بولتن خبری

مرکز تخصصی آپا دانشگاه رازی

شماره چهاردهم

آبان ماه ۱۳۹۸

وای به روزی که بگندد نمک...

(آسیب‌پذیری امنیتی در McAfee)

McAfee™

در این شماره می‌خوانید :

فهرست

صاحب امتیاز:

مرکز تخصصی آپا دانشگاه رازی

صفحه آرایی: **سید احسان حسینی**

سردبیران:

سیده مرضیه حسینی

صبا آزرمی

با همکاری **سیده آرزو حسنی**

آدرس:

کرمانشاه، باغ ابریشم، دانشگاه رازی، دانشکده برق و کامپیوتر، طبقه همکف، مرکز تخصصی آپا

apa@razi.ac.ir

cert.razi.ac.ir

۰۸۳۳۴۳۴۳۲۵۱

اخبار امنیتی

انتشـــار وصله امنیتی مایکروســـافت در پی حملات BlueKeep RDP و استقرار بدافزار CoinMiner

گردآورنده: سیده مرضیه حسینی

شـــرکت مایکروســـافت از کاربران می‌خواهد تا وصله جدید منتشـــر شده را جهت رفع آســـیب‌پذیری BlueKeep RDP اعمال نمایند چـــرا که ایـــن آسیب‌پذیری می‌تواند به حمـــلات موثری منجـــر گردد. اکسپلویـــت Bluekeep می‌تواند برای گسترش بدافزارهای دیگری نیز مورد استفاد قرار گیرد.

در تاریخ 2 نوامبر 2019، Kevin Beaumont - محقق امنیتی - حملات RDPای را کشـــف کرد که منجر به crash شدن ماشین می‌گردد. Marcus Hutchins با تجزیـــه و تحلیل این آســـیب‌پذیری، بیـــان کرد که مهاجمـــان از آسیب‌پذیری Bluekeep برای نصب استخراج‌کننده ارز Monero استفاده می‌کنند.

آســـیب‌پذیری مذکور که شناســـه "CVE-2019-0708" به آن اختصاص داده شده است یـــک نقص اجرای کد از راه دور (RCE) در سرویـــس‌هـــای Remote desktop اســـت کـــه به مهاجمـــان اجازه می‌دهد بـــدون احراز هویت، به دســـتگاه آســـیب‌پذیر دسترســـی پیدا کننـــد. از آنجایی که این آســـیب‌پذیری wormable اســـت می‌توانـــد به ســـرعت در یـــک دوره کوتاه میلیون‌ها دستگاه را به خطر اندازد.

ماژول Bluekeep Metasploit

محققان مایکروســـافت حمله اســـتخراج ارز مربوط به چند مـــاه پیش را با حمله BlueKeep Metasploit مرتبط دانســـتند. هـــر دوی این حملات به یک سرور کنترل و فرمان (command-and-control) متصل هستند و هدف آنها نصب یک استخراج کننده ارز دیجیتال است.

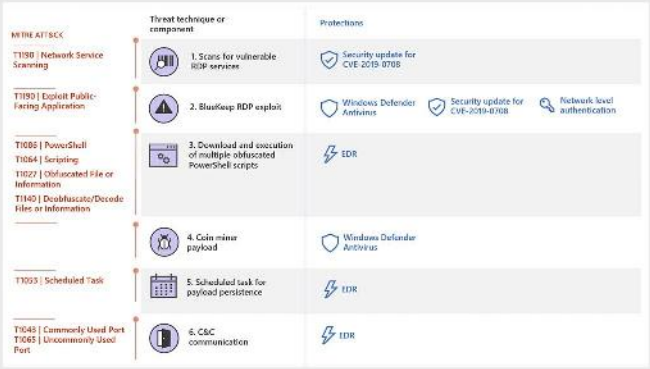
شـــرکت مایکروســـافت با محققان برای بررســـی این حمله همکاری کرده و ماژول اکسپلویت BlueKeep را برای آزمون نفوذ Metasploit مورد استفاده، تأیید کردند.

ماژول اکســـپلویت مورد اســـتفاده در این حمله ناپایدار اســـت زیرا منجر به چندین مرتبه crash شـــدن می‌گردد. مایکروســـافت قابلیتـــی را ایجاد کرده است که کاربران Microsoft Defender ATP که مشابه هانی‌پات‌های Beaumont عمل می‌کند در برابر ماژول Metasploit محافظت می‌شوند.

براساس بررسی‌های این شـــرکت، افزایش crashهای مربوط به RDP به دلیل ماژول ناپایدار BlueKeep Metasploit است.

کمپین‌های استخراج کننده ارز

ایـــن حملات به عنوان یک اســـکنر پورت شـــروع بـــکار می‌کننـــد، اگر این اسکنر متوجه دستگاه RDP آســـیب‌پذیر در اینترنت شود، از ماژول BlueKeep Metasploit برای اجرای یک PowerShell اســـتفاده می‌کند تا بـــــار دیگر PowerShellهای رمزگذاری شده را از سرور مهاجم بارگیری نماید.



اگر یکبار دیگر این Powershellهای رمزگذاری شده اجرا شوند، payload نهایی اســـتخراج ارز و نیز payload متصل شده به ســـرور کنترل و فرمان در آی‌پی 106[.]251[.]100[.]5 را بارگیری می‌کنند.

آی‌پی دیگـــــــری بـــــا شماره 59[.]205[.]104[.]193 به صورت فعـال از آسیب‌پذیری BlueKeep استفاد می‌کند.

مایکروســـافت از کاربران خواســـته اســـت تا وصله امنیتی منتشـــر شده را اعمال نمایند.

✓ توصیه‌های امنیتی

- در صورت عدم استفاده از سرویس‌های Remote Desktop، آن را مسدود کنید.
- پورت 3389، TCP را در فایروال سازمانی مسدود نمایید.
- وصله امنیتی را بر روی دســـتگاه‌های آســـیب‌پذیری کـــه RDP را فعال کرده‌اند، اعمال کنید.

منبع خبر :

https://gbhackers.com/bluekeep-rdp-vulnerability/

Scan Link

انتقال بدافزار و درب پشتی به دستگاه‌های اندرویدی از طریق ۷ اپلیکیشن مخرب در فروشگاه Google play

گردآورنده: صبا آزرمی ویراستار: سیده مرضیه حسینی

7 Malicious Apps from Google Play That Opens a Backdoor to Hackers

محققان 7 برنامه مخرب را در فروشگاه Google play کشف کردند که نرم‌افزارهای تبلیغاتی و بدافزارها را در دستگاه کاربران نصب کرده و یک درب پشتی را برای حمله مهاجمان مستقر می‌سازد.

این برنامه‌ها توسط بیش از 11,000کاربر اندرویدی در Google play دانلود و نصب شده‌اند و منجر به فعالیت‌های مخربی از جمله تخلیه باتری دستگاه و استفاده بیش از حد از داده تلفن همراه می‌شوند.

در حال حاضر بدافزارهای تلفن همراه رو به افزایش هستند و مهاجمان همواره در پی یافتن روش‌ها و تکنیک‌های جدیدی برای دور زدن امنیت Google play و هدف قرار دادن میلیون‌ها کاربر اندرویدی در سراسر جهان هستند.

سه شرکت توسعه دهنده، اپلیکیشن‌های مخرب خود را در Google Play بارگذاری کرده‌اند:

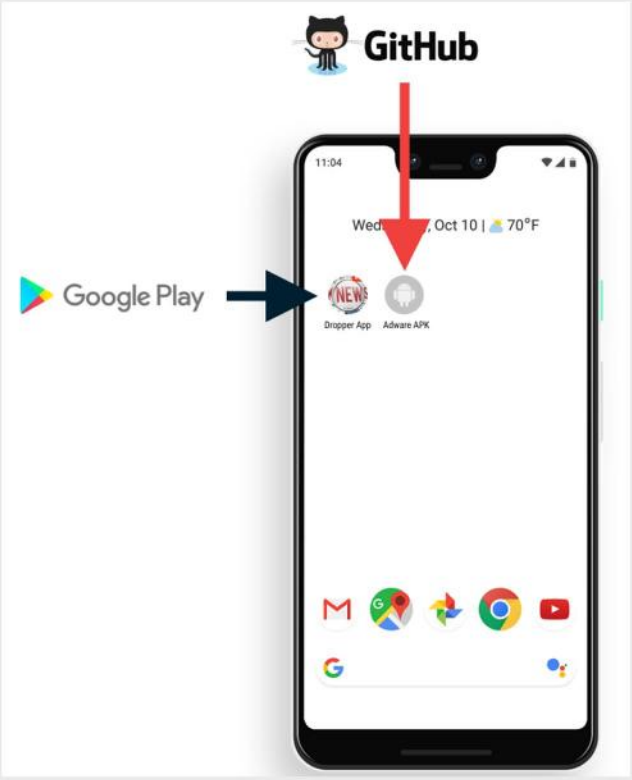
- شرکت PumpApp_ اپلیکیشن‌های Magnifying Glass، Super Bright LED Flashlight
- شرکت LizotMitis_ اپلیکیشن‌های Magnifier، Magnifying Glass with Flashlight، Super-bright Flashlight
- شرکت iSoft LLC_ اپلیکیشن‌های Alarm Clock، Calculator، Free Magnifying Glass

"اپلیکیشن‌های dropper برای دانلود و نصب APKها[1] از repository گیت هاب طراحی شده‌اند و به نوبت یا به درخواست مهاجم بصورت ذره ذره و کم کم کدهای مخرب اجرایی مانند Backdoorها را دریافت کرده و بر روی سیستم هدف نصب می‌کنند. "

Dropperهای بدافزار در حال برقراری ارتباط با گیت‌هاب و در تلاش برای دور زدن بررسی‌های محققان و نیز نرم‌افزارهای امنیتی هستند.

URL گیت‌هاب درون کد اپلیکیشن Dropper قرار گرفته است و برای آن که از آنالیزهای انسانی و اسکن Google Play به دور باشد، کاملاً مبهم است.

محققان از داده‌های مربوط به پیکربندی برنامه dropper و URLهای اضافی پیام مبهم JSON پرده برداشتند و به Adware APK نیز اشاره کردند.



پس از نصب برنامه‌های مخرب APK adware، dropper فعال خواهد شد و 10 دقیقه قبل از شروع فعالیت‌های مخرب خود، صبر می‌کند.

این برنامه، تبلیغات ویدیویی را به صورت تمام صفحه، خارج از برنامه و بدون هیچ گونه واکنشی از طرف کاربر، نمایش می‌دهد و قادر است در هر زمان چندین اپلیکیشن دیگر را برای نمایش تبلیغات و به محض باز کردن قفل دستگاه توسط کاربر اجرا کند.

[1] APK مخفف Android Package Kit و یک فرمت خاص نرم‌افزاری است که برای نصب نرم‌افزار در سیستم‌عامل اندروید استفاده می‌شود.

براســـاس تبلیغات Wandera، اگر صفحه نمایش دســـتگاه خاموش باشد و هیـــچ رمز عبوری بـــرای آن تنظیم نشـــده باشـــد، این ابـــزار تبلیغاتی در فواصـــل زمانی مشـــخص و تا زمانی که کاربـــر متوجه شـــود، صفحه نمایش دستگاه را روشن کرده و تبلیغات ویدیویی را پخش می‌کند.

اما اگر دســـتگاه دارای رمز عبور باشـــد، این ابـــزار نمی تواند رمـــز عبور را دور بزند اما صفحه نمایش را روشـــن کـــرده و تبلیغات ویدیویـــی را در پـــس زمینـــه دســـتگاه اجـــرا می‌کنـــد و باعـــث افزایش بـــار CPU و مصرف باتری می‌شود.

تنهـــا راه حل، متوقـــف کردن تبلیغات به صورت دســـتی اســـت، زیرا حتی بدون هیـــچ گونه واکنشـــی از طرف کاربـــر و هنگامی که تلفـــن همراه در داخل کیف او است، این تبلیغات ویدیویی مدام در حال اجرا هستند.

این برنامه‌ها سیاست‌های گوگل را نیز نقض می‌کنند.

بـــه کاربرانی که ایـــن برنامه‌ها را نصـــب کرده‌اند توصیه می‌شـــود که هم برنامه‌هـــای dropper و هـــم payload برنامه‌هـــا را به صورت دســـتی از حالت نصب خارج کرده و حذف نمایند.

اخیراً شـــرکت Google با شـــرکت‌های امنیتی تلفن همـــراه رایزنی کرده تا قبـــل از نفوذ ایـــن بدافزارها به دســـتگاه کاربر، آن‌ها را کشـــف کند، هدف از انجام این کار، امنیت بیشتر Google است.

منبع خبر :

ttps://gbhackers.com/seven-malicious-apps/

Scan Link

راه‌اندازی نرم‌افزار جاسوسی و تروجان توسط مهاجمان، با هدف ثبت کاراکترهای تایپ‌شده از طریق صفحه کلید و نیز سرقت رمزهای عبور اپلیکیشن‌های ویندوزی!

گردآورنده: صبا آزرمی ویراستار: سیده مرضیه حسینی

محققان به تازگی کمپین مخربی را کشف کرده‌اند که payloadهای مختلفی مانند نرم‌افزار جاسوسی Agent Tesla و تروجان Ave Maria را از طریق اپلیکیشن‌های مختلف ویندوزی به کاربران ارسال می‌کنند. هدف از ارسال این payloadها، سرقت نام کاربری، رمز عبور و نیز ثبت کاراکترهای وارد شده از طریق صفحه کلید می‌باشد.

محققان معتقدند که این نرم‌افزارهای جاسوسی که به RAT[1] تبدیل می‌شوند، ممکن است برای توسعه باج‌افزار مخرب و در جهت سودجویی بیشتر و payload قدرتمند تر، مورد استفاده قرار گیرند.

این payloadها با AutoIT مطابقت دارند. AutoIT یک زبان اسکریپتی است که برای خودکارسازی کارهای اصلی در رابط کاربری گرافیکی ویندوز ایجاد شده است و توسط مجرمان سایبری برای مبهم کردن داده‌های باینری بدافزارها به منظور فرار از تشخیص و شناسایی مورد سوءاستفاده قرار می‌گیرد.

این تکنیک عمدتاً برای دور زدن فیلترهای Spam مورد استفاده قرار گرفته و راهکاری ساده برای قرار دادن فایل‌هـــای ISO مخرب در آخرین نسخـــه ویندوز می باشد.

این بدافزار در سایت Trend Micro به عنوان تروجـــان spy Negasteal یا Agent Tesla (TrojanSpy.Win32.NEGASTEAL.DOCGC)، و تـــروجان دسترســـی از راه دور Ave Maria (RAT) یـــا Warzone (TrojanSpy.Win32.AVEMARIA.T) معرفی گردیده است.

محققان بر این باورند که این کمپین مخرب از طریق آدرس webmail می تواند قربانی را به خطر بیاندازد.

فرآیند آلوده شدن

این بدافزارها غالباً به صورت فایل فشرده (.RAR) در ضمیمه‌ی ایمیل‌هـــای Malspam ارائه می‌شوند. هنگامی که قربانیان، فایل ضمیمه ایمیل را دانلود و آن را از حالت فشرده خـــارج می‌کنند، انواع نرم‌افزارهـای آلوده به بدافزار مخرب Negasteal و Ave Maria به سیستم آنها وارد می‌شود.

بر اساس پژوهش‌های سایت Trend Micro، تکنیک مبهم AutoIT دارای دو لایه است: "داده‌های واقعی بدافزار که در اسکریپت‌های AutoIT (.au3) پنهـــان شده‌اند و اسکریپت‌هایی که توسط کامپایلر AutoIT مانند Aut2Exe به یک فایل اجرایی تبدیل می‌شوند."

به گفته محققان، تروجان Ave Maria برای دور زدن UAC و پردازش توکن‌ها به منظور افزایش امتیازات خود ارائه شده است.

[1] Remote Access Trojan

در پی این آلودگی، تروجان Negasteal/Agent Tesla می‌تواند کاراکترهای وارد شده، webcam، screen capture و نیز اطلاعات ذخیره شده در clipboardها را نظارت و ثبت کند. همچنین نام کاربری و رمز عبور را از پروتکل‌هایی مانند SMTP، POP3، IMAP، HTTP و اپلیکیشن‌های ویندوزی از جمله Microsoft Outlook، Windows Messaging، Internet Explorer، Google Chrome، Foxmail، Thunderbird و Firefox به سرقت ببرد.

در سایت Trend Micro آمده است که: " تروجان Ave Maria می‌تواند فایل‌های دلخواه خود را در سیستم قربانی حذف و یا تغییر داده و همچنین فایل جدیدی ایجاد کند و نیز فرآیندها، دایرکتوری‌ها، فایل‌ها و درایوها را برشمارد، فرآیندهای در حال اجرا را خاتمه داده، فایل‌ها را حذف کند و در نهایت نیز خود را حذف نماید."

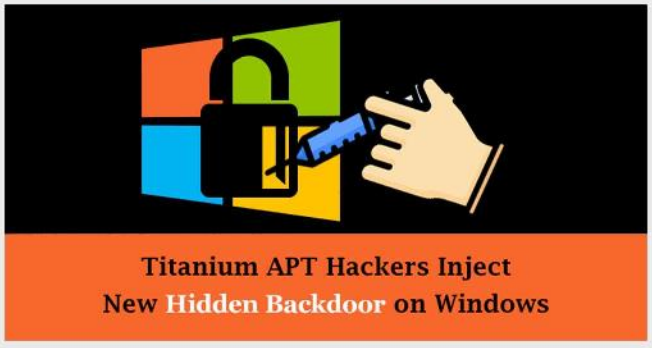
منبع خبر :

https://gbhackers.com/obfusticated-rat-spyware/

Scan Link

تزریق درب پشتی پنهان بر روی ویندوز، با استفاده از تکنیک Fileless (بدون فایل)

گردآورنده: سیده مرضیه حسینی



موج جدیدی از حملات نرم‌افزارهای مخرب توسط گروه هکری Titanium APT بار دیگر آغاز شده است. این حملات از طریق درب پشتی و با تقلید از نرم‌افزارهای مجاز و رایج و استفاده از تکنیک fileless، ویندوز را آلوده می‌کنند.

Titanium APT یکی از پیشرفته‌ترین گروهای هکری است که از تکنیک‌های مختلف و پیچیده‌ای برای حمله به هدف استفاده می‌کند و این روش‌ها و تکنیک‌های حمله، تشخیص فعالیت‌هایشان را بسیار سخت می‌کند.

بعلاوه، سیستم‌فایل بدافزار مربوط به آنها به دلیل استفاده از رمزگذاری و تکنیک‌های fileless برای آلوده کردن قربانیان، نمی‌توانند به عنوان فایل مخرب شناسایی شود.

این گروه به طور عمده منطقه APAC - این منطقه عموماً شامل آسیای شرقی، آسیای جنوبی، آسیای جنوب شرقی و اقیانوسیه می‌شود - را هدف قرار داده است و محققان معتقدند که حمله مذکور بر جنوب و جنوب شرقی آسیا نیز متمرکز شده است.

محققان کسپرسکی دریافتند که این بدافزار در هر مرحله با تقلید از نرم‌افزارهای متداول (مانند نرم‌افزارهای امنیتی، درایور صدا، ابزارهای ایجاد فیلم DVD) پنهان می‌شوند.

مراحل آلوده شدن سیستم

قبل از استقرار درب پشتی بر روی کامپیوترهای ویندوز در آخرین مرحله، عاملان این حمله مراحل پیچیده‌ای همچون حذف کردن، بارگیری و نصب فایل‌های دیگر را انجام می‌دهند.

در هر مرحله از این فرآیند، از نرم‌افزارهای متداولی مانند نرم‌افزارهای امنیتی، نرم‌افزارهای ساخت فیلم‌های DVD و درایورهای صدا جهت گریز از شناسایی استفاده می‌شود.

محققان بر این باورند که مهاجمان با استفاده از یک وب‌سایت درون سازمانی همراه با کد مخرب، اقدام به گسترش این بدافزار می‌کنند.

در یک روش دیگر، این گروه شِل‌کدی را درون یک فرآیند به نام "winlogon.exe" تزریق می‌کنند. winlogon.exe، یک فایل مجاز است که به عنوان یک برنامه ورود به سیستم در ویندوز شناخته می‌شود و چندین عمل مهم مربوط به فرآیند ورود به سیستم را انجام می‌دهد.

این شِل‌کد حاوی کد مستقل از محل است که به سرور C&C متصل می‌شود، یک payload رمزگذاری شده را بارگیری و سپس رمزگشایی می‌کند و با استفاده از رمز عبور قوی شروع بکار می‌کند.

فعالان این گروه هکری، در اکثر مواقع از Wrapper DLLs برای رمزگشایی و بارگذاری فایل‌های رمزگذاری شده بر روی حافظه سیستم استفاده می‌کنند.

در مرحله بعد با استفاده از Windows task installer، یک فایل رمزگذاری شده که می‌تواند از طریق BITS Downloader بارگیری شود بر روی سیستم

قربانی مستقر می‌شود.

کتابخانه بارگیری شـــده، به دانلود فایل‌های رمزگذاری شـــده از سرور C&C و راه‌اندازی آنها کمک می‌کند.

استقرار درب پشتی

در آخرین مرحله‌ی ایـــن فرآیند، مهاجمان از یک نصب‌کننـــده تروجان-درب پشـــتی برای نصب یک درب پشـــتی بر روی سیســـتم قربانی استفـــاده می‌کنند.

این نصب کننده با ارســـال یک درخواســـت خالی به ســـرور C2، یک فرمان از این ســـرور دریافـــت می‌کند. این بدافـــزار همچنیـــن می‌تواند تنظیمات پراکسی را از Internet Explorer دریافت کند.

در پاســـخ، سرور C2 یک فایل PNG که شـــامل داده‌های پنهان استگانوگرافی اســـت ارســـال می‌کند. این داده‌ها با همان کلید درخواســـت‌های ســـرور C&C رمزگذاری می‌شـــوند. این داده‌های رمزگذاری شـــده حاوی دســـتورات مربوط به درب پشتی برای سرقت داده‌های قربانیان است.

منبع خبر :

https://gbhackers.com/titanium-apt/

Scan Link

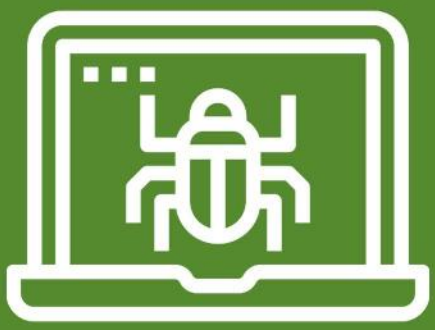
اخبار کوتاه

وبلاگ‌های Blagger و Wordpress مورد حمله هکری قرار گرفتند!

اخیراً مهاجمان توانسته‌اند تعدادی از وبلاگ‌های Wordpress و Blogger را هک کرده و از وبلاگ‌های هک شده برای ایجاد پست‌هایی با مضمون اینکه کامپیوتر وبلاگ نویس هک شده است، استفاده کنند. مهاجم در این پست‌ها ادعا می‌کند که علاوه بر تغییر رمزهای عبور توانسته بصورت مخفیانه فیلم‌های خصوصی از قربانی که همان وبلاگ‌نویس است، ضبط کند. چنین تهدیداتی معمولاً برای فردی که مورد حمله قرار گرفته و اطلاعات وی افشاء شده است از طریق ایمیل ارسال می‌شود. بررسی‌ها نشـــان می‌دهد حدود 1500 وبلاگ در Blogger و بیش از 200 وبلاگ Wordpress به این روش هک شده‌اند و احتمال می‌رود تعدادی از کاربران، پول درخواستی را به هکر پرداخت کرده باشند.

هموطنان مراقب کلاهبرداری درخصـــوص سهمیه‌بندی بنزین باشند!

کلاهبـــرداران با ارســـال پیامک مبنی بـــر ثبت نام طرح حمایت معیشـــتی دولت و یـــا دریافت ســـهمیه بنزیـــن ویژه تاکســـی‌ها و وســـایل نقلیه عمومـــی به هموطنـــان، متقاضیـــان را بـــه درگاه‌های جعلی موســـوم به فیشـــینگ هدایت و نســـبت به برداشـــت غیرمجاز از حســـاب آن‌ها اقدام می‌کننـــد. معـــاون اجتماعی پلیس فتـــا ناجا گفت: ثبت نـــام در طرح‌های اعلامی از ســـوی دولت و ســـازمان‌های دولتـــی عمدتاً رایگان بـــوده و نیاز به پرداخـــت هیچگونه وجهـــی ندارد. لذا بـــه هموطنان توصیـــه نمود در صـــورت دریافـــت لینک و هدایـــت به صفحـــات پرداخت حتی بـــا مبالغ اندک تأمل نموده و به هیچ عنوان اقدامی ننمایند.



آسیب پذیری

لـــزوم بروزرســـانی مرورگر گـــوگل کروم بـــه دنبال آسیب‌پذیری روز صفرم آن!

گردآورنده: سیده مرضیه حسینی

کاربرانی کـــه از مرورگر کـــروم در کامپیوترهـــای ویندوز، مـــک و لینوکس اســـتفاده می‌کنند لازم اســـت ســـریعاً مرورگر خود را به آخرین نســـخه آن بروزرسانی نمایند.

با انتشـــار نســـخه 78.0.3904.87 کروم، شـــرکت گوگل به میلیاردها کاربر خود هشـــدار داد که برای وصله دو آســـیب‌پذیری با شـــدت بـــالا، مرورگر خود را بروزرســـانی کنند. در یکی از این آســـیب‌پذیری‌ها مهاجمـــان می‌توانند کامپیوترها را در سراسر جهان اکسپلویت نمایند.

تیـــم امنیتی کروم بدون انتشـــار جزئیـــات فنی این آســـیب‌پذیری‌ها، تنها بیان می‌کننـــد کـــه آنهـــا از نـــوع use-after-free می‌باشـــند و یکی از این آسیب‌پذیری‌ها با شناســـه "CVE-2019-13720 " بخش‌های مربوط به صـــــدا در این مرورگر و آســـــیب‌پذیری دیگـــر با شناســـه "CVE-2019-13721 " کتابخانـــه PDFium را تحـــت تأثیر خود قرار خواهد داد.

آســـیب‌پذیری use-after-free نوعی تخریب حافظه اســـت که با تخریب یـــا تغییر داده‌هـــای موجـــود در حافظـــه، یک کاربـــر غیرمجـــاز را قادر می‌ســـازد تـــا ســـطح دسترســـی و امتیـــازات خـــود را در سیســـتم یا نرم‌افزار آسیب‌دیده افزایش دهد.

بنابراین، به واســـطه هردو آســـیب‌پذیری مذکور، مهاجمـــان می‌توانند از راه دور با ترغیـــب کاربران مورد هدف بـــرای بازدید از یک وب‌ســـایت مخرب، امتیازاتـــی را بـــر روی مرورگر کـــروم بدســـت آورنـــد، از محافظت‌های sandbox بگریزنـــد و نیـــز کد مخرب خـــود را بر روی سیســـتم‌های مورد هدف اجرا نمایند.

حملات فعال در آسیب‌پذیری روز صفرم گوگل کروم

آســـیب‌پذیری روز صفرم در مرورگر کروم توســـط محققان کسپرســـکی به نام‌های Anton Ivanov و Alexey Kulaev کشـــف و گزارش شـــده است، آســـیب‌پذیری مربوط بـــه مؤلفه‌های صوتـــی در برنامه کروم در سراســـر جهان مورد اکســـپلویت قـــرار گرفته اســـت، البته در حـــال حاضر هویت مهاجمان مشخص نیست.

تیـــم امنیتی گوگل کـــروم بیان کرد که این شـــرکت از گزارش‌های منتشـــر شده مبنی بر اکسپلویت آسیب‌پذیری "CVE-2019-13720 " آگاه است.

use-after-free یکـــی از رایج‌ترین آســـیب‌پذیری‌هایی اســـت که در چند ماه گذشـــته در مرورگر کروم کشـــف و وصله شـــده اســـت. حدود یک ماه پیش، شـــرکت گوگل بروزرســـانی امنیتی فوری را برای این مرورگر منتشـــر کـــرد تـــا در مجمـــوع 4 آســـیب‌پذیری use-after-free را در مؤلفه‌هـــای مختلـــف آن رفع نماید. در شـــدیدترین آن آســـیب‌پذیری‌ها، یـــک مهاجـــم از راه دور می‌توانـــد کنترل کامل سیســـتم آســـیب‌دیده را بدست گیرد.

چند ماه پیش نیـــز، گوگل پس از اطلاع از اکســـپلویت آســـیب‌پذیری روز صفرم شـــبیه به use-after-free در کـــروم کـــه FileReader این مرورگر را تحت تأثیر قرار می‌داد بروزرسانی امنیتی دیگری را منتشر کرد.

جزئیات فنی اکسپلویت روز صفرم کروم

یک روز پس از انتشـــار بروزرســـانی گوگل بـــرای رفع دو آســـیب‌پذیری با شـــدت بالا در کروم، شـــرکت امنیت ســـایبری کسپرســـکی جزئیات فنی بیشتری را در مورد این آسیب‌پذیری‌ها به این شرکت گزارش داد.

به گفتـــه محققان، مهاجمان یک ســـایت خبـــری به زبان کـــره‌ای را مورد حمله قرار دادند. آنها کد اکســـپلویتی را بر روی این ســـایت قـــرار داده و به واســـطه آن، کامپیوترهـــای بازدید کننده از این ســـایت که از نســـخه‌های آسیب‌پذیر کروم استفاده می‌کنند را مورد حمله خود قرار می‌دادند.

گفتـــه می‌شـــود کـــه ایـــن اکســـپلویت پـــس از اکسپلویـــــت آسیب‌پذیری CVE-2019-13720 کـــروم، در مرحلـــه اول یـــک بدافـــزار را بر روی سیســـتم‌های مـــورد هـــدف نصب می‌کند و پس از آن به یک ســـرور کنترل و فرمـــان (command-and-control) کدگذاری شده و راه دور برای بارگیری payload نهایی

متصل می‌شود.

محققـــان Operation WizardOpium عنوان کردند که این حمله ســـایبری هنوز به گروه خاصی از هکرها نســـبت داده نشـــده اســـت. بـــا این حال، محققـــان شـــباهت‌های را در کـــد ایـــن اکســـپلویت و گـــروه هکـــر Lazarus مشاهده کردند.

برای کســـب اطلاعات بیشـــتر در مورد عملکرد اکســـپلویت آســـیب‌پذیری تـــازه وصله شـــده‌ی کـــروم، می‌توانیـــد به گـــزارش جدیدی که توســـط کسپرسکی منتشر شده است مراجعه نمایید.

وصله جدید در دسترس است، سریعاً گوگل کروم را بروزسانی کنید!

برای وصله دو آســـیب‌پذیری امنیتی مذکور، شـــرکت گوگل انتشـــار نســـخه 78.0.3904.87 مرورگـــر کـــروم را برای سیســـتم‌عامل‌های ویـــنـــدوز، مک و لینوکس را آغاز کرده است.

✓ **توصیه امنیتی**

اگرچه این مرورگر به صورت خودکار، درباره آخرین نسخه موجود به کاربران اطلاع می دهد، امـا توصیه می‌شود با رفتن به منوی Help → About Google Chrome، روند بروزرسانی را به صورت دستی شروع کنید.

علاوه بر این، به کاربران این مرورگر توصیه می‌شود در سریع‌ترین زمان ممکن تمام نرم‌افزارهای سیستم خود را به عنوان یک کاربر غیرمجاز اجرا کنند.

منبع خبر :

https://thehackernews.com/2019/11/chrome-zero-day-update.html

Scan Link

آســـیب‌پذیری جدید PHP و امکـــــان هـــــک شدن سایت‌های درحال اجرا بر روی سرورهای Nginx!

گردآورنده: سیده مرضیه حسینی

در صورتیکه از وب‌سایت‌های مبتنی بر PHP بر روی سرورهای NGINX استفاده می‌کنیـــد و برای بهبود عملکرد و کارایی آن، قابلیت PHP-FPM را فعال کرده‌اید، بدانید کـــه در معرض آســـیب‌پذیری جدیدی قرار دارید کـــه در آن مهاجمان غیرمجاز می‌توانند از راه دور سرور وب‌سایت شما را هک کنند.

به این آسیب‌پذیری شناســـه "CVE-2019-11043" اختصاص داده شده است و وب‌ســـایت‌هایی بـــا پیکربنـــدی خاصـــی از PHP-FPM (کـــه ظاهراً غیرمعمول هم نیست) را تحت تأثیر قرار می‌دهد. قابلیـــت PHP-FPM پیاده‌سازی دیگری از PHP FastCGI اســـت که پردازش‌هایی پیشـــرفته و بسیار کارآمد را برای اسکریپت‌های نوشته شده در زبان برنامه‌نویسی PHP ارائه می‌دهد.

علت اصلی این آسیب‌پذیری، مشکل حافظه "env_path_info" underflow در ماژول PHP-FPM اســـت و ترکیب آن با ســـایر نقص‌هـــا می‌تواند مهاجمان را قادر ســـازد تـــا از راه دور کد دلـــخواه خود را بر روی وب‌سرورهـــای آسیب‌پذیر اجرا کنند.

آســـیب‌پذیری مذکور، توســـط یک محقـــق امنیتـــی در Wallarm به نام Andrew Danau در زمان برگزاری یکی از مسابقات Capture The Flag (CTF) کشـــف شـــد و وی با همکاری دو تـــن از محققان دیگر بـــه نام‌های Omar Ganiev و Emil Lerner توانســـتند آن را به صورت یک اکســـپلویت اجرای کد از راه دور توسعه دهند.

کدام یک از وب‌سایت‌های مبتنی بر PHP در برابر مهاجمان آسیب‌پذیرند؟

اگرچه اکســـپلویت کد اثبـــات مفهومی (PoC) آســـیب‌پذیری مورد بحث به صورت عمومی منتشـــر شـــده اســـت اما به طـــور خاص برای هـــدف قرار دادن ســـرورهای آســـیب‌پذیر در حـــال اجـــرای نســـخه‌های PHP 7+ طراحی شده اســـت، با این وجود، نسخه‌های پیشین PHP نیز تحت تأثیر این آسیب‌پذیری قرار دارند.

به طور خلاصه، یک وب‌سایت آسیب‌پذیر خواهد بود اگر:

- وب‌ســـرور NGINX به صورتی پیکربندی شده باشـــد که درخواست‌های صفحات PHP را به پردازنده PHP-FPM ارسال کند.
- دســـتور "fastcgi_split_path_info" در این پیکربندی وجود داشـــته و شـــامل یک عبارت معمولی باشـــد که با نماد '^' شـــروع می‌شـــود و با نماد '$' خاتمه می‌یابد.
- متغیر PATH_INFO با دستور fastcgi_param تعریف شده است.
- دستوری شـــبیه به "try_files $uri =404" و یا "f $uri-" برای مشخص کردن وجود یا عدم وجود یک فایل، وجود نداشته باشد.

پیکربندی آسیب‌پذیر NGINX و PHP-FPM می‌تواند به صورت زیر باشد:

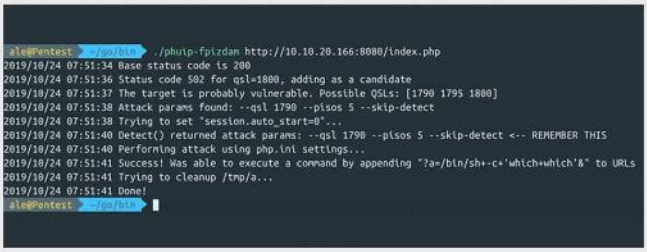
```
location ~ [^/]\.php(/|$) {
  ...
  fastcgi_split_path_info ^(.+?\.php)(/.*)$;
  fastcgi_param PATH_INFO       $fastcgi_path_info;
  fastcgi_pass   php:9000;
  ...
}
```

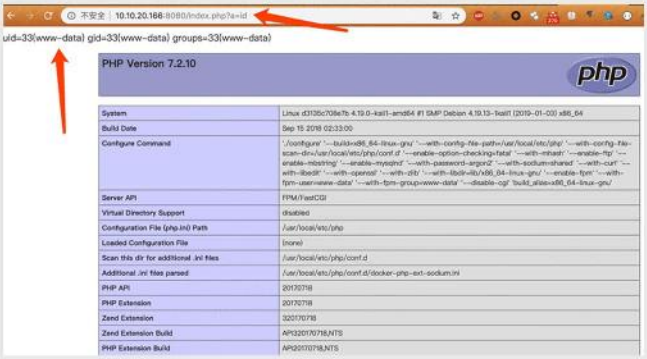
در این مثال، از دستور "fastcgi_split_path_info " برای تقسیم URL صفحات PHP وب به دو بخش استفاده می‌شود، بخش اول یک موتور PHP-FPM برای فهمیدن نام اسکریپت و بخش دوم شامل اطلاعات مسیر آن است.

اکسپلویت اجرای کد از راه دور در PHP FPM چگونه عمل می‌کند؟

به گفته محققان، عبارتی که دستور "fastcgi_split_path_info " را تعریف می‌کند، با استفاده از کاراکتر خط جدید می‌تواند به گونه‌ای دستکاری شود که در نهایت تابع تقسیم کننده URL تمامی اطلاعات مسیر را خالی کند.

در مرحله بعد، از آنجا که یک اشاره‌گر محاسباتی در کد FPM وجود دارد که به اشتباه "env_path_info " را بدون تأیید وجود فایلی بر روی سرور، یک پیشوند مساوی با مسیر اسکریپت php تلقی می‌کند، این مسئله می‌تواند توسط یک مهاجم برای بازنویسی داده‌ها در حافظه با درخواست URLهای خاص ساخته شده از وب‌سایت‌های مورد هدف اکسپلویت شود.





محققان، اکسپلویت کد اثبات مفهومی[1] را برای دستیابی به حافظه و اضافه کردن مقادیر دلخواه php.ini (همانطور که در تصویر نشان داده شده است) در فایل پیکربندی PHP-FPM در یک سرور مورد هدف منتشر کردند که به مهاجمان امکان می‌دهد که با استفاده از یک شِل وب، کد دلخواه خود را اجرا نمایند.

```
var chain = []string{
        "short_open_tag=1",
        "html_errors=0",
        "include_path=/tmp",
        "auto_prepend_file=a",
        "log_errors=1",
        "error_reporting=2",
        "error_log=/tmp/a",
        "extension_dir=\"<?=`\"",
        "extension=\"$_GET[a]`?>\"",
}
```

بروزرسانی‌های PHP 7 برای وصله آسیب‌پذیری FPM منتشر شد

پیکربندی‌های آسیب‌پذیر توسط برخی از ارائه دهندگان میزبانی وب مورد استفاده قرار می‌گیرد و به عنوان بخشی از آموزش‌های PHP-FPM در اینترنت موجود است.

Nextcloud یکی از ارائه دهندگان میزبانی وب که تحت تأثیر این آسیب‌پذیری قرار گرفته است به کاربران خود هشدار داد که پیکربندی پیش‌فرض Nextcloud NGINX در برابر این حمله آسیب‌پذیر است و همچنین به مدیران توصیه می‌کند تا اقدامات لازم و فوری را انجام دهند.

سرانجام پس از گذشت یک ماه از ارسال گزارش این آسیب‌پذیری به تیم توسعه PHP توسط محققان، وصله‌ای برای آن منتشر شد.

از آنجاییکه اکسپلویت کد اثبات مفهومی در حال حاضر موجود است و وصله مربوط به آن نیز به تازگی منتشر شده است، ممکن است مهاجمان با اسکن اینترنت در پی جستجوی وب‌سایت‌های آسیب‌پذیر باشند.

✓ **توصیه امنیتی**

به کاربران توصیه می‌شود حتی در صورت استفاده نکردن از پیکربندی آسیب‌پذیر PHP، آن را به آخرین نسخه یعنی 7.3.11 و 7.2.24 بروزرسانی نمایند.

منبع خبر :

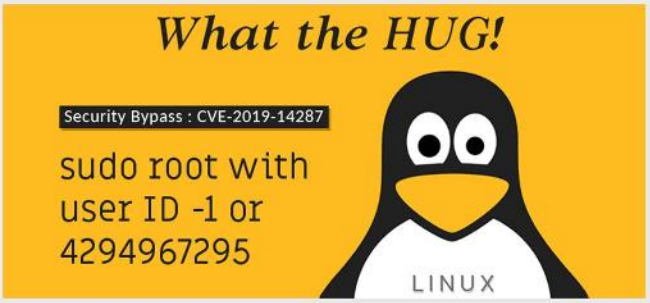
https://thehackernews.com/2019/10/nginx-php-fpm-hacking.html

Scan Link

[1] https://github.com/neex/phuip-fpizdam و https://github.com/jas502n/CVE-2019-11043

آسیب‌پذیری جدید در دستور Sudo سیستم‌عامل لینوکس و امکان اجرای دستورات با سطح دسترسی روت توسط کاربرانی با دسترسی محدود

گردآورنده: صبا آزرمی
ویراستار: سیده مرضیه حسینی



کاربران لینوکس آگاه باشند!

اخیراً آسیب‌پذیری جدیدی در Sudo که یکی از مهم‌ترین، قدرتمندترین و رایج‌ترین دستورات مورد استفاده در اغلب سیستم‌عامل‌های یونیکس و مبتنی بر لینوکس می‌باشد کشف شده است.

این آسیب‌پذیری سیاست امنیتی موجود در Sudo را دور زده و بدین ترتیب به یک کاربر یا برنامه مخرب اجازه می‌دهد تا دستورات دلخواه خود را با سطح دسترسی روت بر روی سیستم لینوکس مورد هدف اجرا کند، حتی زمانی که در "sudoers configuration" این سطح دسترسی برای آن مجاز نیست.

Sudo مخفف "superuser do" و یک دستور سیستمی است که کاربر را قادر می‌سازد برنامه‌ها یا دستوراتی را با سطوح دسترسی مختلف و اغلب با سطح دسترسی root و بدون نیاز به تعویض محیط، اجرا کند.

به طور پیش فرض در اغلب سیستم‌عامل‌های لینوکسی، کلمه کلیدی ALL در خط فرمان RunAs، در مسیر /etc/sudoers - همانطور که در تصویر قابل مشاهده است - به همه کاربران در گروه‌های Admin و sudo اجازه می‌دهد تا به عنوان کاربر مجاز، هر دستوری را بر روی سیستم اجرا کنند.

```
# Host alias specification

# User alias specification

# Cmnd alias specification

# User privilege specification
root    ALL=(ALL:ALL) ALL

# Members of the admin group may gain root privileges
%admin ALL=(ALL) ALL

# Allow members of group sudo to execute any command
%sudo   ALL=(ALL:ALL) ALL

# See sudoers(5) for more information on "#include" directives:

#includedir /etc/sudoers.d
ninja@saffron:~$
```

از آنجا که تفکیک سطوح دسترسی یکی از الگوهای امنیتی اصلی در لینوکس است، کاربران ادمین می‌توانند فایل sudoers را طوری پیکربندی کنند که مشخص شود کدام کاربران مجوز اجرای چه دستوراتی را خواهند داشت.

در این آسیب‌پذیری، حتی در صورتیکه کاربر در اجرای دستورات، محدود و یا با دسترسی روت قادر به اجرای دستوراتی دیگر باشد، می‌تواند از این الگوها و سیاست‌های امنیتی عبور کرده و کنترل سیستم را به طور کامل در دست بگیرد.

به گفته توسعه‌دهندگان Sudo: " این مسئله می‌تواند توسط کاربری با امتیازات Sudo برای اجرای دستوراتی که با دسترسی root قابل اجرا هستند استفاده شود، حتی اگر بر اساس مشخصات خط فرمان Runas و مادامی که کلمه کلیدی ALL در ابتدای آن ذکر شده باشد، دسترسی روت ممنوع باشد."

چگونه این باگ(ضعف) اکسپلویت می‌شود؟ تنها با شناسه کاربری "1-" یا 4294967295

این آسیب‌پذیری با شناسه "CVE-2019-14287" که توسط Joe Vennix از تیم امنیت اطلاعات شرکت اپل کشف شده است نگران‌کننده است، چرا که قابلیت sudo به گونه‌ای طراحی شده است که به کاربران این امکان را می‌دهد تا به عنوان کاربر دیگری و بدون نیاز به رمز عبور او، از رمز عبور ورود خود برای اجرای دستورات استفاده کنند.

نکته جالب آن است که این آسیب‌پذیری می‌تواند تنها با مشخص کردن شناسه کاربری "1-" و یا "4294967295" و اجرای دستوراتی با دسترسی روت، توسط یک مهاجم مورد اکسپلویت قرار گیرد. دلیل آن هم تابعی است که شناسه کاربر را به نام کاربری خود تبدیل می‌کند، بدین صورت که شناسه کاربری 1- و یا معادل آن یعنی "4294967295" را به 0 (شناسه کاربر روت) تلقی می‌کند.

علاوه بر این، به دلیل اینکه شناسه کاربری مشخص شده از طریق دستور "u-"، در پایگاه‌داده مربوط به رمزعبور وجود ندارد، هیچ ماژول سشن PAM ای اجرا نخواهد شد.

این آسیب‌پذیری بر تمام نسخه‌های قبل از نسخه Sudo 1.8.28 تأثیر می‌گذارد و به زودی بروزرسانی آن برای سیستم عامل‌های لینوکس منتشر خواهد شد.

از آنجا که این حمله در یک سناریوی مورد استفاده خاص از فایل

پیکربندی sudoers قابل اجراست، بنابراین نباید بر تعداد زیادی از کاربران تأثیر بگذارد. با این حال، اگر از سیستم‌عامل لینوکس استفاده می‌کنید، توصیه می‌شود هر چه سریع‌تر پکیج Sudo را به آخرین نسخه منتشر شده آن بروزرسانی کنید.

منبع خبر :

https://thehackernews.com/2019/10/linux-sudo-run-as-root-flaw.html

Scan Link

اجرای کد دلخواه و افزایش سطح دسترسی مهاجمان در ویندوز، به دنبال آسیب‌پذیری امنیتی در آنتی‌ویروس McAfee

گردآورنده: سیده مرضیه حسینی

شرکت McAfee یک آسیب‌پذیری را در تمام نسخه‌های آنتی‌ویروس خود وصله کرده است. در این آسیب‌پذیری و در نسخه کلاینت ویندوز آنتی‌ویروس McAfee، مهاجمان می‌توانند کد دلخواه خود را اجرا کرده و به امتیازات SYSTEM دسترسی پیدا کنند.

حساب کاربری SYSTEM یک حساب کاربری داخلی است که توسط سیستم‌عامل ویندوز برای مدیریت سرویس‌هایی که تحت ویندوز اجرا می‌شوند، استفاده می‌شود.

این آسیب‌پذیری نسخه کلاینت ویندوز را در McAfee Total Protection، McAfee Anti-Virus Plus و McAfee Internet Security نسخه R22.16.0 و قبل از آن را تحت تأثیر قرار می‌دهد.

نحوه کشف این آسیب‌پذیری

این آسیب‌پذیری توسط آزمایشگاه‌های SafeBreach در تمام نسخه‌های McAfee کشف شد. برای اکسپلویت این آسیب‌پذیری، مهاجم باید به عنوان یک مدیر اقدام به حمله نماید.

مهاجم می‌تواند از آسیب‌پذیری مذکور برای دور زدن مکانیسم‌های حفاظتی McAfee و دستیابی به پایداری از طریق بارگیری چندین سرویس که به عنوان "NT AUTHORITY\SYSTEM" اجرا می‌شوند، استفاده کند.

از طریق این آنتی‌ویروس، چندین بخش به عنوان یک سرویس اجرا شده ویندوز توسط "NT AUTHORITY\SYSTEM" که دارای مجوز SYSTEM است، اجرا می‌شوند.

به گفته محققان، آنتی‌ویروس McAfee به عنوان "NT AUTHORITY\SYSTEM" در تلاش است تا فایل wbemcomn.dll را از مسیر (c:\Windows\System32\wbem\wbemcomn.dll) بارگذاری کند درحالیکه این فایل به System32 مربوط است و نه به پوشه ystem32\Wbem.

این مسئله محققان را قادر می‌سازد تا یک DLL دلخواه را جهت بارگذاری در این فرآیند بارگذاری نمایند و مکانیسم‌های امنیتی این آنتی‌ویروس را دور بزنند. دلیل این امر نیز این است که پوشه‌های این آنتی‌ویروس توسط یک درایور سیستم‌فایل mini-filter محافظت می‌شوند که حتی توسط یک مدیر، عملیات نوشتن را محدود می‌کند.

این آسیب‌پذیری به مهاجمان امکان بارگذاری و اجرای payloadهای مخرب را با استفاده از چندین سرویس به صورت مداوم و در چارچوب فرآیندهای McAfee می‌دهد.

شناسه اختصاص داده شده به این آسیب‌پذیری "CVE-2019-3648" می‌باشد و در تاریخ 5 آگوست 2019 به شرکت McAfee گزارش داده شد. در حال حاضر آسیب‌پذیری مذکور وصله شده و این شرکت از کاربران خواسته است تا نسخه R22.16.0 را جهت رفع این آسیب‌پذیری نصب کنند.

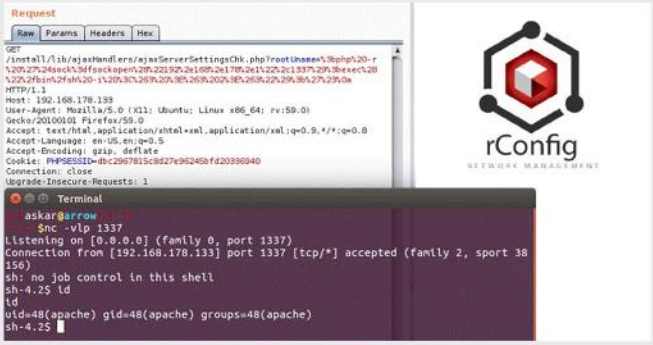
منبع خبر :

https://gbhackers.com/vulnerability-mcafee-antivirus/

Scan Link

هشدار به مدیران IT! دو آسیب‌پذیری بحرانی اجرای کد از راه دور در ابزار rConfig

گردآورنده: سیده مرضیه حسینی



اگـر از ابـزار محبـوب مدیریـت پیکربنـدی شـبکه‌ی rConfig بـرای محافظـت و مدیریـت دسـتگاه‌های شـبکه خـود اسـتفاده می‌کنیـد، به هشـدار مهـم و فوری زیر دقت کنید....

بـه تازگـی، جزئیـات و کد اثبـات مفهومی بـرای دو آسـیب‌پذیری مهـم و بحرانی اجرای کد از راه دور (remote code execution) در ابزار rConfig منتشر شده است.

در یکـی از ایـن آسـیب‌پذیری‌ها، مهاجـم غیر مجـاز می‌تواند از راه دور سـرورهای مورد هدف را به خطر انداخته و به دستگاه‌های شبکه متصل شود.

rConfig کـه بـه زبـان PHP نوشـته شـده اسـت، یـک ابـزار اُپن‌سـورس بـرای مدیریت پیکربندی دسـتگاه‌های شـــبکه اسـت که مهندسـان شـبکه را قـــادر می‌سـازد دسـتگاه‌های شـبکه را پیکربنـدی نماینـد و بـه صـورت مکـــــرر از پیکربندی‌ها اسنپ‌شات بگیرند.

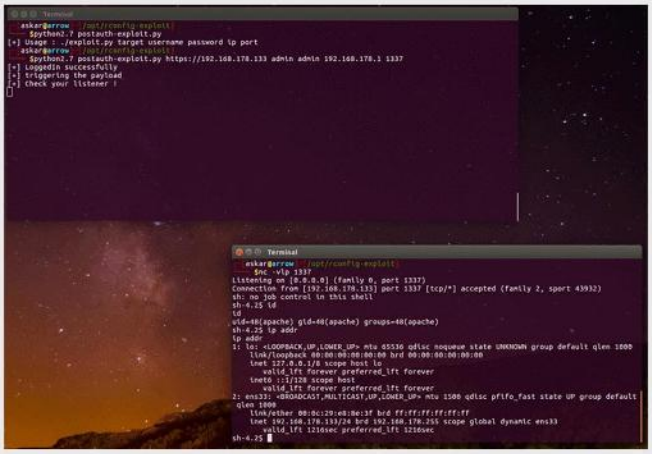
از این ابزار برای مدیریت بیش از 3.3 میلیون دسـتگاه شـبکه از جمله سـوئیچ‌ها، روترها، فایروال‌ها، load-balancer و بهینه‌سازهای WAN استفاده می‌شود.

آنچـــــــه که موجب نگرانی بیشتر می‌شود این است که هـــــر دوی این آسیب‌پذیری‌ها تمام نسخه‌های rConfig از جمله آخرین نسخه آن یعنی 3.9.2 را تحت تأثیر قرار داده و تاکنون نیز هیچ وصله امنیتی برای آنها منتشر نشده است.

هـر یـک از ایـن آسـیب‌پذیری‌ها در یـک فایـل جداگانـه‌ی rConfig قـرار دارند، اولین آسـیب‌پذیری با شناسـه "CVE-2019-16662" می‌تواند از راه دور و بدون نیـاز بـه احـــراز هویت، مـورد اکســپلویت قرار گیـرد. در حالیکه آسـیب‌پذیری دیگـر بـا شناسـه " CVE-2019-16663" قبـل از اینکـه مـورد اکسـپلویت قـرار بگیرد به احراز هویت نیاز دارد.

- آسیب‌پذیری اجرای کد از راه دور احراز هویت نشده (CVE-2019-16662) در فایل ajaxServerSettingsChk.php
- آسیب‌پذیری اجرای کد از راه دور احراز هویت شده (CVE-2019-16663) در فایل search.crud.php

برای اکســـپلویت هر دو مـــورد، یک مهاجـــم تنها کافیســـت از طریق یک پارامتر GET ناقص که برای اجرای دســـتورات مخرب بر روی ســـرور مورد هدف طراحی شده است، به فایل‌های آسیب‌پذیر دسترسی پیدا کند.



همانگونه که در تصویر فوق قابل مشاهده است، کد اثبات مفهومی به مهاجمان اجازه می‌دهد تا یک شِل از راه دور را از سرور قربانی دریافت کنند و به واسطه آن هر دستور دلخواهی را بر روی آن سرور با همان امتیازات برنامه وب، اجرا کنند.

در عین حال، یک محقق امنیتی دیگر این آسیب‌پذیری‌ها را مورد تجزیه و تحلیل قرار داده و کشف کرد که آسیب‌پذیری RCE دوم نیز می‌تواند بدون نیاز به احـــراز هویت در نسخه‌هـــای قبـــل از نسخه rConfig 3.6.0 مورد اکسپلویت قرار گیرد.

با این حـــال، پس از بررسی کد منبع rConfig، مشخص شد کـــه نه تنها rConfig 3.9.2 دارای آسیب‌پذیری است بلکه تمام نسخه‌هـــای آن دارای آسیـــب‌پذیری می‌باشند. علاوه بر این، آســـیب‌پذیری CVE-2019-16663 نیز می‌توانـــد پس از تأیید هویـــت در تمام نســـخه‌هـــای قبل از rConfig 3.6.0 مورد اکسپلویت قرار گیرد.

✓ **توصیه امنیتی**

در صورتی که از ابزار rConfig استفاده می‌کنید، توصیه می‌شود تا زمان انتشار وصله‌های امنیتی، آن را به طور موقت از سرور خود حذف کنید.

منبع خبر :

https://thehackernews.com/2019/11/rConfig-network-vulnerability.html

Scan Link

مقالات آموزشی

حملات فیشینگ و انواع آن

گردآوردنده: سیده آرزو حسنی

حمله فیشینگ چیست؟

یکی از انواع حملات اینترنتی که باعث می‌شود اطلاعات مهمی از حساب‌های کاربری، حساب‌های بانکی و یا اطلاعات شخصی کاربران به سرقت برود، حمله فیشینگ (Phishing) می‌باشد. حمله فیشینگ در واقع نوعی تلاش برای بدست آوردن اطلاعات از طریق جعل محسوب می‌شود که در آن (فیشر) _کسی که حمله فیشینگ را انجام می‌دهد_ با استفاده از برخی متدها، اقدام به شبیه‌سازی یک وب‌سایت، برنامه و یا حتی یک سرویس نموده و با استفاده از آن، اطلاعات کاربران را به سرقت می‌برد.

انواع حملات فیشینگ

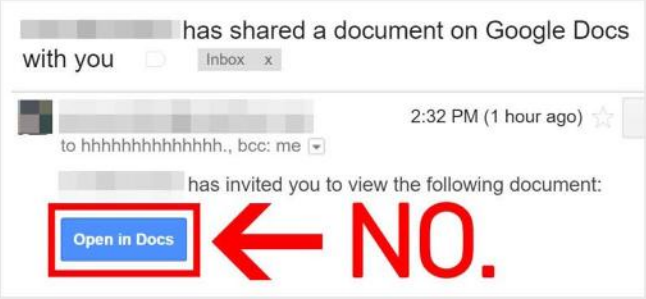
حمله فیشینگ دارای انواع مختلفی بوده که همه آن‌ها تقریباً بر یک پایه و اساس طراحی شده‌اند و آن، جعل است. این حملات معمولاً برای بدست آوردن اطلاعات حساب‌های بانکی مورد استفاده قرار می‌گیرند و طبیعتاً سیستم‌های پرداخت و خرید اینترنتی بیشتر از همه، مستعد این نوع حمله هستند.

1. فیشینگ فریبنده (deceptive phishing)

این نوع حمله عموماً از طریق ایمیل صورت می‌گیرد و فیشر با ارسال یک ایمیل از یک آدرس جعلی که بسیار شبیه به آدرس اصلی است، به روش‌های گوناگون از کاربر می‌خواهد تا روی لینک مورد نظرش کلیک کند. به عنوان مثال فیشر یک ایمیل با آدرسی بسیار شبیه به بانک A که کاربر در آن حسابی ایجاد کرده است ارسال می کند. در این ایمیل از کاربر خواسته شده است که هر چه سریعتر نسبت به تکمیل اطلاعات خود و جلوگیری از مسدود شدن حساب، اقدام نماید. بدین منظور کاربر باید روی لینکی که در ایمیل ضمیمه شده است کلیک کرده و سپس به صفحه تکمیل اطلاعات وارد شود.

اگر کاربر بدون دقت کافی به ارسال‌کننده پیام و صفحه‌ای که به آن هدایت شده است، شروع به وارد کردن اطلاعات خود نماید، در حقیقت این اطلاعات را به فیشر سپرده است. این نوع حمله جزء شایع‌ترین حملات بوده و معمولاً فیشرها از جملات دستوری و فریب‌دهنده برای ترغیب کاربران استفاده می‌کنند.

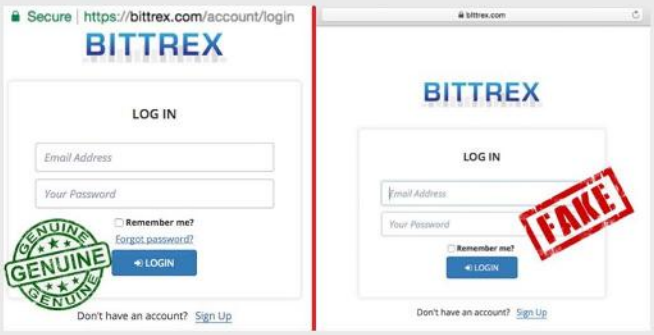
تصویر زیر نمونه‌ای از یک ایمیل فیشینگ را نشان می‌دهد که از کاربر می‌خواهد تا بر روی دکمه مشخص‌شده کلیک کند.



2. جعل وب سایت

یکی دیگر از حملات شایع فیشینگ، استفاده از جعل وب‌سایت است. در این حمله فیشر اقدام به ساخت یک صفحه اینترنتی مشابه صفحه اصلی نموده و از طریق اعتمادی که کاربران به آن صفحه اصلی داشته و عدم توجه دقیق به آدرس وب سایت، اقدام به جمع‌آوری اطلاعات کاربران می‌نماید.

نمونه‌ای از فیشینگ وب‌سایت خرید و فروش بیت کوین که در آدرس سایت به جای Bittrex از Blttrex استفاده شده است در تصویر زیر قابل مشاهده است.



3. فارمینگ

نوع پیشرفته‌ای از حمله جعل وب‌سایت می‌باشد که در آن هدف اصلی حمله DNS ها می‌باشند DNS .که وظیفه تبدیل آدرس به آی‌پی را دارد در این نوع حمله مورد هدف قرار می‌گیرد و فیشر یک آی‌پی اشتباه را به جای آی‌پی درست به وب‌سایت مورد نظر تزریق می‌کند. در این هنگام حتی اگر کاربر دقیقاً همان آدرس اصلی را تایپ کرده و به آن وارد شود، به دلیل DNS های اشتباه به آی‌پی دیگری ارجاع داده شده و در نهایت اطلاعات فرد به سرقت خواهد رفت.

تصویر زیر نمونه‌ای را نشان می‌دهد که در آن وب‌سایت اپل به صورت فرضی به این روش مورد حمله قرار گرفته است.

منبع خبر :

https://superfamilyprotector.com/blog/%D9%81%DB%8C%D8%B4%DB%8C%D9%86%DA%AF-%DA%86%DB%8C%D8%B3%D8%AA/

Scan Link

اخبار کوتاه

آسیب پذیری شبکه 5g در برابر حملات سایبری!

به تازگی محققان فعال در حوزه فناوری و امنیت سایبری دریافته و اعلام کرده‌اند که شبکه 5G در برابر انواع حملات و نفوذ هکرها آسیب‌پذیری بالایی دارد. به گفته محققان، آسیب‌پذیری‌های متعددی در این شبکه وجود دارد که این امکان را فراهم می‌کند تا هکرها و اشخاص ثالث موقعیت مکانی لحظه‌ای افراد را ردیابی کرده و همچنین پیام‌های امنیتی تقلبی و اشتباه برای آن‌ها ارسال کنند. همچنین این ضعف‌های امنیتی در شبکه 5G به سوء استفاده‌کنندگان اجازه می‌دهد که دسترسی افراد مورد نظر به شبکه مذکور را به طور کلی قطع کنند.

به امنیت «پیامک‌ها» اعتماد نکنید!

کارشناسان هشدار داده‌اند پیامک‌ها قبل از رسیدن به مقصد چند مسیر مختلف را طی می‌کنند، به این ترتیب مجرمان سایبری می توانند اطلاعات آن‌ها را در یکی از این مسیرها سرقت کنند. به گفته کارشناسان، این سرویس رمزگذاری نشده است و پیامک‌ها قبل از رسیدن به مقصد چند مسیر مختلف را طی می‌کنند. در همین راستا کارشناسان از کاربران می‌خواهند از پیامک استفاده نکنند و به جای آن از اپلیکیشن‌های پیام‌رسان استفاده نمایند تا به این وسیله از اطلاعاتشان محافظت کنند.

امنیت کاربر رایانه

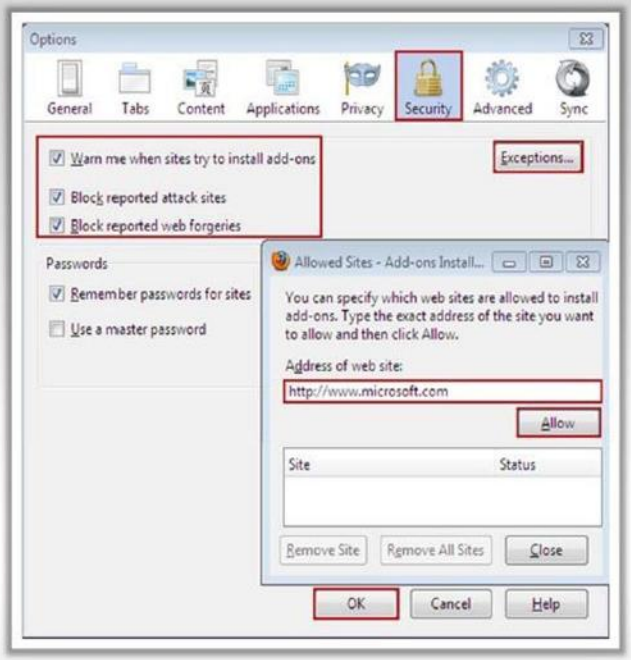
امنیت اینترنت

امنیت اینترنت یکی از شاخه‌های امنیت کامپیوتر است که به طور ویژه به اینترنت پرداخته و غالباً با مسئله امنیت مرورگر در ارتباط است که برمبنای یافتن راهکارها و الگوریتم‌هایی می‌باشد که ضد حملات اینترنتی است. قطعاً تاکنون اخبار متعددی در خصوص سرقت اطلاعات حساس نظیر شماره کارت اعتباری و یا شیوع یک ویروس کامپیوتری شنیده‌اید و شاید شما نیز از جمله قربانیان این نوع حملات بوده‌اید. آگاهی از تهدیدات موجود و عملیات لازم به منظور حفاظت در مقابل آن‌ها، یکی از روش‌های مهم و مناسب دفاعی است.

در این شماره از بولتن خبری، در فصل "امنیت اینترنت" قصد داریم به بیان روش‌های مختلف جهت افزایش امنیت مرورگر موزیلا فایرفاکس، مرورگر گوگل کروم و امنیت IM و موتور جستجو بپردازیم. ادامه مبحث امنیت اینترنت را در شماره‌های بعدی بولتن خبری دنبال کنید.

با ما همراه باشید...

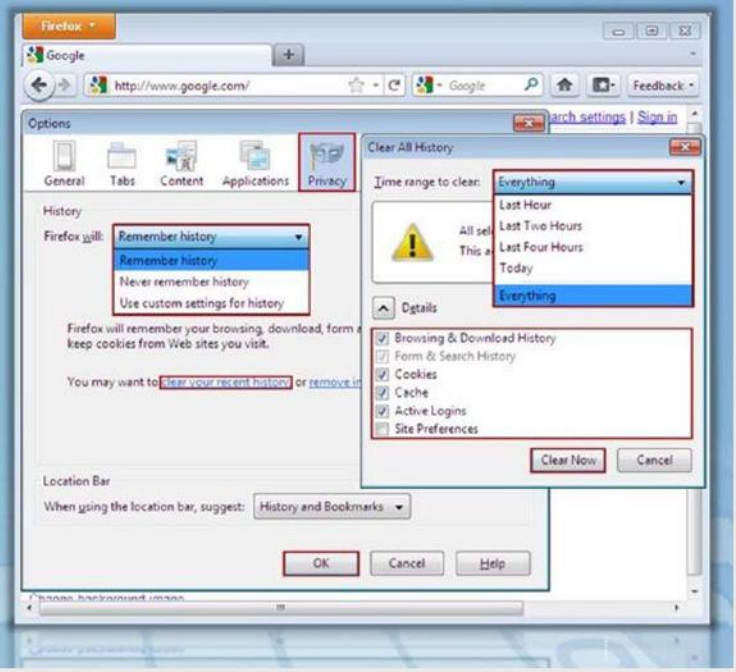
موزیلا فایرفاکس: تنظیمات امنیتی



- از پنجره Options گزینه Security را انتخاب نمایید
- گزینه Warn me when sites try to install add-ons را تیک بزنید، به طوری که مرورگر قبل از نصب add-onها کاربر را مطلع نماید
- بر روی دکمه Exceptions کلیک نموده و در باکس Address of Website، URL را وارد نمایید، سپس بر روی Allow کلیک کنید تا مشخص گردد کدام یک از وب سایت ها مجاز به نصب افزونه می باشند
- به منظور جلوگیری از بازدید وب سایت های مخرب تیک گزینه Block reported attack sites را بزنید
- به منظور بررسی اینکه آیا سایت بازدید شده سعی در سرقت اطلاعات داشته یا خیر، تیک گزینه Block reported web forgeries را بزنید
- به منظور جلوگیری از به خاطر سپردن پسوردها توسط مرورگر و استفاده از آن ها برای ورود به سایت های بازدید شده، تیک گزینه Remember passwords for sites را بردارید

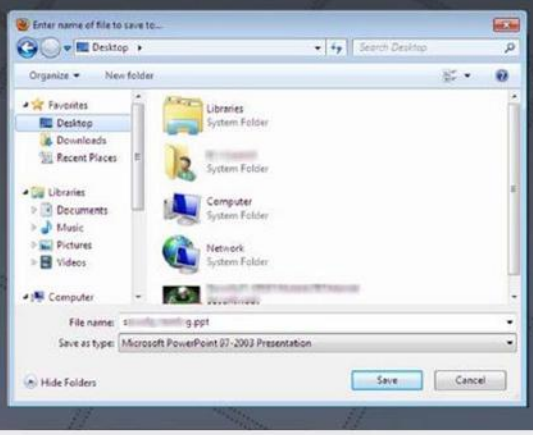
موزیلا فایرفاکس: تنظیمات حریم خصوصی

- در پنجره Options، Privacy را انتخاب نمایید
- کاربر می تواند انتخاب کند که مرورگر تاریخچه مرور اینترنت را به خاطر بسپارد یا خیر
- برای حذف تاریخچه مرورگر بر روی clear your history کلیک نمایید
- در پنجره Clear All History از قسمت Time range to clear محدوده زمانی دلخواه خود را انتخاب کنید
- در قسمت پایین پنجره، گزینه هایی را که میخواهید پاک شوند تیک زده و سپس بر روی Clear Now کلیک نمایید



امن سازی دانلودِ فایل ها

- از پذیرش دانلود فایل از منابع ناشناس در اینترنت جداً اجتناب نمایید
- چنین دانلودهایی ممکن است حاوی فایل های مخرب بوده و موجب کاهش سرعت عملکرد سیستم گردند



فایل های دانلود شده به طور پیش فرض در مسیر زیر ذخیره می شوند:

My Documents → Downloads

- کاربر ممکن است مرورگر را به گونه ای پیکربندی نماید که فایل ها در مسیر دیگری ذخیره شوند

امن سازی دانلودِ فایل ها

تنظیم گزینه های دانلود در فایرفاکس

- به منظور پیکربندی تنظیمات دانلود در موزیلا فایرفاکس، ->Tool ->Options **General** را انتخاب کنید
- برای اینکه هر بار هنگام دانلود فایل، مرورگر محل ذخیره فایل را از کاربر بپرسد تیک گزینه **Always ask me where to save the file** را بزنید
- اگر این گزینه تیک نداشته باشد مرورگر هنگام دانلود فایل بدون هیچ علامتی فایل را در **مسیر پیش فرض** ذخیره می کند

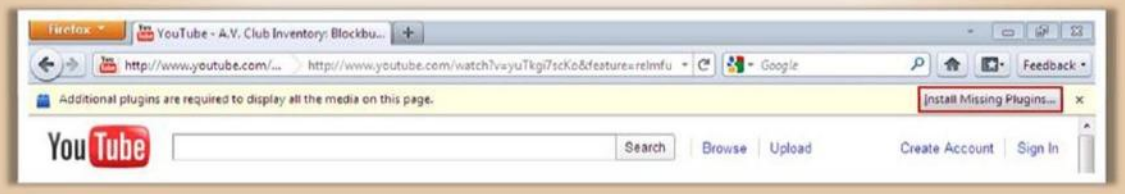
نصب پلاگین ها

1 هنگام باز کردن برخی از وب سایت ها پیغام **Install Missing Plugins** نشان داده می شود

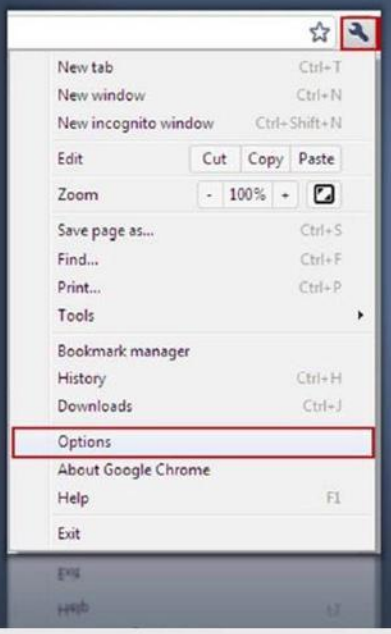
2 پلاگین ها برای نشان دادن **فایل ها**، **گرافیک ها** یا **پخش ویدئو** در یک صفحه وب مورد نیاز هستند

3 بررسی نمایید که آیا منبع پلاگین از دست رفته **قابل اعتماد** هست یا خیر؟

4 قبل از نصب یک پلاگین، ابتدا آن را با یک **آنتی ویروس** اسکن نمایید



تنظیمات امنیت و حریم خصوصی گوگل کروم

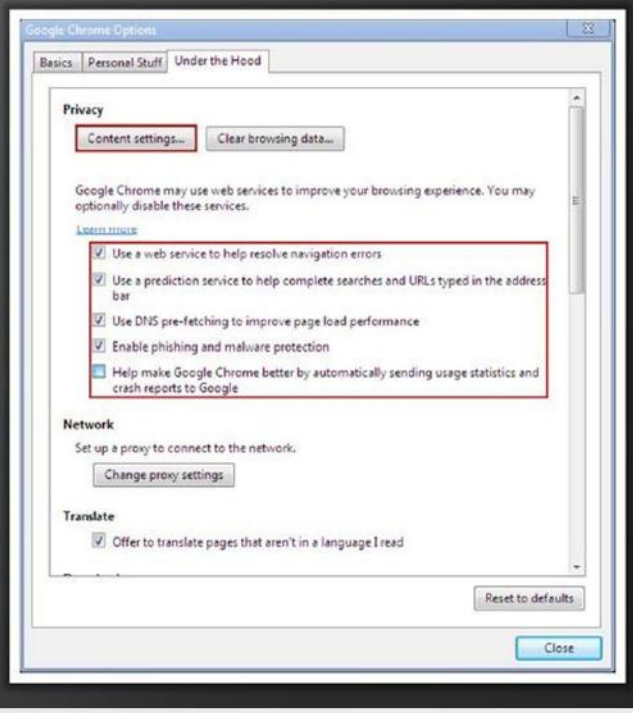


گوگل کروم را باز کنید

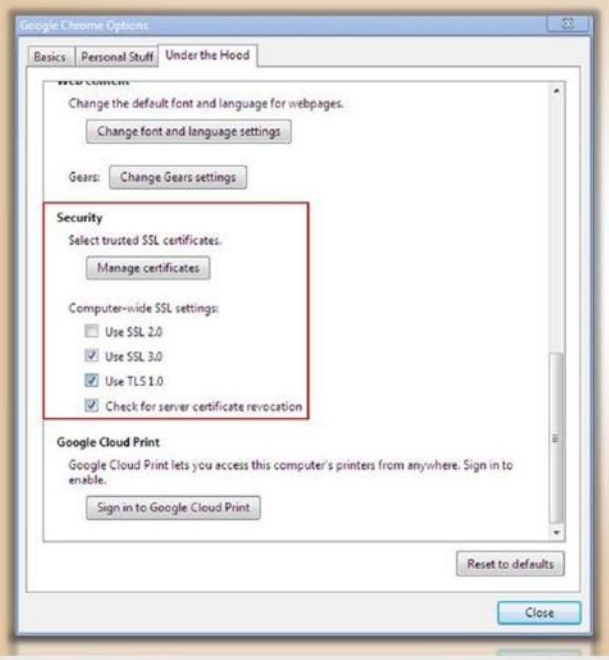
بر روی آیکون کلیک نموده و سپس **Options** را انتخاب نمایید

گوگل کروم:
تنظیمات حریم خصوصی

- در پنجره Google Chrome Options بر روی تب Under the Hood کلیک نمایید
- در قسمت Privacy، وب سرویس های دلخواه را تیک بزنید
- گزینه Use DNS pre_fetching to improve را تیک بزنید page load performance
- DNS pre_fetching مخفف Domain Name می باشد System pre_fetching
- هنگامی که کاربر از یک صفحه وب بازدید می کند، گوگل کروم می تواند آدرس های آی پی لینک های موجود در صفحه وب را یافته یا Pre_fetch نماید
- برای جلوگیری از باز شدن سایت های مخرب توسط مرورگر، گزینه Enable phishing and را تیک بزنید malware protection



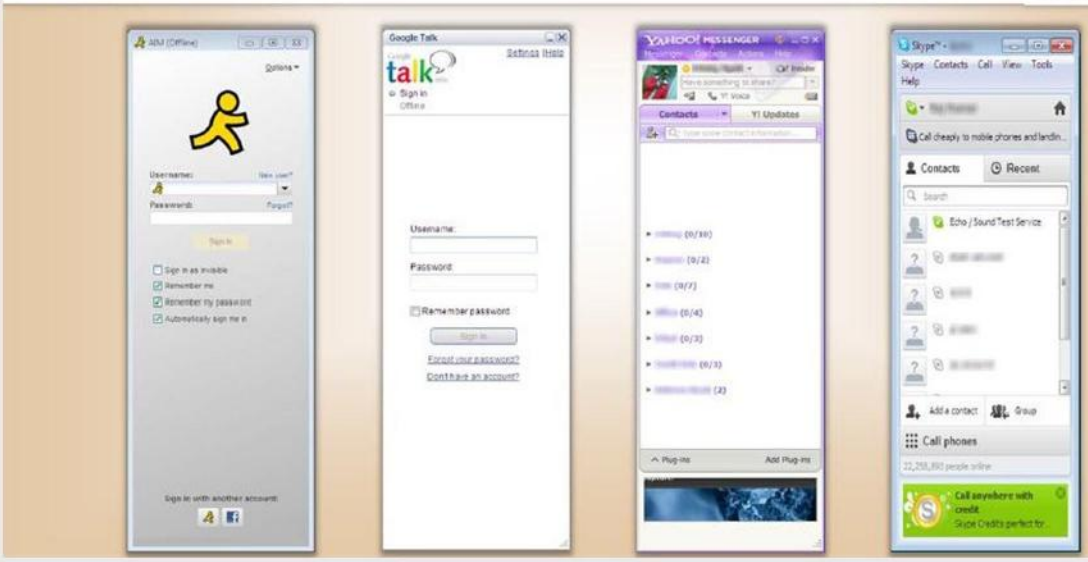
گوگل کروم: تنظیمات امنیتی



- Secure Sockets Layer (SSL) یک پروتکل اینترنتی است‌که توسط بسیاری از وب سایت ها برای اطمینان از رمزگذاری و انتقال امن داده مورد استفاده قرار می گیرد
- تنظیمات SSL در مرورگرهای وب به صورت پیش فرض فعال است
- برخی از وب سایت ها به نسخه قدیمی تر SSL 2.0 نیاز دارند، در چنین شرایطی تیک گزینه Use SSL 2.0 را بزنید
- گزینه check for server certificate revocation را برای فعالسازی تأیید لحظه ای اعتبار گواهی نامه ی وب سایت تیک بزنید

پیام رسان فوری(IMing)

پیام رسان فوری(IMing) به کاربر امکان می دهد که با استفاده از برنامه های نرم افزاری بتواند با دیگران از طریق اینترنت ارتباط برقرار نماید



مسائل امنیتی پیام رسان فوری

IMWorm

- کرمی که موجب آسیب رساندن به کامپیوتر شده و تمامی مخاطبین موجود در لیست مخاطب IM را آلوده می کند
- IMWorm تلاش می کند خود را به تمام مخاطبین موجود در لیست مخاطب کاربر ارسال نماید

مهندسی اجتماعی

- مهندسی اجتماعی از طریق تعاملات انسانی صورت می گیرد، این تعاملات شامل فریب دادن افراد از طریق IM و به دست آوردن اطلاعات شخصی آن ها می باشد

اسپم از طریق IM(SPIM)

- SPIM اسپمی است که به جای ایمیل، از طریق IM ارسال می گردد
- سیستم های IM مانند یاهو مسنجر، AIM، Windows Live messenger و چت روم ها در شبکه های اجتماعی از جمله مواردی هستند که توسط فرستندگان اسپم هدف قرار داده می شوند

اقدامات امنیتی برای پیام رسان های فوری

جستجو در وب

اخبار داخلی

برگزاری همایش بررسی روش‌های نوین پدافند سایبری

در تاریخ ۲۱ آبان ۱۳۹۸، همایش بررسی روش‌های نوین پدافند سایبری، با میزبانی مرکز تخصصی آپا دانشگاه رازی و با همکاری اداره فناوری اطلاعات استان، در سالن همایش سازمان مدیریت و برنامه‌ریزی استان برگزار گردید. این مراسم با هدف آشنایی با حملات سایبری نسل جدید، راهکارهای مقابله با آن‌ها و نیز پیاده‌سازی راهکارهای عملیاتی برگزار شد.

حامد منکرسی، مدیر مرکز تخصصی آپا دانشگاه رازی کرمانشاه در خصوص سخنرانان این همایش، افزود: در این همایش شهریار بهنیا مدیرکل ارتباطات و فناوری اطلاعات استان به بیان اقدامات انجام شده در استان در راستای افزایش امنیت سایبری، غلامرضا مرتضوی، مدیرکل پدافند غیرعامل استان به بیان اهمیت امنیت سایبری در پدافند غیرعامل و همچنین افشین کریمی معاون توسعه مدیریت و منابع استانداری کرمانشاه به اهمیت توجه به توسعه امنیت سایبری در مدیریت استان پرداختند.

در این همایش مفهوم شکار تهدیدات سایبری (threat hunting) توسط دکتر حامد منکرسی تشریح شد. ایشان همچنین به لزوم توجه سازمانها به امر آموزش در راستای تربیت شکارچیان خطرات و تهدیدات سایبری در سازمانها پرداختند. بیان شد که با تکیه صرف به ابزارهای امنیتی نمی توان حملات پیچیده به ویژه حملات APT را تشخیص داد.

در ادامه، سند جامع امنیت فناوری اطلاعات کشور توسط فرهاد مردوخی مدیر آزمایشگاه معماری سازمانی دانشگاه رازی، بررسی چالش‌ها و مشکلات پیش‌روی دفاع سایبری در کشور توسط محمد ایمانی مدیر فناوری اطلاعات استانداری کرمانشاه و راهکارهای مقابله با حملات سایبری نوین توسط حصاری مقدم انجام شد.

در پایان نیز حامد منکرسی در رابطه با آغاز دور جدید ثبت‌نام دوره‌های آموزشی مرکز آپا، که با هدف افزایش آگاهی و ارتقاء امنیت در سطح استان برگزار می‌گردد اشاره نموده و خاطرنشان کردند که مرکز آپا در راستای انجام رسالت خویش، دوره‌های آموزشی مرتبط با این حوزه را به صورت فصلی و دوره‌ای برگزار نموده و آماده‌ی هر گونه آگاهی‌رسانی، امداد و پشتیبانی در زمینه امنیت سایبری می‌باشد.

این مراسم با جلسه پرسش و پاسخ میان سخنرانان همایش و افراد حاضر در سالن، در خصوص نحوه اجرای راهکارهای عملی در سطح استان و تشریح روش‌های نوین پدافند سایبری خاتمه یافت.


مرکز تخصصی آپا دانشگاه رازی