بسم الله الرحمن الرحیم

پاپسا

شماره هفتم، بهمن ماه ۱۳۹۳

پایگاه اطلاع رسانی پدافند سایبری ایران

صاحب امتیاز:

سازمان پدافند غیرعامل کشور

قرارگاه پدافند سایبری کشور

تولید و نشر:

موسسه سایبربان

فهرست مطالب

مقدمه

در حال حاضر، بخش عمده ای از فعالیت ها و تعاملات اقتصادی، تجاری، فرهنگی، اجتماعی و حاکمیتی کشور، در کلیه سطوح، اعم از افراد، موسسات غیر دولتی و نهاد های دولتی و حاکمیتی، در فضای سایبر انجام میگیرد. زیر ساخت ها و سامانه های حیاتی و حساس کشور ، یا خود، بخشی از فضای سایبری کشور را تشکیل میدهند و یا از طریق این فضا، کنترل، مدیریت و بهره برداری میشوند و عمده اطلاعات حیاتی و حساس کشور نیز، به این فضا منتقل و یا اساساً در این فضا، شکل گرفته است. عمده فعالیت های رسانه ای به این فضا منتقل شده، بیشتر مبادلات مالی از طریق این فضا انجام میگیرد و نسبت قابل توجهی از وقت و فعالیت های شهروندان، صرف تعامل در این حوزه میگردد. سهم درآمد حاصل از کسب و کار های فضای سایبر در تولید ناخالص ملی افزایش چشمگیر یافته و از میان شاخص های تعیین شده برای سنجش میزان توسعه یافتگی کشور، شاخص های حوزه سایبر، سهم عمده ای را به خود اختصاص داده اند. بخش قابل توجهی از سرمایه های مادی و معنوی کشور، صرف این حوزه شده و بخش قابل توجهی از درآمد های مادی و اکتسابات معنوی شهروندان نیز از این حوزه کسب شده و یا تاثیر عمده می پذیرد. به عبارت دیگر، وجوه مختلف زندگی شهروندان، به معنای واقعی، با این فضا درآمیخته و هر گونه بی ثباتی، نا امنی و چالش در این حوزه، مستقیماً وجوه مختلف زندگی شهروندان را متاثر خواهد نمود.

بررسی سوابق جنگ ها و انقلاب های مخملی شکل گرفته طی دو دهه اخیر، در کشور های مختلف، که منجر به براندازی حکومت ها و نابودی منابع و زیر ساخت های آن شده است، بیانگر این واقعیت است که عمده این جنگ ها و انقلاب ها، با یک جنگ سایبری شروع و یا حمایت شده است.

مروری بر وقایع و حوادث سال های اخیر کشور، مؤید این واقعیت است که بخش عمده ای از تهدید های موجود علیه کشور، به ویژه در زیر ساخت های حیاتی، یا مستقیماً از فضای سایبر نشأت می گیرند و یا این فضا را هدف تهدید مستقیم خود قرار می دهند. بنابراین:

با توجه به آسیب پذیری های ذاتی موجود در فضای سایبری و روند رو به رشد مهاجرت از دنیای سنتی به این فضا، ریسک سامانه های مبتنی بر فناوری اطلاعات، که برای اقتصاد کشور حیاتی میباشند، را افزایش میدهد.

پیچیدگی روز افزون و رو به ازدیاد سامانه ها و شبکه های مبتنی بر فناوری اطلاعات چالش های امنیتی را برای کشور در بر دارد.

بر این اساس ارتقاء پایداری عملیاتی و امنیت و مصون سازی زیر ساخت ها به ویژه مراکز حیاتی و حساس برای کشور بسیار حائز اهمیت تلقی میشود.

چشم انداز پدافند سایبری کشور

با یاری خداوند قادر متعال، «جمهوری اسلامی ایران در افق ۱۴۰۴»، دست یافته به زیست بوم ملی سایبری امن، مصون و پایدار در برابر تهدیدات و حملات سایبری دشمن و قدرت برتر پدافند سایبری در بین کشورهای منطقه و دارای جایگاهی ممتاز[1] در جهان با ویژگی های زیر می باشد:

برخوردار از:

۱. نظام جامع بومی پدافند سایبری هوشمند، پایدار و مقاوم، انحصاری، ابتکاری، ، لایه به لایه، پیش کنش گر، شبکه ای، چابک و منعطف در سطوح ملی، دستگاهی و استانی

۲. نظام فرماندهی و کنترل جامع و هوشمند با قابلیت رصد، پایش، تشخیص، هشدار و فرماندهی و کنترل به هنگام صحنه عملیات پدافند سایبری

۳. مصونیت در زیرساخت های حیاتی، استحکام و پایداری در زیر ساخت های حساس و امنیت و ایمنی در زیر ساخت های مهم

۴. سرمایه های انسانی مؤمن، متعهد ، مجرب، آموزش دیده و متخصص در حوزه پدافند سایبری و دارای تفکر بسیجی و روحیه جهادی

۵. نظام دیپلماسی پدافند سایبری فعال، متعامل، مشارکت جو و مدافع منافع ملی سایبری

[1] : منظور از جایگاه ممتاز در جهان: قدرت اول الی پنجمی جهان می باشد.

ارزش‌های اساسی حاکم بر حوزه پدافند سایبری کشور

۱ خودباوری و خوداتکایی

بر اساس تعالیم عالیه اسلام و فرمایشات حضرات معصومین(علیهم السلام)، همچنین با توجه به تدابیر رهبر کبیر انقلاب اسلامی ایران و خلف صالح ایشان، مقام معظم رهبری، ملت ایران می تواند با توکل به ذات لایزال الهی و با شناخت، باور و تکیه بر توانمندی های ارزنده خود، در بسیاری از موارد به خوداتکایی دست یابد تا به سرعت وابستگی خود را به بیگانگان به حداقل برساند.

۲ اعتماد سازی، اطمینان بخشی

اقدامات کشور در حوزه پدافند سایبری باید در راستای جلب اعتماد عمومی و ایجاد اطمینان خاطر در قلوب مردم باشد. این دو عامل نقشی کلیدی در توفیق مجموعه فعالیت های این حوزه دارند. جلب اعتماد عمومی و ایجاد اطمینان قلبی از نتایج حاصل از اقدامات پدافند سایبری امری ضروری و اجتناب ناپذیر است.

۳ نوآوری و خلاقیت

با توجه به بهره گیری فضای سایبری از دانش ها و فناوری های نوین و پیچیده ترشدن امکانات سخت افزاری و نرم افزاری این فضا، لازمه مصون سازی و امنیت بخشی به زیرساخت های حیاتی و حساس کشور، برخورداری از توان نوآوری، ابتکار و خلاقیت در تمامی سطوح نیروی انسانی این حوزه می باشد.

۴ رعایت اخلاق اسلامی

لازمه کار در حوزه پیچیده و گسترده سایبری، که معمولاً با برتری نسبی کشورهای متخاصم همراه است، برخورداری نیروی انسانی در سطوح مختلف از ارزش های والای انسانی-اسلامی از قبیل ایمان، صداقت، سلامت، تعهد، امانت، رازداری، سلحشوری، التزام به مبانی اعتقادی اسلام ناب محمدی و تفکر بسیجی می باشد

اخبار

استقرار هکرهای کره شمالی در یکی از شهرهای چین

یکی از اساتید علوم رایانه کره شمالی که از این کشور متواری شده است، ادعا می‌کند که « اداره ۱۲۱» کره شمالی، در یکی از شهرهای کشور چین، به انجام عملیات سایبری خود مشغول است.

کیم هیونگ وانگ (Kim Heung-Kwang) ، استاد علوم رایانه که در سال ۲۰۰۴ از کره شمالی به کره جنوبی پناهنده شده است، در مصاحبه با خبرگزاری CNN اعلام کرد که شبکه مخفی ۱۲۱ کره شمالی، در اواخر دهه ۹۰ میلادی در یکی از شهرهای کشور چین دایر شده است، اما تا سال ۲۰۰۵ هیچ گونه عملیات سایبری از این ارتش در مقیاس بزرگ انجام نشده است.

در اوایل ژانویه وزارت دفاع کره جنوبی اعلام داشت که کره شمالی تعداد سربازان ارتش سایبری خود را به شش هزار نفر افزایش داده است. این ارتش که با نام «اداره ۱۲۱» معرفی شده، سال‌ها است در جنگ سایبری سرمایه‌گذاری کرده و اعضای آن از حرفه‌ای‌ترین متخصصان رایانه این کشور تشکیل شده اند.

وانگ ادعا می‌کند شهر شن‌یانگ (SHENYANG) در نزدیکی مرز کره شمالی و چین، دارای یک زیرساخت اینترنتی مناسب است و برای اهداف سایبری ارتش ۱۲۱ کره شمالی در نظر گرفته شده است. بسیاری از کارشناسان امنیتی ادعا می‌کنند که کره شمالی بیشترین ترافیک اتصال به اینترنت خود را از طریق کشور چین دریافت کند.

وی در ادامه افزود اهداف اصلی هکرهای گروه ۱۲۱، کشورهایی مانند ایالات متحده آمریکا، کره جنوبی و ژاپن می باشند که همواره در روابط دیپلماتیک خود با کره شمالی مشکل دارند.

کشور کره جنوبی در همراهی با دولت‌های غربی، بر این باور است که حملات سایبری اخیر به شرکت سونی پیکچرز، توسط هکرهای دولتی کره شمالی صورت پذیرفته است. همچنین مقامات کره جنوبی ادعا می‌کنند حمله سایبری به سامانه‌های رایانه‌ای بانک‌های این کشور در سال ۲۰۱۳ نیز توسط کره شمالی صورت گرفته است.

علت اصلی هک شدن جی پی مورگان مشخص شد

پس از گذشت ماه‌ها از سرقت اطلاعاتی بانک جی پی مورگان، مشخص شد که هکرها از بدافزارهای مخرب و پیچیده استفاده نکرده‌اند.

در اوایل سال جاری خبرگزاری‌های ایالات متحده اعلام کردند که گروهی از هکرهای ناشناس توانستند با نفوذ به سرورهای بانک جی پی مورگان، میلیون‌ها داده سپرده‌گذاران این بانک بزرگ را به سرقت ببرند. در حال حاضر محققان امنیتی پس از ماه‌ها تلاش و بررسی این حمله سایبری، متوجه شدند که این سرقت اطلاعاتی از طریق بدافزارهای پیچیده انجام نشده است.

به گزارش نیویورک تایمز، یکی از شعبه‌های اصلی این بانک در زمینه به روز رسانی یکی از سرورهای خود با احراز هویت دو عاملی کوتاهی کرده و همین موضوع علت اصلی این حادثه بیان شده است.

در ادامه این گزارش هک شدن بانک جی پی مورگان با هک اخیر شرکت سونی مقایسه و عنوان شده است که شرکت سونی توسط بدافزارهای پیچیده و خطرناکی هک گردیده، اما بانک مذکور تنها به دلیل کوتاهی مسئولان امنیتی در امر به روز رسانی، خسارت هنگفتی را متحمل شده است.

نیویورک تایمز ادعا می‌کند مقامات بانک جی پی مورگان با صرف هزینه‌ای معادل ۲۵۰ میلیون دلار، تلاش کردند تا امنیت سایبری

خود را بالا ببرند و رضایت مشتریان خود را بدست آورند، اما نه تنها این موضوع تاثیر گذار نبوده، بلکه با از دست دادن اعتبار خود نزد مشتریان، خسارات مالی فراوانی به این بانک وارد شده است.

یک گروه از محققان، متشکل از کارشناسان امنیت سایبری و عوامل آژانس امنیت ملی آمریکا (NSA)، برای شناسایی عوامل این حمله سایبری در تلاش می‌باشند. مقامات ایالات متحده ادعا می‌کنند که دولت روسیه به دلیل تحریم‌های اقتصادی آمریکا علیه این کشور، در این حملات نقش دارد.

بانک جی پی مورگان مدعی است که این حمله هیچگونه سرقت مالی را به همراه نداشته ولی کلمات عبور، شماره تلفن و اطلاعات شخصی مشتریان به سرقت رفته است.

هک شدن حساب‌های فیس‌بوک توسط آسیب پذیری خطرناک در اندروید

محققان آسیب پذیری امنیتی خطرناکی را در مرورگر وب سیستم عامل Android 4.4 و نسخه های قدیمی‌تر شناسایی کرده‌اند که به مهاجم اجازه می‌دهد تا SOP را دور بزند.

SOP یا همان Same Origin Policy، مفهوم مهمی در مدل امنیت نرم افزار وب است. آسیب پذیری SOP اندروید که با شناسه CVE-2014-6041شناخته می‌شود، اولین بار در ابتدای ماه سپتامبر و توسط یک محقق امنیتی با نام رافای بالوچ (Rafay Baloch) شناسایی شد. وی متوجه شد که مرورگر AOSP نصب شده بر روی اندروید ۴,۲,۱، که در حقیقت پلتفرم متن باز اندروید می‌باشد، به حفره امنیتی SOP آسیب پذیر است و به یک وب سایت مخرب اجازه می‌دهد تا به سرقت اطلاعات کاربران بپردازد.

محققان امنیتی شرکت امنیتی ترند میکرو در همکاری با محققان فیس بوک متوجه شدند که بسیاری از کاربران فیس بوک، مورد حملات سایبری قرار گرفته‌اند که توسط این حفره امنیتی خاص در مرورگر وب به اجرا در می‌آیند.

SOP در واقع برای جلوگیری از صفحات بارگذاری شده‌ای طراحی شده است که بخشی از اطلاعات منابع خود را ندارند. همچنین این مدل امنیتی نرم افزار وب، تضمین می‌کند که هیچ شخص ثالثی نمی‌تواند کدی را بدون اجازه صاحب سایت تزریق کند.

اما متاسفانه SOP ، قربانی آسیب پذیری «کراس سایت اسکریپتینگ» شده است که در نسخه‌های قدیمی‌تر گوشی‌های هوشمند اندرویدی به اجرا در می‌آید و به مهاجمان کمک می کند تا یک فایل جاوا اسکریپت مخرب ذخیره شده در حساب ذخیره سازی ابری قربانیان را به کار گیرند.

در این حمله خاص، یک لینک با استفاده از یک صفحه فیس بوک خاص به کار گرفته می‌شود و کاربران فیس بوک را به یک وب سایت مخرب متصل می‌کند.

کد جاوا اسکریپت به مهاجم اجازه می‌دهد تا وظایف مختلفی را در حساب فیس بوک قربانی به انجام برساند. بررسی محققان نشان می‌دهد هکرها با استفاده از کد جاوا اسکریپت، توانایی انجام هر کاری را در حساب هک شده فیس بوک کاربر را دارند. برخی از این فعالیت‌ها عبارتند از: اضافه کردن دوستان، Like کردن و دنبال کردن هر صفحه فیس بوک، اصلاح اشتراک‌ها و سرقت نشانه دسترسی به قربانی و ارسال آنها به سرور خود.

محققان ترند میکرو و فیس بوک در تلاش هستند تا عوامل این حمله سایبری را شناسایی کنند و از حملات احتمالی بر روی نسخه‌های جدیدتر اندروید جلوگیری نمایند.

هک کردن دستگاه های NAS توسط بدافزار SHELLSHOCK

محققان امنیتی به تازگی بدافزار مخربی را شناسایی کرده‌اند که برای کاشت درب‌های پشتی (**Backdoors**) در شبکه متصل به سیستم‌های ذخیره سازی **NAS** طراحی شده است. این دستگاه ها توسط کشور تایوان ساخته شده و گفته می‌شود که بدافزار مذکور دسترسی کامل به مطالب این دستگاه‌ها را دارا می‌باشد.

به گفته محققان امنیتی موسسه **Sans**، این بدافزار با سوء استفاده از آسیب پذیری معروف **GNU Bash** که با عنوان **ShellShock** نیز شناخته می‌شود، در دستگاه‌های **QNAP** به کار گرفته می شود. لازم به ذکر است که سیستم عامل به کار گرفته شده در این دستگاه‌ها لینوکس است.

یوهانس اولریش، مدیر موسسه **SANS** ، در وبلاگ خود نوشت: « این حمله یک اسکریپت **QNAP CGI** را هدف قرار داده و برای اجرای **Shellshock** در دستگاه های **QNAP** در نظر گرفته شده است. این اسکریپت، بدون احراز هویت قابل دسترس است و سپس یک اسکریپت پوسته ساده را راه اندازی می‌کند که قابلیت دانلود و اجرای بدافزارهای مخرب اضافی را دارد.

آسیب پذیری **Shellshock**، در میان آسیب پذیری‌های مهم و جدی اینترنت قرار می گیرد که در سال جاری میلادی شناسایی شد و به عنوان آسیب پذیری در **Bash**، بسیاری از سیستم های لینوکس، یونیکس و حتی **XP** را تحت تاثیر قرار داد. این حفره امنیتی یک اشکال عمده در **GNU Bash** است که به مهاجمان توانایی اجرای دستورات پوسته (**shell**) در سیستم های آسیب پذیر با استفاده از متغیرهای خاص و دستکاری شده را می‌دهد.

استقبال ژاپن از رفتار آمریکا با کره شمالی

به گزارش خبر گزاری کیودو، فومیو کیشیدا وزیر امور خارجه ژاپن، از رفتار آمریکا با کره شمالی در موضوع حمله سایبری به شرکت سونی پیکچرز استقبال کرد.

حملات سایبری به مجموعه سونی خسارات زیادی را به بخش‌های مختلف سونی وارد کرده است. این حملات در پی ساخت یک فیلم کمدی به نام «مصاحبه» توسط شرکت آمریکایی سونی پیکچرز اینترتینمنت (Sony Pictures Entertainment) آغاز شد. سونی پیکچرز هدف اصلی این حملات بود اما تقریباً هر شرکت یا موجودیت تجاری که نامی از سونی در خود داشت قربانی حملات شد؛ از پلی‌استیشن گرفته تا گوشی‌های هوشمند اکسپریا در لیست قربانیان حملات حضور دارند. از اولین روزهای حملات، دولت آمریکا، کره شمالی را در این زمینه مقصر می‌دانست زیرا موضوع این کمدی هالیوودی، ترور رهبر کره شمالی است. سازمان تحقیقات فدرال آمریکا (FBI) در گزارشی که کارشناسان آن را از دلایل قابل قبول فنی خالی می‌دانستند، اعلام کرد کره شمالی عامل حملات سایبری به مجموعه سونی است.

این رویدادها تا تهدید سالن‌های سینمایی که قصد داشتند فیلم «مصاحبه» را به نمایش بگذارند، یادآوری حملات ۱۱ سپتامبر، و لغو اکران پیش رفت. کره شمالی همواره اتهام‌ها در مورد هک سونی را رد می‌کند. پیونگ یانگ حتی پیشنهاد داده بود برای بررسی حملات به سونی، گروه تحقیقاتی مشترک تشکیل شود. باراک اوباما در نطق پایان سال ۲۰۱۴ از سونی به خاطر لغو اکران این فیلم انتقاد و اعلام کرد کره شمالی باید منتظر عواقب این حملات باشد.

بسیاری از کارشناسان امنیت رایانه معتقدند پیونگ یانگ از ظرفیت لازم برای انجام چنین حملاتی برخوردار نیست. به باور برخی کارشناسان و مقامات سیاسی روسیه و چین عوامل احتمالی حملات هستند.

در روزهای اخیر دولت آمریکا تحریم‌های جدیدی بر ضد کره شمالی وضع کرد که خشم مقامات این کشور را در پی داشت.

فومیو کیشیدا وزیر امور خارجه ژاپن، از رفتار آمریکا با کره شمالی در موضوع حمله سایبری به شرکت سونی پیکچرز استقبال کرد. در مکالمه تلفنی فومیو کیشیدا و جان کری در ۶ ژانویه، دو طرف در خصوص همکاری و واکنش در زمینه حمله سایبری به سونی به توافق رسیدند.

چین به دنبال قطع ارتباط کامل با گوگل

دولت چین تلاش می‌کند تا حضور گوگل در این کشور را از بین ببرد و حتی بازار این غول اینترنتی در جهان را تضعیف کند.

دولت چین در اقدام جدید خود علیه گوگل، جیمیل را برای کاربران خود مسدود کرد.

به گزارش خبرگزاری رویترز، وب سایت GreatFire.org که توسط گروه‌های مدافع آزادی بیان در چین فعالیت می‌کند اعلام کردند که تعداد زیادی از آدرس‌های فعال وب جیمیل در چین قطع شده است.

در همین ارتباط یکی از اعضای GreatFire.org اعلام کرد: «من فکر می‌کنم دولت چین تلاش می‌کند تا حضور بیشتر گوگل در این کشور را از بین ببرد و حتی بازار این غول اینترنتی در خارج از کشور را نیز ضعیف کند.» وی در ادامه افزود: «

تصور کنید که کاربران جیمیل دیگر با کاربران چینی در ارتباط نباشند. به همین دلیل بسیاری از مردم در خارج از چین مجبور خواهند شد تا به جای استفاده از جیمیل، از سرویس‌های دیگر استفاده نمایند.»

گزارش شفافیت گوگل نیز نشان می‌دهد که ترافیک خدمات این شرکت در کشور چین، با افت شدیدی مواجه شده است.

چین کنترل شدیدی را بر روی اینترنت به اجرا در آورده است و البته هیچ نشانه ای از مخالفت مردم این کشور با دولت در این زمینه وجود ندارد. کشور چین دارای پیچیده‌ترین مکانیسم سانسور اینترنت در جهان است، سیستمی که با عنوان فایروال بزرگ چین شناخته می‌شود.

چین متهم به نصب درب پشتی در گوشی‌های اندرویدی

تولید کنندگان گوشی‌های هوشمند در چین، بارها به دلیل نصب درب‌های پشتی در محصولات خود مورد انتقاد قرار گرفته اند.

مدل‌های محبوب گوشی‌های هوشمند چینی، از جمله Xiaomi و Star N9500، از جمله سازندگان تلفن همراه هستند که همواره در لیست اتهام مقامات آمریکایی قرار دارند. در حال حاضر، ششمین شرکت تولید کننده تلفن‌های هوشمند در سراسر جهان، با نام Coolpad نیز به این لیست پیوسته است.

یک شرکت امنیتی در ایالات متحده در گزارشی، شرکت Coolpad را متهم به جاسوسی از کاربران چینی کرده است. مقامات این شرکت ادعا می‌کنند میلیون‌ها گوشی اندرویدی ساخت شرکت Coolpad، از همان آغاز تولید شامل درب‌های پشتی بودند که قادر به ردیابی کاربران، ارائه تبلیغات ناخواسته و نصب برنامه‌های غیر مجاز بر روی گوشی بدون اطلاع کاربران خود هستند.

محققان امنیتی شرکت پالو آلتو Palo Alto Networks اعلام کردند درب پشتی را با نام «CoolReaper» شناسایی کرده اند که از پیش بر روی دستگاه‌های اندرویدی Coolpad نصب شده و عمدتاً در کشورهای چین و تایوان به فروش می‌رسند. CoolReaper به مهاجمان اجازه می‌دهد تا به طور کامل اطلاعات کاربران را به سرقت ببرند.

گفته می‌شود این درب پشتی، حریم خصوصی بیش از ۱۰ میلیون کاربر در سراسر جهان را در معرض خطر قرار داده است. به گفته رایان اولسون، مدیر اطلاعاتی شرکت پالو آلتو، CoolReaper به راحتی می‌تواند بدون رضایت کاربر هر برنامه آندرویدی را دانلود و حتی نصب کند. از جمله قابلیت‌های دیگر این درب‌پشتی می‌توان اتصال به سرورهای فرماندهی و کنترل (C & C)، پاک کردن داده‌های کاربر، حذف برنامه‌های موجود، غیر فعال کردن برنامه‌های کاربردی سیستم و ارسال یا درج SMS یا MMS با پیام های دلخواه اشاره کرد.

لازم به ذکر است که مقامات چینی تاکنون واکنشی را نسبت به ادعاهای این شرکت آمریکایی انجام نداده‌اند.

افشاگری اسنودن درباره حملات سایبری آمریکا علیه کشورها

ادوارد اسنودن، پیمانکار سابق آژانس امنیت ملی آمریکا گفت این کشور با حمله سایبری به تاسیسات اتمی ایران آغازگر روند جهانی حملات سایبری مخرب علیه کشورهای دیگر بوده است.

اسنودن در مصاحبه با شبکه تلویزیونی پی بی اس گفت آمریکا با به کار بردن ویروس «استاکس نت» علیه تاسیسات اتمی ایران در سال ۲۰۰۷ و ۲۰۰۸، اولین کشوری بود که از بدافزارها علیه دیگر کشورها استفاده کرد.

اسنودن که در حال حاضر در روسیه تحت پناهندگی موقت به سر می برد مامور سابق آژانس اطلاعات مرکزی آمریکا (سیا) و پیمانکار سابق آژانس امنیت ملی این کشور است که از ماه ژوئن سال ۲۰۱۳ هزاران سند طبقه بندی شده را در مورد برنامه‌های نظارتی آمریکا افشا کرد.

اسنودن در ادامه گفتگویش با این شبکه گفت: «مهم است که مشخص کنیم این روند را از زمان راه اندازی استاکس نت علیه برنامه هسته‌ای ایران آغاز کرده‌ایم.»

وی در ادامه گفت: « منصفانه است که بگوییم این پیچیده‌ترین حمله سایبری بوده که تا به حال کسی دیده است.»

استاکس نت یک ویروس رایانه‌ای است که طبق گزارشات، توسط آمریکا و اسرائیل در دولت جورج بوش، رئیس جمهور پیشین آمریکا توسعه داده شده است.

کارشناسان بر این باورند که برای توسعه ویروس استاکس نت به بزرگترین و پرهزینه‌ترین تلاش‌ها در تاریخ بدافزارها نیاز است هر چند این

ویروس نتوانست آسیب قابل توجهی به برنامه انرژی اتمی ایران وارد کند.

اسناد طبقه بندی شده که اسنودن به دست آورده است نشان می‌دهد سازمان‌های اطلاعاتی آمریکا نقاط ضعف فنی را کشف و حتی ایجاد کرده‌اند که امکان جاسوسی از تماس‌های تلفنی، ایمیل‌ها و دیگر راه‌های ارتباطی در سراسر جهان را به ماموران آمریکایی می‌دهد .

فرماندهی سایبری آمریکا افسران نیروی هوایی این کشور را استخدام می‌کند

فرماندهی سایبری آمریکا قصد دارد برای محافظت از نیروی هوایی این کشور، ٦ هزار نفر را در ۱۳۳ گروه ماموریت سایبری به کار گیرد.

فرماندهی سایبری آمریکا اعلام کرد در سال جاری تعدادی از افسران نیروی هوایی این کشور را در گروه ۳۹ این نیرو که ماموریت های سایبری دارد جذب خواهد کرد. قرار است این گروه طی دو سال آینده تشکیل شود. فرماندهی سایبری آمریکا همچنین اعلام کرد برای تشکیل گروه‌های سایبری نیروی هوایی به ۱۷۱۵ تن از افسران این نیرو نیاز دارد. این اقدام بخشی از تلاش وزارت دفاع آمریکا برای تشکیل ۱۳۳ گروه ماموریت سایبری تا سال ۲۰۱۷ است. در مجموع ۶ هزار نیرو در این گروه‌ها حضور خواهند داشت.

سرهنگ جوزف هرالد (Col. Joseph Herold) از مشاوران دفتر فرماندهی نیروی هوایی آمریکا گفت: «فقط نیروهای ماموریت سایبری در حال گسترش نیستند، بلکه دیگر نیروهایی که وظیفه حمایت از واحد ۲۴ نیروی هوایی را دارند نیز گسترش خواهند یافت». واحد ۲۴ نیروی هوایی آمریکا موظف است از شبکه‌های این نیروی حفاظت و دفاع کند.

هرالد افزود: «ما در نیروی هوایی واحدهایی با ماموریت‌های گوناگون داریم. برخی از آنان به صورت خاص وظیفه دارند شبکه‌های نیروی هوایی را راهبری کرده و از آنان دفاع کنند».

ایر فورس تایمز نوشت: «نیروی هوایی از این راه می‌تواند بدون نیاز به

منابع جدید، از نیروهای انسانی موجود بیشتر استفاده کند».

به اعتقاد هرالد، کار کردن در گروه‌های محافظت سایبری برای اعضاء نکته شیرین دیگری نیز دارد. این اعضاء علاوه بر آموزش‌های نظامی نیروی هوایی، می‌توانند از تخصص و تجربه غیر نظامی خود نیز استفاده کنند.

به گفته هرالد تلاش برای رسیدن به حداقل‌هایی که فرماندهی سایبری آمریکا تعیین کرده و آماده سازی همزمان نیروهایی جدید، برای مجموعه نیروی هوایی آمریکا به یک چالش تبدیل شده است.

هرالد در پایان گفت: «ما مجبوریم افراد شایسته را به خدمت بگیریم آن هم از مسیر درست، تا بتوانیم همه افراد را به سرعت لازم برسانیم و از برنامه زمانی عقب نمانیم».

حمله سایبری به نیروگاه‌های اتمی کره جنوبی و مرگ ۳ نفر

مقامات برنامه اتمی کره جنوبی از هک شدن سامانه‌های رایانه‌ای نیروگاه‌های اتمی این کشور خبر دادند. این خبر نگرانی‌ها در خصوص امنیت تاسیسات مجاور برنامه هسته‌ای این کشور را افزایش داده است.

مقامات کره‌ای اعلام کرده‌اند که اطلاعات غیر حیاتی این برنامه به سرقت رفته است و خطری ۲۳ رآکتور اتمی موجود در کره جنوبی را تهدید نمی‌کند. اما کارشناسان معتقدند کنترل رآکتورهای اتمی این کشور در معرض خطر هستند.

این بار نیز ایالات متحده مثل حوادث سونی، کره شمالی را مسئول این حملات مخرب بر علیه تاسیسات اتمی کره‌جنوبی دانست. مقامات کره‌ای در حال بررسی موضوع هستند و از بیان اینکه چه کسی مسئول انجام این حملات بوده است، خودداری می‌کنند. در سال ۲۰۱۳ کره جنوبی، کره شمالی را متهم به انجام حملات هکری بر علیه بانک‌ها و رسانه‌های این کشور کرده بود.

چونگ یانگ هو (**Chung Yang-ho**)، معاون وزیر انرژی این کشور در گفت و گوی تلفنی با رویترز، هر گونه خطر و تهدید بر علیه برنامه هسته‌ای این کشور را رد کرده است. خبر گزاری راشاتودی، از تعطیلی ۲ رآکتور هسته‌ای کره جنوبی، بعد از حملات هکری صورت گرفته خبر داد. در پی این حملات و نشت گاز سمی در این نیروگاه، سه تن کشته شدند.

چندین بخش دولت و همچنین پلیس این کشور در حال بررسی موضوع کشته شدن این افراد در نزدیکی رآکتور اتمی شهر اولسان کره جنوبی هستند. شرکت نیروگاه هسته‌ای و آبی این کشور که مسئولیت اداره این سایت در زمان بروز حادثه را بر عهده داشته است، اعلام کرد احتمالاً علت مرگ این سه نفر نشت گاز سمی نیتروژن از شبکه انتقال زمینی بوده است.

البته چوی هی یی (**Choi Hee-ye**)، یکی از مسئولان این شرکت، وجود هرگونه ارتباط بین نشت گاز و حمله هکری صورت گرفته بر علیه تاسیسات اتمی این کشور را رد کرده است.

مقامات کره‌ای، خواستار همکاری چین درتحقیقات درباره این حادثه شدند. این درخواست همکاری، بعد از ردیابی چندین آی پی اینترنتی چینی انجام شد. این آی پی ها، متعلق به شهرهایی از چین بودند که در نزدیکی کره شمالی قرار دارند.

وزارت دفاع دانمارک و واحد تهاجمی جنگ‌های سایبری

اخیراً جزئیات بیشتری از تصمیم دولت دانمارک در خصوص تشکیل واحد تهاجمی جنگ‌های سایبری منتشر شده است. بودجه تشکیل این واحد حدوداً ۷۴ میلیون دلار است.

پایگاه خبری Defense News نوشت :دولت دانمارک قصد دارد برای تشکیل واحد تهاجمی جنگ‌های سایبری (Offensive Cyber Warfare) مبلغ حدود ۴۶۵ میلیون کرون (نزدیک به ۷۴ میلیون دلار آمریکا) به بودجه وزارت دفاع بیفزاید. به گفته مسئولان وزارت دفاع دانمارک این واحد باید طی سال‌های ۲۰۱۷-۲۰۱۵ سازماندهی شود.

کمیسیون دفاع دانمارک در سال ۲۰۱۲ برای اولین بار پیشنهاد تشکیل چنین واحدی را مطرح کرده بود. در سال ۲۰۱۳، «برنامه ملی برای امنیت سایبر» طرحی پیشنهادی با جزئیات اجرایی ارائه کرد و لزوم تشکیل واحد تهاجمی جنگ‌های سایبری را شرح داد. قرار است وزارت دارایی دانمارک این مبلغ را تامین کند. پنجاه درصد این مبلغ برای ساخت و توسعه فناوری‌های تهاجمی پیشرفته و همچنین مهارت‌های تسلیحات سایبری صرف خواهد شد. دانشگاه‌ها و مراکز تحقیقات دفاعی دانمارک در تشکیل این واحد نقش مهمی را ایفا خواهند کرد.

مقامات دانمارک در تشریح دلایل تشکیل این واحد، به جاسوسی‌های سایبری طی سال‌های ۲۰۰۸ تا ۲۰۱۲ اشاره می‌کنند. هدف اصلی آن جاسوسی‌ها سرقت اطلاعات پیمانکاران دفاعی دانمارک بوده که در پروژه ساخت جنگنده F35 محصول شرکت لاکهید مارتین (Lockheed Martin) حضور داشتند. کارشناسان، چین را عامل اصلی جاسوسی‌های سایبری طی سال‌های ۲۰۰۸ تا ۲۰۱۲ می‌دانند اما نمی‌توانند با اطمینان اظهار نظر کنند.

چالش اصلی مقامات دانمارکی، عدم تعریف یکسان تهدید جنگی میان مجلس و وزارت دفاع است. بر اساس قوانین این کشور مجلس باید مجوز آغاز جنگ را صادر کند اما ضعف قانونی موجود به چالشی حل نشده میان مجلس و وزارت دفاع دانمارک تبدیل شده است.

تشکیل گروه تحقیقات سایبر در رژیم صهیونیستی توسط لاکهید مارتین

لاکهید مارتین در حال همکاری با سه شرکت از رژیم صهیونیستی و آمریکا است تا یک سازمان تحقیقات سایبری در بئرشبع بنا کند.

لاکهید مارتین (Lockheed Martin) از همکاری با شرکت‌های EMC، JVP و BGN technologies خبر داد. ای‌ام‌سی، یک شرکت چند ملیتی آمریکایی است که در زمینه امنیت اطلاعات، تحلیل داده‌ها، ذخیره و مجازی‌سازی داده‌ها، مدیریت اطلاعات و رایانش ابری فعالیت می‌کند. جی‌وی‌پی یا شرکای سرمایه‌گذاری اورشلیم (Jerusalem Venture Partners)، نیز یک شرکت سرمایه‌گذاری‌های خطرپذیر است که در حوزه‌های مختلف فناوری اطلاعات و به خصوص امنیت سایبر فعالیت دارد. و آخرین شرکت که مرکز فناورهای دانشگاه بن-گورین (BGN technologies) نام دارد، یکی از شرکت‌های وابسته به این دانشگاه Ben-Gurion University of the Negev) است که مسئولیت تجاری سازی محصولات و اختراعات محققان این دانشگاه را بر عهده دارد. پیش‌تر، این سه شرکت از تصمیم خود برای راه‌اندازی مجموعه‌ای به نام CyberSpark Industry Initiative خبر داده بودند. حالا قرار است لاکهید مارتین نیز به جمع آنان اضافه شود. در خبری که لاکهید مارتین منتشر کرده، آمده است: «سایبراسپارک یک سازمان غیر انتفاعی است که با هدف تسهیل هماهنگی میان بخش‌های دولتی و خصوصی در اسرائیل و جامعه‌ی بین المللی فناوری تشکیل شده است. این هماهنگی با کمک سایبراسپارک انجام خواهد شد که در پارک فناوری‌های پیشرفته بئرشبع واقع است».

قرار است سایبراسپارک با ارتش (IDF)، سازمان‌های دولتی و مراکز دانشگاهی رژیم صهیونیستی همکاری کند. گفته می‌شود سایبراسپارک در منطقه بئرشبع بودجه کلانی را صرف

پژوهش در حوزه سایبر خواهد کرد. لاکهید مارتین به تازگی دفتر نمایندگی خود را در بئرشبع افتتاح کرده است.
جاشوا شانی (Joshua Shani)، مدیرعامل لاکهید مارتین در رژیم صهیونیستی اعلام کرد: «این قدم دیگری از برنامه‌های لاکهید مارتین برای توسعه همکاری‌ها با مراکز صنعتی و دانشگاهی اسرائیل در حوزه‌های اطلاعات، مخابرات و فناوری است. ما باور داریم لاکهید مارتین نقشی کلیدی در شناساندن اسرائیل به عنوان مرکز سایبری مورد احترام جهانیان ایفا خواهد کرد. این امر از طریق ارائه مهارت‌ها، تجربه و سرمایه‌گذاری داخلی در مشاغل محقق خواهد شد».

این اولین بار نیست که شرکت‌های بزرگ آمریکایی در رژیم صهیونیستی سرمایه‌گذاری یا ارائه خدمات می‌کنند. چندی پیش نیز شرکت آمریکایی UST Global از همکاری خود با این رژیم خبر داده بود. سرمایه‌گذاری‌های کلان رژیم صهیونیستی در حوزه سایبر و خدمت رسانی وسیع آمریکایی‌ها موضوعی است که باعث نگرانی بسیاری کشورها شده است. در میان کشورهای نگران از این همکاری‌ها، دوستان نزدیک دو دولت نیز دیده می‌شوند.

LOCKHEED MARTIN

چشم انداز حملات سایبری در سال ۲۰۱۵

حملات سایبری در سال ۲۰۱۵ به شکل بدتری از جانب هکرها ادامه پیدا خواهد کرد و از روش های پیشرفته‌تری برای نفوذ به داخل شبکه‌ها استفاده خواهد شد.

آزمایشگاه امنیتی مک‌آفی پیش‌بینی می‌کند که در سال ۲۰۱۵ جنگ سایبری و جاسوسی دیجیتالی، در استراتژی‌های هکرها قرار می‌گیرد و سرقت اطلاعات به صورت پیشرفته تری ادامه پیدا خواهد کرد. گروه‌های تروریستی فعالیت بیشتری خواهند داشت، حملات اختلال سرویس فلج کننده راه اندازی می‌شوند و استفاده از بدافزارهای مخربی که تمام داده‌های بوت اولیه را از بین می‌برند، افزایش خواهند یافت.

محققان می‌گویند در سال ۲۰۱۵، مجرمان سایبری از روش‌های بهتری برای مخفی‌سازی خود در شبکه قربانی استفاده می‌کنند و بدون اینکه شناسایی شوند به سرقت طولانی مدت اطلاعات می‌پردازند.

در ادامه این گزارش آمده است که هکرهای دولتی از حملات سایبری پیچیده‌تری برای ضربه زدن به زیرساخت‌های حیاتی سایر کشورها استفاده خواهند کرد.

مک‌آفی می‌گوید در حال حاضر

سوء استفاده از دستگاه‌هایی از قبیل وبکم‌ها با امنیت پایین و سیستم‌های کنترل صنعتی موسوم به ICS، از اهداف اصلی هکرها محسوب می شوند، اما موضوع امنیت سایبری در مراقبت‌های بهداشتی به عنوان یک بخش ویژه، نگران کننده است. گفته می‌شود داده‌های مراقبت‌های بهداشتی، در بازار سیاه هکرها حتی با ارزش تر از داده‌های کارت اعتباری، خرید و فروش می‌شوند.

این گزارش می‌افزاید تهدیدات دیگری همچون باج افزارها رشد خواهند کرد، که علاوه بر قفل کردن داده‌ها، قربانیان را به پرداخت پول تهدید می‌کنند. در بخش خرده فروشی، پرداخت دیجیتال در معرض خطر بیشتری قرار می‌گیرد. هکرها حتی ممکن است قادر باشند تا سیستم‌های بی سیم نظیر بلوتوث و ارتباطات میدانی نزدیک (NFC) را که توسط پرداخت‌های موبایل استفاده می‌شوند هدف قرار دهند.

وینسنت ویفر، معاون ارشد شرکت اینتل می‌گوید: سال ۲۰۱۴، سال اعتماد متزلزل است. بازگرداندن اعتماد در سال ۲۰۱۵ نیازمند همکاری قوی‌تر بین دولت‌ها، تصویب استانداردهای جدید سایبری برای جلوگیری از تهدیدات و برقراری امنیت سایبری جدید برای مواردی است که برای تشخیص نیاز به زمان دارند.

امنیت سایبر، بزرگترین دغدغه سرویس‌های جاسوسی رژیم صهیونیستی

مقامات رژیم صهیونیستی، تلاش می‌کنند تا بئرشبع و دانشگاه بن‌گوریون واقع در این منطقه را به بزرگترین مرکز امنیت سایبر خود تبدیل کنند.

واحد ۸۲۰۰، بزرگترین واحد ارتش رژیم صهیونیستی است. این گروه مسئولیت فعالیت‌هایی نظیر استراق سمع و جاسوسی از امواج، همانند فعالیت‌های فناوری‌های پیشرفته را نیز بر عهده دارد. همچنین درصد بسیار زیادی از شرکت‌های نوپا و موسسات فناوری رژیم صهیونیستی، توسط فارغ‌التحصیلان و افراد شاغل در این واحد از ارتش تاسیس شده اند. در کل، واحد فناوری و جاسوسی ارتش اسرائیل (که شامل گروه ۸۲۰۰ نیز می‌شود)، زمینه ساز پرورش بیشترین افراد در رژیم صهیونیستی، در بخش فناوری است. به عنوان مثال، بنیان گذاران فناوری ویز (waze)، از فارغ التحصیلان واحد ۸۲۰۰ ارتش این رژیم بوده‌اند. ویز یک جهت یاب رایج است که سال گذشته گوگل آن را به مبلغ تقریبی یک میلیارد دلار خرید.

آدام سینگولدا (Adam Singolda)، در سال ۲۰۰۷ وب سایت تابولا (Taboola)، را تاسیس کرد. این وب سایت که در حوزه آمار بازدید سایت فعالیت می‌کند، ارزشی برابر ۱/۵ میلیارد دلار دارد. وی قبل از تاسیس این وب سایت، هفت سال در زمینه رمزنگاری پیشرفته، در ارتش رژیم صهیونیستی فعالیت می‌کرده است. بنیان‌گذار wix.com (طراح وبسایت رایگان)، نیز از جمله سربازان واحد ۸۲۰۰ بوده است. به دلیل محرمانه بودن اطلاعات جاسوسی و نبود امکان انتشار عمومی آنها، قابلیت جمع‌آوری آمار نیز برای آنها وجود ندارد، اما کارشناسان بر این باورند که تاثیر واحدهای فناوری و اطلاعات جاسوسی بر زندگی مردم بسیار زیاد می‌باشد. مقامات رژیم صهیونیستی، تلاش گسترده‌ای را برای برقراری یک ارتباط موثر بین نیروی نظامی این کشور و بخش صنعت آغاز کرده‌اند و در همین راستا اقدام به تاسیس شرکت‌های نوپای فناوری اطلاعات تحت نظر واحد فناوری جاسوسی ارتش این کشور نموده‌اند. امنیت سایبر به یک صنعت پررونق در این رژیم تبدیل شده است. در سال ۲۰۱۳، منابع مالی موسسات فناوری اطلاعات این رژیم رشد ۱۴۰ میلیون دلاری داشتند و هم اکنون رژیم صهیونیستی ۱۳ درصد از سهم جهانی تحقیقات در زمینه امنیت سایبر را به خود اختصاص داده است.

بئرشبع نیز به سرعت تبدیل به مرکز مدیریت امنیت سایبر رژیم صهیونیستی شده است. در حدود ۳۰ هزار سرباز از بخش‌های مرتبط، واحد ۸۲۰۰، محاسبات، ارتباطات و فرماندهی سایبری در نزدیکی بئرشبع و یا در داخل این شهر قرار دارند. همچنین دانشگاه بن‌گوریون نیز در داخل این شهر است که بزرگترین دانشگاه این رژیم در زمینه آموزش امنیت سایبر معرفی شده‌است. همچنین این رژیم اقدام به تاسیس یک پارک صنعتی به جهت ایجاد ارتباط بین دانشگاه و واحدهای نظامی کرده‌است که با دویچ تلکام (Deutsche Telecom)، آی بی ام (IBM)، و مرکز تحقیقات لاکهید مارتین (Lockheed Martin) در ارتباط است.

بنیامین نتانیاهو، نخست وزیر رژیم صهیونیستی در اولین کنفرانس فناوری سایبر که با حضور بیش از ۴۵۰ شرکت فعال در صنعت امنیت سایبر برگزار شد، گفت:

«ما فرماندهی سایبری ملی خود را در دانشگاه بئرشبع قرار می‌دهیم. ما دارای یک خط آهن هستیم که تل آویو را به دانشگاه بن گوریون متصل می کند. شما می‌توانید تنها با طی مسافتی در حدود ۱۰۰ یارد، تمامی سه بخش تجهیزات امنیتی، دانشگاه و پارک صنعتی ما را در اختیار داشته باشید. این یک کار بزرگ است».

Blackhat، فیلمی با موضوع امنیت سایبری

هک کردن، تنها در میان کارشناسان امنیت سایبری و مجرمان اینترنتی رخ نمی‌دهد، بلکه یکی از موضوعات جالب توجه برای فیلم سازان هالیوودی به حساب می‌آید.

فیلم‌های هالیوودی مانند «هکرها» در سال ۱۹۹۵ و «اره ماهی» در سال ۲۰۰۱، از جمله فیلم‌هایی هستند که با موضوع هک و امنیت سایبر به اکران در آمدند. در حال حاضر نیز، مایکل مان، کارگردانی فیلمی با نام Blackhat را بر عهده گرفته است که به احتمال زیاد در سال ۲۰۱۵ اکران خواهد شد.

«بلک هت» اصطلاحی است که در مورد هکرهایی که کدهایی مخرب می‌نویسند، نقاط ضعف سیستم را شناسایی و حمله سایبری خود را آغاز می‌کنند به کار می‌رود. مایکل مان نزدیک به دو سال و نیم صرف ساخت تریلر سایبری جدیدش کرده و در این زمینه تحقیقات فراوانی را با محققان امنیتی انجام داده است.

طبق گزارش‌هایی که اخیراً منتشر شده‌اند، مان با چند هکر، از جمله یک هکر زندانی، ملاقات کرده تا فیلمش همخوانی بیشتری با دنیای واقعی داشته باشد. این فیلم که نقش اصلی آن را کریس همسورث بازی می کند، ماجرای یک زندانی آزاد شده است که به همراه والدین آمریکایی-چینی خود در تعقیب یک شبکه جنایی سطح بالای سایبری از شیکاگو و لس آنجلس تا هنگ کنگ و جاکارتا هستند.

همسورث نقش کدگذار و هکر نابغه‌ای را بازی می کند که زندانی است و ناچار می‌شود با مأموران آمریکایی و چینی در این موش و گربه بازی بین‌المللی شرکت کند.

گفته می شود این فیلم در ۱۶ ژانویه ۲۰۱۵ اکران خواهد شد.

جاسوسی NSA از تمامی ترافیک اسکایپ

ادوارد اسنودن، سند جدیدی را از آژانس امنیت ملی آمریکا منتشر نموده که نشان می‌دهد NSA از تمامی کاربران اسکایپ (Skype) جاسوسی کرده است.

روزنامه آلمانی اشپیگل، به تازگی سندی را از آژانس امنیت ملی آمریکا منتشر نموده که نشان می‌دهد این سازمان جاسوسی دسترسی کاملی به صدا، ویدئو، پیام‌های متنی و فایل‌های به اشتراک گذاشته شده کاربران اسکایپ داشته و از آنها جاسوسی کرده است.

دسترسی به اطلاعات اسکایپ، توسط حکمی از سوی یک دادگاه امنیت اطلاعات خارجی در ایالات متحده به تصویب رسیده و NSA نیز آن را به اجرا در آورده است. گفته می‌شود این جاسوسی جزئی از برنامه‌ای موسوم به PRISM است که به آژانس امنیت ملی آمریکا اجازه می‌دهد تا به اهداف امنیتی مشخص خود در اسکایپ دسترسی داشته باشد.

جمع آوری داده‌های اسکایپ در سندی از NSA، در آگوست ۲۰۱۲ تحت عنوان «راهنمای کاربری برای دسترسی به مجموعه داده‌های اسکایپ» منتشر گردید. جزئیات چگونگی شنود تماس صوتی انجام شده در اسکایپ، به وسیله سامانه نوکلئون (NUCLEON) آژانس در آن شرح داده شده است.

در این سند همچنین شیوه‌های یافتن چت‌های متنی و دیگر داده‌های رد و بدل شده بین کاربران هدف در پایگاه داده‌های «شبکه‌های اطلاعاتی دیجیتال» در سرویس PINWALE آژانس به کارکنان آموزش داده شده است.

گفته می‌شود جمع‌آوری و شنود کامل تماس‌های صوتی اسکایپ، از ماه فوریه سال ۲۰۱۱ شروع شده است. آژانس از این زمان قادر بوده تا هر نوع تماس اسکایپی را که در شبکه تحت نظر رد و بدل شده و یا توسط کاربر مظنون انجام شده است را به طور کامل شنود کند.

نکته قابل توجه در این شنودها این است که با توجه به حکم دادگاه، شرکت مایکروسافت همکاری کاملی با آژانس داشته و کلید رمزگذاری داده‌ها را در اختیار آژانس قرار داده تا داده‌های شنود شده به آسانی رمزگشایی شوند.

بدافزار virlock باقابلیت چندریختی

محققان امنیتی بدافزار جدیدی از نوع ransomware (باج افزار) را شناسایی کردند که کاملاً ارتقاء یافته است.

این بدافزار جدید که ویژگی‌های خود را از ransomware ارث برده است، VirRansom یا VirLock نام دارد. این بدافزار می‌تواند فایل‌های کاربر را رمزنگاری کند. هم‌چنین به دلیل وجود خاصیت چندریختی، این بدافزار می‌تواند نمونه‌هایی منحصربه‌فرد و یکتا از خودش ایجاد کند.

VirLock اکثر فرمت‌های رایج را هدف حمله خود قرار می‌دهد و می‌تواند فایل‌ها را با فرمت DOC، PPT، XLS، PDF ، و عکس‌ها را با فرمت PNG, GIF, BMP, PSD, JPG و فایل‌های صوتی و ویدئویی با فرمت MP3 و MPG به همراه فایل‌های ZIP و RAR را رمزنگاری کند.

در حال حاضر محققان امنیتی حداقل 6 نوع از این بدافزار را شناسایی کرده‌اند. آن‌ها اعلام کرده‌اند، ransomware،فایل‌ها را رمزنگاری کرده و پس از آن در یک پنجره پیامی را نمایش می‌دهد.

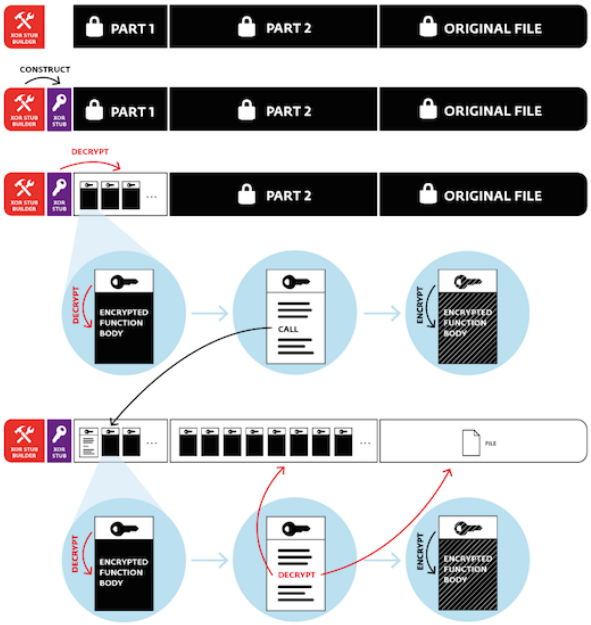
بدافزار VirRandom برخلاف بدافزارهای رمزنگاری معمولی، اجازه می‌دهد تا فایل‌ها به حالت اولیه خود بازگردند اما به طور متوالی با قفل کردن صفحه، کاربر را مجبور می‌کند تا حتماً به هکرها پول پرداخت کند.

هنگامی‌که صفحه کاربر قفل می‌شود، بدافزار، پروسه explorer.exe را از کار می‌اندازد. هم‌چنین اجازه استفاده از Task manager ، هر پروسه‌ای که باعث مقابله با بدافزار شود را نمی‌دهد.

رفتارهای بدافزار ساده است. هنگامی‌که در سیستم قربانی اجرا شود، خود را به یک فایل می‌چسباند. سپس آن را تبدیل به فایل اجرایی exe. می‌کند. پس از اجرا دو نمونه از خود را در مسیر %userprofile% و %allusersprofile% ایجاد می‌کند. باید توجه داشت که این عمل کپی نیست. زیرابه دلیل داشتن خاصیت چندریختی این دو نمونه کاملاً منحصربه‌فرد هستند.

پس از ایجاد نمونه‌ها، در رجیستری کلیدهایی را تحت HKCU و HKLM ایجاد می‌کند. بدین ترتیب هنگامی‌که ویندوز شروع به کار می‌کند، آن‌ها هم اجرا می‌شوند. نمونه جدیدی شناسایی‌شده است که نمونه منحصر به فرد سومی نیز ایجاد می‌کند.

بدافزار پیامی حاوی استفاده از نرم‌افزارهای غیرقانونی و کپی شده را نمایش می‌دهد و کاربر را به نقض قوانین کپی‌رایت محکوم می‌کند.



بانک‌های روسیه هدف گروه Anunak

یک گروه پیچیده هک توانست بیش از 25 میلیون دلار از طریق هک زیرساخت‌های اقتصادی روسیه و سامانه‌های کارت‌خوان کشورهای آمریکایی و اروپایی سرقت کند.

محققان امنیتی، گروه هک پیشرفته‌ای را شناسایی کردند که دارای یک بدافزار اصلی برای پیاده‌سازی حمله‌های خود هستند. آن‌ها این گروه را Anunak نامیده‌اند.

برخلاف اکثر گروه‌های هک که به مشتریان حمله می‌کنند، Anunak به خود مؤسسات مالی حمله می‌کند. آن‌ها به شبکه داخلی این مؤسسات نفوذ می‌کنند و سرورهای داخلی آن‌ها را تحت نظر می‌گیرند. بدین ترتیب آن‌ها می‌توانند حساب‌های بانکی را تغییر دهند یا حتی به ATM ها نیز دسترسی داشته باشند.

از سال 2013 تاکنون Anunak توانسته است به شبکه بیش از 50 بانک روسیه و 5 سیستم پرداخت دسترسی داشته باشند. با این دسترسی‌ها آنها توانسته‌اند بیش از 25 میلیون دلار سرقت کنند. بیشتر این پول‌ها در نیمه دوم 2014 سرقت شده است.

Anunak نفوذ خود را با فرستادن بدافزار آغاز می‌کند. پس از آلوده ساختن سامانه‌های کاربران معمولی، به شبکه داخلی نفوذ می‌کنند. سپس کنترل سرورهای داخلی و لیست حساب‌های کاربری را به دست می‌آورند. این گروه از کی‌لاگرها، اسکنر، بک‌دورهای SSH، نرم‌افزارهای کنترل از راه دور و کرک رمزعبور استفاده می‌کنند.

بااین‌حال ابزار اصلی آن‌ها بدافزار طراحی‌شده توسط خود آن‌ها است. همانطور که گفته شد نام این بدافزار Anunak است. این بدافزار بر اساس بدافزار Carberp توسعه یافته است. Carberp بدافزاری است که به‌منظور حمله به سامانه‌های بانکی طراحی‌شده است. کد منبع آن در سال 2013 منتشر شد. محققان امنیتی باور دارند که بعضی از اعضای گروه Anunak از گروه Carberp هستند که در سال 2013 به دلیل مشکلات داخل اعضا متلاشی شد.

بدافزار لینوکسی Penquin Turla

به دلیل آسیب‌پذیری‌های مودم‌های 4G ، هکرها می‌توانند کنترل کامل سامانه‌های متصل به آن‌ها را به دست بگیرند.

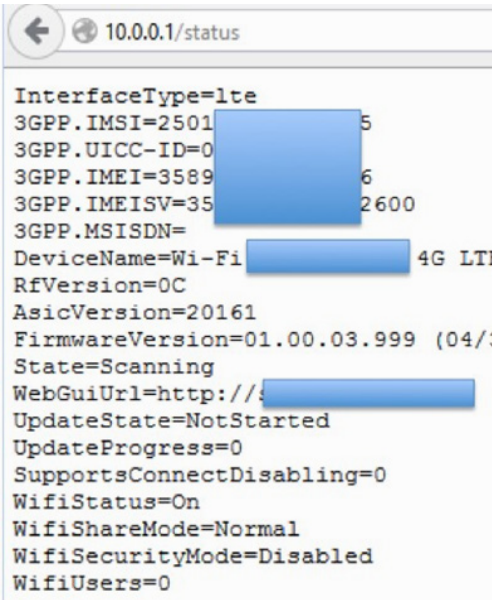
محققان امنیتی نتایج تحقیق خود را بر روی هک مودم و سیم‌کارت‌های 4G منتشر کردند. این تحقیق بر اساس نفوذ به مودم و سیم‌کارت از طریق آسیب‌پذیری‌ها و پیامک در بستر شبکه 4G است.

محققان امنیتی دریافته‌اند که مودم‌های یواس‌بی 4G دارای آسیب‌پذیری‌هایی هستند که می‌توانند کنترل دستگاه‌های متصل به آن را به هکر بدهند.

هم‌چنین آن‌ها توانستند با استفاده از فرستادن پیامک، سیم‌کارت قربانی را قفل و بار ترافیکی دستگاه را شنود کنند و آن را رمزگشایی نمایند.

محققان امنیتی آزمایش خود را بر روی ۶ مدل مختلف مودم یواس‌بی که ۳۰ فرمویر مختلف را اجرا می‌کردند، انجام داده‌اند. از این تعداد تنها ۱۰ درصد به حمله‌ها مقاوم بودند.

محققان امنیتی از روش‌های مختلفی به منظور پیاده‌سازی حمله‌های خود استفاده کردند که حمله‌های مبتنی بر مرورگر مانند CSRF را شامل می‌شد. حمله‌ها، داده‌های مختلفی مانند مشخصات کاربر، نسخه فرمویر، وضعیت Wi-Fi، نام ارائه‌دهنده سرویس موبایل و ... را به دست می‌آوردند. محققان امنیتی حمله‌های جدی‌تر دیگری مانند نصب بدافزارهای بوت را امتحان کردند که از طریق آن می‌توان سیستم کاربر را کنترل کرد.



سامانه‌های مختلفی هم‌اکنون از 4G استفاده می‌کنند که شامل سامانه‌های صنعتی SCADA و ATMها می‌شوند.

محققان امنیتی همچنین به الگوریتم‌های رمزنگاری سیم‌کارت‌ها نیز حمله کردند. با اینکه این حمله‌ها چندان نتیجه‌بخش نبود اما توانست ۲۰ سیم‌کارت از ۱۰۰ سیم‌کارت آزمایش‌شده را هک کنند.

هر دقیقه یک حمله سایبری به شبکه برق انگلستان انجام می‌شود

مجلس بریتانیا اعلام کرد، شبکه برق این کشور تحت حمله‌های سایبری قرار گرفته است به‌طوری که هر دقیقه یک حمله صورت می‌گیرد.

جیمز آربثنات (James Arbuthnot) یکی از اعضای کمیسیون دفاع مجلس انگلستان اعلام کرد که شبکه برق این کشور هدف حمله هکرها قرار دارد. او اضافه کرد که این حمله‌ها پی‌درپی در حال پیاده‌سازی بر روی زیرساخت‌های حساس هستند. به گفته وی این حمله‌ها نه روزانه بلکه به صورت دقیقه‌ای در حال اجرا هستند. این زیرساخت‌ها بسیار حساس بوده و توقف آن‌ها ضربات شدیدی را به اقتصاد وارد می‌کند.

مظنونان اصلی این حمله‌ها تروریست‌ها و هکرهای دولتی اعلام

شده‌اند و درجه حمله نیز به دلیل گستردگی و تعداد آن، بالا گزارش شده است. دولت انگلستان از این حمله‌ها آگاه بوده و منابع لازم را به‌منظور کاهش اثر این حمله‌ها تخصیص داده است. اخیراً اعلام شد بودجه دفاع سایبری انگلیس به ۱,۳ میلیارد دلار افزایش‌یافته است. این مقدار یعنی ۳۲ درصد افزایش نسبت به آنچه در سال ۲۰۱۱ تصویب شده بود.

یکی از مشکلات اصلی دفاع از سامانه‌های صنعتی و زیرساخت‌های کشور، پیشرفت فناوری است که در آنها استفاده می‌شود. با این پیشرفت، تجهیزات بیشتری مورد حمله قرار می‌گیرند. برای نمونه اینترنت اشیا را فرض کنید که برای نظارت مستقیم به کار می‌روند و می‌توانند به‌راحتی هک شوند.

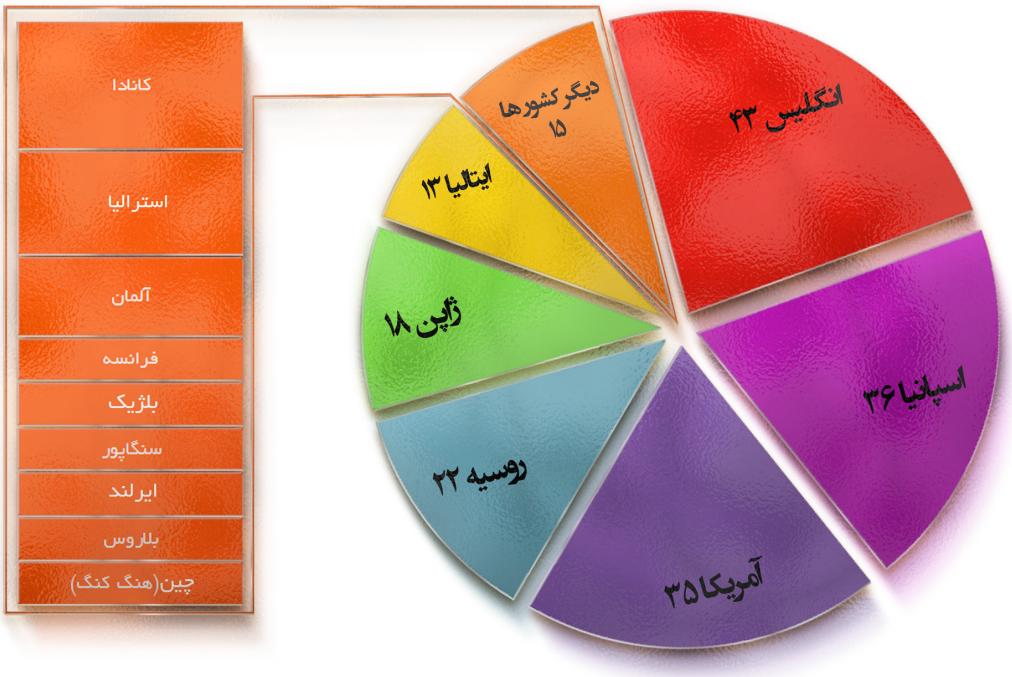
زئوس بازهم قربانی گرفت

نوع جدید بدافزار زئوس به ۱۵۰ بانک و ۲۰ سرویس پرداخت در سراسر دنیا حمله کرد.

محققان امنیتی مدل جدیدی از بدافزار زئوس را شناسایی کردند که مؤسسات مالی را هدف حمله‌های خود قرار داده است. این مدل جدید **Chthonic.Banker.Win32** نام دارد. بنا بر گزارش محققان امنیتی، این بدافزار به ۱۵۰ بانک و ۲۰ سیستم پرداخت حمله کرده است.

تمرکز حمله‌های زئوس بیشتر بر روی بانک‌های آنلاین است. زئوس بدافزاری است که برای پیاده‌سازی حمله‌های سایبری طراحی‌شده است.

بانک‌ها هدف اصلی این بدافزار هستند اما از این بدافزار در حمله‌های **phishing** نیز استفاده‌شده است. درمجموع ۱۵ کشور مورد هجوم این بدافزار قرارگرفته‌اند که شامل کشورهای انگلستان، آمریکا، اسپانیا، روسیه، ژاپن و ایتالیا می‌شود.



مدل جدید زئوس، ویژگی‌های جدیدی را به کد پایه زئوس اضافه کرده است و از تکنیک‌های جدیدی برای بارگذاری ماژول‌ها استفاده می‌کند، با این همه زئوس هنوز از همان الگوریتم‌های رمزنگاری گذشته استفاده می‌کند.

Chthonic سامانه‌های ویندوزی را هدف قرار می‌دهد. این بدافزار در ایمیل‌هایی یافت شده است که شامل فایلی با کدهای مخرب مخفی است. هنگامی که فایل توسط کاربر دانلود و

باز می‌شود، بدافزار وارد سیستم کاربر شده و کدهای مخرب را به پروسه msiexec.exe تزریق می‌کند.

پس‌ازاین مرحله اگر قربانی بخواهد به سیستم آنلاین بانکی وصل شود، کدهای مخرب بدافزار اجراشده و داده‌های حساس کاربر ازجمله نام کاربری، رمز عبور، PIN، شماره تلفن و ... را سرقت و آن‌ها را به هکر ارسال می‌کند. زئوس هم‌چنین شامل کی‌لاگر، سارق میکروفن و جاسوس وب کم نیز می‌شود.

انتشار انواع مختلف بدافزار زئوس به این دلیل است که در بازار مخفی هکرها، کد منبع این بدافزار منتشرشده است. به همین دلیل افراد و گروه‌های زیادی نسخه ارتقاء یافته آن را توسعه داده و برای پیاده‌سازی حمله استفاده می‌کند.

حمله سایبری به کارخانه تولید فولاد آلمان

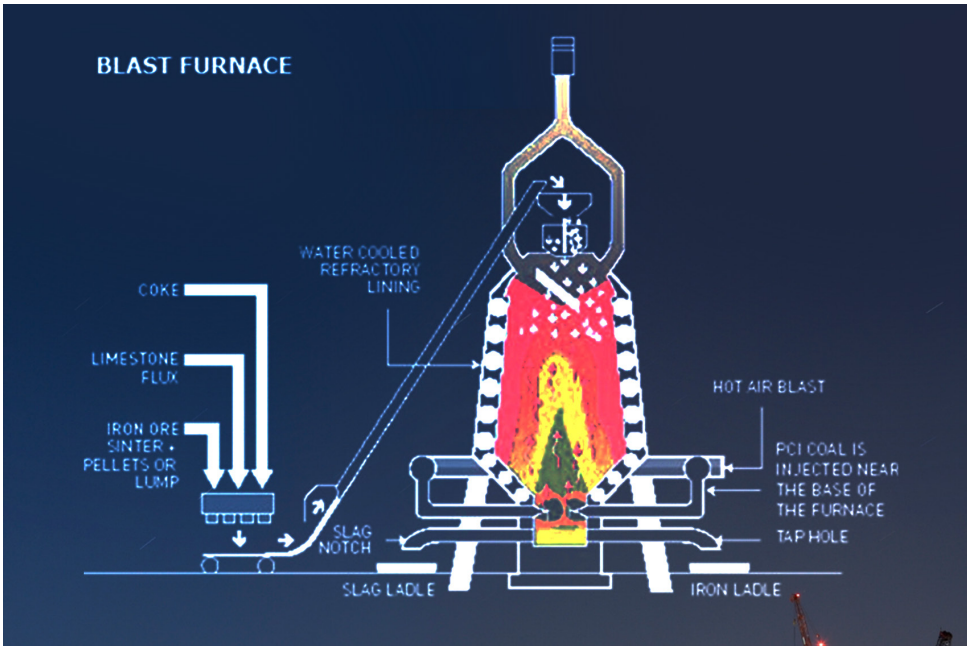
حمله سایبری مهلک به کارخانه تولید فولاد آلمان خسارت‌های سنگینی به این کارخانه تحمیل کرد.

حمله‌های سایبری می‌تواند خسارت‌های شدیدی را به زیرساخت‌های صنعتی و تولیدی وارد کند. محققان امنیتی یکی از این حمله‌های مهلک را به کارخانه تولید فولاد آلمان شناسایی کردند که خسارت شدیدی را به‌جای گذاشته است. بنا بر گزارش دولت آلمان، هکرهایی که هویتشان هنوز نامعلوم است، توانسته‌اند به شبکه داخلی کارخانه تولید فولاد نفوذ کرده و کنترل کوره ذوب را به دست بگیرند.

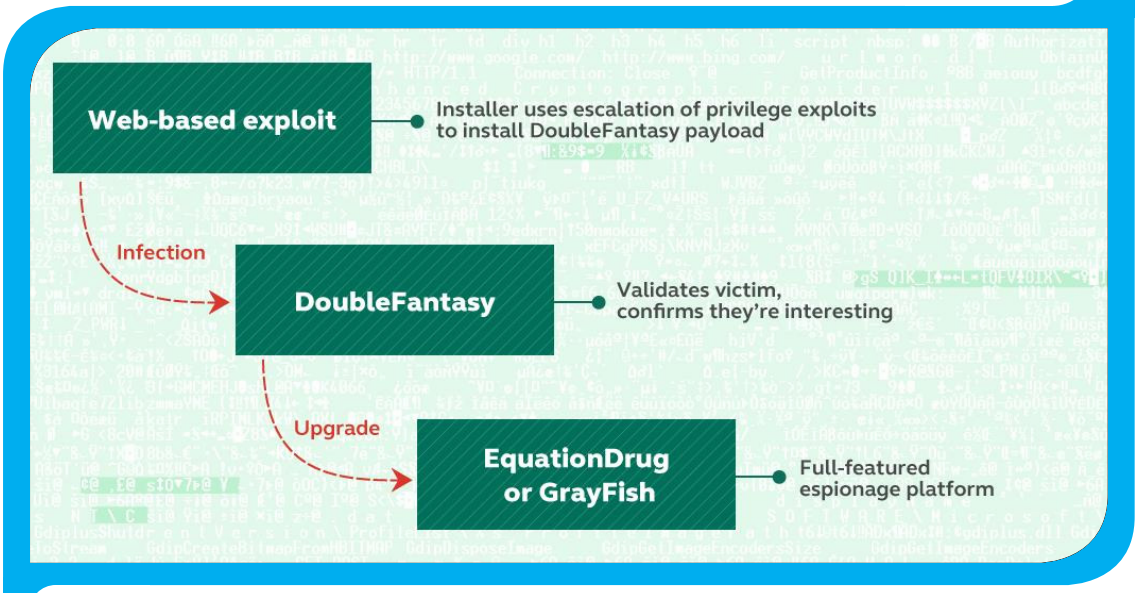
این حمله ابتدا با فرستادن ایمیل‌های مخرب به کاربران کارخانه فولاد و پیاده‌سازی حمله phishing آغازشده است. پس‌ازآنکه هکرها به سیستم داخلی دسترسی پیداکرده‌اند، سطح دسترسی‌های خود را تا کنترل خط تولید محصولات ارتقاء دادند.

هنگامی‌که هکرها توانستند خط تولید را به دست بگیرند، در تولید محصولات وقفه ایجاد کردند و باعث ازکارافتادن چندین‌باره آنها شدند. پس از این حمله‌ها دیگر امکان خاموش کردن کوره ذوب وجود نداشت. هکرها با حملات خود توانستند خسارت سنگینی به کوره ذوب وارد کنند.

بر اساس گزارش محققان امنیتی، این حمله بسیار پیچیده بوده است چرا که هکرها دانش بالایی در مورد دستگاه‌های مختلف صنعتی داشته‌اند و توانسته‌اند به‌سرعت این کار را انجام دهند.



نکته



DoubleFantasy ؛ بدافزاری برای جاسوسی از زیرساخت‌های دولتی

شرکت امنیتی کسپرسکی از تجزیه و تحلیل ابزار جاسوسی با نام DoubleFantasy خبر می‌دهد که با هدف جاسوسی از زیرساخت‌های حیاتی دولت‌ها طراحی شده است.

این بدافزار توسط گروهی با نام Equation توسعه یافته است و باعث نفوذ بدافزارهای پیچیده‌تر به سامانه قربانی می‌شود. همچنین Equation یک گروه جاسوسی سایبری پیشرفته است که به تازگی توسط تیم تحقیقات جهانی و تجزیه و تحلیل کسپرسکی شناسایی شده است.

کسپرسکی نشان داده است که رایانه‌های آلوده به این تروجان، با سرورهای فرماندهی و کنترلی (C & C) مهاجمان ارتباط برقرار کرده و اطلاعات قربانی را سرقت می‌کنند. کارشناسان امنیتی مشخص کردند که یکی از این سرورها در جمهوری چک و دیگری در کشور ایتالیا واقع شده است.

نسخه‌های متعددی از این بدافزار جاسوسی شناسایی شده است، اما به نظر می‌رسد که محبوب‌ترین نسخه‌های آن، ۸ و ۱۲ هستند.

به گزارش کسپرسکی، این بدافزار جاسوسی از ۲۰ سال پیش فعال بوده و از لحاظ پیچیدگی روش‌های به کار گرفته شده در حملات، بر تمامی تهدیداتی که تا به الان شناخته شده‌اند برتری دارد. گروه جاسوسی سایبری Equation از ابزارهایی برای آلوده کردن قربانیان خود استفاده می‌کنند که توسعه آنها بسیار پیچیده و گران است.

شرکت کسپرسکی در بخش دیگری از توضیحات خود درباره این گروه جاسوسی سایبری می‌گوید: « این گروه به استاکس‌نت وابستگی دارد. سازندگان این بدافزار باید به کد منبع درایوهای سخت آلوده دسترسی داشته باشند. چنین کدی می‌تواند آسیب‌پذیری‌هایی را نشان دهد که توسط نویسندگان این جاسوس‌افزار مورد استفاده قرار گرفته‌اند.»

اگر چه بدابزارهای مخرب بر روی سامانه مورد نظر از روش‌های پیشرفته‌ای استفاده می‌کنند، اما DoubleFantasy فقط مرحله اول حمله گروه Equation را به اجرا می‌گذارد، یعنی شناسایی قسمتی از سامانه که اطلاعات ذخیره شده در آن در معرض خطر قرار دارند و برای بررسی حملات پیچیده‌تر به کار گرفته می‌شوند.

اگر Equation هیچ علاقه‌ای به قربانی نداشته باشد، DoubleFantasy تمامی آثار مخرب خود از روی سامانه را حذف می‌کند. این تروجان، امکان سرقت اسامی کاربری و رمزهای عبور بر روی مرورگرهای وب اینترنت اکسپلورر و موزیلا فایرفاکس را نیز دارا می‌باشد.

محققان امنیتی، بدافزار DoubleFantasy را برای اولین بار بر روی یک سی‌دی و پس از جلسه یک کنفرانس علمی در هوستون در سال ۲۰۰۹ شناسایی کردند. این سی‌دی حاوی تصاویری همراه با یک فایل اجرایی مخرب (autorun.exe) بسته‌بندی‌شده بود. در مرحله اولیه، autorun.exe نوع کاربری دسکتاپ را بر روی دستگاه تعیین می‌کند.

چکیده مقالات سایبری

چالش‌های امنیتی کارت‌های هوشمند غیر تماسی و راهکارهای مقابله با آنها
ارائه روشی جدید برای پیاده‌سازی تروژان‌های سخت‌افزاری در بستر شبکه
دفاع سایبری در برابر شبکه جمع‌آوری اطلاعات اشلون
چالش‌ها و راهکارهای مقابله با حملات سایبری علیه کشور
روش رمزنگاری چندریختی برای مقابله با تهدیدات امنیتی نرم‌افزارها

چالش‌های امنیتی کارت‌های هوشمند غیر تماسی و راهکارهای مقابله با آنها

چکیده:

دامنه نفوذ کارت‌های هوشمند غیر تماسی که از فنآوری RFID بهره می‌گیرد با توجه به سهولت کاربرد و امنیتشان در حال گسترش است. یکی از مهم‌ترین مسائل کارت‌های هوشمند چالش‌های امنیتی آنها می‌باشد. در این مقاله تلاش شده است تا ضمن بررسی فنآوری‌های کارت‌های هوشمند غیر تماسی، مسائل امنیتی، تهدیدات و آسیب‌پذیری‌های کارت‌های هوشمند غیر تماسی به بحث گذارده شود. در پایان راهکارهایی جهت جلوگیری از حملات و تهدیدات احتمالی ارائه گردیده است.

کلیدواژه: کارت هوشمند غیر تماسی، RFID، تهدید، حمله، راهکارهای مقابله

۱- دکترا، الکترونیک، دانشگاه آزاد - Poorebrahimi@gmail.com

۲- دانشجوی دکترا، مدیریت فناوری اطلاعات، دانشگاه آزاد اسلامی واحد علوم و تحقیقات تهران - S.nikghadam@srbiau.ac.ir

ارائه روشی جدید برای پیاده‌سازی تروژان‌های سخت‌افزاری در بستر شبکه

چکیده:

با افزایش روزافزون برون‌سپاری ساخت مدارهای مجتمع، خطر جاسازی و ایجاد تغییر در طراحی اولیه توسط شرکت‌های سازنده تراشه افزایش یافته است. اهمیت این مسئله زمانی درک می‌شود که این مدارهای‌مجتمع برای کاربردهای نظامی، اقتصادی، مباحث زیرساختی شبکه‌های رایانه‌ای طراحی شده باشد. اخیراً گزارش‌هایی مبنی بر استفاده نظامی از تروژان‌های سخت‌افزاری با اهداف تخریب، جاسوسی یا اختلال از راه دور، توسط نهادهای امنیتی گزارش شده است. اصولاً دسترسی به دانش طراحی تروژان‌های سخت‌افزاری، امکان مهندسی طرح‌های تخریبی و یا جاسوسی به جهت دسترسی به‌موقع به اطلاعات دشمن را در اختیار قرار می‌دهد. این مقاله به بررسی انواع تروژان‌های سخت‌افزاری، چگونگی ورود آن به سیستم‌های تحت شبکه و نشت اطلاعات بر روی بستر شبکه پرداخته است. هدف از این مقاله ارائه شیوه کارکرد انواع تروژان‌های سخت‌افزاری در بستر شبکه و بررسی گلوگاه‌های طراحی چنین تروژان‌هایی و پیشنهاد روشی جدید برای پیاده‌سازی تروژان‌های سخت‌افزاری در بستر شبکه است.

کلیدواژه: تروژان‌های سخت‌افزاری، کانال‌های پنهان، شبکه، PUF، تراشه‌های شبکه.

۱-دانشجوی کارشناسی ارشد، مهندسی فناوری، اطلاعات دانشگاه گیلان- dourandish@mcs.guilan.ac.ir

۲-استادیار، گروه مهندسی کامپیوتر، دانشگاه گیلان- rebrahimi@guilan.ac.ir

دفاع سایبری در برابر شبکه جمع‌آوری اطلاعات اشلون

محمد سپهری[۱] و علیرضا پور ابراهیم[۲]

چکیده:

اطلاعات یکی از ارکان مهم جنگ‌هاست که در زمان صلح و جنگ باید به موقع جمع‌آوری، پردازش و بهره‌برداری گردد. اشلون شبکه‌ی بسیار وسیع و هوشمند جهانی جمع‌آوری اطلاعات و داده‌ها می‌باشد. مقاله حاضر به بررسی توانمندی‌های شبکه اشلون در جمع‌آوری و پردازش هوشمند اطلاعات و داده‌های تماس‌های تلفنی، دورنگارها، پست‌های الکترونیکی و دیگر داده‌های ارتباطات جهانی که از طریق ماهواره‌ها، شبکه‌های تلفنی، خطوط مایکرویو و رایانه‌ها جابجا می‌شوند، می‌پردازد. سوال اصلی مقاله، اشلون چگونه اطلاعات را رهگیری، جمع‌آوری و تجزیه و تحلیل می‌نماید. نتایج مقاله حاکی از ارائه راه کارهای مقابله با تهدیدات شنود و جمع‌آوری اطلاعات این شبکه می‌باشد. سپس با استفاده از تحقیق موردی زمینه‌ای و جمع‌آوری اطلاعات به‌صورت اسنادی، راه کارهایی به‌منظور کاهش آسیب‌پذیری و مقابله با توانمندی‌ها و تهدیدات شبکه اشلون ارائه می‌گردد.

کلیدواژه: اشلون، دفاع سایبری، اطلاعات الکترونیکی، پدافندغیرعامل

۱- دانشجوی دکترا، مدیریت راهبردی پدافند غیرعامل، مدرس دانشگاه هوایی شهید ستاری

۲-دکترا، دانشگاه عالی دفاع ملی – mohamadadsepehri377@yahoo.mco

چالش‌ها و راهکارهای مقابله با حملات سایبری علیه کشور

بهمن ابراهیمیان[1]

چکیده:

در حال حاضر کشور ما با طیف گسترده‌ای از حملات سایبری مواجه است. مقاله حاضر می‌کوشد تا نتایج پژوهشی که از مخاطب قرار دادن ۲۰ تن از خبرگان مباحث امنیت شبکه و جنگ سایبری به دست آورده است، را ارائه کند. بدین منظور ضمن بر شمردن انواع حملات سایبری، توانمندی‌های کشور در مقابله با این حملات بیان شده است. سپس موانعی که پیش روی این توانمندی‌ها قرار دارند و راه‌کارهای رفع موانع و چگونگی پیاده‌سازی عملی آنها در قالب دو گام «فراگیری و اجماع» و «کمک و یاری رسانی» ارائه گردیده است.

کلیدواژه: فضای سایبر، حمله سایبری، ایران

۱- کارشناس ارشد، مهندسی فناوری اطلاعات، دانشگاه تربیت مدرس– bahman.ebrahimian@modares.ac.ir

روش رمزنگاری چندریختی برای مقابله با تهدیدات امنیتی نرم‌افزارها

تقی تقوی[۱]

چکیده:

هدف این مقاله ارائه راه حلی جهت افزایش امنیت نرم‌افزارها در برابر حملاتی نظیر مهندسی معکوس و تحلیل برای شناخت عملکرد برنامه می‌باشد. در این مقاله یک روش رمزنگاری چندریختی محتوای فایل‌های اجرایی ارائه خواهد شد تا در هربار اجرای برنامه، عملیات رمزنگاری کد اجرایی با کلید جدیدی انجام گیرد تا به راحتی قابل رمزگشایی توسط تحلیل‌گران برنامه نباشد. با استفاده از این روش، صحت برنامه‌ها در حالت ایستا، (یعنی زمانی که برنامه به‌عنوان فایل در حال انتقال یا ذخیره‌سازی است)، قابل تضمین است. اما زمانی که برنامه در حال اجرا باشد، از حالت رمز خارج شده و در حافظه قرار می‌گیرد. کاربران بدخواه با انجام روش‌های مختلف قادر به انجام مهندسی معکوس بر روی برنامه‌های در حال اجرا هستند. آنها با استفاده از ابزارهای خاص و با دسترسی به تصویر حافظه فرآیند در حال اجرا و ذخیره‌سازی آن ، قادر به انجام تحلیل ایستا بر روی برنامه هستند. این مقاله راه حلی برای رفع این مشکل ارائه نموده است. در این روش، اجازه بررسی و تحلیل فضای آدرس برنامه در زمان اجرا به ابزارهای تحلیل و مهندسی معکوس داده نمی‌شود. در این‌صورت ایمنی برنامه در حال اجرا نیز فراهم می‌شود.

کلیدواژه: حملات تزریق کد، مهندسی معکوس، آسیب‌پذیری، رمزنگاری

۱- دانشجوی دکترا، دانشگاه امام حسین(ع)، دانشکده جنگال و دفاع سایبری - ttaghavi@ihu.ac.ir

هشدار ۱ :
مراقب نرم افزارهای جاسوسی در بازی‌ها باشید

Icon	Hostile file	Blocks	Web host
	GTA_SanAndreas_5_Baku_Style.exe	43,619	sha[illegible].az
	KMSpico setup1.exe	20,267	mediafire.com
	Pokemon online.exe	263	multiupload.biz
	Op7 Trainer FREE v3.0.exe	3,647	mega.co.nz
	UGG Public 1.2.exe	3,464	rghost.net
	Winbood_pokertable.exe	358	4shared.com

دانلود بازی‌ها از برخی وب سایت‌های به اشتراک گذاری فایل، سبب سرقت اطلاعات شخصی از سوی جاسوسان اطلاعات می شود.

طبق آمارهای منتشر شده از سوی مایکروسافت، در ماه گذشته، نرم افزاهای جاسوسی بیشترین آسیب را به کاربران زده اند. اکثر این کاربران در کشورهای برزیل، آمریکا و روسیه هستند.

این نرم افزارهای جاسوسی، در ضمن دانلود برخی از بازی‌ها از وب سایت‌های به اشتراک گذاری فایل وجود دارند.

مایکروسافت گفت:»افراد بد اندیش از ایمیل‌های رایج تولید کنندگان بازی‌ها استفاده می کنند تا اطلاعات شخصی افراد را از این طریق به دست آورند.«

کاربران همچنین باید هنگام باز کردن ایمیل‌ها یا پیام‌های اجتماعی که از طرف منابع نامعلوم است هوشیار باشند و البته توجه کنند که فایل‌ها را تنها از سایت رسمی آنها دریافت کنند. نصب نرم‌افزارهای امنیتی و به روزرسانی آنها نیز می‌تواند در این زمینه کمک شایانی کند.

هشدار ۲:
شناسایی بدافزار سرقت اطلاعات در محصولات لنوو

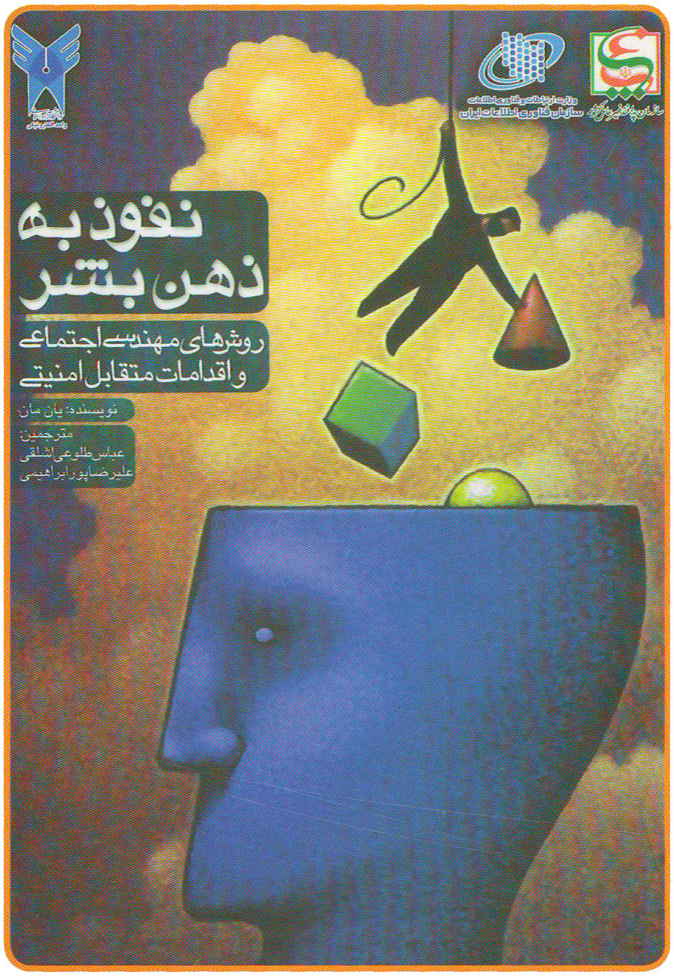
محققان امنیتی بدافزاری را در لپ‌تاپ‌های لنوو شناسایی کرده‌اند که به سرقت اطلاعات کاربران می‌پردازد.

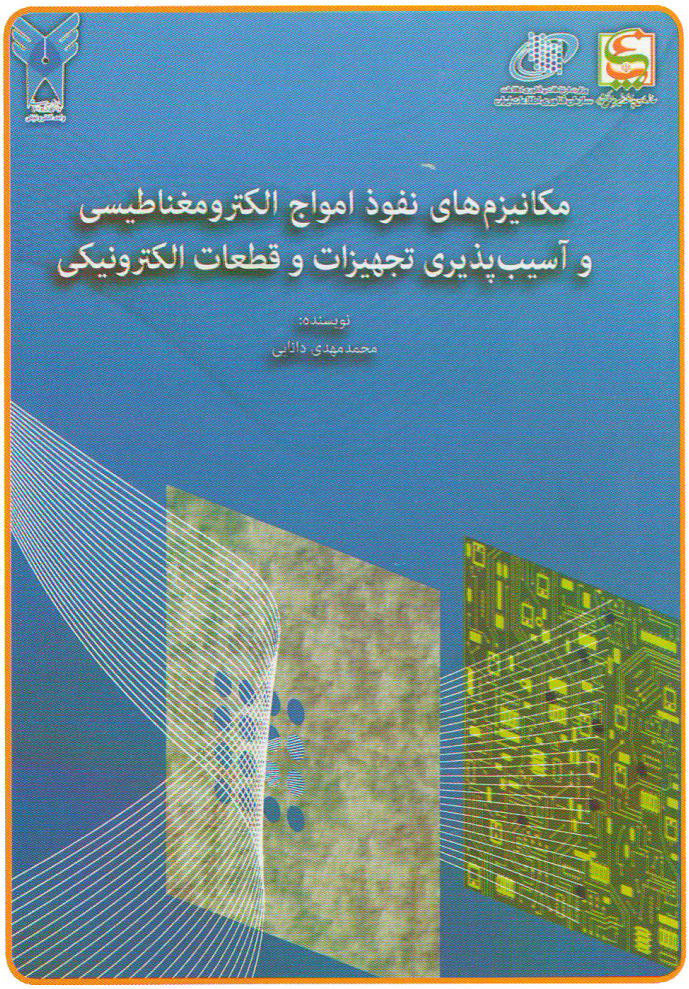
این بدافزار Superfish نام دارد و به طور پیش‌فرض در برخی لپ‌تاپ‌های ساخت شرکت لنوو وجود دارد. Superfish با نفوذ به ارتباطات رمزگذاری شده HTTPS، داده‌های حساس کاربران را به سرقت می‌برد. فعالیت مخرب Superfish تا حدی است که دولت آمریکا نیز وارد عمل شده و بیانیه امنیتی را برای کاربران لنوو منتشر کرده است.

یک محقق امنیتی وب‌گاهی را به نشانی https://filippo.io/Badfish راه‌اندازی کرده است که در آن کاربران می توانند از آلودگی یا عدم آلودگی رایانه خود باخبر شوند. همچنین در این سایت دستورالعمل‌هایی برای پاک‌سازی فایرفاکس و ویندوز از Superfish ارائه شده است.

معرفی کتاب

- نفوذ به ذهن بشر
- مکانیزم های نفوذ امواج الکترومغناطیسی و آسیب پذیری تجهیزات و قطعات الکترونیکی
- نقش کامپیوتر های شخصی در پدافند غیر عامل
- معماری امنیت اطلاعات (جلد اول)
- معماری امنیت اطلاعات (جلد دوم)

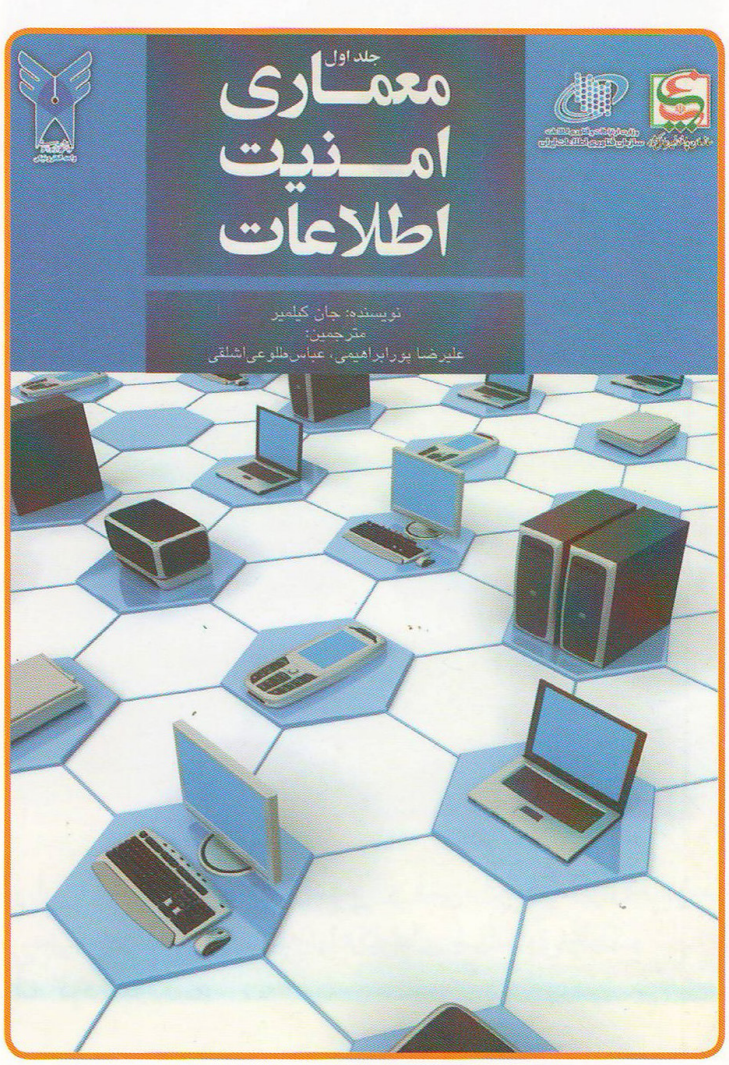

نفوذ به ذهن بتتر
روش‌های مهندسی اجتماعی و اقدامات متقابل امنیتی
نویسنده: یان مان
مترجمین:
عدلس طلوعی اشلقی
علیرضا پورابراهیمی

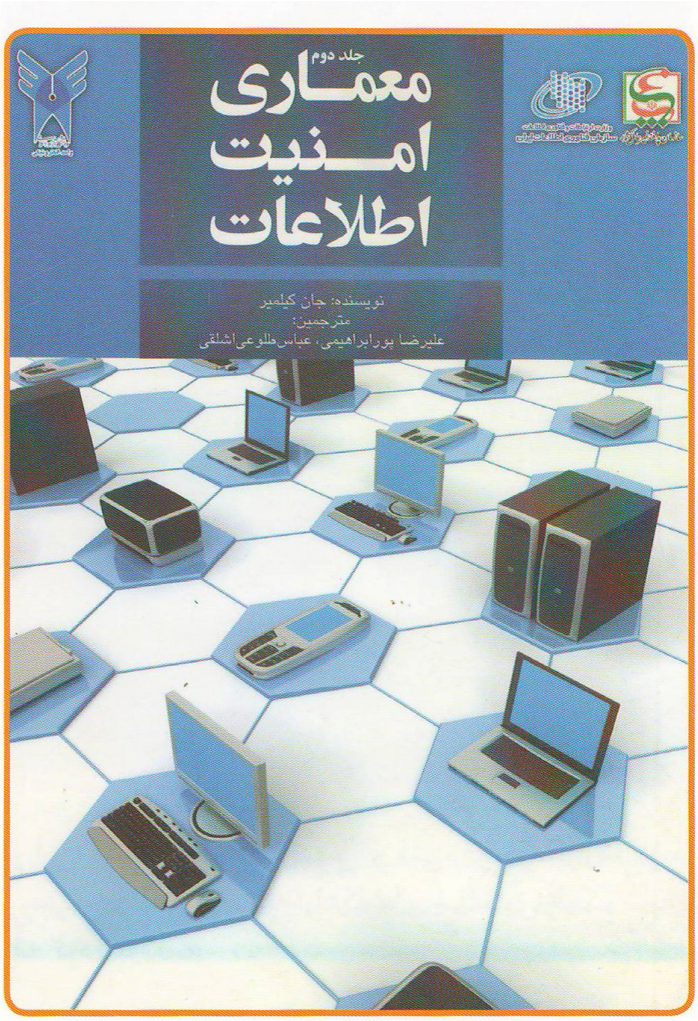


استفاده از مراکز رایانه ای، الکترونیکی و مخابراطی به صورت جزء لاینفک زندگی بشر درآمده است. انواع رایانه ها، شبکه های مخابراطی، مراکز داده، اتاق های سرور و مراکز کنترل صنعتی تقریباً در همه جا وجود دارند و عمده بار اطلاعاتی، پردازشی و ارتباطی را بر دوش می کشند.

پایداری و مداومت کاری بسیاری از فعالیت ها در کشور بستگی به این تجهیزات الکترونیکی دارد. اینجاست که می توان با تاکید گفت مقوله های یاد شده جزو منابع ملی کشور محسوب می شوند. از این رو ضروری به نظر می رسد تا از این منابع که هر روز گسترده تر می شوند، مراقبت اصولی به عمل آید. یکی از مخاطرات جدی تجهیزات الکترونیکی، سیگنال های ناخواسته و امواج الکترومغناطیسی هستند که به انحاء مختلف وجود دارند و می توانند حافظه ها، پردازشگر ها و سایر بخش های الکترونیکی و دیجیتالی را مختل کرده و یا حتی بسوزانند. منابع امواج الکترومغناطیسی شامل تسلیحات الکترومغناطیسی، رعد و برق ، دیزل ژنراتورها، جوشکاری برق، اتفاقات نا خواسته در شبکه های برق، بی سیم ها و یا هر تشعشع کننده دیگری می باشند.

در این کتاب تلاش می گردد به شیوه های حفظ و نگهداری اطلاعات در کامپیوتر های شخصی در شرایط عادی و بحرانی بپردازد و تهدیدات و فرصت های مربوطه را مورد بحث و بررسی قرار دهد.
سر فصل های اساسی مورد بحث در این کتاب به شرح ذیل خواهند بود:
۱-مقدمات امنیت دیجیتال
۲-امنیت نرم افزاری کامپیوتر های شخصی
۳-امنیت سخت افزاری کامپیوتر های شخصی
۴-انواع اطلاعات موجود بر روی کامپیوتر شخصی
۵-بررسی انواع شیوه های رایج گفته شده در رابطه با حفظ اطلاعات در کامپیوتر های شخصی
۶-بررسی روش های رایج حمله به کامپیوتر های شخصی در شرایط عادی و در شرایط بحرانی
۷-بررسی نقش اقدامات پیش گیرانه در رابطه با حفظ اطلاعات در شرایط بحرانی و نقش دفاع غیر عامل در این رابطه
۸-بررسی برخی پژوهش های انجام شده در رابطه با نقش اطلاعات کامپیوتر های شخصی در پدافند غیر عامل


جلد اول
معماری امنیت اطلاعات
نویسنده: جان کیلمیر
مترجمین:
علیرضا پورابراهیمی، عباس طلوعی اشلقی



کتاب های پیش گفته از واحد الکترونیکی دانشگاه آزاد قابل تهیه است