خبرنامه مدیریتی سراج
مرکز نرم‌افزار و سرویس وخدمات سازمان فضای مجازی سراج

اخبار فناوری اطلاعات و ارتباطات

۸۱

هفته نامه | سال دوم | شماره هشتاد و یکم | ۲۹ آبان ۱۳۹۵

تحلیل کسپرسکی در مورد ویندوز ۱۰ روسیه را به این سامانه‌ی عامل بدگمان کرده است

سرویس مبارزه با انحصارطلبی فدرال روسیه (FAS) در حال بررسی است تا متوجه شود که آیا مایکروسافت به واسطه‌ی ویندوز ۱۰ در جایگاه خود در بازار تخطی کرده است یا خیر؛ در واقع این حرکت پس آن آغاز شد که شرکت مستقر در مسکوی کسپرسکی به دیده‌بان و مقامات اتحادیه اروپا شکایت کرد.

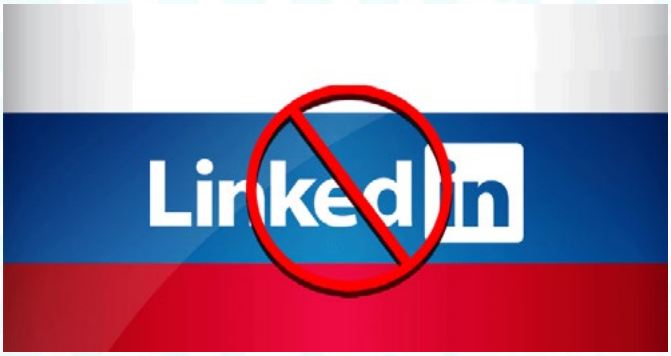
بنیان‌گذار شرکت ضدبدافزاری کسپرسکی، یوجین کسپرسکی، در پستی طولانی در وب‌لاگ خود استدلال کرد که مایکروسافت به عمد و به وسیله‌ی ویندوز ۱۰ سازندگان برنامه‌های کاربردی شخص ثالث را دردسر انداخته است. وی بیان داشت که مایکروسافت مدت زمان لازم برای آزمون سازگاری با سامانه‌ی عامل جدیدش را از ۲ ماه به ۶ روز کاهش داده است.

در نتیجه به کاربران ویندوز ۱۰ اعلام هشدار شده که فقط از برنامه‌های مایکروسافت استفاده کنند، یا نرم‌افزارهای فروشگاه ردموند را برای کار خود انتخاب کنند، فروشگاهی که مایکروسافت با هر بار خرید کاربران از آن سودی به جیب می‌زند. علاوه بر این، هنگامی که کاربران مایکروسافت ویندوز ۱۰ را نصب می‌کنند، این سامانه‌ی عامل بسته‌های امنیتی را از کار می‌اندازد و ضدبدافزار Defender خودش را به جای آن بسته‌ها به اجرا درمی‌آورد و بسته‌های انتخابی کاربر را ناسازگار قلم‌داد می‌کند.

آناتولی گولومولزین، معاون FAS، گفت که زمان کوتاه اختصاص یافته به سازندگان نرم‌افزار و این حقیقت که مایکروسافت بسته‌ی امنیتی ویژه‌ی خودش را دارد، «مزایای غیرقابل توجیهی» را به ردموند اعطا می‌کند، و به همین خاطر است که سازمان تحت کنترل وی مشغول بررسی و کاوش اوضاع می‌باشد.

یوجین کسپرسکی ادعاهایی دیگری را نیز در خصوص ویندوز ۱۰ مایکروسافت مطرح کرد: او اشاره کرد که کاربران ویندوز ۱۰ فقط می‌توانند دو بسته را روی سامانه‌هایشان نصب و اجرا کنند: Defender و یک مورد دیگر. حتی در صورتی که شما Defender را از کار بیاندازید، این نرم‌افزار گاهی اوقات خود را به تکاپو می‌اندازد و نتایج را به کاربر نمایش می‌دهد تا وی را ترغیب به تجدید نظر در نرم‌افزار مورد استفاده‌اش نماید.

لینکدین در کشور روسیه مسدود شد



خبرها حاکی از آن است که بزرگ‌ترین شبکه حرفه‌ای برخط یعنی لینکدین قرار است از روز دوشنبه در روسیه ممنوع شود. این تصمیم در پی رأی دادگاهی در مسکو است که می‌گوید شبکه اجتماعی لینکدین متعلق به مایکروسافت، قوانین حفاظت از داده این کشور را زیر پا گذاشته است.در جولای ۲۰۱۴، ماده‌ای به قانون داده‌های شخصی روسی افزوده شد که شرکت‌های خارجی را ملزم می‌کرد از تاریخ ۱ سپتامبر ۲۰۱۵، داده‌های شخصی کاربران روسی را در داخل روسیه ذخیره کنند. این قانون در جهت محافظت از داده‌های شهروندان روسی بر اساس افشاگری‌های ادوارد اسنودن تصویب شده بود. سازمان تنظیم مقررات رسانه‌ای فدرال روسیه که Roskomnadzor نام دارد تهدید کرده هر شرکتی که اطلاعات شخصی کاربران روسی را بر روی کارگزارهای غیر روسی ذخیره کنند، مسدود خواهد کرد. نه‌تنها لینکدین، بلکه شرکت‌های بزرگ‌تری از جمله واتس‌اپ، فیسبوک و توییتر می‌توانند در فهرست شرکت‌هایی باشند که اگر به این قانون عمل نکنند مسدود شوند. شرکت‌های بزرگی شامل گوگل، اپل و وایبر پیش‌تر اعلام کردند برخی از کارگزارهای خود را به روسیه منتقل کرده‌اند، اما فیسبوک، مایکروسافت و توییتر از پذیرش این قانون سر باز زدند.

بر اساس گزارش نیویورک تایمز، لینکدین نخستین شرکتی است که در اثر عدم همکاری با مقامات محلی روسی و بر اساس حکم دادگاه از فعالیت در خاک روسیه محروم می‌شود.

لینکدین می‌گوید تمایل دارد مذاکراتی را با مقامات روسی برای ادامه فعالیت خود ترتیب دهد. سخنگوی این شرکت می‌گوید: «تصمیم دادگاه روسی این قدرت را دارد تا دسترسی به لینکدین را برای میلیون‌ها کاربری که روسیه داریم و همچنین شرکت‌هایی که از شبکه ما برای ارتقا تجارت خود استفاده می‌کنند قطع کند. ما می‌خواهیم مذاکراتی را با Roskomnadzor ترتیب دهیم تا نگرانی‌های آن‌ها را برطرف کنیم.»

به نظر می‌رسد Roskomnadzor لینکدین را به دلیل سابقه بد این شرکت در مسائل امنیتی به‌عنوان نخستین هدف خود انتخاب کرده است.

باج‌افزار Telecrypt: باج‌افزاری که از تلگرام سوءاستفاده می‌کند

محققان اخیراً باج‌افزار جدیدی را کشف و آن را Telecrypt نام‌گذاری کرده‌اند. این باج‌افزار جدید از پیام‌رسان تلگرام برای ارتباطات دستور و کنترل خود استفاده می‌کند و همچنین اجازه می‌دهد قربانیان از طریق تلگرام با مهاجم در ارتباط باشند.

این بدافزار با نام Trojan-Ransom.Win32.Telecrypt توسط محققان آزمایشگاه کسپرسکی کشف شده و معلوم شده که فقط کاربران در روسیه را هدف قرار داده است. این گروه باج‌افزاری برای اینکه سرویس جدید ارتباطی برای خودشان طراحی نکنند از پروتکل ارتباطی تلگرام سوءاستفاده کرده‌اند.

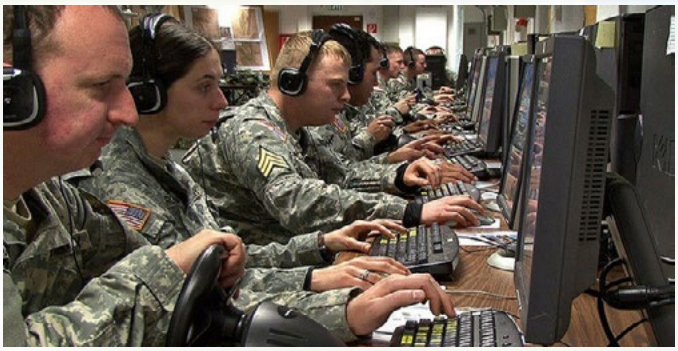
این تروجان نوشته‌شده با دلفی، در مرحله‌ی اول که اجرا شد، یک کلید رمزنگاری و شناسه‌ی آلودگی تولید می‌کند. در ادامه این بدافزار یک بات تلگرام ایجاد کرده و از طریق API تلگرام به مهاجمان اطلاع می‌دهد که آلوده کردن قربانی با موفقیت انجام شد. همچنین اطلاعاتی همچون شماره گفتگو، نام رایانه، شناسه‌ی آلودگی و مقدار اولیه مربوط به کلید رمزنگاری را برای مهاجم ارسال می‌کند.

پس از اینکه بدافزار اطلاعات مربوط به دستگاهِ آلوده را جمع‌آوری کرد، بر روی درایو سخت به دنبال پرونده‌های خاصی گشته و آن‌ها را رمزنگاری می‌کند. در برخی نمونه‌ها مشاهده شده که باج‌افزار به انتهای پرونده‌های رمزنگاری‌شده پسوند .Xcri را اضافه کرده است ولی در برخی موارد هم پسوند خود پرونده دست‌نخورده باقی مانده است.

وقتی پرونده‌ها رمزنگاری شدند، بدافزار یک پرونده‌ی اجرایی را از یک وب‌گاه وردپرس آلوده بارگیری می‌کند. این ماژول بارگیری‌شده که مهاجمان به آن «اطلاع‌دهنده» نیز می‌گویند، پیغام باج‌خواهی را به قربانی نمایش می‌دهد و برای برگرداندن پرونده‌ها 77 دلار باج درخواست می‌کنند. این باج می‌تواند از طریق سرویس پرداخت روسی مانند Qiwi یا Yandex.Money پرداخت شود.

صفحه‌ای که در آن پیام باج‌خواهی نمایش داده می‌شود دارای یک بخش متنی نیز هست که از طریق آن قربانیان می‌توانند با مهاجم در ارتباط باشند. این بخش نیز از سرویس‌های تلگرام سوءاستفاده می‌کند.

ارتش آمریکا: برنامه‌ی پاداش در ازای اشکال برگزار خواهیم کرد



بعد از موفقیتی که در برنامه‌ی پاداش در ازای اشکال پنتاگون با نام «به پنتاگون نفوذ کنید!» حاصل شد، اینک ارتش آمریکا اعلام کرده که قصد دارد در هفته‌های آتی اولین برنامه‌ی پاداش در ازای اشکال خود را اجرا کند.

وزارت دفاع آمریکا در ماه گذشته نزدیک به 7 میلیون دلار قرارداد با گروه‌های HackerOne و Synack منعقد کرده تا در اجرای برنامه‌هایی مشابه با پاداش در ازای اشکالِ پنتاگون به سازمان‌ها کمک کنند. برنامه‌ی مربوط به ارتش آمریکا اولین برنامه‌ای است که با کمک HackerOne قرار است انجام شود.

هدف از این برنامه‌ی پاداش در ازای اشکال که «به ارتش نفوذ کنید!» نام‌گذاری شده، تکمیل کارهای کارکنان امنیت سایبری است. هنوز جزئیات زیادی از این برنامه منتشر نشده است ولی یک خبرگزاری اعلام کرده، بررسی نیازمندی‌های امنیتی وب‌گاه‌ها و پایگاه داده‌هایی که اطلاعات کارکنان در آن ذخیره می‌شود، هدف اصلی این برنامه است.

کارکنان ارتش و دولت می‌توانند در این برنامه شرکت کنند ولی مخاطب اصلی این برنامه متخصصان امنیتی خارج سازمانی هستند. برنامه‌ی نفوذ به پنتاگون در ماه آوریل و می برگزار شد و هر فرد فعال در این حوزه می‌توانست در این برنامه ثبت‌نام کند. در این برنامه نزدیک به 1400 نفوذگر ثبت‌نام کرده و 250 نفر حداقل یک گزارش آسیب‌پذیری ارسال کردند. از بین این گزارش‌هایی که ارسال شده بود، 138 مورد قابل قبول بوده و به آن‌ها جایزه تعلق گرفت. هزینه‌ی برگزاری برنامه‌ی نفوذ به پنتاگون نزدیک به 150هزار دلار بود که نصف آن به‌عنوان جایزه به شرکت‌کنندگان پرداخت شد.

وزارت دفاع حدس می‌زند برای اجرای چنین آزمون آسیب‌پذیری اگر می‌خواست از متخصصان خارج از سازمان استفاده کند، نزدیک به 1 میلیون دلار باید هزینه می‌کرد.

برخلاف نهادهای دولتی، بخش خصوصی مدت زیادی است که فهمیده برنامه‌ی پاداش در ازای اشکال بسیار مفید است. در حال حاضر شرکت‌های بزرگی مثل گوگل، یاهو و فیس‌بوک برای کشف آسیب‌پذیری‌ها در محصولات خود توسط متخصصان حوزه‌ی امنیت، میلیونی هزینه می‌کنند.