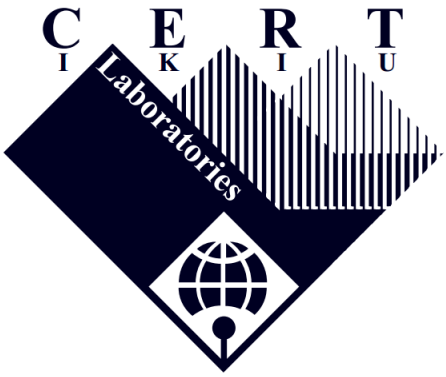

آزمایشگاه تخصصی آپا، قزوین

دانشگاه بین المللی امام خمینی (ره)

هفته نامه تحلیلی رویدادهای امنیتی

شنبه بیست و ششم خرداد ماه ۱۳۹۷

نسخه ۱,۰,۰

بنام خداوند بخشنده و مهربان

یادداشت سردبیر

امروزه هدف اصلی بسیاری از حملات در فضای سایبری به سمت استخراج غیرمجاز ارزهای دیجیتال در حال تغییر است. مهاجمان به این طریق می‌توانند از منابع پردازشی قربانیان خود برای تولید ثروت استفاده نمایند. ارز دیجیتال فناوری بر اساس بلاک‌چین بوده که واحدهای آن می‌توانند از طریق پردازنده‌های مرکزی و گرافیکی نیز استخراج[1] شوند. این واحدها امروزه در بسیاری از صرافی‌ها در جهان قابل تبدیل به سایر ارزهای رایج نظیر دلار و یورو هستند. فرآیند استخراج امری با پردازش‌های سنگین و طولانی بوده که از توان رایانه‌های معمولی خارج است (در استخراج حجم مناسب). بنابراین عدم دسترسی مهاجمان به ابررایانه‌ها می‌تواند به تولید و گسترش بدافزارها و به دنبال آن استفاده غیر مجاز از منابع پردازشی بخش زیادی از کاربران ختم گردد. البته این امر به معنی حذف سایر اهداف مخربانه از جمله جاسوسی‌ها و اجرای حملات توزیع شده انکار خدمت دی.او.اس[2] نبوده و بسیاری از بدافزارها جدید نشان داده‌اند که علاوه بر فرآیند استخراج برخی دیگر از فعالیت‌های مخربانه را نیز انجام می‌دهند.

بررسی بدافزارهای مخرب نشان‌دهنده علاقه مهاجمان فضای سایبری به انتخاب مونرو[3] به عنوان ارز مورد استخراج است. لیست زیر دو دلیل اصلی برای این انتخاب را نشان می‌دهد.

۱- امکان استخراج این ارز در اکثر بسترهای رایانه‌ای
۲- عدم ردیابی تراکنش‌ها در شبکه ارز مونروکه می‌تواند دست مهاجمان را مخفی نگه دارد. در پروژه جدید مونرو حتی آدرس‌های آی.پی نیز مخفی می‌گردند.

سرقت ارز اتریوم معادل با ۲۰ میلیون دلار توسط هکران در هفته پیش خبری بود که نظر بسیاری از افراد فعال در حوزه فناوری اطلاعات را به خود جلب کرد. در این سرقت مهاجمان مستقیما به ابزارهای مدیریت اتریوم حمله کرده و توانستند بخش عظیمی از ارزهای کاربران این شبکه را به حساب خود منتقل کنند. عدم مخفی سازی تراکنش‌ها در شبکه اتریوم در نهایت منجر به تشخیص حساب مورد استفاده هکران در این انتقال گردید. چیزی که در شبکه مونرو وجود نداشته و همین امر منجر به افزایش علاقه هکران به این ارز شده است.

[1]-Mine
[2]-DOS
[3]-Monero

با افزایش حملات، بسیاری از شرکت‌های معتبر در حوزه فناوری اطلاعات نیز به سمت ایجاد نظامی برای مقابله حرکت کرده‌اند. اپل به عنوان یکی از این شرکت‌ها، اخیرا ابزارهای استخراج ارزهای دیجیتال را در فروشگاه رسمی خود مسدود کرده است. شرکت گوگل نیز که چندی پیش افزونه‌های استخراج ارز دیجیتال را در مرورگر کروم[1] مسدود کرده بود اینک از پایان نصب افزونه‌های مستقیم (بدون ارتباط با فروشگاه رسمی کروم) در آینده‌ای نزدیک خبر می‌دهد. ایجاد محدودیت‌های مذکور می‌تواند نگرانی‌های ناشی از حملات این دسته و حتی سایر موارد را تا حد زیادی برطرف کند. البته تجربه نشان داده که دانش ناکافی کاربران و همچنین عدم اقدام مناسب امنیتی همیشه راه را برای اجرای حملات مختلف توسط مهاجمان سایبری باز گذاشته است. مصداق بارز این امر را می‌توان در تمامی خبرهای هفته گذشته مشاهده نمود.

خبرهایی از جمله بدافزار جدید پرولی، افزونه‌های مخرب در مرورگرها و حتی بهره‌گیری از فناوری ای.ام.بی باز در دستگاه‌های اندرویدی که همگی با سوءاستفاده هکران از دانش ناکافی کاربران در حوزه امنیت اطلاعات همراه بوده است. بنابراین امروزه می‌توان عدم رعایت نکات امنیتی کاربران یک سازمان را مهم‌ترین دلیل نفوذ مهاجمان به آن شرکت دانست.

محمد پیشدار

[1]-Chrome

فهرست مطالب

خبر شماره ۱ تاریخ انتشار : ۹۷/۰۳/۲۰

کشف بدافزاری خطرناک به نام پرولی[1]

خلاصه

پژوهشگران حوزه امنیت اطلاعات اخیرا موفق به کشف بدافزاری مخرب و خطرناک به نام پرولی شده‌اند. این بدافزار در مدت کوتاهی توانسته بیش از ۴۰۰۰۰ دستگاه متعلق به ۹۰۰۰ کسب‌کار در حوزه‌های مختلف نظیر تجاری، آموزشی و حتی دولتی را آلوده نماید. این امر در شرایطی رخ داده که زمان زیادی از کشف بدافزار وی.پی.ان فیلتر[2] نمی‌گذرد. بدافزاری که موفق به آلوده‌سازی بخش اعظمی از مسیریاب‌ها و تجهیزات شبکه در سراسر جهان گردید. بر این اساس دو حمله مذکور را می‌توان قدرت نمایی دیگری از هکران در فضای سایبری دانست که وسعت آن نشان‌دهنده نیاز شدید برخی سازمان‌ها به افزایش امنیت اطلاعات می‌باشد. البته سازندگان این بدافزار نیز به خوبی از ضعف سازمان‌ها در این حوزه مطلع بوده‌اند. به همین دلیل مبنای گسترش پرولی را بر اساس بهره‌گیری از برخی اکسپلویت[3]های معروف، تکنیک‌های جستجوی جامع[4] کلمات عبور و حتی سوءاستفاده از پیکربندی‌های ضعیف قرار داده‌اند.

برای مشاهده متن کامل خبر می‌توانید به آدرس زیر مراجعه نمایید.

https://cert.ikiu.ac.ir/news-view.php?nid=40

مرجع اصلی خبر:

The Hacker News Website (https://thehackernews.com/2018/06/prowli-malware-botnet.html)

[1]-Prowli
[2]-VPN Filter
[3]-Exploit
[4]-Brute Force

خبر شماره ۲ تاریخ انتشار : ۹۷/۰۳/۲۱

سرقت ارز اتریوم[1] معادل با ۲۰ میلیون دلار

خلاصه

اخیرا برخی وبگاه‌های امنیتی خبری مبنی بر سرقت ۲۰ میلیون دلار ارز اتریوم منتشر را کرده‌اند. در این سرقت گسترده برخی ابزارهای مشتری[2] با پیکربندی نادرست در شبکه اتریوم مورد حمله قرار گرفته‌اند. مهاجمان فضای سایبری برای این امر حساب‌های دارای پورت باز ۸۵۴۵ را هدف قرار داده‌اند. از این پورت برای مدیریت راه دور[3] حساب‌های کاربری استفاده می‌گردد. مهاجمان از طریق پورت مذکور به سیستم قربانی دسترسی یافته و ارزهای وی را به حساب‌های خود منتقل کرده‌اند.

یک گروه امنیتی در ماه مارس[4] میلادی ضمن تایید فعالیت‌های مخربانه هکران در این راستا هشداری جدی برای کابران خود منتشر کرده است. در گزارش این گروه حدود ۳,۵ واحد اتریوم در آن ماه مورد سرقت قرار می‌گیرد. امروزه دامنه این حملات به شدت گسترش یافته به طوری که سرقت حدود ۳۸۶۴۲ واحد اتریوم تنها توسط یک گروه از هکران مورد تایید قرار گرفته است. این مقدار ارز اتریوم معادل حدود ۲۰۵۰۰۰۰۰ دلار می‌باشد.

برای مشاهده متن کامل خبر می‌توانید به آدرس زیر مراجعه نمایید.

https://cert.ikiu.ac.ir/news-view.php?nid=41

مرجع اصلی خبر:

The Hacker News Website (https://thehackernews.com/2018/06/ethereum-geth-hacking.html)

[1]-Ethereum
[2]-Client
[3]-RPC
[4]- March

خبر شماره ۳ تاریخ انتشار : ۹۷/۰۳/۲۳

تغییر سیاست گوگل در قبال افزونه[1]های مرورگر کروم[2]

خلاصه

احتمالا تاکنون به وبگاه‌های ارائه دهنده افزونه‌های مرورگر کروم در فضای اینترنت برخورد کرده‌اید. بسیاری از این وبگاه‌ها برای نصب افزونه هیچ‌گونه ارتباطی با فروشگاه رسمی کروم[3] برقرار نمی‌کنند. امروز شرکت گوگل در وبلاگ رسمی مرورگر کروم از تصمیم خود برای تغییرات جدی در فرآیند نصب افزونه‌های این مرورگر رونمایی کرد با اجرای این تغییرات نصب افزونه‌های مرورگر کروم با پایان سال ۲۰۱۸ تنها از طریق فروشگاه رسمی این شرکت (برای تمام پلتفرم‌ها) صورت خواهد پذیرفت. این اولین واکنش شرکت گوگل به نصب افزونه‌های غیرمجاز نبوده و از شروع فرآیند مقابله این شرکت با افزونه‌های کاهش دهنده امنیت کاربران و همچنین کاهش‌دهنده سرعت ارتباطات مدت زیادی می‌گذرد. یک نمونه از فعالیت‌ها جلوگیری از نصب افزونه ها استخراج ارز دیجیتال[4] در سال گذشته است.

برای مشاهده متن کامل خبر می‌توانید به آدرس زیر مراجعه نمایید.

https://cert.ikiu.ac.ir/news-view.php?nid=42

مرجع اصلی خبر:

The Hacker News Website (https://thehackernews.com/2018/06/chrome-extension-intallation.html)

[1]-Extension
[2]-Chrome
[3]-Chrome Web Store
[4]- Cryptocurrency Mining

خبر شماره ۴ تاریخ انتشار : ۹۷/۰۳/۲۴

آسیب‌پذیری دستگاه‌های دارای سیستم‌عامل اندروید

خلاصه

سرویس اشکال زدایی راه دور در سیستم‌عامل اندروید (ای.دی.بی[1])، سرویسی است که می‌تواند برای تشخیص و عیب‌یابی مشکلات نرم‌افزاری حتی بدون نیاز به دسترسی فیزیکی نیز مورد استفاده قرار بگیرد. استفاده از این سرویس می‌تواند به اجرای دستورات سیستمی و حتی کنترل کامل دستگاه از طریق خط فرمان[2] بیانجامد. ای.دی.بی را می‌توان در کنار فواید خوبی که داراست به عنوان یک نقطه آسیب‌پذیر خطرناک نیز برای سیستم‌عامل اندروید تلقی نمود. امروزه حتی با وجود هشدارهای فراوان محققان امنیتی در مورد شدت خطر این آسیب‌پذیری، بسیاری از سازندگان دستگاه‌های اندرویدی همچنان به ساخت دستگاه‌هایی با بهره‌گیری فعال از این فناوری ادامه می‌دهند.

برای مشاهده متن کامل خبر می‌توانید به آدرس زیر مراجعه نمایید.

https://cert.ikiu.ac.ir/news-view.php?nid=43

مرجع اصلی خبر:

The Hacker News Website (https://thehackernews.com/2018/06/android-adb-hacking.html)

[1]-ADB
[2]-Command Line Interface.