سینمای پرهیجان سایبری

هنر در مقابل پدیده حملات سایبری و هک، بیکار نمانده است و بسیاری از سینماگران طی سال‌ها، اقدام به ساخت فیلم‌ها و سریال‌های متعددی در این زمینه کرده‌اند. در اینجا نگاهی بسیار کوتاه به ۴ فیلم در حوزه سایبری داریم و پیشنهاد می‌کنیم که اگر آنها را ندیده‌اید، برای‌شان وقتی کنار بگذارید.

ماتریکس
Matrix

IMDb 8.7/10

سال تولید: ۱۹۹۹
کارگردان: لانا و لیلی ماجوفسکی
بازیگران: کیانو ریوز، لارنس فیشبرن، کری-ان ماس و هوگو ویوینگ

این فیلم علمی-تخیلی، آینده‌ای را به تصویر می‌کشد که در آن بشریت در یک سیستم واقعیت مجازی گرفتار شده است. این سامانه به‌وسیله هوش مصنوعی سرکش ایجاد شده است که تمام انسان‌ها را تهدید به نابودی می‌کند.

بازی‌های جنگی
WarGames

IMDb 7.1/10

سال تولید: ۱۹۸۳
کارگردان: جان بدهام
بازیگران: متیو برودریک، الای شیدی، دابنی کلمن و جان وود

یک هکر جوان، به‌طور ناخواسته به یک سامانه رایانه‌ای نظامی دسترسی پیدا می‌کند و باعث آغاز یک جنگ هسته‌ای می‌شود. به‌دنبال این اتفاق، همه وارد یک رقابت مهیج با زمان می‌شوند تا جلوی این فاجعه را بگیرند.

شیادان
Sneakers

IMDb 7.1/10

سال تولید: ۱۹۹۲
کارگردان: فیل آلدن رابینسون
بازیگران: رابرت ردفورد، دن اکروید، بن کینگزلی و مری مک‌دانل

گروهی از هکرهای سابق برای سرقت یک دستگاه رمزنگاری قوی استخدام شده‌اند ولی متوجه می‌شوند که یک سازمان مخوف با انگیزه‌های پنهان آنها را فریب داده است. این فیلم بر عواقب احتمالی نشت داده تأکید دارد.

اولتیماتوم بورن
The Bourne Ultimatum

IMDb 8/10

سال تولید: ۲۰۰۷
کارگردان: پل گرینگرس
بازیگران: مت دیمون، جولیا استایلز، دیوید استراتن و اسکات گلن

بازیگر نقش اول، دچار فراموشی شده و در این بین افرادی به دلایل خاص در پی قتل او هستند. جیسون بورن که هنوز بخش بزرگ و مهمی از گذشته‌اش را به یاد نیاورده، همچنان به‌دنبال نشانه‌هایی از گذشته و احتمالاً آینده‌اش است، به مسکو، لندن، پاریس، ماردید و آمریکا می‌رود. او تحت تعقیب سیا قرار دارد.

با اسکن کد، بخش‌هایی از فیلم ماتریکس را ملاحظه فرمایید.

عصر جرائم سایبری

حملات سایبری، سالانه بیش از ۴۰۰ میلیارد دلار به اقتصاد جهانی خسارت وارد می‌کند. چرا این رخداد همچنان در حال افزایش است؟

افزایش اتصال

- دسترسی به اینترنت به‌طور روزافزون در حال افزایش است.
- سالانه ۲۰۰ میلیون کاربر جدید به اینترنت می‌پیوندند.
- به‌وسیله اینترنت اشیا اکنون نزدیک به ۶ میلیارد دستگاه به اینترنت متصل است.
- اقتصاد الکترونیکی به‌صورت سالانه شاهد رشد بسیار است.

راهبردهای جدید

حملات سایبری بیش از پیش با تاکتیک‌های جدید، فناوری و راهبردها درهم آمیخته شده است. دولتمردان و گروه‌های تروریستی نیز بیشتر درگیر این موضوع شده‌اند.

سیستم‌های حساس

- اینترنت این روزها در بسیاری از حوزه‌های مهم و حساس از جمله سیستم‌های دفاعی، انرژی و مالی حضوری جدی دارد و این شرایط را برای حملات سایبری مهیاتر از قبل کرده است.

Google DQ THE HOME DEPOT TARGET YAHOO! ebay
J.P.Morgan SONY THE WHITE HOUSE WASHINGTON AT&T ups

برخی از غول‌های فناوری که مورد حملات سایبری قرار گرفته‌اند

بیشتر حملات سایبری صورت گرفته در ایران به ترتیب

فیشینگ، حملات DDOS، باج‌افزار و بدافزارها هستند.
نکته مهم اینجاست که «عامل نفوذی» بیشترین و پررنگ‌ترین علت این حملات شناخته شده است.

از هر **۵ کاربر** یک نفر تحت تأثیر حملات سایبری از طریق ایمیل است

۹۶٪

باج‌افزار: نرم‌افزاری مخرب که اطلاعات قربانی را رمزگذاری می‌کند و سپس عاملان آن از طرف مقابل باج خواهی می‌کنند.

نقض داده‌ها در سال ۲۰۲۲ به‌طور متوسط
۴,۳۵۰,۰۰۰ دلار
برای کسب‌وکارها هزینه داشته است

۲۳۶,۰۰۰,۰۰۰
حمله باج‌افزار
در نیمه اول سال ۲۰۲۲ در سراسر جهان رخ داده است.

از حملات سایبری شامل ۹ دسته منحصربه‌فرد است

۱ حمله نرم‌افزاری و نفوذ به رایانه‌ها

۲ سوءاستفاده از اطلاعات توسط پرسنل یک شرکت

۳ نصب فیزیکی همسان‌سازها روی دستگاه‌های خودپرداز برای سرقت رمز عبور

۴ سرقت اطلاعات از طریق نرم‌افزارهای صندوق پرداخت

۵ استفاده از چندین سرور برای غرق کردن سیستم سازمان هدف

۶ ارسال اشتباهی اطلاعات شخصی و انتشار آنها

۷ سرقت لپ‌تاپ، موبایل، فلش و تبلت

۸ استفاده از بدافزار برای آلوده کردن سیستم قربانی

۹ جاسوسی سازمانی

صحبت‌های **سردار غلامرضا جلالی** رئیس سازمان پدافند غیر عامل در خصوص تبدیل ویروس‌های بیولوژیک به سایبری را در قالب یک کلیپ کوتاه با اسکن کد ملاحظه فرمایید.

بالاترین خطر پذیری در حملات سایبری

دولت

پدافند و صنایع هوایی

زیرساخت‌های حیاتی

خرده‌فروشی‌ها

سلامت

امور مالی

مراقب بازی‌ها باشید

| ایلیا اسمعیلی‌پور |
کارشناس بازی‌های رایانه‌ای

بازی‌های رایانه‌ای می‌تواند راهی برای ورود بدافزارهای مختلف به رایانه‌ها، موبایل‌ها و تبلت‌های شما باشد. در زمینه انتشار ویروس‌ها و بدافزارها از طریق بازی‌های رایانه‌ای باید به این نکته مهم اشاره کرد که بازی‌هایی که ناشر ثبت‌شده دارند، به تنهایی دارای بدافزار یا جاسوس‌افزار نیستند، زیرا کنترل کافی روی آن وجود دارد و به‌دلیل مواردی همچون پیگرد قانونی، آنها نظارت دقیقی بر محصولات خود دارند.

شرکت‌های بازی‌سازی چنین حرکتی را نمی‌توانند انجام دهند، زیرا قوانین انتشار نرم‌افزار چنین اجازه‌ای به آنها نمی‌دهد. ولی بازی‌سازهای مستقل می‌توانند در سایت‌هایی که بازی‌ها در آن کنترل نمی‌شود، بدافزار را در قالب بازی آپلود کنند. با این حال، گزارش به ادمین سایت می‌تواند باعث حذف آن بازی از روی پلتفرم مربوطه شود.

در عین حال اگر همان بازی‌هایی که به‌صورت قانونی منتشر می‌شوند، به‌صورت کرک‌شده نصب شوند، خطر وجود بدافزار در نرم‌افزارهای قفل‌شکن یا به‌اصطلاح پچرها (Patchers) نیز وجود دارد. همچنین بازی‌هایی که به‌صورت چندنفری و آنلاین برگزار می‌شود و از زیرساخت شبکه‌ای peer-to-peer (دو رایانه به هم متصل شده و هر رایانه می‌تواند از اطلاعات رایانه دیگر استفاده کند) در آن وجود داشته باشد و درصورت نداشتن امنیت بالا، امکان هک‌شدن و اجرای کد (RCE) وجود خواهد داشت. نمونه اخیر این موضوع، در بازی جی‌تی‌ای (GTA: Online) اتفاق افتاد که کارشناسان امر را به واکنش مجبور کرد. برای همین بازی، یک راه مقابله با هکرها، استفاده از firewall برای مسدود کردن راه ارتباطی است. البته مشکل مربوط به این بازی مرتفع شده که همین اتفاق، درس‌های بسیاری را برای کارشناسان و کاربران در پی داشته است.

به‌طور کلی برای مقابله با این مشکلات بهترین راه، دانلود قانونی بازی از منابع مورد اعتماد است. با این حال، اگر قصد دارید، بازی کرکی دانلود کنید، حتما از سایت‌های معروف دانلود نرم‌افزار ایرانی این کار را انجام دهید، چراکه احتمال وجود بدافزار در آن کمتر خواهد بود. اما راه‌های پیشگیری دیگر، استفاده از نرم‌افزار ضدویروس موقع بازی و البته دنبال کردن اخبار بازی‌هاست.

در مورد بازی‌های مخصوص تلفن‌های همراه نیز چنین چیزی صدق می‌کند. موضوع دانلود نسخه‌های غیرقانونی در گوشی‌های اندرویدی به‌خاطر راحتی دانلود و نصب فایل‌های apk بیشتر از سیستم‌عامل iOS مرسوم است. اینجا نیز ۲ راه‌حل کلی پیش روی شما قرار دارد. اول اینکه سراغ منابع ناشناس برای دانلود اپلیکیشن‌ها نروید و دوم استفاده از آنتی‌ویروس‌های معتبر و فعال در گوشی‌های هوشمند اندرویدی است.