Full Security

http://mag.fullsecurity.org
mag@FullSecurity.org

شماره ۱ بهمن ۱۳۹٤

حمله هکرهای فلسطینی به اف‌بی‌آی

وزارت دادگستری آمریکا می‌گوید در حال تحقیق درباره انتشار اطلاعات تماس ۲۰ هزار کارمند اف‌بی‌آی توسط هکرهای اینترنتی است که رسوایی بزرگی به بار آورده است

✓ در این شماره از نشریه مطالب زیر را می خوانیم:

سرمقاله

به نام یزدان پاک

امام صادق علیه السلام : برای هر چیزی زکاتی است و زکات علم آن است که آن را به اشخاص شایسته بیاموزند.

پیرامون زندگی هر انسانی امروزه کامپیوترهای شخصی و سیستم های متعدد؛ تلفن ثابت و همراه ،کامپیوترهای کیفی، خود پرداز بانکها، دستگاههای کنترل از راه دور، سیستم های ماهواره ای، تلویزیون و دهها ابزار دیگر تلنبار شده است.

شبکه عظیم اینترنت و پیشرفت های علوم اینترنت و گسترش گرایش زندگی به دنیای مجازی باعث تغییر شیوه زندگی انسان به الگوهای مدرن شده است. همین عوامل باعث شده بزهکاری های اجتماعی و ناهنجاریهای مدنی رنگ و بوی مدرنیته به خود بگیرد. دنیای امنیت آکنده از جرم های مختلف و هر روز نیز با تکنیک های جدید کاربران را تهدید می کند و اطلاعات شخصی آنها را با خطر مواجه می سازد.در سالهای اخیر با پیشرفت روزافزون سیستم های عامل علی الخصوص سیستم های عامل تلفن همراه مانند اندروید و IOS و نرم افزارهای متنوع آنها خطر کلاهبرداری، سرقت اطلاعات شخصی و جرایم دیگر این حوزه بیش از پیش احساس می شود.

خرسندیم که با عنایت به خداوند منان و با بهره گیری از دانش روز دنیای امنیت اطلاعات و گردآوری تیم مجرب و کارازموده ای از جوانان پر استعداد این مرز و بوم با تهیه نشریه ای تحت عنوان فول سکوریتی گامی در جهت آشنایی بیشتر و ارتقای امنیت کاربران عزیز کشورمان برداریم.

این نشریه در زمینه ی امنیت اطلاعات،نفوذ و پژوهش های روز این رشته فعالیت مینماید و هدف از این مهم گرداوری اطلاعات به روز و با ارزش برای رشد و ترقی جوانان جویای دانش در این رشته است. باشد تا با توکل بر خدای بزرگ به این مهم دست یابیم.

گروه مدیریت نشریه تخصصی امنیت اطلاعات فول سکوریتی

26 بهمن 1394

انتشار اطلاعات 20 هزار کارمند FBI توسط نفوذگران فلسطینی

وزارت دادگستری آمریکا خبر داده است که در حال تحقیق درباره انتشار اطلاعات تماس 20 هزار کارمند اف بی‌آی توسط هکرهای اینترنتی می باشد که رسوایی بزرگی به بار آورده است. به گزارش نشریه فناوری اطلاعات فول سکوریتی به نقل ازCNN ، تنها چند روز قبل اطلاعات تماس 10 هزار کارمند وزارت امنیت داخلی آمریکا در فضای مجازی منتشر شد و حال اطلاعات 20 هزار کارمند اف بی ای در اینترنت در دسترس همگان قرار گرفته است.

نفوذگران که از یک حساب کاربری در توییتر موسوم به DotGovs برای اطلاع رسانی در مورد فعالیت های خود استفاده می کنند، مدعی شده اند که داده های مذکور را با نفوذ به پایگاه داده وزارت دادگستری آمریکا به دست آورده اند. اطلاعات هک شده شامل اسامی کارمندان، عنوان شغلی، شماره همراه و آدرس های پست الکترونیک آنان است پس ازآنکه هکرها داده های مذکور را منتشر کردند، در حساب توییتری خود این مطلب را به اشتراک عموم قرار دادند:

« خب دوستان، به نظر می رسد وزارت دادگستری آمریکا بالاخره بعد از یک هفته فهمید که رایانه هایش هک شده اند. این وزارتخانه در واکنشی اعلام کرده که در حال بررسی موضوع است و به نظر نمی رسد هنوز اطلاعات حساسی افشا شده باشند. »

هکرهای یاد شده که از هشتگ فلسطین را آزاد کنید استفاده می کنند در پیامی افزوده اند: دولت آمریکا چه زمانی خواهد فهمید که ما تا زمانی که انها روابطشان با اسرائیل را قطع نکنند متوقف نخواهیم شد.

ورژن 2016.1 از Kali Linux رو نمایی شد!

با آغاز شدن سال 2016 میلادی تیم توسعه Kali Linux نسخه جدید و آپدیت شده سیستم عامل کالی لینوکس را بر روی سایت خود قرار دادند که مشکلات نسخه قبلی این سیستم عامل بر طرف شده است و علاقه مندان به کالی لینوکس میتواند نسخه جدید این سیستم عامل را دانلود کنند.

در تاریخ 21 ژوئن سال 2016 میلاد کمپانی Offensive Security توزیع کننده ی سیستم عامل های کالی و بک ترک بالاخره ورژن جدید این سیستم عامل را عرضه کرد. کالی 2016 با ورژن 2016.1 جدید ترین و بروز ترین ابزار های امنیتی را به همرا دارد ! عمده ترین ویژگی این توزیع Rolling base بودن آن می باشد ! ابتدا اجازه دهید تا مختصرا راجع به توزیع های Rolling بیشتر توضیح دهیم :

-توزیع های Rolling لینوکس :

این نوع توزیع های لینوکسی از توزیعاتی هستند که مدام بروز می شوند؛ تقریبا چیزی شبیه به Developers version

از توزیع هایی که از این سیستم استفاده می کنند، می توان به Arch Linux اشاره کرد که یکی از معروفترین و محبوب ترین توزیع های لینوکسی می باشد . خلاصه کلام اینکه این توزیع ها جدیدترین ابزار های خودشان را در معرض کار می گذارند.

کالی ورژن 2016.1 از سیستم رولینگ استفاده می کند که مدام آپدیت های کوچک و بزرگی را ارائه می دهد که رفع باگ یا آپدیت ابزار های امنیتی می شود.

- یکی دیگر از تغییرات مهم این ورژن استفاده از Open VM Tools به جای VMware tools قدیمی است . این پکیج جدید که توسط شرکت VM ارائه شده است تجربه ی بهتری را در اجرای سیستم عامل ها به صورت مجازی ارایه می دهد که در این نسخه از کالی کاملا درست و بی نقص کار می کند .

- استفاده از کرنل جدید نسخه ی 4.3.0.0 که یکی از جدیدترین کرنل های استیبل موجود است که در کارهای اساسی به خوبی خودش را نشان می دهد . این کرنل بهینه تر از کرنل های پیشین می باشد و بسیاری از باگ های آن رفع شده است !

- استفاده از آخرین نسخه های نرم افزار های موجود در کالی ویژگی معمول این توزیع است .

❖ برای ارتقاء Kali Linux 2.0 (Sana) به Kali Linux Rolling Eddition مراحل زیر را طی کنید:

1- ابتدا به دایرکتوری ect/apt/ رفته و فایل source.list را باز و خط کد زیر را در یک خط جدید در انتهای خط کدها اضافه و فایل را ذخیره کنید:

deb http://http.kali.org/kali kali-rolling main non-free contrib

2- حال در ترمینال خود دستورات زیر را اجرا کنید:

apt-get update

apt-get dist-upgrade

3- در انتها نیز با دستور reboot سیستم عامل کالی لینوکس را مجدداً راه اندازی کنید.

استفاده از HTML Source Code در فوت پرینتینگ

در بیشتر مواقع نفوذگر میتواند با خواندن HTML Source Code صفحات یک سایت اطلاعات خوبی در خصوص وب سایت مورد نظر بدست بیاورید. اطلاعاتی همچون سیستم مدیریت محتوا مورد استفاده بر روی سایت ، زبان برنامه نویسی مدیریت محتوا و اطلاعات کاربردی دیگر با خواندن سورس صفحه HTML Source Code قابل جمع آوری میباشد.

یکی از مهمترین اطلاعاتی که در این Source Codeها می توانید بدست بیاورید اطلاعاتی هستند که در قسمت توضیحات درباره مدیریت محتوا نوشته شده اند و آنها را میتوان مورد استفاده قرار داد. این توضیحات هم می توانند بصورت دستی و هم بصورت خودکار توسط سیستم مدیریت محتوا استفاده شوند و بیشتر مدیران سایت ها که از این مدیریت محتوا ها استفاده می کنند چندان توجهی به اطلاعات نوشته شده در مورد مدیریت محتوا نمی کنند که برای یک هکر می تواند بسیار مفید باشد. شما با استفاده از این اطلاعات می توانید متوجه شوید که در پشت صحنه چه اتفاقی در حال رخ دادن است. در بیشتر موارد می توانید در سورس صفحه اطلاعات مهمی همچون شماره تماس یا اطلاعات تماس مدیر یا برنامه نویس وب سایت را پیدا کنید.

همچنین به طور مثال در سیستم مدیریت محتوا وردپرس میتوان با خواندن سورس صفحه اطلاعاتی همچون ورژن نسخه از مدیریت محتوا وردپرس نام پوسته و اطلاعات مهمی همچون پلاگین های نصب شده را بدست آورد که برای نفوذ به یک وب سایت مهم ترین نکته پیدا کردن اطلاعات مهمی همچون نسخه استفاده شده و موارد دیگر میباشد.

همچنین استفاده از این روش به شما امکان پیدا کردن دایرکتوری ها و فایل های مخفی را در سیستم می دهد. علاوه بر این در بعضی قسمت ها شما می توانید یک سری اطلاعات نادرست را به صورت تصادفی وارد کنید و عکس العمل اسکریپت ها در مقابل این داده های اشتباه را تحلیل کنید.

کشف حفره های امنیتی با اسکنر قدرتمند RIPS

در دنیای هک و امنیت همواره اپلیکیشن های مختلفی وجود دارد که با اسکن سایت یا سیستم مدیریت محتوا اقدام به کشف حفره های امنیتی و اسیب پذیری های یک سیستم مدیریت محتوا می کنند که یکی از محبوب ترین این ابزارهای امنیتی، اسکنر Acunetix Web Vullnerability Scanner می باشد که این اسکنر با دریافت آدرس سایت از سوی کاربر اقدام به کشف و شناسایی حفره های موجود در مدیریت سایت مورد نظر می کند.

اما این روزها با کانفیگ مناسب سرورها ابزار هایی امنیتی همانند Acunetix Web Vullnerability Scanner در مواردی متعددی نمی تواند اقدام به اسکن یا شناسایی آسیب پذیری ها کنند. علت این ضعف نیز تعداد درخواست های ارسالی به سمت سرور می باشد که باعث می شود سرور تشخیص دهد IP مورد نظر اقدام به حملات تکذیب سرور می کند و IP را بلاک می کند که در این شرایط اسکنرهای امنیتی نمی توانند به درستی اقدام به بررسی سیستم مدیریت محتوا جهت شناسایی آسیب پذیری ها کنند.

در اینجا میخواهیم یک اسکریپت به نام RIPS که قبلا عرضه شده است را به شما معرفی کنیم.

با نصب این اسکریپت کوچک اما کاربردی این امکان را خواهیم داشت که سورس فایل های سیستم های مدیریت محتوا را در این اسکریپت مورد بررسی قرار دهیم تا حفره های امنیتی موجود را تشخیص داده و نشان دهد سورس فایل ضعف امنیتی دارد یا خیر.

این اسکریپت قابلیت شناسایی اسیب پذیری ها و حفره های امنیتی زیر را در خود دارد:

Code Execution

Command Execution

Cross-Site Scripting

Header Injection

File Disclosure

File Inclusion

File Manipulation

LDAP Injection

SQL Injection

Unserialize with POP

XPath Injection

همچنین قابلیت های کلی RIPS به شرح زیر می باشد:

1-بررسی و ارائه ی آمار آسیب پذیری ها

2-گروه بندی کردن آسیب پذیری ها

3-توضیحاتی در رابطه با هر آسیب پذیری و روش نفوذ با استفاده از این آسیب پذیری

4-ساخت اکسپلویت برای هر آسیب پذیری

5-آمار فایل ها

6-لیست توابع

7-نمایش سورس کد و آدرس فایل بررسی شده

8-جست و جو در میان کدها

9-لیست ورودی ها

10-شناسایی بک دور در اسکریپت

و چندیدن قابلیت دیگر که همه از قابلیت های کلی اسکنر امنیتی RIPS می باشد.

جهت دانلود این اسکریپت می توانید از وب سایت SourceForge استفاده کنید

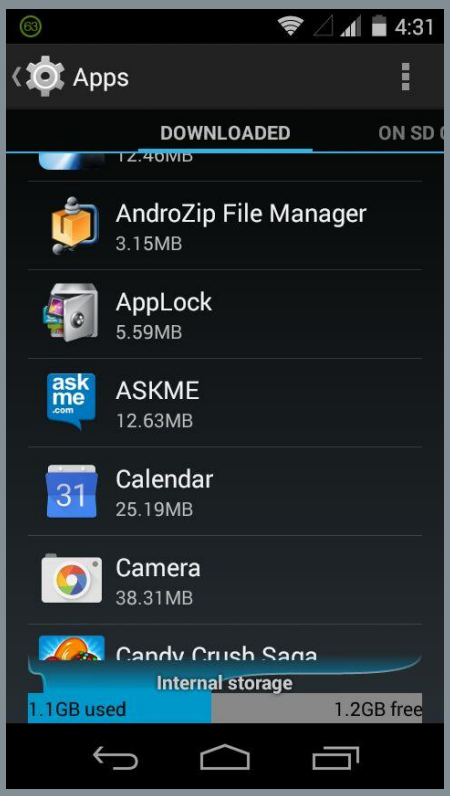
آموزش دورزدن (Bypass) ابزار AppLock در اندروید

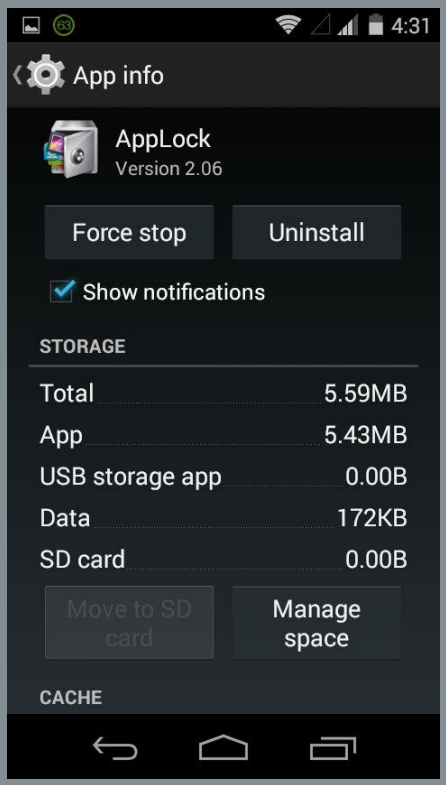
برنامه امنیتی AppLock که برای گوشی های اندروید Android نسخه 2.2 و بالاتر می باشد. با استفاده از این اپلیکیشن می توانیم بر روی برنامه های نصب شده از جمله پیامک و تماس و گالری و ایمیل و سایر برنامه ها پسورد قرار دهیم. اما در مواردی پسورد این اپلیکیشن را فراموش میکنیم و یا مواردی مشابه که در این مواقع به برنامه یا روشی برای حذف این قفل امنیتی احتیاج پیدا می کنیم.

با استفاده از این آموزش میتوان این اپلیکیشن را دور زد و بدون داشتن پسورد اقدام به باز کردن نرم افزار هایی که با استفاده از این برنامه ایمن گردیده اند نمود. در چند روش میتوان اپلیکیشن Applock را در اندروید دور زد:

1- روش اول حذف نرم افزار به صورت کامل میباشد البته این روش در صورتی امکان پذیر میباشد که برای حذف یا نصب اپلیکیشن با استفاده از Applock قفل گزاری نشده باشد.

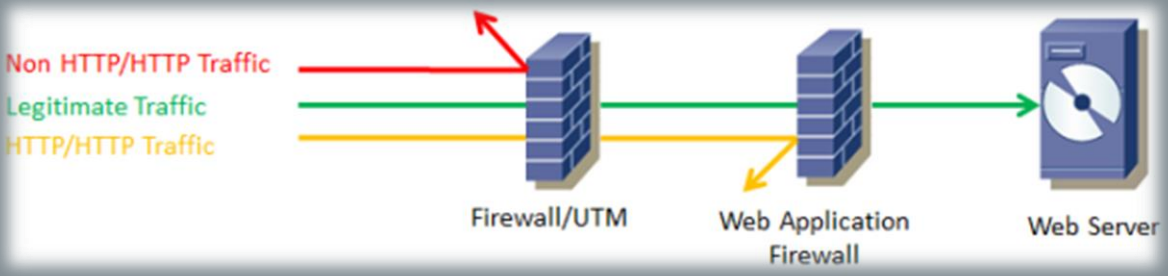
2- روش دوم که 100٪ تضمینی است، غیر فعال کردن Applock میباشد. برای این کار کافی است به Settings گوشی رفته قسمت Apps سپس Manage Applications و از قسمت اپلیکیشن های در حال اجرا بر روی Applock کلیک کنید و سپس اپلیکیشن Applock را Force Stop کنید.





با عمل Force Stop اپلیکیشن غیرفعال خواهد شد و تا زمانی که مجدد Applock اجرا نشود میتوان با خیال راحت اقدام به اجرای اپلیکیشن های محافظت شده توسط Applock نمود.

آشنایی با Web Application Firewall WAF



افرادی در سراسر دنیا وجود دارند که به دلایل مختلف همچون سیاسی، اقتصادی، و موارد دیگر به دنبال هک کردن سایت ها و سرورهای سازمانها و ادارات هستند و متأسفانه در سالهای اخیر کشور عزیز ما از این بحث به دور نبوده و آسیب های فراوانی دیده است که چرا با وجود رخنه ها و حفره های امنیتی بسیاری از سایت های دولتی مورد نفوذ افراد مختلف قرار گرفته اند.

وظیفه اصلی Web Application Firewall WAF ارائه راهکار های امنیتی برای حفاظت از این گونه حملات می باشد و همچنین به منظور ایمن کردن وب سایت ها و برنامه های تحت وب سازمان را شامل می شود. با استفاده از WAF از حملاتی نظیر SQL injection،Cross Site Scripting ، Local File Include ، Remote File Include ، CSRF و سایر آسیب پذیری های تحت وب تا حدی جلوگیری کرد.

Web Application Firewall با فیلتر کردن دستوراتی که در وب هکینگ استفاده میگردد، موجب افزایش امنیت یک سایت میشود؛ به طور مثال در حملات SQL Injection با اجرای دستوراتی همانند Select, Where, From در نوار ادرس مرورگر میتوان اقدام به نفوذ به دیتابیس نمود که یک Web Application Firewall خوب تمامی دستورات را فیلتر میکند که موجب افزایش امنیت یک سرور و سایت میشود.

چگونه مودم وایرلس خود را امن کنیم؟

شور و شوق استفاده از اینترنت و شبکه های مجازی مانند تلگرام و سایر اپلیکیشن ها در کشور عزیزمان ایران موجب شده است تا افراد در هر مکانی که فرصت برای استفاده از اینترنت داشته باشند اقدام به استفاده از این شبکه-های اجتماعی می کنند. امنیت مودم های وایرلس امروزه به خصوص در کشور عزیزمان ایران امری بسیار مهم است چرا که همه تشنه ی اینترنت رایگان برای استفاده از شبکه های اجتماعی مانند تلگرام هستند در این مطلب قصد داریم چند نکته در خصوص ایمن سازی مودم های وایرلس برای شما عزیزان در کانال منتشر کنیم .

ایمن سازی مودم های وایرلس بسیار آسان و اما مهم است چرا که نفوذگران میتوانند با هک کردن مودم وایرلس شما اقدام به سو استفاده های زیادی کنند که بدون این که شما حتی متوجه شوید از اینترنت شما برای سو استفاده و کار های مخرب استفاده شود پس بهتر است امنیت مودم وایرلس خود را نیز مانند گوشی موبایل که حریم خصوصی شماست جدی بگیرید.

با رعایت نکات زیر میتوان امنیت مودم وایرلس خود را به حداکثر رسانید:

1- تنظیم کردن پروتکل های امنیتی

در مودم وایرلس شما ترکیب زیادی از پروتکل ها برای ایمن سازی وایرلس وجود دارد که بحث آن بسیار مفصل است اما انواع مختلف رمز نگاری و روش های احراز هویت و .... فقط همین اندازه بدانید که بهترین گزینه استفاده از استاندارد WAP2 و رمزنگاری AES می باشد. همچنین اطمینان حاصل کنید که WPS مودم شما خاموش باشد چرا که اسیب پذیری در پروتکل WPS کشف شده است که افراد را قادر میسازد که حتی با گوشی اندرویدی خود اقدام به هک کردن وایرلس دیگران کنند.

برای جلوگیری از این امر وارد مودم وایرلس خود شوید و پروتکل WPS مودم وایرلس خود را خاموش کنید.

2- انتخاب یک پسورد مناسب

همیشه در آموزش نکات ایمنی این گزینه به چشم می خورد خصوصا امنیت ایمیل های شخصی در اینجا هم همین قضیه صادق است چرا که شما هر چقدر که از پروتکل های قدرتمند ایمن سازی استفاده کنید اگر رمز شما قابل حدس زدن یا رایج باشد انگار هیچ کار نکرده اید !! رمز مودم شما میتواند بین 8 تا 113 کاراکتر باشد و سعی کنید حداقل از یک رمز 12 رقمی که شامل عدد و حروف باشد را استفاده کنید.

3- نام مودم خود را پنهان کنید

اگر شما نام مودم وایرلس خود را پنهان کنید دیگر افراد به جای اسکن کردن محیط اطراف نمی توانند نام مودم وایرلس شما را پیدا کنند و فقط در صورتی می توانند آن را پیدا کنند که نام آن را از پیش داشته باشند با مخفی کردن نام وایرلس خود میتوانید از حملاتی مانند بروت فورس یا کرک نیز جلوگیری کنید.

4- از قابلیت فیلتر کردن مک آدرس استفاده کنید

سعی کنید که مک آدرس دستگاه های خود را پیدا کنید و سپس در لیست سفید مودم آن هارا تعریف کنید اینگونه مودم هر سیستمی به غیر از سیستم های شما را که قصد وصل شدن به شبکه ی وایفایتان را داشته باشد رد می کند حتی در صورتی که شخص دیگری پسورد شما را داشته باشد باز هم نمی تواند از مودم شما استفاده کند.

بررسی امنیت سرویس های ربات تلگرام

مدتی است که ساخت ربات ها در اپلیکیشن تلگرام رایج و عمومی شده است و امروزه هر فرد بنا به سلیقه و نیاز خود رباتی را برای ارائه خدمات به کاربران ایجاد می کند. برای ایجاد ربات ها در تلگرام می بایست با زبان های برنامه نویسی اشنایی مطلوبی داشت و همچنین میتوان با استفاده از برنامه های خودکاری مثل ربات ساز ها برای ساخت ربات در تلگرام استفاده کرد همچنین وب سایت هایی خدمات ساخت ربات تلگرام را در اختیار کاربران قرار میدهند.

در این بین سوالی پیش می آید که در این مطلب به بررسی ربات ها میپردازیم:

شاید برای بیشتر افراد جای سوال باشد که آیا ربات هایی که به وسیله ی سرویس های ربات ساز تلگرام ساخته می شوند قابل اطمینان هستند؟

در پاسخ به این سوال باید گفت امنیت هیچ سرویسی را نمیتوان به صورت صد درصد تضمین نمود و هر سرویس مشکلات و معایب خود را دارد سازندگان ربات های تلگرام و همچنین ارائه دهندگان این سرویس ها می توانند به پیام هایی که به ربات شما ارسال می شود دسترسی داشته باشند. به طور مثال یک ربات در یک گروه در تلگرام میتواند اقدام به جمع کردن مطالب گفته شده در گروه تلگرام بپردازد و پس از جمع آوری این اطلاعات برای برنامه نویس خود ارسال نمایید.

شاید جای سوال باشد که آیا یک ربات تلگرام میتواند اقدام به هک کردن گوشی شما یا کل اطلاعات تلفن همراه کند؟ باید توجه داشت که این کار در صورتی امکان پذیر خواهد بود که اپلیکیشن تلگرام دارای مشکل امنیتی باشد و نفوذگر یا هکر با نوشتن یک ربات کار خود را آسان نموده و با استفاده از ربات کاربران بیشتری را به بد افزار ها و ویروس ها آلوده کند.

تیم توسعه دهنده تلگرام بار ها مسابقاتی برای شناسایی آسیب پذیری های این سرویس برگزار کرده است که بیشتر آسیب پذیری های این سرور در چند سال اخیر رفع شده اما باید توجه داشت که امنیت یک سرویس هیچ زمان به طور کامل نبوده چرا که شبکه های اجتماعی بزرگتر مثل فیسبوک و.. بار ها توسط افراد مختلف از سرتاسر جهان مورد حمله و نفوذ قرار گرفته اند.

حفظ امنیت در تلگرام با رعایت چند نکته

این روز ها اپلیکیشن پیام رسان تلگرام در کشور عزیزمان ایران جایگاه گسترده ای را پیدا کرده است؛ بطوریکه بیشتر هموطنان ایرانی اقدام به نصب و استفاده از این پیام رسان کرده اند و از پیام رسان تلگرام برای گفتگو با دوستان خود استفاده میکنند. به همین دلیل این اپلیکیشن مورد توجه نفوذگران و هکرها هم قرار گرفته است که سعی در هک کردن اکانت های کاربران دارند. این افراد قادرند تا با روش هایی مانند مهندسی اجتماعی و RAT ها و همچنین ویروسها و روش های مشابه سعی در هک کردن اکانت افراد مختلف در پیام رسان تلگرام می کنند.

در حال حاضر ما سعی داریم که در اینجا با ارائه چند نکته امنیتی موجب جلوگیری از هک شدن هموطنان عزیزمان شویم که قطعاً با رعایت این نکات امنیتی می توانید تا حد مطلوبی از هک شدن حساب خود در تلگرام جلوگیری کنید:

1- سعی کنید تا حد ممکن هیچ فایلی از کانال های تلگرامی با عناوین فریبنده مانند هک تلگرام، هک بازی Clash Of Clans و مواردی از این قبیل را دانلود، نصب و اجرا نکنید.

2- همیشه از نسخه رسمی تلگرام استفاده کنید چرا که در سایر نسخه های تلگرام امکان قرار گرفتن ابزار های جاسوسی که موجب هک شدن کاربران قرار دارد همیشه وجود خواهد داشت همچنین رعایت این نکته تلگرام را فقط از وب سایت رسمی این پیام رسان دانلود کنید یکی از نکات مهم و حیاطی جهت جلوگیری از هک شدن تلگرام میباشد چرا که تیم برنامه نویسان تلگرام نسخه قابل تغییر این اپلیکیشن را به صورت رایگان بر روی وب سایت این شرکت برای استفاده برنامه نویسان قرار داده است که میتوان در سیستم تلگرام هر تغییری که مورد نظر برنامه نویس باشد را ایجاد کرد به همین دلیل میتوان با قرار دادن بکدور و .. روش های مشابه اقدام به جاسوسی از کاربران نمود.

3- تلگرام دارای یک نسخه Desktop برای سیستم عامل های ویندوز و لینوکس هم میباشد که برای استفاده از این نسخه، تلگرام طی یک مرحله اقدام به ارسال کد 5 رقمی بصورت پسام کوتاه به شماره تلفن همراه شخص می کند که هکر با اجرای هنر مهندسی اجتماعی سعی می کند کد 5 رقمی را از کاربر دریافت و فرد قربانی که مورد نظر اوست را هک کند.

سخن پایانی

به لطف خدای منان و حمایت شما بزرگواران عزیز با تلاش شبانه روزی توانستیم اولین نسخه نشریه تخصصی امنیت اطلاعات فول سکوریتی را اتمام و نشر دهیم . با توجه به اینکه شماره اول از این نشریه انتشار داده شد ممکن است با ضعف هایی روبرو باشد که در نسخه های بعدی با بهره گیری از اساتید فن این اشکالات برطرف خواهد شد.

هدف اصلی ما همانطور که گفته شد ارتقای امنیت کاربران کشور عزیزمان ایران است و امیدواریم با انتشار این نشریه گامی هرچند کوچک در این راه نهاده باشیم. لازم است قدردانی زحمات همکاران و اساتید و همگی کسانی که همواره ما در انتشار این نشریه امنیتی که اولین نشریه ماست باشیم.

میلاد صفری – سردبیر نشریه

محمدمهدی قاسمی – سردبیر بخش مقالات

سجاد محمدی نیا – صفحه آرایی و گرافیک

مهران صاحب کوهی – سردبیر بخش امنیت برنامه های کاربردی تحت وب

محمد حکم آبادی – سرپرست بخش اندروید

همچنین از عزیزانی همچون الیاس ملکی و شهرام نوری و سایر کسانی که اسامی آنان محفوظ است کمال تشکر را به عمل می آوریم.

در آخر نیز همچون گذشته منتظر پیشنهادات ، انتقادات و همکاری شما عزیزان هستیم.

info@FullSecurity.org

09356025703

https://fullsecurity.org

https://telegram.me/TheHacking