بسمه تعالی

امنیت سایبری در سال ۲۰۲۰ و پس از آن

گزارش فنی

شناسه سند ..... TR_CyberSecurity2020_13981223

نوع سند ..... گزارش فنی

شماره نگارش ۱/۰

تاریخ نگارش ۱۳۹۸/۱۲/۲۳

طبقه‌بندی سند ..... **عادی**

شاهرود، میدان هفت تیر، بلوار دانشگاه، دانشگاه صنعتی شاهرود، مرکز تخصصی آپا، کد پستی: ۳۶۱۹۹۹۵۱۶۱

(۰۲۳) ۳۲۳۹-۲۲۰۴ (۰۲۳) ۳۲۳۰-۰۲۵۱ cert.shahroodut.ac.ir

فهرست مطالب

چکیده

سال ۲۰۱۹ یک سال غیر قابل پیش‌بینی برای جرائم سایبری بوده است؛ با توجه به جذابیت جرائم سایبری که مدام در حال افزایش‌اند، دورنمای خطراتی که در سال ۲۰۲۰ امنیت سایبری را تهدید می‌کنند، وعده‌ی چالش‌های جدید را می‌دهد. وقتی صحبت از امنیت سایبری می‌شود، پیش‌بینی تهدیدات در مقایسه با واکنش مقابل آن‌ها دارای اهمیت بالاتری است. در یک چشم انداز کلی، تهدیدات به طور مداوم در حال تغییر و تحول است؛ وصله کردن رخنه‌ها و یا انجام به‌روزرسانی‌ها در مقابل تهدیدات دیروز، دیگر کافی نیست. انتظار می‌رود در سال ۲۰۲۰ شاهد افزایش برخی حملات باج‌افزارها، حملات فیشینگ، کلاهبرداری‌های web skimming، exploit kitها و... باشیم.

کلمات کلیدی: امنیت سایبری، باج‌افزار، فضای ابری، مهاجم

۱ مقدمه

با پایان سال ۲۰۱۹، با دانش بیشتری در مورد مهاجمان و تهدیداتی که می‌توان در سال ۲۰۲۰ و پس از آن انتظار داشت عمل خواهیم کرد. در سال‌های اخیر مهاجمان نوآوری و رشد بیشتری داشته‌اند، به همین دلیل برای مقابله با تهدیدات پیش رو بایستی اقدامات لازم صورت گیرد.

در این گزارش به بررسی نظرات مدیران شرکت fireeye، آزمایشگاه Pradeo و آزمایشگاه Malwarebytes در مورد چشم‌انداز امنیت فضای مجازی در سال ۲۰۲۰ می‌پردازیم.

۲ آمادگی برای سال ۲۰۲۰

۲-۱ تغییر امنیت فضای ابری

استفاده از فضای ابری چشم انداز فناوری اطلاعات را بطور کلی تغییر داده و همچنان باعث تغییر خواهد شد. فراگیری رایانش فضای ابری از سرویس‌های تحت وب تا نرم‌افزارها و سپس زیرساخت فضای ابری عمومی، به مرور جای خود را در دنیای فناوری اطلاعات باز کرده است. تا چند سال دیگر مدل‌های سنتی در مراکز داده کاملاً متحول شده و پردازش و تخصیص منابع و ذخیره‌سازی مبتنی بر فناوری‌های رایانش فضای ابری خواهد بود. در این میان سازمان‌های دولتی و نهادهای حکومتی همچنان در ورود به دنیای رایانش فضای ابری تعلل می‌کنند. دغدغه‌های امنیتی و پروتکل‌های دست و پاگیر سازمان‌ها، هر تحول نوآورانه‌ای را با کندی غیر معمول روبه‌رو می‌کند، اما فناوری اطلاعات به هر حال راه خود را به هر سازمانی باز می‌کند. بر

اساس بررسی Cloud Security Alliance (CSA)، کسب‌وکارها به واسطه مقیاس‌پذیری و خودکارسازی وصله امنیتی خود، به سمت ERP فضای ابری گرایش پیدا کرده‌اند. تقریبا دو سوم کسب وکارها تصمیم به انتقال سیستم برنامه‌ریزی منابع سازمان (ERP) خود به سمت فضای ابری گرفته‌اند و یا اینکه این کار را انجام داده‌اند؛ البته هنوز هم چالش‌ها و مشکلاتی در ارتباط با انتقال اطلاعات حساس به فضای ابری، وجود دارند. با برقراری امنیت در فضای ابری وظیفه‌ی سنگین ایجاد امنیت از دوش کاربران برداشته می‌شود. روی آوردن به امنیت در فضای ابری باید به نخستین خط دفاعی یک استراتژی امنیت یکپارچه تبدیل شود. پیاده‌سازی فایروال‌ها، گذرواژه‌های قدرتمند، امنیت داخلی دستگاه‌ها و آموزش کارمندان همگی المان‌های حیاتی یک «دفاع عمیق» هستند. داشتن این رویکرد جامع در تضمین امنیت شبکه‌ی سازمان بسیار مؤثر است. این موضوع در سال ۲۰۲۰ نیازمند تجدید نظر و تفکر توسعه یافته است.

از آن‌جا که سازمان‌ها به طور فزاینده‌ای به نرم‌افزار و راه‌حل‌های فضای ابری وابسته شده‌اند، بسیاری از آن‌ها به تدریج کنترل بر دسترسی به منابع فضای ابری مختلف خود را از دست داده‌اند؛ که باعث می‌شود هکرها از این مسئله برای حملات خود استفاده کنند. در حال حاضر، آمارها حاکی از آن است که ۵۲ درصد از این‌گونه سازمان‌ها در سال گذشته دچار حمله شده‌اند. این تعداد احتمالاً در سال ۲۰۲۰ افزایش خواهد یافت. در اکثر موارد، ایجاد یک سیاست امنیتی واحد برای کنترل دسترسی به فضای ابری، کافی نیست.

استفاده از خدمات اشتراکی و فضای ابری در حال انفجار است و این خدمات همواره تحت حمله مداوم قرار دارند، نوع حملات پیچیده‌تر و روش‌های شناسایی بسیار سخت‌تر خواهند بود. همچنین هدف‌های حمله جدید ظاهر می‌شوند، این بدان معناست که خطرات و آسیب‌های احتمالی در این حوزه که می‌توانند ایجاد شوند، در حال رشد هستند.

تقریبا ۲۰ سال از ظهور فضای ابری و خدمات آن برای سازمان‌ها می‌گذرد؛ و می‌توان ادعا کرد که فضای ابر ایمن است. حال باید به چگونگی ایمن سازی فضای ابر، کار با سیستم‌های فضای ابری و شکاف‌های مهارتی که باعث افزایش خطر در هنگام استفاده نادرست از فضای ابر می‌شود بپردازیم. اولین قدم برای اطمینان از امنیت فضای ابری در سال ۲۰۲۰، امنیت ایمیل و سپس شناسایی محیط ابری مورد استفاده است.

امروزه شاهد افزایش قابلیت‌های امنیتی در فضای ابری هستیم. مشتریان بیشتر از قبل به استفاده از فضای ابری روی آورده‌اند؛ همچنین از چندین شرکت ارائه دهنده فضای ابری استفاده می‌کنند[۱]. بنابراین تامین امنیت فضای ابری برای ارائه دهندگان فضای ابری چالش برانگیزتر خواهد بود. به عنوان متخصصان امنیتی،

[۱] چند ابری متشکل از ابرهایی است که توسط ارائه دهندگان مختلف پذیرفته شده است.

باید این پیچیدگی را درک کنیم، با برنامه‌های امنیتی خود مطابقت داشته و در این چالش‌ها جلوتر از شرکای تجاری خود باشیم.

۲-۲ امنیت موبایل

امنیت موبایل در دو سال گذشته تبدیل به موضوع اصلی برای تیم‌های امنیتی شده است؛ امروزه بیشتر افراد از دستگاه‌های تلفن همراه برای مقاصد کاری خود استفاده می‌کنند. با دستکاری دستگاه‌های تلفن همراه کنترل نشده یکی از افراد سازمان، داده‌های سازمان در خطر انتشار قرار خواهد گرفت. این مسئله به مهاجمان کمک می‌کند که اطلاعات سازمان‌ها را از طریق تلفن‌های همراه شخصی بدزدند. در نتیجه تیم‌های امنیتی به دنبال راه‌حل‌هایی خواهند بود که در صورت دستیابی به تلفن همراه، ایمنی داده‌ها را تضمین کند.

۲-۳ تقویت مهارت‌ها

زمان زیادی برای تغییر روش یک سازمان و انتقال به فضای ابری نیاز است، حتی در مورد سازمان‌هایی که این کار را به بهترین نحو خود انجام می‌دهند حدود یک سال و نیم به طول می‌انجامد تا کل داده‌ها را به فضای ابری منتقل کند.

پیدا کردن نیروی ماهر در حوزه فضای ابری سخت است- اما پیدا کردن نیروی ماهر در حوزه امنیت فضای ابری سخت‌تر است. فقدان مهارت‌ها باعث عقب راندن حتی ماهرترین مراکز عملیات امنیتی (SOC)[۲] خواهد شد. محیط فضای ابری فرآیندهای متفاوتی در زمینه‌های نظارت، تشخیص هویت، پیکربندی و فرآیندهای رمزنگاری دارد. مشتریانی که سعی در انتقال یک برنامه امنیتی به فضای ابری دارند، مجموعه جدیدی از چالش‌ها را تجربه خواهند کرد. بدین منظور باید از تفاوت‌های بین فضای ابری و سایر محیط‌ها آگاه بوده، روی مهارت‌های امنیتی فضای ابری تمرکز کرده و از بررسی منظم امنیت در محیط‌های فضای ابری اطمینان حاصل شود.

[۲] Security Operations Center (SOC) یک تیم بسیار ماهر است که ماموریت آن‌ها نظارت دائم و بهبود وضعیت امنیتی یک سازمان است که اینکار را با شناسایی، آنالیز، جلوگیری و پاسخگویی به حوادث امنیتی انجام می‌دهند و برای این کار از تکنولوژی، فرآیندها و مراحل کمک می‌گیرند.

۲-۴ پیشرفت نفوذگران

طی سال‌های اخیر مهاجمان نوآوری و رشد بیشتری داشته‌اند؛ آن‌ها خلاق‌تر و پیشرفته‌تر می‌شوند و به طور مداوم تکنیک‌های حمله خود را پیچیده‌تر می‌کنند؛ همچنین آن‌ها سطح وسیعی از کشورها را در اختیار دارند. چشم‌انداز امنیت سایبری با سرعت زیادی در حال پیشرفت است.

۲-۵ بهداشت امنیتی

بهداشت امنیتی به اقداماتی گفته می‌شود که کاربران کامپیوتر و سایر دستگاه‌ها برای برقراری و بهبود امنیت آنلاین انجام می‌دهند. بهداشت یکی از موضوعاتی است که بسیاری از افراد به آن بی اعتنا هستند؛ با این حال، برای امنیت بسیار اساسی است و باید با گسترش خدمات، مجدداً مورد توجه قرار گیرد. انتظار می‌رود که در سال ۲۰۲۰ سازمان‌های بیشتری به علت مدیریت ناکارآمد، به افشای داده‌های موجود، داده‌های حساس، پیکربندی‌ها و مؤلفه‌های امنیتی قابل اعتماد بپردازند.

۲-۶ تفکر بدون محدودیت کارمندان

امروزه در سازمان‌ها به افرادی نیاز داریم که تفکر خلاقانه داشته باشند؛ تفکر انتقادی و ترکیب داده‌ها از جمله مهارت‌هایی هستند که طی سال‌های متمادی توسعه یافته و به راحتی قابل آموزش نیستند، در حالی که مهارت‌های فنی دیگری که ممکن است بسیاری از افراد تصور کنند نیاز به سال‌ها آموزش دارند، در حقیقت در یک دوره زمانی کوتاه‌تر به دست می‌آیند. به عنوان رهبران امنیتی، باید بدون محدودیت فکر کنیم؛ همچنین باید در ایده‌های خود در مورد مسائل امنیتی سازمان، ویژگی‌های محیط و کارمندان، تجدید نظر کنیم.

۲-۷ مراقبت از زنجیره تامین

زنجیره تامین فروشندگان تا حد زیادی قابل اطمینان نیست. عدم شفافیت در جزئیات یک محصول می‌تواند منجر به افشای اطلاعات گسترده‌ای شود؛ به خصوص اگر وابسته به یک عملکرد امنیتی خاص باشد و یا نیاز به دسترسی به داده‌هایی داشته باشد که غیرقابل دسترسی یا آسیب‌دیده شده باشند. بدین ترتیب شخصی باید در برخی از مواقع، مسائل امنیتی را بررسی کند.

بخش اعظمی از کد مورد استفاده در محیط‌های ابری با استفاده از کدهای متن باز ساخته شده است. در چند سال گذشته شاهد موقعیت‌هایی بودیم که اجزای نرم‌افزار در به روزرسانی‌های خودکار با کد مخرب آلوده شده است. در سال ۲۰۲۰ و پس از آن، این خطر بیشتر خواهد شد؛ زیرا افراد بیشتری توانایی ایجاد زنجیره‌های تأمین نرم‌افزار را دارند. در حالی که امکان بررسی کلیه کدهای ارائه شده توسط کلیه فروشندگان

یا ارائه دهندگان خدمات امری غیرممکن است، یکی از راه‌های نظارت بر مواجهه‌های احتمالی استفاده از برند مرغوب و خدمات کنترل تهدید دیجیتال است.

۲-۸ دیدگاه وسیع‌تر

امروزه همه سازمان‌ها به نوعی یک هدف احتمالی حمله هستند. حتی اگر یک سازمان کوچک یا به ظاهر ناچیز برای عاملان تهدید باشند، احتمالاً به یک تامین کننده، فروشنده شخص ثالث یا به نوعی به یک هدف بزرگتر و مهم‌تر حمله متصل شده‌اند. در سال ۲۰۲۰ سازمان‌ها باید آگاه باشند که می‌توانند ضعیف‌ترین پیوند باشند و باید دید وسیع‌تری داشته باشند.

در سال ۲۰۲۰ بهترین کاری که رهبران سازمان‌های امنیتی می‌توانند انجام دهند، درک این مسئله است که چه مسائلی باعث شده است که آن‌ها و دیگران در صنعت خود مورد هدف قرار گیرند.

۲-۹ افزایش آگاهی

یکی از بزرگ‌ترین چالش‌هایی که امروزه شرکت‌ها با آن مواجه هستند عدم درک اهمیت پیش‌بینی فعالیت‌های شرکت‌های رقیب است. در اصل، همه تصور می‌کنند که تهدید را می‌شناسند، در صورتی که بیشتر اوقات وقتی نحوه پردازش اطلاعات را توصیف می‌کنند، آشکار می‌شود که کاملاً آنرا نمی‌شناسند. بنابراین باید آگاهی کارمندان افزایش یابد. آنچه سازمان‌ها باید در سال ۲۰۲۰ روی آن کار کنند، چگونگی تولید محتوا و استفاده از آن در عملکرد سازمانی و همچنین شناسایی ابزار پیشرو به صورت مداوم است. یکی از دلایلی که سازمان‌ها در برابر امنیت سایبری مقاومت می‌کنند، فقدان تجربه و عدم آگاهی در مورد آن است. برای رسیدن به امنیت بیشتر در سال ۲۰۲۰، سازمان‌ها باید درک درستی از حملات و پیامدهای آن داشته باشند، بنابراین در نهایت می‌توانند از خود به بهترین نحو دفاع کنند. در حقیقت آن‌ها باید دارایی‌ها، فناوری‌ها و همچنین تاثیر برنامه‌ها و زیرساخت‌های خود را بشناسند. متأسفانه، امروزه اکثر سازمان‌ها دیدگاه جامعی نسبت به دارایی‌های خود ندارند و در سال جدید باید تغییر کنند.

۲-۱۰ حل یک مشکل بزرگ‌تر

اگر بخواهیم به مسئله واقع بینانه بنگریم، تصور تغییر عمده در آینده بعید است؛ مخصوصا زمانی که رشد و انفجار تکنیک‌های جدید حمله را مشاهده می‌کنیم و این در حالی است که توجه عموم مردم به این موضوعات کاهش یافته است. بعنوان مثال حمله DoS، که دیگر مورد توجه عموم نیست، در سال ۲۰۱۹ حدود ۱۵۰ درصد افزایش یافته است.

۲-۱۱ جایگاه ویژه مشاوران عمومی

نقش مشاوران عمومی(GC)[۳] در برنامه امنیت سایبری یک سازمان از بالاترین تا پایین‌ترین رده افزایش یافته و خواهد یافت. امروزه آن‌ها باید در تمام مراحل امنیت سایبری سازمان‌ها نقش موثری ایفا کنند، با اعضای سازمان مشارکت نزدیک داشته باشند و بر آموزش مدیران اجرایی سازمان تمرکز کنند تا بتواند برای نفوذهای احتمالی آمادگی کسب کنند.

۳ پیش‌بینی‌های امنیت سایبری در سال ۲۰۲۰

۳-۱ اهمیت باج‌افزارها

چالش‌های مربوط به باج‌افزارها در سال ۲۰۲۰ به شرح زیر است:

- باج‌افزارها پیشرفته‌تر می‌شوند.
- با وجود پیشرفته‌ترین راه‌حل‌های امنیتی برای ایمیل‌ها، توانایی نفوذ به سیستم‌ها را دارند.
- آلودگی ناشی از باج‌افزارها دارای پیامدهای مخرب است.

امروزه باج‌افزارها (Ransomware) به طور خودکار و با پیچیدگی بیشتر، حتی با پیشرفته‌ترین راه‌حل‌های امنیتی ایمیل نیز توانایی نفوذ به سیستم‌ها را دارند. علاوه بر این، راه‌حل‌های امنیتی فعلی، حملات باج‌افزار را چند ساعت پس از انتشار تشخیص می‌دهند، که اغلب حمله در همین زمان اتفاق می‌افتد. بنابراین حتی هوشمندترین روش‌های مبتنی بر امضا، IDS[۴] و سایر راه‌حل‌های سنتی قادر به تشخیص به اندازه کافی سریع آن نیستند. همان‌طور که می‌بینیم، حملات تقریباً به طور مداوم و هر هفته اتفاق می‌افتند. مهاجمان یک پایگاه از نمونه‌های جدید باج‌افزار ایجاد می‌کنند که شامل تکنیک‌های جدید مبهم‌سازی و دور زدن شناسایی‌ها است؛ سپس بر اساس این تکنیک‌ها نمونه تولید کرده و در سطح وسیع توزیع می‌کنند. مراکز امنیتی تولید ضد بدافزار و ضد باج‌افزار، باید از آن‌ها جلو زده و روش‌هایی را به محصول خود اضافه کنند که قادر به شناسایی نمونه‌های جدید باج‌افزار باشند.

باج‌افزارها با کنار زدن محدودیت‌ها، حملات مشکل‌سازتری نسبت به گذشته بر روی اهداف خود اعمال می‌کنند. آن‌ها روی بخش گسترده‌ای از سازمان‌ها تاثیر می‌گذارند و محدود به بخش یا ناحیه خاصی نیستند

---

[۳] General Counsel

[۴] سیستم تشخیص نفوذ

و باعث می‌شوند که قربانیان آسیب بیشتری را نسبت به باج‌افزارهای بدون هدف را متحمل شوند. با توجه به عملیات موفقیت‌آمیز این باج‌افزارها انتظار می‌رود که عملکرد آن‌ها در سال ۲۰۲۰ هم ادامه پیدا کند.

طبق پیش‌بینی‌های آزمایشگاه Malwarebytes، حملات باج‌افزاری به سازمان‌ها به دلیل تنوع در مسیر حمله، با سرعت بیشتری ادامه خواهد یافت. طی دو سال گذشته توسعه دهندگان بدافزار توجه خود را بیشتر از مصرف‌کنندگان به اهداف تجاری خود معطوف کرده‌اند و باج‌افزار گزینه بسیار مناسبی برای نیل به این هدف می‌باشد. در سال‌های ۲۰۱۷ تا ۲۰۱۹ آسیب‌پذیری‌های بیشتری نسبت به سال‌های گذشته مشاهده شد. آسیب‌پذیری بیشتر به معنای بهره‌برداری بیشتر است. همچنین در سال‌های اخیر موارد زیادی از Emotet و Trickbot مشاهده شد. انتظار می‌رود که در سال ۲۰۲۰، تروجان، dropper، downloader و botnetها نیز گزینه‌های مختلفی برای حملات چند مرحله‌ای به شرکت‌های وابسته ارائه دهند. در نهایت توسعه و شیوع ابزارهای هک مخرب که برای حمله موثر به شبکه‌ها طراحی شده‌اند، نویسندگان و شرکت‌های وابسته به باج افزار را جذب می‌کنند تا از آن‌ها در نفوذ و سپس تخریب زیرساخت‌های تجاری در سال ۲۰۲۰ استفاده کنند. بنابراین مشکل باج‌افزار از بین نخواهد رفت.

۲-۳ تاثیر انتخابات بر امنیت سایبری

انتخابات باعث افزایش تهدیدات سایبری می‌شود. سال ۲۰۲۰ سال انتخاباتی برای ایالات متحده پیش‌بینی شده است. انتظار داریم شاهد افزایش نه تنها جاسوسی سایبری بلکه عملیات نفوذ سایبری که هدف آن‌ها سیستم‌های انتخاباتی، نامزدهای انتخاباتی و رای‌دهندگان است، باشیم. این حوادث امنیتی انتخابات اعتماد رای‌دهندگان ایالات‌متحده را تضعیف خواهند کرد.

اگر نتایج انتخابات ریاست جمهوری خلاف پیش‌بینی‌ها باشد، رای‌دهندگان با دستگاه‌های رای‌دهی لو رفته و انتشار خبر جعلی در اینترنت و شبکه‌های اجتماعی، اعتبار روند رای‌گیری را زیر سوال می‌برند، فعالان دولتی با انتشار اطلاعات نادرست کشور را بی‌ثبات می‌کنند، کلاهبرداران و نویسندگان بدافزار از این انتخابات استفاده کرده و تهدیدات خود را از طریق ایمیل‌های فیشینگ گسترش می‌دهند. انتظار می‌رود که حساب های ربات انسان‌مانند در شبکه‌های اجتماعی ایجاد شود. با توسعه و بهبود هوش مصنوعی، تشخیص این حساب‌ها سخت‌تر خواهد بود زیرا آن‌ها خود را متقاعد کننده جلوه می‌دهند. این فعالیت‌ها در هنگام انتخابات بیشتر اتفاق می‌افتند.

صرف نظر از تاکتیک‌های کلاهبرداری یا مشکلات دستگاه رأی‌دهی که در بالا ذکر شد، تهدید واقعی حمله به قلب و روح ما از طریق رسانه‌های اجتماعی و دستکاری رسانه‌ها خواهد بود.

۳-۳ نقش سیاست‌های جفرافیایی در امنیت سایبری

در سال ۲۰۱۹ شاهد نا آرامی‌های زیادی در سراسر جهان بودیم و کارشناسان نا آرامی‌های بیشتری را در سال ۲۰۲۰ پیش بینی می‌کنند. سیاست‌های جغرافیایی، غالباً عامل مهمی برای هجوم و حملات مخرب هستند. تنش‌های سیاسی بین کشورها باعث ایجاد تهدیدات سایبری خواهد شد. انتظار می‌رود در سال ۲۰۲۰ با افزایش این تنش‌ها شاهد افزایش تهدیدات سایبری باشیم.

۴-۳ سوءاستفاده از اطلاعات شخصی

اگرچه مقامات مقررات جدیدی را برای محافظت از اطلاعات شخصی به تصویب رسانده‌اند، اما به نظر می‌رسد اجرای این مقررات بیشتر از حد انتظار طول می‌کشد. امروزه ارزش داده‌های شخصی مانند اطلاعات بانکی، اعتبار نامه‌ها و... افزایش یافته و افراد بدنیت را به سرقت آن‌ها تشویق می‌کند. برنامک‌های موبایل با داده‌های شخصی هدف‌های بسیار خوبی برای مهاجمان هستند. این برنامک‌ها آسیب‌پذیری محسوب شده و باعث از بین رفتن داده‌های کاربرانی که از آن‌ها استفاده می‌کنند خواهد شد. تا کنون فروشگاه‌های اپلیکیشن قابلیت شناسایی این برنامک‌ها را نداشته اند؛ در نتیجه، نشت داده‌های شخصی افزایش می‌یابد.

۵-۳ حملات phishing

در گذشته حملات فیشینگ با استفاده از دریافت ایمیل از آدرس ایمیل‌هایی ناسازگار که درخواست پرداخت پول یا باز کردن ناشیانه یک فایل می‌کرد، اتفاق می‌افتاد. امروزه حملات phishing تاثیرگذارتر خواهند بود. درسال ۲۰۲۰ باید در انتظار افزایش فیشینگ‌ها و کلاهبرداری‌هایی باشیم که یک فرد خاص، سازمان یا شغل را هدف گرفته است. فیشینگ تلاش می‌کند که از آدرس ایمیل‌های قابل اعتماد کلاهبرداری کرده و دستگاه‌های تلفن همراه را از طریق برنامه‌های پیام رسانی فریب دهد.

۶-۳ پرداخت‌های موبایلی بیشتر کنترل می‌شوند.

دستورالعمل خدمات پرداخت۲(PSD2)[۵] برای استانداردسازی بیشتر پرداخت‌های کارتی، موبایلی و اینترنتی تهیه شده و به طور خاص موانع پیش روی پرداخت‌های اینترنتی و کارتی را کاهش می‌دهد. این دستورالعمل که ابتدا قرار بود در سال ۲۰۱۹ توسط کمیسیون اروپا اجرا شود، به سال ۲۰۲۲ موکول شد تا زمان بیشتری

[۵] دستورالعمل اجرایی فعالیت و نظارت بر ارائه دهندگان خدمات پرداخت الکترونیک

برای آماده‌سازی شرکت‌ها فراهم شود. در نتیجه، طی دو سال آینده ویژگی‌های امنیتی جدید سایبری را مشاهده خواهیم کرد که توسط کلیه سازمان‌هایی که خدمات پرداخت (خرده فروشی، بانک‌ها و ...) در خدمات وب و تلفن همراه خود ارائه می‌دهند، اجرا می‌شوند.

۳-۷ تهدیدات مانای پیشرفته از تلفن همراه بهره‌برداری می‌کند.

تهدیدات مانای پیشرفته[۶] (APT) به حملات تحت شبکه اطلاق می‌شود که یک شخص احراز هویت نشده می‌تواند برای مدت زمان زیادی به صورت ناشناس به شبکه دسترسی پیدا کند. هدف یک حمله APT سرقت اطلاعات است؛ نه صرفاً ضربه زدن به سازمان و یا انجام اعمال خراب کارانه. به همین منظور اغلب هدف این گونه حملات معمولا سازمان‌هایی است که اطلاعات مفیدی در اختیار دارند. در یک حمله معمولی، مهاجم تلاش می‌کند تا به سرعت وارد شده، اطلاعات را سرقت نماید و از شبکه خارج شود تا سیستم‌های تشخیص نفوذ شانس کمتری برای کشف آن‌ها داشته باشند. هرچند در این حملات هدف ورود و خروج سریع نیست و معمولا این گونه حملات، مانا هستند. بدین منظور مهاجم باید دائما کدهای فایل مخرب را بازنویسی نماید و تکنیک‌های پنهان‌سازی پیچیده‌ای (به همین دلیل به آن‌ها Advanced گفته می‌شود) استفاده نماید. در سال ۲۰۲۰، APTها قطعاً پویایی سازمانی را هدف خواهند گرفت.

۳-۸ افزایش کلاهبرداری‌های Web Skimming

تا زمانی که اطلاعاتی برای سرقت وجود داشته باشد، مجرمان تلاش می‌کنند تا مستقیم یا غیرمستقیم تجارت آنلاین را به خطر بیاندازند. حملات غیرمستقیم در واقع خطرناک‌تر، گسترده‌تر و موفق‌تر خواهند بود. حملات skimming در صفحات وب نوعی کلاهبرداری در اینترنت است که با تزریق بدافزار به صفحه پرداخت وب، از طریق تکنیک‌های فیشینگ در خطر سرقت اطلاعات پرداخت قرار گیرد.

محل رخ دادن skimmerها نیز تغییر یافته است؛ بیشتر آن‌ها در فرم پرداخت صورت می‌گیرد، جایی که مشتریان داده‌های پرداخت خود را وارد می‌کنند. با این حال آن‌ها دائما در حال جعل پردازنده‌های پرداخت و جا زدن خود به عنوان کاربران مهندسی اجتماعی با ترفندهایی همانند فیشینگ هستند. به طور کلی، این یک زمینه پویا است که انتظار می‌رود بسیاری از تکنیک‌های حمله جدید معرفی شده در طول سال ۲۰۲۰ را در آن مشاهده کنیم.

---

[۶] Advanced Persistent Threat

۹-۳ فعالیت exploit kit

فعالیت exploit kit[۷] در بالاترین حد خود قرار دارد. از آن جا که استفاده از internet explorer رو به کاهش است، انتظار داریم در سال ۲۰۲۰ شاهد افزایش سوءاستفاده‌ها و آسیب‌پذیری‌های روز صفرم در مرورگرهای Chrome و Chromium باشیم. امسال شاهد تعداد حداقلی از آسیب‌پذیری روز صفرم در Google Chrome بودیم. با اینکه دستیابی به این هدف نادر و دشوار است، فعالیت آن‌ها در حال افزایش است. از آن‌جا که بازار[۸] مرورگر به دلیل تغییر مرورگر Microsoft Edge به موتور Chromium در ژانویه سال ۲۰۲۰ بیشتر تحت سلطه Chrome/Chromium است، مهاجمان این دو را به عنوان اهداف اصلی برای بهره‌برداری می‌بینند. علاوه بر این، انتظار می‌رود حملات drive-by بیشتری شامل بدافزارهای بدون فایل مشاهده کنیم[۹].

۱۰-۳ افزایش حملات ترکیبی با ظرفیت چند مرحله‌ای

حمله چند مرحله‌ای به مهاجم اجازه می‌دهد به یک شبکه در موثرترین روش ممکن نفوذ کند. اولین مرحله جمع آوری اطلاعات است که با استفاده از آن مهاجم بتواند بهترین راه را برای ورود به مرحله بعد در نظر بگیرد که شامل آلودگی بیشتر در شبکه یا فروش آلودگی به شخصی که قصد کشف رمزنگاری یا انتشار بدافزارها را دارد می‌باشد. پیش‌بینی می‌شود در سال ۲۰۲۰ تعداد بیشتری از بدافزارها توسعه پیدا کنند که به منظور برنامه ریزی برای اهداف جنایی خود، زمان ساکن شدن آن‌ها روزها یا حتی هفته‌ها قبل از حمله مهاجمین باشد.

۱۱-۳ افزایش استفاده از داده‌های بیومتریک

سیستم بیومتریک و ردیابی ژنتیکی موجب اعتراض بین‌المللی به قوانین حریم خصوصی داده‌ها خواهد شد. طی یک سال گذشته، شاهد تحولات نگران کننده‌ای در جمع‌آوری، انتشار، فروش، به اشتراک گذاری و سرقت داده‌های مربوط به نرم‌افزارهای ردیابی سلامتی بوده‌ایم؛ کانادا، ایالات متحده و چین بطور مخفیانه پایگاه داده‌های DNA را برای ردیابی مهاجران و شهروندان ایجاد کردند، نیروی انتظامی لندن دوربین‌های

---

[۷] یک exploit kit مجموعه‌ای از exploitها است که یک ابزار ساده برای مدیریت انواع exploitها است.

[۸] market

[۹] می‌توان چندین بدافزار مختلف را با هم و به‌صورت یک مجموعه مجتمع کرد تا حداکثر میزان آسیب به دستگاه قربانی وارد شود. چنین بسته‌های نرم‌افزاری مخربی ممکن است شامل بدافزار بدون فایل (fileless malware) باشند که آنتی‌ویروس‌ها نمی‌توانند به‌راحتی آن‌ها را تشخیص دهند. همان‌طور که از نام این بدافزارها پیداست، این بدافزارها در حافظه RAM دستگاه اجرا می‌شوند و از هیچ فایلی استفاده نمی‌کنند.

تشخیص چهره را در ژانویه سال ۲۰۲۰ در سراسر شهر به دور از چشم شهروندانش دور زد. خرید Google Fitbit باعث نگرانی کاربران در مورد انتشار مربوط به نرم‌افزارهای ردیابی سلامتی به تبلیغ کنندگان شد، هرچند این شرکت علناً اظهار داشت که از این داده‌ها برای تبلیغات Google استفاده نمی‌شود.

مصرف کنندگان معمولاً از این امر که شرکت‌های قانونی و مجرمان سایبری به طور یکسان می‌توانند از وسایل ردیابی سلامت خود برای اهداف غیرمجاز استفاده کنند، آگاه نیستند.

۴ نتیجه‌گیری

در سال ۲۰۱۹ قدم‌های بزرگی در حیطه امنیت فضای سایبری برداشته شد، با این حال مهاجمان و همچنین مدافعان به فعالیت خود ادامه می‌دهند؛ بنابراین باید در سال ۲۰۲۰ برقراری امنیت را هدف اصلی قرار دهیم. در قسمت فضای ابری امنیت برقرار است، اما مهاجمان از ایمیل و سایر روش‌هایی که علیه محیط‌های پیش فرض عمل می‌کند استفاده می‌کنند. ارائه دهندگان فضای ابری، فروشندگان امنیتی و مشتریان همه باید درک کنند که در نهایت چه کسی مسئول امنیت است.

با وجود تعداد زیاد تهدیدات در سراسر دنیا، سال ۲۰۱۹ یک سال جذاب و تهدیدآمیز در فضای مجازی بوده است. تهدیدهای مک و اندروید از نظر حجم و شدت افزایش یافته‌است. سازمان‌ها، دولت‌ها و مدارس با تهدیدهای پیچیده و متنوعی روبرو شدند که هدف آن‌ها مختل ساختن زیرساخت‌های بحرانی بود. نرم‌افزارهای تبلیغاتی برای کاربران مصرف‌کننده و تجاری در همه سیستم عامل‌ها در همه مناطق اشباع شده بود. کیت‌های سوءاستفاده، کمپین‌های مخرب و skimmerها مرورگرها را تهدید کردند.

در دهه گذشته، کاربران معمولی اینترنت، مرورگرها را رها کرده و شروع به استفاده از رسانه‌های اجتماعی با گوشی‌های هوشمند کردند و مینی رایانه جایگزین تلفن‌های ساده شد. کار از راه دور غیر معمول بود، نقض داده‌ها ناشناخته بود و جرائم سایبری، امنیت و حفظ حریم خصوصی داده‌ها به ندرت مورد نگرانی عمومی قرار می‌گرفت.

آنچه روشن است این است که راه‌حل‌ها و تکنیک‌هایی که برای برقراری امنیت در سال ۲۰۱۹ استفاده شده است، برای حفظ امنیت سازمان در سال ۲۰۲۰ به طور خودکار قابل اتکا نیست و هرگز نقش امنیت سایبری، در سازمان‌ها به اهمیت امروز نبوده است.

۵ مراجع

[1] https://resources.malwarebytes.com/files/2020/02/2020_State-of-Malware-Report.pdf

[2] https://content.fireeye.com/predictions/wbnr-the-road-ahead-cyber-security-in-2020-and-beyond

[2] https://blog.pradeo.com/pradeo-cybersecurity-predictions-2020