2017، سال کابوس متخصصان امنیت

# 11 هک، تهدید و رخنه بزرگ سال 2017

اگر جزء آن گروه از افرادی هستید که اخبار مربوط به حوزه امنیت را به طور مستمر دنبال می‌کنند، به‌خوبی به یاد دارید که در شماره 190 ماهنامه شبکه بزرگ‌ترین هک‌های تاریخ آی‌فون را مورد بررسی قرار دادیم. اما در شماره 201 ماهنامه شبکه تصمیم گرفتیم، 11 مورد از بزرگ‌ترین حملات و نقض‌های داده‌ای که سال گذشته میلادی به وقوع پیوستند و باعث شدند تا سازمان‌ها و کاربران در سراسر جهان با چالش جدی روبه‌رو شوند را مورد بررسی قرار دهیم. بدون شک تحلیل دقیق این تحولات به ما کمک می‌کند تا در سال آتی و همچنین سال‌های پیش رو به‌شکل دقیق‌تری از خود و سامانه‌های اطلاعاتی محافظت به عمل آوریم. اما بدون شک سال 2017 همانند یک کابوس شبانه و بدون وقفه برای سازمان‌ها و به‌ویژه کارشناسان امنیتی بود.

بدون اغراق باید بگوییم سال 2017 همراه با مسائل متعدد امنیتی پشت سر گذاشته شد. در سالی که گذشت، شاهد نقض‌های متعدد گذرواژه‌ای، هجمه سنگین حملات بدافزاری و به سرقت رفتن شماره کارت‌های اعتباری بودیم. در حالی که هریک از موارد یاد شده دردسرهای متعددی را برای کاربران و سازمان‌ها به وجود آوردند، اما برای بسیاری از کارشناسان حوزه امنیت شنیدن این اخبار موضوع جدیدی نیست. اما حملات هکری در سال گذشته میلادی به سه موردی که به آن اشاره کردیم محدود نشد و متوجه شدیم که در سال‌های آتی با گونه جدیدی از تهدیدات هکری روبه‌رو خواهیم بود. تجربیات تلخ سال گذشته میلادی به ما نشان داد هکرهای سازمان یافته در تلاش هستند تا به زیرساخت‌های حیاتی نفوذ کنند. ابزارهای قدرتمند هک که در سال گذشته میلادی از سوی هکرها به کار گرفته شد و سازمان‌ها و نهادهای دولتی ایالات متحده را تحت تأثیر خود قرار داد، حجم بسیار بالایی از شماره‌های تأمین اجتماعی که به سرقت رفتند، نفوذ مخفیانه به حریم خصوصی و آنلاین کاربران و شناسایی بدافزارها در نرم‌افزارهای محبوبی که میلیون‌ها کاربر در سراسر جهان از آن استفاده می‌کنند تنها بخشی از بردارهای حمله‌ای بود که سال گذشته میلادی نظاره‌گر آن‌ها بودیم. بدون شک حملات هکری سال گذشته میلادی در سال جدید میلادی نیز تکرار خواهند شد، پس بهتر است برجسته‌ترین رخدادهای سال گذشته میلادی در حوزه امنیت را مورد بررسی قرار دهیم تا در سال جدید به‌شکل بهتری از سامانه‌های خود محافظت کنیم.

## 1*افشای اطلاعات از سوی Shadow Brokers و Vault7

بدون شک مهم‌ترین رخداد امنیتی سال گذشته در ارتباط با افشای اطلاعات محرمانه‌ای بود که به طور مستقیم با نهادهای دولتی ایالات متحده در ارتباط بود. ویکی‌لیکس در ماه مارس اطلاعات گسترده‌ای را تحت عنوان Vault7 منتشر کرد. در این افشاگری ویکی‌لیکس به راهکارهایی اشاره کرد که آژانس‌های دولتی برای نفوذ و استراق سمع از آن‌ها استفاده می‌کنند. در آوریل نیز گروه هکری Shadow Brokers دست به افشاگری بزرگی زدند. این گروه مدعی شد ابزارهایی که سازمان‌های جاسوسی برای نفوذ سایبری از آن‌ها استفاده می‌کنند را به سرقت برده‌اند. در ادامه این گروه تصمیم گرفت این ابزارها را به‌صورت برخط منتشر کنند و در اختیار عموم کاربران قرار دهند. این

افشاگری‌ها باعث نگرانی هرچه بیشتر کارشناسان امنیتی شد، به‌واسطه آنکه هر کاربری به ابزارهای نفوذ دسترسی پیدا کرد و هم اینکه بسیاری از کارشناسان اعلام کردند ما در زمینه امنیت زیرساخت‌های حیاتی باید تجدیدنظر اساسی داشته باشیم.

## 2*نقض داده‌ای Equifax

بدون شک حمله‌ای که در ماه سپتامبر (شهریور ماه) به وقوع پیوست و نقض داده‌ای Equifax نام گرفت، یکی از بدترین و در عین حال دلهره‌آورترین خبرهایی بود که در سال گذشته میلادی شنیدیم. شرکت Equifax یکی از سه مؤسسه اعتباری و مالی بزرگ در ایالات متحده است که اطلاعات مربوط به گردش‌های مالی افراد را در اختیار دارد. هکرها در اوایل ماه آوریل موفق شدند اطلاعات مربوط به شماره تأمین اجتماعی نزدیک به 143 میلیون شهروند ایالات متحده را به سرقت ببرند. به عبارت دقیق‌تر، هکرها اطلاعات بیش از نیمی از شهروندان ایالات متحده را به سرقت بردند. سهل‌انگاری در نصب
وصله‌های امنیتی روی زیرساخت‌های این مؤسسه باعث شد تا هکرها بتوانند از درب پشتی به وجود آمده روی شبکه این شرکت به‌منظور پیاده‌سازی حمله خود استفاده کنند. این هک بزرگ باعث شد تا این شرکت به‌راحتی قرارداد مربوط به ضدجعل هویت را از دست بدهد.

## 3*درب پشتی شناسایی شده در CCleaner

در ماه سپتامبر پژوهشگران امنیتی شرکتی Cisco Talos موفق شدند کدهای مخربی را در نرم‌افزار محبوب CCleaner شناسایی کنند. نرم‌افزار فوق یک بسته کمکی است که برای سیستم عامل ویندوز ارائه شده و به کاربران در پاکسازی و حذف فایل‌ها و تنظیمات زائد کمک می‌کند. بدافزار شناسایی شده در این نرم‌افزار به‌منظور سرقت داده‌های شخصی از کامپیوترهای آلوده مورد استفاده قرار می‌گرفت. تحلیل دقیقی که از سوی شرکت امنیتی AVast انجام شد، نشان داد عملکرد بدافزار به کار گرفته شده در این نرم‌افزار به‌مراتب فراتر از آن چیزی بود که در ابتدا تصور می‌شد. این بدافزار به‌شکل کاملاً هدفمندی کامپیوترهای خاص مستقر در شرکت‌هایی همچون سیسکو، سونی و اچ‌تی‌سی را هدف قرار داده بود. این بدافزار به‌دنبال آن بود تا اطلاعات مخفی و اسرار این سازمان‌ها را به سرقت ببرد. تحقیقات بعدی نشان داد چیزی نزدیک به دو میلیون کاربر در سراسر جهان به بدافزار فوق آلوده شدند. بدافزار شناسایی شده درنهایت در جدیدترین نگارشی که از سوی شرکت سازنده ارائه شد، حذف شد.

## 4*دردسر شرکت کسپرسکی

کمتر کاربری را پیدا می‌کنید که از ماجرای شرکت کسپرسکی بی‌اطلاع باشد. بدون شک چالشی که سال گذشته میلادی برای شرکت کسپرسکی و نرم‌افزار امنیتی این شرکت به وجود آمد، بیشتر از خبر هک شدن سایت‌ها مورد توجه رسانه‌ها قرار گرفت. چالشی که اشاره به این موضوع داشت که ضدویروس این شرکت در نقش یک ابزار جاسوسی عمل می‌کند. در ماه اکتبر وال‌استریت ژورنال گزارش داد که هکرهای دولتی از نرم‌افزار ضدویروس کسپرسکی برای شناسایی و هدف قرار دادن آژانس‌های دولتی ایالات متحده استفاده می‌کردند. البته کسپرسکی به طور قاطع این حرف را رد و اعلام کرد هیچ اطلاعاتی از سوی این نرم‌افزار به سرقت نرفته است. کسپرسکی برای آنکه نشان دهد هیچ‌گونه عمل خلافی در این زمینه انجام نشده است، به شرکت‌های ثالث اجازه داد تا کدهای ضدویروس کسپرسکی را مورد بررسی قرار دهند. اما در مقابل کارشناسان امنیتی اعلام داشتند بررسی کدها نمی‌تواند در این زمینه راهگشا باشد. درنهایت کار به آنجا رسید که به‌کارگیری محصولات این شرکت در ادارات دولتی ایالات متحده ممنوع و دفتر این شرکت در واشنگتن نیز در ماه دسامبر تعطیل شد.

## 5*نقض داده‌ای مرتبط با یک شبکه تلویزیونی

کار چندان ساده‌ای نیست که یک برنامه تلویزیونی کار خود را آغاز کند و در ادامه بتواند مخاطبان میلیونی را به دست آورد. به‌ویژه زمانی که افراد کنجکاو می‌شوند تا بدانند یک استودیو تلویزیونی در نظر دارد در آینده چه کارهایی انجام دهد. این دقیقاً همان چالشی است که شرکت HBO با آن روبه‌رو شد. این شبکه تلویزیونی در ماه جولای در معرض حمله هکری قرار گرفت. در این حمله هکرها ادعا کردند 1.5 ترابایت اطلاعات از کانال تلویزیونی این شبکه به سرقت بردند. در اطلاعات به سرقت رفته، ایمیل‌های مربوط به مدیریت، اطلاعات مربوط به اپیزودهای سریال‌های محبوب این شبکه و همچنین پیش‌نویس‌های مربوط به سریال بازی تاج و تخت نیز به سرقت رفت. در ماه نوامبر این شرکت اعلام کرد موفق شده است هکری که این حمله را انجام داده شناسایی کند.

## 6*افشای هک‌های گسترده سال 2016 یاهو

قبل از آنکه یاهو از سوی ورایزن خریداری شود، این غول اینترنتی بزرگ دو بار در معرض حمله هکری قرار گرفته بود. حملاتی که به طور خاص گذرواژه‌ها و نام کاربری افرادی که در یاهو عضو بودند را به سرقت برد. به عبارت دقیق‌تر، هکرها در سال 2016 موفق شده بودند به‌شکل موفقیت‌آمیزی در دو مرحله به یاهو حمله کنند. این شرکت به‌تازگی حساب‌های کاربری که تحت تأثیر نقض‌های داده‌ای سال 2013 بودند را ترمیم کرده است. اواخر سال 2016 میلادی بود که عنوان شد تعداد حساب‌های کاربری که تحت تأثیر این حمله قرار گرفته بودند نزدیک به یک میلیارد حساب کاربری بوده است. اما در ماه اکتبر یاهو اعلام کرد بیش از سه میلیارد حساب کاربری در جریان این حملات تحت تأثیر قرار گرفته و اطلاعات آن‌ها به سرقت رفته‌اند. به طوری که یاهو اعلام کرد کاربران بهتر است در سریع‌ترین زمان ممکن گذرواژه خود را تغییر دهند.


## 7*باج‌افزار واناکرای

در ماه می بود که اعلام شد باج‌افزاری به‌نام واناکرای برای دومین بار متوالی فعالیت‌های خود را آغاز کرده است. باج‌افزاری که اولین بار در ماه مارس شناسایی شده بود. حملاتی که در ماه می از سوی این باج‌افزار به وقوع پیوست به‌مراتب هراس‌انگیزتر بود، به‌واسطه آنکه هکرها کدهای این باج‌افزار را ویرایش کرده و بخشی را به کدهای مخرب اضافه کرده بودند تا باج‌افزار عملکردی شبیه به یک کرم اینترنتی پیدا کند. رویکردی که درنهایت باعث شد سرعت تکثیر این باج‌افزار دوچندان شود. در ادامه گروه ShadowBrokers در ماه آوریل کشف کردند که باج‌افزار فوق بر پایه یک رخنه امنیتی به‌نام EternalBlue کار می‌کند. حملات واناکرای به دو دلیل با موفقیت همراه بود، اول آنکه هیچ‌کدام از دستگاه‌های آلوده وصله مربوط را دریافت نکرده بودند و دوم آنکه این وصله با تأخیر عرضه شد. این باج‌افزار به اندازه‌ای مهلک بود که مایکروسافت را مجبور کرد برای ویندوز ایکس‌پی و ویندوز سرور 2013 وصله‌هایی را ارائه کند. سرانجام یک کارشناس امنیتی به‌نام کارکوس هاچینس موفق شود سوئیچ مرگ درون این باج‌افزار را شناسایی کند و به کار آن خاتمه دهد.


## 8*خون‌ریزی کلاود (Cloudbleed)

شبکه تحویل محتوای Cloudflare که از مشهورترین شرکت‌ها در این زمینه به شمار می‌رود، در فوریه 2017 از وجود باگی مهم و خطرناک در الگوریتم تجزیه کدهای HTML اطلاع پیدا کرد. این شرکت در اغلب موارد صفحات عادی پروتکل انتقال ابرمتن مشتریان خود را به پروتکل انتقال ابرمتن ایمن تبدیل می‌کند. مکانیسم تجزیه‌کننده به کار گرفته شده از سوی این شرکت این توانایی را دارد تا کارهایی همچون پنهان کردن محتوا از دید بات‌ها، پنهان‌سازی نشانی‌های ایمیل و کار با سامانه AMP گوگل را انجام دهد. اما سامانه تجزیه‌گر به یک رخنه آلوده بود که اجازه می‌داد اطلاعات حساس و مهمی که از سوی موتورهای جست‌وجوگر همچون بینگ و گوگل کش شده افشا شود. این اطلاعات حساس دربرگیرنده پیام‌های خصوصی از سایت‌های قرار ملاقات، چت‌های متنی متعلق به سرویس‌های پیام‌رسان محبوب، ابزارهای مدیریت گذرواژه و رزرو هتل بودند. رخنه CloudFlare شبیه به باگ خون‌ریزی قلبی بود که در سال 2014 کشف شد.

## 9*افشای داده‌های مربوط به رأی‌دهندگان

سرورها امروزه نقش بسیار مهمی در زندگی ما و در شبکه‌های کامپیوتری بازی می‌کنند. در نتیجه نه‌فقط وصله‌های مربوط باعث می‌شوند تا سرورها از دسترس هکرها به دور بمانند، بلکه باید به‌درستی پیکربندی شده باشند تا مانع از افشای داده‌های شخصی شوند. اما شرکت Deep Root Analytics که در زمینه بزرگ داده‌ها به فعالیت اشتغال دارد در ماه ژوئن کشف کرد یکی از سرورهای آمازون به‌دلیل پیکربندی اشتباه، اطلاعات مربوط به 198 میلیون رأی‌دهنده را افشا کرده است. پیکربندی اشتباه سرور از سوی یک تحلیلگر مسائل امنیتی شناسایی شد و هکرها موفق نشدند به این اطلاعات دست پیدا کنند.

## 10*لپ‌تاپ‌های آلوده به کی‌لاگرهای شرکت اچ‌پی

سال 2017 برای شرکت اچ‌پی سال کی‌لاگرها بود. در ماه می بود که یک شرکت امنیتی مستقر در کشور سوئیس موفق شد مدل‌های مختلفی از لپ‌تاپ‌های تولید شده از سوی شرکت اچ‌پی را کشف کند که قادر بودند کلیدهای تایپ شده از سوی کاربران را به سرقت ببرند. نرم‌افزار رباینده کلیدها درون درایور صوتی پنهان شده و حداقل از سال 2015 میلادی تا به امروز در این درایور پنهان بود. درایور به‌منظور هشدار دادن زمانی که کلید مخصوصی روی کامپیوتر فشرده می‌شد طراحی شده بود، اما این درایور در اصل همه کلیدهای تایپ شده از سوی کاربر را ضبط می‌کرد. کلیدهای ضبط شده درون یک فایل غیررمزنگاری شده قرار می‌گرفتند. این نرم‌افزار قادر بود گذرواژه‌ها، نام‌های کاربری و داده‌های خصوصی کاربران را به سرقت ببرد و به‌راحتی برای هک کردن کاربران مورد

استفاده قرار گیرد. در ماه دسامبر نیز یک کارشناس امنیتی دیگر موفق شد یک کی‌لاگر را در درایور لمسی Synaptics لپ‌تاپ‌های اچ‌پی شناسایی کند. کی‌لاگری که روی بیش از 500 مدل نوت‌بوک شرکت اچ‌پی نصب شده بود. خوشبختانه، در این مورد کی‌لاگر به‌طور پیش‌فرض غیرفعال بود، اما در هر دو حالت کی‌لاگرها به‌شکل تصادفی یا اشتباهی روی لپ‌تاپ‌ها نصب شده بودند.

## 11*اختلال در شبکه انتقال برق اوکراین

در ژانویه سال گذشته میلادی، پژوهشگران امنیتی کشف کردند هکرها باعث بروز اختلال در شبکه انتقال برق اوکراین در دسامبر سال 2016 میلادی بوده‌اند. حمله‌ای که در یکی از سردترین ماه‌های سال این کشور به وقوع پیوست. این دومین باری بود که یک حمله سایبری باعث شد شبکه انتقال برق در کشور اوکراین قطع شود. قطعی برق در کشور اوکراین این پرسش مهم را به وجود آورد که آیا هکرها این توانایی را دارند تا به شبکه انتقال برق در کشورهای دیگری همچون ایالات متحده هم حمله کنند؟ جواب این پرسش مثبت است. دو ماه قبل از این اتفاق هکرها موفق شده بودند به زیرساخت‌های ایالات متحده نفوذ کنند. در اواسط ماه دسامبر، رویترز گزارش کرد که هکرها موفق شدند سامانه امنیتی یکی از تأسیسات زیرساختی ایالات متحده را مورد نفوذ قرار دهند. قبل از این اتفاق نیز شرکت سیمانتک در سپتامبر هشدار داده بود که هکرهای سازمان یافته به طور ویژه سازمان‌های مرتبط با انرژی در کشورهای ایالات متحده و دیگر کشورهای اروپایی را هدف قرار داده و در نظر دارند عملیات خرابکارانه‌ای را به مرحله اجرا درآورند. در این گزارش آمده است که حمله سایبری به تأسیسات اتمی دور از انتظار نیست.

**منبع:**

pcworld

**تاریخ انتشار:**
16 فروردین 1397

---

**نشانی منبع:**
https://www.shabakeh-mag.com/security/12170/11-%D9%87%DA%A9%D8%8C-%D8%AA%D9%87%D8%AF%DB%8C%D8%AF-%D9%88-%D8%B1%D8%AE%D9%86%D9%87-%D8%A8%D8%B2%D8%B1%DA%AF-%D8%B3%D8%A7%D9%84-2017