شماره اول - بهمن ۱۳۹۵

خبرنامه "آپا" دانشگاه خوارزمی

در این شماره خواهید خواند:

اضافه کردن ویژگی‌های امنیتی به ویندوز و آفیس ۳۶۵

ابزار های جدید در ویندوز و آفیس ۳۶۵ به مدیریت بهتر دستگاه ها و امنیت سایبری آنها کمک می کند. - صفحه ۲

- **ارتش ربات ها در مقابل کلاهبرداران تلفنی**

هر کسی ممکن است تماسی از سوی کلاهبرداران اینترنتی دریافت کرده باشد. آنها مردم را اغوا می کنند تا بدافزارهایی روی کامپیوترهایشان نصب کنند، یا جزئیات شماره کارت اعتباری شان را در دسترس قرار دهند. بنابراین، اطلاع داشتن از روشهای مقابله با آنها مفید به نظر می رسد. - صفحه ۳

ویروس Stuxnet یا Dugu؟

بیش از ۱۰۰ بانک در سراسر دنیا توسط نوعی از بدافزار بدون فایل مرتبط با Stuxnetمورد تهاجم قرار گرفتند. - صفحه۴

Microsoft

مخاطرات امنیتی در محصولات مایکروسافت در ماه اول سال ۲۰۱۷

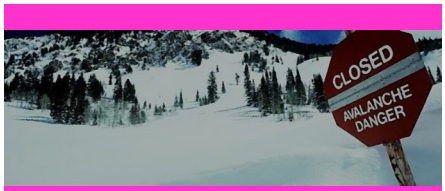
لیستی از مخاطرات امنیتی و آسیب پذیری-های مایکروسافت را در این صفحه ببینید. - صفحه ۷

- **آیا تمامی هک‌ها مخرب‌اند؟**

تمامی هک‌ها مخرب نیستند. از نمونه هک‌هایی که می‌توان گفت با نیت و هدف مثبت انجام شدند می توان حمله به سرورهای سرویس‌ها و وب سایت های کودک آزاری را نام برد. - صفحه ۶

بررسی ابعاد سقوط وب سایت LeakedSource

روز پنج شنبه، ۲۶ ژانویه ۲۰۱۷ وب سایت LeakedSource که در زمینه اطلاع رسانی نقض حقوق حساب‌های کاربری فعالیت می‌کرد، به طور کاملا ناگهانی سقوط کرد. - صفحه ۷



بهمن، زیرساختی برای جاسوس افزارها

"بهمن" به یک زیرساخت شبکه میزبانی بزرگ اشاره دارد که توسط مجرمان اینترنتی برای اهدافی چون فیشینگ، توزیع بد افزار و برنامه های کسب پول مورد استفاده قرار می‌گیرد. - صفحه ۱۰

- **خطرات امنیتی شبکه‌های خصوصی مجازی**

رشد وی پی ان ها را می‌توان همگام با رشد نرم افزارهایی چون ویرایشگرهای عکس و تصاویر دانست. با توجه به ساز و کار وی پی ان ها، بسیاری از آنها از نظر امنیتی مخرب بوده و می‌توان از آنها به عنوان یک کابوس امنیتی یاد کرد.- صفحه ۸ و ۹

اضافه کردن ویژگی‌های امنیتی به ویندوز و آفیس ۳۶۵

مایکروسافت در راستای کمک به صنعت IT در سراسر دنیا، در کنفرانس امنیتی RSA، این غول نرم افزاری اعلام کرد:

ابزار های جدید در ویندوز و آفیس ۳۶۵ به مدیریت بهتر دستگاه ها و امنیت سایبری آنها کمک می کند. سیستم احراز هویت بیومتریک ویندوز به نام "سلام" در نسخه ۱۰ ویندوز دارای دو به روز رسانی است. این سرویس اکنون با سیستم های اکتیو دایرکتوری سمت سایت کاملا سازگار است. برای دستگاه هایی که از طریق بلوتوث ارتباط برقرار می کنند ، ویژگی جدید قفل خودکار قابل دسترسی خواهد بود. کاربران می توانند رایانه و تلفن همراه خود را همگام سازی کنند تا در صورتی که از پشت میز کار خود تا حد معینی دور شدند رایانه آنها خود به خود قفل شود. این ویژگی بسیار به ویژگی دستگاه مورد اعتماد اندروید شباهت دارد.

دستگاه های سرفیس واجد ویژگی جدید "حالت مدیریت" خواهند شد که موجب سطح بندی در قسمت سخت افزار خواهد شد مانند غیرفعال کردن میکروفن یا اتصال به شبکه تا روش های سنتی هک از نفوذ به آن ناتوان باشند. همچنین قادر است تا با فناوری های سیاست گروهی و مدیریت دستگاه های تلفن همراه (MDM) یک پارچه شود تا روند مدیریت دستگاه ها را برای کاربران تسهیل نماید.

آفیس ۳۶۵ نیز دارای ابزار مدیریت امنیتی خودکار برای سازمان هاست که وظیفه آن، تحلیل چگونگی توسعه ویژگی های امنیتی سازمان و رتبه دهی به آنهاست. کاربران همچنین می توانند مشاهده کنند که چه تنظیمات دیگر امنیتی دیگری به منظور پیاده سازی قابل دسترسی است . در این زمینه به زودی سرویس "اطلاعات تهدید" برای آفیس ۳۶۵ راه اندازی خواهد شد که مسئولیت آن ، ارائه تحلیل های عمیق در مورد نقاط ضعف امنیتی به کاربران است.

گردآورنده: حسین علیمرادی

برنامه نویسان به وسیله ارتش ربات ها در مقابل کلاهبرداران تلفنی

هر کسی ممکن است تماسی از سوی کلاهبرداران اینترنتی دریافت کرده باشد. آنها مردم را اغوا می کنند تا بدافزارهایی روی کامپیوترهایشان نصب کنند، یا جزئیات شماره کارت اعتباری شان را در دسترس قرار دهند. بنابراین، اطلاع داشتن از روشهای مقابله با آنها مفید به نظر می رسد.

راجر اندرسون - مشاور مخابرات و صاحب شرکت مخابراتی جولی راجر- بعد از افشای صحبت نامناسب یک فروشنده تلفنی با پسرش، تصمیم گرفت یک ربات تلفنی در مقابل این کلاهبرداران طراحی کند که در حال حاضر آن را به تجار و مصرف کنندگان به فروش می رساند. روش کار ربات به این صورت است که هرگاه یک فروشنده تلفنی (تله مارکتر) تماس می گیرد، افراد می توانند بدون اینکه فروشنده متوجه شود، تماس را به رباتی که صدایی مشابه انسان دارد منتقل نمایند. این ربات می تواند با شخص صحبت کند تا زمانی که خود فروشنده متوجه شود با یک انسان واقعی صحبت نمی کند! ربات به گونه ای طراحی شده است که پاسخ های کلی می دهد مثل »بله«، »اوهوم«، »در حال گوش کردم هستم «البته این صحبت های عمومی همراه با ترفند هایی است مثلا: اوه خدای من، صبرکن! یک زنبور روی آرنج من نشسته، من بخاطر این زنبور مجبورم تکان نخورم و ساکت بمانم، اما شما به صحبت خود ادامه دهید .«صدای ضبط شده ی دیگر شامل صدای یک خانم است که با دخترش در حال دعواست! برای موارد بیشتر می توانید به یوتوب شرکت مراجعه کنید.

بعد از اینکه اندرسون یک پیام تبلیغاتی کلاهبردارانه از "عامل پشتیبانی ویندوز" را در کامپیوتر شخصی خود دریافت کرد، تصمیم گرفت تا ارتش رباتش را در مقابل این کلاهبرداران نیز فرو ببارد!

"من پیام های تبلیغاتی که مدام می گویند کامپیوترم آلوده شده، خسته شده بودم. احساس می کردم مورد هجمه قرار گرفته ام. متوجه شدم که اینها کلاهبرداری است. از بین تمام افراد روی زمین، من تقریبا تنها کسی هستم که تکنولوژی ضربه زدن به تماس های تلفنی مزاحم را دارد. ربات هایی در اختیار دارم که صدایشان به قدر کافی شبیه به انسان است تا وقت کلاهبرداران را تلف کند" ین جملاتی است که اندرسون به شرکت Business Insider گفت. اندرسون تاکید کرد که هرگز از این ربات ها به منظور تماس های خارج از محدوده برای سوءاستفاده نکرده است، و فقط در مقابل کلاهبرداران از آنها بهره برده است. او ابتدا با شماره ای که روی صفحه مانیتورش تبلیغات فرستاده بود تماس گرفت تا مطمئن شود پیام از سوی کلاهبردار است، نه پیام واقعی. سپس یکی از ربات ها را جهت تماس با آن فعال کرد، به گونه ای که صدای ربات، شخص کلاهبردار را متقاعد کرد تا بیش از پنج دقیقه با آن صحبت کند. در همین زمان، اندرسون آنها را با قدرت تمام شوکه کرد!

به این صورت که وی گفت: "من ۱۰۰ مرتبه به طور همزمان با ۲۰ شبکه (با همین شماره مزاحم) تماس گرفتم. آنها پاسخ دادند و با ربات های من صحبت کردند. سپس آنها ربات های مرا پشت خط در انتظار نگه داشتند، سپس شروع کردن به ناسزا گفتن به یکدیگر و فریاد زدن که چه اتفاقی اتفاده است، من می توانستم آنچه در پشت خط اتفاق می افتد را بشنوم. سپس، با همین شماره، ۵۰۰ تماس دیگر با ۲۰ شبکه ی دیگر به صورت همزمان گرفتم. بعد از ۳۰۰ تماس آنها شماره را قطع کردند"

در طول فقط ۱۵-۲۰ دقیقه، اندرسون کار شرکت کلاهبرداری را یکسره کرد. حالا شماره ی تبلیغاتی مزاحم آن شرکت از رده خارج شد. به خاطر این کار از وی متشکریم. اندرسون گفت: "من به طور کامل آنها را نابود کردم"

وی از مردم می خواهد تا شماره های کلاهبرداران که مشابه اینگونه پیام ها را به آنها می فرستند، به او گزارش دهند تا همین بلا را سر آنها بیاورد. اگر شما شماره ای از یک فروشنده تلفنی کلاهبردار دارید که فکر می کنید باید مورد هدف قرار گیرد، کافی است به شرکت اندرسون ایمیل بزنید ."من به شما اطمینان می دهم تلفن های شرکت من بیشتر از آنهاست، حتی اگر آنها تلفن یک ربات را نیز قطع کنند باز هم من می توانم مرکز تماس آنها را ببندم تا از افراد کمتری کلاهبردای کنند".

گردآورنده: حسین علیمرادی

ویروس Stuxnet یا Dugu ؟

بیش از ۱۰۰ بانک در سراسر دنیا توسط نوعی از بدافزار بدون فایل مرتبط با Stuxnet مورد تهاجم قرار گرفتند

هفت سال پیش ویروس Stuxnet توسط نیروهای فضای مجازی آمریکا و اسرائیل تولید شد و به سیستم های اتمی ایران نفوذ کرد و خسارات و تبعات آن موجب شد تا صنعت هسته ای این کشور به دوسال قبل برگردد . اکنون بدافزاری مشابه آن توانسته بیش از ۱۰۰ بانک در دنیا را مورد آسیب پذیری قراردهد . نیروی امنیت فضای مجازی ورسیه با همکاری لابراتوار کاسپرسکای اولین نسخه تکامل یافته این ویروس با نام Duqu 2.0 را شناسایی کردند. کاسپرسکای در تحقیقات اخیر که این بدافزار توانسته به شدت رشد کند و در ۴۰ کشور و حداقل ۱۴۰ موسسه شامل بانک ها ، سازمان های دولتی و شرکت های ارتباطی یافت شده است. تنها ۲۱ مورد آن در آمریکا است.

بعد از اینکه کامپیوتر قربانی بعد از تهاجم برای بار نخست روشن و خاموش می شود ، این بدافزار نام خود را تغییر میدهد تا ردیابی آن توسط کارشناسان امنیتی دشوار گردد. این ویژگی توسط تیم امنیتی یک بانک مورد هدف شناسایی شد درست زمانی که یک نسخه کپی از متاپرتر (جزئی از متا اکسپلویت) را در حافظه فیزیکی بخش کنترلر دامین ماکروسافت پیدا کردند. محققین دریافتند که این بخش از کد توسط پاورشل به حافظه داخلی تزریق شده بود.

یکی از کارشناسان کاسپرسکای در این مورد اظهار داشت: ما فعلا در حال تحقیق بر روی چگونگی عملکرد ویروس هستیم که چگونه تواسته از پاورشل ترکیبی استفاده کند تا مترپرتر را دانلود کند و به سوی منابع سیستمی ویندوز گسیل دهد و از آنها بهره برداری کند.

در مورد اینکه این بدافزار به چه میزان میتواند به روند صعودی خود در آلوده کردن سیستم های مختلف ادامه دهد هنوز نظر دقیقی در دسترس نیست و کارشناسان کاسپرسکای اعلام کرده اند که در آینده جزیئات بیشتری از تحلیل رفتار این ویروس در اختیار خواهند گذاشت.

گردآورنده: حسین علیمرادی

مخاطرات امنیتی در محصولات مایکروسافت در ماه اول سال ۲۰۱۷ و بسته به روزرسانی مربوطه جهت رفع مشکل

نرم افزار	خلاصه	به روز رسانی	شماره به روز رسانی	CVE ID
Microsoft Windows, Microsoft Edge	یک آسیب پذیری امنیتی در Microsoft Edge است و می تواند حقوق دسترسی را در صورت مشاهده یک صفحه خاص افزایش دهد. مهاجمی که موفق به بهره برداری از این آسیب پذیری شود می تواند مجوز بالایی را در دایرکتوری فضا نام یک سیستم آسیب پذیر به دست آورد.	Security Update for Microsoft Edge	۳۲۱۴۲۸ ۸	CVE-2017-0002
Microsoft Office, Microsoft Office Services and Web Apps	یک آسیب پذیری امنیتی در Microsoft Office است و می تواند یک قطعه کد دستکاری شده را از راه دور اجرا کند. مهاجمی که موفق به بهره برداری از این آسیب پذیری شود می تواند یک کد دلخواه را در زمینه سیستم آسیب دیده اجرا کند. کاربران با حقوق دسترسی محدودتر در سیستم کم تر در معرض این آسیب قرار دارند.	Security Update for Microsoft Office	۳۲۱۴۲۹ ۱	CVE-2017-0003
Microsoft Windows, Adobe Flash Player	یک آسیب پذیری امنیتی در Adobe Flash Player برای تمامی نسخه های ویندوز ۸.۱، ویندوز سرور ۲۰۱۲، ویندوز سرور ۲۰۱۲ R2، ویندوز RT 8.1، ویندوز ۱۰ و ویندوز سرور ۲۰۱۶ است.	Security Update for Adobe Flash Player	۳۲۱۴۶۲ ۸	APSB17-02
Microsoft Windows	یک آسیب پذیری امنیتی در خدمت رسانی زیرسیستم امنیتی تشخیص هویت محلی (LSASS) است. مهاجمی که موفق به بهره برداری از این آسیب پذیری می شود می تواند یک انسداد سرویس در خدمات LSASSایجاد کند و باعث راه اندازی مجدد سیستم هدف به صورت خودکار شود.	Security Update for Local Security Authority Subsystem Service	۳۲۱۶۷۷ ۱	CVE-2017-0004

گردآورنده: امین زمانی

آیا تمامی هک‌ها مخرب‌اند؟

تمامی هک‌ها مخرب نیستند. از نمونه هک‌هایی که می‌توان گفت با نیت و هدف مثبت انجام شدند می‌توان حمله به سرورهای سرویس‌ها و وب سایت‌های کودک آزاری را نام برد. از نمونه‌های دیگر این نوع هک های غیر مخرب می‌توان به هک ۱۵۰ هزار پرینتر متصل به اینترنت، توسط یک جوان ۲۳ ساله با نام مستعار Stackoverflowin اشاره کرد. هدف چنین حمله‌ای، همانطور که در ادامه نیز به صورت ضمنی به آن اشاره شده، می‌تواند نوعی آگاهی رسانی به صاحبان کسب و کارها برای حفاظت از تجهیزات متصل به اینترنتشان باشد.

در حمله مذکور، طی یک آخر هفته، پرینترهای بسیاری از ادارات، خانه‌ها و حتی رستوران‌ها به طور کاملا ناگهانی شروع به چاپ پیام‌هایی با محتوای "اخطار نسبت به بستن درگاه‌های باز" کردند. محتوای متون چاپ شده نیز غالبا آدرس ایمیل و توئیتر نام هکر، Stackoverflowin، به همراه تصاویری از ربات و کامپیوتر بود که با استفاده از حروف ASCII کشیده شده بودند.

اما این فرآیند چگونه انجام شد؟

Stackoverflowin این کار را از طریق نوشتن و اجرای اتوماتیک یک اسکریپت انجام داد. اسکریپت مورد نظر وی به صورت خودکار به جستجوی پورت‌های باز پرینترها می‌پرداخت و فرمان چاپ را به این پرینترهای آسیب‌پذیر ارسال می‌کرد.

وی در مصاحبه با وب سایت Bleeping Computer به بیان جزئیات عملکرد این روش هک می‌پردازد و می‌گوید: "پرینترهای آسیب‌پذیر نسبت به این روش حمله، پرینترهایی بودند که پورت پروتکل اینترنتی چاپ، پورت پروتکل چاپ ریموت، و پورت ۹۱۰۰ در آنها باز بودند. این اسکریپت همچنین شامل یک اکسپلویت یا کد مخرب بود که با سوء استفاده از آسیب پذیری اجرای کد به صورت ریموت در پرینترهای Dell Xeon، آنها را مورد حمله و هدف قرار می‌داد."

هر چند که این به اصطلاح حمله، موجب آسیب به پرینترهای تولیدی شرکت های مختلفی چون HP، Dell، Samsung و... شد، اما Stackoverflowin همچنان بر اهداف غیر تخریبی خود در این اقدام تاکید داشت. به گفته این هکر جوان تنها هدف وی، آگاهی مردم و بخصوص سازمان‌ها از خطرات و ریسک موجود در شبکه و کمک به آنها برای حفظ امنیت دستگاه‌هایشان در مقابل حملات جدی احتمالی بود. هر چند که این آگاهی‌رسانی به طریقی غیرحرفه‌ای و پرخطر از طرف وی انجام گرفته است.

گردآورنده: شیوا بهادری

بررسی ابعاد سقوط وب سایت LeakedSource

روز پنج شنبه، ۲۶ ژانویه ۲۰۱۷ وب سایت LeakedSource که در زمینه اطلاع رسانی نقض حقوق حساب‌های کاربری فعالیت می‌کرد، به طور کاملا ناگهانی سقوط کرد و بسیاری از فعالین حوزه‌های امنیت را متعجب ساخت. یکی از محققین خوشنام حوزه امنیت، آقای Troy Hunt، که بر روی سرویسی مشابه سرویس LeakedSource به نام Have I Been Bwned فعالیت می‌کند، به بررسی این مساله پرداخته است.

همانطور که وب سایت ZDNet به آن اشاره می‌کند، LeakedSource یک سرویس انتفاعی در زمینه اطلاع رسانی نقض حقوق اطلاعات و داده ها بود که در زمینه اطلاع‌رسانی اخبار مربوط به نقض داده های حساب‌های کاربری شرکت‌ها و موسسات بزرگی چون Twitter، MySpace و LinkedIn در سال ۲۰۱۶ نقش بسزایی داشت. تنها چند روز پس از این حادثه و قبل از تائید رسمی وقوع آن، برخی وب سایت‌ها و فروم‌های خبری به مورد زیر اشاره کردند:

LeakedSource برای همیشه از کار افتاده و باز نخواهد گشت. صاحبان این سرویس همان روز حادثه مورد بازجویی قرار گرفتند، و فرآیند رسیدگی، تنها به جمع‌آوری منابع ذخیره‌سازی داده‌ها و اطلاعات این وبسایت به همراه سرورهای مورد استفاده آنها اکتفا کرد تا تحت تحقیق و بررسی مقامات فدرال قرار گیرند.

همانطور که آقای Hunt نیز پس از وقوع این حادثه در وبلاگ خود به آن اشاره می‌کند، LeakedSource سرویسی انتفاعی در زمینه اطلاع رسانی نقض حقوق داده‌ها و اطلاعات بود که به کاربران عادی این امکان را می‌داد تا نسبت به اطلاعات حساب‌های کاربری خود و امکان نقض حقوق کاربری خود (به طور مثال امکان انتشار اطلاعات حساب‌هایشان) آگاهی پیدا کنند؛

علاوه بر این، این سرویس در زمینه فروش داده‌های خام حساب‌های نقض شده به افراد متقاضی فعالیت می‌کرد. جالب است که آقای Hunt در اواخر سال ۲۰۱۶ ادعای امکان بروز شبهه در فعالیت های این سرویس را مطرح کرده بود. در آن سال، این محقق امنیتی ادعا می‌کند که به طور مثال جریان‌های داده‌ای ثابتی از داده‌ها در این سرویس ظاهر شده که تا قبل از آن در هیچ یک از محافل معمول تجاری مشاهده نشده است.

در حالیکه تا مدتی پیش گمانه‌زنی ها بر درستی این حدس صحه می گذاشتند، اکنون Hunt با قاطعیت این ادعا را مطرح می‌کند که سرویس LeakedSource به هکرها پیشنهاد می‌کرده تا با استفاده از داده‌های در دسترس این سرویس، حساب‌های هدف دیگری که قابلیت افزوده شدن به پایگاه داده این سرویس داشتند را شناسایی کنند و

با فروش داده‌های آن حساب‌ها به متقاضیان خرید، کسب درآمد کنند. علاقه‌مندان برای کسب اطلاعات بیشتر در ارتباط با سابقه فعالیت‌های LeakedSource می‌توانند به منابع سایت WIRED در این زمینه مراجعه کنند. همینطور مطالعه پست‌های وبلاگ آقای Hunt که بعضا به بررسی جزئیات قوانین پیش روی این سرویس پرداخته، خالی از لطف نیست.

گردآورنده: شیوا بهادری

بررسی خطرات امنیتی شبکه‌های خصوصی مجازی (معرفی ۱۰ نمونه خطرناک)

شبکه های خصوصی مجازی یا وی پی ان همواره از محبوبیت زیادی بین کاربران کامپیوترها برخوردار بوده اند. در سال های اخیر و با رشد ابزارهای هوشمند مبتنی بر اندروید، محبوبیت این نوع شبکه ها بین کاربران این دستگاه‌ها نیز در حال رشد است؛ بطوریکه رشد وی پی ان ها را می‌توان همگام با رشد نرم افزارهایی چون ویرایشگرهای عکس و تصاویر دانست. محققان دریافته‌اند با توجه به ساز و کار وی پی ان ها که در نتیجه آن، به داده‌های مکانی کاربران دسترسی پیدا خواهند کرد، بسیاری از آنها از نظر امنیتی مخرب بوده و می توان از آنها به عنوان یک کابوس امنیتی یاد کرد.

سازمان پژوهش‌های علمی و صنعتی همسود استرالیا به همراهی گروهی از محققان حوزه امنیت از دانشگاه ولز و دانشگاه کالیفرنیا (برکلی) به تحلیل و بررسی ۲۸۳ وی پی ان موجود در فروشگاه گوگل پرداخته اند. نتایج بررسی‌های آنها نشان می‌دهد که:

۳۸٪ از وی پی ان های بررسی شده دارای یک یا چند نوع از آگهی افزارها، تروجان ها، خطرافزارها یا نرم افزارهای جاسوسی هستند.

۶۷٪ از ۲۸۳ وی پی ان تحلیل شده، حداقل توسط یک کتابخانه شخص ثالث ردیابی می‌شوند.

۸۲٪ از این وی پی ان ها به هنگام استفاده کاربر، درخواست های دسترسی به اطلاعات حساسی همچون حساب های کاربری و پیام‌های متنی به وی اعلام می‌کنند.

اما نقاط ضعف این نوع وی پی ان ها به همین اینجا ختم نمی شود. از دیگر نقاط کور وی پی ان های پلتفرم های اندروید می‌توان به موارد زیر اشاره کرد:

۱۸٪ از این وی پی ان ها ترافیک شبکه را رمزگذاری نمی‌کنند.

۱۶٪ از آنها ترافیک را از طریق وی پی ان سایر کاربران (و نه سرورهای مشخص و اختصاصی) مسیریابی می‌کنند.

۸۴٪ از آنها دارای نشت ترافیک در IPv6 هستند.

۶۶٪ از آنها دارای نشت ترافیک در DNS می‌باشند.

در گزارش این گروه به این نکته اشاره شده که نبود رمزگذاری قوی و نشت ترافیک، هر دو می تواند فرآیند ردیابی آنلاین، که عموما توسط دستگاه های میانی شبکه (از طریق استخراج داده های کاربران وای فای های تجاری) یا سازمان‌های ناظر انجام می‌شود را تسهیل کند.

نکته جالب توجه اینجاست که علیرغم تمامی مشکلات ذکر شده، علاقه‌مندی به استفاده از وی پی ان ها کاهش پیدا نکرده است. بطوریکه ۳۷٪ از وی پی ان های تحلیل شده، بیش از ۵۰۰ هزار بار توسط کاربران نصب شده اند و ۲۵٪ از آنها در رتبه بندی و امتیازدهی، ۴ ستاره توسط کاربران به خود اختصاص داده‌اند.

در گزارش ارائه شده، لیست ۱۰ مورد از بدترین وی پی ان های اعلام شده توسط این گروه ارائه شده است. این وی پی ان ها مبتنی بر یافته‌های این محققین و درجه‌بندی‌شان با استفاده از اسکن آنها توسط نرم‌افزارهای آنتی ویروس مشخص شده‌اند. نکته جالب توجه این است که با اعلام نام این وی پی ان ها، برخی از آنها مانند OKVpn، EasyVPN و sFly Network Booster دیگر در فروشگاه گوگل در دسترس نیستند.

گردآورنده: شیوا بهادری

بررسی خطرات امنیتی شبکه‌های خصوصی مجازی (معرفی ۱۰ نمونه خطرناک)

ردیف	نام vpn	کلاس vpn	رتبه vpn	تعداد نصب شده توسط کاربران	رتبه‌بندی بر اساس اسکن با آنتی ویروس
۱	OkVpn	نسخه تبلیغاتی (اولیه)	۴.۲	۱۰۰۰ نفر	۲۴
۲	EasyVpn	نسخه تبلیغاتی	۴.۰	۵۰۰۰۰ نفر	۲۲
۳	SuperVPN	نسخه رایگان	۳.۹	۱۰۰۰۰ نفر	۱۳
۴	Betternet	نسخه رایگان	۴.۳	۵ میلیون نفر	۱۳
۵	CrossVpn	نسخه رایگان	۴.۲	۱۰۰۰۰۰ نفر	۱۱
۶	Archie VPN	نسخه رایگان	۴.۳	۱۰۰۰۰ نفر	۱۰
۷	Hat VPN	نسخه رایگان	۴.۰	۵۰۰۰ نفر	۱۰
۸	sFly Network Booster	نسخه تبلیغاتی	۴.۳	۱۰۰۰ نفر	۱۰
۹	One Click Vpn	نسخه رایگان	۴.۳	۱ میلیون نفر	۶
۱۰	Fast Secure Payment	نسخه تبلیغاتی	۴.۱	۵۰۰۰ نفر	۵

علیرغم تمامی خطراتی که متوجه وی پی ان هاست، تنها درصد اندکی از کاربران –حدود ۱٪- نسبت به تبعات پرریسک استفاده از برخی وی پی ان ها توجه دارند. لزوم تحقیق در ارتباط با این نوع از ابزارها، امری اجتناب ناپذیر است. بخصوص زمانیکه نوع رایگان آنها مورد نظر کاربر است.

گردآورنده: شیوا بهادری

بهمن، زیرساختی برای جاسوس افزارها

"بهمن" به یک زیرساخت شبکه میزبانی بزرگ اشاره دارد که توسط مجرمان اینترنتی برای اهدافی چون حملات فیشینگ، توزیع بد افزار و برنامه های کسب پول مورد استفاده قرار میگیرد. وزارت امنیت ایالات متحده با کمک اداره ی تحقیقات فدرال (FBI) به انتشار این هشدار و اطلاعات فنی در خصوص "بهمن" پرداخته اند.

مجرمان اینترنتی با استفاده از زیر ساخت های باتنت بهمن به میزبانی و توزیع بدافزارهای متنوع برای انواع قربانیان، از جمله هدف قرار دادن ۴۰ موسسه ی مالی بزرگ. قربانیان ممکن است با این بدافزارها اطلاعات حساس خود (ازجمله حساب کاربری مشتریان) را از دست بدهند. سیستم های قربانیان ممکن است همچنین برای انجام سایر فعالیت های مخرب دیگر به خطر بیوفتد. همانند حملات DoS و استفاده از قربانیان برای گسترش سایر بد افزارها.

زیرساخت شبکه های بهمن برای اجرای طرح های مالی مجرمانه نیز استفاده میگردد. در این روش جنایتکاران از افراد برای انتقال پول و یا کالا های به سرقت رفته ویا پولشویی استفاده می کنند.

شبکه بهمن از DNS های شار-سریع، روشی برای پنهان کردن سرورهای جنایتکاران در پشت یک سیستم همواره در حال تغییر همانند یک پراکسی استفاده می کند. در زیر نام بدافزارهایی که برروی این زیر ساخت قرار میگیرند آورده شده اند:

- Windows-encryption Trojan horse (WVT) (aka Matsnu, Injec-tor,Rannoh,Ransomlock.P)
- URLzone (aka Bebloh)
- Citadel
- VM-ZeuS (aka KINS)
- Bugat (aka Feodo, Geodo, Cridex, Dridex, Emotet)
- newGOZ (aka GameOver-ZeuS)
- Tinba (aka TinyBanker)
- Nymaim/GozNym
- Vawtrak (aka Neverquest)
- Marcher
- Pandabanker
- Ranbyus
- Smart App
- TeslaCrypt
- iBanking Trusteer App Tro-jan
- Xswkit

شبکه های بهمن همچنین به عنوان باتنت های شار سریع برای ارتباط سایر باتنت های زیرساخت مورد استفاده قرار می گیرند که در زیر عنوان چندین مورد از آن آورده شده است:

- GetTiny
- Matsnu
- Rovnix
- Urlzone
- QakBot (aka Qbot, PinkSlip Bot)

تاثیر

سیستم ها و کامپیوترهایی که با بد افزارهای بهمن آلوده می شوند ممکن است دست به فعالیت های مخربی همانند سرقت اعتبار کاربران ویا سایر اطلاعات حساس همانند اطلاعات حساب های بانکی و کارت های اعتباری نمایند. برخی از این بدافزارها قابلیت رمزنگاری تمامی اطلاعات کاربران را دارند که در نتیجه ی آن کاربر را ملزم به پرداخت مبلغی برای بازگرداندن اطلاعاتش می کنند. به این بد افزارها باج افزار می گویند. همچنین گونه ای دیگر از بد افزارها به جنایتکاران اجازه ی دسترسی بدون محدودیت به کامپیوتر قربانی را برای انجام هر اموری می دهند. کامپیوترهای آلوده برای حمله هایی چون DDoS مورد استفاده قرار می گیرد.

راه حل

برای جلوگیری از آلوده شدن سیستم های کامپیوتری به این بد افزارها می توان از آنتی ویروس های زیر استفاده نمود.

ESET Online Scanner
F-Secure
McAfee Stinger
Microsoft Safety Scanner
Norton Power Eraser
Trend Micro HouseCall

گردآورنده: محمد مرتضوی

Kharazmi CERT Coordinator Center

مرکز آپا دانشگاه خوارزمی

مدیر مسئول:

دکتر امید مهدی عبادتی

هیات علمی:

دکتر احسان ملکیان

کارشناسان مرکز:

محمدحسین خدامی

سمیه نیا خلیلی

محمد مرتضوی

امین زمانی

حسین علیمرادی

شیوا بهادری

محسن یزدی نژاد

نشانی:

کرج - دانشگاه خوارزمی - کتابخانه‌ی مرکزی - طبقه‌ی همکف - مرکز آپا

تلفن:

۰۲۶۳۴۵۷۵۰۱۲

۰۲۶۳۴۵۷۵۰۱۸

۰۲۶۳۴۵۷۹۶۰۰ (داخلی ۲۶۲۲)

وب سایت:

http://cert.khu.ac.ir/