بولتن خبری

مرکز تخصصی آپا دانشگاه رازی

شماره دوازدهم
تیر و مرداد ماه ۱۳۹۸

هشدار برای دارندگان گوشی های هوشمند!

۴۰٪ برنامه های اندروید و iOS در مقابل هک آسیب پذیر هستند

در این شماره می‌خوانید:

فهرست

مرکز تخصصی آپا دانشگاه رازی
پیشرو در ارائه خدمات امنیت و فناوری اطلاعات

صاحب امتیاز: **مرکز تخصصی آپا دانشگاه رازی**

سردبیر: **سهیلا مرادی**

صفحه آرایی: **سید احسان حسینی**

همکاران این شماره:

سهیلا مرادی
سیده مرضیه حسینی
سیده آرزو حسنی
صبا آزرمی
علیرضا عبدی

آدرس:

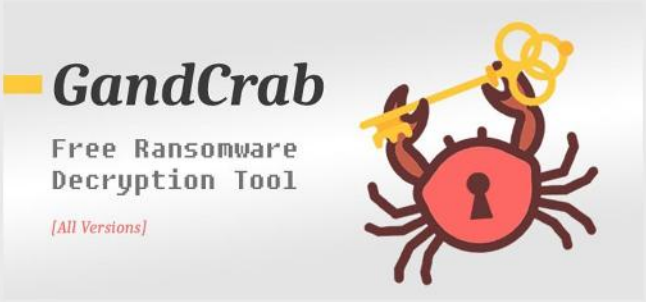
کرمانشـــاه، باغ ابریشـــم، دانشـــگاه رازی، دانشکده برق و کامپیوتر، طبقه همکف، مرکز تخصصی آپا

apa@razi.ac.ir
cert.razi.ac.ir
۰۸۳۳۴۳۴۳۲۵۱

اخبار امنیتی

انتشار ابزار رمزگشایی تمام نسخه‌های باج‌افزار GandCrab و بازیابی فایل‌ها به صورت رایگان

گردآورنده: علیرضا عبدی
ویراستار: سیده مرضیه حسینی



پژوهشگران امنیت سایبری نسخه‌ی جدیدی از ابزار رمزگشایی باج‌افزار GandCrab را منتشر کرده‌اند که می‌تواند میلیون‌ها کاربر آسیب‌دیده از این باج‌افزار را قادر سازد که فایل‌های رمزنگاری شده‌ی خود را به صورت رایگان و بدون پرداخت باج به مجرمان سایبری، بازگشایی کنند.

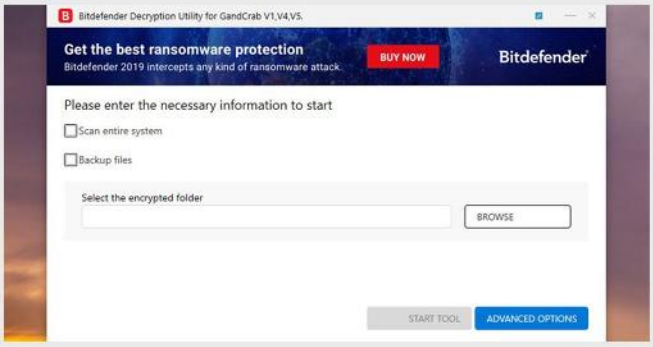
GandCrab یکی از فعال‌ترین باج‌افزارها تا به امروز بوده است که اولین بار در ژانویه سال 2018 بیش از 1.5 میلیون کامپیوتر را آلوده نمود.

با ابزار جدید رمزگشایی باج‌افزار GandCrab که توسط شرکت BitDefender ارائه شده است، فایل‌هایی که با آخرین نسخه‌ی این باج‌افزار یعنی از نسخه 5.0 تا 5.2 و همچنین نسخه‌های قدیمی‌تر آن رمزنگاری شده‌اند، قابل بازگشایی هستند.

شرکت BitDefender در بخشی از یک پروژه به نام "No More Ransom" با همکاری FBI، Europol، پلیس لندن و چندین سازمان اجراکننده قانون در سراسر جهان، به کاربران آسیب‌دیده از این باج‌افزار کمک می‌کنند.

این شرکت (BitDefender) طی ماه‌های اخیر ابزارهای حذف برخی از نسخه‌های قدیمی باج‌افزار GandCrab را منتشر کرده است که به حدود 30،000 قربانی این باج‌افزار کمک می‌کند تا بتوانند داده‌های خود را به صورت رایگان بازیابی کنند. در نتیجه‌ی این اقدام، از پرداخت حدود 50 میلیون دلار باج جلوگیری شده است.

سازندگان باج‌افزار GandCrab اخیراً توقف فعالیت باج‌افزار Ransomware-as-a-Service (RaaS) خود را اعلام نموده‌اند، باج‌افزاری که به موجب آن مهاجمان توانستند بیش از 2 میلیارد دلار از قربانیان باج دریافت کنند.



به گفته محققان شرکت BitDefender: "اگرچه این رقم خیلی اغراق‌آمیز است، اما عملکرد باج‌افزار GandCrab به اندازه کافی برای صاحبان آن کسب درامد کرده است." این توقف عملیات با حذف تمام کلیدها همراه خواهد بود و قربانیان حتی در صورت پرداخت باج هم دیگر قادر به پس گرفتن داده‌های خود نخواهند بود.

طبق گزارش Europol، باج‌افزار GandCrab که از ژانویه سال 2018 شروع به فعالیت کرد، به سرعت به ابزاری برای مهاجمان به عنوان یک باج‌افزار تبدیل شد و تا اواسط سال 2018، 50 درصد از سهم تمام بازار باج‌افزارها را به خود اختصاص داد.

Europol همچنین افزود: "به عنوان نمونه، توزیع‌کنندگان می‌توانند باج‌افزار ransomware-as-a-service را در بازارهای سیاه وب خریداری کرده و آن را در بین قربانیان خود منتشر کنند. در عوض، آن‌ها 40 درصد از سود خود را به توسعه‌دهندگان باج‌افزار پرداخت می‌کنند و 60 درصد آن را برای خود نگه می‌دارند."

بیشتر ویروس‌های کامپیوتری به دلیل عدم رعایت اقدامات ساده امنیتی وارد سیستم می‌شوند، با رعایت چند نکته ساده می‌توان از کامپیوتر خود در برابر حملات باج‌افزار محافظت کرد.

برخی از این اقدامات عبارتند از:

- مراقب ایمیل‌های فیشینگ باشید، هرگز بر روی لینک‌های موجود در ایمیل‌ها کلیک نکنید مگر اینکه منبع آن را تأیید کنید.
- به طور منظم نسخه پشتیبان تهیه کنید، برای اینکه همیشه یک نسخه پشتیبان از کلیه فایل‌ها و اسناد خود داشته باشید، یک روال و برنامه منظم برای پشتیبان‌گیری در نظر بگیرید و نسخه‌های پشتیبان را به یک حافظه خارجی که همیشه به کامپیوترتان متصل نباشد انتقال دهید.

• نرم‌افزار آنتی‌ویروس خود را به روز نگه دارید، همیشه سیستم و نرم‌افزار آنتی‌ویروس خود را به روز نگه دارید تا در برابر آخرین تهدیدات از سیستم خود محافظت کنید.

منبع خبر :

https://thehackernews.com/2019/06/gandcrab-ransomware-decryption-tool.html?m=1

Scan Link

افشاء نقص ۲۰ ساله‌ی وصله نشده در ویندوز توسط گوگل!

گردآورنده: سهیلا مرادی

یکی از محققان امنیتی گوگل، یک نقص 20 ساله‌ی وصله نشده را که دارای شدت آسیب‌پذیری بالا بوده و تمامی نسخه‌های ویندوز _از ویندوز XP تا آخرین نسخه ویندوز 10_ را تحت تأثیر قرار می‌دهد فاش نمود.

این آسیب‌پذیری در نحوه ارتباط سرورها و کلاینت‌های MSCTF وجود دارد، که حتی به برنامه‌های با حق دسترسی پایین و یا برنامه‌های تحت سندباکس اجازه می‌دهد که در برنامه‌های دارای حق دسترسی بالاتر داده‌ها را بخوانند و بنویسند.

MSCTF یک ماژول در Text Services Framework (TSF) سیستم‌عامل ویندوز است، که مواردی مانند روش‌های ورودی، طرح صفحه کلید، پردازش متن و تشخیص گفتار را مدیریت می‌کند.

به طور خلاصه، زمانی که شما می‌خواهید به سیستم ویندوز خود وارد شوید، این ماژول سرویس مانیتور CTF را استارت می‌کند، که به عنوان یک مرجع اصلی برای مدیریت ارتباطات بین کلیه کلاینت‌ها عمل کرده، و در واقع ویندوز برای هر پردازش همین session را اجرا می‌کند.

احتمالاً متوجه سرویس ctfmon در نوار وظیفه [1] شده‌اید، این سرویس مسئولیت اطلاع‌رسانی [2] را در شرایط تغییر طرح کیبورد و یا تغییر روش‌های ورودی به عهده دارد. هسته‌ی سیستم‌عامل برنامه‌ها را وادار می‌کند که به محض اجرا به سرویس ctfmon متصل شده و سپس به تبادل پیام با سایر کلاینت‌ها و دریافت اطلاعیه از سایر سرویس‌ها بپردازند.

این محقق امنیتی به نام Tavis Ormandy، از تیم Google Project Zero، دریافت که هیچ کنترل دسترسی و یا احراز هویتی برای این تعامل صورت نمی‌گیرد، و لذا هر کاربری، هر برنامه‌ای و حتی هر فرآیند تحت سندباکسی می‌تواند اقدامات زیر را انجام دهد:

- اتصال به نشست CTF
- خواندن و نوشتن متن هر پنجره از هر session دیگر، جعل شناسه thread، شناسه فرآیند و HWND
- جا زدن خود به عنوان سرویس CTF و فریب سایر برنامه‌ها (حتی آن‌ها که به سطح دسترسی بالایی نیاز دارند) برای اتصال به آن‌ها
- گریز از سندباکس‌ها و ارتقاء سطح دسترسی

این محقق در پست وبلاگی که امروز منتشر شد نوشت: "در CTF هیچ کنترل دسترسی وجود ندارد، بنابراین شما می‌توانید به نشست فعال کاربر دیگر متصل شوید و به هر برنامه‌ای که می‌خواهید دسترسی پیدا کنید، و یا منظر بمانید تا ادمینِ سیستم وارد شود و سپس نشست وی را سرقت نمایید."

معلوم است که نزدیک به 20 سال دسترسی به نشست‌ها فراهم شده و مرزهای امنیتی NT نقض شده‌اند و در تمام این مدت کسی متوجه این باگ نشده است.

در صورت اکسپلویت این آسیب‌پذیری، ضعف موجود در پروتکل CTF به مهاجمان اجازه می‌دهد تا به راحتی User Interface Privilege Isolation (UIPI) را دور بزنند و حتی به یک فرآیند غیرمجاز اجازه می‌دهد اقدامات زیر را انجام دهد:

- خواندن متن‌های حساس از سایر برنامه‌ها، شامل گذرواژه‌های خارج از دیالوگ باکس‌ها
- به دست آوردن حق دسترسی SYSTEM
- به دست گرفتن کنترل UAC
- ارسال دستور به کنسول ادمین

[1] Task Manager

[2] notifying

- گریز از سندباکس‌های IL/AppContainer با ارسال ورودی به پنجره‌های غیرسندباکس

Ormandy همچنین یک ویدئوی اثبات مفهومی منتشر نموده است که نشان می‌دهد چگونه این باگ برای به دست آوردن حق دسترسی SYSTEM در ویندوز 10 مورد اکسپلویت قرار می‌گیرد.

علاوه بر این، به گفته این محقق، پروتکل CTF دارای نقص‌های خرابی حافظه‌ی بسیاری نیز می‌باشد که می‌تواند در پیکربندی‌های پیش‌فرض مورد سوءاستفاده قرار گیرد.

این محقق همچنین یک ابزار اُپن‌سورس به نام "CTF Exploration Tool" در گیت‌هاب منتشر نموده که به منظور کشف باگ‌های امنیتی موجود در پروتکل CTF ویندوز توسعه داده شده است.

Ormandy این نقص امنیتی و یافته‌های خود را در اواسط ماه می سال جاری به مایکروسافت گزارش نمود، و پس از آنکه مایکروسافت پس از گذشت مهلت 90 روزه در صدد رفع مشکل برنیامد تصمیم گرفت آن را به صورت عمومی فاش نماید.

منبع خبر :

https://thehackernews.com/2019/08/ctfmon-windows-vulnerabilities.html

Scan Link

کشف نقص امنیتی در واتس‌اپ، که اجازه‌ی دستکاری مکالمات را به مهاجمان می‌دهد!

گردآورنده: صبا آزرمی ویراستار: سیده مرضیه حسینی

کارشناسان امنیتی CheckPoint مجموعه‌ای از آسیب‌پذیری‌های واتس‌اپ را کشف نموده‌اند که مهاجمان را قادر می‌سازد مکالمات کاربران را دستکاری کنند!

این تیم امنیتی متشکل از محققانی به نام‌های Dikla Barda, Roman Zaikin و Oded Vanunu می‌باشد. این تیم، سه حمله یافته‌اند که از آسیب‌پذیری‌های موجود در واتس‌اپ برای دستکاری مکالمات کاربران استفاده می‌کنند. این نقص به مهاجمان اجازه می‌دهد تا پیام‌های کاربران را در مکالمات خصوصی و گروهی، دریافت کرده و آن‌ها را دستکاری کنند. کارشناسان در مورد سوءاستفاده از این روش‌های حمله برای گسترش اخبار نادرست از طریق منابع معتبر هشدار می‌دهند.

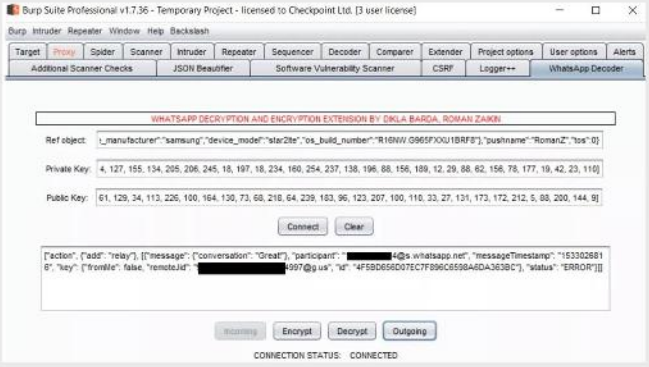
Vanunu در کنفرانس Black Hat که در لاس وگاس برگزار گردید، بیان کرد که این آسیب‌پذیری‌ها در سال 2018 افشا شده، و از آن زمان تا کنون مورد سوءاستفاده قرار گرفته‌اند.

اخیراً پژوهشگاه Check Point از آسیب‌پذیری‌های جدیدی در پیام‌رسان محبوب واتس‌اپ پرده برداشت که با استفاده از این آسیب‌پذیری‌ها می‌توان پیام‌های ارسال شده در مکالمات خصوصی و گروهی را دستکاری کرد و بدین ترتیب به مهاجمان این امکان را می‌دهد تا اخبار و اطلاعات نادرستی را از طریق منابع معتبر و قابل اعتماد منتشر کنند.

روزنامه‌ی Financial Times به نقل از فیسبوک گزارش داد که این آسیب‌پذیری‌ها ناشی از محدودیت‌هایی است که به دلیل ساختار و معماری آنها قابل حل نیستند.

در واتس‌اپ پیام‌های متنی، عکس، تماس، فیلم و یا هر نوع محتوای دیگری که می‌توان در مکالمات ارسال نمود رمزگذاری می‌شود و تنها گیرنده قادر به رمزگشایی آن می‌باشد.

کارشناسان مهندسی معکوس با استفاده از الگوریتم به‌کار گرفته شده جهت رمزگشایی داده‌ها در واتس‌اپ، دریافتند که این نرم‌افزار محبوب از پروتکل "protobuf2" استفاده می‌کند. آن‌ها توانستند داده‌های protobuf2 را به JSON تبدیل کرده و محتوای واقعی ارسال شده را مشاهده نمایند، کارشناسان در تلاشند این داده‌ها را جهت اهداف آزمایشی دستکاری کنند.



این کارشناسان با استفاده از نرم‌افزار Burp Suit، سه روش را برای دستکاری مکالمات، به کار گرفته و این پیام‌رسان محبوب را مورد حمله قرار دادند. آن‌ها این روش‌ها را در کنفرانس Black Hat ارائه نمودند.

سه روش به کار برده شده برای اجرای حمله با استفاده از این آسیب‌پذیری، شامل تمام ترفندهای مهندسی اجتماعی جهت فریب کاربران است، این روش‌ها عبارتند از:

1. استفاده از ویژگی"نقل قول"در مکالمات گروهی برای تغییر هویت فرستنده، حتی اگر آن شخص عضو این گروه نباشد!

2. مهاجم می‌تواند متن پیام ارسالی بین فرستنده و گیرنده را دریافت نموده، آن را تغییر دهد و برای گیرنده ارسال نماید، یا به عبارت دیگر و به اصطلاح، حرف در دهان فرستنده بگذارد!

3. مهاجم می‌تواند در گروه، یک پیام خصوصی را فقط برای یکی دیگر از اعضای گروه ارسال کند، در حالی که این پیام از نظر شخص قربانی یک پیام عمومی است ولی آن پیام فعلاً در گروه منتشر نشده و فقط شخص قربانی آن را می‌بیند و درست زمانی که شخص قربانی پاسخ آن پیام را می‌دهد، متنِ پیامِ خصوصی برای همه‌ی افراد گروه قابل مشاهده است!

در حال حاضر، به نظر می‌رسد که تنها مسئله‌ی تبدیل شدن پیام خصوصی به پیام عمومی (مورد سوم) توسط فیس‌بوک برطرف شده است اما دو مشکل دیگر هنوز به قوت خود باقی مانده‌اند.

آقای Vanunu در این رابطه به BBC گفت: "این آسیب‌پذیری به مهاجمان اجازه می‌دهد تا اخبار جعلی و تقلبی را منتشر کرده و از این طریق به طور کامل مکالمات یک شخص را تغییر دهند."

محققان Check Point به دلیل وسعت این آسیب‌پذیری تصمیم به افشای آن گرفتند.

شایان ذکر است که 30% از جمعیت جهان (بیش از 5/1 میلیارد نفر) از نرم‌افزار واتس‌اپ استفاده می‌کنند به همین دلیل نمی‌توان به سادگی از این آسیب‌پذیری چشم‌پوشی کرد.

منبع خبر :

https://securityaffairs.co/wordpress/89624/hacking/whatsapp-flaws-2.html

Scan Link

هک کامپیوتر مک به کمک کابل جدید O.MG

گردآورنده: صبا آزرمی ویراستار: سهیلا مرادی

گوشی‌ها و کامپیوترهای اپل، در مقایسه با همتایان خود، از لحاظ امنیت از شهرت بیشتری برخوردار هستند، اما نمی‌توان گفت که عاری از خطا می‌باشند. به عنوان مثال، کابل لایتینگ [3] آیفون، جهت دسترسی هکر به رایانه قربانی از راه دور، قابل دستکاری است!

اولین بار در اوایل سال جاری در خصوص کابل‌های O.MG خبرهایی منتشر شد. محقق امنیتی و طراح این کابل به نام Mike Grover، معروف به MG، مدعی شده بود که توسط این کابل می‌توان از راه دور کنترل گوشی‌های هوشمند را به دست گرفت. وی در کنفرانس سالانه‌ی هک Def Con اطلاعات بیشتری از قابلیت‌های این کابل ارائه نمود.

این محقق اظهار داشت: "کابل O.MG در ظاهر شبیه یک کابل معمولی بوده (در واقع از لحاظ ظاهری بسیار شبیه به کابل لایتنیگ است) و مانند آن عمل می‌کند و تا زمانی که مهاجم کنترل کابل را به صورت وایرلس (بی‌سیم) در دست نگیرد، کامپیوتر متوجه این تفاوت نمی‌شود."

از آن‌جا که تشخیص این کابل از سایر کابل‌های مجاز شرکت اپل تا حدی غیرممکن است، به راحتی می‌توان نسخه‌ی دستکاری شده‌ی کابل را با نسخه‌ی اصلی آن، یعنی کابل لایتنیگ، جابجا کرد و یا آن را به یک قربانی هدیه داد!!!

این کابل حاوی یک تراشه‌ی کوچک است که عمل هک را امکان‌پذیر می‌سازد. عملکرد این کابل در ابتدا همان‌گونه است که انتظار می‌رود، اما هکرها به محض وصل شدن به مک می‌توانند از طریق یک هات‌اسپات وای‌فای به کامپیوتر دسترسی پیدا کنند. در صورت نیاز

[3] Lightning cable

می‌توان بعد از عملیات هک، تراشه را از راه دور از بین برد تا هیچ ردی از اقدامات خرابکارانه بر جای نماند.

مهاجمان می‌توانند با استفاده از این کابل کامپیوتر مک را از فاصله 300 متری هک کنند. و البته این مسافت را می‌توان به کمک یک آنتن افزایش داد.

MG در مصاحبه‌ای توضیح داد که: "کابل را می‌توان به گونه‌ای تنظیم نمود که به عنوان یک کلاینت در یك شبکه وایرلس نزدیک عمل کند و اگر آن شبکه به اینترنت متصل باشد، این فاصله نامحدود می‌شود."

MG قصد دارد کابل‌های O.MG را از طریق کمپانی Hak5 به فروش برساند. این کابل و ابزارهای مربوط به آن در حال حاضر برای مشتریان رویداد Def Con به قیمت 200 دلار قابل خریداری است.

منبع خبر :

https://www.techspot.com/news/81392-modified-200-iphone-lightning-cable-hackers-remotely-hijack.html

Scan Link

دستکاری فایلهای رسانه‌ای دریافت شده از واتس‌اپ و تلگرام توسط هکرها

گردآورنده: علیرضا عبدی ویراستار: سیده مرضیه حسینی

اگر بر این باورید که فایل‌های رسانه‌ایِ دریافتی از برنامه‌های پیام‌رسان کاملاً ایمن و به صورت رمزنگاری شده هستند و امکان دستکاری و تغییر توسط مهاجمان در آن‌ها وجود ندارد، باید بگوییم که در اشتباهید!

محققان امنیتی شرکت Symantec، چندین سناریوی جالب را برای حمله به برنامه‌های واتس‌اپ و تلگرام در سیستم‌عامل اندروید منتشر کردند که مهاجمان را قادر می‌سازد تا اخبار جعلی را منتشر کرده و نیز با ارسال وجوهات پرداختی کاربران به حساب‌های جعلی خود از آنها کلاهبرداری کنند.

در این حمله که به نام "Media File Jacking " شناخته می‌شود، هر برنامه‌ی نصب شده بر روی دستگاهِ کاربر می‌تواند به فایل‌های ذخیره شده در حافظه خارجی مانند فایل‌های ذخیره شده توسط سایر برنامه‌های نصب شده در همان دستگاه، دسترسی پیدا کرده و آنها را بازنویسی کند.

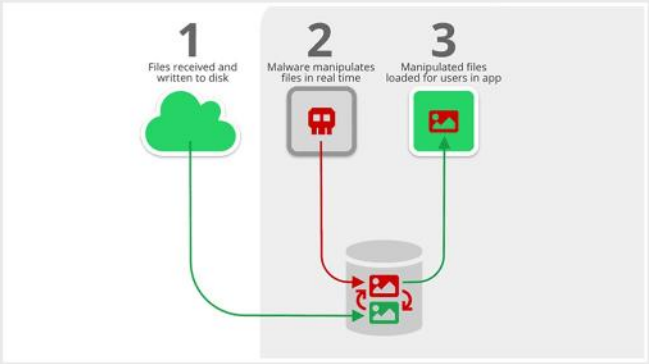
برنامه‌های واتس‌اپ و تلگرام این امکان را به کاربران می‌دهند که فایل‌های دریافتی خود را به دلخواه در حافظه خارجی و یا داخلی دستگاه ذخیره کنند.

برنامه واتس‌اپ اندروید به صورت پیش‌فرض فایل‌های رسانه‌ای را در حافظه خارجی ذخیره می‌کند، در حالی که تلگرام اندروید از حافظه داخلی برای ذخیره کردن فایل‌های کاربران که برای هیچ برنامه کاربردی دیگری قابل دسترسی نیست، استفاده می‌کند.

بسیاری از کاربران تلگرام هنگام به اشتراک گذاشتن فایل‌های رسانه‌ای با استفاده از برنامه‌های ارتباطی دیگر مانند جیمیل، فیس‌بوک یا واتس‌اپ، این تنظیمات را با استفاده از گزینه " ذخیره در گالری " به صورت دستی تغییر می‌دهند.

لازم به ذکر است که این حمله تنها به واتس‌اپ و تلگرام محدود نمی‌شود و بر کارکرد و حریم خصوصی بسیاری از برنامه‌های دیگر اندروید نیز تأثیر می‌گذارد.

حمله "Media File Jacking" چگونه کار می‌کند؟



درست مانند حملات man-in-the-disk، یک برنامه مخرب نصب شده بر روی دستگاه گیرنده می‌تواند فایل‌های رسانه‌ای مانند تصاویر شخصی، مستندات و یا ویدئوهای ارسال شده بین کاربران از طریق حافظه خارجی دستگاه را دریافت و دستکاری کند.

محققان می‌گویند: " این واقعیت که فایل‌ها در داخل حافظه خارجی دستگاه ذخیره شده و بدون مکانیزم‌های امنیتی مناسب بارگذاری می‌شوند، به سایر برنامه‌ها این امکان را می‌دهد تا امنیت فایل‌های رسانه‌ای را به خطر اندازند."

مهاجمان می‌توانند از اعتمادی که بین فرستنده و گیرنده هنگام استفاده از این

برنامه‌هـــا وجـــود دارد برای منافع شـــخصی و برجای گذاشـــتن آثار مخرب استفاده کنند.

محققان چهار ســـناریوی این حمله را تشـــریح کردند، جایی کـــه یک بدافزار می‌توانـــد فایل‌هـــای دریافتی را تجزیـــه و تحلیل کند و منجر بـــه موارد زیر شود:

1. دستکاری تصویر (Image manipulation)

در این ســـناریو، یـــک برنامه به ظاهر ســـالم، اما در واقع مخرب که توســـط کاربر دانلود شـــده اســـت می‌تواند در پس‌زمینـــه اجرا شـــود و در حالی‌که قربانـــی از برنامه واتس‌اپ اســـتفاده می‌کنـــد بدون اطـــلاع او یک حمله Media File Jacking را اجرا کرده و تصاویر شخصی وی را دستکاری کند.

2. دستکاری در پرداخت (Payment manipulation)

در این سناریو که محققان آن را یکی از زیان‌بارترین حملات Media File Jacking می‌دانند، یک مهاجم می‌تواند فاکتور فرســـتاده شـــده توســـط فروشنده به مشـــتریان را دســـتکاری کرده و آن‌ها را بـــه پرداخت وجه به یک حســـاب کنترل شده توسط خود هدایت کند.

3. کلاهبرداری از پیام صوتی (Audio message spoofing)

در این ســـناریو از حملـــه، مهاجمان می‌تواننـــد از اعتماد بیـــن کارمندان در یک ســـازمان سوءاســـتفاده کننـــد. مهاجمان از بازســـازی صـــدا از طریق تکنولـــوژی deep learning بـــرای تغییر پیام صوتی اصلـــی در جهت منافع شخصی خود و یا عملیات خرابکارانه استفاده کنند.

4. انتشار اخبار جعلی

در تلگـــرام، مدیران از " کانال‌ها " برای انتشـــار پیام به تعـــداد نامحدودی از مشـــترکینی که محتوای منتشر شـــده را دریافت می‌کنند اســـتفاده می‌کنند. از طریـــق حمـــلات Media File Jacking، یـــک مهاجم می‌توانـــد فایل‌هـــای رســـانه‌ای که در یک کانـــال قابل اعتماد منتشـــر می‌شـــوند را جهت پخش اخبار جعلی تغییر دهد.

چگونـــه می‌تـــوان از ربـــوده شـــدن فایل‌هـــای اندروید توســـط مهاجمان جلوگیری کرد؟

شـــرکت Symantec پیش از این به تلگرام، فیس بـــوک و واتس‌اپ در مورد حملات Media File Jacking اطلاع داده بود، اما معتقد اســـت که این مسئله توسط گوگل با بروزرسانی بعدی اندروید Q برطرف خواهد شد.

اندروید Q شـــامل یک ویژگی امنیتی جدید به نام Scoped Storage اســـت کـــه نحوه دسترســـی برنامه‌ها بـــه فایل‌هـــای موجود در حافظـــه خارجی دستگاه را تغییر می‌دهد.

Scoped Storage بـــه هر برنامه یک ســـندباکس ذخیره‌ســـازی مجزا در حافظه خارجی دســـتگاه اختصـــاص می‌دهد که در آن هیـــچ برنامه کاربردی دیگـــری نمی‌تواند به طور مســـتقیم به اطلاعات ذخیره‌شـــده توســـط دیگر برنامه‌ها روی دستگاه شما دسترسی داشته باشد.

تـــا آن زمان، کاربـــران می‌تواننـــد با غیرفعال کـــردن ویژگی ذخیره‌ســـازی فایل‌های رســـانه‌ای در حافظه خارجی دســـتگاه، خطر بـــروز چنین حملاتی را کاهـــش دهند. برای انجـــام این کار، کاربـــران اندرویـــد می‌توانند تنظیمات زیر را در دستگاه خود اعمال کنند:

- در واتس‌اپ: Settings <-- Chats <-- گزینه 'Media Visibility' را غیرفعال کنید.
- در تلگـــرام: Settings <-- Chats Settings <-- گزینه 'Save to Gallery' را غیرفعال کنید.

منبع خبر :

https://thehackernews.com/2019/07/media-files-whatsapp-telegram.html

Scan Link

هشدار برای دارندگان گوشی‌های هوشمند!
۴۰٪ برنامه‌های اندروید و iOS در مقابل هک آسیب‌پذیر هستند

گردآورنده: سهیلا مرادی

مســـلماً همه‌ی ما دوســـت داریم برای گوشـــی هوشـــمند خود برنامه‌های جدیـــد نصـــب کنیـــم و از قابلیت‌هـــای متنوع آن‌هـــا بهره‌منـــد گردیم، مخصوصـــاً زمانـــی کـــه برنامـــه‌ای ماننـــد FaceApp، یـــا یـــک

بازی مهیج خیلی مورد توجه کاربران قرار می‌گیرد و دوستان و اطرافیان ما از آن استفاده می‌کنند.

به نظر می‌رشد مشکلی در این میان وجود نداشته باشد، اما آیا تمام برنامه‌ها ایمن و سالم هستند؟ مخصوصاً زمانی که پای امنیت داده‌های شخصی شما در میان باشد؟

تلفن‌های همراه ما از هر چیزی در جهان، حتی از الماس گرانبهاتر هستند، نه به خاطر قیمت بالایی که دارند، بلکه به دلیل داده‌های ارزشمندی که در آن‌ها وجود دارد.

گوشی شما چه اندروید باشد چه iOS، دانلود برنامه در آن درست مانند فراخواندن آسیب‌پذیری‌هاست.

بله کاملاً درست شنیدید!

برنامه‌هایی که ما استفاده می‌کنیم خیلی بیشتر از آنچه که تصور می‌کنیم خطرناک هستند. بیش از یک سوم برنامه‌های اندروید و iOS دارای آسیب‌پذیری‌های خطرناک بوده و احتمالاً تعدادی از آن‌ها داده‌های شخصی ما را در معرض خطر افشاء قرار می‌دهند.

اگر این اطلاعات تنها اطلاعات مربوط به پروفایل ما باشد مشکلی نیست، اما اگر این برنامه‌ها داده‌های شخصی ما _مانند عکس‌ها و فیلم‌های شخصی_ را افشاء کنند دیگر به سادگی نمی‌توان از کنار آن‌ها عبور کرد.

فکر نمی‌کنم هیچ‌کس دوست داشته باشد اطلاعات شخصی خود را با دیگران به اشتراک بگذارد.

بیایید بررسی مختصری در این زمینه داشته باشیم:

آخرین آسیب‌پذیری‌های موجود در برنامه‌های تلفن همراه

قبل از آنکه اتفاقات رخ داده در این زمینه را برایتان تعریف کنم، اجازه دهید اصولی را در خصوص برنامه‌های موبایل مطرح کنم.

سال گذشته، بیش از 205 میلیارد برنامه تلفن همراه دانلود شدند، از آنجا که ما حدود 57% زمان خود را صرف کار با تلفن همراه و تبلت و غیره می‌کنیم، پیش‌بینی می‌شود این تعداد تا سال 2022 به بیش از 250 میلیارد برسد.

آیا می‌توانید آنچه را که دیروز در PDA خود مرور کردید به خاطر آورید؟

این برنامه‌ها می‌توانند اپلیکیشن‌های پیام‌رسان، بانکداری آنلاین، مدیریت حساب موبایل، عملیات تجاری، یا حساب‌های کاربری مربوط به رسانه‌های اجتماعی باشند.

به گفته‌ی محققی از شرکت Juniper، تعداد کاربرانی که از برنامه‌های بانکی استفاده می‌کنند به دو میلیارد رسیده‌اند_ حدود 40% از جمعیت بزرگسال جهان.

ما می‌دانیم که چگونه توسعه‌دهندگان با زحمت به طراحی یک نرم‌افزار توجه می‌کنند تا یک برنامه‌ی خوب را در اختیار ما قرار دهند، ما نیز با خوشحالی برنامه را نصب کرده و اطلاعات شخصی خود را در اختیار برنامه قرار می‌دهیم، اما به ندرت به پیامدهای امنیتی آن فکر می‌کنیم.

کارشناسان امنیتی مرتباً برنامه‌های مختلف موبایل را مورد تجزیه و تحلیل قرار می‌دهند (معمولاً پرکاربردترین برنامه‌ها)، در اینجا به برخی از آخرین یافته‌های ارزیابی امنیتی محققان در برنامه‌های اندروید و iOS اشاره می‌کنیم.

طبق یافته‌ها، 38 درصد از برنامه‌های iOS و 43 درصد از برنامه‌های اندروید دارای آسیب‌پذیری‌های با شدت High هستند.

در اکثر موارد، ضعف در مکانیزم‌های امنیتی موجب ایجاد آسیب‌پذیری می‌گردند (74% در برنامه‌های iOS ، 54% در برنامه‌های اندروید و 42% در مؤلفه‌های سمت سرور)، مانند آسیب‌پذیری‌هایی که در طراحی، رفع باگ و یا در مرحله کدگذاری وجود دارند.

مهم‌ترین مسئله در اینجا، ذخیره ناامن داده‌هاست _که در 76 درصد از اپلیکیشن‌های موبایل یافت شده است. اطلاعات مالی، گذرواژه‌ها، داده‌های شخصی و مکاتبات در معرض خطر هستند.

هکرها به ندرت به دسترسی فیزیکی برای دستیابی به داده‌های شما نیاز دارند، حدود 89 درصد از آسیب‌پذیری‌ها توسط بدافزار و از راه دور قابل اکسپلویت هستند.

بسیاری از حملات به خاطر بی توجهی ما رخ می‌دهند. ارتقاء سطح دسترسی یا نرم‌افزار sideloaded به آن‌ها کمک می‌کند تا راه صحیح را برای حمله پیدا کنند.

باید بدانید که هم برای کاربران و هم برای توسعه‌دهندگان تهدیدات سایبری به یک اندازه خطرساز هستند، یعنی برای برقراری امنیت اپلیکیشن‌های iOS و اندروید، حفاظت سمت سرور و سمت کلاینت هر دو لازم است.

بنابراین برای جلوگیری از حملات چه کاری می‌توان انجام داد؟ چگونه می‌توان هر دو سمت (کلاینت و سرور) را محافظت نمود؟

باید بگوییم که این خطرات با افزایش آگاهی، آموزش و اقدامات پیشگیرانه کاهش می‌یابد.

توصیه‌هایی جهت جلوگیری از حملات سایبری مبتنی بر اپلیکیشن، برای اندروید و iOS

توصیه برای توسعه‌دهندگان اندروید

• از LocalBroadcastManager برای ارسال و دریافت پیام‌ها استفاده کنید.

• اگر برنامه داده‌های حساسی مانند اطلاعات مالی را دریافت می‌کند یا یک صفحه کلید سفارشی را پیاده‌سازی می‌کند، اطمینان حاصل کنید که برنامه به اندازه کافی ایمن باشد تا از حملاتی که صفحه کلید سیستم را دستکاری می‌کنند جلوگیری شود.

• غیرفعال نمودن قابلیت پشتیبان‌گیری برنامه، با قرار دادن مقدار false برای "android:allowBackup"

توصیه برای توسعه‌دهندگان iOS

• اگر برای تعامل بین مؤلفه‌ها باید از لینک استفاده کنید، به سمت لینک‌های جهانی بروید.

• به منظور غیرفعال نمودن صفحه کلیدهای شخص ثالث در داخل برنامه متد "shouldAllowExtensionPointIdentifier" را در UIApplicationDelegate برنامه پیاده کنید.

اقداماتی برای هر دو پلتفرم (اندروید و iOS)

• دستگاه‌های مدرن از بیومرتیک (Touch یا Face ID) در برنامه‌ها استفاده می‌کنند. در این موارد پین کد در دستگاه ذخیره می‌شود. حافظه داخلی (داده‌های حساس) فقط باید در دایرکتوری‌های خاص و با رمزگذاری وجود داشته باشند. iOS دارای Keychain و اندروید دارای Keystore می‌باشد.

• از یک تصویر پس‌زمینه خاص برای پوشش داده‌های حساس روی صفحه استفاده کنید.

• TRACE با استفاده از فلگ httpOnly می‌تواند برای دور زدن محافظت کوکی مورد استفاده قرار گرفته و مدیریت درخواست‌های TRACE را غیرفعال نماید.

• محدودیت در تلاش برای احراز هویت باید هم بر روی سرور اعمال گردد و هم سمت کلاینت.

• داده‌های ورودی توسط کاربر را بر روی سرور فیلتر نمایید. برای مقابله با کاراکترهای ویژه از کدگذاری HTML استفاده نمایید.

• مدت زمان Session باید محدود باشد. Session ID باید هم از سمت سرور و هم از سمت کلاینت پاک شود. سرور باید برای هر بار احراز هویت یک Session جدید ایجاد نماید.

• کارشناسان توصیه می‌کنند که برای برقراری ارتباط امن میان سرور و کلاینت از گواهینامه استفاده شود. این گواهینامه مستقیماً در کد برنامه قرار داده شده و می‌تواند مانع حملات Man-In-The-Middle شود.

توصیه‌هایی برای کاربران

• به فروشگاه‌های برنامه ناشناس اعتماد نکنید. برنامه‌های مشکوک (مانند نسخه‌های کرک شده یا رایگان برنامه‌های پولی) اغلب حاوی کدهای مخرب هستند.

• تلفن همراه خود را برای شارژ به ایستگاه‌های شارژ نامعتبر و یا رایانه‌های شخصی افراد ناشناس متصل نکنید.

• نسخه‌های مدرن سیستم‌عامل‌های موبایل از کاربر برای تأیید اعتبار سؤال می‌کنند. اگر از امنیت سیستمی که می‌خواهید به آن متصل شوید مطمئن نیستید هرگز آن را تأیید نکنید.

• از باز کردن لینک موجود در پیام‌ها و چت‌های افراد ناشناس اجتناب کنید. حتی اگر شخصی را که به شما برنامه‌ای را پیشنهاد می‌دهد می‌شناسید باز هم هوشیارانه عمل کنید.

• سیستم‌عامل و برنامه‌های خود را به محض انتشار بروزرسانی برای آن‌ها، به روز نمایید.

• از ارتقاء سطح دسترسی اجتناب کنید، فراموش نکنید که روت کردن یا jailbreaking نمودن دستگاه مکانیزم‌های امنیتی را غیرفعال نموده و دسترسی به سیستم‌فایل‌های دستگاه را باز می‌کند.

• پین کد شما باید یک عدد تصادفی باشد (یک عبارت نه یک کلمه). از تاریخ تولد، شماره تلفن و یا شماره شناسایی استفاده نکنید. اگر دستگاه شما بیومتریک را پشتیبانی می‌کند (اثرانگشت، تشخیص چهره یا تشخیص صدا) بهتر است از آن استفاده کنید.

• موقع نصب برنامه‌ها هوشیار باشید، اگر تقاضای دسترسی به چیزی دارند که به نظر شما غیرمنطقی است هرگز این دسترسی‌ها را اعطا نکنید.

یادتان باشد هکرها عاشق هدف قرار دادن پلتفرم‌های جدید هستند، و

اطلاعات مالی هستند، فعلاً در مرکز توجه قرار دارند.

نتایج این مطالعه نشان می‌دهد که توسعه‌دهندگان برنامه‌های تلفن همراه، اغلب از امنیت و ذخیره امن اطلاعات غافل هستند و در حال حاضر مسئله اصلی همین است.

از طرف دیگر خودِ کاربران نیز با توسعه قابلیت‌های گوشی، باز کردن لینک‌های مشکوک، غیرفعال کردن قابلیت‌های محافظتی و دانلود برنامه از منابع نامعتبر، ناخواسته به تسخیر شدن گوشی خود کمک می‌کنند.

منبع خبر :

https://gbhackers.com/ios-android-apps-vulnerable/

Scan Link

اخبار کوتاه

کلاهبرداری در محیط واتس‌اپ در قالب "اینترنت رایگان"

در گذشته مجرمان سایبری به منظور کلاهبرداری از قربانیان خود، ایشان را با وعده جایزه فریب می‌دادند.

در جدیدترین نوع این کلاهبرداری‌ها که در پیام‌رسان واتس‌اپ ظاهر شده به قربانیانش وعده"اینترنت رایگان" به مناسبت جشن سالگرد این شرکت را می‌دهد.

چگونه این نوع از کلاهبرداری را تشخیص دهیم؟

اولین قاعده از دید شرکت ESET این است که وب‌سایت شرکت مربوطه را بررسی کنید تا ببینید آیا تبلیغ واقعی یا معتبر باشد.

طی بررسی‌های این شرکت آنتی‌ویروس مشخص شد که شگرد کلاهبرداری "اینترنت رایگان واتس‌اپ" توسط دامنه‌ای اجرا می‌شود که محل بسیاری از کلاهبرداری‌های دیگر در قالب جعل هویت شرکت‌های مشهور می‌باشد.

اگر شخصی روی لینک موجود در این پیام‌های کلاهبردارانه کلیک کند، کاربر را به صفحه‌ایی هدایت می‌کند که از او می‌خواهد به یک سری از سوالات پاسخ و پیشنهاد خود را در مورد برنامه بدهد، سپس از قربانی خواسته می‌شود برای دریافت جایزه حداقل 30 نفر را فرا خواند.

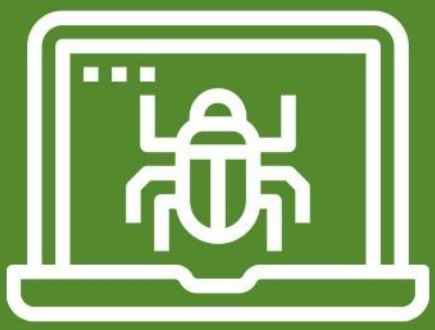
ESET تصریح کرد هدف از این شگرد نصب نرم‌افزارهای مخرب بر روی دستگاه کاربر یا سرقت اطلاعات شخصی کاربران نیست، با این حال نوعی شگرد کلاهبرداری کلیکی با هدف درآمدزایی بر پایه تبلیغات بوده که در نهایت می‌تواند درآمد برای عاملان این شگرد ایجاد کند.

آسیب‌پذیری امنیتی مدیا پلیر محبوب VLC خطری جدی برای میلیون‌ها کاربر

یک آسیب‌پذیری جدی در جدیدترین نسخه مدیا پلیر VLC مشاهده شده که می‌تواند میلیون‌ها کاربر را تحت تأثیر قرار دهد. این نقص باعث فعال شدن «اجرای کد از راه دور» یا RCE، تغییر یا افشای غیر مجاز داده‌ها و فایل‌ها و همچنین ایجاد اختلال کلی در سرویس این مدیا پلیر می‌شود و این یعنی دستگاه کاربران مورد بهره‌برداری هکرها قرار می‌گیرد و آن‌ها می‌توانند بر روی دستگاه کاربر هدف کدهای مخرب اجرا کنند.

بر اساس توئیت ارسال شده از سوی VideoLAN، برنامه VLC در مقابل آسیب‌پذیری اعلام شده ایمن است. مشکل مربوط به کتابخانه ثالثی به نام libebml بوده که بیش از 16 ماه پیش و از زمان نسخه 3.0.3 نرم افزار VLC رفع شده است. به گزارش وبسایت گیزمودو، پایگاه داده National Vulnerability نیز شدت آسیب‌پذیری را از 9.8 (بحرانی) به 5.5 (متوسط) تغییر داده است.

توصیه می‌گردد هر چه سریعتر نرم‌افزار خود را بروزرسانی نمایید.



آسیب پذیری

نقص در آنتی‌ویروس کسپرسکی امکان ردیابی کاربران را فراهم می‌کند!

گردآورنده: سهیلا مرادی

نقص در آنتی‌ویروس کسپرسکی شناسه‌ی اختصاص داده شده به کاربران را برای هر وب‌سایتی که کاربر در طول 4 سال گذشته بازدید نموده است فاش می‌کند.

این آسیب‌پذیری که با شناسه CVE-2019-8286 معرفی شده است، شناسه‌ی اختصاص داده شده به کاربران را برای هر وب‌سایتی که کاربر که در طول 4 سال گذشته بازدید نموده است فاش می‌کند. افشای این شناسه به وب‌سایت‌های بازدید شده و سرویس‌های تجاری شخص ثالث اجازه می‌دهد کاربران آنلاین را ردیابی کنند.

خبر بد این است که کاربران حتی در صورت حذف یا بلاک کردن کوکی‌ها نیز همچنان ممکن است در معرض ردیابی قرار بگیرند.

این آسیب‌پذیری که توسط یک محقق امنیتی به نام Ronald Eikenberg کشف شده است، در ماژول اسکن URL کسپرسکی موسوم به Kaspersky URL Advisor وجود دارد.

راه‌حل امنیتی کسپرسکی بدین صورت است که یک فایل جاوااسکریپت را مستقیماً از راه دور در کد HTML هر وب‌سایتی که توسط کاربران بازدید می‌شود تزریق می‌کند تا امنیت وب‌سایت را بررسی کند (برای بررسی اینکه وب‌سایت در لیست سیاه قرار نداشته باشد، یعنی صفحه متعلق به لیست دامنه‌های فیشینگ نباشد).

این محقق با تجزیه و تحلیل رشته URL جاوااسکریپت، دریافت که این URL حاوی یک رشته‌ی منحصر به فرد برای هر یک از کاربران کسپرسکی است که می‌تواند برای ردیابی کاربران مورد استفاده قرار گیرد. این رشته می‌تواند به راحتی توسط وب‌سایت‌ها، سرویس‌های تبلیغاتی و تحلیلی برای ردیابی کاربران آنلاین مورد استفاده قرار گیرد.

Eikenberg می‌گوید: "اولین بررسی من از اسکریپت کسپرسکی به نام main.js به من نشان داد که، اگر کسپرسکی امنیت یک وب‌سایت را تأیید کند یک آیکون سبزرنگ در نتیجه‌ی جستجوی گوگل به کاربر نشان داده می‌شود. وی می‌گوید: "این می‌تواند پایان تحلیل من باشد، اما یک نکته کوچک وجود داشت، آدرسی که در اسکریپت کسپرسکی لود شده بود حاوی یک رشته‌ی مشکوک بود:

https://gc.kis.v2.scr.kaspersky-labs.com/**9344FDA7-AFDF-4BA0-A915-4D7EEB9A6615**/main.js

قسمتی که در آدرس فوق بولد شده است دارای یک الگوی مشخص می‌باشد. این نوع ساختار با یک اصطلاح جهانی منحصر به فرد به نام Universally Unique Identifier (UUID) شناخته می‌شود.

Eikenberg ، آنتی‌ویروس کسپرسکی را بر روی کامپیوترهای دیگر نیز نصب نمود و متوجه شد که UUID در آدرس منبع هر یک از کامپیوترها با دیگری متفاوت است. وی همچنین دریافت که شناسه‌ها (IDs) ماندگار هستند و با گذشت زمان تغییر نمی‌کنند. این بدان معنی است که شناسه به طور دائمی با هر سیستمی که بر روی آن آنتی‌ویروس کسپرسکی نصب شده است در ارتباط بوده است.

"این ایده‌ی بسیار بدی است. سایر اسکریپت‌هایی که در بستر دامنه‌ی وب‌سایت اجرا می‌شوند، می‌توانند در هر زمانی به کل کد HTML دسترسی پیدا کنند، و این بدان معنی است که می‌توانند ID کسپرسکی را بخوانند. به عبارت دیگر، هر وب‌سایتی می‌تواند ID کسپرسکی را بخواند و از آن برای ردیابی کاربران استفاده کند. اگر همان شناسه جهانی منحصر به فرد برگردد، یا در وب‌سایت دیگری از همان اپراتور ظاهر شود، وب‌سایت‌ها می‌توانند ببینند که از همان کامپیوتر استفاده می‌شود. اگر این فرض درست باشد، کسپرسکی یک مکانیزم ردیابی خطرناک ایجاد نموده است که کوکی‌های به ظاهر قدیمی را ردیابی می‌کند. در این حالت، وب‌سایت‌ها می‌توانند کاربران کسپرسکی را ردیابی کنند، حتی اگر آن‌ها از مرورگر دیگری استفاده نمایند. بدتر از آن این است که ردیابی در حالت پیشرفته‌تر حتی می‌تواند بر حالت ناشناس مرورگر غلبه کند!"

Eikenberg این مشکل را به کسپرسکی گزارش نمود و باگ مذکور در ماه جولای توسط شرکت برطرف شد. اکنون مقدار یکسان (FD126C42-EBFA-4E12-B309-BB3FDD723AC1) به تمام کاربران اختصاص داده می‌شود.

کسپرسکی این باگ امنیتی (CVE-2019-8286) را در محصولات خود، که می‌توانند حریم خصوصی کاربران را با استفاده از این شناسه منحصر به فرد به خطر بیندازند برطرف نموده است.

محصولات تحت تأثیر این آسیب‌پذیری:

Kaspersky Anti-Virus up to 2019

Kaspersky Internet Security up to 2019

Kaspersky Total Security up to 2019

Kaspersky Free Anti-Virus up to 2019

Kaspersky Small Office Security up to 6

کارشناسان خاطرنشان کردند که قابلیت URL Advisor هنوز هم می‌تواند امنیت وب‌سایت را بر روی کامپیوتری که دارای آنتی‌ویروس کسپرسکی می‌باشد بررسی کند، اطلاعاتی که می‌توانند به طُرُق مختلف توسط اسکمرها مورد استفاده قرار گیرند.

به گفته‌ی کارشناسان، این اطلاعات برای مهاجمان بسیار ارزشمند است. چرا که آن‌ها می‌توانند از این اطلاعات برای توزیع بدافزار متناسب با نرم‌افزار حفاظتی سیستم، یا هدایت مرورگر به صفحات جعلی استفاده نمایند.

اگر می‌خواهید قابلیت URL Advisor را غیرفعال نمایید به صورت زیر عمل کنید:

settings--> additional--> network--> un-check traffic processing box

منبع خبر :

https://securityaffairs.co/wordpress/89917/hacking/kaspersky-antivirus-flaw.html

Scan Link

کشف ۴ آسیب‌پذیری Wormable در ریموت دسکتاپ ویندوز

گردآورنده: سهیلا مرادی

اگر از کاربران ویندوز هستید، آب در دست دارید زمین بگذارید و فوراً آخرین وصله‌ی امنیتی منتشر شده برای ویندوز را نصب نمایید!

خبرها حاکی از آن است که سیستم‌عامل ویندوز حاوی 4 آسیب‌پذیری جدید wormable و قابل اجرا از راه دور _مشابه آسیب‌پذیری BlueKeep درRDP که اخیراً وصله شد_ می‌باشد.

هر چهار آسیب‌پذیری مذکور توسط تیم امنیتیِ خودِ مایکروسافت کشف شده، و دارای شناسه‌های CVE-2019-1181، CVE-2019-1182، CVE-2019-1222 و CVE-2019-1226 می‌باشند. این آسیب‌پذیری‌ها می‌توانند توسط مهاجم احراز هویت نشده، از راه دور، اکسپلویت شده و کنترل کامل سیستم قربانی را بدون نیاز به هیچ‌گونه تعاملی با کاربر به مهاجم بسپارند.

دقیقاً همانند نقص BlueKeep در RDP، هر چهار آسیب‌پذیریِ کشف شده wormable هستند، یعنی می‌توانند توسط بدافزارها مورد سوءاستفاده قرار گرفته و خود را به صورت اتوماتیک از سیستمی به سیستم دیگر توزیع نمایند.

گرچه دو آسیب‌پذیری اول تمامی نسخه‌های ویندوز را تحت تأثیر قرار می‌دهند، اما دو آسیب‌پذیری دوم (1222 و 1226) تنها بر Windows 10 و نسخه‌های Windows Server تأثیرگذار خواهند بود.

نکته جالب توجه اینجاست که آسیب‌پذیری‌های مذکور نه Windows Server 2008، Windows Server 2003، Windows XP و نه سرویس RDP را، که مایکروسافت برای خدمات از راه دورِ خود ارائه نموده است، تحت تأثیر قرار نمی‌دهند.

در عوض، این آسیب‌پذیری‌ها در سرویس‌های ریموت دسکتاپ _که قبلاً تحت عنوان Terminal Services شناخته می‌شدند_ وجود داشته و به مهاجم احراز هویت نشده‌ی از راه دور اجازه می‌دهند با ارسال درخواست‌های جعلی از طریق پروتکل RDP در سیستم هدف، آسیب‌پذیری را اکسپلویت نماید.

مایکروسافت اذعان داشت که تاکنون شواهد و مدارکی مبنی بر اکسپلویت شدن این آسیب‌پذیری‌ها گزارش نشده است.

همانطور که گفتیم از آنجا که آسیب‌پذیری‌های مذکور wormable هستند، در صورت عدم بروزرسانی سیستم با آخرین وصله امنیتی منتشر شده، این آسیب‌پذیری‌ها می‌توانند مانند بدافزارهای WannaCry و NotPetya که

در سال 2017 قربانیان زیادی گرفتند و هنوز هم می‌گیرند، به صورت بدافزار توزیع شده و خسارات جبران‌ناپذیری به بار آورند.

بروزرسانی‌های روز سه‌شنبه، 13 آگوست 2019

مایکروسافت در بروزرسانی‌های منتشر شده در تاریخ سه‌شنبه 13 آگوست 2019، علاوه بر 4 آسیب‌پذیری حیاتی ذکر شده، 89 آسیب‌پذیری را نیز به عنوان بخشی از بروزرسانی‌های ماهانه‌ی خود برای نرم‌افزارها در ماه آگوست وصله نمود، که 25 مورد از آن‌ها دارای درجه شدت critical و 64 مورد مهم بودند.

بروزرسانی‌های اخیر (13 آگوست 2109) شامل وصله‌هایی برای نسخه‌های مختلف ویندوز (نسخه‌های مورد حمایت) و سایر محصولات مایکروسافت مانند Internet Explorer، Edge، Office، ChakraCore، Visual Studio سرویس‌های آنلاین و اکتیودایرکتوری می‌باشند.

توجه داشته باشید که تمام آسیب‌پذیری‌های لیست شده در این ماه، بر تمام نسخه‌های windows 10 و تمام نسخه‌های windows Server تأثیر می‌گذارند.

برخی از آسیب‌پذیری‌هایی که دارای درجه شدت بالا هستند می‌توانند منجر به حملات اجرای کد از راه دور شوند، این در حالی است که اکثر آن‌ها موجب ارتقاء سطح دسترسی، حملات منع سرویس، افشای اطلاعات، دور زدن موارد امنیتی، حملات Spoofing، tampering و cross-site scripting می‌شوند.

توصیه امنیتی

اکیداً به کاربران و مدیران سیستم‌ها توصیه می‌شود هر چه سریعتر جدیدترین وصله‌های امنیتی منتشر شده را اعمال نمایند تا از تسخیر سیستم‌های خود توسط هکرها و مجرمان سایبری مصون بمانند.

به منظور اعمال آخرین وصله‌های امنیتی به صورت زیر عمل کنید:

Settings--> Update & Security--> Windows Update--> Check for updates on your computer

منبع خبر :

https://thehackernews.com/2019/08/windows-rdp-wormable-flaws.html

Scan Link

کشف 8 نقص جدید در پروتکل HTTP/2 که وب‌سایت‌ها را در معرض حمله DoS قرار می‌دهد

گردآورنده: سهیلا مرادی

خبرها حاکی از آن است که پیاده‌سازی‌های مختلف HTTP/2 _آخرین نسخه از پروتکل HTTP_ دارای تعدادی آسیب‌پذیری امنیتی بوده که اکثر وب‌سرورهای محبوب مانند Apache، IIS و Nginx را تحت تأثیر قرار می‌دهد.

این پروتکل که در ماه می 2015 به میدان آمد، به منظور بالا بردن سطح امنیت و بهبود سرعت در بارگذاری صفحات وب طراحی شد. امروزه بیش از صدها میلیون وب‌سایت، و به عبارت دیگر حدود 40 درصد از کل سایت‌های اینترنتی از پروتکل HTTP/2 استفاده می‌کنند.

در مجموع 8 آسیب‌پذیری با درجه شدت high در این پروتکل یافت شده است،که 7 مورد از آن‌ها توسط Jonathan Looney از Netflix و یک مورد توسط Piotr Sikora از گوگل، کشف شده‌اند، که به دلیل عملکرد نادرست منابع، هنگام استفاده از ورودی‌های مخرب اجازه می‌دهد کلاینت، صفِ مدیریت کدِ سرور را دچار سربار نماید.

از این آسیب‌پذیری‌ها می‌توان برای اجرای حملات DoS علیه میلیون‌ها سرویس آنلاین و وب‌سایتی که در حال اجرای وب‌سرور با پیاده‌سازی آسیب‌پذیر HTTP/2 هستند استفاده نمود.

سناریوی حمله این‌گونه است که یک کلاینت مخرب از سرور آسیب‌پذیر مورد هدف درخواست می‌کند کاری را انجام دهد که درآن یک پاسخ[۴] تولید شود، اما پس از آن، کلاینت از خواندن پاسخ امتناع ورزیده و موجب می‌گردد که هنگام پردازش درخواست‌ها میزان مصرف حافظه و CPU در سرورِ هدف به حداکثر برسد و سرور از پاسخگویی بازماند.

اکثر آسیب‌پذیری‌هایی که در زیر لیست شده‌اند در لایه انتقال HTTP/2 کار می‌کنند:

[۴] response

CVE-2019-9511 – HTTP/2 "Data Dribble"

CVE-2019-9512 – HTTP/2 "Ping Flood"

CVE-2019-9513 – HTTP/2 "Resource Loop"

CVE-2019-9514 – HTTP/2 "Reset Flood"

CVE-2019-9515 – HTTP/2 "Settings Flood"

CVE-2019-9516 – HTTP/2 "0-Length Headers Leak"

CVE-2017-9517 – HTTP/2 "Internal Data Buffering"

CVE-2019-9518 – HTTP/2 "Request Data/Header Flood"

برخی از این آسیب‌پذیری‌ها به اندازه‌ای کارایی دارند که به تنهایی می‌توانند چندین سرور را نابود کنند. سایر حملات کارایی کمتری دارند، اما این به معنی بی‌خطربودن آن‌ها نیست چرا که همین حملات می‌توانند راه را برای حملات DDoSی که تشخیص و مهار کردن آن‌ها بسیار دشوار است، باز کنند.

البته باید توجه داشت که آسیب‌پذیری‌های مذکور تنها برای ایجاد حملات DoS می‌توانند مورد سوءاستفاده قرار گیرند و به مهاجمان اجازه نمی‌دهند که محرمانگی و یکپارچگی داده‌های موجود در سرورهای آسیب‌پذیر را به خطر بیندازند.

تیم امنیتی Netflix، که با Google و CERT برای افشاء نقص‌های HTTP/2 همکاری نمود، 7 مورد از 8 آسیب‌پذیری را در چندین مورد از پیاده‌سازی‌های این پروتکل در ماه می سال 2019 کشف نموده و آن را به تمامی مسئولین و عاملان دخیل در طراحی این پروتکل گزارش داد.

به گفته تیم امنیتی CERT، بسیاری از عرضه‌کنندگان این پروتکل مانند Nginx، Apache، H2O، Nghttp2، Microsoft (IIS)، Cloudflare، Akamai، Apple (SwiftNIO)، Amazon، Facebook (Proxygen)، Node.js و Envoy proxy در حال حاضر برای آسیب‌پذیری‌های موجود وصله‌های امنیتی مورد نظر را منتشر نموده‌اند.

توصیه می‌گردد به منظور جلوگیری از حملات DoS ناشی از این آسیب‌پذیری‌ها، هر چه سریعتر وصله‌های امنیتی مربوطه را نصب نمایید.

منبع خبر :

https://thehackernews.com/2019/08/http2-dos-vulnerability.html

Scan Link

هک تلفن همراه تنها با پخش یک ویدئو!

گردآورنده: سهیلا مرادی

اگر دستگاه تلفن شما اندرویدی است باید خیلی مراقب باشید!

شما باید هنگام باز کردن فایل‌های ویدئویی خیلی محتاط باشید، خواه این ویدئو را از جایی دانلود کرده باشید یا اینکه کسی برای شما ایمیل کرده باشد.

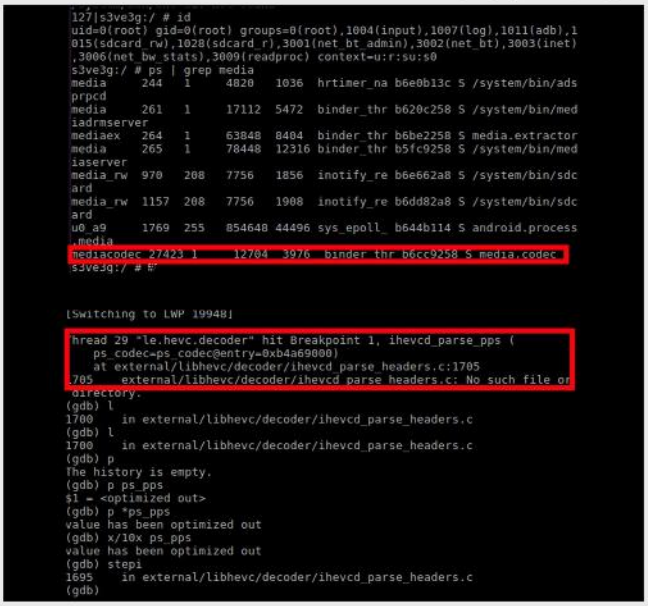
به این دلیل که یک فایل ویدئوی ساختگی می‌تواند تلفن هوشمند شما را تسخیر نماید. متأسفانه خبرها حاکی از آن است که حدود 1 میلیارد دستگاه اندرویدی که دارای نسخه‌های 7.0 تا 0.9 بوده‌اند به دلیل وجود آسیب‌پذیری حیاتی اجرای کد از راه دور تحت تأثیر قرار گرفته‌اند.

این آسیب‌پذیری حیاتی که با شناسه CVE-2019-2107 معرفی شده است، مربوط به چارچوب (فریمورک) رسانه‌ای اندورید است، که اگر اکسپلویت گردد، به یک مهاجم از راه دور اجازه می‌دهد کد دلخواه خود را در دستگاه هدف اجرا نماید.

برای به دست آوردن کنترل کامل دستگاه هدف، تنها چیزی که مهاجم نیاز دارد این است که بتواند کاربر را برای باز کردن یک فایل ویدئوی ساختگی که با برنامه پخش ویدئوی پیش‌فرض اندروید سازگاری دارد فریب دهد. اگرچه گوگل در اواخر ماه جاری وصله‌ی امنیتی مربوطه را برای این رفع این آسیب‌پذیری منتشر نموده است، اما به نظر می‌رسد میلیون‌ها دستگاه اندرویدی هنوز در انتظار دریافت آخرین بروزرسانی‌های امنیتی برای اندورید هستند که باید توسط سازندگان دستگاه‌های مربوطه ارائه شوند.

گوگل در خبرنامه اندروید خود در ماه جولای در توصیف این آسیب‌پذیری این‌گونه نوشت: "شدیدترین آسیب‌پذیری در این بخش [چارچوب رسانه‌ای] مهاجم از راه دور را قادر به استفاده از یک

فایل ساختگی خاص، به منظور اجرای کد دلخواه، در قالب یک فرآیند دارای حق دسترسی می‌کند."



موضوع نگران‌کننده این است یک توسعه‌دهنده اندورید آلمانی به نام مارسیس کوزلوفسکی کد اثبات مفهومی این آسیب‌پذیری را در گیت‌هاب آپلود نموده است.

اگرچه کد اثبات مفهومی به اشتراک‌گذاری شده توسط کوزلوفسکی، یک ویدئوی کدگذاری شده‌ی HEVC است که تنها موجب از کار افتادن برنامه مدیاپلیر می‌شود، اما می‌تواند به مهاجم کمک کند تا اکسپلویت‌های مد نظر خود را برای دستیابی به RCE در دستگاه هدف اجرا نماید.

با این وجود، باید متذکر شد که اگر ویدئوهای مخرب مشابه آنچه توضیح داده شد، از طریق برنامه‌های پیام‌رسان مانند واتس‌اپ یا فیسبوک مسنجر ارسال شوند یا در سرویس‌هایی مانند یوتیوب یا توییتر بارگذاری گردند، حمله کار نخواهد کرد.

این به این دلیل است که سرویس‌های مذکور و موارد مشابه، معمولاً ویدئوها را فشرده و و مجدد رمزگذاری می‌کنند، که این عمل موجب از بین رفتن اثر کد مخرب خواهد شد.

✓ توصیه امنیتی:

بهترین راه مصون ماندن از این حمله، اطمینان از به روز بودن سیستم‌عامل تلفن همراه است که به محض انتشار وصله‌های امنیتی هر چه سریعتر باید به آخرین نسخه آپدیت شود.

همچنین توصیه می‌گردد از دانلود و باز کردن ویدئو از منابع نامعتبر اجتناب نموده و از قوانین مربوط به امنیت و حفظ حریم خصوصی پیروی نمایید.

منبع خبر :

https://thehackernews.com/2019/07/android-media-framework-hack.html

Scan Link

حمله SWAPGS که تمام CPUهای مدرن اینتل را تحت تأثیر قرار می‌دهد

گردآورنده: سهیلا مرادی

مایکروسافت و Red Hat، از کشف گونه‌ی جدیدی از آسیب‌پذیری‌های Spectre خبر می‌دهند که تمام CPUهای اینتل مدرن و نیز پردازنده‌های AMD که تکنولوژی اجرای احتمالی[5] را به کار می‌برند تحت تأثیر قرار می‌دهد.

این آسیب‌پذیری که با شناسه CVE-2019-1125 شناخته می‌شود، به مهاجمین محلی غیرمجاز اجازه می‌دهد که به اطلاعات حساس ذخیره شده در حافظه‌ی هسته‌ی سیستم‌عامل که به سطح دسترسی بسیار بالایی نیاز دارد و حاوی گذرواژه‌ها، توکن‌ها و کلیدهای رمزنگاری می‌باشد دسترسی پیدا کنند.

اجرای احتمالی یک جزء اصلی در طراحی پردازنده‌های مدرن است که به صورت نظری دستورالعمل‌ها را براساس فرض‌هایی انجام می‌دهد که احتمالاً درست هستند. اگر فرضیه‌ها معتبر باشند، اجرا ادامه می‌یابد و اگر نباشد، رد می‌شود.

این اجراهای احتمالی دارای آثار جانبی نیز هستند، که در حالت عدم تفسیر CPU، بازیابی نشده و می‌توانند از طریق حملات side-channel منجر به افشای اطلاعات گردند.

مایکروسافت به صورت مخفیانه وصله امنیتی مورد نظر را برای آسیب‌پذیری مذکور در بروزرسانی روز سه‌شنبه، جولای 2019، منتشر نمود

[5] speculative-execution

اما محققان امنیتی شـــرکت Bitdefender آن را کشـــف، و به صورت عمومی افشاء نمودند.

بـــه گفتـــه‌ی Red Hat، این حملـــه متکی به اجـــرای احتمالی دســـتورات غیرمنتظره SWAPGS پس از پیش‌بینی نادرست می‌باشد.

دستور SWAPGS، از دستورات سیستمی مجاز است که مقادیر رجیستر GS را با مقادیر موجود در رجیســـتر MSR جابجا کرده و فقط بـــرای پردازنده‌های دارای معماری x86-64 در دسترس می‌باشد.

محققان می‌گویند: "از آنجا که دســـتور SWAPGS می‌تواند به صورت احتمالی در مُـــد کاربر اجرا شـــود، مهاجم می‌توانـــد آدرس داده‌هـــای مربوط به هر پردازنده را که معمولاً فقط برای هسته در دسترس است فاش کند."

حمله SWAPGS، Kernel Page-Table Isolation (KPTI) را که در CPUهای مدرن ارائه شـــده، می‌شـــکند و می‌تواند موجب نشـــت اطلاعات حســـاس حافظه‌ی هسته در مُد کاربر شود.

بـــه گفته محققـــان Bitdefender، این حمله جدید می‌توانـــد تمام اقدامات پیشـــگیرانه‌ای را که برای Spectre و Meltdown در اوایل سال 2018 معرفی شـــد، دور بزند و عمـــلاً هر کامپیوتری را در سراســـر جهـــان در معرض خطر قرار دهد.

اگرچه هســـته‌ی لینوکس حاوی ابزاری اســـت که ممکن اســـت طـــی حمله‌ی SWAPGS به سیســـتم‌های لینوکســـی، اکســـپلویت شـــود، اما محققان معتقدند که اکســـپلویت سیســـتم‌های لینوکســـی اندکی سخت‌تر از سیستم‌های ویندوزی است.

از آنجـــا که ایـــن حمله نمی‌توانـــد از راه دور انجام شـــود، بعید اســـت که موجـــب آلودگی‌های بدافـــزاری شـــود، ماننـــد EternalBlue کـــه برای WannaCry مـــورد اســـتفاده قـــرار گرفـــت، در عوض می‌توانـــد به عنوان بخشی از یک حمله بسیار هدفمند مورد سوءاستفاده قرار گیرد.

✓ **توصیه امنیتی:**

کاربـــران تحـــت تأثیر ایـــن آســـیب‌پذیری می‌توانند با بروزرســـانی سیستم‌عامل این مشکل را رفع نمایند.

گوگل نیز برای رفع این آســـیب‌پذیری، در سیســـتم‌عامل ChromeOS 4.19 خـــود، یک وصله‌ی امنیتـــی آماده کرده اســـت که به زودی منتشـــر خواهد شد.

منبع خبر :

https://thehackernews.com/2019/08/swapgs-speculative-execution.html

Scan Link

آســـیب‌پذیری‌های امنیتی VMware کـــه منجر به اجرای کد و ایجاد حمله DoS می‌گردند

گردآورنده: سهیلا مرادی

اخیـــراً Vmware تعدادی آســـیب‌پذیری امنیتی را رفع نموده اســـت که می‌توانـــد منجر به اجرای کد، افشـــای اطلاعـــات و ایجاد شـــرایط DoS با دسترسی‌های کاربر معمولی شود.

محصولات تحت تأثیر این آسیب‌پذیری عبارتند از:

- VMware vSphere ESXi (ESXi)
- VMware Workstation Pro / Player (Workstation)
- VMware Fusion Pro / Fusion (Fusion)

آسیب‌پذیری‌های امنیتی VMware

آسیب‌پذیری‌های خواندن و نوشتن خارج از محدوده که در عملکرد pixel shader مربـــوط به VMware ESXi، Workstation و Fusion وجود دارد. ایـــن آسیب‌پذیری با شناسه‌های زیر شناخته می‌شود:

CVE-2019-5521: آسیب‌پذیری خواندن خارج از محدوده با شدت CVSSv3 = 6.3-7.7

CVE-2019-5684: آسیب‌پذیری نوشتن خارج از محدوده با شدت CVSSv3 = 8.5

اکسپلویت نمودن آسیب‌پذیری

بـــه منظور اکسپلویت این آسیب‌پذیری، مهاجم می‌تواند با اســـتفاده از گرافیک ســـه بعـــدی بـــه ماشـــین مجـــازی دسترســـی داشـــته باشـــد. ایـــن قابلیـــت بـــه صـــورت پیش‌فـــرض در Workstation Pro و Fusion Pro فعـــال است.

آسیب‌پذیری خواندنِ خارج از محدوده به مهاجم اجازه می‌دهد که اطلاعات حساس را از مکان‌های حافظه بخواند. این امر می‌تواند منجر به افشای اطلاعات و اجرای حمله DoS توسط مهاجم (با دسترسی کاربر معمولی) شود.

آسیب‌پذیری نوشتن خارج از محدوده، داده‌های پس از اتمام و یا قبل از شروع را می‌نویسد. اگر هاست تنها یک درایور گرافیکی NVIDIA آسیب‌دیده داشته باشد، این آسیب‌پذیری می‌تواند اکسپلویت شود. اجرای موفقیت‌آمیز اکسپلویت، به مهاجم اجازه می‌دهد کد دلخواه خود را بر روی هاست اجرا نماید.

چگونگی رفع آسیب‌پذیری

با بروزرسانی محصول مورد نظر به آخرین نسخه می‌توان آسیب‌پذیری مذکور را رفع نمود، همچنین راه دیگر، غیرفعال نمودن قابلیت 3D-acceleration است.

- VMware vSphere ESXi (ESXi) (ESXi670-201904101-SG, ESXi650-201903001)
- VMWare Fusion (10.1.6, 11.0.3)
- VMWare Workstation (14.1.6, 15.0.3)

منبع خبر :

https://gbhackers.com/vmware-security-vulnerabilities/

Scan Link

اخبار کوتاه

آیا مرور وب در حالت ناشناس واقعاً فعالیت‌های ما را پنهان می‌کند؟

آیا باز کردن یک پنجره جدید در حالت ناشناس یا Incognito Mode تفاوتی در حفظ حریم شخصی شما ایجاد می‌کند؟ پاسخ کوتاه این است که «خیر». طبق نتایج تحقیقات انجام شده حدود 40% افراد تصور می‌کنند حالت ناشناس، موقعیت مکانی آنها را در وب‌سایت مقصد مخفی می‌کند و یک سوم افراد نیز بر این باورند که با این کار می‌توانند از دید کارفرما پنهان بمانند، در حالی که اینچنین نیست.

در واقع حالت‌های مرور محرمانه به مراتب محدودتر از آن چیزی هستند که فکر می‌کنید، شاید سابقه فعالیت اینترنتی شما به شکل آشکار ثبت نشود، ولی انتظار بیشتری نداشته باشید.

---

3 برنامه که توسط شکارچیان کودکان استفاده می‌شود، همین حالا آن‌ها را حذف کنید

تاکنون نگرانی‌های موجود در دنیا کم نبوده است که اکنون، دولت آمریکا به والدین در مورد سه برنامه دوست‌یابی که بیماران جنسی برای ارتباط با کودکان از آن استفاده می‌کنند، هشدارداده است. شاید باور نکنید اما این برنامه‌ها به کودکان زیر 13 سال اجازه می‌دهند پروفایل‌های دوست‌یابی ایجاد کنند. با این‌کار نه تنها شکارچیان جنسی می‌توانند از طریق پروفایل خود با کودکان تماس بگیرند بلکه می‌توانند براساس سن و مکان نیز جستجو کنند.

این برنامه‌ها Meet24 ، FastMeet و Meet4U هستند، که هنگام نصب تاریخ تولد کاربران، آدرس‌های ایمیل و عکس‌ها را از کاربر می‌گیرند. قانون حمایت از حریم خصوصی آنلاین کودکان، ارائه‌دهندگان برنامه‌ها را موظف می‌کند قبل جمع‌آوری یا به اشتراک گذاری هرگونه اطلاعات شخصی درباره کودکان زیر 13 سال، به والدین آن‌ها اطلاع دهند و رضایت والدین را دریافت کنند. کمیسیون تجارت فدرال گفته که این برنامه‌ها در حالی که سیاست حفظ حریم خصوصی کاربران زیر 13 سال را قبول داشته‌اند از استفاده کودکان زیر 13 سال از برنامه جلوگیری نکرده‌اند.

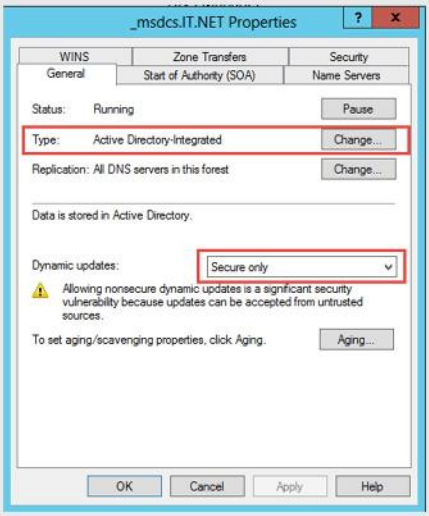
مقالات آموزشی

نقـــص در آنتی‌ویروس کسپرســـکی امـــکان ردیابی کاربران را فراهم می‌کند!

گردآورنده: سیده آرزو حسنی

1- تنها Dynamic Update امن

Dynamic Update می‌تواند Secure و یا Non-Secure باشـــد. به منظور جلوگیری از حملات DNS Spoofing، لازم است Dynamic Updates بر روی Secure Only قرار داده شود.



2- تنظیم Global Query Block List

ویژگـــی Global Query Block List اولین بار در Windows Server 2008 معرفـــی گردید. ایـــن ویژگی باعـــث جلوگیری از ثبـــتHost Name های کاربران مخرب می‌گردد. تمامـــی DNS Serverهای Authoritative برای یک Zone، لازم اســـت با Block Listهای مشابه پیکربندی شود. Block List یک Per-Server Setting به شـــمار مـــی‌رود، لذا ما بین ســـرورها Replicate نخواهد شد.

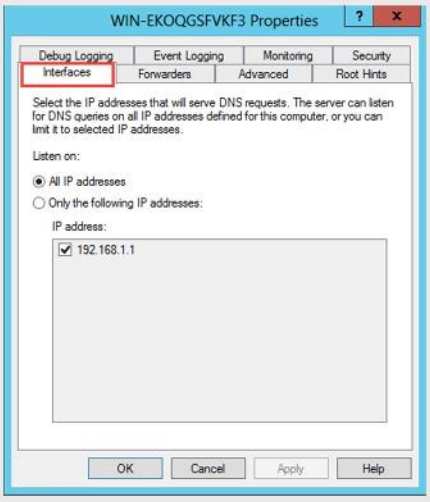
3- پیکربندی Cache Locking

پس از فعال کردن این ویژگی، DNS Server مجوز بازنویسی رکوردهای Cache شـــده در محدوده زمانـــی TTL را نخواهد داد. همچنیـــن این قابلیت باعث بالارفتن امنیت در مقابل حملات Cache Poisoning می‌شـــود. این ویژگی از نســـخه Windows Server 2008 R2 به بعد در دســـترس می‌باشد. جهت پیکربندی Cache Locking می‌توان از دستور ذیل استفاده نمود:

dnscmd /Config /CacheLockingPercent <percent>

4- محدودسازی پاسخ DNS بهInterface های انتخاب شده

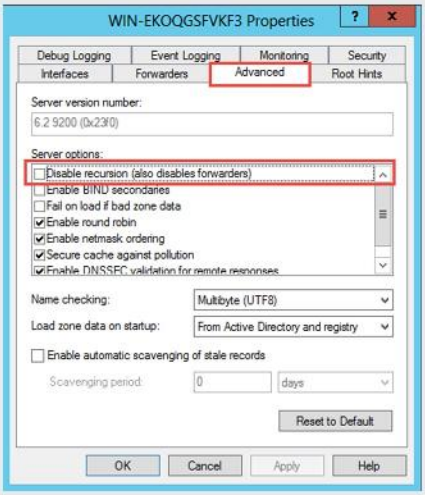
به صورت پیش‌فرض، DNS ســـروری کـــه چندین کارت شـــبکه دارد و یا با چندین IP Address بر روی یک تک Interface پیکربندی شده است، به تمامـــی DNS Query های ارســـالی به همه IP Addressها پاسخ می‌دهد. به منظور بالابردن امنیت DNS Server، لازم است سرویس DNS تنها به آن IP Address که DNS Client آن را به عنوان Preferred Server انتخاب کرده اســـت، پاسخ دهد.



5- غیرفعال‌سازی Recursion

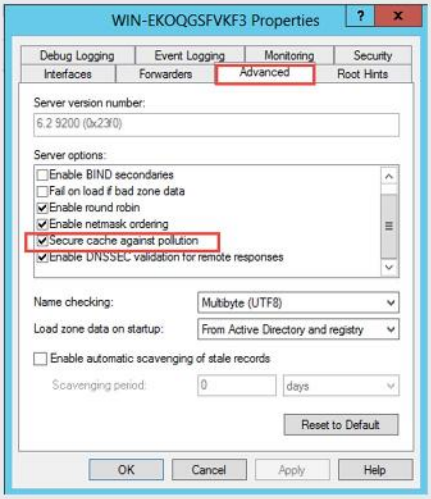
برای محافظـــت از DNS Serverها، لازم اســـت Recursion بر روی تمامی سرورهایـــی که نیاز به انجام Queryهای Recursive ندارند، غیرفعـــال شود. Recursion یک تکنیک Name Resolution به شمار می‌رود کـــه در آن، DNS Server بـــه منظـــور Resolve کـــردن کامل نام، جهت پاســـخ به درخواست کلاینت از ســـایر DNSها Query می‌گیرد و پاسخ آن را به کلاینت ارســـال می‌کنـــد. در صورتی که ایـــن ویژگی فعال باشـــد، مهاجم می‌تواند از فرآیند Recursion اســـتفاده نموده تـــا Domain Name ها با IP Addressهای نادرست Resolve شوند. به صورت پیش‌فرض DNS Server ها،

Recursive Queryهـــا را از طرف کلاینت‌های خـــود وDNS Server هایی که Queryهای DNS Client را Forward کرده‌اند، اجرا می‌کنند.



6- امن‌سازی DNS Cache

به صورت پیش‌فرض DNS Server در مقابل Cache Pollution (هنگامی که پاسخ‌های DNS Query شامل داده‌های Non Authoritative و یا مخرب است) امن اســـت. ویژگی Secure Cache Against Pollution از آلوده کردن DNS Server Cache توسط مهاجم(با Resource Recordهایی که توســـــط DNS Server درخواســـت نشـــده‌اند)، جلوگیری می‌کند. تغییر در تنظیمات پیش‌فرض ســـبب می‌شـــود تا صحت پاســـخ‌هایی که توســـط سرویس DNS Server فراهم می‌شود، کاهش یابد.



7- DNS Queries & Response Validation

به صـــورت دو تکنولوژی که در ذیل در مورد آن توضیح داده شـــده اســـت سبب بـــــالارفتن امنیت بـــا اســـــــتفاده از اعـــــــتبارسنجی ارتباط‌هـــــای Server to Server و Server to Client می‌شوند:

- Domain Name System Security Extensions (DNSSEC)

DNSSEC، مجموعه‌ای از افزونه‌ها اســـت که ســـبب بهبـــود امنیت پروتکل DNS می‌شـــود. این ویژگـــی از Windows Server 2008 R2 به بعد اضافه شده و مـــــوجب می‌شـــــود تا DNS Server و Resolver نسبت بـــه پاسخ‌ها مطمئن باشند. این کار از طریق Digital Signature (امضای دیجیتال) محقق می‌شـــود. همچنین DNS Server، DNSSEC را در مقابل حملات DNS Spoofing محافظت می‌کند.

- IPSEC

ایـــن ویژگی راه حل مناســـبی را جهت محافظت از سیســـتم‌ها و اطلاعات در مقابل حملات شـــبکه فراهم مـــی‌آورد. IPSEC، خطر تغییر اطلاعات ارســـالی بیـــن دو ســـرور (Zone Transfer Data) را کاهش می‌دهـــد. هنگامی‌که IPSEC فعـــال می‌شـــود، هر دو پایانه پیش از شـــروع ارتباط اعتبارســـنجی می‌شـــوند. از این ویژگـــی همچنین می‌تـــوان جهت محافظـــت از ارتباط بیـــن DNS Serverهـــا و کلاینت‌هـــا جهـــــت جلوگیـــــری از Spoofing Attack استفاده نمود.

8- فعال‌سازی Name Protection

به منظور جلوگیـــری از حمـــلات Name Squatting، از Name Protection استفاده کنید.

منبع خبر :

https://technet24.ir/how-secure-dns-service-3488

Scan Link

امنیت کاربر رایانه

پشتیبان‌گیری و بازیابی داده

گاهی اوقات برای کامپیوترهای کاملاً پایدار نیز اتفاقاتی رخ می‌دهد که هرگز انتظارشان را نداشته‌ایم. چنین رویدادهایی ممکن است به از دست رفتن فایل‌های مهم ما منجر شوند و خسارات جبران‌ناپذیری به بار آورند. ضمناً نمی‌توان زمان و هزینه‌ای که باید برای عیب‌یابی و ریکاوری سیستم صرف کنیم را هم نادیده گرفت.

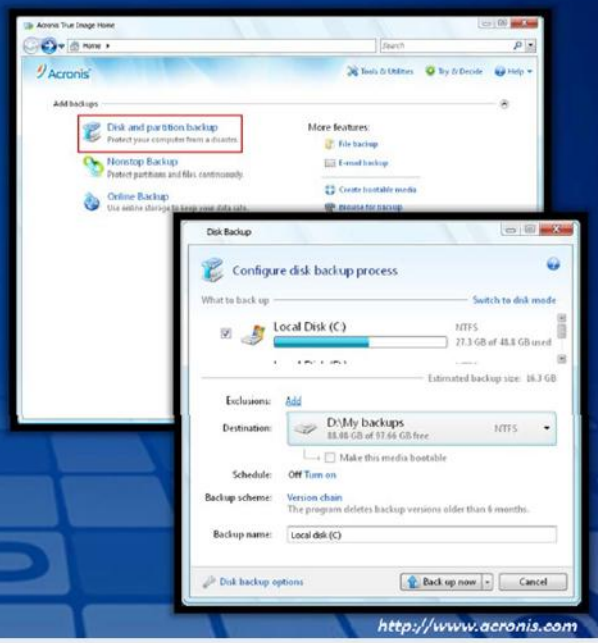
در چنین مواقعی داشتن نسخه‌ی پشتیبان از فایل‌های کلیدی و مسلط بودن به ابزارهای ریکاوری سیستم یک ضرورت محسوب می‌شود.

در این شماره از بولتن خبری، در فصل "پشتیبان‌گیری داده و فرآیند بازگشت از فاجعه" قصد داریم به معرفی ابزارهای مختلف پشتیبان‌گیری و بازیابی داده، و نیز شیوه‌های حفاظت از داده‌های پشتیبان بپردازیم.

با ما همراه باشید...

ابزارهای پشتیبان گیری داده: Acronis True Image Home 2011

- Acronis True Image Home 2011 امکان پشتیبان گیری و بازیابی داده های مربوط به سیستم عامل، برنامه های کاربردی، تنظیمات و فایل های شخصی را به صورت بی وقفه و قابل اطمینان برای کاربران خانگی فراهم می کند
- این ابزار هر پنج دقیقه یک بار به روش پشتیبان گیری افزایشی یک پشتیبان از داده های کاربر تهیه می کند، و بنابراین کاربر را قادر می سازد تا سیستم، فایل ها و پوشه های خود را به هر نقطه ای از وضعیت قبلی بازگرداند
- این ابزار به منظور پشتیبان گیری خودکار از داده ها و فایل های باارزش از طریق اینترنت و ذخیره سازی آن در یک مکان امن، دارای سرویس ذخیره سازی آنلاین می باشد



ابزارهای پشتیبان گیری داده: NovaBACKUP Home Protection

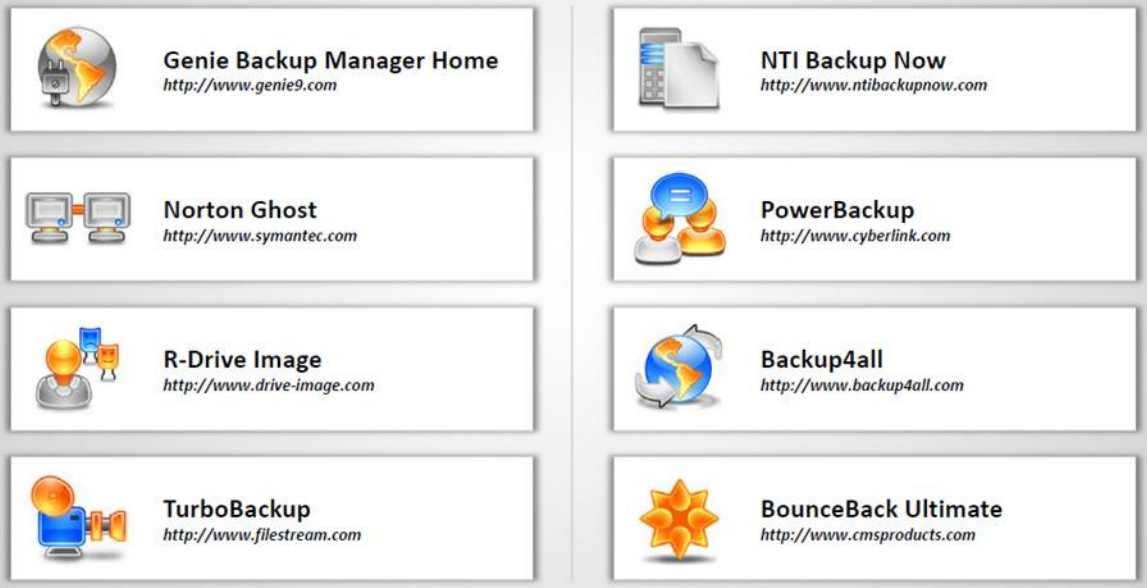
ابزار NovaBACKUP® Home Protection به طور خودکار از تمامی فایل های مهم کاربر پشتیبان گرفته و از آن ها محافظت می نماید

ویژگی ها:

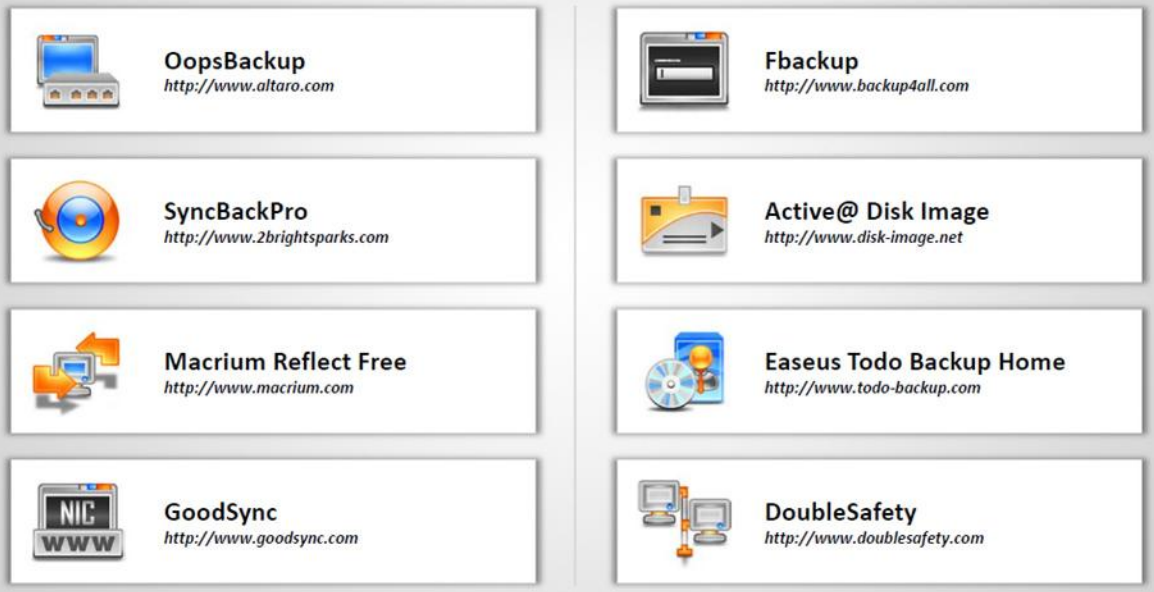
- پردازش های خودکار به طور مداوم پشتیبان را برای کاربر آپدیت می کنند_ بدون نیاز به اینکه کاربر مدام عمل پشتیبان گیری را به خود یادآوری نماید
- مدیریت مرکزی کنترل کامل بر روی داده های پشتیبان را برای کاربر فراهم می‌کند
- قابلیت بازیابی و ایجاد ایمیج از کل دیسک امکان بازیابی کل سیستم را فراهم می آورد
- تکنولوژی Fast Bit با کوچکترین تغییری پشتیبان کاربر را به روز خواهد نمود

http://www.novastor.com

ابزارهای پشتیبان گیری داده برای ویندوز

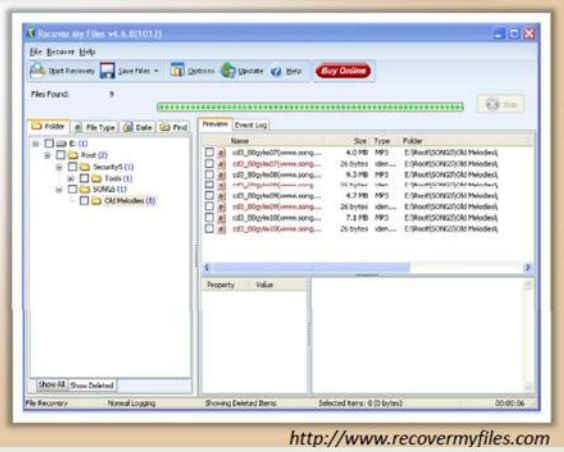


ابزارهای پشتیبان گیری داده برای ویندوز



ابزارهای بازیابی داده: Recover My Files

نرم افزار Recover My Files فایل هایی را که از سطل زباله ویندوز حذف شده اند، یا به دلیل فرمت شدن یا خرابی هارددیسک، آلوده شدن به ویروس و تروجان، خاموش شدن ناگهانی سیستم و یا خرابی نرم افزار از بین رفته اند را بازمی گرداند

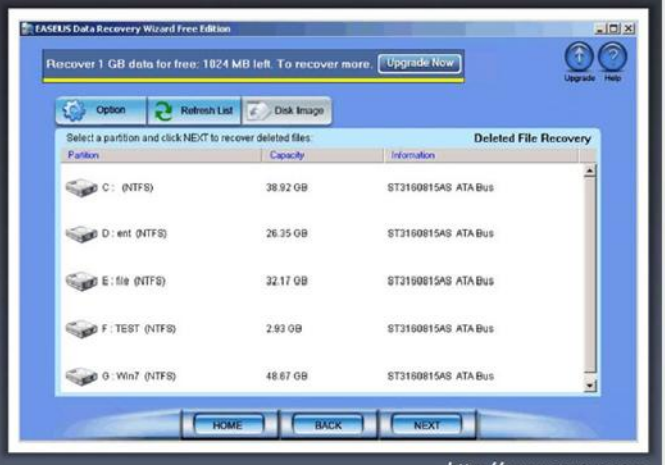


http://www.recovermyfiles.com

ابزارهای بازیابی داده: EASEUS Data Recovery Wizard

EASEUS Data Recovery Wizard یک راه حل جامع بازیابی داده به منظور بازگردانی داده هایی که به دلایل مختلف (مانند آلوده شدن به ویروس، خاموش شدن ناگهانی کامپیوتر و...) از دست رفته یا آسیب دیده اند، برای کاربران کامپیوتر ارائه می نماید

- بازیابی فایل های پاک شده از سطل آشغال ویندوز
- بازیابی فایل پس از فرمت شدن، حتی اگر ویندوز را مجددا نصب کرده باشید
- بازیابی دیسک پس از خراب شدن
- بازیابی داکیومنت های آفیس، عکس ها، تصاویر، فیلم، آهنگ، ایمیل و غیره
- بازیابی فایل های از دست رفته در هارددیسک، یواس بی درایو، کارت حافظه، کارت دوربین، فلاپی دیسک و سایر رسانه های ذخیره سازی



http://www.easeus.com

ابزارهای بازیابی داده برای ویندوز

Advanced Disk Recovery
http://www.systweak.com

File Scavenger Data Recovery
http://www.quetek.com

Handy Recovery
http://www.handyrecovery.com

Windows Data Recovery Software
http://www.diskdoctors.net

R-Studio
http://www.data-recovery-software.net

Quick Recovery for Windows
http://www.recoveryourdata.com

VirtualLab Data Recovery
http://www.binarybiz.com

GetDataBack
http://www.runtime.org

ابزارهای بازیابی داده برای ویندوز

Stellar Phoenix Windows Data Recovery
http://www.stellarinfo.com

Recuva
http://www.piriform.com

MiniTool Power Data Recovery
http://www.powerdatarecovery.com

Partition Wizard Home Edition
http://www.minitool-partitionrecovery.com

SoftPerfect File Recovery
http://www.softperfect.com

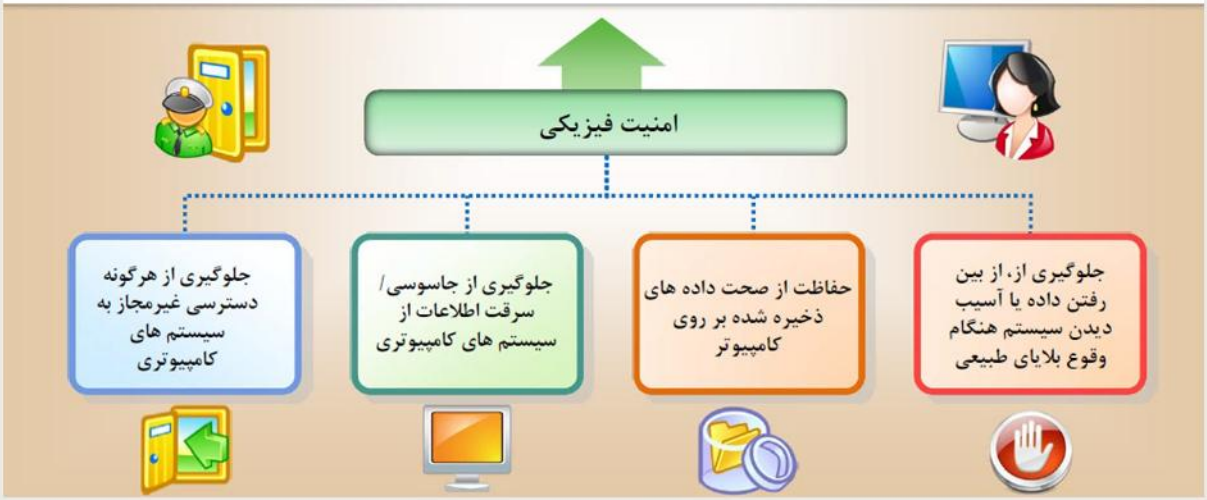
Undelete Plus
http://undeleteplus.com

FreeUndelete
http://www.officerecovery.com

RecoverPlus Photo Recovery
http://www.arcksoft.com

امنیت فیزیکی

- امنیت فیزیکی، اولین لایه حفاظتی برای کامپیوتر و داده هاست
- امنیت فیزیکی شامل حفاظت از دارایی هایی مانند سخت افزار، شبکه و داده، در مقابل حملاتی است که موجب از بین رفتن یا آسیب دیدن آن ها می شوند
- عوامل مختلفی وجود دارند که می توانند امنیت فیزیکی را تحت تأثیر قرار دهند، مانند خرابی، سرقت، گرد و غبار، آتش سوزی، سیل، زلزله و غیره



اقدامات لازم جهت برقراری امنیت فیزیکی: قفل

- قفل ها به عنوان اولین روش کنترل دسترسی فیزیکی برای سیستم های اطلاعاتی و سایر دستگاه های ذخیره سازی قابل جابجایی در نظر گرفته می شوند
- قفل ها با توجه به نحوه طراحی و پیاده سازی، سطوح امنیتی مختلفی ارائه می‌کنند

قفل ها استفاده می شوند برای:

- محدود نمودن افراد غیرمجاز برای استفاده از اتاق کامپیوتر
- جلوگیری از دسترسی غیرمجاز به کامپیوتر، توسط قفل نمودن درها و پنجره های محلی که کامپیوتر درآنجا قرار دارد
- قفل کردن CPU و مانیتور به منظور جلوگیری از به سرقت رفتن آن ها


اقدامات لازم جهت برقراری امنیت فیزیکی: بیومتریک
بیومتریک به شناسایی و تشخیص هویت افراد بر اساس خصوصیات آن ها اشاره دارد
اثرانگشت
اسکن شبکیه
اسکن عنبیه
تکنیک های تشخیص بیومتریک
تشخیص بر اساس ساختار رگ
تشخیص چهره
تشخیص صدا


اقدامات لازم جهت برقراری امنیت فیزیکی: جلوگیری از آتش سوزی
آتش سوزی ممکن است به علت یک اتصال کوتاه رخ دهد، و موجب به بار آمدن خسارات سنگین و جبران ناپذیر گردد، بنابراین توصیه های زیر را مدنظر داشته باشید
اقدامات لازم جهت پیشگیری از آتش سوزی
اتاق را عاری از گرد و غبار نگه داشته، و در اسرع وقت وسایل اضافی و اوراقی را دور بیندازید
از تجهیزاتی که موجب شوک الکتریکی می شوند استفاده نکنید
از سیم کشی درست و ابزار و تجهیزات خوب استفاده کنید
اطمینان حاصل کنید که تمام درب ها و راهروهای اضطراری مشخص شده باشند
باید نحوه استفاده از کپسول آتش نشانی را بدانید
کاربران باید بدانند که در شرایط اضطراری با چه کسی باید تماس بگیرند
در انتهای روز حتما لوازم برقی را از برق بکشید
اطمینان حاصل کنید که سطل زباله به طور مرتب خالی می شود

امن سازی لپ تاپ ها برای جلوگیری از سرقت

سرقت لپ تاپ ها منجر به افشای اطلاعاتی مانند نام های کاربری، پسوردها، داده های محرمانه و نیز جزئیات شبکه ی شرکت یا محیطی که لپ تاپ به آن متصل شده است می گردد

امنیت لپ تاپ

نبایدها

- لپ تاپ را بدون مراقبت در اتومبیل، خارج از محل کار/ منزل رها نکنید
- رمز عبور را فراموش نکنید و از به اشتراک گذاشتن آن با دیگران جداً اجتناب نمایید

بایدها

- شماره سریال لپ تاپ را به خاطر سپرده، و آن را ایمن نگه دارید
- یک پوشش برای لپ تاپ در نظر بگیرید تا بتوانید آن را به راحتی تشخیص دهید
- در صورت به سرقت رفتن لپ تاپ، سریعاً سرقت را گزارش نمایید

اقدامات مقابله با سرقت لپ تاپ

برای داده های بسیار حساس یک third-party privacy protection در نظر بگیرید

داده های حساس را رمزگذاری نموده و از هرآنچه که در لپ تاپ وجود دارد پشتیبان تهیه کنید

برای لپ تاپ خود بیمه کامپیوتر تهیه کنید

برای تنظیمات بایوس لپ تاپ خود یک رمز عبور در نظر بگیرید

از امنیت های مبتنی بر سخت افزار قوی استفاده کنید

بر روی لپ تاپ خود ابزارهای ردیابی نصب کنید تا در زمان به سرقت رفتن لپ تاپ بتوانید مکان آن را ردیابی کنید

خلاصه فصل

- وجود پشتیبان در شرایطی مانند خرابی سخت افزار، سرقت، ساقط شدن سیستم و یا وقوع بلایای طبیعی مورد نیاز است
- کاربران باید هر زمان که تغییری در فایل های مهم ایجاد می شود از آن ها پشتیبان تهیه کنند، به گونه ای که در صورت گم شدن یا آسیب دیدن داده آخرین نسخه کپی آن در دسترس باشد
- پشتیبان گیری آنلاین یا از راه دور روش ذخیره سازی داده خارج از محل فعلی است، که‌در آن محتویات هارددیسک به طور منظم به کامپیوتر دیگری در بستر اینترنت پشتیبان گیری می شود (سرور راه دور)
- پشتیبان گیری نرمال/کامل، افزایشی و تفاضلی انواع پشتیبان گیری در ویندوز هستند
- امنیت فیزیکی شامل حفاظت از دارایی هایی مانند سخت افزار، شبکه و داده، در مقابل حملاتی است که می توانند منجر به از دست رفتن داده یا آسیب دیدن آن شوند
- سرقت لپ تاپ ها منجر به افشای اطلاعاتی مانند نام های کاربری، پسوردها، اطلاعات محرمانه و نیز جزئیات شبکه ی شرکت یا محیطی که لپ تاپ به آن متصل شده است می گردد

چک لیست پشتیبان گیری داده

- پشتیبان گیری از داده های مهمی مانند داکیومنت ها، عکس ها، ایمیل و ... و ذخیره آن بر روی سی دی، دی وی دی ، نوار یا هر نوع دیسک دیگر، در فواصل زمانی منظم
- نگه داری داده های پشتیبان در یک مکان امن
- نگه داری چندین کپی پشتیبان از داده های مهم
- استفاده از تکنیک های رمزگذاری برای حفاظت از داده های پشتیبان
- بررسی ویژگی های پشتیبان گیری زمانبندی شده و خودکار هنگام انتخاب یک ابزار یا سرویس پشتیبان گیری، چرا که پشتیبان گیری دستی مستعد بروز خطاهای انسانی بوده و بنابراین آسیب پذیر است
- بررسی میزان پایداری ارائه دهنده سرویس، در صورت استفاده از سرویس پشتیبان گیری‌آنلاین و بازیابی داده
- تأیید مداوم روند پشتیبان گیری به منظور اثربخشی بهتر

اخبار داخلی

در کمپ تابستانی آپا چه می‌گذرد؟

در تابستان ۹۸ نیز همانند سال‌های گذشته کارآموزانی در مرکز تخصصی آپا دانشگاه رازی مشغول فعالیت هستند.

تابستان امسال در راستای تحقق هدف تربیت ۱۰۰۰ افسر سایبری، به نسبت سال‌های گذشته تعداد کارآموزان بیشتر و زمینه‌های کاری آنان متنوع‌تر است. با توجه به بحران شغلی در کشور و علی‌الخصوص کرمانشاه، و نیز با در نظر گرفتن جایگاه "امنیت" و اهمیت آن در سطح کشور، تربیت نیروهای علاقه‌مند و ماهر در این زمینه می‌تواند کمک شایانی به اشتغال‌زایی داشته باشد. لذا با جذب این نیروها به عنوان کارآموز و واگذاری پروژه‌های حوزه امنیت به آن‌ها میزان توانایی آن‌ها را محک زده و در جهت رشد این توانایی بستر مناسب در این مرکز برای آن‌ها فراهم می‌گردد.

کارآموزان آپایی از اوایل تابستان در این مرکز شروع به فعالیت نموده و همچنان نیز مشغول هستند. طی جلسات متعددی که با حضور این افراد تشکیل گردید متناسب با تخصص و مهارت هر یک، انجام بخشی از پروژه‌های تعریف شده در مرکز آپا به آنان محول شد. تعداد کارآموزان حدود ۱۲ نفر بوده و حوزه فعالیت آن‌ها به شرح ذیل می‌باشد:

- ۲ نفر مشغول در پروژه سایمان
- ۲ نفر مشغول در پروژه سایتبان
- ۴ نفر مشغول در پروژه USB فیلترینگ
- ۱ نفر مشغول در پروژه پارسو
- ۳ نفر تیم ارزیابی امنیتی، که کار ارزیابی امنیتی سایت‌ها را بر عهده داشته و همزمان در مسابقات فتح پرچم (CTF) بین‌المللی شرکت می‌کنند و تا کنون به رتبه‌های خوبی نیز دست یافته‌اند.

کسب مقام در مسابقات بین المللی فتح پرچم (CTF) توسط تیم آپای رازی

- **کسب مقام 63ام با 5100 امتیاز در مسابقات CTF بین المللی peaCTF، از میان 540 تیم**

53	muhenkuo	Kalamazoo Area Math and Science Center	5100
54	InsHack@it	Università Politecnica delle Marche	5100
55	33e3993c99eed4a77cb2d2ad2cd80e13	UNIBO	5100
56	Stupids	Sunrin Internet high school	5100
57	NuffyShell	BSDagents	5100
58	CyberKnuffons	University of Glasgow	5100
59	SinHack	Rajad	5100
60	Pwnage Inc	Microsoft	5100
61	Team Space	TVS	5100
62	GhOstSh3ll	IES Rafael Alberti	5100
63	APA Razi	Razi University	5100
64	The Victors	University of Michigan	5100
65	Contrail	TBD	4600
66	<marquee>team name</marquee>	AAAAAAAAA	4600
67	3 programmierende Randas	TU Ilmenau	4600
68	Hemem_Risha	ErosTet	4600
69	BogoMips	BogoMips	4600
70	KogCoder	Kogakuin University	4600

مسابقه peaCTF یک مسابقه فتح پرچم بین‌المللی است که توسط Philips Exeter Academy برگزار می‌گردد. مرحله اول این مسابقات چالش‌ها در حوزه‌های رمزنگاری، مهندسی معکوس، وب، جرم‌یابی رایانه‌ای و دانش عمومی لینوکس مطرح شد. مرحله دوم مسابقه ۲۳ آگوست ۲۰۱۹ برگزار می‌گردد که تیم آپای رازی با حل تمام چالش‌ها در مرحله اول، به مرحله دوم راه یافت. مرحله دوم این دور از مسابقات ماه آینده به‌صورت آنلاین برگزار می‌گردد.

- **کسب مقام 148ام با 140 امتیاز از میان 775 تیم، و کسب "رتبه اول" از بین تیم‌های ایرانی شرکت‌کننده، در مسابقات CTF بین المللی cybricsCTF**

145	spenaro_t	Unknown	140		20h 58m to end
146	securisec	Unknown	140		20h 34m to end
147	Defenit	South Korea	140		15h 13m to end
148	APA Razi	Iran	140		18h 49m to end
149	SharLike	Russia	140		18h 20m to end
150	Dozer	China	140		16h 49m to end
151	cat	United States	140		14h 8m to end
152	PwsecTeam	India	140		14h 5m to end
153	WhatTheShell?	France	140		12h 11m to end
154	gorogoroumaru	Japan	140		3h 46m to end

مسابقه بین‌المللی فتح پرچم CyBRICS مسابقه‌ای در زمینه امنیت کامپیوتر است که با تلاش مشترک ۶ دانشگاه از کشورهای روسیه، چین، هندوستان و آفریقای جنوبی در ۲۰ جولای ۲۰۱۹ به مدت ۲۴ ساعت برگزار گردید. سؤالات این‌مسابقه‌درزمینه‌web، forencics، reversing، network، crack-the-box و miscellaneous مطرح شده بودند که در قالب ۲۸ سؤال و به صورت Jeopardy-style برگزار گردید.

مرکز تخصصی آپا دانشگاه رازی