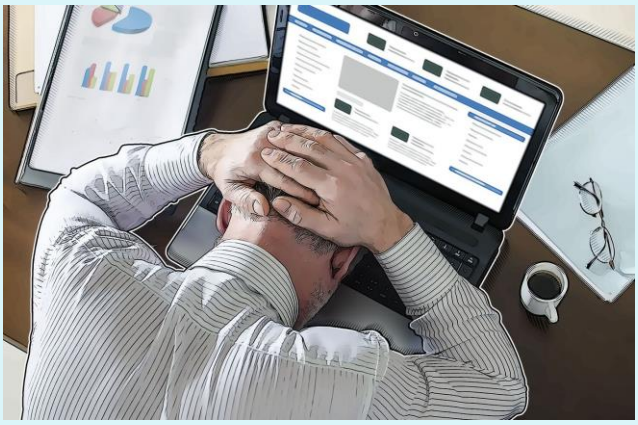
شماره سوم – نیمه اول آذر ۱۳۹۶

# خبرنامه "آپا" دانشگاه محقق اردبیلی

**در این شماره می‌خوانیم:**

- ✓ بزرگترین نشت‌های اطلاعاتی سال ۲۰۱۷
- ✓ نحوه تأمین امنیت سایبری در محیط کار
- ✓ بازگشت باتنت Necurs با پویش باج‌افزار جدید Scarab
- ✓ نرم افزار جلوگیری از سرک کشیدن افراد به گوشی موبایل
- ✓ جاسوسی گوگل حتی با غیرفعال کردن GPS
- ✓ حذف هر عکسی با آسیب‌پذیری موجود در فیس‌بوک
- ✓ پادشاه این روزها: بیت‌کوین – قسمت دوم

045 31505718
cert@uma.ac.ir
اردبیل - خیابان دانشگاه - دانشگاه محقق اردبیلی



## بزرگترین نشت‌های اطلاعاتی سال ۲۰۱۷

نشت اطلاعات اشخاص همه روز اتفاق می‌افتد که برخی از آن‌ها در اخبار گفته می‌شود و برخی دیگر نیز به بیرون درز نمی‌کنند. درسال ۲۰۱۷ میلادی کشور ایالات متحده به تنهایی ۱۶۳ میلیون حساب کاربری در معرض خطر را به خود دیده است (آمار گفته شده بر اساس اطلاعات ارائه شده توسط مرکز تحقیقات سرقت می‌باشد). البته سال میلادی هنوز به پایان خود چند روزی را دارد با این حال ما بزرگترین اتفاقات اتفاق افتاده از ابتدای سال تا کنون را برای شما لیست خواهیم کرد. شایان ذکر است که نشت-های اطلاعاتی شرکت یاهو با ۳ میلیارد حساب کاربری و شرکت اوبر با ۱,۵ میلیون حساب کاربری به دلیل اینکه در سال‌های قبل رخ داده‌اند (شرکت یاهو در سال ۲۰۱۳ و شرکت اوبر در سال ۲۰۱۶) در این لیست قرار نمی‌گیرند.

- **شرکت Avanti – ۱,۶ میلیون حساب کاربری**

شاید تا بحال در مورد **Avanti** چیزی نشنیده باشید ولی احتمالا یکی از همین ماشین‌های فروش خودکار در محل کار شما هم وجود دارد و حتی شاید از یکی از همین ماشین ها تنقلات خریده باشید. در ماه جولای، این شرکت تامین‌کننده سیستم‌های فروش تنقلات برای غذا خوری‌های شرکت‌ها از وجود بدافزار در بعضی از پایانه‌های پرداخت برخی از دستگاه‌هایش خبر داد. مهاجمان با استفاده از بدافزاری پیچیده که منحصرا جهت دسترسی به اطلاعات کارت بانکی کاربران از جمله شماره کارت و تاریخ انقضا و cvv ساخته شده بود موفق به نفوذ به بعضی از دستگاه‌های این شرکت شدند. اینکه دقیقا چطور موفق به انجام این کار شده‌اند هنوز در هاله‌ای از ابهام است.

در بعضی از موارد مهاجم‌ها حتی توانسته‌اند به اطلاعات حیاتی مانند اثرانگشت کاربران که در بعضی از دستگاه‌های مجهز به حسگر اثر انگشت موجود بوده نیز دست یابند اما با این حال تفاوت‌های موجود در تنظیمات دستگاه‌های مختلف باعث شده است که مهاجمان نتوانند کل شبکه را مورد حمله قرار دهند و به همین دلیل این شرکت نتوانسته است آمار دقیقی از میزان خسارات وارد شده را تخمین بزند و اعلام کرد که اطلاعات حساب کاربری حداقل ۱,۶ میلیون کاربر در معرض خطر بوده است.

- **شرکت Election System & Software (ES&S) تولید کننده ماشین‌های رای‌گیری – ۱,۸ میلیون حساب کاربری**

در ماه آگوست کارشناسان امنیت فناوری اطلاعات یک محتوا در وب سرویس ابری آمازون (AWS) یافتند. این محتوا حاوی یک نسخه کپی پشتیبانی از اطلاعات شرکت ES&S بود که یک کمپانی تولید کننده ماشین‌های رای‌گیری و سیستم‌های مدیریت انتخابات است. این اطلاعات شامل تقریبا ۲ میلیون حساب کاربری از ساکنین ایالت ایلی‌نویز(Illinois) آمریکا از جمله نام، آدرس، تاریخ تولد و گرایش حزبی بوده است. این در حالی است که به صورت پیش‌فرض دسترسی به اطلاعات مخازن AWS تنها پس از احراز هویت کاربر امکان‌پذیر است. با این حال بنا به دلایل نامعلومی تنظیمات این سرویس معیوب بوده و باعث دسترسی اطلاعات محتوای موجود برای عموم شده است. هیچ راهی برای دانستن اینکه آیا کسی قبل از متخصصان این محتوا را کشف کرده است یا نه وجود ندارد، اما اطلاعات شخصی ۱,۸ میلیون کاربر قابل دسترسی بوده است.

- **شرکت انتشاراتی Dow Jones – ۲,۲ میلیون حساب کاربری**

حادثه Dow Jones از جهت آرشیو اطلاعات در یک مخزن AWS بسیار شبیه به مورد قبلی این مطلب می‌باشد. لازم

به ذکر است که در این مورد نیز مشکل از تنظیمات بوده است، با این تفاوت که اطلاعات برای همه افراد قابل دسترسی نبوده و فقط کاربران AWS اجازه دسترسی داشته‌اند. این حادثه اطلاعات شخصی و مالی میلیون‌ها نفر از مشترکین مجله Wall Street، Barrons و دیگر مجلات و روزنامه‌ها را به وسیله یکی از بزرگترین شرکت-های منتشرکننده اطلاعات مالی در معرض خطر قرار داد. این که آیا مجرمان سایبری توانسته بودند قبل از اصلاح تنظیمات محتوای ابری به اطلاعات دسترسی یابند یا نه مشخص نیست.

- **شرکت نرم‌افزاری(ajla) – ۵,۵ میلیون حساب کاربری**

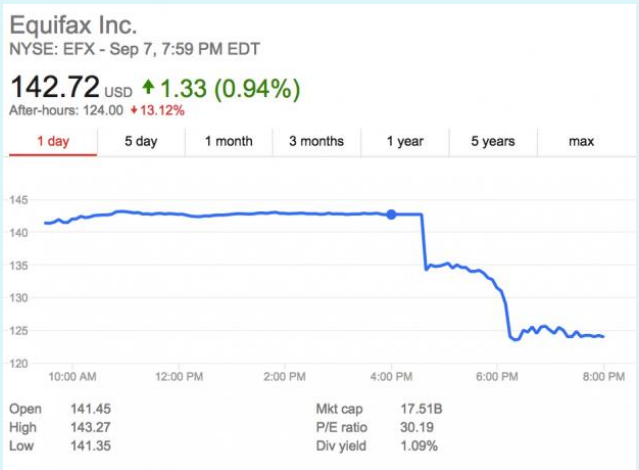
آسیب‌پذیری در نرم‌افزار کاربردی تحت وب یکی از بزرگترین موتورهای جستجوی شغل آنلاین این اجازه را به یک هکر ناشناس داد تا به اطلاعاتی نظیر نام، تاریخ تولد و شماره ملی کاربران ساکن ۱۰ ایالت آمریکا دسترسی پیدا کند. در ماه فوریه این هکر یک حساب کاربری در سیستم ایجاد کرد و از این آسیب‌پذیری برای دسترسی به بیش از ۵,۵ میلیون حساب کاربری استفاده کرد. این نفوذ بعد از دو هفته کشف و پس از آن این آسیب‌پذیری رفع گردید. شرکت **ajla** در یک اعلان رسمی این آسیب‌پذیری را تشریح و اعلام نمود که این اتفاق به خاطر بخشی از بروزرسانی اکتبر ۲۰۱۶ و به دلیل پیکربندی نادرست بوده است.

- **شرکت Equifax __ ۱۴۵,۵ میلیون حساب کاربری**

بزرگترین نشت اطلاعاتی امسال نفوذ به Equifax است. در ماه سپتامبر نمایندگان این شرکت اعلام کردند که مهاجمان به پایگاه‌های‌داده نام مشتریان، شماره‌های ملی، تاریخ تولد و آدرس آن‌ها دسترسی پیدا کرده‌اند. این نشت بیش از یک ماه یعنی از اواسط ماه مه تا آخر ماه جولای ادامه داشته است. برای دسترسی به این اطلاعات مهاجمان از یک آسیب‌پذیری موجود در چارچوب Apache Struts 2 استفاده کرده‌اند. طبق ارزیابی اولیه Equifax، این حمله شامل اطلاعات ۱۴۳ میلیون نفر بوده است اما بعدا این شرکت شمار قربانیان را ۱۴۵,۵ میلیون اعلام کرد.

این حمله بیش از ۲۰۹ هزار کارت‌اعتباری و همچنین اسناد حاوی اطلاعات شخصی ۱۸۲هزار نفر را به خطر انداخته بود. نقصی که باعث این نشت شده بود در ماه مارس توسط Oracle(کمپانی توسعه دهنده چارچوب Apache Struts) رفع گردیده بود، اما بعد از گذشت دو ماه، Equifax یکی از بزرگترین شرکت‌های اعتبارسنجی ایالات متحده هنوز به روزرسانی‌ها را انجام نداده بود.


این رویداد برای مدت‌ها سر تیتر روزنامه‌ها و خبرنامه‌های کشور ایالات متحده ماند و به صورت گسترده مورد بحث و بررسی قرار گرفت.




همچنین به دنبال خبر هک شدن Equifax، ارزش سهام این شرکت از مقدار ۱۴۲ دلار با کاهش شدید به ۱۲۴ دلار نزول ۱۳,۱۲٪ تجربه کرد.

منابع: کسپرسکی و alphr  مترجم: نیلوفر زبردست

## نحوه تامین امنیت سایبری در محیط کار خود

با نزدیک شدن ماه آگاهی رسانی امنیت سایبری می‌خواهیم یادآور شویم که این مقوله هر ساله همه ما را تحت تاثیر قرار می‌دهد. امروز ما بهترین شیوه‌های امنیت در محل کار را معرفی می‌کنیم. چرا باید با امنیت سایبری آشنا شویم با اینکه مسئولیتی نسبت به آن نداریم؟ زیرا اگرچه در زمینه IT کار نمی‌کنید باز هم رعایت نکات مربوط به امنیت سایبری بخشی از شغل شماست، و اگر اشتباهی به خاطر شما اتفاق بیافتد، شما باید پاسخگو باشید.

برای کسانی که در شرکت‌های بزرگ کار می‌کنند بهترین شروع استفاده از راهکارهای ارائه شده از سوی بخش فناوری اطلاعات شرکت خودشان می‌باشد، اما در صورتی که شما یک تیم فناوری اطلاعات یا مشاور امنیتی نداشته باشید، ما برخی نکات را که توسط متخصصین شرکت کسپراسکای تدوین شده است، در این مقاله ارائه می‌کنیم.

**۱- گذرواژه‌هایتان را جایی ننویسید.**

همه می‌دانیم هرکس با وظائف و مشغله کاری زیادی در محل کار روبه‌رو است و به خاطر سپردن گذرواژه‌ها – بخصوص انتخاب گذرواژه‌ای متفاوت و قوی برای هر سرویس و برنامه‌ای - بسیار سخت است. با این حال به اشتراک گذاشتن آن یا نوشتن آن روی کاغذ یادداشت و به نمایش عموم گذاشتن آنها یک راه آسان برای به خطر انداختن امنیت شرکت یا داده‌های شخصی خودتان است. روش‌های متعددی برای نگهداری گذرواژه‌ها وجود دارد که ساده ترین آنها استفاده از یک برنامه مدیریت رمزعبور می‌باشد که گذرواژه‌های امن برای شما تولید می‌کند و آنها را ذخیره می‌کند.

**۲- از شبکه Wi-Fiمطمئن استفاده کنید.**

مهم نیست در چه کاری مشغول به کار هستید، احتمالا بعضی از کارها را خارج از دفتر خود انجام می‌دهید. امروزه به نظر می‌رسد Wi-Fi از ملزومات زندگی می‌باشد از جایگاه‌های سوختگیری تا کافی شاپ‌ها و فرودگاه‌ها همه اینها Wi-Fi رایگان دارند. اگر از Wi-Fi رایگان مکانی استفاده می‌کنید حتما اطمینان حاصل کنید که به خود شبکه‌ای اصلی و مطمئن ارائه دهنده خدمات آن مکان متصل شده‌اید. ممکن است ارائه دهنده، اطلاعات مربوط به شبکه را روی دیوار بنویسد و یا اینکه می‌توانید از یک فردی که آنجا کار می‌کند درباره اطلاعات شبکه سوال کنید. ممکن است فرد مهاجم که قصد سرقت اطلاعات شما را دارد، نام شبکه خود را شبیه شبکه اصلی انتخاب کند، از این رو همه حروف نام شبکه را بررسی کنید و به خاطر شباهت حروف یا چینش نزدیک به هم فریب نخورید. همچنین اگر به Wi-Fi وصل می‌شوید از VPN استفاده کنید و از انجام کارهای مهم و معاملات مالی اجتناب کنید. از سوی دیگر Wi-Fi سازمان شما به خودی خود یک هدف برای انجام حملات و سرقت اطلاعات می باشد. کسب‌وکارهای بزرگ و دارای بخش‌های فناوری اطلاعات، بایستی متخصص‌هایی برای ایمن کردن شبکه Wi-Fi خود داشته باشند. در اینجا نکاتی هم برای کسب و کارهای کوچکتر داریم:

- شبکه خود را با یک گذرواژه قوی ایمن کنید.
- اجازه دسترسی را تنها به کسانی بدهید که نیاز به اتصال به شبکه دارند.
- اگر تعداد بازدیدکنندگان زیادی دارید یک شبکه مهمان درست کنید و محدودیت دسترسی به زیرساخت‌های حیاتی روی آن تعریف کنید.

**۳- از USBهای پیدا شده استفاده نکنید.**

تحقیقات نشان می‌دهد اکثر افرادی که درایو USB را به صورت تصادفی پیدا می‌کنند، متاسفانه آنرا به رایانه ی

خود وصل می‌کنند که این خبر خوشی برای شرکت‌ها نیست. دلیل اینکه یک درایو USB ناشناخته برایتان جالب و فریبنده می‌آید به خاطر است که از محتویات آن خبر ندارید و ممکن است دارای بدافزاری باشد که خسارت‌های جدی به تجهیزات شرکت یا سیستم شما وارد کند.

**۴- در دام Phishing نیافتید.**

یکی از شیوه‌های مورد استفاده توسط مجرمان، جعل هویت یک شخص و یا سازمان شناخته شده برای فرستنده ایمیل جهت ورود به شبکه‌های شرکت می‌باشد. هیچ شرکتی اعم از بزرگ و کوچک از Phishing در امان نیست؛ این اتفاق برای بهترین‌ها هم افتاده است.

در یک کسب و کار کوچک، ممکن است فکر کنید که شما هدف حملات Phishing نیستید، اما داده‌های شما و دسترسی به فایل‌های مشتری‌های شما، خود نکته با اهمیتی است. مجرمان دائماً به فکر دزدیدن اطلاعات شخصی قابل استفاده از پرونده‌های مشتریان شما هستند. آنان با این اطلاعات در بخش سیاه اینترنت(Dark Web) تجارت می‌کنند. پس چگونه از Phishing دور بمانید؟ بسیار ساده است: قبل از کلیک کردن فکر کنید. به چه چیزهایی باید فکر کنید؟

- آیا این لینک سالم است ؟ همیشه قبل از کلیک کردن روی لینکی آنرا چک کنید. موس را بر روی لینک نگه دارید تا URL آن نمایش داده شود و با دقت به غلط‌های املایی و هر بی نظمی دیگری نگاه کنید. چنانچه مطمئن نیستید، یک سربرگ جدید در مرورگر خود باز کنید و قسمت اصلی URL آنرا (صفحه نسخت سایت) دستی وارد کنید.
- آیا پیغام ضمیمه‌ای دارد؟ حتی اگر یک پیام به نظر از یک فرد شناخته شده باشد، با لینک‌ها و پیوست‌ها را با سوءظن برخورد کنید - یکی از همکارانتان می‌تواند هک شده باشد.
- آیا پیام منطقی و واقعی است؟ حتی درمورد پیام‌های داخلی از دفتر خود نیز محتاط باشید. ساختن یک ایمیل تقلبی شبیه به ایمیل واقعی – مثلا تایید یک پرداخت - کار بسیار سختی نیست. اگرچه معمولاً ساختار، نگارش و طرز بیان عجیب یا هر بی‌نظمی غیر منتظره‌ای باعث مشکوک شدن به آن ایمیل می‌شود.

**۵- از داده های مهم نسخه پشتیبان تهیه کنید.**

باج افزارها همچنان به رشد در اینترنت ادامه می‌دهند. به نظر می‌رسد، زمانی که مجرم مانع دسترسی به اطلاعات و حتی کل سیستم رایانه‌ای می‌شود، قربانیان وحشت زده شده و برای برگرداندن اطلاعاتشان باج را پرداخت می‌کنند. شرکت‌ها هم مصون از این موضوع نیستند و حتی می توان گفت، شرکت‌ها هدف‌های مطلوب‌تری هستند زیرا به دلیل با ارزش‌تر بودن اطلاعات آنها، مقدار قابل ملاحظه‌تری در مقایسه با یک شخص قربانی باید در قبال بازگردانی اطلاعاتشان بپردازند.

جالب اینجاست که شما می‌توانید با تهیه نسخه پشتیبان خود را از باج‌افزارها محفوظ دارید. اگر نسخه‌های پشتیبان منظم تهیه نمی‌کنید و گرفتار باج‌افزاری شوید، یا مجبور به از دست دادن داده‌های خود می‌شودی و یا به امید رمزگشاهای رایگان می‌نشینید. اما اگر شما نسخه پشتیبان تهیه کنید به سادگی می‌توانید اطلاعاتتان را برگردانده و به کسب و کارتان ادامه دهید.

**۶- امنیت فیزیکی را رعایت کنید.**

اگر شما در یک دفتر کار فیزیکی (حقیقی) کار می‌کنید یک قسمت از امنیت که همیشه باید در مورد آن حواس‌تان جمع باشد عامل انسانی است. همه در محل کار باید تعهدی نسبت به امنیت دیگران نیز داشته باشند. بنابرین اگر شما شخص ناشناس را در دفترکار یا در حال تلاش برای ورود به آن دیدید از سوال پرسیدن از وی یا خبر دادن به حراست ساختمان اجتناب نکنید. مجرمان برای بدست اوردن دسترسی به محیط کارتان تلاش می‌کنند و این تلاش برای ارتکاب جرم به صورت فیزیکی یا سایبری امر غیر ممکنی نمی‌باشد.

منبع: کسپرسکی  مترجم: عطا ملکی


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

## بازگشت باتنت Necurs با پویش باج‌افزار جدید Scarab

بزرگ‌ترین باتنت مبتنی‌بر هرزنامه‌ی جهان که Necurs نام دارد، در حال توزیع یک نسخه‌ی جدید از باج‌افزار Scarab است. این پویش در روز شکرگزاری (۲۳ نوامبر) آغاز شد. تنها پس از سپری شدن حدود شش ساعت از آغاز این پویش، شرکت امنیتیِ Forcepoint بیش از ۱۲٫۵ میلیون رایانامه‌ی حاوی Necurs را مسدود کرد. پژوهش‌گران این شرکت اظهار کردند که اکثر ترافیک این پویش به دامنه‌ی سطح بالای «.com» ارسال می‌شود. این دامنه بیشتر در کشورهای انگلیس، استرالیا، فرانسه و آلمان مورد استفاده قرار می‌گیرد. باتنت Necurs سابقه‌ی توزیع بدافزارهای بسیاری از جمله تروجان بانکی Dridex، باج‌افزار Locky، و الگوی pump-and-dump را در کارنامه‌ی خود دارد. همچنین در سال جاری این باتنت مخرب باج‌افزارهای Jaff و GlobeImposter را توزیع کرده است. این باتنت در آخرین فعالیت خود شروع به توزیع یک باج‌افزار جدید به نام Scarab کرده است. باج‌افزار Scarab اولین بار در ماه ژوئن سال ۲۰۱۷ میلادی توسط یک پژوهش‌گر به نام Michael Gillespie کشف شد. این پژوهش‌گر، موسس سرویس «ID Ransomwar» نیز می‌باشد. این سرویس به کاربران اجازه می‌دهد که با ارائه‌ی یک یادداشت باج‌خواهی متوجه شوند که چه باج‌افزاری سامانه‌ی آن‌ها را تحت تاثیر قرار داده است. پویش Scarab توسط شرکت امنیتی F-Secure نیز کشف شده است. بنابه گفته‌ی شرکت F-Secure، کد باج‌افزار Scarab مبتنی‌بر کد یک باج‌افزار متن‌باز به نام HiddenTear است که کد منبع آن توسط یک نفوذگر کلاه سفید برای اهداف آموزشی در دسترسی عموم قرار داده شده است. باتنت Necurs یک ابزار بارگیری اسکریپت مخرب به زبان VBS را که با نرم‌افزار فشرده‌سازی 7zip فشرده شده است را توزیع می‌کند. رایانامه‌هایی که توسط باتنت Necurs ارسال می‌شوند، اغلب دارای متن کوتاهی هستند و همچنین عناوینی مرتبط با کسب و کار را شامل می‌شوند؛ در پویش Scarab رایانامه‌های ارسالی ضمیمه‌هایی را ارائه می‌کنند که حاوی تصاویری از اسناد پویش‌شده هستند. عناوین متداول شامل «پویش‌شده به واسطه‌ی...» هستند و یکی از شرکت‌های Lexmark، HP، Cannon، یا Epson به آن اضافه شده‌اند. شرکت Forcepoint اعلام کرد: «دامنه‌های بارگیری که به عنوان بخشی از این پویش مورد استفاده قرار گرفته‌اند، وب‌گاه‌های آسیب‌دیده‌ای هستند که قبلا توسط پویش‌های مبتنی‌بر باتنت Necurs استفاده شده‌اند. این احتمال وجود دارد که بسیاری از سازمان‌ها این دامنه‌ها را در فهرست سیاه خود قرار داده باشند، اما این پویش به قدری گسترده است که احتمالا سامانه‌های زیادی را با باج‌افزار جدید Scarab تحت تاثیر قرار خواهد داد.» اگر ابزار بارگیری که در این پویش توزیع می‌شود، اجرا شده و باج‌افزار Scarab نصب شود، این باج‌افزار پرونده‌های موجود در سامانه‌ی قربانی را رمزگذاری می‌کند و پسوند scarab.[suupport@protonmail.com] را به این پرونده‌ها اضافه می‌کند. آدرس رایانامه‌ای که بخشی از این پسوند است، همان آدرس رایانامه‌ای است که در یادداشت باج‌خواهی نیز ارائه شده است. نام یادداشت باج‌خواهی که در این پویش جدید در پوشه‌های آسیب‌دیده قرار داده می‌شود عبارت «اگر می‌خواهید تمام پرونده‌های خود را برگردانید، لطفا این‌را بخوانید.» است. مهاجم در این یادداشت مقدار دقیق باج درخواستی مشخص نکرده و به جای آن گفته است که مبلغ درخواستی به سرعت پاسخ‌دهی از سمت قربانی بستگی دارد. با این وجود، این مهاجم برای این‌که اثبات کند که واقعا پرونده‌های آسیب‌دیده را رمزگشای می‌کند، پیشنهاد داده است که سه پرونده را به صورت رایگان رمزگشایی کند، در بخشی از یادداشت باج‌خواهی ذکر شده است: «قبل از پرداخت، شما می‌توانید سه پرونده برای ما ارسال کنید تا به صورت رایگان آن‌ها را رمزگشایی کنیم.»

منبع: securityweek  مترجم: مهندس معصومه خیری

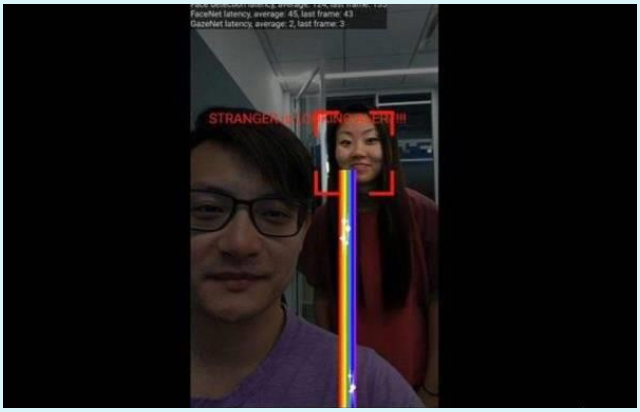
## حملات بدون استفاده از بدافزار در سال ۲۰۱۸

تیم امنیتی پاندا (Panda Security) ۷۵ میلیون بدافزار جدید را به تنهایی در نه ماهه اول سال ۲۰۱۷ کشف کرده است و برای سال ۲۰۱۸ در مورد حملاتی که از ابزارهای غیرمخرب سوء استفاده خواهندکرد، هشدار داده است. ارائه‌دهندگان سرویس های امنیتی اسپانیایی در گزارش سالیانه PandaLabs در سال ۲۰۱۷ ادعا کرده‌اند که تا بیستم ماه سپتامبر هر روز حدودا ۲۸۵ هزار نمونه از بدافزارها را شناسایی کرده‌اند. در بررسی گزارش‌های ۱۰ سال گذشته، ۴ فایل یافت می‌شود که مربوط به باج‌افزار مشهور WannaCry می‌باشد و همچنین دو لینک به ابزار مشهور بهینه‌سازی سرعت رایانه‌ها یعنی CCleaner وجود دارد. بیش از ۹۹ درصد از بدافزارهای شناخته شده در این سال توسط Panda فقط یکبار دیده شده است؛ به این معنی که تولیدکنندگان بدافزارها کدهای خود را هر بار با آسیب‌های جدیدی تغییر می‌دهند. با این حال، ارائه‌دهندگان در مورد " حملاتی که از ابزارهای غیرمخرب سوء استفاده می‌کنند" و در سال ۲۰۱۸ افزایش می‌یابند، هشدار داده‌اند. آنها با اشاره به آمار Verizon اینکه در حدودا نیمی از تخلف‌های ثبت شده (۴۹ درصد) در آخرین گزارش بررسی داده‌های غیر ایمن، هیچ بدافزاری یافت نشد. این موارد شامل ابزارهای مورد استفاده توسط مدیران شبکه می‌باشد، جایی که حساب کاربری مدیران با استفاده از کرک کردن، هک کردن یا حدس اعتبارنامه ورود ربوده شده است. لوئیس کورونس مدیر فنی InfoSecurity می‌گوید: "صحبت من در مورد ابزارهایی مانند Powershell مایکروسافت می‌باشد که در ارتش سوئیس بدون مدیر اصلی بکارگرفته شده و همزمان مورد حملات هکرها قرار گرفته است. بعنوان مثال، چند هفته قبل حمله‌ای خودکار را کشف کردیم که از ترکیب تکنیک‌های مختلفی از جمله استفاده از ضعف Powershell، دستکاری Mimikatz و بیشتر برای اجرای داده کاوی Monero در کامپیوترهای در معرض خطر، استفاده شده بود." این گزارش‌ها بیان می‌کنند که چنین تکنیک‌های جدید نیازمند تیم امنیتی فناوری اطلاعات برای بررسی دقیق‌تر در مورد چگونگی شناسایی و جلوگیری از تهدیدات سایبری برای سال بعد می‌باشد. در ارتباط با تهدیدات دیگر در سال ۲۰۱۸ ، این گزارش سیلی از حملات اینترنت اشیا و تهدیدات موبایل ، باج افزارها، تبلیغات ایمنی و یک اکوسیستم جنگ سایبری پیچیده با مهاجمانی که حملات خود را با تغییر عملکردهای نادرست مقادیر Flagها، مخفی می‌کنند را برجسته می‌کند.

منبع:infosecurity مترجم: مهندس ابوالفضل علیقلی‌وند

## نرم افزار جلوگیری از سرک کشیدن افراد به گوشی موبایل

محققان گوگل نرم افزاری جدیدی برای موبایل پیکسل ساخته اند که به کاربر هشدار می‌دهد کسی مشغول سرک کشیدن در نمایشگر موبایل آنها است. این نرم افزار با استفاده از دوربین جلوی دستگاه و هوش مصنوعی صورت‌هایی که روبروی نمایشگر قرار دارند را اسکن می‌کند. هنگامی که این نرم‌افزار فرد دیگری غیر از کاربر را رصد می‌کند که مشغول تماشای نمایشگر است، به او هشدار می‌دهد. این نرم‌افزار که «محافظ الکترونیک نمایشگر» نام گرفته، تصویری از فرد را با نوعی استیکر رنگین‌کمان نشان‌گذاری می‌کند و قادر است در ۲ میلیونم ثانیه نگاه فرد دیگری به موبایل کاربر را رصد کند و به کاربر خصوصاً هنگامی که مشغول خواندن اطلاعات حساس در اماکن عمومی است هشدار دهد.



منبع : وبسایت نمناک

## افشای اطلاعات میلیون‌ها کاربر اوبر

سال ۲۰۰۹ سرویسی به نام اوبر (Uber) در آمریکا راه‌اندازی شد. اوبر ایده ساده‌ای داشت: سفارش تاکسی به کمک برنامه موبایل. ایده اوبر به سرعت فراگیر شد، به نحوی که شرکت‌های بسیاری در سراسر جهان تلاش کردند مجموعه‌ای شبیه آن را در کشور خود راه‌اندازی نمایند. در این میان خوشبختانه ایران هم بی‌نصیب نمانده و «تاکسی یاب» تجربه‌ای متفاوت از حمل و نقل را با خود به کشورمان آورده‌است. اما چندی پیش اوبر از افشای اطلاعات کاربران خود خبر داد. شرکت اوبر تایید کرده است که در ماه اکتبر سال ۲۰۱۶ میلادی تعدادی از هکرها موفق شده بودند به سرورهای این شرکت نفوذ کرده و به اطلاعات ۵۷ میلیون از کاربران و رانندگان عضو اوبر دسترسی پیدا کنند. به همین دلیل هم بوده که جو سالیوان (رئیس بخش امنیت شرکت اوبر) سال گذشته به همراه یکی از معاونان خود از این شرکت اخراج شد. در این حمله سایبری، اطلاعات بالغ بر ۵۰ میلیون مشترک و هفت میلیون راننده عضو اوبر به سرقت رفته است که شماره گواهینامه ۶۰۰ هزار نفر از رانندگان نیز جزء آن بوده است. همچنین شرکت اوبر تایید کرده است که به منظور جلوگیری از افشای اطلاعات توسط هکرها، ۱۰۰ هزار دلار به عنوان حق السکوت پرداخت کرده است. هکرها با استفاده از یکی از مخازن ناامن موجود در گیت‌هاب که توسط مهندسان این شرکت استفاده می‌شد، اطلاعات مورد نیاز برای نفوذ در سرورهای اوبر را که توسط آمازون میزبانی می‌شود، به دست آورده بودند. اوبر به منظور حل مشکلات بوجود آمده دوباره به سراغ مشاور ارشد امنیتی سابق سازمان امنیت ملی رفته تا بتواند از راهکارهای وی در راستای افزایش امنیت و جبران خسارات وارده استفاده کرده و چهره مخدوش خود را در اذهان عمومی بهبود دهد. با اینکه شواهدی مبنی بر اینکه هکرها اطلاعات مورد نظر را از بین برده اند، وجود ندارد. اما شرکت اوبر مدعی شده است که هکرها پس از دریافت مبلغ مورد نیاز خود اطلاعات را از بین برده‌اند و این شرکت از نابودی اطلاعات مطمئن است.

بر اساس قانون اوبر باید افشای اطلاعات خود را به داستان عالی اطلاع می‌داد در حالیکه براساس ادعای رانندگان این سازمان، حتی به خود رانندگان هم اطلاع داده نشده است.

منبع ۱:bloomberg منبع۲:theguardian

گردآورنده: مهندس سمیرا سیفی

## جاسوسی گوگل حتی با غیرفعال کردن GPS

به گزارش گاردین گوگل به تازگی اعتراف کرده است که قادر است توسط گوشی‌های هوشمند اطلاعات مکانی، موقعیت کاربران را حتی زمانی که سیستم GPS موقعیت‌یاب گوشی‌های هوشمند غیرفعال و سیم کارت خارج از گوشی می‌باشد، بدست آورد. گوگل از ژانویه سال جاری میلادی برای چنین عملی از دکل‌های مخابراتی استفاده کرده است و بدین وسیله اطلاعات موقعیت مکانی کاربران را از طریق این دکل‌های مخابراتی به دست آورده و این داده‌ها را به صورت رمزگذاری شده برای سرورهای خود ارسال می‌کند.

این شرکت بیان کرد که اطلاعات مکانی افراد ذخیره نمی‌شوند و هر بار با موقعیت مکانی جدید جایگزین می‌شود. همچنین مدعی شد که استفاده از موقعیت مکانی تا ماه نوامبر پایان یافته است. گوگل دلیل استفاده از این روش را افزایش سرعت ارسال پیام اعلام کرده است. بسیاری از سرویس‌هایی که توسط گوشی‌های هوشمند فراهم می‌شوند مانند نقشه‌ها ، داده‌های موقعیت مکانی برای ارائه آب و هوا، نتایج اخبار محلی، خدمات خرید، از روش پیگیری موقعیت مکانی کاربران استفاده می‌کند.

اما در همه موارد با قطع کردن موقعیت مکانی و خارج کردن سیم‌کارت از پیگیری موقعیت مکانی جلوگیری می‌شود. درحالیکه این امکان در روش پیگیری موقعیت گوگل وجود ندارد.

منبع خبر:theguardian  مترجم: مهندس سمیرا سیفی


## حذف هر عکسی با آسیب‌پذیری موجود در فیس‌بوک

در اوایل ماه نوامبر، فیس‌بوک از یک ویژگی جدید برای ارسال نظرات حاوی عکس‌ها و تصاویر متحرک GIF خبر داد. پویا دارابی پژوهشگر ایرانی در حوزه امنیت و توسعه‌دهنده‌ی وب این ویژگی را مدت کوتاهی پس از راه‌اندازی آن تجزیه و تحلیل نموده و کشف کرد که این ویژگی یک آسیب‌پذیری را معرفی می‌کند که به آسانی قابل بهره‌برداری است.

هنگامی که یک کاربر یک نظر را ثبت می‌کند، این درخواست ارسال‌شده به سرورهای فیس‌بوک شامل شناسه‌ی فایل تصویر اضافه شده به نظر است و کاربران می‌توانند شناسه‌ی تصویر درخواست را با شناسه‌ی هر عکسی در فیس‌بوک جایگزین کنند و این تصویر در نظر ثبت‌شده نمایش داده شود. پویا دارابی گزارش داد هنگامی که نویسنده‌ی نظر پست را حذف کند، تصویری که شناسه‌ی آن به درخواست اضافه شده بود نیز از فیس‌بوک حذف می‌شود.

این آسیب‌پذیری در سوم ماه نوامبر به فیس‌بوک گزارش شد و در همان روز یک راه‌حل موقتی برای آن ارائه شد. این شرکت در پنجم ماه نوامبر یک وصله‌ی کامل را ارائه داد. یک پاداش ۱۰ هزار دلاری در ازای کشف این اشکال به پژوهش‌گر پرداخت شده است. این پژوهشگر یک پست وبلاگی و یک ویدئویی منتشر کرده است که این آسیب‌پذیری را توضیح می‌دهد.

این اولین بار نیست که دارابی یک پاداش قابل توجهی از فیس‌بوک دریافت کرده است؛ در سال ۲۰۱۵ میلادی، غول رسانه‌ی اجتماعی برای دور زدن سامانه‌های حفاظت دربرابر درخواست تقلبی (CSRF) مبلغ ۱۵ هزار دلار به او پاداش داد. سال بعد نیز پاداش ۷۵۰۰ دلاری برای ضعف‌های مشابه دریافت کرد.

این نوع آسیب‌پذیری‌ها در فیس‌بوک غیرعادی نیستند. در سال‌های گذشته، پژوهشگران چند آسیب‌پذیری را گزارش دادند که برای حذف نظرات، ویدئوها و تصاویر از فیس‌بوک مورد بهره‌برداری قرار می‌گرفتند. این حفره‌های امنیتی که در بیشتر موارد شامل جایگزین کردن شناسه‌ی منابع مورد هدف در یک درخواست است، برای پژوهشگران تقریباً ۱۰ هزار دلار درآمد داشت.

فیس‌بوک، میلیون‌ها دلار برای پژوهشگرانی پرداخت کرده است که آسیب‌پذیری‌های موجود در شبکه‌ی رسانه‌ی اجتماعی را از زمان راه‌اندازی برنامه‌ی پاداش در ازای اشکال آن در سال ۲۰۱۱ میلادی کشف کردند.

منبع ۱: وبسایت ایسیس (news.asis.io)

منبع ۲: blog.darabi.me

## هشدار مهم به کاربران اینترنت

کاربران به سایت‌هایی که وارد می‌شوند باید به اندازه کافی دقت کنند. به تازگی سایت pldn.ir توسط کارشناسان امنیت سایبری پادویش رصد شده است که این سایت و تمام آدرس‌هایی که به pldn.ir ختم می‌شوند (تعدادی از آن‌ها در زیر نمایش داده شده است) در واقع یک سایت Redirector می باشند.

- work.pldn.ir
- nemikham-bebinamet98.pldn.ir
- game.pldn.ir
- shabakeh.pldn.ir

زمانی که شما این سایت را باز می‌کنید به صورت تصادفی به صفحات دیگری هدایت می‌شوید که برخی از آن صفحات آلوده بوده و با استفاده از مهندسی اجتماعی تلاش می‌کنند تا شما را به دانلود فایل های آلوده ترغیب کنند.

منبع : فاتح‌گر

## پادشاه این روزها: بیت‌کوین – قسمت دوم

در شماره قبلی خبرنامه، در مورد بیت‌کوین، ویژگی‌های آن، چگونگی ساخت و نگهداری آن مطالبی ارائه دادیم. در این شماره می‌خواهیم در مورد افسانه‌ها و دروغ‌های بزرگی که درباره بیت‌کوین رواج یافته، صحبت کنیم.

✓ **بیت کوین ها ارزش حقیقی ندارند**

این موضوع به شدت بین کاربران مورد بحث قرار می‌گیرد. طرفداران این دروغ می‌گویند که چون بیت‌کوین تحت نظارت دولت نیست، پس پشتوانه‌ای ندارد و در حقیقت فقط یک عدد است. اما خوب است که آن‌ها بدانند ارزش با عرضه و تقاضا تعیین می‌شود. اگر از چیزی در داد و ستد استفاده شود، می‌تواند به عنوان پول مورد استفاده قرار بگیرد. حال ممکن است این چیز یک بشکه نفت باشد یا یک رمزنگاری مثل بیت کوین.

✓ **غیرقانونی است، چون یک پول رسمی نیست**

سؤال بزرگ دیگر درباره بیت‌کوین این است که آیا این یک ارز قانونی است. در ایالات متحده و بسیاری از کشورهای دیگر پول رسمی شامل سکه و اسکناس‌هایی است که توسط دولت برای انجام مبادلات ارائه می‌شوند. اما این به این معنی نیست که بیت‌کوین غیرقانونی هستند، زیرا دولت ایالات متحده آن را به عنوان ارز دیجیتال طبقه‌بندی کرده است. البته در چند کشور استفاده از بیت‌کوین غیرقانونی اعلام شده است، اما اکثریت دولت‌ها یا درباره بیت‌کوین سکوت کرده‌اند و یا آن را رسما قانونی اعلام کرده‌اند.

✓ **بیت‌کوین در درجه اول برای فساد و پولشویی استفاده می‌شود**

بیت‌کوین هم یک نوع ارز است. مانند دلار یا هر ارز دیگری. از بیت‌کوین می‌شود برای کارهای خیر استفاده کرد و هم می‌شود برای فساد و پولشویی از آن بهره برد. از آنجایی که امنیت بیت‌کوین بسیار بالاست، دلار و ارزهای سنتی بیشتر از بیت‌کوین در معرض فساد هستند. این اصلا عادلانه نیست که بیت‌کوین را در درجه ی اول برای فساد و پولوشویی بدانیم.

✓ **بیت کوین موجب فرار مالیاتی می شود**

استدلال این افراد این است که چون بیت‌کوین تراکنش‌ها را ناشناس انجام می‌دهد، می‌تواند باعث فرار از مالیات شود. اما باید توجه کنیم که به هر حال فردی که تراکنش‌ها را انجام می‌دهد، نمی‌تواند تا ابد آن را در کیف پول خود نگهداری کند و باید آن را برای کاری استفاده کند و یا بیت‌کوین هایش را بفروشد همچنین شیوه زندگی و دارایی‌های او ثبت شده است. راه‌های زیادی برای فرار مالیاتی وجود دارد و این را مطمئن باشید که بیت‌کوین بهترین راه این کار نیست.

✓ **بیت کوین ها به صورت رایگان اهدا می‌شوند**

داوید سیسرکیویچ گفت کسانی که فرایند استخراج بیت‌کوین را نمی‌دانند، فکر می‌کنند که بیت‌کوین‌ها به صورت رایگان اهدا می‌شوند. در واقع، بیت‌کوین‌ها طی یک فرآیند فشرده محاسباتی استخراج می شوند. تراکنش های بیت‌کوین توسط بلاک‌چین تأیید می‌شوند. ماینرها (استخراج کنندگان) کامپیوترهای قدرتمندی را به شبکه وصل می‌کنند که تراکنش‌های بیت‌کوین را پردازش و تأیید می‌کنند و در ازای این کار به عنوان پاداش به آن ها بیت‌کوین داده می شود. به عبارت دیگر آن‌ها بیت‌کوین‌ها را با فعالیت کامپیوترهای خود به دست می‌آورند. سختی استخراج به دلیل افزایش تراکنش‌ها و کمتر شدن کوین‌هایی که می‌توان استخراج کرد، روز به روز بیشتر می‌شود. بیت‌کوین فقط تا ۲۱ میلیون واحد قابل استخراج است که احتمال می‌رود تا سال ۲۱۴۰ طول بکشد.

✓ **بیت کوین یک طرح بزرگ پانزی است**

ترفند پانزی (Ponzi Scheme) یک عملیات سرمایه‌گذاری کلاه‌بردارانه است. در این ترفند به سرمایه‌گذاران سودهایی برگردانده می‌شود که از بهره‌های متعارف به شیوه‌ای غیرعادی بالاترند. البته این سود از پول سرمایه‌گذاران بعدی تأمین می‌شود و شرکت یا فرد دریافت‌کننده سرمایه نیازی به انجام کار اقتصادی با پول دریافتی ندارد. نام این ترفند از نام چارلز پانزی گرفته شده‌است.


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

از آنجایی که بیت‌کوین یک شبکه همتا به همتا و متن باز است هیچ نهاد مرکزی برای هدایت این پروژه وجود ندارد در حالی که در ترفند پانزی، شرکت‌های کلاهبردار توسط مدیران کنترل می‌شوند. این مضحک ترین دروغ درباره بیت‌کوین است.

✓ **پس از اینکه تعداد بیت کوین به ۲۱ میلیون رسید دیگر تراکنش ها تایید نمی‌شوند**

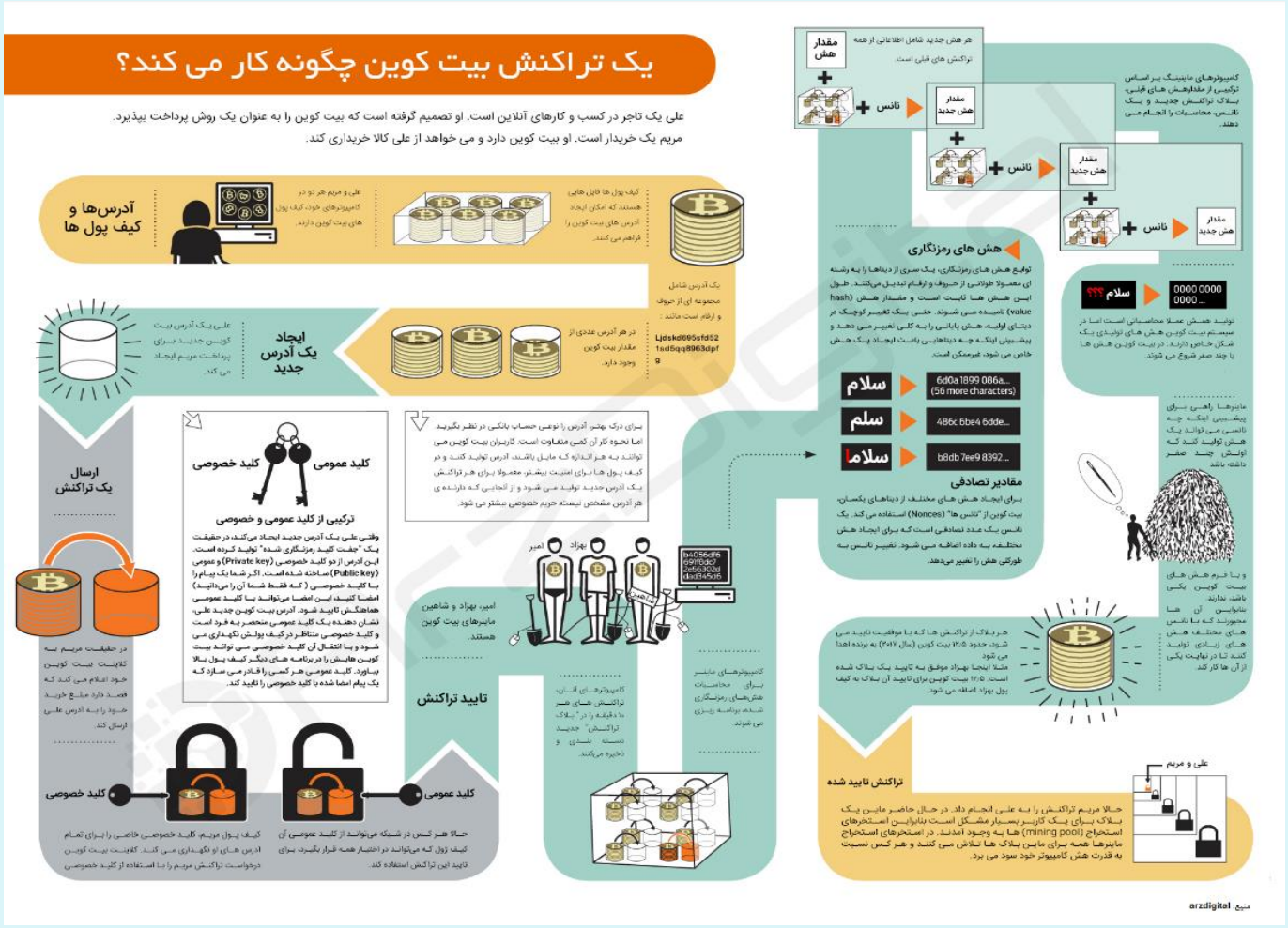
برخی از مردم در شبکه‌های اجتماعی اعلام کردند که وقتی دیگر بیت‌کوینی استخراج نشود، انگیزه‌ای برای ماینرها وجود نخواهد داشت و شبکه نابود خواهد شد. این مسئله ممکن است برای خود شما هم جای سوال باشد.

پس از اینکه ۲۱ میلیون بیت کوین استخراج شد، استخراج بیت‌کوین متوقف می‌شود. اما شبکه باید تضمین شده باشد و کار کند. انگیزه ماینر ها ممکن است کم شود، اما تولید بلاک‌های جدید در شبکه توزیع مهم است. وقتی بیت‌کوین‌ها دیگر استخراج نشوند به گردش خواهند افتاد و حجم تراکنش‌ها بالا خواهد رفت، پس ماینرها بازهم می‌توانند از تأیید تراکنش ها و کارمزد آن‌ها کسب درآمد کنند.

✓ **بیت کوین هک شده است**

همین اواخر که صرافی btc-e به دلیل کلاهبرداری بسته شد، افراد زیادی فکر کردند که بیت‌کوین هک شده است، شاید برای شما خنده دار باشد ولی این داستان واقعی است! این یکی از افسانه های بزرگ بیت‌کوین است. بیت کوین به هیچ وجه قابل هک نیست چون توسط بلاک چین بین میلیون‌ها کامپیوتر توزیع شده است. فرآیند یک تراکنش بیت کوین را در شکل زیر می‌توان دید. البته فقط در چند مورد آسیب‌پذیر بودن کیف پول‌ها و سایت‌ها باعث به سرقت رفتن بیت‌کوین ها شده است.

منبع: arzdigit گردآورنده: مهندس وحید فتحی



## 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 سیستم‌های 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.

**آزمایشگاه و مرکز تخصصی آپا دانشگاه محقق اردبیلی**
**cert.uma.ac.ir**


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