتند که اگر همچنان می‌خواهند از طریق اینترنت درآمد داشته باشند، مجبور به تغییر روش هستند. بسیاری از آنها دریافت خود را براساس میزان واقعی فروش قرار دادند. بقیه به راه‌های جدید تبلیغ فکر کردند. آنها به روشی تازه رسیدند که اجازه‌ی تبلیغ محصولات را بدون داشتن وب‌گاه می‌داد و به ترتیب نرم‌افزارهای جاسوسی پدید آمدند.

در ابتدا جاسوسی در دل برنامه‌های رایگان قرار می‌گرفت اما بعدها به ترفندهای دیگری رو آوردند و آن بهره‌گیری از سوءاستفاده‌های هکری برای نصب نرم‌افزار جاسوسی روی رایانه‌ها بود. اگر از سیستم‌های عامل رایج استفاده می‌کنید، شانس داشتن نرم‌افزار جاسوسی روی سامانه بیشتر است. به‌راحتی می‌توان ادعا کرد که بسیاری از کاربران خانگی روی رایانه خود جاسوس دارند.

تولید ویروس آسان است؛ با داشتن اطلاعات مختصری، می‌توان با بهره‌گیری از شکاف‌های امنیتی، باعث آشفتگی در شبکه‌ها و سامانه‌های استفاده‌کنندگان پست الکترونیکی شد. با مطالعه‌ی بعضی وب‌گاه‌ها، می‌توان با بعضی از شکاف‌های موجود در outlook و نحوه‌ی بهره‌گیری از آنها آشنا شد؛ حتی بعضی از کدها نیز در دسترس خواهد بود و با تغییرات اندکی می‌توان ویروسی تولید کنید که کدهای مورد نظر را اجرا کند. برای مثال می‌توان ویروسی تولید نمود که به‌محض باز کردن پست الکترونیکی توسط شخص قربانی، کدهای مورد نظر اجرا شوند. به این ترتیب تمام فایل‌های HTML آلوده می‌شوند و این ویروس به تمام آدرس‌های موجود در دفترچه‌ی آدرس سامانه آلوده شده فرستاده می‌شود. در اصل ویژگی کلیدی این

ویروس، اجرا شدن آن به‌محض باز شدن پست الکترونیکی حاوی HTML آسیب‌رسان است.

انواع نرم‌افزارهای جاسوسی

نرم افزار جاسوسی خانگی (Domestic Spyware)

نرم‌افزاری است که توسط صاحبان رایانه‌ها به‌منظور آگاهی یافتن از تأثیرهای اینترنت بر شبکه‌های رایانه‌ای خودشان خریداری و نصب می‌شود. مدیران از این نرم‌افزار برای آگاهی از فعالیت‌های آنلاین کارمندان استفاده می‌کنند. بعضی افراد نیز برای اطلاع از فعالیت‌های سایر اعضای خانواده، استفاده می‌کنند. مانند: مشاهده‌ی محتویات اتاق‌های گفت‌وگو توسط والدینی که کودکانشان در آنها شرکت می‌کنند.

یک شخص ثالث نیز می‌تواند نرم‌افزار جاسوسی را بدون آگاهی صاحب رایانه نصب کند. مجریان قانون از نرم‌افزارهای جاسوسی برای آگاهی یافتن از فعالیت مجرمانی استفاده می‌کنند که این مجرمان، خود از همین نرم‌افزارهای جاسوسی برای حصول اطلاعات از رایانه‌های شخصی به قصد دزدی دارایی‌ها استفاده کرده‌اند.

نرم افزار جاسوسی تجاری[1]

این نرم‌افزار که به‌عنوان Adware نیز شناخته می‌شود، نرم‌افزاری است که برای تعقیب فعالیت‌های وب‌گردی کاربران اینترنت استفاده می‌شود. اطلاعات حاصل از تعقیب فعالیت‌های وب‌گردی کاربران اینترنت، کاربردهای گوناگونی دارد. خریداران این‌گونه اطلاعات، سازمان‌های اطلاعاتی یا شرکت‌های بازاریاب هستند. یکی از مشتریان دائم این‌گونه اطلاعات، شرکت‌های بازاریاب هستند تا با بهره‌گیری از این اطلاعات، کاربران را با تبلیغات خاص، مورد هدف قرار دهند و از این طریق، علایق کاربران را به‌دست می‌آورند و تبلیغاتی را انجام می‌دهند که با علایق کاربران مطابقت داشته و بر آنها اثرگذار باشد.

به‌دست آوردن اطلاعاتی که علایق کاربران را نشان می‌دهد، موجب خوشحالی تبلیغ‌کنندگان می‌شود. در گذشته بازاریابان برای فهمیدن علایق افراد، باید آنها را از طریق برگزاری مسابقات یا موارد مشابه تطمیع می‌کردند. روش‌های قدیمی کسب

---

۱. Spyware Commercial

اطلاعات شخصی هنوز وجود دارد اما در آن روش‌ها، قدرت خواندن و اطلاع از سرنوشت از اطلاعات شخصی و پذیرفتن یا نپذیرفتن آنها توسط افراد وجود دارد. به هر حال، اطلاع از سلیقه‌ها به‌صورت پنهانی با استفاده از نرم‌افزارهای جاسوسی بسیار آسان شده است و تصویر کامل‌تری به صنعت بازاریابی ارائه می‌کند.

ثبت‌کنندگان نشانی‌های وب و صفحات نمایش

ثبت‌کنندگان نشانی‌های وب، وب‌گاه‌ها و صفحات دیده شده را ردیابی می‌کنند. ثبت‌کنندگان صفحه نمایش می‌توانند یک تصویری سیاه و سفید کوچک از صفحه‌ی پیش‌روی شما را در هر زمان بگیرند و این تصاویر را بدون اطلاع، ذخیره یا ارسال کنند. این روش‌ها برای جاسوسی‌های خانگی متداول است.

ثبت‌کنندگان چت و پست الکترونیکی

نرم‌افزار ثبت کننده یک رونوشت متنی از تمام پست‌های الکترونیکی وارد شونده و خارج شونده و چت‌ها تهیه می‌کند. یک جاسوس خانگی به کرات از این روش استفاده می‌کند.

ثبت‌کنندگان کلید وکلمات عبور

هنگامی که کاربر مشغول کار با رایانه است، یک نفر بالای سر وی ایستاده است و اعمال او را نظارت می‌کند. ثبت‌کننده‌ی کلمه‌ی عبور این کار را می‌کند؛ یعنی کلمه‌ی عبور تایپ شده را ردگیری می‌کند و تمام آنچه را که تایپ می‌شود، ثبت می‌کند.

حشرات وبی

حشرات وبی به‌عنوان جاسوسان تبلیغ کننده یا نرم‌افزارهای تبلیغ شناخته می‌شوند. هنگامی که چنین نرم‌افزاری روی رایانه است، بعد از انجام بعضی کارها، مانند: تایپ کردن عبارتی در موتور جست‌وجو، پنجره‌های باز شونده‌ی تبلیغاتی خاصی را مرتبط با عنوان‌های مورد جست‌وجو دریافت می‌کنند. این تبلیغات حتی گاهی می‌تواند زمانی که به اینترنت متصل نیستید بر صفحه ظاهر شود. اگر به‌طور پیوسته صفحات تبلیغاتی بیاید، نشان می‌دهد که به احتمال قوی یک حشره‌ی وبی روی رایانه نصب شده است.

مرورگر ربایان

بعضی افراد، رایانه‌ی دیگران را برای استفاده‌ی خودشان به خدمت می‌گیرند. کاربران نرم‌افزارهای جاسوسی می‌توانند مرورگر را برای ارسال اسپم‌هایشان از طریق خدمات‌دهنده‌ی اینترنت بربایند. به این معنی که یک اسپم‌ساز انگل می‌تواند هزاران پست الکترونیکی اسپمی را از طریق اتصال رایانه به اینترنت و آدرس پشتیبانی خدمات اینترنتی ارسال نماید.

دسترسی‌های باسرعت بالا به اینترنت، هدف این نوع کاربران قرار می‌گیرد. بیشتر قربانیان متوجه نمی‌شوند که از اعتبار آنها سوءاستفاده شده است تا به خاطر شکایت علیه اسپم‌ها، خدمات دهنده‌ی اینترنت اتصالشان را قطع کنند.

مودم ربایان

اگر برای اتصال به اینترنت از یک مودم و خط تلفن استفاده می‌شود، یک سوءاستفاده کننده ممکن است قادر باشد یک شماره‌گیر آنلاین برای برقراری یک اتصال جدید اینترنت روی رایانه نصب کند. این اتصال ممکن است یک اتصال از راه دور با هزینه‌ی بالا باشد. هنگامی که قبض تلفن دریافت می‌شود، شک به‌وجود خواهد آمد. این نرم‌افزارهای جاسوسی اغلب داخل اسپم و پست‌های الکترونیکی قرار گرفته و با بازکردن پست الکترونیکی می‌تواند به‌صورت سهوی باعث آغاز نصب شماره‌گیر شود. پیگیری این نوع سوءاستفاده کننده، کار آسانی نیست؛ زیرا آنها می‌دانند که قبض تلفن قبل از اینکه فرصت پیگیری باشد، پرداخت خواهد شد.

رایانه ربایان

رایانه ربایان میانبرهای اینترنتی را در پوشه‌های مطلوب کاربر بدون خبر دادن به وی قرار می‌دهند. این میانبرها باعث می‌شوند که بسیاری به‌طور اتفاقی از وب‌گاه‌شان بازدید نمایند و به این ترتیب به‌صورت مصنوعی آمار مراجعه به وب‌گاه خود را بالا ببرند. این اتفاق به آنها اجازه‌ی دریافت مبالغ بیشتری را از تبلیغات در وب‌گاه‌شان می‌دهد که هزینه‌ی پرداخت شده آن در واقع زمان و پهنای بازه‌ای است که از کاربران گرفته می‌شود. گاهی تنها راه خلاص شدن از شر این لینک‌های مزاحم، پاک

کردن آنها از داخل «ریجیستری» است. به هر حال ممکن است نرم‌افزار جاسوسی طوری طراحی شده باشد که با هر بار راه‌اندازی مجدد رایانه، خودش را در داخل «ریجیستری» قرار دهد. تنها اقدام پدافندغیرعامل، فرمت کردن «هارد» رایانه با استفاده از یک برنامه‌ی ضدجاسوسی بسیار قدرتمند است.

تروا‌ها و ویروس‌ها

اسب چوبی، پوششی بود که یونانیان برای ورود به شهر تروا استفاده کردند، نرم‌افزار تروا برای سوءاستفاده از رایانه‌ها، خود را به‌شکلی بی‌ضرر در می‌آورد. داده‌ی رایانه‌ای ممکن است رونوشت، توزیع یا تخریب شود.

ویروس نیز شبیه تروا عمل می‌کند، با این تفاوت که قدرت ایجاد شبیه خود را دارد تا باعث خسارت به رایانه‌های بیشتری شود. به هر حال هردوی این نرم‌افزارهای آسیب‌رسان می‌توانند تحت تعریف نرم‌افزار جاسوسی قرار بگیرند؛ زیرا کاربر از وجودشان بی‌اطلاع است و هدف واقعی آنان را نمی‌داند.

چند نمونه از شگردهای معمول مورد استفاده برای فریب دادن کاربران برای نصب نرم‌افزارهای جاسوسی

- باز کردن پست الکترونیکی اسپمی
- کلیک نمودن روی پنجره‌های بازشونده‌ی فریبنده
- دانلود رایگان برنامه‌ها، بازی‌ها، ابزارها و غیره
- برنامه‌های اشتراک فایل
- مشاهده‌ی وب‌گاه‌های غیراخلاقی و...
- نرم‌افزارهای اجرای فایل‌های صوتی و تصویری آنلاین

یکی از بزرگ‌ترین اشتباهاتی که کاربران انجام می‌دهند این است که قبل از شروع گشت‌وگذار در وب، تنظیمات سطح امنیتی خود را بسیار پایین انتخاب می‌کنند. سطح امنیتی پایین به برنامه‌های جاسوسی به‌سادگی اجازه‌ی ذخیره شدن در حافظه‌ی رایانه را می‌دهد.

اقدام‌های پدافند غیرعامل برای دور نگه داشتن نرم‌افزارهای جاسوسی

- تنظیم سطح امنیتی به سطح پیش گزیده یا بالاتر
- نظارت دقیق بر آنچه دانلود می‌کنید

- به‌روز نگه داشتن سیستم عامل رایانه
- نصب یک برنامه ضدجاسوسی؛ برنامه‌ی ضدجاسوسی، محل برنامه‌های جاسوسی را که بدون اطلاع وارد شده‌اند تعیین می‌کند؛ آنها را قرنطینه و سپس پاک می‌کند
- باید به احساس و غریزه رجوع شود؛ اگر منبعی آشنا یا قابل اعتماد به‌نظر نمی‌رسد، پست الکترونیکی را باز نکنید و وب‌گاه را نبینید. برنامه‌های مورد نیاز خود را از منبع قابل اعتماد دیگری دریافت کنید. گاهی وقت‌ها، برنامه‌های مجانی ارزش دردسر بعدی را ندارند! هنگامی که با یک پیشنهاد فریبنده برخوردید به انگیزه‌ی آن دقت کنید. چرا یک نفر می‌خواهد به‌روزرسانی مرتب و مجانی ارائه دهد؟! دنبالش نروید.
- از تجربه‌های دیگران برای فهمیدن اینکه کدام نرم‌افزارها درون خود به برنامه‌های جاسوسی پناه داده‌اند استفاده کنید. در عرض چند ثانیه می‌توانید جست‌وجویی انجام دهید تا بفهمید دیگران در مورد نرم‌افزارهای اجرای فایل‌های صوتی و تصویری آنلاین چه می‌گویند.

نکته: نرم‌افزارهای ضدویروس به‌تنهایی برای محافظت در مقابل حمله‌ی ویروس‌های رایانه‌ای فعلی و آینده کافی نیست. علاوه بر این، گاهی به ابزارهای قوی‌تر برای بررسی محتوای پست‌های الکترونیکی و فایل‌های ناشناس برای حفاظت در مقابل حملات و ویروس‌های آن (منظور از ویروس پست الکترونیکی، ویروسی است که از طریق پست الکترونیکی گسترش می یابد) و جلوگیری از نشت اطلاعات نیاز است.

پدافند غیرعامل با رویکرد پیشگیرانه برای حفاظت فضای مجازی

در این روش، محتوای تمام پست‌های الکترونیکی وارد شونده و خارج شونده قبل از رسیدن به کاربران، در سطح سرور بررسی می‌شود. به این ترتیب تمام محتوای مضر از پست الکترونیکی آلوده حذف شده و سپس به کاربر فرستاده می‌شود. ناجا با نصب یک فیلتر جامع برای بررسی محتوای پست‌های الکترونیکی و یک دروازه‌ی ضدویروس روی خدمات‌دهنده‌ی پست الکترونیکی، می‌تواند در مقابل

آسیب‌رسانی‌های بالقوه و از بین رفتن زمان مفید کار توسط ویروس‌های فعلی و آینده، خود را محافظت کند.

قابلیت‌های یک فیلتر خوب برای جلوگیری از آلوده شدن خدمات دهنده (سرور) پست الکترونیکی توسط ویروس‌های پست الکترونیکی به‌شرح زیر است:

- بررسی محتوای پست الکترونیکی
- کشف بهره‌برداری‌ها از شکاف‌های امنیتی
- تحلیل خطرها
- راه‌حل‌های ضدویروسی

نتیجه‌گیری

پیشرفت فناوری، دسترسی غیرمحسوس و مؤثر سازمان‌های اطلاعاتی دشمن را به اطلاعات رایانه‌ها ممکن کرده است. استفاده از روش جمع‌آوری رایانه‌ای به‌گونه‌ای است که بدون داشتن کوچک‌ترین خطری برای سازمان‌های اطلاعاتی، آنها را به مقصودشان می‌رساند.

تغییر شیوه‌های جمع‌آوری اطلاعات و پیشرفت آنها و از طرفی ایجاد شیوه‌های ارتباطی در فضای مجازی، تا حدودی باعث تغییر چهره‌ی مظنونین و به‌تبع آن تغییر شاخص‌های مظنونیت شده است. امروزه گسترش ارتباطات جاسوسی مانند: ارتباطات اینترنتی، ماهواره‌ای و ... فضایی جدید را در مقابل سازمان‌های جاسوسی قرار داده است. شیوه‌های نوین ارتباطی در این فضا به این دلیل می‌تواند یک تهدید محسوب شود اما اگر از همین شیوه‌ها برای تشخیص مظنونین استفاده شود، می‌تواند به‌عنوان یک فرصت نیز به‌کار آید. به عنوان مثال: FBI سازمان ضداطلاعاتی امریکا، اقدام به طراحی و راه‌اندازی سامانه‌ای به نام «کارنیوور» نموده است.

رشد قارچ‌گونه‌ی جرایم در حوزه‌ی فضای تولید و تبادل اطلاعات، مثل کلاهبرداری‌های اینترنتی، جعل داده‌ها و عنوان‌ها، سرقت اطلاعات، تجاوز به حریم خصوصی اشخاص و گروه‌ها، هک و نفوذ به سامانه‌های رایانه‌ای و اینترنتی، هرزه‌نگاری و جاسوسی شبکه‌ای ایجاب می‌کند که سازمان‌های نظامی و انتظامی، به

امنیت و حفاظت از اطلاعات خود در فضای مجازی اهمیت داده و به این مهم، با دیدی حرفه‌ای و تخصصی بنگرند. همچنین با توجه به تصویب قانون جرایم رایانه‌ای در مجلس شورای اسلامی و لزوم تعیین ضوابط قضایی برای این قانون و نیز مصوبه‌های کمیسیون فتای جمهوری اسلامی ایران مبنی بر تشکیل پلیس فضای تبادل اطلاعات، این پلیس در بهمن ماه سال ۱۳۸۹ به دستور فرمانده‌ی محترم ناجا تشکیل شد (کوچی،۱۳۹۳ : ١٦٤).

پیشنهادها

با عنایت به اهمیت و نقش به‌سزای پدافند غیرعامل برای مقابله با جاسوسی در فضای تولید و تبادل اطلاعات، موارد زیر توسط محقق پیشنهاد می‌شود و پیوسته باید مدنظر کاربران و مدیران و فرماندهان ناجا باشد :

۱. استفاده از چندین موتور ضدویروس برای بالا بردن نرخ کشف ویروس و پاسخ سریع‌تر به ویروس جدید
۲. بررسی پیوست‌های پست الکترونیکی در سامانه‌ی اینترنت ناجا برای مصونیت در مقابله ضمیمه‌های خطرناک
۳. ایجاد یک سپر در مقابل شکاف‌های امنیتی برای محافظت در برابر ویروس‌های فعلی و آتی بر پایه‌ی شکاف‌های امنیتی
٤. به‌کارگیری یک موتور بررسی خطرها HTML با توان بالا در سرور مرکزی ناجا
۵. طراحی یک پویش‌گر تروا‌ها و فایل‌های اجرایی برای کشف فایل‌های اجرایی آسیب‌رسان و نصب در سرورهای مرکزی معاونت‌های مستقل ناجا
٦. آموزش کاربردی کارکنان ناجا در خصوص باز نکردن پست‌های الکترونیکی ناشناخته
۷. دریافت بازخورد از کاربران، مدیران و کارکنان فنی توسط امنیت فاوا
۸. به‌روزرسانی روش‌های امنیتی توسط امنیت فاوا
۹. به‌روزرسانی سامانه‌های حفاظت و مراقبت اطلاعات، متناسب با پیشرفت فناوری‌های جاسوسی و کسب اطلاعات لازم

منابع و مآخذ

- آلمژان، پیر (۱۳٦۹)، «**جاسوسی و ضدجاسوسی**»، ترجمه ابوالحسن سروقدم، مشهد: مؤسسه چاپ و انتشارات آستان قدس رضوی.
- سروری، اسدا.. (۱۳۹۲)، «**پدافند غیرعامل**»، دانشگاه علوم انتظامی امین.
- سی.بونی؛ ویلیام، ال؛ کواسیچ، جرالد (۱۳۸۲)، «**جاسوسی شبکه‌ای**»، ترجمه معاونت پژوهشی دانشکده امام باقر(ع)، تهران، انتشارات دانشکده امام باقر(ع).
- عباسی، محمد (۱۳۸٤)، «**پنهان‌سازی اطلاعات با شیوه‌ی استگانوگرافی**»، امنیت پژوهی، شماره ۱۱.
- فریدل، ران (۱۳۸۲)، «**دنیای مدرن جاسوسی**»، ترجمه معاونت پژوهشی دانشکده امام باقر(ع)، تهران، انتشارات دانشکده امام باقر (ع).
- کوچی، سعید (۱۳۹۳)، «**جایگاه امنیت در فضای سایبر**»، فصلنامه مطالعات حفاظت و امنیت، شماره۳۱.
- واحدی، مرتضی؛ نصراصفهانی، مجید (۱۳۹۱)، «**پدافند غیرعامل و امنیت در فضای سایبر**»، دانشکده فارابی ارتش.
- یحیایی، ابراهیم؛ حیدری، محمد؛ اشراقی، امیر (۱۳۸۲)، «**حقایقی از جنگ سلطه و سقوط صدام**»، تهران : انتشارات دافوس آجا.