حمیدرضا خاتونی
سردبیر کلیک

هکرها و مجرمان سایبری از روش‌های مختلفی برای حمله به گوشی‌های تلفن همراه و نرم‌افزارهای هوشمند استفاده می‌کنند. در ادامه، ۱۰ روش متداول حمله سایبری به این دستگاه‌ها و نرم‌افزارها آورده شده است.

بکدورها (Backdoor Attacks):

بکدورها دروازه‌های پنهانی هستند که هکرها از طریق آنها می‌توانند به سیستم‌ها بدون احراز هویت وارد شوند. بکدور در برخی روترهای تولیدی توسط شرکت‌ها به طور عمدی یا غیرعمدی اضافه شده بود و هکرها توانستند از این راه وارد شبکه‌ها شوند.

تزریق SQL Injection (SQL):

این نوع حمله به هکر اجازه می‌دهد با وارد کردن دستورات SQL در یک برنامه کاربردی، به پایگاه داده‌ها دسترسی پیدا کرده و اطلاعات حساس را به‌دست آورد.

در سال ۲۰۱۴، بیش از ۱۰۰ هزار وب‌سایت توسط یک آسیب‌پذیری SQL Injection هک شدند.

(Man-i

ـاط بین
ـکه آنها

مهندسی اجتماعی (Social Engineering):

هکر از تکنیک‌های روان‌شناسی برای فریب افراد استفاده می‌کند تا اطلاعات محرمانه‌ای مثل رمز عبور را فاش کنند.

در سال ۲۰۱۱، هکرها با استفاده از مهندسی اجتماعی به حساب‌های ایمیل برخی از کارمندان امنیتی RSA دسترسی پیدا کردند.

فیشینگ (Phishing):

فیشینگ زمانی است که هکرها با ارسال ایمیل‌ها یا پیام‌هایی که به نظر معتبر می‌رسند، کاربران را فریب می‌دهند تا اطلاعات حساس‌شان مثل رمز عبور یا شماره کارت بانکی را فاش کنند.

در سال ۲۰۱۶، حمله فیشینگ به ایمیل کمپین انتخابات هیلاری کلینتون منجر به سرقت اطلاعات شخصی شد.

حمله زنجیره تامین (Supply Chain Attack):

در این حمله، هکرها به یکی از بخش‌های زنجیره تامین که ممکن است کمتر امنیتی باشد، نفوذ می‌کنند تا به هدف اصلی برسند.

هک SolarWinds در سال ۲۰۲۰ که یک آپدیت آلوده به بدافزار به بیش از ۱۸ هزار مشتری، از جمله شرکت‌های بزرگ و سازمان‌های دولتی، منتقل شد.

آپدیت‌های مخرب (Malicious Software Update):

هکرها با دستکاری آپدیت‌های نرم‌افزاری، بدافزار را به دستگاه کاربران منتقل می‌کنند.

حمله NotPetya در سال ۲۰۱۷ که از طریق یک آپدیت مخرب نرم‌افزاری در اوکراین گسترش یافت.