۶۱

نشریه تخصصی امنیت سایبری مرکز آپا دانشگاه کردستان
شماره نخست /تیرماه ۱۳۹۷

- معرفی حملات ۸۰۲.۱۱
- رمزگشایی کلیدهای ذخیره شده وایرلس با C++
- تهدیدات بدافزارهای موبایلی و تکامل این بدافزارها
- مروری بر آسیب‌پذیری‌های سیسکو تا کنون
- جدیدترین بدافزارها و روند رشد آن‌ها در ماه اخیر
- پیکربندی امن مودم ADSL
- چگونگی انتخاب کلمه عبور قدرتمند

آپا مخفف عبارت آگاهی‌رســـانی، پشتیبانی و امداد رخدادهای رایانه‌ای است و معادل بومی اصطلاح CERT می‌باشـــد. مرکز آپا دانشگاه کردستان، در راستای انجام فعالیت‌های خود در زمینه آگاهی و اطلاع رســـانی، با بکارگیری نیروهای متخصص و پتانسیل‌های پژوهشی در استان کردستان اقدام به انتشار نشریه ای الکترونیکی در حوزه امنیت فضای سایبری نموده است.

مخاطبان اصلی نشـــریه کارشناســـان و متخصصان فناوری اطلاعات و شبکه، دانشجویان و علاقمندان فضای سایبری است. مطالب این نشریه عموماً محورهای زیر را شامل می شود:

- اطلاع رسانی رخدادهای اخیر فضای سایبری
- آگاهی‌رسانی نســـبت به آخرین تهدیدات و آسیب‌پذیری ابزارهای فضای مجازی
- آموزش‌های عمومی در جهت ارتقاء دانش عمومی امنیت

شـــایان ذکر اســـت، با توجه به گســـترش روزافزون شـــبکه‌های بی‌سیم و آسیب‌پذیری‌های فراوان این شبکه‌ها، مطالب این شماره نشریه به حوزه دانش و امنیت در این شبکه‌ها اختصاص می‌یابد.

ویرا، اسم نشریه، واژه‌ای در زبان کردی به معنی صاحب‌فکر و هوشمند است.
مرکز آپا دانشگاه کردستان از راهنمایی و مساعدت آقایان دکتر جباری و دکتر بزدوده در انتخاب اسم نشریه کمال تقدیر و تشکر را دارد.

سردبیر: هادی گلباغی
سردبیر فنی: مسلم حقیقیان
ویراستار : تیم فنی مرکز آپا دانشگاه کردستان
طـراحی و صـفحـه‌آرایی: آریان اسماعیل زاده
نویسندگان :
مسلم حقیقیان / فرشته کیاست / محمد حبیبی / میلاد منصوری / هادی گلباغی
تلفن مرکز :۰۸۷۳۳۶۶۲۹۳۲
نشانی مجله:کردستان- بلوار پاسداران-دانشگاه کردستان-مرکز آپا
نشانی وبسایت: www.cert.uok.ac.ir
ایمیل : apa@uok.ac.ir

فهرست مطالب

۰۲ تازه ها
۰۷ مقاله‌های آموزشی
۱۲ دفتر تقلب(CheatSheet)
۱٤ معرفی ابزار، مقاله، کتاب
۱۸ گزارش تحلیلی و گزارش آسیب پذیری
۲٦ جدیدترین بدافزارها
۳۳ امنیت عمومی

| تازه ها

سرتیتر خبر های مهم ماه گذشته

- آسیب‌پذیری‌های چندگانه گوگل کروم و اجازه اجرای کد دلخواه
- گوگل سازندگان تجهیزات اصلی (OEMs) اندروید را به ارائه آپدیت‌های منظم مجبور می‌کند
- بدافزار DNS-Hijacking کاربران iOS، اندروید و دسکتاپ را در سراسر جهان مورد هدف قرار می‌دهد
- آسیب‌پذیری چندگانه در Microsoft Office PowerPoint & Excel برای سیستم‌عامل مک اجازه اجرای کد از راه دور را می‌دهد
- آسیب‌پذیری تزریق فرمان در DHCP لینوکس
- آسیب‌پذیری‌های چندگانه فایرفاکس و اجازه اجرای کد دلخواه
- انتشار به‌روزرسانی‌های امنیتی شرکت اپل
- انتشار گسترده بدافزار VPNFilter و آلودگی بیش از ۵۰۰ هزار روتر
- انتشار بدافزار استخراج‌کننده ارز دیجیتال تحت عنوان‌های فیلترشکن تلگرام و ادعیه ماه رمضان
- سیل هشدارهای امنیتی و اختلال در پاسخگویی به آن‌ها

افزونه‌های کروم و سرقت پسوردهای فیسبوک کاربران

مترجم: شادی شهریاری

یکی از رایج‌ترین روش‌های مهاجمین سایبری برای گسترش نرم‌افزارهای مخرب، فریفتن کاربران رسانه‌های اجتماعی برای بازدید از نسخه‌های معروف رسانه‌های محبوب است.

محققان امنیتی در مورد یک مجموعه بدفزار جدید که حداقل از ماه مارس امسال فعال بوده و اکنون بیش از صدهزار کاربر در سراسر جهان را آلوده کرده‌است،هشدار داده‌اند.

Nigelthorn، بدافزاری که از طریق لینک‌های مهندسی اجتماعی فیس‌بوک به سرعت در حال گسترش است و سیستم‌های قربانی را با افزونه‌های مخرب مرورگر آلوده می‌کند، مجوزهای آن‌ها را به سرقت می‌برد و استخراج‌کننده‌های ارز را بر روی سیستم قربانی نصب می‌کند.

این بدافزار از طریق حداقل هفت افزونه تحت تاثیر قرار می‌گیرد که همه‌ی آن‌ها از فروشگاه رسمی وب کروم میزبانی شده‌اند.

این افزونه‌های مخرب مرورگر کروم نخستین بار توسط شرکت امنیت سایبری Radware کشف شد. براساس گزارش منتشر شده توسط این شرکت، اپراتورهای بدافزار از کپی‌های قانونی افزونه‌های کروم استفاده می‌کنند و یک اسکریپت مخرب کوتاه را به منظور دور زدن بررسی اعتبار، به آن‌ها تزریق می‌کنند.

محققان این بدافزار را به دلیل اینکه یک کپی از افزونه‌ی معروف Nigelify (که همه‌ی عکس‌های صفحه‌ی وب را با فرمت GIF جایگزین می‌کرد) بود Nigelthorn نامگذاری نمودند.

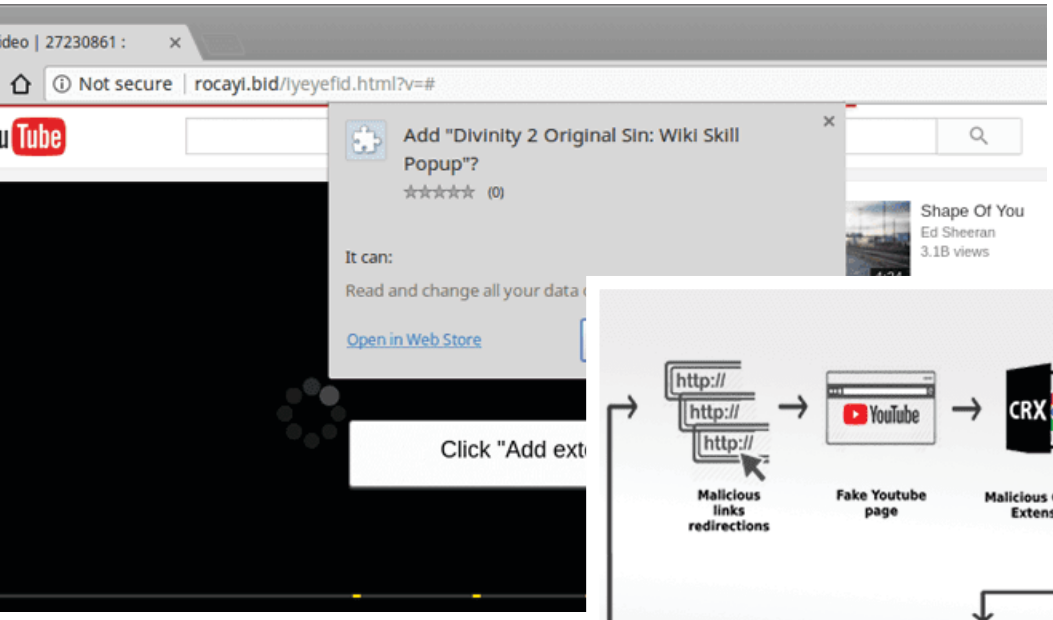
Nigelthorn توسط لینک‌های فیسبوک گسترش می‌یابد که در صورت کلیک، قربانیان را به یک صفحه‌ی جعلی یوتیوب هدایت می‌کند و از آن‌ها می‌خواهد برای ادامه‌ی نمایش ویدیو، یک افزونه مخرب کروم را دانلود نمایند. پس از نصب، افزونه یک کد جاوا اسکریپت مخرب را اجرا می‌کند که کامپیوتر قربانی را بخشی از یک باتنت می‌کند.

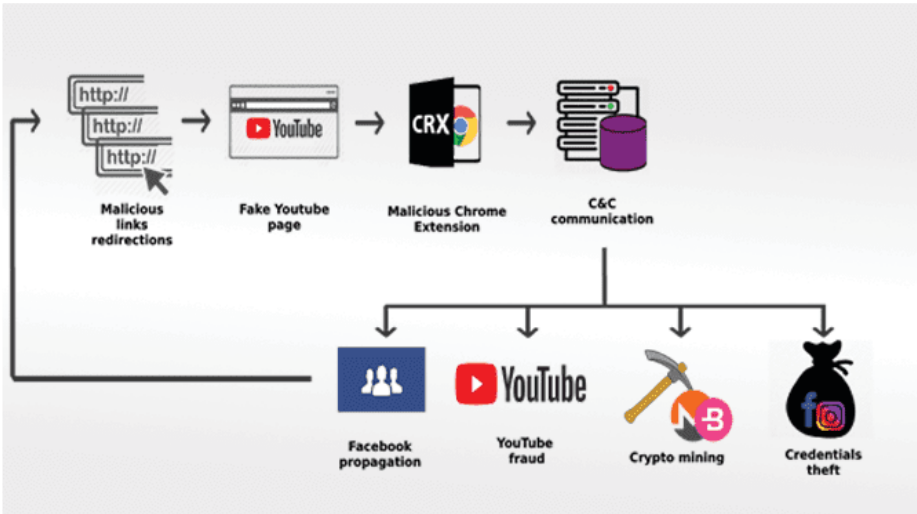
Digimine، یک بدافزار مشابه است که در سال گذشته برای ارسال لینک‌های مسنجر فیسبوک ظاهر شد. این بدافزار یک افزونه‌ی مخرب را نصب می‌کند و به مهاجم اجازه‌ی دسترسی به پروفایل فیسبوک قربانی را می دهد و همین بدافزار را از طریق Messenger به لیست دوستان وی ارسال می‌کند.

NigelThorn پسوردهای فیس‌بوک و اینستاگرام را به سرقت می‌برد

بدافزار جدید به طورعمده بر سرقت مجوزهای حساب‌های فیسبوک و نمایش مشخصات عمومی قربانیان و جمع‌آوری جزئیات از حساب‌های آنها متمرکز است. از این اطلاعات به سرقت‌رفته، برای ارسال لینک‌های مخرب به دوستان قربانی آلوده مورد استفاده قرار می گیرد تا همان افزونه‌های مخرب را نصب کنند. اگر هر یک از دوستان قربانی روی لینک کلیک کنند کل پروسه‌ی آلوده‌شدن دوباره آغاز می‌شود.

NigelThorn، همچنین یک ابزار استخراج‌کننده ارز دیجیتال مبتنی بر مرورگر را دانلود می‌کند که به استخراج ارز دیجیتال شامل Monero، Bytecoin یا Electroneum را می‌پردازد. بنظر میرسد که در طول فقط ۶ روز، مهاجمان حدود ۱۰۰۰ دلار ارز دیجیتال را به طور عمده از Monero تولید کرده‌اند.





Nigelthorn، همچنین اجازه‌ی حذف افزونه‌های مخرب را به کاربر نمی‌دهد و به طور اتوماتیک، هر بار که کاربر زبانه‌ی حذف‌کردن را باز می‌کند، افزونه مخرب را می‌بندد.

Name	Extension Id	Installation count
Nigelify	gmddfjhfjgbmabkihepijkanhmlooajl	25000
PwnerLike	kajjcgpohlkdcjfkcbkkbhapafcblaom	9000
Alt-j	anbnajjakpmfdofijejenaclbceejlll	Removed in less than a day - no statistics
Fix-case	jkkmcoihchcflfjnigngdegbemipdlnl	Removed in less than a day - no statistics
Divinity 2 Original Sin: Wiki Skill Popup	ajmchakbijebimbgcohecngliijaddin	Removed in less than a day - no statistics
keeprivate	edpoobbacbcmfpnfpjoambjbihhobooi	Removed in less than a day - no statistics
iHabno	opfogdennafhaoihhkocppaajlkpbfbn	New app (as of May 9)

لیست افزونه‌های مخرب کروم

۷ افزونه جعلی که خود را به عنوان افزونه‌های قانونی درآورده اند در ادامه لیست شده است.

گوگل همه‌ی افزونه‌های لیست‌شده در جدول را حذف کرده‌است، اما اگر هرکدام از آن‌ها را نصب کرده‌اید توصیه می‌شود که آن را حذف کرده یا پسورد فیس‌بوک، اینستاگرام و اکانت‌های دیگری که دارید را تغییر دهید. به کاربران همیشه توصیه می‌گردد که حین بازدید از سایت‌ها و کلیک روی لینک‌ها در مقابل مهندسی اجتماعی هوشیار باشند.

منبع: thehackernews.com

حدود ۷۵٪ از سرورهای Open Redis با نرم افزارهای مخرب آلوده شده‌اند

■ مترجم: فرشته کیاست

یک سخنگوی محققان امنیتی Imperva گفت که اکثر سرورهای Redis که در اینترنت بدون هیچ‌گونه مکانیزم تأیید هویت در محل نصب شده‌اند، احتمالا از بدافزار استفاده می‌کنند. کارشناسان این شرکت در چند ماه گذشته طی یک آزمایش بر روی این سرورها و پس از استفاده از سرورهای honeypot مبتنی بر Redis به این نتیجه رسیدند که سرورهای Redis تحت تاثیر بدافزارهایی هستند. با استفاده از سرورهای هانی‌پات یک بات‌نت با نام ReddisWannaMine کشف شده که بصورت مخفیانه به استخراج ارز دیجیتال بر روی سرورهای باز Redis می‌پردازد.

عملیات بات‌نت: استفاده مجدد از کلید SSH

Imperva گفت، "ما متوجه شدیم که مهاجمان مختلف از کلیدها و/یا مقادیر یکسان برای انجام حملات استفاده می‌کنند. وی همچنین افزود "یک کلید یا مقدار مشترک بین سرورهای چندگانه نشانه واضحی از فعالیت‌های بات‌نت مخرب است."

مهاجمان یک جفت کلید/ مقدار را در حافظه قرار داده و سپس آن را در یک فایل در دیسک در جاییکه فایل اجرا می‌شود ذخیره می‌کنند (/ e.g etc/crontabs, /var/spool/cron/crontab etc). مهاجمان معمولا مقادیری را قرار می‌دهند که شامل دستورات دانلود منابع از راه دور و اجرا هستند. نوع دیگری از دستورات رایج اضافه کردن کلیدهای SSH است، بنابراین مهاجمان می‌توانند از راه دور به ماشین دسترسی داشته‌باشد.

حدود ۷۵ درصد از سرورهای Redis مورد آزمایش قرار گرفته آلوده شده‌اند.

آزمایش Imperva کلیدهای حمله را گرفته و ۷۲ هزار سرور Redis را در دسترس عموم قرار داد تا ببینند آیا آنها از هر حمله‌ای که توسط هانی‌پات‌ها ثبت شده‌اند میزبانی می‌کنند.

در این آزمایش بیش از دو سوم سرورهای باز Redis دارای کلیدهای مخرب بوده و سه چهارم سرورها دارای مقادیر مخرب هستند که نشان می‌دهد که این سرور آلوده است. همچنین، طبق داده‌های Honeypot Imperva، سرورهای آلوده با کلید پشتیبان از یک بات‌نت متوسط (IP ۶۱۰) در چین (۸۶ درصد IPها) مورد حمله قرار گرفتند.

مهاجمان با ۲۹۵ آی‌پی بیش از ۷۵ هزار بار مشتریان این سرورها را مورد حمله قرار دادند. این حملات شامل تزریق XSS، SQL، آپلود فایلهای مخرب، اجرای کد از راه دور و غیره است. محققان اظهار داشتند که این تعداد نشان می‌دهد که مهاجمان از سرورهای آسیب‌پذیر Redis استفاده می‌کنند تا حملات بیشتری را از طرف مهاجم انجام دهند.

در شکل ۱ لیست کلیدها و مقادیر مخرب بدست آمده از این آزمایش آورده‌شده است.

برخی از کلید های SSH مخرب به مدت دو سال فعال بوده‌اند

کلید SSH با نام crackit که در لیست بالا آمده‌است و یک تهدید شناخته شده می‌باشد، سال‌ها مورد استفاده قرار گرفته است. این کلید مخرب قبلا بر روی ۶۳۳۸ سرور Redis توسط محققان Risk Based Security در جولای ۲۰۱۶ یافت شده‌است.

یک ماه بعد، همان کلید توسط محققان Duo Lab بر روی بیش از ۱۳،۰۰۰ سرور Redis یافت شده بود که ۲ بیت‌کوین به عنوان باج گرفته بود.

برای در امان ماندن از این تهدید، ادمین‌های سرور باید فایل پیکربندی سرور را برای فعال‌سازی یک سیستم احراز هویت، تغییر دهند.

Nadav Avital، مدیر گروه تحقیقات امنیتی در Imperva، گفت: "سرور Redis نباید در معرض عموم قرارگیرد(به اینترنت متصل شوند) زیرا هیچ احراز هویت از پیش تعیین شده‌ای در آن وجود ندارد. از این سرورها برای داده‌های حساس استفاده نکنید زیرا تمام داده‌ها به صورت آشکار و بدون رمزنگاری ذخیره می‌شوند." وی در ادامه افزود که دلیل این که ۷۵ درصد از سرورهای Redis باز با آلوده می‌شوند، به احتمال زیاد به این دلیل است که آنها به طور مستقیم به اینترنت دسترسی دارند.

منبع: bleepingcomputer.com

Malicious Keys	%of infected servers
backup1, backup2, backup3	68
crackit	19
trojan	7
tt,1, godkey, x, session, zyptziqxibzioeikboom	<1

Malicious Values	%of infected servers
curl	75
wget	75
lynx	67
ssh-rsa	20
chmod, /dev/tcp	<1

شکل ۱. رایج ترین کلیدهای SSH مخرب موجود در داده‌های هانی‌پات Imperva

۲۷ درصد تیم‌های امنیتی به صورت روزانه در حدود یک میلیون هشدار امنیتی دریافت می‌کنند

■ مترجم: هادی گلباغی

شرکت امنیتی Imperva به تازگی بررسی جدیدی در خصوص نرخ هشدارهای امنیتی که توسط تیم‌های امنیتی دریافت می‌شود را انجام داده است. طبق نتایج این بررسی‌ها در حدود ۲۷ درصد تیم‌های امنیتی به طور میانگین یک میلیون هشدار را به صورت روزانه دریافت می‌کنند. با توجه به این که تعداد این هشدارها بسیار بالا است اما متخصصین فناوری اطلاعات برخی از این هشدارها را نادیده می‌گیرند و ۴ درصد از متخصصین اعلان‌های مربوط به هشدارها را غیر فعال کرده‌اند.

برای حل مشکل دریافت این حجم از هشدارهای امنیتی، این شرکت یک نرم‌افزار به نام تحلیل حملات را توسعه داده است که به متخصصین امنیتی برای عدم دریافت هشدارهای غیر ضروری کمک کرده و تمرکز را بر آسیب‌پذیری‌های امنیتی که برای برنامه‌ها دارای اهمیت بالا و حساس هستند بگذارد. این برنامه برای هر نوع مقیاسی و در هر محیطی مانند WAP یا Hybrid Cloud قابل استفاده است و با استفاده از الگوریتم‌های یادگیری ماشین پیشرفته برای بهینه‌سازی و خودکارسازی فرآیند معمول اعلان هشدارها و رخدادها، قادر است زمان اختصاص داده شده برای این امور را بسیار کاهش دهد. می‌دانیم که آسیب‌پذیری‌های امنیتی برای برنامه‌های کاربردی دارای حساسیت بالایی است اما برای این حساسیت نیز مقیاسی وجود دارد.

آقای Eldad Chai معاون ارشد مدیریت محصولات شرکت امنیتی Imperva در این خصوص می‌گوید « در واقع تیم‌های سازمان‌های امنیتی برخی اوقات با سیلی از هشدارهای امنیتی مواجه می‌شوند که کار آن‌ها را مختل می‌کند. با بهره بردن از قدرت هوش مصنوعی، یک راه‌حل برای کاهش اعلان تهدیداتی که اصولا حساس و دارای اهمیت نبوده‌اند پیشنهاد شده است.»

همچنین در ادامه توضیح می‌دهد که این راه‌حل به مشتریان اجازه می‌دهد که الگوها جهانی در خصوص اعلان هشدارها را دنبال کرده و به دنبال الگوی شخصی در این حوزه نباشند تا قادر باشند در زمان سریعتری به الگوهای جدید واکنش نشان داده و در زمان کمتری این امور انجام شود.

تیم‌های امنیتی در سازمان‌ها نقش بسیار مهمی دارند ولی این مطلوب نیست که متخصصین زیادی را برای هرگونه تهدید امنیتی با هر نوع حساسیتی در برنامه‌ها اختصاص دهند. طبق این بررسی‌ها ۵۶ درصد متخصصین امنیتی موضوع را بخاطر تعداد اشتباه‌های کاذب یا False positive زیاد نادیده می‌گیرند. تعداد زیادی از این درخواست‌ها مربوط به آسیب‌پذیری‌هایی است که در حقیقت به هم مربوط بوده و باهم ترکیب می‌شوند و بهتر است که با استفاده از تکنیک‌های یادگیری ماشین حملات تحلیل گردند و تعداد اشتباه‌های کاذب کاهش پیدا کنند.

منبع : latesthackingnews.com

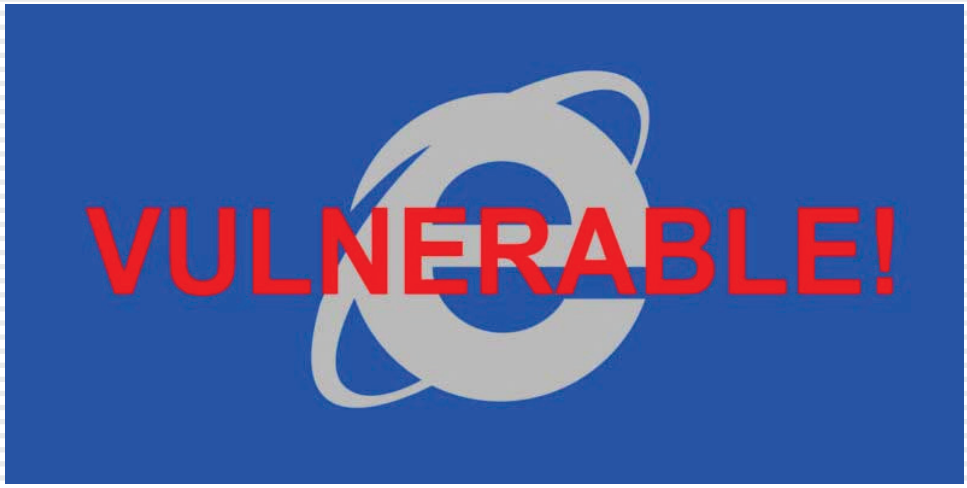
اشکال در مرورگر Microsoft Edge امکان دستیابی مهاجمان به اطلاعات حساس کاربران را فراهم می‌کند

■ مترجم: فرشته کیاست

یک توسعه‌دهنده امنیتی گوگل مشکل مهم امنیتی در مرورگر Microsoft Edge و تا حدودی در مرورگر فایرفاکس یافته که این امکان را برای یک مهاجم فراهم می‌کند تا به اطلاعات خصوصی فرد قربانی دسترسی داشته باشد. طبق گفته Jake Archibald که به طور تصادفی این حفره امنیتی را پیدا کرده، این مشکل موجب می‌شود تا شما وقتی با مرورگر Microsoft Edge سایتی را بازدید می‌کنید، صاحب آن سایت می‌تواند ایمیل‌ها، محتویات فیسبوک و اطلاعات هر حساب دیگر شما را بخواند بدون آنکه شما آگاه شوید. این آسیب‌پذیری با شناسه:

CVE-2018- 8235

این امکان را به مهاجم می‌دهد تا از راه دور محتوای زبانه‌ها یا تب‌های دیگر مرورگر قربانی را بازیابی کند که می‌تواند شامل سایت‌هایی هم شود که نیاز به تایید هویت خود فرد دارند. از چهار مرورگر اصلی این مشکل امنیتی عمدتاً بر Microsoft Edge تأثیرگذار است که در هفته گذشته وصله این آسیب‌پذیری را منتشر کرده‌است. تنها نسخه بتا در مرورگر فایرفاکس تحت تأثیر این آسیب‌پذیری قرار دارد و مرورگرهای Safari و کروم تحت تأثیر نیستند. این نقص مرتبط با مرورگرهایی است که درخواست‌های متقابل مبدا را به محتوای چند رسانه ای مربوط می‌سازند. طبق گفته Bleeping Computer این آسیب‌پذیری زمانی مورد سوءاستفاده قرار می‌گیرد که یک سایت مخرب از فراهم‌کنندگان سرویس استفاده کند تا محتوای داخل یک تگ <audio> را از دامنه دیگری بارگذاری کند، درحالیکه از پارامتر "range" برای استخراج تنها یک بخش از آن فایل استفاده می‌شود. مرورگرها هیچوقت هنگام بارگذاری فایل‌های داخل تگ audio از جاهای دیگر و کمک فراهم‌کنندگان سرویس استفاده نمی‌کنند و یک وب‌سایت مخرب می‌تواند چنین محتوایی را از یک سایت دیگر بدون بررسی بدست آورد. پس از فریب قربانی به بازدید چنین سایتی مهاجم می‌تواند محافظت از مرورگر با نام CORS (Cross-Origin Resource Sharing) را متوقف سازد. وظیفه این بخش این است که بطور معمول دستیابی سایت‌ها را به محتوای سایر سایت‌ها متوقف کند. مایکروسافت این مشکل را اینگونه توصیف می‌کند: آسیب‌پذیری دور زدن ویژگی امنیتی زمانی ایجاد می‌شود که Microsoft Edge به اشتباه درخواست‌های مبدأهای مختلف را اداره می‌کند. به گفته مایکروسافت، مهاجمی از آسیب‌پذیری سوءاستفاده می‌کند می‌تواند مرورگر را به ارسال داده‌هایی که به طریق دیگری محدود می‌شود، تحمیل کند. از آنجاییکه شرکت مایکروسافت اخیراً وصله‌ای برای این آسیب‌پذیری منتشر کرده‌است به کاربران توصیه می‌شود مرورگر خود را به‌روزرسانی کنند.



ارائه استاندارد جدید WPA3 و افزایش امنیت وای‌فای

■ مترجم: فرشته کیاست

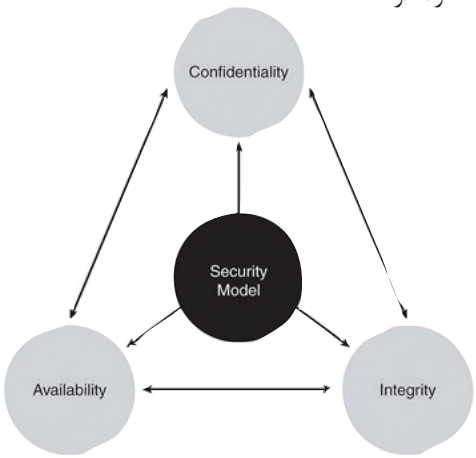
اتحادیه Wi-Fi در روز دوشنبه WPA3 که یک پروتکل امنیتی جدید وای‌فای برای افزایش امنیت بی‌سیم است را به طور رسمی راه اندازی کرد. بر طبق گفته این اتحادیه یک گروه غیرانتفاعی که استانداردهای شبکه وای‌فای را تأیید می‌کند، استاندارد جدیدی با ویژگی‌های جدید مانند ساده‌سازی امنیت وای‌فای، تأیید اعتبار قوی‌تر و افزایش قدرت رمزنگاری ارائه می‌دهد. این نسخه جدید WPA برای دو کاربرد سازمانی و شخصی ارائه می‌شود. آنها تعدادی از ویژگی‌ها مانند آخرین روش‌های امنیتی و عدم پذیرش پروتکل‌های قدیمی را به اشتراک می‌گذارند، اما هر حالت عملیاتی همچنین شامل قابلیت‌های اضافی است که با توجه به تفاوت‌های بین استفاده و الزامات شبکه‌های خانگی در برابر شبکه‌های سازمانی درنظر گرفته شده‌است. یکی از پیشرفت‌های امنیتی قابل توجهی که WPA3 به ارمغان آورده است، محافظت در برابر حملات حدس زدن رمز عبور مانند حملات فرهنگ لغت (dictionary attack) است. این حفاظت جدید به لطف دستیابی به احراز هویت دست تکانی با نام SAE (Authentication of Equals) می‌باشد و همچنین بر مواردی که کاربران رمزهای عبور ساده و آسان برای شکستن را انتخاب می‌کنند اعمال می‌گردد. علاوه بر این، WPA3 از محرمانگی فوروارد پشتیبانی می‌کند، به این معنی که حتی اگر یک رمز عبور به خطر بیافتد، مهاجمان نمی‌توانند ترافیک وای‌فای را که قبل از ورود به سیستم منتقل شده‌اند، رمزگشایی کنند. توجه داشته باشید که ویژگی‌های جدید بار اضافی و یا مزاحمت برای کاربر ایجاد نمی‌کند. برای شبکه‌های سازمانی، WPA3 رمزنگاری قدرتمندی با طول ۱۹۲ بیتی را ارائه می‌دهد، و همچنین حمایت‌های بیشتری برای شبکه‌های انتقال اطلاعات حساس مانند دولت و مالی ارائه می‌دهد. علاوه بر این، ویژگی اتصال ساده وای‌فای (Wi-Fi Easy Connect) در نظر گرفته شده است که به طور ایمن یک دستگاه با اینترفیس محدود یا بدون اینترفیس (به ویژه دستگاه‌های IoT) به شبکه متصل شود. این کار از طریق اسکن کردن کدهای QR با گوشی‌های هوشمند انجام می‌شود. نسخه جدید این پروتکل با تکنولوژی Wi-Fi CERTIFIED Enhanced Open در اوایل ماه جاری راه‌اندازی خواهد شد. این تکنولوژی از رمزنگاری داده‌های منفرد (individualized) پشتیبانی می‌کند تا از خطر تهدیداتی مانند حملات مرد میانی (MiTM) جلوگیری کند. WPA3 جانشین WPA2 است که در سال ۲۰۰۴ راه اندازی و به طور گسترده‌ای برای امنیت ترافیک وای‌فای استفاده می‌شود. تنها کاری که مانده اتحادیه انجام دهد وارد کردن محصولات WPA3 فعال در بازار است که ممکن است نیاز به زمان زیادی داشته باشد. در حال حاضر، WPA3 برای دستگاه های تازه تولید شده اختیاری است. طبق اعلام اتحادیه انتظار می‌رود WPA3 در اواخر سال جاری به اجرا درآید و در اواخر سال ۲۰۱۹ به تصویب رسید.

| مقاله های آموزشی

انواع حملات شبکه‌های وایرلس

■ نویسنده: مسلم حقیقیان

سه اصل اساسی امنیت شبکه‌های رایانه‌ای محرمانگی، جامعیت و در دسترس بودن است. برای رسیدن به امنیت واقعی، تمام این سه اصل به‌طور خاص موردنیاز است که با استفاده از آن‌ها در امنیت شبکه، می‌توان تا درصد بالایی امنیت را تضمین نمود. مهاجمین همیشه در تلاش هستند تا یکی یا بیشتر از این سه اصل امنیتی را به خطر اندازند.



محرمانگی(Confidentiality)

به معنای آن است که اطلاعات فقط در دسترس کسانی قرار گیرد که به آن نیاز دارند و این‌گونه تعریف‌شده است. به‌عنوان‌مثال از دست دادن این ویژگی امنیتی معادل است با بیرون رفتن قسمتی از پرونده محرمانه یک شرکت و امکان دسترسی به آن توسط مطبوعات که نامطلوب است.

یکپارچگی(Integrity)

بیشتر مفهومی است که به علوم سیستمی بازمی‌گردد و به‌طور خلاصه می‌توان به صورت زیر تعریف کرد:

- تغییرات در اطلاعات فقط باید توسط افراد یا پروسه‌های مشخص و مجاز انجام گیرد.
- تغییرات بدون اجازه و بدون دلیل حتی توسط افراد یا پروسه‌های مجاز نباید صورت بگیرد.
- یکپارچگی اطلاعات باید در درون و بیرون سیستم حفظ شود. به این معنی که یک داده مشخص چه در درون سیستم و چه در خارج از آن باید یکسان باشد و اگر تغییر کند باید هم‌زمان درون و برون سیستم از آن آگاه شوند.

دسترس‌پذیری(Availability)

این پارامتر ضمانت می‌کند که یک سیستم همواره باید در دسترس باشد و بتواند کار خود را انجام دهد. بنابراین حتی اگر همه موارد ایمنی مدنظر باشد اما عواملی باعث خوابیدن سیستم شوند مانند قطع برق، ازنظر یک سیستم امنیتی این سیستم ایمن نیست. اما جدای از مسائل بالا پارامترهای دیگری نیز هستند که باوجودآنکه از همین اصول گرفته می‌شوند برای خود شخصیت جداگانه‌ای پیدا کرده‌اند. در این میان می‌توان به مفاهیمی نظیر Identification به معنی تقاضای شناسایی به هنگام دسترسی کاربر به سیستم، Authentication به معنی مشخص کردن هویت کاربر، Authorization به معنی مشخص کردن میزان دسترسی کاربر به منابع، Accountability به معنی قابلیت حسابرسی از عملکرد سیستم اشاره کرد.

انواع حملات شبکه‌های وایرلس

شبکه‌های Wireless یا بی‌سیم مدت‌زمانی است که در کشور ما روند رو به رشدی داشته است. در حال حاضر در دانشگاه‌ها، فرودگاه‌ها، مراکز تجاری و اماکنی نظیر آن‌ها دسترسی به اینترنت از طریق شبکه Wireless امکان‌پذیر است. اما نکته‌ای که وجود دارد این است که اگر ایجاد به یک شبکه بی‌سیم برای همه امکان‌پذیر است بنابراین استفاده از آن برای مجرمان و خلاف‌کاران نیز مجاز است! به همین دلیل است که امن‌سازی این شبکه‌ها و آزمون نفوذ آن بسیار حائز اهمیت است.

حملات کنترل دسترسی

درصورتی‌که بر روی شبکه وایرلس اقدامات امنیتی نظیر Mac Filtering یا Access Control صورت گرفته باشد از مجموعه حملات کنترل دسترسی جهت دور زدن اقدامات امنیتی استفاده می‌شود که دارای انواع مختلف می‌باشند که در جدول (۱) آن‌ها را معرفی می‌نماییم.

حملات علیه محرمانگی

حملات علیه محرمانگی برای جمع‌آوری اطلاعات خصوصی با رهگیری آن بر روی لینک بی‌سیم تلاش می‌کند داده‌ها در داخل یک شبکه وایرلس رمزگذاری شده یا به‌صورت شفاف ارسال می‌شوند. اگر داده‌ها رمزگذاری شوند، این حملات شامل شکستن رمزگذاری و پیدا کردن کلید می‌شود. علاوه بر این شامل حملات دیگر مانند استراق سمع، شکستن پسورد ، حملات فیشینگ بر روی نقطه‌ی دسترسی(AP) و حملات مرد میانی نیز است. انواع حملات علیه محرمانگی شامل موارد جدول (۲) است.

در ادامه به معرفی ابزارهای آزمون نفوذ در شبکه‌های وایرلس بر اساس این سه اصل امنیتی می‌پردازیم.

حملات یکپارچگی

حملات یکپارچگی را می‌توان یک مشخصه دانست که بر اساس آن اطمینان حاصل می‌شود که داده‌ها در هنگام انتقال از نقطه A به نقطه B بدون هیچ تغییر یا مشکل انتقال پیدا می‌کند. در شبکه‌های وایرلس ۸۰۲,۱۱، یک مهاجم می‌تواند با قرار گرفتن در همان سطح فرکانسی به سوءاستفاده از داده‌ها بپردازد. همچنین در این حملات، هکرها فریم‌های جعلی کنترلی یا مدیریتی و یا دیتا را تحت یک شبکه وایرلس ارسال می‌کنند تا دستگاههای وایرلس را از مسیر خود منحرف نمایند.

حملات علیه احراز هویت

حملات DoS ساده هستند، اما از آن‌ها می‌توان تنها برای اهداف محدود استفاده کرد. دسترسی به شبکه می‌تواند مهاجم با مزایای بسیار بیشتری را فراهم کند. ازآنجا که مشخصات اولیه ۸۰۲,۱۱ یک مکانیزم تائید اعتبار ناقص را تعریف می‌کند IEEE مکانیسم‌های احراز هویت جدید را بر اساس ۸۰۲,۱x و EAP معرفی کرده است. در این نوع حملات هکر سعی در شکستن مکانیسم‌های امنیتی احراز هویت را دارد.

حملات علیه در دسترس بودن

هدف این‌گونه حملات ایجاد مانعی در تحویل سرویس وایرلس به کاربر مجاز است که این کار را یا از طریق از دسترس خارج کردن منابع انجام می‌دهند و یا مانعی در دسترسی به آن‌ها ایجاد می‌کنند. حملاتی زیادی وجود دارند که در این دسته‌بندی می‌گنجند؛ در زیر به برخی از آن‌ها اشاره می‌کنیم.

جدول ۱ . انواع حملات کنترل دسترسی

نوع حمله	توضیحات
War Driving	شناسایی شبکه های وایرلس با گوش دادن به beacon و ارسال درخواست Probe به سمت آن‌ها انجام می‌شود.
Rogue Access Points	ایجاد یک نقطه اتصال ناامن یا مجازی زیر نظر فایروال که باعث باز شدن یک در پشتی باز در داخل شبکه قابل‌اعتماد می‌شود.
Ad Hoc Associations	این حمله شامل اتصال مستقیم به یک ایستگاه غیرقانونی برای دور زدن امنیت AP یا حمله به ایستگاه می‌شود. این نوع حملات با نقش مستقیم کارت شبکه وایرلس و یا دانگل (USB Wireless) صورت می‌پذیرد.
MAC Spoofing	این حملات شامل تغییر آدرس مک نفوذگر به آدرس مک مسیریاب و یا هر سیستم مجاز در داخل شبکه است.
802.1X RADIUS Cracking	این حمله باهدف به دست آوردن رمز رادیوی اقدام به بروت فورس احراز هویت EAP از طریق درخواست دسترسی ۸۰۲٫۱X برای نقطه اتصال جعلی مورداستفاده قرار می‌گیرد.

جدول ۲ . انواع حملات علیه محرمانگی

نوع حمله	توضیحات
Eavesdropping	در این حملات با گرفتن و رمزگشایی ترافیک انتقال داده شده که به‌صورت محافظت نشده می‌باشند مهاجم اقدام به گرفتن اطلاعات بالقوه حساس می‌کند.
WEP Key Cracking	این حملات شامل گرفتن اطلاعات برای بازیابی کلید WEP با استفاده از روش‌های غیرفعال یا فعال است.
Evil Twin AP	در این حملات مهاجم یک نقطه دسترسی جعلی را با نام یک نقطه دسترسی مجاز ایجاد می‌کند تا کاربر فریب خورده و وارد آن شبکه شود.
AP Phishing	این حمله با اجرا کردن یک وب سرور جعلی یا وب‌سایت بر روی شبکه Evil Twin اقدام به سرقت اطلاعات، رمزهای عبور و ... می‌کند.
MITM	شکلی از استراق سمع فعال است که در آن حمله‌کننده اتصالات مستقلی را با قربانیان برقرار می‌کند و پیام‌های مابین آن‌ها را بازپخش می‌کند، به‌گونه‌ای که آن‌ها را متقاعد می‌کند که با یکدیگر به‌طور مستقیم در طول یک اتصال خصوصی، صحبت می‌کنند؛ درحالی‌که تمام مکالمات توسط حمله‌کننده کنترل می‌شود.

جدول ۳. انواع حملات علیه یکپارچگی

نوع حمله	توضیحات
802.11 Frame Injection	در این حملات مهاجم به ارسال و یا دست‌کاری فریم‌های جعلی ۸۰۲٫۱۱ می‌پردازد برای این منظور هکر باید به اسنیف داده‌های بین شبکه‌ای بپردازد و اگر داده‌ها مطابق با یک الگوی مشخص‌شده در فایل‌های پیکربندی باشد، محتوای سفارشی مانند AP داخل شبکه وایرلس تزریق می‌شود و هکر به‌عنوان سرویس‌دهنده در نظر گرفته می‌شود.
802.11 Data Replay	در این حملات مهاجم مانند حملات Frame injection به گرفتن پکت ها به‌گونه‌ای که از ارسال آن‌ها جلوگیری شود و یک داده جدید که حاوی محتوای خاص است را جایگزین می‌کند و برای سرویس‌گیرنده ارسال می‌نماید.
802.1X EAP Replay	در این حملات مهاجم اقدام به گرفتن پروتکل احراز هویت قابل‌تعمیم بین کاربر و دستگاه AP می‌پردازد تا بتواند بعداً از آن‌ها استفاده کند.
802.1X RADIUS Replay	در این حملات هکر به گرفتن پیام‌های RADIUS بین دستگاه AP و سرور احراز هویت می‌پردازد تا بتواند بعداً از آن‌ها استفاده نماید.

جدول ۴. حملات علیه احراز هویت

نوع حمله	توضیحات
PSK Cracking	در این حملات مهاجم سعی در به دست آورد کلیدهای WPA/WPA۲ PSK در داخل فریم Handshake از طریق حملات فرهنگ لغت یا BruteFroce و Hybrid و ... را دارد.
Application Login Theft	در این حملات هکر اقدام به دزدیدن و به دست آوردن کلمه عبور از طریق پروتکل‌های رمزنگاری نشده می‌کند.
Domain Login Cracking	در آن حملات مهاجم اقدام به گرفتن پسورد حساب‌های کاربری ویندوز از طریق شکستن پسوردهای هش شده پروتکل Netbios با حملات مختلف مانند Bruteforce، حملات فرهنگ لغت و جداول Rainbow و... می‌پردازد.
VPN Login Cracking	در آن حملات مهاجم اقدام به گرفتن پسورد PPPT یا IPSec به‌صورت رمزنگاری‌شده می‌کند تا آن‌ها را رمزگشایی کند.
802.1X Identity Theft	این حملات اقدام به بدست آوردن روش‌های احراز هویت بدون رمزنگاری در 802.1X می‌نمایید مانند EAP-GTC
802.1X Password Guessing	در این حمله هکر اقدام به گرفتن داده‌های رمزنگاری‌شده از نوع EAP می‌کند تا بتواند با استفاده از حملات مختلف پسورد رمزنگاری‌شده را رمزگشایی کند.
802.1X EAP Downgrade	در این حملات هکر اقدام به مجبور کردن یک سرور 802.1X برای ارائه یک نوع تائید هویت ضعیف با استفاده از جعل بسته‌های EAP-Response / Nak می‌کند.

جدول ۵. انواع حملات علیه در دسترسی بودن

نوع حمله	توضیحات
AP Thief	به‌صورت فیزیکی اکسس پوینت را از شبکه خارج می‌کنند.
Queensland DoS	با سوءاستفاده از مکانیزم ارزیابی کانال CSMA/CA، طوری نشان خواهد داد که کانال موردنظر اشغال است. در این صورت گره دیگری تا زمان آزاد شدن کانال، اطلاعات را ارسال نمی‌کند. برای این کار کارت شبکه شما باید از حالت CW Tx پشتیبانی کند.
802.11 Beacon Flood	در این حمله مهاجم اقدام به ایجاد هزاران ۸۰۲٫۱۱ beacons می‌کند تا ایستگاه کاری نتواند AP واقعی را شناسایی کند.
802.11 Associate / Authenticate Flood	در این حملات مهاجم اقدام به ارسال احراز هویت‌ها و ارتباطات جعلی می‌کند تا جدول ارتباط AP پر شود و دیگر قادر به ایجاد ارتباط با سیستم‌های قانونی و غیر جعلی را نداشته باشد.
802.11 TKIP MIC Exploit	در این حمله مهاجم اقدام به تولید داده‌های نامعتبر TKIP برای عبور از آستانه خطای MIC در APهای شبکه می‌کند تا سرویس‌های شبکه را به تعلیق بیاندازد.
802.11 Deauthenticate Flood	در این حملات مهاجم اقدام به ایجاد سیلی از APها با پیام EAP-Start می‌کند تا از این طریق بتواند منابع شبکه را مصرف و یا موجب کرش کردن آن‌ها و یا و موجب حذف کاربرهای متصل به آن شود.
802.1X EAP-Failure	در این حمله مهاجم تبادل یک 802.1x EAP مجاز را زیر نظر گرفته و سپس به Station یک پیام جعلی EAP-Failure ارسال می‌کند تا منابع داخلی شبکه را مشغول نماید.
802.1X EAP-of-Death	در این حملات مهاجم اقدام به ارسال یک درخواست شناخته‌شده نادرست برای هویت EAP در 802.1x می‌کند.
802.1X EAP Length Attacks	در این حمله مهاجم اقدام به ارسال پیام‌های خاص EAP با فیلدهای طولی طولانی می‌کند که باعث شلوغی زیاد یک سرور AP یا RADIUS می‌کند و نهایتاً باعث خراب شدن و از کار افتاده شدن آن‌ها می‌شود.

بررسی الگوریتم رمزنگاری پسوردهای ذخیره شده وایرلس

■ نویسنده: مسلم حقیقیان

مقدمه

برنامه های محدودی به‌منظور دستیابی به پسوردهای ذخیره‌شده وایرلسهایی که از قبل به آن‌ها متصل شده‌اید وجود دارد. به‌عنوان‌مثال ۲ برنامه زیر از معروف‌ترین آن‌ها هستند.

http://www.nirsoft.net/utils/wireless_key.html

http://securityxploded.com/wifi-password-decryptor.php

در این مقاله به بررسی نحوه نوشتن این‌گونه برنامه ها می‌پردازیم.

محل ذخیره سازی رمزعبور و طریقه رمزنگاری آن

در هر بار وارد کردن پسورد WIFI و ورود به آن تمامی آن پسوردها در فایل‌هایی با پسورد XML در داخل پوشه زیر ذخیره می‌شوند.

C:\ProgramData\Microsoft\Wlansvc\Profiles\Interfac

در این فایل‌ها مشخصات هر WiFi نیز آورده شده است که محتویات این فایل‌ها به شکل زیر است .

```
<?xml version=""1.0?>
<WLANProfile xmlns="http://www.microsoft.com/networking/WLAN/profile/v"1>
<name>Cisco</name>
<SSIDConfig>
<SSID>
<hex>436998736F3236312338</hex>
<name>L4tr0d3ctism</name>
</SSID>
</SSIDConfig>
<connectionType>ESS</connectionType>
<connectionMode>auto</connectionMode>
<MSM>
<security>
<authEncryption>
<authentication>WPA2PSK</authentication>
<encryption>AES</encryption>
<useOneX>false</useOneX>
</authEncryption>
<sharedKey>
<keyType>passPhrase</keyType>
<protected>true</protected>
<keyMaterial>7h15is4f4k3P455w0rDf0r7h154r71c13...</keyMaterial>
</sharedKey>
</security>
</MSM>
</WLANProfile>
```

همان‌طور که می‌بینید اطلاعاتی را می‌توان از طریق این XML فایل‌ها در مورد یک WiFi به دست آورد مانند Name , connectionType , connectionMode , authentication و ... اما بحث اصلی در مورد مقدار keyMaterial است که همان پسورد به‌صورت رمزنگاری‌شده است.

رشته بالا مقدار رمزنگاری‌شده پسورد SSID موردنظر است که با استفاده از تابع CryptProtectData رمزنگاری‌شده است. این تابع یکی از پرکاربردترین تابع‌های رمزنگاری در سیستم‌عامل‌های مایکروسافت است که ساختار آن به شکل زیر است:

```
BOOL CryptProtectData
(
  DATA_BLOB*                  pDataIn,
  LPCWSTR                     szDataDescr,
  DATA_BLOB*                  pOptionalEntropy,
  PVOID                       pvReserved,
  CRYPTPROTECT_PROMPTSTRUCT*  pPromptStruct,
  DWORD                       dwFlags,
  DATA_BLOB*                  pDataOut
)
```

این تابع به رمزنگاری داده‌ها با استفاده از ساختار DATA_BLOB می‌پردازد که دارای یک کلید جهت رمزگشایی است که این کلید را با استفاده از شناسه دستگاه فعلی و سیستم اعتبارسنجی کاربر ایجاد می‌کند. درنتیجه شما می‌توانید با وارد کردن اطلاعات مربوط به اعتبارسنجی کاربر این رشته رمزنگاری‌شده را رمزگشایی نمایید.

در زیر به بررسی مؤلفه‌های این تابع می‌پردازیم.

pDataIn : این مؤلفه یک اشاره‌گر به ساختار DATA_BLOB است که حاوی متن ساده یا همان رمز عبور برای کدگذاری است که توسط برنامه‌نویس باید وارد شود.

szDataDescr : در این قسمت توضیحاتی در مورد رشته وارد شده می‌توانیم بنویسیم که البته می‌توان مقدار آن را نیز NULL قرار داد.

pOptionalEntropy : جهت اضافه کردن آنتروپی یا کدگذاری منبع جهت پیچیده‌تر کردن مقدار رمزنگاری‌شده از این مؤلفه استفاده می‌شود در اصل کدگذاری منبع، تلاش می‌کند تا داده‌ها را به‌صورت فشرده از یک منبع دربیاورد تا بتواند آن‌ها را به‌صورت مؤثر انتقال دهد.

pvReserved : این مقدار به‌صورت رزرو شده جهت توسعه این تابع ایجادشده است که مقدار آن فعلاً باید NULL باشد.

pPromptStruct : یک اشارهگر به ساختار CRYPTPROTECT_PROMPTSTRUCT است که اطلاعاتی در مورد زمان و مکان فراهم می‌کند که می‌توانید مقدار آن را NULL قرار دهید.

dwFlags : این مؤلفه گزینه‌هایی را برای رمزنگاری انتخاب می‌کند که عملیات رمزگشایی توسط تمام حسابهای کاربری انجام شود و... شما می‌توانید مقدار آن را با ۰ مقداردهی کنید.

pDataOut : بعد از استفاده از این تابع مقدار رمزگذاری شده در این مؤلفه قرار می‌گیرد.

اگر شما برنامه‌نویس در C/C ++ باشید روش استفاده از این تابع به شکل زیر است:

```
DATA_BLOB DataIn;
DATA_BLOB DataOut;
BYTE *pbDataInput =(BYTE *)"Hello world of data protection.";
DWORD cbDataInput = strlen((char *)pbDataInput)1+;

DataIn.pbData = pbDataInput;
DataIn.cbData = cbDataInput;

if(CryptProtectData(
    &DataIn,
    L"This is the description string.",
    NULL,
    NULL,
    NULL,
    0,
```

```
    &DataOut))
 {
     printf("The encryption phase worked.\n");
 }
 else
 {
    printf("Encryption error using
CryptProtectData.\n");
    exit(1);
 }
```

سیستم عامل ویندوز نیز به همین شکل مقدار DataOut را به‌صورت String در داخل KeyMaterial قرار میدهد و خروجی به شکل زیر است:

```
7h15is4f4k3P455w0rDf0r7h154r71c13...
```

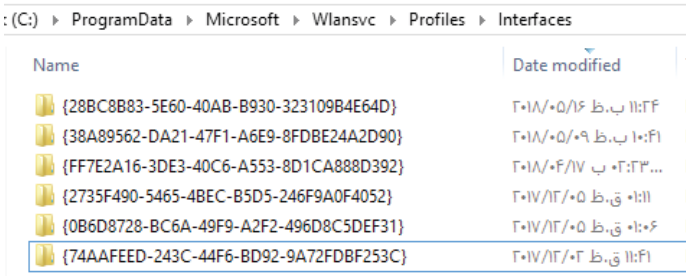
رمزگشایی مقدار KeyMaterial

همان‌طور که در بالا گفته شد جهت رمزنگاری از تابع cryptprotectdata استفاده می‌شود و جهت آسان کردن کار برنامه‌نویسان خود تابعی را بانام CryptUnprotectData فراهم کرده است تا بتوان مقادیر رمزگذاری شده توسط تابع cryptprotectdata را رمزگشایی نمود.

به دلیل اینکه مقدار برگشتی به‌صورت رشتهای در فایل XML ذخیره می‌شود اول از همه باید با استفاده از تابع CryptStringToBinary باید مقدار رشتهای را به باینری تبدیل کرده و سپس آن را به تابع CryptUnprotectData داد تا مقدار را رمزگشایی کند.

طریقه استفاده از تابع CryptStringToBinary به شکل زیر است:

```
 WCHAR szKey[] = L"7h15i54f4k3P455w0rDf0r7h154r7
1c13...";
 BYTE byKey[1024];
 DWORD cbBinary, dwFlags, dwSkip;
```




```
 CryptStringToBinary (szKey, lstrlenW(szKey), CRYPT_
STRING_HEX,byKey, &cbBinary, &dwSkip, &dwFlags);
```

سپس درصورتی‌که عملیات با موفقیت انجام شود مقدار خروجی را برای تابع CryptProtectData آماده می‌کنیم.

```
 if (!bIsSuccess) __leave;
        DataOut.cbData = cbBinary;
        DataOut.pbData = (BYTE*)byKey;
```

حال فقط کافی است مقدار DATAOUT را به‌عنوان ورودی به تابع CryptProtectData بدهیم به شکل زیر:

```
 if (CryptUnprotectData (&DataOut, NULL, NULL, NULL,
NULL, 0, &DataVerify)){
 _tprintf(TEXT("The decrypted data is: %hs\n"),
DataVerify.pbData);
```

توسعه بهتر برنامه

در حالت کلی تمامی برنامه های ساخته شده فعلی دارای یک مشکل اساسی میباشند که آن نیز این است که رمزعبور آخرین واسط سخت افزاری نصب شده برروی سیستم عامل را برای شما رمزگشایی میکنند که شما برای رفع این محدودیت کافیست تمام واسطها را انتخاب کرده و مقادیر Keymaterial فایلهای داخل آن‌ها را برای رمزگشایی به تابع CryptUnprotectData بدهید.

همانطور که در شکل بالا مشخص است در هر بار حذف و نصب سخت افزاری کارت شبکه وایرلس یک واسط جدید با ایدی خاص ایجاد میشود که شامل تمام پروفایلهای مربوط به اتصالات وایرلس می باشد.

متاسفانه بعد از حذف کامل یک کارت شبکه و نصب کارت شبکه جدید تمامی SSIDهایی که از قبل به آن وصل شده‌اید و رمزعبور آن‌ها ذخیره شده است از سیستم عامل پاک نمی‌شود و این امر میتواند برای کاربر مخاطره آمیز باشد.

دفتر تقلب

نویسنده: محمد حبیبی

تست نفوذ شبکه وایرلس با رمز گذاری WEP

فعال کردن کارت شبکه وایرلس	ifconfig [wlan Interface] up
تغییر حالت کارت شبکه به مود مانیتورینگ در کانال مشخص شده	airmon-ng start [wlan Interface] [Channel]
تست قابلیت Packet Injection کارت شبکه	aireplay-ng -9 -e [AP Name] -a [router bssid] [monitor interface]
شروع به ذخیره IVs های تولید شده توسط اکسس پوینت هدف	airodump-ng –c 9 –bssid [router bssid] –w [output file name] [monitor interface]
شروع به ایجاد اعتبار سنجی‌های جعلی با استفاده از مک آدرس یکی از کاربران اکسس پوینت هدف	aireplay-ng -1 0 -e [AP Name] -a [router bssid] -h [client bssid] [monitor interface]
ارسال درخواست‌های ARP برای اکسس پوینت با استفاده از مک آدرس یکی از کاربران AP هدف	aireplay-ng -3 -b [router bssid] -h [client bssid] [monitor interface]
شروع به کرک کردن رمز عبور با استفاده از فایل ذخیره شده از IVsهای	aircrack-ng -b [router bssid] [output file name]

تست نفوذ شبکه وایرلس با رمز گذاری WPA/WPA2

فعال کردن کارت شبکه وایرلس	ifconfig [wlan Interface] up
تغییر حالت کارت شبکه به مود مانیتورینگ	airmon-ng start [wlan Interface]
با اعمال این دستور لیست اکسس پوینت‌های موجود را مشاهده میکنیم	airodump-ng [monitor interface]
با اجرای این دستور ترافیک شبکه اکسس پوینت هدف را ذخیره میکنیم	airodump-ng -c [channel] --bssid [router bssid] -w [Output Directory] [monitor interface]
ارسال درخواست deauthentication برای اکسس پوینت هدف با استفاده از مک آدرس یکی از کاربران تایید شده	aireplay-ng –2 0 –a [router bssid] –c [client bssid] [monitor interface]
شروع به فرایند کرک handshake ذخیره شده در فایل	aircrack-ng -a2 -b [router bssid] -w [path to wordlist] ./*.cap

معرفی ابزار، مقاله، کتاب

■ معرف: مسلم حقیقیان

ابـــزار aircrack-ng یک مجموعه کامل از ابزارها برای ارزیابی امنیت شبکه WiFi است. این ابزار از استانداردهای مختلف مانند 802.11a , 802.11b , 802.11g پشتیبانی می‌کند و برای ورژن‌های مختلف آن بـــرای تمامی پلتفرم‌های linux ، FreeBSD، OpenBSD، OS X و window وجود دارد.

ابـــزار aircrack-ng نه تنها توانایی انجام آزمون نفوذ بر روی شبکه را انجام می‌دهد بلکه می‌تواند شبکه را مورد حمله قرار دهد و به هکر اجازه می‌دهد که به پسورد دسترسی پیدا کند.

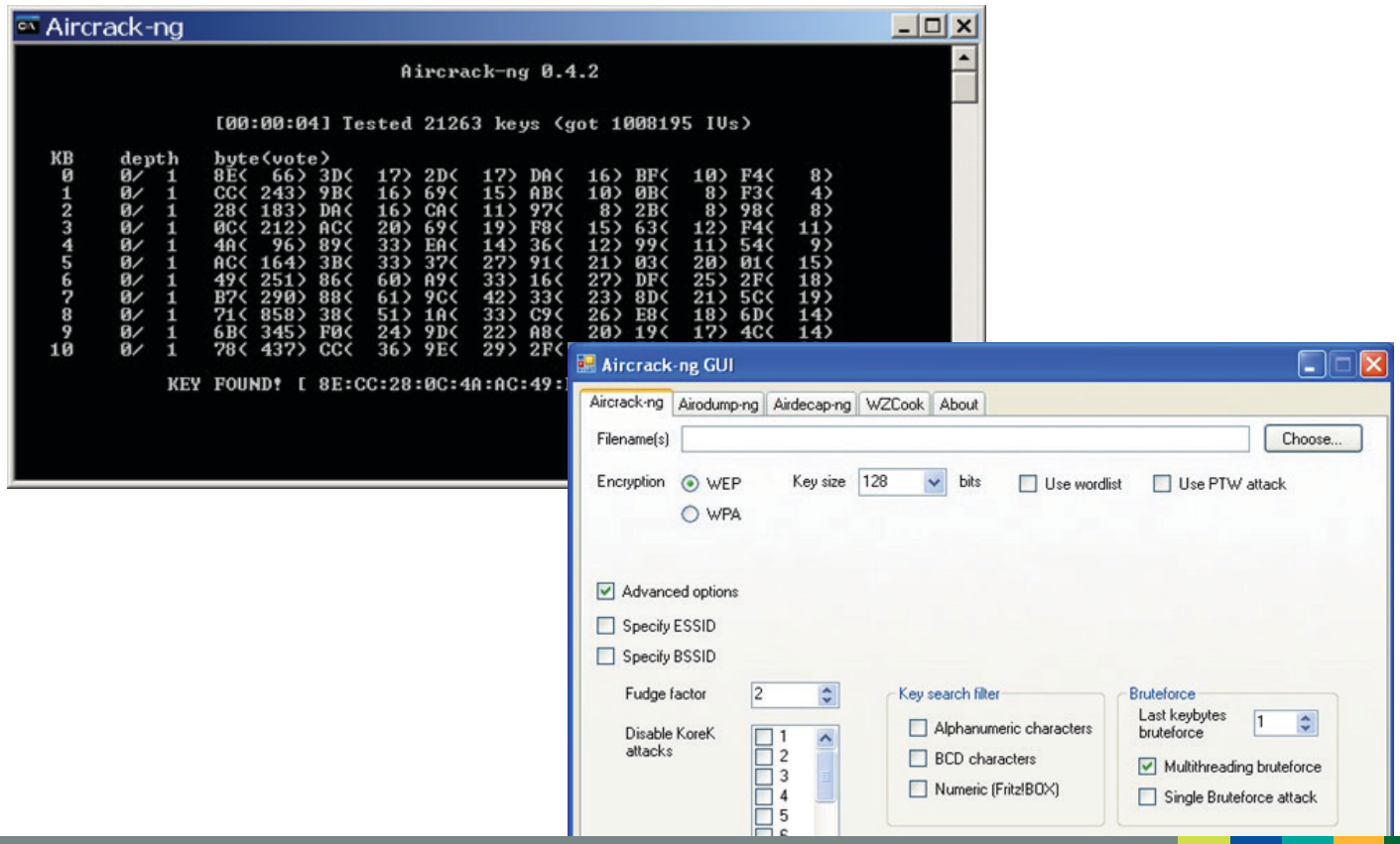
از ویژگی‌های این برنامه می‌توان به موارد زیر اشاره نمود:

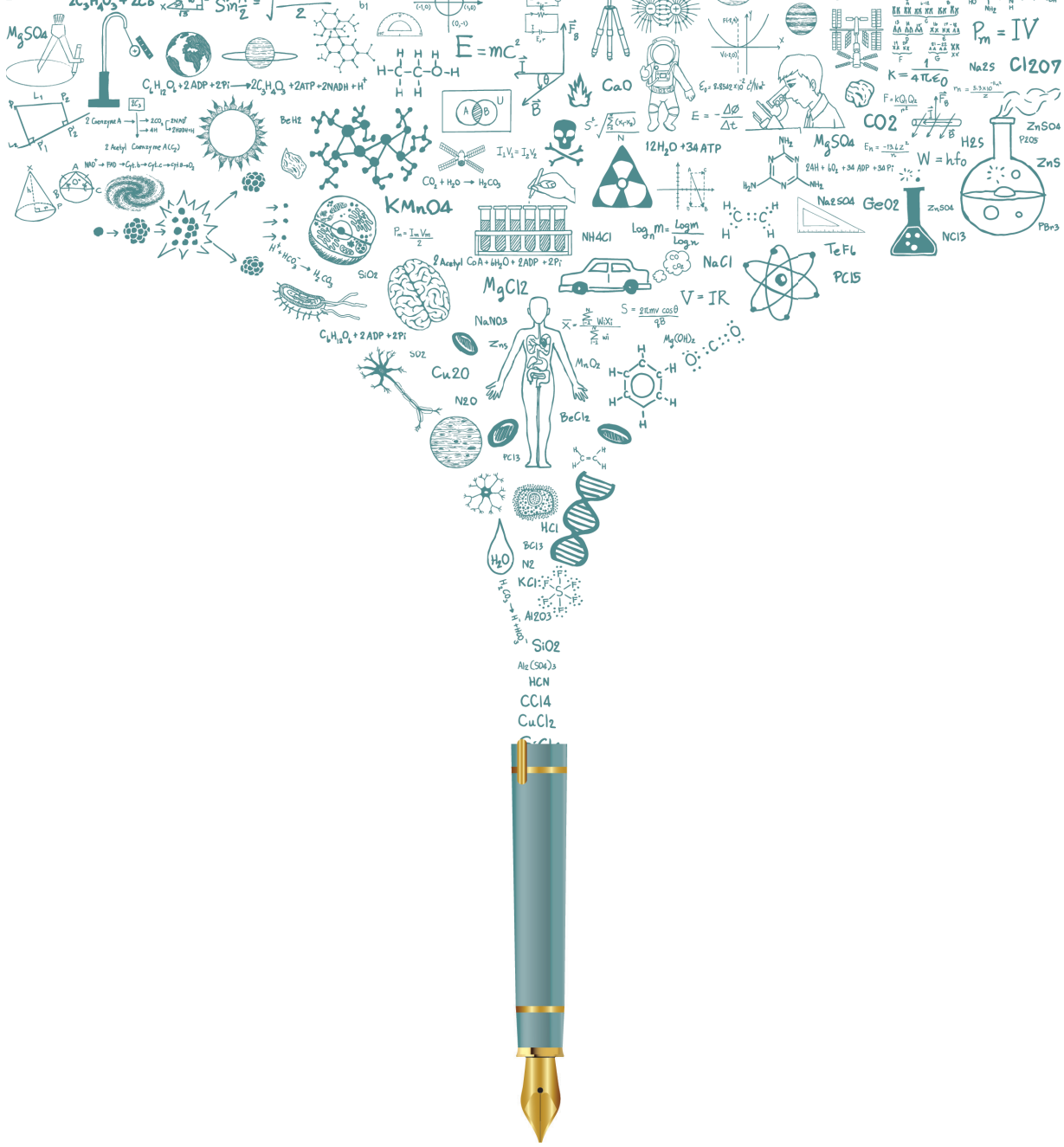
- نظارت: ثبت بســـته و صدور داده‌ها بـــه فایل‌های متنی برای پردازش بیشتر توسط ابزارهای ثالث
- حمله: حمله پاسخ، ایجاد نقاط دسترسی جعلی از طریق تزریق بسته
- آزمـــون: چک کردن کارت‌هـــای WiFi و قابلیت‌های درایور (ثبت و تزریق)
- کرک رمزهای عبور WEP و WPA و WPA2

مجموعه نرم افزاری aircrack شامل نرم افزارهای زیر است.

لازم به ذکر اســـت که این ابزار دارای یک ورژن GUI نیز است که توسط خود توسعه دهنده این برنامه نوشته شده است.

نام ابزار	توضیحات
aircrack-ng	برنامه‌ای جهت شکستن پسوردهای WEP 802.11 و PSK-WPA/WPA2
airdecap-ng	جهت رمزگشـــایی بستههای دریافت شـــده (Capture File) از پروتکلهای WEP,WPA/ WPA2 استفاده می‌شود.
airmon-ng	ابزاری برای فعال سازی monitor-mode در کارت شبکه‌های وایرلس
aireplay-ng	ابزاری برای تزریق بسته به درون شبکه‌های وایرلس.
Airodump	Airodump-ng برای گرفتن بسته فریم‌های خام 802.11 استفاده می‌شود و مخصوصا برای جمع‌آوری (WEP IV (Vectorisation Vector بەمنظور استفاده از آن‌ها در aircrack-ng است.
airtun-ng	یک برنامه جهت ساختن رابط تونل مجازی است.
packetforge-ng	ابزاری برای ســـاخت انواع مختلفی از بسته‌های رمزگذاری شده که از آن می‌توان برای تزریق استفاده کرد.
airbase-ng	ابزاری برای ســـاخت اکسس پوینت‌های جعلی و تقلبی که به ما امکان استفاده از حملات MITM را می‌دهد.
airdecloak-ng	ابزاری برای حذف فایل WEP Cloak از فایل‌های pcap.
airolib-ng	برای ذخیره و مدیریت لیست‌های essid و password ها و کلیدهای PMK و از آن‌ها در شکستن پسوردهای WPA / WPA2 در AirCrack-ng استفاده می‌کند.
airserv-ng	کارت بی‌ســـیم سرور TCP/IP است که اجازه استفاده چند برنامه را به‌صورت هم‌زمان به این کارت را می‌دهد.
esside-ng	این ابزار امکان برقراری ارتباط به نقطه دسترسی که با الگوریتم رمزگذاری WEP پیکربندی شده است را بدون دانستن کلید می‌دهد.
tkiptun-ng	ابزاری برای انجام حملات WPA/TKIP با اســـتفاده از تزریق چند فریم به WPA TKIP شـــبکه با QoS
wessid-ng	این ابزار شـــامل تعدادی از روش‌های یکپارچه برای به دســـت آوردن کلیـــد WEP در کمترین زمان ممکن است.





معرفی مقاله

انواع حملات شبکه های Wi-Fi و ابزارهای ارزیابی امنیتی آن

معرف: محمد حبیبی

باوجودآنکه به نظر می‌رسد که از نظر فنی عبارت شبکه بی‌سیم جهت اشاره به هر نوع شبکه‌ای که بی‌سیم باشد به کار می‌رود. این اصطلاح بیشتر برای اشاره به شبکه‌های ارتباطی استفاده می‌شود که در آن گره‌ها بدون استفاده از سیم به یکدیگر متصل می‌شوند برای نمونه یک شبکه رایانه‌ای نوعی از شبکه‌های ارتباطی است. از آنجا که شـــبکه‌های بی‌ســـیم، در دنیای کنونی هرچه بیشتر در حال گسترش هستند و با توجه به ماهیت این دسته از شبکه‌ها، که بر اساس سیگنال‌های رادیویی‌اند، مهم‌ترین نکته در راه استفاده از این فنّاوری، آگاهی از نقاط قوت و ضعف آن است. نظر به لزوم آگاهی از خطرات استفاده از این شبکه‌ها، با وجود امکانات نهفته در آن‌ها که به مدد پیکربندی صحیح می‌توان به سطح قابل قبولی از بعد امنیتی دست‌یافت، بنا داریم در این مقاله به بررسی حملات در شبکه‌های بی‌سیم و معرفی ابزارهای موردنیاز در آزمون نفوذپذیری آن پرداخته شده است.

نام نویسنده مقاله: مسلم حقیقیان
تاریخ انتشار: ۱۳۹۷
زبان: فارسی
تعداد صفحات: ۵۷

لینک دانلود:

■ معرف: مسلم حقیقیان

در کتاب تست نفوذ وایرلس , کار را با آموزش مفاهیم مقدماتی شبکه وایرلس شروع کرده, شما را با ابزارهای خط فرمان و نحوه استفاده از آن‌ها آشنا کرده است. به منظور اجرای آزمایش‌های متنوع کتاب پیش نیازها و ابزارهای مورد نیاز را به شما معرفی کرده و در ادامه یک محیط تست آزمایشی ایجاد خواهد کرد.
اولین فاز اسکن محیط می‌باشد. کار را با شنود محیط آغاز کرده , عبور از پیکربندی های امنیتی را پیاده سازی کرده و به شکستن مدل‌های مختلف رمزنگاری خواهد پرداخت. حمله را به زیرساخت WLAN تغییر مسیر داده ولی به زیرساخت اکتفا نکرده و کلاینت ها را هدف قرار می‌دهد. در ادامه حملات و تکنیک‌های پیشرفته وایرلس را اجرا خواهد کرد و شما را با شیوه پیاده سازی حملات بر روی شبکه های Enterprise آشنا خواهد نمود. در این کتاب متدولوژی تست نفوذ وایرلس معرفی شده و خواننده را با حملات WPS آشنا کرده و به اکسپلوییت دستگاه‌های وایرلس خواهد پرداخت. سناریوهای متنوع حملات شخص واسط و حملات دوقلو شرور را اجرا کرده و به شنود پیشرفته شبکه وایرلس پرداخته و با جدیدترین ابزارهای تست نفوذ وایرلس آشنا کرده و ده‌ها آزمایش مختلف را اجرا می‌کند. در سه فصل پایانی سعی خواهد کرد تا سناریوهای اجرا شده را این بار با استفاده از اسکریپت‌های بش اجرا کرده و فرایند تست نفوذ را اتوماسیون کرده تا در زمان صرفه جویی شود. در این بخش پایانی یاد می گیریم چگونه می توان با استفاده از بش, اسکریپت های قدرتمند ایجاد کرده و ده پروژه اسکریپت نویسی را اجرا کنیم.

نام کتاب : کتاب تست نفوذ وایرلس
تاریخ انتشار : فروردین ۱۳۹۶
موضوع : امنیت شبکه
سطح آموزش : مقدماتی تا پیشرفته
تعداد صفحات : ۷۴۱ صفحه
نسخه : پی دی اف (PDF)
نویسنده و مترجم : محمد شریعتی مهر

خرید و سفارش:

| گزارش تحلیلی و آسیب پذیری

تهدیدات بدافزارهای موبایلی و تکامل این بدافزارها

تهدیدات در حوزه موبایل

■ نویسنده: هادی گلباغی

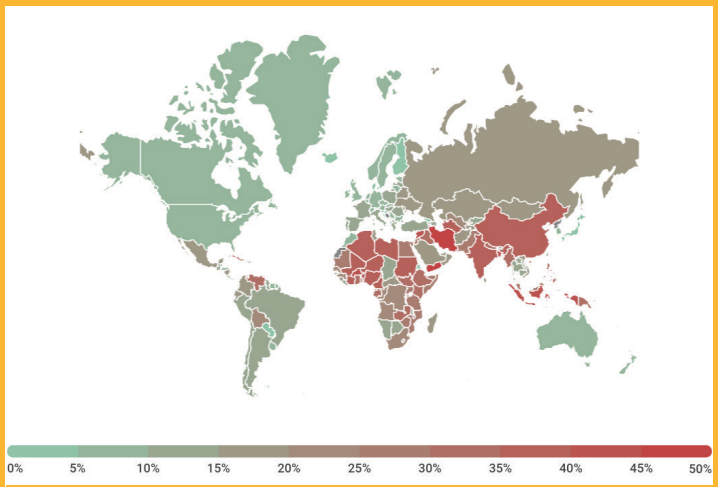
حملات مخرب موبایلی در حدود ۲۳۰ کشـــور در ســـال ۲۰۱۷ صورت گرفته اســـت که جغرافیای این حملات در شـــکل ۱ نشان داده شده است. در جدول ۱ نیز ۱۰ کشوری که بیشترین حملات بدافزار موبایلی داشـــته‌اند را نشـــان می‌دهد(اعداد بر اساس درصد کاربـــران مورد حمله قرار گرفته می‌باشـــد). ایران با ۵۷,۲۵ درصد دارای بالاترین فراوانی بوده اســـت که در سال ۲۰۱۶ دارای جایگاه دوم در این لیســـت بود و در ســـال ۲۰۱۷ در رتبه اول قرار گرفته اســـت و جای خود را با بنگلادش عوض کرده است. در سال ۲۰۱۷ بیشـــتر از نیمی از کاربران موبایل در ایـــران بدافزارهای موبایلی را تجربه کرده‌اند. بیشترین فراوانی بدافزارها در ایران مربوط به خانواده Ewind بوده که مربوط به برنامه‌های تبلیغاتی هستند و همچنین خانـــواده تروجـــان Trojan.AndroidOS.Hiddapp نیز دارای فراوانی بالایی بوده است.

در جایـــگاه دوم بنگلادش با ۴۲,۷۶ درصد قرار دارد که کاربران این کشـــور به طور معمول مورد حمله تبلیغ‌افزارها قرار گرفته‌اند. همچنیـــن تروجـــان Trojan.AndroidOS.Agent.gp که یک برنامه مخرب اســـت، قادر به ســـرقت پول کاربر از طریق برقراری تماس برای حق بیمه می‌باشـــد و دارای رشد بالایی بوده است. به طور تقریبی در همه کشورها مطرح‌ترین برنامه‌های مخرب مربوط به برنامه‌هایی بوده‌اند که از طریق تبلیغات کسب درآمد می‌کنند. در هند نیز با ۳۶,۴۲ درصد که در رتبه هشـــتم اســـت تبلیغ‌افزار AdWare.AndroidOS.Agent.n دارای بالاتریـــن فراوانی اســـت که با کلیک به روی صفحـــات وب یک صفحه ابتدا برای تبلیغات باز می‌شـــود که بدون دانش کاربر بـــا هرگونه کلیکی این تبلیغات نمایش داده خواهند شد. سایر بدافزارهای موبایلی با فراوانی بالا در هند خانواده Loapi بوده اســـت که این مورد نیز با کلیک بر روی صفحات وب و نمایش تبلیغات درآمد کســـب می‌کند. در یک نگاه کلی آمار مربوط به بدافزارهای موبایلی در ســـال ۲۰۱۷ به صورت زیر بوده است:

باج‌افزارهای موبایلی : ۵۴۴۱۰۷
پکیج‌های مخرب نصب شده : ۵۷۳۰۹۱۶
تروجان‌های بانکی موبایل : ۹۴۳۶۸

انواع بدافزارهای موبایلی

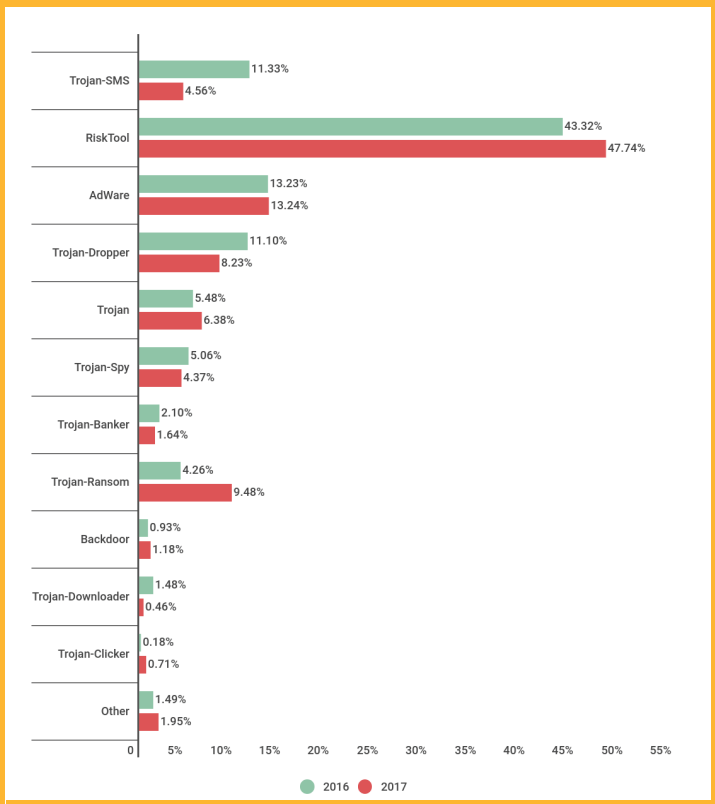
در سال ۲۰۱۷ فراوانی مربوط به انواع مختلف بدافزارهای موبایلی به صورت شکل ۲ بوده است که در آن مقایسه‌ای هم با سال ۲۰۱۶ انجام شده است.



شکل ۱.جغرافیای مربوط به تهدیدات موبایلی بر اساس تعداد حملات انجام گرفته در سال ۲۰۱۷

	Country*	%**
1	Iran	57.25
2	Bangladesh	42.76
3	Indonesia	41.14
4	Algeria	38.22
5	Nigeria	38.11
6	China	37.63
7	Côte d'Ivoire	37.12
8	India	36.42
9	Nepal	34.03
10	Kenya	33.20

جدول ۱.آمار مربوط به کشورهایی که دارای بیشترین تهدیدات موبایلی بوده‌اند.



شکل ۲. توزیع بدافزارهای موبایلی جدید بر اساس انواع آن‌ها و مقایسه سال‌های ۲۰۱۶ و ۲۰۱۷

لیست ۲۰ بدافزار موبایلی با بالاترین درصد فراوانی

در شکل ۳ فقط بدافزارهای موبایلی مخرب قرار داده شده‌اند و برنامه‌هایی که به صورت بالقوه خطرناک باشند و یا غیرمطمئن باشند مانند تبلیغ‌افزارها و یا Risktool ها قرار داده نشده‌اند. همانند سال‌های گذشته جایگاه نخست مربوط به DangerousObject.Multi.Generic که ۶۶٫۹۹ درصد بوده است که برای برنامه‌های مخرب مورد استفاده می‌باشد که توسط

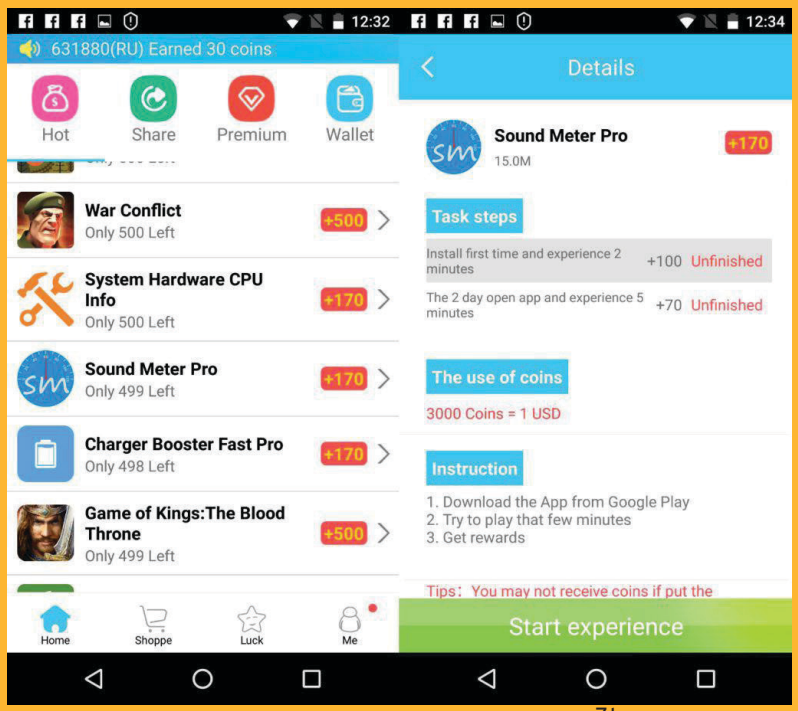
	Verdict	%*
1	DangerousObject.Multi.Generic	66.99%
2	Trojan.AndroidOS.Boogr.gsh	10.63%
3	Trojan.AndroidOS.Hiddad.an	4.36%
4	Trojan-Dropper.AndroidOS.Hqwar.i	3.32%
5	Backdoor.AndroidOS.Ztorg.a	2.50%
6	Backdoor.AndroidOS.Ztorg.c	2.42%
7	Trojan.AndroidOS.Sivu.c	2.35%
8	Trojan.AndroidOS.Hiddad.pac	1.83%
9	Trojan.AndroidOS.Hiddad.v	1.67%
10	Trojan-Dropper.AndroidOS.Agent.hb	1.63%
11	Trojan.AndroidOS.Ztorg.ag	1.58%
12	Trojan-Banker.AndroidOS.Svpeng.q	1.55%
13	Trojan.AndroidOS.Hiddad.ax	1.53%
14	Trojan.AndroidOS.Agent.gp	1.49%
15	Trojan.AndroidOS.Loapi.b	1.46%
16	Trojan.AndroidOS.Hiddapp.u	1.39%
17	Trojan.AndroidOS.Agent.rx	1.36%
18	Trojan.AndroidOS.Triada.dl	1.33%
19	Trojan.AndroidOS.Iop.c	1.31%

شکل ۳. لیست ۲۰ بدافزار موبایلی که بر اساس درصد کاربران بیشتری را مورد حمله قرار داده‌اند

```
__pid_t __fastcall dvmHeapSourceStartupBeforeFork(int a1, int a2, int a3, int a4)
{
  __pid_t result; // r0@1
  __pid_t v5; // r0@2
  int v6; // r0@2
  const char *v7; // [sp+0h] [bp-54h]@2
  int v8; // [sp+4h] [bp-50h]@2
  int v9; // [sp+24h] [bp-30h]@1
  int v10; // [sp+28h] [bp-2Ch]@1
  int v11; // [sp+2Ch] [bp-28h]@1

  v9 = a2;
  v10 = a3;
  v11 = a4;
  result = linux_eabi_syscall(__NR_fork);
  if ( !result )
  {
    v5 = linux_eabi_syscall(__NR_setsid);
    v7 = "/system/bin/ip";
    v8 = 0;
    v6 = linux_eabi_syscall(__NR_execve, "/system/bin/ip", (char *const *__attribute__((__org_arrdim(0,0))) )&v7, 0);
    result = 0;
  }
  return result;
}
```

شکل ۴. کتاب‌خانه‌های آلوده شده با Trojan.AndroidOS.Dvmap.a



شکل ۵. خانواده تروجان Ztorg که از طریق فروشگاه گوگل پلی توزیع شد و به صورت گسترده و فعال برای تبلیغات استفاده شده است.

تکنولوژی‌های ابری شناسایی شده است. تکنولوژی‌های ابری زمانی‌که بانک اطلاعاتی آنتی‌ویروس دارای امضای خاصی نباشد و برنامه مخرب توسط روش‌های اکتشافی کشف نشود بسیار مفید خواهد بود. اساساً آخرین بدافزارها بر این اساس شناسایی شده‌اند.

مواردی که در سال ۲۰۱۷ در بدافزارهای موبایلی شایع و مطرح بوده‌اند در ادامه مورد بررسی قرار می‌گیرند.

بدافزارهای موبایلی سطح هسته (Rooting mobile malware) : تسلیم نشدنی

در سال‌های اخیر بدافزارهای موبایلی سطح هسته بزرگترین مشکل کاربران اندرویدی بوده است. این تروجان بسیار سخت شناسایی شده و دارای مجموعه‌ای توانایی بوده و برای مجرمان سایبری بسیار محبوب است. هدف اصلی آن‌ها نمایش تعداد بسیاری تبلیغات و حتی ممکن است به صورت پنهانی یک اپلیکیشن را نصب کرده و برای تبلیغات از آن استفاده کنند. در برخی موارد، نمایش بسیار زیاد تبلیغات و تاخیر در اجرای فرمان‌ها و دستورات می‌تواند دستگاه موبایل را غیر قابل استفاده کند.

این بدافزارهای سطح هسته معمولا سعی در به‌دست آوردن سطح دسترسی super-user که با بهره‌برداری از آسیب‌پذیری‌های سیستم قادر به هر کاری خواهند بود را دارند. آن‌ها ماژول‌های خود را در پوشه سیستم نصب کرده و بدین‌وسیله از حذف خود محافظت می‌کنند. در برخی موارد مانند Ztorg حتی با تنظیم مجدد دستگاه به تنظیمات کارخانه نیز این بدافزار مخرب پاک نخواهد شد. زمانی قضیه حادتر می‌شود که فهمید این تروجان در فروشگاه گوگل پلی توزیع شده است که در حدود ۱۰۰ اپلیکیشن با انواع مختلف Ztorg آلوده و تغییر داده شده‌اند. به عنوان مثال یک مورد از آن‌ها بالاتر از یک میلیون بار طبق آمار خود فروشگاه نصب شده است.

یک مثال دیگر Trojan.AndroidOS.Dvmap.a است. این تروجان از سطح دسترسی root برای تزریق کد مخرب در داخل کتاب‌خانه‌های اجرایی سیستم استفاده می‌کند. این مورد نیز در فروشگاه گوگل پلی توزیع شده است و بالاتر از ۵۰ هزار بار دانلود شده است. در عکس ۴ نمونه کد این تروجان نشان داده شده است.

تعداد حملات انجام شده به کاربران با استفاده از بدافزارهای موبایلی سطح هسته در سال ۲۰۱۷ نسبت به سال‌های قبل کاهش داشته است. با این حال این نوع تهدیدات هنوز هم یکی از انواع رایج بدافزارها هستند به طوری‌که نیمی از تروجان‌های ۲۰ بدافزار با بالاترین فراوانی، شامل این مورد هستند که توانایی دسترسی به سطح دسترسی هسته را دارند. کاهش تعداد این نوع بدافزارها در سال اخیر نیز می‌تواند به دلیل کاهش تعداد دستگاه‌هایی است که نسخه‌های قدیمی‌تر اندروید را استفاده می‌کنند که این مجموعه هدف این دسته از بدافزارها است. بنابر داده‌های آزمایشگاه کسپرسکی درصد کاربرانی که از دستگاه‌های اندرویدی نسخه ۵ و ماقبل از آن استفاده می‌کنند از ۸۵ درصد در سال ۲۰۱۶ به ۵۷ درصد در سال ۲۰۱۷ کاهش پیدا کرده‌اند در حالیکه نسبت کاربران اندروید نسخه ۶ به بالا بیش از دو برابر شده‌اند. بطور دقیق‌تر این آمار از ۲۱ درصد در سال ۲۰۱۶ به ۵۰ درصد در سال ۲۰۱۷ رسیده‌اند که ۶ درصد کاربران دستگاه‌های خود را در سال ۲۰۱۶ و ۷ درصد نیز در سال ۲۰۱۷ به‌روزرسانی کرده‌اند. جدیدترین نسخه‌های اندروید هنوز دارای آسیب‌پذیری رایجی که به کاربر اجازه دسترسی Super-user را بدهد که لازمه بدافزارهای سطح هسته هستند، نداشته است. در شکل ۵ خانواده تروجان Ztorg که از طریق فروشگاه گوگل پلی توزیع شده است نشان داده می‌شود.

البته کاهش آمار تعداد این نوع بدافزارها به این معنی نیست که توسعه‌دهندگان به طور کامل از معرض خطر قرارگیری توسط این تروجان راحت شده‌اند. این تروجان به شکل‌های دیگری در دستگاه‌های موبایلی به صورت تبلیغات، دانلودها و مراحل اولیه نصب برخی اپلیکیشن‌ها در حال گسترش است درحالیکه بهره‌برداری از آسیب‌پذیری برای به دست آوردن سطح دسترسی Super-User

هم انجام نگرفته است. علاوه بر این هنوز هم حذف آن‌ها از بخش‌های مختلف سیستم مانند بخش ادمین دستگاه کار پیچیده و سختی است.

در حقیقت در طی سال‌های اخیر مهاجمان تمام سعی خود را برای تغییر و تصحیح قابلیت‌های تروجان خود بر اساس کسب سود و پایداری آن انجام داده‌اند. به عنوان مثال خانواده Ztorg از یک طرح مالی جدید که شامل پیام‌های پرداخت متنی بود استفاده می‌کرد. در این نمونه خاص دو مورد از آن‌ها توسط آزمایشگاه کسپرسکی به عنوان Trojan-SMS.AndroidOS.Ztorg.a شناسایی شد که از گوگل پلی ده‌ها هزار بار دانلود شده بودند. علاوه بر این ماژول‌هایی اضافه در خانواده استاندارد تروجان Ztorg کشف شدند که نه تنها می‌توانستند پیام متنی پرداخت را ارسال کنند بلکه قادر به سرقت پول از حساب کاربر با کلیک در سایت همراه با اشتراک WAP بوده‌اند. برای انجام این کار تروجان از یک فایل JS مخصوص که از یک سرور مجرمانه دانلود می‌شود استفاده می‌کند. در شکل ۶ تروجان Trojan-SMS.AndroidOS.Ztorg.a که در فروشگاه گوگل پلی توزیع شده بود نشان داده شده است.

بازگشت کلیک‌کننده‌های WAP (Wireless Application Protocol)

این دسته نه تنها بدافزارهای سطح هسته را ایجاد می‌کنند بلکه برای پرداخت صورت‌حساب‌های WAP مورد استفاده هستند به شکلی که در سال ۲۰۱۷ تعداد زیادی از تروجان‌های WAP کشف شده‌اند. گرچه این رفتار نشان از دسته جدیدی از تروجان‌ها نیست چون که تروجان Trojan-SMS.AndroidOS.Podec از سال ۲۰۱۵ به این شکل رفتار کرده است اما در سال ۲۰۱۷ آمار نشانگر رشد تعداد کلیک‌های WAP بوده است. در شکل ۷ یک نمونه از این تروجان و در شکل ۸ یک بخش از کد آن نشان داده شده است.

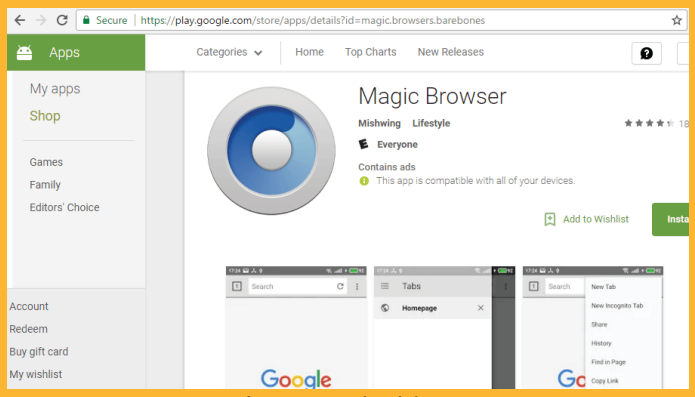
این تروجان به صورت کلی طبق دستورالعملی کار می‌کند به این شکل که لیست‌های زیادی را از سرورهای C&C دریافت کرده و آن‌ها را دنبال کرده و بر روی بخش‌هایی که به صورت اختصاصی فایل JS را ایجاد می‌کنند کلیک خواهد شد. در این موارد بدافزار از صفحات معمول تبلیغات بازدید می‌کند به عنوان مثال آن‌ها به جای سرقت پول کاربر، از سود دریافتی از تبلیغات بهره می‌برند. در موارد دیگر آن‌ها صفحات را با اشتراک WAP که از پول حساب کاربر است بازدید می‌کنند.

یک صفحه با امکان پرداخت WAP به طور معمول به صفحه یک اپراتور موبایلی هدایت می‌شود که کاربر برای پرداخت برای خدمات آن را تایید می‌کند. با این حال آن‌ها تروجان را متوقف نمی‌کنند و قادر به کلیک در این صفحه خواهند بود. همچنین آن‌ها قادر به حذف پیام‌های ارسالی اپراتور موبایلی که شامل اطلاعات پرداخت و هزینه‌های خدمات است، هستند.

توسعه پویای تروجان‌های موبایل بانکی

در سال‌های اخیر موبایل بانک‌ها به شکل گسترده‌ای در حال توسعه هستند که این خود شیوه جدیدی برای سرقت پول است. نمونه‌هایی از موبایل بانک‌های تقلبی کشف شده است که نه تنها به اپلیکیشن مالی حمله کرده است بلکه به اپلیکیشن‌های رزرو تاکسی، هتل‌ها، بلیط و غیره نیز حمله کرده‌اند. رابط کاربری این تروجان به این صورت است که پنجره‌ای با استفاده از فیشینگ باز شده که از کاربر جزئیات اطلاعات بانکی را خواهد پرسید. نکته قابل توجه این است که این اقدامات از دید کاربر کاملا طبیعی و نرمال به نظر می‌رسد و برنامه به صورت هدفمندی طراحی شده تا پرداخت‌ها را انجام داده و ممکن است داده‌هایی را از کاربر دریافت کند. یک نمونه از کد تروجان Trojan-Banker.AndroidOS. Faketoken.q به صورت شکل ۹ است.

آخرین نسخه سیستم‌عامل اندروید شامل تعداد زیادی ابزار است که برای جلوگیری از ورود بدافزارها و اقدامات مخرب طراحی شده‌اند. با این حال، تروجان‌های بانکی به طور مداوم در حال پیدا کردن شیوه‌هایی برای دور زدن این محدودیت‌های جدید هستند که در سال ۲۰۱۷ نمونه‌های متعددی از این موارد مشاهده شده است. در ماه جولای سال ۲۰۱۷ یک تروجان بانکی جدید کشف شد. این تروجان که نام آن AndroidOS.Svpeng.ae است توانایی رساندن خود به بالاترین سطح دسترسی لازم را دارا بود. این تروجان محدودیت‌ها را با استفاده از دسترسی به سرویس‌ها دور می‌زند که این توابع اندروید برای ایجاد اپلیکیشن‌ها بوده است. تروجان از قربانی برای اجازه دسترسی برای استفاده از دسترسی به سرویس‌ها سوال می‌پرسد و مجوزهای دسترسی را به صورت پویا که شامل توانایی ارسال و دریافت sms، برقراری تماس و خواندن لیست مخاطبین بوده است، دریافت می‌کند. این تروجان همچنین خود را به لیست ادمین‌های دستگاه اضافه کرده که منجر به عدم حذف برنامه خواهد شد. به علاوه اینکه داده‌های کاربر که در دستگاه وارد می‌کند را به سرقت می‌برد و همانند یک Keylogger عمل می‌کند. در شکل ۱۰ نشان داده شده است که Svpeng خود را به لیست ادمین‌ها اضافه می‌کند.

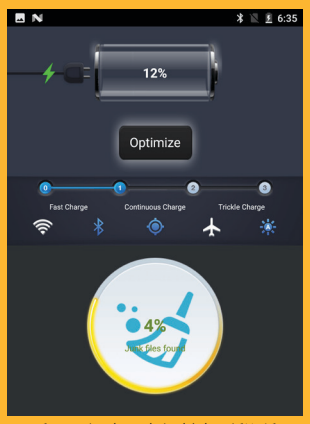


شکل ۶. تروجان Trojan-SMS.AndroidOS.Ztorg.a در فروشگاه گوگل پلی

در ماه آگوست سال ۲۰۱۷، یکی دیگر از بدافزارهایی که از شیوه دسترسی به سرویس خانواده بدافزارهای تلفن همراه Svpeng استفاده می‌کرد شناسایی شد. این دسته با ایجاد تغییر دارای هدف متفاوتی بود که دستگاه موبایل را مسدود کرده و فایل‌های کاربر را رمزنگاری می‌کند و برای بازگردانی فایل‌ها خواستار بیت کوین شده بودند. در شکل ۱۱ باجافزار موبایلی Trojan-Banker.AndroidOS. Svpeng.ag نشان داده شده است.

فراز و نشیب‌های باجافزارهای موبایلی

باجافزارهای موبایلی در شش ماهه اول سال ۲۰۱۷ با نرخ بسیار بالایی دارای رشد بوده‌اند به شکلی که تعداد آن در شش ماه در حدود ۱,۶ برابر کل سال ۲۰۱۶ بوده است. البته از ماه ژوئن ۲۰۱۷ دوباره آمار به حالت نرمال برگشت. جالب توجه این است که این رشد فقط توسط یک خانواده باجافزار انجام گرفت که نام آن Ransom. AndroidOS.Congur است. بالای ۸۳ درصد از باجافزارهای موبایلی نصب شده در سال ۲۰۱۷ مربوط به این خانواده بوده است. اساس کار آن نیز ساده است به این صورت که پین کد مربوط به دستگاه را تغییر داده و یا اعمال کرده و از مالک خواهان ارتباط با مهاجم از طریق پیام رسان QQ بوده است. در شکل ۱۲ باجافزار Trojan-Ransom. AndroidOS.Fusob نشان داده شده است.



شکل ۷. کاربر رابط استانداردی را مشاهده می‌کند درحالیکه تروجان Trojan-Clicker. AndroidOS.Xafekopy در حال سرقت پول می‌باشد.

با بررسی ساختار کد باجافزارهای جدید و شیوه کار آن‌ها می‌توان نتیجه گرفت که در آینده همچنان باجافزارهای موبایلی باقی می‌مانند و قابلیت ساده و موثر

```
var isFindSuccess = false;
FindLP();
function FindLP(){

        var beelineId = new Array("wapSubmitBtn");
        for(var i = 0;i < beelineId.length;i++){
                var value = getDataByTagId(beelineId[i]);
                if(doResult(value,theValue1)){
                        break;
                }
        }

        if (isFindSuccess) {
                return;
        } else {
                androidLog("step beeline1");
        }

        var teleclickClass = new Array("right");
        for(var i = 0;i < teleclickClass.length;i++){
                var value = getDataByTagClassName(teleclickClass[i]);
                if(doResult(value,theValue2)){
                        break;
                }
        }
```

شکل ۸. بخشی از کد مربوط به فایل JS استفاده شده در تروجان Trojan-Clicker.AndroidOS. Xafekopy برای کلیک بر روی دکمه

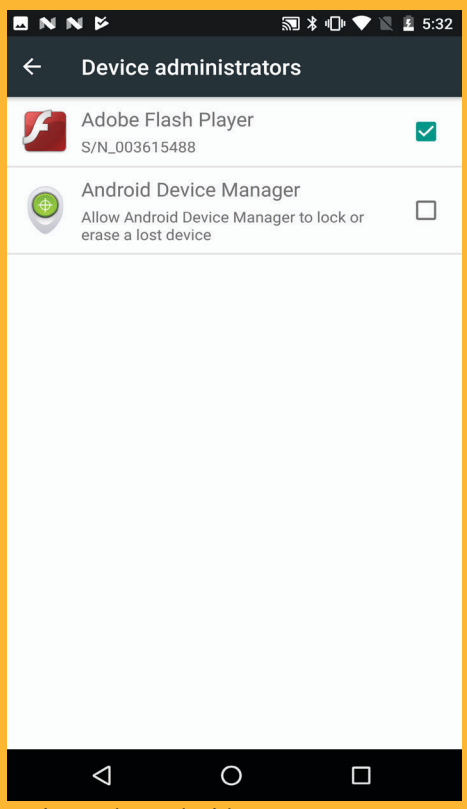
خود را حفظ کرده و شیوه و تکنیک‌های آن‌ها تقریبا بدون تغییر است. به طور مثال در انواع مختلف آن‌ها تمامی صفحه به طور کامل پوشانده می‌شود و فعالیت‌های دستگاه مسدود گشته و قفل می‌شود و یا فایل‌ها رمزنگاری می‌شوند. لازم به ذکر است که دو خانواده باج‌افزارهای موبایلی مطرح به نام Svpeng و Faketokenبا تغییراتی که به وجود آورده‌اند قادر به رمزنگاری فایل‌های کاربر هستند هر چند که قابلیت رمزنگاری فایل‌ها که از انواع عملکرد باج‌افزارها است در میان باج‌افزارهای موبایلی محبوب نیست.

منابع :

securelist.com

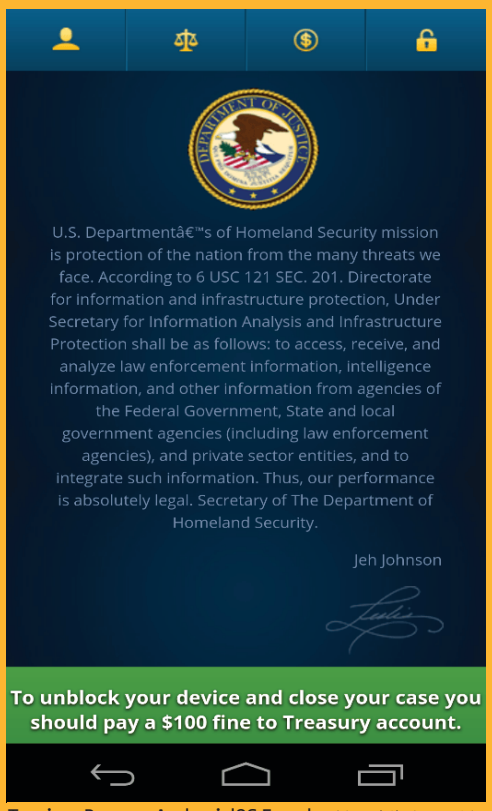
```
if(arg2.contains("ru.sberbankmobile")) {
    this.b();
}
else if(arg2.contains("com.android.vending")) {
    this.c();
}
else if(arg2.contains("com.idamob.tinkoff.android")) {
    this.h();
}
else if(arg2.contains("ru.vtb24.mobilebanking.android")) {
    this.i();
}
else if(arg2.contains("ru.alfabank.mobile.android")) {
    this.j();
}
else if(arg2.contains("ru.raiffeisennews")) {
    this.k();
}
else if(arg2.contains("ru.yandex.taxi")) {
    this.l();
}
else if(arg2.contains("ru.aviasales")) {
    this.m();
}
else if(arg2.contains("com.ubercab")) {
    this.g();
}
else if(arg2.contains("ru.gibdd_pay.app")) {
    this.n();
}
else if(arg2.contains("com.booking")) {
    this.f();
}
else if(arg2.contains("com.gettaxi.android")) {
    this.e();
}
else if(arg2.contains("com.google.android.apps.walletnfcrel")) {
    this.d();
```

شکل ۹. کد مربوط به تروجان Trojan-Banker.AndroidOS.Faketoken.q



شکل ۱۱. باج‌افزار Trojan-Banker.AndroidOS.Svpeng.ag

شکل ۱۰. Svpeng خود را به لیست ادمین دستگاه اضافه می‌کند



شکل ۱۲. باج افزار موبایلی Trojan-Ransom.AndroidOS.Fusob

مروری بر آسیب‌پذیری‌های سیسکو از ۱۹۹۹ تا سال ۲۰۱۸

■ مترجم: فرشته کیاست

در ایـــن گزارش قصـــد داریم آماری از آســـیب‌پذیری‌های مربوط به محصولات سیسکو در سال‌های اخیر ارائه دهیم. طبق نتایج این آمار آســـیب‌پذیری نوع DOS رایجترین نوع آسیب‌پذیری مربوط به محصولات سیسکو می‌باشد.

تعداد آســـیب‌پذیری به تفکیک هر ســـال از سال ۱۹۹۹ تا کنون در شـــکل (۱) نشان داده شده‌است. طبق این نمودار به مرور زمان تعداد آسیب‌پذیری‌های سیسکو افزایش یافته است و این تعداد در ســـال ۲۰۱۷ به ماکزیمم مقدار یعنی ۴۹۱ تعداد آسیب‌پذیری رسیده است.

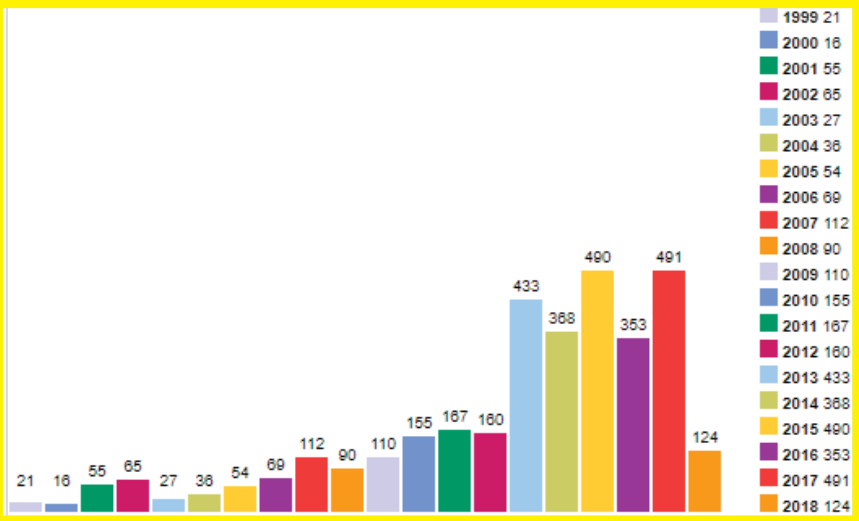
شـــکل (۲) تعداد آســـیب پذیری‌های سیسکو به تفکیک نوع نشـــان داده شده اســـت. این آمار نشـــان می‌دهد که آســـیب‌پذیری مربوط به DOS بیشترین تعداد در سال‌های اخیر را در محصولات سیســـکو داشته است و ۴۷ درصد از کل آسیب‌پذیری ها مربوط به این نوع است.

در دو نمودار زیر (شـــکل های ۳ و ۴) تعداد آسیب‌پذیری از ســـال ۱۹۹۹ تا کنون ارائه شده اســـت. شکل(۳) دو نوع آســـیب پذیری مهم و رایج Execute Code و DOS ارائه شده اســـت. طبق این نمودار آسیب‌پذیریDOS رشد قابل ملاحظه‌ای داشته‌اســـت و با مقایسه با شکل (۴) می بینیم که این نوع آسیب‌پذیری در مقایسه با دیگر آسیب‌پذیری‌ها رشـــد و تعداد بسیار بیشتری داشـــته‌اند. همچنین از سال ۲۰۱۲ این رشد شدت بیشتری یافته است. بنابراین توجه به این آســـیب‌پذیری در سال آتی از اهمیت ویژه ای برخوردار است.

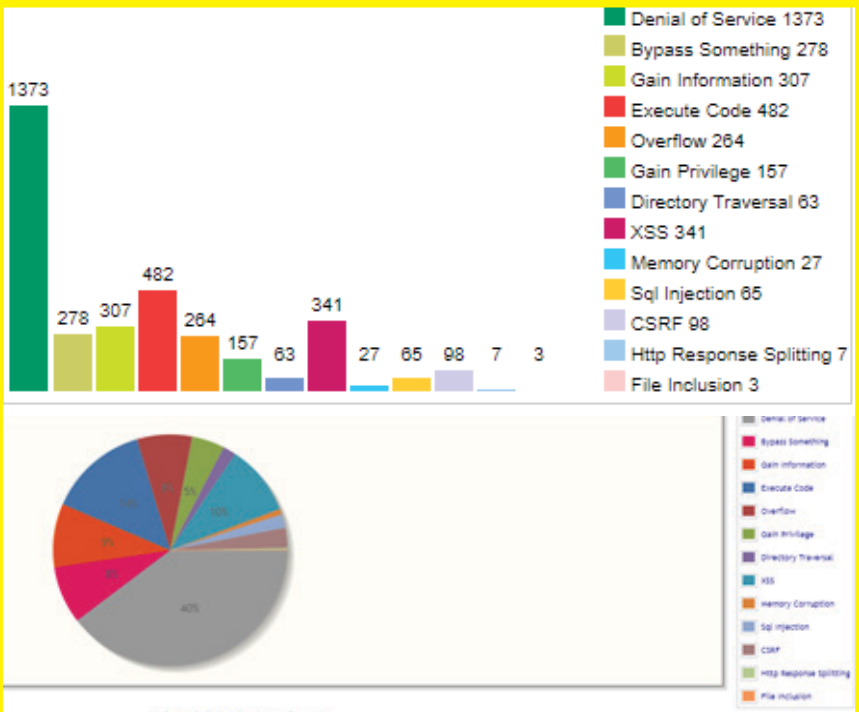
در نمودار شکل ۵ تعداد آسیب‌پذیری ها در سه سال گذشته به تفکیک درجه حساسیت نشان داده شده است. بیشترین تعداد آسیب پذیری ها در پنج سال گذشته مربوط به آسیب پذیری های متوسط و کم می باشد. همچنین آسیب پذیری های خطرناک نیز تعداد کمی ندارد.

در شـــکل‌های (۶ و ۷) تعداد هر ســـطح آسیب‌پذیری را به تفکیک سال و درجه حساسیت مشاهده می‌نمایید. همانطور که مشخص است تعداد آسیب‌پذیری های سطح خطرناک به مرور کاهش یافته است. اما همچنان این آسیب پذیری‌ها موجود هســـتند. در چهار ماه اول سال ۲۰۱۸ ، ۴۸ آسیب پذیری با نرخ بیشتر از ۷ وجود دارند.

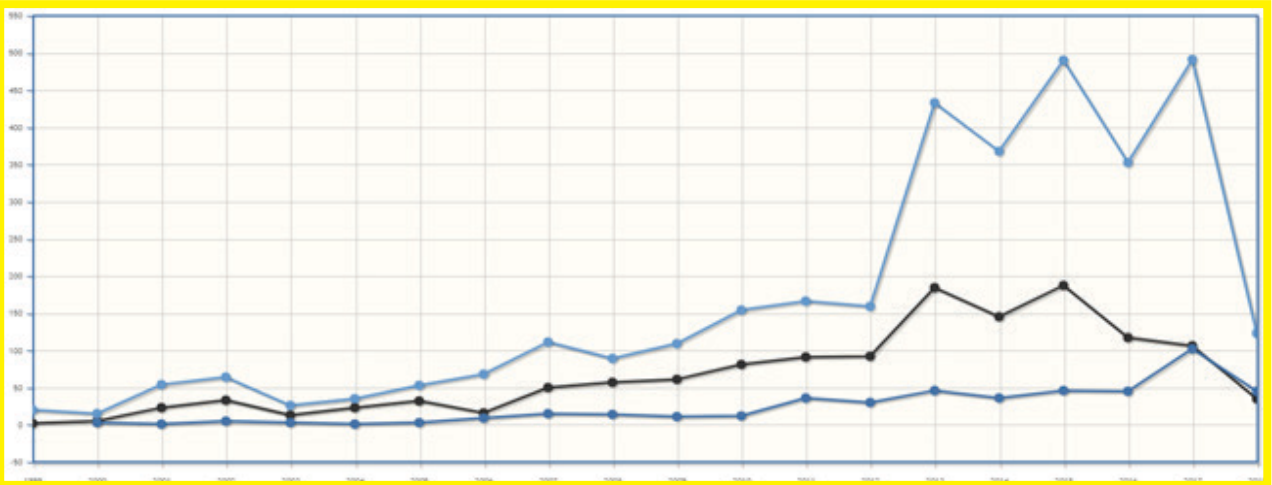
مرجع: www.cvedetails.com



شکل ۱. نمودار تعداد آسیب‌پذیری‌های شرکت سیسکو به تفکیک سال

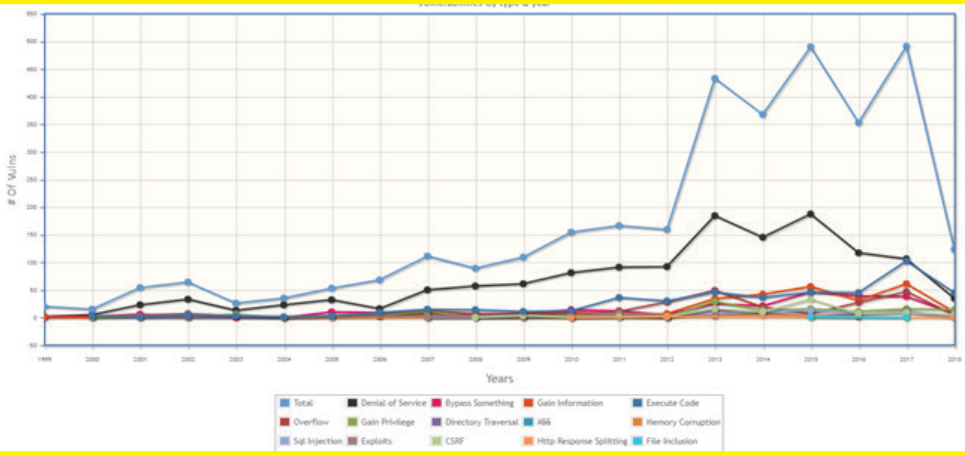


شکل ۲. نمودار تعداد آسیب‌پذیری‌های شرکت سیسکو به تفکیک نوع

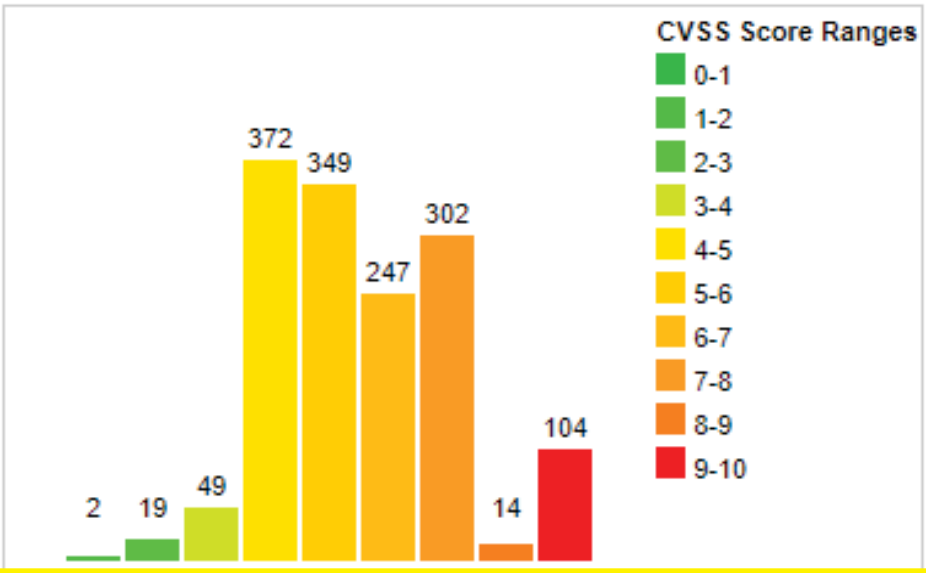


شکل ۳.نمودار تعداد آسیب‌پذیری‌های شرکت سیسکو از سال ۱۹۹۹ تا کنون

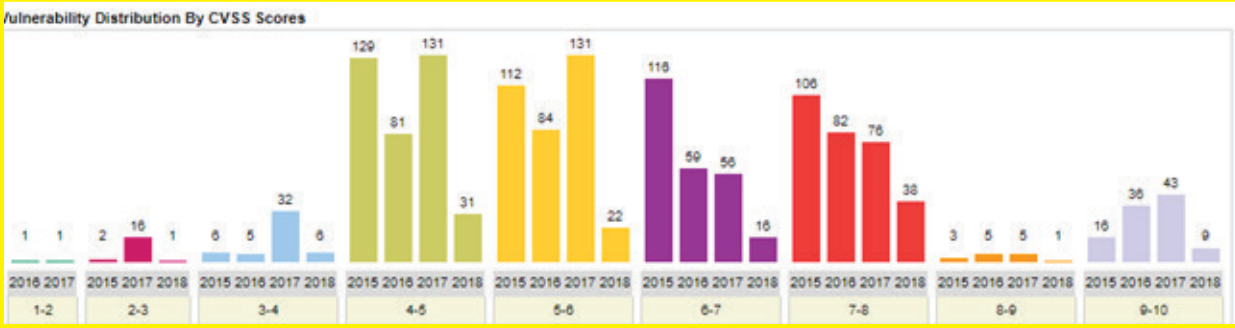
شکل ۴. نمودار تعداد آسیب‌پذیری‌های شرکت سیسکو از سال ۱۹۹۹ تا کنون



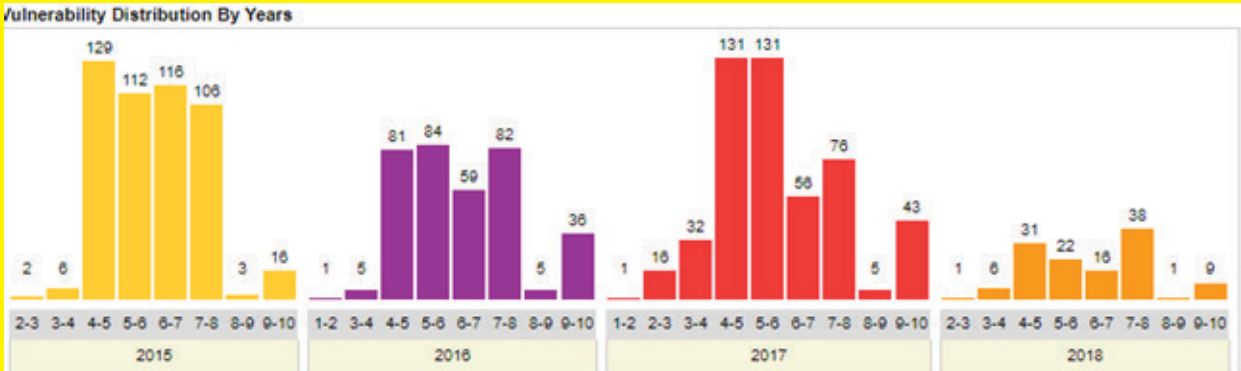
شکل ۵. نمودار تعداد آسیب‌پذیری‌های شرکت سیسکو در سه سال گذشته



شکل ۶. نمودار تعداد آسیب‌پذیری‌های شرکت سیسکو بر اساس درجه حساسیت در سه سال اخیر



شکل ۷. نمودار تعداد آسیب‌پذیری‌های شرکت سیسکو در سه سال اخیر



آسیب پذیری های مهم سیسکو در ماه می ۲۰۱۸

■ مترجم: فرشته کیاست

آسیب‌پذیری دسترسی غیرمجاز در Cisco Digital Network Architecture Center

این آسیب‌پذیری در زیر سیستم مدیریتی کانتینر (container) در مرکز Cisco Digital Network Architecture (DNA) می‌تواند امکان دور زدن احراز هویت و به دست آوردن سطح دسترسی بالاتر را برای مهاجم از راه دور فراهم کند.این آسیب‌پذیری ناشی از پیکربندی پیش‌فرض ناامن زیرسیستم مدیریتی کانتینر Kubernetes در مرکز DNA است. مهاجمی که قابلیت دسترسی به پورت سرویس Kubernetes را داشته باشد می‌تواند دستوراتی با سطح دسترسی بالاتر اجرا کند.سیسکو به روز رسانی های نرم افزاری را که مربوط به این آسیب پذیری است، منتشر کرده است.

محصولات آسیب‌پذیر:

این آسیب‌پذیری بر نرم‌افزار Cisco DNA Center نسخه ۱,۱,۳ و نسخه‌های قبل از آن، تاثیرگذار است.برای مشخص کردن نسخه نرم‌افزار DNA Center می‌توانید با استفاده از مرورگر وب و از طریق پروتکل HTTPS به Cisco DNA Center GUI لاگین کنید. بر روی setting کلیک کرده و گزینه About DNA Center را از منوی کشویی انتخاب کنید. بر روی Show Packages کلیک کنید تا نسخه نرم‌افزار را ببینید.

راه‌حل: در بخش پشتیبانی سایت سیسکو(https://www.cisco.com/c/en/us/support/index.html) آپدیت‌های مربوط به این آسیب‌پذیری دستگاه مورد تهاجم را دانلود نمایید.

Cisco Digital Network Architecture Center Unauthorized Access Vulnerability	بحرانی (Critical)
CVE0268-2018-	شناسه آسیب‌پذیری
Base - 10.0	CVSS Score
1.0 Final	نسخه
CSCvi47253	شناسه باگ‌های سیسکو
دسترسی غیرمجاز (Unauthorized Access)	تاثیر
2018 May 16:00 16 GMT	تاریخ به‌روزرسانی

آسیب‌پذیری منع سرویس در Wireless LAN Controller سیسکو از طریق بارگذاری مجدد IP Fragment

این آسیب‌پذیری در تابع سرهم‌سازی قطعات در IP Version 4 (IPv4) که در نرم افزار کنترل‌کننده شبکه بی‌سیم سیسکو سری‌های ۳۵۰۰، ۵۵۰۰ و ۸۵۰۰ موجود است، می‌تواند امکان راه‌اندازی مجدد دستگاه آسیب دیده را برای مهاجم از راه دور فراهم نماید. این عمل می‌تواند موجب حمله منع سرویس گردد. این آسیب‌پذیری زمانی رخ می‌دهد که نرم افزار ذکر شده برخی از بسته های IPV4 را دوباره بارگذاری نماید. مهاجم می‌تواند با ارسال fragment های ناقص IPV4 از این آسیب‌پذیری سواستفاده کند. این آسیب‌پذیری در نرم‌افزار Wireless LAN Controllers دو نسخه 8.5.103.0 و 8.5.105.0 وجود دارد.

سیسکو به‌روزرسانی‌های نرم‌افزاری را که مربوط به این آسیب پذیری است، منتشر کرده است.

محصولات آسیب‌پذیر:

این آسیب‌پذیری بر روی تمام نسخه‌های ۸,۴ و ماقبل آن برای سری‌های ۵۵۰۰ و ۸۵۰۰ محصول Wireless LAN Controllers و همچنین دو نسخه ۸,۵,۱۰۳,۰ و ۸,۵,۱۰۵,۰ برای سری‌های ۳۵۰۰، ۵۵۰۰ و ۸۵۰۰ محصول Wireless LAN Controller تاثیرگذار است.

برای تشخیص اینکه کدام نسخه Cisco Wireless LAN Controller در یک دستگاه اجرا می‌شود، می‌توان از رابط وب controller یا CLI استفاده کرد. برای استفاده از رابط وب، مراحل زیر را انجام دهید:

۱- با استفاده از مرورگر وارد رابط وب controller شوید.

۲- روی تب Monitor کلیک کنید.

۳- در بخش چپ بر روی Summary کلیلک کنید.

۴- در زیر Controller Summary، نسخه نرم‌افزار که در حال حاضر بر روی دستگاه اجرا می‌شود را نشان می‌دهد.

برای استفاده از CLI از طریق Telnet به controller لاگین کنید، دستور show sysinfo را صادر کرده و سپس در خروجی دستور به مقدار فیلد Product Version مراجعه کنید. مثال زیر نمایشی از خروجی این دستور برای دستگاهی که نرم افزار Cisco WLC نسخه ۸,۳,۱۰۲,۰ است.

```
(wlc)> show sysinfo
Manufacturer's Name..................... Cisco Systems Inc.
Product Name............................ Cisco Controller
Product Version......................... 8.3.102.0
Bootloader Version...................... 1.0.1
Field Recovery Image Version............ 6.0.182.0
Firmware Version........................ FPGA 1.3, Env 1.6, USB console 1.27
Build Type.............................. DATA + WPS
```

برای تعیین اینکه کدام نسخه Cisco Mobility Express Software در یک دستگاه اجرا می شود، می‌توان از رابط وب یا CLI دستگاه استفاده کرد. برای استفاده از رابط وب، مراحل زیر را انجام دهید:

۱- با استفاده از مرورگر، به رابط وب وارد شوید.

۲- گزینه System Software > Software Upgrade را انتخاب کنید.

۳- به مقدار فیلد System Software Version مراجعه کنید.

۴- از طریق Telnet یا نشست SSH به اکسس پوینت لاگین کنید.

۵- دستور show version را صادر کرده و به خروجی آن مراجعه کنید.

مثال زیر نمایشی از خروجی این دستور برای اکسس پوینت Cisco Aironet 1852i که نرم‌افزار Cisco Mobility Express نسخه 8.3.111.0 را اجرا می‌کند، است.

```
AP# show version
cisco AIR-AP1852I-UXK9 ARMv7 Processor rev 0 (v71) with 525160/997184K bytes of memory.
Processor board ID RFDP2BCR021
AP Running Image : 8.3.111.0
Primary Boot Image : 8.3.111.0
Backup Boot Image : 8.1.106.33
AP Image type : MOBILITY EXPRESS IMAGE
AP Configuration : MOBILITY EXPRESS CAPABLE
```

راه‌حل:

در بخش پشتیبانی سایت سیسکو(https://www.cisco.com/c/en/us/support/index.html) آپدیت‌های مربوط به این آسیب‌پذیری دستگاه مورد تهاجم را دانلود نمایید.

Cisco Wireless LAN Controller IP Fragment Reassembly Denial of Service Vulnerability	خطرناک(High)
CVE0252-2018-	شناسه آسیب‌پذیری
Base - 8.6	CVSS Score
1.0	نسخه
CSCvf89222	شناسه باگ‌های سیسکو
آسیب‌پذیری منع سرویس (DOS)	تاثیر
2018 May 16:00 2 GMT	تاریخ انتشار

| جدیدترین بدافزار ها

پنج بدافزار شایع در ماه گذشته

■ نویسنده:هادی گلباغی

۱

نام بدافزار شناسایی شده : W32.Variant:Gen.21gr.1201

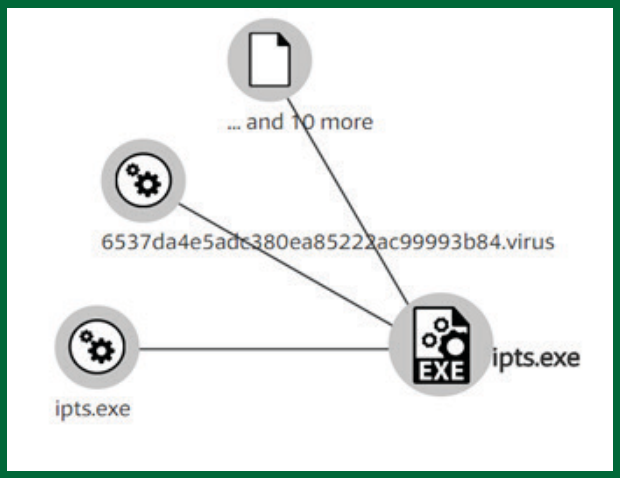
اطلاعاتی مختصر از بدافزار:

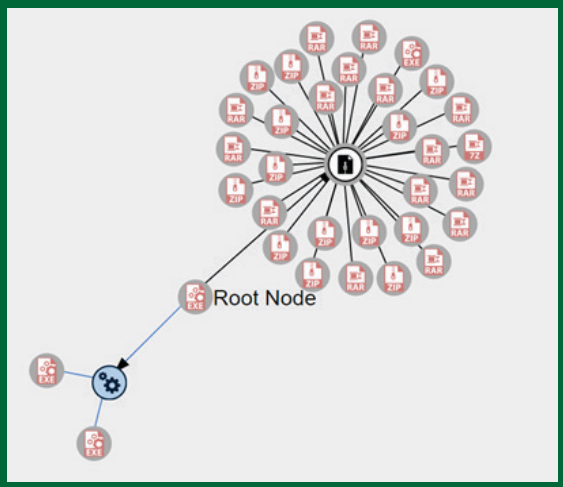
نام فایل	ipts.exe
نوع بدافزار	Trojan
SHA 256	be904d34fdc803c60df5ddde64016e3ab1bd331d 2875b863c6085acc24557394
MD5	15a05c3741d7374cdf8a2dc20c58c3cf
نوع فایل	Win32 EXE
حق نشر	Copyright 2016 Spiritsoft All Rights Reserve
Magic	PE32 executable for MS Windows (GUI) Intel -32 80386bit
TRiD	Win64 Executable (generic) (%72.3) Win32 Executable (generic) (%11.8) OS/2 Executable (generic) (%5.3) Generic Win/DOS Executable (%5.2) DOS Executable Generic (%5.2)
حجم فایل	1.03 MB

آنتی ویروس شناسایی کننده و نام بدافزار در این آنتی ویروس به صورت جدول زیر است.

نام آنتی ویروس	نام بدافزار
BitDefender	Gen:Variant.Johnnie.96313
CAT-QuickHeal	Trojan.IGENERIC
eScan	Gen:Variant.Johnnie.96313
ESET-NOD۳۲	a variant of Win32/FlowSpirit.N potentially unsafe
F-Secure	Gen:Variant.Johnnie.96313
GData	Gen:Variant.Johnnie.96313
Kaspersky	not-a-virus:NetTool.Win32. TrafficExchange.b
McAfee	Artemis!15A05C3741D7
Panda	Trj/GdSda.A
Sophos AV	Generic PUA IE (PUA)
Symantec	Trojan.Gen.2
TrendMicro	TROJ_GEN.R014C0ODF18

گراف ارتباطات مربوط به بدافزار:





۲

نام بدافزار شناسایی شده :

W32.Generic:Gen.21gl.1201

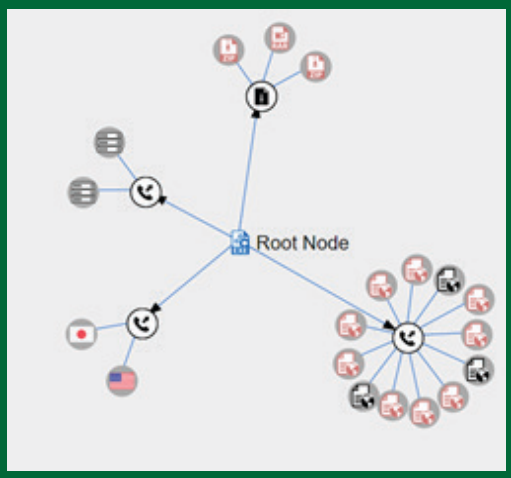
اطلاعاتی مختصر از بدافزار:

نام فایل	mf2016341595.exe
نوع بدافزار	Trojan
SHA 256	15716598f456637a3be3d6c5ac91266142266a9910f6f3f85cfd193ec1d6ed8b
MD5	799b30f47060ca05d80ece53866e01cc
نوع فایل	Win32 EXE
حق نشر	نامشخص
Magic	PE32 executable for MS Windows (GUI) Intel -32 80386bit
TRiD	Win32 Executable MS Visual C++ 5.0 %55.6)) Win32 Executable MS Visual C++ (generic) (%28.6) Win32 Dynamic Link Library (generic) (%6) Win32 Executable (generic) (%4.1) OS/2 Executable (generic) (%1.8)

آنتی ویروس شناسایی کننده و نام بدافزار در این آنتی ویروس به صورت جدول زیر است.

نام آنتی ویروس	نام بدافزار
Avast	Win32:Malware-gen
CAT-QuickHeal	Trojan.IGENERIC
eScan	Trojan.Generic.22412359
ESET-NOD۳۲	a variant of Win32/ FlowSpirit.N potentially unsafe
F-Secure	Trojan.Generic.22412359
GData	Trojan.Generic.22412359
McAfee	RDN/Generic PUP.x
Microsoft	Trojan:Win32/Occamy.C
Panda	Trj/GdSda.A
Sophos AV	Mal/Generic-S
Symantec	Trojan.Gen
TrendMicro	TROJ_GEN.R002C0OED18

گراف ارتباطات مربوط به بدافزار:



۳

نام بدافزار شناسایی شده :

W32.Variant:Gen.21gk.1201

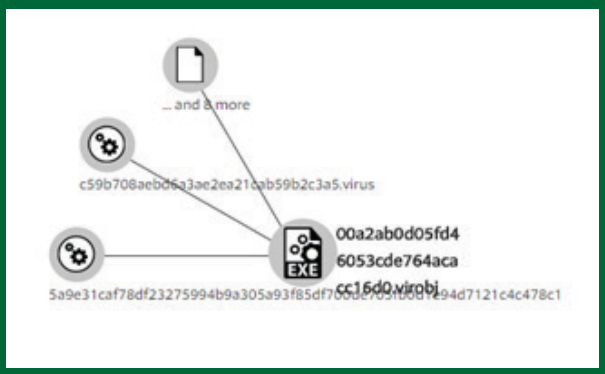
اطلاعاتی مختصر از بدافزار:

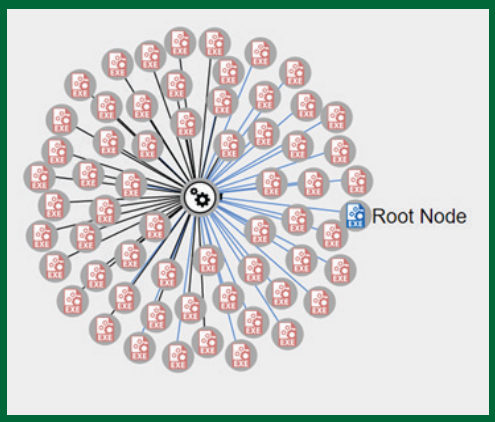
نام فایل	ojec.exe
نوع بدافزار	Trojan
SHA 256	a84a97e3434ec5efcffe3fa230755a9cdf24583c237bee91191d2f97565040cb
MD5	00a2ab0d05fd46053cde764acacc16d0
نوع فایل	Win32 EXE
حق نشر	نامشخص
Magic	PE32 executable for MS Windows (GUI) Intel -32 80386bit
TRiD	UPX compressed Win32 Executable (%42.1) Win32 EXE Yoda's Crypter (%41.4) Win32 Executable (generic) (%7) OS/2 Executable (generic) (%3.1) Generic Win/DOS Executable (%3.1)
حجم فایل	5.17 KB

آنتی ویروس شناسایی کننده و نام بدافزار در این آنتی ویروس به صورت جدول زیر است.

نام آنتی ویروس	نام بدافزار
Avast	Win32:Malware-gen
AVG	Win32:Malware-gen
Avira	TR/Crypt.ULPM.Gen
BitDefender	Gen:Variant.Razy.280645
CAT-QuickHeal	Trojan.IGENERIC
eScan	Gen:Variant.Razy.280645
ESET-NOD۳۲	a variant of Win32/ClipBanker.CI
F-Secure	Gen:Variant.Razy.280645
GData	Gen:Variant.Razy.280645
Kaspersky	UDS:DangerousObject.Multi.Generic
McAfee	Generic.dst
Microsoft	Trojan:Win32/Tiggre!rfn
Panda	Adware/SecurityProtection
Sophos AV	Mal/EncPk-AIQ
Symantec	Trojan.Gen.2
TrendMicro	TROJ_GEN.R03AC0RE118

گراف ارتباطات مربوط به بدافزار:





۴

نام بدافزار شناسایی شده :
PUA.Osx.Dropper.Gt32supportgeeks::in03.talos

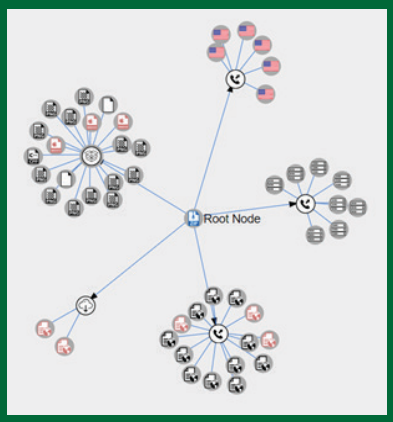
اطلاعاتی مختصر از بدافزار:

نام فایل	helperamc.zip
نوع بدافزار	Trojan
SHA 256	bb5ca947a9ed44d46e2845bdc3eac1bd368577aa40a8dcd1fae29b8da5b0253e
MD5	9ff32613fc850c9937257665ec051e699ff
نوع فایل	ZIP
حق نشر	Advanced Mac Cleaner
Magic	Zip archive data, at least v1.0 to extract
TRiD	Konfabulator widget (%40) Mozilla Firefox browser extension (%40) ZIP compressed archive (%20)
حجم فایل	1.4 MB

آنتی ویروس شناسایی کننده و نام بدافزار در این آنتی ویروس به صورت جدول زیر است.

نام آنتی ویروس	نام بدافزار
Avast	MacOS:AMC-BL [PUP]
AVG	MacOS:AMC-BL [PUP]
Avira	OSX/GT32SupportGeeks.prkjk
BitDefender	Gen:Variant.Application.MAC.AMCleaner.1
ESET-NOD۳۲	a variant of OSX/GT32SupportGeeks.BJ potentially unwanted
F-Secure	Gen:Variant.Application.MAC
GData	Application.MAC.AMCleaner.GH
McAfee	RDN/Generic.osx
Sophos AV	Generic PUA IJ (PUA)
Symantec	OSX.Malcol.2
TrendMicro	TROJ_FR.70214C3D
Microsoft	Trojan:Win32/Tiggre!rfn
Panda	Adware/SecurityProtection
Sophos AV	Mal/EncPk-AIQ
Symantec	Trojan.Gen.2
TrendMicro	TROJ_GEN.R03AC0RE118

گراف ارتباطات مربوط به بدافزار:



۵

نام بدافزار شناسایی شده : W32.AgentWDCR:Gen.21gn.1201

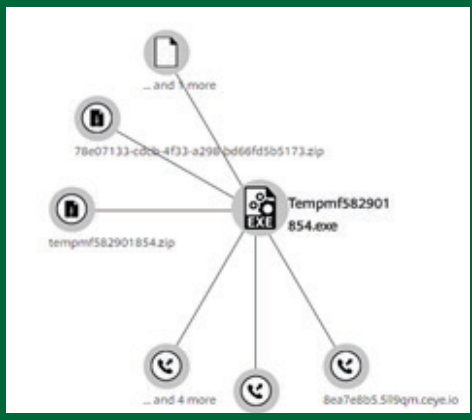
اطلاعاتی مختصر از بدافزار:

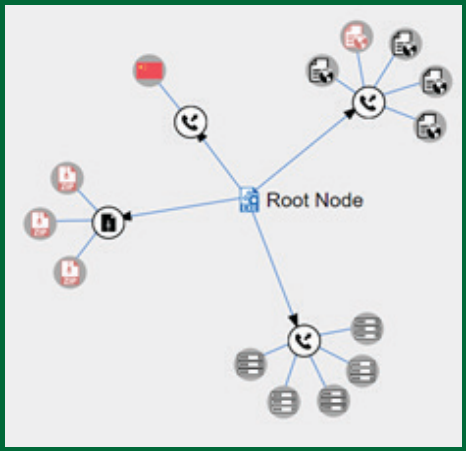
نام فایل	Tempmf582901854.exe
نوع بدافزار	Trojan
SHA 256	c3e530cc005583b47322b6649ddc0dab1b64bcf22b124a492606763c52fb048f
MD5	e2ea315d9a83e7577053f52c974f6a5a
نوع فایل	Win32 EXE
حق نشر	نامشخص
Magic	PE32 executable for MS Windows (GUI) Intel -32 80386bit
TRiD	Win32 Executable MS Visual C++ (generic) (%41) Win64 Executable (generic) (%36.3) Win32 Dynamic Link Library (generic) (%8.6) Win32 Executable (generic) (%5.9) OS/2 Executable (generic) (%2.6)

آنتی ویروس شناسایی کننده و نام بدافزار در این آنتی ویروس به صورت جدول زیر است.

نام آنتی ویروس	نام بدافزار
Avast	Win32:Malware-gen
AVG	Win32:Malware-gen
Avira	TR/Clavior.snnqp
BitDefender	Trojan.AgentWDCR.NEV
CAT-QuickHeal	Trojan.Dynamer
eScan	Trojan.AgentWDCR.NEV
ESET-NOD۳۲	Win32/Agent.YWQ
F-Secure	Trojan.AgentWDCR.NEV
GData	Win32.Trojan.Agent.H9U4K4
Kaspersky	Trojan.Win32.Agentb.izsa
McAfee	RDN/Generic.bfr
Microsoft	Trojan:Win32/Dynamer!ac
Panda	Trj/WLT.D
Sophos AV	Troj/DwnLdr-VMJ
Symantec	Trojan.Gen
TrendMicro	TROJ_DLOADER.JEJOVR

گراف ارتباطات مربوط به بدافزار:





۱۰ بدافزار مخرب در ماه می ۲۰۱۸

■ نویسنده: هادی گلباغی

آمار مربوط به رشـــد بدافزارها در ماه می همانند ماه آوریل روند نزولی را نشـــان می‌دهـــد که کاهش قابل توجه تکثیر بدافزارهای Emotet ادامه داشـــته اســـت و فعالیت Kovter نیز دارای روند کاهشی بوده است که منجر به کاهش ۳۳ درصدی فعالیت ۱۰ بدافزار مخرب در این شده است. این کاهش فعالیت ۱۰ بدافزار مخرب نیز افت ۲۹ درصدی فعالیت کل بدافزارها را به دنبال داشته است. در ماه می ۲۰۱۸ فعالیت ZeuS در آمار کاهش را نشـــان می‌دهد. نمودار مربوط به Malspam همانند روند ماه گذشـــته اســـت به این دلیل که فعالیت‌های Emotet و Kovter دارای کاهش بوده اســـت و روند نزولی در آمار آن مشهود است. در این ماه فعالیتی برای Malvertisement در بین ۱۰ بدافزار با رشد بالا ثبت نشده است اما همچنان این دسته فعالیت‌های بدخواهانه را ادامه می‌دهند.

خانواده‌های مخربی که در این ماه بسیار مطرح بوده‌اند به صورت زیر است :

Dropped : ایـــن بدافزارها از بدافزارهای موجود بر روی سیســـتم و یا از کیت‌های بهره‌برداری، استفاده می‌کنند.

Malvertising : بدافزارهایی که برای تبلیغات مخرب استفاده می‌شوند.

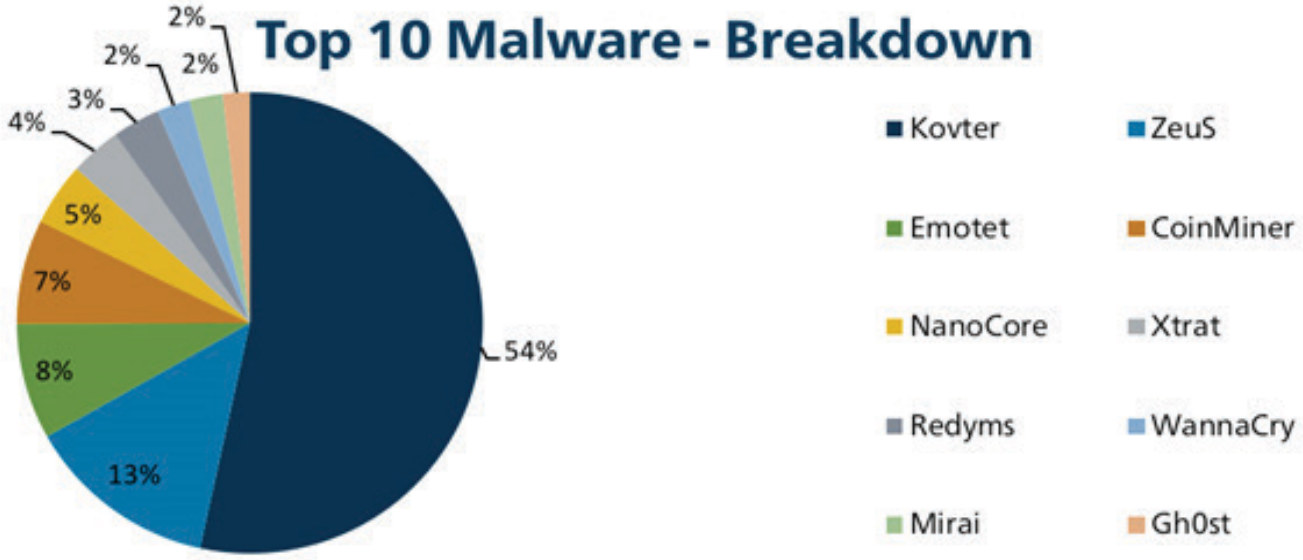
Multiple : بدافزارهایی که در حال حاضر دارای حداقل دو بردار خواهند بود.

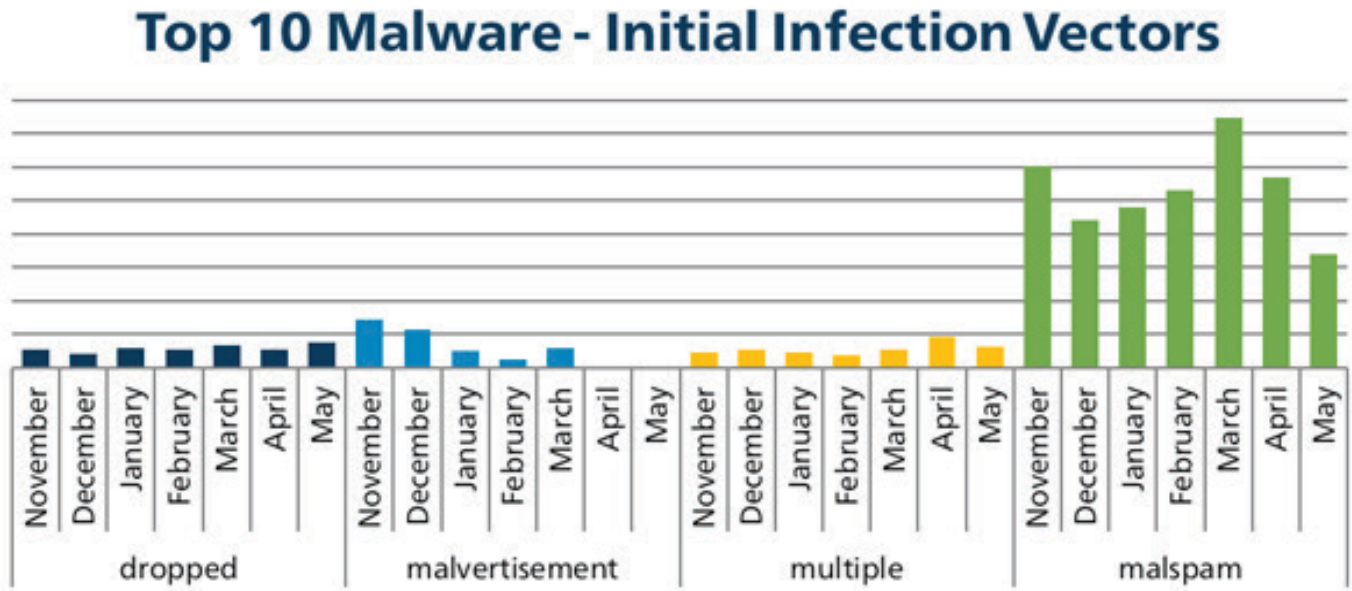
Malspam : ایمیل‌های ناخواســـته که کاربر را ترغیب به دانلود بدافزار از سایت‌های مخرب یا باز کردن پیوست‌های مخرب ایمیل‌ها می‌کند.

۱۰ بدافزاری که بیشترین تخریب را در ماه می سال ۲۰۱۸ داشته‌اند :

۱. Kovter
۲. Zeus
۳. NanoCore
۴. Redyms
۵. Mirai
۶. CoinMiner
۷. WannaCry
۸. Emotet
۹. Ch۰st
۱۰. Latentbot

منبع : cisecurity.org





امنیت عمومی

راهکارهایی برای حفظ امنیت Wi-Fi خانگی

■ نویسنده: هادی گلباغی

یکی از جنبه‌های مهم در زندگی امروزی استفاده مردم در سطحی گسترده از وایفای خانگی است. دیگر باید پذیرفت که تعداد شبکه‌های بی‌سیم به‌سرعت در حال افزایش است. در سال ۲۰۱۰، ۲۰ میلیون شبکه Wi-Fi در سرتاسر جهان وجود داشت، و تنها در ۷ سال این تعداد به ۱۴ برابر افزایش یافته است.

این رشد در همه سیستم‌عامل‌ها و همه دستگاه‌ها بوده است به این صورت که گوشی‌های هوشمند، لپ‌تاپ‌ها و تبلت‌ها نیز این رشد را به همراه داشته است اما به صورت پیش‌فرض امنیت دستگاه‌های بر بستر شبکه‌های بی‌سیم ضعیف است و می‌تواند حتی به مهاجمان بی‌تجربه هم اجازه آسیب به شبکه را بدهد. اگر مجرمان سایبری بتوانند اطلاعات Wi-Fi شما را به دست آورند، تقریباً مهم نیست که رمز عبور شما چقدر قوی است یا اینکه نرم‌افزار شما تا چه حد به روز است. بنابراین باید بررسی کنید که تاکنون چه اقدامات امنیتی را برای امنیت Wi-Fi خانگی خود انجام داده‌اید؟

در زیر مواردی برای به حداکثر رساندن امنیت دستگاه Wi-Fi شما پیشنهاد شده است که می‌توان با رعایت آن‌ها قدم‌های مثبتی به سوی امنیت برداشت.

۱. انتخاب یک نام غیر آشنا و مخفی نمودن نام آن

یکی از اولین اقداماتی که باید انجام داد عبارت است از تغییر نام شبکه Wi-Fi خود، که به‌عنوان SSID شناخته‌شده است و می‌تواند حداکثر شامل ۳۲ کاراکتر باشد. از SSID جهت مشخص نمودن اینکه وایرلس به کدام دستگاه متصل شود استفاده می‌شود. شبکه خانگی خود را به نام یا نام خانوادگی خود تنظیم نکنید؛ مسلماً شما نمی‌خواهید هنگامی که ۳ الی ۴ دستگاه Wi-Fi در همسایگی یکدیگر قرار دارند، آن‌ها در نگاه اول تشخیص دهند که کدام شبکه بی‌سیم متعلق به شما است. یک مسئله بسیار مهم و آسان این است که برای دستگاه مودم بی‌سیم خود یک نام غیر آشنا انتخاب کرده و SSID خود را مخفی کنید.

نکته : مخفی کردن SSID به تنهایی منجر به امن شدن شبکه شما نمی‌شود ولی یکی از قدم‌های مثبت در جهت امن سازی شبکه بی سیم است.

۲. انتخاب یک رمز عبور پیچیده، طولانی و دارای حروف کوچک، بزرگ، اعداد و علائم خاص

همه مهاجمان می‌دانند که دستگاه بی‌سیم شما با یک رمز عبور پیش‌فرض تنظیم می‌شود و به‌راحتی می‌توانند رمز عبور آن را حدس بزنند، به خصوص اگر آن‌ها سازنده را بشناسند. رمز عبور بی‌سیم مطلوب باید حداقل ۸ کاراکتر باشد و شامل اعداد، حروف و نمادهای مختلف باشد. در خصوص انتخاب گذرواژه مناسب در مقاله بعدی همین شماره با جزئیات بیشتری توضیحاتی ارائه شده است.

۳. استفاده از پروتکل امنیتی WPA2 با رمزنگاری AES/PSK

تجهیزات Wi-Fi از قالب‌های مختلف رمزنگاری پشتیبانی می‌کنند. الگوریتم‌های رمزنگاری، پیام‌های ارسال شده در بستر شبکه‌های بی‌سیم را به‌گونه‌ای رمزنگاری می‌کند که به آسانی به صورت متن آشکار در دسترس نباشند. در شبکه‌های بی سیم پروتکل‌های مختلفی برای احراز هویت وجود دارد مانند WEP، WPA یا WPA2

که WEP برای اولین بار در دهه ۱۹۹۰ توسعه یافت، بنابراین با توجه به استانداردهای مدرن، قدیمی و به‌راحتی قابل نفوذ است. WPA بیشتر الگوریتمی موقت بین WEP و WPA۲ بود و هنوز هم به‌عنوان یک زبان رمزگذاری، از آن استفاده می‌شود. WPA2 دارای انواع مختلفی است. یکی از آن‌ها TKIP است که یک روش رمزنگاری بسیار قدیمی است که با WPA توسعه یافت، بنابراین بسیار ایمن نیست. دیگری AES و PSK هستند که یک سیستم رمزگذاری پیشرفته می‌باشند.

بنابراین بهترین تنظیمات رمزنگاری برای افزایش امنیت Wi-Fi شما استفاده از پروتکل WPA2و رمزنگاری PSK یا AES و یا هردوی آن‌ها است.

۴. افزایش امنیت با انتخاب رمز عبور مناسب برای دستگاه بی سیم

برای پیکربندی و تنظیم مودم معمولاً یک صفحه وب وجود دارد که از طریق آن می‌توان وارد تنظیمات دستگاه بی‌سیم شد. بیشتر روترهای Wi-Fi به شکل پیش‌فرض بر روی نام کاربری و گذرواژه admin یا support تنظیم شده‌اند که به این وسیله راه برای ورود مهاجم هموارشده است. تغییر گذرواژه و نام Wi-Fi به‌تنهایی اقدامات امنیتی خوبی هستند ولی در صورت امکان یک گام جلوتر بروید و نام کاربری را هم از نام پیش‌فرض تغییر دهید.

۵. غیرفعال کردن دسترسی و کنترل از راه دور

در بیشتر مودم‌ها اجازه دسترسی به Wi-Fi فقط از طریق دستگاه‌های متصل وجود دارد با این حال، برخی از آن‌ها اجازه دسترسی از راه دور را نیز می‌دهند. هنگامی که گزینه دسترسی از راه دور را غیرفعال کنید، مجرمان سایبری قادر به دسترسی به دستگاه بی‌سیم شما، با دستگاهی که به شبکه بی‌سیم وصل نباشد، نیستند. امکان پیکربندی از طریق WAN را در مودم خود غیرفعال کنید.

۶. به‌روزرسانی Firmware دستگاه مودم

همواره یکی از چالش‌های امنیتی عدم به‌روزرسانی نرم‌افزار و سیستم‌عامل‌ها است. نرم‌افزار، بخش مهمی از امنیت شبکه بی‌سیم شماست. سیستم‌عامل دستگاه بی سیم، مانند هر نرم‌افزار دیگری، نقایصی دارد که می‌تواند آسیب‌پذیری‌های عمده‌ای داشته باشد و توسط مهاجم مورد سوءاستفاده قرار گیرند. متأسفانه، بسیاری از دستگاه‌های بی سیم گزینه‌ای برای به‌روزرسانی خودکار نرم‌افزار ندارند، بنابراین شما باید به‌روزرسانی را به‌صورت دستی انجام دهید. حتی سایر دستگاه‌های بی سیم هم که می‌توانند به‌صورت خودکار آپدیت شوند، گاهی نیاز به تنظیم مجدد دارند.

۷.غیر فعال کردن WPS بر روی دستگاه بی سیم

WPS مخفف Wireless Protection Setup است و استانداردی برای برقرار کردن شبکه‌های بی سیم خانگی به شکلی امن و آسان است. هدف این استاندارد تسهیل روند پیکربندی امنیتی شبکه‌های بی سیم می‌باشد و به همین دلیل است که قبلاً Wi-Fi Simple Config نامیده می‌شد. این پروتکل به منظور میسر کردن امنیت برای کاربرانی طراحی شده که اطلاعات کمی در مورد امنیت شبکه‌های بی سیم دارند. اما WPS دارای آسیب‌پذیری است که به راحتی توسط مهاجم مورد بهره‌برداری قرار گیرد به همین دلیل در پیکربندی مودم باید آن را غیر فعال نمایید.

۸. فعال کردن قابلیت MAC Filtering بر روی دستگاه مودم

MAC Address یک شناسه سخت‌افزاری است که برای هر دستگاه داخل شبکه در دنیا منحصر به فرد می‌باشد. یکی دیگر از راه‌کارهای مفید استفاده از سیستم MAC Filtering است تا بتوان سدی را در مقابل MAC address های غریبه ایجاد کرد و در صورت لزوم به MAC addressهایی اجازه دسترسی داده و یا به MAC addressهای خاصی اجازه دسترسی را نداد.

انتخاب یک رمز عبور مناسب

■ نویسنده: محمد حبیبی

استفاده از رمز عبور ضعیف یک مشکل جدی است. که ممکن است حتی امنیت یک سیستم بدون آسیب‌پذیری را به خطر بیاندازد. برای انتخاب یک گذر واژه مناسب نیاز است موارد زیر بررسی شود :

۱-از رمزهای ضعیفی مثل ۱۲۳۴۵۶ یا خود کلمه password استفاده نکنید.

۲-از بکارگیری یک رمز برای چند حساب کاربری پرهیز کنید.

بهتر است برای هر یک از حساب های خود یک رمز جداگانه استفاده کنید.

۳-از بکارگیری یک قالب تکراری در رمز عبور پرهیز کنید.

۴-اگر نگران فراموش کردن رمز عبور هستید، می توانید از یک نرم افزار مدیریت پسورد استفاده کنید.

۵-از کلمات عبور مانند تاریخ تولد، اعضای خوانواده، شماره موبایل یا موارد مشابه که قابل حدس باشد و به هیچ عنوان استفاده نکنید.

۶-از کلمات عبور یکسان برای وب سایت های مختلف یا ایمیل آدرس‌های مختلف استفاده نکنید. تا حد ممکن سعی شود برای هر حساب کاربری از یک پسورد کتفاوت استفاده شود.

۷-کلمات عبور را حداقل ۱۰ کاراکتری انتخاب کنید ، هر چه تعداد کاراکتر ها بیشتر باشد امکان شکستن آن کمتر است.

۸-کلمات عبور را به صورت ترکیبی از اعداد , علائم و حروف الفبای کوچک و بزرگ انتخاب کنید به عنوان مثال 100~wD&GRWs کلمه عبور مناسبی می باشد.

۹-کلمات عبور را در فایل های غیر قابل دسترس و محو شده نگهداری کنید و به هیچ عنوان در دسترس اشخاص دیگر نباشد.

۱۰- به طور مرتب چند هفته یک بار کلمه عبور خود را تغییر دهید و با کلمه عبور قدرتمند دیگری جایگزین کنید.

۱۱-در صورتی که کلمه عبور خود را برای رفع مشکلاتی به مدیر فنی سایت یا مدیریت هاست یا غیره اعلام کردید پس از اتمام کار حتماً کلمه عبور را تغییر دهید.

۱۲-از تست کلمات عبور خود در وب سایت‌ها یا اپلیکیشن‌هایی که میزان قدرت یک کلمه عبور را از نظر پیچیدگی محاسبه میکنند پرهیز کنید. در صورت تمایل به استفاده از این وب سایت‌ها از کلمات دیگر و غیر مشابه به الگوی کلمه عبور خود استفاده کنید.

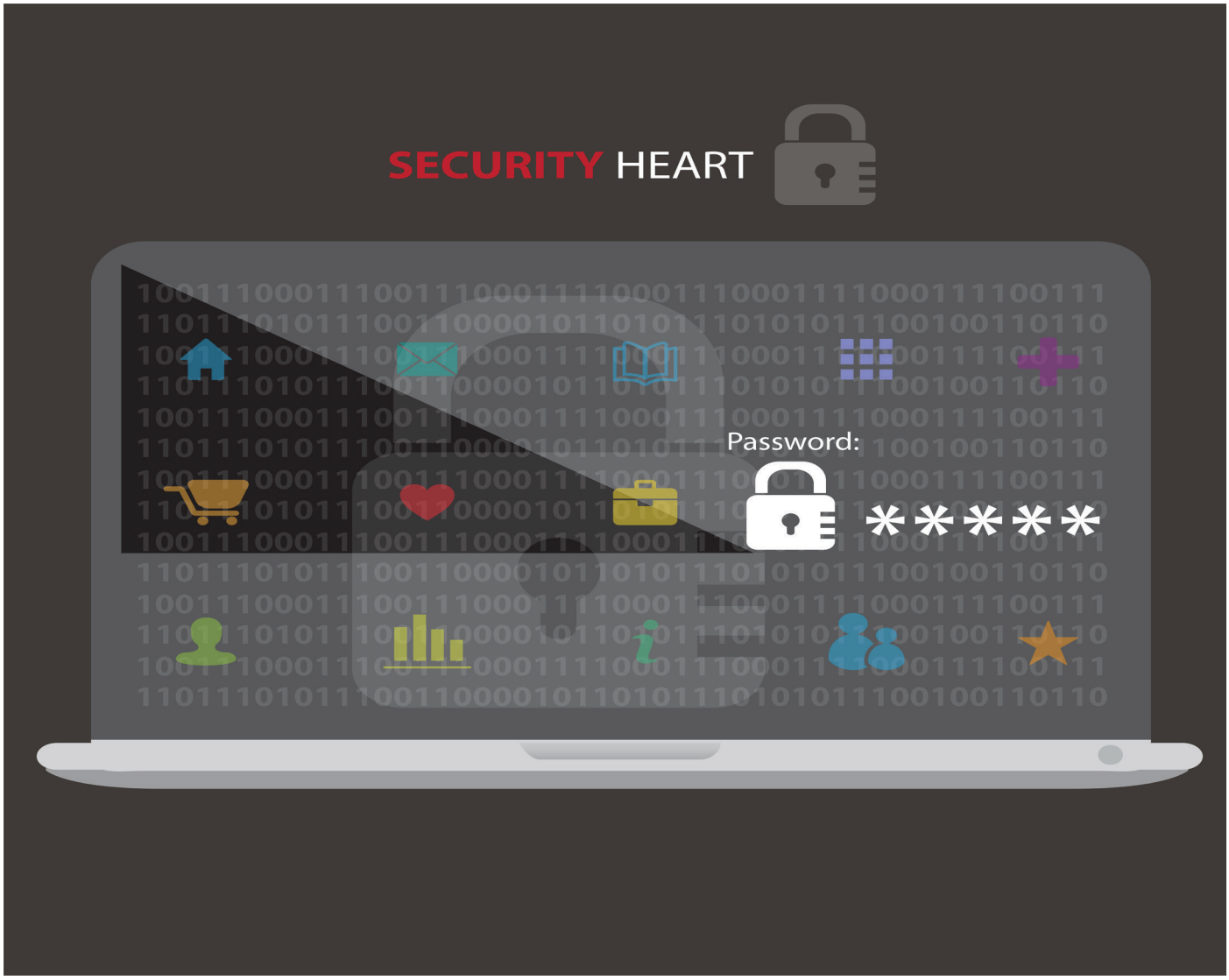
۱۳-به هیچ وجه از پسورد دیگران استفاده نکنید.

۱۴-از طریق لینک‌ها و یا فرم‌هایی که ممکن است با یک ایمیل به دست شما برسد به حساب‌های کاربری و بانکی خود وارد نشوید. فقط از طریق سایت مربوطه و معتبر نام کاربری و رمز عبور خود را وارد کنید.

۱۵-اگر در یک وب‌سایت از یک سوال امنیتی برای بازیابی کلمه عبور استفاده شده است، سعی کنید جواب سوال امنیتی برای دیگران غیرقابل حدس و مبهم باشد.

۱۶-اگر در یک وبسایت از یک ایمیل و یا شماره موبایل برای بازیابی کلمه عبور استفاده کرده‌اید مطمئن شوید شخص دیگری به این ایمیل/شماره دسترسی ندارد.

۱۷-سعی کنید در صورت امکان تایید دو مرحله‌ای را برای ورود به حساب‌های کاربری خود فعال کنید.



KURD CERT

مرکز آپا دانشگاه کردستان