مرکز تخصصی آپا
دانشگاه صنعتی اصفهان

امنیت فضای سایبری
سال ۹۸

مروری بر وضعیت امنیت سایبری ایران و جهان
سال ۱۳۹۸

گزارش سالانه

مروری بر وضعیت امنیت سایبری ایران و جهان سال ۱۳۹۸

مرکز تخصصی آپا دانشگاه صنعتی اصفهان

بهار ۱۳۹۹

۱ مقدمه

در عصر اطلاعات و با گره خوردن زندگی به دنیای دیجیتال، رخدادهای سایبری دیگر اخباری مخصوص به متخصصان و کارشناسان این حوزه نیست و در زندگی همه افراد جامعه موثر است. اخبار سایبری را امروزه نه تنها در وب‌سایت‌ها و خبرگزاری‌های تخصصی، بلکه در خبرگزاری‌های عمومی هم می‌توان یافت.

در سال گذشته شاهد رخدادهای فراوانی در حوزه سایبری بودیم. رخدادهایی که گاه به کوچکی یک خسارت سایبری به یک سازمان بوده و گاهی تا سطح روابط بین‌المللی کشورها بزرگ بوده است. از حملات باج‌افزاری به سازمان‌های دولتی و شرکت‌ها گرفته تا حملات هدف‌مند به زیرساخت‌های دولتی کشورها و جاسوسی‌های مختلف.

رخدادهای سایبری گاه به کوچکی خسارت به یک سازمان بوده و گاه تا حد تنش بین‌المللی بین کشورها بزرگ بوده‌اند.

در این گزارش سعی نموده‌ایم با مروری بر رخدادهای مهم امنیت سایبری در سال گذشته و بررسی آماری آن‌ها، چشم‌اندازی از فضای سایبری ایران و جهان در سال گذشته بسازیم. امیدواریم این چشم‌انداز بتواند توجه علاقه‌مندان، کارشناسان و مدیران این حوزه را جلب نموده و در تصمیم‌گیری‌های آینده آن‌ها مفید باشد.

این گزارش در شش فصل تهیه شده است. در فصل دوم گزارش به باج‌افزارها به عنوان داستان امسال می‌پردازیم. باج‌افزارها که در دو سال اخیر پس از رشد استخراج‌کننده‌های رمزارز رتبه اولین بدافزارها را از دست داده بودند، با تغییر استراتژی باز هم توانستند در صدر اخبار سال گذشته قرار گیرند. در این فصل به حملات هدف‌مند این بدافزارها و افشای اطلاعات قربانیان پرداخته‌ایم.

در فصل سوم روند بدافزارها در سال گذشته را بررسی کرده و مروری بر تهدیدات بدافزاری سیستم‌عامل‌های ویندوز، اندروید و مک انجام داده و به حملات مطرح وب در سال گذشته پرداخته‌ایم.

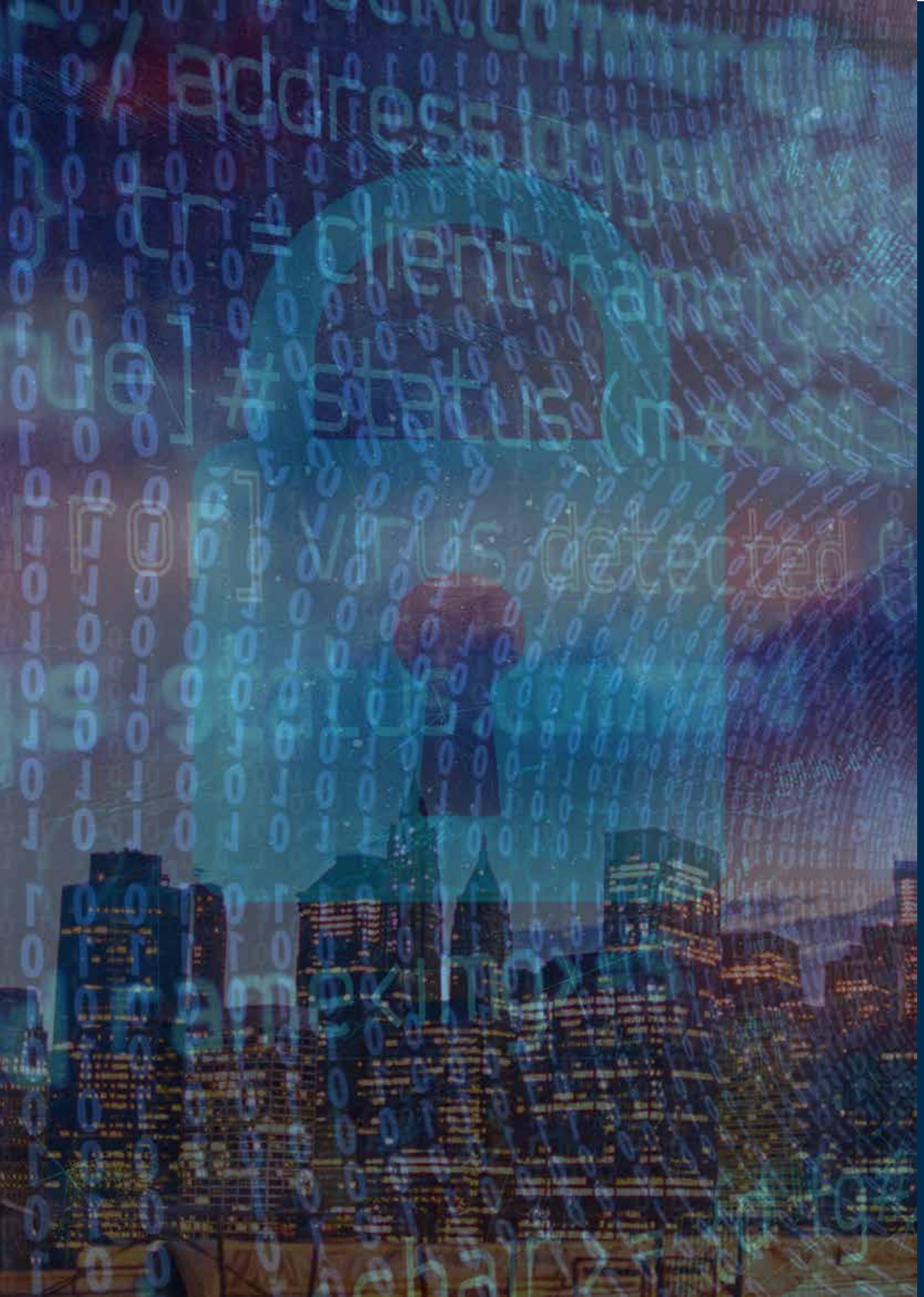
در فصل چهارم آسیب‌پذیری‌های سال گذشته و آمار آن‌ها را بر اساس سطح خطر، محصولات آسیب‌پذیر و بسیاری از ویژگی‌های دیگر بررسی نموده‌ایم.

فصل پنجم را به مرور اخبار مهم امنیتی در جهان در سال ۹۸ اختصاص داده‌ایم.

در فصل ششم به وضعیت سایبری کشور در سال گذشته پرداخته‌ایم. در ابتدا مسایل مهم حوزه امنیت در سال گذشته مرور کرده و سپس آماری از آلودگی‌ها و آسیب‌پذیری‌های کشور ارائه نموده‌ایم.

در فصل هفتم نیز پس از پیش‌بینی تهدیدات سال جدید، توصیه‌هایی برای افزایش امنیت و مقابله با تهدیدات سایبری را مطرح کرده‌ایم.

فهرست



۲

داستان سال: سازمان‌ها در تسخیر باج‌افزارها

باج‌افزارها با تغییر استراتژی حملات خود در سال گذشته باز هم به تیتر اول اخبار سایبری رفتند

۲ داستان سال: سازمان‌ها در تسخیر باج‌افزارها

سال‌ها است که باج‌افزارها، کاربران نهایی و سیستم‌های خصوصی را هدف قرار می‌دهند. اما به نظر می‌رسد که چپاول کاربران عادی برای مجرمین سایبری دیگر کافی نیست. آن‌ها اکنون، چشم طمع به قربانیان بزرگ‌تر و البته ثروتمندتری دارند. باج‌افزارها، بدافزارهای بسیار خطرناکی هستند که در بسیاری از موارد خسارت‌های آن‌ها برای قربانی جبران‌ناپذیر است. در یکی دو سال اخیر، کاربران ایرانی همچون بسیاری از کاربران سراسر جهان، بیش از همیشه آلوده به باج‌افزارها شده‌اند. از این رو در این بخش به طور ویژه به بررسی عملکرد این دسته از بدافزارها پرداخته‌ایم و پیشنهادهایی برای در امان ماندن از آن‌ها ارائه می‌کنیم.

آمار سال‌های گذشته شرکت کسپراسکی نشان می‌دهد که سهم باج‌افزارها، نسبت به تعداد بدافزارهای کشف‌شده از ۲٫۸ درصد به ۳٫۵ درصد رسیده است و رشد حدوداً یک درصدی داشته است. با توجه به اینکه باج‌افزارها خسارت‌های زیادی برای سیستم‌ها دارند و موجب از بین رفتن دسترسی کاربر به اطلاعات خود می‌شوند، این افزایش درصد به ظاهر ناچیز هم اهمیت دارد و نباید دست کم گرفته شود.

با وجود اینکه باج‌افزارها از الگوریتم‌ها و پروتکل‌های قدرتمند و پیچیده‌ای برای رمزنگاری استفاده می‌کنند، اما به طور کلی روش همگی آن‌ها ساده و یکسان است: رمز کردن اطلاعات قربانیان و درخواست باج در ازای در اختیار قرار دادن کلید رمزگشایی. متاسفانه در اکثر مواقع، تنها راه بازگردانی فایل‌ها در اختیار داشتن کلیدِ رمزگشایی فایل‌ها است و بدون کلید امکان بازگردانی فایل‌های رمزشده وجود ندارد. برخی توسعه‌دهندگان باج‌افزار، توزیع بدافزار را هم خود به عهده می‌گیرند اما برخی دیگر، توزیع آن را به گروه دیگری واگذار کرده و باج‌های دریافت شده را شریک می‌شوند. اما این روند در سال گذشته چهره متفاوتی به خود گرفت. تمرکز باج‌افزارها به سمت یک هدف جدید تغییر کرد: ادارات شهری و سازمان‌های دولتی! حمله به شهرداری بالتیمور، یکی از شهرهای ایالت مریلند امریکا، یکی از اولین حملات گسترده باج‌افزاری بود که سازمان‌های مهم شهری را هدف قرار داده بود و بسیاری از سرویس‌ها را از کار انداخت. هکرها برای بازگردانی اطلاعات، ده‌ها میلیون دلار باج تقاضا کردند! طبق آمار کسپراسکی در طول سال گذشته لااقل ۱۷۴ اداره و سازمان شهری و دولتی مورد حمله باج‌افزاری قرار گرفتند. این آمار به معنای رشد ۶۰ درصدی حملات باج‌افزاری به ادارات شهری و سازمان‌ها در سال گذشته بوده است. با اینکه مقدار باج‌های درخواست‌شده در برخی از این حملات دقیقاً مشخص نیست، اما در بازه‌ای بین ۵ هزار تا ۵ میلیون دلار است و میانگین آن‌ها به بیش از یک میلیون دلار می‌رسد. البته مقدار باج با توجه به اینکه اداره یا سازمان چقدر بزرگ بوده، متغیر بوده است. البته به چند دلیل خسارت سازمان‌ها با مبالغ خواسته‌شده متفاوت است. اول اینکه برخی از سازمان‌ها و شرکت‌ها از بیمه تهدیدات سایبری برخوردار بودند و توانستند هزینه خسارت را از بیمه دریافت کنند. برخی دیگر با رسیدگی به حادثه توانستند حمله را خنثی کنند و بدون پرداخت باج، اثرات منفی حمله را دفع کنند. سازمان‌های دیگری مانند شهرداری بالتیمور امریکا، تسلیم نشدند و به جای پرداخت باج با صرف هزینه‌ای بیشتر، شبکه خود را بازیابی کردند. اگرچه پرداخت باج، هزینه‌ای کمتری به آن‌ها متحمل می‌کرد اما هزینهٔ امن‌سازی شبکه‌ها و سیستم‌ها را نباید با میزان باج درخواستی مقایسه کرد. همچنین باید در نظر داشت وقتی اداره و یا سازمانی مورد حمله باج‌افزاری قرار می‌گیرد بررسی حمله، ارزیابی شبکه و سیستم‌ها و امن‌سازی آن‌ها، فعالیت‌های بسیار ضروری برای سازمان هستند که انجام آن‌ها، هزینهٔ ثانویه‌ای برای سازمان است.

سناریوهای این حملات باج‌افزاری مختلف بوده است، ولی تقریباً همه این حملات از دو نکته کلیدی استفاده می‌کردند: مهندسی اجتماعی و سوءاستفاده از ضعف‌های امنیتی سیستم‌ها و نرم‌افزارهای به‌روز نشده!

جالب است بدانید که هنوز یک‌پنجم آلودگی‌های باج‌افزاری از طریق سوءاستفاده از همان آسیب‌پذیری انجام می‌گیرد که واناکرای از آن بهره می‌برد و شرکت مایکروسافت دو سال و نیم پیش برای آن وصله منتشر نموده است! یکی دیگر از روش‌های حمله، آلوده کردن کارکنان سازمان و به تبع آن، آلوده کردن خود سازمان است. از آنجایی که آموزش‌های امنیتی کارکنان سازمان‌ها هنوز جدی گرفته نمی‌شود، شرکت‌ها و سازمان‌ها ضربه‌های سنگینی از عدم آموزش امنیتی کارکنان سازمان خود می‌خورند. در میان سازمان‌ها و اداراتی که در سال گذشته مورد حملات باج‌افزاری قرار گرفتند، مدارس و دانشگاه‌ها قربانیان بیشتری داشته است. به گزارش شرکت کسپراسکی، ۶۱ درصد حملات علیه مدارس و دانشگاه‌ها بوده است. شهرداری‌ها و ادارات خدمات شهری نیز ۲۹ درصد از قربانیان این حملات بوده‌اند. در رتبه سوم نیز بیمارستان‌ها با ۷ درصد قرار دارند.

هکرها با حمله به مراکز شهری و سازمان‌ها به دنبال باج‌های میلیون دلاری هستند.

باج‌افزارها به دنبال سازمان‌ها

حال ببینیم کدامیک از باج‌افزارها بیشترین فعالیت و تمرکز را روی این اهداف جدید داشته‌اند: همه سازمان‌ها و شرکت‌هایی که مورد حمله باج‌افزاری قرار گرفتند جزئیات فنی حمله را منتشر نکرده‌اند، اما باج‌افزار Ryuk، یکی از فعال‌ترین باج‌افزارها با اهداف سازمانی و دولتی است که فعالیت خود را از نیمه دوم سال ۲۰۱۸ شروع کرده است. Ryuk قربانیان خود را در سراسر دنیا هدف قرار داده؛ با این حال ۸٫۶ درصد اهداف آن از آلمان، ۸ درصد از چین و ایران با ۵ درصد در رتبه ششم قربانیان این باج‌افزار بوده است.

باج‌افزار Ryuk معمولاً به صورت مستقیم قربانیان خود را آلوده نمی‌کند و به صورت چند مرحله‌ای حملات خود را اجرا می‌کند. در مرحله اول، بات‌نت اموتت (Emotet) از طریق هرزنامه به سیستم قربانیان می‌رسد و پس از آلوده کردن سیستم قربانی، باج‌افزار را دانلود و سیستم را آلوده می‌کند. یکی از ویژگی‌های جالب Ryuk که آن را خطرناک‌تر می‌کند این است که این باج‌افزار سیستم‌هایی که در حالت خواب هستند را به صورت خودکار روشن کرده و اطلاعات آن‌ها را رمز می‌کند. از دیگر ویژگی‌های Ryuk که آن را تبدیل به یک باج‌افزار خطرناک می‌کند، تزریق کد به پردازش‌های قانونی سیستم برای جلوگیری از شناسایی، متوقف کردن برنامه‌های تجاری به منظور رمز کردن موفق فایل‌های مربوط به آن‌ها و متوقف کردن مکانیزم‌های امنیتی سیستم است.

خانواده باج‌افزاری دیگری که از ۲۰۱۶ فعال شده، Scarab است. این باج‌افزار همچنان در حال توسعه و قربانی گرفتن از سراسر جهان است. باج‌افزار Scarab نیز برای حمله به سازمان‌ها و اداره‌ها استفاده می‌شود. البته این باج‌افزار علاوه بر سازمان‌ها و اداره‌ها به کاربران شخصی نیز حمله می‌کند. این باج‌افزار با نام‌های Purga و Amnesia نیز شناخته می‌شود. توسعه‌دهندگان این باج‌افزار به صورت عمده از کمپین‌های هرزنامه‌ای و حملات جستجوی کامل روی پروتکل RDP برای توزیع این بدافزار استفاده می‌کنند. این باج‌افزار به دقت طراحی شده و تاکنون چند بار الگوریتم رمزنگاری و نحوه تولید کلید خود را تغییر داده است. باج‌افزار دیگری که فعالیت زیادی در حمله به سازمان‌ها و شرکت‌ها داشته، باج‌افزار STOP است که با نام STOP

Djvu نیز شناخته می‌شود. این باج‌افزار که در اواخر سال ۲۰۱۸ برای اولین بار مشاهده شد، در سال اخیر فعالیت زیادی داشته و بر اساس آمار کسپراسکی بیش از ۲۰ هزار قربانی در سراسر جهان داشته است. این باج‌افزار در کشور ما نیز فعالیت زیادی داشته و درصد زیادی از آلودگی‌ها به باج‌افزار را به خود اختصاص داده است. این باج‌افزار از الگوریتم‌های Salsa20 و RSA برای تولید و تبادل و ذخیره کلید استفاده می‌کند. این کلیدها بسته به وضعیت در دسترس بودن یا نبودن سرور کنترل و فرمان باج‌افزار می‌توانند آفلاین و یا آنلاین تولید شوند. کلید آفلاین باج‌افزار ممکن است روی سیستم قربانی یافت شود.

باج‌افزارها سارقان جدید اطلاعات

حمله به سازمان‌ها و ادارات دولتی تنها تغییر استراتژی باج‌افزارها در سال گذشته نبوده و برخی از آن‌ها قبل از رمزگذاری فایل‌ها اقدام به سرقت فایل‌های قربانیان می‌نمایند. از اطلاعات سرقت شده به منظور تحت فشار قرار دادن قربانیان برای پرداخت باج و تهدید به افشای این اطلاعات استفاده می‌شود. باج‌افزارهای Sodinokibi و Maze از پیشگامان این روند بودند. باج‌افزار Maze پس از اینکه پاسخی در مقابل درخواست باج یک میلیون دلاری از یک سازمان دولتی نگرفت، اطلاعات آن‌ها را روی اینترنت منتشر نمود.

پس از Maze و Sodinokibi باج‌افزارهای دیگری همچون Nemty نیز این راه را در پیش گرفتند. با افزایش این رفتار جدید باج‌افزارها، اکنون باید هر حمله باج‌افزاری را یک نشت داده نیز در نظر گرفت. به نظر می‌رسد در سال پیش رو باج‌افزارهای بیشتری از این روش برای تحت فشار گذاشتن قربانیان خود برای دریافت باج استفاده نمایند. از این رو این دسته از بدافزارهای پر سر و صدای چند سال گذشته احتمالاً امسال با سرقت داده در کنار حملات هدف‌مند، خطرناک‌تر شده و ضربات مهلک‌تری به قربانیان خود وارد می‌نمایند.

نتیجه‌گیری و پیشنهاد

امسال سال حملات باج‌افزاری به ادارات و سازمانهای دولتی بود و احتمالاً این روند در سال پیش رو نیز مشاهده خواهد شد. به دلایل مختلف این نوع حملات باج‌افزاری در حال افزایش هستند.

۱. در بسیاری از کشورها تمرکز شرکت‌ها و سازمان‌های دولتی به‌جای انجام امن‌سازی و اجرای ارزیابی‌های امنیتی، به گرفتن خسارت از بیمه است. به عبارت دیگر، سازمان‌ها در حال حاضر به جای ارتقای امنیت خود، باج را به مجرمین پرداخت می‌کنند به این امید که بیمه خسارت آن‌ها را پرداخت کند. این امر حملات باج‌افزاری را به شدت ترویج می‌کند.

۲. سازمان‌ها و ادارات شهری و دولتی معمولاً شبکه بزرگی شامل چند نهاد مختلف هستند که حمله به آن‌ها می‌تواند موجب توزیع آلودگی در چند نهاد به صورت همزمان شود و خسارت زیادی به بار آورد. آسیب بالای چنین مجموعه بزرگی،دریافت باج را برای صاحبان باج‌افزارها ساده می‌نماید.

۳. داده‌هایی که در شبکه‌های سازمانی و ادارات شهری وجود دارد، داده‌های حیاتی و مهمی است که برای کارهای روزمره شهری و کشوری به آن‌ها نیاز است و می‌تواند تاثیر مستقیمی روی زندگی شهروندان مرتبط با آن سازمان داشته باشد. از این رو حساسیت عمومی روی آن‌ها وجود داشته و موجب می‌شود احتمال پرداخت باج برای پس گرفتن این اطلاعات بالا رود.

اکنون هر حمله باج‌افزاری را یک نشت داده نیز باید در نظر گرفت.

با این حال با رعایت مواردی می‌توان به اپیدمی حملات باج‌افزاری به سازمان‌ها و شرکت‌ها، پایان داد:

- لازم و ضروری است که به‌روزرسانی‌های امنیتی به محض انتشار روی همه سیستم‌های سازمان نصب شوند. بسیاری از حملات سایبری از آسیب‌پذیری‌هایی استفاده می‌کنند که پیش از این، وصله برای آن‌ها منتشر شده است. بنابراین نصب وصله‌های رفع این آسیب‌پذیری‌ها می‌تواند در مقابل این حملات، سازمان را مقاوم نماید.
- دسترسی‌های از راه دور به شبکه سازمان باید تنها با وی‌پی‌ان و استفاده از کلمات عبور امن برای حساب‌های دامنه باشد.
- لازم است یک برنامه پشتیبان گیری منظم و به‌روز تهیه شود تا اگر به هر دلیلی، اطلاعات از دست رفت (حملات بدافزاری یا مشکلات سخت‌افزاری) بتوان اطلاعات را بازگردانی کرد. علاوه بر ذخیره پشتیبان روی حافظه‌های فیزیکی، می‌توان برای امنیت بیشتر آن را روی بستر ابری امنی نیز ذخیره کرد.
- به یاد داشته باشید که فعالیت باج‌افزارها یک فعالیت مجرمانه است. پس شما نباید به مجرمین باج پرداخت کنید! اگر قربانی حملات باج‌افزاری شدید به سازمان‌های مرتبط با رسیدگی به این حوادث گزارش دهید. به یاد داشته باشید که برخی اوقات پرداخت باج، تنها راه بازگردانی اطلاعات نیست!
- به کارمندان خود اصول اولیه امنیت سایبری را آموزش دهید. کاربران آموزش‌ندیده می‌توانند تهدیدات بزرگی برای سازمان باشند و کاربران آموزش‌دیده می‌توانند حملات را در گام اول متوقف و یا لااقل تشخیص دهند.
- مکانیزم‌های امنیتی برای مقابله با باج‌افزارها تدارک ببینید. ضدویروس‌های قدرتمند، ضدباج‌افزارها و سایر مکانیزم‌های امنیتی می‌توانند امنیت شما را در مقابل این حملات بالا ببرند.

۳

بدافزارها

نگاهی بر رخدادهای دنیای بدافزارها در سال گذشته

۳ بدافزارها

۱.۳ مقدمه

بدافزارها در سال ۹۸ حامل یک پیام روشن برای ما بودند: مجرمین سایبری اکنون بیش از هر چیزی، خواهان قربانی کردن سازمان‌ها هستند. گواه این مطلب، خبرهایی است که از سراسر دنیا در مورد درگیر شدن سازمان‌های مهم به بدافزارهای خطرناک و به ویژه نوع خاص آن، باج‌افزارها در سال اخیر منتشر شده است. البته این به این معنا نیست که مجرمین سایبری از قربانیان همیشگی خود یعنی کاربران شخصی دست کشیده باشند.

نکتهٔ دیگری که با بررسی فعالیت بدافزارها در سال اخیر مشاهده کردیم، فعالیت گسترده تبلیغ‌افزارها است. تبلیغ‌افزارها، گسترده‌ترین حملات را علیه سیستم‌عامل ویندوز و مک در سال اخیر پیاده کرده‌اند و این نشان می‌دهد که این نوع بدافزارها در حال حاضر یکی از درآمدزاترین روش‌ها برای مجرمین سایبری هستند و از طرف دیگر به اندازهٔ سایر بدافزارها به دام آنتی‌ویروس‌ها و برنامه‌های امنیتی سیستم‌عامل‌ها نمی‌افتند. در این گزارش به مهم‌ترین خانواده‌های تبلیغ‌افزارها و نوع عملکرد آن‌ها اشاره می‌کنیم.

نرخ شدید افزایش تهدیدها علیه سیستم‌عامل مک، یکی دیگر از مواردی جالبی است که در این گزارش به آن پرداخته‌ایم و شاید برای شیفتگان این سیستم‌عامل قابل توجه باشد. مجرمان سایبری در سال ۹۸ هم با متنوع کردن روش‌های هک، ابداع تکنیک‌های بدیع فرار و مخفی‌کاری و بهره‌گیری از تبلیغ‌افزارهای اندرویدی تا جایی که می‌توانستند از کاربران عادی تا سازمان‌های مهم را درگیر کردند تا صنعت جرایم سایبری را بیش از پیش گسترش دهند.

در این گزارش به صورت جداگانه به بررسی مهم‌ترین و گسترده‌ترین حملات بدافزاری می‌پردازیم که در سال اخیر سیستم‌عامل ویندوز، مک، اندروید و هم چنین وب را تهدید کرده‌اند. لازم به ذکر است که به دلیل اهمیت باج‌افزارها و تهدیدات خطرناک و خسارات عمدتاً جبران‌ناپذیری که باج‌افزارها در سال اخیر برای کاربران عادی و به ویژه سازمان‌ها ایجاد کرده‌اند، این بدافزار را در بخش قبل با عنوان داستان سال بررسی کردیم.

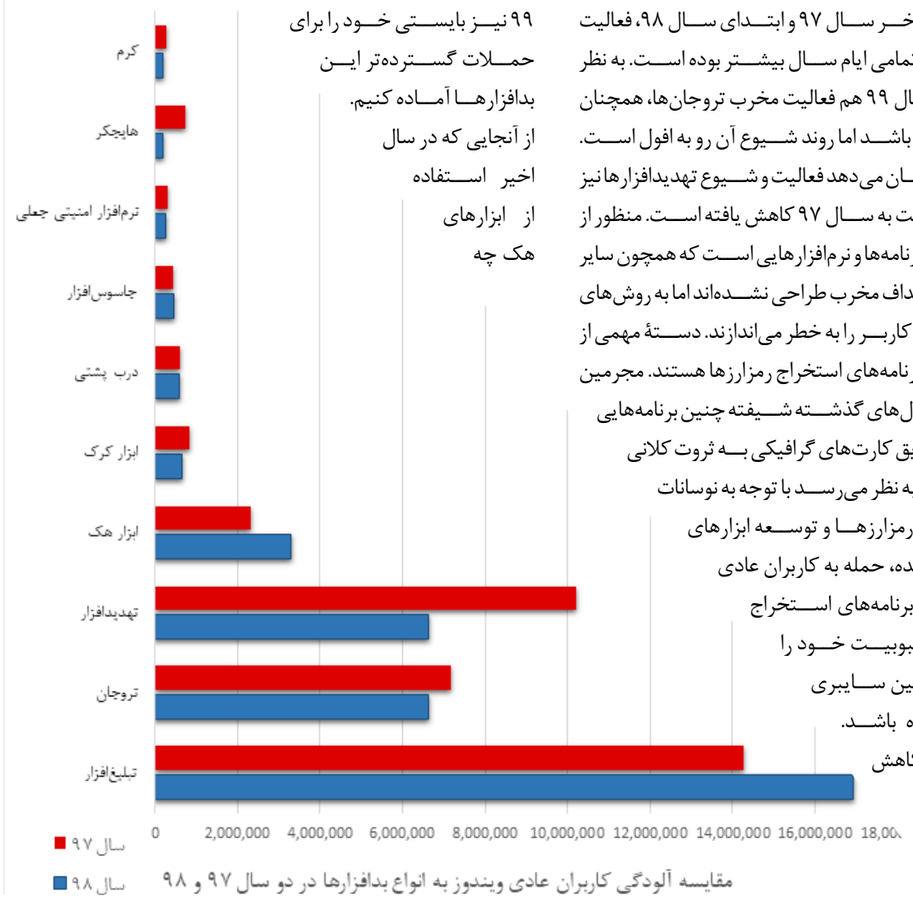
مجرمین سایبری بیش از هر چیز به دنبال قربانی کردن سازمان‌ها هستند!

۲.۳ بدافزارهای ویندوزی در سال ۹۸

گزارش‌های آماری آنتی‌ویروس‌های معتبر نشان می‌دهد که اگرچه همچنان آمار کاربران عادی ویندوزی که توسط بدافزارها آلوده می‌شوند چندین برابر سازمان‌های آلوده‌شده است اما تهدیدهای سازمانی بیش از هر زمانی رو به افزایش هستند.

بدافزارهای ویندوزی علیه کاربران عادی

با بررسی انواع بدافزارهایی که در سال ۹۸، کاربران عادی ویندوز را هدف قرار داده‌اند، مشخص شده است که تبلیغ‌افزارها بیشترین تهدید علیه کاربران عادی بوده‌اند. شیوع آن‌ها در کل سال تقریباً به صورت یکنواخت بوده است. فعالیت تروجان‌ها در سال اخیر اگرچه به نسبت سال‌های گذشته کمتر شده است، اما به لطف کمپین اموتت (Emotet) همچنان دومین تهدید علیه کاربران عادی بوده است. اواخر سال ۹۷ و ابتدای سال ۹۸، فعالیت تروجان‌ها از تمامی ایام سال بیشتر بوده است. به نظر می‌رسد در سال ۹۹ هم فعالیت مخرب تروجان‌ها، همچنان دردسرآفرین باشد اما روند شیوع آن رو به افول است. بررسی‌ها نشان می‌دهد فعالیت و شیوع تهدیدافزارها نیز در سال ۹۸ نسبت به سال ۹۷ کاهش یافته است. منظور از تهدیدافزارها، برنامه‌ها و نرم‌افزارهایی است که همچون سایر بدافزارها با اهداف مخرب طراحی نشده‌اند اما به روش‌های مختلف، امنیت کاربر را به خطر می‌اندازند. دستهٔ مهمی از تهدیدافزارها، برنامه‌های استخراج رمزارزها هستند. مجرمین سایبری سال‌های گذشته شیفته چنین برنامه‌هایی بودند تا از طریق کارت‌های گرافیکی به ثروت کلانی دست یابند. اما به نظر می‌رسد با توجه به نوسانات شدید قیمت رمزارزها و توسعه ابزارهای تشخیص‌دهنده، حمله به کاربران عادی با استفاده از برنامه‌های استخراج رمزارزها، محبوبیت خود را در بین مجرمین سایبری از دست داده باشد. روند رو به کاهش نفوذ این دسته از بدافزارها علیه کاربران عادی در طول سال ۹۸ گویای این مطلب است. ابزارهای هک (Hacktool) در سال ۹۸ از لحاظ میزان شیوع و آلودگی، چهارمین تهدید علیه کاربران معمولی ویندوزی بوده‌اند. ابزارهای هک زیرمجموعه تهدیدافزارها محسوب می‌شوند، اما روند شیوع آن‌ها برخلاف سایر تهدیدافزارها در سال ۹۸ به شدت صعودی بوده است. به طور مثال آنتی‌ویروس MalwareBytes اعلام کرده است که در سال ۹۸ ابزارهای هک را ۴۲ درصد بیشتر از سال ۹۷ تشخیص داده است. قابل ذکر است که ابزارهای هک نیز همچون سایر تهدیدافزارها به قصد خرابکاری ساخته نشده‌اند، اما مهاجمین از آن‌ها برای نفوذ به سیستم قربانی، جمع‌آوری اطلاعات و آلوده کردن سیستم به سایر بدافزارها سوءاستفاده می‌کنند. روند رو به رشد ابزارهای هک در سال ۹۸ نگران کننده است و به نظر می‌رسد در سال ۹۹ نیز بایستی خود را برای حملات گسترده‌تر این بدافزارها آماده کنیم. از آنجایی که در سال اخیر استفاده از ابزارهای هک چه

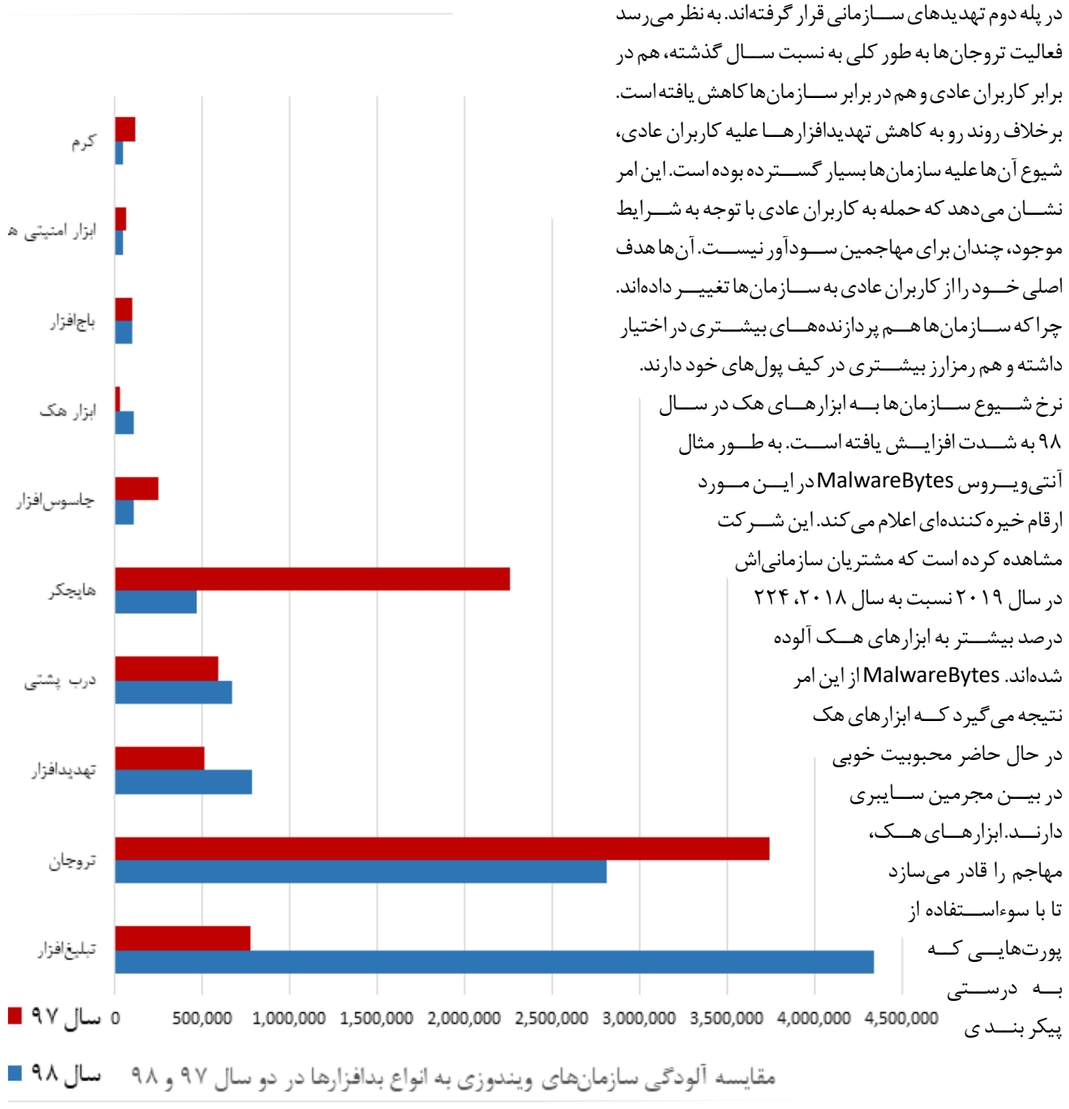


مقایسه آلودگی کاربران عادی ویندوز به انواع بدافزارها در دو سال ۹۷ و ۹۸

علیه کاربران عادی و چه علیه سازمان‌ها بسیار افزایش یافته است، مشخص است که این دسته بدافزار در حال حاضر تجارت بسیار سودآوری برای مهاجمین فراهم کرده است.

بدافزارهای ویندوزی علیه سازمان‌ها

برای سازمان‌ها نیز، تبلیغ‌افزارها اولین تهدید امنیتی هستند. البته موج گسترده فعالیت آن‌ها در اواخر سال ۹۷ و ابتدای سال ۹۸ بوده است و به نظر می‌رسد هر چه به سال ۹۹ نزدیک می‌شویم، فعالیت آن‌ها کمتر شده است. تروجان‌ها که در سال ۹۷ اولین تهدید علیه سازمان‌ها بودند، جایگاه نخست خود را از دست داده‌اند و پس از تبلیغ‌افزارها در پله دوم تهدیدهای سازمانی قرار گرفته‌اند. به نظر می‌رسد فعالیت تروجان‌ها به طور کلی به نسبت سال گذشته، هم در برابر کاربران عادی و هم در برابر سازمان‌ها کاهش یافته است. برخلاف روند رو به کاهش تهدیدافزارها علیه کاربران عادی، شیوع آن‌ها علیه سازمان‌ها بسیار گسترده بوده است. این امر نشان می‌دهد که حمله به کاربران عادی با توجه به شرایط موجود، چندان برای مهاجمین سودآور نیست. آن‌ها هدف اصلی خود را از کاربران عادی به سازمان‌ها تغییر داده‌اند. چرا که سازمان‌ها هم پردازنده‌های بیشتری در اختیار داشته و هم رمزارز بیشتری در کیف پول‌های خود دارند. نرخ شیوع سازمان‌ها به ابزارهای هک در سال ۹۸ به شدت افزایش یافته است. به طور مثال آنتی‌ویروس MalwareBytes در این مورد ارقام خیره‌کننده‌ای اعلام می‌کند. این شرکت مشاهده کرده است که مشتریان سازمانی‌اش در سال ۲۰۱۹ نسبت به سال ۲۰۱۸، ۲۲۴ درصد بیشتر به ابزارهای هک آلوده شده‌اند. MalwareBytes از این امر نتیجه می‌گیرد که ابزارهای هک در حال حاضر محبوبیت خوبی در بین مجرمین سایبری دارند. ابزارهای هک، مهاجم را قادر می‌سازد تا با سوءاستفاده از پورت‌هایی که به درستی پیکر بندی نشده‌اند و آسیب‌پذیری‌های وصله‌نشده، شبکه‌های سازمان‌ها را آلوده کنند. یکی دیگر از علت‌های افزایش شیوع ابزارهای هک این است که برخی از بدافزارهای دیگر همچون Mimikatz در عملیات خود از ابزارهای هک بهره می‌برند. در سال اخیر حجم وسیعی از بدافزارهای درب پشتی درون شبکه سازمان‌ها مشاهده شده است که یکی از مهم‌ترین خانواده‌های آن‌ها Vools بوده است. شواهد حاکی از آن است که تعداد حملات درب پشتی نسبت به سال گذشته افزایش یافته و اوج حملات درب پشتی در سال ۱۳۹۸ مربوط به ماه خرداد بوده است.



مقایسه آلودگی سازمان‌های ویندوزی به انواع بدافزارها در دو سال ۹۷ و ۹۸

۳.۳ تهدیدهای علیه وب در سال ۹۸

تجربه نشان می‌دهد که هر وب‌سایتی چه بزرگ و معروف باشد و چه کوچک و ناشناس در مقابل مجرمین سایبری آسیب‌پذیر است. در سمت کاربران نیز مرورگرها از این قاعده مستثنی نیستند. در سال ۹۸، مرورگر گوگل کروم از سایر رقبای خود یعنی موزیلا فایرفاکس و مایکروسافت اج جلو افتاده است و نه فقط کاربران بیشتر، بلکه مجرمین سایبری بیشتری هم به خود جذب کرده است. این امر سبب شده تا فعلاً این مرورگر محبوب به شدت هدف تهدیدهای امنیتی قرار بگیرد. اینترنت اکسپلورر نیز در سال ۹۸ همچنان مورد بهره‌برداری مهاجمان قرار گرفت و باعث شده دانلودهای ناخواسته و بی‌اجازه همچنان کارساز باشند.

اسکیمرهای وب

در سال ۹۸ بیشترین تهدید در حوزه وب، اسکیمرهای کارت‌های اعتباری آنلاین بوده‌اند؛ چرا که یکی از سریع‌ترین و بی‌واسطه‌ترین روش‌های کسب درآمد برای مجرمین سایبری است. اسکیمر کد مخربی است که به وبسایت‌های خرید آنلاین و صفحات پرداخت تزریق می شود و اطلاعات حساسی که قربانی تایپ می کند همچون نام، شماره کارت را رصد و ضبط می کند. مهاجم با کمک اسکیمرها، نه نیازی به آلوده کردن سیستم کاربر دارد (برخلاف تروجان‌های بانکی) و نه نیازی به فریب دادن کاربر به روش‌های مهندسی اجتماعی دارد (برخلاف حملات فیشینگ). اسکیمر در سکوت عمل می کند و مهم‌تر، آن که می‌تواند در مقابل همه دستگاه‌ها و مرورگرها، کار خود را انجام دهد. مقابله با اسکیمرهای وب نیز کار مشکلی است، چرا که از طریق اکسپلویت‌ها، ماشین را به تسخیر خود در نمی‌آورند و می‌توانند درون زیرساخت‌های فروشگاه‌های آنلاین باقی بمانند. برای مقابله با آن‌ها باید زیرساخت‌های تسخیرشده شناسایی و مسدود شوند. این در حالی است که بسیاری از اسکیمرها به صورت مجازی نامرئی هستند چرا که به کدهای سمت سرور وابسته‌اند و از سمت کاربر به سختی قابل تشخیص هستند.

کیت‌های اکسپلویت

به نظر می‌رسد در سال ۹۸، اینترنت اکسپلورر یک تنه زحمت زنده نگه داشتن دانلودهای drive-by را کشیده است. دانلودهای drive-by، دانلودهای ناخواسته‌ای هستند که بدون اجازه و یا حتی اطلاع صاحب سیستم انجام می‌شوند. به طور مثال کاربر روی یک لینک مخرب کلیک می کند و بدافزارها و برنامه‌های مخرب به دور از چشم کاربر در پس زمینه روی سیستم وی دانلود می‌شوند. پژوهشگران در سال ۱۹۸ اکسپلویت کیت‌های خلاقانه‌ای شناسایی کرده‌اند که نشان می‌دهد مهاجمان همچنان از این بدافزار دل نکنده‌اند. این اکسپلویت‌ها اگرچه از هیچ آسیب‌پذیری روزصفر می استفاده نمی کنند، اما برای پنهان شدن از جعبه شنی و توزیع پیلودهای خود، روش‌های جدید و هوشمندانه‌ای دارند. فعال‌ترین اکسپلویت کیت‌های سال ۹۸، Spelevo، Fallout و RIG بوده‌اند که به عنوان سارق اطلاعات، باج‌افزار و سایر بدافزارها فعالیت کرده‌اند. یکی از اکسپلویت کیت‌های پیشرفته‌ای که در سال ۹۸ توجه پژوهشگران امنیتی را به خود جلب کرد، Underminer است که پیلود و ترفندهای منحصر به فردی دارد. از جمله این که از روش‌های پنهان‌نگاری برای فریب دادن پژوهشگران استفاده کرده است.

کمپین‌های مخرب و لینک‌های تغییر مسیر

یکی از عادت‌های مهاجمین ایجاد کمپین‌های مخرب است تا از هیچ تلاشی برای آلوده کردن کاربران فروگذار نکرده باشند. مهم‌ترین فعالیت مهاجمین نیز در این کمپین‌ها، توزیع به‌روزرسانی‌های جعلی نرم‌افزارهای پرکاربرد و محبوب کاربران است. قفل کننده‌های صفحه، یکی از این روش‌ها است. قفل کننده‌های صفحه، بدافزارهایی هستند که صفحه مرورگر را قفل می کنند و به کاربر پیغام‌هایی جعلی نشان می‌دهند. در این پیغام‌ها به کاربر گفته می‌شود که سیستم وی آلوده است و ترافیک ارسالی وی مسدود شده است یا یکی از نرم‌افزارهای سیستم کاربر منقضی شده است و باید آن را به روز کند. این پیغام‌ها در نهایت کاربر را به یک صفحه جعلی هدایت می کنند. به نظر می‌رسد گوگل کروم، بیشترین هدف این نوع بدافزارها باشد ولی در موزیلا فایرفاکس نیز مواردی از این نوع کلاه‌برداری دیده شده است.

۴.۳ بدافزارهای اندرویدی

کاربران ایرانی چند سالی است که رتبه اول آلودگی‌های بدافزاری دستگاه‌های موبایل را در جهان دارند. کسپراسکی گزارش داده است که کاربران ایرانی‌اش بیش از هر کشور دیگری در سال اخیر گرفتار تبلیغ‌افزارها و به ویژه نوع AdWare.AndroidOS.Agent.fa بوده‌اند. کسپراسکی پس از این تبلیغ‌افزار، تروجان Trojan.AndroidOS.Hiddapp.bn و تهدیدافزار RiskTool.AndroidOS.Dnotua.yfe را به عنوان شایع‌ترین بدافزارهای اندرویدی سال اخیر در کشورمان معرفی کرده است. قابل ذکر است پس از کشور ایران به ترتیب پاکستان، بنگلادش، الجزایر و هندوستان در صدر بیشترین آلودگی به بدافزارهای موبایل هستند. وقایع غیرمنتظره‌ای که در رابطه با برنامهٔ محبوب CamScanner در گوگل‌پلی رخ داد، یکی دیگر از خبرهای مهم سال اخیر در رابطه با بدافزارهای اندرویدی است. در نسخهٔ جدید این برنامه، کتابخانه‌ای وجود داشت که محتوی یک تروجان بود. این امر به شدت به شهرت این برنامه پر مخاطب ضربه زد.

بدافزارهای از پیش نصب شده و کارخانه‌ای

شاید به نظرتان عجیب و تا حدودی مضحک برسد که گوشی تلفن همراه در همان زمان ساخت در کارخانه آلوده به بدافزار باشد. اما متاسفانه این امر واقعیت دارد. در دی‌ماه سال ۹۸ آزمایشگاه امنیتی MalwareBytes خبری در مورد گوشی‌های اندرویدی ساخت کشور چین منتشر کرد که در زمان ساخت، آلوده به نرم‌افزار مخرب ادوپس (Adups) شده‌اند. این نرم افزار به عنوان یک نصب‌کننده خودکار وظیفه به‌روزرسانی سفت‌افزار را دارد، ولی هم زمان اطلاعات شخصی کاربران را هم سرقت می‌کند. جالب این جاست که بدانید این اولین باری نیست که این شرکت چینی اقدام به چنین کاری می‌کند. در سال ۹۵ نیز در مورد ادوپس و فعالیت مجرمانه آن به این شرکت اخطار داده شده بود.

جاسوس‌افزارها، نوعی از تهدیدهای اندرویدی

در سال ۹۸ بیش از صد جاسوس‌افزار جدید اندرویدی کشف شده است که نشان می‌دهد باید بیش از گذشته مراقب این نوع بدافزار خطرناک بود. جاسوس‌افزارها اطلاعات شخص را بدون اطلاع وی جمع‌آوری می‌کنند. موقعیت مکانی، عکس، ایمیل، پیامک، فهرست تماس‌ها و مخاطبین از جمله اطلاعاتی هستند که جاسوس‌افزارها جمع‌آوری می‌کنند. برخی از جاسوس‌افزارها هیچ آیکونی ندارند و حتی ممکن است از راه دور کنترل شوند و میکروفن و دوربین گوشی قربانی را بدون هیچ علامتی در صفحه روشن و فعال کنند. متاسفانه برخی از این جاسوس‌افزارها حتی در گوگل‌پلی و آی‌تونز هم حضور دارند.

۵.۳ بدافزارهای مک

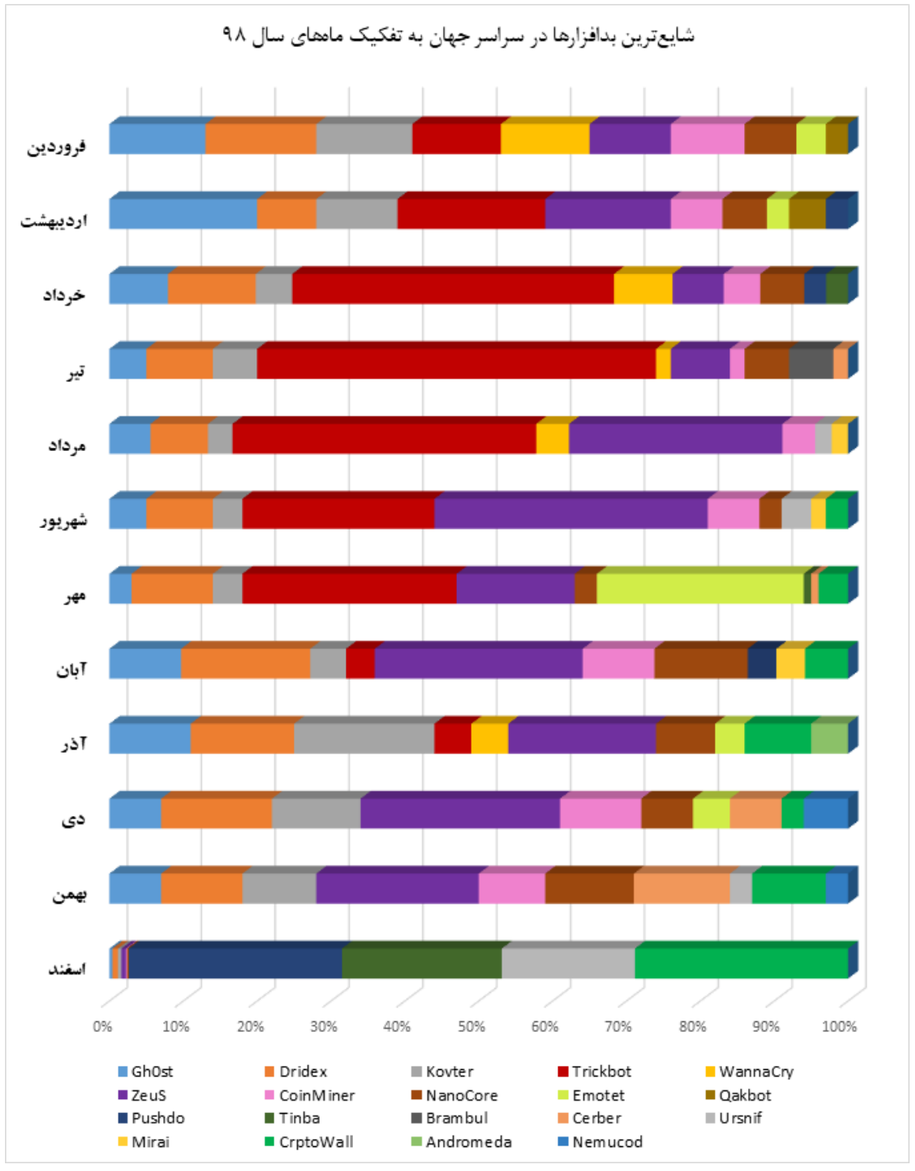
در سال ۹۸ به نظر می‌رسد مجرمین سایبری به شدت به سیستم‌عامل مک علاقه‌مند شده‌اند. نرخ چند برابر شدهٔ تهدیدهای امنیتی علیه این سیستم‌عامل گویای این مطلب است. این افزایش به قدری شدید بوده است که در سال اخیر و در سطح جهانی، کاربران مک بیشتر از کاربران ویندوزی در معرض تهدیدهای امنیتی بوده‌اند! البته نکته مهم این است که عمدهٔ تهدیدهای امنیتی علیه مک، تبلیغ‌افزارها و PUP ها (برنامه‌های که به صورت بالقوه ناخواسته‌اند) بوده‌اند که به نسبت سایر بدافزارها، چندان تخریبگر نیستند و بیشتر ایجاد مزاحمت برای کاربر می‌کنند. کارشناسان یکی از دلایل این امر را عملکرد سیستم‌های امنیتی macOS می‌دانند. چرا که این سیستم‌ها به اندازه‌ای که در برابر سایر بدافزارها حساس هستند در برابر تبلیغ‌افزارها و PUPها حساس نیستند. از میان بدافزارهای مطرح مک، همگی یا از نوع تبلیغ‌افزار و یا از نوع PUPها هستند. بدافزارهای PUP شناخته‌شده بیشتر برنامه‌های پاک‌کننده هستند.

بدافزار نیوتب

در صدر این لیست بدافزار نیوتب (NewTab) قرار گرفته است که از نوع تبلیغ‌افزار شناخته شده است. این بدافزار بیشتر از طریق صفحات رهگیری بسته، پرواز، نقشه‌های جعلی یا مسیریاب‌های جعلی گسترش می‌یابد. این بدافزار، مسیر جستجوهای کاربر را در صفحه مرورگر تغییر می‌دهد.

بدافزار جونیو

بدافزار جونیو (Genieo) یکی دیگر از تبلیغ‌افزارهایی است که می‌تواند از آسیب‌پذیری‌های سیستم سوءاستفاده کند. این بدافزار قدیمی از سال ۲۰۱۳ تاکنون توانسته تا فعالیت مخرب خود علیه مک را حفظ کند. این بدافزار با تغییر زیرکانهٔ روش‌های خود توانسته است که در طول سال‌های متوالی همچنان به عنوان یک تهدید علیه کاربران مک باشد. بدافزار جونیو مسیر جستجوی کاربران و صفحه اصلی مرورگر آن‌ها را به صفحات خود تغییر می‌دهد. صفحه‌های این بدافزار اسم‌های مختلفی ولی ظاهر مشابهی دارند. در یک مرورگر آلوده، موتور جستجو با این بدافزار جایگزین می‌شود. به این ترتیب کاربر به صفحات تبلیغاتی هدایت می‌شود که مجرمین سایبری از آن‌ها درآمدزایی می‌کنند. جالب این جاست که حذف این بدافزار مشکل است؛ حتی ممکن در واکنش به حذف شدن، اعمال تخریبی خود را افزایش دهد، به طوری که به یک بدافزار تمام عیار تبدیل شود.



۴

آسیب‌پذیری‌ها

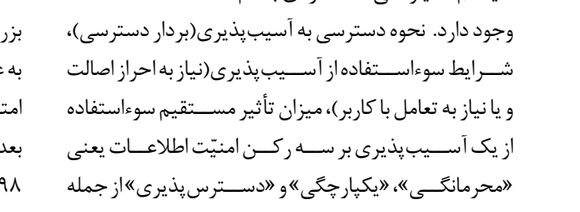
در فضای سایبری امروز، آسیب‌پذیری‌ها شهاب‌سنگ‌های کوچک و
بزرگی هستند که با احتمال زیادی به شما برخورد خواهند کرد

۴ آسیب‌پذیری‌ها

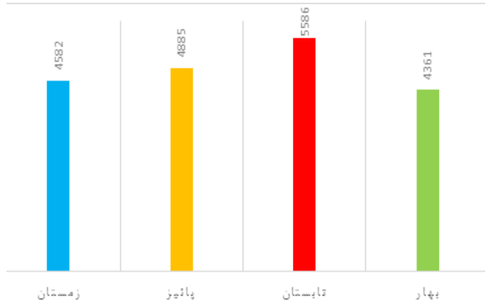
۱.۴ مقدمه

آسیب‌پذیری‌ها به ضعف‌ها و مشکلات یک سیستم گفته می‌شود که فرد مهاجم می‌تواند با سوءاستفاده از آن‌ها اقدام به انجام عملی نماید که در حالت عادی مجاز به انجام آن نیست. می‌توان گفت آسیب‌پذیری‌ها دریچه ورود مهاجمین به سیستم‌ها هستند. تشخیص، مدیریت و رفع به موقع آن‌ها می‌تواند مانع بسیاری از تهدیدات امنیتی شده و سیستم را در مقابل حملات محافظت نماید. در این بخش، به ارایه و بررسی آمار و ارقام مرتبط با آسیب‌پذیری‌های اعلانی سال ۱۳۹۸ پرداخته می‌شود. داده‌های این بخش تعداد آسیب‌پذیری‌ها در این سال به تفکیک ماه و فصل، سطح خطر آسیب‌پذیری‌ها، عوامل موثر در تعیین سطح خطر، ارزش آن‌ها و انواع محصولات آسیب‌پذیر را شامل می‌شود.

در این گزارش به بررسی کمّی آسیب‌پذیری‌های سال ۱۳۹۸ اکتفا نشده است. بلکه ملاک‌های کیفی از جمله سطح خطر و ویژگی‌های تعیین‌کننده آن نیز ارائه شده است. سطح خطر آسیب‌پذیری‌ها از آن جهت مهم است که نشان می‌دهد بدون در نظر گرفتن شرایط محیطی، یک آسیب‌پذیری چرا و تا چه اندازه‌ای می‌تواند خطرآفرین باشد. همچنین نوع محصولاتی است که بیشترین آسیب‌پذیری را داشته‌اند برآوردی از محصولاتی که در سال پیش رو بایستی بیشتر مراقبت شوند، بدست می‌دهد. در سال ۱۳۹۸، در پایگاه ثبت آسیب‌پذیری VulDB در مجموع ۱۹۴۱۴ آسیب‌پذیری ثبت شده است. چنانچه نمودار زیر نشان می‌دهد؛ تعداد آسیب‌پذیری‌ها در طول سال روندی نوسانی داشته است. ماه مرداد با ۲۲۹۰ آسیب‌پذیری، بیش‌ترین و ماه بهمن با ۱۰۱۱ آسیب‌پذیری کم‌ترین تعداد آسیب‌پذیری را داشته‌اند. نمودار ۲ نشان می‌دهد که تابستان ۱۳۹۸ با ۵۵۸۶ آسیب‌پذیری، داغ‌ترین فصل انتشار آسیب‌پذیری‌ها بوده است. همچنین بهار سال گذشته با ۴۳۶۱ آسیب‌پذیری، امن‌ترین فصل سال بوده و حدوداً ۲۸ درصد از آسیب‌پذیری‌ها متعلّق به این فصل هستند. در سال ۱۳۹۸ به طور متوسط در هر روز بیش از ۵۳ آسیب‌پذیری گزارش شده است.



تعداد آسیب‌پذیری‌ها به تفکیک ماه



تعداد آسیب‌پذیری‌ها به تفکیک فصل

۲.۴ میزان اهمیت آسیب‌پذیری‌ها

آسیب‌پذیری‌ها درجه اهمیّت متفاوتی دارند. با توجّه به تعداد بالای آسیب‌پذیری‌های منتشر شده در هر روز و عدم امکان رسیدگی موازی به تمامی آن‌ها، بحث تعیین درجه اهمیّت و اولویت‌بندی آن‌ها امری ضروری است. از این رو با در نظر گرفتن آن دسته از مشخّصات آسیب‌پذیری که به ذات آن بستگی داشته و در طی زمان ثابت بوده و به محیط سازمان یا کاربران بستگی ندارد، امتیازی به هر آسیب‌پذیری اختصاص داده می‌شود. برای رتبه‌بندی آسیب‌پذیری‌ها سیستم امتیازدهی استانداردی به نام CVSS وجود دارد. نحوه دسترسی به آسیب‌پذیری(بردار دسترسی)، شرایط سوءاستفاده از آسیب‌پذیری(نیاز به احراز اصالت و یا نیاز به تعامل با کاربر)، میزان تأثیر مستقیم سوءاستفاده از یک آسیب‌پذیری بر سه رکن امنیّت اطلاعات یعنی «محرمانگی»، «یکپارچگی» و «دسترس‌پذیری» از جمله موارد درنظر گرفته شده در این استاندارد حین محاسبه امتیاز می‌باشند. برای مثال آخرین نسخه استاندارد CVSS از روابط زیر برای محاسبهٔ امتیاز هر آسیب‌پذیری استفاده می‌کند. عدد حاصل که با نام امتیاز مبنا شناخته می‌شود، مستقل از شرایط محیط سازمان یا کاربر است. علاوه بر این امتیاز، هر سازمان بایستی با توجّه به ویژگی‌های محیطی، امتیاز محیطی هر آسیب‌پذیری را محاسبه نماید.

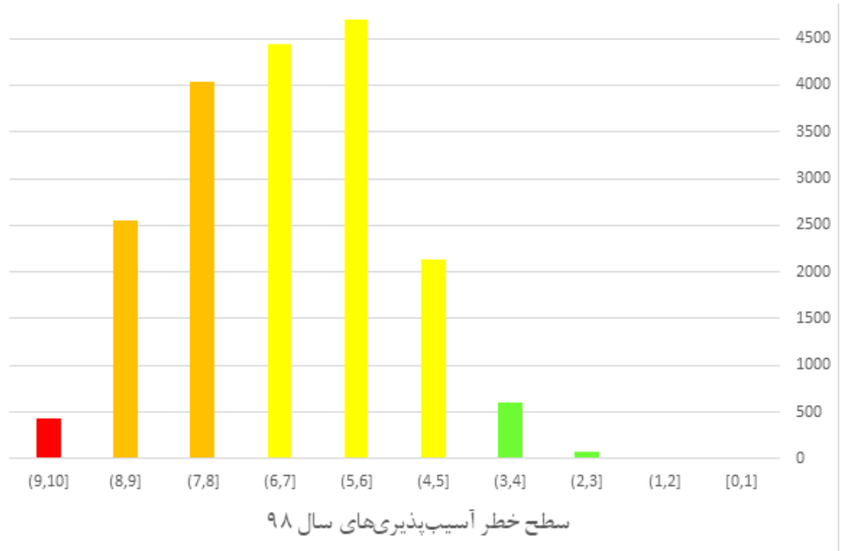
آسیب‌پذیری‌ها باید بر اساس سطح اهمیت و خطر اولویت‌بندی شوند.

پایگاه رسمی اعلام آسیب‌پذیری VulDB با استفاده از استاندارد CVSS، امتیاز آسیب‌پذیری‌های اعلام شده را تعیین می‌کند. در این استاندارد هر آسیب‌پذیری امتیازی بین صفر تا ده را دریافت می‌کند. بزرگی این عدد نشان از سطح خطر آسیب‌پذیری دارد. به عبارت دیگر، صفر کم‌خطرترین آسیب‌پذیری و ده، امتیاز پرخطرترین آسیب‌پذیری است. نمودار صفحه بعد، سطح خطر آسیب‌پذیری‌های منتشرشده در سال ۱۳۹۸ را با توجّه به استاندارد CVSS نشان می‌دهد.

$$Exploitability = 20 \times AccessVector \times AttackComplexity \times Authentication$$

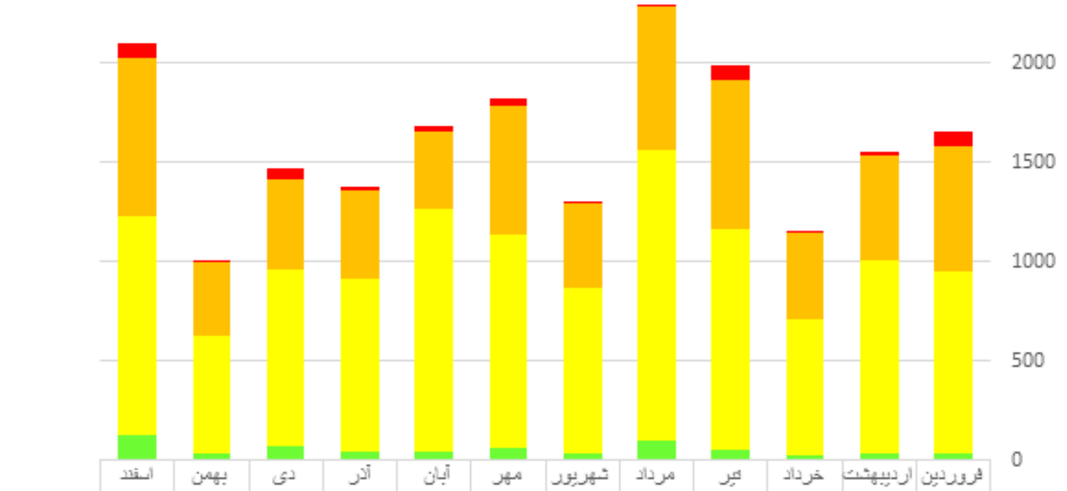
$$Impact = 10.41 \times (1 - (1 - ConfImpact) \times (1 - IntegImpact) \times (1 - AvailImpact))$$

$$f(Impact) = \begin{cases} 0, & \text{if } Impact = 0 \\ 1.176, & \text{otherwise} \end{cases}$$



سطح خطر آسیب‌پذیری‌های سال ۹۸

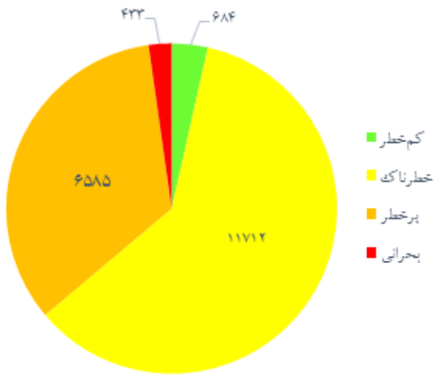
با توجّه به این امتیازها می‌توان آسیب‌پذیری‌ها را به چهار گروه کم‌خطر، خطرناک، پرخطر و بحرانی دسته‌بندی کرد. دسته کم‌خطر شامل آسیب‌پذیری‌های با امتیاز بین ۰ تا ۴ می‌باشند. سوءاستفاده از این دسته از آسیب‌پذیری‌ها نیازمند برقراری شرایط ویژه‌ای بوده و معمولاً تهدید جدّی محسوب نمی‌شوند. با این حال نمی‌توان به‌طور کلّی آن‌ها را نادیده گرفت و از همین رو لازم است آگاهی‌رسانی کافی درخصوص آن‌ها صورت پذیرد تا سازمان‌های آسیب‌پذیر در مقابل آن، نسبت به رفع آسیب‌پذیری مورد نظر اقدام نمایند. آسیب‌پذیری‌های با امتیاز بین ۴ و ۷ را در دسته آسیب‌پذیری‌های خطرناک دسته‌بندی می‌کنند. این آسیب‌پذیری‌ها نیازمند توجّه بیشتری بوده و لازم است علاوه بر اطلّاع‌رسانی به موقع، نسبت به برطرف نمودن آن اقدام نمود. آسیب‌پذیری‌های با امتیاز بین ۷ تا ۹ را آسیب‌پذیری‌های پرخطر می‌نامند. این آسیب‌پذیری‌ها می‌توانند اثرات مخرّبی برای کاربران و سازمان‌ها داشته باشند و لازم است هرچه زودتر برای مقابله با این آسیب‌پذیری‌ها برنامه‌ریزی شود. آسیب‌پذیری‌های با امتیاز بالاتر از ۹ را آسیب‌پذیری‌های بحرانی می‌نامند. این آسیب‌پذیری‌ها تهدیدی بسیار جدّی برای سازمان به حساب می‌آیند و در اسرع وقت باید برطرف شده و جلوی سوء استفاده از آن‌ها گرفته شود. در نمودار زیر آسیب‌پذیری‌های سال ۱۳۹۸ به تفکیک میزان خطر در هر ماه نشان داده شده است.



	اسفند	بهمن	دی	آذر	آبان	مهر	شهریور	مرداد	تیر	خرداد	اردیبهشت	فروردین
بحرانی	79	17	58	21	26	38	14	10	73	12	15	70
پرخطر	796	368	451	442	393	645	423	720	753	433	532	629
خطرناک	1095	591	892	869	1216	1073	832	1459	1113	684	971	917
کم‌خطر	131	35	69	49	46	67	38	101	50	26	35	37

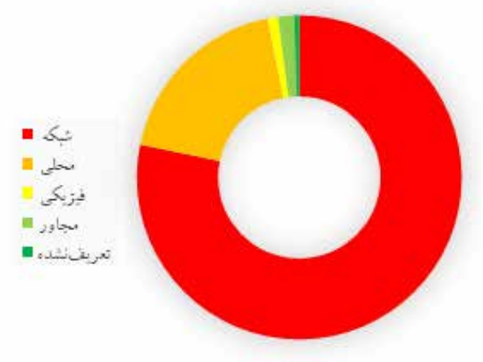
سطح خطر آسیب‌پذیری‌ها به تفکیک ماه

در نمودار زیر نیز مجموع تعداد آسیب‌پذیری‌های ثبت شده در سال ۱۳۹۸ به تفکیک امتیاز مبنای آن‌ها نشان داده شده است.



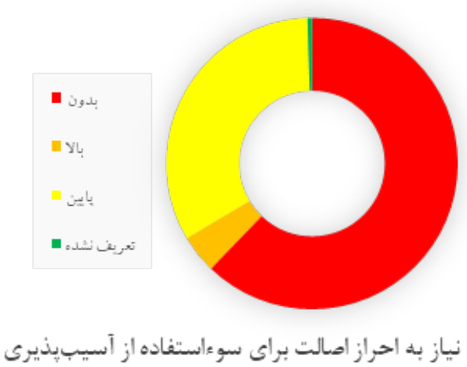
تعداد آسیب‌پذیری‌ها به تفکیک سطح خطر

چنانچه گفته شد در استاندارد CVSS یکی از معیارهای تعیین سطح خطر آسیب‌پذیری، بردار دسترسی است. این معیار نشان می‌دهد که آسیب‌پذیری چگونه موردسوءاستفاده قرار می‌گیرد؛ اگر آسیب‌پذیری بتواند به صورت از راه دور (از طریق شبکه) موردسوءاستفاده قرار گیرد، امتیاز آن بیشتر می‌شود و اگر برای سوءاستفاده از آسیب‌پذیری، نیاز به دسترسی فیزیکی باشد، امتیاز آن کم‌تر خواهد بود. نمودار زیر بردار دسترسی آسیب‌پذیری‌های سال گذشته را نشان می‌دهد. مشاهده می‌شود که حدود ۷۸٪ آسیب‌پذیری‌های منتشرشده به صورت از راه دور و از طریق شبکه قابل سوءاستفاده هستند.



بردار دسترسی آسیب‌پذیری‌های سال ۹۸

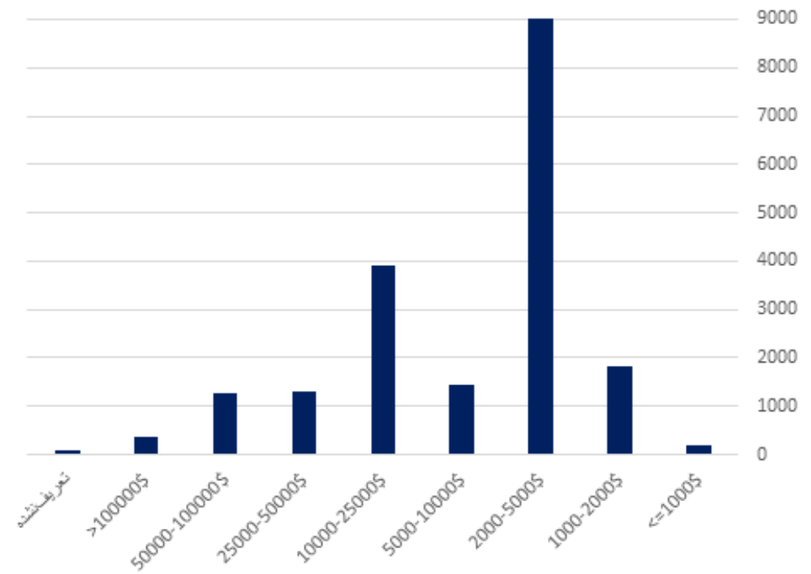
برای سوءاستفاده از ۱۹٪ آسیب‌پذیری‌ها، مهاجم بایستی در شبکه سیستم هدف باشد. برای دسترسی به ۲٪ از این آسیب‌پذیری‌ها، مهاجم باید از طریق لینک لایه دو شبکه به سیستم متصل باشد یا اصطلاحاً مجاور سیستم هدف باشد. نهایتاً برای سوءاستفاده از ۱٪ از آسیب‌پذیری‌های سال ۱۳۹۸، نیاز به دسترسی مستقیم یا فیزیکی به سیستم هدف است. معیار دیگری که در تعیین سطح خطر آسیب‌پذیری‌ها لحاظ می‌شود، نیاز به احراز اصالت مهاجم برای سوءاستفاده از آسیب‌پذیری است. منظور از این معیار این نیست که روند احراز اصالت تا چه اندازه پیچیده است و چقدر کار را برای مهاجم سخت‌تر می‌سازد. بلکه منظور آن است که آیا مهاجم نیازی به فراهم کردن اعتبارنامه‌ها و استفاده از آن‌ها برای محرز شدن اصالتش به عنوان پیش‌نیاز حمله دارد یا خیر. برای سوءاستفاده از برخی آسیب‌پذیری‌ها، مهاجم به احراز اصالت نیازی ندارد. بدیهی است که چنین آسیب‌پذیری‌هایی سطح خطر بالاتری خواهند داشت. همچنین برای بعضی آسیب‌پذیری‌ها کافی است مهاجم یک بار احراز اصالت شود. در اینصورت معیار احراز اصالت، مقدار کم خواهد گرفت و اگر نیاز به چندین بار احراز اصالت باشد، مقدار این معیار بالا خواهد بود. چنانچه نمودار زیر نشان می‌دهد برای سوءاستفاده از ۶۲٪ از آسیب‌پذیری‌های سال ۱۳۹۸ نیازی به احراز اصالت نیست که درصد قابل توجّهی است.



نیاز به احراز اصالت برای سوءاستفاده از آسیب‌پذیری

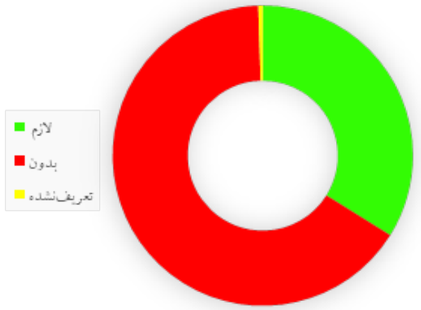
۳.۴ارزش روز صفر آسیب‌پذیری‌ها

بررسی آسیب‌پذیری‌ها با توجّه به ارزش روزصفر آن‌ها نیز می‌تواند اطلاعات مناسبی در اختیار قرار دهد. الگوریتم خاصی برای تعیین ارزش روز صفر یک آسیب‌پذیری وجود دارد. مقدار محاسبه‌شده عموماً با قیمت آسیب‌پذیری در بازار بهره‌جویی مطابقت دارد. امّا ارزش روزصفر یک آسیب‌پذیری، ارزش یا قیمتی است که آسیب‌پذیری قبل از اعلان عمومی و افشا دارد. ارزش‌گذاری روزصفر آسیب‌پذیری‌های سال ۱۳۹۸ در پایگاه داده VulDB در نمودار زیر ارائه شده است. چنانچه مشهود است بیشتر آسیب‌پذیری‌های سال ۱۳۹۸ در بازه ۲هزار الی ۵هزار دلار قیمت‌گذاری شده‌اند.



ارزش روز صفر آسیب‌پذیری‌ها

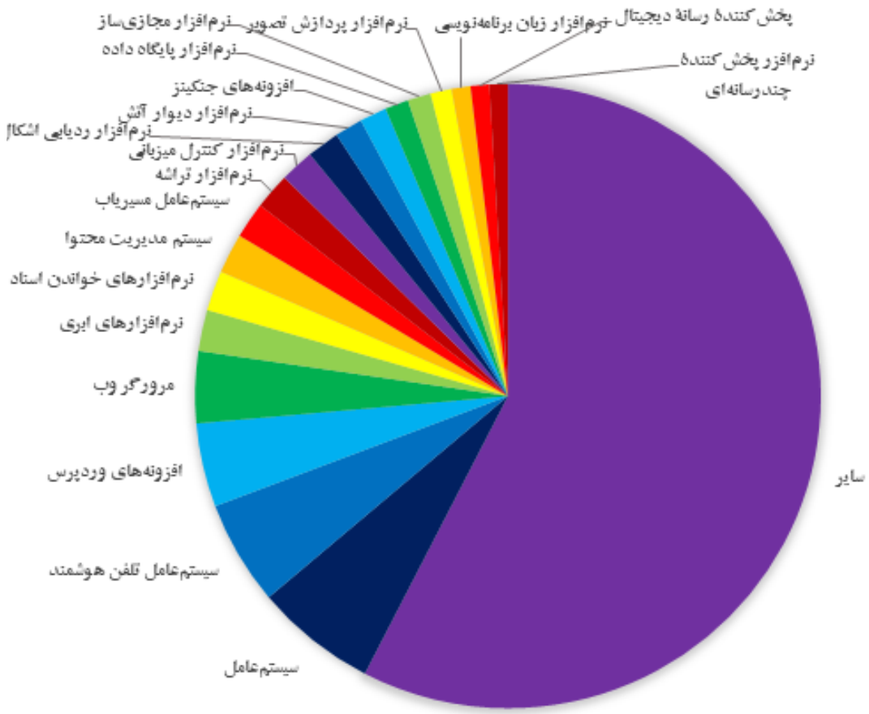
در کنار معیار نیاز به احراز اصالت، نیاز به تعامل با کاربر نیزسختی سوءاستفاده از یک آسیب‌پذیری را تعیین می‌کند. اگر برای سوءاستفاده از آسیب‌پذیری نیاز به تعامل با کاربر باشد، مهاجم بایستی پیش از حمله زمینه فریب کاربر را فراهم کند. برای این کار معمولاً از تکنیک‌های مهندسی اجتماعی استفاده می‌شود. اگر سوءاستفاده از آسیب‌پذیری به تعامل با کاربر وابسته نباشد، آسان‌تر بوده و از این رو امتیاز آسیب‌پذیری بیشتر خواهد بود. نمودار مقابل نشان می‌دهد که بالغ بر ۶۶٪ آسیب‌پذیری‌های سال ۱۳۹۸ بدون تعامل با کاربر قابل‌سوءاستفاده بوده‌اند.



نیاز به تعامل با کاربر برای سوءاستفاده از آسیب‌پذیری

۴.۴نوع محصولات آسیب‌پذیر

تحلیل آمار انواع محصولات دارای آسیب‌پذیری نیز حاوی اطلاعات حائز اهمیّتی است. نمودار ۱۰ نسبت انواع محصولاتی که سال گذشته آسیب‌پذیری آن‌ها منتشر شده است را نشان می‌دهد. بیشترین آسیب‌پذیری‌ها در سال ۱۳۹۸ مربوط به سیستم‌های عامل بوده است. سیستم‌عامل تلفن‌های هوشمند، افزونه‌های وردپرس، مرورگرهای وب، نرم‌افزارهای ابری و نرم‌افزارهای خواندن اسناد در رده‌هایی بعدی اعلان آسیب‌پذیری هستند. به دلیل تنوّع زیاد محصولات، دسته‌ای با عنوان «سایر» در نمودار وجود دارد.



انواع محصولات دارای آسیب‌پذیری

تعداد زیاد آسیب‌پذیری‌ها و رشد آن‌ها نسبت به سال گذشته، لزوم توجه جدّی به بحث مدیریت آسیب‌پذیری در سازمان‌ها را روشن‌تر می‌نماید. بدین منظور لازم است تیم امنیت شبکه هر سازمان به طور پیوسته اخبار آسیب‌پذیری‌های مختلف و به خصوص آسیب‌پذیری‌هایی که در ارتباط با تجهیزات و یا نرم‌افزارهای مورد استفاده در آن سازمان را رصد کرده و با به‌روزرسانی نرم‌افزارها و اعمال وصله‌های امنیتی منتشر شده، اقدام به امن‌سازی شبکه کنند. تیم کارشناسی مرکز تخصصی آپا دانشگاه صنعتی اصفهان، مهم‌ترین آسیب‌پذیری‌ها را به صورت هفتگی در وب‌سایت خود به نشانی www.nsec.ir منتشر می‌کند.

۵

رخدادهای مهم امنیتی جهان در سال ۹۸

مروری بر رخدادهای مهم جهان در سال ۹۸

۵ رخدادهای مهم امنیتی جهان در سال ۹۸

۱.۵ مقدمه

اگر در سال اخیر، اخبار سایبری سراسر جهان را دنبال کرده باشید، احتمالاً متوجه شده‌اید که نشت/نقض اطلاعات سازمان‌ها و شرکت‌های مهم یکی از پرتکرارترین خبرهای سال ۹۸ بوده است. این امر در کنار رسوایی شرکت‌های مشهوری که حریم خصوصی کاربران خود را نقض می‌کنند، موج گسترده‌ای از اعتراض کاربران سراسر دنیا را شکل داده است. به طوری که به نظر می‌رسد، کاربران بیش از هر زمان دیگری خواهان تصویب قوانینی در جهت حفظ حریم خصوصی هستند. در این بخش به بررسی چند نشت اطلاعات مهم سال ۹۸ می‌پردازیم و سپس از تحولات مثبتی گزارش می دهیم که در برخی از کشورها و شرکت‌ها، برای حل مشکل حریم خصوصی اتخاذ شده است. در ادامه، وضعیت کمپین‌هایی تروجان‌های دسترسی از راه دور و همچنین وضعیت یکی از گروه‌های خطرناک سرقت کننده DNS را بررسی می کنیم که از رخدادهای مهم سال ۹۸ هستند. در ادامه به آسیب‌پذیری‌های حیاتی گوشی‌های هوشمند اندرویدی اشاره می کنیم که امنیت میلیون‌ها کاربر را تحت‌الشعاع قرار داده‌اند. در انتها به خبر بازنشستگی ویندوز ۷ می‌پردازیم و تبعات امنیتی آن را توضیح می‌دهیم که کاربران این سیستم‌عامل از این پس با آن روبه‌رو هستند.

۲.۵ رخدادهای مهم سال ۹۸

نشت اطلاعات شرکت سیتریکس

سیتریکس (Citrix)، یک شرکت بسیار مشهور نرم‌افزاری است که سرور، برنامه‌های مجازی‌ساز و فناوری‌های شبکه‌ای و محاسبات ابری ارائه می‌دهد. بنا به گزارش سیتریکس که در اردیبهشت ۹۸ به طور عمومی منتشر شد، هکرها از مهرماه تا اواسط اسفند ۹۷ دسترسی متناوبی به شبکهٔ داخلی این شرکت داشته‌اند. هکرها در این مدت فایل‌هایی را از روی سیستم‌های شرکت سیتریکس سرقت می کنند که شامل اطلاعات کارمندان شرکت و برخی اطلاعات مالی بوده است. این شرکت معتقد است که عامل این حمله تکنیک اسپری کردن رمزعبور است؛ یعنی مهاجم سیستم‌ها را اسکن می کند و سعی می کند با سوءاستفاده از رمزعبورهای ضعیف و رایج آن‌ها از موانع عبور کند. این امر لزوم استفاده از رمزعبور قوی را یادآوری می کند. قابل ذکر است که تعداد قربانیان این حمله نامشخص است اما این شرکت به حدود ۴۰۰ هزار شرکت دیگر و همچنین سازمان‌های جهانی سرویس ارائه می‌دهد.

نشت داده فیس‌بوک

فیس‌بوک که پیش از این بارها نشان داده است که در حفظ و نگهداری حریم خصوصی کاربرانش بسیار سهل‌انگار است و حتی فراتر از سهل‌انگاری، حاضر به فروش اطلاعات کاربرانش هم می‌شود (اشاره به رسوایی فیس‌بوک و مؤسسه کمبریج‌آنالیتیکا)، سال ۹۸ هم دوباره با نشت اطلاعات ۴۱۹ میلیون از حساب‌های کاربری خود، خبرساز شد. این اطلاعات که روی یک سرور محافظت‌نشده و بدون رمزعبور قرار داشت، نشان می‌داد که هر حساب کاربری با چه شماره موبایلی ثبت شده است. اما اتفاق دیگری که در مورد فیس‌بوک در سال ۹۸ افتاد، افشای حجم انبوهی از اطلاعات حساب‌های کاربری فیس‌بوک در سرور ابری آمازون بود.

در فیس‌بوک دو چیز اهمیت ندارد: حریم خصوصی و امنیت کاربران!

تیم امنیتی UpGuard کشف کرد که دو رخداد نشت اطلاعاتی حجیم در دو منطقه مختلف اتفاق افتاده است که در مجموع ۵۴۰ میلیون رکورد از اطلاعات فیس‌بوک شامل لایک‌ها، اسامی حساب‌ها و بسیاری از موارد دیگر در معرض دید عموم قرار گرفته است. به نظر می‌رسد با توجه به اطلاعاتی که در این اتفاق افشا شد، فیس بوک نتواند خسارت این نشت اطلاعات گسترده را جبران کند. البته منظور از خسارت، خسارت مالی نیست بلکه بیشتر خسارت واردشده به حریم خصوصی میلیون‌ها انسان است که اکنون اطلاعات شخصی‌شان در اختیار بسیاری قرار دارد. در رابطه با فیس‌بوک و اقدامات اخیرش در بخش حریم خصوصی بیشتر پرداخته‌ایم.

نشت داده اینستاگرام

شبکه اجتماعی اینستاگرام که در حال حاضر به شرکت فیس‌بوک تعلق دارد، همانند فیس‌بوک چندان شهرت خوبی در حفظ حریم خصوصی کاربران خود ندارد. در سال ۹۸، اینستاگرام هم درگیر یک نشت اطلاعات گسترده بود. در این مورد مشخص شد که اطلاعات میلیون‌ها افراد مشهور و تأثیرگذار (اصطلاحاً سلبریتی) اینستاگرام در پایگاه دادهٔ آنلاین و محافظت‌نشده‌ای قرار داشته است. به نظر می‌رسد این اطلاعات که شامل شماره همراه، ایمیل و در مواردی موقعیت جغرافیایی این افراد است توسط یک شرکتی بازاریابی دیجیتال به نام Chtrbox از بمبئی جمع‌آوری شده است. البته بایستی توجه کرد که فارغ از بحث نشت اطلاعات، بسیاری از کاربران اینستاگرام با سهل‌انگاری حجم زیادی از اطلاعات زندگی شخصی‌شان را در اینستاگرام به اشتراک می گذارند. جالب این جا است که فضای این برنامه به گونه‌ای است که بیش از سایر شبکه‌های اجتماعی، کاربران را به اشتراک‌گذاری روزمره و در معرض عموم قرار دادن زندگی شخصی‌شان تشویق می‌کند. این در حالی است که ممکن است سازمان‌ها یا افراد مختلف با جمع‌آوری این اطلاعات به طرق مختلف اقدام به سوءاستفاده و یا حتی تهدید این کاربران کنند.

حریم خصوصی

در سال‌های اخیر همواره شاهد بوده‌ایم که بسیاری از شرکت‌ها و سازمان‌های بزرگ در سراسر جهان به خود اجازه داده‌اند تا حریم خصوصی کاربران خود را نقض کنند، اطلاعاتی که از کاربران خود به امانت در اختیار دارند را به سازمان‌های دیگر بفروشند یا از آن سوءاستفاده کنند. این رفتار غیراخلاقی و البته غیرقانونی شرکت‌ها در بسیاری از موارد اعتراضات کاربران آن‌ها را برمی‌انگیخت اما متاسفانه این اعتراضات جز در مواردی خاص، نتیجه‌ای در پی نداشت. تا این که در سال گذشته، کاربران جدی‌تر از همیشه نسبت به نقض حریم خصوصی و جمع‌آوری داده‌های شخصی‌شان اعتراض کردند. این اعتراضات، موج گسترده‌ای را شکل داد که انگشت اتهام آن به سوی فعالیت‌های مرموز پلتفرم‌های محبوبی همچون فیس‌بوک و گوگل بود. به طور مثال از گوگل خواسته شد تا توضیح بدهد که به چه دلیل در یکی از محصولات خانگی خود، میکروفون قرار داده است و حتی فراموش کرده است که این موضوع را به مشتریان خود اطلاع بدهد! نتیجه این اعتراضات در بسیاری کشورها این شد که قانون‌گذاران، قوانین جدیدی در رابطه با حریم خصوصی شهروندان خود تصویب کنند و کنترل سختگیرانه‌تری روی سازمان‌های و شرکت‌ها داشته باشند. به طور مثال در ایالات متحده امریکا در سال اخیر، ده‌ها لایحه و اصلاحیه وضع شد که در آن‌ها تلاش شده است همچون مقررات عمومی حفاظت از داده اتحادیه اروپا (GDPR)، شرکت‌های فناوری را ملزم به حفاظت از داده‌های کاربران خود کند و همچنین تنها در صورتی بتوانند اطلاعات حساس کاربران را جمع‌آوری کنند که پیش از آن کاربر به آن‌ها به طور صریح و روشن اجازه بدهد. همچنین این قوانین به شهروندان امریکایی اجازه می‌دهد که انواع خاصی از داده‌های خود را حذف و اصلاح کنند و از شرکتی به شرکتی دیگر جابه‌جا کنند. از دیگر اقداماتی که در سال اخیر در حوزه ارتقای حریم

خصوصی کاربران صورت گرفته است می‌توان به انتشار نسخه دسکتاپ مرورگر Ghostery اشاره کرد. این مرورگر با حذف اشکالات جاوااسکریتیِ بسیاری از سایت‌ها به ردیاب‌ها اجازه نمی‌دهد که اطلاعات کاربران را جمع‌آوری کنند. همچنین شرکت اپل از ارائه سرویس Single Sign-On به کاربران خود خبر داده است که در آن ایمیل واقعی کاربر با نهادهای سوم شخص به اشتراک گذاشته نمی‌شود. با انتشار خبر این که برنامه اندرویدی Ring (از محصولات شرکت آمازون) اطلاعات کاربران خود را بدون اجازه برای ردیاب‌هایی همچون API Graph Facebook ارسال می‌کند، اعتراضات گسترده‌ای را ایجاد کرد که در پی آن سناتور امریکایی از توسعه دهندگان این برنامه توضیح خواست. مارک زاکربرگ، مدیر فیس بوک، پس از رسوایی‌های مختلف در رابطه با جمع‌آوری و فروختن اطلاعات کاربران فیس‌بوکی قول داده است که این بار شرایطی را فراهم کند که در آن واقعاً به حریم خصوصی کاربران احترام گذاشته شود. در این راستا قرار است ویژگی‌های متعددی به فیس‌بوک اضافه شود تا کاربران خود در رابطه با حریم خصوصی داده‌هایشان تصمیم بگیرند. به نظر می‌رسد فیس‌بوک به زودی از رمزنگاری انتها به انتها نیز برخوردار شود.

شنود کامل مکالمات و هک دوربین گوشی‌های سامسونگ

در سال ۹۸ محققان آسیب‌پذیری امنیتی را کشف کردند که برنامه‌های دوربین گوگل و دوربین سامسونگ را تحت‌تأثیر قرار می‌داد. مهاجم با سوءاستفاده از این آسیب پذیری می‌توانست که کنترل کامل دوربین گوشی قربانی را به دست آورد. اما نکته جالب این جا بود که این آسیب‌پذیری تنها اختیار دوربین را به مهاجم نمی‌داد بلکه مهاجم می‌توانست کلیه مکالمات قربانی را شنود یا در صورت تمایل ضبط کند. تمامی فعالیت‌های مهاجم در پس‌زمینه انجام می‌شد که به همین علت قربانی متوجه حمله نمی‌شد. اما در سال ۹۸ آسیب‌پذیری‌های حیاتی دیگری نیز در گوشی‌های گلکسی S10، S9، S8 و نوت ۱۰ و ۹ کشف شد که میلیون‌ها کاربر این برند مشهور را تحت‌تأثیر قرار می‌داد.

پایان کار ویندوز ۷

یکی از خبرهای مهم سال ۹۸، به پایان رسیدن دوران خدمت ویندوز ۷ سالخورده است که به طور رسمی در دی‌ماه به اتمام رسید. این بدان معنا است که کارمندان سازمان‌ها و به‌طور کلی تمامی کاربرانی ویندوز ۷ دیگر از وصله‌های و به‌روزرسانی‌های امنیتی بهره‌مند نخواهند شد مگر اینکه هزینه‌ای به‌طور جداگانه‌ای برای این پشتیبانی بپردازند. در همین راستا مایکروسافت از کاربرانی که هنوز از ویندوز ۷ استفاده می کنند درخواست کرد تا با نصب ویندوز ۱۰ امنیت خود را ارتقا دهند و از خدمات فنی و به‌روزرسانی‌های امنیتی بهره ببرند. در حال حاضر تخمین زده شده که تعداد کاربران ویندوز ۷ به ۲۰۰ میلیون می‌رسد. قابل ذکر است که اگر کاربران سیستم‌عامل خود را ارتقا ندهند با آسیب‌پذیری‌های امنیتی و اشکالات نرم‌افزاری روبه‌رو خواهند شد. چراکه مایکروسافت دیگر وظیفه‌ای در رفع اشکالات و فراهم کردن امنیت این سیستم‌عامل ندارد؛ درنتیجه کاربرانی که قصد دارند همچنان از سیستم‌عامل ویندوز ۷ استفاده کنند، در معرض حملات سایبری بیشتری قرار خواهند گرفت.

دیگر زمان بازنشستگی ویندوز ۷ و استفاده از نسخه‌های جدیدتر ویندوز است.

فعالیت RATها

تروجان‌های دسترسی از راه دور یا به اختصار RAT برنامه‌هایی هستند که به مهاجم توانایی نظارت مخفیانه و دسترسی غیرمجاز به سیستم قربانی را می‌دهند. این بدافزارها عموماً رفتار برنامه‌های ضبط کننده کلید را تقلید می کنند. مثلاً کلیدهای فشرده شده کاربر، نام‌های کاربری، رمزعبور، اسکرین‌شات، تاریخچه مرورگر، محتوای ایمیل‌ها و چت‌ها را ذخیره می کنند. اما تفاوت RAT با ضبط کننده کلید این است که مهاجم با کمک RAT می‌تواند حتی فراتر از یک بیننده، تنظیمات سیستم قربانی را تغییر دهد. یکی از مواردی مهمی که در مورد RATها باید دانست این است که مهاجم می‌تواند با اختیارات سطح ادمین و دسترسی به خط فرمان هرآنچه را که می‌خواهد روی سیستم قربانی انجام دهد. گروه تحقیقاتی سیسکو تالوس معتقد است در سال ۹۹ فعالیت گسترده‌ای از RATها مشاهده خواهیم کرد. از شواهد مشخص است که Orcus RAT و RevengeRAT در صدر فعال‌ترین RATهای حال حاضر باشند چرا که کمپین‌های مختلفی را علیه مؤسسات مالی، دولتی و

سازمان‌های مهم تشکیل داده‌اند. از جمله تکنیک‌های مهم این بدافزارها می‌توان به موارد زیر اشاره کرد:

- استفاده از روش‌های ماندگاری مرتبط با بدافزار fileless
- روش‌های پنهان‌کاری با هدف پوشاندن زیرساخت‌های C2
- بهره‌گیری از روش‌های فرار از آنتی‌ویروس‌ها و جعبه شن

سرقت DNS

به نظر می‌رسد فعالیت گروه هکری Sea Turtle در سال ۹۸ همچنان پرقوت ادامه داشته است. این گروه از جمله گروه‌هایی است که به ربودن (هایجک) DNS می‌پردازد. منظور از سرقت DNS، فعالیت مخربی است که در آن مهاجم سبب می‌شود تا درخواست‌های DNS قربانی به جای ترجمه به آدرس آی‌پی اصلی به آی‌پی مدنظر مهاجم ترجمه شود. گروه Sea Turtle در کمین سازمان‌هایی است که دامنه‌های سطح بالا (TLD) را کنترل می‌کنند. این گروه با کشف آسیب‌پذیری‌های این سازمان‌ها، کنترل سرور را برای کل دامنه‌ها به دست می‌آورند. به طوری که مهاجم می‌تواند تمامی آدرس‌های آی‌پی که در پاسخ به کوئری‌های DNS ارسال می‌شود را کنترل کند. از جمله فعالیت‌های این گروه این بوده است که رکوردهای DNS سرورهای ایمیل را تغییر داده‌اند تا مانع وارد شدن کاربران به سامانه‌های ایمیلی شوند. این امر نه تنها به مهاجمین کمک کرد تا اطلاعات بین کاربران و سامانه ایمیلی آن‌ها را بخوانند بلکه باعث شد گواهی‌های کاربران را نیز سرقت کنند. گروه تحقیقاتی سیسکو تالوس گزارش داده است که گروه Sea Turtle در حال ایجاد گروه‌های جدید و دوبرابر کردن توان خود با اضافه کردن زیرساخت‌های جدید است. این در حالی است که برخی از فعالیت‌های آن‌ها در سال اخیر توسط محققین افشا شد اما این امر نه تنها فعالیت آن‌ها را کم نکرد بلکه گویی انگیزه‌ای جدید به این گروه خطرناک تزریق کرده است.

۶

وضعیت سایبری ایران در سال ۹۸

مروری بر رخدادهای مهم امنیتی کشور در سال ۹۸

به همراه بررسی آماری آلودگی‌ها و آسیب‌پذیری‌های کشور در سال گذشته

۶ وضعیت سایبری ایران در سال ۹۸

۱.۶ مقدمه

سال ۹۸ سالی مملو از اتفاق‌های مختلف مرتبط با امنیت فضای سایبری کشور بود. اگر مروری کوتاه روی رخدادهای سال ۹۸ داشته باشیم، حتما نقش پررنگ فضای سایبری را در این اخبار متوجه خواهیم شد. امسال شاهد رخدادهای گوناگونی در فضای سایبری کشور بودیم. در این قسمت علاوه بر مرور مهم‌ترین رخدادهای امنیتی سال گذشته، به بررسی آمار آلودگی‌ها، آسیب‌پذیری‌ها و بدافزارهای فعال در کشور می‌پردازیم.

۲.۶ رخدادهای مهم سال ۹۸

تلگرام

بی‌شک تلگرام و سرنوشت آن یکی از مسائل مهم حوزه سایبری در کشور ما است. این پیام‌رسان علی‌رغم فیلتر شدن در سال ۹۷، یکی از پراستفاده‌ترین پیام‌رسان‌های سال گذشته کاربران ایرانی بوده و نقش مهمی در به‌خطر افتادن امنیت و حریم خصوصی کاربران ایرانی و به‌خصوص کاربران موبایل داشته است. یکی از مشکلات امنیتی که تلگرام از ابتدای نفوذ خود در میان کاربران ایرانی ایجاد نمود، امکانات بالای این برنامه بود! تلگرام اولین پیام‌رسان محبوب ایرانیان بود که امکان ارسال فایل و برنامه داشت. این امکان موجب توزیع بدافزارها و برنامه‌های آلوده موبایلی در گروه‌ها و کانال‌های مختلف این پیام‌رسان شده است. متاسفانه تعداد زیادی از کاربران با نصب این برنامه‌ها آلوده به بدافزار شده‌اند. اما با فیلترینگ تلگرام در سال ۹۷، کاربران ایرانی بر خلاف دفعات قبلی به پیام‌رسان دیگری کوچ نکردند و این امر مشکلات امنیتی دیگری را به همراه آورد. متن باز بودن قسمت سمت کاربر تلگرام و فیلترینگ این موقعیت را ایجاد نمود که پوسته‌های غیررسمی تلگرام با امکان دور زدن فیلترینگ در میان کاربران ایرانی محبوبیت پیدا کنند. تلگرام طلایی، موبوگرام، هاتگرام و بسیاری از نسخه‌های غیررسمی تلگرام که به راحتی در بازارهای ایرانی برنامه‌های کاربردی و در شبکه‌های اجتماعی در دسترس کاربران قرار داشت، مخاطبان زیادی را به خود جذب کردند. گفته شده است که تلگرام طلایی به تنهایی ۴۵ میلیون کاربر ایرانی داشته است. با گسترش پوسته‌های غیررسمی، بسیاری از کارشناسان و سازمان‌های متولی امنیت ابراز نگرانی کرده و به کاربران هشدار دادند که از این پوسته‌ها استفاده نکنند. در طول زمان نیز مشخص شد که برخی از این پوسته‌ها، اطلاعات را نه فقط برای سرورهای تلگرام بلکه برای سرورهای خود نیز ارسال می‌کنند. این امر سبب گمان‌هایی در مورد جاسوسی بودن برخی از این پوسته‌ها و نقض حریم خصوصی کاربران شد. در اردیبهشت و خردادماه سال ۹۸، پوسته‌های غیررسمی تلگرام از دید مکانیزم‌های امنیتی گوگل‌پلی به عنوان بدافزار شناخته شدند و از دستگاه‌های کاربران حذف شدند. با حذف این برنامه‌ها از روی گوشی کاربران اندروید، این پوسته‌ها نیز به کار خود پایان دادند و بسیاری از آن‌ها فعالیت رسمی خود را متوقف کردند. با این حال انتشار و توزیع نسخه‌های غیررسمی و گاهی آلوده به بدافزار برخی از پوسته‌ها بر روی گروه‌ها و کانال‌های تلگرامی به طور قطع موجب نقض حریم خصوصی کاربران مستقیم آن‌ها و حتی مخاطبین آن کاربران می‌شود.

تلگرام نقش مهمی در به‌خطر افتادن امنیت و حریم خصوصی کاربران ایرانی داشته است!

از سوی دیگر پس از فیلتر تلگرام، کاربرانی که تمایل به استفاده از این پیام‌رسان را داشتند رو به استفاده از وی‌پی‌ان آوردند. به همین جهت استفاده از وی‌پی‌ان برای دور زدن فیلترینگ میان کاربران ایرانی رشد بسیاری پیدا کرد. لازم به توضیح نیست که استفاده از وی‌پی‌ان‌های رایگان چقدر می‌تواند حریم خصوصی و امنیت کاربران را به خطر بیاندازد. بسیاری از این سرویس‌های وی‌پی‌ان رایگان بارها جاسوس‌افزار تشخیص داده شده‌اند و مشخص شده است که امنیت و حریم خصوصی استفاده‌کنندگان آن‌ها را به خطر می‌اندازند. همچنین استفاده گسترده از وی‌پی‌ان موجب شده بسیاری از ترافیک کشور که می‌توانست در داخل کشور مسیریابی شود، ابتدا به خارج از کشور هدایت شود و سپس به داخل کشور بازگردانده شود. این رفت و برگشت ترافیک هم بار زیادی به شبکه کشور تحمیل می‌کند. اما وی‌پی‌ان تنها راه دور زدن فیلترینگ در تلگرام نیست. تلگرام برای کاربرانی که به دلیل فیلترینگ نمی‌توانند از این پیام‌رسان استفاده کنند، پروکسی‌های MTproto را ارائه نمود. این پروکسی‌های داخلی امکان دور زدن فیلترینگ را تنها برای پیام‌رسان تلگرام فراهم می‌کنند و دیگر نیازی به استفاده از وی‌پی‌ان و عبور همه ترافیک موبایل از آن نیست. مدیرعامل تلگرام مدعی است که این پروکسی‌ها امن هستند و سرور پروکسی امکان دسترسی به پیام‌های کاربران را ندارد. اما این پروکسی‌ها یک کانال را به عنوان کانال تبلیغاتی به کاربر نشان می‌دهند که گاهی علاوه بر نمایش پیام‌های زیاد و بعضاً نامناسب، امکان توزیع بدافزار و برنامه‌های آلوده را فراهم می‌کند. ضمناً در آذر ماه سال ۹۸، سرورهای پروکسی تلگرام عامل حمله DDoS به یکی از سرویس‌دهنده‌های ابری کشور شدند. در بهمن ماه و پس از حوادث ترور سردار سلیمانی و حادثه دلخراش سقوط هواپیما، رکورد استفاده از تلگرام در بین کاربران ایرانی شکسته شد. این امر نشان می‌دهد که کاربران ایرانی تصمیم ندارند استفاده از این پیام‌رسان را کنار بگذارند. به نظر می‌رسد در سال جدید نیز قرار نیست مشکلات امنیتی مرتبط با تلگرام به پایان برسد. در روزهای ابتدایی امسال خبر افشای اطلاعات ۴۲ میلیون کاربر ایرانی تلگرام توجه بسیاری را به خود جلب کرد. این اطلاعات که روی یک سرور بدون محافظت وجود داشت، اکنون در انجمن‌های هکری به فروش می‌رسد. شماره تماس، نام و شناسه کاربری و برخی دیگر از اطلاعات کاربران در این پایگاه داده موجود است. امیدواریم در سال جدید با اتخاذ سیاست‌های درست در قبال این پیام‌رسان، تهدیدات امنیتی اشاره شده برای کاربران ایرانی کاهش یابد.

رمزپویا

فیشینگ و سرقت از حساب‌های بانکی کاربران یکی از چالش‌های سیستم بانکی کشور و پلیس فتا در سال‌های گذشته بوده است. برای رفع این مشکل، طرح رمز پویا ارائه شد. اجرای این طرح به دلیل آماده نبودن زیرساخت‌های اجرایی لازم چند بار به تاخیر افتاد ولی در فصل پایانی سال به سرانجام رسید. هدف طرح رمز پویا، جایگزینی رمز دوم ثابت با رمزهای زمان‌دار یکبار مصرف است تا امکان سوءاستفاده از رمز دوم کاربران و سرقت از حساب آن‌ها از بین برود. این طرح موجب برطرف شدن بسیاری از سرقت‌ها شد ولی خود مشکلاتی برای کاربران فراهم کرد. به نظر می‌رسد مسأله‌ای که از ابتدا در این طرح نادیده گرفته شده، راحتی کار با سیستم برای عموم مردم است. در ابتدا هر بانک یک برنامه موبایل جداگانه ارائه کرد. این

امر باعث شد افرادی که چند حساب بانکی داشتند مجبور شوند برنامه‌های متعلق به همه بانک‌ها را نصب کنند. این در حالی است که فعال‌سازی این برنامه‌ها نیز برای یک کاربر عادی، ساده نیست و کارکنان بانک‌ها نیز به دلیل مراجعه زیاد برای رفع مشکلات این برنامه‌ها و نحوه استفاده از آن‌ها با مشکل مواجه شدند. همچنین برخی از این برنامه‌ها دارای ضعف‌های اجرایی و یا امنیتی بود که استفاده از آن‌ها را برای برخی ناممکن می‌کرد.

در ادامه این طرحِ پر سر و صدا از سامانه هریم بانک مرکزی رونمایی شد و با پیوستن بانک‌های مختلف به این سامانه بسیاری از مشکلات دشواری استفاده از برنامه‌های مختلف برای دریافت رمز دوم پویا مرتفع شد.

اکنون هرگاه به قصد خرید به درگاه اینترنتی مراجعه شود، یک دکمه درخواست رمز دوم پویا وجود دارد که با انتخاب آن، سامانه هریم، رمز یکبار مصرف را برای کاربر پیامک می‌کند تا مشکل دشواری استفاده از برنامه‌های مختلف حل شود. اما هنوز کارشناسان در مورد این طرح نظرات مختلفی دارند. برخی معتقدند علی‌رغم اینکه این طرح توانسته مانع بسیاری از حملات فیشینگ روی حساب‌های بانکی شود، نتوانسته به صورت کامل امنیت کاربران را تامین کند. اگرچه روی آوردن به سامانه هریم بسیاری از مشکلات تجربه کاربری این طرح را به‌خصوص برای کاربران عمومی را برطرف کرد، اما با این حال ارسال پیامک، روش امنی برای دریافت رمز نیست. برای تامین امنیت شاید بهتر بود به جای حذف رمز دوم ثابت و جایگزینی آن با رمز پویا، پارامتری دیگر مثل CVV2 پویا می‌شد و یا رمز از دو مولفه ثابت و پویا تشکیل می‌شد تا مولفه دانسته کاربر که یکی از اجزای امنیت است حفظ می‌شد! اکنون رمز حساب کاربران تنها به شماره موبایلی که در بانک تعریف شده وابسته است و اگر این دسترسی به دست فرد دیگری بیافتد، امنیت کاربر کاملاً نقض می‌شود. باید دید در سال جدید این طرح پر سر و صدای بانکی می‌تواند نیازهای امنیتی جامعه را تامین کند یا بازهم دستخوش تغییر خواهد شد؟!

رمز پویا توانسته مانع بسیاری از حملات فیشینگ روی حساب‌های بانکی شود.

تنش‌های بین‌المللی سایبری

سال ۹۸ سالی پر تنش برای کشور ایران بود. اتفاقاتی که در عرصه بین‌المللی رخ داد و به صورت مستقیم یا غیرمستقیم به کشورمان مربوط می‌شد و یا تلاش می‌شد که این رخدادها به ایران ربط داده شود. امسال را شاید بتوان پر تنش‌ترین سال میان ایران و امریکا دانست. سالی که شروع آن با اعلام سپاه پاسداران جمهوری اسلامی به عنوان یک سازمان تروریستی از دید امریکا شروع شد؛ پهپاد امریکایی در آب‌های سرزمینی ایران در خلیج فارس ساقط شد؛ تحریم‌ها استمرار یافت و حلقه‌اش تنگ‌تر شد؛ نفت‌کش ایرانی توسط انگلیس توقیف شد؛ نفتکش انگلیسی در خلیج فارس توقیف شد؛ ترور سردار سلیمانی اتفاق افتاد و پایگاه عین‌الاسد در پاسخ به آن ترور موشک‌باران شد. همه این‌ها، رخدادهایی بودند که سالی پر تنش را برای کشور ما در حوزه بین‌المللی رقم زدند. البته امریکا و متحدانش برخی اتفاقات دیگر در منطقه را به قول خود به گروه‌های نیابتی ایران نسبت دادند! اتفاقاتی نظیر حمله به تاسیسات نفتی آرامکو که یمن اعلام کرد در پاسخ به حملات اتحاد عربستان علیه این کشور، این تاسیسات را هدف قرار داده است. باید این نکته را در نظر داشته باشیم که هر تنش و رخدادی در دنیای بیرونی، در حوزه سایبر نیز بازتاب داشته و تنش‌ها در این حوزه نیز ادامه خواهد یافت! در ابتدای سال با مشاهده روند افزایش فشار امریکا به ایران، کارشناسان در مورد لزوم آمادگی برای دفاع سایبری هشدار دادند. به‌خصوص که در زیرساخت شبکه کشور عمدتاً از محصولات امریکایی استفاده شده و این مساله می‌تواند نقطه ضعف ما در حملات سایبری باشد. تنگ‌تر شدن حلقه تحریم‌ها موجب شد برخی از محصولات امنیت سایبری در کشور از کار بیافتند. به عنوان مثال در تیرماه مجوزهای UTMهای سایبروم شرکت سوفوس که در ایران مورد استفاده قرار می‌گرفت، غیرفعال شد. البته مسئله تحریم همواره چالشی برای خرید و پشتیبانی از محصولات زیرساخت بوده است که در ایران استفاده می‌شوند. همزمان با تنش‌های بین‌المللی و فشارهای بیرونی به کشور، گزارش‌هایی در مورد گروه‌های هکری منتسب به ایران و نقش داشتن آن‌ها در حملات به کشورهای حوزه خلیج فارس، اروپایی و زیرساخت‌های امریکا منتشر شد. پیچیده شدن حملات گروه Muddy Water، گسترش فعالیت‌های گروه‌های هکری APT33 و APT34، جمع‌آوری اطلاعات از کشورهای منطقه، سرقت اطلاعات از دانشگاه‌های امریکایی از تیترهای خبری و گزارش‌های تحلیلی بودند که در سال گذشته از فعالیت‌های گروه‌های هکری منتسب به ایران منتشر شد.

در مقابل نیز ادعاهایی از طرف‌های مقابل در مورد نفوذ به شبکه‌های ایران و حملات سایبری علیه ایران در خبرهای سال گذشته دیده می‌شد. ادعای نفوذ به سیستم موشکی ایران پس از ساقط کردن پهپاد امریکایی، حمله سایبری به ایران پس از حملات موشکی به تاسیسات آرامکو و حملات منع دسترسی علیه شبکه اینترنت ایران که در سال گذشته چند بار اتفاق افتاد از این دست خبرها در سال گذشته بودند. با توجه به شرایط پر تنش ایران به‌خصوص در مقابل امریکا به نظر می‌رسد این رخدادها در سال پیش‌رو نیز ادامه داشته باشند. هرچند که ممکن است حجم تنش کاهش یابد، ولی باید برای دفاع سایبری آماده بود و شبکه‌ها و زیرساخت‌های سایبری خود را برای مقابله با تهدیدات سایبری تقویت کرد.

افشاگری‌های جدید از حملات قدیمی

در سال گذشته دو خبر مهم در مورد حملات قدیمی به کشور ما منتشر شد. اولین خبر در مورد نقش سرویس اطلاعاتی هلند در توزیع بدافزار استاکس‌نت بود. خبر بعدی نیز در مورد فروش اطلاعات سری کشورها به سرویس‌های جاسوسی آلمان و امریکا توسط شرکت تولیدکننده تجهیزات امن کریپتوای جی. با اینکه ده سال از تشخیص استاکس‌نت که هدف آن ایجاد اخلال در زیرساخت هسته‌ای ایران بود می‌گذرد، باز هم اخبار جدیدی از این بدافزار پیچیده شنیده می‌شود. در سال گذشته یاهونیوز گزارشی در مورد نقش کشورهای اروپایی در توزیع این بدافزار منتشر نمود. در گزارش یاهونیوز به نقش سرویس اطلاعاتی هلند در توزیع و انتشار ویروس استاکس‌نت اشاره شده است. به گفته یاهونیوز پنج کشور امریکا، اسراییل، هلند، فرانسه و آلمان با عنوان پروژه بازی‌های المپیک (۵ کشور یادآور ۵ حلقه نماد المپیک) در تولید و توزیع این ویروس با هدف اخلال در زیرساخت هسته‌ای کشور ما همکاری داشته‌اند. خبر دیگری که کشور ما را نیز تحت تاثیر قرار می‌دهد، پروژه کریپتوگیت است. شرکت سوییسی کریپتوای‌جی (Crypto AG) از فروشندگان تجهیزات رمزنگاری با مشتریانی در سراسر جهان است. ایران هم یکی از صدها کشور مشتری این شرکت بوده که از این تجهیزات برای ارتباطات امن استفاده می‌نموده است. سال گذشته گزارشی در مورد فراهم بودن امکان شنود این دستگاه‌ها برای سرویس‌های اطلاعاتی امریکا و آلمان برای سال‌ها منتشر شد. این گزارش که از آن به عنوان کودتای اطلاعاتی قرن نام برده شد، سر و صدای زیادی در سال گذشته به راه انداخت.

کلاه‌برداری، فیشینگ و قمار

رخدادهای مهم همیشه بستر خوبی برای کلاه‌برداری و سایت‌های فیشینگ بوده‌اند. سایت‌هایی که با بهانه‌های مختلف و موضوعات داغ روز، اقدام به سرقت و کلاه‌برداری از افراد می‌کنند. سال گذشته همزمان با انتشار خبرهایی همچون استفاده از کارت سوخت و یارانه معیشتی به سرعت سایت‌هایی جعلی برای سرقت اطلاعات بانکی کاربران تحت عنوان این موضوع‌ها ایجاد شدند. پیامک‌هایی که از افراد، اطلاعاتشان را درخواست می‌کرد یا آن‌ها را به سایت‌های فیشینگ راهنمایی می‌کردند، موارد دیگری هستند که در این رابطه مشاهده شد. البته رمز دوم پویا توانست تا حد زیادی از حملات فیشینگ بانکی جلوگیری کند. ولی معدود سایت‌هایی بودند که فیشینگ را حتی در شرایط رمز دوم پویا نیز انجام داده و توانسته بودند قربانی بگیرند. سهولت استفاده سایت‌های شرط‌بندی و قمار از درگاه‌های بانکی نیز یکی دیگر از ابهامات سال گذشته بود. به‌نظر می‌رسد که بایستی قوانین موجود در این حوزه بازنگری شده و نظارت بیشتری اعمال شود.

قطع اینترنت

پس از وقوع اتفاقات آبان ماه، شورای عالی امنیت ملی تصمیم به قطع اینترنت کشور گرفت. این تصمیم تبعات زیادی داشت. از کار افتادن بسیاری از کسب و کارها در دوران قطعی اینترنت، عدم دسترسی به بسیاری از سرویس‌های بیرون از کشور و به روز نشدن سیستم‌های داخلی تنها برخی از مشکلات این تصمیم بودند. اما این بدعت مشخص نمود که باید تا حد امکان وابستگی‌های غیرضروری را به شبکه خارج از کشور کم کرد تا در صورت تکرار، شاهد مشکلات کمتری بود. البته بایستی توجه داشت که تکرار این جنس تصمیم‌ها ممکن است افراد را به سمت دسترسی به اینترنت از راه‌های دیگری هدایت کند که تامین امنیت شبکه و کشور را با چالش‌های جدی‌تری روبرو می‌کند.

نشت اطلاعات

یکی از مهم‌ترین اتفاقات سال گذشته در حوزه امنیت

سایبری، نشت اطلاعات کاربران است. امروزه افراد به دلایل مختلف اطلاعات شخصی خود را در سامانه‌های مختلف وارد می‌کنند. کم‌ترین انتظار کاربران این است که از این اطلاعات به صورت امن نگه‌داری شود و در دسترس دیگران قرار نگیرد. اما به نظر می‌رسد که به‌دلیل عدم وجود قوانین تنبیهی، متاسفانه مساله امنیت اطلاعات کاربران ایرانی به اندازه کافی جدی گرفته نشده است. موارد متعدد نشت اطلاعات کاربران در سال گذشته موید این ادعا است. در اردیبهشت‌ماه ۹۸ خبری مبنی بر نشت اطلاعات کاربران کافه بازار منتشر شد. البته کافه بازار در پاسخ اعلام کرد که نفوذ به یکی از زیرسیستم‌های آن رخ داده و امنیت کاربران با خطر روبرو نشده است. کافه بازار از اینکه دچار چنین مشکلی شده است، عذرخواهی کرد.

در هفته دوم خردادماه سایت تامین اجتماعی هک شد. گروه هکری موسوم به تپندگان، عامل این حمله سایبری بودند. اما خوشبختانه در این حمله نیز اطلاعات کاربران افشا نشد. همچنین در سال گذشته اطلاعات شناسنامه‌ای و بانکی هزاران کاربر چندین سایت مبادله ارز نشت یافت. این سایت‌ها برای ارائه سرویس به کاربران خود، عکس کارت بانکی، کارت ملی و چهره شخص را در درخواست می‌کردند. دلیل این درخواست، عدم وجود یک سرویس تایید هویت مرکزی و قانون الزام تایید هویت کاربران است. البته سهل‌انگاری مدیران سایت‌ها در حفظ امنیت اطلاعات کاربران خود، کاملاً محرز است. در آذر ماه برخی کاربران ایمیل‌هایی دریافت کردند که حاوی اطلاعات بانکی بیش از ۱۰ میلیون کاربر بانک‌های ملت، تجارت و سرمایه بود. این اطلاعات شامل رمز کاربران نمی‌شد، ولی اطلاعات کارت بانکی و سایر اطلاعات کاربری در آن‌ها وجود داشت. بانک‌ها در مورد این نشت داده اظهار نظر ننمودند، ولی وزیر ارتباطات گفت این نشت داده از سمت یکی از پیمانکاران قبلی یک سیستم بانکی بوده و اطلاعات به روز نبوده است. این گزارش نشت داده که توسط شرکت امنیتی ClearSky منتشر شد، به تیتر اخبار نیویورک تایمز رسید. یکی دیگر از خبرهای مهم نشت اطلاعات، هک سایت فروش و رزرو بلیط و هتل علی‌بابا بود. علی‌بابا از کاربران خود بابت این مساله عذرخواهی کرد و از آن‌ها درخواست نمود که رمز عبور خود را تغییر دهند.

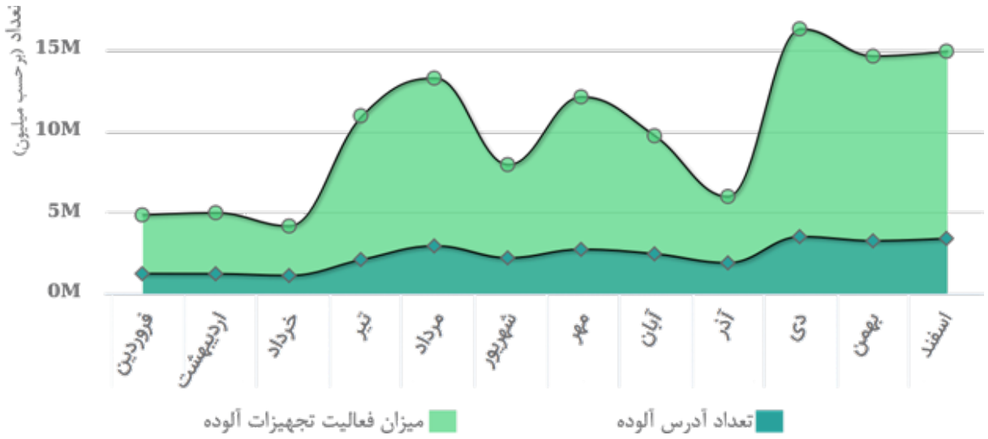
خبرهای افشای اطلاعات در سال ۹۸ کم نبود، ولی هیچ کدام به اندازه نشت اطلاعات ۴۲ میلیون کاربر ایرانی تلگرام در اولین روزهای سال ۹۹ خبرساز نشدند. در اولین روزهای فروردین ۱۳۹۹ خبری مبنی بر نشت اطلاعات کاربری ۴۲ میلیون کاربر ایرانی تلگرام منتشر شد که به صورت ناامن روی یک سرور با نام سامانه شکار نگهداری می‌شد. این خبر اولین دومینوی افشای اطلاعات سال ۹۹ بود و پس از آن خبر افشای اطلاعات ۵ میلیون کاربر سیب‌اپ، فروشگاه ایرانی برنامه‌های آیفون منتشر شد و هکرها اعلام کردند که این اطلاعات را به فروش می‌رسانند. سیب‌اپ نیز در واکنش به این خبر با انتشار بیانیه‌ای، ضمن عذرخواهی از کاربران، تنظیم اشتباه فایروال را دلیل افشای اطلاعات کاربران نامید.

دومینوی نشت اطلاعات سایت‌ها و سامانه‌های داخلی نشان از عدم توجه لازم به حفاظت از اطلاعات کاربران در سامانه‌ها دارد!

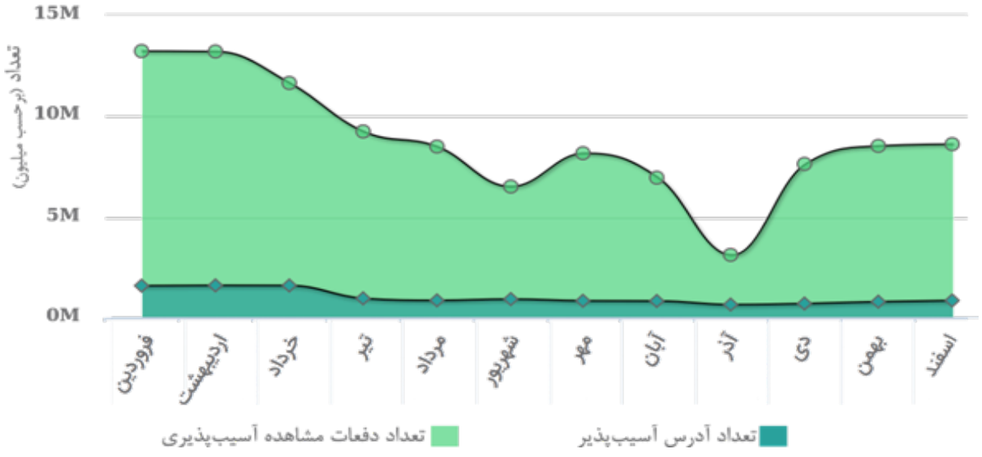
دومینوی سوم، انتشار اطلاعات ثبت احوال کاربران ایرانی بود. علت نشت این اطلاعات، استفاده ناامن از این اطلاعات در سامانه مقابله با کرونا توسط وزارت بهداشت اعلام شد. سخنگوی سازمان ثبت احوال این نشت اطلاعات را تایید کرده است. همچنین یک بات تلگرامی ادعا کرد که اطلاعات هویتی ۱۳۲ میلیون ایرانی، در قید حیات و درگذشته، را در اختیار دارد که شامل کدهای ملی، سن، شهر و در قید حیات بودن افراد است. هنوز مشخص نیست این اطلاعات از چه سامانه و یا سایتی نشت یافته است. نشت اطلاعات کاربران سایت رجا، سایت مخابرات ایران، نامه‌های اداری هواپیمایی‌های هما و ماهان و کاربران سایت سازمان امور دانشجویان کشور از دیگر اخبار حوزه نشت داده در کشور است که در زمان نگارش این متن منتشر شده، هرچند که هنوز توسط صاحبان و متولیان آن‌ها تایید نشده است. موارد اشاره شده تنها بخشی از مهمترین اخبار مهم راجع به افشای داده کاربران در سال گذشته بودند. روند رو به رشد افشای اطلاعات کاربران ایرانی نشان از این دارد که در این حوزه ضعف‌های زیادی در کشور وجود دارد. همچنین عدم وجود یک قانون مشخص در مورد حفاظت از اطلاعات کاربران و ایفای مناسب نقش رگولاتوری در این زمینه یکی از علل اصلی عدم توجه به امنیت اطلاعات کاربران است. قابل ذکر است قوانینی مثل قانون GDPR اتحادیه اروپا می‌تواند سهمی در ارتقاء امنیت اطلاعات کاربران داشته باشد.

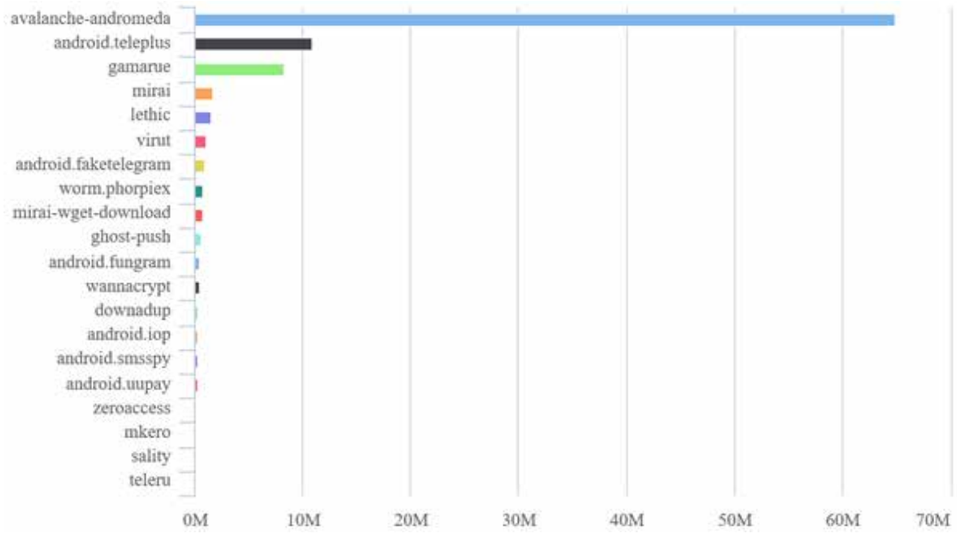
۳.۶ وضعیت امنیت کشور در سال ۱۳۹۸

سامانه ملی بینا، یکی از سامانه‌های سپر ملی دژفا است. این سامانه وظیفه دریافت، پردازش و اعلان گزارش آسیب‌پذیری‌ها و آلودگی‌های منتخب را برعهده دارد. نگاهی جامع به آمار سال ۱۳۹۸ جمع‌آوری شده توسط این سامانه (شکل ۱) نشان می‌دهد که در این سال، در مجموع ۹۱,۵۸۳,۷۱۱ مرتبه هشدار درخصوص مشاهده ترافیک مربوط به میزبان‌های آلوده به بدافزار مشاهده شده است. به‌طور متوسط، این تعداد در هر ماه مربوط به ۲۵ درصد از کل فضای آدرس **IP** کشور است. اما به‌خاطر تعداد زیاد کاربران خانگی آلوده که آدرس آن‌ها متناوباً تغییر می‌کند، در کل سال عملاً برای بیش از ۶۰ درصد از کل فضای آدرس IP کشور گزارش آلودگی دریافت شده است. نگاه دقیق‌تر به آمار نشان می‌دهد که تعداد آدرس‌های آلوده تقریباً در تمامی ماه‌ها روندی افزایشی داشته و از ۱,۲۳۲,۶۳۶ مورد در ماه فروردین به ۳,۳۹۸,۲۶۳ در ماه اسفند افزایش یافته است. اما در ماه مرداد از فصل تابستان و ماه مهر از فصل پائیز و کلیه ماه‌های فصل زمستان بر میزان فعالیت تجهیزات آلوده افزوده شده است.



از نظر تعداد آسیب‌پذیری نیز در سال گذشته درمجموع ۹۳,۱۱۴,۱۲۱ مرتبه هشدار درخصوص آدرس‌های دارای آسیب‌پذیری‌های منتخب (اغلب از نوع پیکربندی نامناسب) ثبت شده است. این تعداد مربوط به ۳۰ درصد از کل آدرس‌های IP کشور در طول سال است.



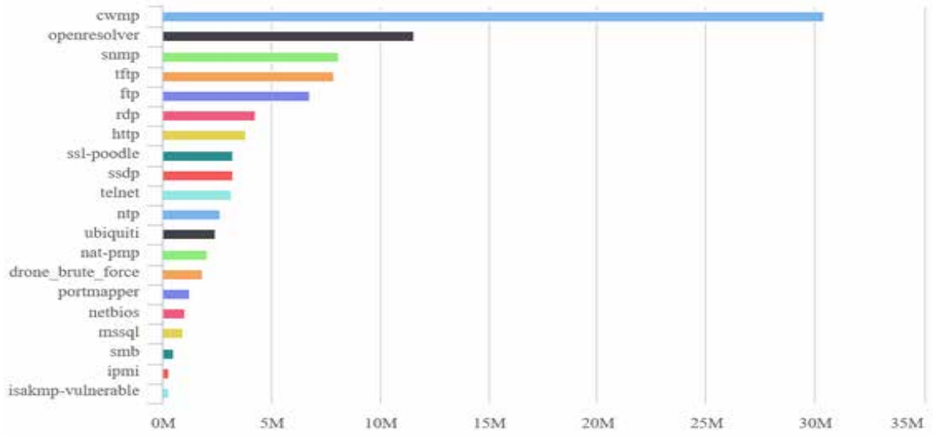


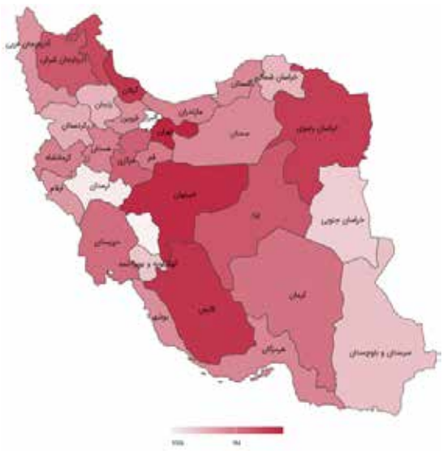
نگاه دقیق‌تر به نمودارهای صفحه قبلی نشان می‌دهد که خوشبختانه تعداد آدرس‌های آسیب‌پذیر دارای شیب نزولی بوده و از ۱,۵۹۱,۹۷۹ مورد در ماه فروردین به ۸۵۸,۷۷۹ مورد در ماه اسفند کاهش یافته است. بررسی آلودگی‌ها نیز نشان می‌دهد که بات avalanche-andromeda با بیش از ۶۴,۸۷۵,۳۷۰ مورد گزارش به عنوان پرتکرارترین بدافزار سال ۱۳۹۸ در سطح کشور مطرح بوده است. android.teleplus و gamarue در رده‌های دوم و سوم قرار دارند. در جدول ۱، تعداد دفعات گزارش ثبت شده برای ده عدد از فعال‌ترین بدافزارهای کشور آورده شده است.

ردیف	نام بدافزار	تعداد دفعات گزارش
۱	avalanche-andromeda	۶۴,۸۷۵,۳۷۰
۲	android.teleplus	۱۰,۸۶۵,۵۹۷
۳	gamarue	۸,۳۶۱,۵۶۱
۴	mirai	۱,۷۵۲,۵۱۸
۵	lethic	۱,۵۲۳,۹۳۸
۶	virut	۱,۱۲۸,۶۴۹
۷	android.faketelegram	۹۰۷,۹۳۱
۸	phorpiex	۷۵۰,۰۵۱
۹	mirai-wget-download	۷۲۰,۵۲۲
۱۰	ghost	۶۵۹,۴۲۸

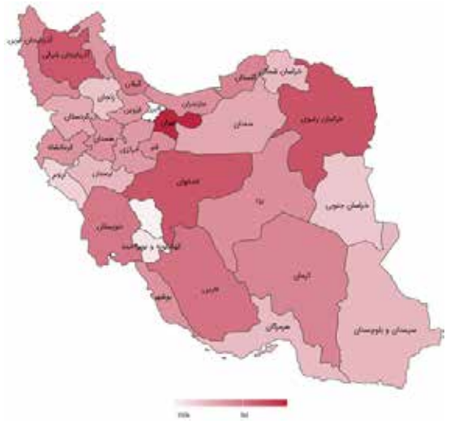
از نقطه نظر آسیب‌پذیری نیز پروتکل لایه کاربردی cwmp در صدر جدول قرار دارد. سرویس‌دهنده‌های DNS دارای پیکربندی نامناسب و تجهیزات دارای پیکربندی نامناسب SNMP در رده‌های دوم و سوم قرار دارند.

ردیف	نام آسیب‌پذیری	تعداد دفعات گزارش
۱	cwmp	۳۰,۴۳۵,۹۸۸
۲	openresolver	۱۱,۵۴۷,۸۹۰
۳	snmp	۸,۱۴۲,۰۰۸
۴	tftp	۷,۸۷۶,۳۶۵
۵	ftp	۶,۷۵۲,۹۰۸
۶	rdp	۴,۲۸۰,۰۲۹
۷	http	۳,۸۵۵,۳۱۶
۸	ssl-poodle	۳,۲۵۸,۳۸۳
۹	ssdp	۳,۲۵۷,۰۲۸
۱۰	telnet	۳,۱۴۷,۳۹۳





از نظر پراکندگی آدرس‌های آلوده به بدافزار، استان تهران دارای رتبه اول (بیش از ۵۳ میلیون گزارش) و استان‌های خراسان رضوی (بیش از ۲ میلیون گزارش) و اصفهان (بیش از یک میلیون و هشتصد هزار گزارش) در رتبه‌های دوم و سوم قرار دارند. کمترین تعداد گزارش آلودگی به بدافزار ثبت شده در کل کشور نیز مربوط به استان‌های چهارمحال و بختیاری (با ۷۰,۷۷۳ مورد) و کهکیلویه و بویراحمد (با ۹۲,۶۲۴ مورد) است.



از نظر آدرس‌های آسیب‌پذیر، مجدداً استان تهران با بیش از ۵۷ میلیون مورد گزارش آسیب‌پذیری در صدر جدول قرار داشته و استان‌های اصفهان (بیش از ۵ میلیون مورد گزارش) و گیلان و فارس (بیش از ۴ میلیون گزارش) در رتبه‌های بعدی قرار دارند. کمترین تعداد گزارش آسیب‌پذیری ثبت شده در کل کشور نیز مربوط به استان‌های چهارمحال و بختیاری (با ۸۸,۴۳۸ مورد) و لرستان (با ۱۰۴,۷۱۱ مورد) است.

بیشترین تعداد گزارش آلودگی به بدافزار ثبت شده در سامانه مربوط به آدرس با ۱۶ رقم اول 5.202 است. برای این آدرس، ۳,۱۸۰ مرتبه گزارش آلودگی در سال ۱۳۹۸ ثبت شده است. در جدول ۳ فهرست مبهم‌سازی شده ده آدرس IP کشور آورده شده است که بیشترین گزارش‌های آلودگی به بدافزار را داشته‌اند.

ردیف	IP	شهر	تعداد گزارش آلودگی
۱	5.202.x.x	تهران	۳,۱۸۰
۲	151.239.x.x	تهران	۱,۹۶۴
۳	151.239.x.x	تهران	۱,۴۰۵
۴	31.58.x.x	سمنان	۱,۲۸۳
۵	82.99.x.x	کرج	۱,۱۴۲
۶	151.239.x.x	بندرانزلی	۱,۰۵۱
۷	185.168.x.x	تهران	۱,۰۱۰
۸	93.119.x.x	تهران	۹۹۱
۹	46.225.x.x	گلستان	۹۷۳
۱۰	185.109.x.x	بندر بوشهر	۹۵۲

۷

چشم‌انداز سال ۱۳۹۹

چشم‌انداز فضای سایبری در سال پیش رو و توصیه‌هایی برای افزایش
امنیت بیشتر در سال جدید

۷ چشم‌انداز سال ۱۳۹۹

۱.۷ روند تهدیدات سایبری در سال جدید

با بررسی اتفاقات سال گذشته و بررسی روندهای حوادث و حملات سایبری می‌توان نگاهی به آینده تهدیدات سایبری در سال جدید داشت. در ادامه پیش‌بینی تهدیدات سایبری در سال جدید بر اساس نظرات محققین امنیت سایبری را مرور می‌کنیم.

باج‌افزارهای هدفمند

همانطور که قبلا نیز گفته شد اگرچه روند شیوع باج‌افزارها به صورت کلی در سطح جهان با کاهش جدی روبرو بوده است، ولی به نظر می‌رسد مجرمان سایبری از این دسته بدافزارها با اهداف مشخص، بیشتر استفاده می‌نمایند. بنابراین پیش‌بینی می‌شود سازمان‌ها و صنایع در سال جدید، قربانیان حملات باج‌افزاری باشند. همچنین تهدید به انتشار داده‌های قربانیان حملات باج‌افزاری، یکی از حربه‌های جدید مجرمین سایبری به منظور دریافت باج از قربانیان بوده و به نظر می‌رسد این رویه در سال جدید ادامه یابد. از سوی دیگر بررسی‌ها نشان می‌دهد، حملات باج‌افزاری دیگر منحصر به کامپیوترهای شخصی نبوده و همه تجهیزات هوشمند متصل به اینترنت مانند تلویزیون‌های هوشمند، ساعت‌های هوشمند، تجهیزات خانه هوشمند، خودروهای هوشمند و... را مورد هدف قرار خواهند داد.

حملات زیرساختی

بررسی‌ها نشان می‌دهد در سال‌های اخیر، نفوذ به زیرساخت شبکه بیش از پیش مورد توجه مجرمین سایبری قرار گرفته است. بر این اساس گروه‌های هکری با تسخیر تجهیزات شبکه در صدد در اختیار گرفتن شبکه‌ها بر می‌آیند تا در زمان مناسب از این شبکه برای حملات بات و یا سایر حملات مخفیانه استفاده نمایند. آشکار شدن نفوذ گروه‌های هکری به چندین شبکه سلولی مخابراتی در سطح جهان در سال‌های اخیر و سوء استفاده از آن یک گواه جدی بر این مدعا است. همچنین در سال‌هاج اخیر با توسعه اینترنت اشیا، حملات زیرساختی جذابیت بیشتری برای مجرمین سایبری ایجاد کرده است. در همین راستا نفوذ به شبکه زیرساخت‌های حساس کشورها در سال گذشته مورد توجه جدی قرار گرفت، ربودن اطلاعات حساس از یکی از آزمایشگاه‌های ناسا با استفاده از یک Rasbperry Pi و نیز اختلال در خطوط هوایی برخی کشورها مانند انگلستان به خاطر پرواز غیر منتظره پهپاد در مسیر هوایی فرودگاه (که گفته شده است به خاطر یک حمله سایبری بوده است) نمونه‌هایی از تحت تاثیر قرار گرفتن سازمان‌های حساس کشورها به خاطر حملات زیرساختی سایبری بوده است. شاید بتوان اختلال در عملکرد پدافند غیرعامل برخی کشورها در موقعیت‌های حساس در این سال‌ها را نیز در همین راستا مورد بررسی قرار داد. به هر حال به نظر می‌رسد توجه به این حملات زیرساختی بایستی بیش از پیش در سال آینده مورد رصد قرار گیرد.

گروه‌های هکری با تسخیر تجهیزات شبکه به دنبال در اختیار گرفتن شبکه‌ها هستند!

روش‌های تکامل یافته در حملات سایبری

به دنبال توسعه راه‌کارهای دفاعی، مجرمین سایبری از روش‌های جدیدتر و پیچیده‌تری در آینده استفاده خواهند کرد. به عنوان نمونه استفاده از مکانیزم‌های جداسازی و انزوا در نرم‌افزارهای Microsoft word و سایر نرم‌افزارها که زمانی طعمه مناسبی برای اجرای حملات فیشینگ هدفمند، محسوب می‌شدند هکرها را به سمت و سوی استفاده از روش‌های جدیدتری مانند Quantum Insert به منظور انتشار بدافزارها سوق داده است. همچنین استفاده از روش‌های نامتعارف به منظور دسترسی به داده‌ها مورد توجه جدی‌تر از سوی هکرها قرار گرفته است. استفاده از مکانیزم‌های سیگنالینگ در شبکه‌های wifi و 4G در این راستا مشاهده شده است. بدین ترتیب به نظر می‌رسد در آینده، استفاده از روش‌های DOH یا DNS over HTTPS به منظور پنهان‌سازی رفتار مهاجمین، بیش از پیش مورد استفاده قرار خواهد گرفت. گروه‌های هکری همچنین تلاش بیشتری خواهند داشت تا در مسیر زنجیره تامین سامانه‌ها در آن‌ها نفوذ داشته باشند. به عنوان نمونه، نفوذ در کتابخانه‌های مورد استفاده در سامانه‌ها، فرآیند کشف یک عملیات مخرب را به شدت دشوار می‌سازد. به هر حال آگاهی از آخرین روش‌های مورد استفاده توسط مجرمین سایبری می‌تواند باعث آمادگی هرچه بیشتر متخصصین امنیت سایبری در برابر حوادث احتمالی و تلاش برای پیشگیری از وقوع آن‌ها شود.

موبایل‌های هوشمند، قربانیان رو به رشد حملات سایبری

در سال‌های اخیر حجم بیشتری از اطلاعات افراد در موبایل‌های هوشمند ذخیره می‌شود و این تجهیزات هوشمند بیش از پیش در زندگی تک تک افراد نقش ایفا می‌نمایند. بنابراین به صورت طبیعی، موبایل‌های هوشمند نسبت به کامپیوترهای شخصی به اهداف جذاب‌تری برای مجرمین سایبری بدل شده‌اند. افزایش حجم سرمایه‌گذاری گروه‌های هکری برای در اختیار گرفتن آسیب‌پذیری‌های روز صفرم سیستم‌عامل‌های موبایل بر صحت این گزاره تاکید می‌کند. به هر حال به نظر می‌رسد در سال جدید، روند افزایشی تهدیدات سایبری بر روی تجهیزات موبایل هوشمند ادامه یافته و بایستی در کنار آگاهی‌بخشی بیشتر به کاربران این تجهیزات، رعایت الزامات امنیتی بر روی این تجهیزات، بیش از پیش مورد توجه قرار گیرد.

تهدیدات فناوری‌های نوظهور

نسل پنجم شبکه‌های موبایل، با فراهم ساختن پهنای باند بسیار زیاد می‌تواند زمینه راه‌اندازی حملات سایبری با حجم بیشتر توسط گروه‌های هکری را ایجاد نماید. از سوی دیگر با توجه به فراگیر شدن فناوری‌های نسل پنجم در سراسر جهان، امکان سوء استفاده از آسیب‌پذیری‌های احتمالی آن بیشتر فراهم خواهد شد. هوش مصنوعی و یادگیری ماشین یکی از فناوری‌های نوین و روبه‌رشد و جذاب سال‌های اخیر به حساب می‌آید، استفاده بیش از پیش از این فناوری، زمینه تهدیدات سایبری تازه‌ای را فراهم خواهد ساخت. آسیب‌پذیری‌های موجود در پیاده‌سازی‌های گوناگون این فناوری در سامانه‌ها و تجهیزات گوناگون، توجه هکرها را بیش از پیش به سوء استفاده از آن‌ها جلب خواهد کرد. یکی از نمونه‌های جالب توجه در این راستا فناوری جعل عمیق یا deep fake است. در این روش تصاویر و فیلم‌های موجود بر روی تصاویر یا فیلم‌های منبع قرار داده می‌شود و با استفاده از روش‌های یادگیری ماشین یک ویدیوی جعلی از ترکیب فیلم‌های موجود و منبع ایجاد می‌گردد که در آن فرد یا افرادی را در حال انجام یک کار در موقعیتی نشان می‌دهد که هرگز در واقعیت اتفاق نیفتاده است. این فناوری یکی از جدی‌ترین تهدیدات سایبری از نوع جعل در سال‌های آینده خواهد بود.

۲.۷ توصیه‌های امنیتی عمومی برای سازمان‌ها

بررسی مهمترین حوادث سایبری در سال گذشته و مطالعه روند تهدیدات سایبری در سال جدید نشان می‌دهد همه سازمان‌ها و کسب و کارها به شکل‌های گوناگون در معرض حملات و حوادث سایبری هستند. اما به نظر می‌رسد درصد کمی از سازمان‌هایی که با شواهدی مبنی بر حادثه سایبری روبرو بوده‌اند درخواست سرویس رسیدگی به حادثه داشته‌اند. به نظر می‌رسد این عدد در میان سازمان‌های کشور ما بسیار کمتر باشد. این مسئله بایستی به صورت جدی از سوی نهادهای متولی امنیت سایبری کشور مد نظر قرار گیرد و با به کارگیری تمهیداتی، ضمن الزام تشکیل گروه‌های پاسخ سریع به حوادث در سازمان‌ها، راهکارهایی را به منظور ارایه سرویس امداد سایبری به سازمان‌ها فراهم سازند. در این بخش با دسته‌بندی حوادث سایبری در سازمان‌ها، توصیه‌های امنیتی پیشنهادی به منظور پیشگیری از حملات و حوادث سایبری ارایه می‌شود.

توصیه‌های عمومی

- در پیش گرفتن یک برنامه دفاع سایبری منسجم بر اساس استانداردهای موجود در سازمان
- پیاده‌سازی روال رسیدگی سریع به حوادث سایبری
- انجام ارزیابی امنیتی در دوره‌های زمانی منظم برای همه زیرساخت فناوری اطلاعات سازمان
- اجرای برنامه آموزش و آگاهی‌رسانی سایبری در سازمان
- پیاده‌سازی روال مدیریت وصله متمرکز به منظور به‌روزرسانی همه میزبان‌ها در شبکه سازمان
- راه‌اندازی یک راهکار تحلیل ترافیک شبکه
- پشتیبان‌گیری خودکار داده‌ها بر روی تجهیزاتی که قابلیت نوشتن بعد از آن نداشته باشد.

توصیه‌های ویژه بر اساس منشا حملات سایبری

بر اساس بررسی‌های انجام شده، سرویس RDP به عنوان منشا اولیه در بسیاری از حملات سایبری مورد استفاده قرار گرفته است. در اغلب موارد مهاجم با استفاده از نتایج یک حمله جستجوی کامل بر روی سرویس RDP، با اطلاعات یک کاربر موجه به سیستم ورود پیدا کرده است. این حملات به طور معمول به دلیل استفاده از گذرواژه‌های ضعیف، پس از چند ساعت به نتیجه رسیده است. بر این اساس، مهاجم پیش از شروع حمله ابتدا دسترسی را به دست آورده است. در این موارد با استفاده از روش‌های مهندسی اجتماعی و یا با استفاده از منابع ناامن که دسترسی عمومی در آن‌ها وجود داشته است، به این اطلاعات کاربری دست پیدا کرده است(به عنوان نمونه مواردی وجود داشته است که یک کارمند از یک گذرواژه در چندین محل استفاده کرده بوده است). ۳۳ درصد حملات به دلیل کمبود آگاهی امنیتی در بین کارکنان سازمان‌ها رخ داده است. دانلود یک فایل و یا باز کردن یک لینک مخرب سبب نفوذ یک فایل مخرب و یا نفوذ یک هکر به شبکه سازمان شده است. بنابراین آموزش امنیت فناوری اطلاعات برای کارکنان و ارایه هشدارهای به موقع می‌تواند امکان موفقیت حملات ناشی از مهندسی اجتماعی را به شدت کاهش دهد.

به منظور پیشگیری از وقوع این حملات توصیه‌های زیر پیشنهاد می گردد:

- محدود ساختن دسترسی به هر رابط مدیریت از راه دور به یک آدرس IP خاص. این رابط‌ها تنها بایستی از تعداد محدود و مشخصی ماشین قابل دسترسی باشند. از راه‌کارهای شخص ثالث به منظور رمزنگاری استفاده نمایید.
- سیاست سختی برای گذرواژه‌ها در سیستم‌های فناوری اطلاعات سازمان اعمال نمایید.
- از سیاست حداقل دسترسی ممتاز استفاده نموده و از استفاده از حساب‌های کاربری با دسترسی ممتاز در هر محل اجتناب بورزید.
- سیستم احراز هویت دوعاملی را در سازمان مستقر نمایید.
- از نرم‌افزارهای امنیت نقاط نهایی بر روی همه میزبان‌های موجود در شبکه استفاده نمایید و از به روز بودن آن‌ها اطمینان حاصل کنید.
- از یک سندباکس به منظور تحلیل هر فایل دانلود شده از منابع خارجی استفاده نمایید.
- به مقوله آگاهی‌رسانی امنیت سایبری در بین کارکنان، مدیران و کارشناسان فناوری اطلاعات در سازمان توجه ویژه‌ایی داشته باشید. این کار بایستی با برگزاری جلسات آگاهی‌رسانی امنیت سایبری در دوره‌های زمانی منظم انجام پذیرد.

باج‌افزارها

به نظر می‌رسد در طول سال گذشته در میان حوادث سایبری، بیشترین درخواست‌های رسیدگی به حادثه مربوط به حوادث باج‌افزاری بوده است. شاید بتوان رشد سریع، دشواری در تشخیص زودهنگام و بارز بودن عواقب آن را از دلایل این حجم از درخواست در میان قربانیان دانست.

پیشگیری

برای کاربران

- از سامانه‌ها و برنامه‌های امنیتی مناسب، قدرت‌مند و به‌روز روی سیستم‌های خود استفاده نمایید.
- برنامه‌ها و سیستم‌عامل‌های خود را به‌روز نگه دارید.
- ضمیمه‌ها و فایل‌های مشکوک ایمیل را باز نکنید.
- فایل‌های مورد نظر خود را از منابع معتبر و مطمئن دانلود نمایید.
- از اطلاعات حساس خود نسخه پشتیبان تهیه کنید.

برای سازمان

- از نصب و به‌روز بودن آنتی‌ویروس و ضد باج‌افزار روی همه سیستم‌های سازمان اطمینان حاصل نمایید.
- تنظیمات امنیتی لازم را روی پورت‌ها و دسترسی‌های مربوطه انجام دهید.
- از به‌روز بودن برنامه‌های همه سیستم‌ها اطمینان حاصل نمایید.
- تنظیمات امنیتی سرور ایمیل را به منظور دریافت کمترین هرزنامه‌ها انجام دهند.
- سیستم پشتیبان‌گیری خودکار از داده‌ها را در سازمان راه‌اندازی نمایید.

پس از کشف حادثه

- جداسازی میزبان و بخشی از شبکه که حادثه در آن رخ داده است به منظور جلوگیری از پیشرفت حمله
- گرفتن snapshot از RAM و یک image از هارد دیسک به منظور بررسی‌های جزیی‌تر در آینده
- بررسی فایل‌های رمزشده به منظور تشخیص نوع بدافزار، این کار زمینه انجام مجموعه‌ایی از اقدامات اولیه برای پاسخ به رخداد را فراهم می‌سازد.
- بررسی دقیق‌تر حادثه به منظور یافتن عوامل اولیه حمله و یافتن درب پشتی‌های احتمالی در جهت جلوگیری از بازرخداد حادثه

مرکز تخصصی آپا دانشگاه صنعتی اصفهان

۵۲

مرکز تخصصی آپا
دانشگاه صنعتی اصفهان

بهار ۱۳۹۹