بولتن خبری

مرکز تخصصی آپا دانشگاه رازی

شماره هفدهم

بهمن ماه ۱۳۹۸

باز هم سیسکو و آسیب‌پذیری‌های بحرانی

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

حذف فایل‌های پشتیبان، کپی برداری و رمزگذاری فایل‌های ویندوز توسط باج‌افزار Snake

محققان باج‌افزار جدیدی به نام Snake (به معنای مار) کشف کرده‌اند. این باج‌افزار که به زبان Golang نوشته شده است، کاربران ویندوز را به منظور رمزگذاری فایل‌های سیستم و حذف Volume Shadow Copies که سیستم‌عامل از آن برای تهیه نسخه پشتیبان استفاده می‌کند، هدف قرار می‌دهد.

باج‌افزار Snake دارای ساختاری هدفمند است که شامل ویژگی‌های یک باج‌افزار استاندارد و برخی عملکردهای پیچیده‌تر است.

توسعه‌دهندگان این باج‌افزار، زبان Golang را برای نوشتن برخی از جدیدترین خانواده‌های باج‌فزار انتخاب کرده و برخی از RaaS (Ransomware as a Service) ها را بکار می‌گیرند زیرا برای تمام پلتفرم‌ها، انعطاف‌پذیر و کاملاً اپن سورس است.

به اعتقاد محققان، این باج‌افزار می‌تواند آسیب‌های بسیار جدی و خطرناکی را به سیستم‌های آلوده وارد نماید.

باج‌افزار Snake، پلتفرم‌های خاص مانند SCADA، ابزارهای مدیریت سازمان، برنامه‌های کاربردی سیستم و همچنین برخی از برنامه‌های کاربردی خاص از جمله VMware Tools، Microsoft System Center Operations Manager، Nimbus، Honeywell HMIWeb و FLEXnet را مورد هدف قرار می‌دهد.

فرآیند آلوده کردن باج‌افزار Snake

پس از آلوده شدن سیستم توسط باج‌افزار مذکور، فایل‌های مربوطه با داده‌های رمزگذاری شده بازنویسی می‌شوند و پسوند فایل‌های رمزگذاری شده به "EKANS" تغییر می‌کند. همچنین به فایل‌های تغییر یافته، کاراکترهای تصادفی اضافه شده که باعث می‌شود تشخیص خانواده این باج‌افزار خاص، مشکل‌تر گردد.

Name	Date modified	Type
7z1900-x64.exevQycM	1/21/2020 1:53 PM	EXEVQYCM File
ClassicShellSetup_4_3_1.exeZkiPv	1/21/2020 1:53 PM	EXEZKIPV File
GoogleChromeEnterpriseBundle64.zipaZIyo	1/21/2020 1:53 PM	ZIPAZIYO File
python-3.7.4.exeHbcMu	1/21/2020 1:53 PM	EXEHBCMU File
sn1.exeenOBt		EXEENOBT File
snake1.exeVbJVL	1/21/2020 1:53 PM	EXEVBJVL File

توسعه‌دهندگان بدافزار، از هر دو رمزنگاری متقارن و نامتقارن برای رمزگذاری فایل‌های سیستم قربانی استفاده کرده‌اند.

یک کلید متقارن برای رمزگذاری و رمزگشایی فایل‌ها مورد نیاز است، در این حالت، کلید متقارن برای رمزگذاری فایل‌های قربانی با کلید عمومی مهاجم استفاده می‌شود و فرآیند رمزگشایی تنها با داشتن کلید خصوصی مهاجمان امکان‌پذیر است.

از آنجاییکه مهاجمان از key lengths (AES-256, RSA-2048) استفاده می‌کنند، این امر باعث می‌شود شکستن کلید و رمزگشایی داده‌ها غیرممکن شود.

باج‌افزار Snake، فرآیندهای مختلف سیستم که در تصویر زیر لیست آنها مشخص شده است را خاتمه می‌دهد.

bluestripecollector.exe	msmdsrv.exe	prproficymgr.exe
ccflic0.exe	musnotificationux.exe	prrds.exe
ccflic4.exe	n.exe	prreader.exe
cdm.exe	nimbus.exe	prrouter.exe
certificateprovider.exe	npmdagent.exe	prschedulemgr.exe
client.exe	ntevl.exe	prstubber.exe
client64.exe	ntservices.exe	prsummarymgr.exe
collwrap.exe	pralarmmgr.exe	prwriter.exe
config_api_service.exe	prcalculationmgr.exe	reportingservicesservice.exe
dsmcsvc.exe	prconfigmgr.exe	server_eventlog.exe
epmd.exe	prdatabasemgr.exe	server_runtime.exe
erlsrv.exe	premailengine.exe	spooler.exe
fnplicensingservice.exe	preventmgr.exe	sqlservr.exe
hasplmv.exe	prftpengine.exe	taskhostw.exe
hdb.exe	prgateway.exe	vgauthservice.exe
healthservice.exe	prlicensemgr.exe	vmacthlp.exe
ilicensesvc.exe	proficy administrator.exe	vmtoolsd.exe
inet_gethost.exe	proficyclient.exe	win32sysinfo.exe
keysvc.exe	proficypublisherservice.exe	winvnc4.exe
managementagenthost.exe	proficyserver.exe	workflowresttest.exe
monitoringhost.exe	proficysts.exe	
msdtssrvr.exe	prprintserver.exe	

مطابق تحقیقات SentinelOne، اگر این حمله با سطح دسترسی ادمین اجرا شود، یادداشت‌های تصادفی در مسیر c:\users\public\desktop\Fix-Your-Files.txt نوشته می‌شوند در غیر این صورت در مسیر c:\users\AppData\Local\VirtualStore نوشته خواهند شد.

هنگامیکه Snake فرآیند آلوده کردن سیستم را کامل و فایل‌های آن را رمزگذاری کرد، پس از آن یادداشت‌های مربوط به خود را که حاوی جزئیاتی در مورد چگونگی رمزگشایی فایل‌هاست، حذف می‌کند.

```
| What happened to your files?

We breached your corporate network and encrypted the data on your computers.
    The encrypted data includes documents, databases, photos and more -

all were encrypted using a military grade encryption algorithms (AES-256 and
    RSA-2048). You cannot access those files right now. But dont worry!

You can still get those files back and be up and running again in no time.

| How to contact us to get your files back?

The only way to restore your files is by purchasing a decryption tool loaded
    with a private key we created specifically for your network.

Once run on an effected computer, the tool will decrypt all encrypted files -
    and you can resume day-to-day operations, preferably with

better cyber security in mind. If you are interested in purchasing the
    decryption tool contact us at bapcocrypt@ctemplar.com

| How can you be certain we have the decryption tool?

In your mail to us attach up to 3 files (up to 3MB, no databases or
    spreadsheets).

We will send them back to you decrypted.
```

یادداشت باج‌افزار

به جای ارائه آدرس وب برای دریافت باج، به قربانیان گفته می‌شود تا از طریق آدرس ایمیل موجود در یادداشت باج‌افزار "bapcocrypt @ ctemplar.com" برای دریافت کلید رمزگشایی از مهاجم، با آنها تماس گرفته شود.

منبع خبر :

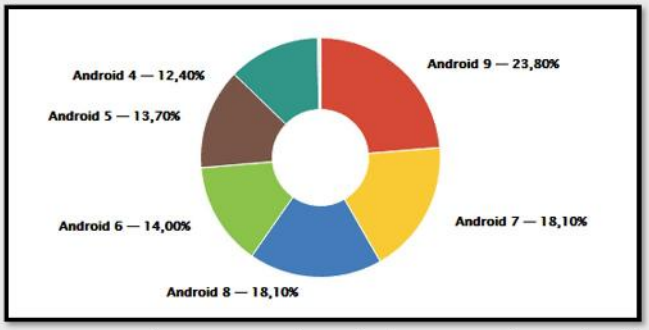
https://gbhackers.com/snake-ransomware/

Scan Link

انتشار نسخه جدید بدافزار Android.Xiny اندروید

محققان نوع جدیدی از بدافزار ارتقاء یافته Android.Xiny را کشف کرده‌اند. این بدافزار تنها نسخه‌های قدیمی اندروید، یعنی نسخه 5.1 و قبل‌تر از آن را با هدف دستیابی به سطح دسترسی روت، مورد حمله قرار می‌دهد. طبق گزارشی که در تاریخ هفتم ماه مه 2019 از طرف شرکت گوگل منتشر شد، 25.2٪ از کاربران هنوز از نسخه 5.1 و پایین‌تر اندروید استفاده می‌کنند.

با توجه به اینکه دیگر وصله امنیتی برای نسخه‌های ذکر شده اندروید منتشر نخواهد شد، بنابراین جای تعجب نیست که توسعه‌دهندگان بدافزار هنوز هم در صدد حمله به آن‌ها باشند.



با اکسپلویت این آسیب‌پذیری، مهاجمان می‌توانند در سیستم قربانی به دسترسی روت برسند و اقدامات دلخواه خود را انجام دهند.

بدافزار Android.Xiny برای اولین بار در سال 2015 فعالیت‌های خود شامل برقراری ارتباطات از راه دور، دریافت اطلاعات ورودی صفحه کلید، جمع‌آوری اطلاعات سیستم، انتقال سایر بدافزارها به سیستم و اجرای حمله انکار سرویس[1] را آغاز کرد.

علاوه بر این، بدافزار Android.Xiny.5261، برخی از برنامه‌های از پیش نصب شده و نیز برنامه‌هایی که معمولاً برای دسترسی ریشه استفاده می‌شوند را جهت آزاد شدن فضای حافظه حذف می‌کند.

[1] DOS

علاوه بر این، بدافزار Android.Xiny.5261، برخی از برنامه‌های از پیش نصب شده و نیز برنامه‌هایی که معمولاً برای دسترسی ریشه استفاده می‌شوند را جهت آزاد شدن فضای حافظه حذف می‌کند.

نسخه جدید Android.Xiny

براساس پست منتشر شده در وبلاگ Dr.Web: "نسخه‌ی جدید این بدافزار دارای مکانیزم دفاعی دو لایه‌ای است که با استقرار در دستگاه قربانی، آن دسته از اپلیکیشن‌هایی که به کاربر دسترسی روت می‌دهند را حذف کرده و این در حالیست که فایل کتابخانه‌ی تغییریافته libc.so این بدافزار، مانع از نصب مجدد این برنامه‌ها توسط کاربر می‌شود."

مهاجمان با اکسپلویت این آسیب‌پذیری می‌توانند به سطح دسترسی روت دست پیدا کرده و از این طریق ماژول نصب‌کننده را راه‌اندازی کنند، پس از آن، "/system/bin/debuggerd" و "/system/bin/debuggerd" جهت راه‌اندازی خودکار، و نیز دایرکتوری‌های سیستم بروزرسانی می‌شوند. این بدافزار حاوی لیستی از اپلیکیشن‌ها و فایل‌هایست که جهت آزاد کردن فضای دستگاه، حذف می‌شوند. فایل بعدی نسخه‌ی پیشرفته libc.so است که جایگزین نسخه‌ی اصلی می‌شود. مهاجمان این تغییرات را با هدف مسدود کردن برنامه‌های با دسترسی روت، انجام می‌دهند.

اگر دستگاه شما به این بدافزار آلوده شد، بهترین راه نصب مجدد یک سیستم‌عامل بر روی آن است، اما به خاطر داشته باشید که ممکن است این عمل منجر به حذف تمامی اطلاعات شما شود.

منبع خبر :

https://gbhackers.com/android-xiny-malware/

Scan Link

حذف 197 افزونه‌ی مخرب از مرورگر FIREFOX توسط MOZILLA

طی دو هفته‌ی گذشته، تیم بررسی Mozilla add-on، 197 افزونه‌ی (add-on) مرورگر Mozilla را به دلیل اجرای کد مخرب، سرقت اطلاعات کاربر یا استفاده از ابهام سازی جهت مخفی‌کردن کد منبعشان، ممنوع ساخته است.

Mozilla به‌منظور جلوگیری از نصب جدید این افزونه‌های مخرب، آن‌ها را از پورتال Add-on حذف و در مرورگرهای کاربرانی که قبلاً آن‌ها را نصب کرده‌اند، غیرفعال کرده است.

اکثر این ممنوعیت‌ها، مربوط به 129 افزونه‌ی ارایه‌شده توسط 2Ring (ارایه‌دهنده‌ی نرم‌افزار B2B) است. اجرای این ممنوعیت بدین دلیل است که این افزونه‌ها کد را از یک کارگزار راه‌دور دانلود و اجرا می‌کنند. در حالیکه طبق قوانین Mozilla، افزونه‌ها باید تمامی کدهایشان را از خودشان داشته باشند و نباید کد را به صورت پویا از مکان‌های راه دور دانلود کنند. دانلود کد از یک کارگزار راه‌دور به عاملین تهدید اجازه می‌دهد کد مخرب را زمانی که یک بار به صورت پویا از یک کارگزار تحت کنترلشان دانلود می‌شود، درون مرورگر اجرا کنند.

شش افزونه‌ی ارایه‌شده توسط Tamo Junto Caixa و سه افزونه‌ای که به نظر می‌آمد محصولات جعلی حق اشتراک (premium) باشند نیز به دلیل دانلود و اجرای کد راه دور ممنوع شده‌اند.

برخی از ممنوعیت‌ها به دلیل جمع‌آوری غیرقانونی اطلاعات کاربران اعمال شده‌اند. کارمندان Mozilla یک افزونه‌ی بی‌نام، افزونه‌های WeatherPool and Your Social، Pdfviewer-tools، RoliTrade و Rolimons Plus را به دلیل جمع‌آوری غیرقانونی اطلاعات کاربران ممنوع کرده‌اند.

این ممنوعیت‌ها به دلیل رفتارهای مخرب افزونه‌ها نیز بر روی آن‌ها اعمال شده است. بازرسان Mozilla، 30 افزونه را که انواع مختلف رفتارهای مخرب را نمایش می‌دادند، ممنوع کردند. موزیلا فقط شناسه‌های این افزونه‌ها را ذکر کرده است، نه نامشان. بنابراین توسعه‌دهندگان این افزونه‌ها می‌توانند با حذف رفتار مخرب افزونه‌هایشان، در مورد ممنوعیتشان درخواست تجدیدنظر کنند. یکی از افزونه‌هایی که مراحل تجدیدنظر را پشت سر گذاشته است، افزونه‌ی Like4Like.org است. گویا این افزونه ابتدا اعتبارنامه‌ها یا نشانه‌های (token) وب‌سایت‌های رسانه‌های اجتماعی را جمع‌آوری و به سایتی دیگر ارسال می‌کرد. رفتار مخرب دیگر، در افزونه‌ی FromDocToPDF کشف شده است. به گفته‌ی مهندسان Mozilla، این افزونه محتوای راه دور را به برگ جدیدی از Firefox بارگذاری می‌کرد. افزونه‌ی دیگری از Firefox به نام Fake Youtube Downloader نیز به دلیل تلاش برای نصب بدافزار دیگری در مرورگرهای کاربران، ممنوع شده است.

افزونه‌هایی همچون EasyScarch for Firefox، EasyZipTab، FlixTab، ConvertToPDF و FlixTab Search نیز برای بریدن و جمع‌آوری عبارت‌های جستجویی کاربران (یک جرم به وضوح قابل ممنوع شدن) ممنوع شدند.

کارمندان امنیتی Mozilla، دسته‌های دوتایی، نه‌تایی و سه‌تایی از افزونه‌ها را به دلیل استفاده از کد مبهم (روشی که ارایه‌دهندگان افزونه با استفاده از آن، خواندن کد را به منظور مخفی‌کردن رفتار مخرب افزونه، دشوار می‌سازند) ممنوع کردند.

به نظر می‌رسد این حرکت Mozilla در ادامه‌ی بررسی مستحکم او از افزونه‌های مرورگر به منظور حفظ حریم شخصی کاربران است. Mozilla در ماه دسامبر سال 2019 نیز، افزونه‌های Avast و AVG را از Firefox بدین دلیل که مشکوک به جاسوسی‌کردن کاربران بودند، حذف کرد.

از آنجاییکه بسیاری از افزونه‌ها توسط ارایه‌دهندگان شناخته‌شده نوشته نشده‌اند، بنابراین بهتر است هنگام استفاده از آن‌ها دقت بیشتری اعمال شود:

- تا آنجا که ممکن است افزونه‌های کمتر و تنها از فروشگاه‌های رسمی نصب شوند.
- نظرات و بازخوردهای کاربرانی که افزونه‌ی موردنظر را نصب کرده‌اند حتماً مورد بررسی

قرار گیرد.

- به اعتبار توسعه‌دهنده، اینکه چه میزان در مقابل سؤالات مسئولیت‌پذیر هستند و اینکه هر چند وقت یک بار نسخه‌های به‌روزرسانی را ارسال می‌کنند توجه شود.
- مجوزهای درخواست‌شده مورد مطالعه قرار گیرد (در Firefox, Options > Extensions and Themes > Manage) و بررسی شود آیا مطابق با ویژگی‌های افزونه است یا خیر. اگر این مجوزها تغییر کردند باید نسبت به آن‌ها مشکوک شد.

منبع خبر :
https://cert.ir/news/12883

Scan Link

اخبار کوتاه

سوءاستفاده هکرها از بحران ویروس کرونا برای انتشار بدافزار

متخصصان موسسه امنیتی IBM X-Force از حملات سایبری جدیدی خبر داده‌اند که در آن هکرها ایمیلی را به قربانیان خود ارسال کرده و مدعی نفوذ کرونا ویروس به کشور می‌شوند. در این ایمیل فایل‌هایی قرار دارد که ظاهرا حاوی اسناد راهنما در مورد ویروس کرونا است اما در واقع آلوده بوده و به محض دانلود شروع به نصب بدافزار Emotet می‌کند. این بدافزار نه تنها اجازه سرقت اطلاعات مهم کاربر را به هکر می‌دهد بلکه امکان انتقال فایل‌های خطرناک از جمله باج‌افزار را به سیستم قربانی فراهم می‌سازد.

هشدار در خصوص خطرات شارژ تلفن همراه در اماکن عمومی

مهاجمان و هکرها به‌راحتی می‌توانند به تجهیزات هوشمند شما دسترسی داشته باشند! هکرها با دست‌کاری و فروش سیم شارژرهای غیراستاندارد و نصب تجهیزات انتقال داده در آن‌ها و یا دست‌کاری ایستگاه‌های شارژ عمومی در سطح شهر، امکان دسترسی به دستگاه‌های مردم را از راه دور فراهم یا بدافزار خاصی را وارد دستگاه‌های هوشمند مردم می‌کنند و همچنین می‌توانند عکس‌های تلفن قربانی را به‌منظور باج‌گیری یا آلوده کردن دستگاه با ویروس از راه دور دانلود کنند. کارشناسان به کاربران توصیه کردند سعی کنند از ایستگاه‌های شارژ در اماکن عمومی خودداری کنند و یک منبع تغذیه قابل‌حمل (پاور بانک) را برای شارژ دستگاه هوشمند خود در بیرون از منزل یا کابل‌های USB که فاقد قابلیت انتقال داده هستند و مخصوص شارژ هستند استفاده نمایند.

اپلیکیشن‌های نامعتبر را جهت دریافت رمز یکبار مصرف نصب نکنید

افراد سودجو ، با توجه به اجرای طرح دریافت رمز دوم یکبار مصرف پویا اقدام به تبلیغ و ارائه خدمات به شهروندان با طراحی اپلیکیشن‌های جعلی سعی دارند اعتماد کاربران را در فضای مجازی جلب نمایند. تا شهروندان را قربانی برخی اهداف شوم خود کنند. با دانلود و نصب این اپلیکیشن‌ها سرقت اطلاعات ذخیره شده بر روی گوشی همراه یا سیستم‌ها صورت می‌گیرد. استفاده از رمز یکبار مصرف گام مهمی برای حفظ امنیت اطلاعات مالی کاربران بوده لذا کاربران برای فعال‌سازی رمز یکبار مصرف حتما با مراجعه به سایت بانک مربوطه، راهنمای فعال کردن رمز یکبار مصرف را مطالعه کنند و جهت دریافت اپلیکیشن رمز پویا به فروشگاه‌های معتبر و یا شعب بانک مراجعه کنند.

فریب تبلیغات کاذب اینترنتی را نخورید

یکی از آسیب‌های مهم که اکثر افراد با آن درگیر هستند، کلاهبرداری اینترنتی است که در نهایت منجر به برداشت غیرمجاز از حساب بانکی مالباختگان می شود. خرید در بستر فضای مجازی باید از طریق فروشگاه‌های معتبر دارای نماد اعتماد الکترونیکی ENAMAD باشد. کاربران مراقب باشند فریب تبلیغات کاذب افراد کلاهبردار را نخورند.

بدافزار Emotet با الگوی اسپم اخاذی می‌کند

بدافزار Emotet با یک الگوی اسپم شروع کرده و وانمود می‌کند که کامپیوتر گیرنده، هک شده و داده‌های آن‌ها به سرقت برده شده است.

Emotet از طریق ایمیل‌های اسپم، توزیع شده و معمولاً از الگوهای مبتنی بر یک موضوع خاص مانند نامه‌های صوتی، اسناد اسکن شده، گزارش‌ها و فاکتورها استفاده می‌کنند. هدف همه این ایمیل‌ها فریب گیرنده ایمیل در جهت باز کردن یک سند ضمیمه Word بوده که از آن طریق سعی در بارگذاری و نصب بدافزار Emotet روی کامپیوترها دارند.

بعد از آن، این بدافزار از طریق کامپیوترهای آلوده برای ارسال بیشتر اسپم‌های مخرب، بارگذاری و نصب سایر بدافزارها بر روی دستگاه‌ها استفاده می‌کند.

از تابستان 2018 در حال ارسال ایمیل‌هایی هستند که بیان می‌کنند کامپیوتر گیرنده ایمیل هک شده است و مهاجم ویدویی از شما ثبت کرده است. مهاجمان در ایمیل‌های ارسالی تهدید می‌کنند در صورت عدم پرداخت مبلغی مشخص، ویدیوی ضبط شده آن‌ها را به دوستان و خانواده گیرنده ارسال می‌کنند.

این ایمیل‌ها کلاهبرداری بوده و مهاجمان هیچ گونه ویدیویی در دسترس ندارند، اما مردم را به اندازه کافی ترسانده‌اند که در یک هفته بیش از 50 هزار دلار پرداخته شده است. در یک الگوی جدید مهاجمان بیان می‌کنند که رایانه‌تان هک شده است و داده‌های شما به سرقت رفته است.

در ادامه، در ایمیل به کاربران گفته می‌شود جهت دستورالعمل پرداخت مبلغ مشخص، فایل ضمیمه پیوستی را باز کنند که در غیر صورت اطلاعات به سرقت رفته آن‌ها فروخته می‌شود.

با توجه به شدت آلودگی این بدافزار، کاربران باید نسبت به هرگونه ایمیل ناشناسی که دریافت می‌کنند، حساس باشند، مخصوصا در مواردی که ایمیل دارای پیوست‌های Word باشد.

کاربران به جای باز نمودن پیوست ایمیل‌های مشکوک، باید با فرستنده ایمیل تماس بگیرند و یا موضوع را با سرپرست شبکه خود در میان بگذارند.

آسیب پذیری

کشف 5 آسیب پذیری بحرانی روز صفرم در پروتکل Discovery سیسکو

محققان 5 آسیب‌پذیری بحرانی را با عنوان CDPwn در پروتکل Discovery سیسکو که در چندین محصول سیسکو از جمله روترها، سوئیچ‌ها، تلفن‌های تحت شبکه و دوربین ها مورد استفاده قرار می‌گیرد، کشف کردند.

پروتکلDiscovery، که با عنوان CDP هم شناخته می‌شود، یک پروتکل اختصاصی لایه 2 شبکه است که در محصولات سیسکو مورد استفاده قرار می‌گیرد.

چهار مورد از این 5 آسیب‌پذیری، آسیب‌پذیری‌های اجرای کد از راه دور (RCE) هستند که 10 میلیون کاربر را تحت تأثیر قرار داده‌اند و به مهاجمان این امکان را می‌دهند تا دستگاه‌های آسیب‌پذیر را به طور کامل و بدون هیچ گونه تعاملی از جانب کاربر، کنترل نمایند.

یکی از این آسیب‌پذیری‌ها نیز موجب حمله Denial of Service (DoS) در FXOS، IOS XR و نرم‌افزار NX-OS سیسکو در روترهای هدف می‌شود و به نوبه خود، باعث اختلال کامل شبکه‌های هدف می‌گردد.

دستگاه‌های تحت تأثیر

چندین دستگاه Enterprise تحت تأثیر این آسیب‌پذیری‌های روز صفرم قرار دارند و اکسپلویت موفق آنها باعث ایجاد خسارات شدید در ده‌ها میلیون دستگاه شبکه در شرکت ها و سازمان‌ها خواهد شد.

لیست دستگاه‌های آسیب‌پذیر به شرح زیر است:

روترها:

- روترهای Aggregation Services سری ASR 9000

- (Carrier Routing System (CRS
- Firepower سری 1000
- Firepower سری 2100
- Firepower سری 4100
- Firepower 9300 Security Appliances
- روتر IOS XRv 9000
- روترهای White box اجرا کننده IOS XR سیسکو

سوئیچ‌ها:

- Nexus 1000 Virtual Edge
- سوئیچ Nexus 1000V
- سوئیچ‌های سری Nexus 3000
- سوئیچ‌های سری Nexus 5500
- سوئیچ‌های سری Nexus 5600
- سوئیچ‌های سری Nexus 6000
- سوئیچ‌های سری Nexus 7000
- سوئیچ‌های فابریک سری Nexus 9000
- سوئیچ‌های Multilayer سری MDS 9000
- (Network Convergence System (NCS سری 1000
- (Network Convergence System (NCS سری 5000
- روترهای Network Convergence System (NCS) 540
- (Network Convergence System (NCS سری 5500
- روترهای Network Convergence System (NCS) 560
- (Network Convergence System (NCS سری 6000
- Fabric Interconnects سری UCS 6200
- Fabric Interconnects سری UCS 6300
- Fabric Interconnects سری UCS 6400

IP Phones (تلفن‌های تحت شبکه):

- IP Conference Phone 7832
- IP Conference Phone 8832
- IP Phone 6800 Series
- IP Phone 7800 Series
- IP Phone 8800 Series
- IP Phone 8851 Series
- Unified IP Conference Phone 8831
- Wireless IP Phone 8821
- Wireless IP Phone 8821-EX

IP Cameras (دوربین‌های تحت شبکه):

- دوربین‌های Video Surveillance سری 8000

4 آسیب‌پذیری اجرای کد از راه دور

مهاجمان می‌توانند با ارسال پکت‌های جعلی و مخرب CDP به دستگاه‌های مورد هدف سیسکو، هر 4 آسیب‌پذیری موثر بر اجرای جداگانه مکانیزم CDPرا مورد اکسپلویت قرار دهند.

1. آسیب‌پذیری اجرای کد از راه دور در پروتکل Discovery در نرم‌افزار NX-OS سیسکو

آسیب‌پذیری سرریز پشته در تجزیه پکت‌های CDP که نرم‌افزار NX-OS سیسکو را تحت تأثیر قرار داده است، به مهاجمان اجازه می‌دهد تا به دلیل یک پکت CDP شامل قسمت‌های زیادی از درخواست PoE(Power over Ethernet) اقدام به تریگر نمایند.

مهاجم با ارسال یک پکت مجاز CDP با سطح قدرت بیشتر از تعداد کل توان دریافتی مورد انتظار سوئیچ، می‌تواند موجب سرریز پشته شود و کنترل کاملی بر روی سوئیچ و زیرساخت شبکه پیدا کند.

شناسه اختصاص داده شده به این آسیب‌پذیری "CVE-2020-3119" می‌باشد.

2. حملات RCE و DOS در Cisco Voice over IP Phone

این آسیب‌پذیری، با سرریز پشته در تابع تجزیه کننده Port ID، می‌تواند برای اجرای کد در تلفن تحت شبکه مورد اکسپلویت قرار گیرد.

مهاجمان می‌توانند با ارسال پکت جعلی و مخرب CDP به صورت مستقیم از داخل سوئیچ دستگاه‌های مورد هدف، این آسیب‌پذیری را در تلفن‌های تحت شبکه، تریگر نمایند.

شناسه اختصاص داده شده به این آسیب‌پذیری "CVE-2020-311" می‌باشد.

3. آسیب‌پذیری CDP Format String در IOS-XR سیسکو

این آسیب‌پذیری هنگام تجزیه فیلدهای رشته‌ای خاص مانند شناسه دستگاه و شناسه پورت برای بسته‌های CDP ورودی در اجرای CDP در نرم‌افزار IOS XR رخ می‌دهد. در این حالت، مهاجم برای کنترل پارامتر رشته که منجر به سرریز پشته می‌شود اقدام به اجرای کد از راه دور کرده و کنترل کامل روتر هدف را بدست می‌آورد.

آسیب‌پذیری مذکور با شناسه "CVE-2020-3118" شناخته می‌شود.

4. حملات RCE و DOS در CDP دوربین‌های سری Video Surveillance 8000 سیسکو

آسیب‌پذیری سرریز Heap در تجزیه بسته‌های CDP در دوربین‌های سری 8000 سیسکو به مهاجمان اجازه می‌دهد تا پس از رسیدن به شرایط لازم، اقدام به اجرای کد از راه دور نمایند.

شناسه آن "CVE-2020-3110" است.

شدت خطر آسیب‌پذیری‌های ذکر شده

براساس گزارش Armis، اکسپلویت آنها می‌تواند منجر به موارد زیر گردد:

- اختلال در قطعه بندی شبکه

- سرقت داده‌های ترافیک شبکه که از طریق روترها و سوئیچ‌های سازمان عبور می‌کنند
- دسترسی به سایر دستگاه‌ها با حملات man-in-the-middle از طریق جداسازی و تغییر ترافیک سوئیچ
- سرقت داده‌ها و اطلاعات حساس مانند تماس‌های تلفنی از دستگاه‌هایی همچون تلفن‌های شبکه و ویدئوهای دوربین‌های تحت شبکه

بروزرسانی امنیتی سیسکو

سیسکو با رفع تمام این آسیب‌پذیری‌ها ، وصله‌های امنیتی را نیز برای دستگاه‌های آسیب‌دیده منتشر کرده است. به کارکنان سازمان‌ها توصیه می‌شود که در اسرع وقت وصله‌های امنیتی را اعمال نمایند.

منبع خبر :

https://gbhackers.com/zero-day-vulnerability-affected-cisco-cdp-devices/

Scan Link

آسیب‌پذیری بحرانی OpenSMTPD و حمله مهاجمان به میل سرورهای لینوکس و OpenBSD

محققان امنیت سایبری یک آسیب‌پذیری بحرانی جدید با شناسه "CVE-2020-7247" را در سرور ایمیل OpenSMTPD کشف کرده‌اند که می‌تواند به مهاجمان از راه دور اجازه دهد تا کنترل کامل BSD و بسیاری از سرورهای مبتنی بر لینوکس را بدست گیرند.

OpenSMTPD یک پیاده‌سازی این سورس از پروتکل سمت سرور SMTP است که در ابتدا به عنوان بخشی از پروژه OpenBSD توسعه داده شد اما در حال حاضر بر روی بسیاری از سیستم‌های مبتنی بر یونیکس به صورت از پیش نصب شده وجود دارد.

طبق تحقیقات آزمایشگاه Qualys -کاشف این آسیب‌پذیری- این نقص مربوط به تابع اعتبارسنجی آدرس فرستنده‌ی OpenSMTPD، به نام ()smtp_mailaddr است که می‌تواند برای اجرای دستورات دلخواه shell با بالاترین سطح دسترسی روت، بر روی یک سرور آسیب‌پذیر و تنها با ارسال پیام‌های جعلی خاص به آن سرور، مورد اکسپلویت قرار گیرد.

آسیب‌پذیری ذکر شده، نسخه 6.6 سیستم‌عامل OpenBSD را تحت تأثیر قرار می‌دهد.

به گفته محققان، اکسپلویت این آسیب‌پذیری از لحاظ تعداد کاراکترها محدودیت‌هایی دارد (حداکثر 64 کاراکتر مجاز است) و کاراکترها باید محدود شوند ('$', '|').

محققان Qualys توانستند با استفاده از تکنیکی برگرفته از کرم Morris (یکی از اولین کرم‌های رایانه‌ای که از طریق اینترنت توزیع می‌شود) با اجرای بدنه ایمیل به عنوان یک شل اسکریپت Sendmail، به این محدودیت‌ها غلبه کنند.

علاوه براین، محققان همچنین یک کد اثبات مفهومی را برای تشریح آسیب‌پذیری OpenSMTPD منتشر کرده‌اند. آنها وجود این آسیب‌پذیری را به توسعه دهندگان OpenSMTPD گزارش داده‌اند و به دنبال آن، نسخه OpenSMTPD p16.6.2 به همراه یک وصله امنیتی و همچنین یک بروزرسانی برای کاربرانOpenBSD منتشر شده است.

به کاربران توصیه می‌شود هر چه سریع‌تر این وصله امنیتی را اعمال نمایند.

منبع خبر :

https://thehackernews.com/2020/01/openbsd-opensmtpd-hacking.html

Scan Link

آسیب‌پذیری در Microsoft Azure و کنترل سرورهای ابری توسط مهاجمان

محققان امنیت سایبریِ Check Point در تاریخ 30 ژانویه 2020، جزئیات دو آسیب‌پذیری خطرناک و وصله شده را در سرویس‌های Azure مایکروسافت افشا کردند که در صورت اکسپلویت آن‌ها، مهاجمان می‌توانند چندین کسب و کار که برنامه‌های وب و برنامه‌های تلفن همراه خود را در Azure اجرا می‌کنند، مورد هدف قرار دهند.

Azure App Service یک سرویس یکپارچه و کاملاً مدیریت شده است که به کاربران امکان می‌دهد تا برنامه‌های وب و موبایل مورد نظر خود را بر روی هر پلتفرم دلخواه ایجاد کنند و جهت انجام خودکارِ فرآیندهای تجاری، به راحتی آن‌ها را با راه حل‌های SaaS[1] و اپلیکیشن‌های ON-PREMISE[2] ادغام کنند.

براساس گزارشی که محققان با The Hacker News به اشتراک گذاشتند، اولین آسیب‌پذیری امنیتی با شناسه‌ی "CVE-2019-1234" یک حمله جعل درخواست است که Azure Stack را تحت تأثیر قرار می‌دهد. Azure Stack یک راه‌حل نرم‌افزاری محاسبات ابری ترکیبی توسط مایکروسافت است.

در صورت اکسپلویت آسیب‌پذیری ذکر شده، مهاجمان قادر خواهند بود به اسکرین‌شات‌ها و اطلاعات حساس هر ماشین مجازی که در بستر Azure روی یک ماشین مجازی مشترک، اختصاصی و یا مجزا در حال اجراست دسترسی داشته باشند.

به گفته محققان این نقص از طریق Microsoft Azure Stack Portal قابل

[1] Software as a Service یا همان شیوه ارائه خدمات نرم‌افزاری بر روی فضای ابری.

[2] در گذشته ارائه خدمات نرم‌افزارهای تجاری به شکلی بود که شرکت خریدار می‌بایست سرورهای خود را با هزینه بسیار زیادی نصب و پیکربندی می‌کرد، نرم‌افزار را استقرار می‌داد و پس از مدت زمان نسبتاً زیادی، استفاده از سیستم ممکن می‌شد، این شیوه همان شیوه ON-PREMISE است.

اکسپلویت است، یک رابط کاربری که کاربران می‌توانند با استفاده از Azure Stack، به فضاهای ابری که ایجاد کرده‌اند دسترسی داشته باشند.

محققان با استفاده از API، راهی برای بدست آوردن نام و شناسه (ID) ماشین مجازی، اطلاعات سخت‌افزاری از جمله هسته‌ها و نیز حافظه ماشین مورد نظر یافتند و همانطور که در تصویر زیر قابل مشاهده است، از آن به همراه درخواست‌های غیرمجاز HTTP، جهت ربودن اسکرین‌شات‌ها استفاده می‌کنند.

آسیب‌پذیری دوم با شناسه‌ی "CVE-2019-1372"، یک نقص اجرای کد از راه دور است که Azure App Service را در Azure Stack تحت تأثیر قرار می‌دهد، این امر باعث می شود مهاجم بتواند کنترل کاملی بر روی کل سرورهای Azure داشته و در نتیجه کنترل کد تجاری شرکت را بدست آورد.

نکته‌ی جالب توجه آن است که مهاجم با ایجاد یک حساب کاربری رایگـــان توسط Azure Cloud، می‌تواند هر دو آسیب‌پذیریِ نام برده را اکسپلویت کرده و توابع مخرب را بر روی آن اجـــرا کند و همچنین از این طریق به پورتال Azure Stack کـــــاربر، درخواست‌های غیرمجاز HTTP ارسال نماید.

Check Point یک پست فنی جامع در خصوص آسیب‌پذیری دوم منتشر کرد، اما به طور خلاصه می‌توان گفت، در روش DWASSVC، یک سرویس، مسئولِ مدیریت و اجرای اپلیکیشن‌های به تصرف درآمده و نیز انجام عملیات IIS است که در واقع اپلیکیشن‌های به تصرف درآمده را اجرا کرده و با سایر Task[1] ها ارتباط برقرار می‌کند.

از آنجا که Azure Stack موفق به بررسی طول بافر، پیش از کپی حافظه در آن نشده است، لذا مهاجم می‌تواند با ارسال یک پیام ساختگیِ خاص به سرویس DWASSVC، این نقـــص را اکسپلویت کرده وکـــد مخرب را از راه دور با بـــالاتریـــــن سطـــح دسترسی (NT AUTHORITY/SYSTEM) بر روی سرور اجرا کند.

Ronen Shustin یکی از محققانِ Check Point و کسی کـــــه هر دوی ایـــــن آسیب‌پذیری‌ها را کشف کرد؛ سال گذشته این موضوع را به مایکروسافت گزارش داد و مانع از ایجاد خسارت‌های جبران ناپذیر توسط هکرها شد و این شرکت نیز در سال گذشته پس از وصله‌ی هر دو آسیب‌پذیری، 40,000 دلار به وی جایزه داد.

منبع خبر :

https://thehackernews.com/2020/01/microsoft-azure-vulnerabilities.html

Scan Link

هشـدار مایکروسـافت در خصـوص آسـیب‌پذیری روز صفـرم مرورگر Internet Explorer

مایکروسافت یک بیانیه امنیتی فوری مبنی بر هشدار به میلیون‌ها کاربر خود در خصوص آسیب‌پذیری روز صفرم مرورگر اکسپلورر صادر کرده است. این آسیب‌پذیری به صورت گسترده توسط مهاجمان مورد اکسپلویت قرار گرفته و تاکنون نیز هیچ وصله امنیتی برای آن منتشر نشده است.

آسیب‌پذیری مذکور با شناسه "CVE-2020-0674" و درجـــه شدت متوسط، در objectهای موتور اسکریپتِ حافظه‌ی مرورگر اینترنت اکسپلورر وجود دارد و منجر به اجرای کد از راه دور می‌شود و از طریق کتابخانه JScript.dll کار خود را آغاز می‌کند.

مهاجم با فریب قربانی مبنی بر باز کردن یک صفحه ساختگی وب در مرورگر آسیب‌پذیر، می‌تواند از راه دور کد دلخواه خود را بر روی سیستم قربانی اجرا کرده و کنترل کامل آن را بدست گیرد.

به گفته‌ی کارشناسان: "این آسیب‌پذیری حافظه را به گونه‌ای تخریب می‌کند که مهاجم به راحتی کد دلخواه خود را در بستر کاربر فعلی اجرا کند. مهاجمی که بتواند این آسیب‌پذیری را با موفقیت اکسپلویت نماید، می‌تواند تمامی سطوح دسترسی قربانی را به دست آورد."

"در صورتی که قربانی با سطح دسترسی ادمین وارد سیستم شده باشد، مهاجمی که موفق به اکسپلویت این آسیب‌پذیری شده است می‌تواند کنترل سیستم آسیب‌دیده را به دست گیرد، برنامه‌های مورد نظرش را نصب کند، داده‌ها را تغییر دهد، مشاهده و حذف نماید، یا می‌تواند یک حساب کاربری جدید با تمام سطوح دسترسی ایجاد کند."

مایکروسافت با اطلاع از این حملات، در تلاش است تا هر چه سریع‌تر آن‌ها را رفع نماید، و تا زمان انتشار وصله امنیتی برای این آسیب‌پذیری، به کاربران خود توصیه می‌کند تا با انجام اقدامات پیشگیرانه از حملات سایبری در امان باشند.

مرورگر اینترنت اکسپلورر نسخه‌ی 9، 10 و 11 بر روی ویندوزهای 10، 8.1 و نیز ویندوز 7، تحت تأثیر این آسیب‌پذیری قرار دارند.

راه حل مقابله در برابر حملات تا انتشار وصله امنیتی این آسیب‌پذیری!

به گفته کارشناسان، جلوگیری از بارگذاری کتابخانه JScript.dll به صـــورت دستی، می‌تواند مانع از اکسپلویت این آسیب‌پذیری شود.

برای محدود کردن دسترسی JScript.dll، دستورات زیر را با سطح دسترسی ادمین در ویندوز خود اجرا کنید:

در سیستم‌های 32 بیتی:

```
takeown / f% windir% \ system32 \ jscript.dll

cacls% windir% \ system32 \ jscript.dll / E / P everyone: N
```

[1] وظیفه

در سیستم‌های 64 بیتی:

```
takeown / f% windir% \ syswow64 \ jscript.dll
cacls% windir% \ syswow64 \ jscript.dll / E / P everyone: N
takeown / f% windir% \ system32 \ jscript.dll
cacls% windir% \ system32 \ jscript.dll / E / P everyone: N
```

و هنگامی که وصله‌ی این آسیب‌پذیری منتشر شد، کاربران باید با استفاده از دستورات زیر تنظیمات را به حالت قبل بازگردانند:

در سیستم‌های 32 بیتی:

```
cacls %windir%\system32\jscript.dll /E /R everyone
```

در سیستم‌های 64 بیتی:

```
cacls %windir%\system32\jscript.dll /E /R everyone
cacls %windir%\syswow64\jscript.dll /E /R everyone
```

لازم به ذکر است برخی از وب سایت‌ها و یا قابلیت‌های متکی به کتابخانه آسیب‌پذیر JScript.dll، ممکن است پس از غیرفعال‌سازی این کتابخانه از کار بیافتند، پس کاربران در نظر داشته باشند که به محض انتشار بروزرسانی این مرورگر، آن را اعمال نمایند.

منبع خبر :

https://thehackernews.com/2020/01/internet-explorer-zero-day-attack.html

Scan Link

امکان اجرای غیرمجاز دستورات روت در پی آسیب‌پذیری موجود در SUDO

Joe Vennix یکی از اعضای بخش امنیت شرکت اپل، آسیب‌پذیری مهم دیگری در ابزار سودو یافته است که تحت یک پیکربندی خاص، می‌تواند به برنامه‌های مخرب و یا کاربران با سطح دسترسی پایین اجازه دهد دستورات دلخواه را با سطح دسترسی روت در سیستم‌عامل لینوکس یا مک اجرا کنند.

سودو یکی از مهم‌ترین برنامه‌های قدرتمند و کاربردی است که به عنوان یک دستور اصلی از پیش نصب شده بر روی سیستم‌عامل‌های مک و تقریباً تمام سیستم‌عامل‌های مبتنی بر یونیکس یا لینوکس ارائه می‌شود.

این برنامه به گونه‌ای طراحی شده است که به کاربران اجازه می‌دهد بدون تعویض محیط خود، برنامه‌ها یا دستورات را با امتیازات کاربر دیگری اجرا کنند.

آسیب‌پذیری مذکور با شناسه‌ی CVE-2019-18634، یک مسئله‌ی سرریز بافر مبتنی بر پشته است که در نسخه‌های قبل از 1.8.26 سودو وجود دارد.

به گفته‌ی Vennix، این آسیب‌پذیری تنها در صورت فعال بودن گزینه‌ی "pwfeedback" در فایل پیکربندی "sudoers"و با رویت علامت ستاره (*) هنگام وارد کردن رمز عبور توسط کاربر، اکسپلویت می‌شود.

لازم به ذکر است گزینه‌ی pwfeedback به صورت پیش‌فرض در نسخه‌های به‌روزتر سودو و یا بسیاری از پکیج‌های دیگر، فعال نیست، اما برخی از توزیع‌های لینوکس مانند Linux Mint و Elementary OS آن را در فایل‌های پیش‌فرض "sudoers" فعال می‌کنند.

```
Exploiting the bug does not require sudo permissions, merely that
pwfeedback be enabled.

For example:

  $ perl -e 'print(("A" x 100 . "\x{00}") x 50)' | sudo -S id
    Password: Segmentation fault

There are two flaws that contribute to this vulnerability:

    1.  The "pwfeedback" option is not ignored, as it should be,
        when reading from something other than a terminal device.
        Due to the lack of a terminal, the saved version of the
        line erase character remains at its initialized value of 0.

    2.  The code that erases the line of asterisks does not
        properly reset the buffer position if there is a write
        error, but it does reset the remaining buffer length.
        As a result, the getln() function can write past the
        end of the buffer.
```

علاوه بر این، با فعال بودن گزینه‌ی pwfeedback، این آسیب‌پذیری حتی توسط کاربری که مجوز sudo را ندارد نیز می‌تواند اکسپلویت شود.

Todd C. Miller توسعه‌دهنده سودو اذعان داشت: "این نقص می‌تواند با عبور یک ورودی بزرگ به سودو از طریق pipe و هنگام بکارگیری رمز عبور، تکثیر شود، زیرا مهاجم کنترل کامل داده‌های مورد استفاده برای سرریز بافر را داشته و احتمال اکسپلویت آن زیاد است."

اگر تحت تأثیر این آسیب‌پذیری قرار گرفته‌اید، هر چه سریع‌تر به‌روزرسانی لازم را انجام دهید.

جهت بررسی آنکه آیا پیکربندی sudoers در سیستم شما تحت تأثیر این آسیب‌پذیری قرار گرفته است یا خیر، می‌توانید دستور "sudo -l" را در خط فرمان لینوکس یا macOS اجرا کنید و فعال بودن گزینه‌ی "pwfeedback" و "Matching Defaults entries" را بررسی کنید.

در صورت فعال بودن، می‌توانید با تغییر "Defaults pwfeedback" به "Defaults !pwfeedback" در فایل پیکربندی"sudoers"، مانع از اکسپلویت این آسیب‌پذیری شوید.

به گفته‌ی Vennixf، وصله‌ی نسخه‌ی 1.8.31 سودو در اواخر ماه ژانویه منتشر شد.

Miller افزود: " نقص موجود در نسخه‌های 1.8.26 تا 1.8.30 سودو، به دلیل تغییر عملکرد سودوی نسخه‌ی 1.8.26، قابل اکسپلویت نیست."

شرکت اپل نیز در اواخر ماه ژانویه وصله‌ی این آسیب‌پذیری را برای macOS High Sierra 10.13.6, macOS Mojave 10.14.6 و macOS Catalina 10.15.2 منتشر کرد.

منبع خبر :

https://thehackernews.com/2020/02/sudo-linux-vulnerability.html

Scan Link

مقالات آموزشی

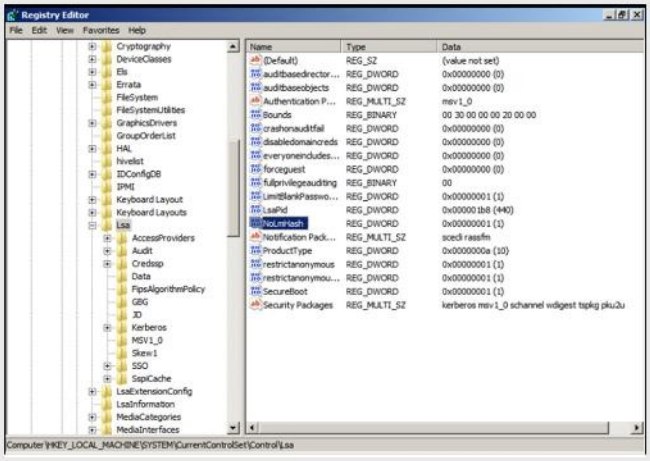
امن‌سازی SAM (Security Account Manager)

سرورهای Stand-alone نام حساب‌های کاربری و رمزعبورهای یک طرفه (غیر قابل بازگشت) هش شده‌ی SAM (Security Account Manager) درLMHash رجیستری می‌باشد. معمولاً فقط اعضای گروه Administrators به اطلاعات حساب دسترسی دارند.

اگرچه رمزهای عبور واقعاً در SAM ذخیره نمی‌شوند و هش‌های رمز عبور برگشت‌پذیر نیستند، اما اگر مهاجمی بتواند یک کپی از پایگاه داده‌ی SAMبه دست آورد، می‌تواند با استفاده از تکنیک‌های bruce force رمز عبور، نام کاربری و رمزعبور معتبر را بدست آورد. با ایجاد کلید NoLMHash در رجیستری، فضـــــای ذخیره‌سازی LMHash را در SAM محدود نمایید.

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\

به منظور ایجاد این کلید، در مسیر فوق بر روی Lsa کلیک راست نموده و New را بزنید، سپس DWORD Value را انتخاب کرده و NoLMHash را تایپ نمایید، پس از آن، بر روی NoLMHashی که جدید ایجاد کرده‌اید کلیک راست نموده و Modify را انتخاب کنید، سپس مقدار 1را به آن اختصاص دهید.



جهت کسب اطلاعات بیشتر می‌توانید به مقاله‌ی زیر مراجعه نمایید:

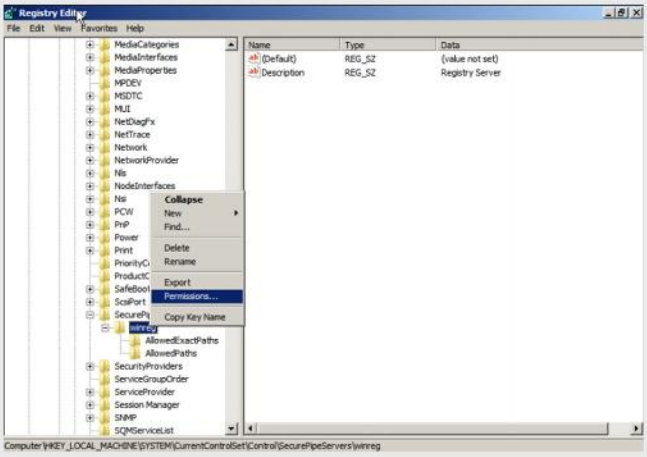
Microsoft Knowledge Base article 299656, "New Registry Key to Remove LM

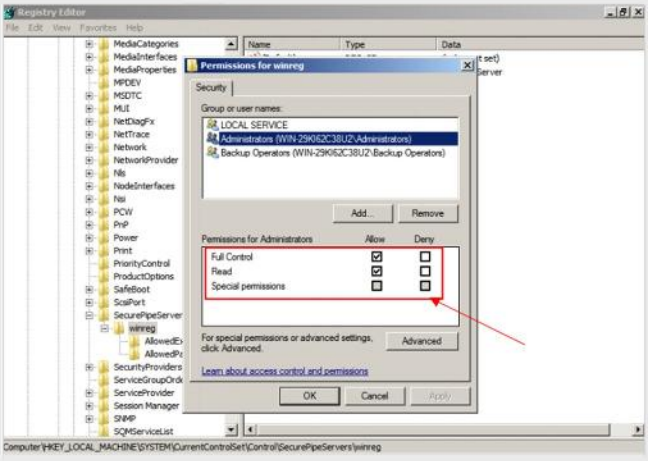
Hashes from Active Directory and Security Account Manager.

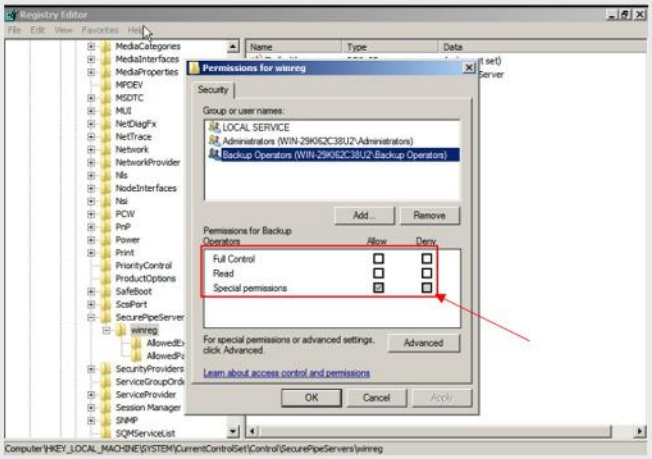
محدود نمودن دسترسی از راه دور مدیران به تنظیمات رجیستری

کلید Winreg تعیین می‌کند که آیا کلیدهای رجیستری برای دسترسی از راه دور در دسترس هستند یاخیر. به طور پیش‌فرض، این کلید به گونه‌ای پیکربندی شده است کـه کاربران نتوانند از راه دور کلیدهای رجیستری را مشاهده نمایند و فقط کاربرانی که سطح دسترسی بالایی دارند می‌توانند آن را تغییر دهند. در ویندوز 2000 و ویندوز سرور 2003، به طور پیش‌فرض دسترسی از راه دور به رجیستری، به اعضای گروه دارای دسترسـی Administrator محـدود شده است. گـروه Backup operators وگـروه Administrators کامل (Full Control) و گروه Backup operatorsتنها دارای

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurePipeServers\winreg







نکته: توجه داشته باشید که تعدادی از سرویس‌ها نیازمند دسترسی از راه دور به رجیستری هستند. برای اینکه ببینید آیا سیستم شما نیازمند محدود نمودن دسترسی از راه دور به رجیستری هست یا خیر، مقاله‌ی زیر را مطالعه فرمایید:

Microsoft Knowledge Base article 153183, "How to Restrict Access to the Registry from a Remote Computer,"

اخبار کوتاه

ممنوعیت استفاده از واتس‌آپ برای مقامات سازمان ملل

سخنگوی سازمان ملل اظهار داشت که مقامات سازمان ملل از استفاده WhatsApp برای اهداف ارتباطی منع شده‌اند زیرا آنها WhatsApp را یک کانال ناامن می‌دانند.

مقامات سازمان ملل متحد، عربستان سعودی را به هک کردن تلفن هوشمند صاحب واشنگتن پست و Jeff Bezos مدیرعامل آمازون از طریق واتس‌آپ متهم کردند. این کارشناس سازمان ملل همچنین گفت ما اطلاعات مرتبطی داریم که درگیری محمد بن سلمان ولیعهد عربستان سعودی در هک کردن تلفن Bezos را روشن می‌کند.

در پاسخ به این سؤال که آیا Antonio Guterres دبیر کل سازمان ملل با ولیعهد عربستان سعودی یا هر یک از رهبران جهان با استفاده از واتس‌آپ ارتباط برقرار کرده است، این مساله را انکار کرد.

سخنگوی سازمان ملل، Farhan Haq اظهار داشت که از تمام مقامات ارشد سازمان ملل خواسته شده که از واتس‌آپ استفاده نکنند، زیرا آن را یک کانال ناامن برای برقراری ارتباط می‌دانند. وی اظهارات خود را با بیان اینکه، طبق دستورالعمل‌های اعلام شده توسط سازمان ملل متحد، قاطعانه معتقد است که دبیر کل سازمان ملل از واتس‌آپ استفاده نمی‌کند، خاتمه داد و سازمان ملل نیز به همه اعضا دستور داده که از ژانویه سال 2019 از استفاده واتس‌آپ خودداری کنند.

از طرف دیگر، واتس‌آپ خاطرنشان کرد که امنیت و حریم خصوصی کاربران را در مقایسه با سایر برنامه‌های شبکه‌های اجتماعی بسیار جدی می‌داند.

Oded Vanunu ، کارشناس امنیت دیجیتال گفت: هر برنامه‌ای دارای نقص است که می تواند توسط هکرهای حرفه‌ای به طریقی یا روش دیگر مورد سوء استفاده قرار بگیرد. وی با بیان اینکه سیاست‌های امنیتی واتس‌آپ هنوز رویایی برای بسیاری از دیگر برنامه‌های رسانه‌های اجتماعی است، اظهارات خود را خاتمه داد.

امنیت کاربر رایانه

امنیت ایمیل

ایمیل اهمیت بسیار زیادی در زندگی دیجیتال ما دارد و خیلی از افراد برای برقراری ارتباط با همکاران، دوستان و خانواده از ایمیل استفاده می‌کنند. همچنین ایمیل محل چک کردن اخبار وبسایت‌هایی که در آن‌ها اشتراک داریم، تصاویر، داکیومنت‌ها و نامه‌های دیجیتال مختلف با موضوعات گوناگون است.

حال با توجه به اهمیت این موضوع، در این شماره از بولتن خبری و در فصل "امنیت ایمیل" به تهدیدات امنیتی ایمیل می‌پردازیم. ادامه مبحث امنیت ایمیل را در شماره‌های بعدی بولتن خبری دنبال کنید.

با ما همراه باشید...

سیستم های مختلف ایمیل چگونه کار می کنند؟

- ایمیل (پست الکترونیک) یک روش تبادل پیام های دیجیتالی از یک فرستنده به یک یا چند گیرنده است.
- شرکت هایی مانند Microsoft ، Yahoo، Google وAOL از حساب های ایمیل رایگان خود استفاده می کنند.
- حساب های ایمیل، از هر مرورگر وب یا کلاینت ایمیل مانند Microsoft Outlook، Mozilla Thunderbird و غیره قابل دسترسی است

امنیت ایمیل

- ارتباط از طریق ایمیل به طور ۱۰۰ درصد امن نیست
- ایمیل های ناامن، به مهاجمان اجازه می دهند تا به اطلاعات شخصی و حساس کاربر دسترسی پیدا کنند
- اگر امن سازی صورت نگرفته باشد، ایمیل های فرستاده یا دریافت شده می تواند جعل ویا توسط دیگران خوانده شود
- ایمیل ها یکی از منابع ویروس ها و برنامه های مخرب هستند
- لازم است که ایمیل ها برای ارتباطات امن و حفاظت از حریم خصوصی، ایمن شوند

تهدیدات امنیتی ایمیل

هدایت کاربر به یک آدرس مخرب

ایمیل هل ممکن است حاوی لینک به و سایت های مخرب و یا دارای مطالب مربوط به pornographic باشند

پیوست های مخرب ایمیل

فایل های ضمیمه ممکن است حاوی یک ویروس، تروجان، کرم ها keylogger وغیره باشد و باز کردن چنین پیوست هایی کامپیوتر را آلوده می کند

فیشینگ

ایمیل های Phishing قربانیان را برای ارائه اطلاعات شخصی فریب می دهد

Spamming

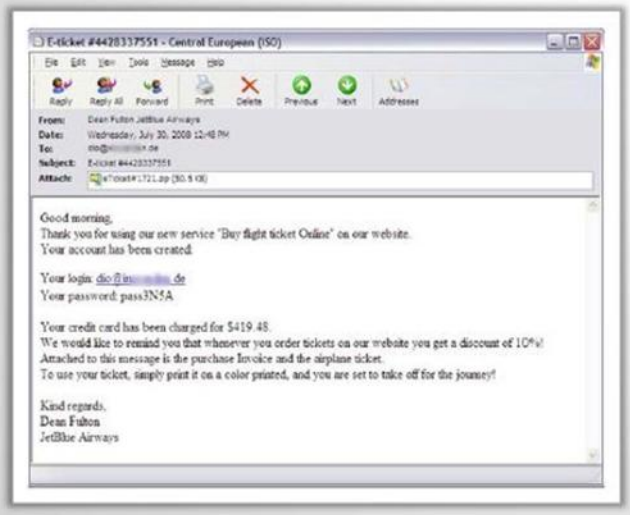
کاربر ممکن است ایمیل های اسپمی را دریافت کند که حاوی نرم افزار های مخرب باشد که به مهاجمین اجازه می دهد تا کامپیوتر کاربر را کنترل کند

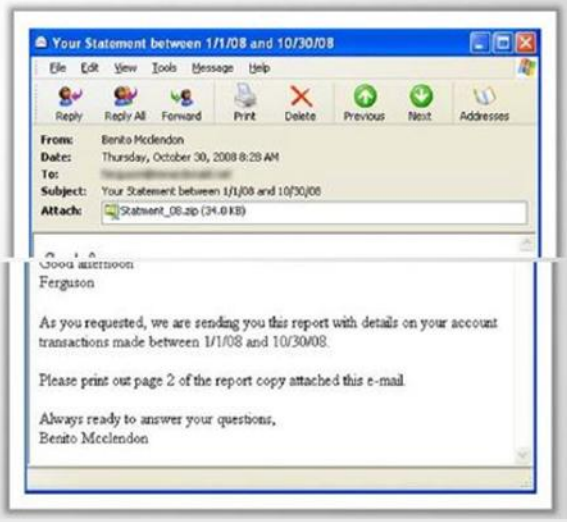
ایمیل Hoax/Chain

ممکن است کاربر ایمیل های جعلی دریافت کند که شامل اطلاعات اشتباهی است که به او می گوید نامه ای را ارسال کند

پیوست های مخرب ایمیل

- پیوست های ایمیل تهدیدات امنیتی عمده ایمیل هستند، زیرا آنها ساده ترین و قوی ترین راه ها را برای حمله به یک کامپیوتر، به مهاجمان ارائه می دهند
- بیشتر پیوست های مخرب، یک ویروس، تروجان، نرم افزار جاسوسی یا هر نوع دیگر از بدافزار را نصب می کنندکه به زودی شما آنها را باز می کنید





پیوست های ایمیل: هشدارها

بررسی کنید که ایمیل از یکی از مخاطبین شما فرستاده شده است

قبل از باز کردن ایمیل ها، تمام پیوست های آنها را ذخیره و اسکن کنید

پیوست های حاوی فایل هایی با پسوندهای مشکوک و ناشناخته باز نکنید
به عنوان مثال:
*.exe, *.vbs,*.bat,*.ini, *.bin, *.com, *.pif, *.zzx

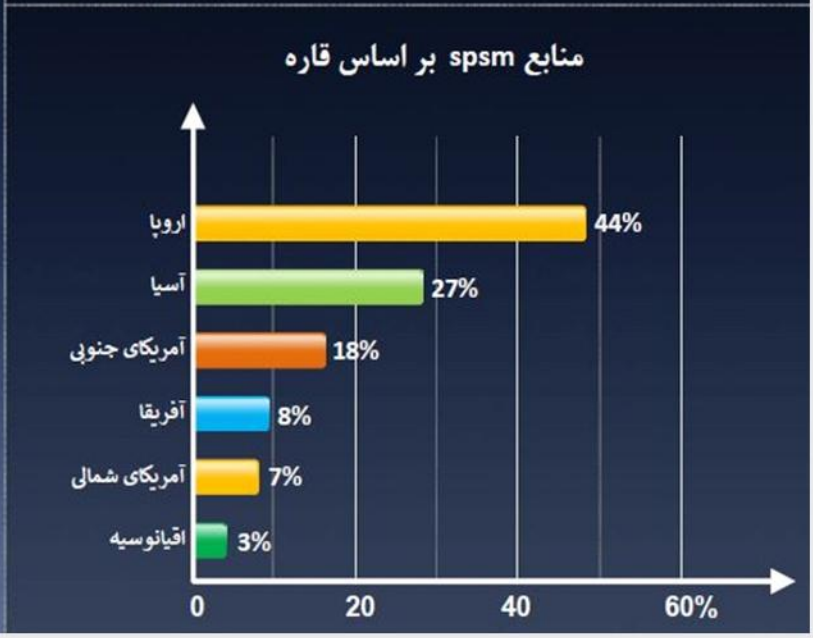
بررسی کنید که آیا ایمیل از یک منبع قابل اعتماد دریافت شده است یا خیر

هرگز پیوست های ایمیل ارسال شده از منابع غیرقابل اعتماد را باز نکنید

بررسی کنید که آیا موضوع ایمیل با نام پیوست هماهنگی دارند یا خیر

Spamming

- استفاده از سیستم های ایمیل برای ارسال توده پیام های ناخواسته، بدون در نظر گرفتن صندوق های پستی کاربران است
- ایمیل های اسپم ممکن است حاوی برنامه های کامپیوتری مخرب مانند ویروس ها و تروجان ها باشند
- طبق گفته سیمانتک، اسپم ۸۹.۱ درصد از کل ترافیک ایمیل را تشکیل می دهد

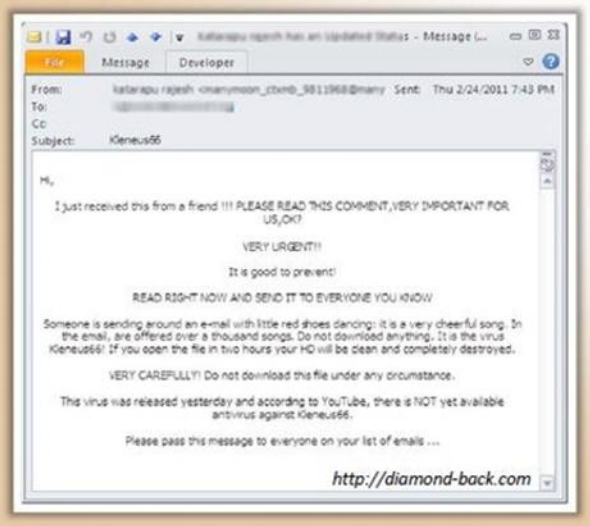


ابزار آنتی اسپم SPAMfighter

این ابزار از تمام حساب های ایمیل در یک کامپیوتر در برابر "فیشینگ" ، سرقت هویت و دیگر فریب های ایمیل محافظت می کند

ایمیل های Hoax/Chain و Scam

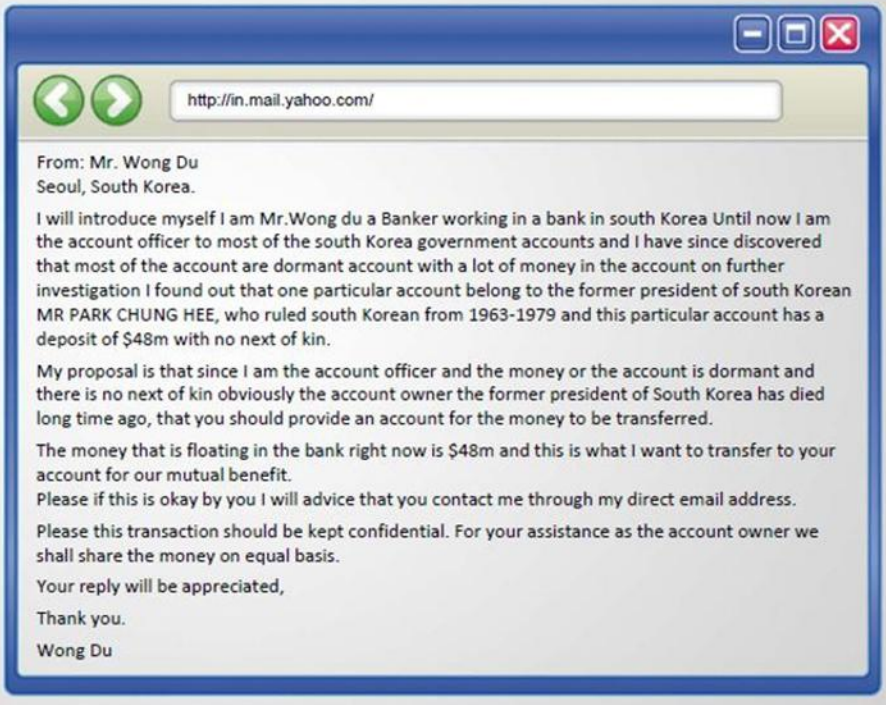
- **Hoaxs**، پیام های هشدار در مورد تهدیدات غیرواقعی به گیرندگان ایمیل هستند
- همچنین به کاربران در مورد **اثرات نامطلوب** ارسال نکردن آن ایمیل به دیگران هشدار داده می شود

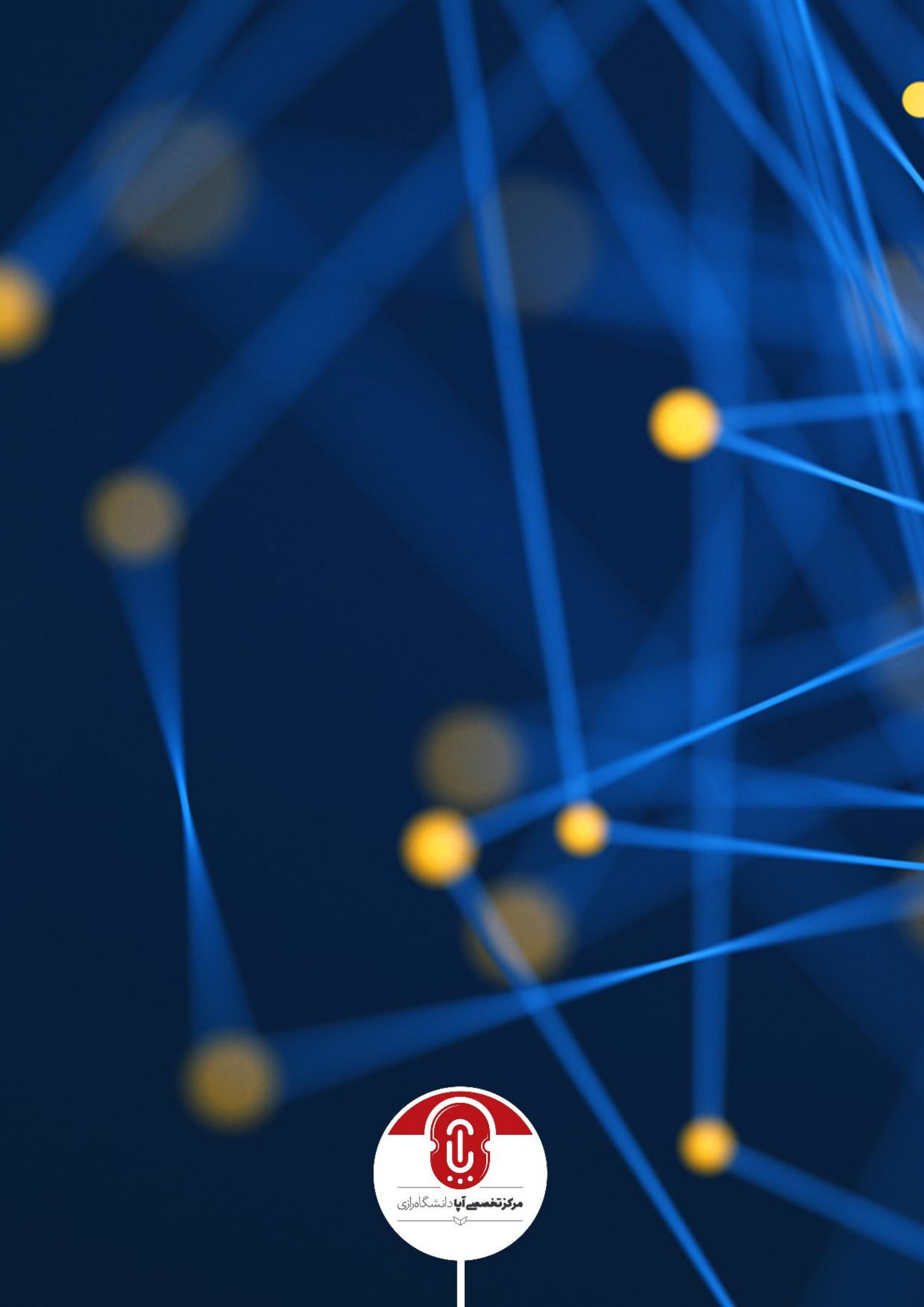


- یک ایمیل **Scam**، اطلاعات شخصی مانند اطلاعات حساب بانکی، شماره کارت اعتباری، رمز عبور و غیره را از کاربر درخواست می کند
- فرستنده ایمیل **Scam**،همچنین ممکن است از گیرنده بخواهد که ایمیل را به تمام کسانی که در لیست مخاطبانش وجود دارند ارسال کند

کلاهبرداری نیجریه ای

- کلاهبرداری نیجریه ای یا Nigerian Scam نوعی پیش پرداخت یا انتقال پول است
- دلیل نام گذاری این کلاهبرداری به کلاهبرداری نیجریه ای این است که ابتدا در نیجریه آغاز شده است اما می تواند در هر جای دنیا انجام شود
- با استفاده از این کلاهبرداری، کلاهبرداران با ارسال یک ایمیل و پیشنهاد یک سهم در یک سرمایه هنگفت پول با شما تماس می گیرند
- آنها می گویند که می خواهند پولی را که در طی جنگ های داخلی در بانک ها بلوکه شده است ، به حساب شما انتقال دهند
- همچنین آنها ممکن است دلایل مختلفی از قبیل مشکلات ارثی بزرگ، محدودیت های دولت یا مالیات در کشور کلاهبردار را ذکر کنند
- کلاهبرداران از شما می خواهند که پول یا اطلاعات حساب بانکی خود را برای کمک به آنها در انتقال این پول ارسال کنید




مرکز تخصصی آپا دانشگاه رازی