حملات هک حکومتی

پیشگیری، محافظت و واکنش مناسب

درس‌نامه

توانا
TAVAANA

حملات هک حکومتی

پیشگیری، محافظت و واکنش مناسب

درس‌نامه

توانا TAVAANA
آموزشکده آنلاین برای جامعه مدنی ایران
e-collaborative for civic education

توانا
TAVAANA

www.tavaana.org

پروژهٔ

e-collaborative
for civic education

www.eciviced.org

حملات هک حکومتی؛ پیشگیری، محافظت و واکنش مناسب
درس‌نامه

ناشر: E-Collaborative for Civic Education

بهار ۱۴۰۴

---

e-collaborative
for civic education

ECCE (E-Collaborative Civic Education) یک سازمان غیرانتفاعی در ایالات متحده آمریکا تحت 501c3 است که از فناوری اطلاعات و ارتباطات برای آموزش و ارتقای سطح شهروندی و زندگی سیاسی دموکراتیک استفاده می‌کند.

ما به عنوان بنیان‌گذاران و مدیران این سازمان اشتیاق عمیق مشترکی داریم که شکل‌دهنده ایده‌های جوامع باز است. همچنین برای ما، شهروند، دانش شهروندی، مسئولیت و وظیفه شهروندی یک فرد در محافظت از جامعه سیاسی دموکراتیک پایه و اساس کار است؛ همان‌طور که حقوق عام بشر که هر شهروندی باید از آن‌ها برخوردار باشد، اساسی و بنیادی هستند. ECCE دموکراسی را تنها نظام سیاسی قادر به تأمین طیف کاملی از آزادی‌های شهروندی و سیاسی برای تک‌تک شهروندان و امنیت، برابری و عدالت می‌داند. ما دموکراسی را مجموعه‌ای از ارزش‌ها، نهادها و فرایندها می‌دانیم که مبشر صلح، توسعه، تحمل و مدارا، تکثرگرایی و جوامعی شایسته‌سالار است که به کرامت انسانی و دستاوردهای انسانی ارج می‌گذارند.

ما پروژه اصلی ECCE یعنی «آموزشکده توانا: آموزشکده مجازی برای جامعه مدنی ایران» را در سال ۲۰۱۰ تاسیس کردیم. آموزشکده توانا در ارائه منابع و آموزش در دنیای مجازی در ایران، یک نهاد پیشرو است. توانا با ارائه دوره‌های آموزشی زنده در حین حفظ امنیت و با ناشناس‌ماندن دانشجویان، به یک جامعه آموزشی قابل اعتماد برای دانشجویان در سراسر کشور تبدیل شده است. این دروس در موضوعاتی متنوع مانند نهادهای دموکراتیک، امنیت دیجیتال، حقوق زنان، وب‌نویسی، جدایی دین و دولت و توانایی‌های رهبری ارائه می‌شوند. آموزشکده توانا آموزش زنده دروس و سمینارهای مجازی را با برنامه‌هایی مثل مطالعات موردی در جنبش‌های اجتماعی و گذارهای دموکراتیک، مصاحبه با کنشگران و روشنفکران، دستورالعمل‌های خودآموز، کتابخانه مطالب توصیفی، ابزارهای کمکی و راهنمایی برای آموزشگران ایرانی و حمایت مداوم و ارائه مشاوره آموزشی برای دانشجویان تکمیل کرده است.

تلاش ما برای توسعه توانایی‌های آموزشکده توانا متوجه گردآوردن بهترین متفکران ایران و صداهای حذف‌شده است. به همین ترتیب، به دنبال انتشار و ارتقای آثار مکتوب روشنفکران ایرانی هستیم که ایده‌های آنان در جمهوری اسلامی ممنوع شده است.

یکی از نقاط تمرکز تلاش توانا، ترجمه متون کلاسیک دموکراسی و مقالات معاصر در این باره و نیز ترجمه آثار مرتبط با جامعه مدنی، حقوق بشر، حاکمیت قانون، روزنامه‌نگاری، کنشگری و فناوری اطلاعات و ارتباطات است. امید ما این است که این متون بتواند سهمی در غنای فردی هم‌وطنان ایرانی و برساختن نهادهای دموکراتیک و جامعه‌ای باز در ایران داشته باشد.

سپاسگزار بازتاب نظرات و پیشنهادهای شما!

فهرست

پیش‌گفتار

دوره آموزشی «حملات هک حکومتی پیشگیری، محافظت و واکنش مناسب» در بهار ۱۴۰۴ خورشیدی برگزار شد. این دوره ویژه کاربران و کنش‌گرانی است که در اینترنت فعال هستند و به واسطه نوع فعالیت‌شان در معرض هک حکومتی از سوی جمهوری اسلامی قرار دارند. به عبارت دیگر، این دوره آغازی است بر ایجاد دغدغه عمومی و توجه کنش‌گران سیاسی و مدنی به حملات شرورانه‌ای که جمهوری اسلامی ایران و دیگر بازیگران مستبد علیه کاربران و شهروندان خواهان تغییر، به اجرا می‌گذارند. بر همین اساس ما با تمرکز بر انواعی از حملات هکری توسط حکومت‌ها، نهادها یا هکرهای برخوردار از حمایت حکومتی و دولتی این بحث مهم را پیش برده‌ایم. در خلال دوره نیز با ذکر چندین مثال از عملیات واقعی هک علیه روزنامه‌نگاران، محققان و فعالان جامعه مدنی، به تدبیرها و ترفندهایی اشاره می‌شود که می‌توانند به محدودکردن خسارت‌های حملات هکری حکومتی و مقاومت در برابر آن کمک کنند.

اکنون درس‌نامه پیش رو، شامل متن آموزشی دوره، در قالب یک کتابچه در دسترس شما قرار می‌گیرد. امیدواریم با راهکارهای ارائه‌شده در این مجموعه، بتوانیم قدمی در مسیر افزایش آگاهی کاربران و کنش‌گران فعال در حوزه‌های مختلف در مقابله با هک‌های حکومتی برداشته باشیم.

درس نخست
مقدمه‌ای بر حملات هکری حکومت‌های اقتدارگرا

دولت یا حکومت در این درس‌نامه به مجموعه‌ای از نهادها اطلاق می‌شود که مراکز امنیتی، قوای قهریه و دادگاه‌ها را در اختیار دارد و می‌تواند از امکاناتی نظیر زیرساخت شرکت‌های تلفن همراه یا پلیس فضای مجازی - مثلا برای دستیابی به داده‌های مربوط به فعالیت آنلاین کاربران یا نهادهای مدنی - استفاده کند. همان‌طور که می‌بینید، در این‌جا حکومت یا دولت می‌تواند، حتی به اشکال مردم‌سالار حکومت اطلاق شود. چراکه در بسیاری از کشورهای مردم‌سالار هم، نهادهای قانونی و تحت نظارت نمایندگان منتخب مردم در پارلمان، در بسیاری از موارد - مثل جرائم سازمان‌یافته - خواستار دسترسی به داده‌های بسیاری از شهروندان یا نهادهای حامی حقوق آن‌ها می‌شوند.

بر خلاف جوامع آزاد که در آن، چنین دسترسی‌ای نیازمند احکام قضایی و ساز و کارهای مستحکم حقوقی است، نظام‌های تمامیت‌خواه و اقتدارگرا، اساسا حقی برای شهروندان در زمینه حفظ و حفاظت از داده‌ها و فعالیت دیجیتال‌شان قائل نیستند.

۵ روش حکومت‌های اقتدارگرا برای محدودسازی اینترنت و نقض حریم خصوصی

۱- فیلترینگ، قطع یا کندی اینترنت و ایجاد اختلال در دسترسی آزاد شهروندان به اطلاعات آزاد و جهانی.

۲- الزام کاربران اینترنت و موبایل به ثبت‌نام دستگاه‌های هوشمند خود با استفاده از نام و کد ملی، آدرس و دیگر مشخصات فردی.
۳- تملک بر و سوءاستفاده از زیرساخت‌های مخابراتی و حتی شرکت‌های به‌ظاهر خصوصی ارائه‌کننده خدمات موبایل و اینترنت، که در واقع همه مرتبط با نهادهای دولتی و مخصوصا نظامی‌اند.
۴- الزام ارائه‌کنندگان خدمات اینترنت و موبایل به ذخیره تمام فعالیت‌های آنلاین یا موبایلی کاربران برای مدت طولانی.
۵- سوءاستفاده از دسترسی به زیرساخت‌های اینترنت و موبایل برای نفوذ، مراقبت و سرقت داده‌های کاربران.

بحث ما در این کتابچه بر موارد دوم تا پنجم، متمرکز است، خصوصا شیوه‌هایی که در سال‌های گذشته به شکلی روبه‌رشد و فزاینده توسط جمهوری‌اسلامی علیه فعالان مدنی و کنش‌گران استفاده شده است.

جمع‌آوری اطلاعات و رصد رقبا، برای حکومت‌ها همواره از ارزشی بسیار بالا برخوردار بوده است. در قرن بیستم، با ظهور نخستین ابزارهای الکترونیک، دولت‌ها، طیف گسترده‌ای از این ابزارها را با هدف شنود، تعقیب و مراقبت، و به صورت کلی - جمع‌آوری اطلاعات - به کار گرفتند.

تکنولوژی شنود مکالمات تلفنی، رمزگشایی از ارتباطات رادیویی و نصب میکروفن‌های بسیار کوچک در سال‌های آغازین قرن بیستم و بعد از آن، کنترل رفت‌وآمد از طریق نصب دوربین در مناطق مختلف یا استفاده از تکنولوژی‌های جدیدتری چون ماهواره، همه و همه در خدمت دستیابی دولت‌ها به اطلاعات حساس و ذی‌قیمت قرار گرفتند.

با ظهور و همگانی‌شدن اینترنت در سال‌های پایانی قرن بیستم و ظهور شبکه‌های اجتماعی در دهه آغازین قرن ۲۱ میلادی، حجم اطلاعات برآمده از تعاملات دیجیتال شهروندان سطح نادیده‌ای از رشد انفجارگونه را تجربه کرد.

در این میان استفاده از تکنولوژی دیجیتال توسط کاربران، به‌روشنی موجبات نگرانی دولت‌ها - خصوصا پلیس و دستگاه‌های امنیتی - را فراهم‌آورد. نگرانی‌های به‌جا و موجهی، دولت‌ها را به مطالعه قوانین و راهکارهایی برای تضمین امنیت و حفاظت از شهروندان وا

داشت. از جمله «نگرانی از سلامت دیجیتال کودکان» و «امکان سوءاستفاده تبهکاران از امکانات دنیای دیجیتال در دنیای آزاد و قانون‌مدار».

حکومت‌های اقتدارگرا و مستبد اما، تمام توان خود را برای توقف «گردش آزاد اطلاعات» در دنیای دیجیتال به کار گرفتند. در این میان فعالان مدنی، وکلا، فعالان حقوق بشر و تمام شهروندانی که قصد بهره‌گیری از اینترنت برای بیان مطالبات خود را داشتند، هدف ایجاد محدودیت و سانسور در دنیای مجازی، ارعاب آنلاین و حملات هکری دولتی قرار گرفتند.

در آغاز قرن بیست‌ویکم این نوع حملات، مرزهای سیاسی قدرت‌های اقتدارگرا عبور کرده و ارعاب دیجیتال منتقدان، شکلی بین‌المللی پیدا کرد. حکومت‌های اقتدارگرا یا تمامیت‌خواه، معمولا به شیوه‌ای مستقیم یا غیرمستقیم ارتباطات الکترونیک، موبایل و اینترنت کشورهای خود را کنترل می‌کنند. در جمهوری اسلامی ایران، حکومت، تمام اشکال ارتباطات الکترونیک را از طریق درگاه‌های ورود و خروج داده، مخابرات و شرکت ارتباطات زیرساخت کنترل می‌کند. همچنین همه شرکت‌های ارائه‌دهنده خدمات اینترنت ثابت و موبایل نیز به صورتی آشکار یا پنهان در اختیار حکومت‌اند.

طی مباحث آتی کتابچه، اشکال متفاوتی از سوءاستفاده حکومت‌های بسته - نظیر جمهوری اسلامی ایران - از زیرساخت‌های الکترونیک را به تفصیل شرح خواهیم داد.

۵ هدف اصلی سوءاستفاده حکومت‌های بسته از زیرساخت‌های الکترونیک

لازم به یادآوری است که در بیش‌تر حملات هکری علیه فعالان یا گروه‌های مطالبه‌گر، عموما هر ۵ راهبرد به صورت ترکیبی دنبال می‌شود.

۱- مراقبت و رصد فعالیت

فرض کنید فردی از داخل یک سازمان بازرگانی دولتی تصمیم به افشای موارد سوءاستفاده و اختلاس گرفته است. او با گروهی از روزنامه‌نگاران یا فعالان مدنی از طریق ایمیل و تلگرام در تماس است تا فایل‌های پی.دی.اف مربوط به اختلاس، تصاویر و همچنین فایل صوتی مکالماتِ پرداخت رشوه به مدیران را در اختیار کنش‌گران قرار دهد. طبعا در این مورد حکومت با شنود، هک جی‌میل و تلاش برای نفوذ به تلفن همراه و کامپیوترهای شخصی

کنش‌گران، به دنبال شناسایی منبع اطلاعات، بازداشت او و امحای تمام اطلاعات و از آن مهم‌تر جلوگیری از درز آن به عرصه عمومی خواهد بود.

۲- آزار و ارعاب

در مورد پیشین، یعنی تماس و همکاری با فردی از داخل یک سازمان دولتی که قصد افشای فساد و رشوه را دارد، هم، فرد افشاگر و هم کنش‌گران مرتبط با او می‌توانند هدف آزار و ارعاب از طریق هک باشند. مثلا با افشای عکس‌ها و ویدئوهای خصوصی و تخریب شخصیت از طریق شبکه‌های اجتماعی.

یکی از رایج‌ترین اشکال این نوع آزار، هک ایمیل، تلفن همراه، شبکه‌های اجتماعی و پیام‌رسان‌های فرد مورد نظر و سپس افشای بخشی از آن اطلاعات در فضای آنلاین با هدف ایجاد مشکل برای قربانی در حوزه‌هایی مانند روابط خانوادگی، اجتماعی، شغلی و مواردی از این دست است.

۳- ایجاد اخلال یا توقف فعالیت‌های آنلاین نامطلوب از نظر حکومت

تصور کنید یک سایت خبری - تحلیلی یا یک حساب تلگرام پرمخاطب به دلیل انتشار اسناد و موارد نقض حقوق بشر در ایران، مورد توجه رسانه‌ها و مجامع بین‌المللی قرار گرفته و مخاطبان بسیاری دارد. در اشکال مشابه، طیف گسترده‌ای از حملات هکری مثلا برای به‌دست‌آوردن و سرقت دامنه یا حساب تلگرام صورت می‌پذیرد. همچین دسترسی به هاست یا فضای میزبانِ سایت و همچنین حملات موسوم به DDOS برای پایین‌آوردن و ازکارانداختن سرور از جمله روش‌های بسیار مرسوم حکومت‌های اقتدارگرا برای خاموش‌کردن صدای مخالفان است.

۴- بدنام‌کردن فعالان و منتقدان و خدشه‌واردکردن به اعتبار آن‌ها

در این مورد، هنگام بحث پیرامون آزار و اذیت آنلاین قدری صحبت کردیم. اما به طور خلاصه کنش‌گران و چهره‌های برخوردار از اعتماد و علاقه شهروندان همواره در معرض چنین حملاتی قرار دارند. به این معنا که با هک و کنکاش آنلاین داده‌های شخصی ایشان مثلا ایمیل، اسنادی به صورتی بعضا دستکاری‌شده در فضای عمومی با هدف بدنام‌کردن و

خدشه واردکردن به اعتبار فعال مورد حمله منتشر می‌شود. در اکثر موارد، این اسناد قصد دارند از کنش‌گر مزبور چهره‌ای غیرقابل اعتماد، حریص، طمع‌کار و فردی ترسیم کنند که به دلایلی چون منفعت مالی دست به اعتراض و مطالبه‌گری زده است.

۵- ایجاد خسارت از طریق ضربات حقوقی و مالی

ایجاد خسارت و دفن‌کردن کنش‌گران زیر انبوهی از مشکلات حقوقی و مالی، بدهی، عوارض مالیاتی با اهداف سیاسی و هزینه‌های دادگاه و نظایر آن، یکی از مرسوم‌ترین ترفندهای حکومت‌های سرکوبگر است که از آن در سال‌های اخیر به طرز فزاینده‌ای به جای سرکوب سخت و مستقیم استفاده می‌شود. هکِ مکاتبات درونی یک نهاد یا سازمان مدنی، می‌تواند به دستگاه‌های امنیتی برای پیداکردن انواع مستمسک در پوشش حقوقی یا مالیاتی و نظایر آن کمک کند.

آزمون ارزیابی

لطفا با دقت به پرسش‌ها پاسخ دهید. این کار کمک می‌کند درک خود از مطالب درس را ارزیابی کنید. پاسخ‌های درست در بخش پاسخ‌نامه در پایان کتاب در دسترس است.

۱- «هک ایمیل، تلفن همراه، شبکه‌های اجتماعی و پیام‌رسان‌های قربانی و سپس افشای بخشی از اطلاعات او در فضای آنلاین با هدف ایجاد مشکل برایش در حوزه‌هایی مانند روابط خانوادگی، اجتماعی، شغلی و مواردی از این دست». عبارت قبل، مصداق کدام نوع سوءاستفاده است؟

الف) ایجاد خسارت از طریق ضربات حقوقی

ب) بدنام‌کردن و خدشه‌واردن‌کردن به اعتبار فعالان

ج) مراقبت و رصد فعالیت

د) آزار و ارعاب

۲- کدام گزینه صحیح است؟

الف) در جمهوری اسلامی حدود سه‌چهارم از شرکت‌های ارائه‌دهنده خدمات اینترنت ثابت و موبایل در اختیار حکومت‌اند.

ب) در جمهوری اسلامی همه شرکت‌های ارائه‌دهنده خدمات اینترنت ثابت و موبایل در اختیار حکومت‌اند.

ج) جمهوری اسلامی توان نظارت مستقیم بر همه شرکت‌های ارائه‌دهنده خدمات اینترنت ثابت و موبایل را ندارد.

د) جمهوری اسلامی توان نظارت غیرمستقیم (نامحسوس) بر همه شرکت‌های ارائه‌دهنده خدمات اینترنت ثابت و موبایل را ندارد.

۳- هک مکاتبات رسمی و درونی یک نهاد یا سازمان مدنی، چگونه می‌تواند به دستگاه‌های امنیتی کمک کند؟

الف) پیداکردن انواع مستمسک در پوشش حقوقی یا مالیاتی و نظایر آن

ب) زمینه‌سازی طیف گسترده‌ای از حملات هکری برای به‌دست‌آوردن و سرقت

دامنه یا حساب تلگرام
ج) افشای موارد سوءاستفاده و اختلاس در میان مخالفان
د) افشای تصاویر خصوصی، ویدئوهای خصوصی و تخریب شخصیت افراد و سازمان

درس دوم
دسته‌بندی حملات هکری حکومت‌های اقتدارگرا

۲ هدف اصلی نظام‌های اقتدارگرا برای هک منتقدان

حملات هک حکومتی یا دولتی، به صورتی بسیار ساده، دو هدف اصلی و مشخص را دنبال می‌کنند:

۱- هک حکومتی برای این انجام می‌شود که کنش‌گران و منتقدان، فعالیت در فضای دیجیتال و اساسا عرصه فعالیت مدنی را برای همیشه ترک کنند. مثلا یک کانال تلگرامی با چند میلیون مخاطب هک شود تا گردانندگان آن، فعالیت آنلاین و سپس غیرآنلاین خود را به‌کل کنار بگذارند.

۲- دوم این‌که آسیب فعالیت آنلاین منتقدان و کنش‌گران به نظام مستبد و اقتدارگرا را کاهش دهند. مثلا با دسترسی به محتوای چت‌های خصوصی گردانندگان آن کانال تلگرام، قبل از انتشار مدارکی که می‌تواند برای دولت و حکومت ایجاد مشکل کند، منابع، شناسایی و بازداشت شوند و از افشای بیش‌تر موارد جلوگیری شود.

متداول‌ترین نوع حملات علیه فعالان جامعه مدنی در ایران، مانند نیزه‌ای طراحی شده که برای هدف قراردادن یک فعال سیاسی-اجتماعیِ خاص یا یک نهاد، موسسه، روزنامه و

رسانه منتقد حکومت، به کار می‌رود.

نوک پیکان این نیزه، ۳ ضلع دارد:

۱- ضلع اول، سوءاستفاده از امکانات زیرساختی دولتی، مثلا دسترسی به پیامک‌های ردوبدل‌شده همه کاربران ایرانی است.

۲- ضلع دوم، مطالعه عمیق حفره‌ها و آسیب‌پذیری‌های ابزارهای فنی مورد استفاده کاربران مثلا ایمیل است. دولت‌های مستبد محدودیت مالی یا قانونی چندانی در استخدام هکر و شناسایی روش‌های نفوذ به تلفن یا ایمیل شهروندان ندارند. حکومت ایران بارها تلاش کرده است که گواهینامه‌های بین‌المللی و امنیتیِ مثلا شرکت Google را جعل کند و به حساب‌های کاربری شماری از کاربران نفوذ کند.

۳- ضلع سوم و مهم‌ترین ضلع این حملات، مهندسی اجتماعی یا فریب است. تقریبا همه حملات هکری بر بستری از فریب بنا می‌شوند. مثلا به جای هک حساب یک فعال اجتماعی یا روزنامه‌نگار، تلفن مادر سالخورده او هک می‌شود و از طریق ارسال لینک آلوده از تلفن مادر، این بار مهاجمان موفق به نفوذ در تلفن هوشمند او می‌شوند.

فیشینگ؛ متداول‌ترین نوع حملات علیه فعالان و منتقدان در ایران

فیشینگ را می‌توان خیلی ساده به ماهیگیری با استفاده از طعمه تشبیه کرد. تقریبا در همه انواع مختلف فیشینگ بر اساس اشکالی بعضا پیچیده از فریب، طراحی می‌شوند. مثلا در نیمه‌های شب، زمانی که بسیار خواب‌آلود هستید، پیامکی را دریافت می‌کنید که به‌ظاهر، دوستی قابل اعتماد برای شما نوشته است. با این مضمون که تصاویر بسیار خصوصی شما در تلگرام یا ایکس پخش شده. شوک و ضربه دریافت این پیامک، چنان شدید است که شما بدون لحظه‌ای تامل، روی لینک داخل پیامک کلیک می‌کنید. بلافاصله با صفحه اصلی شبکه اجتماعی «ایکس»، «تلگرام» یا «جی‌میل» مواجه می‌شوید که از شما می‌خواهد برای اطمینان بیش‌تر رمز عبور یا کد تلفن خود را وارد کنید. این معمول‌ترین شکل حملات موسوم به فیشینگ است.

اجازه دهید درباره این نوع از حمله هکری بیش‌تر بحث کنیم. با این سوال می‌توانیم بحث را پیش ببریم که چند عنصر فریب در این حمله که مثال زدیم قابل شناسایی است؟

۱- نیمه‌شب از آن جهت انتخاب شده که خواب‌آلودگی و اضطرار، هشیاری و شک

شما را کاهش می‌دهد. شاید اگر این پیامک در طول روز برای شما ارسال شده بود، بلافاصله پس از دریافت آن به دوست ارسال‌کننده‌تان زنگ می‌زدید.
۲- تصاویر بسیار خصوصی از آن جهت عنوان می‌شود که مانند یک ضربه شوک‌آور، تمرکز و شک و تردید شما را از بین می‌برد تا شما را وادار به عکس‌العمل سریع و نسنجیده کنید.
۳- لینکی که از شما خواسته می‌شود روی آن کلیک کنید، سایت و گذرگاهی تقلبی است اما بسیار شبیه به سایت‌های اصلی مثلا ایکس، تلگرام یا جی‌میل طراحی شده. به طوری که اگر بسیار ریز به آدرس آن سایت دقت کنید، می‌بینید که تفاوتی بسیار جزئی با آدرس اصلی سایت‌های ایکس، تلگرام یا جی‌میل دارد. اما تفاوتی که برای ۹۹ درصد کاربران در حالت عادی - بدون مطالعه جزئیات کامل صفحه - قابل تشخیص سریع نیست.

انواع حملات فیشینگ، بسته به قربانی و هدف

برای حملات موسوم به فیشینگ انواع و اقسام دسته‌بندی‌های مختلف وجود دارد. مثلا بسته به انتخاب قربانی و هدف حمله فیشینگ، سه دسته‌بندی عمومی برای این نوع حمله هکری وجود دارد.

۱- فیشینگ

در فیشینگ جمع بسیار زیاد و غیرهدفمندی از قربانیان انتخاب می‌شوند. فرض کنید یک کانال تلگرامی سرگرمی هک شده است، برای همه هزاران اعضای این کانال، یک لینک آلوده ارسال می‌شود مانند تور ماهیگیری و تعدادی از دریافت‌کنندگان، روی لینک کلیک می‌کنند و مثلا پسورد جی‌میل خود را در سایت فیشینگ و جعلی‌ای که بسیار هم شبیه جی‌میل اصلی است، وارد می‌کنند و در نتیجه، آن را از دست می‌دهند.

۲- فیشینگ هدفمند با نیزه یا Spear-Phishing

در این‌جا بر خلاف فیشینگ عمومی، قربانی و هدف از ابتدا انتخاب شده و به جای تور ماهیگیری از چیزی مثل نیزه برای شکار او استفاده می‌شود. قربانی می‌تواند یک کنش‌گر، یک نهاد مدنی یا یک رسانه باشد. مثلا برای یک روزنامه‌نگار منتقد، ایمیلی به‌ظاهر موجه - اما جعلی - از یک

نهاد بین‌المللی مثل سازمان عفو بین‌الملل ارسال می‌شود که در آن از نامزدی روزنامه‌نگار برای دریافت جایزه‌ای بین‌المللی خبر داده می‌شود. در این ایمیل دو فایل ورد و پی.دی.اف وجود دارد که از قربانی خواسته شده که قبل از دریافت جایزه، آن را مطالعه کند. به محض بازشدن، این دو فایل آلوده کاملا کنترل تلفن هوشمند و کامپیوتر قربانی را در اختیار می‌گیرند.

۳- صید نهنگ یا Whale Phishing

صید نهنگ، نوع خاصی از مورد دوم یا فیشینگ با نیزه است که در آن قربانیِ انتخاب‌شده، فردی بسیار مهم و شاخص است. مثلا رهبر یک حزب منتقد یا یک ناراضی سرشناس. انتخاب او از این جهت صورت می‌گیرد که پس از دستیابی به تلفن یا کامپیوترِ نهنگ یا طعمه سرشناس، به‌راحتی می‌توان در پوشش هویت او برای شمار زیادی از فعالان منتقد لینک و فایل‌های آلوده فرستاد و اطلاعاتی را که به طرق معمولی قابل دسترسی نیست را با جعل هویت و پوشش فردِ شاخص و مهم، به دست‌آورد.

علاوه بر سه تقسیم‌بندی قبلی، به لحاظ متد، شیوه و ابزار مورد استفاده، ۶ نوع فیشینگ وجود دارد که در ادامه به آن‌ها می‌پردازیم.

۶ شیوه عمده برای حملات فیشینگ

۱- فیشینگ با ایمیل

در این روش، ایمیلی به دقت طراحی و برای قربانی ارسال می‌شود. معمولا در موضوع ایمیل عنوانی حساس و بسیار فوری به چشم می‌خورد مثل این‌که: «بانک شما هک شده» یا «یک پاکت پستی منتظر دریافت توسط شما ست» و عناوینی از این دست. در این ایمیل، یا لینک‌های آلوده‌ای وجود دارد که شما را به سایتی شبیه جی‌میل یا بانک الکترونیکی و غیره‌تان رهنمون می‌کند یا فایل‌های آلوده‌ای مثلا با فرمت ورد و موارد مشابه ضمیمه شده‌اند که دستگاه تلفن هوشمند یا کامپیوتر شما را آلوده می‌کنند.

۲- فیشینگ با پیامک یا پیام‌رسان

در این مورد که مشابه ایمیل ناامن است، این بار پیامی به صورت SMS یا پیامی در واتس‌اپ، تلگرام و دیگر پیام‌رسان‌ها برای شما ارسال می‌شود که مثلا از شما می‌خواهد کد

دریافتی از شرکت گوگل را وارد کنید. این پیام می‌تواند از سوی ارسال‌کننده‌ای ناشناس باشد یا یکی از دوستان و از طرف آشنایان شما، که قبلا توسط مهاجمان هک شده است.

۳- فیشینگ با استفاده از شبکه‌های اجتماعی

در این نوع از حمله فشینیگ، انواع و اقسام حیله‌ها مثلا استفاده از تصاویر جذاب جنسی یا حساب‌های کاربری‌ای شبیه به دوستان نزدیک شما مورد سوءاستفاده قرار می‌گیرند و با ارسال لینک یا فایلِ آلوده هک می‌شوید.

مانند موارد قبلی در این نوع از حملات هم، ممکن است مهاجمین به جای هک مستقیم شما، اول حسابِ مثلا اینستاگرام مادربزرگ یا شوهرخاله شما را هک کنند و بعدا از آن حساب هک‌شده، برای شما فایل و لینک آلوده ارسال کنند. عملی که با هدف جلب اعتماد شما و ترغیب شما به کلیک‌کردن روی طعمه طراحی شده است.

۴- فیشینگ صوتی

در این مورد، فردی ناشناس حتی با تقلید صدای افراد آشنا، سعی می‌کند خود را کارمند بانک یا اداره مالیات یا حتی از نزدیکان شما معرفی کند و مثلا پسورد دومرحله‌ای تلگرام یا جی‌میل شما را طی یک تماس صوتیِ تلفنی یا در یک پیام‌رسان از شما مطالبه می‌کند. این‌جا هم همان ترفندهای فریب و مهندسیِ اجتماعی استفاده می‌شود. مثلا ادعا می‌شود «حساب شما هک شده است و ما به رمز عبور تلفنی شما فورا نیاز داریم».

۵- فیشینگ با وای‌فای یا آلوده‌کردن DNS

نوع بسیار خطرناک از انواع فیشینگ، سوءاستفاده از وای‌فای است. مثلا فردی با یک دستگاه وای‌فای تقلبی و با اسم و شناسه وای‌فایی دقیقا شبیه دفتر یک نهاد مدنی یا منزل یک کنش‌گر در کنار پنجره خانه قربانی کمین می‌کند، به محض بازگشت قربانی به منزل، ممکن است او تصادفا تلفن یا کامپیوتر خود را به آن وای‌فای متصل کند و از آن‌جا به بعد راه برای مهاجم برای دزدیدن پسوردهای شما یا انتقال شما به سایتی قلابی و در ظاهر شبیه جی‌میل هموار می‌شود. همین کار می‌تواند بدون دخالت دستگاه وایرلس و با آلوده‌کردن DNS یا سرویس نشانی‌دهی دستگاه‌های شما صورت پذیرد. با دستکاری

این سرویس، مثلا پس از دریافت فایلی آلوده، مهاجم می‌تواند از این پس شما را به جای Google مثلا به سایتی آلوده و تقلبی به نام Gooogle۱ (گوگل‌وان) بفرستد و رمزعبور شما را به سرقت برد.

۶- فیشینگ مرد میانی یا Man-in-the-Middle

این روش، نوع پیچیده‌ای از حملات فیشینگ است که بارها در ایران توسط حکومت انجام شده است. در این مورد ارتباط امن مثلا میان کامپیوتر یا تلفن همراه شما با سرورهای شرکت گوگل یا اینستاگرام از شرکت متا، مختل می‌شود و شما به جای اتصال مستقیم به گوگل، متا، تلگرام و غیره، به دستگاه‌های شنود میانی یک نهاد امنیتی برخوردار از پشتیبانی حکومت متصل می‌شوید، و تمام اتصالات و ارسال و دریافت ایمیل‌ها و دیگر داده‌های شما، توسط مرد میانی ضبط و کنترل می‌شود. البته در بسیاری از این موارد چنانچه در جلسات بعدی توضیح خواهیم داد، گوگل و دیگر شرکت‌های تکنولوژی شناخته‌شده، کاربران خود در ایران را از چنین حملاتی مطلع می‌کنند.

آزمون ارزیابی

لطفا با دقت به پرسش‌ها پاسخ دهید. این کار کمک می‌کند درک خود از مطالب درس را ارزیابی کنید. پاسخ‌های درست در بخش پاسخ‌نامه در پایان کتاب در دسترس است.

۱- یک گروه هکری سازمان‌یافته، دستگاه آنلاین مادر یک روزنامه‌نگار را هک می‌کند و از آن طریق به اطلاعات آن روزنامه‌نگار دست می‌یابد. با توجه به این اطلاعات، این روش مصداق کدام نوع حمله است:

الف) هک مستقیم

ب) فیشینگ

ج) مهندسی اجتماعی و فریب

د) فیشینگ یا نفوذ استروترفینگ

۲- کدام مورد برای یک حمله فیشینگ درست است؟

الف) حمله‌کننده همواره ساعات شلوغ روز را برای حمله انتخاب می‌کند تا افراد متوجه حمله نشوند.

ب) حمله‌کننده نیمه‌شب را برای حمله انتخاب می‌کند تا افراد هشیاری کم‌تری داشته باشند.

ج) حمله‌کننده از واردکردن شوک اجتناب می‌کند تا کسی مشکوک نشود.

د) حمله‌کننده فقط از یک عنصر فریب استفاده می‌کند تا کسی مشکوک نشود.

۳- فردی ناشناس، سعی می‌کند خود را کارمند بانک یا اداره مالیات یا حتی از نزدیکان شما معرفی کند و پسورد دومرحله‌ای تلگرام یا جی‌میل شما را طی یک تماس صوتیِ تلفنی یا در یک پیام‌رسان از شما مطالبه می‌کند. کدام مطلب درست است؟

الف) این نمونه‌ای از فیشینگ مرد میانی است.

ب) این نمونه‌ای از فیشینگ با ایمیل است.

ج) این نمونه‌ای از فیشینگ صوتی است.
د) این نمونه‌ای از فیشینگ نیست.

درس سوم
مطالعه موردی ۲ حمله هکری جمهوری اسلامی

مهم‌ترین حربه حکومت‌های سرکوبگر برای سرکوب مخالفان، ارعاب آنان است. آن‌ها تلاش می‌کنند تک‌تک فعالان و منتقدان را از هر نوع استفاده و فعالیت در دنیای دیجیتال و ابزارهای آن بترسانند. مثلا جمهوری اسلامی ایران بارها ادعا کرده است که به همه محتوای ایمیل کاربران اینترنت دسترسی دارد، همه فعالیت‌های آنلاین آنان را کنترل می‌کند، هویت همه صاحبان حساب در شبکه‌های اجتماعی را در اختیار دارد و ده‌ها ادعای گزاف و غیرواقعی و مشابه دیگر.

مطالعه موردی ده‌ها مورد از آزار و اذیت حکومت علیه کاربران به ما می‌گوید آنچه مثلا به «افشای هویت کاربران ناشناس ایرانی» انجامیده است، نه توانایی‌های خارق‌العاده، عجیب و مخوف حکومت، که غالبا سهل‌انگاری، ندانم‌کاری و اشتباهات مکرر خود این کاربران است. مثلا آن‌ها با شرکت در یک پویش اینترنتی، تصویری را منتشر کرده‌اند که پاره‌ای از مشخصات محل سکونت، کار یا خودروی شخصی‌شان در آن پیدا بوده است.

مواردی که در ادامه می‌آیند همه از رویدادهای واقعی و تلاش جمهوری اسلامی ایران برای هک فعالان منتقدی انتخاب شده که نامِ واقعی‌شان حذف شده است.

۱- تماس تلفنی فوری برای به‌دست‌آوردن حساب گوگل یک کنش‌گر

تلفن یک فعال شناخته‌شده رسانه‌ای مدنی در نیمه‌های شب زنگ می‌خورد، فردی از پشت خط نام او را میان همهمه و شلوغی صدا می‌کند و به‌سرعت می‌گوید: من الان در فرودگاه گیر کرده‌ام و تلفن خودم مشکل پیدا کرده، لطفا محبت کنید الان کدی را که از سمت شرکت گوگل برای من قرار بوده ارسال شود را همین الان بخوانید. اما آیا می‌دانید این‌جا، ما با چه نوع حمله‌ای طرفیم و از حمله‌کنندگان چه می‌دانیم؟ با توضیح ۴ نکته این سوال را پاسخ می‌دهیم:

الف) حمله‌کنندگان قصد نفوذ به حساب گوگل فرد مورد نظر را دارند. برای همین به کدی که سیستم تایید هویت دومرحله‌ای گوگل برای صاحبان اکانت ارسال می‌کند، نیاز دارند.

ب) حمله‌کنندگان به شکلی رمز عبور و شناسه قربانی را به دست آورده‌اند، چون بدون دراختیارداشتن رمز عبور، گوگل کد تایید هویت را ارسال نمی‌کند.

ج) حمله‌کنندگان، «نیمه‌شب»، «همهمه»، «اضطرار» و «نوع‌دوستی قربانی»، همه و همه را ابزار فریب و مهندسی اجتماعی کرده‌اند تا قربانی به دلیل خستگی یا خواب‌آلودگی و ایجاد جو اضطراری و میل درونی کمک به هم‌نوع، دستپاچه شده و کد را در اختیار فرد آن سوی خط تلفن قرار دهد.

د) پس از دریافت کد، آن‌ها رمز عبور - و از آن مهم‌تر - شماره تلفن سیستم تایید هویت دومرحله‌ای گوگل قربانی را به‌سرعت تغییر خواهند داد و بلافاصله تمام داده‌های او را دانلود و سرقت خواهند کرد. تمام ایمیل‌ها، چت‌ها، تصاویر گوگل‌فوتوز، سابقه و تاریخچه جستجو، سابقه و تاریخچه مرورگر کروم و از طریق Google Map Timeline هم تمام نقاطی را که قربانی در همه ساعات روز و شب در حرکت بوده و بسیاری اطلاعات دیگر را از این راه به دست می‌آورند.

۲- دریافت ایمیل جعلی از یک چهره شناخته‌شده

سه فعال مدنی، مشغول به کار در یک نهاد بزرگ، شناخته‌شده خیریه و مدنی‌اند. ما این سه فعال را امید، الهام و رضا نامیده‌ایم. الهام مدیر نهاد مدنی است. جی‌میل او حاوی حساس‌ترین موارد مثلا ارتباطات شخصی او، مکاتبات‌اش با نهادهای بین‌المللی و

رسانه‌های جهانی و همچنین لیست کامل دریافتی، پرداختی و کمک‌های مردمی است. رضا مسئول ارتباطات است و با رسانه‌های داخلی و خارجی، با فعالان، اینفلوئنسرها، سلبریتی‌ها و دیگران از طرق مختلفی - از تلفن گرفته تا پلتفورم‌هایی چون اینستاگرام، تلگرام و واتس‌اپ - در ارتباط است. امید نسبت به دیگران اطلاعات فنی بیش‌تری دارد. او مسئول پیکربندی و تنظیمات مودم وایرلس دفتر، کامپیوترها و چاپگرها ست.

قبل از دیگران، رضا ایمیلی از یک چهره شناخته‌شده خارجی دریافت می‌کند که برای سازمانی معتبر مشغول فعالیت است. فعال رسانه‌ای شناخته‌شده، خبر بسیار خوبی را با رضا به اشتراک گذاشته و آن این است که نهاد آن‌ها برنده جایزه‌ای بزرگ و بین‌المللی شده است.

او در این ایمیل از رضا خواسته است که به سایت موسسه آنان سر بزند و در یک نظرسنجی شرکت کند. رضا بلافاصله در این نظرسنجی شرکت می‌کند. در آخرین مرحله از نظرسنجی و پس از ارسال پاسخ به سوالات، از رضا خواسته می‌شود تا پرسش‌ها را در فایلی با فرمت مایکروسافت‌ورد دانلود و برای دو همکار دیگر خود یعنی الهام و امید ارسال کند.

۷ نکته در بررسی این حمله

۱- فردی در جایگاه یک فعال سرشناس ظاهر شده است.

۲- مهاجمان، وب‌سایتی با ظاهری کاملا معتبر و قابل اعتماد را طوری طراحی کرده‌اند که اگر رضا یا هر فرد دیگری برای اطمینان از هویت فریبنده ارسال‌کنندگان ایمیل، قصد تحقیق داشته باشد، این بررسی منجر به ایجاد شک و شبهه نشود.

۳- در داخل این وب‌سایت نام افرادی شناخته‌شده و قابل اعتماد به عنوان مدیران و دست‌اندرکاران طرح آمده است تا بیش‌تر اعتمادزایی شود.

۴- صحبت از اعطای جایزه‌ای مهم و بین‌المللی است که بلافاصله به ابراز احساسات و شادمانی دریافت‌کنندگان خبر می‌انجامد بدون آن‌که تردید چندانی راجع به راست‌آزمایی آن به خود راه دهند.

۵- ایجاد تماس از کانال رضا که به دلیل موقعیت خود نخستین رابط سازمان با دنیای بیرون است، انجام شده. پس از این تماس، دیگران آدرس وب‌سایت آلوده و فایل‌های

آلوده را از دوست و همکار خود - یعنی رضا - دریافت خواهند کرد و به همین دلیل با اعتماد بیش‌تری به وب‌سایت مراجعه کرده یا فایل‌ها را باز خواهند کرد.
۶- وب‌سایتی که از او درخواست شده تا برای نظرسنجی از آن طریق اقدام کنند، حامل کدهای آلوده‌ای است که کامپیوتر یا تلفن هوشمند فردِ مراجعه‌کننده را به نوعی بدافزار آلوده خواهد کرد.
۷- فایل‌های اتصال‌داده‌شده هم همگی آلوده‌اند. این فایل‌ها انواع خاصی از بدافزارها را روی دستگاه‌های قربانی نصب خواهند کرد که در همین بخش درباره آن بیش‌تر توضیح خواهیم داد.

۳ نوع بدافزار برای هک

۱- بدافزارهای دسترسی از راه دور یا Remote Access

نرم‌افزار الصاق‌شده، خیلی راحت دسترسی از راه دور را روی کامپیوتر قربانی ایجاد خواهد کرد. این امکانی است که سیستم‌های عامل - مثلا برای دسترسی شرکت‌های سرویس‌دهنده از راه دور - یا خود کاربران وقتی در خانه یا دفتر نیستند، ایجاد کرده‌اند اما در این‌جا به صورت غیرمجاز، فرد مهاجم از بیرون کنترل صددرصدی کامپیوتر شما را در دست می‌گیرد. مثلا می‌تواند از راه دور دوربین شما را روشن کند یا از صفحه دستگاه شما اسکرین‌شات بگیرد یا همه فایل‌های شما را روی دستگاه خود دانلود کند و فایل‌های آلوده بیش‌تری را روی دستگاه شما آپلود کند. همچنین او می‌تواند نرم‌افزار کروم یا واتس‌اپ شما را باز کرده و با همه دوستان‌تان به اسم شما گفت‌وگو کند.

۲- بدافزارهای موسوم به Key Loggers

این بدافزار خیلی ساده هر کلیدی را که روی کی‌بورد کامپیوتر یا صفحه نمایش موبایل یا تبلت شما فشار داده شود، به صورت رشته‌ای شبیه به ایمیل برای فرد مهاجم ارسال می‌کند. فرض کنید شما کامپیوتر را روشن می‌کنید و رمز عبور خود را وارد می‌کنید. او بلافاصله این رمز عبور را دریافت می‌کند. بعد شما برای واردشدن به جی‌میل، شناسه و رمز عبور خود و حتی سیستم تایید هویت دومرحله‌ای را وارد می‌کنید. او همه این اطلاعات را بلافاصله دریافت می‌کند و وارد جی‌میل شما می‌شود.

۳- بدافزارهای موسوم به روزِ صفر یا Zero-Day Exploits

یکی از فایل‌های ارسال‌شده برای رضا، حاوی بدافزاری به نام «روز صفر» است که در آغاز و برای ماه‌ها هیچ‌کاری نمی‌کند اما به انتظار تاریخی ازپیش‌تعیین‌شده می‌نشیند و در آن تاریخ مثلا قبل از برگزاری نشست سازمان مدنیِ هدف حملات، فعال می‌شود و همه اطلاعات را به سرقت می‌برد سپس همه داده‌ها را پاک می‌کند و تمام کامپیوترها و اکانت‌های سازمان قربانی را یکجا از بین می‌برد و از کار می‌اندازد.

فراموش نکنید که خانواده بدافزارها و حملات هکری، تنها منحصر به این ۳ مورد نیست و ده‌ها و صدها نوع مختلف از حملات وجود دارند اما بیش‌ترین میزان حملات علیه کاربران ایرانی تاکنون در قالب اشکال این چند نوع حمله - یعنی ترکیبی از فریب و سپس نصب نرم‌افزار آلوده به شیوه‌ای که توضیح داریم - انجام گرفته است.

آزمون ارزیابی

لطفا با دقت به پرسش‌ها پاسخ دهید. این کار کمک می‌کند درک خود از مطالب درس را ارزیابی کنید. پاسخ‌های درست در بخش پاسخ‌نامه در پایان کتاب در دسترس است.

۱- مهم‌ترین حربه حکومت‌های سرکوبگر برای سرکوب مخالفان ... است.

الف) ارعاب و ترساندن

ب) تقویت نیروهای مجازی (سایبری) و نیروهای سطح جامعه

ج) رصد خاموش و نامحسوس فعالیت‌ها

د) هک و جمع‌آوری اطلاعات آنلاین و غیرآنلاین

۲- تلفن یک فعال شناخته‌شده رسانه‌ایِ مدنی در نیمه‌های شب زنگ می‌خورد، فردی از پشت خط نام او را میان همهمه و شلوغی صدا می‌کند و به‌سرعت می‌گوید: من الان در فرودگاه گیر کرده‌ام و تلفن خودم مشکل پیدا کرده، لطفا محبت کنید الان کدی را که از سمت شرکت گوگل برای من قرار بوده ارسال شود را همین الان بخوانید.

کدام گزینه صحیح است؟

الف) حمله‌کنندگان رمز عبور یا شناسه قربانی را ندارند و می‌خواهند آن را به دست آورند.

ب) در صورت موفقیت آن‌ها پسورد و شماره تلفن سیستم تایید هویت دومرحله‌ای گوگل قربانی را به‌سرعت تغییر خواهند داد.

ج) در صورت موفقیت آن‌ها پسورد گوگل قربانی را به‌سرعت تغییر خواهند داد اما شماره تلفن ثبت شده را نمی‌توانند تغییر دهند چرا که به تلفن فرد دسترسی ندارند

د) سیستم تایید هویت دومرحله‌ای در این موقعیت، توان موفقیت حمله‌کنندگان را به صفر کاهش خواهد داد.

۳- کدام گزینه اشتباه است؟

الف) آنچه به «افشای هویت کاربران ناشناس ایرانی» انجامیده است ندانم‌کاری و اشتباهات مکرر این کاربران است.

ب) هک‌شدن از طریق سرویس جی‌میل امکان‌پذیر است.

ج) بدافزارها می‌توانند هم کی‌بورد کامپیوتر و هم صفحه نمایش موبایل را هدف قرار داده اطلاعات شما را برای مهاجمان ارسال می‌کند.

د) مهم‌ترین خصوصیت تمامی حملات بدافزاری سرعت این نوع حملات برای کاهش احتمال کشف‌شدن است و به این دلیل این حملات در کم‌تر از چند ثانیه پس از نفوذ صورت می‌گیرد.

جلسه چهارم
حملات هکری با پشتیبانی جمهوری اسلامی، ۱

خشونت‌های پس از انتخابات سال ۱۳۸۸ و جنبش سبز

پس از شروع اعتراضات در تقلب به انتخابات سال ۱۳۸۸، جدال میان فعالان و آنچه در ابتدا ارتش سایبری جمهوری‌اسلامی‌ایران نامیده می‌شد، شکل تازه‌ای به خود گرفت. هک سایت ایکس (Twitter سابق) که از آن زمان به شکل گسترده‌ای مورد استفاده معترضان قرار می‌گرفت، یکی از این سلسله عملیات‌ها بود. همچنین شمار بسیار گسترده‌ای عملیات هک صورت گرفت؛ علیه وبسایت‌های وابسته به رهبران جنبش اعتراضی سال ۸۸ مثل هک سایت «موج سبز آزادی» و «جرس»، یا همچنین علیه رسانه‌های فارسی زبان داخل ایران چون «خبرنامه امیرکبیر» و خارج از کشور ایران مثل «رادیو زمانه».

به لحاظ فنی تقریبا همه این عملیات‌ها بر پایه مهندسی اجتماعی و فریب و سپس دستیابی غیرمجاز به اطلاعات داخلی این سایت‌ها صورت می‌پذیرفت. برای مثال در مورد هک شبکه اجتماعی ایکس (توییتر) یا همان ایکس کنونی، ایمیل‌هایی به شیوه فیشینگِ هدفمند که پیش‌تر درباره آن توضیح دادیم، برای فریب ارائه‌دهندگان سرویس‌هایی چون نام دامنه (Domain) و همچنین DNS ایکس (توییتر) ارسال شده بود. این ایمیل‌ها در ظاهر طوری طراحی شده بود که موجه، معتبر و از داخل شرکت ایکس (توییتر) به نظر آید. پس از دستیابی مهاجمان به DNS، ترافیک سایت ایکس

(توییتر) به صفحه‌ای با تصویر و مشخصات ارتش سایبری جمهوری اسلامی ایران هدایت می‌شد.

هک گواهینامه‌های امنیتی شرکت‌های گوگل، کومودو و DigiNotar در سال‌های ۹۰ تا ۹۲

این سلسله عملیات دولتی، قدری با دیگر عملیات هک از سوی جمهوری اسلامی متفاوت‌اند. برای توضیح این هک لازم است قدری راجع به گواهینامه‌های امنیتی، مثلا گواهینامه‌های SSL، صحبت کنیم. فرض کنید شما قصد دارید با سرویس ارسال ایمیل یا تماس شنیداری یا دیداری مثلا از شرکت گوگل با دوست خود در کالیفرنیا صحبت کنید. این تماس مانند ارسال نامه است. گوگل در ۲ مرحله و با رمزگذاری نسبتا محکمی از تعلقِ نامه به شما و دریافت آن توسط دوستتان مطمئن می‌شود و در این میان هیچ فرد دیگری که طبعا کلید اول - یعنی رمزگذاری مختص فرستنده - و کلید دوم - یعنی رمزگذاری مختص گیرنده - را در اختیار ندارد، نمی‌تواند محتوای نامه را بخواند، نمی‌تواند خود را به جای شما جا بزند و برای دوستتان از قول شما نامه ارسال کند. همچنین کسی نمی‌تواند خود را جای دوست شما جای بزند و نامه را دریافت دارد. این رمزگذاری بر پایه گواهینامه‌های امنیتی است که صدور آن‌ها فقط و فقط در انحصار شرکت‌های معتبر و شناخته‌شده است. در سلسله هک مربوط به شرکت‌های کومودو و DigiNotar - مهاجمان با ارسال بدافزار، موفق به صدور گواهینامه‌های جعلی امنیت از سوی دو شرکت مورد اعتماد گوگل و چند نرم‌افزار دیگر مثل اسکایپ شدند.

در مرحله بعدی از این‌گواهینامه‌های جعلی، برای حملات موسوم به «مرد میانی» استفاده شد. به عبارت دیگر این‌جا مهاجمان می‌توانستند در میانه‌ی راهِ کامپیوتر قربانیان و شرکتی مثل گوگل قرار بگیرند و داده‌های خصوصی قربانی را سرقت کنند. قربانیان به دقت انتخاب شده بودند و گروهی از افراد منتقد جمهوری اسلامی بودند. ویژگی دیگر این عملیات، سوءاستفاده از زیرساخت‌های ملی اینترنت در ایران مانند مخابرات بود. سرانجام به دلیل استفاده شمار بالایی از ایرانیان از مرورگر کروم، این حملات توسط گوگل کشف و گواهینامه‌ها سرقت‌شده ابطال شد و از جمعی از کاربران ایرانی گوگل خواسته شد که سریعا رمزهای عبور خود را تغییر دهند و همچنین سیستم تایید هویت دومرحله‌ای را فعال کنند.

سلسله عملیات‌های هکری گروه بچه‌گربه ملوس (Charming Kitten) از آغاز دهه ۱۳۹۰

گروه هکری «بچه‌گربه ملوس» شناخته‌شده‌ترین گروه هکری وابسته به حکومت جمهوری اسلامی در جهان است. ما در این مبحث قصد ارائه فهرستی از عملیات منسوب به این گروه، علیه اهدافی در داخل و خارج از ایران را نداریم و فقط شیوه‌های مورد استفاده این گروه را به اختصار توضیح می‌دهیم. گروه بچه‌گربه ملوس که در میان متخصصان امنیت سایبری با کد APT۳۵ شناخته می‌شود، تمامِ یک دهه گذشته را به آزمودن و ارتقای شیوه‌های متعدد فریب و همچنین توسعه و استفاده از بدافزارهای مختلف گذرانده است.

این گروه، حملات هکری موفقیت‌آمیزی را علیه هزاران هدف ایرانی و غیرایرانی در داخل و خارج از مرزهای ایران انجام داده است. گرچه از طیف بسیار گسترده‌ای از ترفندهای نفوذ در این حملات استفاده شده، اما به صورت خلاصه بیش‌تر این حملات از دو الگوی مشخص تبعیت می‌کنند که در ادامه به توضیح درباره آن‌ها می‌پردازیم:

۱- ایمیلی از طرف شرکت گوگل به شماری از فعالان سیاسی ارسال می‌شود که مثلا جی‌میل شما هک شده است یا در خطر است و باید پسورد آن را عوض کنید. قربانی بدون دقت لازم و بلافاصله روی لینک داخل نامه کلیک می‌کند و با سایتی بسیار مشابه گوگل مواجه می‌شود. او شناسه و رمز عبور خود را در این سایت وارد می‌کند. مهاجمان بلافاصله با همان شناسه و رمز عبور برای ورود به گوگل تلاش می‌کنند، گوگل از آنان کد تایید هویت دومرحله‌ای می‌خواهد، آنان بلافاصله در وبسایت جعلی که بسیار هم شبیه گوگل است، از قربانی درخواست ورود کدی را می‌کنند که لحظه‌ای پیش از گوگل دریافت کرده. با ورود این کد کنترل حساب گوگل قربانی به صورت کامل در اختیار هکرها قرار می‌گیرد. آنان پس از آن به‌راحتی اطلاعات کاربر قربانی را به سرقت می‌برند و همه مکالمات دیجیتال او را مانیتور می‌کنند.

۲- در حالت دوم، گروه بچه‌گربه ملوس با صبر و حوصله و امکانات بسیار در شبکه‌های اجتماعی مثل فیس‌بوک، حساب‌های کاربری تا حد امکان با ظاهری واقعی می‌سازند و مثلا شمار زیادی همکار و اعضای خانواده به صورت ساختگی به آن حساب‌ها اضافه می‌شوند که در صورت شک، واقعی به نظر برسند. از این حساب‌های جعلی برای فریب قربانیان، ارسال پیام یا فایل‌های آلوده به آن‌ها استفاده می‌شود. بلافاصله پس

از بازکردن فایل توسط این افراد، دسترسی مهاجم به دستگاه قربانی میسر می‌شود. پس از این، انواع و اقسام بدافزارهای ضبطِ صفحه کلید یا همان (Keylogger) یا ثبت متناوب اسکرین‌شات و حتی روشن‌کردن وب‌کم و ضبط تصویر محیط برای مهاجم میسر می‌شود.

آنچه گروه گربه‌های ملوس را از دیگر گروه‌های هکری ایرانی متمایز می‌کند، حجم بسیار بالای امکانات و جزئیات نسبتا ریز و دقیقی است که با ماه‌ها و بلکه سال‌ها فعالیت توسط این گروه خلق می‌شود. سایت‌های جعلی، دانشگاه‌ها و استادان تقلبی دانشگاه و خلاصه هر شیوه‌ای که با آن بتوان اعتماد قربانیان را جلب کرد.

هک تلگرام با سوءاستفاده از سیستم پیامک در میانه دهه ۹۰

با رواج استفاده از نرم‌افزار تلگرام در میانه دهه ۹۰ در ایران، تلگرام برای میلیون‌ها ایرانی به محبوب‌ترین پیام‌رسان و شبکه‌اجتماعی تبدیل شد. ایرانیان تلگرام را برای طیف گسترده‌ای از فعالیت‌های آنلاین، از ارسال پیام شنیداری و تماس دیداری گرفته تا گروه‌های خانوادگی یا مطالعه اخبار و حتی خدمات پس از فروش، به کار گرفتند. در این میان حکومت ایران همواره خواستار دسترسی و نظارت بر پیام‌ها و در کل محتوای ردوبدل‌شده میان میلیون‌ها ایرانی بود، امری که تلگرام به‌روشنی و به دلیل احترام به حقوق کاربران در حفظ اطلاعات خصوصی آن‌ها با آن، مخالفت می‌کرد.

هکرهای وابسته به جمهوری اسلامی از آغاز سال ۱۳۹۵ با سوءاستفاده از پیامک‌هایی که تلگرام به هنگام ورود کاربران، تغییر رمز عبور یا بازکردن حساب مثلا در کامپیوتر شخصی برای آنان ارسال می‌کرد، به جای کاربران، این پیامک‌ها را دریافت می‌کردند و وارد حساب تلگرام آن‌ها می‌شدند و داده‌هایی چون لیست مخاطبان و آرشیو چت‌های متنی، صوتی و تصویری او را به سرقت می‌بردند.

همان‌طور که حتما متوجه شده‌اید در این میان، کاربر کار خاصی را انجام نمی‌دهد و حتی شاید خبری از این‌که افرادی هفته‌ها و ماه‌ها ست که وارد حسابش می‌شود، ندارد. این‌جا ما به جای فریب و مهندسی اجتماعی با نوعی «سوءاستفاده گسترده از زیرساخت‌های ملی مواجهیم و صد البته اگر قربانی، از پیش در آرشیو و ضبط موارد متنی،

صوتی و تصویری احتیاط بیش‌تری به خرج می‌داد، ضرر این عملیات هکری هم به حداقل می‌رسید.

گستردگی و تنوع گروه‌های هکری وابسته به حکومت ایران به قدری است که می‌توان جدولی طولانی از لیست آنان منتشر کرد. ما در این مبحث می‌توانیم به ده‌ها عملیات هک مثلا علیه فعالان حقوق زنان و محیط‌زیست یا هک فعالان حقوق بشر و نهادهای حقوق بشری اشاره کنیم هر چند که قصد ورود به جزئیات ریز و فنی این سلسله عملیات را نداریم، همچنین عملیاتی چون حملات گروه «بچه گربه مارپیچی» (Helix Kitten) ترکیبی از قربانیان ایرانی و غیرایرانی را در نظر گرفته بود.

به هر حال با گذشت بیش از ۲۰ سال از نخستین حملات هکری وابسته به جمهوری اسلامی، امروزه شرکت‌های بزرگ تکنولوژی مثل گوگل، اپل، متا، مایکروسافت و تلگرام، اطلاعاتی به مراتب بهتر و ابزارهایی بسیار کارآمدتر از دو دهه پیش را در اختیار دارند. این امر تا حد زیادی می‌تواند به صدور و ارسال هشدارهایی نسبتا صریح به آن دسته از کاربران ایرانی کمک کند که ممکن است امنیت دیجیتال‌شان در خطر باشد.

آزمون ارزیابی

لطفا با دقت به پرسش‌ها پاسخ دهید. این کار کمک می‌کند درک خود از مطالب درس را ارزیابی کنید. پاسخ‌های درست در بخش پاسخ‌نامه در پایان کتاب در دسترس است.

۱- پس از شروع اعتراضات در تقلب به انتخابات سال ۱۳۸۸، عملیات هک بیش‌تر به چه صورتی بود؟

الف) هک مستقیم و و شناسایی شرکت‌کنندگان در اعتراضات

ب) حملات DDoS و شناسایی شرکت‌کنندگان در اعتراضات

ج) مهندسی اجتماعی و فریب و سپس دستیابی غیرمجاز به اطلاعات داخلی

د) استروترفینگ و سپس رصد فعالیت

هـ) نمی‌دانم

۲- کدام مورد درباره گروه بچه‌گربه ملوس یا Charming Kitten نادرست است؟

الف) گروه «بچه‌گربه ملوس» گروه هکری وابسته به حکومت اسلامی است.

ب) «بچه‌گربه ملوس» قادر است از طریق ظاهرسازیِ شرکت امن و شناخته‌شده‌ای مانند گوگل، اقدام به هک کند.

ج) «بچه‌گربه ملوس» برای نفوذ، از سایت‌های جعلی، دانشگاه‌ها و حتی استادان تقلبی بهره می‌برد.

د) «بچه‌گربه ملوس» از طیف بسیار گسترده‌ای از ترفندهای نفوذ استفاده می‌کند که از الگوهای مشخصی تبعیت نمی‌کنند.

هـ) نمی‌دانم

۳- کدام مورد درست است؟

الف) به دلیل پیشرفت دانش شرکت‌ها، امروزه امکان هک‌شدن از طریق حساب جعلی در شبکه اجتماعی وجود ندارد.

ب) هکرها در شبکه‌های اجتماعی، حساب‌های کاربری تا حد امکان با ظاهری واقعی می‌سازند، اما این حساب‌ها معمولا چراغ‌خاموش هستند و فالوئر زیادی نمی‌گیرند تا

شک کسی برانگیخته نشود.
ج) هکرها در شبکه‌های اجتماعی، حساب‌های کاربریِ تا حد امکان با ظاهری واقعی می‌سازند، شمار زیادی دنبال‌کننده به آن حساب‌ها اضافه می‌شوند که شک کسی برانگیخته نشود.
د) هکرها فقط برای مدت کوتاهی تا پیش از لو رفتن و کشف‌شدن هک، می‌توانند در حساب سایرین فعالیت کنند، و به همین دلیل آن‌ها به سرعت حساب قربانی را نابود می‌کنند.
هـ) نمی‌دانم

درس پنجم
حملات هکری با پشتیبانی جمهوری‌اسلامی، ۲

صورت‌بندی این درس باز هم بر اساس عملیات گروه‌های هکری وابسته به حکومت ایران است که در جلسه پیشین به آن اشاره شد. همان‌طور که پیش‌تر گفته شد، محققان و شرکت‌های معتبر امنیت سایبری در جهان از اسامی بعضا چندگانه‌ای برای توصیف این گروه‌ها استفاده می‌کنند. گرچه حکومت جمهوری اسلامی ایران، به صورت رسمی هرگز مسئولیت این‌گروه‌های هکری را نپذیرفته است اما برای اثبات ارتباط آنان با نهادهای امنیتی ایران، کوهی از اسناد و مدارک غیرقابل انکار وجود دارد.

ما در این درس به صورتی گذرا به کد یا شناسه‌ای که متخصصان امنیت سایبری در جهان به این گروه‌ها داده‌اند و روی آن توافق نظر دارند، اشاره می‌کنیم. مثلا گروه بدنام «بچه‌گربه ملوس» در ادبیات مرسوم فنی «APT35» نامیده می‌شود. APT مخفف Advanced Persistent Threat به معنی تهدید پیچیده و مستمر است. پیچیده از آن جهت که مجموعه نسبتا پیچیده‌ای از ابزارها و ترفندها در اختیار این گروه‌های هکری قرار دارد که معمولا نهادهای امنیتی یا دولت‌ها قادر به تامین آن هستند و مستمر از آن جهت که گروه به دنبال منافع آنی نیست و ترجیح می‌دهد مثلا فعالیت قربانیان را برای سال‌ها تحت نظر قرار دهد.

دانستن نام و کد این گروه‌ها الزامی نیست و فقط کافی ست به جبعه‌ابزارهایی که

هر یک از این گروه‌ها برای رخنه به کامپیوتر، تلفن هوشمند و دیگر دستگاه‌های دیجیتال قربانیان، استفاده می‌کنند، توجه کنید. هکرها از ابزارهای مختلفی برای رخنه به کامپیوتر و تلفن هوشمند شما استفاده می‌کنند. استفاده از این ابزارها تقریبا در همه موارد تنها با نوعی از فریب، حیله‌گری و گول‌زدن قربانی ممکن است. یعنی قربانی، باز در تقریبا اغلب موارد، خودش، ندانسته یا در اثر اهمال و بی‌اطلاعی به هکرها برای نفوذ به مجموعه اطلاعات محافظت‌شده خود کمک می‌کند.

در ادامه، دفاع در برابر این ابزارها را به همراه شناسایی ترفندهای فریب بررسی خواهیم کرد، هر چند که در مورد فریب و مهندسی اجتماعی در درس ششم و درباره تجربیات قربانیان این حملات، در درس هشتم بیش‌تر توضیح خواهیم داد.

مطالعه موردی: گروه APT33

شیوه اصلی این گروه برای فریب، تبلیغ برای پیشنهاد موقعیت‌های شغلی جذاب است. این گروه با ارسال ایمیل یا تماس در شبکه‌های اجتماعی و پیام‌رسان‌ها، قربانیان خود را با پیشنهاد موقعیت‌های شغلی، ترغیب به کلیک روی لینک سایت‌های آلوده می‌کند. پس از ورود قربانی به سایت آلوده، از بدافزارهای متعددی برای نفوذ به مرورگرهای دستگاه او، استفاده می‌شود.

تدابیر و ترفندها: چه باید کرد؟

۱- به هیچ وجه روی هیچ لینک ارسالی در شبکه‌های اجتماعی، توسط هیچ کس، حتی کسانی که می‌شناسید، کلیک نکنید. خطر همواره زمانی بیش‌تر است که لینک ارسال‌شده با سرویس‌های کوتاه‌کننده‌ی لینک اینترنتی، چون bitly یا tinyurl و goo.gl استفاده شده باشد.

۲- مرورگرهای خود را همواره به‌روز کنید، شرکت‌هایی مانند گوگل و اپل دائما مرورگرهای خود را علیه چنین تهدیداتی به‌روز می‌کنند.

۳- برای مراجعه به سایت‌های ناشناس و مثلا لینکی که با سرویس‌های کوتاه‌کننده‌ی لینک‌های اینترنتی مثل bitly یا tinyurl یا goo.gl کوتاه شده، حتما و حتما از حالت ناشناسِ مرورگرتان مثلا حالت Private در سافاری یا Incognito در کروم استفاده کنید.

۴- هرگز فایل‌های ارسالی از سوی هیچ کس را باز نکنید. از افراد بخواهید اطلاعات مورد نیاز را در بدنه ایمیل به صورت متن برای شما ارسال کنند. خطرناک‌ترین فایل‌ها، فایل‌هایی هستند که با اپلیکیشن‌های واتس‌اپ، تلگرام یا از طریق شبکه‌های اجتماعی و همین‌طور به شکل پیامک برای شما ارسال می‌شوند. پس از آن فایل‌های الصاقی در جی‌میل می‌توانند حاوی بدافزار و ویروس باشند. گوگل همه فایل‌های الصاقی را به دنبال بدافزار و ویروس اسکن می‌کند اما این اسکن، ۱۰۰ درصد امنیت آن فایل را تضمین نمی‌کند. هر چند که وجود آن درصد بسیار بالایی از بدافزارها را شناسایی و از دانلود فایل جلوگیری می‌کند.
۵- توجه داشته باشید که اگر فردی برای شما فایلی در جی‌میل ارسال کرد که مجهز به رمز عبور بود یا به شکل یک فایل فشرده یا zip بود که گوگل توانایی اسکن و چک آن فایل را ندارد، به احتمال قریب به یقین آن فایل حاوی ویروس و بدافزار است.

حملات Brute Force

این گروه همچنین از حملات موسوم به Brute Force یا جستجوی فراگیر برای ورود به حساب‌های کاربری قربانیان مثل جی‌میل استفاده می‌کند. در این حملات بعضا میلیون‌ها واژه مختلف به جای رمز عبور شما پشت‌سرهم وارد می‌شود تا یکی از آن‌ها درست از کار درآمده و مهاجم موفق به شکستن قفل شما شود.

تدابیر و ترفندها: چه باید کرد؟

مقابله با حملات Brute Force یا جستجوی فراگیر نسبتا ساده است که با ۴ راهکار می‌توان اقدام کرد.
۱- رمز عبوری انتخاب کنید که حاوی ترکیبی از حروف بزرگ و کوچک، علائمی مثل #%$@! و اعداد باشد، البته با طولی بیش از ۱۲ کاراکتر. فراموش نکنید که رمز عبورهای شما در حساب‌های مختلف‌تان نباید یکسان باشند.
۲- سایت haveibeenpwned.com را دائما چک کنید، این سایت وجود ایمیل شما در داده‌های قابل خرید و فروش هکرها روی دارک‌نت را دائما جستجو می‌کند. به محض اطلاع از وجود ایمیل خود در دارک‌نت، تمام رمزعبورهای مشابه رمز عبور آن ایمیل را عوض کنید. همانطور که گفتیم هرگز از یک رمز عبور مشابه برای همه حساب‌های خود استفاده نکنید.

۳- تمام ابزارهای دیجیتال و تمام حساب‌های کاربری خود مثل حساب جی‌میل‌تان را مجهز کنید به سیستم تایید هویت دومرحله‌ای؛ با چند روش مختلف: مثلا دستگاه ایجاد کد سخت‌افزاری، یا نرم‌افزارهایی مثل Google یا Microsoft Authenticator و تایید هویت با ارسال پیامک یا تماس صوتی به تلفن همراه. حتما از چند روش ترکیبی مثلا Authenticator به همراه تلفن یا ۲ تلفن مختلف، دومی در شکل تلفن پشتیبان یا Backup Phone، استفاده کنید.

۴- حافظه مرورگرهای خود را دائما پاک کنید، روی هیچ کامپیوتری جز کامپیوتر خودتان به ایمیل و دیگر حساب‌های اصلی‌تان متصل نشوید. اگر چاره‌ای جز این کار ندارید مثلا در یک هتل حتما بایستی با کامپیوتر هتل به ایمیل خود وصل شوید، حتما و حتما از حالت مرورگر ناشناس استفاده کنید و حتما پس از استفاده، ایمیل‌تان را لاگ‌آوت یا خروج کامل کنید و سپس با بستن پنجره و خاموش‌کردن کامپیوتر مطمئن شوید که کسی امکان ورود به حساب شما را نخواهد داشت.

مطالعه موردی: گروه APT34

ابزار اصلی این گروه نیز فیشینگ هدفمند یا Spear Phishing است. این گروه هکری مرتبط با جمهوری اسلامی ایران، شمار نسبتا بالایی حساب کاربری در شبکه‌های اجتماعی مختلف ایجاد می‌کند تا برای هویت کاربر یا موسسه‌ی طعمه‌ای که از آن برای شکار قربانیان استفاده می‌کند، اعتبار بیش‌تر و بیش‌تری داشته باشند.

یکی از شگردهای این گروه سوءاستفاده از شبکه لینکدین Linkedin و ایجاد کاربران جعلی است که تشخیص جعلی‌بودن‌شان برای فرد معمولی بسیار سخت است. آن‌ها به نظر کاربرانی هستند که دارای ارتباطاتی زیاد با دیگر افرادی‌اند که آن‌ها واقعا در موسسات آکادمیک، علمی و بعضا در دولت‌ها مشغول کار هستند. فرض کنید کاربری به نام Dr.Albert Smith به عنوان استاد روابط بین‌الملل از موسسه‌ای در دانشگاه آکسفورد با شما تماس می‌گیرد و خواستار همکاری شما با یک پروژه تحقیقاتی می‌شود، او در ایمیل خود فایل ورد یا پی.دی.افی را ضمیمه می‌کند که شما حتما باید آن را مطالعه کنید و به آن پاسخ دهید.

این فایل احتمالا حاوی بدافزاری در قالب «اسب تروا» یا «تروجان» است که راه

را برای نفوذ بی‌سروصدای مهاجمان به دستگاه شما باز می‌کند. از آن پس آنان کنترل همه دستگاه‌های دیجیتال شما را با دزدیدن شناسه، رمزعبور و حتی کد تایید هویت دومرحله‌ای گوگل شما به دست خواهند گرفت.

تدابیر و ترفندها: چه باید کرد؟

این‌جا هم راهکار اصلی کلیک‌نکردن روی لینک‌ها و همچنین بازنکردن فایل‌ها ست که پیش‌تر گفته شد. اما با فریب در شکل معرفی مهاجم در لباس استاد دانشگاه، مدیر موسسه دولتی یا غیردولتی چه باید کرد؟

اگر فردی ادعا کرد از دانشگاه هاروارد، آکسفورد یا هر موسسه سرشناس دیگری با شما تماس می‌گیرد، بلافاصله با شماره و ایمیلی غیر از آنچه در ایمیل دریافتی‌تان ذکر شده، تماس بگیرید. با دوستان و کسانی که اطلاع بیش‌تری از آن موسسه دارند تماس بگیرید و خیلی ساده بپرسید من چنین ایمیلی دریافت کرده‌ام آیا این ایمیل معتبر است؟ آیا هویت این افراد واقعی است؟ بسیاری از مهاجمان از هویت افراد واقعی سوءاستفاده می‌کنند. این هم راه ساده‌ای دارد با فردی که اسم او در ایمیل آمده از طریق صفحه معتبرش در دانشگاه، موسسه یا محل کار واقعی او تماس بگیرید و بپرسید آیا این ایمیل را شما برای من فرستاده‌اید؟ همین ترفند ساده ۹۰درصدِ تهدیدهای فریب را خنثی می‌کند

به خاطر داشته باشید که در مجموعه حملات گروه APT34 بیش‌ترین قربانیان افرادی بوده‌اند که سیستم عامل، مرورگرها و بسته‌ی نرم‌افزاری یا Microsoft Office خود را به‌روز نکرده بودند. پس هر روز که کامپیوتر یا تلفن هوشمند خود را روشن می‌کنید، می‌بایستی قبل از هر کار دیگری، اطمینان حاصل کنید که تمام نرم‌افزارهای شما خصوصا سیستم‌عامل، مرورگر و همچنین نرم‌افزارهای Office و آکروبات شما آخرین بسته به‌روزرسانی را دریافت کرده‌اند.

آزمون ارزیابی

لطفا با دقت به پرسش‌ها پاسخ دهید. این کار کمک می‌کند درک خود از مطالب درس را ارزیابی کنید. پاسخ‌های درست در بخش پاسخ‌نامه در پایان کتاب در دسترس است.

۱- بر اساس درس ارائه شده، حکومت ایران نسبت به گروه‌های هکری خود چه موضعی دارد؟

الف) با بیان و ابراز قدرت و توانایی خود در هک کردن، معترضان را ساکت می‌کند.
ب) تنها در موارد معدودی مسئولیت هک را پذیرفته است.
ج) به صورت رسمی مسئولیت این‌گروه‌های هکری را نپذیرفته است.
د) با هدف ایجاد سردرگمی موضع خود را مرتب عوض می‌کند.
هـ) نمی‌دانم.

۲- بر اساس درس ارائه‌شده، کدام مورد درست است؟

الف) روی هیچ لینک ارسالی در شبکه‌های اجتماعی، توسط هیچ کس، حتی کسانی که می‌شناسید، کلیک نکنید.
ب) سرویس‌های کوتاه‌کننده‌ی لینک اینترنتی خطر ردیابی و هک را کاهش می‌دهند.
ج) «حالت ناشناس مرورگر مثلا حالت Incognito در کروم تاثیری بر افزایش امنیت کاربران ندارند.
د) اگر به جای ارسال فایل مطلبی را در بدنه ایمیل دریافت کنید احتمال هک‌شدن و یا گرفتن بدافزار تغییر نمی‌کند.
هـ) نمی‌دانم.

۳- بر اساس درس ارائه شده، کدام مورد نادرست است؟

الف) برای مقابله با حملات Brute Force یا جستجوی فراگیر نیاز به رمز عبور قوی و مناسب است.
ب) می‌توان وجود ایمیل خود را در میان داده‌های قابل خرید و فروش چک کرد و در صورت نیاز

رمز عبور را تغییر داد.
ج) دسترسی به ایمیل با کامپیوتر یک هتل از طریق حالت ناشناس مرورگر، تاثیر مثبتی در امنیت کاربر دارد.
د) در حملات Brute Force یا جستجوی فراگیر، هکرها از سرویس جستجو (سرچ) گوگل سوءاستفاده می‌کنند.
هـ) نمی‌دانم.

درس ششم
کارگاه: مهندسی اجتماعی و فریب؛ ابزار اصلی حملات هکری

همان‌طور که بارها پیش از این در جلسات مختلف این دوره عنوان شد، حملات هکری جمهوری اسلامی ایران از طریق ترکیبی از فریب و ابزارهای فنی است. در بیش‌تر این حملات، فریب قربانیانِ هدف حمله، بخش بسیار بزرگی از مجموعه عملیات هک را تشکیل می‌دهد. در ادامه مثالی می‌زنیم که به آن دقت کنید، زیرا در این مثال ۹۹درصد عملیات هک را فریب و اغوا و فقط شاید یک درصد آن را استفاده از ابزارهای فنی تشکیل می‌دهد.

هک حساب روزنامه‌نگاران با استفاده از جعل نام رها اعتمادی

گروهی از هکرها با سوءاستفاده از نام رها اعتمادی، یکی از فعالان رسانه‌ای دو دهه اخیر، در سال ۲۰۱۵ حساب کاربریِ جعلی‌ای را در شبکه‌های اجتماعی ایجاد کردند. آنان سپس با تگ‌کردن شمار نسبتا بالایی از روزنامه‌نگاران، از آن‌ها درخواست کردند که حساب کاربری جعلی رها اعتمادی را دنبال کنند تا بتوانند برایشان پیامی مهم را ارسال کنند. هکرها برای هر کاربری که این حساب جعلی را دنبال می‌کرد، با ارسال پیامی خصوصی از آنان می‌خواستند که به نظرسنجی بسیار مهم و خصوصی که فقط برای مدیر

یک شبکه تلویزیونی تهیه می‌شود، پاسخ دهند. به جای نظرسنجی از آنان خواسته شد که به تماس اسکایپ فردی از همکاران رها اعتمادیِ جعلی پاسخ دهند و در برابر اصرار مصاحبه‌شوندگان برای روشن‌کردن دوربین اسکایپ گفته شد که وب‌کم خبرنگارِ جعلی ایراد پیدا کرده و روشن نمی‌شود. نتیجه این‌که بسیاری از خبرنگاران حاضر به مصاحبه تصویری شدند در حالی که چند نفر از آنان جعلی‌بودن این مصاحبه را دریافتند و آن را به صورت علنی اعلام کردند.

همان‌طور که می‌بینید، فریب، هسته‌ی اصلی این عملیات را تشکیل می‌دهد. در سال‌های نخستین فراگیری شبکه‌های اجتماعی مثل فیس‌بوک، افراد به دلیل عدم آگاهی از امنیت دیجیتال، تعداد بسیار زیادی از کسانی که نمی‌شناختند را به فهرست دوستان خود اضافه می‌کردند. با گذشت زمان و ایجاد مشکلات بسیار، از کلاهبرداری گرفته تا آزار و اذیت، امروزه اکثر افراد در انتخاب و قبول‌کردن درخواست‌های‌دوستی دقت بیش‌تری می‌کنند. اما این دقت همچنان کامل و صددرصدی نیست.

در مثالی که گفتیم، همان‌طور که دیدید جمع بسیار زیادی از سرشناس‌ترین روزنامه‌نگاران ایرانی به دلیل وجود دوستان مشترک بسیار، درخواست دوستی رها اعتمادیِ جعلی را پذیرفته‌اند. این اقدام می‌تواند در اشکال مختلفی تکرار شود، فرض کنید مهاجمی که قصد هک حساب‌های کاربری شما را دارد، قبل از هک شما، به‌سادگی حساب کاربری پدربزرگ یا عموی شما را هک کند، کاری که به دلیل سالخوردگی آن‌ها و احتمالا ناآگاهی از اصول امنیت دیجیتال، نسبتا ساده‌تر است. شما نیز به دلیل اعتماد کامل حتما روی لینک یا فایلی که پدربزرگ یا عمویتان فرستاده کلیک خواهید کرد.

عملکرد و سابقه هکرهای مرتبط با دولت ایران نشان داده است که آنان در کمپین‌ها و عملیات مختلف هک خود همیشه به دنبال ضعیف‌ترین حلقه‌ی زنجیر می‌گردند. مثلا برای هک یک نهاد مدنی یا روزنامه، معمولا اول به سراغ نوجوانان، سالخوردگان یا افرادی می‌روند که اطلاعات فنی آن‌ها نزدیک به صفر باشد.

در ادامه، بر منوال درس پیش به بررسی شمار بیش‌تری از حملات واقعی گروه‌های هکری مرتبط با دولت ایران ادامه خواهیم داد. در خلال این بررسی مثال‌هایی ارائه خواهد شد با هدف برجسته‌نمایی نقش «فریب» و «اغوا»، در گشودن در و نفوذ به فضای دیجیتال قربانیان، کامپیوتر، تلفن همراه و دیگر ابزارهای آن‌ها.

گروه APT35

چنانچه در رس‌های پیشین گفتیم، این گروه مشهورترین گروه هکری مرتبط با جمهوری اسلامی ایران است و با نام‌های دیگری نیز چون «بچه‌گربه ملوس» در سطح بین‌المللی و میان کارشناسان امنیت سایبری شناخته‌می‌شود.

این گروه هم مثل دیگر گروه‌ها از حیله‌هایی چون ایجاد پروفایل جعلیِ به‌ظاهر معتبر، در شبکه‌های اجتماعی - خصوصا در قالب روزنامه‌نگار یا استاد دانشگاه - استفاده می‌کند

این پروفایل‌ها همان‌طور که پیش‌تر گفتیم، مثلا در شبکه لینکدین با تعداد بسیار زیادی از پروفایل‌های جعلی و بعضا حقیقی مرتبط‌اند که بعضی از این‌ها افرادی از آشنایان یا دوستان قربانی هستند که بدون تحقیق، درخواست ارتباط این هکرها را پذیرفته‌اند. سپس هکرها به سراغ قربانی اصلی می‌روند. در نتیجه، قربانی هم به مهاجم (که با تعدادی از آشنایان او مرتبط است) اعتماد می‌کند و به صفحات آلوده‌ی پیشنهادی او می‌رود یا فایل‌های آلوده‌ای که او فرستاده است را باز می‌کند.

در ادامه قصد داریم در قالب یک فهرست به وجه دیگری از عملیات فریب اشاره کنیم.

فریب: سوءاستفاده از اخبار داغ و وقایع مهم روز

همه کاربران علاقه ویژه‌ای به کسب اطلاعات از جوانب مختلفِ اخبار مهم و سرنوشت‌سازی مانند انتخابات‌ها، مواردی مثل همه‌گیری کرونا، مسابقات المپیک، جنگ، سوءقصد و ترور و مواردی از این قبیل دارند. گروه APT۳۵ در همه سال‌های فعالیت خود از توجه و علاقه قربانیان به این اخبار برای آلوده‌کردن دستگاه‌های آن‌ها استفاده کرده است. در ادامه به بررسی عنصر فریب می‌پردازیم که این گروه هکری در چندین واقعه مهم، که روزانه اخبار و حواشی بسیاری از آن منتشر می‌شد، از آن استفاده کرده است.

سال ۲۰۱۵: مذاکرات و توافق هسته‌ای موسوم به «برجام»

APT35 از توجه روزنامه‌نگاران و دیگر افراد دست‌اندرکار و علاقه‌مند به نتایج مذاکرات موسوم به ۵+۱ باخبر بود. این گروه با ارسال ایمیلی به شماری از قربانیان ادعا می‌کند از اخبار پشت‌پ رده این مذاکرات با خبر است. سایت‌های خبری جعلی و آلوده‌ای از پیش طراحی شده است و برخی از قربانیان با بازکردن ایمیل‌ها و کلیک روی لینک‌های داخل

آن، وارد سایت‌های آلوده‌ای می‌شوند که برای هک کامپیوترشان طراحی شده‌اند.

سال ۲۰۱۶: بهانه انتخابات ایران و مجددا جنگ داخلی سوریه

در این سال مجددا با تعدادی از دست‌اندرکاران و روزنامه‌نگارانِ هدف تماس گرفته می‌شود تا برای اطلاع از اخبار و تحلیل‌های اختصاصی به سایت‌های آلوده مراجعه کنند. در این سایت‌ها بخشی بسیار مشابه صفحات اصلی وجود دارد که در آن از شناسه و رمز عبور مثلا جی‌میل یا یاهوی آنان سوال می‌شود. این صفحات برای سرقت رمز عبور و دیگر اطلاعات قربانیان طراحی شده‌اند.

همین رویه در سال‌های بعد هم دنبال شده است.

سال ۲۰۱۷: جنگ داخلی سوریه
سال ۲۰۱۸: جام جهانی فوتبال
سال ۲۰۱۸: انتخابات میان‌دوره‌ای ایالات متحده
سال ۲۰۱۹: اخبار پشت‌پرده تغییرات در تیم سیاست خارجی ترامپ
سال ۲۰۲۰: همه‌گیری کرونا
سال ۲۰۲۱: المپیک توکیو
سال ۲۰۲۲: جنگ اوکراین

در تمامی این سال‌ها گروه APT۳۵ با سوءاستفاده از کنجکاوی و علاقه کاربران و فعالان به اخبار مهم، و فریب آنان با ادعای دراختیارداشتن اخبار پشت پرده، قربانیان خود را به صفحات آلوده‌ای هدایت کرده است که قرار است در آن رمز عبور و کد تایید هویت دومرحله‌ای ایمیل‌شان سرقت شود.

تدابیر و ترفندها: چه باید کرد؟

خیلی ساده، می‌توان گفت که در ۹۹.۹۹ درصد موارد، فردِ ناشناسی که ادعا می‌کند اخبار پشت‌پرده و سرّی و ویژه شما را در اختیار دارد، هکر است و به دنبال سرقت اطلاعات یا دیگر منابع شما ست. به این ایمیل‌ها اعتماد نکنید، روی هیچ لینکی چه از طریق ایمیل و چه از طریق شبکه‌های اجتماعی یا پیام‌رسان‌ها هرگز کلیک نکنید.

استفاده هکرهای APT35 از فریب برای هک وب‌سایت شرکت HBO

در جریان هک وبسایت شرکت بزرگ تولید فیلم و سریال HBO، هکرهای APT۳۵، از شگردی نسبتا معمول برای به‌دست‌آوردن رمز عبور و شناسه قربانیِ ازپیش‌انتخاب‌شده استفاده کردند. این شگرد به این ترتیب است که مثلا شما در شرکت HBO یا هر شرکت، دانشگاه، اداره یا نهاد غیردولتی دیگری مشغول به کار هستید. ایمیل خود را باز می‌کنید و می‌بینید ایمیلی کاملا واقعی از نام دامنه HBO، شرکت یا دانشگاه و از این دست مراکز دریافت کرده‌اید. یک نفر از کارمندان IT یا قسمت فنی یا یکی از کارمندان قسمت نیروی انسانی یا مالی از شما درخواست کرده که کپی شناسنامه یا مدارک دیگری را برای او در لینک داخل نامه ارسال کنید. شما وارد لینک می‌شوید، صفحه بازشده از شما خواسته رمز عبورتان را وارد کنید. با انجام این کار شما به‌راحتی هک می‌شوید.

APT35 این شگرد - یعنی سوءاستفاده از نام دامنه و ظاهرشدن در لباس یکی از همکاران از بخش فنی، نیروی انسانی و مالی را - بارها علیه قربانیان مختلف به کار برده است.

تدابیر و ترفندها: چه باید کرد؟

باز هم بسیار ساده، تلفن را بردارید و با فردی که برای شما ایمیل فرستاده و ادعا می‌کند همکار شماست تماس بگیرید. شماره تلفن او را نه از داخل آن ایمیل ارسالی، که از دوستان و همکاران و بخش‌های مرتبط اداره یا نهاد خود بگیرید و نه حتی از راه جستجوی گوگل. خیلی ساده مطمئن شوید که آیا چنین فردی وجود دارد یا نه؟ آیا ایمیل را او فرستاده است و سوالاتی از این دست. قبل از اطمینانِ ۱۰۰درصدی هرگز روی هیچ لینکی کلیک نکنید.

هکرها بیش‌تر در چه لباسی ظاهر می‌شوند؟

با بررسی دقیق حملات هکری مرتبط با دولت ایران در سال‌های ۲۰۱۰ تا ۲۰۲۳ سه پوشش جعلی، بیش‌ترین موارد فریب را تشکیل می‌دهند:

۱- روزنامه‌نگار

۲- استادان دانشگاه و محققان

۳- ریکرتِر (Recruiter) یا فردی که دنبال استخدام افراد جویای شغل است

البته موارد جعلی برای فریب در این سه مورد خلاصه نمی‌شوند و بسیار بیش از این سه موردند. مثلا برای هک فردی که در صنایع شیمیایی مشغول به کار است، معمولا یک شناسه و پروفایل جعلی فردی ساخته می‌شود که او نیز در صنایع شیمیایی شاغل و صاحبِ نام و شبکه است.

موارد بعدی تنها شماری از پروفایل‌های جعلی است که هکرهای مرتبط با جمهوری اسلامی در سال‌های گذشته مورد سوءاستفاده قرارداده‌اند، آن‌ها را می‌توان در ۹ گروه مختلف تقسیم‌بندی کرد:

۱- کارمند بخش فنی و آی.تی
۲- متخصص و محقق بهداشت و درمان
۳- کارمند کمک‌های انسان‌دوستانه سازمان ملل
۴- دیپلمات
۵- نهاد حقوق بشری
۶- نهادی که با اعطای فاند (یا کمک هزینه) از پروژه‌های مدنی حمایت می‌کند
۷- بازرس و ناظر انتخاباتی
۸- جعل هویت مدیران اقتصادی
۹- انجمن خیریه و بشردوستانه جعلی

تدابیر و ترفندها: چه باید کرد؟

قبل از کلیک روی هر نوع لینکی خصوصا از افراد مدعی مشاغل بالا، از وجود آن نهاد مدنی اطمینان حاصل کنید. اگر کسی خود را دیپلمات معرفی می‌کند از او بخواهید شماره داخلی خود در سفارت را به شما بدهد که از طریق شماره شناخته‌شده سفارت با او تماس‌بگیرید. همین ترفند را درباره بیش‌تر این مشاغل می‌توان به کار برد و باز هم تکرار می‌کنیم. فایل متصل به ایمیل چنین افرادی را باز نکنید. به سایت‌های داخل ایمیل نروید و از همه مهم‌تر هرگز پسورد و رمزعبور خود را در سایتی که از طریق چنین ایمیلی واردش شده‌اید تایپ نکنید.

آزمون ارزیابی

لطفا با دقت به پرسش‌ها پاسخ دهید. این کار کمک می‌کند درک خود از مطالب درس را ارزیابی کنید. پاسخ‌های درست در بخش پاسخ‌نامه در پایان کتاب در دسترس است.

۱- کدام مورد درست است؟

الف) هکرها چند سال پیش حساب کاربری متعلق به رها اعتمادی را به دست گرفتند و از طریق آن، افراد بسیاری را فریب دادند.

ب) در مورد بالا، کاربران عادی زیادی در دام این فریب افتادند اما اکثر خبرنگاران متوجه فریب شدند.

ج) در مورد بالا، نرم افزار اسکایپ از ابزارهای استفاده شده در عملیات فریب بود.

د) در آغاز کار فیسبوک، افراد محتاط بودند و در انتخاب و قبول درخواست دوستی دقت بیش‌تری داشتند.

هـ) نمی‌دانم.

۲- کدام گزینه نمونه فریب انجام شده توسط گروه «بچه‌گربه ملوس» نیست؟

الف) استفاده از وقایعی که توجه و نظارت زیادی به آن وجود دارد مانند اخبار انتخابات یا بیماری کووید.

ب) فعالیت با عنوان اطلاع رسانی از اخبار پشت پرده بین المللی.

ج) تماس مستقیم با افراد سرشناس و نفوذ و ارسال لینک.

د) هک سایت شرکت رسانه‌ای یونایتد مدیا و فریب از طریق سرویس آی تی آن سایت.

هـ) نمی‌دانم.

۳- کدام مورد معمولا نمونه پوشش جعلی پرکاربرد برای فریب کاربران نیست؟

الف) روزنامه‌نگار

ب) استاد دانشگاه یا پژوهشگر

ج) خواننده یا نوازنده سرشناس
د) فردی که دنبال استخدام دیگران است.

جلسه هفتم
تلفن‌های هوشمند و حملات هکری

۶ نوع تهدید گروه‌های هکری علیه تلفن همراه کنش‌گران ایرانی

به روال درس‌های پیشین، ۶ مورد از تهدیدهای واقعا رخ‌داده علیه تلفن همراه کنش‌گران ایرانی را مرور می‌کنیم.

۱- نسخه‌های جعلی تلگرام

همان‌طور که می‌دانید، بخش قابل توجهی از تعاملات دیجیتال ایرانیان روی پیام‌رسان تلگرام صورت می‌گیرد. پیام‌رسان تلگرام امکان ارتباط شنیداری و متنی کدگذاری‌شده را در شکلی برای کاربران فراهم می‌کند که مطلوب نظام‌های مستبد نیست. پس از سال‌ها تلاش برای فیلتر و قطع تلگرام، نهادهای وابسته به حکومت در ایران و البته گروه‌های هکری، اقدام به انتشار نسخه‌های موازی و بعضا حاوی بدافزار پیام‌رسان تلگرام کردند. این نسخه‌ها حتی در بازارهای داخلی اپلیکیشن‌ها مثل «کافه بازار» و حتی در «فروشگاه رسمی گوگل» برای نصب توسط کاربران عرضه شد. خطرناک‌ترین انواع این اپلیکیشن‌ها، اپ‌هایی بودند که فایل APK آن برای استفاده کاربران جایی در اینترنت آپلود می‌شد و لینک دانلود و آموزش نصب آن برای کاربران ارسال می‌شد. این نرم‌افزارهای آلوده که به بسیاری از حیاتی‌ترین منابع تلفن شما دسترسی داشتند، می‌توانستند صدای مکالمات

و صداهای پیرامونی دستگاه تلفن هوشمند شما را ضبط کنند، دوربین را روشن کنند، کلیدهای فشرده را ضبط کنند و عکس‌ها و فیلم‌های قبلاذخیره‌شده در تلفن را به سرقت ببرند. آن‌ها همچنین با دسترسی به موقعیت‌یاب تلفنِ قربانی می‌توانستند موقعیت جغرافیایی و رفت‌وآمدهای او را کنترل کنند.

تدابیر و ترفندها: چه باید کرد؟

اپلیکیشن‌هایی که با سوءاستفاده از نام اپلیکیشن‌های معتبر و معروف طراحی شده‌اند، عموما آلوده‌اند. «موبوگرام»، «تلگرام طلایی»، «تلگرام فارسی»، «واتس‌اپ فارسی» و «یاهوی فارسی»، همه و همه به دنبال سرقت اطلاعات حساس شما هستند. اساسا نام مشابه اپلیکیشن‌های مشهور می‌بایست خودش نوعی اعلام خطر باشد برایش شما.

۲- این اپلیکیشن را نصب کنید تا در قرعه‌کشی ۱۰ میلیارد تومانی ما شرکت کنید

دومین راه تهدید گروه‌های هکری علیه کنش‌گران ایرانی ارسال پیام‌های فریبنده‌ای است مانند: «این اپلیکیشن را نصب کنید تا در قرعه‌کشی ۱۰میلیارد تومانی ما شرکت کنید». گروه‌های هکری از عناوین فریبنده شبیه به این پیام، برای اغوا و فریب قربانیان استفاده می‌کنند، به این ترتیب که پس از نصب اپلیکیشن، هکر به تمام منابع حساس تلفن شما دسترسی خواهد داشت.

تدابیر و ترفندها: چه باید کرد؟

اساسا هیچ اپلیکیشن غیرضروری را نصب نکنید. تلفن، مخصوصا تلفن کاری و حساس شما، جای نصب اپلیکیشن برای شرکت در قرعه‌کشی، اپلیکیشن‌های بازی و سرگرمی، اپلیکیشن تبدیل صدای انسان به خروس و اپلیکیشن ناشناس و گمنام دوست‌یابی نیست. این اپلیکیشن‌ها، حتی اگر آلوده نباشند، تاکید می‌کنیم حتی اگر آلوده نباشند، به بسیاری از داده‌های حساس شما مثلا لیست آدرس یا دفتر تلفن شما دسترسی غیرضروری خواهند داشت.

حتی اگر اپلیکیشنی را نصب کرده‌اید که در ماه گذشته، سه ماه گذشته و گذشته کوتاه‌تر

از آن، هرگز آن را باز نکرده‌اید، بلافاصله همین امروز این اپلیکیشن را حذف کنید. اپلیکیشن کم‌تر، امنیت بیش‌تر.

۳- «اپلیکیشن جدید هوش مصنوعی فارسی را دیده‌ای؟»

سومین تهدید استفاده از تیترهای فریبنده و جذاب است برای ترغیب کاربران به دانلود اپلیکیشنی که حاوی بدافزار است. مثلا چنین پیامی به کاربران ارسال می‌شود: «اپلیکیشن جدید هوش مصنوعی فارسی را دیده‌ای؟». هدف این است که کاربر را به فروشگاه اپلیکیشنی مثل کافه‌بازار بفرستد. بخش بسیار بزرگی از بدافزارها و نرم‌افزارهای مورد استفاده هکرها در قالب اپلیکیشن‌های بازی و سرگرمی جاسازی می‌شوند، منتهی به دلیل مجهزبودن شرکت‌هایی مثل گوگل و اپل به ابزارهای شناسایی نرم‌افزارهای مخرب، شانس زیادی برای تایید عرضه در دو فروشگاه App Store و Google Play ندارند.

تدابیر و ترفندها: چه باید کرد؟

بسته به نوع تلفن شما، آی.او.اس یا اندروید، فقط و فقط دو فروشگاه اپلیکیشن امن برای شما در جهان وجود دارد: فروشگاه App Store، فروشگاه صد درصد رسمی شرکت اپل، و فروشگاه Google Play متعلق به شرکت گوگل. فروشگاه امنِ سومی در کار نیست. ممکن است بپرسید بسیاری از اپلیکیشن‌های ایرانی را در این دو فروشگاه نمی‌توان یافت. دلیل خیلی ساده‌ای دارد. به خاطر این‌که احتمالا امن نبوده‌اند و موازین و قواعد امنیتی گوگل و اپل را نقض کرده‌اند. فراموش نکنید در صورت دانلود اپلیکیشن از کافه‌بازار یا هر فروشگاه غیرمجاز دیگری، مسئولیت امنیت این اپلیکیشن با خود شما خواهد بود و بس.

۴- «این فایل می‌تواند تلگرام شما را سریع، قابل گذشتن از فیلتر و بسیار کارآمد کند، امتحان کن!»

مورد دیگر، انتشار فایل APK با عنوانی ترغیب‌کننده است. مثلا: «این فایل می‌تواند تلگرام شما را سریع، قابل گذشتن از فیلتر و بسیار کارآمد کند، امتحان کن!»

هکرها در بسیاری از موارد فایل‌های دستکاری‌شده APK را حتی به صورتی غیرهدفمند در مکان‌های مختلفی در وب آپلود می‌کنند تا قربانیان پس از جستجو به صورتی تصادفی آن

را دانلود و نصب کنند. پس از نصب فایل APK که مستلزم خاموش‌کردن کنترل‌های ایمنی تلفن هوشمند شما است، در اکثر موارد کنترل تلفن شما در اختیار هکرها قرار می‌گیرد.

تدابیر و ترفندها: چه باید کرد؟

دانلود و نصب فایل APK در ۹۹درصد موارد، برای کاربر معمولی، مساوی هک و از بین‌رفتن داده‌ها است. APK خطرناک است حتی اگر در توضیح آن نوشته شده باشد: پس از دانلود این APK شما یک‌میلیارد تومان جایزه خواهید برد. هرگز APK را دانلود و نصب نکنید. و در تلفن‌های خود گزینه دانلود از فروشگاه‌های شخص ثالث یا Third Party را تحت هیچ عنوانی فعال نکنید.

۵- ارسال فایل‌های آلوده برای کاربران با عنوان به‌روزرسانی

هکرهای مرتبط با جمهوری اسلامی ایران در بسیاری موارد با ارسال فایل‌های آلوده به قربانیان، ادعا کرده‌اند که برای بالابردن امنیت تلفن‌شان - مثلا بایستی واتس‌اپ خود را - توسط فایلی که برایشان ارسال شده، به‌روز کنند، غافل از این‌که خود این فایل در واقع بدافزاری برای هک تلفن قربانی است.

تدابیر و ترفندها: چه باید کرد؟

فعالان و کنش‌گران باید به این امر واقف باشند که اپلیکیشن‌های قابل اعتمادی مانند «اینستاگرام»، «واتس‌اپ» یا «جی‌میل»، خود قادرند خود را به‌روز کنند و هیچ نیازی به فایل جانبی برای این کار ندارند. علاوه بر آن، فروشگاه‌های Apple Store یا Google Play دائما از شما می‌خواهند که این اپلیکیشن‌ها را از داخل اپل‌استور یا گوگل‌پلی آپدیت کنید. اگر فایلی با عنوان آپدیت تلگرام یا واتس‌اپ و یا فارسی‌ساز یاهو دریافت کردید، یقین بدانید آن فایل آلوده است و به دنبال هک تلفن شما ست.

۶- وی.پی.ان‌ها و سرورهای پروکسی آلوده

حکومت ایران به شکلی گسترده اینترنت آزاد را فیلتر می‌کند. بنابراین بسیار طبیعی است که اکثریت کاربران ایرانی دائما به دنبال انواع و اقسام وی.پی.ان و سرورها و کانفیگ‌ها

(Configurations) مختلفی باشند که دسترسی آن‌ها به اینترنت آزاد را تسهیل کند. متاسفانه دستگاه‌های امنیتی و هکرهای مرتبط و غیرمرتبط با حکومت ایران در حد بسیار گسترده‌ای، از غیرقانونی‌بودن، و نبود شفافیت در بازار خرید و فروش وی.پی.ان سوءاستفاده می‌کنند. بخش بزرگی از وی.پی.ان‌های عرضه‌شده در ایران از معیارها و ضوابط شناخته‌شده وی.پی.ان در جهان پیروی نمی‌کنند. مثلا متاداده‌های مربوط به شهروندان و آدرس آی.پی آنان و بسیاری دیگر از داده‌هایشان را برای مدت طولانی ذخیره می‌کنند. امری که با توجه به الزامِ دارندگان تلفن همراه در ایران به رجیستری یا همان ثبت نام دستگاه، تقریبا مساوی احراز هویت آن‌ها است.

تدابیر و ترفندها: چه باید کرد؟

فقط و فقط از وی.پی.ان‌های معتبر بین‌المللی که امنیت اتصال و حریم خصوصی شما را رعایت می‌کنند، استفاده کنید. سایت‌هایی مثل تواناتک به صورت مرتب فهرستی از ابزارهای عبور از فیلترینگ را منتشر می‌کنند. از وی.پی.ان‌های مجانی استفاده نکنید. استفاده از ابزارهایی مانند «تور» و «سایفون» - البته اگر از سایت اصلی دانلود و نصب شوند - خطر کم‌تری دارند تا VPN های ناشناس و بعضا مجانی. بهترین کار برای انتخاب VPN، کمک‌گرفتن از فردی با اطلاعات عمیق از امنیت دیجیتال است.

علاوه بر تدابیری که گفتیم، همان‌طور که بارها تاکید کرده‌ایم سیستم عامل IOS و اندروید خود را دائما به‌روز کنید و برای آن ترکیبی از رمز عبور قوی و عوامل بیولوژیک مثل اثرانگشت تعیین کنید. همچنین در قسمت »اپلیکیشن‌های من» در گوگل‌پلی و اپ‌استور شرکت اپل، اپلیکیشن‌های خود را نیز به‌روز کنید. زیرا بسیاری از حملات علیه تلفن شما با استفاده از حفره‌های امنیتی اپلیکیشن‌های قدیمی صورت می‌گیرد.

۱۲ نکته ضروری برای مقابله با خطرات هک تلفن هوشمند توسط هکرهای حکومتی

در این بخش، به صورت خلاصه برای مقابله با خطرات ناشی از هک تلفن‌هوشمند توسط هکرهای مرتبط با حکومت ایران، ۱۲ نکته ضروری را یادآوری می‌کنیم.

۱- تلفن همراه خود و اپلیکیشن‌های آن را دائما به‌روز کنید.

۲- تلفن همراه خود را مجهز به رمز عبور قوی و تایید هویت بیولوژیک مثل اثر انگشت و مردمک چشم کنید.
۳- تلفن همراه خود را کدگذاری یا encrypted کنید، تنها در این صورت هنگام سرقت یا گم‌شدن تلفن می‌توان از امنیت نسبی داده‌های ذخیره‌شده مثل عکس‌ها و فیلم‌ها اطمینان حاصل کرد.
۴- تلفن شخصی و کاری جداگانه داشته باشید. فایل‌ها، صداها، فیلم‌ها و کلا داده‌های حساس شخصی نباید روی تلفن‌کاری شما باشند. از سوی دیگر داده‌های حساس کاری هم به هیچ وجه نباید روی تلفن شخصی شما منتقل شوند.
۵- به هیچ فرد دیگری اجازه ندهید از تلفن هوشمند شما استفاده کند. افراد حتی به طور ناخواسته می‌توانند تلفن شما را آلوده به ویروس و بدافزار کنند.
۶- قبل از فروش یا هدیه‌دادن تلفن خود، تمام فایل‌های آن را پاک و غیرقابل بازیافت کنید.
۷- از سرویس موقعیت‌یاب فقط و فقط در مواقع ضروری استفاده کنید.
۸- میزان دسترسی اپلیکیشن‌ها را دائما کنترل کنید. چه دلیلی دارد اپلیکیشن آشپزی به دوربین یا میکروفن یا لیست دوستان شما دسترسی داشته باشد؟
۹- تا حد امکان از تلفن دست‌دوم برای کارهای حساس استفاده نکنید. پس از خرید تلفن دست دوم تمام داده‌های آن را با برگرداندن به تنظیمات کارخانه پاک و سپس همه چیز را از نو نصب کنید.
۱۰- سرویس find my phone را فعال کنید. این سرویس می‌تواند موقعیت تلفن گم‌شده شما را به شما نشان دهد یا آن را از راه دور پاک کند تا داده‌های شما در تلفنِ به‌سرقت‌رفته مورد سوءاستفاده قرار نگیرد.
۱۱- تلفن هوشمند هر چند ماه یک‌بار نیازمند رفت و روب و نصب مجدد سیستم عامل و اپلیکیشن‌ها ست. این عمل نه تنها به امنیت دستگاه شما کمک می‌کند بلکه کارآیی آن را نیز بالا خواهد برد.
۱۲- در مکان‌های عمومی مثل هتل یا رستوران از وای‌فای استفاده نکنید. هکرها مخصوصا در اماکن عمومی می‌توانند از وای‌فای عمومی یا پابلیک برای نفوذ به تلفن شما استفاده کنند.

آزمون ارزیابی

لطفا با دقت به پرسش‌ها پاسخ دهید. این کار کمک می‌کند درک خود از مطالب درس را ارزیابی کنید. پاسخ‌های درست در بخش پاسخ‌نامه در پایان کتاب در دسترس است.

۱- کدام گزینه نادرست است؟

الف) ارتباط شنیداری و متنی کدگذاری نشده، برای نظام‌های مستبد مطلوب نیست

ب) حتی «فروشگاه رسمی گوگل» هم حاوی نسخه‌های حاوی بدافزار تلگرام بوده است.

ج) بعضی از فایل‌های APK می‌توانند صدای مکالمات و صداهای پیرامونی دستگاه تلفن هوشمند شما را ضبط کنند.

د) موبوگرام تنها نرم‌افزار موازی امن برای تلگرام بود اما تقریبا همه موارد دیگر ناامن بودند.

هـ) نمی‌دانم.

۲- کدام گزینه نادرست است؟

الف) نبود بسیاری از اپلیکیشن‌های ایرانی در «اپ استور» به دلیل ناامنی یا نقض موازین اپل است.

ب) فایل‌های APK با اطلاعات فنی یا عنوان ترغیب‌کننده منتشر می‌شوند.

ج) برای افزایش امنیت، نرم‌افزارهای پیام‌رسان را باید همواره با نصب و اجرای فایل‌های آپدیت، به‌روز کرد.

د) ذخیره طولانی‌مدت متاداده‌های شهروندان خلاف معیارهای شناخته‌شده وی.پی.ان است.

هـ) هیچ کدام / نمی‌دانم.

۳- کدام مورد بخشی از نکات ضروری مقابله با هک موبایل نیست؟

الف) تلفن شخصی و کاری جداگانه داشته باشید.

ب) سرویس Find My phone را فعال کنید.

ج) میزان دسترسی اپلیکیشن‌ها را کنترل کنید.
د) از سرویس موقعیت‌یاب استفاده نکنید.
هـ) نمی‌دانم.

جلسه هشتم
جمع‌بندی و مروری بر تجربیات فعالان قربانی حملات هکری

با صدای بلند اعلام کنید عملیات هکری در جریان است

در بیش‌تر موارد بررسی‌شده از سوی کارشناسان معتبر سایبری در جهان، هکرهای مرتبط با ایران معمولا از یک عملیات هک و از یک اتاق فرمان و کنترل مشترک، استفاده از ابزارهای مخرب را، همزمان علیه چند فعال مدنی، چند نهاد یا چند سازمان دنبال می‌کنند؛ نه فقط یک فرد! بنابراین اگر یک نفر از افراد مورد حمله، آگاهانه یا تصادفا متوجه شود که هدف حملات هکری دولتی قرار دارد، یا هدف عملیات فریب و اغوا در آینده نزدیک است یا اساسا هک شده است، نخستین واکنش باید، افشاء و اعلام بی‌درنگ ماجرا به صورت تمام و کمال باشد. نترسید!

کاربران عموما از اعلام این‌که فریب خورده‌اند، هک شده‌اند یا هدف عملیات هک و حمله قرارگرفته اند خجالت و شرم دارند. اما با اعلام عمومی بدون آن‌که باعث ترس و وحشت دیگران شوید، دهها و شاید صدها قربانی دیگر را نجات خواهید داد. کارشناسان سایبری جهانی بلافاصله مورد شما را به دنبال ردپای هکرهای مرتبط با ایران بررسی می‌کنند و مجموعه عملیات آنان شاید حتی قبل از شروع متوقف شود.

همان‌طور که در مثال مربوط به جعل هویت رها اعتمادی توسط هکرها در سال ۲۰۱۵ دیدیم اعلام ماجرا با صدای بلند و به روشنی، عملیات را علیه ده‌ها هدف دیگر ناکام گذاشت؛ گرچه پیش از آن شماری اندک از فعالان فریب حساب جعلی موسوم به رها اعتمادی را خورده بودند، بدون آن‌که حتی خود متوجه شده و طبعا دیگران را مطلع کرده باشند.

مورد دیگر در سال‌های اخیر اعلام عمومی فردی به نام سارا شکوهی است. پروفایل جعلی فردی با ظاهری جذاب توسط APT۳۵ به عنوان محقق و همکار «شورای آتلانتیک» ایجاد می‌شود و با شمار زیادی از افراد فعال و مرتبط با ایران اقدام به برقراری تماس می‌کند. مثلا برای یک کارشناس دیگر، فایل آلوده حاوی درخواست مصاحبه راجع به پروژه‌ای مربوط به ایران می‌فرستد.

هالی دگرس (HOLLY DAGRES)، از کارشناسان ایرانیِ این نهاد، پس از آن‌که ماجرا را می‌شنود به‌روشنی و با بهترین انتخاب از طریق شبکه‌های اجتماعی اعلام می‌کند که «سارا شکوهی» وجود خارجی ندارد و این یک عملیات هک و فیشینگ است. او از همه افرادی که از آن‌ها درخواست مصاحبه شده، می‌خواهد که سریعا رمزهای عبور خود را عوض کنند.

به کوچک‌ترین نشانه‌ها دقت کنید

وقتی مشغول استفاده از جی‌میل هستید، در پایین سمت راست تصویر، همیشه دو واژه را می‌توانید مشاهده کنید: Last activiy و Details. آخرین زمان فعالیت شما آن‌جا نمایش داده می‌شود، اما مثلا اگر همه ۸ ساعت گذشته را خواب بوده و تلفن و کامپیوتر شما خاموش بوده‌اند، اگر آخرین فعالیت شما زمان ۳ ساعت گذشته را نشان می‌دهد، اندکی مایه نگرانی است. و این سوال باید پیش بیاید که چه کسی مشغول فعالیت با گوگل شما بوده؟

روی گزینه Details کلیک کنید، آن‌جا نشانه‌های IP و آدرس‌های اینترنتی که از آن برای اتصال به گوگل شما استفاده شده را خواهید دید. باید چک کنید که آیا همه آن‌ها همسان یا مربوط به کشور و شهر محل سکونت شما هستند؟ توجه کنید که این آی.پی‌ها می‌تواند متفاوت باشد. مثلا در صورتی که از وی.پی.ان یا سرویس‌هایی مثل

«پروکسی» (Proxy) یا «تور» (Tor) استفاده می‌کنید. یا این‌که همزمان با یک تبلت، موبایل و کامپیوتر یکی با وای‌فای خانه و دو دستگاه دیگر با دو سیم‌کارت متفاوت به اینترنت متصل‌اید. اما اگر در هفت ساعت گذشته فردی مثلا از ترکیه یا چین یا آمریکا به اکانت گوگل شما دسترسی داشته در حالی که شما در ایران زندگی می‌کنید، این واقعا مایه نگرانی است و می‌بایست سریعا رمزهای عبور خود را عوض کنید و سیستم تایید هویت دومرحله‌ای را فعال کنید.

همیشه این نشانه‌های کوچک است که پرده از بزرگ‌ترین عملیات هک بر می‌دارد. مواردی مثل ایمیلی که شما نفرستاده‌اید اما دوستی می‌گوید دریافت کرده، سبزبودن چراغ حساب و آنلاین‌بودن شما در واتس‌اپ و تلگرام وقتی که تلفن‌تان خاموش بوده، ایمیل‌هایی که خوانده یا پاک شده‌اند اما شما آن‌ها را باز نکرده‌اید.

هکرهای دولتی هم مثل همه تبهکارانِ دیگر ممکن است حتی علی‌رغم توجه به ریزترین جزئیات، اشتباه کنند. دقت شما این اشتباه آنان را می‌تواند تبدیل به شکست سهمگین عملیات هک علیه ده‌ها و صدها فعال و کنش‌گر دیگر کند.

چرا می‌خواهند شما را هک کنند؟

متاسفانه بیش‌تر عملیات هک حکومتی در ایران، اگر انتخاب هدف به صورتی آگاهانه صورت پذیرفته باشد، کور و بی‌هدف نیست و برای کسب اطلاعات، جهت پروژه‌ای خاص انجام می‌شود. بیش‌تر این عملیات برای تحت‌فشارقراردادن زندانیان سیاسی، گرفتن اعتراف اجباری و شوهای تلویزیونی پروپاگاندای جمهوری اسلامی مورد استفاده قرار می‌گیرند.

هکرها نیازمند اسناد و مدارکی هستند تا دروغ‌های خود را برای مخاطبان باورپذیر کنند. اما ماجرا می‌تواند از این هم جدی‌تر باشد. متاسفانه برخی از این موارد قدری نگران‌کننده‌اند. بگذارید مثالی بزنیم:

محققی ساکن اروپا که سال‌هاست در مورد ایران مطالعه کرده، برای دیدار خانواده‌اش راهی ایران است. چند هفته قبل از سفر، متوجه می‌شود که از حساب گوگل او یک Take Out صورت گرفته است. Take out دانلود صدها مگابایت یا ده‌ها گیگابایت داده‌ی مربوط به حساب کاربر از سرورهای شرکت گوگل است. تمام تصاویر ذخیره‌شده در حساب گوگل، ایمیل، تاریخچه مرورگر، تاریخچه جستجو، تاریخچه موقعیت‌یاب مکانی، چت‌های

گوگل و تمام فایل‌های درایو، Google Doc و دیگر نسخه‌های پشتیبانِ شما را می‌توان با یک کلیک از سرورهای گوگل به طور یکجا و در قالب چند فایل دانلود کرد.

این محقق، خودش درخواست Google Take out نکرده پس حتما فرد دیگری داده‌های او را به سرقت برده است. همین اتفاق برای فیس‌بوک او هم افتاده است. البته او بدون این‌که بداند، آرشیو واتس‌اپ خود را هم در گوگل درایو ذخیره کرده است. پس آن‌را هم برده‌اند.

سوال این است که چرا، احتمالا دولت ایران به دنبال همه‌ی این اطلاعات است؟ پاسخ دقیق به این سوال ناممکن است، اما احتیاط می‌گوید در شرایطی که بسیاری از اطلاعات سرقت‌شده می‌تواند به فشار بر او، بازداشت و آزار او و دیگران بینجامد، ضمن اعلام علنی موضوع، متاسفانه می‌بایست سفر خود به ایران را هم متوقف و لغو کند.

مثال‌های مشابهی از شرکت در یک کنفرانس، ملاقات با فردی ناشناس، سفر به یک کشور سوم و خصوصا درخواست مصاحبه‌هایی با وب‌کم وجود دارد. هک همیشه باید این سوال را برای شما به وجود آورد که چرا؟ آن‌ها به دنبال چه هستند و با این داده‌ها چه خواهند کرد؟

سه تدبیری که هکرهای حکومتی بیش از هر چیز از آن واهمه دارند

۱- تنظیم رمز عبور چند مرحله‌ای

عبور از رمزگذاری چندمرحله‌ای، مثلا رمز عبور قوی، تایید هویت بیومتریک، تایید هویت با یک دستگاه مطمئن، قفل سخت‌افزاری و بعد نرم‌افزارهایی مثل گوگل Authenti-cator بدترین خبر برای هکرها ست. هر کدام از این اقدامات مانع بسیار اساسی بر سر راه هکرها هستند. خصوصا مواردی مانند قفل‌های سخت‌افزاری یا موارد بیولوژیک واقعا قادرند هکرها را در میانه راه متوقف کنند. بنابراین تلفن‌همراه، حساب‌های گوگل و کلا سخت‌افزارهای حاوی داده‌های حساس خود را به این موارد مجهز کنید.

۲- رمزگذاری یا Encryption داده‌ها

رمزگذاری داده‌ها، مثلا استفاده از File Vault در کامپیوترهای Apple، یا BitLocker و Device encryption ویندوز و مشابه آن در دستگاه‌های اندروید و آی.او.اس و

همچنین کلا رمزگذاری هر نوع فلش‌دیسک، هارددیسکِ اکسترنال و کارت حافظه‌ی حاوی اطلاعات حساس، مشکلات بزرگی را برای هکرهای این نوع سخت‌افزارها و حتی سارقان فیزیکی خلق خواهد کرد. فقط توجه داشته باشید که اگر رمز عبورِ فایل‌های رمزگذاری‌شده را فراموش کنید، به احتمال ۹۹.۹۹ درصد آن‌ها را برای همیشه از دست خواهید داد. پس در حفظ این رمزهای عبور جدی باشید.

۳- گرفتن نسخه پشتیبان از اطلاعات

یکی از ترفندهای هکرها برای حمله به نهادهای مدنی و فعالان، نابودی داده‌ها و ایجاد مشکل و توقف فعالیت‌های آنان است. مثلا شما ده‌هاهزار صفحه سند و گفت‌وگو از موارد نقض حقوق بشر را جمع‌آوری کرده‌اید یا فیلم مستندی از فساد دولتی آماده پخش دارید بر مبنای اطلاعات یک دفتر حقوقی که به مدارک مهمی از بی‌قانونی دست یافته است. طبیعتا هکرهای دولتی به دنبال نابودی این اسنادند. اما اگر چند نسخه پشتیبان داشته باشید، مثلا یک نسخه روی گوگل‌کلاود به صورت فشرده و رمزگذاری‌شده، دیگری روی Dropbox یا OneDrive و همچنین نسخه سومی روی کارت حافظه‌ای با رمزگذاری قوی ذخیره شده باشد، حتی با هک نیمی از این حساب‌ها باز هم فایل‌های شما برای همیشه از بین نخواهد رفت.

آزمون ارزیابی

لطفا با دقت به پرسش‌ها پاسخ دهید. این کار کمک می‌کند درک خود از مطالب درس را ارزیابی کنید. پاسخ‌های درست در بخش پاسخ‌نامه در پایان کتاب در دسترس است.

۱- کدام گزینه درست است؟

الف) نخستین واکنش پس از آگاه‌شدن از حمله یا هک، اعلان آن است.
ب) پس از آگاه‌شدن از حمله یا هک، اعلان عمومی آن موجب افزایش خطر می‌شود.
ج) عملیات هک عموما با تمرکز هکرها بر یک فرد انجام می‌شود.
د) مورد حمله هکری به اسم حساب رها اعتمادی، به دلیل واکنش درست به آن، عملیات را متوقف نمود
هـ) نمی‌دانم.

۲- کدام گزینه درست است؟

الف) در ماجرای شورای آتلانتیک، هویت واقعی هالی دگرس در واقع سارا شکوهی بود.
ب) ماجرای شورای آتلانتیک حمله فیشینگ نبود.
ج) سارا شکوهی از روی یک فایل آلوده قربانی هکرها شده بود.
د) درخواست عمومی تغییر رمز عبور در ماجرای شورای آتلانتیک برای افزایش امنیت بود.
هـ) نمی‌دانم.

۳- کدام گزینه نادرست است؟

الف) شما می‌توانید آی.پی‌های متصل به سرویس گوگل خود را مشاهده کنید.
ب) اگر سرویس «لست اکتیویتی» در جی‌میل، شما آخرین فعالیت شما را کم‌تر از دوازده ساعت نشان دهد، نشانه خطر است.
ج) آی.پی‌های خود شما در هنگام استفاده از سرویس تور می‌تواند متنوع باشند.
د) بعضی از عملیات هک حکومتی به صورت کور و بی‌هدف صورت می‌گیرد.
هـ) نمی‌دانم.

پاسخ‌نامه

در این بخش پاسخ‌های پرسش‌های آزمون ارزیابی درس‌ها را مشاهده می‌کنید.

درس یک: ۱: د / ۲: ب / ۳: الف
درس دو: ۱: ج / ۲: ب / ۳: ج
درس سه: ۱: الف / ۲: ب / ۳: د
درس چهار: ۱: ج / ۲: د / ۳: ج
درس پنج: ۱: ج / ۲: الف / ۳: د
درس شش: ۱: ج / ۲: د / ۳: ج
درس هفت: ۱: د / ۲: ج / ۳: د
درس هشت: ۱: الف / ۲: د / ۳: ب