هکرهایی با کلاه‌های رنگی

رنگ‌بندی هکرها، نشان از روش‌ها و عملکرد آنها دارد

استفاده از رنگ‌های کلاه، استعاره‌ای برای نشان‌دادن قهرمانان و تبهکاران در فیلم‌های وسترن آمریکایی دهه ۱۹۵۰است. در آن فیلم‌ها، بچه‌های خوب کلاه سفید می‌گذاشتند. حالا اما صنعت فناوری استعاره رنگ کلاه را حفظ کرده و گسترش داده است. این رنگ‌ها، محدوده و تکامل افراد درگیر در هک را توصیف می‌کند.

هکرهای کلاه سفید

فردی در این نقش بر یافتن و رفع آسیب‌پذیری‌های امنیتی تمرکز می‌کند؛ آنها همچنین ممکن است عنوان شغلی آزمایش‌کننده نفوذ را داشته باشند. وظایف شغلی یک هکر اخلاقی امکان دارد شامل تحقیق در مورد آسیب‌پذیری‌های شبکه، تست امنیت سیستم کامپیوتری، شناسایی و ثبت نقایص امنیتی و ارائه یافته‌های خود و پیشنهاد راه‌حل‌ها به مشتریان بشود. برای کار به‌عنوان یک هکر اخلاقی، به دانش فنی سخت‌افزار شبکه کامپیوتری مانند روترها و سرورها نیاز دارید. همچنین باید در روند فناوری اطلاعات و امنیت سایبری به‌روز باشید. در نهایت، برای به اشتراک گذاشتن یافته‌های خود با سهامداران و تصمیم‌گیرندگان، به مهارت‌های ارتباطی خوبی نیاز دارید.

هکرهای کلاه‌سیاه

معمولاً انگیزه‌های مخربی دارند و در جهت روبه‌روی قانون عمل می‌کنند. اگر شخصی را تصور کنید که ویروس‌های رایانه‌ای را به جهان ارسال می‌کند، کسی که سعی در سرقت و فروش اطلاعات شخصی حساس دارد یا شخصی که تلاش می‌کند به سیستم‌های رایانه‌ای شرکت نفوذ کند، احتمالاً به یک هکر کلاه سیاه فکر می‌کنید! همه این اقدامات غیرقانونی هستند و اکثر هکرهای کلاه سیاه، آنها را برای منافع مالی و شخصی انجام می‌دهند. آنها همچنین ممکن است این کارها را برای اعتراض به یک موضوع یا مجازات یک سازمان با به خطر انداختن داده‌ها و قطع کردن عملیات آن انجام دهند. کلاهبرداری‌های فیشینگ، باج‌افزار، ویروس یا بدافزار، مهندسی اجتماعی و حملات بی‌رحمانه، کارهای مرتبط با هکرهای کلاه سیاه محسوب می‌شوند.

هکرهای کلاه‌قرمز

هکرهای کلاه قرمز، اقدامات تهاجمی و هوشیارانه‌ای را علیه هکرهای کلاه سیاه انجام می‌دهند. کلاه قرمزها ممکن است سیستم کلاه سیاه را هک یا سعی کنند داده‌های آنها را با هدف توقف رفتارهای مخرب از بین ببرند. کلاه قرمزها همچنین ممکن است برای بازگرداندن اطلاعات به صاحبان قانونی کار کنند. اگرچه هکرهای کلاه قرمز بر توقف هکرهای کلاه سیاه تمرکز می‌کنند، اما آنها ممکن است عمداً دست به اقدامات غیراخلاقی یا غیرقانونی بزنند؛ زیرا به‌دنبال مجازات هکرهای کلاه سیاه‌هستند.

هکرهای کلاه زرد

تمرکز هکرهای کلاه زرد بر شبکه‌های اجتماعی است. آنها در بیشتر موارد قصد بدی دارند و تلاش می‌کنند تا حساب‌های فیسبوک، توییتر یا سایر رسانه‌های اجتماعی را هک یا سرقت کنند. طبیعی به‌نظر می‌رسد که چنین اقداماتی غیرقانونی محسوب می‌شوند. انگیزه هکرهای کلاه زرد دستیابی به اطلاعات شخصی یا انتقام گرفتن از یک فرد یا سازمان است.

هکرهای کلاه‌خاکستری

همانطور که از نام آنها پیداست، هکرهای کلاه خاکستری جایگاه متوسطی در اخلاق و قانون دارند. به زبان ساده، هکرهای کلاه خاکستری ممکن است کارهای خوبی را به روش‌های غیراخلاقی انجام دهند. آنها شاید یک سیستم را بدون اطلاع یا اجازه مالک هک و یا به‌جای سرقت، به اشتراک‌گذاری یا سود بردن از اطلاعات به‌دست آمده، آسیب‌پذیری‌هایی را پیدا کنند؛ ممکن است برای رفع مشکل از قربانی خود درخواست پول کنند. اما اگر سازمانی امتناع کند، امکان دارد که این آسیب‌پذیری را عمومی کنند! در حالی که تلاش برای هک بدون اجازه، غیراخلاقی و غیرقانونی است و هکرهای کلاه خاکستری معمولاً به‌دنبال منافع شخصی یا مالی نیستند.

کلاه سفیدها در مقابل کلاه سیاه‌ها

White Hat Vs. Black Hat Hackers

هکر کلاه‌سفید		هکر کلاه‌سیاه
آسیب‌پذیری‌های امنیتی را شناسایی می‌کند و راهکار برای رفع ارائه می‌دهد	قصد و نیت	آسیب‌پذیری‌ها را شناسایی کرده و از آنها بهره‌برداری شخصی می‌کند
حفاظت از داده‌های شخصی و تجاری	انگیزه‌ها	سود مالی، ضربه‌زدن به یک شخص یا شرکت
بله؛ به‌صورت قانونی	استخدام	بله؛ به‌صورت غیرقانونی
۷۵ - ۱۳۰هزار دلار	درآمد سالانه	نامشخص - ادعای یک‌میلیون دلاری
قانونی با حقوق و مزایای شغلی	مشروعیت	غیرقانونی و بدون حقوق و مزایای شغلی

نفوذ از طریق گوشی همراه

یکی از روش‌های سرقت اطلاعات از سازمان‌ها، استفاده از گوشی‌های همراه پرسنل آن سازمان است. با اسکن کد، ویدئویی را در این خصوص ملاحظه کنید.

کلیک

ما تحت‌تأثیر قرار می‌گیریم و روی آن کلیک می‌کنیم. می‌خواهید بدانید آنچه باعث می‌شود کلیک کنید، چیست؟ با اسکن کد، ویدئویی را در این خصوص تماشا کنید.

هوش مصنوعی به دفع حملات سایبری کمک می‌کند

| جنیفر ترلویچ |
مدیرعامل شرکت امنیت سایبری فلیکس روسیه

الگوریتم‌های هوش مصنوعی تمامی درخواست‌ها، حملات و بازدیدهای عادی از سایت‌ها و سرورهای مشتریان را مورد تجزیه و تحلیل قرار می‌دهد. این الگوریتم‌ها، رفتارهای بازدیدکنندگان را نیز بررسی می‌کنند. اگر ویروس یا یک بدافزار باشد نیز دارای رفتارهایی است که هوش مصنوعی قادر به تشخیص آن خواهد بود. در واقع رفتارهای یکسانی که این بدافزارها و ویروس‌ها دارند به AI در زمینه شناسایی کمک می‌کند. اگر به یکی از سرورهای مشتریان ما (مشتریان شرکت فلیکس) در نقطه‌ای از جهان حمله شده باشد، آنگاه هوش مصنوعی قادر به بررسی سایر سرورها درخصوص حملات مشابه است. وقتی بتوانیم یکی را شناسایی کنیم، آمادگی آن را خواهیم داشت که در سرورهای دیگر نیز به دفاع بپردازیم. معتقدم هوش مصنوعی زمانی که با انسان‌ها کار کند، می‌تواند قوی‌تر شود. باور ندارم که هوش مصنوعی بتواند جایگزین انسان شود، اما می‌تواند کارها را سریع‌تر از انسان‌ها انجام دهد. اگرچه هوش مصنوعی می‌تواند خیلی سریع و در کسری از ثانیه، یک حمله سایبری را تشخیص دهد، اما بازهم به انسان‌های متخصصی نیاز داریم که در ادامه کار به چاره‌اندیشی بپردازند. در همه حوزه‌ها نیز چنین است و هوش مصنوعی می‌تواند توانایی انجام کارهای گوناگون را بالاتر ببرد اما نمی‌تواند جایگزین انسان شود.

در آینده هوش مصنوعی هم به توانایی مهاجمان سایبری خواهد افزود و هم باعث افزایش قدرت مدافعان در این زمینه خواهد بود. نباید این را فراموش کنیم که مهاجمان همواره کوشیده‌اند تا یک گام جلوتر از مدافعان باشند. اما با کمک هوش مصنوعی، مدافعان سایبری این شانس را خواهند داشت تا یک گام از مهاجمان جلوتر باشند.

ایران در زمینه فناوری پیشرفت بسیار خوبی داشته است. شرکت‌های خوب فراوانی در ایران وجود دارند که به مراکز داده، خدمات ارائه می‌دهند و در رایانش ابری فعالیت می‌کنند. ما به‌دنبال مشتریانی در ایران هستیم، چراکه امنیت سایبری موضوع بسیار مهمی به‌حساب می‌آید و ما در شرکت خود، تنها به کشورهای دوست روسیه همچون ایران خدمات ارائه می‌دهیم.