کسب و کار هکرها در ۱۰ پرده

نگاهی به جزوه‌ی یک هکر

هکرها
چگونه فکر می‌کنند
و
چگونه به سیستم
شما وارد می‌شوند

جزوه‌ای برای کسب سود از طریق حملات هدفمند

قبل از اینکه به جزئیات تکینک‌های یک کلاهبرداری بی عیب و نقص و پول‌ساز بپردازیم، بیایید نگاهی بیاندازیم به اصول این نمایش.

قبل از هر چیز، این چیزی است که ما نمی‌خواهیم‌انجام دهیم. برنامه‌ی ما این نیست که تمام اینترنت را با بدافزارها و هرزنامه‌ها پر کنیم یا میلیون‌ها وبسایت را با تزریق SQL آلوده کنیم.

ما بر اساس آسیب‌پذیری‌هایی که پیدا می‌کنیم، کار خود را به شرکت‌ها و صنایعی محدود می‌کنیم. و سپس با علم به اینکه دیگر کمپانی‌ها از همان آسیب‌پذیری رنج می‌برند کار خود را گسترش می‌دهیم.

اگر این کار را درست انجام دهید به گنجینه ای از داده‌های با ارزش دست خواهید یافت. با استفاده از این داده‌ها می‌توانید از ملت اخاذی کنید یا آن‌ها را به رقبا - و یا حتی دولت‌ها - بفروشید.

۷۶٪

سازمان‌های آلوده شده به فرد دیگری نیاز داشتند که به آن‌ها بگوید آلوده شده اند

۴۸٪

سازمان‌ها توسط هیئت‌های رگولاتوری از این امر آگاه شدند

۲۵٪

آن‌ها توسط نهادهای اجرای قانون آگاه شدند

۱٪

توسط مردم

۲٪

توسط یک طرف‌سوم

پرده‌ی ۱: طبق برنامه دست به حمله زدن

برویم سر اصل مطلب که به دست آورد پول ساده باشد. بیشتر اوقات، انجام حملات رقت‌انگیز هدفمند پنج مرحله دارد:

تحقیق‌کنید: کار خود را با بررسی هدف مورد نظر آغاز کنید. درون اطلاعاتی که در دسترس عموم قرار دارد کندوکاو کنید و با راه خود را به درون اطلاعات قابل استخراج درباره‌ی سیستم‌های IT آن‌ها مهندسی اجتماعی کنید.

نفوذ کنید: از این اطلاعات برای یافتن کارمند مناسب برای فیشینگ با نیزه استفاده کرده و پس از پیدا کردن آسیب‌پذیری مناسب آن را با کدهای مخرب خود آلوده کنید.

منتشرشوید: پس از اینکه یک سیستم را تصاحب کردید، از اتصالات آن استفاده کنید تا در شبکه پخش شوید. از این رو اگر در یک سیستم شناسایی شدید هنوز روی دیگر سیستم‌ها کنترل خواهید داشت.

آلوده‌کنید: هنگامی که با تمامی‌سوراخ سنبه‌ها و قلق‌های شبکه و اتصالات هدف آشنا شدید، ابزارهای بیشتری نصب کنید تا به نحوی جدی داده‌ها را به سرقت برده و آن‌ها را جمع‌آوری کنید.

تخلیه‌کنید: آخرسر، باید تمامی‌داده‌ها را از آن جا خارج کنید. از میان تمامی گزینه‌هایی که دارید، ترافیک عمومی‌وب عملکرد خوبی خواهد داشت.

با این پول تنها یک ماشین فراری نخواهید خرید.
می‌توانید یک ناوگان از آن‌ها را بخرید.

پرده‌ی ۲: تخصص‌سپاری و برون‌سپاری

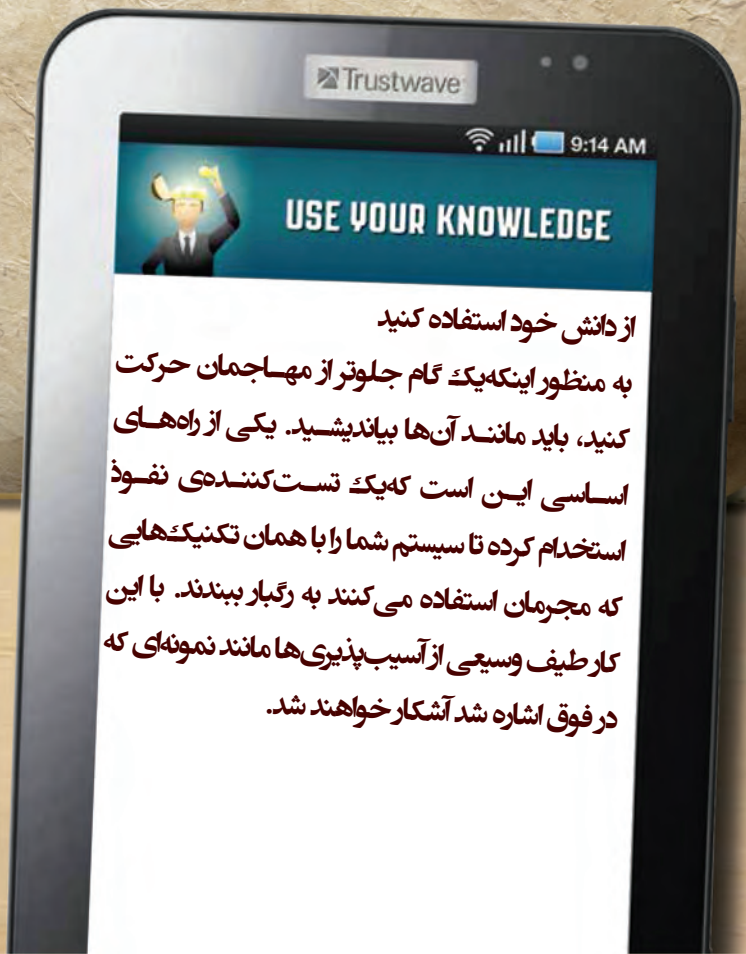
مساله این نیست که شما چه می‌دانید، مساله این است که چه کسی را می‌شناسید. تیم مافیایی خود متشکل از تخصص‌های مختلف را دور هم جمع کرده تا کمپین چندمرحله‌ای خود را به اجرا بگذارید. همانند غارنشین‌ها که کار را به دو قسمت یعنی شکار و جمع‌آوری تقسیم می‌کردند، شما هم کارها را به هک‌کردن و کلاهبرداری تقسیم کنید.

تیم را همانگونه که دوست دارید تشکیل دهید. افرادی را استخدام کنید، منابع را به عرضه‌کنندگان کیت‌های بدافزاری برون‌سپاری کنید، حتی می‌توانید در خلال یک شراکت مساوی کار کنید.

فقط یادتان باشد: جایی برای تازه‌کارها نیست. اگر آن‌ها نتوانند **caps lock** را پیدا کنند یا آن را هجی کنند، یا مهارت‌های کدنویسی آن‌ها بهتر از یک بچه‌ی خردسال نباشد، بهترین کار خداحافظی است.

$$> \frac{۱}{۳}$$

بیش از یک سوم نفوذ به داده‌های سازمان‌ها در خلال کسب‌وکارهای فرانشیز صورت می‌پذیرد.



پرده‌ی ۳: حملات خود را گسترش دهید

بعد از اینکه تیم کماندویی خود را تشکیل دادید، باید تمام آسیب‌پذیری‌ها را تا قطره‌ی آخر بخشکانید.

آیا به‌یک اکسپلویت برای یک آسیب‌پذیری جدید در سیستم POS یک خرده فروشی دست پیدا کرده‌یا آن را خریداری کرده‌اید؟ شاید این POS متعلق به‌یک بقالی کوچک در سانفرانسیسکو باشد، ولی شاید هم همان آسیب‌پذیری و پیکربندی سیستم در تمامی‌دستگاه‌های POS متعلق به فرانشیزهای همان برند حاکم باشد.

پس، عزیزم، بلیط شما پانچ شده و غذا حاضر است. می‌توانید ده‌ها برابر داده به سرقت ببرید، ولی تنها زحمت نفوذ به‌یک مکان را به خود بدهید.

لیست تخصص های مجرمان سایبری براساس FBI

- کدنویس ها: آنهایی که بدافزار و ابزارهای سرقت داده می نویسند.
- فروشندگان: داده‌های به سرقت رفته، بدافزارها و غیره
- متخصصان ITمجرم: گردانندگان زیر ساخت های خرابکارانه مانند سرورها
- هکرها: آلوده کننده های نرم افزارها و آسیب پذیری های شبکه
- کلاهبردارها: مهندسان اجتماعی، فیشرها و...

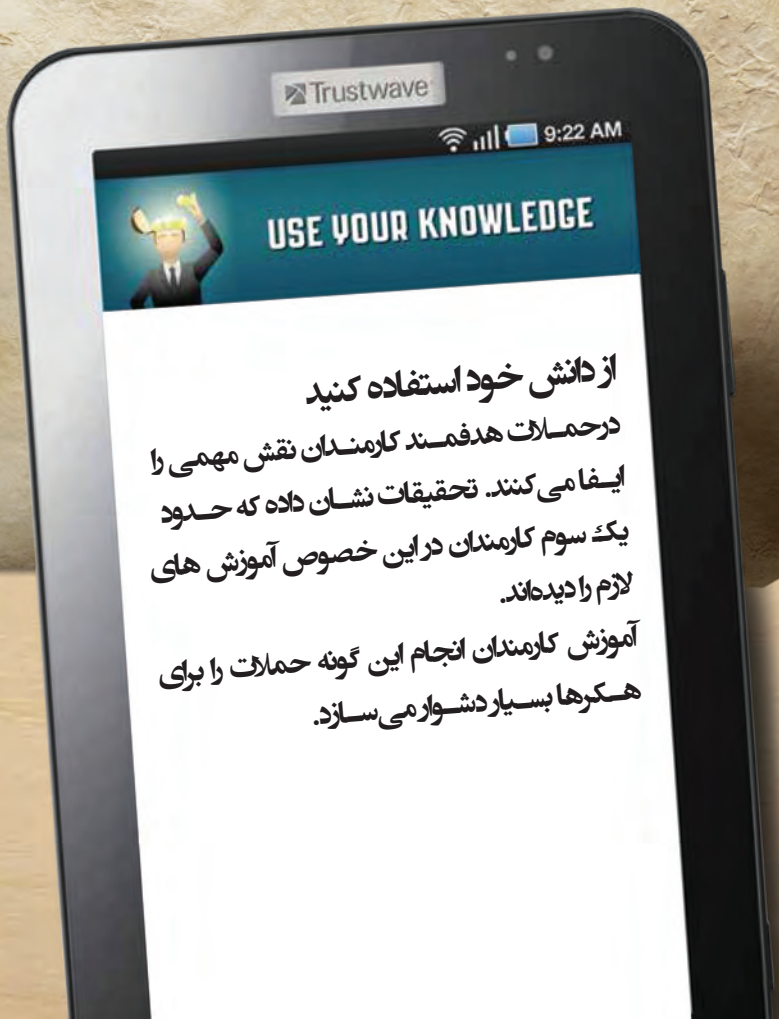
پرده‌ی ۴: بازی نکنید، از بازیگر بازی بگیرید

به احتمال زیاد کارمندان هدف بیشتر از آنچه که فکرش را بکنید و حتی بدون آگاهی شما بسیار کمکتان کنند. آن‌ها به شما اطلاعات می‌دهند، شما را کمک می‌کنند تا بدافزارها را روی سیستم شان بارگذاری کنید، و حتی هنگامی‌که نیاز داشته باشید دزدکی وارد یک ساختمان شوید در را برایتان باز نگه می‌دارند. این گونه آدم‌ها باید در دو مرحله‌ی نخست حمله‌یعنی تحقیق و نفوذ، بهترین دوستان شما باشند.

• اگر به اطلاعات نیاز داشتید – در مورد چارت سازمانی، موقعیت مکانی دیتاسنتر، تکنولوژی‌هایی که استفاده می‌کنند – با فردی که این اطلاعات را در اختیار دارد تماس بگیرید و وانمود کنید که از دپارتمان دیگری هستید و به سادگی هر چه تمامتر فقط سوالات خود را بپرسید. از هر ده بار، نه بار این کارمندان با مهربانی تمام پاسخ شما را خواهند داد.

۳۰٪

شرکت‌های بزرگ اذعان داشتند که مهندسی اجتماعی در هر رویداد به طور متوسط ۱۰۰۰۰۰ دلار برایشان زیانبار بوده است.



• موارد اورژانسی که واقعی و رسمی‌به نظر برسند همیشه جواب خواهند داد. طوری عمل کنید که گویی برای انجام یک پروژه‌ی حیاتی به کمک نیاز دارید و در غیر این صورت سرتان از تن جدا خواهد شد. این روش زمانی به نحو احسن کارآمد خواهد بود که نام رئیس رئیس آن‌ها را بدانید.

• اگر کارمند هدف شما در ردیف بالای زنجیره‌ی غذایی قرار داشته و آنقدر همه را دشمن می‌پندارد که در دام طعمه‌ی شما قرار نمی‌گیرد، سعی کنید فرد دیگری از هم‌رکاب‌های وی را انتخاب کنید و روی او کار کنید. بسیاری از ادمین‌ها – حتی ادمین‌های موقت – در ایستگاه‌هایی اقامت دارند و به سیستم‌هایی دسترسی دارند که کامپیوتر روسا هم به آن متصل است.

• تبریک می‌گم – شما یک شغل در منابع انسانی را احراز کرده‌اید. وانمود کنید که‌یک استخدام‌کننده هستید. در این بازار، قضاوت افراد کاملاً تحت تاثیر قرار خواهد گرفت اگر فکر کنند شغل جدیدی در افق نمایان است.

• بسته به اینکه چقدر می‌خواهید روی این حمله مانور دهید، حتی ممکن است لازم باشد روی مهندسی اجتماعی عینی سرمایه‌گذاری کنید. یک یونیفرم تحویل‌دهنده‌ی کالا بپوشید، چند شاخه گل بیاورید و ببینید که آیا شما را به داخل ساختمان راه می‌دهند یا خیر.

۴۸٪

شرکت‌های‌بزرگ طی دوسال‌اخیرمورد تهاجم حملات مهندسی اجتماعی قرار گرفته‌اند

۷۰٪

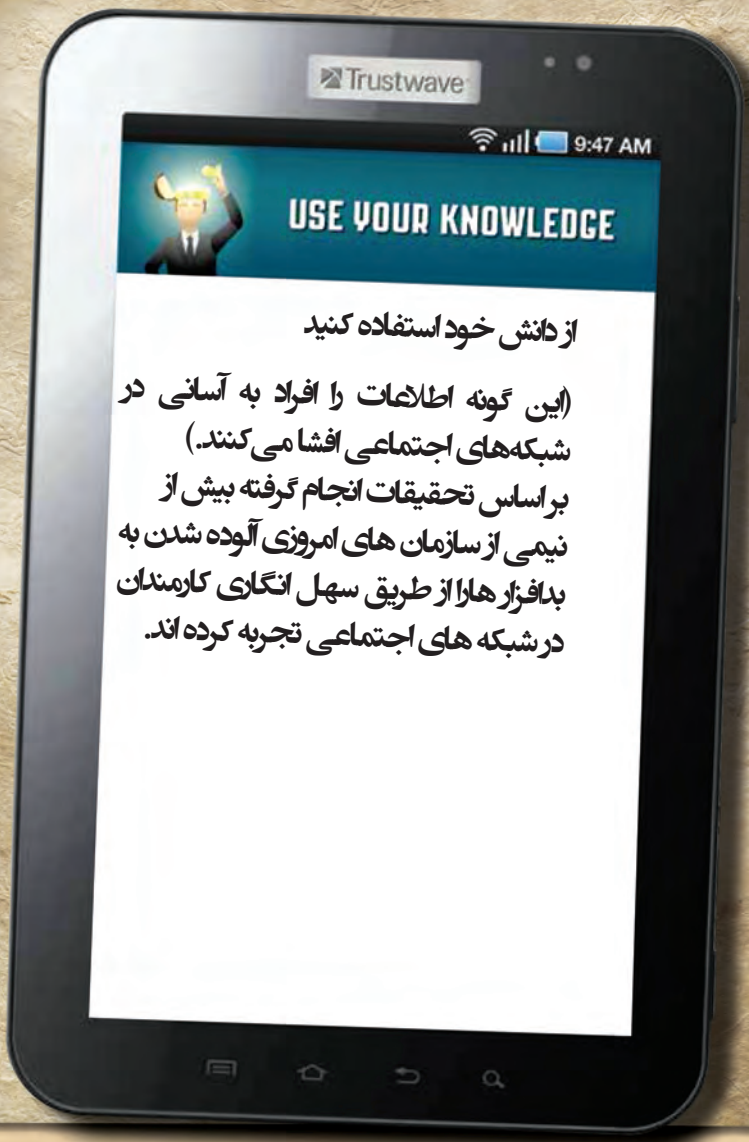
کارمندان جوان مرتباً خط‌مشی‌های IT را نادیده می‌گیرند

SOURCES:

[1]www.securingthehuman.org/blog/2011/09/22/justifying-your-awareness-program-with-social-engineering-survey

[2]www.eweek.com/c/a/Security/Younger-Employees-Ignore-IT-Policies-Dont-Think-About-Security-Says-Cisco-274940/

[3]www.securingthehuman.org/blog/2011/09/22/justifying-your-awareness-program-with-social-engineering-survey



۳۲/۸٪

گذرواژه‌ها حاوی نام‌هایی هستند که جزء ۱۰۰ نام پرطرفدار دختر و پسر هستند.

۱۶/۷٪

گذرواژه‌ها حاوی نام‌هایی هستند که جزء ۱۰۰ نام پرطرفدار برای سگ‌ها هستند.

پرده‌ی ۵ : برای بررسی‌های بهتر اجتماعی شوید

گاهی حتی نیاز نیست که در مورد یک سری اطلاعات از کارمندان سوال کنید. چون خودشان این اطلاعات را روی توئیتر خود پست می‌کنند. از رسانه‌های اجتماعی استفاده کنید تا انواع داده‌ها و اطلاعات شیرین را کسب کنید. با ساختن یک صفحه‌ی فیسبوک قلابی و فریب دادن دیگری به دوست شدن با وی ممکن است به اطلاعات زیر دست پیدا کنید:

•به چه دبیرستان یا کالجی می‌رفتند
نام خانوادگی قبل از ازدواج مادرشان
•تاریخ تولدشان
•اسم حیوان خانگی
•حقایقی در مورد شغلشان: عنوان، ارتقای شغلی، نام رئیس، پروژه‌های بزرگی که در راه هستند و غیره.

همه‌ی این‌ها ممکن است اشاره‌هایی به گذرواژه‌ها، یا پاسخ به سوالات ورود به سیستم باشند که می‌توانند راه را برای کمپین هدف شما هموار کنند. حتی اگر مستقیماً با فرد دوست نشوید، می‌توانید با دوست شدن با یکی از دوستان وی، به اطلاعات مهم دست پیدا کنید. به نحوی خبیثانه هوشمند، نه؟

همچنین برای تشکیل یک پرونده‌ی روانی از یک کارمند که معلوم می‌شود همان ابزاری است که می‌تواند شما را در نفوذ اولیه‌یاری دهد، شبکه‌های اجتماعی بسیار خوب عمل می‌کنند. اگر بدانید که چه سرگرمی‌هایی را دنبال می‌کنند، از چه تیم‌هایی حمایت می‌کنند و یا هر گونه اطلاعات شخصی دیگر، آن گاه می‌توانید طعمه‌ی بهینه را ساخته و او را به بازدید از سایت آلوده شده‌یا باز کردن سند مخرب ترغیب کنید.

«امروزه مجرمان سایبری از موتورهای جست و جو و شبکه های اجتماعی برای نفوذ به شرکت های بزرگ استفاده می کنند.»

– بایرون آکوهیدو

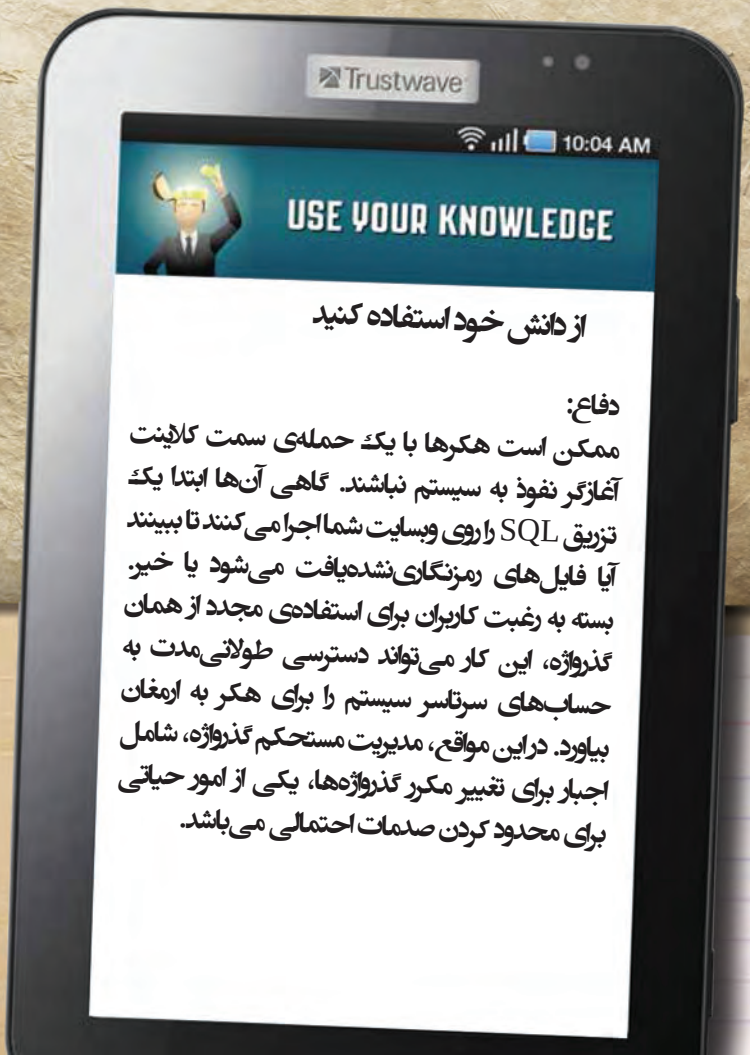
پرده‌ی ۶: به دنبال هر نقطه ضعف ممکن بگردید

چرا پنجره را بشکنید وقتی که کلید در ورودی را در دست دارید؟ در هر قسمت از راه به دنبال اطلاعات ورود کاربری باشید. هدف شماره دو این است که با معماری زیرساخت‌های IT شرکت هدف آشنا شده تا جعبه‌ابزار بدافزاری مناسب را انتخاب کرده یا اینکه چیزی را بسازید که بتواند به شما در بازگشایی قفل‌های شناخته شده کمک کند. این اطلاعات ممکن است هرچیزی باشد، از فایل‌های رمزنگاری شده گرفته تا آدرس‌های IP شرکت تا اطلاعات مربوط به نسخه‌ی دارایی‌هایی که سازمان پیاده‌سازی کرده است.

تقریبا شبکه‌ی هر شرکتی که فکرش را بکنید به اندازه‌ی اینجا تا ماه دارای آسیب‌پذیری می‌باشد. حتی اگر شرکت هدف شما عاری از آسیب‌پذیری بود، به احتمال زیاد یک فروشنده‌ی طرف‌سومی یا شرکت شریکی که راهی به شبکه دارد دارای این آسیب‌پذیری‌ها می‌باشد.

۳۰٪

تجهیزات ApacheTomcat که دارای رابط اداری دسترس‌پذیر می‌باشد دارای گذرواژه‌ی پیش فرض هستند.



The most common corporate password is Password1, because it just barely meets the minimum complexity requirements of Active Directory for length, capitalization and numerical figures[6]

آیا باید از آسیب‌پذیری‌های روز صفری که هنوز توسط شرکت عرضه‌کننده وصله نشده اند استفاده کنید؟ بله، قطعاً. اگر به اندازه‌ی کافی باهوش باشید، این کار نقش بزرگی را در برنامه‌ی شما ایفا خواهد کرد.

آسیب‌پذیری‌های روزصفر عالی هستند. ولی پیدا کردن و اکسپلویت آن‌ها هزینه‌بردار است، و این در حالی است که آسیب‌پذیری‌های شناخته‌شده ممکن است کاملاً باز باشند و باز باقی بمانند. بیشتر دپارتمان‌های IT آنقدر سرشان شلوغ است که زحمت وصله کردن حفره‌های امنیتی را به خود نمی‌دهند.

در موقعیت‌هایی که به دنبال اطلاعات بسیار خاصی می‌باشید، مثلاً شماتیک‌ها و طرح‌های ساخت که می‌خواهید برای یک شرکت رقیب یا یک دولت دیگر به سرقت ببرید، و در آن از شناسایی شدن بسیار احتراز می‌کنید، سر کیسه را شل کردن و پرداختن به کشف و اکسپلویت روزصفر منطقی می‌باشد.

ولی اگر موضوع انتشار بدافزار در یک شرکتی است که می‌دانید (با حدس می‌زنید) دارای سیستم‌های وصله‌نشده است، منطقی تر این است که از آسیب‌پذیری‌های قدیمی آن استفاده کنید.

۴۲٪

سازمان‌هادارای پرسنل IT هستند که‌گذرواژه‌هایا دسترسی به‌سیستم‌ها و اپلیکیشن‌ها را به اشتراک می‌گذارند.

۴۸٪

آن‌هاگذرواژه‌های اعطایی را ظرف مدت ۹۰ روز تغییر نمی‌دهند

۴۰٪

یا بیشتر از سازمان‌ها دارای فرآیندهای‌غیررسمی‌وصله کردن هستند و یا اصلاً برنامه‌ی مناسبی برای آن ندارند.

SOURCES:

[4]www.liebsoft.com/Password_Security_Survey/

[5]www.liebsoft.com/Password_Security_Survey/

[6]www.trustwave.com/global-security-report

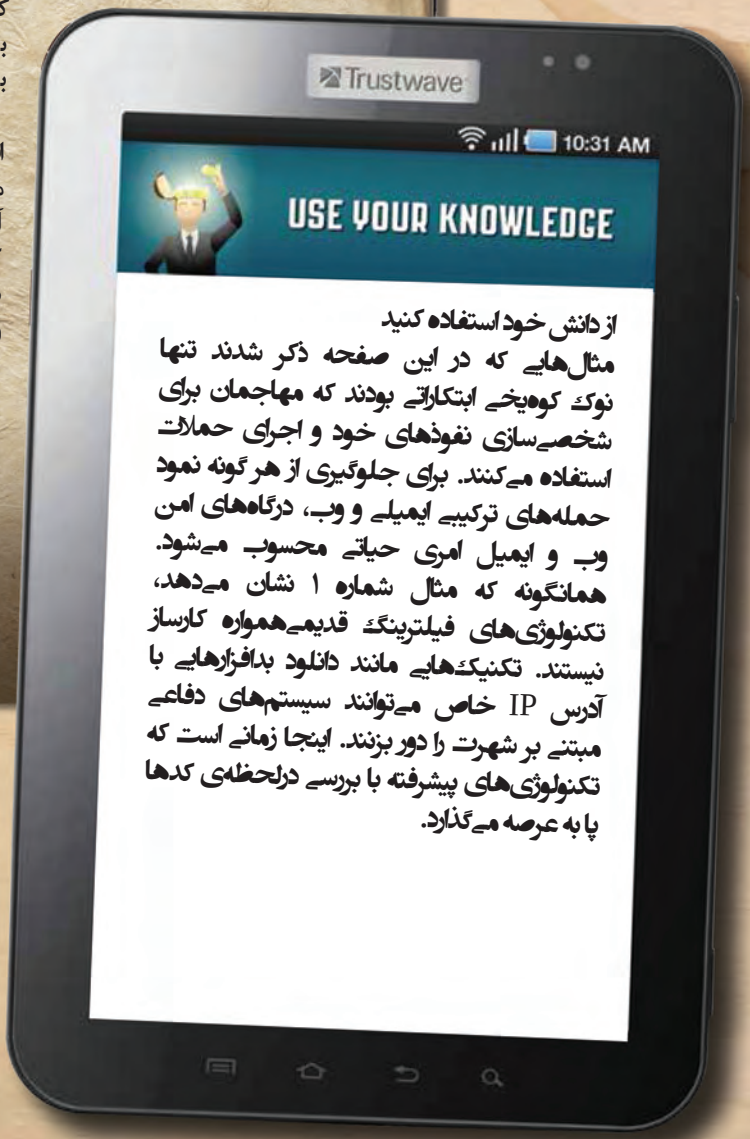
[7]https://securosis.com/assets/library/main/quant-survey-report-072709.pdf

پرده‌ی ۷: حملات وب و ایمیل را بازابداع کنید

پس از اینکه خدمه‌ی شما تکالیف خود روی اهداف را به خوبی انجام دادند، زمان آن می‌رسد که قلاب‌های خود را به خط کرده و منتظر به دام افتادن قربانی شوید. برخی از موثرترین سناریوهای نفوذ بسیار قدیمی‌هستند – شما با ایمیل‌ها، پیغام‌ها و یا پیام‌های شبکه‌های اجتماعی مردم را مورد حملات فیشینگ قرار داده و آن‌ها را به بازدید از یک سایت آلوده‌یا دانلود یک فایل اجرایی مخرب ترغیب می‌کنید. اکنون از اطلاعاتی که جمع آوری کرده‌اید برای تناسب بیشتر این تعاملات استفاده کنید! طعمه‌ای بسازید که باورپذیر باشد و قلابی که آنقدر بی‌درد به نظر برسد که آن‌ها حتی حس نکنند به خشکی آورده شده‌اند.

این‌گونه‌عمل‌کنید:

مثال شماره ۱: هکرهای شما یک آسیب‌پذیری عالی را در پلتفرم نرم‌افزاری که عموما توسط شرکت‌های حوزه‌ی سرگرمی‌استفاده می‌شود پیدا کرده اند. ولی شما برای اکسپلویت آن به کنترل یک سیستم با دسترسی نیاز دارید. خوشبختانه، در جامعه‌ی سرگرمی‌افراد زیادی هستند که کشته‌ومرده‌ی شایعات هستند. از آنجایی که بسیاری از شرکت‌های هدف شما درهالیوود قرار گرفته اند، از تزریق **SQL** استفاده کرده تا برخی از سایت‌های محلی مربوط به شایعات را با کدی که روی



سیستم بازدیدکنندگان دانلود می‌شود آلوده کنید. برای اینکه از شناسایی شدن توسط فیلترهای مزاحم مبتنی بر شهرت و اعتبار در امان بمانید، آن را طوری تنظیم می‌کنید که تنها با سیستم‌هایی تعامل کند که دارای آدرس‌های IP از لس آنجلس باشند.

مثال شماره ۲: شما یک مدیر میانی حسابداری را پیدا می‌کنید که به سیستم‌هایی دسترسی دارد که حاوی بسیاری از اطلاعات باارزش مالی و داده‌های مشتریان است. در فیسبوک با او گرم می‌گیرید و او را قانع می‌کنید که در یک مجمع حرفه‌ای برای حسابداران او را دیده‌اید. از استاتوس‌های این دوست جدید شما می‌فهمید که وی علاقه‌ی زیادی به عکاسی دارد. پس به هکرها و کدنویس‌های خود می‌گویید که‌یک یک وبسایت مربوط به علاقه‌مندان به عکاسی را طراحی کرده و در آن کدها و فایل‌های دانلود درایوبای را بارگذاری کنند. هنگامی‌که او نکاتی در خصوص دوربین‌های SLR را مطالعه می‌کند، کدهای مخرب شما به صورت نهان در حال بارگذاری است.

مثال شماره ۳: شما به چارت سازمانی شرکت هدف خود دست پیدا کرده و در یک پست وبلاگ شرکت درمی‌یابیدکه آن‌ها در یک اقدام استراتژیک می‌خواهند جان اسمیت را در دپارتمان بازاریابی استخدام کنند. سپس یک حساب Gmail تحت عنوان مدیر منابع انسانی (HR manager) ساخته و از آن برای نوشتن یک ایمیل استفاده می‌کنید که وانمود می‌کند دفتر منابع انسانی طی یک اشتباه اطلاعات مربوط به حقوق و مزایای جان اسمیت را در اختیار همگان قرار داده است. کارمندان فایل پیوست JohnSmithCompensation.xls را باز کرده و... بنگ! کنجکاوی باعث مرگ شبکه شد.

۵۰٪

حملات هدفمند در ابتدا از استفاده از وب شروع می‌شوند

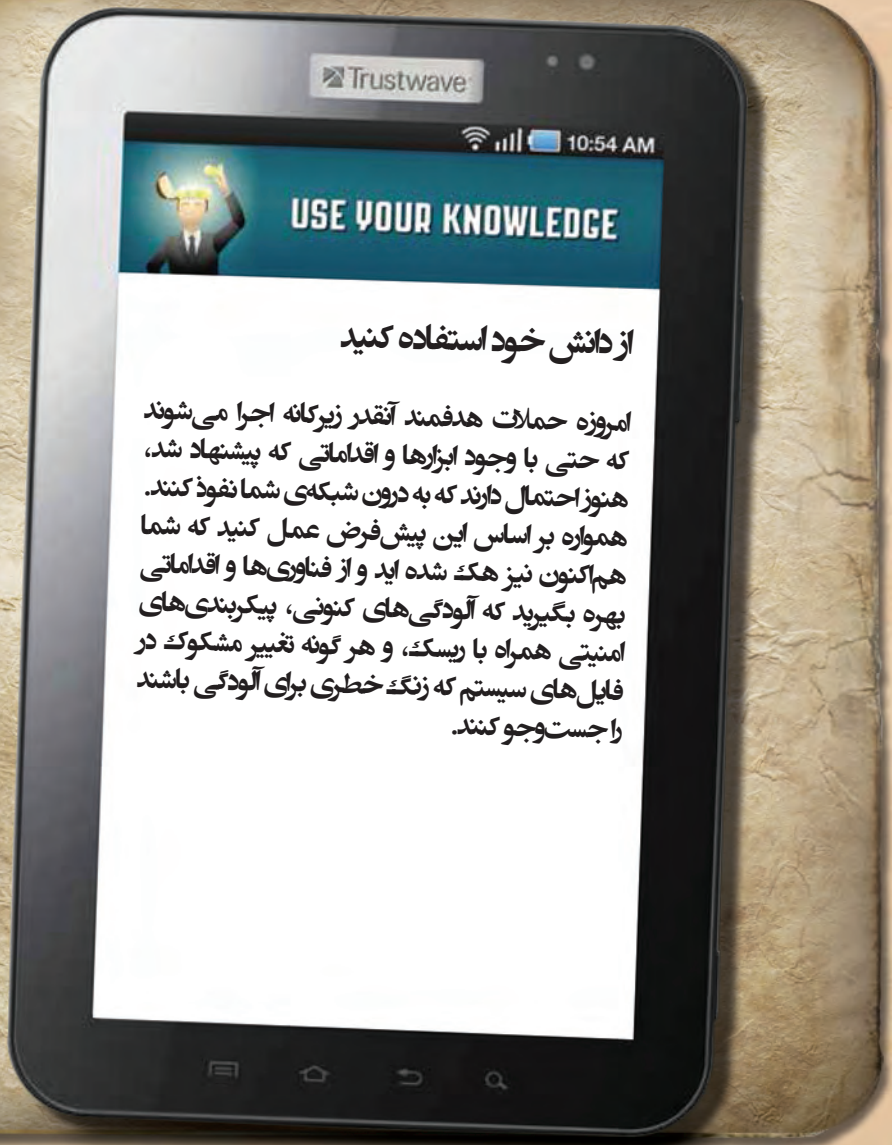
۴۸٪

حملات هدفمند در ابتدا از استفاده از ایمیل‌ها شروع می‌شوند

۲٪

آن‌هاازطریق دستگاه‌های محلی شروع می‌شوند

اگر موضوع انتشار بدافزار در یک شرکتی است که می‌دانید (یا حدس می‌زنید) دارای سیستم‌های وصله‌نشده است، منطقی‌تر این است که از آسیب‌پذیری‌های قدیمی‌آن استفاده کنید.



از دانش خود استفاده کنید

امروزه حملات هدفمند آنقدر زیرکانه اجرا می‌شوند که حتی با وجود ابزارها و اقداماتی که پیشنهاد شد، هنوز احتمال دارند که به درون شبکه‌ی شما نفوذ کنند. همواره بر اساس این پیش‌فرض عمل کنید که شما هم‌اکنون نیز هک شده اید و از فناوری‌ها و اقداماتی بهره بگیرید که آلودگی‌های کنونی، پیکربندی‌های امنیتی همراه با ریسک، و هر گونه تغییر مشکوک در فایل‌های سیستم که زنگ خطری برای آلودگی باشند را جست‌وجو کنند.

پرده‌ی ۸: در فکر راه‌های فرعی باشید

یک در پشتی به داخل شبکه‌ی یک شرکت خوب است، ولی داشتن چند در همیشه بهتر است. اگر می‌خواهید مدت زمان زیادی را در شبکه‌ی یک شرکت بمانید، مجبورید از همان آلودگی اولیه‌ی سمت کلاینت استفاده کرده تا به راه‌های فرعی داخل شبکه نفوذ کنید. از این طریق، اگر نفوذ نخست شما شناسایی شده و بسته‌ی بدافزاری شما از روی شبکه حذف شده، می‌توانید هنوز هم در قسمت‌های دیگر دست به فرمان باشید.

راز موفقیت در این کار؟ باید با تنوع فراوان در شبکه منتشر شوید. باید روی سیستم‌های مختلف از کدهای مختلف و بارهای مختلفی استفاده کنید، زیرا هنگامی‌که‌یک نوع از آن‌ها شناسایی شد، به احتمال زیاد تمام کدهایی که رفتاری مشابه دارند را روی شبکه اسکن خواهند کرد. ولی اگر نقاط پایانی زیادی را با بدافزارهای مختلف کنترل کنید، به احتمال زیاد حتی اطلاع نخواهند یافت که هنوز آلوده هستند.

۷۶٪

بررسی‌های مربوط به پاسخ به رویداد، یک طرف‌سومی‌مسئول پشتیبانی از سیستم، توسعه و نگهداری محیط‌های کسب‌وکاری باعث ایجاد نقص‌های امنیتی بوده‌اند.

۸۸٪

بدافزارها توسط ضدویروس‌های سنتی شناسایی نمی‌شوند

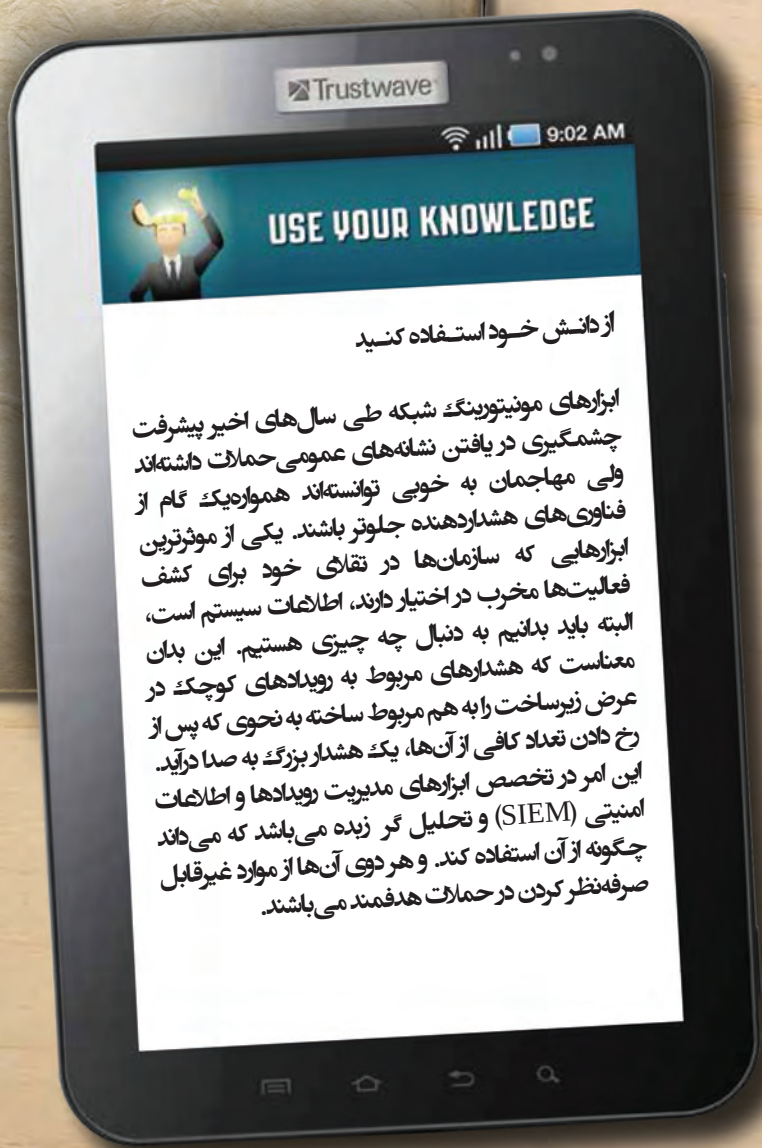
اطلاعاتی در مورد دشمن:

- ۴۱.۲٪ بدافزارها از HTTPS برای تخلیه داده‌ها استفاده می‌کنند.
- ۲۹.۴٪ از FTP استفاده می‌کنند.
- ۱۱.۸ ٪ از SMTP استفاده می‌کنند.

پرده‌ی ۹: جلوی چشم همگان پنهان شوید

در این حملات هدفمند، قایم‌باشک نام این بازی است. شاید گاهی فقط بخواهید به روش سنتی با سروصدای زیاد وارد شده، تا جایی که می‌توانید غارت کنید یا اینکه با اطلاعات مشخصی از آن جا خارج شوید. ولی مناسب‌ترین و پرسودترین راه این است که پایگاه داده را در طولانی مدت و جرعه جرعه بخشکانید.
نفوذ خود را با یک صداخفه‌کن فنی تجهیز کنید. قطعاً تمایلی ندارید هنگامی‌که آنجا یواشکی و دزدکی روی انگشتان پا راه می‌روید به‌یک گلدان گرانقیمت بخورید و آن را با سروصدای زیادی بشکنید. هر حرکتی باید برنامه‌ریزی‌شده باشد تا از به صدا در آمدن زنگ خطرها احتراز شود. هنگامی‌که برای جمع‌آوری داده و کنترل درهای پشتی ابزارهای خود را روی سیستم بارگذاری می‌کنید،
به نکته‌های زیر توجه کنید:

- از بدافزارهایی که خود را تکثیر می‌کنند دوری کنید.
- بدافزارها را در پوشه‌های سیستم کپی کرده و آن‌ها را به شکلی در آورید که مانند فرآیندهای طبیعی جلوه کنند.
- از حساب‌های وبمیل استفاده کنید تا ترافیک دستور و کنترل رمزنگاری شده با SSL را به درهای پشتی خود هدایت کنید.
- برای مخفی کردن دوتایی‌های مخرب خود از ابزارهای بسته‌بند (packer) استفاده کنید.
- اگر توانستید، برخی از عوامل بدافزار را روی ابر ذخیره کنید.



از دانش خود استفاده کنید

ابزارهای مونیتورینگ شبکه طی سال‌های اخیر پیشرفت چشمگیری در یافتن نشانه‌های عمومی حملات داشته‌اند ولی مهاجمان به خوبی توانسته‌اند همواره‌یک گام از فناوری‌های هشداردهنده جلوتر باشند. یکی از موثرترین ابزارهایی که سازمان‌ها در تقلای خود برای کشف فعالیت‌ها مخرب در اختیار دارند، اطلاعات سیستم است، البته باید بدانیم به دنبال چه چیزی هستیم. این بدان معناست که هشدارهای مربوط به رویدادهای کوچک در عرض زیرساخت را به هم مربوط ساخته به نحوی که پس از رخ دادن تعداد کافی از آن‌ها، یک هشدار بزرگ به صدا درآید. این امر در تخصص ابزارهای مدیریت رویدادها و اطلاعات امنیتی (SIEM) و تحلیل گر زبده می‌باشد که می‌داند چگونه از آن استفاده کند. و هر دوی آن‌ها از موارد غیرقابل صرفه‌نظر کردن در حملات هدفمند می‌باشند.

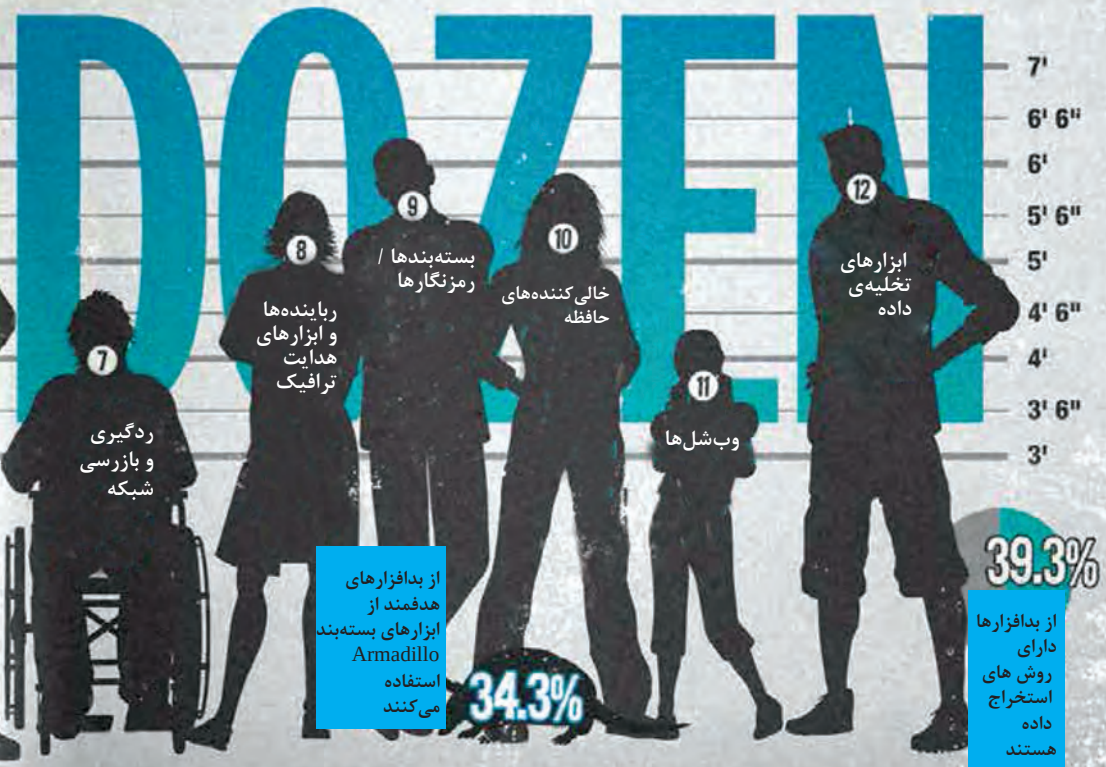
پرده‌ی ۱۰: داده‌ها را به آرامی تخلیه کنید

پس ممکن است شما یک فیشر با نیزه‌ی حرفه‌ای باشید، در نفوذ به شبکه بسیار ماهر بوده و مانند یک سگ شکاری شامه‌ی خوبی برای پیدا کردن داده‌های آبدار داشته باشید. ولی اگر نتوانید داده‌ها را از شبکه خارج کنید، این‌ها به هیچ دردی نمی‌خورد. صبور باشید! تخلیه‌ی آرام و بی‌سروصدا سرقت حجم بیشتری از داده‌ها بدون روشن کردن آلارم‌ها و توقف کارتان در اواسط راه را میسر می‌کند.

از شانس خوب شما بیشتر شرکت‌ها فایروال‌های خود را به گونه‌ای تنظیم نمی‌کنند که ترافیک برون‌شبکه‌ای را مسدود کنند، از این رو گزینه‌های زیادی در اختیار شماست. استفاده از ترافیک عمومی‌وب یکی از کارامدترین راه‌ها برای نشت آرام داده‌ها به خارج از شبکه‌ی شرکت است. با استفاده از ترافیک HTTPS می‌توان بدون شناسایی شدن توسط سیستم‌های جلوگیری از نشت داده و با پنهان کردن داده‌ها زیر عبای SSL داده‌ها را خارج کرد.

از آن جایی که آخر بازی در حملات هدفمند سرقت داده است، کار منطقی این است که از ابزارهای داده محور استفاده کنید. رمز گذاری داده ها را فراموش نکنید زیرا در صورت ربوده شدن داده ها، برای سارق استفاده ای نخواهد داشت.

دوازده مرد خبیث در حملات هدفمند



این ابزارها مجرمان را قادر می‌سازد تا به آسانی داده‌ها را از طریق ارسال ترافیک به کانال‌های مخفی از شبکه خارج کنند.

مجرمان از کد وب‌شل استفاده می‌کنند تا درهای پشتی را روی سرور وب بکارند که به سختی قابل شناسایی باشند. این سرورها می‌توانند دسترسی به اطلاعات درون شبکه را برای هکرها به ارمغان بیاورند.

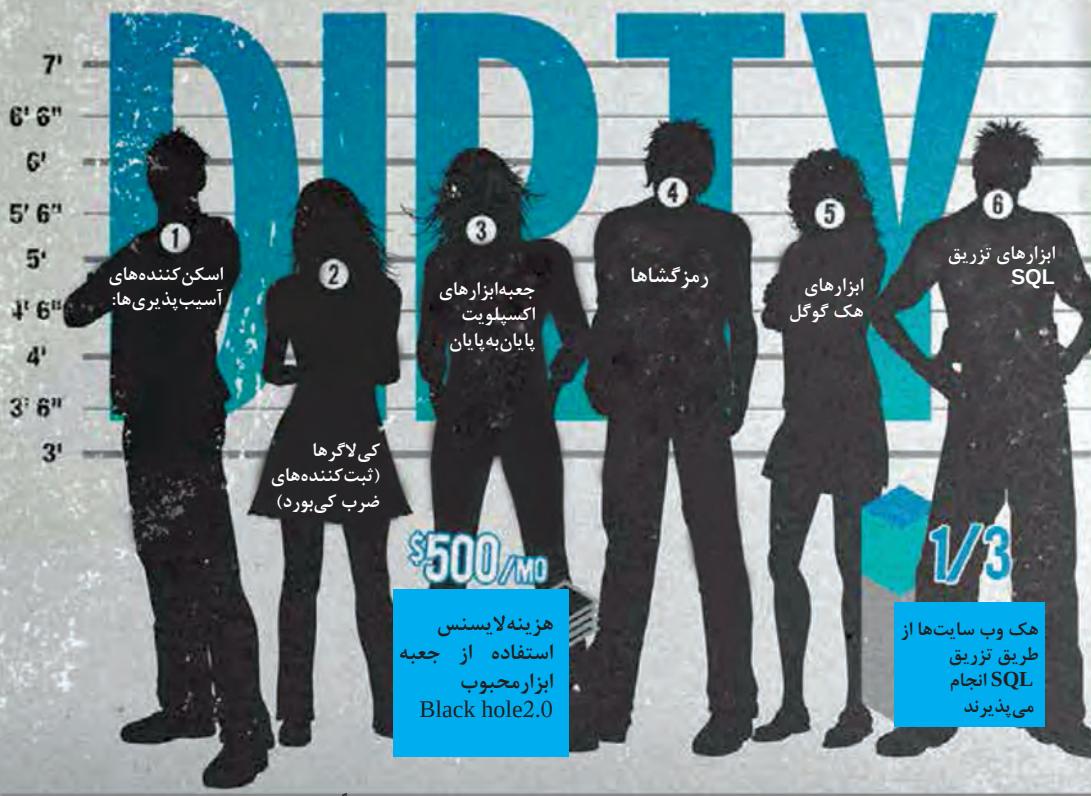
طی زمانی که کاربر فرآیند رمزگذاری را آغاز می‌کند، مهاجمان می‌توانند با استفاده از تکنیک‌های خود از این به این داده‌ها حمله کرده و به آرامی آن‌ها را از روی حافظه به سرقت ببرند.

برای اینکه از شناسایی توسط ضدویروس‌ها در امان بمانند، بدافزارها از بسته‌بندها و رمزنگارها استفاده می‌کنند تا دوتایی‌های خود را پنهان کنند.

این ابزارها مجرمان را قادر می‌سازند تا نوع رفتار ترافیک وب را تغییر دهند. کاربران را به مقصدهایی مخرب هدایت کرده، نشست‌های وب را می‌ربایند، و برای به دست آوردن اطلاعات مطلوب خود ترافیک وب را استراق سمع می‌کنند.

هکرها از ردگیرهای و ابزارهای رسم نقشه‌ی شبکه استفاده می‌کنند تا درک بهتری از معماری شبکه پیدا کرده و به نحوی عمیق تر در آن نفوذ کنند.

TARGETED ATTAC



آسیب‌پذیری‌های تزریق SQL از متداول ترین ابزارها برای سرقت از پایگاه داده‌هایی موجود در وب می‌باشد و به آسانی به واسطه‌ی این ابزارهای خودکارکننده‌ی اسکن و اکسپلویت پیدا می‌شوند.

بسیاری از دستگاه‌های حساس متصل به اینترنت اطلاعاتی را در خصوص اینکه چگونه آن‌ها را هک کرد به نمایش می‌گذارند. ابزارهای این موتور جست‌وجو شکار این گونه اطلاعات را خودکار می‌سازد.

پس از اینکه هکرها جای پای محکمی‌در سیستم یا شبکه پیدا کردند، می‌توانند از رمزگشاها استفاده کرده به فایل‌های رمزگذاری شده حمله کرده و اطلاعات مربوط به ورود به حساب‌ها را استخراج کرده و شبکه را به طور کامل آلوده کنند.

کیت‌های پایان‌به‌پایان مجرمان معمولی را قادر می‌سازند تا یک کمپین کاملاً خودکار را با کمترین دانش فنی ممکن اجرا کنند.

معمولاً این ابزارها با بار بدافزاری که از طریق مهندسی اجتماعی وارد سیستم‌ها می‌شود در یک بسته قرار دارند و ضربات کیبورد کاربران را برای دستیابی به گذرواژه‌هاییشان ثبت می‌کنند.

برخی از این اسکنرها شبکه‌های آلوده‌شده را وارسی کرده و به دنبال آسیب‌پذیری‌های دیگر می‌گردند، در حالی که دیگر اسکنرها در اینترنت به جست‌وجوی پورت‌های باز و اپ‌های وب ضعیف آماده برای اکسپلویت مشغول هستند.