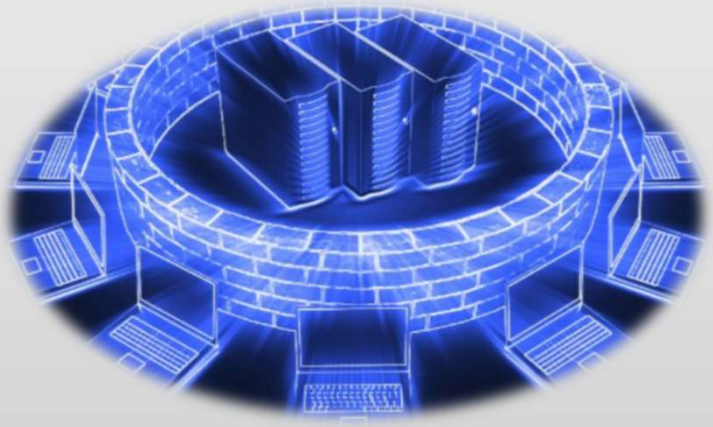
آشنایی با حملات سایبری
درون سازمانی
و
امنیت در شبکه‌های اجتماعی

اهداف



1. آشنایی با اهمیت حفاظت از اطلاعات سازمان
2. آشنایی با حملات سایبری در سازمان ها
3. آشنایی با نحوه جلوگیری و مقابله با حملات سایبری
4. آشنایی با نحوه حفاظت از سیستم های درون سازمانی
5. امنیت شبکه های اجتماعی

مرکز تخصصی آپا دانشگاه تحصیلات تکمیلی صنعتی کرمان
apa@kgut.ac.ir | 03433778508

- اطلاعات عنصری حیاتی است که بقای سازمان ها به شدت به آن وابسته است و نیازمند راهکارهای حفاظتی مناسب؛ جهت جلوگیری از تخریب، دستکاری، حذف و یا ایجاد وقفه در خدمات است.
- گسترش روز افزون تهدیدات و افزایش حملات سایبری به سازمانها در سالهای اخیر، نشان دهنده آن است که شیوه‌های دفاع فعلی در برابر این تهدیدات دیگر جوابگو نیست و سازمانها نیازمند بکارگیری تدابیر اصولی تر در این حوزه هستند.
- **خسارات جبران‌ناپذیر ناشی از وجود یک حفره یا مشکل امنیتی در سازمان ها:**
  - ✓ از دست دادن اعتبار فعلی سازمان در میان رقبا
  - ✓ کاهش درآمدهای سازمانی
  - ✓ افزایش هزینه‌های سازمانی
  - ✓ سلب اعتماد مشتریان و سرمایه‌گذاران و حتی کارمندان
  - ✓ کاهش مشتریان سازمان

Cybersecurity

مرکز تخصصی آپا دانشگاه تحصیلات تکمیلی صنعتی کرمان
apa@kgut.ac.ir | 03433778508

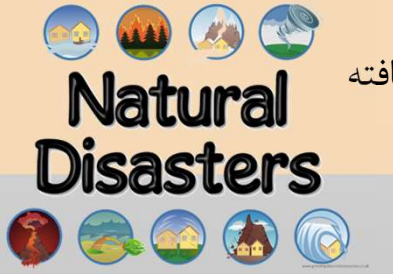
برخی از عوامل تهدیدکننده اطلاعات در سازمان‌ها

تهدیدات نرم‌افزاری

- نفوذ به فایروال‌ها
- بدافزارها (ویروسها، تراواها، کرمها)
- انتشار غیرمجاز یا تخریب داده‌ها
- جاسوسی سازمان یافته به وسیله ابزارهای دیجیتالی.

تهدیدات فیزیکی

- بلایای طبیعی (آتشسوزی، زلزله، و...)
- دزدی
- تخریب
- تداخل‌های فیزیکی
- تخریب شبکه
- جاسوسی سازمان‌یافته



مرکز تخصصی آپا دانشگاه تحصیلات تکمیلی صنعتی کرمان
apa@kgut.ac.ir | 03433778508

Cybersecurity

برای ارتقاء سطح امنیت در سازمان‌ها مراحل زیر پیشنهاد می‌شود

- شناسایی منابع حساس سازمانی جهت محافظت
- شناسایی تهدیدات بالقوه سازمان
- تصمیم‌گیری درباره چگونگی مقابله با تهدیدات شناسایی شده
- پیاده‌سازی راه‌کارهای امنیتی مقرون به صرفه جهت محافظت از دارایی‌های شناسایی شده
- مرور مجدد تمام فعالیت‌های مذکور به صورت مستمر و منظم در صورت مشاهده ضعف یا تهدید جدید

مرکز تخصصی آپا دانشگاه تحصیلات تکمیلی صنعتی کرمان
apa@kgut.ac.ir | 03433778508

اقداماتی برای پیاده‌سازی راه‌کارهای امنیتی مقرون به صرفه و سیستم امنیتی پویا

ایجاد مراکز امداد جهت حملات سایبری احتمالی

استفاده از نرم‌افزارهای کاربردی جهت هر چه بیشتر سیستمی کردن امور و کاهش خطاهای انسانی

مدیران و کارمندان به طور پیوسته آموزش‌های امنیتی را دریافت کنند.

با استفاده از سیستم مدیریت امنیت اطلاعات (ISMS)، یک سری کنترل‌ها و محدودیت‌ها برای دسترسی افراد مختلف در سطوح سازمانی مختلف ایجاد شود.

ایجاد شبکه‌های اینترنتی امن با پهنای باند مناسب

تجهیز آزمایشگاه‌های تحقیق و توسعه در مراکز تحقیقاتی

مرکز تخصصی آپا دانشگاه تحصیلات تکمیلی صنعتی کرمان
apa@kgut.ac.ir | 03433778508

Cybersecurity

مثلث امنیت CIA

مرکز تخصصی آپا دانشگاه تحصیلات تکمیلی صنعتی کرمان
apa@kgut.ac.ir | 03433778508

حمله‌ی مرد میانی

- نفوذگر بین دو کامپیوتر که در حال تبادل اطلاعات هستند قرار می‌گیرد.
- نفوذگر ترتیبی را اتخاذ می کند که دو کامپیوتر از وجود او بی‌اطلاع باشند.
- به این ترتیب دسترسی کاملی به اطلاعات دارد. یعنی هم می‌تواند آنها را دریافت کند و هم می‌تواند آنها را مطابق میل خودتغییر دهد و به نفر بعدی تحویل دهد.
- سیستم‌های Wireless در معرض این حمله قراردارند.

استراق سمع

- دراین نوع حمله، مهاجم بدون اطلاع طرفین تبادل داده، اطلاعات و پیام‌ها را شنود می‌کند. این حمله می‌تواند توسط کاربر داخلی و یا خارجی صورت گیرد.
- در این نوع حمله مهاجم می‌تواند از اطلاعات مهم سازمان مانند اطلاعات مالی، پرسنلی و نیز نامه‌نگاری‌هایی که در بستر شبکه صورت می‌گیرد گرفته تا حتی تماس‌های تلفنی که در بستر شبکه صورت می‌گیرد را شنود نماید.

حمله‌ی DOS

- در این نوع حمله، مهاجم از طریق روش های خاص تمام منابع مورد نیاز کاربران سازمان را در اختیار گرفته و در نهایت باعث می شود که کاربران شبکه نتوانند از منابع و اطلاعات وارتباطات استفاده کنند.
- به عنوان مثال از طریق این حمله امکان ارسال نامه از طریق اتوماسیون اداری و یا ثبت تراکنش های مالی در سرور مالی امکان ناپذیر می گردد.

باج افزار

(اخاذی مدرن)

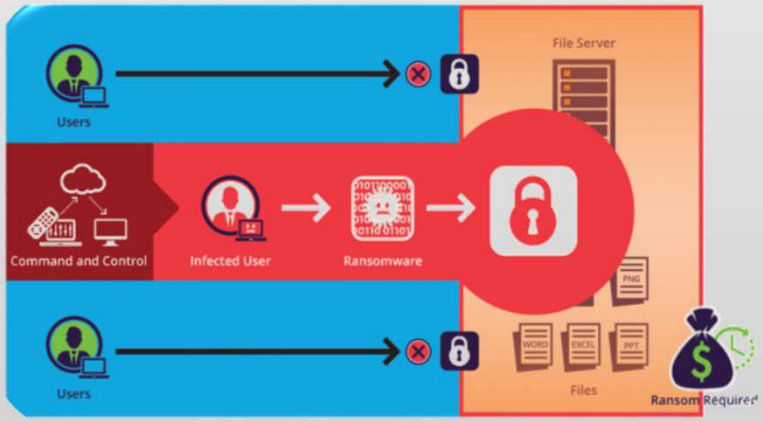
- باج افزار نوعی از بد افزارها است که به مجرمان این امکان را می دهد تا بتوانند از طریق یک **کنترل از راه دور**، کامپیوتر قربانی را **قفل** کنند به طوری که کاربر نتواند از سیستم خود استفاده کند و سپس یک پنجره پاپ آپ روی کامپیوتر شخص نمایان کنند تا به او بگویند که **این قفل باز نمی شود تا زمانی که هزینه ای را برای باز کردن آن بپردازید.**

- گاهی هکرها با قرار دادن یک تصویر نامناسب روی کامپیوتر شخص یا اتهام فعالیت غیر قانونی به آن ها، شخص را تحت فشار می گذارند که هر چه سریع تر پول درخواستی آنها را پرداخت کنند تا هکر ها قفل کامپیوتر آنها را باز کنند.

مرکز تخصصی آپا دانشگاه تحصیلات تکمیلی صنعتی کرمان
apa@kgut.ac.ir | 03433778508

Cybersecurity

- فرد شیاد یا همان هکر تمام اطلاعات کامپیوتر شما را **رمزگذاری** می کند و هنگامی که کامپیوتر خود را روشن می کنید، با یک پیغام از سوی هکر مواجه شوید که در آن دستورات لازم جهت پرداخت پول به منظور رمزگشایی اطلاعات، توضیح داده شده است.



- معمولا درخواست هکرها این است که وجه مورد نظر با استفاده از **پول دیجیتالی بیت کوین** پرداخت شود؛ زیرا ردیابی فردی که پول از این طریق به او پرداخته می شود؛ غیر ممکن است و هر چقدر در پرداخت وجه درخواست شده تعلل شود، نفوذ باج افزار به سیستم بیشتر می شود.

- به طور کلی باج افزارها چهار نوع می باشند:

1. باج افزار **رمزنگار**
2. باج افزارهای **غیر رمزنگار**
3. باج افزار **موبایلی** **(شایع ترین)**
4. **Leakware** (تهدید به افشای اطلاعات)

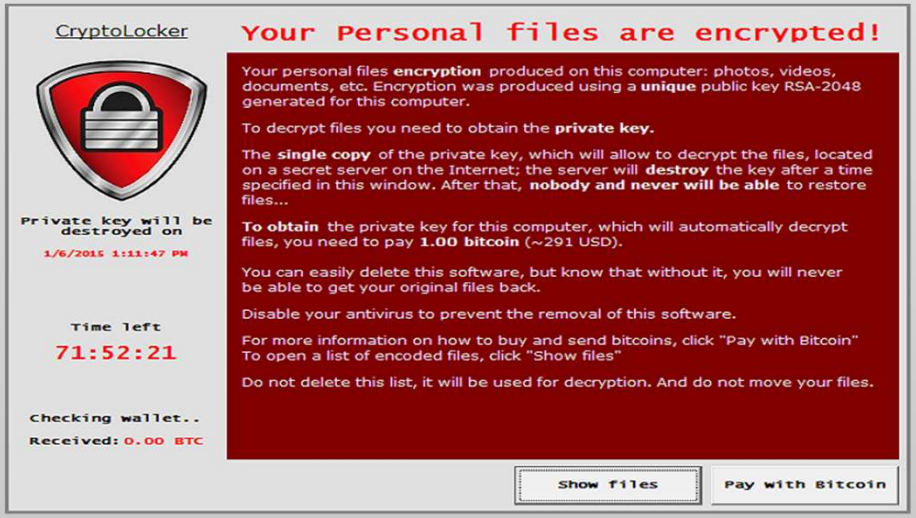
باج افزارهای موبایلی به صورت تصاعدی در حال افزایش هستند و بیشتر سیستم عامل اندروید را هدف قرار داده اند.

این باج افزارها با قرارگیری در گوشی تلفن همراه هوشمند، تمامی اطلاعات آن را رمزنگاری کرده و حتی گوشی قربانی را قفل می نمایند.

مرکز تخصصی آپا دانشگاه تحصیلات تکمیلی صنعتی کرمان
apa@kgut.ac.ir | 03433778508

باج افزار کریپتولاکر (Cryptolocker):

کریپتولاکر، جزو مشهورترین باج افزارهای شناخته شده می باشد که در سال ۲۰۱۳ شناسایی گردید. این برنامه مخرب با استفاده از یک **کلید ۲۰۴۸** بیتی اقدام به رمزنگاری فایل های سیستم قربانی می نمود که عملیات رمزگشایی آن بدون کلید، با توجه به سرعت پردازشی یک کامپیوتر معمولی، ممکن است صدها سال به طول بیانجامد! به همین دلیل کریپتولاکر یکی از خطرناکترین برنامه های باج افزار می باشد که پس از اقدام به عملیات خرابکارانه خود، کاربر را نیز تهدید می نمود که در صورت پرداخت نکردن مبلغ مورد نظر پس از سه روز، کلید رمزگشایی از بین خواهد رفت و دیگر قادر به بازگشایی فایل های خود نخواهید بود.



مرکز تخصصی آپا دانشگاه تحصیلات تکمیلی صنعتی کرمان
apa@kgut.ac.ir | 03433778508

Cybersecurity

واناکرای (Wannacry):

همانطور که اشاره شد، واناکرای از جمله باج افزارهای جدیدی است که به تازگی شناسایی شده و تاکنون توانسته است بیش از **۲۰۰ هزار** رایانه شخصی و اداری را آلوده نماید. هدف واناکرای بیشتر سیستم های سازمانی و اداری می باشد که حاضرند برای اطلاعات با ارزش خود، مبالغ هنگفتی بپردازند.

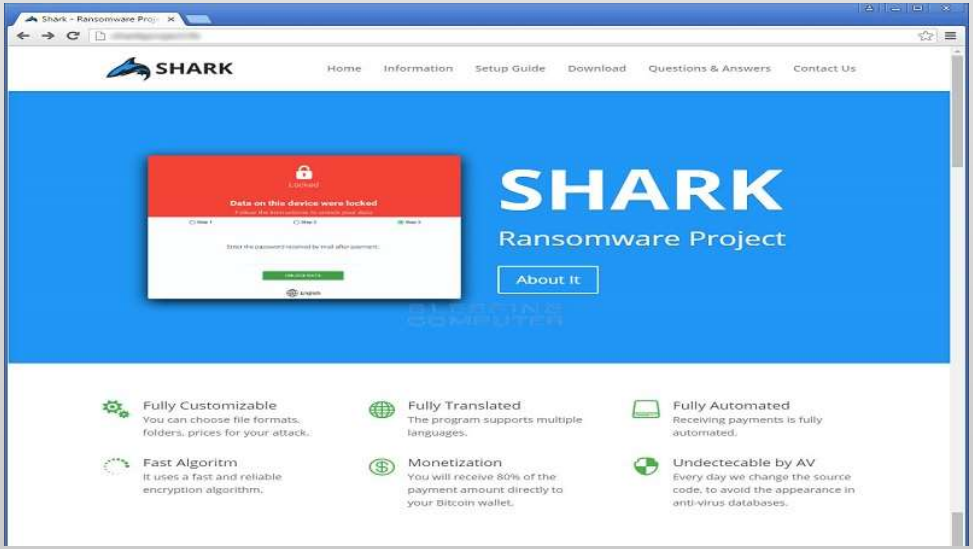
این باج افزار تنها در صورت پرداخت **بیت کوین** (پول اینترنتی غیر قابل ردیابی) به مبلغ ۳۰۰ دلار، کلید رمزگشایی را در اختیار کاربر قرار می دهد و تاکنون تنها شرکت های امنیتی توانسته اند راه پیشگیری از ورود آن به سیستم ها را شناسایی نمایند. در صورت آلوده شدن به واناکرای، در حال حاضر هیچ راهی به جز پرداخت مبلغ مورد تقاضا وجود نداشته و در صورت نپرداختن آن طی سه روز، مبلغ به ۶۰۰ دلار تغییر خواهد نمود.

مرکز تخصصی آپا دانشگاه تحصیلات تکمیلی صنعتی کرمان
apa@kgut.ac.ir | 03433778508

Cybersecurity

باج افزار شارک (Shark) :

این باج افزار در حقیقت یک کد توسعه باج افزار می باشد که به افرادی که دانشی در این زمینه ندارند، اجازه می دهد به سادگی باج افزار خود را ساخته و آن را روی سیستم های دلخواهشان پیاده سازی کنند. این سیستم در ازای هر باج افزاری که روی سیستم قربانی نصب می گردد، ۲۰ درصد هزینه باج را برای خود برداشته و مابقی آن را در اختیار توسعه دهنده برنامه قرار می دهد. از آنجا که این برنامه توانایی ساخت برنامه های مخرب به هر فردی را می دهد، بسیار خطرناک بوده و می تواند تبعات بسیار تاثیرگذاری به همراه خود داشته باشد.

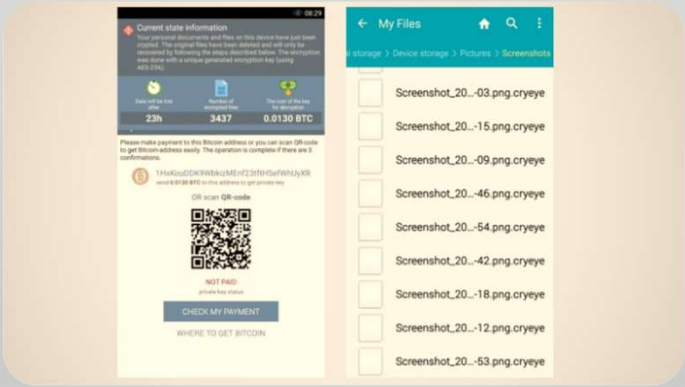


مرکز تخصصی آپا دانشگاه تحصیلات تکمیلی صنعتی کرمان
apa@kgut.ac.ir | 03433778508

Cybersecurity

باج افزار دابل لاکر (DoubleLocker):

این باج افزار که به تازگی توسط **تیم امنیتی ESET** شناسایی شده است یک **باج افزار موبایلی** و مخصوص سیستم عامل **اندروید** است که پس از نصب روی گوشی قربانی ، درخواست استفاده از سرویس گوگل پلی را خواهد داد و پس از اجازه دسترسی، اقدام به فعالیت های مخربانه خود خواهد نمود. باج افزار پس از فعال شدن، اقدام به دانلود برنامه **لانچر** خود نموده و سپس با فشردن کلید Home فعال شده و اقدام به قفل نمودن دستگاه خواهد نمود. در همین فاصله که شما مشغول امتحان نمودن رمزهای متعدد برای بازکردن گوشی خود هستید، باج افزار تمامی اطلاعات گوشی شما را با **الگوریتم AES** رمزنگاری کرده و تنها ۲۴ ساعت به شما وقت می دهد تا مبلغ خواسته شده را پرداخت نمایید. در صورت پرداخت شدن، کلید رمزگشایی برای باج افزار ارسال شده و خود برنامه اقدام به بازگشایی فایلها و باز کردن قفل برنامه خواهد نمود. لازم به ذکر است که این برنامه در حال حاضر هیچ راه مقابله ای برای آن پیدا نشده است و تنها راه پاک کردن تمامی اطلاعات و یا فلش زدن گوشی می باشد.



مرکز تخصصی آپا دانشگاه تحصیلات تکمیلی صنعتی کرمان
apa@kgut.ac.ir | 03433778508

Cybersecurity

خطرات :

زمانی که شما سهواً خطاهای زیر را انجام دهید، امکان دارد کامپیوتر شما درگیر باج افزار شود:

- باز کردن یک ایمیل حاوی ضمیمه مخرب.
- کلیک روی لینک های مخرب که در ایمیل، شبکه های اجتماعی یا سایت ها قرار دارد.
- بازدید از سایت های مخرب که اغلب دارای ماهیت مستهجن هستند.
- باز کردن ماکرو های فاسد در اسناد برنامه.
- اتصال به دستگاه های جانبی usb مثل memory، هارد اکسترنال ، mp3 player و ...
- استفاده از سی دی یا فلاپی های فاسد در کامپیوتر خود.

مرکز تخصصی آپا دانشگاه تحصیلات تکمیلی صنعتی کرمان
apa@kgut.ac.ir | 03433778508

Cybersecurity

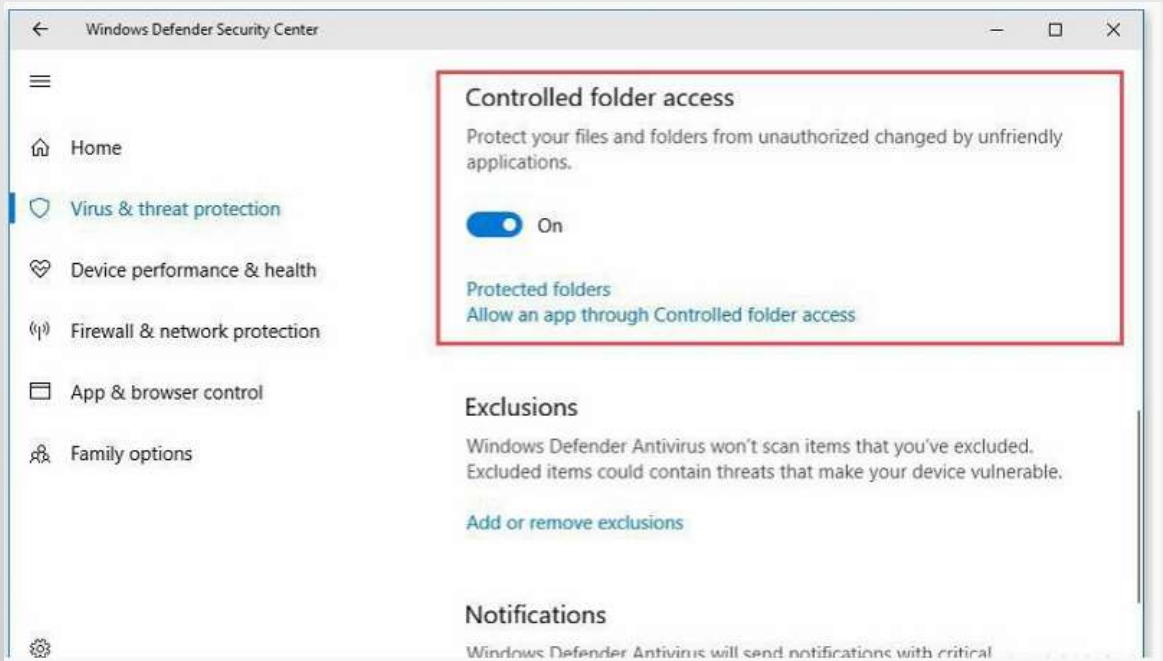
جلوگیری از ورود باج افزار:

- هیچ گاه به ایمیل های ناشناس پاسخ ندهید یا ایمیل هایی را که در قسمت spam ایمیلتان قرار دارد را باز نکنید.
- تنها از وب سایت های امن یا وب سایت هایی که می شناسید استفاده کنید.
- قبل از آنلاین شدن، از وجود آنتی ویروس و دیوار آتش مؤثر و به روز رسانی کامپیوتر خود مطمئن شوید و در صورت امکان از antispyware نیز استفاده کنید.
- به طور منظم از اطلاعات خود نسخه پشتیبان تهیه کنید چرا که برخی از باج افزار ها می توانند حتی فایل های مبتنی بر ابر ذخیره سازی را نیز آلوده کنند.

مرکز تخصصی آپا دانشگاه تحصیلات تکمیلی صنعتی کرمان
apa@kgut.ac.ir | 03433778508

Cybersecurity

آموزش مقابله با باج افزار در ویندوز ۱۰ :



با فعال سازی گزینه مشخص شده، می توان راهی برای مقابله با باج افزار در ویندوز 10 ، ایجاد نمود.

- ✓ با همین یک ترفند ساده شما قادر خواهید بود به سادگی جلوی ورود بسیاری از باج افزارها را به سیستم خود گرفته و با آن ها مقابله نمایید. این گزینه در آپدیت های اخیر ویندوز ۱۰ موجود است و احتمالا برای فعال سازی آن نیاز به تهیه نسخه اسنشال می باشد.

مرکز تخصصی آپا دانشگاه تحصیلات تکمیلی صنعتی کرمان
apa@kgut.ac.ir | 03433778508

Cybersecurity

اگر درگیر باج افزار شدید :

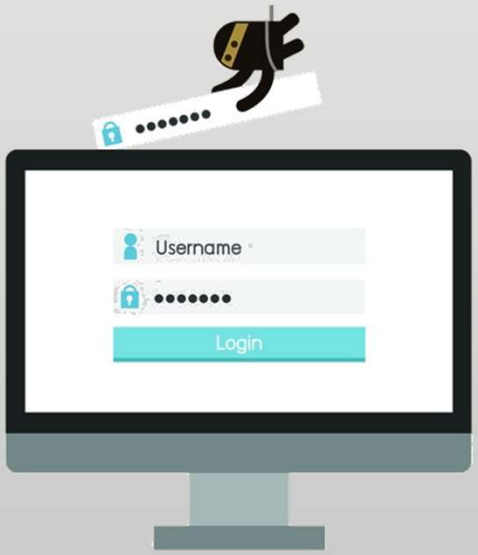
۱ – برای حذف باج افزار یا دیگر نرم افزارهای مخرب که ممکن است روی کامپیوتر شما نصب شده باشد، یک scan کامل با یک solution امنیتی مناسب و به روز انجام دهید.

۲ – اگر کامپیوتر شما از طریق باج افزار قفل شده باشد، حتماً برای مشاوره و راهنمایی از یک منبع قابل اعتماد استفاده کنید و به هیچ وجه پول را واریز نکنید چرا که حتی اگر آن ها قفل کامپیوتر شما را باز کنند، پس از مدتی دوباره از شما باج گیری و کامپیوتر شما را قفل می کنند. بنابراین به دنبال یک راه قطعی و مطمئن باشید.

مرکز تخصصی آپا دانشگاه تحصیلات تکمیلی صنعتی کرمان
apa@kgut.ac.ir | 03433778508

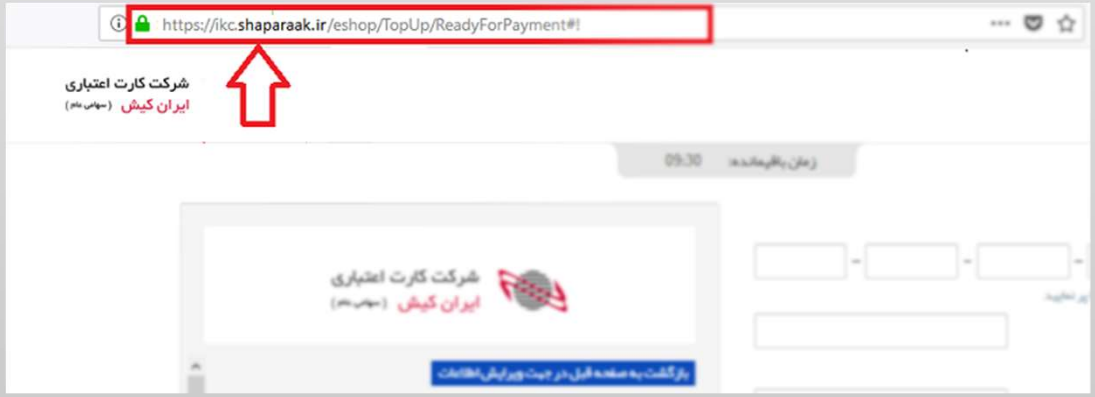
Cybersecurity

- نوعی تلاش برای بدست آوردن اطلاعات از طریق جعل محسوب می شود.
- **فیشر** (کسی که حمله فیشینگ را انجام می دهد) با استفاده از برخی متدها، اقدام به شبیه سازی یک وبسایت، برنامه و یا حتی یک سرویس نموده و با استفاده از آن، اطلاعات کاربران را به سرقت می برد.



مرکز تخصصی آپا دانشگاه تحصیلات تکمیلی صنعتی کرمان
apa@kgut.ac.ir | 03433778508

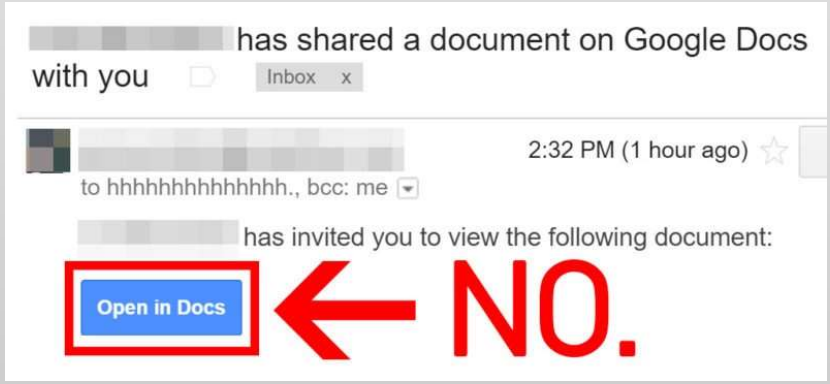
- فیشر اقدام به ساخت یک دامنه با آدرس اینترنتی shaparak.in یا shaparok.ir می نماید و آن را در وب‌سایت‌های مختلف قرار داده و یا از طریق انجام حمله SQL Injection به یک وب سایت هدف، تزریق می‌کند.
- در این هنگام کاربر که قصد خریدی آنلاین را دارد، بجای متصل شدن به درگاه shaparak.ir به درگاه shaparak.in متصل شده و اطلاعات کارت خود از قبیل شماره کارت، رمز دوم، Cvv2و حتی تاریخ انقضای آن را وارد می‌کند.
- نمونه ای از یک آدرس فیشینگ که آدرس به صورت shaparaak و همراه با دو a نوشته شده است.



مرکز تخصصی آپا دانشگاه تحصیلات تکمیلی صنعتی کرمان
apa@kgut.ac.ir | 03433778508

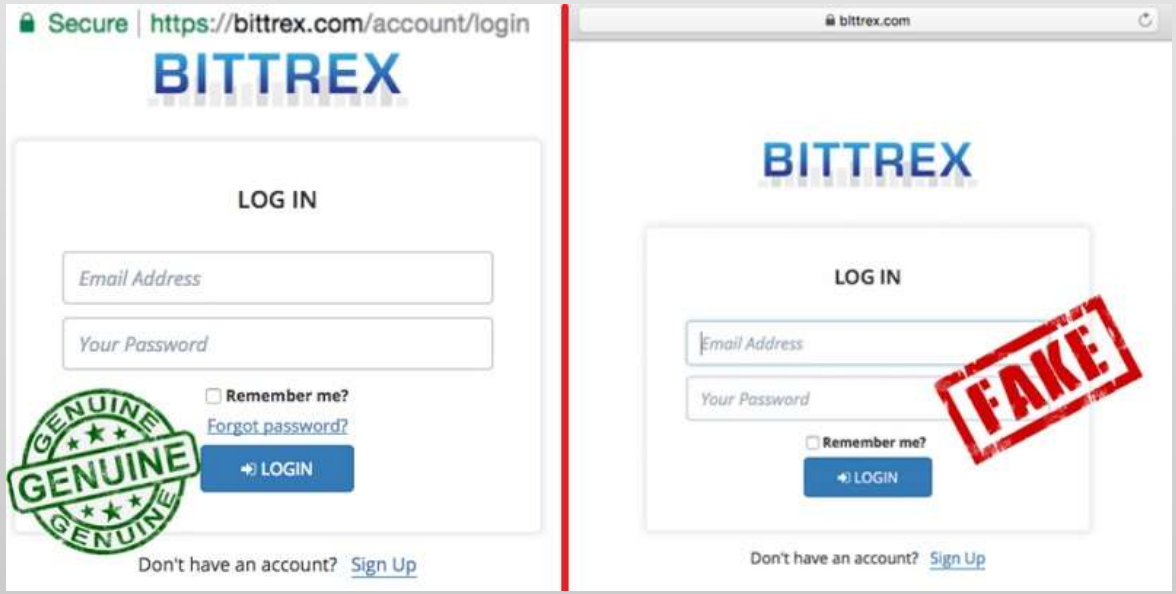
Cybersecurity

- **فیشینگ فریبنده (deceptive phishing)**
  - ✓ این نوع حمله عموما از طریق **ایمیل** صورت می گیرد و فیشر با ارسال یک ایمیل از یک آدرس جعلی که بسیار شبیه به آدرس اصلی است، به روش های گوناگون از کاربر می خواهد تا روی لینک مورد نظرش کلیک کند و سپس به صفحه تکمیل اطلاعات وارد شود که در حقیقت این اطلاعات به فیشر سپرده می شود.



- **جعل وب سایت**

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



مرکز تخصصی آپا دانشگاه تحصیلات تکمیلی صنعتی کرمان
apa@kgut.ac.ir | 03433778508

Cybersecurity

- **فارمینگ**

✓ نوع پیشرفته ای از حمله جعل وب سایت می باشد که در آن هدف اصلی حمله **DNS**ها می باشند.

✓ DNS که وظیفه تبدیل آدرس به آی پی را دارد در این نوع حمله مورد هدف قرار می گیرد و فیشر یک آی پی اشتباه را به جای ip درست به وب سایت مورد نظرش تزریق می کند. در این هنگام حتی اگر کاربر دقیقا همان آدرس اصلی را تایپ کرده و به آن وارد شود، به دلیل DNS های اشتباه به آی پی دیگری ارجاع داده شده و در نهایت اطلاعاتش به سرقت خواهد رفت.

✓ این نوع حمله نیازمند دانش زیادی برای فیشر بوده و به سادگی قابل انجام نیست. اما به هر حال dns سرورهایی که از لایه های امنیتی خوبی برخوردار نباشند، مستعد انجام چنین حمله ای خواهند بود.

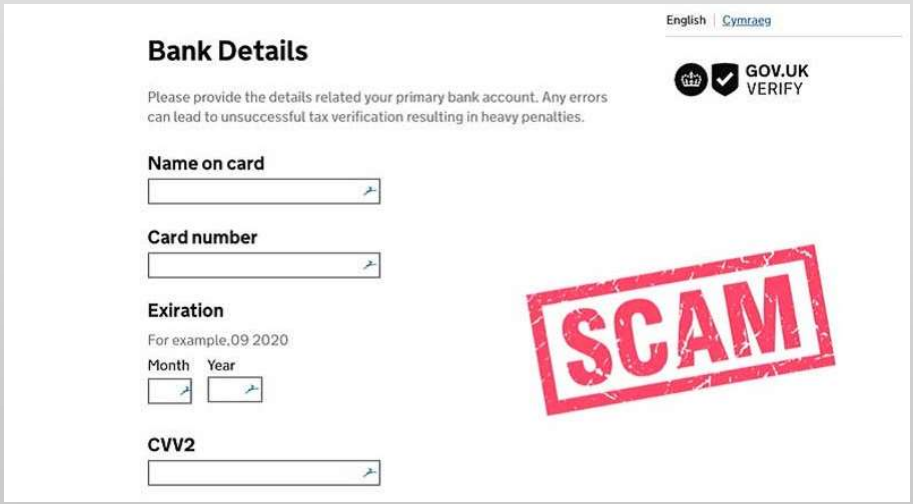
مرکز تخصصی آپا دانشگاه تحصیلات تکمیلی صنعتی کرمان
apa@kgut.ac.ir | 03433778508

Cybersecurity

- **فیشینگ درگاه های پرداخت**

✓ در این روش فیشر یک وب سایت راه اندازی کرده و در آن اقدام به فروش اقلام و یا سرویس های مختلف می کند. معمولا این وب سایت ها اسم و رسم چندانی نداشته و تنها قیمت پایین خدمات و کالاهای آن ها ترغیب کننده می باشد.

✓ پس از این که کاربر اطلاعات کارت بانکی خود را وارد نمود، بسته به نظر فیشر، یا پیغام خطا در تراکنش و یا پیغام موفقیت آمیز بودن خرید برای کاربر ارسال می گردد ولی اطلاعات کارت بانکی در پایگاه داده وب سایت ذخیره شده و می توان از آن استفاده نمود.



مرکز تخصصی آپا دانشگاه تحصیلات تکمیلی صنعتی کرمان
apa@kgut.ac.ir | 03433778508

Cybersecurity

- **فیشینگ تلفنی**

✓ این نوع حمله نیز همچون حمله از طریق ایمیل سعی دارد تا کاربر را مجاب کند تا اطلاعات خود را بازگو نماید.

✓ در این نوع حمله معمولا فیشر با استفاده از یک شماره **تلفن** ناشناس با کاربر تماس گرفته و یا به وی پیام ارسال می کند.

✓ پس از آن فیشر خود را مسئول بانکی که کاربر در آن حساب دارد معرفی کرده و سپس از کاربر می خواهد تا برخی اطلاعات خود را جهت تکمیل پرونده و یا هر موضوع دیگری، بازگو نماید.

✓ اگر کاربر این اطلاعات را به فیشر بدهد، حمله با موفقیت انجام شده است.

مرکز تخصصی آپا دانشگاه تحصیلات تکمیلی صنعتی کرمان
apa@kgut.ac.ir | 03433778508

Cybersecurity

جعل اپلیکیشن ها و نرم افزارها

در این روش فیشر با استفاده از دانش برنامه نویسی خود یک اپلیکیشن دقیقا شبیه به اپلیکیشنی بانکی یا مالی، نظیر اپلیکیشن‌های **"اپ، بانک ملی** یا سایر بانک ها" نموده و سپس آن را از طریق منابع گوناگون، همچون شبکه‌های اجتماعی و برنامه‌های پیام‌رسانی، انتشار می دهد.

کاربران به تصور اینکه نسخه جدیدی از اپلیکیشنی که از آن استفاده می‌کند منتشر شده، اقدام به دانلود اپلیکیشن مربوطه نموده و سپس به انجام امور روزمره خود، همچون خرید شارژ و یا پرداخت قبوض با استفاده از آن اپلیکیشن می‌کنند.

این اپلیکیشن‌ها معمولا یک پیغام خطا به کاربر نشان می‌دهند که پس از آن کاربر مجاب می‌شود تا آن را پاک کرده و همان نسخه اصلی خود را نصب کند.

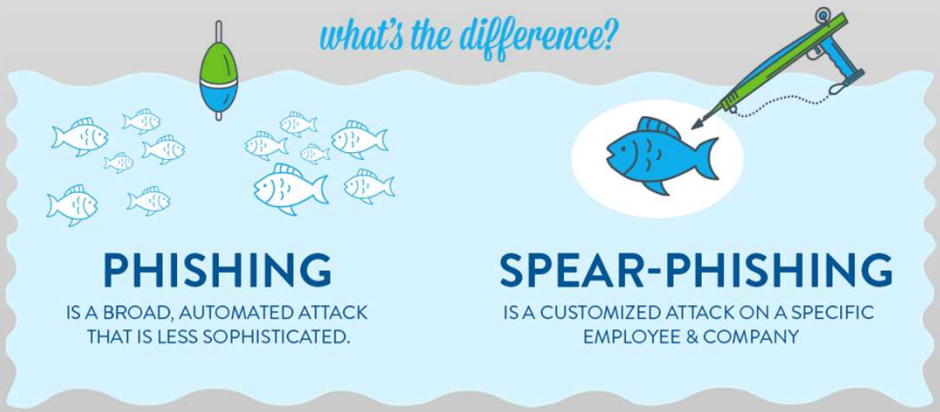
با همان یک بار وارد کردن اطلاعات در اپلیکیشن، تمامی داده‌های مورد نیاز فیشر به دست آمده است و از آن پس فیشر می‌تواند به راحتی از این اطلاعات استفاده کرده و حساب بانکی شما را خالی نماید.

مرکز تخصصی آپا دانشگاه تحصیلات تکمیلی صنعتی کرمان
apa@kgut.ac.ir | 03433778508

Cybersecurity

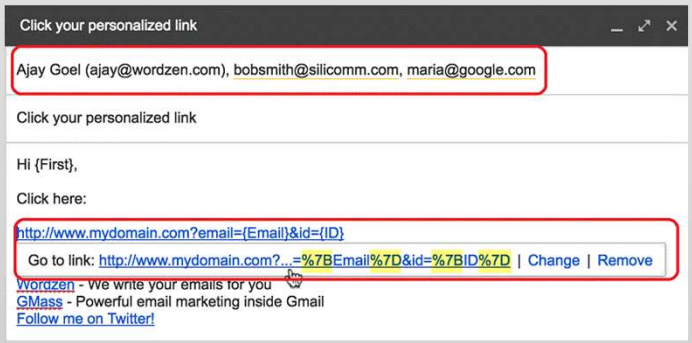
Spear Phishing

- spear phishing به معنای جمع آوری مشخصات شخصی افراد ، شامل نام ، سال تولد و سایر اطلاعات مشابه ، قبل از انجام حمله ی اصلی فیشینگ است. در واقع spear phishing، فراهم کردن مقدمات حمله ی اصلی فیشینگ است.
- با استفاده از spear phishing، اطلاعاتی جمع آوری میشود که ایمیل های حاوی لینک ، مستند تر به نظر برسند و با دارا بودن مشخصات محرمانه ، کاربر به لینک ارسال شده اعتماد کند.



مرکز تخصصی آپا دانشگاه تحصیلات تکمیلی صنعتی کرمان
apa@kgut.ac.ir | 03433778508

- دقت در آدرس درگاه
- از وارد کردن اطلاعات کارت خود در درگاه‌های بی نام و نشان، دارای غلط املایی و مشکوک به شدت پرهیز کنید.
- تمامی درگاه‌های پرداخت از HTTPS پشتیبانی کرده و در قسمت آدرس بار مرورگر، قابل مشاهده می‌باشند. پس از درگاه‌هایی که https نبوده و فاقد رمزنگاری هستند به هیچ وجه استفاده نکنید.
- اطلاعات خود را فاش نکنید.
- عدم خرید از وب سایت‌های نامعتبر
- دقت در محتوا، آدرس فرستنده و لینک‌های ارسال شده در ایمیل
- دقت در نصب برنامه ها و نرم افزارها
- برای حساب های کاربری مختلف، از پسوردهای یکسان استفاده نکنید.
- از شبکه‌های عمومی استفاده نکنید.
- به صورت دوره‌ای اطلاعات حساب خود را تغییر دهید.



مرکز تخصصی آپا دانشگاه تحصیلات تکمیلی صنعتی کرمان
apa@kgut.ac.ir | 03433778508

مقابله در برابر حملاتSpear Phishing

در صورتی که ایمیلی از جانب دوست قدیمی یا همکارتان دریافت می‌کنید، از طریق ایمیل پاسخ گوی آن ها نباشید و با آن ها تماس بگیرید. چون ممکن است آدرس درج شده تنها سوء استفاده از اسم اشخاص باشد و در اصل جعلی باشد.

هیچ گاه به شماره تماس‌های موجود در ایمیل ها اعتماد نکنید و سعی کنید شماره های رسمی یک شرکت را پیدا کنید و در خصوص ارسال ایمیل، با آن ها مشورت کنید.

ارسال و دریافت ایمیل ها را کنترل کنید.

مرکز تخصصی آپا دانشگاه تحصیلات تکمیلی صنعتی کرمان
apa@kgut.ac.ir | 03433778508

Cybersecurity

محبوب‌ترین شبکه اجتماعی در ایران

- طبق آخرین آمارهای منتشر شده، هم‌اکنون بیش از ۴۵ میلیون و ۸۰۰ هزار نفر کاربر ایرانی در تلگرام عضو هستند.
- ایرانی‌ها بیشترین کاربران حاضر در تلگرام را تشکیل می‌دهند.

پرطرفدارترین اپلیکیشن اشتراک تصویر

- اینستاگرام پس از تلگرام، دومین شبکه در لیست محبوب ترین شبکه های اجتماعی در ایران است.

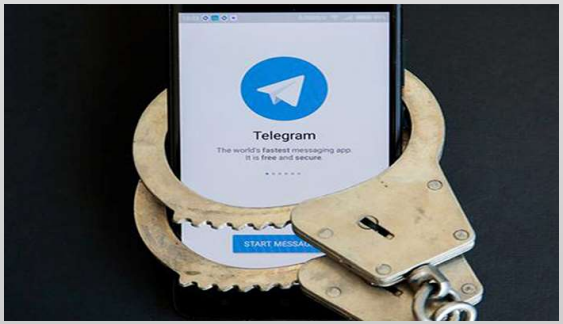
پاتوق خبرنگاران و سیاست‌مداران ایرانی

- اگرچه توییتر طرفداران زیادی در میان مردم عادی ندارد اما سیاست‌مداران، خبرنگاران و دنبال‌کنندگان اخبار از اصلی‌ترین طرفداران این شبکه اجتماعی هستند.

واتس اپ؛ انتقال فایل‌های مختلف بدون پایین آمدن کیفیت

- در این اپلیکیشن می‌توان علاوه بر فرستادن متن، فایل‌های مختلف مانند پی دی اف و اسناد حجیم را بدون پایین آمدن کیفیت ارسال کرد و همین موضوع باعث شد تا به سرعت مورد توجه کاربران قرار بگیرد.
- رمزگذاری پیام‌ها پیش از ارسال و جلوگیری از سرقت اطلاعات افراد، از دیگر قابلیت‌های مورد توجه واتس اپ است.

- هشدار وزارت ارتباطات: نسخه **فیلترشکن تلگرام** و نسخه‌های غیر رسمی را نصب نکنید!
- **از دسترس خارج شدن تلگرام** در سال ۹۶، فرصت مناسبی برای رشد پیام‌رسان‌های ایرانی به شمار می‌رفت.
- افزایش استفاده از **فیلتر شکن‌ها** اولین نتیجه فیلتر شدن تلگرام
- در این میان به جز پیام‌رسان‌های ایرانی برخی **کلاینت‌های غیر رسمی تلگرام** نیز رشد قابل توجهی داشتند.
- **تلگرام طلایی** محبوب‌ترین کلاینت غیررسمی تلگرام بعد از فیلتر شدن آن می باشد.
- ماجرای استقرار سرورهای تلگرام طلایی و هاتگرام در ساختمان وزارت ارتباطات



مرکز تخصصی آپا دانشگاه تحصیلات تکمیلی صنعتی کرمان
apa@kgut.ac.ir | 03433778508

تروجانی که از طریق تلگرام، از کاربران جاسوسی می‌کند:

Android.Spy.377.origin

Added to Dr.Web virus database: 2017-06-20
Virus description was added: 2017-06-21

تروجان مذکور که Android.Spy.377.origin نام دارد در واقع یک ابزار مدیریت از راه دور RAT است که در ظاهر اپلیکیشن‌های سالم و بی خطر انتشار می یابد.

در قالب اپلیکیشن هایی به نام اینستا پلاس Insta Plus، پروفایل چکر Profile Checker و Cleaner Pro به تلفن‌های هوشمند و تبلت های اندرویدی وارد شود.

این تروجان پس از پاک کردن آیکن میان بر، اطلاعاتی مثل فهرست مخاطبین دفترچه تلفن، پیامک های ارسالی و دریافتی و اطلاعات حساب کاربری گوگل صاحب دیوایس را کپی کرده و سپس آن ها را در فایل‌های تکست پیست و ذخیره می نماید.

برای شناسایی صاحب دیوایس، قادر به گرفتن عکس توسط دوربین سلفی موبایل یا تبلت قربانی هم هست.

تروجان کلیه اطلاعات و تصاویر به سرقت رفته را در مرکز کنترل خود بارگذاری می‌کند، و از طریق ارسال سیگنال به رباتی مخصوص در تلگرام موفقیت آمیز بودن آلوده شدن دیوایس را به اطلاعات مجرمان سایبری می‌رساند.

پس از سرقت اطلاعات، تروجان مجددا به ربات تلگرام متصل شده و منتظر پاسخ ربات برای ارسال دستورات کنترل می‌شود. دستورات دریافتی می‌توانند شامل برقراری تماس تلفنی، ارسال یک پیامک، دریافت موقعیت جغرافیایی کاربر، حذف فایل و موارد دیگری باشند.

مرکز تخصصی آپا دانشگاه تحصیلات تکمیلی صنعتی کرمان
apa@kgut.ac.ir | 03433778508

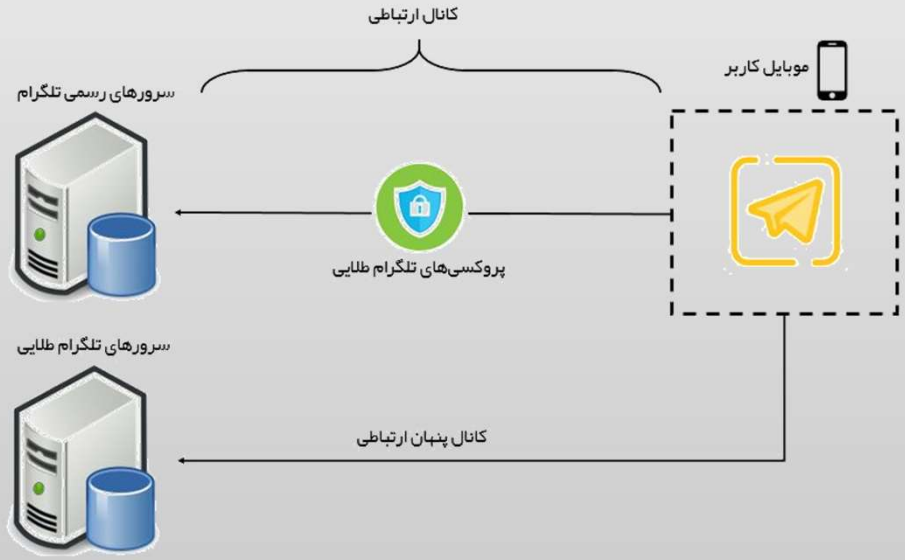
Cybersecurity

- تلگرام طلایی حدود ۲۵ میلین کاربر دارد.
- چندین بار در سال بروزرسانی می‌شود.
- هیچ شرکت یا نهاد دولتی و خصوصی مسئولیت توسعه و پشتیبانی آن را برعهده ندارد.
- هیچ سایت یا Licensing Agreement معتبری ندارد.
- این میزان ناشناس بودن توسعه دهندگان و مالکان حقوقی نگرانی‌هایی درباره غیرقانونی بودن فعالیت‌های این برنامه ایجاد می‌کند.
- "پاول دورف" که رئیس تلگرام است در کشور خودش به‌عنوان یک اغتشاشگر شناخته می‌شود و با تکرار حادثه‌ای شبیه آشوب‌های ایران در روسیه و به‌کارگیری مردم علیه حکومت خود از آن کشور خارج شده است.
- تلگرام شبکه‌ای است که به‌واسطه به‌کارگیری مدیریت هوشمند در آن به حدود ۱۶ دسته از اطلاعات کاربران مثل شماره تلفن، تقویم کاری، عکس‌ها، مکان و... دسترسی دارد.
- این اطلاعات در سرورهایی انبار می‌شود که در کشور ما نیستند، روی آن‌ها داده‌کاوی صورت می‌گیرد و بعد از پردازش اطلاعات داده‌های حجیم یا همان BIG DATA به‌وجود می‌آیند، بیگ دیتاهایی که به‌راحتی با آن می‌توانند به موضوعات ریز اطلاعاتی هر جامعه پی ببرند.

تلگرام طلایی سرورهایی دارد که موبایل کاربر به‌صورت ناخواسته با آن‌ها ارتباط برقرار می‌کند!

- **تلگرام طلایی یک کلاینت تلگرام است** و در ظاهر سرورهای مجزا ندارد بلکه از زیرساخت سرورهای تلگرام برای رد و بدل کردن پیام استفاده می‌کند که علاوه بر سرورهای رسمی تلگرام، **تلگرام طلایی سرورهایی دارد که موبایل کاربر به‌صورت ناخواسته با آن‌ها ارتباط برقرار می‌کند.**

جریان‌داده از تلگرام طلایی تا سرورهای تلگرام



مرکز تخصصی آپا دانشگاه تحصیلات تکمیلی صنعتی کرمان
apa@kgut.ac.ir | 03433778508

Cybersecurity

بررسی تلگرام طلایی

قابلیت‌های سرقت اطلاعات شخصی توسط تلگرام طلایی:

- می‌تواند لیست تمام گروه‌ها و ربات‌ها که کاربر در آن‌ها عضو است را به سرورهای خود ارسال کند.
- امکان ارسال لیست تمام کانال‌هایی که کاربر در آن‌ها عضو هست و اینکه آیا کاربر مدیر آن کانال است یا نه؟
- امکان دریافت و ارسال لیست تمام مخاطبین کاربر به همراه نام‌کاربری آن‌ها
- امکان ارسال موقعیت مکانی کاربر به سرورهای تلگرام طلایی
- امکان سرقت کد Authentication تلگرام که با استفاده از آن می‌توان به اکانت تلگرام کاربر مد نظر دسترسی کامل پیدا کرد.
- ارسال اطلاعات پروکسی سرور ذخیره شده روی کلاینت به سرورهای تلگرام طلایی.

مرکز تخصصی آپا دانشگاه تحصیلات تکمیلی صنعتی کرمان
apa@kgut.ac.ir | 03433778508

Cybersecurity

بررسی تلگرام طلایی

با یکی از بزرگترین ابزارهای جاسوسی و یکی از بزرگترین Botnetهای تاریخ ایران مواجه هستیم ...

اعمالی که تلگرام طلایی بدون اطلاع کاربر از طرف او انجام می‌دهد:

- امکان بازدید یک URL خاص توسط کاربران به صورت مخفی (برای انجام حملات DDoS یا افزایش آمار بازدید یک سایت استفاده می‌شود)
- امکان بیرون رفتن و پاک کردن کانال توسط مدیر کانال
- امکان ریپورت کردن یک کانال خاص توسط کاربران به صورت مخفی
- امکان عضو کردن کاربر در یک کانال خاص به صورت اجباری

هر کسی می‌تواند با شنود شبکه، به راحتی اطلاعات شخصی‌ای که به سرورهای تلگرام طلایی ارسال می‌شوند را ببیند.

بررسی تلگرام طلایی

تلگرام طلایی جاسوسی می کند: بررسی کد جاوا کلاینت تلگرام طلایی

1) برخی از فعالیت‌های نامتعارف و غیرقانونی تلگرام طلایی که با نوتیفیکیشن فعال می‌شود.
2) سرویس هایی که در کلاینت تلگرام طلایی در حال اجرا هستند و به صورت دوره‌ای گزارش‌هایی برای سرور تلگرام طلایی می‌فرستند.
3) قابلیت‌هایی که با یک رخداد خاص مثلا دریافت پیام خاصی فعال می‌شوند.

در متن هشدار مرکز ماهر در گزارشی در بهمن ماه ۹۶ آمده است:

" از آنجا که تلگرام برنامه‌ای متن باز است و هر روز چندین نسخه غیررسمی از آن ایجاد می‌شود و از طرفی شناسایی و بررسی همه این نسخه‌ها کار مشکلی است، لذا توصیه می‌شود **کاربران از نصب هرگونه نسخه غیررسمی و تایید نشده تلگرام خودداری کنند.**"

مرکز تخصصی آپا دانشگاه تحصیلات تکمیلی صنعتی کرمان
apa@kgut.ac.ir | 03433778508

تهدیدهای امنیتی حاصل از بکارگیری شبکه‌های اجتماعی در سازمان‌ها

- ✓ ایمیل‌های فیشینگ که شرحی از سایت‌های شبکه‌های اجتماعی به افراد می‌دهند، اما در واقع آن‌ها را به بازدید از وب‌سایت‌های کلاهبرداری تشویق می‌کنند.
- ✓ پست‌ها و توئیت‌هایی که از طرف همکاران، مشتریان، توزیع کنندگان و سایر افراد است، مشوق افراد در تماس با سایت‌های نامناسب و کلاهبرداری است.
- ✓ کلاهبرداران، سارقان هویت یا هکرها، صفحه و یا حساب افراد را هک می‌کنند و یا اطلاعات محرمانه آنان را به سرقت می‌برند.
- ✓ ممکن است در عکس‌ها یا پیوست‌های پیام، نرم افزارهای جاسوسی وجود داشته باشد.
- ✓ افشای ناخواسته اطلاعات محرمانه توسط افراد (کارمندان، مشتریان یا هر کدام از افرادی که در تماس با سازمان هستند).
- ✓ افشای عمدی اطلاعات محرمانه که به انگیزه‌های متفاوت از قبیل سود مالی، شهرت، کلاهبرداری و در معرض خطر قرار دادن هویت صورت می‌گیرد.

مرکز تخصصی آپا دانشگاه تحصیلات تکمیلی صنعتی کرمان
apa@kgut.ac.ir | 03433778508

راهکارهای حفظ امنیت در شبکه‌های اجتماعی

- ✓ دسترسی به حساب کاربری شبکه‌های اجتماعی مورد استفاده شرکت را تنها در اختیار افرادی قرار دهید که برای پیشبرد کار به آن نیاز دارند.
- ✓ آموزش‌های لازم برای استفاده امن از شبکه‌ها
- ✓ دسترسی کسانی که سازمان شما را ترک کردند خیلی فوری متوقف کنید.
- ✓ اگر دسترسی به یکسری از شبکه ها همانند فیس بوک، توئیتر و غیره مورد نیاز است، دسترسی به انواع دیگر شبکه ها را محدود کنید؛ زیرا اگر نظارت کافی نداشته باشید ممکن است آن ها هدف هک کردن قرار بگیرند.

مرکز تخصصی آپا دانشگاه تحصیلات تکمیلی صنعتی کرمان
apa@kgut.ac.ir | 03433778508

راهکارهای حفظ امنیت در شبکه‌های اجتماعی

- ✓ در مورد انتشار هرگونه اطلاعات محرمانه در مورد کار، مدیران و کارمندان و یا مشتریان و پروفایلتان در پست ها و توئیت‌ها هشیار باشید.
- ✓ از پسوردهای قوی استفاده کنید.
- ✓ روی ایمیل‌هایی که از طرف رقبای کاری برای شما ارسال می‌شود، نظارت دقیق داشته باشید.
- ✓ به پاسخ‌هایی که به ایمیل‌ها و پست‌های شما داده می شود نظارت داشته باشید.

مرکز تخصصی آپا دانشگاه تحصیلات تکمیلی صنعتی کرمان
apa@kgut.ac.ir | 03433778508

راهکارهای حفظ امنیت در شبکه‌های اجتماعی

- ✓ یاد بگیرید که چگونه می‌توانید به شکل صحیحی از این شبکه‌ها استفاده کنید.
- ✓ از امکانات موجود در حریم شخصی برای محدود کردن دسترسی دیگران به پروفایلتان استفاده کنید.
- ✓ در مورد افرادی که اجازه استفاده از حساب کاربری شبکه هایتان را به آنها داده‌اید محتاط باشید.
- ✓ مطمئن شوید که شما و همکارانتان در مقابل حملات فیشینگ و دیگر فعالیت‌های مهندسی اجتماعی که با هدف جمع‌آوری پسوردهای رسانه‌های اجتماعی سازمان‌دهی شده است، ایمن هستید و تحت محافظت قرار دارید.
- ✓ مطمئن شوید که نرم افزارهای اینترنتی و فایروال شما به روز و اثربخش هستند و قبل از آنلاین شدن شما اجرا می شوند.
- ✓ نسبت به مدت زمانی که کارمندان و همکاران شما در سایت‌های غیر مرتبط با کار می‌گذرانند آگاه باشید تا بتوانید نظارت بر فعالیت‌های آنلاین آن‌ها داشته باشید.

مرکز تخصصی آپا دانشگاه تحصیلات تکمیلی صنعتی کرمان
apa@kgut.ac.ir | 03433778508

Cybersecurity

با تشکر از توجه شما

مرکز تخصصی آپا دانشگاه تحصیلات تکمیلی صنعتی کرمان
apa@kgut.ac.ir | 03433778508