صدرا فیروزمند
معلم و پژوهشگر سواد اطلاعاتی و رسانه‌ای

دنیای پنیری سایبر و حفره‌های امنیتی آن

دانشنامهٔ سواد اطلاعاتی ـ ۳

مقدمه

ویژگی بی‌جسمی فضای رایانه‌ای، با وجود مزایای ویژه‌اش[1]، خطر جسمی را نیز پایین آورده است. بدین معنا که اگر فردی در دنیای واقعی از ترس دستگیرشدن اقدام به دزدی نمی‌کند، در فضای بی‌جسم رایانه‌ای احساس خطر کمتری می‌کند و راحت‌تر اعمال مجرمانه انجام می‌دهد. از این‌رو، با گسترش اینترنت، گونهٔ جدیدی از جرم‌ها نیز شکل گرفتند که می‌توانند بدون دخالت جسم، قربانیانی شبانه‌روزی (بی‌زمان) و همه‌جایی (بی‌مکان) داشته باشند! شدت گسترش این نوع جرم‌ها به‌گونه‌ای است که طبق برخی برآوردها، سالانه بیش از ۸ تریلیون دلار به دولت‌ها، سازمان‌ها، شرکت‌ها و اشخاص حقیقی ضرر وارد می‌کند. برای مقایسه: بودجهٔ دولت آمریکا در سال ۲۰۲۳ حدود ۵٬۸ تریلیون دلار بوده است! (cybersecurityventures.com). یا طبق گزارش آژانس ملی جرم و جنایت انگلستان، ۵۳ درصد از کل جرم‌های انجام‌گرفته در سال ۲۰۱۶ در این کشور به جرم‌های رایانه‌ای مربوط بوده است (raconteur.net)!

در این شماره قصد داریم با برخی گونه‌های مهم جرم‌های رایانه‌ای بیشتر آشنا شویم که از قدیم نیکو گفته‌اند: «علاج واقعه قبل از وقوع باید کرد...»

در تعریفی عامیانه می‌توان نفوذ به دستگاه‌ها و شبکه‌های رایانه‌ای از طریق حفره‌های امنیتی آن‌ها و دسترسی به اطلاعات محرمانه یا سوءاستفاده از آن دستگاه‌ها را «رخنه» (هك) دانست. بر همین اساس، کسی را که چنین نفوذی را ترتیب می‌دهد، «رخنه‌گر» (هکر) می‌نامند. یک دسته‌بندی متعارف از آن‌ها چنین است: رخنه‌گرهای «کلاه‌سیاه» (مجرمان رایانه‌ای که انگیزهٔ اصلی آن‌ها اخاذی یا تخریب سامانه‌های رایانه‌ای فرد یا سازمان قربانی است)؛ «کلاه‌سفید» (متخصصان امنیت رایانه که شرکت‌ها و سازمان‌ها آن‌ها را استخدام می‌کنند تا میزان آسیب‌پذیری دستگاه‌ها را آزمایش کنند)؛ «کلاه‌خاکستری» (افراد کنجکاوی که بدون اطلاع به سامانه‌ها نفوذ می‌کنند و پس از یافتن حفره‌های امنیتی، آن‌ها را در قبال کسب پول یا کسب آوازه و شهرت به سازمان مربوطه گزارش می‌کنند)

اما رخنه را بنا به روش نفوذ نیز می‌توان به دسته‌هایی تقسیم کرد. برخی از متداول‌ترین دسته‌ها عبارت‌اند از:

● **حمله‌های منع سرویس (دی‌اُس)[۲]:** آنچه معمولاً در رسانه‌ها دربارهٔ رخنه (هک) و از دسترس خارج‌شدن وبگاه سازمان‌های دولتی در ایران و خارج از ایران می‌شنوید، عموماً از این نوع است. در این روش که به لحاظ فنی از سایر روش‌های رخنه ساده‌تر، اما دفع و مقابله با آن دشوارتر است، مهاجم تعداد زیادی درخواست جعلی را از طریق رایانهٔ خود به وبگاه هدف ارسال می‌کند تا با مشغول و سردرگم کردن آن، با این سیل درخواست‌ها، دسترسی کاربران واقعی را به وبگاه و پاسخ‌گویی به آن مختل کند.

معمولاً وبگاه‌ها برای جلوگیری از این‌گونه حمله‌ها با استفاده از سامانهٔ احراز هویت «کپچا»[۳]، همان سامانه‌ای که بعد از چندین بار تکرار جست‌وجوی یک عبارت در زمان کوتاه در گوگل یا بازکردن مکرر صفحهٔ یک وبگاه نمایش داده می‌شود و از شما می‌خواهد به سؤالی (ریاضی یا تصویری یا متنی) پاسخ بدهید، درخواست‌های واقعی را از درخواست‌های جعلی و روبات‌گونه تفکیک می‌کنند. البته این کافی نیست و مهاجمان می‌توانند برای دورزدن این سپر دفاعی، به جای ارسال درخواست‌های متعدد از یک دستگاه، آن را میان چندین دستگاه توزیع کنند و به این ترتیب وبگاه قربانی را میان درخواست مکرر و توزیع‌شده، کور و سردرگم کنند. به این روش «دی‌دی‌اُس» (حمله‌های منع سرویس توزیع‌شده)[۴] می‌گویند و سامانه‌هایی تشخیصی مثل کلود فلیر[۵] یا گوگل پروجکت شیلد[۶] به همین منظور توسعه یافته‌اند (Curran, 2018).

● **حمله‌های جست‌وجوی فراگیر[۷]:** این‌گونه حمله یکی از روش‌های مرسومی است که از آن برای به‌دست‌آوردن رمز عبور افراد استفاده می‌شود. طی این روش، رخنه‌گر تمام احتمالات ممکن برای رمز عبور را به کمک نرم‌افزارهای خاص (که برای مثال توان پردازش ۱۵ میلیون رمز در ثانیه را دارد) امتحان می‌کند تا سرانجام از طریق یکی از آن‌ها وارد محیط کاربر شود. البته به‌طور مشخص این روش نیازمند قدری زمان و قدرت پردازش بالاست اما از آنجا که اغلب کاربران از رمز عبورهای مشابه و متداولی مثل ۱۲۳۴۵۶ یا abcdef یا «نام‌خانوادگی+ سال تولد») استفاده می‌کنند، رخنه‌گرها ابتدا حملهٔ خود را با فهرستی از این‌گونه عبارت‌ها آغاز می‌کنند[۸]. از طرف دیگر، اغلب وبگاه‌ها برای جلوگیری از این‌گونه حمله‌ها، تعداد بار واردکردن رمز عبور اشتباه را محدود می‌کنند یا از احراز هویت دوعاملی (رمز عبور + پیامک) استفاده می‌کنند. اما با وجود این ضروری است کاربران نیز به جای استفاده از رمز عبورهای ساده و قابل حدس، عبارت‌های پیچیده‌تر (عدد+ حرف + علامت) را به‌عنوان رمز عبور خود تعیین کنند. ضمن اینکه برای همهٔ حساب‌های کاربری خود از یک عبارت ثابت نیز استفاده نکنند تا در صورت افشای رمز یک حساب، سایر حساب‌ها به خطر نیفتند.

● **ساخت نقطهٔ دسترسی جعلی:** در این روش رخنه‌گر (هکر) یک نقطهٔ دسترسی (اکسس پوینت) جعلی، مثلاً وای‌فای عمومی با نام «ایرپورت وایرلس»[۹] یا «کافی وای‌فای»[۱۰] یا «وای‌فای رایگان»[۱۱] ایجاد می‌کند و منتظر متصل‌شدن کاربران به آن می‌ماند تا به محض اتصال، تخلیهٔ اطلاعات قربانی را شروع کند. از حیث کیفری نیز در اغلب کشورهای دنیا، از جمله ایران، قوانین مبارزه با جرم‌های رایانه‌ای با تعریف مجازات‌هایی، به دنبال مقابله با رخنه‌گرها هستند. هر چند باید توجه داشت، تا پیش از این، خطر رخنه صرفاً به دنیای مجازی محدود بود، در حالی که امروزه گسترش «اینترنت اشیا»[۱۲] و متصل‌شدن دستگاه‌هایی نظیر خودرو، وسایل منزل و فناوری‌های پوشیدنی به اینترنت، نگرانی‌های جدی‌تری را نسبت به احتمال هک‌شدن این ابزارها و خطر حاصل از آن در دنیای واقعی ایجاد کرده است. فرض کنید مهاجمان با رخنه در خانهٔ هوشمند شما، تمام چراغ‌ها را خاموش و درها را قفل کنند و فقط در ازای دریافت وجه به شما اجازهٔ خروج از خانه را بدهند! یا رخنه در خودروی هوشمند شما چه تبعاتی می‌تواند داشته باشد؟!

بدافزار

«بدافزار» گونه‌ای نرم‌افزار و کد رایانه‌ای مخرب است که با اهدافی خاص نظیر حذف فایل‌ها و ازبین‌بردن اطلاعات یا ایجاد دسترسی‌های غیرمجاز یا جمع‌آوری اطلاعات شخصی یا ایجاد اختلال در عملکرد سامانه طراحی و منتشر می‌شوند. بدافزارها را می‌توان به گونه‌هایی تقسیم کرد، اما سه نوع از آن‌ها میان کاربران متداول و پرابتلاترند:

● **اسب تروآ یا تروجان**[۱۴]**:** ایدهٔ این نوع بدافزار در واقع برگرفته از افسانهٔ یونانی جنگ تروا است که در آن یونانی‌ها یک اسب چوبی عظیم به شهر تروآ هدیه کردند. اهالی تروآ اسب چوبی را به داخل قلعهٔ شهر خود بردند، غافل از اینکه سربازان یونانی داخل اسب پنهان شده‌اند و به هنگام شب و در حالی که ترویایی‌ها در خواب بودند، شهر را اشغال کردند. بر این اساس، بدافزارهای تروجان در ظاهر نرم‌افزارهای کاربردی و ساده‌ای هستند (مثل برنامک «صفحه‌کلید زیبای گوشی همراه» یا «افزایش‌دهندهٔ سرعت گوشی» یا حتی یک بازی ساده و کودکانه) که کاربران به وسوسهٔ رایگان و جذاب‌بودن آن‌ها، یا به طمع جایزه و کسب درآمد، آن‌ها را نصب می‌کنند، غافل از اینکه به محض نصب و اجرای برنامه، کدهای مخرب برنامه فعال می‌شوند و متناسب با هدفی که برای آن برنامه‌ریزی شده‌اند، در پس‌زمینه شروع به فعالیت می‌کنند: مثلاً گونه‌ای از آن‌ها که با نام «باج‌گیر»[۱۵] شناخته می‌شوند، پرونده‌ها (فایل) و اطلاعات کاربر را گروگان می‌گیرند و با تهدید به پاک کردن آن‌ها، از وی طلب پول می‌کنند. یا «کی‌لاگر»[۱۶] نوعی تروجان است که به‌صورت پنهان تمام حرکات موشی (ماوس) و دکمه‌هایی را که کاربر روی صفحه‌کلید می‌فشارد ثبت و برای رخنه‌گر ارسال می‌کند. تبلیغ‌افزار[۱۷] گونه دیگری از تروجان‌هاست که تمام رفتارهای مجازی کاربر را ثبت و به شرکت‌های بازاریابی ارسال می‌کند تا با تحلیل آن بتوانند به کاربر محتوای تبلیغاتی اختصاصی نمایش دهند (Jackson, 2018).

● **ویروس:** ویروس‌ها شناخته‌شده‌ترین نوع از بدافزارها هستند که خاصیت تکثیرشوندگی دارند. این بدافزارها به پرونده‌های اجرایی دستگاه (مثلاً در ویندوز پرونده‌های با پسوند.exe) متصل می‌شوند و با هر بار اجرای یک نرم‌افزار، در پس‌زمینه فعال می‌شوند و ضمن ایجاد اختلال در عملکرد دستگاه (مثلاً افزایش مصرف برق، خارج‌کردن آن از اختیار یا پنهان‌کردن پوشه‌ها) سایر پرونده‌های اجرایی را نیز آلوده می‌کنند. از این‌رو، با انتقال پروندهٔ آلوده از دستگاهی به دستگاه دیگر، ویروس نیز منتقل می‌شود. از طرف دیگر، ویروس‌ها این قابلیت را دارند که با تغییر شکل مدام خود، ماهیت مخرب کدهایشان را از نرم‌افزارهای امنیتی مخفی نگه‌دارند. برای همین شرکت‌های تولیدکنندهٔ نرم‌افزار ضدویروس، پس از بررسی مداوم کدها در آزمایشگاه‌های خود، به‌صورت روزانه بانک اطلاعاتی نمونه ویروس‌ها را به‌روز و برای شناسایی به نرم‌افزارشان اضافه می‌کنند.

● **کِرم**[۱۸]**:** برخلاف ویروس‌ها که برای اجرا به پرونده‌های اجرایی متصل می‌شدند و تا زمانی که آن پرونده توسط کاربر اجرا نشود، غیرفعال باقی می‌مانند، بدافزارهایی از نوع «کِرم» به‌صورت خودکار و مستقل در دستگاه مشغول به فعالیت و تکثیر می‌شوند. از این‌رو کرم‌ها، نسبت به ویروس‌ها، سرعت بالاتری در آلوده‌سازی دارند و چون برای فعالیت مخرب خود احتیاج ندارند به پرونده‌های اجرایی متصل شوند، می‌توانند در شبکهٔ رایانه‌ها نیز منتشر شوند. یکی از پیچیده‌ترین نمونه‌های این نوع بدافزار، «استاکس‌نت» بود که در سال ۱۳۸۹ شمسی (۲۰۱۰ م.) از طریق حافظهٔ همراه «یو اس بی»، گریزانه(سانتریفیوژ)های تأسیسات هسته‌ای نطنز را آلوده کرده بود و قصد داشت با ایجاد تغییرات ناگهانی در سرعت چرخش گریزانه (سانتریفیوژ)ها، آن‌ها را منفجر کند.

طعمه‌گذاری (فیشینگ)

یکی از رایج‌ترین و پرقربانی‌ترین گونه از جرم‌های رایانه‌ای در کشور ما و بسیاری از نقاط دیگر دنیا طعمه‌گذاری (فیشینگ)[۱۹] است. در این روش، مهاجم از طریق ارسال طعمه برای قربانیان، منتظر می‌ماند آن‌ها در قلاب گیر کنند تا او اطلاعاتشان را تخلیه کند[۱۹].

این روش را نیز می‌توان بنا به نحوهٔ به‌دام‌انداختن قربانی، به گونه‌هایی تقسیم کرد. برای مثال:

● **رایانامه (ایمیل):** ابتدایی و قدیمی‌ترین مدل به قلاب انداختن اینترنتی، ارسال رایانامه جعلی با عنوان، اسامی و نشانی‌های شبیه به شرکت‌های رسمی (نظیر گوگل یا اینستاگرام) به کاربران و تقاضای ارسال اطلاعات شخصی مثل رمز عبور حساب کاربری از آن‌هاست. البته سرویس‌های ارائه‌دهندهٔ خدمات رایانه‌نامه با ارتقای الگوریتم‌های

تشخیصی خود رایانامه‌های مشکوک را در دستهٔ هرزنامه[20] قرار می‌دهند.گوگل حتی بازی تعاملی کوچکی برای آموزش روش‌های شناسایی رایانامه‌های طمع‌گذاری (فیشینگ) طراحی کرده است. اما این روش ساده همچنان قربانیان زیادی می‌گیرد.

● **وبگاه و صفحه‌های پرداخت جعلی:** در این روش، مهاجمان یک وبگاه فروشگاهی یا درگاه پرداخت جعلی با ظاهری کاملاً مشابه صفحات واقعی و رسمی طراحی می‌کنند و از شما می‌خواهند اطلاعات بانکی خود را وارد کنید. اما به محض واردکردن این اطلاعات، هکر از آن‌ها استفاده و حساب بانکی شما را تخلیه می‌کند. البته الزامی‌کردن «رمز یکبارمصرف پویا» در خریدهای اینترنتی توسط بانک مرکزی، گامی مهم و مؤثر برای مقابله با این کلاه‌برداری‌ها بوده است؛ هرچند همچنان ممکن است رخنه‌گرها از طریق برنامک‌های تروجان به پیامک رمز پویای شما نیز دست پیدا کنند.

● **پیام‌رسان:** در این روش که به طور عمده بر بستر نرم‌افزارهای پیام‌رسان یا حتی پیامک رخ می‌دهد، فرد ناشناسی پیام‌های تحریک‌کننده مثل «اخطار قطع یارانه» یا «صدور شکواییه» یا «بدهی مالیاتی» یا «در جایزهٔ چندمیلیونی برنده شدید» ارسال می‌کند و از شما می‌خواهد با ورود به پیوند درج‌شده در پیام یا نصب نرم‌افزار ارسالی، اطلاعات خود را وارد کنید. در حالی که مکرراً اعلام شده است، نهادهای رسمی دولتی به هیچ‌نوع اطلاعیه‌های خود را از طریق پیام‌رسان و الزام به نصب نرم‌افزار اعلام نمی‌کنند و اختصاص سرشماری‌های نامی مثل «V.Behdasht» یا «Bank ...» برای مقابله با این‌گونه کلاه‌برداری‌ها صورت گرفته است.

● **دستکاری پیوند (لینک):** در برخی موارد، مهاجمان پیوند اینترنتی را که ظاهری بسیار شبیه به پیوند اصلی مورد انتظار دارد (مثلاً acliran.ir به جای adliran.ir) برای شما ارسال می‌کنند و از شما می‌خواهند با کلیک روی آن وارد وبگاه شوید و اطلاعات را وارد کنید. در برخی موارد دیگر، عنوان پیوند درج‌شده در متن وبگاه با پیوند واقعی الصاق‌شده به آن متفاوت است و لازم است پیش از تلیک روی پیوند، به پیش‌نمایش نشانی آن در گوشهٔ مرورگر توجه کنید.

● **مهندسی اجتماعی:** «مهندسی اجتماعی»[21] نه یک رشتهٔ دانشگاهی، بلکه مجموعه‌ای از روش‌هاست که از آن‌ها برای واداشتن افراد به انجام یک عمل یا تخلیهٔ اطلاعاتی آن‌ها استفاده می‌شود. بدین معنا که مهاجم ضمن تعامل شخص هدف، با قراردادن وی در شرایط خاص اجتماعی، او را ناآگاهانه به دادن اطلاعات یا انجام اقدامی سوق می‌دهد. البته اگرچه در ارتباطات روزمره و واقعی نیز ممکن است استفاده شوند، اما با گسترش ارتباطات بی‌جسم مجازی و میل به خودافشاگری کاربران در شبکه‌های اجتماعی، سهولت و گسترش بیشتری یافته‌است.

پی‌نوشت‌ها

۱. برای آشنایی با ویژگی «بی‌جسمی» فضای سایبر، ر.ک به مقالهٔ طرح درس‌های سواد اطلاعاتی در شمارهٔ بهمن‌ماه ۱۴۰۱ همین مجله

2. DoS : Denial of Service

3.CAPTCHA : سروازهٔ عبارت «Completely Automated Public Turing test to tell Computers and Human Apart» به معنی «آزمون همگانی کاملاً خودکار تورینگ برای مجزاکردن انسان از رایانه».

4.DDoS :Distributed Denial of Service

5.Cloudflare

6.Google Project Shield

7.Brute Force

۸. برای مثال در این فهرست، مجموعه‌ای از ۱۰ میلیون رمز عبور متداول قرار دارد که اغلب کاربران در دنیا از آن‌ها استفاده می‌کنند:
https://raw.githubusercontent.com/danielmiessler/SecLists/master/Passwords/Common-Credentials/10-million-password-list-top-1000000.txt

9.Airport Wireless

10.Café Wi-Fi

11.Free Wi-Fi

12. IoT: Internet of Things

13. Malware

14.Trojan

15. Ransomware

16. Keylogger

17. Adware

18. Worm

۱۹.اطلاق فیشینگ به این روش به خاطر شباهت آن به ماهیگیری (Fishing) است.

20. Spam

21. Social Engeneering

منابع

1.https://cybersecurityventures.com/cybercrime-to-cost-the-world-8-trillion-annually-in-2023/

2.ttps://www.raconteur.net/report/fighting-fraud-2016/is-future-cyber-crime-a-nightmare-scenario/

3.Curran, K. (2018). Hacking. The SAGE Encyclopedia of the Internet (p. 411). SAGE Publications Ltd.

4.https://www.hivesystems.io/blog/are-your-passwords-in-the-green

5. https://www.setakit.com/mag/credential-stuffing-attack/

6. https://www.hamyarit.com/blog/hacking/

7. https://rc.majlis.ir/fa/law/show/135717

8. Jackson, L. (2018). Malware. The SAGE Encyclopedia of the Internet (p. 619). SAGE Publications Ltd.

9. https://www.dw.com/fa-ir/ویروس-استاکسنت-چگونه-وارد-تاسیسات-هسته ای-خطنز-شد/a-50271881

10. https://phishingquiz.withgoogle.com/

11.https://firstdraftnews.org/wp-content/uploads/2019/10/Information_Disorder_Digital_AW.pdf

12.https://motamem.org/%D9%81%DB%8C%DA%A9%D9%86%DB%8C%D9%88%D8%B2-%DA%86%DB%8C%D8%B3%D8%AA

13.https://www.yektanet.com/blog/50221/what-is-yellow-content

14.https://papers.ssrn.com/sol3/Delivery.cfm/SSRN_ID2958790_code2090195.pdf