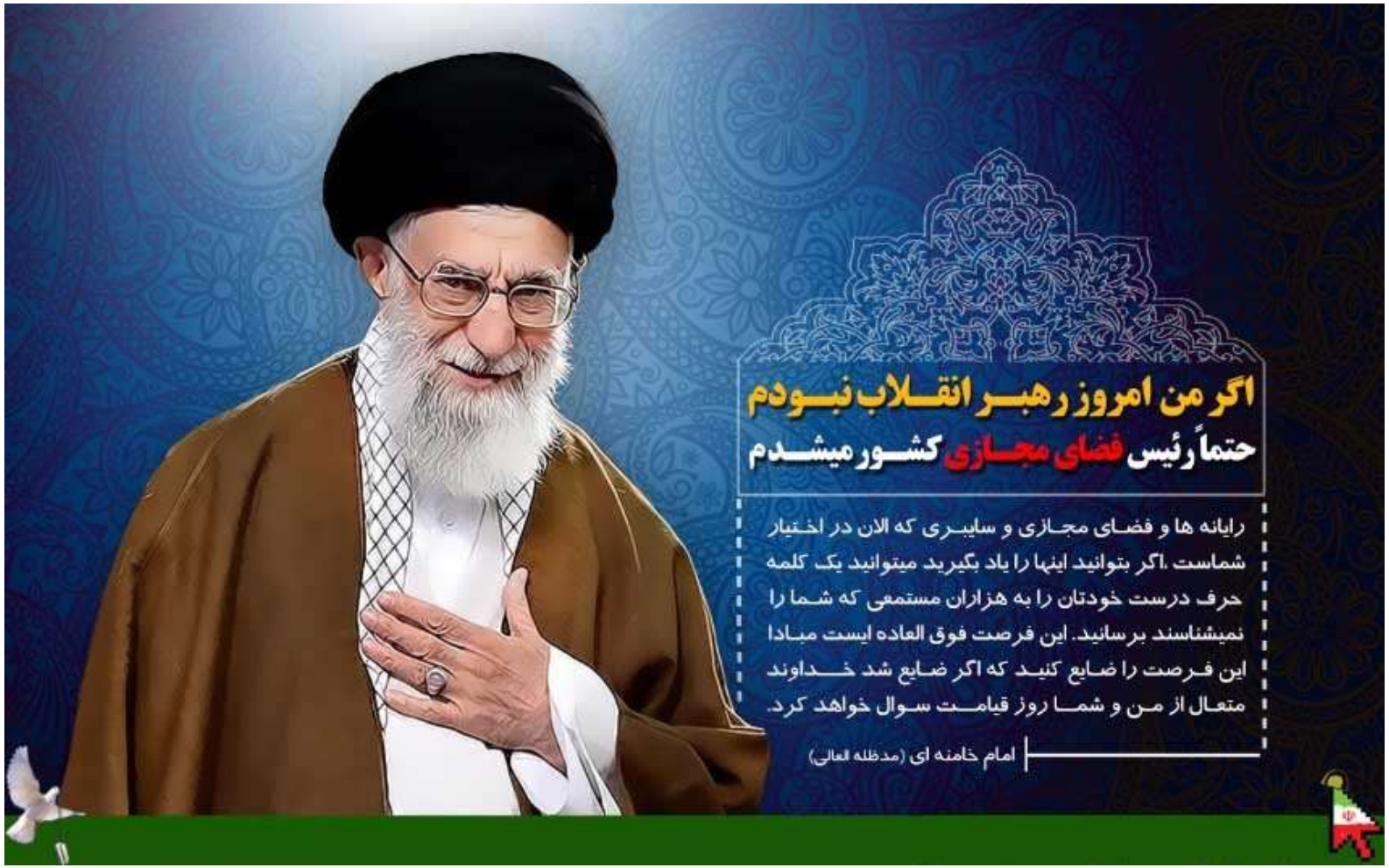

بسم الله الرحمن الرحیم


اگر من امروز رهبر انقلاب نبودم
حتماً رئیس فضای مجازی کشور میشدم
رایانه ها و فضای مجازی و سایبری که الان در اختیار شماست ،اگر بتوانید اینها را یاد بگیرید میتوانید یک کلمه حرف درست خودتان را به هزاران مستمعی که شما را نمیشناسند برسانید. این فرصت فوق العاده ایست مبادا این فرصت را ضایع کنید که اگر ضایع شد خداوند متعال از من و شما روز قیامت سوال خواهد کرد.
امام خامنه ای (مدظله العالی)

امنیت اطلاعات و حفاظت از داده ها در بحران

ارائه دهنده: مهندس بابک مرادی

مدیریت آمار و فناوری اطلاعات دانشگاه
علوم پزشکی کرمانشاه

تاریخ ارائه: شهریور 1404

KEVIN MITNICK

شرکت ها میلیون ها دلار را برای فایروال‌ها، رمزگذاری و دستگاه‌های دسترسی ایمن خرج می‌کنند و این پول هدر می‌رود. هیچ یک از این اقدامات به ضعیف‌ترین حلقه در زنجیره امنیتی یعنی منابع انسانی، نمی‌پردازد.

تعریف پدافند غیرعامل

پدافند غیرعامل یا همان دفاع بدون اسلحه یکی از بخش‌های مهم و نوین الگوی دفاع در جمهوری اسلامی است که متولی صیانت از مردم و حفاظت از زیرساخت‌های حیاتی در برابر تهدیدات است.

«پدافند غیرعامل» با مفهوم کلی دفاع در برابر تهاجم بدون استفاده از سلاح و درگیرشدن مستقیم، سابقه‌ای طولانی در تاریخ بشری و به قدمت خلقت انسان دارد.

فهرست مطالب

چکیده

در دنیای امروز با فراگیر شدن فناوریها و استفاده گسترده از اینترنت، امنیت سایبری به یک مساله حیاتی تبدیل شده است. ایران هم با توسعه فناوریهای ارتباطی و اطلاعات، با چالشهایی مختص به خود در حوزه امنیت سایبری مواجه است. در این مجال، ابتدا به تعریف امنیت و اهمیت آن می پردازیم. سپس، چالشهای امنیتی موجود را شناسایی و تحلیل می کنیم. این چالشها شامل حملات سایبری، نفوذهای هکرها و آسیب به زیرساختهای ارتباطی و اطلاعاتی است. سپس، راهکارهای مؤثری را بررسی میکنیم که می تواند به تأمین امنیت اطلاعات کمک کند

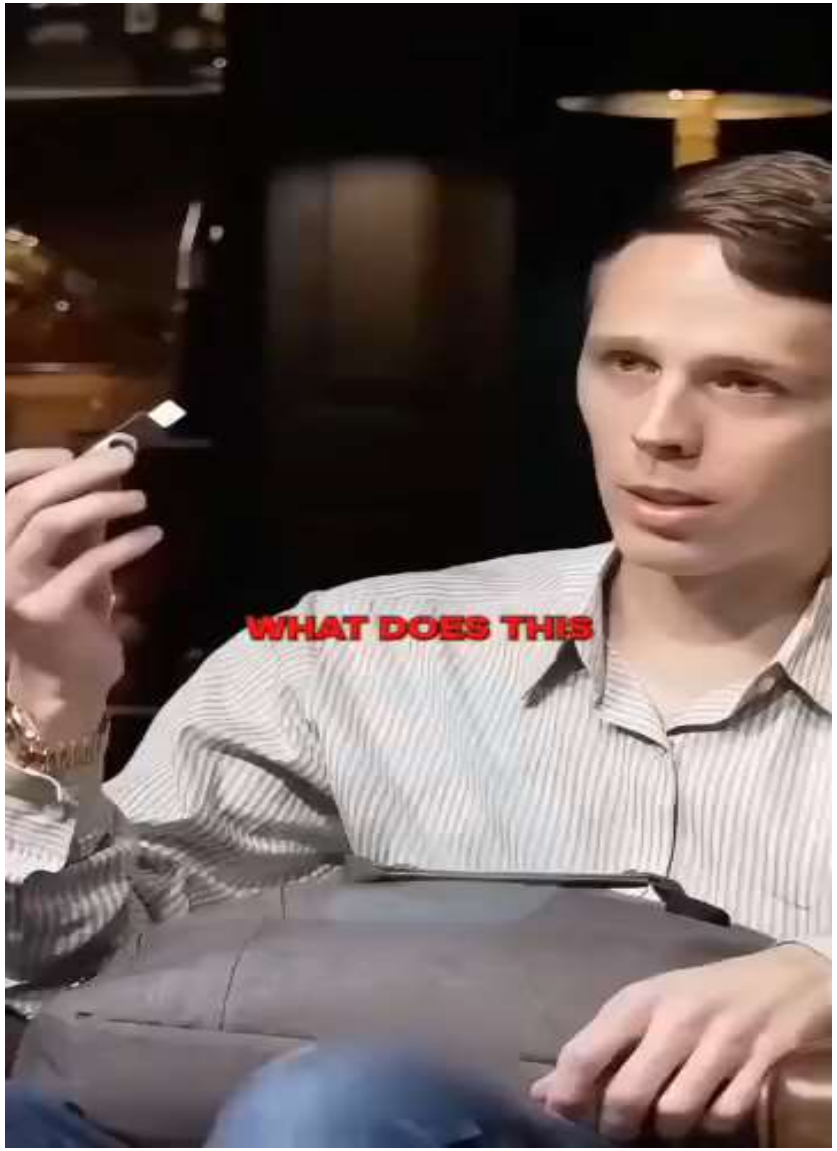
مقدمه

امنیت مانند یک زنجیر است و قدرت هر زنجیر به استحکام ضعیف ترین حلقه آن برمی گردد. امنیت تنها به رایانه، شبکه و سیستم های اطلاعاتی محدود نمی شود و انسان در این حلقه نقش مهمی دارد و ضعیف ترین حلقه زنجیر است که با آموزش می تواند خطرات را مدیریت کند.

95%

of all successful cyber attacks is caused by human error

Source: IBM Cyber Security Intelligence Index


WHAT DOES THIS

چرا امنیت دیجیتال مهم تر از همیشه است؟

۱ **رشد حملات سایبری** آمار جهانی از افزایش روز افزون حملات سایبری حکایت می کند مثل فیشینگ، مهندسی اجتماعی. امروزه هکرها فقط به دنبال سرقت اطلاعات نیستند بلکه اطلاعات را گروگان می گیرند.

۲ **دیجیتالی شدن زندگی شخصی** اطلاعاتی که ما روز مره در فضای دیجیتال ثبت می کنیم از قبیل خریدها و پیام ها، بخشی از هویت ما است. لذا با افزایش اطلاعات مسئولیت حفاظت از آن بیشتر می شود و نشت آن می تواند باعث آزارهای سایبری یا تهدیدات فیزیکی شود

۳ **گسترش دورکاری و کار از راه دور** در زمان کرونا جهان به کار از راه دور روی آورد. این سبک کاری شکاف های امنیتی جدیدی ایجاد کرد.اتصال کارکنان از طریق شبکه های خانگی و استفاده از دستگاه های شخصی برای دسترسی به اطلاعات سازمان و عدم نظارت کافی خطر نفوذ به اطلاعات حساس را افزایش داد.

۴ **اینترنت اشیاء و تهدیدات نا شناخته** دستگاه هایی مانند تلویزیون های هوشمند، دوربین های نظارتی، یخچا لها همگی امروز به اینترنت متصل هستند. اما بسیاری از این دستگاه ها از استانداردهای امنیتی بالایی برخوردار نیستند.یک هکر می تواند از طریق آسیب پذیری دوربین خانگی به شبکه نفوذ کند. لذا امنیت به گوشی و لپ تاپ محدود نمی شود.

۵ **نقش آموزش و فرهنگسازی** بسیاری از نفوذها از طریق خطاهای انسانی صورت می گیرد. کلیک روی لینک های مشکوک، بازکردن فایل های ناشناس، استفاده از رمز های ضعیف، همه رفتارهایی هستند که می توانند راه نفوذ مهاجمان را باز کنند. لذا آموزش کاربران به اندازه ابزارهای فنی اهمیت دارد.

۶ **هوش مصنوعی و تهدیدات نوظهور** در حالیکه هوش مصنوعی فرصت های زیادی را در حوزه فناوری فراهم کرده، اما تهدیدات نوینی نیز با خود آورده است تحلیل رفتاری اتوماتیک، جعل چت های صوتی و تصویری از جمله خطراتی است ناشی از سوء استفاده از فناوری های نوین

۷ **اعتماد عمومی و اعتبار برند** برای سازمان ها، امنیت اطلاعات تنها یک الزام فنی نیست بلکه یک فاکتور کلیدی در اعتماد سازی است از دست رفتن اعتماد کاربران به دلیل نشت اطلاعات کاربران می تواند آسیب جبران ناپذیری به برند وارد کند.

۸ **آینده ای وابسته تر به فناوری** با ظهور فناوری هایی مثل متاورس، بلاک چین و رایانش کوانتومی وابستگی بشر به دنیای دیجیتال روز به روز بیشتر خواهد شد اگر امنیت دیجیتال در کانون توجه قرار نگیرد آینده ای که با آن روبه رو می شویم نه تنها هوشمند تر بلکه خطرناک تر نیز خواهد بود..

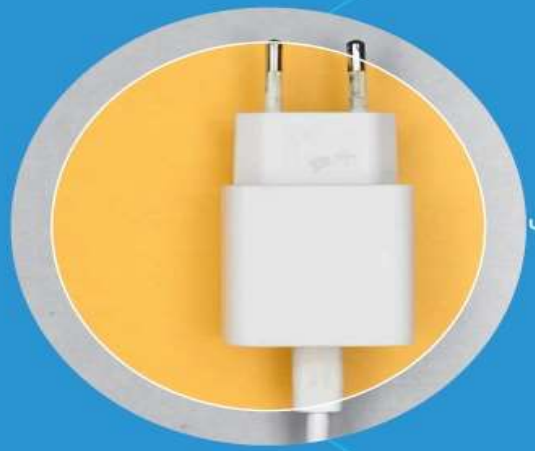
چگونه رمز عبور قوی و مدیریت‌شده داشته باشیم؟

رمز عبور، دروازه ورود ما به دنیای دیجیتال است. هر حساب کاربری – از ایمیل گرفته تا حساب بانکی، شبکه‌های اجتماعی و حتی سرویس‌های اداری – وابسته به رمز عبور است. با وجود اهمیت بالای این موضوع، همچنان بسیاری از کاربران از رمزهای ساده، تکراری یا قابل حدس استفاده می‌کنند.

امنیت دیجیتال با رمز عبور شروع می شود انتخاب رمز قوی ، استفاده از ابزارهای امن برای مدیریت آن، و رعایت اصول امنیتی می تواند تا حد زیادی از تهدیدات سایبری جلوگیری کند. این کار نه تنها از اطلاعات شما محافظت می کند. بلکه به امنیت کلی فضای دیجیتال نیز کمک می کند.

نکته مهم دیگر که باید توجه ویژه داشت این است که زمان هک شدن یک کلمه عبور رابطه نمایی با تعداد کاراکترهای آن دارد بنابراین تنها مقدار کمی افزایش در طول پسورد می تواند مدت زمان مورد نیاز برای هک کردن را به شدت افزایش دهد

STORY SCENARIO



سناریوی داستانی

وقتی یک شارژر ساده شبکه سازمانی را زمین زد

صبح‌چیز از یک روز عادی کاری شروع شد. شرکت مهندسی «آراد دیتا»، فعال در زمینه طراحی سامانه‌های کنترل صنعتی، در تدارک ارائه طرحی مهم به یکی از مشتریان دولتی بود. سالن جلسات در طبقه پنجم آماده ارائه بود، مدیر پروژه‌ها در اتاق کنفرانس جلسه‌ای فشرده داشت، و تیم فنی درگیر هماهنگی آخرین نسخه فایل‌های طراحی شده بودند. در همین شلوغی و رفت‌وآمدها، یک شیء کوچک و به‌ظاهر بی‌اهمیت جا مانده بود: شارژر یک گوشی موبایل.


این یک کابل شارژ اورجینال آیفونه
Original Equipment Manufacture (OEM)
This is an
OEM iPhone cable

تهدیدات کلیدی امنیت داده ها

1. خرابی سیستم یا دیسک سخت
2. ویروس های رایانه ای
3. حذف عمدی اطلاعات توسط کاربران غیر مجاز یا هکرها
4. حذف تصادفی اطلاعات توسط همکاران
5. از بین رفتن اطلاعات در اثر بلایای طبیعی
6. اقدامات تروریستی یا جنگی

انواع بدافزارها

۱

ویروس ها

در صورت دخالت انسان تکثیر می شود و به اطلاعات روی رایانه آسیب می زند.

۲

کرم ها

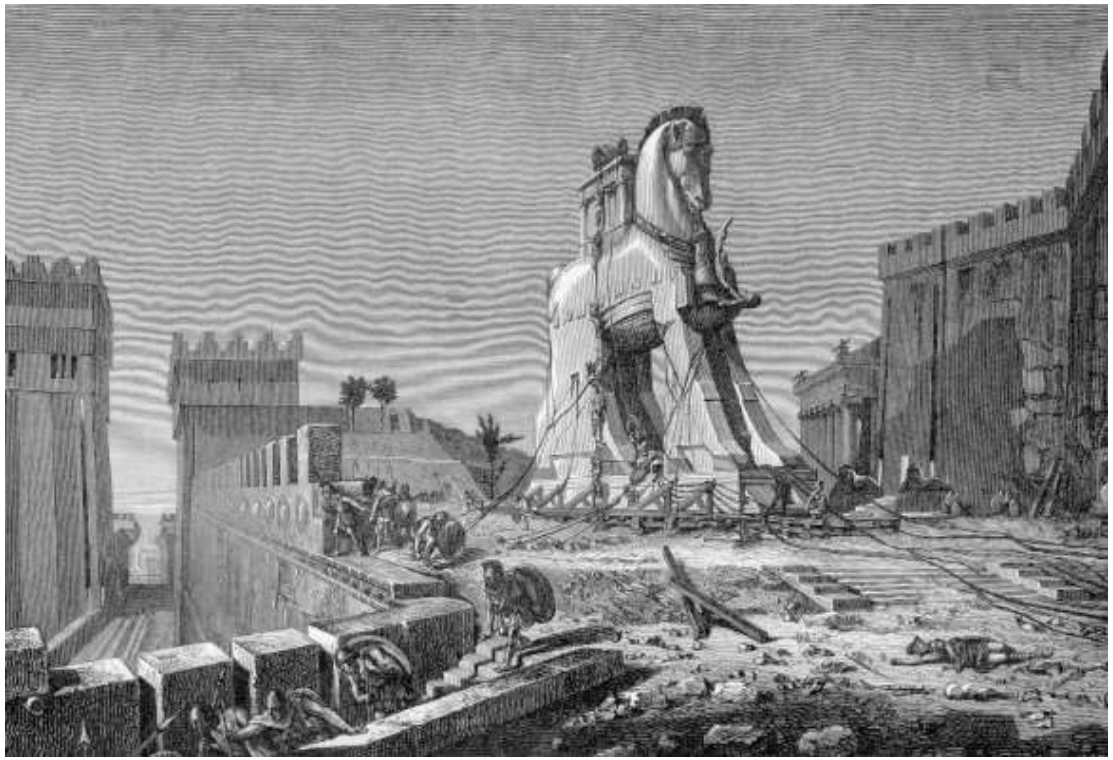
برخلاف ویروس ، خود تکثیر است و از شبکه ها برای ارسال نسخه ای از خود به رایانه های دیگر استفاده می کند.

۳

تروجان ها

غیر خود تکثیر شونده است که در پوشش یک برنامه معتبر وانمود می کند بی ضرر است اما پس از ورود به رایانه قربانی دست به اقدامات مخرب و ویران کننده ای می زند.

ویروس تروجان (Trojan virus)، نام خود را از اسبِ تروا گرفته‌است که داستانِ اصلی آن را می‌توان در حماسه‌ی «انئید» ویرجیل و «ادیسه»ی هومر پیدا کرد. در این داستان، دشمنانِ شهر تروا با استفاده از اسبی که سربازان در داخل آن پنهان شده بودند و وانمود می‌کردند هدیه است، به داخل شهر راه پیدا کردند.



چرا نامِ این اسب برای ویروس تروجان، نام بسیار مناسبی است:
۱- در داستان، مهاجمان سال‌ها شهر را محاصره کرده بودند اما نمی‌توانستند به آن وارد شوند اما با اسب تروا این کار محقق شد. ویروس تروجان هم یک راهکار مناسب برای سیستم‌هایی است که تاکنون ویروس‌های مختلف نتوانسته‌اند به آن‌ها نفوذ کنند.
۲- مهاجمین اسب تروا را به‌عنوان یک هدیه وارد شهر کردند. کاری که ویروس تروجان انجام می‌دهد؛ خودش را به‌عنوان یک فایل مجاز جا می‌زند و وارد سیستم می‌شود.
۳- سربازانی که در داخلِ اسب بودند، توانستند کنترل دفاعی شهر را در دست بگیرند. ویروس تروجان هم همین کار را انجام می‌دهد؛ و کنترل سیستم یا موبایل را در دست می‌گیرد و آن را در برابر سایر ویروس‌ها و بدافزارها، آسیب‌پذیر می‌کند.

۱۱ مورد از معروف‌ترین انواع تروجان

تروجان‌ها انواع مختلفی دارند که هکرها بر اساس نوع کاری که قصد انجام آن را دارند و میزان نفوذپذیری دستگاه قربانی، تصمیم می‌گیرند که از کدام یک از آن‌ها استفاده کنند. در ادامه مهم‌ترین انواع تروجان معرفی شده‌است:

۱- ویروس تروجان Backdoor

به مهاجم این امکان را می‌دهد تا از راه دور به سیستم یا موبایل قربانی دسترسی پیدا کند. و کنترل کامل دستگاه را در دست بگیرد. به‌عنوان مثال می‌تواند فایل‌ها را حذف کند، داده‌های مهم را سرقت کند و یا یک بدافزار دیگر را روی سیستم بارگذاری کند.

2- ویروس تروجان DDoS

برای حملاتی برنامه‌ریزی شده‌است که روی شبکه ترافیک بیش از حد ایجاد می‌کند. با این کار، میزان پردازش موردنیاز در سرور به‌حدی می‌رسد که منابع کافی برای آن وجود ندارد و بدین ترتیب، سرور در اصطلاح Downمی‌شود.

3- ویروس تروجان Exploit

این نوع از تروجان معمولاً در قالب یک برنامه روی کامپیوتر یا موبایل پنهان شده و با نصب نرم‌افزار، کُدهای مخرب را روی دستگاه قربانی قرار می‌دهد. در این روش قربانی معمولاً با استفاده از یک حمله‌ی فیشینگ (phishing) هدف قرار می‌گیرد و سپس با استفاده از کُدهای مخربی که در دلِ نرم‌افزار قرار گرفته است، از اطلاعات و داده‌های دستگاه سوء استفاده می‌شود.

4- تروجان Mailfinder

هدف ویروس تروجان Mailfinderجمع‌آوری و سرعت آدرس‌های ایمیلی است که روی کامپیوتر یا داده‌های ذخیره شده در موبایل قربانی قرار دارد. وقتی نفوذگر به این هدف دست پیدا کرد، می‌تواند از این اطلاعات برای اهداف بعدی خود استفاده کند.

5- تروجان Ransom

ویروس تروجان Ransomبه‌دنبال این است تا از طریقی به کامپیوتر قربانی دسترسی پیدا کند و سپس، عملکرد کلی آن و یا دسترسی به اطلاعات را مسدود کند. بعد از این کار، مهاجم برای اینکه اجازه‌ی دسترسی به داده‌ها یا کامپیوتر را بدهد، شروع به باج‌گیری از قربانی می‌کند.

6- تروجان Rootkit

بعضی موارد مهاجم نیاز دارد تا یک بدافزار روی سیستم قربانی راه‌اندازی کند تا از شناسایی و حذف بدافزارهای دیگر جلوگیری کند. بدین ترتیب در صورتی‌که بدافزار دیگری روی دستگاه قربانی راه‌اندازی شود، امکان شناسایی آن وجود ندارد. این تروجان معمولاً در ترکیب با تروجان‌های دیگر کار می‌کند و به بدافزارها این امکان را می‌دهد تا مدت زمان بیشتری روی دستگاه قربانی باقی بمانند.

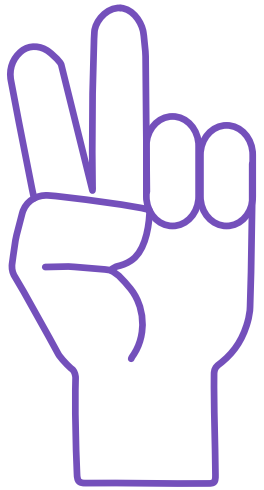
7- تروجان Spy

وظیفه‌ی تروجان Spyهمان‌طور که از نامِ آن هم پیدا است، قرارگیری روی کامپیوتر یا موبایل قربانی و جاسوسی از آن است. در صورتی‌که این ویروس تروجان روی دستگاه قرار گیرد، می‌تواند فعالیت کیبورد را ثبت کند، از صفحه‌ی دستگاه اسکرین شات بگیرد و یا حتی دوربین دستگاه را به‌دلخواه خود روشن کند. این تروجان علاوه بر اینکه می‌تواند امنیت اطلاعات را به خطر اندازد، همچنین موجب نقض حریم خصوصیِ قربانی می‌شود.

روش های سرقت اطلاعات با بدافزار

بات نت ها(شبکه ربات ها)

بات مخفف ربات است و در اصطلاح به یک سیستم آلوده به ربات، بات یا زامبی می گو یند.هکر با ارسال حجم زیادی از درخواست ها به سمت سرور سعی می کند شبکه را از دسترس کاربرانش خارج کند که به DDoS معروف است سپس مهاجم در ازای توقف حمله اقدام به اخاذی می کند.

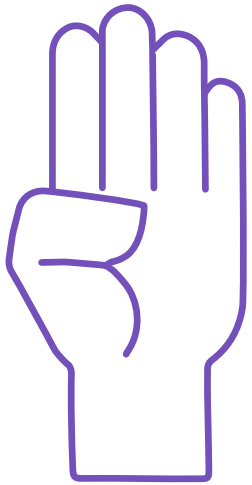


باج افزارها

برخی هکرها، از نوعی بدافزار مخرب به نا م باج افزار استفاده می کنند که تمام داد ه ها را با الگوریتم های رمزنگاری، رمز گذار ی کرده و دسترسی مالک را به این داده ه ا مسدود می کند.

جاسوس افزارها

هکرها از نرم افزارهای جاسوسی برای نظارت بر فعالیت های کاربر استفاده می کند. جاسوس افزارها می توانند ضربه دکمه صفحه کلید را ضبط کنند، از صفحه نمایش عکس بگیرند یا برنام ه هایی که اجرا می شود را ببینند.



کی لاگرها

دکمه نگار، ضبط کننده کلید یا کی لاگر، ابزا ری مبتنی بر سخت افزار یا نرم افزار است که برای ردیابی یا ضبط دکمه های زده شده از روی صفحه کلید استفاده می شود

مقابله با چالش ها و تهدیدات

۱

به روزرسانی زیرساختهای امنیتی

تقویت و به روزرسانی شبکه ها، سیستم ها و نرم افزارها به همراه پیاده سازی ابزارها و سیستم های امنیتی مناسب.

۲

آگاه سازی و آموزش

آموزش جامعه در مورد روشهای مقابله با تهدیدهای سایبری، ایجاد نهادهای آگاهی و ارتقاء آگاهی فردی و سازمانی در حوزه امنیت سایبری

۳

قوانین و سیاستها

تدوین و اجرای قوانین و سیاستهای ضروری برای امنیت سایبری به همراه ایجاد نهادهای نظارتی

۴

همکاری و هماهنگی

ایجاد همکاری بین بخشهای مختلف جامعه مانند دولت، بخش عمومی و بخش خصوصی برای مقابله با تهدیدات سایبری و تبادل اطلاعات امنیتی.

۵

توسعه توانمندی های ملی

تسهیل توسعه صنعت امنیت سایبری و فناوریهای مربوطه در داخل کشور، ایجاد گروههای تخصصی برای پاسخگویی به تهدیدات سایبری

مدیریت امن داده ها

پشتیبان ابزار مهمی برای ایمن کردن رایانه در برابر حملات است

رویه های پشتیبان گیری:

- تهیه پشتیبان به صورت برنامه ریز ی شده باشد
- **فایل پشتیبان باید فشرده با شد**
- پشتیبان گیری در ساعاتی کم کاری سیستم باشد

۱ بازیابی اطلاعات

در بازه زمانی منظم روی رایانه ای غیر از رایانه مادر

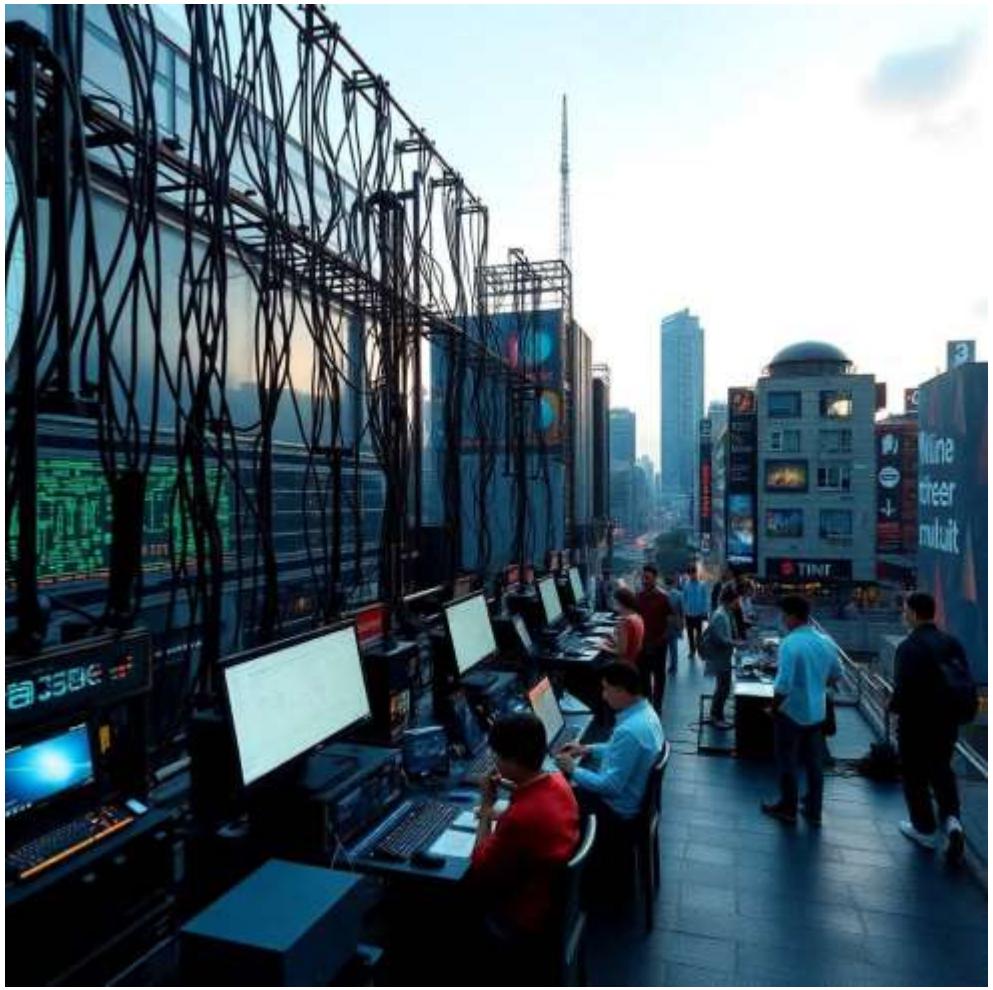
۲ ویروس یابی

فایل پشتیبان ویروس یابی شده سپس به محل ذخیره اصلی منتقل شود

۳ فضای اختصاصی

هر سرور فضای پشتیبان اختصاصی خود را داشته باشد

تدابیر فرهنگی برای مقابله با چالشهای امنیتی سایبری



آگاهی کارکنان

آموزش کارکنان درباره مسائل امنیتی سایبری، هرچند کوچک، میتواند تأثیر قابل توجهی بر امنیت سیستمها و اطلاعات محسوب شود

سیاستها و راهنماها

تدوین و اجرای سیاستها و راهنماهای قوی درباره امنیت سایبری میتواند به افراد کمک کند تا به طور مسئولانه با امنیت سیستمها و اطلاعات برخورد کنند

مرور و بررسی مداوم

ممکن است چالش های امنیتی تغییر کننده باشند لذا ارزیابی دوره ای ، مراجعه به منابع به روز و تعامل مستمر با گروههای امنیتی میتواند تدابیر امنیتی را به روز نگه دارد

نتیجه

- با توجه به پیچیدگی و تنوع روش های حملات سایبری، استفاده از تدابیر فنی و فرهنگی مناسب می تواند به شدت امنیت سایبری را تقویت و آسیب پذیری ها را کاهش دهد.
- تدابیر فنی مانند استفاده از احراز هویت محکم و پیکربندی صحیح سیستمها و شبکه ها، امکان ایجاد پدیده ایمنی در برابر حملات را فراهم می کنند.
- همچنین، تدابیر فرهنگی مانند آگاهی کارکنان درباره مسائل امنیتی، سیاست ها و راهنماها، و بازبینی مداوم میتوانند به آگاهی و رفتار مسئولانه نسبت به امنیت سایبری کمک کنند.
- تهیه فایل پشتیبان با رعایت پروتکل های امن می تواند سیستم را از هر آسیبی مصون دارد.
- بهتر است فایل پشتیبانی قبل از انتقال به رسانه اصلی توسط یک سیستم ایزوله مجددا ویروس یابی شود.

با تشکر از توجه شما!