بولتن خبری

مرکز تخصصی آپا دانشگاه رازی

شماره نوزدهم

فروردین ماه ۱۳۹۹

بی نصیب نماندن SQL Server از حمله هکرها!

در این شماره می‌خوانید :

فهرست

صاحب امتیاز:
مرکز تخصصـــی آپـا دانشگـاه رازی

صفحه آرایی: **سید احسان حسینی**

سردبیران:
سیده مرضیه حسینی
صبا آزرمی

با همکاری
سیده آرزو حسنی

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

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

اخبار امنیتی

آسیب‌پذیری بحرانی RCE در افزونه وردپرس و حمله به 200,000 وب‌سایت

محققان Wordfence از دو آسیب‌پذیری RCE در یک افزونه سئوی وردپرس به نام Rank Math خبر دادند که به هکرها اجازه می‌دهد تا نزدیک به 200,000 وب‌سایت آسیب‌پذیر را مورد حمله قرار دهند و از راه دور به آنها دسترسی پیدا کنند.

Rank Math یک افزونه سئوی وردپرس با 200,000 نصب فعال است و ویژگی‌های مختلف سئو از جمله Setup Wizard، Google Schema Markup و Optimizes Unlimited Keywords را ارائه می‌دهد.

آسیب‌پذیری اول که بسیار بحرانی است به هکرها امکان می‌دهد متاداده‌های دلخواه خود از جمله امکان اعطا یا ابطال سطح دسترسی مدیر را بروزرسانی کنند.

در آسیب‌پذیری دوم هکرها می‌توانند قربانیان را به سمت هر وب‌سایت و هر قسمت از آن هدایت کنند.

یکی از ویژگی‌های سئوی افزونه Rank Math، به کاربران اجازه می‌دهد تا متاداده‌ها را بروزرسانی کنند.

تابعی به نام "update_metadata"، که در تصویر زیر قابل مشاهده است، برای بروزرسانی پست‌های موجود به کار می‌رود یا می‌تواند برای حذف یا بروزرسانی متاداده‌ها برای پست‌هایی که این آسیب‌پذیری بحرانی را فعال می‌کنند استفاده شود و مورد اکسپلویت قرار گیرد.

```
register_rest_route(
    $this->namespace,
    '/updateMeta',
    [
        'methods'  => WP_REST_Server::CREATABLE,
        'callback' => [ $this, 'update_metadata' ],
        'args'     => $this->get_update_metadata_args(),
    ]
);
```

طبق گزارش WordFence، مجوزهای دسترسی کاربران وردپرس در جدول usermeta ذخیره می‌شوند بدین معنی که یک مهاجم احراز هویت نشده می‌تواند به امتیازات کاربر مدیر دست یابد و امتیازات موجود مدیر را حذف کند.

دومین آسیب‌پذیری در یک ماژول قرار دارد که می‌تواند برای ایجاد ریدایرکت

در یک سایت استفاده شود.

به گفته محققان، این ریدایرکت نمی‌تواند روی یک فایل یا فولدر موجود روی سرور، از جمله صفحه اصلی سایت، تنظیم شود. همین موضوع، این آسیب‌پذیری را تـــا حدی محدود می‌کند درحالیکه یک هکـــر می‌تواند از اکثر مکان‌های سایت از جملـــه مکان جدید، یک ریدایرکت ایجاد کند.

هکر همچنین، دسترسی به محتوای موجود در سایت به جز صفحه اصلی را قفل می‌کند و بازدیدکنندگان را به وب‌سایت مخربی که توسط هکر میزبانی می‌شود هدایت می‌کند.

منبع خبر :

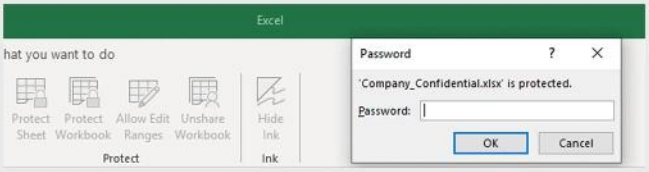
https://gbhackers.com/wordpress-plugin-bug/

Scan Link

انتشار بدافزار LimeRAT از طریق فایل اکسل

محققان امنیتی Mimecast کمپین مخربی کشف کرده‌اند که با استفاده از صفحات اکسلی که دارای رمز عبور هستند اقدام بـــه انتشار بدافزار LimeRAT مـــی‌کنند. مایکروسافت آفیس یکی از محبوبترین ابزارها در بین کاربران است، به همین دلیل از طرف مجرمان سایبری برای انتشار بدافزار مورد توجه و استفاده قرار می‌گیرد.

در این حمله، هکر از فایل اکسل دارای رمز عبور استفاده می‌کند. برای رمزگشایی این فایل، قربانیان باید رمز عبور VelvetSweatshop را وارد کنند و بار دیگر آن را روی ماکروهای مخرب تعبیه شده رمزگشایی کنند.



پی‌لود[1] نهایی، بدافزار LimeRAT است، یک تروجان مخرب دسترسی از راه دور که امکان دسترسی کامل به دستگاه قربانی را به هکر می‌دهد.

به گفته محققان، در این حمله خاص، مجرمان سایبری همچنین با ترکیب روش‌های دیگر در تلاش برای فریب سیستم‌های ضد بدافزار[2] با استفاده از رمزگذاری محتوای صفحات بودند از این رو این اکسپلویت و پی‌لود را مخفی می‌کردند.

این بدافزار به مجرمان سایبری اجازه می‌دهد تا پی‌لود را با ویژگی‌های مختلف، شخصی سازی کنند. پس از نصب بدافزار در دستگاه، جزئیاتی از جمله سیستم‌عامل، CPU، منطقه جغرافیایی (کشور)، کاربر و سایر جزئیات بدست می‌آید. قابلیت‌های این پی‌لود عبارتند از: استخراج ارز دیجیتال، کرم، قفل ضربه زدن به کلید، صفحه نمایش، سرقت اطلاعات و باج‌افزار. بدافزار LimeRAT بیشتر به عنوان پیوست ایمیل، تبلیغات مخرب آنلاین، مهندسی اجتماعی و کرک‌های نرم‌افزار توزیع شده است.

این یکی از قدرتمندترین RATها برای ویندوز است که در به زبان Visual Basic .NET کدنویسی شده است. این شهرت به دلیل تکنیک‌های گریز از آنتی‌ویروس‌ها، ویژگی‌های ضد ماشین‌مجازی، ردپای ناچیز و ارتباطات رمزگذاری شده است.

یکی دیگر از ویژگی‌های جالب این بدافزار، استفاده از پورت‌های متعدد برای ارتباطات است که باعث افزونگی کانال‌های ارتباطی می‌شود. این ارتباط با سرور C&C است که با استفاده از الگوریتم AES رمزگذاری شده است.

منبع خبر :

https://gbhackers.com/limerat-malware/

Scan Link

استقرار درب پشـــــتی بـر روی هـــــزاران SQL Server مایکروسافت!

محققان امنیتی از موج جدید حمله گسترده بدافزاری به نام Vollgar کـــــه قدمت آن به ماه می سال 2018 برمی‌گردد، خبر می‌دهند. این بدافزار با هدف قرار دادن سیستم‌های ویندوزی که MS-SQL را در حـــال اجرا دارند، سعی در نصب درب پشتی[3] و ســـایر بدافزارها از جمله ابزارهای دسترسی از راه دور چند منظوره[4] و استخراج کننده‌های ارز دیجیتال دارد.

Microsoft SQL Server یک سیستم مدیریت پایگاه‌داده رابطه‌ای است که توسط مایکروسافت به عنوان یک پلتفرم محبوب پایگاه‌داده در شبکه‌های مختلف سازمانی در سراسر جهان توسعه یافته است.

به گفته‌ی محققان، طی هفته‌های اخیر مهاجمان موفق شده‌اند تقریباً 2000-3000 سرور پایگاه‌داده را با موفقیت آلوده کنند، قربانیان احتمالی متعلق به بخش‌های مراقبت بهداشتی، حمل و نقل هوایی، فناوری اطلاعات و ارتباطات و نیز آموزش عالی در سراسر چین، هند، آمریکا، کره جنوبی و ترکیه می‌باشند.

خوشبختانه محققان اسکریپتی برای کاربرانی که نگران این موضوع هستند، منتشر کرده‌اند تا نشان دهد که MS-SQL و ویندوز آن‌ها به خطر افتاده است یا خیر.

---

[1] payload
[2] anti-malware
[3] backdoor
[4] remote access tools(RATs)

حمله‌ی Vollgar، با تلاش برای ورود به سرورهای MS-SQL از طریق brute-force کار خود را آغاز می‌کند که در صورت موفقیت‌آمیز بودن این حمله، به interloper اجازه می‌دهد تعدادی از پیکربندی‌ها را جهت اجرای دستورات مخرب MS-SQL و نیز دانلود دودویی‌های[1] مخرب، تغییر دهد.

پس از اطمینان از آن که فایل‌های cmd.exe و ftp.exe، مجوزهای لازم برای اجرا شدن را پیدا کردند، مهاجم از طریق حمله‌ی Vollgar و با سطح دسترسی بالا، اقدام به ایجاد درب پشتی جدید در پایگاه‌داده‌ی MS-SQL و نیز سیستم‌عامل می‌کند.

پس از اتمام تنظیمات اولیه، این حمله اقدام به ایجاد اسکریپت‌های دانلود کننده (دو اسکریپت VBS و یک اسکریپت FTP) کرده که "دو مرتبه" اجرا می‌شوند به این صورت که جهت جلوگیری از شکست‌های احتمالی، هر بار، مکان متفاوتی را روی سیستم فایل لوکال، مورد هدف قرار می‌دهد.

یکی از پی‌لودهای اولیه، به نام SQLAGENTIDC.exe یا SQLAGENTVDC.exe، ابتدا اقدام به از بین بردن لیست طولانی از فرآیندهایی که هدف آن‌ها تأمین امنیت منابع سیستم است کرده و سپس آنها را از دستگاه آلوده حذف می‌کند.

براساس مشاهدات شرکت امنیت سایبری: "در بین فایل‌ها (بر روی سرور C&C)، ابزار حمله‌ی MS-SQL، مسئول اسکن دامنه‌ی IPها، بروت‌فورس پایگاه‌داده‌ی هدف و اجرای از راه دور دستورات بوده است."

هنگامی که یک کلاینت ویندوز آلوده شده، به سرور 2C پینگ می‌زند، دیگری نیز اطلاعات مختلف دستگاه از جمله IP عمومی، موقعیت، نسخه سیستم عامل، نام کامپیوتر و مدل CPU را به سرقت می‌برد.

Guardicore افزود، با آن که دو برنامه‌ی 2C نصب شده توسط دو مبدا مختلف تولید شده‌اند، اما آن‌ها در قابلیت‌های کنترل از راه دور از جمله بارگذاری فایل‌ها، نصب سرویس‌های جدید ویندوز، keylogging، ضبط صفحه[2]، فعال کردن دوربین و میکروفن و حتی آغاز یک حمله‌ی انکار سرویس توزیع‌شده[3] دارای شباهت‌هایی هستند.

جهت جلوگیری از حملات بروت‌فورس، از رمز عبور قوی استفاده کنید!

باتوجه به آن که حدود نیم میلیون دستگاه، در حال اجرا و استفاده از MS-SQL هستند و از آنجا که مهاجمان در جستجوی پایگاه‌داده‌های ضعیف جهت سرقت اطلاعات حساس می‌باشند، لذا ضروری است سرورهای MS-SQL که در معرض اینترنت قرار دارند از لحاظ امنیتی ایمن شوند.

براساس تحقیقات Guardicore، آنچه که سرورهای پایگاه‌داده را جدای از قدرت CPU آن‌ها جذاب می‌کند، حجم عظیم داده‌های آن‌ها است. این ماشین‌ها احتمالا اطلاعات شخصی کاربران مانند نام‌کاربری، رمز عبور، شماره کارت‌های اعتباری و غیره را ذخیره می‌کنند که تنها با یک بروت‌فورس ساده می‌توانند در اختیار مهاجمان قرار گیرند."

منبع خبر :

https://thehackernews.com/2020/04/backdoor-.html

Scan Link

[1] binary
[2] screen capturing
[3] Distributed Denial-of-Service (DDoS)

اخبار کوتاه

افشای اطلاعات ۴۲ میلیون کاربر ایرانی تلگرام، توسط یک نسخه غیر رسمی تلگرام

اطلاعات 42 میلیون کاربر ایرانی تلگرام افشا شده است. این اطلاعات اکنون در سطح اینترنت با 500 دلار فروخته می‌شود و منبع آن، نه خود تلگرام، بلکه یکی از نسخه‌های غیر رسمی این اپلیکیشن ذکر شده است. باب دیاچنکو، پژوهشگر امنیت سایبری که این دیتابیس را در سطح وب کشف کرده، اعلام می‌کند که داده‌های دیتابیس شامل اطلاعات بیشتر از 42 میلیون کاربر ایرانی تلگرام، مانند آی‌دی تلگرام، نام کاربری، شماره تماس، هش‌ها و کلیدهای دیجیتالی می‌شود. این گزارش می‌گوید اطلاعات توسط گروهی به نام «سامانه شکار» و ظاهرا به شکل ناخواسته منتشر شده است. پس از دانلود دیتابیس هم هیچ رمز عبوری برای استفاده از آن نیاز نبوده است. سخنگوی تلگرام در گفتگو با وب‌سایت Comparitech اعلام کرده است که داده‌ها مربوط به یک نسخه غیر رسمی از تلگرام است؛ نسخه‌ای که هیچ ارتباط مستقیمی با این کمپانی ندارد.

تلگرام یک اپلیکیشن متن-باز است که به سایر اپلیکیش‌ها اجازه می‌دهد نسخه‌ای با ویژگی‌های مورد نظر خود را بر بستر هسته‌ی اصلی تلگرام بسازند. از آنجایی که تلگرام در اردیبهشت 97 در ایران فیلتر شد، بسیاری از کاربران برای ادامه‌ی استفاده از این پیام‌رسان و ارتباط با آشنایان خود از نسخه‌های غیر رسمی در ایران استفاده کردند که به شکل غیرقابل باور و پر هزینه‌ای قادر بودند فیلترینگ تلگرام را دور بزنند.

مرکز ماهر درباره معرفی دیتابیس‌های حفاظت نشده به مراجع قضایی هشدار داد

مرکز ماهر خطاب به کلیه دستگاه‌های دولتی و حاکمیتی و همچنین صاحبان کسب‌وکارها بیانیه‌ای را در خصوص افشای گسترده اطلاعات کاربران منتشر کرده است. این مرکز با «تاسف بار» خواندن ادامه‌ی درز گسترده اطلاعات، اعلام می‌کند که این موضوع، نقض حریم خصوصی کاربران و شهروندان است و می‌تواند تهدیدهای مختلفی را برای آن‌ها به وجود بیاورد. مرکز ماهر در همین راستا اعلام می‌کند که از تاریخ 12 فروردین، فراتر از وظایف خود، پایش بانک‌های اطلاعاتی را آغاز کرده و در صورت یافتن ضعف، به صورت خصوصی یا عمومی در رابطه با آن‌ها هشدار خواهد داد. پس از 48 ساعت در صورت بی‌توجهی به هشدارهای اعلام شده، این موارد به دلیل به خطر انداختن امنیت شهروندان به مراجع قضایی معرفی می‌شوند. مرکز ماهر اعلام می‌کند که منشا مشترک اتفاقات اخیر، وجود بانک‌های اطلاعات کاملا حفاظت نشده یا دارای حفاظت خیلی ضعیف در سطح اینترنت است که باعث می‌شود افراد سوءاستفاده‌گر بتوانند به راحتی به این بانک‌ها دسترسی پیدا کرده و باعث بروز مشکلات جدی برای مردم و کسب و کارها شوند. مرکز ماهر در پایان بیانیه‌اش ابراز امیدواری کرده است که صاحبان بانک‌های اطلاعاتی که داده‌ها و اطلاعات شخصی مردم به صورت امانت در اختیار آنها است نسبت به حفظ این امانت و حریم خصوصی شهروندان هم بر اساس قانون و هم بر اساس مسئولیت اجتماعی، حساسیت لازم را داشته باشند و در این راه هشدارهای اعلام‌شده را جدی تلقی نمایند.

آسیب پذیری

رفع دو آسیب‌پذیری روز صفرم در مرورگر فایرفاکس

موزیلا با انتشار Firefox 74.0.1 و Firefox ESR 68.6.1 دو آسیب‌پذیری حیاتی روز صفرم را که به طور گسترده مورد اکسپلویت قرار گرفته بود، وصله کرد.

هر دو آسیب‌پذیری توسط محققان امنیتی به نام‌های Francisco Alonso و Javier Marcos به عنوان آسیب‌پذیری‌های روز صفرم گزارش شده‌اند.

این آسیب‌پذیری‌های بحرانی اجرای کد از راه دور[1]، در سیستم‌هایی که نسخه Firefox 74.0.0 و قبل تر را در حال اجرا دارند مورد حمله و اکسپلویت قرار گرفته‌اند.

هکرها با اکسپلویت این آسیب‌پذیری‌ها، اقدام به از کار انداختن Firefox در حال اجرا در سیستم‌عامل‌های ویندوز، مک و لینوکس می‌کنند.

آسیب‌پذیری اول با شناسه "CVE-2020-6819" یک آسیب‌پذیری Use after free است که به هکرها اجازه می‌دهد تا از راه دور یک هسته دلخواه[2] را اجرا کنند و سیستم مورد هدف را از کار بیندازند.

دومین آسیب‌پذیری با شناسه "CVE-2020-6820" می‌تواند هنگام مدیریت یک ReadableStream مورد اکسپلویت قرار گیرد.

هر دو آسیب‌پذیری مذکور، هکرها را قادر می‌سازند تا کد دلخواه خود را اجرا کنند و بسته به امتیازات مربوط به کاربر، اقدام به نصب برنامه کنند، داده‌ها را مشاهده و حذف کرده و یا تغییر دهند و حساب‌های کاربری جدیدی با تمام حقوق کاربری ایجاد کنند.

به تمام کاربران فایرفاکس توصیه می‌شود بروزرسانی‌های ارائه شده توسط موزیلا را در سیستم‌های آسیب‌پذیر اعمال نمایند و همچنین از بازدید از وب‌سایت‌های نامطئن و پیوندهایی که منابع ناشناس دارند اجتناب کنند.

منبع خبر :

https://gbhackers.com/firefox-74-0-1-fixes-2-zero-day-bugs/

Scan Link

[1] remote code execution

[2] arbitrary core

آسیب‌پذیری بحرانی اجرای کد از راه دور در سیستم عامل مبتنی بر لینوکس OpenWrt

محققان امنیتی از یک آسیب‌پذیری بحرانی اجرای کد از راه دور (remote code execution) در سیستم عامل مبتنی بر لینوکس OpenWrt پرده برداشتند که به مهاجمان اجازه می‌دهد تا پی‌لود[1] مخرب را در سیستم‌عامل‌های آسیب پذیر تزریق کنند.

OpenWrt یک سیستم‌عامل مبتنی بر لینوکس است که عمدتا در دستگاه‌ها و روترهای شبکه برای مسیریابی ترافیک شبکه مورد استفاده قرار می‌گیرد و بر روی میلیون‌ها دستگاه در سراسر جهان نصب شده است.

این آسیب‌پذیری در تجزیه لیست پکیج‌های opkg سیستم‌عامل OpenWrt (Opkg Package Manage) به مدیر بسته اجازه می‌دهد تا SHA-256 checksums تعبیه شده در شاخص repository امضا شده را نادیده بگیرد و به دنبال آن، مهاجم می‌تواند بررسی صحت و درستی ipk artifacts. دانلود شده را دور بزند.

محققی به نام GuidoVranken توضیح داد که هنگام آماده‌سازی یک تسک Mayhem برای opkg، این آسیب‌پذیری را به طور اتفاقی کشف کرده است. Mayhem می‌تواند داده‌ها را از طریق یک فایل یا از طریق یک سوکت شبکه ارائه دهد.

فرآیند اکسپلویت آسیب‌پذیری RCE در OpenWRT

برای اکسپلویت آسیب‌پذیری ذکر شده، مهاجم به ارائه پکیج‌های ناقص از وب سرور نیاز دارد. او همچنین به رهگیری ارتباط بین دستگاه و downloads.openwrt.org و یا کنترل سرور DNS ای که توسط دستگاه برای ساخت downloads.openwrt.org برای یک وب سرور کنترل شده توسط مهاجم استفاده می‌شود، نیاز دارد.

در حقیقت، opkg در OpenWrt به صورت root اجرا می‌شود که امکان نوشتن در تمام سیستم‌فایل‌ها و تزریق از راه دور کد دلخواه با پکیج‌های .ipk ساختگی با یک پی‌لود مخرب را به مهاجمان می‌دهد.

به آسیب‌پذیری مذکور شناسه " CVE-2020-7982 " اختصاص داده شده است و در حال حاضر در آخرین نسخه OpenWrt وصله شده و در اختیار کاربران قرار گرفته است.

نحوه بروزرسانی:

با استفاده از دستورات زیر می‌توان تمام repositoryها را بروزرسانی کرد.

```
cd /tmp
opkg update
opkg download opkg
zcat ./opkg-lists/openwrt_base | grep -A10 "Package: opkg" | grep SHA256sum
sha256sum ./opkg_2020-01-25-c09fe209-1_*.ipk
```

منبع خبر :

https://gbhackers.com/severe-rce-vulnerability-in-openwrt/

آخرین بروزرسانی آسیب‌پذیری DoS در پروتکل SNMP نرم‌افزار NX-OS سیسکو


Cisco Security Advisory

Cisco NX-OS Software Authenticated Simple Network Ma
Denial of Service Vulnerability

High

Advisory ID:	cisco-sa-20180620-nxossnmp	CVE-2018-0291	Download CVRF
First Published:	2018 June 20 16:00 GMT	CWE-20	Download PDF
Last Updated:	2020 March 27 19:00 GMT		Email
Version 1.4:	Final		
Workarounds:	No workarounds available		
Cisco Bug IDs:	CSCuw99630		
	CSCvg71290		
	CSCvj67977		
CVSS Score:	Base 7.7		

آخرین و جدیدترین بروزرسانی مربوط به یک آسیب‌پذیری با شناسه CVE-2018-0291 و شدت بالا در پردازنده پکت ورودی SNMP(Simple Network Management Protocol) مربوط به نرم‌افزار NX-OS سیسکو در تاریخ 27 مارس 2020 منتشر شد. در این آسیب‌پذیری یک مهاجم تایید هویت شده می‌تواند از راه دور و به صورت غیرمنتظره موجب ری‌استارت شدن برنامه SNMP بر روی یک دستگاه آسیب‌دیده شود.

پروتکل SNMP، یک پروتکل لایه برنامه است که یک چارچوب استاندارد و یک زبان مشترک برای نظارت و مدیریت دستگاه‌های شبکه فراهم می‌کند. این پروتکل یک قالب پیام برای ارتباط بین مدیران SNMP و ایجنت‌ها (agents) تعریف می‌کند.

این آسیب‌پذیری به دلیل اعتبارسنجی نادرست واحدهای داده‌ی پروتکل SNMP در پکت‌های SNMP اتفاق می‌افتد. مهاجم می‌تواند با ارسال یک بسته جعلی SNMP به یک دستگاه آسیب‌دیده، از این آسیب‌پذیری بهره‌برداری نماید. یک اکسپلویت موفقیت‌آمیز به مهاجم اجازه می‌دهد تا برنامه SNMP را چندین مرتبه ری‌استارت کرده و منجر به راه‌اندازی مجدد در سطح سیستم و اجرای حمله DoS شود.

در حال حاضر هیچ راه‌حلی برای رفع این آسیب‌پذیری ارائه نشده است اما سیسکو بروزرسانی‌های نرم‌افزاری را منتشر کرده است.

محصولات نام برده در زیر، در صورتیکه دارای نسخه آسیب‌پذیر نرم‌افزار NX-OS باشند، تحت تاثیر این آسیب‌پذیری قرار می‌گیرند:

- Nexus 2000 Series Switches
- Nexus 3000 Series Switches

[1] payload

- Nexus 3500 Platform Switches
- Nexus 3600 Platform Switches
- Nexus 5500 Platform Switches
- Nexus 5600 Platform Switches
- Nexus 6000 Series Switches
- Nexus 7000 Series Switches
- Nexus 7700 Series Switches
- Nexus 9000 Series Switches in standalone NX-OS mode
- Nexus 9500 R-Series Line Cards and Fabric Modules
- UCS 6100 Series Fabric Interconnects
- UCS 6200 Series Fabric Interconnects
- UCS 6300 Series Fabric Interconnects

سیسکو تایید کرده است که این آسیب‌پذیری بر روی محصولات زیر تاثیر نمی‌گذارد:

- Firepower 2100 Series
- Firepower 4100 Series Next-Generation Firewall
- Firepower 9300 Security Appliance
- MDS 9000 Series Multilayer Switches
- Nexus 1000V Series Switches
- Nexus 1100 Series Cloud Services Platforms
- Nexus 9000 Series Fabric Switches in Application Centric Infrastructure (ACI) mode

با توجه به اینکه سوئیچ‌های سری Nexus 4000 سیسکو و Nexus 5010 یا Nexus 5020 به پایان عمر خود رسیده‌اند بنابراین شرکت سیسکو در مورد اینکه آیا این سوئیچ‌ها تحت تاثیر آسیب‌پذیری مذکور قرار می‌گیرند یا خیر، هیچ بررسی و تحقیقی به عمل نیاورده است.

این آسیب‌پذیری تمام نسخه‌های SNMP (نسخه‌های1 ، 2c و 3) را تحت تاثیر قرار می‌دهد و مهاجم می‌تواند با راسال یک پکت خاص SNMP به دستگاه آسیب‌پذیر از طریق پروتکل IPv4 یا IPv6، آسیب‌پذیری ذکر شده را مورد اکسپلویت قرار دهد. لازم به ذکر است که تنها از طریق ترافیک هدایت شده به سیستم آسیب‌دیده می‌توان این آسیب‌پذیری را اکسپلویت کرد.

برای اکسپلویت این آسیب‌پذیری از طریق نسخه 2c یا قبل تر SNMP، مهاجم باید از رشته جامع فقط خواندنی SNMP برای سیستم آسیب‌دیده اطلاع داشته باشد. این رشته رمز عبوری است که برای محدود کردن دسترسی‌های read-only و read-write به داده‌های SNMP روی دستگاه اعمال می‌شود. این رشته‌ها مانند تمام رمزهای عبور، باید با دقت انتخاب شوند تا از بی اهمیت نبودن آنها اطمینان حاصل شود. همچنین آنها باید در فواصل منظم و مطابق با سیاست‌های امنیتی شبکه، تغییر کنند. به عنوان مثال زمانیکه مدیر شبکه نقش‌ها را تغییر می‌دهد یا اینکه سازمان را ترک می‌کند.

برای اکسپلویت در نسخه SNMP 3، مهاجم باید دارای اعتبار کاربر در سیستم آسیب‌دیده باشد.

راه‌حل

در حال حاضر راه حلی برای رفع این آسیب‌پذیری ارائه نشده است اما به عنوان یک راه حل پیشگیرانه، مدیران می‌توانند یک لیست کنترل دسترسی (ACL) را بر روی یک SNMP پیکربندی کنند تا درخواست‌های دریافتی SNMP را فیلتر کرده تا اطمینان حاصل شود که نمونه‌برداری SNMP تنها توسط کلاینت‌های قابل اعتماد انجام می‌شود.

برای مشاهده بروزرسانی‌های نرم‌افزاری منتشر شده توسط شرکت سیسکو می‌توانید به لینک زیر مراجعه نمایید.

منبع خبر :

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180620-nxossnmp

Scan Link

انتشار به‌روزرسانی‌های امنیتی برای چندین محصول VMware

VMware سه آسیب‌پذیری جدی در محصولات خود از جمله یک نقص مهم در Workstation و Fusion را که می‌تواند برای اجرای کد دلخواه از سیستم‌عامل مهمان بر روی میزبان مورد سوءاستفاده قرار بگیرد، برطرف کرد.

اولین نقص مهم، با شناسه‌ی "CVE-2020-3947" ردیابی می‌شود و در نتیجه‌ی یک اشکال سوءاستفاده پس از آزادسازی در مؤلفه‌ی "vmnetdhcp" ایجاد می‌شود.

سوءاستفاده‌ی موفقیت‌آمیز از این مسئله ممکن است منجر به اجرای کد بر روی میزبان از مهمان شود یا ممکن است به مهاجمان اجازه دهد تا شرایط انکار سرویس "vmnetdhcp" را در دستگاه میزبان، ایجاد کنند.

یکی دیگر از آسیب‌پذیری‌های وصله‌شده، نقصی با شناسه‌ی "CVE-2020-3948" است. این نقص یک مسئله با شدت بالا است که به مهاجمین محلی اجازه‌ی دسترسی به یک ماشین مجازی مهمان لینوکس (VM) با ابزارهای VMware نصب شده، می‌دهد تا بتوانند امتیازات خود را افزایش دهند.

VMهای مهمان لینوکس که در VMware Workstation و Fusion کار می‌کنند، دارای آسیب‌پذیری محلی هستند که به دلیل مجوز پرونده در Cortado Thinprint، افزایش یافته است.

سوءاستفاده از این نقص فقط درصورتی امکان‌پذیر است که چاپ مجازی در مهمان VM فعال شود. (چاپ مجازی به‌طور پیش فرض در Workstation و Fusion فعـــال نمی‌شود)

هر دو ضعف بر Workstation نسخه‌ی x.15 بر روی هر سیستم‌عامل و Fusion نسخه‌ی x.11 در macOS تأثیر می‌گذارند. وصله‌ها به ترتیب شامل نسخه‌های 15.5.2 و 11.5.2 هستند.

آخرین آسیب‌پذیری که به‌عنوان "CVE-2019-5543" ردیابی شده است، یک مسئله‌ی افزایش امتیاز با شدت بالا است که بر Workstation، VMware Horizon Client و کنسول از راه دور (VMRC) در ویندوز تأثیر می‌گذارد.

این حفره‌ی امنیتی به یک مهاجم محلی اجازه می‌دهد تا مانند هر کاربری دستوراتی را اجرا کند. دلیل وجود این آسیب‌پذیری این است که پوشه‌ی حاوی پرونده‌های پیکربندی‌شده برای سرویس داوری USB VMware توسط همه‌ی کاربران قابل نوشتن است.

وصله‌هـــای ایـن نقص در نسخه‌ی 15.5.2 بـــرای Workstation، 5.3.0 برای VMware Horizon Client و نسخه‌ی 11.0.0 در VMRC برای ویندوز گنجانده شده‌اند.

به کـــاربران و مدیران توصیه می‌شود بـــا تـــوجه به محصول مـورد استفـــاده‌ی خـود، به‌روزرسانی‌های لازم را اعمال کنند.

منبع خبر :

https://cert.ir/news/12967

Scan Link

اخبار کوتاه

آپدیت جدید ویندوز ۱۰ سیستم کاربران را حین بـــازی از کار می‌اندازد

یکی از آپدیت های جدید ویندوز 10 موجب از کار افتادن کامپیوتر کاربران حین بازی یا تماشای ویدیو می شود. به نظر می رسد مایکروسافت هنوز تلاشی برای رفع مشکل نکرده است. آپدیتی که مقصر این اتفاق است با کد KB4541335 شناخته مـی شود و در روز 5 فروردین و به عنوان یک به روز رسانی اختیاری ارائه شده و هدف آن رفع برخـــی از باگ های ویندوز 10 نسخه 1909 و 1903 بوده است. با وجود این که به نظر می رسد بیشتر کاربران با نصب این آپدیت مشکلی نداشته اند اما برخی به مشکلاتی از جمله هنگ کردن سیستم در زمان بازی اشاره کرده اند. برخی دیگر هم گفته اند که حین مشاهده ویدیو در یوتیـــوب بـــا مشکـــل صفحـه آبی مـــرگ (بـــلو اسکـرین) و پیغـــام whea_uncorrectable_error مواجه شده اند. همچنین تعدادی دیگر از کند شدن کامپیوتر در زمان شارژ شدن لپتاپ و استفاده بالا از پردازنده گفته اند و مدعی شده اند که بخش هایی از رابط کاربری ویندوز 10 هم هنگ کرده است. خوشبختانه از آنجایی که نصب آپدیت KB4541335 اختیاری است مشکل چندانی را برای بسیاری از کاربران ایجاد نمی کند و مـــی توان نصب آن را نادیده گرفت. اگر شما هـــم با این مشکلات مواجه شده‌اید کافی است آپدیت را به طریق زیر حذف کنید: از طریق منوی استارت به بخش Settings بروید، سپس به بخش Update & security بروید، در پنجره‌ای که باز می‌شود روی Windows Update از منوی سمت چپ کلیک کنید، روی View update history و سپس روی Uninstall updates کلیک کنید، در پنجره جدید، آپدیت KB4541335 را یافته و با کلیک راست گزینه Uninstall را بزنید. با طی کردن مراحل بالا انتظار می‌رود مشکل مرتبط با آپدیت KB4541335 رفع شود.

دسترسی هکرها به وبکم تمام محصولات اپل از طریق مرورگر سافاری

اپل همواره به عنوان شرکتی شناخته می‌شود که نگاهی ویژه به امنیت کاربران خود دارد. با این حال این کمپانی در طول سالیان گذشته با امنیت مرورگر سافاری مشکلاتی داشته است. اخیرا یک محقق حوزه امنیت توانسته باگی در این مرورگر پیدا کند که به هکرها اجازه می‌دهد به دوربین سلفی یا وبکم و میکروفون دستگاه‌های کاربران دسترسی داشته باشند. این محقق که رایان پیکرن (Ryan Pickren) نام دارد، پیش از عمومی کردن این حفره امنیتی، ابتدا آن را با اپل در میان گذاشته است. این کمپانی نیز بلافاصله و یک روز بعد از مطلع شدن از این باگ، آن را تایید کرده و پچ مورد نیاز برای برطرف کردن آن را همراه با آپدیت‌های ماه ژانویه و مارس 2020 منتشر کرده است. با این حال تنها کاری که یک فرد برای هک شدن دستگاه‌های خود باید انجام می‌داد، کلیک روی یک لینک آلوده بود. این کار به کمک دسترسی‌های مجاز وب سایت شناخته شده صورت می‌گیرد و هکرها به نوعی از این دسترسی‌ها سوءاستفاده می‌کنند. در بدترین حالت، یک هکر می‌تواند محتوای نمایش داده شده برای شما را با دیگران به اشتراک بگذارد.

ربوده شدن ترافیک اینترنتی گوگل، آمازون و چند شرکت دیگر توسط اپراتور روسی

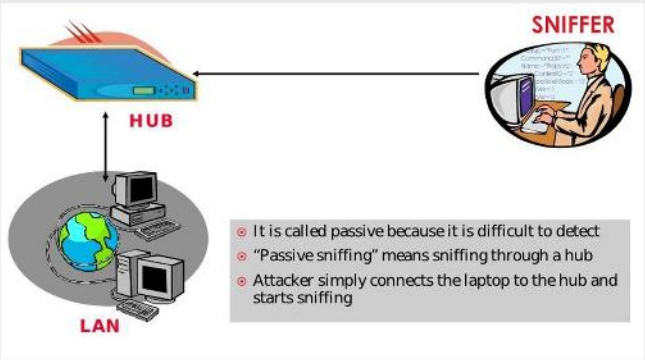
اوایل هفته جاری ترافیک بیش از 200 شبکه تحویل محتوای بزرگ دنیا (CDN) و ارائه دهندگـــان میزبانی ابری، به طرز مشکوکی به شرکـــت مخابـــراتی روس تلکام (Rostelecom) هدایت شد. این اپراتور که به دولت روسیه وابسته است، در گذشته ترافیک اینترنت برخی شرکت‌ها را ربوده و متخصصین آن را مشکوک قلمداد کرده‌اند.

این حادثه بالـــغ بر 8800 مسیر ترافیک اینترنت در بیش از 200 شبکه را تحت تـاثیر قرار داده و شرکت‌های فعال در بازار CDN از جمله گوگل، آمازون، فیسبوک و شرکت‌های دیگری در آن دخیل بوده‌اند.

این حادثه، ربودن پروتکل اینترنت (BGP Hijack) نامیده شده و هکرها می توانند به وسیله آن ترافیک اینترنت را ذخیره کرده و بعداً تحلیل و رمزگشایی کنند. ربودن پروتکل اینترنت از اواسط دهه 90 میلادی به یکی از معضلات اینترنت تبدیل شد و محققان در طول چند سال گذشته با پروژه‌های مختلف به دنبال تقویت امنیت پروتکل‌هـــای BGP بوده‌اند. البته بکارگیری پروتکل‌های جدید به کندی صورت گرفته و ربوده شدن مسیرهای اینترنت همچنان به طور مرتب رخ می‌دهند.

مقالات آموزشی

Sniffer چیست؟



Sniffer چیست؟

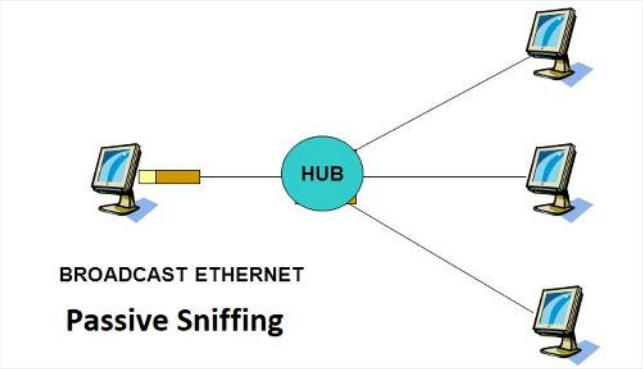
اسنیفر برنامه یا ابزاری است برای استراق سمع کردن ترافیک شبکه آن هم بوسیله گرفتن اطلاعاتی که روی شبکه در حال تبادل هستند، که در این روش از تکنولوژی جلوگیری اطلاعاتی استفاده می‌شود. مکانیزم انجام این کار به این صورت است که اترنت بر مبنای اشتراک گذاری ساخته شده است و بیشتر شبکه از تکنولوژی broadcast استفـــاده می‌کنند که ارسال یک پیام به یک کامپیوتر می‌تواند توسط کامپیوترهای دیگر هم خوانده شود. به صورت معمولی کلیه کامپیوترها بجز کامپیوتری که مقصد پیام هست پیام را نادیده می‌گیرند. اما این امکان وجود دارد روشی به کاربرد که کامپیوتر پیامی هم که به آن مربوط نیست را بخوانند. این روش همان اسنیف کردن اطلاعات می‌باشد. بسیاری از افرادی که توسط سوئیچ به شبکه وصل هستند از خطر اسنیف در امان هستند. اما همین کامپیوترها نسبت به اسنیف کردن هم نقطه ضعف خواهند داشت در صورتی که سوئیچ به یک هاب وصل شده باشد.

Passive Sniffing چیست ؟

همان‌طورکه در بخش فوق توضیح داده شد یکی از روش‌های بدست آوردن اطلاعات از جمله پسوردها و اطلاعات احراز هویتی در شبکه شنود کردن یا Sniff کردن شبکه است ابزارهای زیادی برای Sniff کردن شبکه وجود دارند که ما آن‌ها را به عنوان Packet Sniffer می‌شناسیم اما اینگونه ابزارها به ندرت در شبکه‌ها برای هک مورد استفاده قرار می‌گیرند و شاید این موضوع برای شما جالب باشد. این محدودیتی است که در ساختار Switchها و روترها در شبکه وجود دارد ، بر اساس قوانین شنود ، شما به عنوان یک Sniffer صرفاً می‌توانید در Collision Domainای که در آن هستید Packet ها را شنود کنید و از داده‌هایی که در سایر Collision Domain ها دیگر وجود دارند بی اطلاع خواهید بود. با توجه به اینکه نرم افزارهای Sniffer در لایه پیوند داده یا Data-Link فعالیت می‌کنند می‌توانند کلیه Frameهایی که در یک شبکه LAN رد و بدل می‌شود و البته سیستم‌هایی که بر روی آن‌ها نرم افزار Sniffer وجود دارد را در اصطلاح شنود یا Capture کنند. نرم افزارهای شنود یا Snifferها کارت شبکه شما را از حـــــالت Promiscuous یا بی قید خارج می‌کنند و همه نوع Packet ای را دریافت می‌کنند و

هیچ Packetای Drop نمی‌شود.

در حملات Passive Sniffing مهاجم بر روی کلیه کامپیوترهای یک شبکه LAN نرم افزار شنود نصب می‌کند که از نظر ساختاری بسیار پیچیده است و هم تقریبا کمتر کسی این روزها امکان شنود به این روش را دارد. قبلا با توجه به مکانیزم کاری که در HUBها وجود داشت و داده‌ها در کلیه پورت‌ها ارسال می‌شدند نرم افزار Sniffer هم می‌توانست داده‌های کل شبکه LAN را به یکباره شنود کند اما این روزها که دیگر از HUB استفاده نمی‌شود. شنود به راحتی صورت نمی‌گردد.



اگر بحث سال‌های دور را داشته باشیم ، این نوع Sniff کردن شبکه را Passive Sniffing می‌نامند چون هکر نیازی به انجام هیچ کاری برای دریافت اطلاعات از شبکه ندارد. ابزارهای Sniffing براحتی اطلاعات مورد نیازشان را در این محیط به دست می آوردند. این نوع شنود در شبکه های وایرلس هم کاربرد دارد و وقتی صحبت از Passive Sniffing در شبکه‌های وایرلس می‌شود یعنی اینکه ما صرفاً با یک کارت شبکه وایرلس نرم افزار شنود را اجرا می‌کنیم و منتظر می‌شویم که Packet ای به ما برسد تا آن را Capture کنیم. همانطور که می‌دانید درحال حاضر رسماً Passive Sniffing در شبکه‌های کابلی منسوخ شده است اما در شبکه های وایرلس همچنان قابل استفاده است. نکته مهمی که در Passive Sniffing وجود دارد این است که کسی متوجه حضور مهاجم نمی‌شود. اگر کسی موفق به Passive Sniffing شود اطلاعات بسیار زیادی را می‌تواند به دست بیاورد که از آن جمله می‌توانیم به پسوردها و نام‌های کاربری و غیره اشاره کنیم. قابل ذکر است این نوع حملات این روزها صرفا بر روی شبکه‌های وایرلس و بصورت بسیار کند قابل اجرا هستند.

Active Sniffing چیست ؟

در خصوص مکانیزم Passive Sniffing صحبت کردیم و به معایب این روش را اشاره کردیم اما مزیت بزرگ Passive Sniffing برای هکرها ناشناس ماندن مهاجم است. در ادامه می‌خواهیم در خصوص Active Sniffing صحبت کنیم. زمانیکه صحبت از یک فعالیت Active در شبکه می‌شود یعنی شما ارتباطی مستقیم با سیستم هدف برقرار می‌کنید و طبیعتاً قابل شناسایی‌تر خواهد بود. اگر فرض کنیم در شبکه‌ای که دارای Switch است مهاجم قصد شنود داشته باشد رسماً Passive Sniffing کاربردی ندارد پس بنابراین Switch را در اصطلاح فنی Overflow می‌کند یعنی آنقدر ترافیک برای سویچ ارسال می‌کند که سویچ قادر به مدیریت آن نباشد و در اصطلاح Overflow یا سرریز می‌شود. در این حالت نرم افزارهای شنود قادر هستند تعداد بسیار زیادی MAC Address جعلی را به سمت سویچ ارسال کنند و جدول آدرس MAC یا MAC Table را سرریز می‌کند و با سرریز شدن این جدول سویچ فرد قربانی تبدیل به یک HUB می‌شود و ترافیک را بر روی تمامی پورت‌های خود ارسال می‌کند و متاسفانه فرآیند شنود مهاجم کامل می‌شود. طبیعی است که با توجه به ایجاد شدن ترافیک بسیار زیاد احتمال شناسایی هکر بسیار زیاد است. اما همین مکانیزم برای شبکه‌های وایرلس نیز صادق است ، در Passive Wireless Sniff شما منتظر هستید که Access Point برای سیستم شما یک بسته ارسال کند که ممکن است مدت‌ها زمان ببرد، در Active Wireless Sniffing بصورت جعلی برای Access Point درخواست‌های زیادی ارسال شده تا مجبور به پاسخگویی و در نتیجه امکان شنود آن شود. این روزها وقتی صحبت از شنود در شبکه می‌شود منظور ما Active Sniffing است.

راه های مقابله با Sniffing

- محدود کردن دسترسی فیزیکی به شبکه و مطمئن شدن از اینکه packet sniffer نمی‌تواند نصب شود
- استفاده از مک آدرس‌های static و اضافه کردن آن‌ها به ARP table و همچنین استفاده از ip static
- استفاده از PGP,S/MIPE,VPN,IPSec,SSL/TLS و همچنین استفاده از پسوردهای یکبار مصرف
- استفاده از پروتکل‌های امن برقراری session مثل ssh و secure copy(SCP) و غیره
- استفاده از پروتکل‌های رمزنگاری قوی در شبکه های وایرلس نظیر wpa2 و wpa3
- اضافه کردن مک آدرس gateway شبکه به ARP table به صورت استاتیک
- استفاده از ابزارهایی که promiscuous mode را تشخیص می‌دهند.
- استفاده از رمزنگاری برای محافظت از اطلاعات
- استفاده از Switch به جای HUB
- استفاده از SFTP به جای FTP
- استفاده از IPv6به جای IPv4
- استفاده از پروتکل https بجای http

منبع خبر :

https://security.tosinso.com

Scan Link

امنیت کاربر رایانه

مهندسی اجتماعی و سرقت هویت

مهندسی اجتماعی یک متد غیر فنی نفوذ به یک سیستم یا یک شبکه است. این کار در واقع فریب دادن کاربران یک سیستم و متقاعد کردن آنها به انجام کارهای پرفایده برای هکر است. مانند گرفتن اطلاعاتی از آنها که بتوان در شکستن یا دور زدن مکانیزم امنیتی استفاده کرد. درک مفهوم مهندسی اجتماعی مهم است زیرا هکرها می‌توانند با استفاده از آن به عنصر انسانی یک سیستم حمله کرده و معیارهای فنی امنیتی را دور بزنند. این متد را می توان در جمع آوری اطلاعات قبل یا طی یک حمله استفاده کرد.

حال با توجه به اهمیت این موضوع، در این شماره از بولتن خبری و در فصل " مهندسی اجتماعی و سرقت هویت " به بیان مفهوم و روش‌های آن می‌پردازیم.

با ما همراه باشید...

سرقت هویت چیست؟

سرقت هویت یا جعل شناسه، اشاره به جرمی دارد که در آن، هکر با استفاده از اطلاعات شناسایی فردی مانند: تاریخ تولد، شماره شناسنامه یا کد ملی، شماره گواهینامه رانندگی و غیره، از هویت شخص قربانی سوء استفاده کند

هکرها با هویت سرقت شده چه می کنند؟

هکرها با هویت سرقت شده چه می کنند؟

نمونه ای از سرقت هویت

کارت اصلی

سرقت هویت

هکر عکس خود را به جای عکس صاحب اصلی کارت قرار داده است

مهندسی اجتماعی


مثال هایی از مهندسی اجتماعی
سلام، ما از شرکت نرم افزاری CONSESCOهستیم.
ما به دنبال استخدام افراد جدید برای تیم برنامه نویسی
خود هستیم
شماره تماس شما را از پورتال های مشاغل محبوب
بدست آوردیم
لطفاً جزئیات و مشخصات شغل خود، اطلاعات پروژه
فعلی و آدرس محل سکونت خود را اعلام کنید


هکر به عنوان کارمند بانک با مشتری تماس می گیرد
سلام، من از طرف بانک با شما تماس می
گیرم
با توجه به افزایش تهدیدات، ما تصمیم
گرفتیم که سیستم امنیتی بانک را با
قابلیت های ایمنی بیشتری به روز کنیم.
لطفا اطلاعات شخصی خود را بیان کنید
که ما مطمئن شویم شما صاحب اصلی
حساب هستید

مثال پشتیبانی فنی

مهندسی اجتماعی مبتنی بر اشخاص

مهندسی اجتماعی مبتنی بر کامپیوتر

Hoax ایمیل هایی هستند که هشدارهایی را مبنی بر وجود ویروس ها یا تروجان های جدید در سیستم به کاربران ارسال می کنند

جمع آوری **اطلاعات شخصی** از طریق چت کردن با کاربران آنلاین به منظور به دست آوردن اطلاعات شخصی نظیر تاریخ تولد آن ها و غیره انجام می شود

pop up های ویندوز:هنگامی که کاربران در حال جستجو در اینترنت هستند ناگهان این پیام ها ظاهر می شوند و اطلاعات کاربران را برای ورود به سایت یا حساب ایمیل آن ها می پرسند

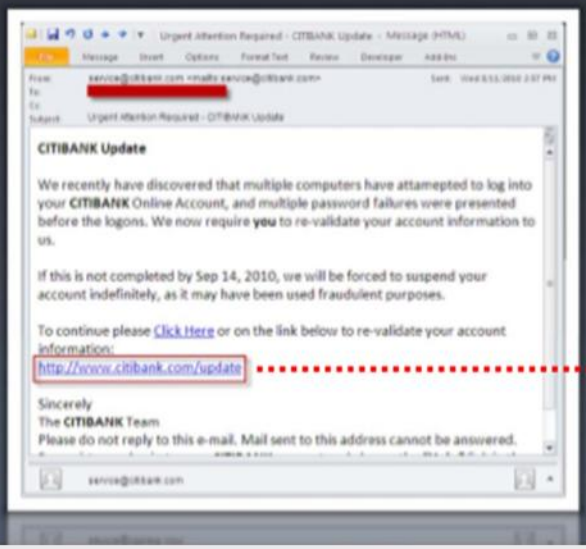
نامه های زنجیره ای ایمیل هایی هستند که هدایای رایگان مانند پول و نرم افزار را ارائه می دهند با این شرط که کاربر باید ایمیل را به تعداد افراد ذکر شده ارسال کند

ایمیل های غیر ضروری، نامطلوب و ناخواسته که برای جمع آوری اطلاعات کاربران مانند اطلاعات مالی، اطلاعات شبکه و غیره ارسال می شوند

مهندسی اجتماعی مبتنی بر کامپیوتر:

فیشینگ (Phishing)

- یک **ایمیل غیرقانونی** که **ادعا می کند** از یک سایت قانونی است،و تلاش می کند اطلاعات شخصی یا حساب کاربر را بدست آورد
- **ایمیل های فیشینگ** یا pup up ها کاربران را به صفحات وب جعلی،مشابه سایت های قابل اعتماد هدایت می کنند و از آنها می خواهند اطلاعات شخصی خود را ارائه دهند



هشدارهای امنیتی جعلی

- هشدار دهنده های امنیتی جعلی، ایمیل ها یا پنجره های پاپ آپ هستند که به نظر می رسد از یک سخت افزار مشهور یا یک تولید کننده مشهور نرم افزار مانند مایکروسافت و غیره باشد
- یک هشدار به کاربر نشان می دهد مبنی بر این که سیستم آلوده شده است و سپس یک فایل پیوست یا یک لینک برای پچ کردن سیستم ارائه می دهد
- Scammer ها دانلود پچ ها را به کاربران پیشنهاد می کنند
- تله، فایلی حاوی برنامه های مخرب است که ممکن است سیستم کاربر را آلوده کند

مهندسی اجتماعی مبتنی بر کامپیوتر از طریق وب سایت های شبکه های اجتماعی

مهندسی اجتماعی مبتنی بر کامپیوتر از طریق وب سایت های شبکه های اجتماعی مانند Orkut, Facebook, MySpace, LinkedIn, Twitter و غیره انجام می شود

هکرها از وب سایت های شبکه های اجتماعی، برای بهره برداری از اطلاعات کاربران استفاده می کنند .


مرکز تخصصی آپا دانشگاه رازی