نفوذ سایبری

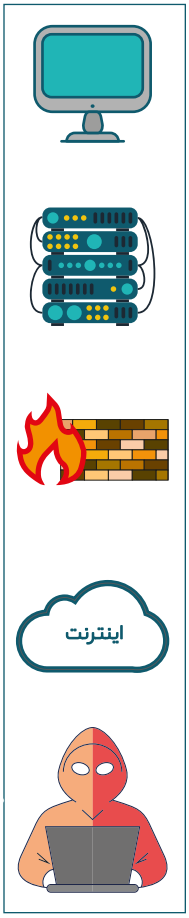
هکرها چگونه به سازمان شما نفوذ می‌کنند؟

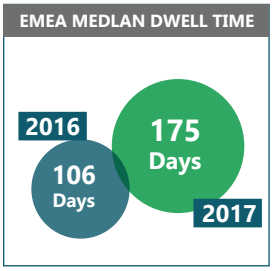
مجتبا مصطفوی
@mojtabamostly

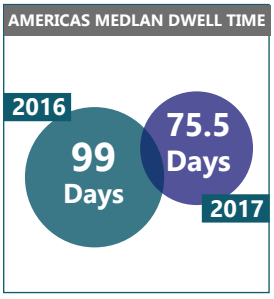
پاییز ۱۳۹۷

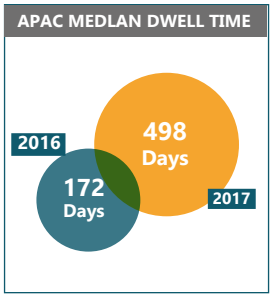
در سال‌های اخیر حملات سایبری هدفمند به دولت‌ها با سرعت بالایی رو به گسترش بوده و به یکی از شاخص‌های مهم قدرت برای کشورهای مهاجم تبدیل شده است. در این کتابچه ابتدا به بررسی وضعیت فعلی این حملات در سطح دنیا و ایران، سپس به چکیده‌ی روش‌های مقابله با آن‌ها پرداخته‌ایم. در پایان نیز یک سناریوی فرضی نفوذ به یک سازمان دولتی آمده است.

فهرست



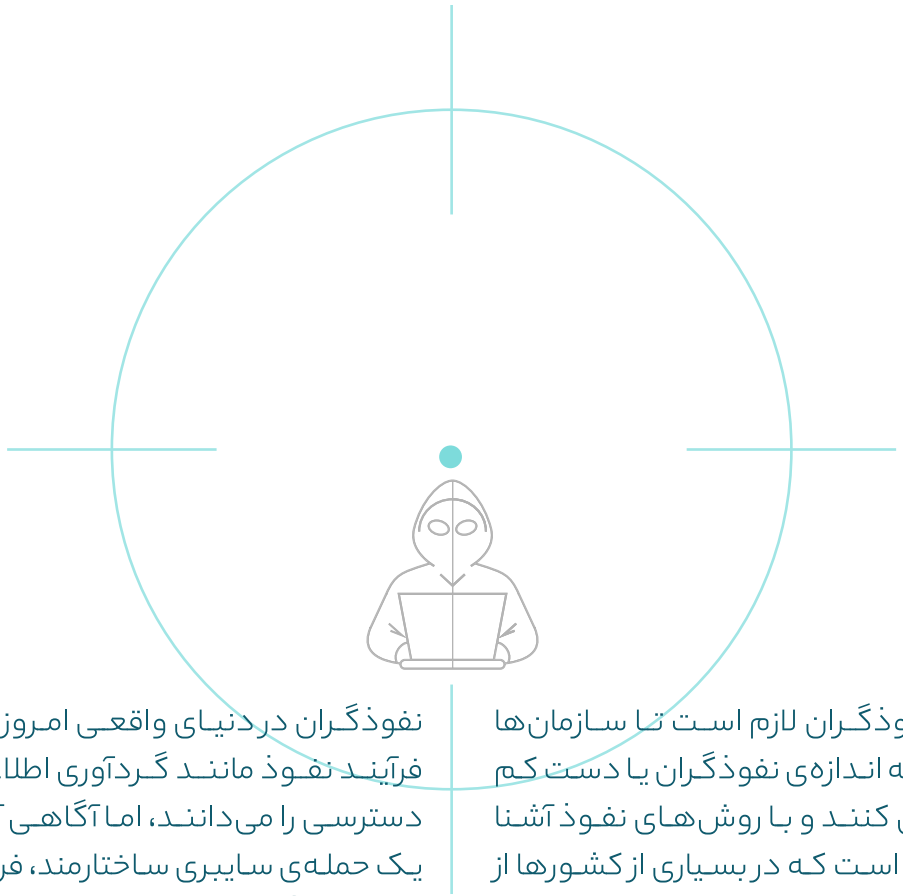






مقدمه

در گذشته هکرها با برخی اهداف شخصی مانند کسب شهرت، سرقت از حساب بانکی اشخاص و... یا با اهداف سیاسی و اجتماعی (مانند هکتیویست‌ها) حملات خود را طراحی و اجرا می‌کردند. در سال‌های اخیر افزون‌بر موارد گفته شده، شاهد شکل‌گیری و رشد درخور توجه گروه دیگری از هکرها بوده‌ایم که با حمایت دولت‌ها شکل گرفته‌اند و به نوبه‌ی خود می‌توانند به مراتب خطرناک‌تر از گروه‌های دیگر باشند. در واقع از زمانی‌که کشورها به قدرت حملات سایبری و قابلیت‌های آن پی بردند، شروع به استخدام و آموزش هکرها و سرمایه‌گذاری سنگین در این زمینه کردند. این سرمایه‌گذاری‌ها سبب شد تا هکرهای دولتی دیگر دغدغه‌هایی مانند درآمد و شغل نداشته باشند و تمام تمرکز خود را صرف توسعه‌ی روش‌های نفوذ پیشرفته کنند. به این ترتیب، نفوذ در سال‌های اخیر شکل جدیدی به خود گرفته است، به‌گونه‌ای که گروه‌های هکری زیر چتر حمایت دولت‌ها از بالاترین سطوح تخصص و تجهیزات در زمینه‌های مختلف علوم کامپیوتر (از دانش‌های اساسی نفوذ مانند برنامه‌نویسی بدافزار گرفته تا حتا در برخی کشورها دانش هوش مصنوعی و یادگیری ماشین) بهره‌مند شده‌اند. این نفوذگران در حملات خود می‌توانند به‌دنبال اهداف مختلفی باشند که از جمله مهم‌ترین آن‌ها می‌توان به جاسوسی و سرقت اطلاعات از دیگر کشورها، تخریب زیرساخت‌های حیاتی (مانند برق، آب و...)، جابه‌جایی پول یا پول‌شویی، اهداف نظامی و... اشاره کرد.



برای مقابله با این نفوذگران لازم است تا سازمان‌ها دانش سایبری خود را به اندازه‌ی نفوذگران یا دست کم در حدود آن به‌روزرسانی کنند و با روش‌های نفوذ آشنا باشند. به همین دلیل است که در بسیاری از کشورها از نفوذگران کلاه‌سفید در کنار متخصصان امنیتی استفاده می‌کنند تا با دید کامل‌تری نسبت به گذشته، خود را برای مقابله با حملات سایبری و پاسخ‌گویی به آن‌ها آماده کنند.

متاسفانه در کشور ما نه‌تنها تدبیری برای حمایت یا تربیت هکرهای کلاه‌سفید و بهره‌مندی از دانش آن‌ها در راستای افزایش امنیت سایبری کشور اندیشیده نشده است، بلکه به نظر نمی‌آید برنامه‌ی مشخصی نیز در این زمینه برای آینده‌ی نزدیک وجود داشته باشد (دست کم تا جایی که ما اطلاع داریم).

یکی دیگر از مشکلاتی که در بین کارشناسان فناوری اطلاعات و حتا بسیاری از کارشناسان امنیتی کشور مشاهده می‌شود این است که بیش‌تر اوقات، تصور واضح و درستی از نفوذ و روش‌های مورد استفاده‌ی نفوذگران در دنیای واقعی امروز ندارند. در واقع کلیات فرآیند نفوذ مانند گردآوری اطلاعات، حمله و گسترش دسترسی را می‌دانند، اما آگاهی آن‌ها درباره‌ی جزییات یک حمله‌ی سایبری ساختارمند، فراتر از دوره‌های ابتدایی مانند CEH نمی‌رود.

برای نمونه، می‌توان به ناکامی‌های رخ‌داده در راهبری SIEMهای بیش‌تر سازمان‌های دولتی اشاره کرد که تجربه‌ی موفق راه‌اندازی این سامانه‌ها (منطبق با استاندارد روز دنیا) در کشور (جدا از انتخاب محصول داخلی یا خارجی) بسیار نادر است.

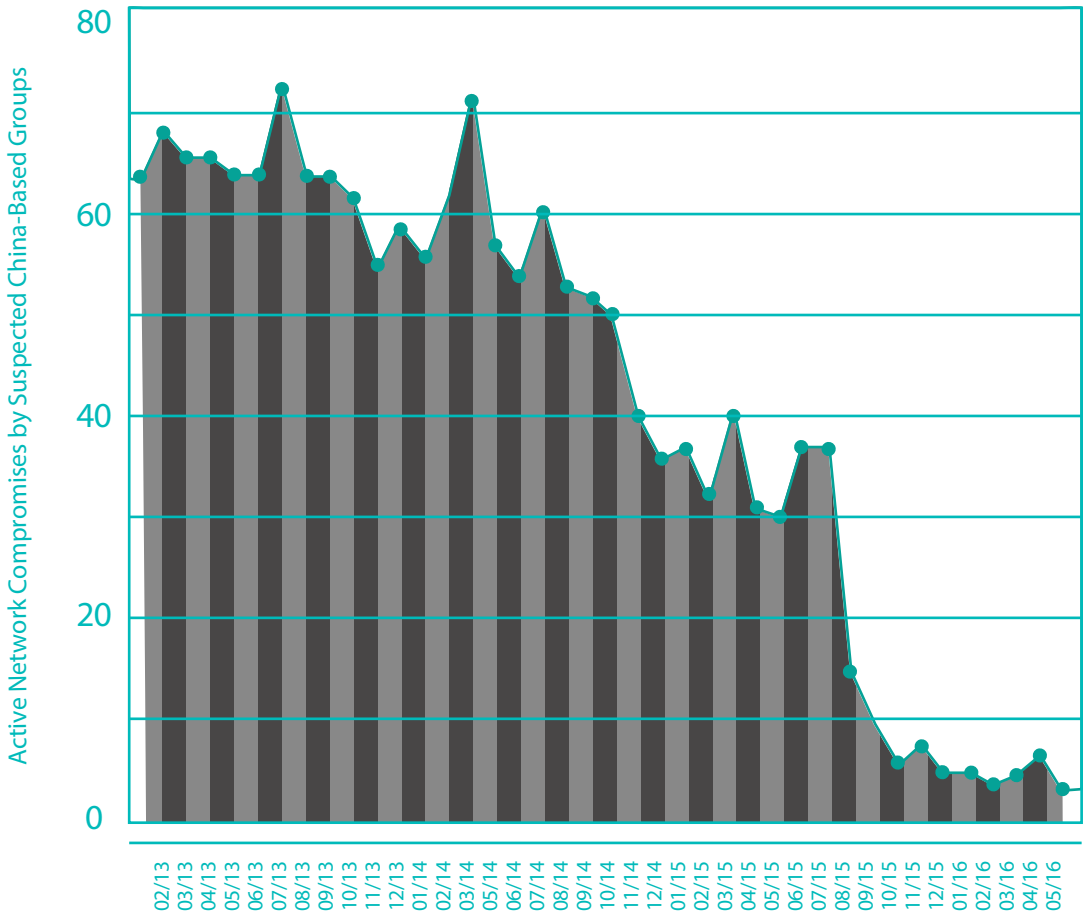
البته این موضوع به معنی دانش پایین تمام افراد فعال در حوزه‌ی امنیت سایبری کشور نیست، اما نمی‌توان این واقعیت را پنهان کرد که تعداد متخصصان با دانش روز امنیت سایبری فعال در داخل کشور بسیار کم و به‌هیچ‌وجه پاسخ‌گوی نیاز امنیتی امروز ما نیست. نباید این موضوع را نیز از نظر دور داشت که از همین تعداد متخصص نیز حمایت نشده است و از دانش آن‌ها به‌درستی استفاده نمی‌شود.

حملات سایبری هدفمند در سطح دنیا و ایران

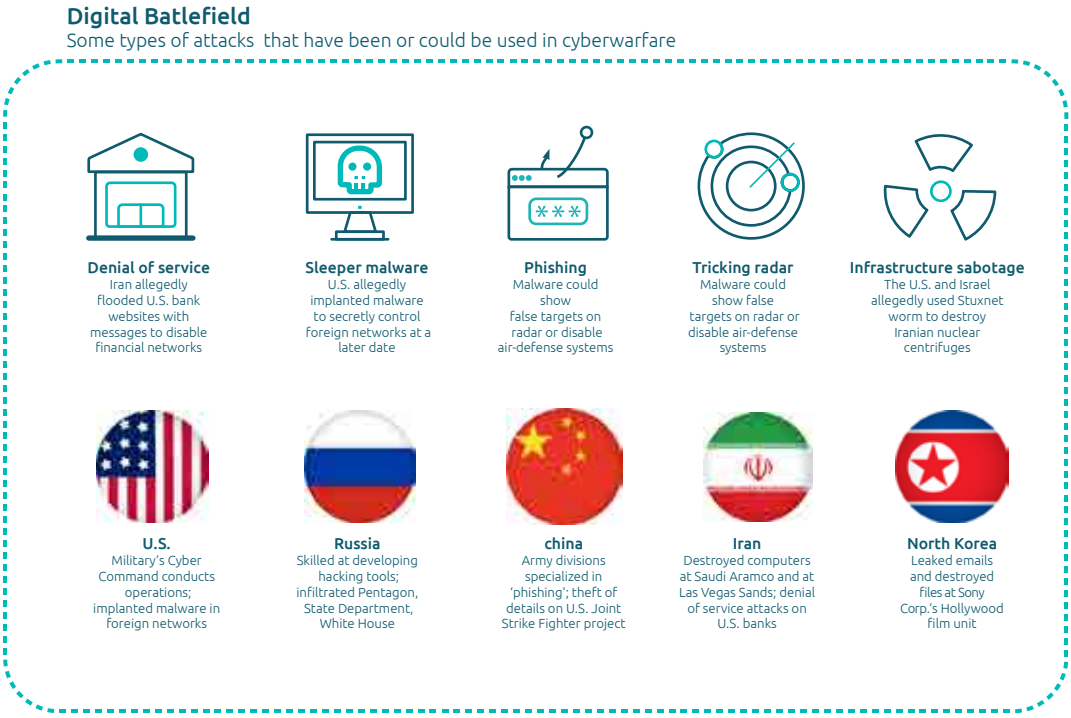
همان‌گونه که در مقدمه شرح داده شد، در سال‌های اخیر شاهد گسترش حملات سایبری سازماندهی‌شده در سطح دنیا بوده‌ایم. در واقع بسیاری از دولت‌ها توان حمله و دفاع سایبری یک کشور را یکی از مولفه‌های قدرت آن کشور به‌شمار می‌آورند. از سوی دیگر، کشورها به این نتیجه رسیده‌اند که با استفاده از حملات سایبری می‌توانند کشورهای مخالف خود را تحت فشار گذاشته یا اطلاعات و فناوری‌های رده‌بندی‌شده آن کشورها را به سرقت برند. به همین دلیل است که روزبه‌روز شاهد افزایش تعداد حملات (با پشتوانه‌ی دولتی) شناسایی‌شده‌ی شرکت‌های امنیتی در سطح دنیا هستیم.

برای نمونه، درباره‌ی حملات سایبری سازماندهی‌شده می‌توان به حملات متعدد نفوذگران چینی به تاسیسات زیرساختی و شرکت‌های high-tech آمریکایی در سال‌های اخیر اشاره کرد. این حملات درنهایت منجر به عقد یک تفاهم‌نامه‌ی سایبری بین دو کشور در تاریخ سپتامبر ۲۰۱۵ میلادی شد . براساس گزارش شرکت Fireeye کشور چین پس از این تفاهم‌نامه تعداد حملات خود را به مراتب کاهش داد، اما هیچ‌گاه این حملات را متوقف نکرد. به بیان دیگر، تعداد حملات سایبری چینی‌ها بسیار کم‌تر، اما دقیق‌تر و هدفمندتر شد تا فشار سیاسی کم‌تری را از سوی آمریکا تحمل کنند.

این مطلب در شکل زیر به‌خوبی نمایش داده شده است.



برخی از انواع حملات سایبری مهم رخ داده در سطح دنیا و کشورهایی که نقش پررنگی در زمینه‌ی جنگ‌های سایبری دنیا دارند از نگاه نشریه‌ی وال استریت ژورنال[1] در این تصویر نمایش داده شده است. همان‌گونه که مشاهده می‌کنید حملاتی را نیز به ایران نسبت داده‌اند.



برخی از تفاوت‌های موجود میان حملات سایبری پشتیبانی‌شده‌ی دولت‌ها با سایر انواع حملات سایبری در زیر آمده است:

- اهداف این حملات نسبت به اهداف نفوذگران عادی متفاوت است (حمله به زیرساخت‌های حیاتی، جاسوسی اطلاعات و...).

- ممکن است هدف اصلی، تنها دسترسی گرفتن از یک سازمان استراتژیک (قربانی) باشد تا در زمان مناسب حمله‌ی دیگری به زیرساخت قربانی انجام شود. بازه‌ی زمانی بین نفوذ اولیه و انجام عملیاتی مانند تخریب زیرساخت، می‌تواند ماه‌ها یا حتا سال‌ها به طول انجامد.

- در اصطلاح کم‌ترین سروصدا[2] را ایجاد می‌کنند (برای نمونه از کارهایی مانند deface وب‌سایت یا سایر فعالیت‌هایی که سبب لو رفتن نفوذ بشود، خودداری می‌کنند).

- از ابزارهای آماده استفاده نمی‌شود (به‌دلایل مختلف مانند کاهش مخاطرات ناشی از شناسایی شدن توسط آنتی‌ویروس‌ها و سایر تجهیزات امنیتی، پاسخ‌گویی به نیازهای خاص نفوذگر و...).

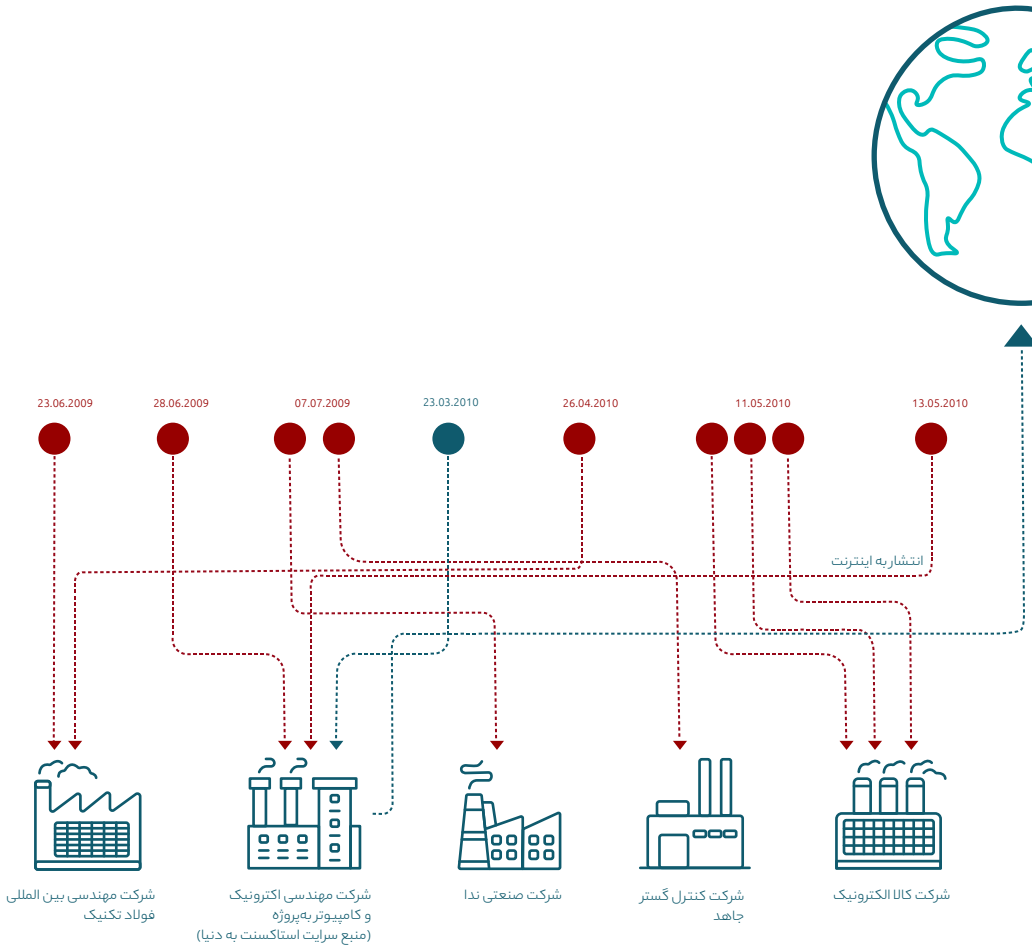
- شناسایی هویت نفوذگران همیشه یکی از مشکلات پلیس سایبری یا سایر نهادهای قانونی بوده است. درباره‌ی نفوذگران دولتی با توجه به امکاناتی که دولت‌ها برای نفوذگران خود فراهم می‌کنند، شناسایی هویت این نفوذگرها به‌مراتب دشوارتر نیز خواهد شد.

۱. Wall street journal (WSJ)
۲. کم ترین تغییر در شبکه و محتوای وب‌سایت‌ها

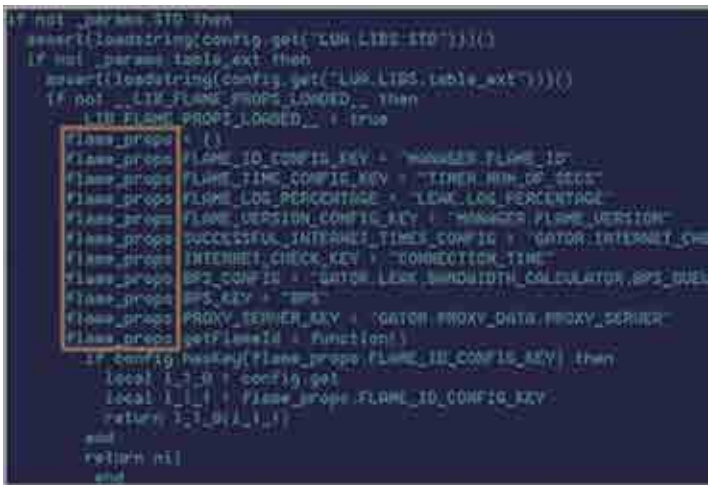
ایران، هدف حملات سایبری

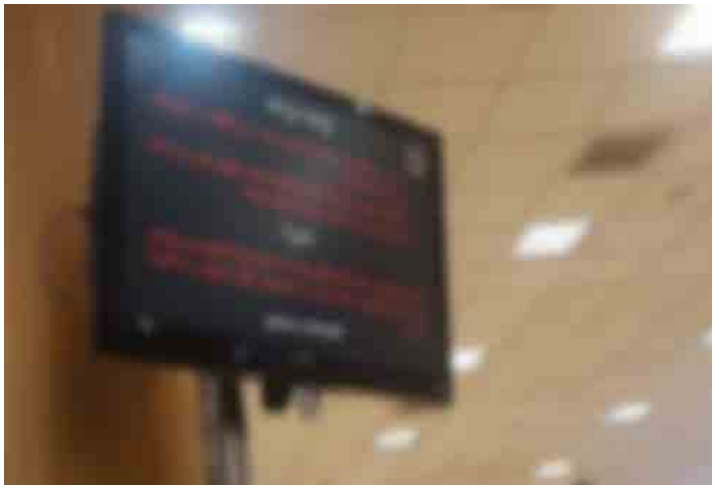
در بخش پیشین، موضوع رشد حملات سایبری دولتی در دنیا و برخی از دلایل و ویژگی‌های آن بررسی شد. حال شاید این پرسش به ذهن برسد که آیا کشور ایران نیز در معرض حملات سایبری قرار دارد؟ و اگر پاسخ مثبت است، این حملات چه‌قدر می‌توانند تاثیرگذار باشند؟ آیا نتیجه‌ی این حملات تنها یک تعداد وب‌سایت Deface شده است؟
با یک جست‌وجوی به‌نسبت ساده در آرشیو سایت‌های خبری فارسی و غیرفارسی می‌توان به پاسخ این پرسش‌ها دست پیدا کرد. برای نمونه، از بین حملات سایبری سازمان‌یافته علیه سازمان‌های دولتی کشور (که رسانه‌ای شدند) می‌توان به موارد زیر اشاره کرد:

۱. **Stuxnet:** در این حمله بدافزار بسیار پیشرفته و پیچیده‌ای با هدف آلوده‌سازی زیرساخت نیروگاه‌های اتمی کشور و آسیب‌رساندن به سانتریفیوژهای[1] در حال فعالیت، به‌کار گرفته شد. این بدافزار نخستین‌بار در سال ۲۰۱۰ میلادی شناسایی و با آن مقابله شد. پس از آن، Stuxnet پیچیده‌ترین حمله‌ی تاریخ سایبری نام گرفت و روند جنگ‌های سایبری در دنیا را دست‌خوش تغییرات بزرگی کرد. نخستین سازمان‌های شناسایی‌شده (به گزارش شرکت Kaspersky) که به این بدافزار آلوده شده بوده‌اند، در شکل زیر نمایش داده شده است.



۱. Centrifuge





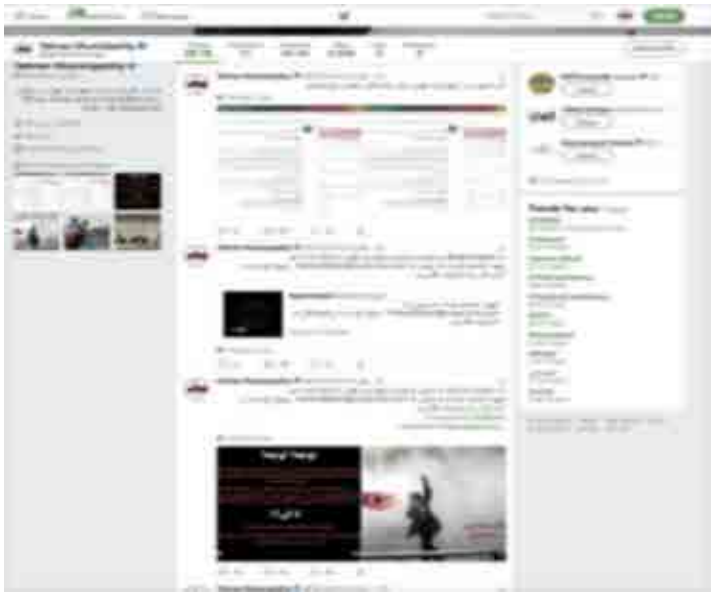
۲. **Flame:** بدافزار دیگری است که با هدف جاسوسی از سازمان‌های دولتی ایران و برخی کشورهای دیگر خاورمیانه طراحی و فعال شده بود. به بیان دیگر، هدف این بدافزار سرقت اطلاعات محرمانه‌ی دولتی ایران و چه‌بسا برخی کشورهای منطقه بوده است. این بدافزار دو سال بعد از Stuxnet یعنی در سال ۲۰۱۲ میلادی شناسایی شد. در شکل مقابل بخشی از کد این بدافزار نمایش داده شده است.

۳. **حمله به زیرساخت وزارت نفت ایران:** در سال ۲۰۱۲ میلادی در یک حمله‌ی سایبری و با استفاده از بدافزاری که (با توجه به عملکرد خود) wiper نام‌گذاری شد، بخشی از اطلاعات موجود روی سرورهای مرکز داده‌ی وزارت نفت و سازمان‌های تابعه‌ی آن را برای همیشه از بین برد یا به‌اصطلاح wipe کرد.

این حملات در سال‌های اخیر به قوت خود باقی بوده و گاهی شدت بیش‌تری نیز یافته است. برای نمونه، برخی از مهم‌ترین حملات سایبری به کشور در سال ۱۳۹۷ که در رسانه‌ها خبرساز شدند عبارت‌اند از:

۱. حمله به زیرساخت‌های ارتباطی و مراکز داده‌ی کشور با استفاده از آسیب‌پذیری موجود در تجهیزات Cisco، که اختلال در زیرساخت‌های ارتباطی کشور را به‌دنبال داشت. بنابر اطلاعیه‌ی وزارت ارتباطات و فناوری اطلاعات، حدود ۳۵۰۰ مسیریاب در این حمله از کار افتادند (پیکربندی آن‌ها به پیکربندی پیش‌فرض اولیه تغییر داده شد).

۲. نفوذ به شبکه‌ی فرودگاه‌های مشهد و تبریز و نمایش تصاویر مورد نظر نفوذگران در نمایش‌گرهای این فرودگاه‌ها که در شکل‌های مقابل برخی از این تصاویر آمده است.



۳. مجموعه حملاتی که بنابر گفته‌ی پلیس فتا به ۱۱ بانک از مجموع ۳۲ بانک موجود در کشور (حدود یک سوم) و با هدف ایجاد اختلال‌های جدی در زیرساخت مالی و بانکی کشور انجام شد.

۴. نفوذ به ایمیل و حساب‌های شهرداری تهران در شبکه‌های مجازی که منجر به افشای بخشی از ایمیل‌های این سازمان و ارسال پست‌هایی در حساب توییتر این سازمان شد. در شکل‌ها بخشی از این موارد نمایش داده شده است.

با توجه به موارد گفته شده، می‌توان نتیجه گرفت ارگان‌های دولتی ایران در ده سال اخیر قربانی انواع حملات سایبری با هدف‌های متفاوت بوده‌اند. البته موارد گفته شده و سایر حملات منتشرشده در رسانه‌های خبری، تنها بخش کمی از کل ماجرا هستند، می‌توان تخمین زد که تعداد حملات به زیرساخت‌های دولتی به‌مراتب بیش از این‌ها بوده است. در بخش بعد به بررسی دلایل این موضوع می‌پردازیم.

آیا تمام حملات سایبری موفق، در رسانه‌های خبری اعلام می‌شوند؟

پاسخ این پرسش منفی است. در حقیقت حملات سایبری اعلام شده در رسانه‌های خبری تنها بخش کوچکی از تعداد واقعی حملات را شامل می‌شوند. نه‌تنها بسیاری از حملات سایبری هیچ‌گاه رسانه‌ای نمی‌شوند بلکه در واقعیت ممکن است بسیاری از آن‌ها هیچ‌گاه شناسایی هم نشوند. به بیان دیگر، این امکان وجود دارد که یک سازمان دولتی هیچ‌گاه متوجه نشود که بخشی از اطلاعات حیاتی‌اش را نفوذگران به سرقت برده‌اند. هم‌چنین سازمانی که در زیرساخت امنیتی خود ضعف دارد، حتا ممکن است هیچ‌گاه متوجه‌ی نفوذ مهاجمان به شبکه و فعالیت آن‌ها در شبکه‌ی خود نشود.

به‌طور کلی، مهم‌ترین دلایل رسانه‌ای نشدن بسیاری از حملات سایبری به شرح زیر است:

- کارشناسان سازمان قربانی متوجه نمی‌شوند که سازمان مورد نفوذ قرار گرفته است.
- کارشناس امنیت یا سایر پرسنل سازمان متوجه حمله‌ی سایبری می‌شوند، اما به‌دلیل ترس از مجازات یا از دست دادن کار خود، حمله‌ی رخ‌داده را تمام‌شده تلقی کرده و به سازمان اعلام نمی‌کنند.
- سازمان متوجه‌ی حمله‌ی سایبری می‌شود، اما به‌منظور محافظت از اعتبار خود، از رسانه‌ای شدن این حملات جلوگیری می‌کند.
- افزون‌بر موارد گفته شده، شرکت‌های ایرانی فعال در زمینه‌ی امنیت سایبری نیز درباره‌ی شناسایی نفوذگران و ارایه‌ی گزارش‌های موردی یا حتا سالانه در این زمینه، عملکرد پذیرفته‌شده‌ای نداشته‌اند.

با توجه به موارد گفته شده، می‌توان با احتمال بالا گفت حملات سایبری که در رسانه‌ها منتشر می‌شوند، تنها بخش کوچکی از تعداد واقعی حملات سایبری به زیرساخت‌ها و سازمان‌های دولتی کشور را تشکیل می‌دهند. پس این نیاز به‌شدت احساس می‌شود که سازمان‌ها باید دیدگاه خود نسبت به حملات سایبری را تغییر دهند و به واقعیت نزدیک‌تر شوند.

یکی از مشکلات اساسی برخی سازمان‌های دولتی، ناآشنایی با راه‌های ورود مهاجمان به شبکه‌شان است؛ در نتیجه، تمرکز و بودجه‌ی خود را روی برخی از راه‌های نفوذ (مانند وب‌سایت‌های سازمان) می‌گذارند، درحالی‌که راه‌های نفوذ دیگر را به حال خود باقی گذاشته‌اند (مانند راهکارهای ارتباط از راه دور، ایمیل‌های سازمان و...).

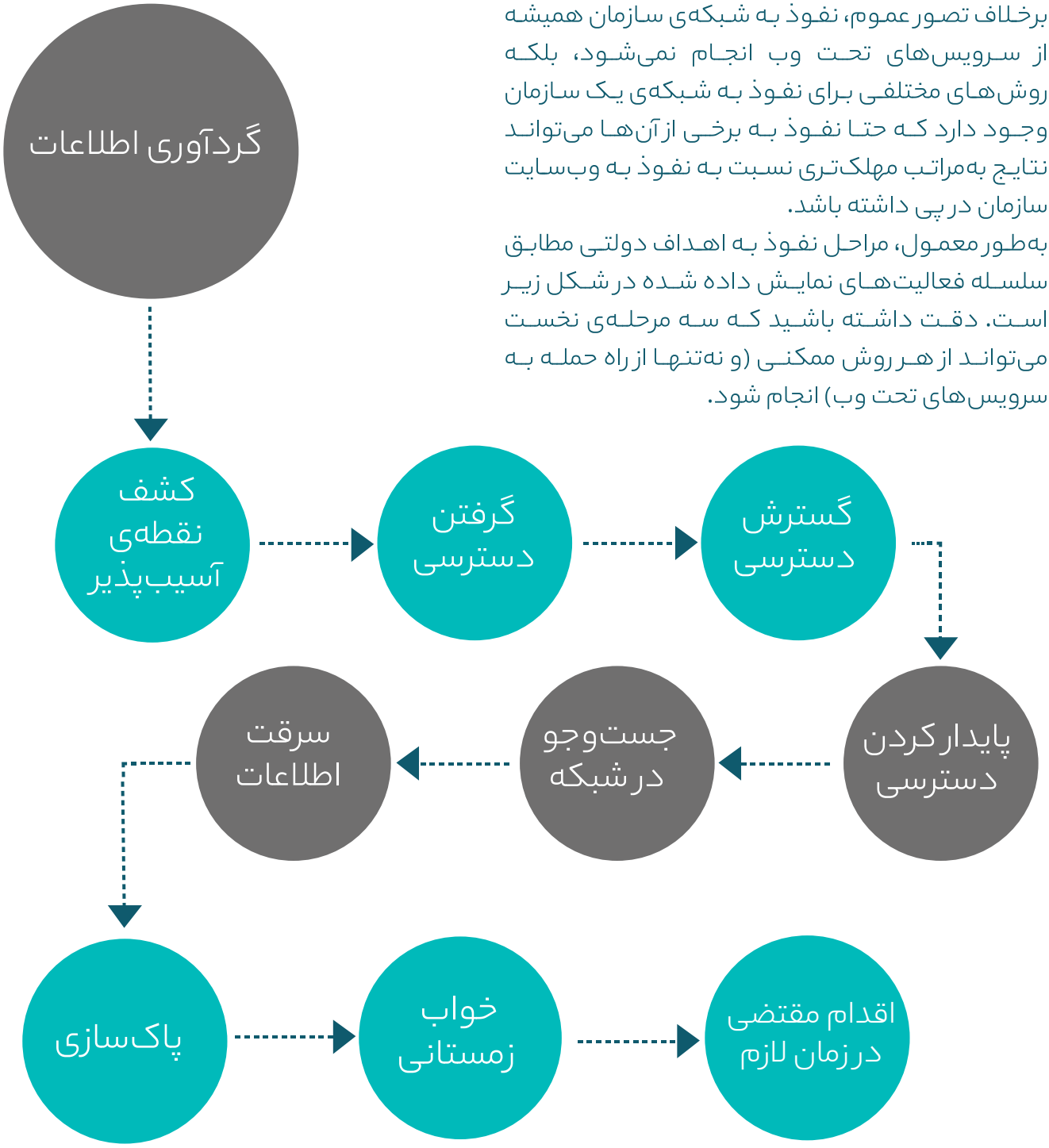
به نظر می‌رسد یکی از نخستین گام‌های اساسی در طراحی یک معماری امنیت چند لایه، آشنایی با راه‌های نفوذ است تا سازمان‌ها بتوانند با دید جامع‌تری نسبت به طراحی امنیت شبکه و سامانه‌های اطلاعاتی خود اقدام کنند.

با توجه به موارد گفته شده، در بخش بعد انواع روش‌های متداول نفوذ به شبکه‌ی سازمان‌ها که مورد توجه نفوذگران هستند، بررسی شده است.

انواع روش‌های متداول نفوذ به شبکه‌ی سازمان‌ها

برخلاف تصور عموم، نفوذ به شبکه‌ی سازمان همیشه از سرویس‌های تحت وب انجام نمی‌شود، بلکه روش‌های مختلفی برای نفوذ به شبکه‌ی یک سازمان وجود دارد که حتا نفوذ به برخی از آن‌ها می‌تواند نتایج به‌مراتب مهلک‌تری نسبت به نفوذ به وب‌سایت سازمان در پی داشته باشد.

به‌طور معمول، مراحل نفوذ به اهداف دولتی مطابق سلسله فعالیت‌های نمایش داده شده در شکل زیر است. دقت داشته باشید که سه مرحله‌ی نخست می‌تواند از هر روش ممکنی (و نه‌تنها از راه حمله به سرویس‌های تحت وب) انجام شود.



در بخش‌های بعد راه‌های متداول نفوذگران برای نفوذ به شبکه‌ی یک سازمان دولتی یا شرکت خصوصی، به همراه خلاصه‌ای از راهکارهای کلی برای مقابله با آن‌ها شرح داده شده است.

نفوذ به زیرساخت از راه سرویس‌های تحت وب

یکی از قدیمی‌ترین روش‌های متداول برای نفوذ به سازمان، اقدام به هک وب‌سایت یا سایر سرویس‌های تحت وب آن سازمان است. برخی از حملات متداول مورد استفاده در این روش به شرح زیر است:

- **SSRF**[1]: مهاجم امکان ارسال درخواست‌های ساختگی از طرف یک برنامه‌ی کاربردی وب آسیب‌پذیر را دارد. این حمله بیش‌تر برای نفوذ به سامانه‌های داخلی[2] (به‌واسطه‌ی برنامه‌ی کاربردی وب آسیب‌پذیر) که مهاجم به‌طور مستقیم به آن‌ها دسترسی ندارد، استفاده می‌شود.

- **SQL Injection**[3]: مهاجم با سواستفاده از انواع آسیب‌پذیری‌های مرتبط با بانک‌های اطلاعاتی مبتنی‌بر SQL، کد مخرب خود را توسط سرور SQL اجرا می‌کند. برای نمونه، اگر یک وب‌سایت در برابر حمله‌ی SQL injection آسیب‌پذیر باشد، ممکن است مهاجم کد خود را در یک کادر متنی (برای نمونه بخش نظرات کاربران) موجود در وب‌سایت بنویسد و سرور SQL را مجبور کند تا اطلاعات ذخیره شده در جداول پایگاه داده را (مانند بخشی از گذرواژه‌های ذخیره شده) برای مهاجم نمایش دهد.

- **Code Injection**: در این آسیب‌پذیری، مهاجم می‌تواند کد مخرب خود را به سرور تزریق و اثر آن را مشاهده کند. در بسیاری از موارد، با استفاده از تزریق کد برنامه، امکان اجرای فرامین سیستم‌عاملی میسر می‌شود. علت وجود چنین آسیب‌پذیری خطرناکی، تفسیر ناامن کدهای ارسالی کاربر توسط سامانه است.

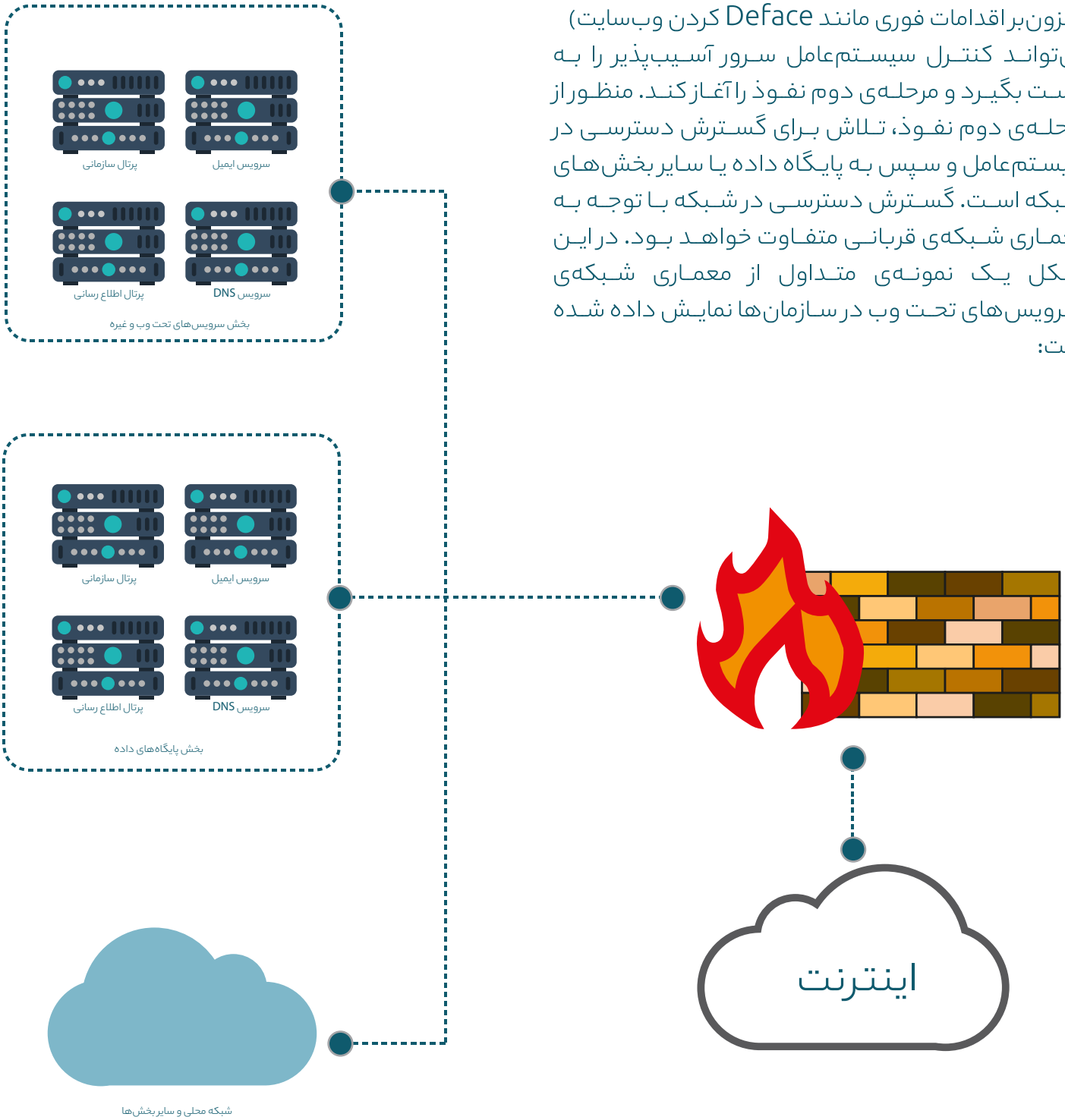
- **XSS**[4]: این مدل حملات نیز از راه تزریق کدهای مخرب انجام می‌شود، با این تفاوت که در این‌جا سرور وب‌سایت، هدف مستقیم حمله نیست و کاربران بازدیدکننده از وب‌سایت آسیب‌پذیر مورد نظر مهاجم هستند. در واقع هنگامی‌که کاربر با استفاده از مرورگر اینترنتی خود از وب‌سایت آلوده بازدید می‌کند، کد مخرب روی رایانه‌ی کاربر اجرا خواهد شد. برای نمونه، با آسیب‌پذیر بودن یک وب‌سایت، مهاجم می‌تواند کد مخرب مورد نظر خود را در بخشی از وب‌سایت (مانند بخش نظرات کاربران، URL و...) ذخیره کند تا هرگاه کاربری از این بخش سایت بازدید کرد، کد به‌شکل خودکار روی رایانه‌ی آن کاربر اجرا شود. نتیجه‌ی اجرای کد مخرب در رایانه‌ی کاربر، بستگی به خواست مهاجم دارد، برای نمونه، ممکن است اطلاعاتی را که پس از آن توسط کاربر در مرورگر اینترنتی وارد می‌شود، به سرقت ببرد.

- **XXE**: این حمله زمانی رخ می‌دهد که ورودی XML حاوی یک مرجع[5] به یک موجودیت خارجی[6] باشد که توسط یک XML parser پردازش شود. این آسیب‌پذیری بیش‌تر ناشی از پیکربندی ضعیف امنیتی parser است و مهاجم با تزریق اسکریپت مخرب XML قادر خواهد بود تا برخی فعالیت‌های مورد نیاز خود را توسط سرور آسیب‌پذیر اجرا کند.

- **CSRF**[7]: حمله‌ی جعل درخواست یکی از حملات رایج در محیط وب است. در این حمله، مهاجم اقدام به جعل درخواست کاربر اصالت‌سنجی‌شده دیگری می‌کند، به این شکل که درخواست‌های مخرب از وب‌سایتی که کاربر بازدید می‌کند به تارنمای دیگری که مهاجم حدس می‌زند کاربر از قبل در آن تصدیق اصالت شده است، فرستاده می‌شوند. بیش‌تر برنامه‌های کاربردی تحت وب مانند شبکه‌های اجتماعی، واسط پست الکترونیک مبتنی‌بر مرورگر، بانکداری آنلاین و واسط‌های وب تجهیزات شبکه ممکن است هدف حملات ناشی از این نوع آسیب‌پذیری‌ها قرار گیرند.

۱. Server-side Request Forgery
۲. Internal Network and Applications
۳. گاهی به‌شکل SQLi نیز بیان می‌شود.
۴. Cross-site Scripting
۵. XML External Entity
۶. External Entity
۷. Cross-site request forgery

با موفقیت‌آمیز بودن نفوذ به وب‌سایت سازمان، مهاجم (افزون‌بر اقدامات فوری مانند Deface کردن وب‌سایت) می‌تواند کنترل سیستم‌عامل سرور آسیب‌پذیر را به دست بگیرد و مرحله‌ی دوم نفوذ را آغاز کند. منظور از مرحله‌ی دوم نفوذ، تلاش برای گسترش دسترسی در سیستم‌عامل و سپس به پایگاه داده یا سایر بخش‌های شبکه است. گسترش دسترسی در شبکه با توجه به معماری شبکه‌ی قربانی متفاوت خواهد بود. در این شکل یک نمونه‌ی متداول از معماری شبکه‌ی سرویس‌های تحت وب در سازمان‌ها نمایش داده شده است:



در بخش بعد راهکارهای مقابله و پیش‌گیری از حملات سایبری موفق به سرویس‌های تحت وب به‌شکل خلاصه شرح داده شده است.

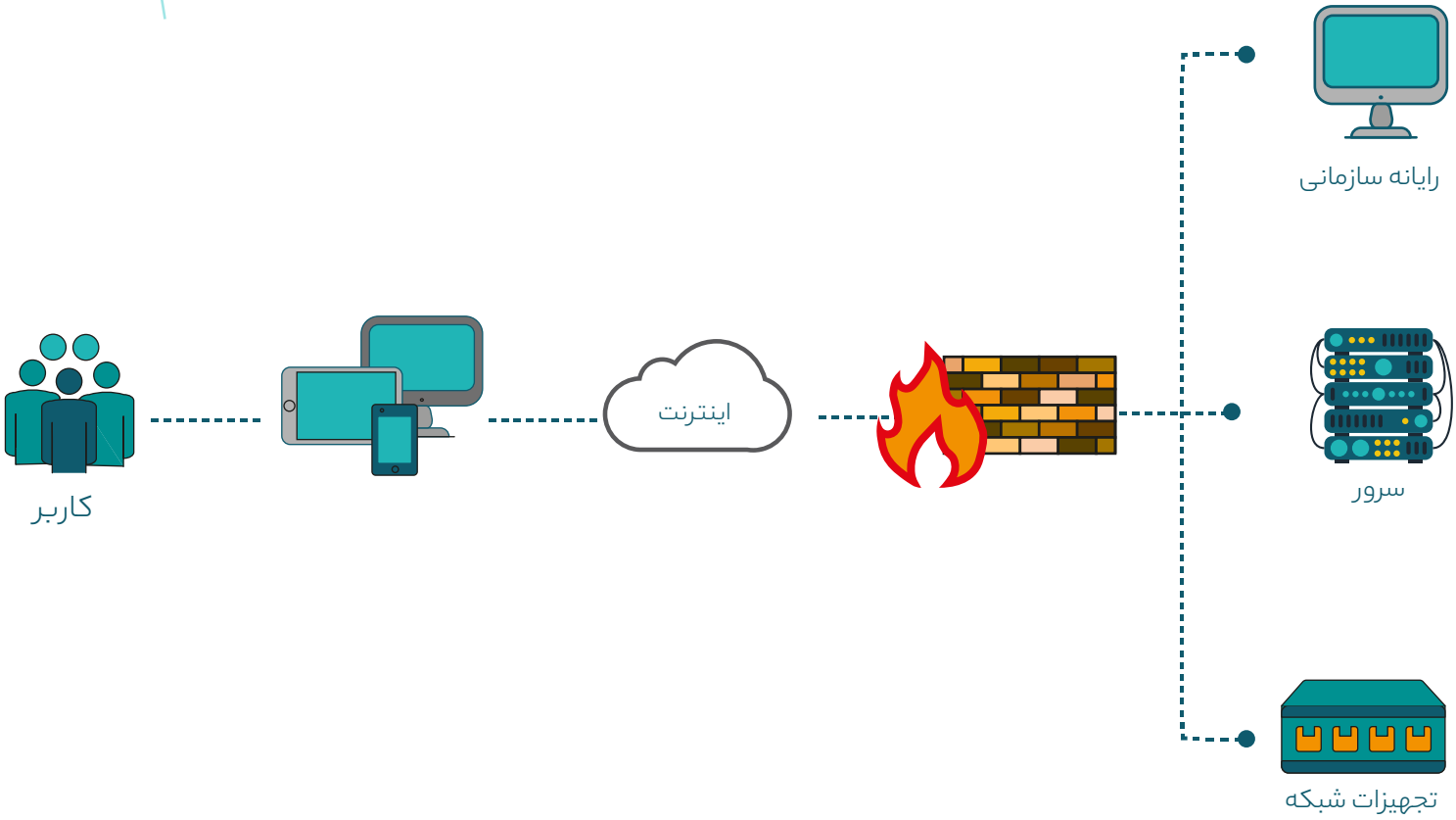
راهکارهای مقابله با نفوذ به زیرساخت به واسطه‌ی سرویس‌های تحت وب

برخی از مهم‌ترین راهکارهای متداول در راستای جلوگیری از حملات تحت وب، به شرح زیر است:

۱. تولید نرم‌افزارهای تحت وب براساس چرخه‌ی تولید امن نرم‌افزار[۱]
۲.انجام آزمون نفوذپذیری روی سامانه‌های تحت وب در محیط عملیاتی و به‌شکل دوره‌ای
۳.راه‌اندازی برنامه‌ی «پاداش در قبال کشف آسیب‌پذیری» یا همان باگ‌بانتی[۲]
۴.استفاده از تجهیزات امنیتی لایه‌ی کاربردی، از جمله WAF[۳]
۵.مقاوم‌سازی[۴] سیستم‌عامل‌ها و زیرساخت

در واقع راهکارهای بسیار متعدد و متنوعی برای مقابله با حملات تحت وب وجود دارد که پرداختن به تمام روش‌ها خارج از حوصله‌ی این مقاله است و در این‌جا به همین موارد کلی بسنده می‌کنیم.

نفوذ از طریق راهکارهای ارتباط از راه دور



۱. Secure Software Development Life Cycle
۲. Bug Bounty Program
۳. Web Application Firewall
۴. Hardening

امروزه نیاز به ارتباط از راه دور با رایانه‌ها، سرورها و تجهیزات شبکه در بیش‌تر سازمان‌ها وجود دارد. برای نمونه، می‌توان به نیازهایی چون دورکاری پرسنل سازمان، مدیریت تجهیزات موجود در شعب مختلف به‌کمک کارشناسان سازمانی مستقر در ساختمان مرکزی، دریافت خدمات پشتیبانی از شرکت‌های پیمانکار و ده‌ها مورد دیگر اشاره کرد. با توجه به نوع نیاز موجود، از راهکارها و پروتکل‌های مختلفی در زمینه‌ی ارتباط از راه دور استفاده می‌شود. پرکاربردترین این موارد عبارت‌اند از:

- **Telnet**: یکی از پروتکل‌های قدیمی و ناامن است که بیش‌تر به‌منظور ارتباط متنی برای مدیریت تجهیزات شبکه یا سرورهای مبتنی‌بر یونیکس[1] کاربرد دارد.
- **SSH**[2]: مشابه پروتکل Telnet و درواقع جایگزینی امن‌تر برای این پروتکل است. البته این پروتکل کاربردهای دیگری مانند انتقال فایل نیز دارد.
- **RDP**[3]: به‌منظور ارتباط تصویری با سرورهای مبتنی‌بر سیستم‌عامل ویندوز استفاده می‌شود.
- **VNC**[4]: این پروتکل نیز برای ارتباط تصویری با سرورها کاربرد دارد. از این پروتکل هم برای ارتباط با سرورهای مبتنی‌بر ویندوز و هم برای ارتباط با سرورهای مبتنی‌بر لینوکس استفاده می‌شود.
- **شبکه‌ی خصوصی مجازی یا VPN**[5]: کاربردهای آن را می‌توان به دو گروه اصلی ارتباط شبکه به شبکه و ارتباط کاربر به شبکه دسته‌بندی کرد که در این مقاله بیش‌تر کاربرد دوم مورد نظر ما است. پروتکل‌های مختلفی به‌منظور راه‌اندازی VPN وجود دارد که برخی از پرکاربردترین آن‌ها در سازمان‌ها به شرح زیر است:
  - **IPSec**: این پروتکل بیش‌تر با استفاده از پروتکل UDP پیاده‌سازی می‌شود و امروزه بیش‌تر برای ارتباطات بین شبکه‌ای کاربرد دارد.
  - **PPTP**[6]: پروتکل PPTP مبتنی‌بر TCP است و از مزایای آن می‌توان به Stability بالا اشاره کرد.
  - **SSL VPN**: در این‌جا VPN براساس پروتکل SSL پیاده‌سازی می‌شود. امروزه این پروتکل برای ارتباط کاربران با شبکه بسیار متداول است و تمام تجهیزات امنیتی از آن پشتیبانی می‌کنند.
- **زیرساخت میزکارمجازی VDI**[7]: که برای نمونه،می‌توان به محصولات و راهکارهای ارایه شده‌ی شرکت‌های VMWare و Citrix اشاره کرد.
- **سایر سرویس‌های ارتباط تصویری راه دور:** در سازمان‌ها از این سرویس‌ها بیش‌تر به‌منظور دریافت خدمات پشتیبانی از متخصصان و شرکت‌های پیمانکار استفاده می‌شود.
  از نمونه‌های پرکاربرد این سرویس‌ها در کشور می‌توان به TeamViewer و Ammyy Admin اشاره کرد.

روش‌های متداول نفوذ با استفاده از راهکارهای ارتباط از راه دور

با توجه به شیوه‌ی کاربرد یا پیاده‌سازی هر کدام از پروتکل‌های شرح داده شده در بخش قبل، مهاجمان می‌توانند از روش‌های مختلفی برای نفوذ استفاده کنند. به‌طور کلی، می‌توان این روش‌ها را به‌شکل زیر دسته‌بندی کرد:

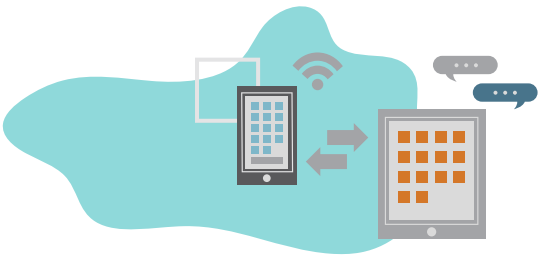
- **حملات Brute force**: در این روش مهاجمان رمز عبورهای متعددی را با نام‌های کاربری مختلف امتحان می‌کنند تا اگر رمز عبور قابل حدس یا ضعیف باشد، بتوانند به سرویس قربانی وارد شوند.

- **حملات Password Spray**: مشابه حمله Brute force است با این تفاوت که تعداد بسیار کمی رمز عبور (برای نمونه، ۲ رمز عبور) پرکاربرد بین کاربران را روی تعداد بالایی از کاربران امتحان می‌کنند. احتمال موفقیت این روش نسبت به روش قبل کم‌تر است اما مزیت آن در این است که حساسیت بسیار کم‌تری در تجهیزات امنیتی قربانی (Firewall، IDS، SIEM) ایجاد می‌کند و در نتیجه احتمال شناسایی حمله توسط SOC سازمان کاهش می‌یابد.

- **حملات مهندسی اجتماعی**[1]: در این حملات مهاجم با سواستفاده از روابط کاری و اجتماعی روزانه پرسنل سازمان قربانی تلاش می‌کند تا رمز عبور یا اطلاعات حیاتی آن‌ها را به سرقت ببرد. استفاده از این روش بین نفوذگران به‌شدت در حال رشد است. از دلایل استقبال مهاجمان از این حملات می‌توان به مواردی مانند عدم نیاز به دانش فنی بالا، نقض بخش درخور توجهی از تمهیدات امنیتی سازمان توسط خود پرسنل و کارشناسان آن سازمان، شناسایی دشوار آن به هنگام موفقیت‌آمیز بودن و... اشاره کرد.

- **اکسپلویت**[2] **آسیب‌پذیری‌های موجود:** با توجه به شیوه‌ی پیاده‌سازی و پیکربندی سرویس‌های ارتباط از راه دور توسط سازمان قربانی، ممکن است مهاجمان از آسیب‌پذیری‌های احتمالی مختلفی بتوانند سواستفاده کنند.

برای نمونه، می‌توان به آسیب‌پذیری‌های مبتنی‌بر وب (مانند صفحه‌ی ورود VPNها)، رمز عبور یا پیکربندی پیش فرض، آسیب‌پذیری‌های ذاتی موجود در پروتکل (مانند Heartbleed SSL) و... اشاره کرد.



به‌طور کلی، نفوذ به شبکه با استفاده از سرویس‌های ارتباط از راه دور می‌تواند تبعات جبران‌ناپذیری برای سازمان قربانی در پی داشته باشد. از طرفی معماری شبکه‌ی قربانی نیز تاثیر بسیار مهمی در تعیین سطح مخاطرات ناشی از این نوع حملات خواهد داشت. برای نمونه، شبکه‌ای که به‌درستی بخش‌بندی و کنترل دسترسی در آن پیاده‌سازی شده باشد کار را برای نفوذگران دشوارتر خواهد کرد.

در بخش بعد برخی از راهکارهای موثر برای مقابله با این نوع حملات به‌طور اجمالی شرح داده شده است.

۱. Social engineering
۲. Exploit

مقابله با نفوذ مهاجمان از طریق راهکارهای ارتباط از راه دور

برای مقابله‌ی موثر با حملات سایبری لازم است که متخصصان دفاع سایبری در کنار استانداردهای امنیتی، از خلاقیت شخصی نیز برخوردار باشند. در واقع، نفوذگران افراد خلاقی هستند و با استانداردهای امنیتی به‌تنهایی نمی‌توان در مقابل تفکر خلاق انسانی ایستادگی کرد. بنابراین با ترکیب روش‌های گوناگون پیش‌گیرانه و شناسایی، راهکارهای بسیار متنوعی برای مقابله با مهاجمان می‌توان تعریف کرد. در این بخش به بررسی برخی از روش‌های موثر برای مقابله با نفوذ مهاجمان از طریق راهکارهای ارتباط از راه دور سازمان پرداخته می‌شود.
راهکارهای ارایه شده در این بخش را به دو گروه کلی خط‌مشی‌های امنیتی[1] و قوانین SIEM تقسیم می‌کنیم.

برخی از خط‌مشی‌های امنیتی که می‌تواند کار را برای مهاجمان دشوارتر کند عبارت‌اند از:

- حداقل کردن تعداد راهکارهای ارتباط از راه دور سازمان، به‌گونه‌ای که به‌راحتی بتوان آن‌ها را کنترل کرد.
- استفاده از روش‌های احراز هویت دو یا چند عاملی برای تمام راهکارهای ارتباط از راه دور سازمان.
- تا جایی‌که امکان دارد سرویس‌هایی مانند RDP، Telnet و SSH به‌طور مستقیم از اینترنت دردسترس نباشند. برای نمونه، کارشناسان پس از ارتباط با شبکه‌ی سازمان از طریق VPN امکان دسترسی به این سرویس‌ها را داشته باشند.
- استفاده از رمز عبورهای پیچیده با حداقل طول ۱۲ کاراکتر.
- پیاده‌سازی کنترل دسترسی سخت‌گیرانه در ارتباطات VPN و به‌طور کلی در تمام راهکارهای ارتباط از راه دور. برای نمونه، هنگام ارایه‌ی دسترسی VPN به یک کاربر، آن فرد تنها به سرویس مورد نیاز خود روی نشانی IP مورد نظر دسترسی داشته باشد و نتواند تمام یا بخشی از شبکه را مشاهده کند.
- بخش‌بندی شبکه به‌گونه‌ای که اگر مهاجم به یک سرور دسترسی پیدا کرد از طریق آن به تمام منابع شبکه دسترسی مستقیم نداشته باشد. در این حالت ممکن است مهاجم مجبور شود تا حملات بیش‌تری را برای گسترش دسترسی خود انجام دهد که این امر احتمال شناسایی مهاجم را توسط سامانه‌ی SIEM سازمان افزایش خواهد داد. برای بخش‌بندی سخت‌گیرانه‌ی شبکه می‌توان از راهکار Private VLAN یا راهکارهای مشابه و جایگزین آن نیز بهره برد.
- شرکت مایکروسافت در طراحی سیستم‌عامل‌های ویندوز سرور ۲۰۱۶ (و سرویس‌های مربوطه مانند Active Directory) و ویندوز ۱۰، از راهکارهای پیش‌گیرانه‌ی متعددی برای مقابله با نفوذگران استفاده کرده است و مهاجرت به این نسخه از سیستم‌عامل‌ها به شدت توصیه می‌شود.
- تعریف و اعمال خط‌مشی‌های سخت‌گیرانه به‌روزرسانی تمام سرویس‌ها و سیستم‌عامل‌های موجود در شبکه‌ی سازمان.
- تعریف خط‌مشی امنیتی در راستای ممنوعیت استفاده از راهکارهای ارتباط از راه دور که کنترل و مدیریت آن‌ها برای واحد امنیت سازمان دشوار است.
مانند TeamViewer و موارد مشابه آن.

۱. Security Policy

در کنار خط‌مشی‌های تعریف‌شده، لازم است تا توانایی شناسایی رفتارهای مشکوک در شبکه را نیز با استفاده از تجهیزات امنیتی و سامانه‌ی SIEM تقویت کرد. برخی از قوانین تعریف‌شدنی در سامانه‌ی SIEM به‌منظور شناسایی رفتار مهاجمان برای نفوذ به راهکارهای ارتباط از راه دور سازمان، به شرح زیر است:

- برای نمونه اگر در یک بازه‌ی زمانی ۳۰ دقیقه‌ای روی هر سرویس، تعداد فراوانی تلاش برای ورود (احراز هویت) ثبت شود، احتمال وجود یک حمله‌ی Brute Force یا Password Spray وجود دارد. اگر سازمان تنها از رمز عبور (احراز هویت تک‌عاملی) برای احراز هویت سرویس راه دور خود استفاده می‌کند، باید خط‌مشی‌ها و راهکارهای به‌شدت سخت‌گیرانه‌ای را برای مقابله با حملات Brute Force تدبیر کند.

- اگر از یک نشانی IP و در یک بازه‌ی زمانی مشخص، روی سرویس‌های مختلف سازمان برای احراز هویت تلاش شده باشد، این مورد شبیه به حمله‌ی Password Spray است. حتا اگر روی هر سرویس تنها یک‌بار برای ورود تلاش شده باشد.

- اگر از نشانی‌های IP مختلف به یک سرویس خاص، در یک بازه‌ی زمانی مشخص برای احراز هویت تلاش شده باشد این مورد نیازمند بررسی است، حتا اگر تمام احراز هویت‌ها به موفقیت انجام شده باشند.

- اگر به یک سرویس ارتباط از راه دور سازمان از نشانی IP یک کشور دیگر (به‌ویژه کشورهایی که سازمان هیچ نماینده یا شعبه‌ای در آن کشور ندارد) احراز هویت موفق انجام شده باشد، این مورد باید به دقت بررسی شود.

- اگر پس از یک احراز هویت موفق در سرویس ارتباط از راه دور (برای نمونه، VPN سازمان) تلاش شده است تا با یک یا چند تا از سرورها یا سرویس‌های حیاتی سازمان ارتباط برقرار شود، این مورد نباید از دید کارشناسان امنیت سازمان دور بماند.

- هرگونه تغییر در پیکربندی سرویس‌های ارتباط از راه دور باید مانیتور شود و یک پیام هشدار برای گروه امنیت سازمان ارسال کند.

- ترافیک سرویس‌های ارتباط از راه دور (هم ترافیک ورودی و هم ترافیک خروجی) باید با دقت مانیتور و تغییرات ترافیکی مشکوک، بررسی شوند.

- اگر بدافزاری در شبکه شناسایی شود که آن بدافزار را یکی از کاربران VPN یا سایر راهکارهای ارتباط از راه دور اجرا کرده باشد، در این مورد سامانه باید یک پیام هشدار با اولویت بسیار بالا ایجاد کند.

- به‌منظور مقابله با حملات نفوذگران، با توجه به نوع کسب‌وکار سازمان و سطح حساسیت آن در برابر حملات سایبری لازم است تا خط‌مشی‌های امنیتی و قوانین بسیار متعددی تعریف و پیاده‌سازی شود که در این سند تنها به برخی از نمونه‌های مهم آن اشاره شده است.

حملات مبتنی‌بر مهندسی اجتماعی

حملات مهندسی اجتماعی حملات غیرفنی (Non-Technical) هستند که به‌جای هدف قرار دادن سامانه‌ها و پروتکل‌های شبکه، پرسنل سازمان را هدف قرار می‌دهند. در این حملات مهاجمان از روابط انسانی به‌منظور سرقت اطلاعات محرمانه یا اجرای بدافزارهای خود در شبکه‌ی قربانی بهره می‌برند. میزان موفقیت حملات مهندسی اجتماعی به توانایی نفوذگر در متقاعد کردن قربانی به انجام فعالیت مورد نظر، هم‌چنین میزان آگاهی فرد قربانی بستگی دارد. به همین دلیل مهاجمان سناریوهای مختلفی برای اجرای حملات خود طراحی می‌کنند. برای نمونه، برخی از سناریوهای متداول در این حملات به شرح زیر است:

- **ارسال ایمیل از سوی یک فرستنده ناآشنا اما با موضوع جذاب برای قربانی:** برای نمونه، ایمیلی را در نظر بگیرید که از قربانی درخواست می‌کند تا یک سند آلوده را که در ظاهر حاوی اطلاعات مربوط به یک بسته‌ی پستی است و از خارج کشور برای قربانی ارسال شده، دانلود و روی رایانه‌ی خود اجرا کند.

- **ارسال ایمیل از سوی یک شرکت یا سازمان آشنا برای قربانی:** برای نمونه، ارسال ایمیل از یکی از بانک‌های کشور که قربانی در آن حساب بانکی دارد، با این ادعا که برنده‌ی جایزه شده است و باید به نشانی که در ایمیل گفته شده، برود و با رمز عبور خود در آن وارد شود.

- **ارسال ایمیل از سوی یک فرد آشنا به قربانی:** فرض کنید از یکی از دوستان یا همکاران خود ایمیلی دریافت کنید که حاوی یک سند docx، فایل موسیقی یا هر نوع فایل دیگری باشد. چه‌قدر نسبت به باز کردن آن فایل در رایانه‌ی خود مقاومت می‌کنید؟

- **قرار دادن یک حافظه‌ی USB, CD یا هر نوع حافظه‌ی دیگری دردسترس پرسنل سازمان قربانی:** فرض کنید در پارکینگ سازمان یک حافظه‌ی USB با حجم ۶۴گیگابایت پیدا کنید. آیا این حافظه را به رایانه‌ی خود متصل می‌کنید؟ یا آن را تحویل واحد امنیت سازمان می‌دهید؟

در واقع بخش درخور توجهی از حملات مهندسی با استفاده از ارسال ایمیل‌هایی انجام می‌شود که یا حاوی فایلی برای دانلود یا یک لینک در بخش محتوای خود هستند و از کاربر می‌خواهند که روی آن کلیک کند. امروزه حملات مبتنی‌بر مهندسی اجتماعی یکی از بزرگ‌ترین تهدیدات سایبری علیه سازمان‌ها و شرکت‌ها در سراسر دنیا به‌شمار می‌آید. حملات مهندسی اجتماعی بیش‌تر بر مبنای علوم روان‌شناسی طراحی می‌شوند و اجرای این حملات در مقایسه با حملاتی که در بخش‌های دیگر شرح داده شد، به دانش فنی بالایی نیاز ندارد.

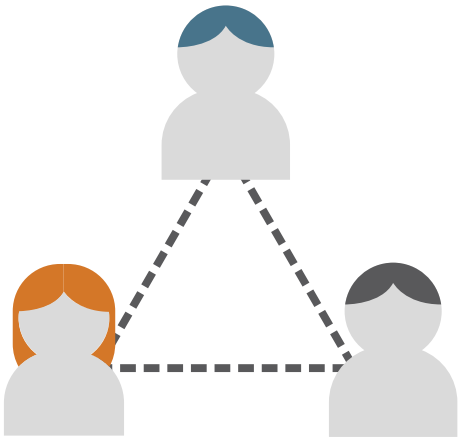
مقابله با حملات مهندسی اجتماعی

مهم نیست چه‌قدر برای تجهیزات امنیتی خود در شبکه هزینه کرده باشید (تجهیزاتی مانند فایروال، سامانه‌ی شناسایی نفوذ[1] و...)، پرسنل سازمان ممکن است هنوز در برابر حملات مهندسی اجتماعی آسیب‌پذیر باشند. البته امروزه تجهیزات و راهکارهایی برای مقابله با این نوع حملات ارایه شده است که سازمان‌ها را در راستای مقابله با این حملات یاری می‌کنند، اما نخستین و مهم‌ترین لایه‌ی دفاعی، خود افراد سازمان هستند که باید آموزش‌دیده و هوشیار باشند.

مهم‌ترین راهکارهای مقابله با حملات مهندسی اجتماعی عبارت‌اند از:

- آموزش تمام پرسنل و مدیران سازمان به‌منظور آشنایی آنان با حملات مهندسی اجتماعی، روش‌های متداول مورد استفاده‌ی مهاجمان، اقدامات مناسب هنگام مشاهده‌ی موارد مشکوک و...
- تدوین خط‌مشی در سازمان و طراحی راهکارها و زیرساخت لازم برای اعلام موارد مشکوک توسط کاربران سازمان و پاسخ‌گویی سریع واحد امنیت به حملات شناسایی‌شده.
- استفاده از روش‌های احراز هویت دو یا چند عاملی به‌ویژه برای سرویس‌هایی که از طریق اینترنت دردسترس هستند.
- استفاده از تجهیزات امنیت ایمیل[2] به‌منظور ارزیابی امنیتی تمام ایمیل‌های دریافت شده، فایل‌های پیوست، لینک‌های موجود در ایمیل‌ها، مقابله با هرزنامه‌ها[3] و...
- استفاده از خط‌مشی‌هایی در شبکه به‌منظور عدم امکان نصب نرم‌افزارهای متفرقه توسط کاربران
- استفاده از خط‌مشی‌هایی در راستای عدم امکان اجرا شدن انواع اسکریپت‌های غیرضروری در رایانه کاربران و حتا سرورهای شبکه.
- غیرفعال کردن امکان Macro در نرم‌افزارهای MS Office در تمام سطح شبکه.
- به‌روز نگه داشتن سیستم‌عامل، مرورگر وب، آنتی‌ویروس و سایر ابزارهای کاربردی کاربران سازمان.
- انجام تست نفوذ تخصصی مبتنی‌بر روش‌های مهندسی اجتماعی به‌شکل دوره‌ای و به‌منظور شناسایی نقاط ضعف سازمان.

پرداختن به جزییات بیش‌تر این نوع حملات، خارج از حوصله‌ی این مقاله است، زیرا مبحث حملات مهندسی اجتماعی بسیار مفصل است و لازم است تا در یک مقاله‌ی جداگانه به‌طور کامل مورد بررسی قرار گیرد.



۱. IDS
۲. Email security
۳. Spam

اکسپلویت آسیب‌پذیری‌های سیستم‌عامل و سرویس‌ها

اکسپلویت به زبان ساده بهره‌گیری از نقاط ضعف یا همان آسیب‌پذیری‌های[1] موجود در سیستم‌عامل، نرم‌افزار، پروتکل یا هر برنامه‌ی دیگری به‌منظور اجرای دستورات مورد نظر مهاجم در سامانه‌ی قربانی یا ایجاد اختلال در سرویس‌دهی آن است.

دلیل وجود این آسیب‌پذیری می‌تواند شیوه‌ی برنامه‌نویسی، کتاب‌خانه‌های مورد استفاده یا هر علت دیگری باشد. وجود این آسیب‌پذیری‌ها حتا در پیشرفته‌ترین سیستم‌عامل‌ها و سرویس‌ها نیز امری اجتناب‌ناپذیر است و به همین دلیل روزانه شاهد معرفی تعداد بالایی آسیب‌پذیری توسط کارشناسان و شرکت‌های امنیتی هستیم. اکسپلویت‌ها با اهداف مختلفی طراحی و اجرا می‌شوند که برخی از متداول‌ترین این اهداف به شرح زیر است:

- نفوذ به سامانه‌ی آسیب‌پذیر
- گسترش دسترسی در رایانه یا شبکه‌ی آسیب‌پذیر
- نصب بدافزار در سامانه‌ی آسیب‌پذیر
- دسترسی به داده‌های حساس موجود در سامانه‌ی آسیب‌پذیر
- ایجاد اختلال در سرویس‌دهی سامانه‌ی آسیب‌پذیر یا از کارانداختن آن

اکسپلویت‌ها با توجه به نوع عملکردشان می‌توانند در مراحل مختلف یک حمله‌ی APT استفاده شوند. برای نمونه، ممکن است در حمله‌ای از یک آسیب‌پذیری برای نفوذ اولیه به سازمان قربانی استفاده کرد و در حمله‌ای دیگر ابتدا با یکی از روش‌هایی که پیش‌تر گفته شد به سازمان قربانی نفوذ کرد، سپس از آسیب‌پذیری‌های موجود در شبکه، برای گسترش دسترسی بهره برد.

اکسپلویت‌ها را بسته به روش عملکرد آن‌ها و نوع حملاتی که با استفاده از آن‌ها انجام می‌شود، به روش‌های مختلفی می‌توان دسته‌بندی کرد. یکی از معروف‌ترین انواع آن، اکسپلویت‌های zero-day است که از آسیب‌پذیری‌های zero-day بهره می‌برد. آسیب‌پذیری zero-day در واقع آسیب‌پذیری است که به جز نفوذگران هیچ شخص یا شرکتی (حتا شرکت تولیدکننده‌ی آن سامانه) از آن اطلاع ندارد. به این ترتیب تا زمانی‌که این آسیب‌پذیری zero-day بماند، مهاجمان هر جا به سامانه‌ی آسیب‌پذیر دسترسی پیدا کنند، می‌توانند از اکسپلویت خود بهره‌برداری کنند.

بیش‌تر این آسیب‌پذیری‌ها پس از مدتی شناسایی و توسط شرکت مربوطه با ارایه‌ی بسته‌های به‌روزرسانی برطرف می‌شوند. طبیعی است که از لحظه‌ی شناسایی یک آسیب‌پذیری zero-day تا ارایه بسته‌ی به‌روزرسانی و نصب این بسته روی بیش‌تر سامانه‌های آسیب‌پذیر، ممکن است به بازه‌ی زمانی بین چند هفته تا چند ماه نیاز باشد. این اکسپلویت‌ها zero-day به‌شمار نمی‌آیند، اما این بازه‌ی زمانی به‌نسبت طولانی، فرصت خوبی برای دیگر مهاجمان است تا در نفوذهای خود از این آسیب‌پذیری‌ها بهره‌برداری کنند.

۱. Vulnerability

مقابله با حملات مبتنی بر اکسپلویت‌های zero-day و غیر zero-day

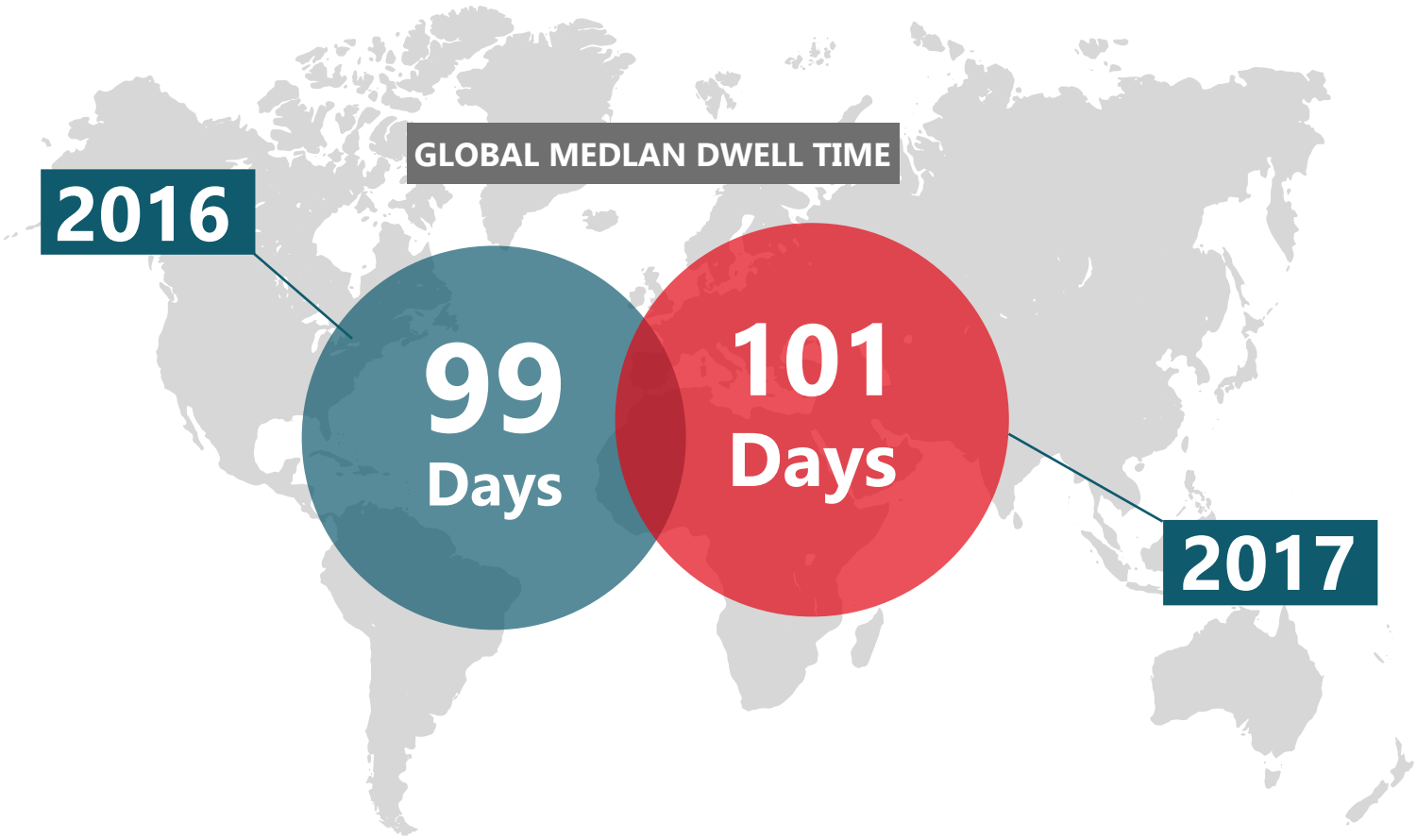
بهترین راه برای مقابله با اکسپلویت‌های غیر zero-day به‌روز رسانی مداوم تمام سیستم‌عامل‌ها، تجهیزات شبکه و سایر سرویس‌ها است. پس از ارایه بسته به روزرسانی امنیتی توسط شرکت ارایه‌دهنده سامانه آسیب‌پذیر، هر روز تاخیر در نصب این بسته‌ها معادل باز گذاشتن یک مسیر نفوذ به سامانه‌های اطلاعاتی سازمان برای نفوذگران است.

اما مقابله با نفوذگرهایی که مجهز به اکسپلویت‌های zero-day هستند (برای نمونه، گروه‌های نفوذی که توسط دولت‌ها پشتیبانی می‌شوند) بسیار پیچیده‌تر است. تجهیزات امنیتی متداول مانند IDS، Firewall و... به‌تنهایی نمی‌توانند راهکار دفاعی مطمینی در برابر این گروه‌های مهاجم باشند. در واقع به همین دلیل است که گفته می‌شود هیچ‌گاه یک سازمان نمی‌تواند تنها با استفاده از تجهیزات و متخصصان امنیتی از نفوذ تمام مهاجمان به سامانه‌های اطلاعاتی خود جلوگیری کند.

موثرترین روش برای مقابله با این حملات، افزایش توان شناسایی رفتارهای مشکوک در سطح سیستم‌عامل و شبکه است. برای این منظور می‌توان از سامانه‌های SIEM در واحد SOC استفاده کرد. البته دستیابی به یک سامانه‌ی SIEM قابل اتکا در سازمان به عوامل متعددی وابسته است که برخی از مهم‌ترین آن‌ها در ادامه آمده است.

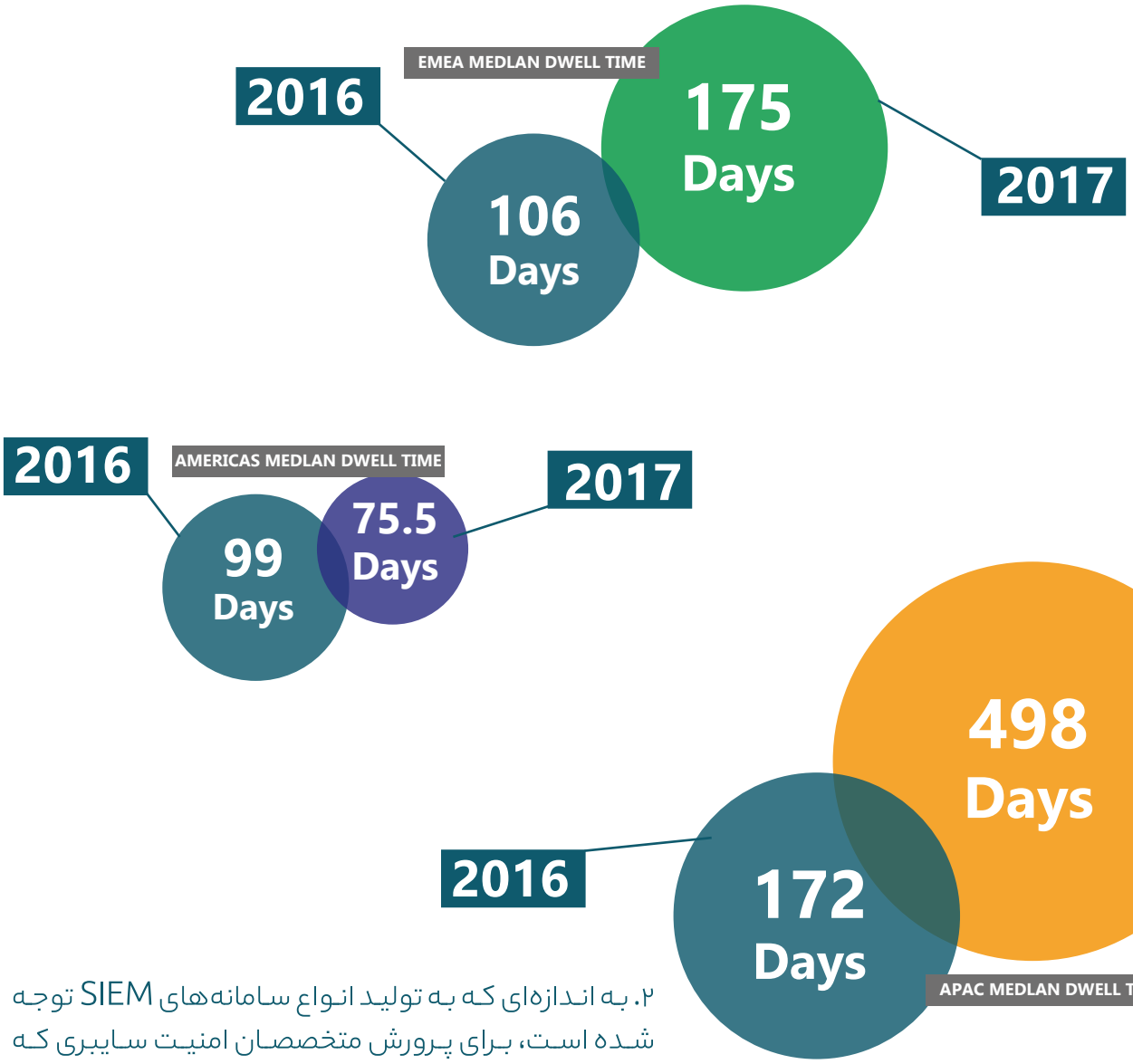
- بهره‌مندی از یک سامانه‌ی SIEM استاندارد که از حداقل امکانات مورد نیاز برخوردار باشد؛ برای نمونه، امکان شناسایی و تحلیل ارتباط بین وقایع گردآوری‌شده از انواع مختلف سیستم‌عامل‌ها، سرویس‌ها و تجهیزات مختلف شبکه را با آسیب‌پذیری‌های شناسایی‌شده و ارزش مشخص‌شده برای دارایی‌های سازمان را در تحلیل‌های خود داشته باشد.
- وجود متخصصانی که با رفتار نفوذگران در شبکه و سامانه‌های اطلاعاتی آفلاین و آنلاین آشنایی کامل داشته باشند و به بیان ساده‌تر، بدانند که باید به‌دنبال چه نوع رفتارهای مشکوکی در سازمان باشند.
- تعریف انواع قواعد به‌منظور شناسایی وقایع مشکوک توسط این متخصصان و به‌روزرسانی مداوم این قواعد به‌منظور پوشش دادن جدیدترین روش‌های نفوذ و گسترش دسترسی.
- امکان پاسخ‌گویی سریع به اتفاقات مشکوک به حمله، بدافزار و موارد مشابه.
- بهره‌مندی سازمان از خدماتی مشابه تیم قرمز به‌منظور شناسایی نقاط ضعف و آسیب‌پذیری‌هایی که ممکن است از چشم متخصصان امنیت دور بماند [شرح خدمات تیم قرمز در یک مقاله‌ی جداگانه ارایه و بررسی خواهد شد].

یکی از مباحثی که امروزه مورد توجه شرکت‌ها و متخصصان امنیت سایبری در دنیا قرار گرفته، افزایش سرعت شناسایی نفوذگرانی است که موفق شده‌اند به شبکه‌ی سازمان نفوذ کنند. این موضوع سبب پدید آمدن مفهومی جدید شده است که شرکت Fireeye آن را «مدت زمان دویل[1]» می‌نامد. «مدت زمان دویل» را می‌توان این‌گونه تعریف کرد: «تعداد روزها، در فاصله‌ی بین نخستین فعالیت ثبت شده از مهاجم در شبکه‌ی قربانی تا تاریخ شناسایی آن توسط گروه امنیت سازمان». شکل زیر مقدار میانه زمان دویل (دقت داشته باشید که از «میانگین» استفاده نشده است) در سطح دنیاست که شرکت Fireeye برای سال‌های ۲۰۱۶ و ۲۰۱۷ میلادی ارایه کرده است:



۱. Dwell time

در شکل زیر نیز مقایسه‌ی مقدار میانه‌ی زمان دویل در قاره‌های مختلف در سال‌های ۲۰۱۶ و ۲۰۱۷ میلادی نمایش داده شده است:



با توجه به موارد گفته شده متاسفانه در ایران با دو مشکل بزرگ در زمینه‌ی بهره‌مندی سازمان‌ها از سامانه‌های SIEM روبه‌رو هستیم:

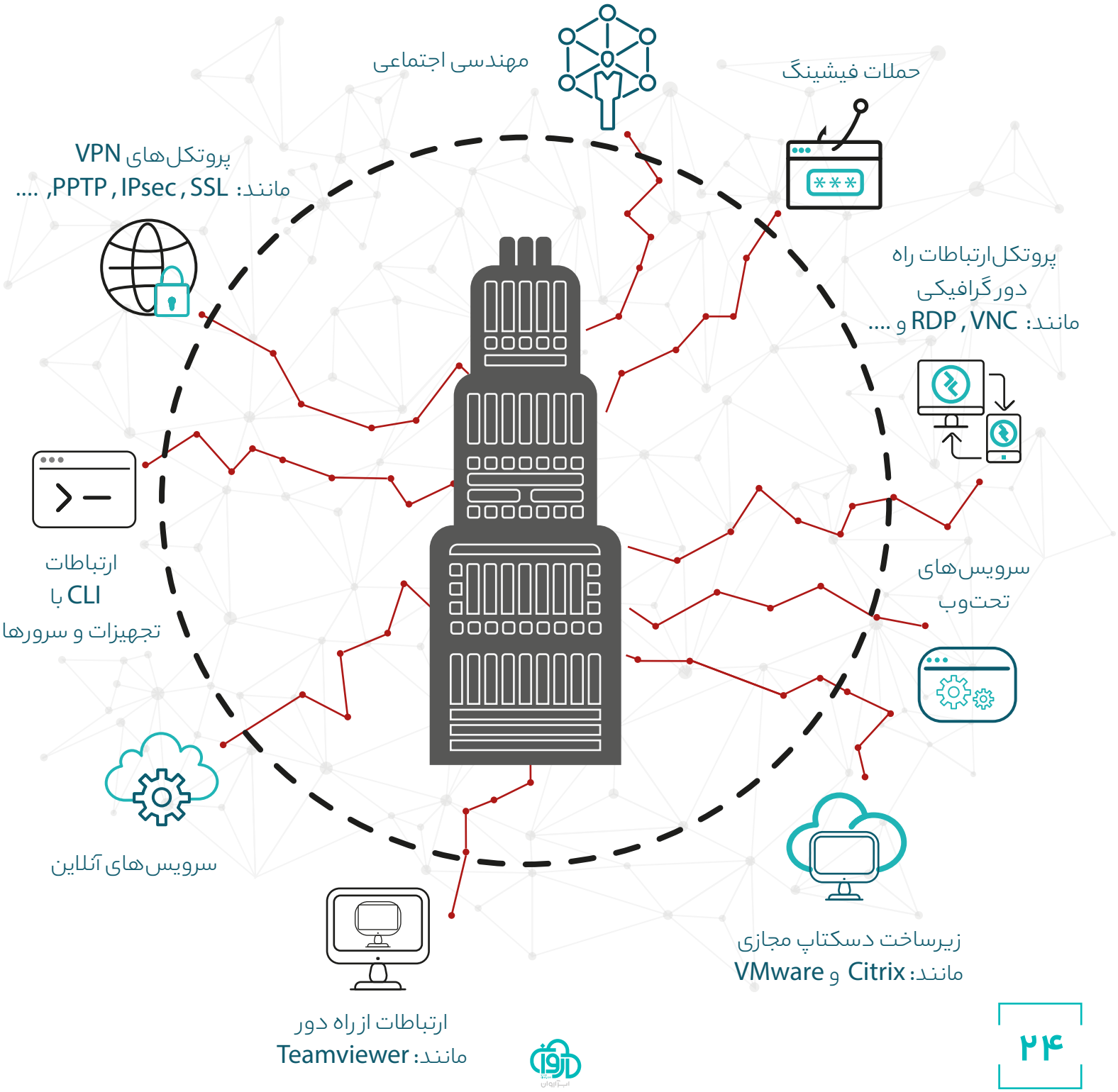
۱. بیش‌تر سامانه‌های SIEM ارایه شده‌ی بومی از نظر کیفیت و امکانات در مقایسه با نمونه‌های خارجی خود هنوز مسیر طولانی در پیش دارند.

۲. به اندازه‌ای که به تولید انواع سامانه‌های SIEM توجه شده است، برای پرورش متخصصان امنیت سایبری که توانایی راهبری این سامانه‌ها را داشته باشند، تلاشی انجام نمی‌شود. به همین دلیل تعداد متخصصان موجود به هیچ‌وجه پاسخ‌گوی سطح نیاز فعلی کشور نخواهد بود.

مبحث مقابله با حملات مبتنی‌بر اکسپلویت‌های zero-day بسیار گسترده است و لازم است تا در مقاله‌ای مجزا به بررسی جوانب مختلف این موضوع پرداخته شود.

نفوذ به سازمان قربانی در یک نگاه

در بخش‌های قبل مروری اجمالی داشتیم بر روش‌های متداولی که مهاجمان برای نفوذ به زیرساخت سازمان‌ها و شرکت‌ها از آن‌ها بهره می‌برند. اما استفاده از یک تصویر مناسب می‌تواند حق مطلب را بهتر از ده‌ها صفحه محتوا ادا کند و به همین دلیل، خلاصه‌ی تمام روش‌های نفوذ که در بخش‌های قبل شرح داده شد در شکل زیر نمایش داده شده است.



شبیه‌سازی یک حمله‌ی سایبری در سطح متوسط

یکی از دلایل اصلی نگارش این سری از مقالات، افزایش آگاهی کارشناسان فعال در حوزه‌ی فناوری اطلاعات با روش‌های مورد استفاده‌ی نفوذگران در دنیای امروز است تا بتوانند با دیدگاه وسیع‌تری نسبت به مقابله با حملات سایبری اقدام کنند. به همین دلیل در آخرین بخش هر مقاله به شبیه‌سازی یک حمله‌ی سایبری از مراحل ابتدایی حمله تا دستیابی به هدف نهایی حمله توسط نفوذگران می‌پردازیم.

در این بخش برای نخستین شبیه‌سازی، یک حمله‌ی سایبری با سطح فنی متوسط (به این معنی که این حمله را یک شخص یا گروه نفوذ با سطح دانش فنی متوسط می‌تواند انجام دهد) شرح داده شده است.

یک سازمان فرضی را در نظر بگیرید که یک نفوذگر قصد حمله به آن را دارد. در این مقاله این سازمان را «سازمان هدف» می‌نامیم و فرض می‌کنیم دامنه‌ی رسمی آن سازمان target-org.com نام دارد. سازمان هدف وظیفه‌ی ارایه‌ی یک خدمت عمومی در سطح کشور را به‌عهده دارد و به همین دلیل در پایگاه داده‌های خود اطلاعات شخصی بخش درخورتوجهی از جمعیت کشور را ذخیره کرده است. در ادامه به‌منظور باورپذیرتر کردن داستان، سناریوی حمله به‌شکل سوم‌شخص از دیدگاه یک نفوذگر با نام مستعار «نفوذگر سیاه» روایت می‌شود.

گفتنی است، مطالب گفته شده از نظر فنی بررسی و تایید شده هستند، اما به برخی دلایل تجربی از ارایه‌ی تمام جزییات فنی خودداری شده است.

شناسایی هدف

«نفوذگر سیاه» در قدم نخست با استفاده از nslookup نشانی IP دامنه target-org.com را بررسی می‌کند که معادل 172.16.30.50 است. در گام بعد، با استفاده از یک سرویس whois برای کسب اطلاعات بیش‌تر درباره‌ی نشانی IP مذکور، متوجه می‌شود بازه‌ی نشانی 172.16.30.0/26 به نام سازمان هدف ثبت شده است. بی‌درنگ با استفاده از یک ابزار اسکنر (مانند NMAP) این Range را به‌منظور شناسایی تمام سرویس‌های آنلاین سازمان هدف اسکن و در مجموع ۲۸ سرویس مختلف را شناسایی می‌کند.

نفوذگر سیاه پس از بررسی‌های اولیه، متوجه می‌شود سازمان هدف تمام ۲۸ سرویس شناسایی‌شده را به‌خوبی امن‌سازی کرده است و در حال حاضر امکان نفوذ به سازمان با استفاده از این سرویس‌ها ممکن نیست. اما ناامید نمی‌شود و دوباره گردآوری اطلاعات بیش‌تر از سازمان هدف را آغاز می‌کند.

به‌دلیل ایراداتی که در پیکربندی سرویس‌های مبتنی‌بر سرور ویندوز وجود دارد، اطلاعاتی از قبیل نام دامین اکتیو دایرکتوری داخلی سازمان (target.local) و غیره را به‌دست می‌آورد و با این‌که این اطلاعات پس از نفوذ ممکن است استفاده شوند، اما در آن لحظه برای او کاربردی ندارند. به این ترتیب، هنوز لازم است تا تلاش بیش‌تری برای گردآوری اطلاعات داشته باشد. به همین دلیل، از چند تکنیک ساده برای شناسایی دامنه‌ها و زیردامنه‌های سازمان هدف استفاده می‌کند. در یکی از این روش‌ها، با استفاده از ابزار AQUATONE دامنه‌ی target-org.com را به‌منظور پیدا کردن زیردامنه‌های جدید Bruteforce می‌کند و همان‌طور که در شکل زیر نمایش داده شده است در خروجی آن به چند زیردامنه‌ی جدید برمی‌خورد:

```
172.16.30.50 ,target-org.com
172.16.30.50 ,www.target-org.com
172.16.30.26 ,news.target-org.com
172.16.30.14 ,cdn.target-org.com
172.16.30.31 ,email.target-org.com
10.172.116.48 ,self.target-org.com
```

و متوجه یک زیردامنه از سازمان (self.target-org.com) می‌شود که نشانی IP این دامنه متفاوت از Range شناسایی شده‌ی قبل است، اما با بررسی نشانی‌های مجاور مشخص است که این نشانی نیز به سازمان هدف تعلق دارد.

به این ترتیب، نفوذگر سیاه امیدوار می‌شود که شاید سازمان هدف، توجه کم‌تری به این بخش از سرویس‌های خود داشته باشد، زیرا این کم‌توجهی احتمال وجود آسیب‌پذیری یا پیکربندی اشتباه را افزایش می‌دهد.

با بررسی IPهای مجاور، یک سرویس Jenkins قدیمی توجه او را به خود جلب می‌کند. با یک جست‌وجوی ساده متوجه دو آسیب‌پذیری اجرای کد از راه دور[1] روی این سرویس می‌شود که عبارت‌اند از:

- CVE-2016-9299
- CVE-2015-8103

۱. Remote Code Execution (RCE)

نفوذ اولیه به سازمان هدف و گسترش دسترسی در شبکه

به این ترتیب، نخستین دسترسی از سرویس Jenkins به‌دست می‌آید و مشخص می‌شود این سرویس روی سرور ویندوزی نصب شده است.

گفتنی است که سرویس Jenkins به شما امکان اجرای دستورات روی سیستم‌عامل (هم در ویندوز و هم در لینوکس) را نیز می‌دهد که یک مورد پرکاربرد آن استفاده از قابلیت «Execute Windows Batch Command» است. این قابلیت در شکل زیر نمایش داده شده است.

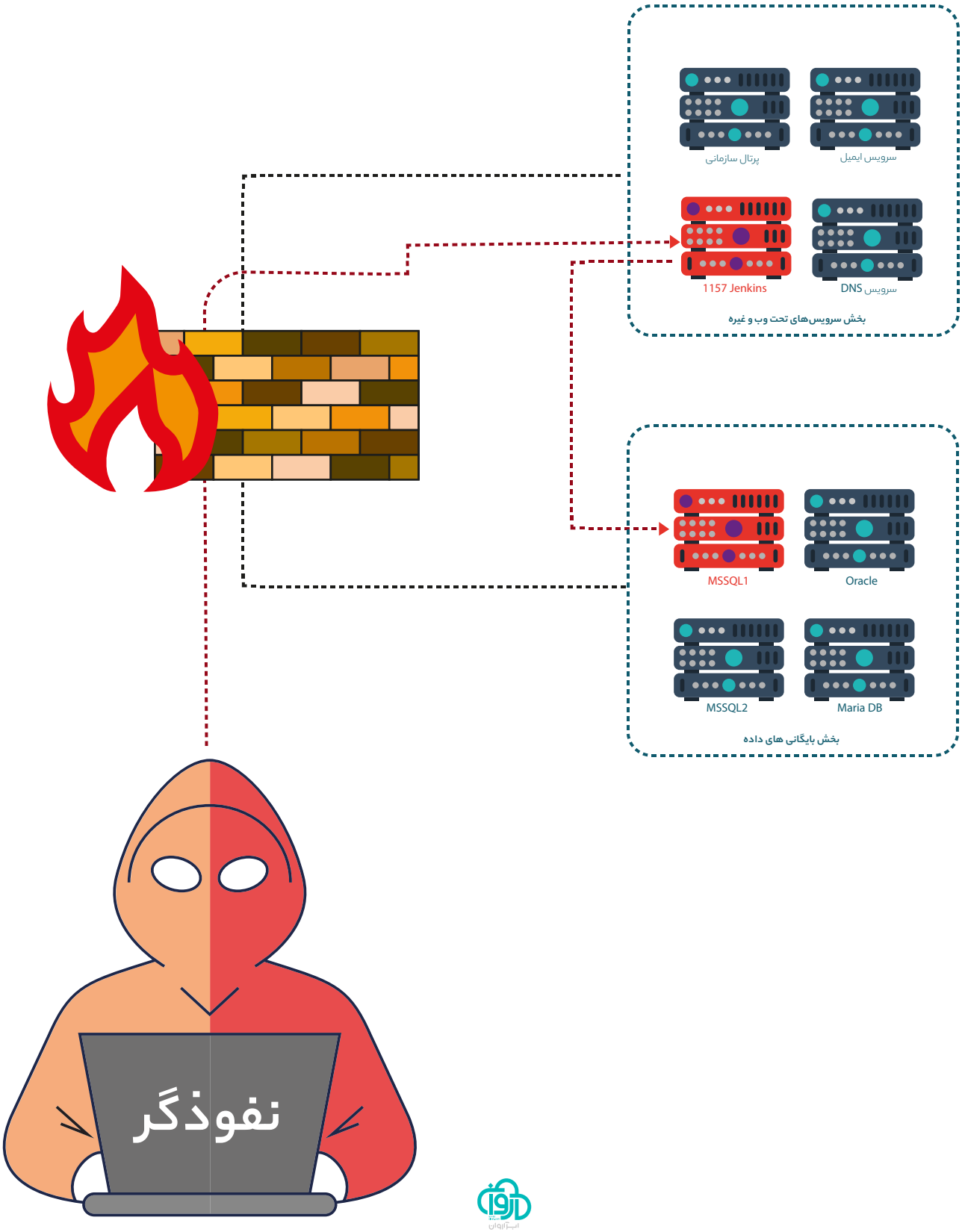
با اجرای دستور whoami پاسخ زیر از سیستم‌عامل دریافت می‌شود که مشخص می‌کند سطح دسترسی این سرویس در سیستم‌عامل بالاترین سطح دسترسی (یعنی دسترسی system) است:

```
nt authority\system
```

سازمان هدف برای افزایش امنیت، شبکه‌ی خود را به بخش‌های مختلف تقسیم کرده سرورهای پایگاه داده را در یک بخش مجزا از بخش سرویس‌های وب قرار داده است. نفوذگر سیاه با توجه به تجربیات قبلی خود می‌داند SQL server امکان اجرای دستورات با سطح دسترسی بالا روی سیستم‌عامل را دارد. با یک جست‌وجوی ساده همان‌گونه که در نمونه‌ی زیر می‌بینید، شیوه‌ی اجرای دستورات سیستم‌عامل در SQL server را پیدا می‌کند. با توجه به این که حساب کاربری sa امکان اجرای دستورات با سطح دسترسی بالا روی سیستم‌عامل را دارد، پس از آن، گرفتن دسترسی از این سرور نیز برای نفوذگر سیاه کار دشواری نیست.

```
EXEC xp_cmdshell 'dir c:\';
GO
```

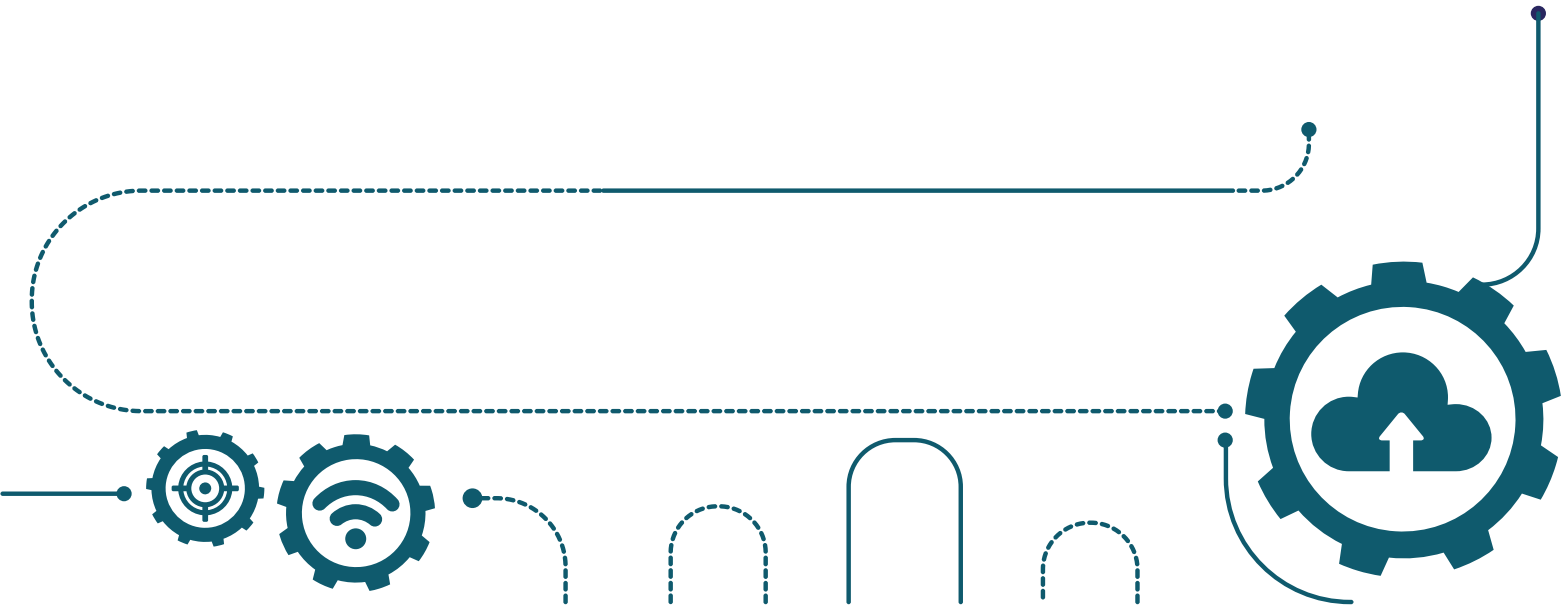
به این ترتیب، همان‌گونه که در شکل زیر نمایش داده شده است، نفوذگر سیاه دسترسی خود در شبکه‌ی سازمان هدف را به بخش پایگاه‌های داده گسترش می‌دهد.



در ادامه‌ی کار و با استخراج NTLM hash از هر دو سرور مشخص می‌شود یک نام کاربری به نام noc-monit با سطح دسترسی بالا (عضو گروه administrators محلی) بین دو سرور، مشترک است و با اجرای یک حمله‌ی Brute Force چند ساعته در سیستم خود موفق به شکستن آن رمز عبور می‌شود. از این نقطه به بعد تنها کافی است گشتی بین سرورهای پایگاه داده بزند و با استفاده از دستور زیر از پایگاه داده‌های موردنظر خود یک نسخه‌ی پشتیبان تهیه کند:

```
USE Targetdb;
GO
BACKUP DATABASE Targetdb
TO DISK = 'Z:\SQLServerBackups\ Targetdb.Bak'
  WITH FORMAT,
    MEDIANAME = 'Z_SQLServerBackups',
    NAME = 'Full Backup of Targetdb';
GO
```

نفوذگر سیاه در آخرین مرحله، با استفاده از پروتکل FTP فایل‌های پشتیبان تهیه شده از پایگاه‌های داده را به سرورهای خود منتقل می‌کند. از این لحظه به بعد، کار او در شبکه‌ی قربانی تمام شده است.
فعالیت‌های بعدی در شبکه‌ی قربانی می‌تواند براساس اهداف آینده‌ی نفوذگر سیاه مشخص شود. برای نمونه، شب می‌تواند تمام سرورهای پایگاه داده و سرویس‌های وب موجود در سازمان را از کار بیاندازد و اطلاعات موجود روی آن‌ها را پاک کند تا سازمان در ارایه‌ی خدمات آنلاین به کاربران خود دچار اختلالات جدی شود؛ یا به‌منظور حفظ دسترسی خود برای آینده در شبکه‌ی سازمان هدف یک یا چند backdoor در سامانه‌ها نصب کند و بدون سروصدا از شبکه خارج شود.



چگونه با استفاده از یک SIEM با پیکربندی درست می‌توانستیم این نفوذ را به‌موقع شناسایی کنیم؟

در واقع سناریوی شرح داده شده در بخش قبل، ترکیبی از چند حمله و روش‌های گفته شده توسط نفوذگران در برنامه‌های باگ‌بانتی hackerone.com و کنفرانس‌های امنیتی معتبر است. اکنون که داستان نفوذ انجام شده را می‌دانیم به‌راحتی می‌توان قواعدی را برای شناسایی این مهاجمان با استفاده از سامانه‌ی SIEM تعریف کرد.
فرض کنید با بررسی انواع سناریوهای حملات سایبری که متخصصان امنیت در کنفرانس‌های امنیت و نفوذ برگزار شده در سراسر دنیا، ارایه داده‌اند، تا چه اندازه می‌توان قابلیت شناسایی نفوذگران در شبکه‌های سازمان را (با پیکربندی مجدد SIEM) افزایش داد؟
از سوی دیگر، کارشناسان امنیت و واحد SOC سازمان‌ها پس از آشنا شدن با این سناریوها و با بهره‌گیری از دانش امنیت قبلی خود می‌توانند اقدامات مناسب‌تری را در راستای مقابله با حملات مشابه طراحی و اجرا کنند.
برخی از موارد امنیتی که با استفاده از آن‌ها می‌توان نفوذگر شبیه‌سازی‌شده در بخش قبل را شناسایی یا با آن مقابله کرد به شرح زیر است:

- شناسایی پورت اسکن انجام شده و افزایش حساسیت روی نشانی مبدا این اسکن‌ها توسط SIEM.
- شناسایی تست نفوذهای انجام شده روی سرویس‌های تحت وب سازمان و اعلام هشدار به کارشناسان توسط سامانه‌ی SIEM.
- اختصاص اهمیت یک‌سان به امنیت تمام سرویس‌های سازمان (به‌ویژه سرویس‌هایی که از اینترنت دردسترس هستند).
- بررسی پیکربندی سرویس‌های تحت وب به‌منظور این‌که با سطح دسترسی بسیار بالا در سیستم‌عامل (مانند Admin یا System) اجرا نشوند.
- عدم استفاده از حساب‌های کاربری پایگاه داده با سطح دسترسی بالا (مانند sa) برای ارتباط سرویس‌های وب، هم‌چنین عدم ذخیره‌ی آن‌ها در فایل‌های پیکربندی.
- به‌روزرسانی خودکار تمام سیستم‌عامل‌ها (به‌ویژه سرویس‌هایی که از اینترنت دردسترس هستند).
- آگاهی از سرویس‌های تحت وب و سایر سرویس‌های سازمان که امکان اجرای دستور روی سیستم‌عامل را دارند و اعمال تدابیر امنیتی در این زمینه.
- عدم استفاده از یک نام کاربری مشابه در تعداد بالایی از سرورها (به‌ویژه با دسترسی سطح بالا).
- اعمال مانیتورینگ روی احراز هویت‌های موفق و ناموفق در سازمان به‌منظور شناسایی رفتارهای غیرعادی و مشکوک در SIEM (در نمونه‌ی بخش قبل، تعداد بالایی احراز هویت موفق با یک نام کاربری در یک بازه‌ی زمانی به نسبت کوتاه رخ داد).
- بستن تمام پروتکل‌های غیرضروری (مانند FTP) از داخل شبکه به‌سمت اینترنت روی فایروال‌های سازمان
- اهمیت دادن به امنیت تمام سرویس‌ها و سامانه‌ها، جدا از سطح اهمیت آن‌ها برای کسب‌وکار سازمان، زیرا در این حالت سامانه‌های ناامن موجود در شبکه‌ی سازمان، امنیت سامانه‌های امن‌سازی شده را نیز مورد تهدید قرار خواهند داد.

جمع‌بندی و کارهای آینده

در این مقاله به بررسی اجمالی وضعیت حملات سایبری در سطح دنیا و ایران پرداخته شد و با توجه موارد گفته شده، دیدیم که در سال‌های اخیر، سازمان‌های ایران با انواع مختلفی از حملات سایبری روبه‌رو بوده‌اند. از سوی دیگر، به نظر می‌رسد کشور در به‌کارگیری راهکارهای دفاع سایبری نوین و به‌ویژه تربیت متخصصان سایبری، عملکرد موفقی نداشته است.

از مهم‌ترین دلایل تعداد کم متخصصان سایبری می‌توان به ناکارآمدی زیرساخت آموزش عالی کشور در این زمینه، هم‌چنین مهاجرت متخصصان به کشورهای غربی اشاره کرد.

اگر برنامه‌ای برای تربیت تعداد بیش‌تر این متخصصان نداشته باشیم، این امر با توجه به گسترش حملات سایبری در دنیا، می‌تواند در آینده‌ی نزدیک مشکلات جبران‌ناپذیری را برای کشور به‌همراه داشته باشد.

با توجه به موارد گفته شده، تصمیم گرفتیم تا در حد توان خود نسبت به تولید محتوای با کیفیت در زمینه‌ی امنیت تهاجمی اقدام کنیم. در نخستین مقاله به بررسی روش‌های متداول نفوذ به شبکه‌های سازمان‌ها و یک سناریوی به نسبت ساده‌ی نفوذ به شبکه پرداخته شد. در مقاله‌های بعدی با توجه به بازخورد دریافت شده از سوی شما مخاطبان، موضوعات دیگری در زمینه‌های امنیت تهاجمی و بهبود مراکز SOC پوشش داده خواهد شد.

برخی از این موضوعات عبارت‌اند از:

۱.شرح خدمات تیم‌های قرمز و مقایسه‌ی آن با خدمات ارزیابی آسیب‌پذیری و تست نفوذ

۲.حملات مبتنی‌بر مهندسی اجتماعی: پیش و پس از اجرای حمله

۳.حملات مبتنی‌بر سرویس‌های تحت وب: پیش و پس از اجرای حمله

۴.آیا می‌توان با نفوذهای مبتنی‌بر اکسپلویت‌های zero-day مقابله کرد؟

همان‌گونه که گفته شد، ممکن است با توجه به بازخورد مخاطبان پس از انتشار هر مقاله، موضوعات گفته شده تغییر کند یا موضوعات جدیدی به آن‌ها اضافه شود.

مراجع

[1] https://nahamsec.com/secure-your-jenkins-instance-or-hackers-will-force-you-to/
[2] https://docs.telerik.com/devtools/justmock/continuous-integration/jenkins-ci
[3] https://docs.microsoft.com/en-us/sql/relational-databases/ sytem-stored-procedures/xp-cmdshell-transact-sql?view=sql-server2017-
[4] https://github.com/michenriksen/aquatone
[5] https://fas.org/sgp/crs/row/IN10376.pdf
[6] https://goo.gl/Y2qwWn


arvan
cloud.com
ابر آروان


سازمان پدافند غیرعامل کشور


مرکز ماهر
مرکز مدیریت امداد و هماهنگی عملیات خدادهای رایانه‌ای


مرکز سمتا