خبرنامه افتا

۲۰

مردادماه ۱۳۹۶

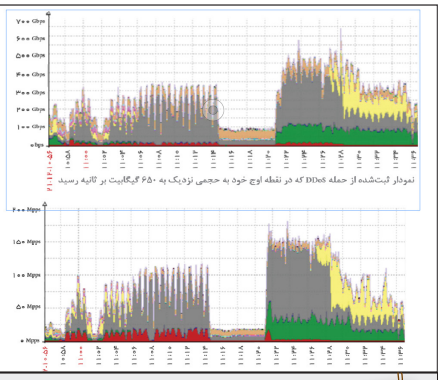
آینده افتا در سیستم‌های کنترل صنعتی

مخاطرات ناشی از ساختار امنیت نرم‌افزارهای کدباز

مؤثرترین شیوه‌های پاکسازی داده‌ها از روی SSD

تقابل مقررات و امنیت

آنچه در این خبرنامه می‌خوانید:



بدافزار

شرکت Imperva گزارش داد:

رقابت بات‌نت الیت با بدافزار Mirai در حملات DDoS

بات‌نت لیت با اجرای حملاتی با حجم ۶۵۰ گیگابیت بر ثانیه نشان داد که رقیبی قدرتمند برای بات‌نت‌های مبتنی بر بدافزار Mirai است که پیش از این، انحصار این نوع حملات را در دست داشتند.

صفحه ۴

بدافزار

بازخورد مایکروسافت به گزارش اخیر چک‌پوینت:

درباره بدافزار Fireball اغراق شده است

شرکت مایکروسافت ضمن اظهار تردید نسبت به گزارش تحقیقاتی شرکت چک‌پوینت در خصوص بدافزار Fireball، گفته است که با وجود تکامل این بدافزار در طول زمان، روش اولیه و اصلی آلوده‌سازی آن همچنان یکسان است. مایکروسافت ادعا می‌کند یافته‌های شرکت چک‌پوینت بر مبنای تعداد بازدیدها از صفحات جستجوی بدافزار و نه میزان جمع‌آوری داده‌های دستگاه‌های نهایی صورت گرفته‌اند و ممکن است دقیق نباشند.

صفحه ۵

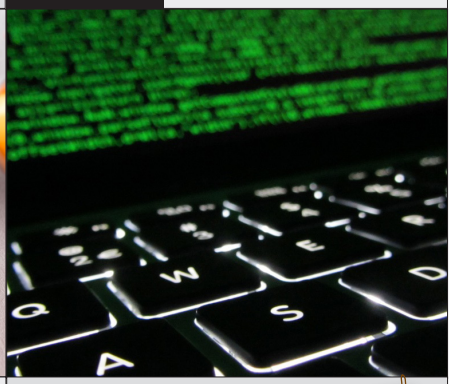
دانشی

نتایج بررسی آزمایشگاه NSS نشان می‌دهد:

میزان کارایی فایروال‌های نسل جدید

آزمایشگاه NSS با بررسی ۱۱ فایروال نسل جدید (NGFW) از ۱۰ سازنده پیشرو در بازار، نتایج جالبی را ارائه کرده است. بیش از ۸۰ درصد از این فایروال‌های نسل جدید، قادر به تشخیص روش‌های گریز از شناسایی حملات نبودند.

صفحه ۷



دانشی

کارشناسان هشدار دادند:

مخاطرات ناشی از ساختار امنیت نرم‌افزارهای کدباز

برنامه‌های کـــاربردی نوین دارای مؤلفه‌های نرم‌افزاری شخص ثالث هستند؛ مؤلفه‌های شخص ثالثی که به علت کدباز بودن می‌توانند در هزاران مؤلفه دیگر نیز به کار گرفته و تکرار شوند. در نتیجه، با کشف یک آسیب‌پذیری در کدهای منبع‌باز، تمام آن مؤلفه‌ها آسیب‌پذیر می‌شوند. اغلب سازمان‌ها نیز درک درستی نسبت به آسیب‌پذیری‌های امنیتی همراه با کدها ندارند.

صفحه ۹

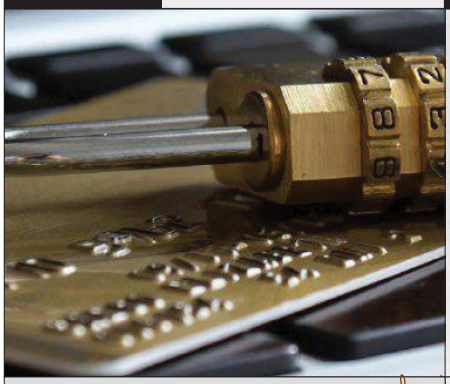
دانشی

نتایج نظرسنجی از ۳۰۰ کارشناس امنیتی:

مؤثرترین شیوه‌های پاکسازی داده‌ها از روی SSD

بسیاری از رخنه‌های امنیتی، ناشی از سهل‌انگاری در امحای داده‌های موجود در درایوها است. یک گزارش امنیتی جدید نشان می‌دهد که اغلب سازمان‌ها برای پیشگیری از وقوع رخنه به داده‌های موجود در درایوهای حالت جامد (SSD)، متکی به شیوه‌های رمزگذاری و فرمت مداوم درایوها هستند.

صفحه ۱۱



دانشی

شنا بر خلاف جریان رودخانه:

تقابل مقررات و امنیت

در سخنرانی کلیدی همایش Security BSides امسال، به مسئله تقابل امنیت و مقررات پرداخته شد. در این جلسه، از سه مسئله تعدد چارچوب‌های مقرراتی، پیروی از مقررات به عنوان یک نمایش امنیتی و زیاد از حد وسواس به خرج دادن در بررسی همه چیز به عنوان چالش‌های اصلی در مسیر حفظ تعادل میان اجرای تجربیات برتر امنیتی و پیروی از مقررات یاد شد.

صفحه ۱۳

دانشی

لزوم ایجاد تغییر در طراحی ICSها:

نواقص عمده در طراحی سیستم‌های کنترل صنعتی

شبکه‌های سیستم‌های کنترل صنعتی (ICS) تبدیل به اهداف ساده‌ای برای هکرها شده‌اند، زیرا این شبکه‌ها فاقد کنترل‌های امنیتی ابتدایی و ساده مانند سیستم‌های احراز هویت هستند و از ارتباطات رمزگذاری‌شده پشتیبانی نمی‌کنند. اگر کنترل‌های امنیتی در این شبکه‌ها وجود نداشته باشند، رفع آسیب‌پذیری‌ها نمی‌تواند مانع از دسترسی خرابکاران به این شبکه‌ها شود.

صفحه ۱۴

دانشی

هشدار کارشناسان امنیتی:

عواقب افشای آسیب‌پذیری‌ها در سیستم‌های کنترل صنعتی

فضای سیستم‌های کنترل صنعتی (ICS) بسیار متفاوت از فضای مرسوم حوزه IT است و افشای آسیب‌پذیری‌ها در این حوزه، یک شمشیر دولبه و بسیار تیز است؛ چراکه پیش از تلاش برای عیب‌یابی و به‌روزرسانی این آسیب‌پذیری‌ها، راه را برای ورود مهاجمان سایبری باز می‌کنیم.

صفحه ۱۶

دانشی

بررسی یکی از مهم‌ترین مسائل افتا در سال ۲۰۱۷:

آینده افتا در سیستم‌های کنترل صنعتی

حملات سایبری به سیستم‌های کنترل صنعتی (ICS)، طیف گسترده‌ای از صنایع و زیرساخت‌های حساس را تحت تأثیر قرار می‌دهد، زیرا همه این صنایع از تجهیزاتی استفاده می‌کنند که توسط تعداد مشخصی از سازندگان تولید می‌شوند. شواهدی وجود دارد که نشان می‌دهد در آینده بر شدت و تعداد این حملات افزوده خواهد شد.

صفحه ۱۸

دانشی

چالش‌های فناوری و امنیت:

هدف گرفتن اینترنت اشیا در زیرساخت‌های حیاتی

بدون شک، تعداد دستگاه‌های اینترنت اشیا (IoT) در آینده به رقمی بسیار بزرگ خواهد رسید. اما در کنار هر فناوری جدیدی، پای مسائل امنیتی نیز در میان است. طبق آمارها، بیشتر دستگاه‌های متصل به اینترنت اشیا از حفاظت کافی برخوردار نیستند و با این که به‌کارگیری فناوری IoT در زیرساخت‌های حیاتی با مزیت‌های فراوانی همراه است، اما مخاطراتی جدی نیز در پی دارد؛ کافی است به حادثه باتنت Mirai نگاهی انداخت.

صفحه ۲۰

دانشی | آسیب‌پذیری | بدافزار

اخبار کوتاه

۱- دسترسی کارکنان سابق سازمان‌ها به شبکه، تهدیدی جدی
۲- نیروهای داخلی سازمان، هدف حملات خارجی
۳- نیروهای داخلی، عامل بیشتر آسیب‌ها به سازمان
۴- عدم توانایی نیمی از متخصصان ICS در شناسایی حملات شبکه‌هایشان
۵- امنیت برنامه‌های کاربردی
۶- کمبود شدید نیرو در حوزه افتا
۷- نسخه جدید باج‌افزار Petya
۸- افزایش حملات باج‌افزاری در سال ۲۰۱۷
۹- امکان تشخیص گذرواژه‌های تایپ‌شده از طریق امواج ساطع‌شده مغز
۱۰- کشف آسیب‌پذیری‌هایی در گوشی‌های هوشمند Lenovo VIBE
۱۱- قابلیت‌های مین‌فرم Z شرکت IBM

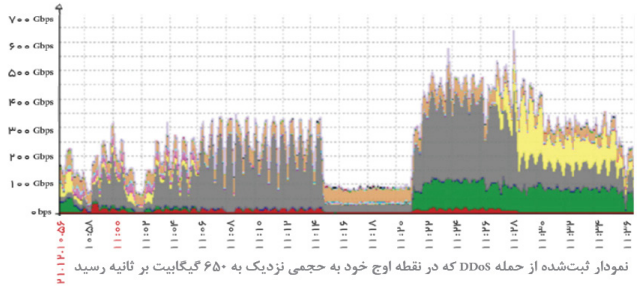
صفحه ۲۳

رقابت بات‌نت لیت با بدافزار Mirai در حملات DDoS

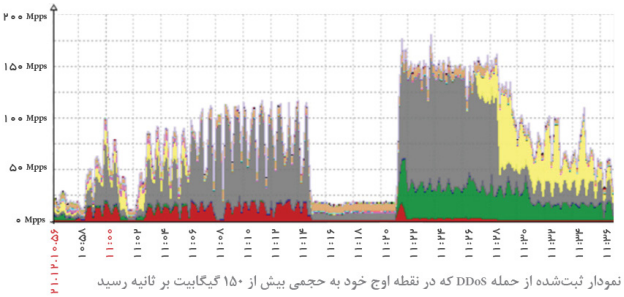
بات‌نت الیت[1] با اجرای حملاتی با حجم ۶۵۰ گیگابیت بر ثانیه نشان داد که رقیبی قدرتمند برای بات‌نت‌های مبتنی بر بدافزار Mirai است که پیش از این، انحصار این نوع حملات را در دست داشتند.

به گفته شرکت Imperva که در زمینه مقابله با حملات DDoS فعالیت می‌کند، بات‌نت‌های DDoS مبتنی بر بدافزار Mirai انحصار حملات DDoS با برونداد بالا را از دست داده‌اند. این شرکت در ۲۱ دسامبر سال ۲۰۱۶، یک حمله DDoS را با حجم بیش از ۶۵۰ گیگابیت بر ثانیه و مقیاسی بالغ بر ۱۵۰ میلیون بسته بر ثانیه، متوقف کرد. این حمله در دو موج مختلف انجام شد و در هر دوی آن‌ها، شبکه Imperva به این دلیل مورد حمله قرار گرفت که مهاجم قادر به شناسایی آدرس IP هدف نبود و این آدرس در پشت شبکه‌های پراکسی شرکت پنهان شده بود.

اولین موج حمله همان‌طور که در شکل زیر معلوم است، در نقطه اوج خود به حجم ۴۰۰ گیگابیت بر ثانیه رسید و مدت ۲۰ دقیقه به طول انجامید. همان‌گونه که مشخص است اولین سیل بسته‌ها موفقیت چندانی حاصل نکرد و درست پنج دقیقه بعد مهاجم دوباره با یک شبکه DDoS بزرگ‌تر که در هر ثانیه بیش از ۶۵۰ گیگابیت ترافیک ناخواسته را به سمت شبکه Imperva هدایت می‌کرد، به میدان برگشت.



نمودار ثبت‌شده از حمله DDoS که در نقطه اوج خود به حجمی نزدیک به ۶۵۰ گیگابیت بر ثانیه رسید



نمودار ثبت‌شده از حمله DDoS که در نقطه اوج خود به حجمی بیش از ۱۵۰ گیگابیت بر ثانیه رسید

این حمله دوم تنها ۱۷ دقیقه طول کشید؛ چراکه بعد از آن مهاجم متوجه شد نمی‌تواند شبکه هدف را از کار بیندازد. در مقایسه با حملاتی که به OVH، وب‌سایت KrebsOnSecurity و Dyn صورت گرفت و چندین روز به طول انجامید، این حمله خیلی چشمگیر نبود.

استفاده از یک بات‌نت کاملاً جدید در حمله اخیر

نکته جالبی که درباره این حمله می‌توان به آن اشاره کرد، بات‌نتی بود که این حمله را به مرحله اجرا درآورد. تا به حال حملاتی با این اندازه، تنها از جانب بات‌نت‌هایی صورت می‌گرفتند که بدافزار Mirai آن‌ها را ایجاد کرده بود. همان‌طور که می‌دانید، Mirai بدافزاری است که برای آلوده کردن و دزدی از دستگاه‌های هوشمند اینترنت اشیا (IoT) طراحی شده است.

کارکنان Imperva نام این بات‌نت ناشناخته را لیت گذاشتند؛ چراکه بسیاری از گزینه‌های TCP در بسته‌های ترافیک ناخواسته ارسالی از بات‌نت، طوری چیده شده بودند که عدد «1337» را نشان می‌دادند. این عدد نماینده عبارت «الیت»[2] در نوشتار به روش L33t است (توضیح مترجم: روش L33t الفبایی است برای نوشتن زبان انگلیسی که بر روی اینترنت به کار می‌رود. در این الفبا از کاراکترهای مختلف اَسکی برای جایگزین کردن حروف لاتین استفاده می‌شود. این اصطلاح از واژه elite گرفته شده است و نوعی خاص از نوشتنِ نشانه‌ای را توصیف می‌کند).

تفاوت‌های الیت با Mirai

محققان سه تفاوت اصلی در نحوه عملکرد این دو بات‌نت یافتند. اولین و مهم‌ترین این تفاوت‌ها این است که بدافزار Mirai و بات‌نت‌های آن از ویژگی‌ها و قابلیت‌های فنی برای اجرای حملات گسترده SYN، برخوردار نیستند. این در حالی است که حمله الیت این ویژگی‌ها را دارا بود.

دوم این که در تمام بسته‌های ترافیک ناخواسته بات‌نت Mirai، گزینه‌های TCP خاصی ثبت شده بود که در بسته‌های مشاهده‌شده در حمله الیت این گزینه‌ها دیده نمی‌شدند.

سومین و آخرین تفاوت این بود که محتوای بسته‌های حمله DDoS بدافزار Mirai، از رشته‌های متنی تصادفی ساخته شده بودند؛ اما در حمله اخیر، بات‌نت لیت محتوایی را از فایل‌های واقعی سیستم به داخل بسته‌های TCP در حمله DDoS تعبیه می‌کرد و آن‌ها را از طریق شبکه Imperva ارسال می‌نمود.

تمام این نشانه‌ها حاکی از وجود بات‌نت جدیدی است که نمی‌تواند بات‌نت اصلاح‌شده Mirai باشد. هرچند ریشه بات‌نت الیت دارای ویژگی‌هایی نیست که ثابت کند این بات‌نت از دستگاه‌های آلوده IoT تشکیل شده است، جالب است بدانید تا به حال هیچ بات‌نتی که از رایانه‌های دسکتاپ تشکیل شده باشد نتوانسته است به چنین برونداد بالایی برای حملات DDoS دست یابد. حملاتی با بیش از ۵۰۰ گیگابیت بر ثانیه تنها در حوزه بات‌نت‌های IoT قرار می‌گرفتند.

منبع: www.bleepingcomputer.com

۱- Leet

۲- elite

درباره بدافزار Fireball اغراق شده است

شرکت مایکروسافت ضمن اظهار تردید نسبت به گزارش تحقیقاتی شرکت چک‌پوینت در خصوص بدافزار Fireball، گفته است که با وجود تکامل این بدافزار در طول زمان، روش اولیه و اصلی آلوده‌سازی آن همچنان یکسان است. مایکروسافت ادعا می‌کند یافته‌های شرکت چک‌پوینت بر مبنای تعداد بازدیدها از صفحات جستجوی بدافزار و نه میزان جمع‌آوری داده‌های دستگاه‌های نهایی صورت گرفته‌اند و ممکن است دقیق نباشند.

باور جمعی بر این است که بدافزار Fireball تهدیدی جدی برای کاربران و همچنین سازمان‌ها ایجاد می‌نماید؛ اما مایکروسافت نسبت به گزارش‌های مربوط به این بدافزار اظهار تردید کرده است. بر اساس نظر همیش اودیا، محقق تیم Windows Defender، گزارش‌های اخیر درباره جرایم سایبری Fireball احتمالاً با اغراق همراه بوده است.

مقاله تحقیقاتی اخیر شرکت چک‌پوینت ادعا کرده است که Rafotech، یک آژانس بازاریابی دیجیتالی بزرگ در پکن، طرح بدافزار Fireball را اداره می‌نماید. این مقاله بیان داشت که «بدافزار Fireball تهدیدی بزرگ برای اکوسیستم سایبری جهانی است که ۲۵۰ میلیون دستگاه را آلوده ساخته است و یک‌پنجم شبکه‌های سازمانی را نیز تحت کنترل گرفته است». شرکت چک‌پوینت ادعا می‌کند که ۲۰ درصد از تمامی شبکه‌های سازمانی به طریقی تحت تأثیر Fireball قرار گرفته‌اند و بیشتر این آلودگی‌ها نیز در کشورهای آمریکا، چین، اندونزی، هند و برزیل در حال وقوع است.

مایکروسافت از سال ۲۰۱۵ در حال ردگیری و تعقیب بدافزار Fireball بوده و اظهار نموده است که اگرچه روش تاکتیکی این بدافزار در طول زمان تکامل یافته است، اما روش اولیه و اصلی مورد استفاده برای آلوده نمودن سیستم‌های آسیب‌پذیر از طریق بسته‌بندی نرم‌افزاری همچنان بدون تغییر باقی مانده است.

بدافزار Fireball همراه با برنامه‌هایی که کاربران از طریق مرورگر اینترنت دانلود می‌کنند، نصب می‌شود و بیشتر از همه، در کنار برنامه‌های قفل‌شکن[۱]، تولید سریال[۲] و سرقت محتوای دارای حق کپی[۳] نظیر بازی، موسیقی و برنامه کاربردی مشاهده شده است.

۱- crack

۲- keygen

۳- pirated content

در زمان دانلود، غالباً برنامه‌های سالمی نیز درون بسته نرم‌افزار وجود دارد. با این حال، این برنامه‌های سالم میزبان فرایندهایی هستند که در ادامه برای بارگذاری کدهای مخرب با روشی خاص به کار گرفته می‌شوند؛ روشی که مایکروسافت آن را «تلاشی برای گریز از روش‌های شناسایی مبتنی بر رفتار»[۴] توصیف می‌نماید.

شرکت مایکروسافت در طی سه سال گذشته، با زیر نظر داشتن عاملان تهدید بدافزار Fireball، پی برده است که تمرکز آن‌ها روی تداوم و پایستگی بدافزار، درآمدزایی از طریق تبلیغات و ربایش[۵] تنظیمات صفحه اصلی و بخش جستجوی مرورگر در دستگاه‌های آلوده بوده است.

میزان شیوع بدافزار Fireball در جهان

معمول‌ترین ابزارهای بدافزاری بسته‌بندی‌شده در Fireball عبارتند از: BrowserModifier:Win32/SupTab و BrowserModifier:Win32/Sasquor.

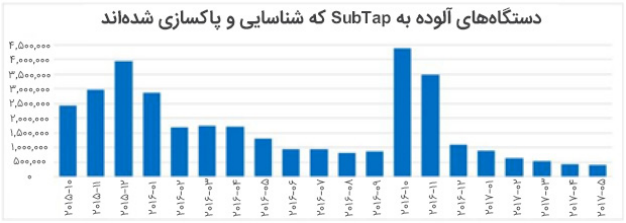
هنگامی که یکی از این بسته‌های نرم‌افزاری غیرقابل‌تشخیص بر روی سیستمی نصب گردد، در اولین حمله بدافزار Fireball، صفحات اصلی مرورگر و تنظیمات پیش‌فرض صفحه اصلی ربوده می‌شوند. این کار از طریق تغییر مستقیم تنظیمات مرورگر یا ایجاد میانبرهایی جدید برای راه‌اندازی مرورگرهای قانونی انجام می‌گیرد.

سپس اگر کاربر جستجویی از طریق موتور اپراتور بدافزار انجام دهد، مهاجمان به واسطه نمایش تبلیغات در مرورگر درآمد کسب خواهند نمود. بدافزار Fireball همچنین از افزونه‌ها[۶] و اعمال تغییرات در تنظیمات مرورگر برای بهبود درآمدزایی از تبلیغات بهره می‌گیرد؛ از قابلیت ردگیری از طریق پیکسل[۷] جهت جمع‌آوری اطلاعات خصوصی استفاده می‌کند؛ و همچنین قادر است حملات بدافزاری بیشتری را به سیستم‌های آلوده وارد نماید.

پس از تحقیقات شرکت چک‌پوینت بر روی شدت، بردارهای آلودگی[۸] و میزان مشکل‌آفرینی بدافزار Fireball، مایکروسافت بیان نمود که یافته‌های این شرکت، به جای تکیه بر میزان جمع‌آوری داده‌های دستگاه‌های نهایی، بر اساس تعداد بازدیدها از صفحات جستجوی بدافزار بوده است.

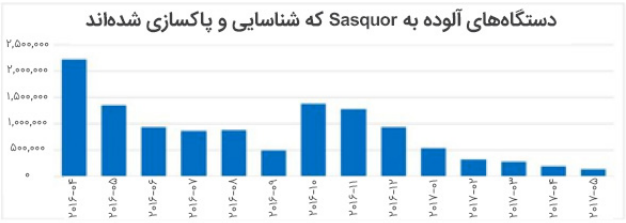
بنابراین، ممکن است این نتایج منطقی و دقیق نباشند؛ زیرا همه رایانه‌هایی که از این صفحات بازدید می‌کنند، آلوده نیستند و این برآوردها به جای بررسی ترافیکی که معمولاً توسط آلودگی‌های بدافزاری تولید می‌گردد، بر اساس داده‌های رتبه‌بندی Alexa و عادت‌های معمول در جستجو صورت گرفته‌اند.

مایکروسافت با بررسی ۳۰۰ میلیون کلاینت آنتی‌ویروس Windows Defender که از سال ۲۰۱۵ فعال بوده‌اند، اعلام کرد که نمودارهای زیر احتمالاً اطلاعات کامل‌تری درباره مقیاس بدافزار Fireball نمایش می‌دهند.



تعداد دستگاه‌های آلوده به BrowserModifier:Win32/SupTab که محصولات ضدبدافزار مایکروسافت شناسایی و پاکسازی نموده‌اند.

افزایش ناگهانی شناسایی دستگاه‌های آلوده در اکتبر ۲۰۱۶، همزمان با افزوده شدن خانواده SupTab به ابزار MSRT[۹] بوده است (توضیح مترجم: MSRT ابزار پاکسازی نرم‌افزارهای مخرب مایکروسافت است).



تعداد دستگاه‌های آلوده به BrowserModifier:Win32/Sasquor که محصولات ضدبدافزار مایکروسافت شناسایی و پاکسازی نموده‌اند.

مایکروسافت می‌گوید تیم امنیتی این شرکت اخیراً هیچ تغییری در راهبرد بدافزار Fireball مشاهده نکرده است. اودیا نیز توضیح داد: «زنجیره آلودگی بدافزار Fireball شامل انواعی از بسته‌های نرم‌افزاری و بدافزاری است که به طور مخفیانه برنامه‌های کاربردی دیگری را هم نصب می‌کنند. کاربران نیازمند آن دسته از راه‌حل‌های امنیتی هستند که تمامی مؤلفه‌های این نوع آلودگی را شناسایی و حذف کنند».

بسته‌های حاوی نرم‌افزارهای ناخواسته از پیش نصب‌شده[۱۰]، جاسوس‌افزار[۱۱] و فایل‌های مخرب غیرمعمول نیستند؛ اما سیستم‌های مجهز به آنتی‌ویروس Windows Defender موجود بر روی ویندوز یا برنامه‌های شخص ثالث دیگری نظیر AVG، کاسپرسکی و Bitdefender می‌توانند بدافزار Fireball را پیش از نفوذ به سیستم، شناسایی و حذف نمایند.

در واکنش به شکایت‌های شرکت کاسپرسکی، مایکروسافت اعتراف کرد که سیستم‌عامل ویندوز ۱۰ موقتاً نرم‌افزارهای آنتی‌ویروس شخص ثالث را غیرفعال می‌کند. شرکت مایکروسافت متهم شده بود که از چنین روش‌هایی برای تبلیغ و ترویج سیستم Windows Defender استفاده می‌کند؛ اما در جواب استدلال نمود که حصول اطمینان از حفاظت دائمی کاربران در برابر تهدیدات امنیتی، نخستین نگرانی این شرکت است.

منبع: www.zdnet.com

۴- an attempt to evade behavior-based detection
۵- hijack
۶- plugins
۷- pixel tracking
۸- infection vectors
۹- Malicious Software Removal Tool
۱۰- crapware
۱۱- spyware

میزان کارایی فایروال‌های نسل جدید

آزمایشگاه NSS با بررسی ۱۱ فایروال نسل جدید[۱] (NGFW) از ۱۰ سازنده پیشرو در بازار، نتایج جالبی را ارائه کرده است. بیش از ۸۰ درصد از این فایروال‌های نسل جدید، قادر به تشخیص روش‌های گریز از شناسایی حملات نبودند.

آزمایشگاه NSS به تازگی ۱۱ مورد از فایروال‌های نسل جدید را مورد آزمایش و بررسی قرار داده است. این فایروال‌ها به لحاظ میزان اثربخشی امنیتی آن‌ها و همچنین هزینه کل مالکیتشان[۲] (TCO) مورد آزمایش قرار گرفتند. از میان فایروال‌های نسل جدیدی که در این آزمایش‌ها حضور داشتند، هفت فایروال به عنوان محصول «توصیه‌شده» و چهار محصول نیز به عنوان محصولاتی معرفی شدند که در استفاده از آن‌ها باید «احتیاط شود». بیش از ۸۰ درصد از محصولاتی که مورد آزمایش قرار گرفتند، در تشخیص یک یا چند روش گریز از شناسایی حمله ناکام ماندند. ناکامی در تشخیص روش‌های گریز از شناسایی حمله، وزن سنگینی در امتیاز نهایی مربوط به اثربخشی امنیتی داشت. رتبه میانگین مربوط به اثربخشی امنیتی ۶۷٫۳ درصد بود.

جیسون برونیک، مدیر فنی آزمایشگاه NSS، گفت: «بازار فایروال‌های نسل جدید یکی از بزرگ‌ترین و بالغ‌ترین بازارهای امنیتی است. تهدیدات دائماً در حال تکامل هستند و در آزمایش امسال، تنها دو محصول توانستند در برابر تمام روش‌های گریز از شناسایی، مقاومت کنند». وی افزود بسیاری از سازندگان این فایروال‌ها گرچه

۱- next generation firewall

۲- total cost of ownership

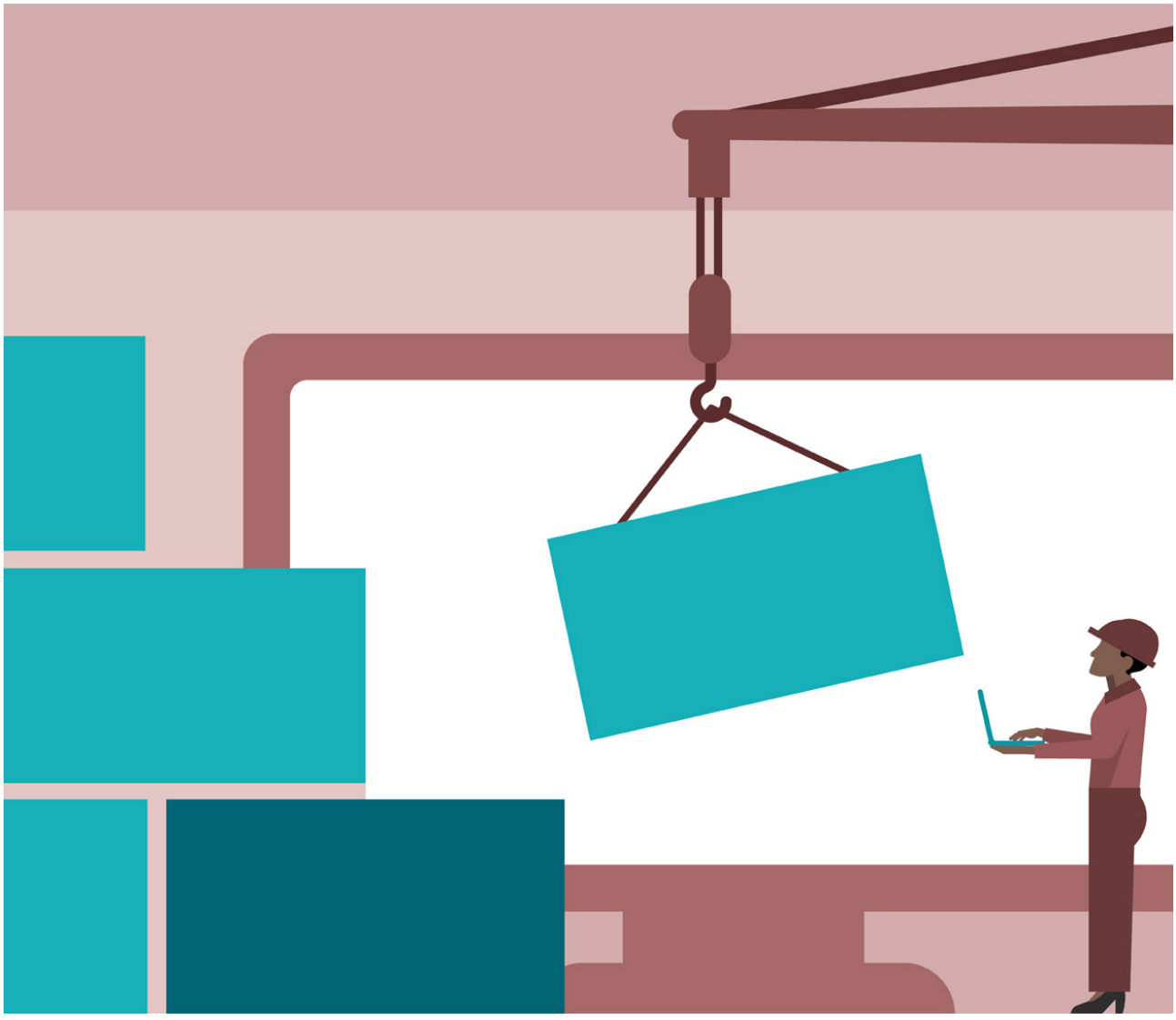
امتیاز محصولاتشان در این آزمایش تحت تأثیر قرار گرفته بود، اما محصولات خود را بعد از اعلام نتایج، سریعاً عیب‌یابی کردند تا سطح امنیت آن‌ها را بهبود بخشند. این امر نشان می‌دهد سازندگان مذکور تا چه حد توانایی واکنش به چشم‌انداز در حال تکامل تهدیدات را دارا هستند.

فایروال‌های نسل جدید یکی از مؤلفه‌های مهم در راهبرد دفاع در عمق هستند. سطح مستعد حمله در محیط‌های سازمانی دائماً در حال گسترش است. این گسترش به چند دلیل رخ می‌دهد، از جمله به دلیل گسترش برنامه‌های کاربردی سازمانی، به‌کارگیری وسیع سیاست‌های استفاده از دستگاه شخصی در سازمان (BYOD)، محیط‌های ابری دوگانه، الزامات عملیاتی خاصی مثل اجرای سیاست‌های امنیت و IT و نیاز به عیب‌یابی مستمر دستگاه‌ها و سیستم‌عامل‌ها. سازمان‌ها در حال حاضر روی فایروال‌های نسل جدیدی سرمایه‌گذاری می‌کنند که این الزامات را برطرف کنند و بردارهای حمله‌ای که مهاجمان سایبری می‌توانند با استفاده از آن‌ها به محیط سازمان حمله کنند را کاهش دهند.

این آزمایش گروهی، هفتمین سری آزمایش‌های فایروال‌های نسل جدید است که در آزمایشگاه‌های NSS انجام می‌پذیرد. روش آزمایش اخیر، موارد کاربری بیشتری را مورد توجه قرار داده است تا الزامات فعلی دنیای امروزی در رابطه با اثربخشی امنیتی بیشتر و رمزگذاری بهتر را پشتیبانی کند. در این آزمایش به طور خاص، طیف تکنیک‌های گریز از شناسایی گسترش یافته‌اند تا علاوه بر تهدیدات موجود، حملات جدید و مجهز امروزی را نیز شامل شوند. نگرانی درباره شیوه‌های گریز از شناسایی رو به افزایش است، چراکه بسیاری از اکسپلویت‌ها با استفاده از این شیوه‌های ساده در ترافیک HTTP، قادر خواهند بود تمهیدات امنیتی را دور بزنند.

میزان کلی اثربخشی امنیتی در محصولات مورد آزمایش از ۲۵,۸ درصد تا ۹۹,۹ درصد را شامل می‌شد. هفت مورد از این ۱۱ محصول، رتبه‌هایی بالاتر از ۷۸,۵ درصد دریافت کردند. میانگین هزینه مالکیت این محصولات به ازای هر مگابیت بر ثانیه از ترافیک حفاظت‌شده، ۲۵,۲ دلار بوده است. در این بین، هشت محصول رتبه‌ای بالاتر از میانگین دریافت کردند و سه محصول نیز رتبه‌ای پایین‌تر از میانگین را به خود اختصاص دادند.

منبع: www.infosecurity-magazine.com



مخاطرات ناشی از ساختار امنیت نرم‌افزارهای کدباز

برنامه‌های کـــاربردی نوین دارای مؤلفه‌های نرم‌افزاری شخص ثالث هستند؛ مؤلفه‌های شخص ثالثی که به علت کدباز بودن می‌توانند در هزاران مؤلفه دیگر نیز به کار گرفته و تکرار شوند. در نتیجه، با کشف یک آسیب‌پذیری در کدهای منبع‌باز، تمام آن مؤلفه‌ها آسیب‌پذیر می‌شوند. اغلب سازمان‌ها نیز درک درستی نسبت به آسیب‌پذیری‌های امنیتی همراه با کدها ندارند.

تقریباً همه برنامه‌های کاربردی و کسب‌وکارهای نوین از ماژول‌های کدباز[1] استفاده می‌کنند. پس تلاش برای تمایز قائل شدن میان نرم‌افزار اختصاصی و کدباز اتلاف وقت است؛ چراکه برنامه‌های کاربردی دارای مؤلفه‌های نرم‌افزاری شخص ثالث هستند. بسیاری از این مؤلفه‌ها نیز کدباز هستند و حتی تعداد بسیار کمی از سازمان‌ها درک درستی نسبت به آسیب‌پذیری‌های امنیتی همراه با کدها دارند. دسترسی و تأثیر آسیب‌پذیری‌های کدهای منبع‌باز تنها پس از سوءاستفاده، و در برخی موارد مدت‌ها بعد از سوءاستفاده، آشکار می‌شوند؛ اما دنیای کسب‌وکار به هر صورت به سمت نرم‌افزارهای توسعه‌یافته در جامعه[2] رفته است. نظرسنجی شرکت Black Duck از مدیران اجرایی ارشد و کارشناسان ارشد IT در سال ۲۰۱۵ نشان داد که استفاده از نرم‌افزارهای کدباز از سال ۲۰۱۰ تقریباً دو برابر شده است.

باور نادرست در خصوص امنیت کدباز

نظریه محبوب «با داشتن چشم‌های کافی، تمام باگ‌ها سطحی و ناچیز هستند»[3] در مورد نرم‌افزارهای کدباز تنها زمانی درست است که همه این چشم‌ها روی یک وظیفه یکسان متمرکز شوند. در این نظریه، به این نکته توجه نمی‌شود که اغلب کاربران به طور خاص به دنبال آسیب‌پذیری‌های امنیتی نیستند؛ حتی اگر هم در پی این موضوع باشند، صلاحیت و توانایی یافتن آن‌ها را ندارند.
اغلب برنامه‌نویسانی که پروژه‌های کدباز می‌نویسند و از پروژه‌های

۱- open-source modules
۲- community-developed software
۳- given enough eyeballs, all bugs are shallow

کدباز استفاده می‌کنند، ذهنیت امنیتی ندارند و اگر تجزیه‌وتحلیل کد انجام نشود، آسیب‌پذیری‌ها می‌توانند به برنامه کاربردی شما راه پیدا کنند و موفقیت آن را تهدید نمایند. کدهای منبع‌باز مزایای امنیتی خودشان را دارند، مثلاً وقتی تردیدی در مورد امنیت وجود دارد، می‌توان آن‌ها را ممیزی و تصحیح نمود، اما ذاتاً از امنیت بیشتری برخوردار نیستند. همه ما شاهد بوده‌ایم که آسیب‌پذیری‌های امنیتی مؤلفه‌های کدباز، نظیر هارت‌بلید[۴] و شل‌شاک[۵]، می‌توانند چه آسیب‌هایی به بار بیاورند.

زمانی که هارت‌بلید افشا شد، حدود نیم میلیون از وب‌سرورهای امن اینترنت که توسط مقامات مورد اعتماد تأیید شده بودند، نسبت به حمله آسیب‌پذیر بودند. این امر شرایط را برای سرقت کلیدهای خصوصی، کوکی‌های جلسه[۶] و گذرواژه‌هایی مهیا ساخت که به مهاجمان امکان می‌دادند تا خود را به جای کاربران دیگر جا بزنند. از آنجایی که حمله، قطعاتی از حافظه را به صورت تصادفی انتخاب می‌کرد، هر اطلاعاتی که در حافظه نگهداری می‌شد، می‌توانست برای هر مهاجمی که به اندازه کافی سماجت و پافشاری به خرج می‌داد، افشا شود.

همین طور چند ساعت بعد از افشای شل‌شاک، مهاجمان بات‌نت‌هایی[۷] از رایانه‌های آسیب‌پذیر ساختند و حملات DDoS انجام دادند. میلیون‌ها حمله و کاوش در روزهای پس از این افشا اتفاق افتاد. این حملات، خاصیت سریع‌الانتشار بودن یک اکوسیستم مؤلفه کدباز را آشکار می‌کنند. یک تک‌مؤلفه کدباز می‌تواند در صدها مؤلفه دیگر نیز استفاده شود؛ در نتیجه یک نقص به همه مؤلفه‌هایی که به مؤلفه اول وابسته هستند، تکثیر می‌شود.

تأخیر در به‌روزرسانی آسیب‌پذیری‌ها

اگر مهاجمان یک آسیب‌پذیری بحرانی در کدهای منبع‌باز بیابند، می‌توانند به صدها هزار سیستمی که از آن مؤلفه در برنامه‌های کاربردی خود استفاده می‌کنند، حمله نمایند؛ اما این بدان معنا نیست که به‌روزرسانی‌ها نیز به سرعت ارائه می‌گردند. طبق مقاله «وضعیت امنیت کدباز در برنامه‌های کاربردی تجاری»[۸]، میانگین عمر یک آسیب‌پذیری کدباز بیش از پنج سال است.

از آنجا که بسیاری از سازمان‌ها مؤلفه‌های کدباز را ردگیری نمی‌کنند، چیزی هم در مورد آسیب‌پذیری‌های کدباز در کدهای خود نمی‌دانند. سایت‌ها و برنامه‌های کاربردی به سرقت می‌روند، چون نرم‌افزارهای شخص ثالث به‌روزرسانی نمی‌شوند و همچنین به این علت که ماژول‌های کدباز نیز غالباً دارای نسخه‌های ناامنی هستند که تا مدت‌ها پس از منتشر شدن نسخه‌های به‌روزرسانی‌شده آن‌ها، هنوز هم برای دانلود در دسترس هستند. بسیاری از سازمان‌ها با تعریف کردن نسخه‌های خاصی در ساخت‌های[۹] خود و به این بهانه که به‌روزرسانی مشکلاتی از نظر سازگاری نسخه‌ها ایجاد خواهد کرد، همچنان به استفاده از نسخه‌های ناامن ادامه می‌دهند.

شرکت Black Duck در نظرسنجی سال ۲۰۱۶ با عنوان «آینده نرم‌افزارهای کدباز»[۱۰] به این نتیجه رسید که مدیریت و امنیت کدباز با روند به‌کارگیری نرم‌افزارهای کدباز همگام نبوده است. در حال حاضر، ۵۰ درصد از سازمان‌ها هیچ‌گونه سیاست رسمی برای انتخاب و تأیید کدهای منبع‌باز ندارند؛ ۴۷ درصد از سازمان‌ها هیچ‌گونه فرایند رسمی برای ردگیری کدهای منبع‌باز خود در نظر نگرفته‌اند؛ و بیش از یک سوم از سازمان‌ها نیز مطلقاً هیچ فرایندی برای شناسایی، ردگیری یا به‌روزرسانی آسیب‌پذیری‌های کدباز شناخته‌شده ندارند.

همچنین این مشکل به سازمان‌های جزئی و کوچک محدود نمی‌شود. اعضای لیست ۵۰۰ سازمان برتر جهان[۱۱] به تنهایی و طی یک سال، نزدیک به سه میلیون مؤلفه ناامن دانلود کردند؛ رقمی که با توجه به افزایش تعداد حملات سایبری، شوکه‌کننده است. معاون امنیتی شرکت Black Duck پیش‌بینی می‌نماید که «تعداد حملات سایبری مبتنی بر آسیب‌پذیری‌های کدباز شناخته‌شده می‌تواند در ابعاد واقعی تا ۲۰ درصد افزایش پیدا کند». هکرها پی برده‌اند که برنامه‌های کاربردی در اغلب سازمان‌ها نقطه ضعفِ تمهیدات دفاعی افتا هستند و این که اکسپلویت‌های کدباز موجود دارای بازگشت سرمایه[۱۲] (ROI) بالایی هستند که به آن‌ها این امکان را می‌دهد تا هزاران سایت، برنامه کاربردی و دستگاه‌های متصل به اینترنت اشیا (IoT) را با حداقل تلاش مورد حمله قرار دهند.

امکان اصلاح آسیب‌پذیری‌های کدباز رده‌سازمانی وجود دارد، اما سازمان‌ها باید امنیت کدباز را در اولویت قرار دهند. صنایعی که دارای مقررات بیشتری هستند، معمولاً از امنیت کمتری برخوردارند؛ چراکه آن‌ها فقط آسیب‌پذیری‌هایی را اصلاح می‌کنند که به واسطه مقررات الزامی هستند. این سازمان‌ها تلاش خود را صرف پیروی از مقررات، و نه امنیت، می‌کنند و به علت هزینه آزمون پیروی از مقررات، سرعت به‌روزرسانی در آن‌ها بسیار کندتر است. صنایعی که مقررات کمتری دارند، می‌توانند وقتی که آسیب‌پذیری اصلاح می‌شود، یک به‌روزرسانی خاص‌منظوره[۱۳] انجام دهند.

در بسیاری از سازمان‌ها، چرخه‌های به‌روزرسانی با یک برنامه ثابت اجرا می‌شوند؛ بنابراین مسائل امنیتی در اولویت‌بندی قابلیت‌ها به عقب رانده می‌شوند. برنامه‌نویس‌ها و تیم‌های IT باید در هنگام توسعه یا به‌کارگیری برنامه‌های کاربردی، برای امنیت نیز به اندازه کارکرد اولویت قائل شوند. سازمان‌ها هم باید برنامه‌نویس‌ها را به انجام این کار تشویق و تحریک نمایند. اگر سازمان‌ها صرفاً به قابلیت‌ها توجه کنند، برنامه‌نویسان نیز فقط کارکرد را در اولویت قرار خواهند داد.

منبع: sdtimes.com

۴- Heartbleed

۵- Shellshock

۶- session cookies

۷- botnet

۸- The State of Open Source Security in Commercial Applications

۹- build

۱۰- Future of Open Source

۱۱- Global 500 organizations

۱۲- Return on Investment

۱۳- ad-hoc

مؤثرترین شیوه‌های پاکسازی داده‌ها از روی SSD

بسیاری از رخنه‌های امنیتی، ناشی از سهل‌انگاری در امحای داده‌های موجود در درایوها است. یک گزارش امنیتی جدید نشان می‌دهد که اغلب سازمان‌ها برای پیشگیری از وقوع رخنه به داده‌های موجود در درایوهای حالت جامد (SSD)، متکی به شیوه‌های رمزگذاری و فرمت مداوم درایوها هستند.

طی سال‌های اخیر، شمار روزافزونی از موارد رخنه به داده‌ها ناشی از حذف نادرست داده‌ها و ذخیره آن‌ها به شیوه‌ای ناامن روی درایوها رخ داده‌اند. طبق گزارش شرکت Blancco Technology Group، سازمان‌ها برای جلوگیری از دسترسی و رخنه به اطلاعات حساس شخصی و سازمانی روی درایوهای SSD با چالش‌های بی‌شماری در داخل و خارج از سازمان روبرو هستند.

بر اساس این گزارش که با نظرسنجی از بیش از ۳۰۰ متخصص IT از آمریکا، کانادا، مکزیک، بریتانیا، فرانسه، آلمان، هند، ژاپن و چین تهیه شده است، ۶۲ درصد سازمان‌ها معتقدند رمزگذاری برای پیشگیری از دسترسی و رخنه به داده‌ها کافی است. علاوه بر این، ۷۰ درصد سازمان‌ها اظهار داشتند به منظور پیشگیری از سرقت یا از دست رفتن داده‌های SSD از رمزگذاری استفاده می‌کنند و ۳۵ درصد نیز گفتند برای این کار، درایوهای خود را مرتباً فرمت می‌کنند. همچنین، وقتی سیستم‌های IT سازمان که حاوی SSDها هستند به آخر عمر خود می‌رسند و بایستی امحا، بازیافت یا فروخته شوند، بیش از نیمی از سازمان‌ها (۵۶ درصد) آن‌ها را به ارائه‌دهندگان خدمات امحا یا بازیافت تجهیزات IT می‌فرستند تا داده‌های روی آن‌ها را پاک کنند یا این کار را به یک مشاور امنیت IT در خارج از سازمان می‌سپارند.

مهم‌ترین یافته‌ها در این گزارش

- SSDها حاوی حجم وسیعی از اطلاعات حساس شخصی و سازمانی هستند. ۴۷ درصد سازمان‌ها اطلاعات شخصی کارکنان و همچنین داده‌های کسب‌وکار خود را روی SSD ذخیره می‌کنند.
- گم شدن یا سرقت درایوها و افشای داده‌ها توسط برخی کارکنان برای کسب منافع شخصی، جزو چالش‌های کم‌اهمیت در امنیت SSD قرار دارند. گم شدن یا سرقت درایوها با هشت درصد و افشای داده‌ها توسط کارکنان با هدف منفعت مالی یا شخصی با پنج درصد، در پایین فهرست چالش‌های امنیت SSD سازمان‌ها قرار دارند.

- سازمان‌ها هنگام انتخاب ارائه‌دهنده خدمات امحا یا بازیافت سیستم‌های IT، کارایی و هزینه را مهم‌تر از امنیت داده‌ها می‌دانند. ۴۹ درصد از سازمان‌ها، کارایی و هزینه را مهم‌ترین عوامل در انتخاب ارائه‌دهنده خدمات امحای سیستم‌های IT می‌دانند. همچنین، تنها ۱۶ درصد سازمان‌ها توانایی ارائه‌دهندگان در حذف دائمی تمام داده‌ها را مد نظر قرار می‌دهند و ۱۳ درصد از سازمان‌ها، گواهینامه‌ها و توصیه‌های مؤسسات و اتحادیه‌ها را در انتخاب خود دخیل می‌کنند.
- اگرچه میزان اعتماد به تمهیدات امنیت SSD بالا است، اما نظارت بر ارائه‌دهندگان خدمات امحا یا بازیافت سیستم‌های IT جزو اولویت‌های پایین است. اگرچه ۸۹ درصد پاسخ‌دهندگان به این نظرسنجی مطمئن هستند که دسترسی یا رخنه به داده‌ها پس از امحا، بازیافت یا فروش SSDها امکان‌پذیر نیست، اما ۲۷ درصد آن‌ها اذعان کردند هیچ گونه فرایند رسمی برای نظارت بر نحوه پاک کردن داده‌ها از روی SSD توسط این ارائه‌دهندگان ندارند.

اهمیت حفاظت از داده‌های SSD

ریچارد استینون، مدیر راهبردهای شرکت Blancco، عنوان کرد: «نتایج این نظرسنجی نشان‌دهنده مشکلاتی است که بسیاری از سازمان‌ها برای مدیریت، ذخیره‌سازی و حفاظت از داده‌های SSD با آن‌ها مواجه هستند. این یافته‌ها همچنین بر وجود مشکل بزرگ‌تری در امنیت داده‌ها دلالت می‌کنند. بسیاری از سازمان‌ها و اشخاص برای پیشگیری از گم شدن یا سرقت داده‌های SSD و کاهش احتمال وقوع رخنه به داده‌های خود، اعتماد و اتکای زیادی به روش‌های رمزگذاری و فرمت مجدد درایوها دارند. اما رمزگذاری داده‌ها نیز چالش‌های امنیتی خاص خود را دارد که اغلب هنگام حفاظت از داده‌های SSD نادیده گرفته می‌شوند. تجزیه‌وتحلیل ۲۰۰ درایو مستعمل که از سایت eBay و Craigslist خریداری شده بودند، نشان داد که فرمت مجدد SSDها ممکن است منجر به بازیابی و افشای انواع مختلف اطلاعات شخصی و سازمانی شود. سازمان‌ها به هیچ وجه نباید در نحوه مدیریت و پاک کردن SSDها سهل‌انگاری کنند. در غیر این صورت، وقوع رخنه به داده‌هایشان بسیار محتمل خواهد بود».

نمونه‌ای از چنین رویدادی، رخنه اخیر به داده‌های شرکت بیمه پزشکی Centene بود. در ماه ژانویه سال ۲۰۱۶، این شرکت شش هارد درایو خود را گم کرد. این درایوها بخشی از یک پروژه داده‌محور بودند که از نتایج آزمایشگاهی برای بهبود نتایج پزشکی بیمه‌شدگان استفاده می‌کرد. درایوهای گم‌شده حاوی اطلاعات پزشکی حدود ۹۵۰ هزار نفر از بیمه‌شدگان به همراه نام، تاریخ تولد، شماره تأمین اجتماعی و شماره شناسایی آن‌ها بودند.

منبع: www.helpnetsecurity.com

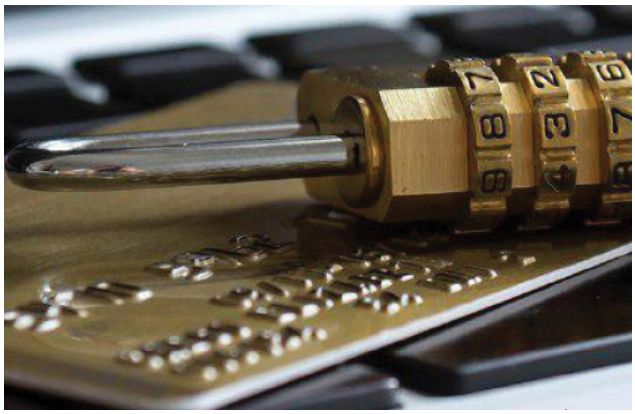
تقابل مقررات و امنیت

در سخنرانی کلیدی همایش Security BSides امسال، به مسئله تقابل امنیت و مقررات پرداخته شد. در این جلسه، از سه مسئله تعدد چارچوب‌های مقرراتی، پیروی از مقررات به عنوان یک نمایش امنیتی و زیاد از حد وسواس به خرج دادن در بررسی همه چیز به عنوان چالش‌های اصلی در مسیر حفظ تعادل میان اجرای تجربیات برتر امنیتی و پیروی از مقررات یاد شد.

رابرت وود هنگام ارائه سخنرانی کلیدی در همایش Security BSides 2017 در سان‌فرانسیسکو، موضوع مبارزه طولانی‌مدت میان امنیت و مقررات را مطرح کرد و برخی چالش‌های کلیدی در اجرای تجربیات برتر امنیتی در کنار پیروی از مقررات را مورد بحث قرار داد. در این جلسه که «شنا بر خلاف جریان رودخانه: مقررات در برابر امنیت»[1] نام داشت، وود به سه مسئله اصلی پرداخت که بسیاری از مشکلات امنیتی و مقرراتی فعلی را ایجاد نموده‌اند. وود توضیح داد که مسئله اول به این حقیقت مربوط است که در حال حاضر، هزاران هزار چارچوب مقرراتی مختلف وجود دارد و ما «در حال غرق‌شدن در پیچیدگی‌های مربوط به پیروی از مقررات» رها شده‌ایم. این امر باعث می‌گردد تیم‌های امنیتی که همین الان نیز تحت فشار کاری فراوانی قرار دارند، با مسائل اضافی بیشتری درگیر شوند.

مسئله دوم، موضوع «پیروی از مقررات به عنوان یک نمایش امنیتی» است. این نمایش در حال حاضر به روالی عادی برای شرکت‌ها تبدیل شده است تا هنگام مواجهه با ممیزی‌ها، خود را به بهترین شکل ممکن نمایش دهند و از خود تصویری به عنوان یک شرکت تابع مقررات امنیتی و قانون‌مدار از نظر موازین کسب‌وکاری ارائه نمایند. با این حال، نه تنها این تصویر غالباً تصویری واقع‌گرایانه از میزان تبعیت آنان از مقررات نیست؛ بلکه به علت وجود محدودیت‌های بودجه‌ای، چارچوب‌های کنترلی به‌کاررفته معمولاً در پوشش دادن برخی بردارهای حمله[2] بسیار رایج، نظیر مهندسی اجتماعی[3]، ناتوان هستند. در نهایت، وود با این بیان به آخرین مشکل اشاره کرد: وسواس «هیچ چیز نباید از چشم پنهان بماند». در این وضعیت، افراد چنان مشتاق و درگیر ردگیری تمامی کنترل‌ها هستند که تجربیات برتر امنیتی را فراموش می‌کنند و نسبت به این که آیا کنترل‌های پیاده‌سازی‌شده حقیقتاً کارامد هستند یا خیر، غافل می‌گردند.

وود ادامه داد: «موقعیت کنونی ما بدین ترتیب است یا حداقل این موقعیتی است که ما در آن قرار داشته‌ایم. بنابراین اکنون زمان آن فرا



رسیده است تا از خود بپرسیم که چگونه می‌توانیم این شرایط را تغییر دهیم». سپس، موارد زیر را به عنوان راهبردهایی مفید برای ایجاد این تغییر پیشنهاد داد:

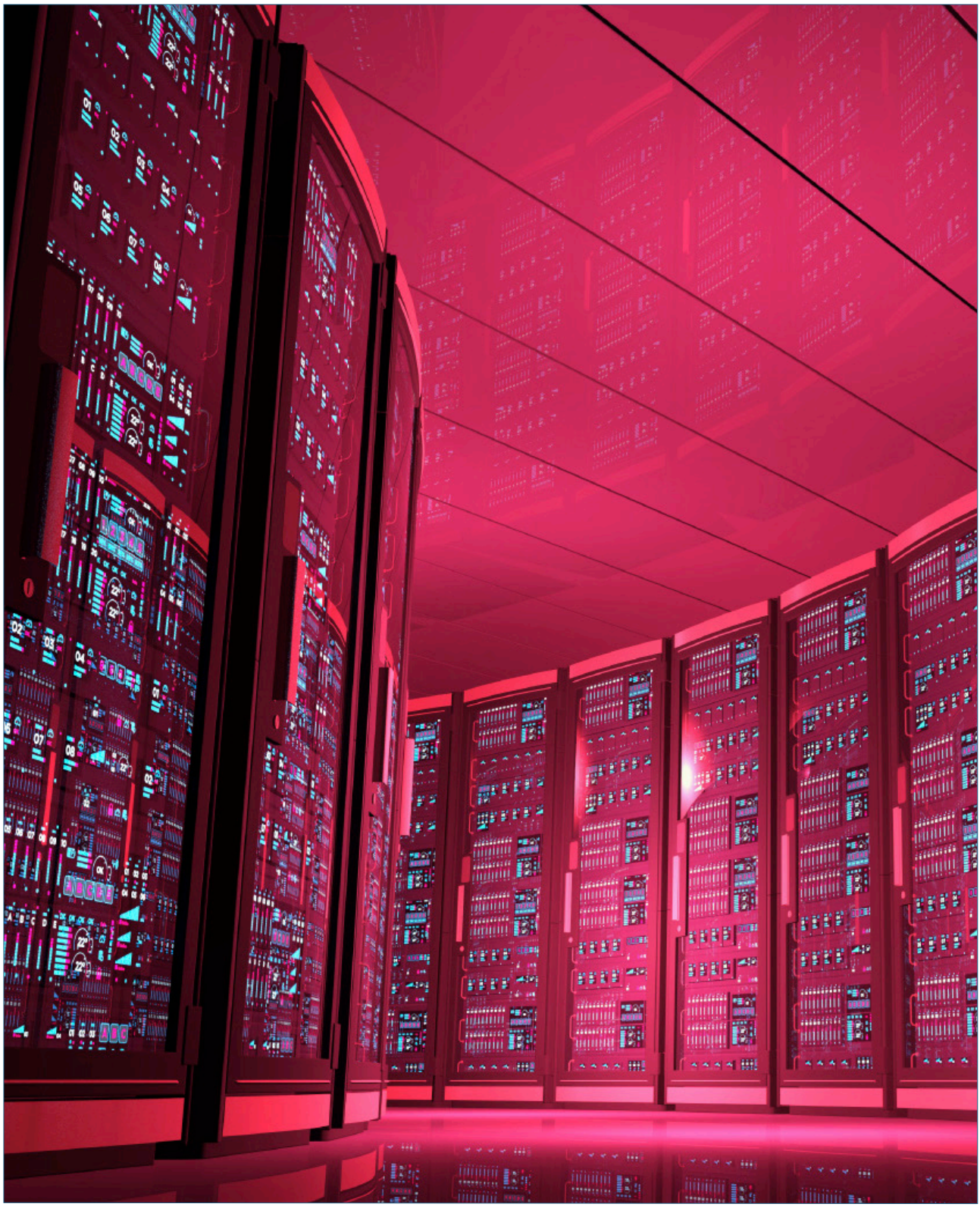
- افراد و تشکیلاتی را که می‌توانند در ایجاد این تغییرات یاری‌دهنده باشند، بیابید؛
- بفهمید مهم‌ترین مسائل برای آن افراد و تشکیلات چه هستند؛ آیا مسئله تماماً به مقررات مربوط می‌شود یا وجه امنیت مهم‌تر است؟
- تلاش‌ها و اقدامات خود را آشکار نمایید. از فعالیت در پشت پرده اجتناب کنید و به افراد نشان دهید که چه مقدار کار باید واقعاً انجام شود و این که پیروی از مقررات کار چندانی پیش نمی‌برد؛
- مسئله پیروی از مقررات را برای افرادی که این مسئله حقیقتاً بر روی آن‌ها تأثیرگذار است، به مسئله‌ای شخصی تبدیل کنید؛ با آن‌ها با زبان خودشان ارتباط برقرار نمایید؛
- مهلت زمانی تعیین کنید و افراد را پاسخگو و مسئول بدارید؛
- خودکارسازی را در رویه‌های پیروی از مقررات و پایش میزان پیروی از مقررات پیاده‌سازی نمایید؛ هر چه ما بیشتر از خودکارسازی استفاده کنیم، موقعیت ما بهتر خواهد شد.

سپس، وود استدلال نمود که گام بزرگ دیگر در مسیر مقابله با مشکلات، این است که بپذیریم نیاز داریم توصیفی جدید از بحث مخاطره بیان کنیم. او گفت: «ما باید از این که صرفاً به موارد امنیتی عناوینی چون خطر کم، متوسط و زیاد نسبت بدهیم، فاصله بگیریم؛ زیرا این عناوین ممکن است توسط افراد مختلف به شکل کاملاً متفاوتی تفسیر گردند». وود ادامه داد: «من تأکید می‌کنم که باید هر چه سریع‌تر به سمت سنجش و آزمون با ارقام و اعداد روی بیاورید. بحث و جدل نمودن و باطل خواندن آمار و ارقام بسیار دشوارتر از باطل خواندن کیفیت‌هایی نظیر کم، متوسط و زیاد است؛ زیرا هر کسی می‌تواند تفسیر و نظر خودش را درباره این کیفیت‌ها داشته باشد».

منبع: www.infosecurity-magazine.com

۱- Swimming Upstream: Regulation vs Security
۲- attack vectors
۳- social engineering

نواقص عمده در طراحی سیستم‌های کنترل صنعتی



شبکه‌های سیستم‌های کنترل صنعتی (ICS) تبدیل به اهداف ساده‌ای برای هکرها شده‌اند، زیرا این شبکه‌ها فاقد کنترل‌های امنیتی ابتدایی و ساده مانند سیستم‌های احراز هویت هستند و از ارتباطات رمزگذاری‌شده پشتیبانی نمی‌کنند. اگر کنترل‌های امنیتی در این شبکه‌ها وجود نداشته باشند، رفع آسیب‌پذیری‌ها نمی‌تواند مانع از دسترسی خرابکاران به این شبکه‌ها شود.

این یک واقعیت آشکار است که محیط اکثر سیستم‌های کنترل صنعتی بدون در نظر گرفتن افتا ساخته شده‌اند، زیرا این محیط‌ها قبل از پیدایش تهدیدات سایبری طراحی شده‌اند. این شبکه‌ها به مدت چند دهه توسط شکاف‌های هوایی[1] حفاظت شده‌اند و ارتباطی با دنیای بیرون نداشته‌اند (توضیح مترجم: در حفاظت به شیوه شکاف هوایی، شبکه به طور فیزیکی از تمامی شبکه‌ها و دستگاه‌های دیگر مجزا می‌شود). با رواج فناوری‌های تجاری آماده[2] (COTS) در دهه ۱۹۹۰ که جایگزین سخت‌افزارها و نرم‌افزارهای صنعتی اختصاصی و سفارشی شدند و همچنین با افزایش اتصال به اینترنت و شبکه‌های سازمانی، ICSها بیش‌ازپیش در معرض تهدیدات سایبری و نفوذ قرار گرفتند.

تأثیر آسیب‌پذیری‌ها و نواقص طراحی

محیط‌های ICS نیز همانند شبکه‌های IT مستعد آسیب‌پذیری‌های نرم‌افزاری و سخت‌افزاری هستند. طی سال‌های اخیر، تعداد گزارش‌ها از آسیب‌پذیری‌های ICS به میزان چشمگیری افزایش یافته است. با این که چنین آسیب‌پذیری‌هایی می‌توانند مخاطرات زیادی برای سیستم‌های کنترل صنعتی ایجاد کنند، نظیر آسیب‌پذیریِ کشف‌شده در نرم‌افزار Schneider Electric Unity Pro، اما هکرها می‌توانند بدون سوءاستفاده از این آسیب‌پذیری‌ها نیز به یک شبکه ICS نفوذ کنند و در عملیات‌های آن اختلال به وجود آورند. توجه بیش‌ازحد به تعداد زیاد گزارش‌ها از آسیب‌پذیری‌های ICS، یک نکته بسیار مهم را نادیده گذاشته است؛ و آن هم این که حتی وقتی یک سازمان صنعتی تمام آسیب‌پذیری‌های سیستم‌های خود را رفع کرده است، هنوز هم نواقصی در طراحی این سیستم‌ها وجود دارند که هکرها به راحتی می‌توانند از آن‌ها سوءاستفاده کرده و به ICS نفوذ کنند.

شبکه‌های ICS تبدیل به اهداف ساده‌ای برای هکرها شده‌اند، زیرا این شبکه‌ها فاقد کنترل‌های امنیتی ابتدایی و ساده مانند سیستم‌های احراز هویت هستند و از ارتباطات رمزگذاری‌شده پشتیبانی نمی‌کنند. از دید امنیت IT، این یک نقص بزرگ در طراحی این سیستم‌ها است که امنیت کل محیط ICS را تحت تأثیر قرار می‌دهد. این بدان معنی است که تمام افرادی که به شبکه دسترسی دارند می‌توانند کد و پیکربندی کنترلر را تغییر دهند و اختلالاتی جدی در عملیات‌های سیستم ایجاد کنند و تأثیرات فاجعه‌باری بر ایمنی و قابلیت‌اطمینان کارخانه‌ها و تجهیزات صنعتی وارد آورند.

پدیداری[3] و کنترل در شبکه‌های ICS

شبکه‌های ICS فاقد پدیداری لازم هستند (توضیح مترجم: پدیداری بدین معنا است که سیستم به گونه‌ای طراحی و پیاده‌سازی شود که هیچ اقدامی در آن، دور از دید کنترل‌های امنیتی انجام نگیرد). این باعث می‌شود که کارکنان بخش امنیت و مهندسی قادر به شناسایی هکرهایی که به دارایی‌های مهم سازمان نفوذ می‌کنند یا پیمانکارانی که تغییرات غیرمجازی را روی پیکربندی کنترلر اعمال می‌کنند، نباشند. اگر کارکنان ندانند دقیقاً چه اتفاقی در شبکه‌ها می‌افتد، نمی‌توانند حوادث را شناسایی کنند و نسبت به آن‌ها عکس‌العمل نشان دهند؛ حوادثی که ممکن است به واسطه تهدیدات سایبری یا خطای انسانی به وجود بیایند.

به دلیل فقدان کنترل‌های امنیتی، همه افرادی که به شبکه‌های ICS دسترسی دارند می‌توانند عمداً یا سهواً تغییراتی فنی در control-plane کنترلرهایی ایجاد کنند که فرایندهای صنعتی را مدیریت می‌کنند. شناسایی تغییرات control-plane کنترلرها، نظیر به‌روزرسانی کدها و تغییر پیکربندی، بسیار دشوار است. شناسایی این تغییرات ممکن است روزها یا هفته‌ها طول بکشد و مهم‌تر از آن، واکنش به حوادث و بازگرداندن سیستم به وضعیت اصلی خود، کار بسیار سختی است. این عوامل به شدت احتمال اختلالات عملیاتی را افزایش می‌دهند و باعث می‌شوند کاهش تهدیدات به فرایندی پیچیده تبدیل شود که به صرف منابع و زمان زیادی نیاز دارد.

اگر سازمانی بتواند تمام فعالیت‌هایی که روی شبکه ICS رخ می‌دهند را به صورت بلادرنگ پیگیری کند، می‌تواند حوادث را به سرعت شناسایی کند، علت آن‌ها را بیابد و نسبت به فعالیت خرابکارانه یا نادرست واکنش نشان دهد. تا زمانی که هیچ کنترل امنیتی خاصی برای جلوگیری از تغییرات مخرب یا غیرمجاز وجود نداشته باشد، نواقص طراحی ICS همچنان بر وضعیت امنیت آن‌ها تأثیرگذار خواهد بود و آن‌ها را به شدت در معرض نفوذ قرار خواهد داد. اگر کنترل‌های امنیتی در سیستم وجود نداشته باشند، رفع آسیب‌پذیری‌ها نمی‌تواند مانع از دسترسی خرابکاران به کنترلرهای شبکه‌های ICS شود یا مخاطرات نفوذ را کاهش دهد.

منبع: www.securityweek.com

۱- air-gap

۲- commercial off the shelf

۳- visibility

عواقب افشای آسیب‌پذیری‌ها در سیستم‌های کنترل صنعتی

فضای سیستم‌های کنترل صنعتی[1] (ICS) بسیار متفاوت از فضای مرسوم حوزه IT است و افشای آسیب‌پذیری‌ها در این حوزه، یک شمشیر دولبه و بسیار تیز است؛ چرا که پیش از تلاش برای عیب‌یابی و به‌روزرسانی این آسیب‌پذیری‌ها، راه را برای ورود مهاجمان سایبری باز می‌کنیم.

طی سال گذشته، خطوط قرمز ICSها که تصور می‌شد هکرها نمی‌توانند از آن‌ها عبور کنند، به شدت کم‌رنگ شده است. اگرچه هنوز حملات مزاحم و مخرب به این سیستم‌ها فراگیر نشده‌اند، اما این حملات دیگر از حالت نظری خارج شده‌اند و واقعیت یافته‌اند. ICSها می‌توانند هدف خوبی برای جنگ‌های سایبری باشند. با این حال حتی اگر سناریوی جنگ سایبری را نیز نادیده بگیریم، ICSها برای نسل جدید مجرمان سایبری که از باج‌افزارها[2] استفاده می‌کنند نیز اهداف جذابی به نظر می‌رسند. همچنین ممکن است این حملات به سمت سیستم‌ها و شبکه‌های فناوری عملیاتی[3] (OT) که از مهم‌ترین زیرساخت‌های فیزیکی و مجازی جهان پشتیبانی می‌کنند، گرایش پیدا کنند.

با گسترش این تحولات شاهد خواهیم بود که سازندگان قدیمی، راه‌حل‌هایی را با برچسب ICS روانه بازار کنند، نقش‌آفرینانی جدید با راه‌حل‌های هدفمند وارد بازار گردند و موجی از تحقیقات عمومی در مورد آسیب‌پذیری‌های ICS انجام شود. کشف آسیب‌پذیری‌ها و انتشار اخبار آن‌ها جزو اقدامات کارشناسان امنیت است، اما کشف آسیب‌پذیری‌های ICS کار بسیار طاقت‌فرسایی است.

این فضا با فضای مرسوم حوزه IT کاملاً متفاوت است و افشای آسیب‌پذیری‌ها در این حوزه که وسعتی بسیار فراتر از IT را در برمی‌گیرد، یک شمشیر دولبه و بسیار تیز است. وقتی یک آسیب‌پذیری افشا می‌شود، قاعدتاً باید سازندگان سیستم‌های ICS را تحریک کند که راهبردهای طراحی امنیت خود را بهبود بخشند و صاحبان دارایی‌ها را نسبت به بردارهای احتمالی حملات حساس‌تر نماید. اما در واقعیت، نمی‌توان آسیب‌پذیری‌های OT را

۱- industrial control systems
۲- ransomware
۳- operational technology

به سرعت آسیب‌پذیری‌های حوزه IT رفع کرد. در ادامه، علت این موضوع را بررسی می‌کنیم.

تجربه و بلوغ

وقتی بحث به‌روزرسانی و رفع آسیب‌پذیری‌های امنیتی مطرح می‌شود، می‌توان دید که سازندگان ICS راه درازی را در این حوزه پیموده‌اند. با این حال، سطح تجربه و بلوغ آن‌ها هنوز با سطح بلوغ و تجربه دنیای نرم‌افزارهای IT یکسان نیست و آن‌ها معمولاً نمی‌توانند آسیب‌پذیری‌هایی که تازه کشف شده‌اند را با همان سرعت رفع کنند. علت چیست؟ این سازمان‌ها معمولاً نرم‌افزارها و سخت‌افزارهای خود را با تمرکز بر ویژگی‌هایی نظیر قابلیت اطمینان، عملکرد بلادرنگ و کار بی‌وقفه تولید می‌کنند و تمرکز اصلی آنان روی امنیت نیست؛ به همین دلیل، تولیدات آنان توسط مهندسان طراحی می‌شوند، نه کارشناسان امنیت. البته این روند در حال تغییر است؛ زیرا انتظار می‌رود که مهندسان ICS نیز از یک چرخه توسعه امن و قابل‌قبول پیروی کنند. این موضوع به وضوح در استانداردهای ISA و IEC 62443-4-1 که قرار است در سال ۲۰۱۷ منتشر شوند، بیان شده است. با این حال، تحقق این تغییر در صنعت، به چند سال زمان نیاز دارد.

چرخه عمر طولانی

چرخه عمر مؤلفه‌های ICS می‌تواند بین ۲۵ تا ۳۵ سال باشد. بیشتر فناوری‌های فعلی از نظر پشتیبانی، در پایان چرخه عمر خود قرار دارند. محققان آسیب‌پذیری‌هایی را در مؤلفه‌های رایج ICS افشا کرده‌اند و مشکلاتی را بیان کرده‌اند که هرگز رفع نخواهند شد. این آسیب‌پذیری‌ها را به عنوان آسیب‌پذیری‌های «روز ابد»[۴] نام‌گذاری کرده‌اند. به عنوان مثال، طبق یافته‌های گزارش جدید فایرآی، در ۳۳ درصد آسیب‌پذیری‌های افشاشده هیچ به‌روزرسانی خاصی هنگام افشای آن‌ها وجود نداشته است.

به‌روزرسانی چیست؟

به‌روزرسانی و رفع آسیب‌پذیری‌های ICS منوط به میزان استفاده صاحبان یا اپراتورها از این سیستم‌ها است. اما در این موضوع، مغایرتی با حوزه امنیت وجود دارد، زیرا:

- اکثر صاحبان این سیستم‌ها یا اپراتورها نمی‌توانند هزینه وقفه در سیستم‌ها برای نصب به‌روزرسانی‌ها را بپردازند. کسب‌وکار این افراد تولید است، نه اداره شبکه‌های امن. این یکی از تفاوت‌های بزرگ این حوزه با IT است. در سطح دو و سه شبکه‌های ICS که دارای سیستم‌های مبتنی بر ویندوز هستند ممکن است امکان به‌روزرسانی سیستم‌ها وجود داشته باشد؛ اما در سطح یک که کنترلرهای منطقی قابل‌برنامه‌نویسی[۵] (PLC) قرار دارند، برای به‌روزرسانی ثابت‌افزار[۶] معمولاً باید PLCها و کنترلرها را از شبکه خارج کرد. در این صنعت، قطع سیستم به ضرر کسب‌وکار است؛ در نتیجه به‌روزرسانی نیز صورت نمی‌گیرد.
- اکثر صاحبان یا اپراتورها شکاف میان IT و OT را به طور کامل پر نکرده‌اند؛ یعنی چالش‌های سازمانی مانع به‌روزرسانی می‌شوند. مسئولیت سیستم‌های OT بر عهده مهندسان است و آنان مسائل امنیتی را به قدر کافی درک نمی‌کنند. تیم‌های امنیت IT مسئول امنیت هستند، اما به دلیل تأثیر منفی قطعی سیستم‌ها بر کسب‌وکار، نمی‌توانند سیاست‌های خود را اعمال کنند.
- شناسایی آسیب‌پذیری‌ها و به‌روزرسانی آن‌ها وقتی از عهده راهبر یا اپراتور بر می‌آید که وی دقیقاً بداند چه چیزی در شبکه قرار دارد. در شبکه‌های صنعتی این موضوع اصلاً رعایت نمی‌شود. در نتیجه، تا زمانی که ذی‌نفعان از آگاهی و پدیداری[۷] بهتر و عمیق‌تری نسبت به دارایی‌های خود برخوردار نباشند، چرخه شناسایی و به‌روزرسانی آسیب‌پذیری‌ها کاری از پیش نخواهد برد (توضیح مترجم: پدیداری، بدین معنا است که سیستم به گونه‌ای طراحی و پیاده‌سازی شود که هیچ اقدامی در آن، دور از دید کنترل‌های امنیتی انجام نگیرد).

تحمیل سازندگان ICS برای به‌روزرسانی

در حوزه IT می‌توان از طریق افشای آسیب‌پذیری‌ها، سازنده را مجبور به ارائه بسته به‌روزرسانی کرد؛ اما در ICS چنین نیست. حوزه ICS با دنیایی که به آن عادت داریم، فرق دارد. افشای آسیب‌پذیری‌های ICS قبل از عرضه به‌روزرسانی توسط سازنده، تنها به نفع مجرمان سایبری است. این افشاها باعث می‌شود مهاجمان برای راه‌اندازی حملات خود به مهارت بالایی نیاز نداشته باشند. محققان کارکشته در این حوزه واقعیت مهمی را در مورد امنیت ICS عنوان می‌کنند و آن هم این است که برای هک یک فرایند در شبکه ICS نیازی به اکسپلویت جدیدترین و بزرگ‌ترین آسیب‌پذیری‌ها نیست. شکاف‌های امنیتی در این سیستم‌ها به شدت گسترده هستند و به عیب‌یابی نیاز دارند. از این رو، هکرهای ماهر می‌توانند از راه‌های بی‌شماری برای ورود به این سیستم‌ها استفاده کنند و دیگر لازم نیست با افشای آسیب‌پذیری‌ها، روش‌های حمله به فضای ICS را به هکرهای مبتدی نیز یاد دهیم.

به عنوان نتیجه‌گیری باید گفت که نمی‌توان دقت و حساسیتی که صنعت امنیت در مورد آسیب‌پذیری‌های محیط IT دارد را به آسیب‌پذیری‌های محیط ICS بسط داد. در ICS، همکاری با همه افراد و سازمان‌ها اهمیتی حتی بیشتر از حوزه IT خواهد داشت. در نتیجه، ما به عنوان محققان امنیت باید به صاحبان و سازندگان ICS کمک کنیم تا بر حل مشکلات سیستمی تمرکز کنند و تلاش‌های خود را در رفع مسائلی که ظاهراً خبرساز هستند اما راه‌حل ماندگاری ارائه نمی‌کنند، هدر ندهند.

منبع: www.darkreading.com

۴- forever-day

۵- Programmable Logic Controllers

۶- firmware

۷- visibility

آینده افتا در سیستم‌های کنترل صنعتی

حملات سایبری به سیستم‌های کنترل صنعتی (ICS)، طیف گسترده‌ای از صنایع و زیرساخت‌های حساس را تحت تأثیر قرار می‌دهد، زیرا همه این صنایع از تجهیزاتی استفاده می‌کنند که توسط تعداد مشخصی از سازندگان تولید می‌شوند. شواهدی وجود دارد که نشان می‌دهد در آینده بر شدت و تعداد این حملات افزوده خواهد شد.

از ابتدای سال جدید میلادی شاهد انتشار اخبار مربوط به وقوع چندین حادثه امنیتی در سیستم‌های کنترل صنعتی بودیم. رسانه‌ها معمولاً این اخبار را با حساسیت زیادی منتشر می‌کنند. در نتیجه، میزان آگاهی و نگرانی از حملات سایبری به زیرساخت‌های حساس صنعتی در سراسر جهان افزایش یافته است. می‌توان گفت که در ادامه سال ۲۰۱۷، امنیت سیستم‌های کنترل صنعتی همچنان یکی از موضوعات داغ رسانه‌ها خواهد بود. شواهد این امر را در ادامه بررسی می‌نماییم:

۱. افزایش تهدیدات ناشی از بدافزارهای جدید ICS

در آینده‌ای نزدیک شاهد پیدایش بدافزارهای جدیدی خواهیم بود که فناوری‌های ICS را هدف قرار می‌دهند و به پروتکل‌های مهندسی این سیستم‌ها حمله می‌کنند تا عملکرد کنترلرهای منطقی قابل‌برنامه‌نویسی (PLC) و دیگر کنترلرهای صنعتی را تغییر دهند. اگر این نوع بدافزارها به طور افسارگسیخته در فضای سایبری منتشر شوند، طیف گسترده‌ای از صنایع و زیرساخت‌های حساس را تحت تأثیر قرار خواهند داد؛ چراکه همه این صنایع از تجهیزاتی استفاده می‌کنند که توسط تعداد محدودی از سازندگان تولید

می‌شوند. دانش و امکانات لازم برای ساخت این نوع بدافزارها مدتی است که وجود دارد. تنها دلیل عدم ساخت آن، نگرانی از تأثیرات سیاسی و فیزیکی احتمالی چنین ابزار مخربی است.

۲. آغاز جنگ‌های فیزیکی-سایبری

برای نخستین بار در تاریخ آمریکا، کلمات «حمله سایبری»، «هک» و «جنگ سایبری» تبدیل به اصلی‌ترین موضوعات در انتخابات ریاست جمهوری شدند. برخی از مقامات عالی‌رتبه آمریکا، حوادث اخیر مربوط به هک سازمان‌های آمریکایی توسط کشورهای دیگر را به عنوان «اقدامات جنگی» طبقه‌بندی کرده‌اند. گستره این میدان نبرد به سرعت افزایش می‌یابد و به زودی دستگاه‌هایی ساخته خواهند شد که برخلاف هدف فعلی حملات سایبری که انتشار داده‌های مسروقه است، تأثیر گسترده‌تری بر روی اهداف خود خواهند داشت.

وقوع یک حمله افسارگسیخته در سیستم‌های ICS می‌تواند سازمان‌هایی را تحت تأثیر قرار دهد که اصولاً هدف این حمله نبوده‌اند. به عنوان مثال، اکسپلویتی که برای حمله به یک PLC در یک پالایشگاه نفت ساخته شده است می‌تواند به آسانسورها، توربین‌ها یا تجهیزات و فرایندهای صنعتی دیگری نیز که از دستگاه‌های تولیدشده توسط سازنده یکسانی استفاده می‌کنند آسیب برساند.

۳. رواج بیشتر هکتیویسم[1] در ICS

با توجه به تغییرات سیاسی اخیر در بریتانیا، آمریکا و مناطق دیگر جهان، کاملاً مشخص است که یک تغییر ایدئولوژیک در جهان در حال روی دادن است. ممکن است این تغییر باعث شود برخی افراد از حقوق اجتماعی خود محروم شوند و به اقدامات خشن، اعتراضات سایبری یا تروریسم سایبری تمایل پیدا کنند. گروه‌های هکتیویسم به پالایشگاه‌های پتروشیمی، سکوهای حفاری نفت و دیگر زیرساخت‌های صنعتی حمله خواهند کرد تا فجایع زیست‌محیطی ایجاد کنند و بدین طریق، توجه افکار عمومی را به سمت مشکلات خود جلب کنند؛ زیرا روش‌های قدیمی خرابکاری سایبری دیگر چندان برای افکار عمومی جذاب نیستند.

۴. نیروگاه‌ها، هدف اخاذی سایبری

امروزه تمام افراد در معرض اخاذی سایبری قرار دارند. با از بین رفتن شکاف‌های هوایی[2] در شبکه‌های صنعتی، مهاجمان سایبری به دستگاه‌های فیزیکی حمله خواهند کرد تا از اپراتورهای این تجهیزات، اخاذی کنند (توضیح مترجم: در حفاظت به شیوه شکاف هوایی، شبکه به طور فیزیکی از تمامی شبکه‌ها و دستگاه‌های دیگر مجزا می‌شود). باج‌افزارها،[3] سیستم‌های اسکادا[4] و ICS و حتی PLC ها را آلوده خواهند کرد. در حملات باج‌افزارها معمولاً پیامی ظاهر می‌شود که می‌گوید فایل‌های شما رمزگذاری شده‌اند؛ اما این پیام در سیستم‌های اسکادا چنین خواهد بود: «PLCهای شما در عرض ۲۴ ساعت خاموش خواهند شد، مگر این که مبلغ باج را پرداخت کنید».

۵. دستیابی مهاجمان به «دکمه قرمز»

امروزه تقریباً به راحتی می‌توان در شبکه‌های ICS رخنه کرد. از این رو، روزبه‌روز خرابکاران بیشتری به این شبکه‌ها دسترسی پیدا خواهند کرد؛ چه خرابکاران سیاسی و چه مجرمان. خرابکاران از این دسترسی برای وارد کردن آسیب‌های سریع و موقت استفاده نخواهند کرد، بلکه آن را به عنوان یک «دکمه قرمز» به کار می‌گیرند که به عنوان بخشی از یک حمله بزرگ‌تر یا اهرم فشار در مذاکرات عمل می‌کند.

۶. افزایش اتصال زیرساخت‌های فیزیکی به اینترنت

افزایش ناگهانی دستگاه‌های مربوط به ICS که به ابر و شبکه‌های دیگر متصل می‌شوند، منجر به استفاده از انواع بیشتری از CPUها و تجهیزات مربوط به شبکه در ICS می‌شود و این تجهیزات نیز جزو اهداف حملات مجرمان سایبری قرار می‌گیرند. سازندگان روزبه‌روز محصولات بیشتری را وارد بازار می‌کنند که قابلیت مدیریت از راه دور دارند، سازگار با ابر هستند یا قابلیت‌های ارتباطات بی‌سیم دارند. بنابراین، افزایش پیچیدگی و قابلیت اتصال شبکه‌های ICS باعث می‌شود این شبکه‌ها بیش از پیش در معرض تهدیدات خارجی قرار بگیرند.

نتیجه‌گیری

اگر این پیش‌بینی‌ها در مورد تهدیدات صنعتی درست از آب درآیند، یکی از مهم‌ترین نگرانی‌ها این است که احتمال بروز آسیب‌های جانبی در سطح گسترده، بسیار بالا است. از آنجا که این حملات، فناوری‌های خاص ICS را هدف می‌گیرند و بیشتر این فناوری‌ها در طیف وسیعی از صنایع مورد استفاده قرار می‌گیرند، وقوع یک حمله افسارگسیخته در این سیستم‌ها می‌تواند سازمان‌هایی را تحت تأثیر قرار دهد که اصولاً هدف این حمله نبوده‌اند. به عنوان مثال، اکسپلویتی که برای حمله به یک PLC در یک پالایشگاه نفت ساخته شده است می‌تواند به آسانسورها، توربین‌ها یا تجهیزات و فرایندهای صنعتی دیگری نیز که از دستگاه‌های تولیدشده توسط سازنده یکسانی استفاده می‌کنند آسیب برساند.

منبع: www.securityweek.com

۱- Hacktivism
۲- air-gaps
۳- Ransomware
۴- SCADA

چالش‌های فناوری و امنیت:

هدف گرفتن اینترنت اشیا در زیرساخت‌های حیاتی

بدون شک، تعداد دستگاه‌های اینترنت اشیا (IoT) در آینده به رقمی بسیار بزرگ خواهد رسید. اما در کنار هر فناوری جدیدی، پای مسائل امنیتی نیز در میان است. طبق آمارها، بیشتر دستگاه‌های متصل به اینترنت اشیا از حفاظت کافی برخوردار نیستند و با این که به‌کارگیری فناوری IoT در زیرساخت‌های حیاتی با مزیت‌های فراوانی همراه است، اما مخاطراتی جدی نیز در پی دارد؛ کافی است به حادثه باتنت Mirai نگاهی انداخت.

فناوری اینترنت اشیا در حال حاضر فراگیرتر از آنی است که بسیاری از کاربران تصور می‌کنند. سیستم‌های زیرمجموعه IoT در گستره‌ای از محیط‌ها و کاربردها، حتی خارج از حلقه‌های مشتریان، پدیدار می‌شوند. امروزه، تمامی گروه‌ها، از کسب‌وکارهای سازمانی گرفته تا حکومت‌های شهری، در حال بهره‌برداری از دستگاه‌های هوشمند و مجهز به بلوتوث و اینترنت هستند تا قابلیت‌های حیاتی متعددی را امکان‌پذیر سازند.

بررسی این محیط نشان می‌دهد که پیش‌بینی‌های بلندپروازانه برخی صاحب‌نظران در صنعت در خصوص این حوزه چندان هم دور از ذهن نیست. بر اساس گفته لئو سان، یکی از کارشناسان مؤسسه خدمات مالی The Motley Fool، سیسکو برآورد نموده است که تا سال ۲۰۲۰ مجموعاً ۵۰ میلیارد دستگاه به شبکه IoT متصل خواهند شد؛ از طرف دیگر، شرکت اینتل حتی از این فراتر رفته و پیش‌بینی کرده است که تا سال ۲۰۲۰ بالغ بر ۲۰۰ میلیارد دستگاه در مجموعه IoT قرار خواهند گرفت.

اکنون که این دستگاه‌ها هر روز سهم بیشتری از زیرساخت‌های حیاتی در شهرها و کسب‌وکارها را در سراسر جهان تشکیل می‌دهند، IoT نیز جذابیت بیشتری برای هکرها یافته است. سیستم‌های هوشمند زیر حمله مهاجمان قرار دارند و سازمان‌های مجری و پشتیبانی‌کننده این فناوری باید گام‌های مناسبی برای حفاظت از این فناوری بردارند.

توصیفی دقیق‌تر از موتور جستجوی Shodan

محققان شرکت ترند مایکرو با نام‌های نومان هیوک، استفان هیلت و ناتاشا هلبرگ، اخیراً بررسی عمیق‌تری روی Shodan انجام داده‌اند. Shodan یک موتور جستجو است که دستگاه‌های متصل به اینترنت، از جمله دستگاه‌های IoT، را فهرست می‌نماید. بر اساس یافته‌های این محققان، تعداد زیادی از دستگاه‌های نام‌برده در Shodan به خاطر پیکربندی ضعیف و ملاحظات امنیتی دیگر، در معرض دسترسی و حفاظت‌نشده هستند. در حقیقت، این محققان موفق به شناسایی شهرهایی شدند که بیشترین تعداد دستگاه‌های

حفاظت‌نشده در آن‌ها قرار دارد. در ذیل، خلاصه‌ای از یافته‌ها و رتبه‌بندی بزرگ‌ترین شهرهای آمریکا از لحاظ این فهرست ارائه شده است:

- شهر هیوستن دارای بیشترین تعداد وب‌کم‌های حفاظت‌نشده است و شیکاگو نیز با بیش از یک هزار و ۵۰۰ دستگاه وب‌کم حفاظت‌نشده در جایگاه بعدی قرار دارد.
- شهر لس‌آنجلس رتبه اول از نظر وب‌سرورهای حفاظت‌نشده را به خود اختصاص داد و هیوستن در جایگاه دوم قرار گرفت.
- مسئله جالب توجه آن است که شهرهای کوچک‌تر، نظیر لافایت در ایالت لوئیزیانا و سَنت‌پاول در ایالت مینسوتا، دارای بیشترین دارایی‌های سایبری حفاظت‌نشده در دولت هستند و در این زمینه، از شهرداری‌های بزرگ‌تری نظیر دنور و واشنگتن نیز پیشی گرفته‌اند.

اما این تنها آغاز راه است؛ مقاله شرکت ترند مایکرو با عنوان «شهرهای آمریکا در معرض خطر: صنایع و سیستم‌های کنترل صنعتی»[1] نشان داد که دستگاه‌های فعال در بخش آموزش و پرورش، خدمات رفاهی و خدمات اضطراری نیز هیچ دفاعی در برابر حملات ندارند. به طور کلی، شهرهای هیوستن و لافایت دارای بیشترین تعداد دستگاه‌های حفاظت‌نشده در بخش ارائه خدمات اضطراری هستند. علاوه بر این، در حالی که تعداد قابل توجهی از دستگاه‌های حفاظت‌نشده در بخش آموزش و پرورش در سرتاسر آمریکا وجود دارد، در این میان فیلادلفیا با ۶۵ هزار دستگاه نهایی حفاظت‌نشده و آسیب‌پذیر، رتبه اول را به خود اختصاص می‌دهد.

با توجه به این که شهرها امروزه از سیستم‌های هوشمند بیشتر بهره‌برداری می‌کنند، آیا دستگاه‌های حفاظت‌نشده، مسئولان و شهروندان را در معرض مخاطرات قرار می‌دهند؟

همپوشانی IoT و زیرساخت‌های حیاتی، دست‌مایه قدرت هکرها

هنگامی که سیستم‌های مربوط به زیرساخت‌های حیاتی، نظیر آن‌هایی که در مواقع اضطراری به کار می‌روند، با فناوری ترکیب می‌شوند، شهرها از مزایای فراوانی برخوردار می‌گردند. استفاده از سیستم‌های متصل به شبکه آسان‌تر است و استفاده رایج و متداول از آن می‌تواند در مواقعی که زمان از اهمیت فراوانی برخوردار است، تأثیر بزرگی داشته باشد. اما در صورتی که به شکل صحیح از این سیستم‌ها حفاظت نشود، ممکن است افراد نادرستی به آن‌ها دسترسی یابند و برای کارهایی استفاده شوند که در آغاز به هیچ وجه مد نظر نبودند.

هکرها در همین چند ماه اخیر، قدرت و توانمندی‌های خود را در شهر دالاس آمریکا به منصه ظهور گذاشتند و نشان دادند که در صورت همپوشانی زیرساخت‌های حیاتی و IoT با فعالیت‌های مجرمانه سایبری، چه وقایعی می‌تواند رخ دهد. روزنامه گاردین از واقعه‌ای در شهر دالاس گزارش داد که اهالی این شهر در نیمه‌های شب با به صدا درآمدن آژیر خطر در سراسر شهر از خواب بیدار شده بودند. با این حال، هیچ رخداد خاصی وجود نداشت که مسبب به صدا درآمدن آژیر اضطراری باشد.

مهاجمان توانسته بودند سیستم آژیر اضطراری را هک نمایند و کنترل آن را در اختیار بگیرند و سپس، در ساعت ۲۳ و ۴۲ دقیقه آژیر خطر را فعال کردند. این سیستم ۱۵ بار و هر بار به مدت ۹۰ ثانیه به صدا در آمد و مسئولان نهایتاً در ساعت یک و ۱۷ دقیقه بامداد توانستند آن را غیرفعال سازند.

هنگامی که سیستم‌های مربوط به زیرساخت‌های حیاتی، نظیر آن‌هایی که در مواقع اضطراری به کار می‌روند، با فناوری ترکیب می‌شوند، شهرها از مزایای فراوانی برخوردار می‌گردند. استفاده از سیستم‌های متصل به شبکه آسان‌تر است و استفاده رایج و متداول از آن می‌تواند در مواقعی که زمان از اهمیت فراوانی برخوردار است، تأثیر بزرگی داشته باشد. اما در صورتی که به شکل صحیح از این سیستم‌ها حفاظت نشود، ممکن است افراد نادرستی به آن‌ها دسترسی یابند و برای کارهایی استفاده شوند که در آغاز به هیچ وجه مد نظر نبودند.

راکی واز، رئیس سازمان مدیریت شرایط اضطراری دالاس، بیان داشت: «ما آژیر را در سریع‌ترین زمان ممکن غیرفعال نمودیم و تمامی جوانب احتیاطی و پروتکل‌هایی را که باید به منظور حصول اطمینان از در معرض خطر قرار نگرفتن ۱۵۶ سیستم آژیر خود از آن‌ها پیروی می‌کردیم، در نظر گرفتیم».

مسئولان اطلاعات دقیقی درباره فرایند به‌کاررفته برای هک کردن این سیستم ارائه نکردند؛ اما به نظر آن‌ها، این حادثه از سمت مجرمان سایبری در داخل شهر منشأ گرفته بود. با این که هیچ فردی در خلال این حادثه آسیب ندید، اما این واقعه نشان داد که از چه راه‌هایی می‌توان یک سیستم فناوری حیاتی را در معرض مخاطره قرار داد. نه تنها ساکنان این شهر باید صدای وحشت‌آفرین آژیر اضطراری را برای مدتی طولانی تحمل می‌کردند، بلکه بخش‌های خدماتی شهر نیز درگیر تلاش برای مقابله با این حمله بودند؛ از جمله متصدیان بخش خدمات اضطراری محلی که چهار هزار و ۴۰۰ تماس درباره آژیر اضطراری دریافت کردند و در این میان، فقط ۸۰۰ تماس در یک بازه زمانی ۱۵ دقیقه‌ای در حدود نیمه‌شب برقرار شده بود.

استفاده از بات‌نت‌ها در هک کردن و به دست گرفتن کنترل دستگاه‌های IoT

حمله گروهی از هکرهای متجاوز به سیستم آژیر اضطراری شهر و به

۱- US Cities Exposed: Industries and ICS

دست گرفتن کنترل آن در برابر حادثه‌ای که در ادامه ذکر می‌گردد، بی‌اهمیت جلوه می‌کند. در اواخر سال ۲۰۱۶، گزارش‌هایی درباره باتنت Mirai منتشر گردید؛ نوعی بدافزار بسیار قدرتمند که توانایی حمله به دستگاه‌های IoT و استفاده از دستگاه‌های IoT آلوده برای اجرای حملات بعدی را دارد.

یک متخصص امنیتی به نام برایان کربز در نوامبر سال ۲۰۱۶ گزارش کرد که بدافزار Mirai با موفقیت کنترل دستگاه‌های IoT دارای امنیت ضعیف را در اختیار گرفته است و در حال بهره‌برداری از آن‌ها است؛ از جمله آن دسته از دوربین‌های تحت شبکه (IP) و مسیریاب‌های اینترنتی که ذاتاً سیستم حفاظتی ضعیفی داشتند. در حقیقت، بدافزار Mirai چنان قدرتمند گردید که در پاییز همان سال، وب‌سایت شخصی خود کربز نیز با یک حمله باتنت Mirai با سرعت ۶۲۰ گیگابیت در ثانیه از کار افتاد. پس از گذشت زمانی نه چندان طولانی، رفته‌رفته گزارش‌هایی درباره حمله بدافزار Mirai به کشور لیبریا منتشر شد مبنی بر آن که اقدامات خرابکارانه این بدافزار، زیرساخت مخابراتی این کشور را هدف گرفته بودند.

کوین بومانت، یک معمار امنیتی در انگلیس، نیز به دنبال کربز طی گزارشی نوشت: «ما به واسطه پایش می‌توانیم وب‌سایت‌هایی را ببینیم که در همین کشور میزبانی می‌شوند و طی این حملات غیرفعال می‌گردند. علاوه بر این، یک منبع آگاه و فعال در یکی از شرکت‌های مخابراتی داخل کشور به خبرنگاری گفته است که آن‌ها در خلال این حملات، اتصال‌پذیری اینترنتی نوسان‌داری را دقیقاً در زمان‌های یکسان با حملات تجربه می‌کنند. این حملات به شدت نگران‌کننده هستند؛ زیرا به فرد پشت پرده بدافزار Mirai اشاره می‌کنند که به قدری توانمند است که می‌تواند به طور جدی روی سیستم‌های یک کشور تأثیر بگذارد».

منابع خبری متعدد دیگری نظیر The Hacker News و BBC و ZDNet نیز در ادامه این رخداد را پوشش دادند. با این حال، کربز پس از عدم‌اطمینان نسبت به توانایی بدافزار Mirai برای از کار انداختن کل زیرساخت مخابراتی یک کشور، بررسی‌های بیشتری در این زمینه انجام داد. برخی منابع تأیید نمودند که هکرهای بدافزار Mirai از این باتنت برای انجام حمله‌ای ۵۰۰ گیگابیتی در ثانیه علیه یک ارائه‌دهنده خدمات موبایل در لیبریا استفاده کرده‌اند؛ اما این شرکت از قابلیت حفاظت در برابر حملات DDoS برخوردار بوده است که اندکی پس از آغاز حمله، فعال گردیده بود. در حالی که لیبریا با مشکل عدم ارائه سرویس در سطح ملی مواجه نگردید؛ اما باتنت Mirai و وقوع این حادثه باعث روشن شدن چندین حقیقت بسیار مهم شدند. بدافزار Mirai به خوبی آشکار ساخت که عوامل و افراد خرابکار و مجهز به بدافزارهای مناسب می‌توانند چه کارهایی با دستگاه‌های IoT ناامن انجام دهند؛ این مطلب صحت دارد که قدرت تهاجمی این آلودگی بدافزاری از جانب دستگاه‌هایی تأمین می‌شد که این باتنت را تشکیل می‌دادند و از فعالیت‌های آن پشتیبانی می‌کردند. به این ترتیب، حفاظت مناسب از همه دستگاه‌های متصل به شبکه، از سیستم‌های بزرگ گرفته تا تک‌تک دستگاه‌های نهایی، الزامی و ضروری است.

بدافزار Mirai همچنین پتانسیل و فرصتی را که در سطح شهری و کشوری در حوزه زیرساخت‌های حیاتی برای هکرها وجود دارد، نشان می‌دهد. حملاتی که به این قبیل سیستم‌ها صورت می‌گیرند، خاص و متمایز نیستند؛ با این حال، شدت و تعداد آن‌ها در حال افزایش است.

منبع: blog.trendmicro.com

اخبار کوتاه

دسترسی کارکنان سابق سازمان‌ها به شبکه، تهدیدی جدی

طبق تحقیق شرکت OneLogin، بیش از نیمی از کارکنان سابق سازمان‌ها حتی بعد از ترک همیشگی آن، هنوز به شبکه سازمانی دسترسی دارند. در واقع، کسب‌وکارها در حفاظت از شبکه خود در برابر تهدیدات ناشی از این دسته از کارکنان چندان موفق نبوده‌اند. این در حالی است که به عنوان مثال، حدود یک‌چهارم رخنه به داده‌های سازمان‌ها در انگلیس توسط همین کارکنان صورت گرفته است.

نیروهای داخلی سازمان، هدف حملات خارجی

متخصصان مؤسسه SANS معتقدند با اینکه تهدیدات ناشی از نیروهای خودی همیشه یکی از نگرانی‌های اصلی سازمان‌ها به شمار می‌رود، اما اکثر سازمان‌ها به این مسئله کمتر توجه می‌کنند که در اغلب حملات خارجی، یکی از نیروهای داخلی سازمان که به حساس‌ترین داده‌ها دسترسی دارد، هدف گرفته می‌شود؛ چراکه فریب دادن یک کاربر آسان‌تر از فریب دادن سیستم امنیتی است.

نیروهای داخلی، عامل بیشتر آسیب‌ها به سازمان

طبق نظرسنجی اخیر مؤسسه SANS در خصوص تهدیدات داخلی سازمان‌ها، تنها ۲۳ درصد پاسخ‌دهندگان اعلام کردند که مهاجمان خارجی بیشترین آسیب را می‌زنند. ۳۶ درصد گفتند بدترین رخنه‌ها توسط نیروهای داخلی سازمان و به صورت غیرعمدی صورت می‌گیرد و ۴۰ درصد معتقد بودند بیشترین آسیب توسط آن دسته از نیروهای داخلی سازمان رخ می‌دهد که نیت خرابکارانه دارند. با وجود این آمار، تنها ۱۸ درصد پاسخ‌دهندگان گفتند برنامه‌های رسمی در زمینه واکنش به حوادث ناشی از نیروهای داخلی دارند، ۴۹ درصد در حال تدوین چنین برنامه‌ای هستند و ۳۱ درصد هیچ برنامه رسمی یا حتی آمادگی لازم را برای مقابله با چنین تهدیداتی ندارند.

عدم توانایی نیمی از متخصصان ICS در شناسایی حملات شبکه‌هایشان

طبق تحقیق مؤسسه SANS، ۴۰درصد متخصصان امنیت سیستم‌های کنترل صنعتی نسبت به شبکه‌های ICS خود احاطه کامل ندارند و قادر به شناسایی حملات نیستند. این در حالی است که ۶۹ درصد متخصصان معتقدند تهدیدات مربوط به این سیستم‌ها بسیار جدی و بحران‌آفرین هستند. سه تهدید اصلی این حوزه عبارتند از: دستگاه‌های حفاظت‌نشده، حملات دولتی و باج‌افزارها.

امنیت برنامه‌های کاربردی

طبق نظرسنجی اخیر شرکت SANS با موضوع آینده امنیت برنامه‌های کاربردی، ۴۸ درصد از پاسخ‌دهندگان، آموزش توسعه‌دهندگان را جزو سه فرایند مهم در امنیت برنامه‌های کاربردی دانسته‌اند. تا سال ۲۰۲۰، دانشگاه‌های بیشتری دوره‌های آموزش توسعه امن را برگزار خواهند کرد و مهارت توسعه‌دهندگان نه فقط با معیارهای عملکرد و سرعت ارائه برنامه‌های کاربردی، بلکه به لحاظ میزان امنیت کدهای آنان طبق استانداردهای خاص ارزیابی خواهد شد.

کمبود شدید نیرو در حوزه افتا

طبق گفته مدیرعامل شرکت سیمانتک، در سال ۲۰۱۵ بیش از ۲۰۰ هزار موقعیت شغلی در حوزه افتا خالی ماندند و پیش‌بینی می‌شود که این کمبود نیرو تا سال ۲۰۱۹ به ۱٫۵ میلیون شغل برسد. برای رفع این مشکل، باید درمان‌های موقت را کنار گذاشت و از راه‌حل‌های اساسی استفاده کرد؛ به عبارتی باید مشکل بنیادین ضعف امنیت در کدنویسی نرم‌افزارها را حل نمود.

نسخه جدید باج‌افزار Petya

نسخه جدید باج‌افزار Petya مجداً مراکزی در اوکراین را آلوده کرده است. نسخه جدید این بدافزار از طریق SMB خود را تکثیر می‌نماید و به جای رمز کردن کل فایل‌ها جدول اصلی فایل را رمز می‌کند. همچنین، یک اعتبارنامه جعلی مایکروسافت نیز به فایل‌های آن الصاق شده است. مبلغ تعیین‌شده برای رمزگشایی فایل‌ها ۳۰۰ دلار است و آلودگی اولیه از طریق ایمیل انجام می‌شود. به گزارش برخی منابع، نیروگاه هسته‌ای چرنوبیل نیز به این بدافزار آلوده شده است.

افزایش حملات باج‌افزاری در سال ۲۰۱۷

طبق یک نظرسنجی از ۳۳۰ متخصص IT و افتا، ۶۵ درصد سازمان‌ها در سال ۲۰۱۷ مورد حمله بدافزارها قرار گرفتند. این رقم در سال ۲۰۱۶ حدود ۵۶ درصد بود. در سال ۲۰۱۷، حدود ۲۳ درصد سازمان‌ها با باج‌افزار روبرو شدند که ۹ درصد آن‌ها گفتند باج را پرداخت کردند. در حالی که همه سازمان‌های مورد بررسی اعلام کردند در سال ۲۰۱۶ هیچ باجی پرداخت نکردند.

امکان تشخیص گذرواژه‌های تایپ‌شده از طریق امواج ساطع‌شده مغز

طبق نتایج تحقیقات منتشرشده دانشگاه‌های آلاباما و کالیفرنیا ریورساید، در زمان استفاده از هدست‌های الکتروانسفالوگرافی (EEG) که اغلب در بازی‌های رایانه‌ای مورد استفاده قرار می‌گیرند، امکان تشخیص گذرواژه‌های تایپ‌شده از طریق امواج ساطع‌شده از مغز وجود دارد. در این تحقیق ۴۶ درصد پین‌های چهار رقمی و ۳۷ درصد پین‌های شش رقمی از طریق امواج مغزی به‌درستی تشخیص داده شده‌اند.

کشف آسیب‌پذیری‌هایی در گوشی‌های هوشمند Lenovo VIBE

به گفته محققان امنیتی، گوشی‌های هوشمند Lenovo VIBE دارای آسیب‌پذیری‌هایی هستند که به مهاجم امکان دسترسی فیزیکی به دستگاه را می‌دهند. شرکت Lenovo توضیح داد تنها دستگاه‌هایی که قفل ایمنی مانند پین‌کد یا گذرواژه برای صفحه‌نمایش خود ندارند، در معرض خطر هستند. مهاجم از طریق این آسیب‌پذیری می‌تواند دسترسی روت داشته باشد و دستگاه و برنامه‌های کاربردی را دستکاری کند.

قابلیت‌های مین‌فرم z شرکت IBM

مین‌فریم Z شرکت IBM می‌تواند تمام داده‌های سازمان‌ها را به صورت انتها به انتها رمزگذاری کند. این مین‌فریم می‌تواند بیش از ۱۲ میلیارد تراکنش رمزگذاری‌شده در روز انجام دهد. به گفته این شرکت، در سال ۲۰۱۶ بیش از چهار میلیارد رخنه به داده‌ها صورت گرفت که نسبت به ۲۰۱۵ حدود ۵۵۶ درصد افزایش داشت. از ۹ میلیارد رخنه‌ای که در پنج سال گذشته انجام شد، تنها چهار درصد داده‌ها رمزگذاری شده بودند. تحقیق اخیر IBM نشان داد استفاده گسترده از رمزگذاری یکی از عوامل اصلی در کاهش هزینه ناشی از رخنه به داده‌هاست. هدف این مین‌فریم حفاظت از سیستم‌های بانک‌ها، مراکز بهداشت و درمان، دولت‌ها و عرضه‌کنندگان محصول به مصرف‌کننده در کل دنیا است.