شماره اول – نیمه اول آبان ۱۳۹۶

خبرنامه "آپا" دانشگاه محقق اردبیلی

045 31505718

cert@uma.ac.ir

اردبیل - خیابان دانشگاه - دانشگاه محقق اردبیلی

پنهان شدن «سیا» پشت کاسپرسکی روسی

سازمان سیا منبع ویروس‌های خود را با استفاده از نام «کاسپرسکی» مخفی می‌کند.

با استناد به سایت «ویکی لیکس»، کد ویژه ساخته شده توسط سازمان «سیا» آمریکا امکان استتار برنامه‌های ویروسی سازمان را ممکن می‌سازد که هنگام بررسی منبع ویروس، سازمان و شرکت‌ها و از جمله شرکت روسی ضد ویروس«لاباراتوریا کاسپرسکی» نشان داده می‌شوند.

مطابق با داده‌های سایت ویکی لیکس ابزار جدید «هایو» عنوان شده است. هدف آن این است که حتی با کشف ویروس در کامپیوتر، برنامه اشاره‌ای به سازنده آن «سیا» نمی‌کند. با کمک «هایو» می‌توان چند برنامه ویروسی را در دامین‌های مختلفی که سازمان «سیا» در سرورهای عمومی اجاره می‌کند بکار انداخت.

در سایت نامبرده گفته می‌شود که در سه مورد ابزار ویروسی به شبیه‌سازی مجوزهای شرکت «کاسپرسکی» دست زده است.

وزارت امنیت ملی آمریکا به تمام ادارات دولتی و شرکت‌های مرتبط با آنها سه ماه مهلت داد تا اقدامات خودداری استفاده از برنامه ضد ویروس «کاسپرسکی» را به انجام برسانند، زیرا به گفته وزارت امنیت ملی آمریکا، ممکن است از برنامه «کاسپرسکی» برای آسیب به امنیت ملی آمریکا استفاده شود.

در شرکت «کاسپرسکی» اطمینان دادند که این شرکت در جاسوسی سایبری به هیچ کشوری کمک نمی‌کند.

منبع: https://t.me/ict_security

وضعیت حملات امنیتی به صنایع جهانی اکتبر ۲۰۱۷

به گزارش کاسپرسکی ۱۵ کشوری که بیشترین حملات صنعتی را در ماه اکتبر داشته اند به شرح زیر می باشد. کشورها به ترتیب از اول عبارت‌اند: ویتنام، الجزیره، مراکش، اندونزی، چین، پرو، عربستان سعودی، هند، جمهوری اسلامی ایران، امارات، مالزی، مکزیک، ترکیه، قزاقستان و تایوان

منبع: کاسپرسکی

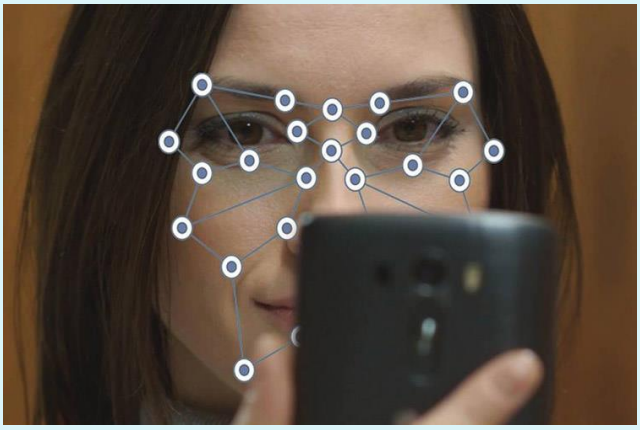
نسخه تقلبی برنامه واتساپ با یک میلیون دانلود

براساس گزارش کاربران وب‌سایت reddit یک نسخه تقلبی از برنامه واتساپ در فروشگاه معتبر Google Play بیش از یک میلیون دانلود داشته است. این برنامه که به ویروس تبلیغاتی آلوده بوده است به کمک اضافه نمودن یک فاصله بین دو کاراکتر نامی مشابه نام شرکت سازنده برنامه یعنی WhatsApp inc انتخاب و از این طریق اعتماد کاربران را جلب نموده بود. البته در حال حاضر این برنامه از فروشگاه Google Paly حذف گردیده است. در حال حاضر با جستجوی «واتساپ» تعداد برنامه های نمایش داده شده در نتایج قابل تامل می‌باشد.

منبع:

https://www.hackread.com/1-million-android-users-downloaded-fake-whatsapp-app/

دنیای پس از رمزعبور چگونه خواهد بود؟



امروزه حفظ امنیت سایبری به یکی از مشکل‌های عمده‌ی شرکت‌های بزرگ تبدیل شده است .به این منظور روش‌های مختلف و جدیدی برای حفظ امنیت بیشتر ارائه شده‌اند که در این مقاله به آن‌ها می‌پردازیم.

هدف بسیاری از شرکت‌ها احراز هویت مشتری و شناسه‌های کارمندی به شیوه‌ای تقریبا نامرئی است که تنها یک ثانیه زمان ببرد. برای مثال می‌توان به ورود یک خریدار به وب‌سایت، یا اجرای عملیات در پشت‌صحنه در حین فعالیت کارمندان اشاره کرد. برای دستیابی به این هدف و توانایی بررسی دقیق هویت کارمندان و مشتریان، شرکت‌ها از فناوری‌های جدید مثل اسکن‌های بیومتریک چهره و اثر انگشت و سیستم‌های نظارت بر رفتار استفاده می‌کنند، برای مثال این سیستم‌ها نشان می‌دهند شما اخیرا از کدام برنامه بیشتر استفاده کردید. با حرفه‌ای‌تر شدن هکرها، رمزعبورهای سنتی امنیت کمتری خواهند داشت. داده‌های اخیر سازمان گزارش اعتبار Equifax احتمال افزایش سؤال‌هایی در مورد استفاده از شماره‌های امنیت اجتماعی و داده‌های شخصی دیگر برای احراز هویت یک شخص و پیشبرد بهتر روش‌های احراز هویت را بالا می‌برد. با این که امنیت مساله‌ی بسیار مهمی است، شرکت‌ها به دنبال ارائه‌ی یک تجربه‌ی یکپارچه برای کارمندان و مشتریانی هستند که نمی‌خواهند زیاد درگیر رمزهای عبور شوند. شرکت مستر کارت لپ‌تاپ‌هایی را در اختیار کارمندان خود گذاشته است که مجهز به قرائت‌گرهای تعبیه‌شده‌ی اثر انگشت و یک فناوری تست هستند که چهره‌ی کارمندان را قبل از ورود به ساختمان اداره اسکن می‌کند. مسترکارد با بررسی یک قابلیت پیشرفته‌ی دیگر، موفق به دستیابی به فناوری NuData شد که قادر به شناسایی مشتریان بر اساس نحوه‌ی گرفتن تلفن همراه و دیگر رفتارهای بیومتریک است. به گفته‌ی ران گرین، مدیر امنیتی مسترکارد، نیروی محرکه و روبه‌جلو، حذف رمزهای عبور است. شرکت‌ها با کار روی امنیت بدون مداخله در تجربه‌ی کاربری، قدم در یک راه باریک می‌گذارند. در صورتی که نیازی به رمز عبور نباشد، ممکن است داده‌های بعضی مشتریان از امنیت کمتری برخوردار باشند. اما اگر برنامه‌های مبتنی بر رفتار بسیار حساس باشند و بر اساس منطق مثبت کاذب مثل مسدودسازی دسترسی کاربری که حروف را اشتباه تایپ کرده عمل کنند، این مساله آزار دهنده خواهد بود. استیو ویلسون، محقق در زمینه‌ی هویت دیجیتال و معاون و تحلیل‌گر ارشد مؤسسه‌ی تحقیقاتی Constellation می‌گوید: با پیشرفت فناوری، تشخیص چهره هم با چالش‌های مشابهی روبه‌رو خواهد شد. برای مثال یک اتاق کم‌نور یا صورت اصلاح نشده، ممکن است از دسترسی شخص به برنامه جلوگیری کند. مثل هر مقیاس دیگر احراز هویت، این ابزارها در معرض استراق‌سمع هکرها هم قرار می‌گیرند. یک تصویر یا انیمیشن باکیفیت یا در بعضی نمونه‌ها یک آواتار متحرک می‌تواند بعضی از سیستم‌های تشخیص چهره را فریب دهد. شرکت‌ها روش‌های خلاقانه‌ای را برای مبارزه با این مشکل در نظر دارند .دیوید ورگارا، مدیر شرکت بازاریابی محصول جهانی، می‌گوید: مؤسسه‌ی بین‌المللی امنیتی داده‌ی Vasco ، سازنده‌ی فناوری‌های امنیت سایبری، از فناوری «کشف زنده» استفاده می‌کند که برای بررسی زنده‌بودن کاربران از آن‌ها می‌خواهد چشمک زده یا سر خود را بچرخانند. مقیاس‌های احراز هویت بیومتریک با وجود محدودیت‌هایی مثل تشخیص چهره، مسیر اصلی خود را حفظ کرده‌اند. شرکت اپل هم اعلام کرده است از تشخیص چهره به عنوان روشی برای بازگشایی قفل آخرین تلفن

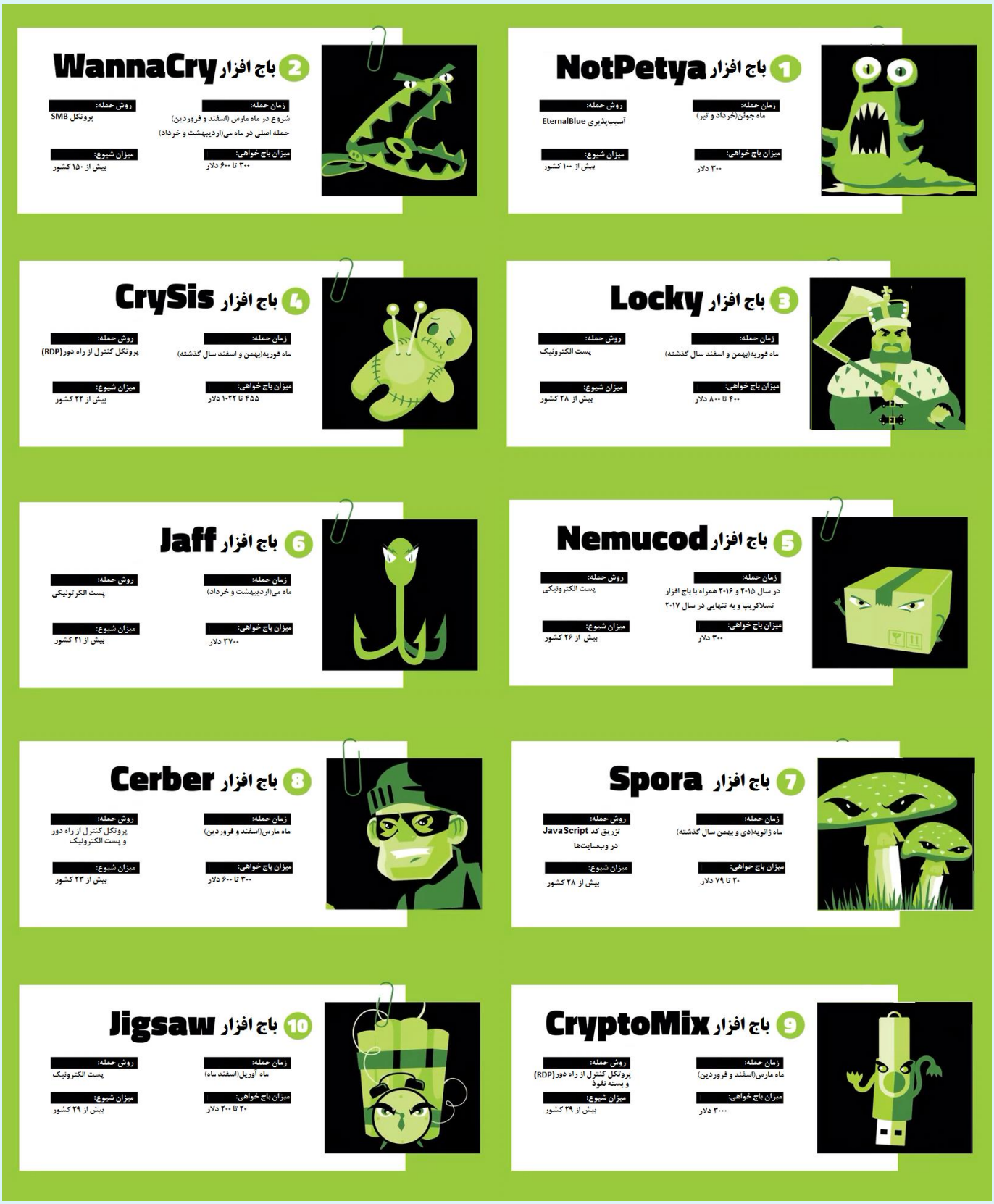
هوشمند خود iPhone X استفاده کرده است که سهم زیادی در محبوبیت این فناوری داشته است. به گفته‌ی تحلیل‌گر Forrester Reasearch ، آندرس سزار: بعضی از شرکت‌ها برای احراز هویت کاربران در حین استفاده از یک برنامه، از سیستم‌های یادگیری ماشین استفاده می‌کنند. این مقیاس‌ها که به شدت وابسته به رفتار هستند و به الگوهای متداول رفتاری فرد در کاربرد تکنولوژی دقت می‌کنند، نسبتا جدید هستند اما توجه زیادی را به خود جلب کرده‌اند.

ورگارا نیز می‌گوید: تحلیل خودکار الگوهای رفتاری کاربران، که می‌تواند شامل صدها نقطه‌ی داده‌ای گسسته مثل سرعت تایپ باشد، یک دستاورد بزرگ در احراز هویت به شمار می‌رود؛ زیرا به سازمان‌ها اجازه می‌دهد به جای تکیه بر یک رمزعبور مدت‌دار به نظارت امنیت در زمان واقعی بپردازند. احراز هویت مبتنی بر رفتار، به دلیل پتانسیل بهبود تجربه‌ی کاربری و در نتیجه زیرساخت یک شرکت، در درجه‌ی اول متمرکز بر مشتری است. مؤسسه‌ی بیمه‌ی سلامت Aetna در حال اجرای مقیاس‌های امنیتی رفتار محور برای برنامه‌های وب و موبایل خود است که شامل گزینه‌هایی برای معیارهای بیومتریک مثل ضربات انگشت است. این فناوری مشخصات اعضای Aetna از جمله انواع حرکت آن‌ها برای یک برنامه یا سرعت تایپ را جمع‌آوری کرده و داده‌ها را در یک موتور ریسک وارد می‌کند. این موتور بر اساس داده‌های مربوط به رفتار مشتری در یک برنامه و نوع دستگاه، می‌توانید تصویری از رفتار «نرمال» را در زمان تقریبی دو هفته ایجاد کند. اگر رفتارهای شخصی، دارای انحراف قابل توجهی نسبت به رفتارهای متداول او باشد، سیستم این انحراف را درنظر می‌گیرد. اگر یک مشتری تلفن خود را به دوستش بدهد، برنامه دوست او را به عنوان یک شخص دیگر شناسایی می‌کند و یک شکل دیگر از احراز هویت مثل لغزاندن انگشت روی صفحه‌ی نمایش را درخواست می‌کند. به گفته‌ی ویلسون صدا هم در حال حاضر به یک بحث داغ در استارت‌آپ‌ها تبدیل شده است. سیستم‌های شناسایی صوتی وجود دارند

که برای ساخت یک «اثر صوتی» منحصربه فرد می‌توانند به یادگیری و بررسی آهنگ گفتار، لهجه و تلفظ و دیگر معیارها بپردازند. بعضی شرکت‌ها نیز به ساخت الگوریتم‌هایی می‌پردازند که از صوت برای تعیین سرنخ‌های زمینه‌ای برای مثال گوینده‌ای که تحت فشار یا اجبار سخن می‌گوید، استفاده می‌کنند. دیگر معیارهای احرازهویت بیومتریک قابل توسعه شامل ابزارهای تشخیص دست‌خط، اسکنرهایی که کاربران را بر اساس شکل گوش آن‌ها شناسایی می‌کنند و حتی نشانه‌گذارهای شناسه‌ای هستند که از DNA شخص به دست می‌آیند. به گفته‌ی ویلسون صرف‌نظر از شکلی که روش‌های احراز هویت در آینده به خود می‌گیرند، موضوع حائز اهمیت دستیابی به بیومتریکی است که مشتریان بتوانند از آن استفاده کنند. شرکت‌ها نباید به یک ابزار واحد احراز هویت وابسته باشند. کارشناسان یک روش لایه‌ای امنیتی را توصیه می‌کنند که از ترکیب روش‌های بیومتریکی، نظارت رفتار و حتی رمزهای عبور استفاده می‌کنند.

منبع: https://www.wsj.com

مشخصات ده باج‌افزار ویرانگر سال ۲۰۱۷



منبع: https://www.techrepublic.com/article/the-top-10-worst-ransomware-attacks-of-2017-so-far/

آدرس: دانشگاه محقق اردبیلی، دانشکده فنی و مهندسی، مرکز آپا دانشگاه محقق اردبیلی (۴۵)۳۱۵۰۵۷۱۸
cert.uma.ac.ir | cert@uma.ac.ir

باج افزار فارسی ستمگر (Tyrant)

در چند وقت اخیر فضای سایبری کشور با باج‌افزار جدید مواجه شده که نکته قابل توجه در این مورد به خصوص فارسی بودن و داشتن ارتباط تلگرامی آن می‌باشد. بر اساس گزارش‌های رسیده باج افزار ستمگر(Tyrant) در پوشش نرم‌افزار IP سایفون قربانیان خود را فریب داده و منتشر گردیده است. این باج‌افزار بعد رمزنمودن فایل‌های موجود در سیستم پیغام زیر را به زبان فارسی به کاربران نمایش می‌دهد: " اگر در حال دیدن این پیام هستید، بدان معنی است که سیستم شما به باج‌افزار تایرنت آلوده شده و تمام فایل‌ها، پوشه‌ها و درایوهای سیستم شما درگیر و توسط الگوریتم‌های بسیار پیچیده (ای‌بی‌اس‌آی و ای‌ای‌اس) رمزنگاری و کلید رمزگشایی فایل‌های شما به‌صورت خودکار برای ما ارسال شده است." این باج‌افزار مبلغ ۱۵ دلار را در ۲۴ ساعت از طریق وب‌مانی برای رمزگشایی فایل‌ها درخواست می‌نماید. پشتیبانی تلگرام و ایمیل نیز راه‌های ارتباطی کاربران در نظر گرفته شده است. محقق شرکت امنیتی جی‌دیتا اولین بار در تاریخ ۱۶ اکتبر متوجه این باج افزار شده بود. البته پرداخت این مبلغ کمکی باه قربانی برای دستیابی به فایل‌های خود توصیه نکرده و مشاهد گردیده پس از پرداخت مبلغ پشتیبانی حتی از پاسخ دادن نیز امتناع می نماید.

باج افزار ستمگر مبتنی برباج افزار متن باز DUMB بوده که با بررسی انجام شده مشخص گردیده حتی به دلیل تغییرات اعمال شده در سورس این باج افزار نسبت به منبع متن باز خود ضعیف‌تر عمل کرده و حتی در مواردی قادر به رمز نمودن همه‌ی فایل‌های موجود در سیستم نیز نمی‌شود و پس از ریبوت سیستم نیز این باج افزار قادر به اجرای خود نمی‌باشد. شایان ذکر است باج افزار ستمگر از شیوه رمزنگاری مرسوم باج افزارها موسوم به کلید عمومی و خصوصی استفاده نکرده و دارای یک کلید عمومی می باشد.

روش های پیشگیری:

* از دریافت فایل‌های اجرایی در شبکه‌های اجتماعی و اجرای فایل‌های ناشناخته و مشکوک خودداری کنید.
* از دانلود و اجرای فایل‌های پیوست ایمیل‌های ناشناس و هرزنامه‌ها پرهیز کنید.
* سیستم عامل و آنتی ویروس سیستم خود را دایما به‌روزرسانی کنید.
* تا جای ممکن از دسترسی راه دور استفاده نکنید و در صورت عدم امکان حذف دسترسی راه دور، تمهیدات امنیتی را به طور دقیق رعایت کنید.
* از مجوز دسترسی Administrator بر روی سیستم‌های کاربران سازمان استفاده نکنید.

منبع: مرکز ماهر

آدرس: دانشگاه محقق اردبیلی، دانشکده فنی و مهندسی، مرکز آپا دانشگاه محقق اردبیلی ۳۱۵۰۵۷۱۸(۴۵)
cert.uma.ac.ir | cert@uma.ac.ir

اصلاح آسیب‌پذیری حیاتی Zero-Day در مرورگرهای فایرفاکس و Tor

یک آسیب‌پذیری حیاتی در فایرفاکس به‌صورت فعال در سطح اینترنت بهره‌برداری شد. به همین جهت هر دو پروژه موزیلا و Tor برای این آسیب‌پذیری وصله امنیتی منتشر کردند. این آسیب‌پذیری به مهاجمان اجازه می‌داد تا از راه دور کدهای مخرب را بر روی سیستم‌عامل ویندوز از طریق آسیب‌پذیری خطای حافظه در مرورگر فایرفاکس اجرا کنند. بسته مرورگر Tor ، نسخه منبع باز مرورگر فایرفاکس، منبع باز است که ارتباطی از طریق شبکه ناشناس Tor برقرار می‌کند که آدرس IP عمومی کاربران خود را مخفی می‌کند. در روز چهارشنبه (۳۰ نوامبر ۲۰۱۶)، یک مقام رسمی از شبکه anonymity در یک advisoryنوشته است: "این مشکل امنیتی که دلیل انتشار فوری وصله موردنظر است، در حال حاضر بر روی سیستم‌های دارای ویندوز به‌صورت فعال در حال بهره‌برداری است. اگرچه در حال حاضر کد بهره‌بردار مشابهی برای کاربران لینوکس یا OS X وجود ندارد، مبنای اصلی این آسیب‌پذیری بر روی دیگر پلتفرم‌ها نیز تأثیرگذار است. بنابراین ما قویاً به‌تمامی کاربران پیشنهاد می‌دهیم هرچه سریع‌تر مرورگر Torخود را به‌روزرسانی کنند." به‌محض اینکه پروژه Tor نسخه به‌روزرسانی را برای مرورگر خود منتشر کرد، موزیلا نیز یک خبر در post blog منتشر کرد که گفته بود این شرکت در حال حاضر نسخه به‌روزرسانی شده فایرفاکس را که این آسیب‌پذیری را اصلاح کرده است، منتشر کرده است. این آسیب‌پذیری که CVE-2016-9079 نام‌گذاری شده است و در دسته‌بندی خیلی مهم قرار گرفته است، همچنین بر روی نرم‌افزار Mozilla Thunderbird که مربوط به پست الکترونیک است، تأثیرگذار است و نسخه ESR آن توسط مرورگر Tor استفاده می‌شود. مقام رسمی امنیتی موزیلا، Daniel Veditz، گفته است: "این بهره‌بردار، از این آسیب‌پذیری در فایرفاکس استفاده کرده تا به مهاجمان اجازه دهد تا یک کد دلخواه را بر روی سیستم مورد هدف اجرا کنند. این عملیات توسط باز کردن یک صفحه وب توسط قربانی که شامل کد SVG و جاوا اسکریپت مخرب است، انجام می‌شود. این آسیب‌پذیری از این قابلیت استفاده کرده تا آدرس‌های IPو MAC سیستم مورد هدف را جمع‌آوری کند و آن‌ها را به سرور مرکزی گزارش کند. بااینکه payload این بهره‌بردار تنها در ویندوز کار می‌کند، این آسیب‌پذیری در Mac OSو لینوکس نیز وجود دارد. " به کاربران فایرفاکس و Tor به شدت توصیه می‌شود تا هرچه سریع‌تر مرورگرهای خود را به آخرین نسخه فایرفاکس یعنی ۵۰،۰،۲ و آخرین نسخه Tor یعنی ۶،۰،۷ به‌روزرسانی کنند. در همین حال، کاربرانی که از Tor و نسخه‌های mainstream فایرفاکس استفاده می‌کنند، می‌توانند slider امنیتی فایرفاکس را بر روی High قرار دهند تا نسبت به حملات مهاجمان در امان باشند.

منبع : https://apa.aut.ac.ir

مشاهده اخبارهای جعلی توییتر در گوگل

گوگل یکی از شرکت‌های پیشرفته و سودآور جهان می‌باشد که گاهی اوقات اخبار خنده‌دار و دروغین نیز را از طریق یک موتور جستجو در بین تمام کاربران خود پخش می‌کند. گوگل شرکت معتبری می‌باشد در واقع خیلی معتبر که توانسته در ماه گذشته حدود ۲,۷ بیلیون دلار درآمد کسب کند. با این وجود اخبار کذب بخش زیادی از خبرهای گوگل را شامل می شود. بخشی از تولید خبرهای کذب از سال ۲۰۱۵ زمانی که گوگل از نتایج توییتر استفاده کرد شروع شد. در واقع توییتر یک منبع خبری بسیار خوب است اما این منبع خبری گاهی اخبار کذب را نوعی بیان می کند که حتی روزنامه نگاران ماهر را که متخصص تشخیص خبر جعلی و واقعی هستند دچار اشتباه می‌کند. گوگل می‌تواند از نتایج توییتر استفاده نکند یا آنها را اعتبار سنجی کند اما اینکه چرا این کار در گوگل انجام نمی‌شود سوالیست که جوابی برای آن داده نشده است.

منبع۱: https://latesthackingnews.com

منبع۲: http://mashable.com

جاسوسی ایرانیان بوسیله یک بدافزار اندرویدی

محققان شرکت امنیتی'دکتر وب' (Dr.Web)، تروجان اندرویدی جدیدی را کشف کرده‌اند که با استفاده از تلگرام، از ایرانیان جاسوسی می‌کند. بدافزار یاد شده اطلاعات کابران را سرقت و اعمال خرابکارانه نیز انجام می‌دهد. بدافزار یادشده با نام‌های جذابی همچون"اینستا پلاس"، "پروفایل چکر" یا "Cleaner Pro" کاربران به نصب خود ترغیب می‌نماید. نام این بدافزار "Android.Spy.377.origin" بوده و در دسته‌بندی ابزار مدیریت از راه دور قرار می‌گیرد(RAT). پس از نصب بدافزار کاربر را به بررسی میزان محبوبیت خود بین کاربران تشویق و از او اطلاعات ورود به تلگرام را درخواست می‌نماید. پس از دریافت اطلاعات از کاربر اعدادی تصادفی را تولید و با نام بازدیدکنندگان نمایش می‌دهد. بعد از زمان کوتاهی برنامه میانبر خود را از صفحه پاک و کارهای مخرب خود را به صورت مخفیانه آغاز می‌نماید. فهرست مخاطبان، پیام‌های کوتاه ارسالی و دریافتی، اطلاعات حساب‌های کاربری سرقت و همچنین با ثبت تصویری از صاحب گوشی طریق دوربین جلو اطلاعات را به مرکز کنترل خود مخابره می‌نماید. ارتباط با ربات تلگرامی این بدافزار برای تعیین نوع اعمال مخرب نیز از ویژگی‌های دیگرش بوده و برقراری تماس، ارسال پیام‌کوتاه، نصب برنامه،ارسال فایل، مشخص کردن موقعیت مکانی و حذف فایل نمونه ای از اعمال خرابکارانه می‌باشد. پس از هر عمل خرابکارانه نیز با ربات تلگرامی ارتباط برقرار کرده و گزارش عمل خود را می‌نماید. جهت حفظ امنیت دستگاه خود برنامه‌های موردنیاز را از google paly و یا سایر بازارهای معتبر دانلود نمایید. از برنامه‌های تولیدکنندگان معتبر استفاده فرمائید و همچنین نصب برنامه‌های غیررسمی برای پیام‌رسان‌ها و یا شبکه‌های اجتماعی خودداری فرمائید. برنامه‌های ارائه شده در این بسترها نیز معمولا دچار بدافزارهای می‌باشند پس از دانلود و نصب آنها به شدت دوری کنید.

منبع: دکتروب

توئیتر هک شد

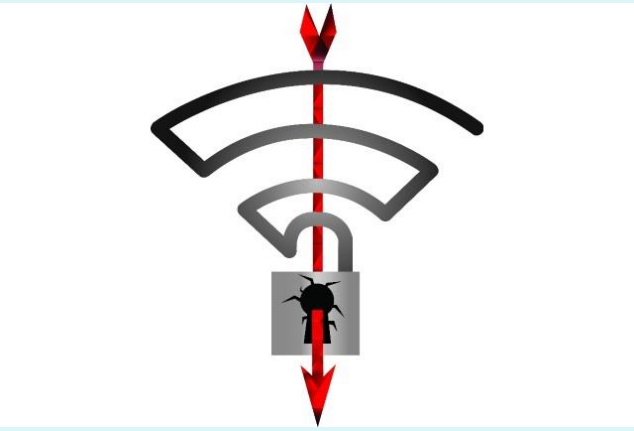
دو کاربر آلمانی توئیتر با موفقیت این شبکه اجتماعی را هک کردند و مطلبی با ۳۵ هزار حرف در آن ارسال کردند.

شبکه اجتماعی توئیتر به کاربران امکان ارسال مطالب بلند و طولانی را نمی‌دهد و افراد باید مطالب خود را در ۲۸۰ کاراکتر خلاصه و ارسال کنند. ارسال این مطلب طولانی و پر از حروف و کاراکترهای مختلف مورد توجه بسیاری از کاربران توئیتر قرار گرفت و آن‌ها به بحث در مورد شیوه هک شدن این شبکه اجتماعی پرداختند. توئیتر به فاصله کوتاهی بعد از مشخص شدن هک این شبکه اجتماعی، مطلب ارسالی را پاک کرد. اما بحث و تبادل نظر برخی کاربران در مورد ضرورت برطرف شدن محدودیت اعمال شده توئیتر ادامه یافت. این شبکه اجتماعی فعلا فعالیت عوامل ارسال این توئیت طولانی را هم ناممکن کرده ولی حساب کاربری آنها بعد از مدتی تعلیق و به حالت عادی بازگشته است. آن‌ها بابت این کار خود از توئیتر عذرخواهی کرده‌اند. مدیران توئیتر می‌گویند مشکلی که ارسال این پیام طولانی را ممکن کرده بود، برطرف کرده‌اند.

منبع: https://www.mehrnews.com/news/4137407/

در جنگل زندگی کنید چون که وای‌فای‌ها آسیب-پذیر شده‌اند.

محقق امنیتی Mathy Vanhoef درحال‌حاضر اخیرا آسیب‌پذیری وای‌فای جدی در پروتکل رمزگذاری WPA2را افشا کرده است. اکثر دستگاه‌ها و روترها درحال‌حاضر به WPA2 متکی هستند تا ترافیک WiFi خود را رمزگذاری کنند، بنابراین احتمال دارد شما تحت تاثیر قرار گیرید.



بیشتر آسیب‌پذیری‌ها در سراسر جهان توسط کاربران نادیده گرفته می‌شود و حتی اگر میلیون‌ها کاربر دچار آلودگی شوند، پس از مدتی فراموش خواهند شد و ارزش چندانی نخواهند داشت. اما خبری که امروز به آن پرداخته‌ایم در مورد آسیب‌پذیری است که به احتمال زیاد، بزرگی آن از شکافی که در یاهو بوجود آمده بود و میلیاردها کاربر را در سراسر جهان آلوده ساخته بود، عمیق‌تر است. محققان به تازگی آسیب‌پذیری جدیدی را کشف کرده‌اند که تمام شبکه‌های وای‌فای را ناامن می‌سازد و باعث به خطر افتادن حساب‌های کاربری کاربران می‌شود.

محققان دریافته‌اند که دستگاه‌هایی با سیستم‌عامل‌های اندروید، iOS ، لینوکس، macOS ، ویندوز و دیگر سیستم عامل‌ها به برخی از این تغییرات آسیب‌پذیر هستند و این بدان معنی است که تقریبا هر دستگاهی می‌تواند به خطر بیفتد و آلوده شود. این نوع از حمله را حمله نصب مجدد کلید (key reinstallation attack) یا به اختصار KRACK نامیده‌اند.

برای اجرای این حمله، هکر می‌بایستی یک شبکه‌ی وای‌فای به نام (SSID) را به عنوان یک شبکه موجود ایجاد نموده و کاربر خاصی را مورد هدف قرار دهد. هنگامی که هکر تشخیص دهد که کاربر در حال اتصال به شبکه اصلی است، آن‌ها می‌توانند بسته‌های ویژه‌ای را که دستگاه را به کانال‌های دیگر متصل می‌کنند را ایجاد و در نهایت کاربر را به شبکه جعلی با همان نام پیوند می‌دهند. پس از گذر از این مرحله، هکرها با بکارگیری یک نقص در پیاده‌سازی پروتکل‌های رمزنگاری می‌توانند کلید رمزنگاری را که کاربر از آن استفاده می‌کرده را به یک رشته از صفر تغییر دهند و بدین ترتیب هکر می‌تواند به تمام اطلاعاتی که کاربر بارگیری و بارگزاری (آپلود و دانلود) می‌کند، دسترسی یابد.

بنابراین با استفاده از این ابزار در شبکه جعلی، هکر می‌تواند به لاگین و پسورد کاربران دسترسی یابد که این به معنای سرقت اطلاعات آن ها خواهد بود.

برای اکثر افرادی که نمی‌خواهند و نمی‌توانند وای‌فای را به طور کامل متوقف کنند، ممکن است زمان برای انتقال به جنگل و به دور از همسایگان فرا رسیده باشد. مارک زوکربرگ (موسس و رئیس فیس‌بوک) خانه‌های اطراف خانه خود را خریده و همه آن‌ها را تخریب کرده تا ضریب امنیتی خود را بالا ببرد! بدیهی است که این استراتژی بسیار گران است.

منبع:
https://www.pcworld.com/article/3233308/security/krack-wi-fi-security-flaw-faq-tips.html

افزایش بدافزارهای فوق‌العاده مخفی با امضای دیجیتالی در سایه‌ی وبِ تاریک

حدس بزنید کدام‌یک گران‌تر از گذرنامه‌های جعلی آمریکایی است، کارت‌های اعتباری به سرقت رفته و حتی اسلحه‌ها در وبِ تاریک یا گواهی‌نامه‌های امضاء شده با کد دیجیتالی؟

مطالعه‌ی اخیر انجام شده توسط موسسه‌ی تحقیقات امنیت سایبری (CSRI) در این هفته نشان داد که گواهی‌نامه‌های به سرقت رفته‌ی امضاء شده با کد دیجیتالی به‌راحتی برای خرید هرکسی بر روی وبِ تاریک تا ۱۲۰۰ دلار در دسترس هستند، در حالی که دسترسی به اقلام غیرمجاز قیمتی به مراتب کم‌تر دارد! همانطور که می‌دانید، گواهی‌نامه‌های دیجیتالی صادر شده توسط یک صادرکننده‌ی گواهی‌نامه‌ی مورد اعتماد (CA)، برای برنامه‌ها و نرم‌افزارهای رایانه‌ای رمزنگاری شده مورد استفاده قرار گرفته و برای رایانه‌ی شما به‌منظور اجرای این برنامه‌ها، بدون هیچ‌گونه پیام هشداردهنده‌ای، مورد اعتماد هستند. با این حال، نویسنده‌ی بدافزار و نفوذگرها که همیشه درجستجوی روش‌های پیشرفته برای دور زدن راهکارهای امنیتی هستند، در سال‌های اخیر گواهی‌نامه‌های دیجیتالی مورد اعتماد را مورد بهره‌برداری قرار داده‌اند. نفوذگرها به‌منظور امضای کد مخرب خود، از گواهی‌نامه‌های امضاء شده با کد آسیب‌دیده‌ی مرتبط با فروشندگان معتبر نرم‌افزار استفاده می‌کنند. با این کار، احتمال شناسایی بدافزار آن‌ها بر روی شبکه‌های تشکیلات اقتصادی مورد هدف و دستگاه‌های مصرف‌کننده کاهش می‌یابد. بدافزار معروفِ Stuxnet نیز که در سال ۲۰۰۹ میلادی تاسیسات پردازش هسته‌ای ایران را مورد هدف قرار داد، از گواهی‌نامه‌های دیجیتالی قانونی استفاده می‌کرد. همچنین، به لطف رویکردی مشابه، با توجه به به‌روزرسانی نرم‌افزار دیجیتالی امضاء شده، آلودگی‌های بارگیری شده با نرم‌افزار CCleaner امکان‌پذیر شد.

گسترشِ بدافزارهای امضاء شده‌ی دیجیتالی مخفی در سال‌های اخیر

با این حال، تحقیقات جداگانه‌ی انجام شده توسط گروهی از پژوهش‌گران امنیتی نشان دادند که بدافزارهای امضاء شده‌ی دیجیتالی، بسیار شایع‌تر از قبل شده‌اند. محققان دانشگاه مری‌لند گفتند که درمجموع، ۳۲۵ نمونه از بدافزارهای امضاء شده یافته‌اند که ۱۸۹ مورد از آن‌ها (۵۸,۲ درصد) امضای دیجیتالی معتبر داشته و ۱۳۶ مورد، امضای دیجیتالی ناقص دارند.

پژوهش‌گران گزارش دادند: «این امضاهای ناقص برای توسعه‌دهندگان بدافزار بسیار مفید هستند. ما متوجه شدیم که رونویسی یک امضای Authenticode از یک نمونه‌ی قانونی به یک نمونه‌ی بدافزاری بدون امضاء بسیار ساده است که ممکن است به بدافزار برای دور زدن شناسایی AV کمک کند.»

۱۸۹ نمونه از بدافزارهایی که به‌صورت صحیح امضاء شده بودند، با استفاده از ۱۱۱ گواهی‌نامه‌ی منحصربه‌فرد آسیب‌دیده‌ی صادر شده توسط صادرکننده‌های گواهی‌نامه‌ی شناخته شده تولید شده و برای امضای نرم‌افزارهای قانونی مورد استفاده قرار گرفتند. درحال حاضر، ۲۷ مورد از این گواهی‌نامه‌ی آسیب‌دیده لغو شده‌اند، هرچند بدافزار توسط یکی از ۸۴ گواهی‌نامه‌ی باقی‌مانده که لغو نشده‌اند، امضاء شده و تا زمانی که دارای یک نشانگر معتبر باشد، مورد اعتماد خواهد بود. محققان گفتند: «بخش بزرگی (۸۸,۸ درصد) از خانواده بدافزارها به یک گواهی‌نامه‌ی منفرد وابسته هستند، که نشان می‌دهد گواهی‌نامه‌های مورد بهره‌برداری قرار گرفته،

به‌جای اشخاص ثالث، عمدتاً توسط نویسندگان بدافزار کنترل می‌شوند.» محققان فهرستی از گواهی‌نامه‌های مورد بهره‌برداری قرار گرفته را بر روی وب‌گاه signedmalware.org منتشر کرده‌اند.

لغو گواهی‌نامه‌ی به سرقت رفته، بدافزار را بلافاصله متوقف نمی‌کند

محققان دریافتند حتی زمانی که یک امضاء معتبر نیست، حداقل ۳۴ محصول ضدبدافزار موفق به بررسی اعتبار گواهی‌نامه نشدند، در نهایت، اجازه می‌دهند تا کد مخرب بر روی سامانه‌ی هدف اجرا شود. محققان آزمایش‌هایی را نیز برای تعیین اینکه آیا امضاهای ناقص می‌توانند شناسایی ضدبدافزارها را تحت تاثیر قرار دهند، انجام دادند. برای اثبات این موضوع، آن‌ها ۵ نمونه از باج‌افزارهای امضاء نشده‌ی تصادفی را بارگیری کردند که تقریباً تمام برنامه‌های ضدبدافزاری، نمونه‌های مخرب را شناسایی کردند. محققان سپس ۲ گواهی‌نامه‌ی منقضی شده که قبلاً برای امضای یک نرم‌افزار قانونی و یک بدافزار استفاده شده بودند را گرفته و از آن‌ها برای امضای هریک از ۵ نمونه‌ی باج‌افزار استفاده کردند. محققان هنگام تجزیه و تحلیل ۱۰ نمونه‌ی جدید دریافتند که بسیاری از محصولات ضدبدافزاری موفق به شناسایی بدافزارها نشدند. ۳محصول برتر ضدبدافزاری، nProtect، Tencent و Paloalto، نمونه‌های باج‌افزاری امضاء نشده را به‌عنوان بدافزار شناسایی کردند، اما ۸ مورد از ۱۰ باج‌افزار را به‌عنوان بدافزار بی‌خطر (خوش‌خیم) در نظر گرفتند. حتی موتورهای ضدبدافزاری محبوب از آزمایشگاه کسپرسکی، مایکروسافت، ترندمیکرو، سمانتیک و کومودو نیز موفق به شناسایی برخی از نمونه‌های مخرب شناخته شده نشدند.دیگر بسته‌های ضدبدافزاری تحت تاثیر قرار گرفته، شامل CrowdStrike، Fortinet، Avira، Malwarebytes، SentinelOne، Sophos، ترندمیکرو و Qihoo می‌باشند. محققان گفتند: «ما معتقدیم که عدم توانایی در شناسایی نمونه‌های بدافزاری، ناشی از این واقعیت است که در هنگام فیلتر کردن و اولویت‌بندی فهرست پرونده‌ها برای پویش به‌منظور کاهش سربار محاسباتی اعمال شده بر روی میزبان کاربر، ضدبدافزارها حساب‌های کاربری را به‌صورت دیجیتال امضاء می‌کنند. با این حال، پیاده‌سازی نادرست بررسی‌های امضای Authenticode در بسیاری از ضدبدافزارها، نویسندگان بدافزار را قادر می‌سازد تا با یک روش ساده و ارزان، از شناسایی فرار کنند.» پژوهش‌گران اضافه کردند که این موضوع را به شرکت‌های ضدبدافزاری تحت تاثیر قرار گرفته، گزارش داده‌اند و یکی از آن‌ها تایید کرد که محصولات آن‌ها قادر به بررسی درست امضاها نبوده و برای حل این مشکل، برنامه‌ریزی کرده‌اند.

منبع: وبگاه اخبار امنیتی فناوری اطلاعات و ارتباطات

آزمایشگاه و مرکز تخصصی آپا دانشگاه محقق اردبیلی

با توجه به افزایش تعداد حوادث امنیتی رایانه‌ای و لزوم وجود مراکز تخصصی دانشگاهی برای پشتیبانی و رفع نیازهای پژوهشی جامعه در این حوزه، و با انگیزه ارتقای دانش و توان مهندسی در حوزه امنیت سیستم‌های کامپیوتری و پردازش اطلاعات و انتقال نتایج به جامعه، آزمایشگاه و مرکز تخصصی آپا دانشگاه محقق اردبیلی، از اواخر سال ۱۳۹۴ فعالیت خود را آغاز نمود و از زمان آغاز فعالیت، اقدامات زیر صورت گرفته است:

۱. ارزیابی امنیتی و انجام آزمون نفوذپذیری سامانه‌ها و شبکه‌های رایانه‌ای

تست نفوذ یا ارزیابی امنیتی روشی است که توسط آن قادر می‌توان آسیب‌پذیری‌های موجود در نرم‌افزارها، شبکه، وب‌سایت و بانک‌های اطلاعاتی خود را شناسایی کرده و پیش از آنکه نفوذگران واقعی به سیستم وارد شوند، امنیت سیستم خود را افزایش داد. این روش با استفاده از ارزیابی جنبه‌های مختلف امنیتی کمک می‌کند تا با کاهش دادن ریسک‌های امنیتی موجود، احتمال نفوذ غیرمجاز به شبکه کاهش یابد.

۲. مشاوره در زمینه امن‌سازی سامانه‌ها و شبکه رایانه‌ای

با توجه فعالیت‌های مختلفی که آزمایشگاه و مرکز تخصصی آپا دانشگاه محقق اردبیلی در زمینه زیرساخت‌های امنیتی مانند پیاده‌سازی سیستم مدیریت امنیت اطلاعات، پیاده‌سازی انواع ابزارهای امنیتی، تدوین الگوهای امنیتی داشته است، کارشناسان این مرکز دارای دیدی جامع نسبت به مسایل امنیتی با توجه به اهداف استراتژیک و راهبردی و با توجه به موجودیت‌های هر سازمان دارند و آماده ارائه راهکار امنیت اطلاعات و شبکه در تمامی سازمان‌ها با ویژگی‌ها و موجودیت‌های مختلف می‌باشند. خدمات و راهکارهای امنیت اطلاعات و سیستم‌های کامپیوتری این مرکز، با بررسی وضعیت فعلی سیستم های موجود در سازمان آغاز می‌شود و با بهره‌گیری از تکنولوژی و تخصص روز، با معماری و اجرای راه حل‌های جامع ایمن سازی سیستم های کامپیوتری ، کامل می گردد.

۳. برگزاری دوره‌های آموزشی در زمنیه دانش امنیتی برای سازمان‌ها و نهادهای زیربط

امنیت فضای سایبری فرآیندی است و باید آن را گام به گام و به روز جلو برد بنابراین آزمایشگاه و مرکز تخصصی آپا دانشگاه محقق اردبیلی با هدف ارتقائ دانش امنیت اطلاعات متولیان فاوای سازمان‌ها و نیز به منظور تربیت نیروهای متخصص چندین دوره کارگاه‌های آموزشی برگزار نموده است.

۴. تولید نرم‌افزارهای امنیتی

آزمایشگاه و مرکز تخصصی آپا دانشگاه محقق اردبیلی با هدف ارتقا سطح امنیت فضای سایبری به تولید نرم افزارهای امنیتی اقدام نموده است که عبارت است از: سامانه تحلیل‌گر فایل‌های اجرائی (ستفا)، دیده‌بان، رادار

۵. پاسخگویی به حملات

آزمایشگاه و مرکز تخصصی آپای دانشگاه محقق اردبیلی به محض دریافت درخواستی مبنی بر وقوع حملاتی تحت وب، زیرساخت‌های شبکه، سامانه‌های اداری و حملات بدافزاری در اسرع وقت با سازمان مورد حمله ارتباط برقرار می‌کند و با شناسایی نوع و فرایند حمله، مولفه‌های مربوط به آسیب‌پذیری سیستم، راهکارهای مناسب برای جلوگیری از حمله مجدد و بهره‌برداری از ضعف سیستم را ارائه می‌دهد همچنین با شناسایی نقاط ضعف سیستم و ارائه مشاوره برای رفع این نقاط آسیب‌پذیر سیستم را در مقابل حملات جدید مقاوم می‌سازد.

تهیه و تنظیم: آزمایشگاه و مرکز تخصصی آپا دانشگاه محقق اردبیلی

Cert.uma.ac.ir