بسمه‌تعالی

چشم‌انداز تهدید برای سامانه‌های کنترل صنعتی در شش‌ماهه‌ی اول سال ۲۰۱۷

فهرست مطالب

۱ مقدمه ۳
۲ حوادث اصلی در شش ماه اول سال ۲۰۱۷ ..... ۳
۲-۱ سلاح سایبری CrashOverride/Industroyer ۳
۲-۲ اختلال در شبکه‌ی دوربین‌های مدار بسته‌ی پلیس واشنگتن ۵
۲-۳ هک‌شدن سیستم هشدار اضطراری دالاس ۵
۲-۴ بات‌نت Persirai IoT ۵
۲-۵ استفاده از نامه‌های الکترونیکی تجاری در حمله به شرکت‌های صنعتی ۶
۲-۶ WikiLeaks: آرشیو سازمان سیا ۷
۲-۷ Shadow Brokers: آرشیو NSA ۸
۳ حملات باج‌افزاری ۸
۳-۱ شیوع WannaCry ۱۱
۳-۲ حمله‌ی ExPetr (Petya) ۱۴
۴ آمار تهدید ۱۶
۴-۱ متدولوژی ۱۶
۴-۲ درصد رایانه‌هایی که موردحمله قرارگرفته‌اند ۱۷
۴-۳ توزیع جغرافیایی حملات بر سامانه‌های خودکارسازی صنعتی ۱۹
۴-۴ بدافزار در سامانه‌های خودکارسازی صنعتی ۲۰
۴-۵ منابع آلوده‌کننده سامانه‌های خودکارسازی صنعتی ۲۰
۴-۶ بسترهای مورداستفاده توسط بدافزار ۲۱
۵ توصیه‌های پیشنهادی ۲۲
۶ نتیجه‌گیری ۲۴

۱ مقدمه

سامانه‌های کنترل صنعتی[۱] به‌منزله‌ی هسته‌ی مرکزی کنترل و نظارت زیرساخت‌های حیاتی نظیر شبکه‌های انتقال و توزیع برق، نیروگاه‌های هسته‌ای، پالایشگاه‌ها، شبکه‌های آب و کارخانه‌های نفت و گاز هستند؛ اما با توجه به قدیمی بودن این سامانه‌ها، به امنیت آن‌ها توجه چندانی نشده است. همچنین امروزه، ادغام سامانه‌های IT با سامانه‌های کنترل صنعتی باعث شده است که حفظ امنیت این سامانه‌ها در مقابل مخاطرات خارجی و از راه دور، ضرورت بیشتری پیدا می‌کند.

اولین گام برای رسیدن به این هدف، شناسایی چشم‌انداز تهدید برای چنین سامانه‌هایی است. در این گزارش، گروه تحقیقاتی آزمایشگاه کسپرسکی، نتایج تحقیقات خود را در مورد چشم‌انداز تهدیدات سامانه‌های کنترل صنعتی در شش‌ماهه‌ی اول سال ۲۰۱۷ ارایه داده است. بر اساس این تحقیقات، کشور ایران جزء ۱۰ کشور اولی است که سامانه‌های کنترل صنعتی آن‌ها به باج‌افزارهای رمزگذاری آلوده‌شده‌اند. همچنین در بین ۱۵ کشوری که بالاترین درصد سامانه‌های کنترل صنعتی موردحمله قرارگرفته را در نیمه‌ی اول سال ۲۰۱۷ دارا بودند، رتبه هفتم را داراست.

۲ حوادث اصلی در شش ماه اول سال ۲۰۱۷

مخاطرات مربوط به سامانه‌های کنترل صنعتی ممکن است ناشی از منابع متعددی باشند، ازجمله‌ی آن‌ها می‌توان به دولت‌ها، گروه‌های تروریستی، کارکنان ناراضی، مشکلات، حوادث، بلایای طبیعی و همچنین اقدامات تصادفی یا مغرضانه‌ی نیروهای داخلی اشاره نمود. در ادامه، برخی از حوادث مربوط به سامانه‌های کنترل صنعتی در شش ماهه‌ی اول سال ۲۰۱۷ شرح داده خواهد شد.

۲-۱ بدافزار CrashOverride/Industroyer

در ماه ژوئن سال ۲۰۱۷، نتایج تحقیقات مربوط به بدافزار CrashOverride/Industroyer منتشر شد. کارشناسان شرکت ESET، Dragos Inc و تعدادی از محققان مستقل به این نتیجه رسیدند که این بدافزار، به‌منظور اختلال در کار سامانه‌های کنترل صنعتی، به‌خصوص پست‌های برق، طراحی شده است. به‌علاوه

[۱] Industrial Control Systems (ICS)

CrashOverride/Industroyer قادر به کنترل مستقیم سوئیچ‌ها و قطع‌کننده‌ها در مدارهای پست الکتریکی است.

این بدافزار با چهار پروتکل IEC 60870-5-101 (aka IEC 101), IEC 60870-5-104 (aka IEC 104), IEC 618 و OLE کار می‌کند که به‌طور گسترده در بخش برق، مدیریت حمل‌ونقل، تأمین آب و سایر زیرساخت‌های حیاتی استفاده می‌شود. توسعه‌دهندگان CrashOverride/Industroyer می‌توانند این برنامه را برای حمله به هر محیط صنعتی که از پروتکل‌های ارتباطی موردنظر استفاده می‌کنند، مجدداً پیکربندی کنند. به احتمال زیاد، این بدافزار برای حمله به سامانه‌های مختلف (به‌جای یک سامانه‌ی خاص) طراحی شده است.

یکی دیگر از ویژگی‌های مهم CrashOverride/Industroyer این است که این بدافزار دارای ابزاری اضافی است که آسیب‌پذیری‌های خانواده‌ی SIPROTEC زیمنس را مورد سوءاستفاده قرار می‌دهد. اگر این بدافزار از این ابزار استفاده کند و ولتاژ از سطح خطرناکی بیشتر شود، آنگاه ممکن است آسیب فقط به خراب شدن منبع‌برق محدود نشود. این حمله می‌تواند با فعالیت نادرست سامانه‌های حفاظتی، موجب آسیب‌دیدگی تجهیزات شود.

کارشناسان ESET معتقدند که CrashOverride/Industroyer ممکن است با قطعی کامل برق شهر کییف (پایتخت اوکراین) در دسامبر سال ۲۰۱۶ ارتباط داشته باشد. با توجه به اظهارات مسئولین ایستگاه برق Ukrenergo، قطع برق در این ایستگاه، به دلیل تأثیر خارجی بر روی سیستم SCADA[۲] آن بود.

قابلیت‌های CrashOverride/Industroyer به مهارت‌های توسعه‌دهندگان و دانش کامل آن‌ها از نحوه‌ی کار سامانه‌های کنترل صنعتی در امکانات برق بستگی دارد. بعید است که این نوع بدافزار بدون دسترسی به سخت‌افزارهایی که در چنین سامانه‌هایی بکار گرفته می‌شوند، قابل توسعه باشد.

این بدافزار احتمالاً پس از Stuxnet، جدی‌ترین تهدید شناخته‌شده برای سامانه‌های کنترل صنعتی است.

[۲] Supervisory Control and Data Acquisition- نظارت کنترل و جمع‌آوری داده‌ها

۲-۲ اختلال در شبکه‌ی دوربین‌های مداربسته‌ی پلیس واشنگتن

در اواسط ماه ژانویه، ۸ روز پیش از آغاز دولت دونالد ترامپ، سیستم نظارت تصویری اداره‌ی پلیس واشنگتن، قطع شد. ۱۲۳ دستگاه از ۱۸۷ دستگاه ذخیره‌سازی داده‌ها که برای ضبط تصاویر ویدئویی دوربین‌های نصب‌شده در اماکن عمومی استفاده می‌شدند، به یک باج‌افزار رمزگذار آلوده شدند. طبق گزارش واشنگتن‌پست، علی‌رغم نزدیکی به مراسم افتتاحیه‌ی ریاست جمهوری، این شهر هیچ باجی پرداخت نکرد و برای بازیابی دستگاه‌های آلوده، نرم‌افزار تمامی آن‌ها به‌صورت آفلاین دوباره نصب شدند.

۲-۳ هک‌شدن سیستم هشدار اضطراری دالاس

در آوریل سال ۲۰۱۷، ساکنین شهر دالاس، عواقب یک حمله‌ی سایبری به سیستم ایمنی را تجربه کردند. در این حمله، در فاصله‌ی ۹۰ دقیقه، تمامی آژیرهای اضطراری شهر (۱۵۶ آژیر خطر) در ۱۵ دوره‌ی ۹۰ ثانیه‌ای به‌صدا درآمدند. مهندسان تنها توانستند آژیرها را در اواخر شب، بعدازاینکه سیستم رادیویی و تکرارکننده‌های آن را به‌طور دستی خاموش کردند، متوقف کنند. بدون افشای جزئیات، مقامات این شهر اعلام کردند که این حمله از طریق یک سیگنال رادیویی انجام شده است. دو روز طول کشید تا سامانه‌ها به عملیات عادی خود بازگشتند.

۲-٤ بات‌نت Persirai IoT

در ماه آوریل سال ۲۰۱۷، پژوهشگری به نام «پیر کیم» اظهار داشت که بیش از ۱۰۰۰ مدل دوربین IP از ۳۵۴ فروشنده‌ی مختلف، آسیب‌پذیری خطرناکی در کارگزار وب دارند. علاوه بر توصیف دقیق مشکل، کیم بخش‌هایی از کد و اطلاعاتی را منتشر کرد که بیش از ۱۸۵،۰۰۰ دوربین آسیب‌پذیر را می‌توان از طریق Shodan شناسایی کرد. به گفته‌ی این محقق، هدف او در انتشار این اطلاعات، جلب‌توجه بسیاری از تولیدکنندگان دوربین، نسبت به این آسیب‌پذیری بود.

در اوایل ماه مه سال ۲۰۱۷، کارشناسان Trend Micro یک بات‌نت جدید IoT به نام "Persirai" را که از دوربین‌های آسیب‌پذیر تشکیل شده بود، کشف کردند. طبق گفته‌ی Trend Micro، مجرمان سایبری از این بات‌نت در درجه‌ی اول برای حملات DDoS استفاده می‌کنند.

۲-۵ استفاده از نامه‌های الکترونیکی تجاری در حمله به شرکت‌های صنعتی

کارشناسان آزمایشگاه ICS CERT گزارشی در مورد حملات نامه‌های الکترونیکی تجاری توسط فعالان تهدید نیجریه‌ای ارایه کردند که عمدتاً شرکت‌های صنعتی بزرگ و حمل‌ونقل را مورد هدف قرار می‌دادند. در حملات تحلیل‌شده توسط آزمایشگاه کسپرسکی، شرکت‌های صنعتی، بیش از ۸۰ درصد قربانیان بالقوه را تشکیل می‌دهند. در مجموع، بیش از ۵۰۰ شرکت موردحمله در بیش از ۵۰ کشور شناسایی شدند.

در مرحله‌ی اول، کلاه‌برداران، نامه‌های الکترونیکی با پیوست‌های مخرب را به آدرس‌های شرکت ارسال می‌کنند. بدافزار مورداستفاده در این حملات، برای سرقت اطلاعات محرمانه و در بعضی موارد برای نصب ابزارهای کنترل از راه دور به صورت مخفی در سامانه‌های آلوده طراحی می‌شوند. پس از آلوده کردن یک رایانه‌ی شرکتی، مهاجمان تصاویری از مکاتبات کارمند را با استفاده از نرم‌افزارهای مخرب و یا تنظیم مجدد پیام‌های پنهان از صندوق پستی رایانه‌ی موردحمله، در صندوق پستی خود قرار می‌دهند. این کار آن‌ها را قادر می‌سازد تا معاملاتی که در شرکت در حال آماده‌سازی هستند را ردیابی کنند.

پس از انتخاب مهم‌ترین معامله، مهاجمان نام‌هایی برای دامنه ثبت می‌کنند که شباهت بسیاری به نام‌های شرکت‌های فروشنده دارند. با استفاده از دامنه‌های ثبت‌شده‌ی جدید، مجرمان سایبری می‌توانند یک حمله‌ی مردمیانی[۳] را انجام دهند. آن‌ها نامه الکترونیکی را با فاکتور فروشنده برداشت می‌کنند و آن را به صندوق پستی در یک دامنه‌ی ماحیگیری با جزئیات حساب کاربری متعلق به مهاجمان، ارسال می‌کنند. متناوباً، آن‌ها می‌توانند از طرف فروشنده درخواستی برای تغییر فوری جزئیات بانکی، علاوه بر پست الکترونیکی قانونی فروشنده که شامل فاکتور است، ارسال کنند.

گزینه‌ی دیگر برای مجرمان اینترنتی این است که با استفاده از تروجان‌ها، برنامه‌های جاسوسی و/یا در پشتی به صندوق پستی قانونی یکی از کارمندان شرکت حمله‌شده دسترسی پیدا کنند و سپس پست‌های الکترونیکی جعلی را از آن صندوق پستی ارسال کنند. ماحیگیر همچنین می‌تواند نامه‌های الکترونیکی خود را از طرف فروشنده با سربرگ نامه‌های الکترونیکی جعلی که به صندوق پستی قانونی فروشنده به‌عنوان فرستنده اشاره دارد، ارسال کند.

---

[۳] Man-in-the-middle

چنین حملاتی برای شرکت‌های صنعتی خطرناک هستند؛ زیرا در صورت موفقیت‌آمیز بودن حمله، خریدار نه‌تنها پول را از دست می‌دهد، بلکه قادر به دریافت کالایی که در آن زمان نیاز دارد نیز نخواهد بود. این موضوع می‌تواند برای شرکت‌های صنعتی مهم باشد. اگر کالاها، مواد اولیه‌ی مورداستفاده در تولید یا قطعات یدکی موردنیاز برای تعمیر تجهیزات باشند، عدم تحویل آن‌ها می‌تواند به خرابی یا عدم انجام تعمیرات برنامه‌ریزی‌شده یا راه‌اندازی مجدد کار منجر شود.

عواقب احتمالی دیگری نیز وجود دارد. برنامه‌های جاسوسی که توسط ماحیگیرها به کار گرفته می‌شوند، اطلاعات متنوعی را از دستگاه‌های آلوده، به کارگزارهای فرمان و کنترل آن‌ها، ازجمله اطلاعات مربوط به عملیات شرکت‌های صنعتی و دارایی‌های اصلی، مانند اطلاعات مربوط به قراردادها و پروژه‌ها، ارسال می‌کنند..

تاکنون، کارشناسان هیچ‌گونه اطلاعاتی را که توسط مهاجمان در بازار سیاه فروخته‌شده باشند، مشاهده نکردند. بااین‌حال، روشن است که این نوع از حملات برای شرکت‌های موردحمله، علاوه بر ضرر مستقیم مالی در معاملات خاص، تهدیدات جدی‌تر دیگری را نیز وارد می‌کند.

۲-۶ WikiLeaks: آرشیو سازمان سیا

از پیشرفت‌های مهم در شش ماه اول سال ۲۰۱۷، نشت آرشیوی از واحد ویژه‌ی آژانس مرکزی اطلاعات آمریکا بود. این آرشیو، حاوی اطلاعاتی در مورد ابزارهای هکری سازمان سیا، بدافزارها، ازجمله سوءاستفاده‌ی روز صفر، ابزار دسترسی از راه دور مخرب و اسناد مربوطه بود که بخشی از این آرشیو، توسط WikiLeaks منتشر شد.

این رونمایی به‌عنوان Vault 7 شناخته و از ماه مارس سال ۲۰۱۷، حدود ۹۰۰۰ سند در مجموعه‌ای از نشریات منتشرشده است. این اسناد، جزئیات قابلیت‌های سیا در رابطه با مخفی کردن دستگاه‌های مختلف الکترونیکی را، از تلفن‌های همراه و تلویزیون‌های هوشمند تا سامانه‌های شرکت‌های سازمانی، به‌طور دقیق توصیف می‌کند. بدافزار CIA، نرم‌افزارهای ویندوز، مک، لینوکس، آیفون، اندروید، تلویزیون هوشمند و مسیریاب‌ها را هدف قرار می‌دهد.

اسناد منتشرشده توسط WikiLeaks، آسیب‌پذیری‌های متعددی را فهرست می‌کند. به‌طور خاص، پس از انتشار Seoul 7، سیسکو به مشتریان خود یک آسیب‌پذیری بحرانی را هشدار داد که می‌توانست مهاجم را

قادر به اجرای کد دلخواه و کنترل بیش از ۳۰۰ مدل مختلف از سوئیچ‌ها و مسیریاب‌های خود کند (این آسیب‌پذیری در ماه مه حل شد).

به گفته‌ی کارشناسان، بیشتر آسیب‌پذیری‌های موجود در این لیست، قبل از انتشار Wikileaks توسط تولیدکنندگان آن‌ها حل شده بود. Wikileaks اطلاعاتی در مورد ابزارهای هک یا سوءاستفاده فاش نکرده است. بااین‌حال، حتی بخشی که منتشر شد، می‌تواند به مجرمان سایبری کمک کند تا سلاح‌های مخرب خود را توسعه دهند و بر اساس اطلاعات منتشرشده در Vault 7، حملات توده‌ای و نفوذ مخفیانه را طراحی کنند.

۲-۷ Shadow Brokers: آرشیو NSA

در ماه آوریل، گروه هکری Shadow Brokers، دسترسی به آرشیو آژانس امنیت ملی (NSA) که شامل ابزارهای سوءاستفاده و ابزار حمله است را امکان‌پذیر ساختند.

داده‌هایی که به صورت عمومی منتشر شدند، شامل سوءاستفاده از تجهیزات شبکه و مسیریاب‌ها، سامانه‌های بانکی، سامانه‌های یونیکس و نسخه‌های مختلف ویندوز هستند. بعضی از آسیب‌پذیری‌های منتشرشده، آسیب‌پذیری‌های روز صفر از پیش ناشناخته بودند.

مایکروسافت اعلام کرد که بیشتر آسیب‌پذیری‌های منتشرشده از این آرشیو یا رفع شده‌اند یا برای ویندوز ۷ و نسخه‌های بالاتر بی‌اهمیت هستند. مایکروسافت سه ماه پیش از انتشار Shadow Brokers، این آسیب‌پذیری‌ها را در وصله‌ی MS17-10 رفع کرده بود.

این وصله همچنین یک آسیب‌پذیری در SMBv1 که توسط NSA هدف قرار گرفته بود و EternalBlue و EternalRomance را مورد سوءاستفاده قرار می‌داد را نیز رفع کرد. یک ماه و نیم بعد از انتشار Shadow Brokers، این سوءاستفاده‌ها برای توزیع برنامه‌های باج‌افزاری رمزگذاری شده‌ی WannaCry و ExPetr (Petya) مورداستفاده قرار گرفتند.

۳ حملات باج‌افزاری

نیمه‌ی اول سال ۲۰۱۷ یادآور حملات باج‌افزار رمزگذاری است. شیوع WannaCry و حملات ExPetr، توجه گسترده‌ی مردم را به خود جلب کرد.

باج‌افزار، تهدید قابل‌توجهی برای شرکت‌ها، ازجمله شرکت‌های صنعتی است. این امر به‌ویژه برای شرکت‌هایی که امکانات زیرساختی حیاتی دارند، خطرناک است؛ زیرا فعالیت این بدافزار می‌تواند فرآیندهای صنعتی را مختل کند.

طبق آمار ارایه‌شده، ۰/۵ درصد از رایانه‌های زیرساختی صنعتی سازمان‌ها، حداقل یک‌بار در نیمه‌ی اول سال ۲۰۱۷ موردحمله‌ی باج‌افزار رمزگذار قرارگرفته‌اند.

۱۰ کشور اولی که سامانه‌های کنترل صنعتی آن‌ها توسط باج‌افزار رمزگذاری موردحمله قرار گرفتند، در جدول ۳-۱ نشان داده‌شده‌اند. همان‌طور که مشاهده می‌شود، کشور ایران نیز در بین این ۱۰ کشور قرار دارد.

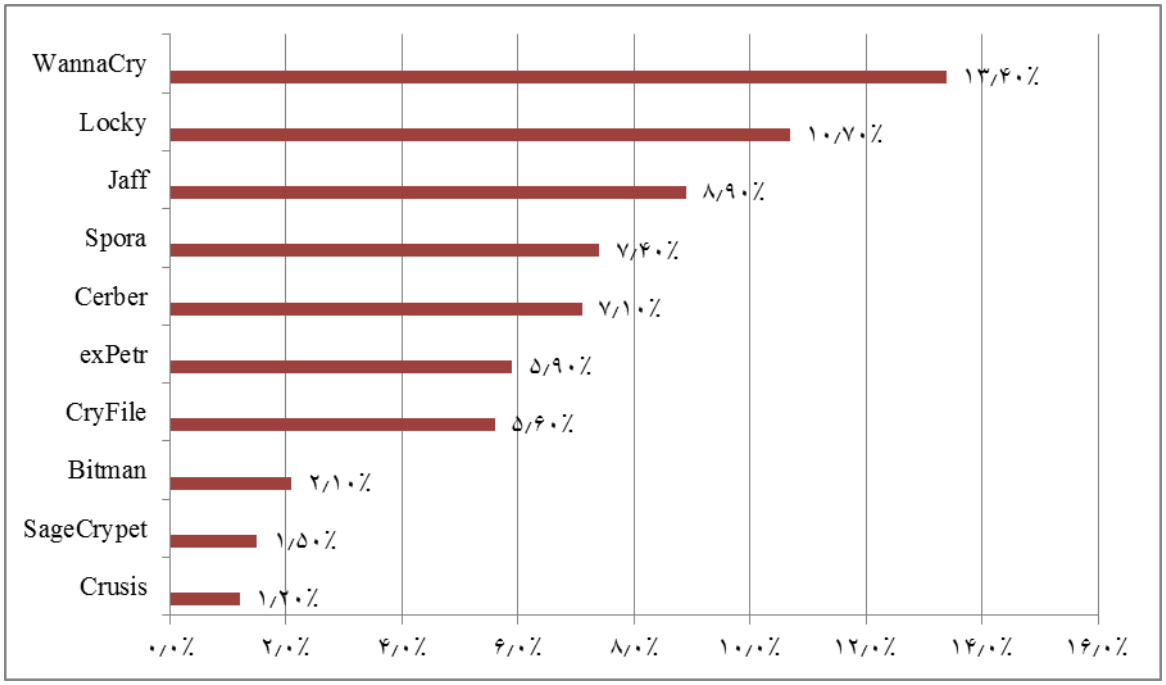
جدول ۳-۱ کشورهای برتری که بر اساس درصد رایانه‌های کنترل صنعتی توسط باج‌افزار رمزگذاری موردحمله قرارگرفته‌اند

	کشور	درصد سامانه‌های موردحمله قرارگرفته
۱	اوکراین	٪۱/۳۳
۲	مالزی	٪۱/۳۱
۳	دانمارک	٪۱/۱۲
۴	کره	٪۱/۰۶
۵	ترکیه	٪۰/۸۸
۶	برزیل	٪۰/۸۵
۷	روسیه	٪۰/۸۰
۸	رومانی	٪۰/۶۷
۹	**ایران**	**٪۰/۶۵**
۱۰	استرالیا	٪۰/۶۵

در شش ماه اول سال ۲۰۱۷، بیشترین تعداد رایانه‌ی کنترل صنعتی موردحمله قرارگرفته، توسط WannaCry آلوده‌شده بودند.

در طول این ماه‌ها، حملات باج‌افزار رمزگذاری متعلق به ۳۳ خانواده‌ی مختلف، در رایانه‌های ICS مسدود شدند. خوشبختانه، هیچ برنامه‌ای که به‌طور خاص برای مسدود کردن نرم‌افزار خودکارسازی صنعتی طراحی شده باشد، در بین نمونه‌های مخرب شناسایی‌شده، یافت نشد.

در نیمه‌ی اول سال ۲۰۱۷، باج‌افزار WannaCry بالاترین رتبه را در رابطه با تعداد ماشین‌هایی که به این باج‌افزار آلوده‌شده‌اند، کسب کرد؛ این یعنی ۱۳/۴ درصد از تمام رایانه‌های بنیادی صنعتی، توسط باج‌افزار رمزگذاری موردحمله قرار گرفتند (نمودار ۳-۱).



نمودار ۳-۱ ده خانواده‌ی برتر تروجان‌های رمزگذاری در نیمه‌ی اول سال ۲۰۱۷

باید توجه داشت که موقعیت‌های دوم و پنجم در این رتبه‌بندی، به دو خانواده‌ی Locky و Cerber تعلق دارند که بر اساس نظر کارشناسان گوگل و محققان دانشکده مهندسی Tandom از دانشگاه نیویورک، در دو سال گذشته بیشترین سود را برای مجرمان سایبری کسب کرده‌اند (به ترتیب ۷/۸ و ۶/۹ میلیون دلار).

اغلب این تروجان‌های رمزگذار برتر، از طریق هرزنامه‌های الکترونیکی، به‌عنوان ارتباطات کسب‌وکار توزیع‌شده‌اند. نامه‌های الکترونیکی با دانلود کننده‌های مخرب متصل به آن‌ها یا همراه با لینک به دانلودکننده‌های بدافزارهای رمزگذار، در متن پیام ارسال می‌شوند.

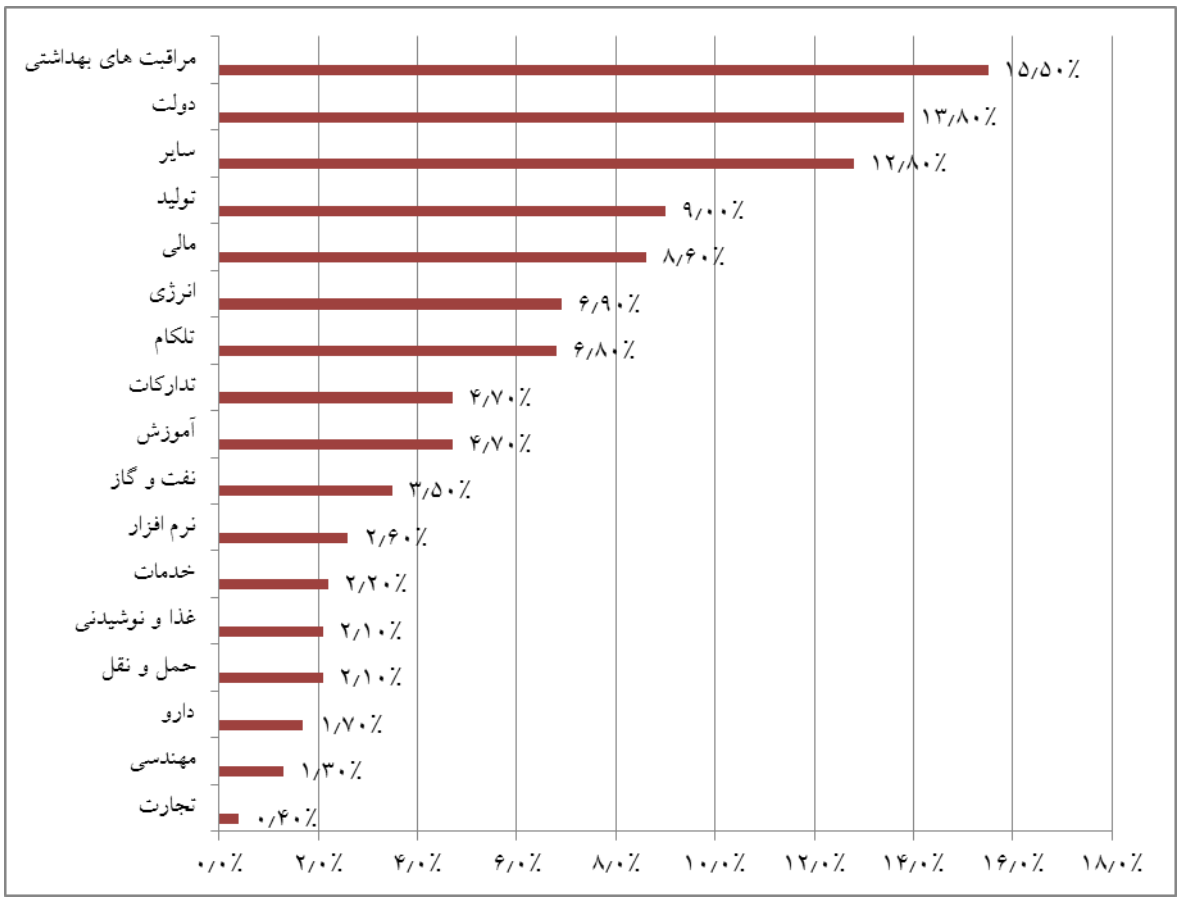
WannaCry و ExPetr رایج‌ترین باج‌افزارهای نیمه‌ی اول سال ۲۰۱۷ بودند. میزان استفاده از آن‌ها و میزان تأثیرشان بر روی رایانه‌ها بی‌سابقه بود. این امر تا حد زیادی به دلیل اکسپلویت‌های آژانس امنیت ملی (NSA) است که توسط گروه Shadow Brokers در ماه آوریل ۲۰۱۷ در دسترس عموم قرار گرفت.

۳-۱ شیوع WannaCry

انتشار WannaCry در ۱۲ مه آغاز و به‌سرعت تبدیل به یک موضوع همه‌گیر شد که رایانه‌های ۱۵۰ کشور در سراسر جهان را تحت تأثیر قرار داد.

شرکت‌هایی که موردحمله‌ی WannaCry قرار گرفتند شامل آن‌هایی بودند که در انواع مختلف تولید، پالایشگاه‌های نفت، زیرساخت‌های شهری و امکانات شبکه‌ی توزیع برق حضور داشتند (نمودار ۳-۲).

طبق داده‌های شبکه‌ی کسپرسکی، در ابتدای ماه ژوئن، شرکت‌هایی توسط WannaCry موردحمله قرارگرفته که منجر به خرابی تأسیسات صنعتی و زیرساخت‌های اجتماعی شده است؛ بنابراین نیاز است تا سازمان‌ها یا زیرساخت‌های حساس در این رابطه هشیار باشند و تدابیر امنیتی لازم را به‌کارگیرند. توزیع شرکت‌های آلوده‌شده به این باج‌افزار در نمودار زیر نشان داده شده است.



نمودار ۳-۲ توزیع شرکت‌های موردحمله قرارگرفته توسط WannaCry در ماه مه و ژوئن سال ۲۰۱۷

شرکت رنو مجبور شد تا عملیات چندین کارخانه‌ی خود را متوقف کند. یکی از خطوط تولید نیسان در حداقل یک مورد تحت تاثیر قرار گرفت و تولید در یکی از کارخانه‌های هوندا در سایامای ژاپن متوقف شد.

روزنامه اسپانیایی الماندو تأیید کرد که چندین شرکت صنعتی اسپانیا ازجمله گاز نچرال (تأمین‌کننده‌ی گاز طبیعی) و ایبرداولا (یک شرکت برق) تحت تاثیر WannaCry قرار گرفتند.

علاوه بر این امکانات زیربنایی، زیرساخت‌های اجتماعی ازجمله مؤسسات بهداشتی تحت تأثیر قرار گرفتند. طبق گزارش‌ها، بسیاری از بیمارستان‌ها قادر به دسترسی به پرونده‌های پزشکی بیماران نبودند، درنتیجه برخی از عملیات پزشکی لغو شدند.

بعدها مشخص شد که نرم‌افزار نصب‌شده بر روی برخی از دستگاه‌های پزشکی نیز دارای آسیب‌پذیری CVE-2017-0143 (MS17-010) بودند که توسط EternalBlue مورد سوءاستفاده قرار گرفتند. در اواسط ماه مه، زیمنس یک بیانیه و توصیه‌نامه‌ی امنیتی برای سامانه‌های تصویربرداری رزونانس مغناطیسی و

ایستگاه‌های کاری تشخیصی چندمنظوره صادر کرد که می‌توانست تحت تأثیر حمله‌ی WannaCry قرار بگیرد.

همان‌طور که قبلاً گفته شد، مهاجمان از یک سوءاستفاده‌ی آژانس امنیت ملی (NSA) استفاده می‌کنند (یک گونه‌ی اصلاح‌شده از EternalBlue که از آسیب‌پذیری CVE-2017-0143 در اجزای سرویس SMBv1 ویندوز بهره می‌گیرد). اگرچه مایکروسافت در ماه مارس یک وصله برای این آسیب‌پذیری منتشر کرد (بیانیه امنیتی MS17-010)؛ اما بر اساس برآورد یوروپول، بیش از ۲۰۰،۰۰۰ رایانه تحت تأثیر شیوع این باج‌افزار قرار گرفتند.

برای سوءاستفاده از این آسیب‌پذیری، اتصال به یک دستگاه از راه دور در درگاه‌های ۱۳۹ و ۴۴۵ TCP ضروری است. این بدافزار، دستگاه‌های با درگاه ۴۴۵ TCP قابل‌دسترسی برای اتصال را، شناسایی می‌کند. اگر آسیب‌پذیری به‌طور موفقیت‌آمیز مورد سوءاستفاده قرار گیرد، این بدافزار کنترل سامانه را به دست گرفته و شروع به رمزگذاری فایل‌ها می‌کند. پس از آلوده کردن رایانه، WannaCry با استفاده از همان سوءاستفاده‌ی EternalBlue، برای آسیب‌پذیری در اجزای سرویس SMBv1 در سراسر شبکه‌ی محلی گسترش می‌یابد.

به‌طورمعمول، سامانه‌های صنعتی در محیط شبکه‌ی کنترلی، یا به‌طور مستقیم به اینترنت متصل نمی‌شوند یا دسترسی به اینترنت از طریق شبکه‌ی شرکتی با استفاده از NAT، دیوار آتش و یک پروکسی کارگزار شرکتی ارایه می‌شود که باید از هرگونه آلودگی این سامانه‌ها از طریق اینترنت جلوگیری کند. بااین‌حال، طبق اطلاعات به‌دست‌آمده، حداقل ده‌ها رایانه که بخشی از سامانه‌های کنترل صنعتی بودند، توسط کرم رمزگذاری WannaCry موردحمله قرار گرفتند. در مواردی که رایانه‌ها به‌درستی محافظت نشده بودند، به این باج‌افزار آلوده و فایل‌هایشان رمزگذاری شدند. این امر می‌تواند منجر به شکست یا اختلال در عملکرد سامانه‌های کنترل صنعتی در این شرکت‌ها و اختلال در چرخه‌ی تولید آن‌ها شود.

آلودگی WannaCry ممکن است به علت خطاهای پیکربندی شبکه‌های معمولی نیز باشند. طبق تجزیه‌وتحلیل‌های انجام‌شده، در اغلب موارد، سامانه‌های خودکارسازی صنعتی توسط نرم‌افزار WannaCry، از شبکه‌ی شرکت محلی و از طریق اتصالات VPN موردحمله قرارگرفته‌اند.

۲-۳ حمله‌ی ExPetr (Petya)

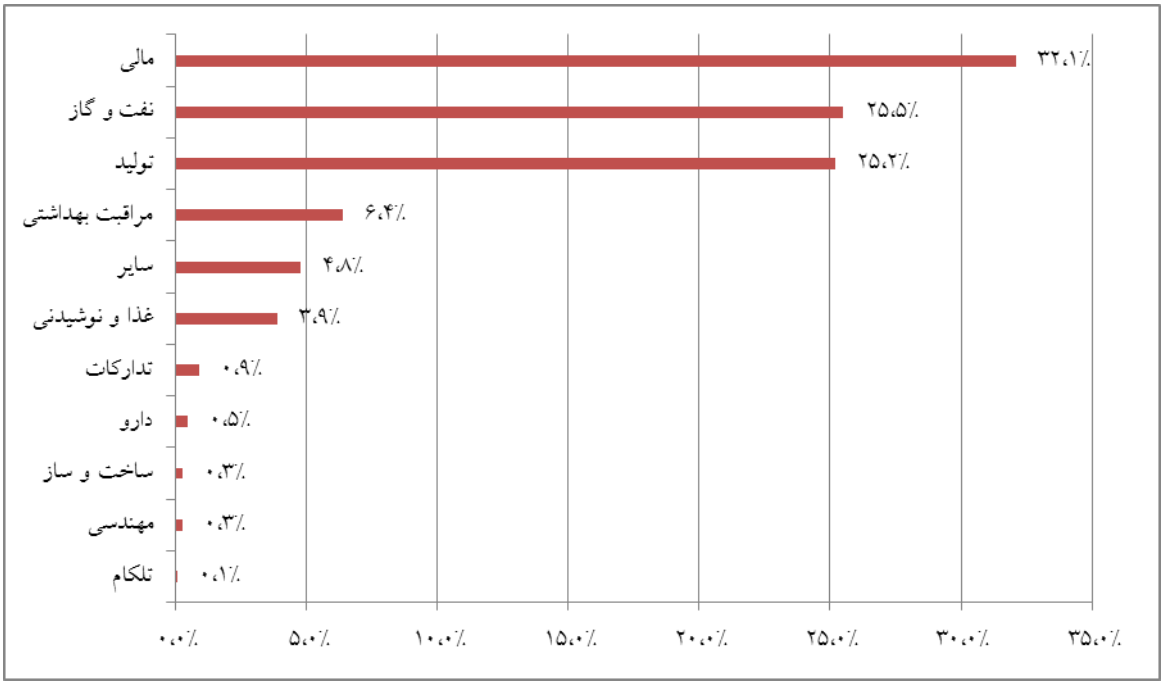
حمله ExPetr که در صبح روز ۲۷ ژوئن در روسیه و اوکراین آغاز شد و سپس به اروپا گسترش یافت، روی برخی از صنایع و خدمات مهم تأثیر گذاشت.

در اوکراین، قربانیان شامل شرکت‌های بخش برق، بانک‌های اوکراین، متروی شهر کییف، فرودگاه بوریسپل کییف، فرودگاه خارکف و ایستگاه نظارت رادیویی چرنوبیل بودند. در روسیه، گزارش‌ها در حدود همان زمان ظاهر شدند که کارگزاران شرکت رزنف توسط یک «حمله‌ی هکر قدرتمند» آسیب دیدند. پس از آن مشخص شد که سایر شرکت‌های صنعتی، ازجمله گروه تولیدکننده‌ی غول‌پیکر Evraz، گروه HMS که شامل شرکت‌هایی مانند Sibneftemash، HMS Neftemash و Giprotyumenneftegaz بودند، تحت تأثیر حملات بدافزار رمزگذار قرار گرفتند.

بعدها گزارش‌های مربوط به شیوع این حمله از سایر کشورهای اروپایی آغاز شد. قربانیان شامل شرکت Merck، شرکت بزرگ داروسازی Maersk و ده‌ها شرکت دیگر ازجمله SaintGobain (شرکت بزرگ صنعتی در فرانسه) بودند.

سامانه‌ای که بارگیری و تخلیه‌ی کانتینرها را در یکی از پایانه‌های بندر Jawaharlal Nehru Port Trust (بزرگ‌ترین بندر کانتینری هند که توسط AP Moller-Maersk اداره می‌شود) کنترل می‌کند، توسط این حمله دچار اختلال شد. پس از حمله، این سامانه دیگر نمی‌توانست تعیین کند که چه نوع حمل‌ونقلی متعلق به آن‌هاست.

طبق تجزیه‌وتحلیل‌های انجام‌شده بر روی توزیع صنایع مورد هدف قرارگرفته توسط ExPetr(Petya)، حداقل ۵۰٪ از شرکت‌های موردحمله، از تولید و صنایع نفت و گاز بودند (نمودار ۳-۳).



نمودار ۳-۳ توزیع صنایعی که مورد هدف ExPetr قرار گرفتند

برای آلوده کردن رایانه‌ها و راه‌اندازی نرم‌افزارهای مخرب بر روی آن‌ها، مجرمان سایبری از روش به‌روزرسانی برنامه‌ی گردش الکترونیکی شخص ثالثی به نام M.E.Doc استفاده می‌کنند. علاوه‌براین، مشخص شده است که حداقل از وب‌سایت مشروع آلوده‌ای برای هدایت درخواست‌ها به یک فایل مخرب (به‌اصطلاح حمله‌ی سوراخ آبی) استفاده می‌شود. ExPetr از سوءاستفاده‌های NSA (EternalBlue و EternalRomance) استفاده می‌کند. بهره‌گیری از این مکانیزم، باعث آلودگی رایانه‌هایی می‌شود که از طریق VPN، به شبکه‌ی محلی آلوده متصل می‌شوند.

این بدافزار خود را از راه دور و با استفاده از ابزار PsExec و WMI، با اعتبار به سرقت رفته از کاربر فعلی و استفاده از برنامه‌ای اختصاصی مانند Mimikatz که در منابع مخرب ذخیره شده است، در رایانه‌های شبکه‌ی محلی راه‌اندازی می‌کند. ExPetr علاوه بر رمزگذاری اطلاعات، MBR ماشین آلوده را نیز بازنویسی می‌کند.

WannaCry و ExPetr هردو به‌عنوان باج‌افزار رمزگذاری دسته‌بندی می‌شوند. گروه‌های بعد از این برنامه‌های مخرب کاملاً متفاوت هستند. بااین‌حال، به نظر می‌رسید که هر دو گروه می‌توانستند مقدار زیادی پول از حملات موفقیت‌آمیز خود به دست آورند؛ اما به دلایل مختلف این کار را انجام ندادند.

ExPetr به‌طورجدی یک باج‌افزار نیست. محققان خیلی زود متوجه شدند که به دلیل اشتباهات در کد آن، حتی مهاجمان نمی‌توانند پرونده‌های قربانیان را رمزگشایی کنند. این بدان معنی است که این تروجان درواقع متعلق به کلاس بدافزاری است که فقط اطلاعات را از بین می‌برد (به‌عنوان‌مثال پاک می‌کند). به احتمال زیاد

هدف واقعی از حملات ExPetr این بود که از پرداخت باج استفاده نکنند (تقاضای جبران ممکن است ماسکی برای اقدامات خرابکارانه باشد).

بعضی از کارشناسان معتقدند که در مورد WannaCry نیز پول هدف اصلی بازیگران مخرب آن نبوده است.

کارشناسان آزمایشگاه کسپرسکی معتقدند که توزیع فعال بدافزارهای رمزگذاری ادامه دارد. نویسندگان این تروجان‌ها به‌طور فزاینده‌ای محصولات خود را با استفاده از مدل SaaS (نرم‌افزار به‌عنوان سرویس) توزیع می‌کنند. این مدل به آن دسته از مجرمان سایبری که از مهارت، منابع یا انگیزه‌ی اندکی برخوردارند، این امکان را می‌دهد که نرم‌افزارهای مخرب خود را برای کسب پول از طریق اخاذی اینترنتی توسعه دهند.

شرکت‌های صنعتی با حملات مخرب رمزگذاری شده در کنار سازمان‌های دیگر هدف قرار می‌گیرند. تاکنون، هیچ مورد معتبری از حملات باج‌افزاری هدفمند علیه شرکت‌های صنعتی وجود نداشته است که هدف اصلی آن‌ها گرفتن باج باشد. چنین حملاتی عمدتاً علیه سازمان‌های مالی انجام شده است. به‌طور کل، هیچ بدافزار رمزگذاری که به‌طور خاص برای نرم‌افزار خودکارسازی صنعتی باشد، طراحی نشده است.

متأسفانه حتی آلودگی تصادفی رایانه‌ها در یک شبکه‌ی صنعتی با استفاده از بدافزارهای رمزگذاری می‌تواند باعث خرابی یا ازکارافتادگی سامانه‌های خودکارسازی صنعتی و اختلال در چرخه‌های تولیدی شرکت شود.

۴ آمار تهدید

تمام داده‌های آماری مورداستفاده در این گزارش، با استفاده از شبکه‌ی امنیت کسپرسکی (KSN) ارایه شده است. داده‌ها از طرف کاربرانی دریافت شدند که رضایت دادند تا انتقال داده‌ها به صورت ناشناس از رایانه‌هایشان صورت گیرد.

٤-۱ متدولوژی

داده‌ها از رایانه‌های محافظت‌شده توسط محصولات آزمایشگاه کسپرسکی دریافت شده‌اند که ICS CERT آزمایشگاه کسپرسکی آن‌ها را به‌عنوان بخشی از زیرساخت‌های صنعتی در سازمان‌ها طبقه‌بندی کرده است. این گروه، رایانه‌های تحت ویندوزی است که یک یا چندین توابع زیر را انجام می‌دهند:

- کارگزارهای کنترل نظارت و جمع‌آوری اطلاعات (SCADA)،
- کارگزارهای ذخیره‌ی داده (Historian)،
- دروازه‌های داده (OPC)،

- ایستگاه‌های ثابت مهندسان و اپراتورها،
- ایستگاه‌های کاری تلفن همراه مهندسان و اپراتورها،
- رابط کاربری انسان (HMI).

این گروه همچنین شامل رایانه‌های کارکنان در سازمان‌های پیمانکاری و رایانه‌های مدیران شبکه‌های کنترل صنعتی و توسعه‌دهندگان نرم‌افزارهایی است که نرم‌افزار را برای سامانه‌های خودکارسازی صنعتی توسعه می‌دهند.

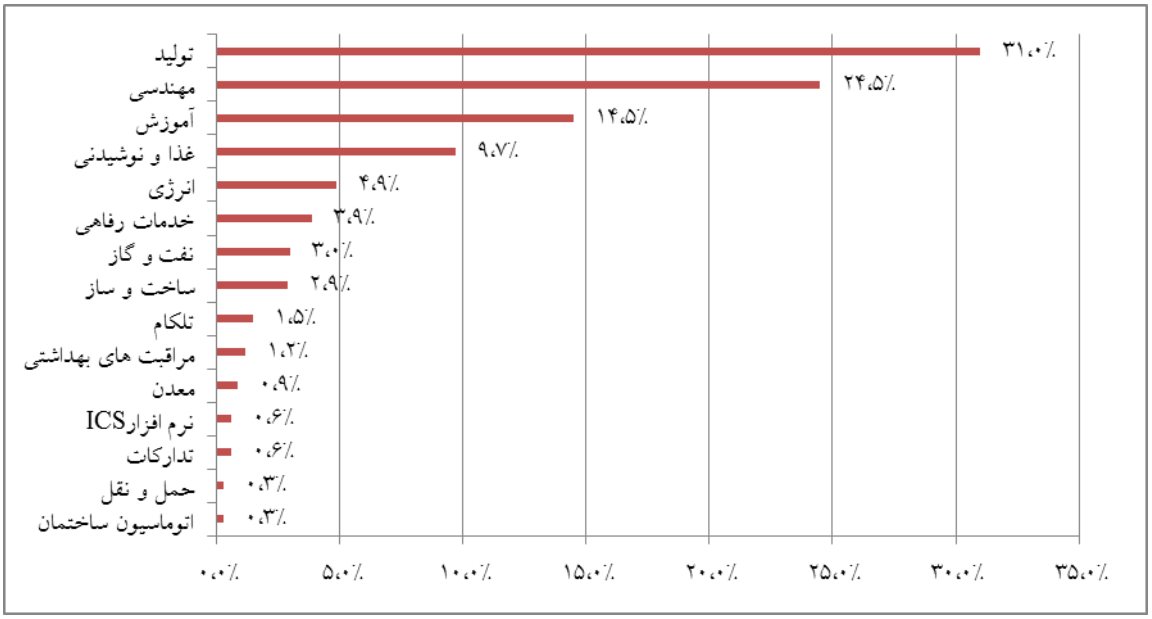
طبق اهداف این گزارش، رایانه‌های موردحمله، آن‌هایی هستند که از راه‌حل‌های امنیتی کسپرسکی حداقل یک‌بار در طی دوره‌ی گزارش استفاده کرده‌اند. هنگام تعیین درصد ماشین‌های موردحمله، از نسبت رایانه‌های منحصربه‌فرد موردحمله به همه‌ی رایانه‌های نمونه استفاده می‌شود.

باید توجه داشت که محدودیت دسترسی به اینترنت می‌تواند برای رایانه‌ها در داخل یک شبکه‌ی صنعتی و رایانه‌هایی که زیرساخت آن شبکه صنعتی را تشکیل می‌دهند، به‌طور قابل‌توجهی متفاوت باشد. کارگزارهای ICS و ایستگاه‌های کاری ثابت مهندسان و اپراتورها اغلب به دلیل محدودیت‌های خاص شبکه‌های صنعتی، دسترسی مستقیم به اینترنت ندارند. ایستگاه‌های کاری مدیران سامانه/ شبکه، توسعه‌دهندگان و سازندگان سامانه‌های خودکارسازی صنعتی و همچنین رایانه‌های پیمانکارانی که به شبکه‌ی صنعتی متصل هستند (به‌عنوان‌مثال برای نظارت و پشتیبانی فنی) ممکن است دارای اتصالات اینترنتی مکرر یا حتی تمام‌وقت باشند.

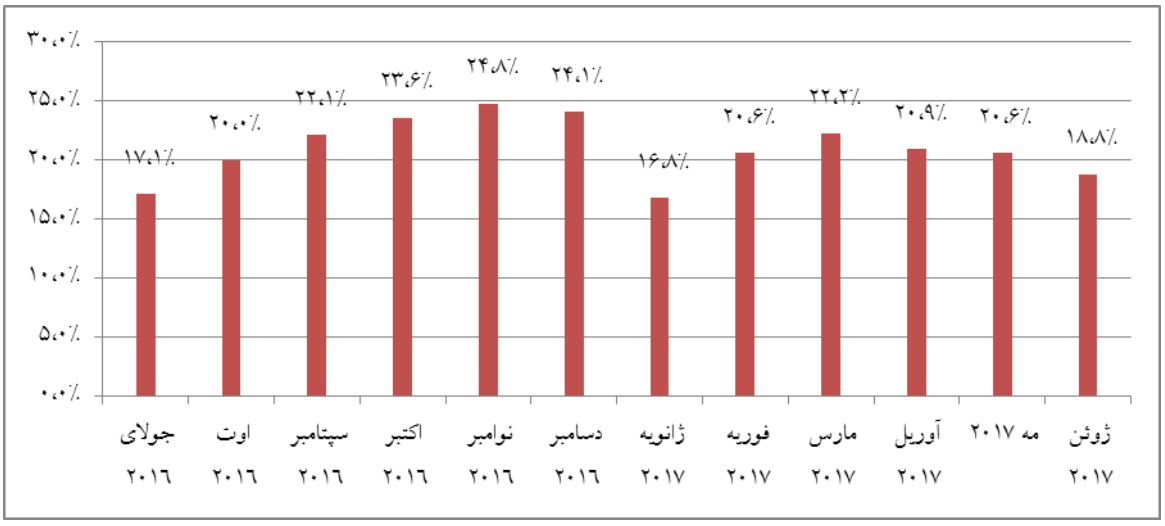
٤-٢ درصد رایانه‌هایی که موردحمله قرارگرفته‌اند

در نیمه‌ی اول سال ۲۰۱۷، محصولات آزمایشگاه کسپرسکی، ۳۷/۶ درصد از حملات به رایانه‌های ICS تحت حفاظت خود را در سطح جهانی مسدود کردند که ۱/۶ درصد کمتر از نیمه‌ی دوم سال ۲۰۱۶ است.

رایانه‌های ICS در شرکت‌های تولیدی که مواد مختلف، تجهیزات و کالاها را تولید می‌کنند، حدود یک‌سوم از حملات را تشکیل می‌دهند (نمودار ۴-۱).



نمودار ۴-۱ توزیع رایانه‌های ICS موردحمله قرارگرفته در نیمه‌ی اول سال ۲۰۱۷



نمودار ۴-۲ درصد رایانه‌های موردحمله قرارگرفته در هر ماه، از ژوئن سال ۲۰۱۶ تا ژوئن سال ۲۰۱۷

درحالی‌که نسبت ماشین‌آلات موردحمله قرارگرفته در نیمه‌ی دوم سال ۲۰۱۶ از یک ماه به ماه بعد افزایش می‌یافت، این تغییر در شش ماه اول سال ۲۰۱۷ تا حدودی متفاوت بود. فعالیت مهاجمان در ماه ژانویه کاهش پیدا کرد و نسبت رایانه‌های موردحمله قرارگرفته، به سطح سابق خود در ماه‌های فوریه و مارس افزایش پیدا کرد و از ماه آوریل تا جولای به‌تدریج کاهش یافت (نمودار ۴-۲).

٤-٣ توزیع جغرافیایی حملات بر سامانه‌های خودکارسازی صنعتی

۱۵ کشوری که بالاترین درصد رایانه‌های ICS موردحمله قرارگرفته را در نیمه‌ی اول سال ۲۰۱۷ دارا بودند، در جدول ۴-۱ نشان داده شده‌اند. همان‌طور که مشاهده می‌شود، کشور ما با **۵۵/۳** درصد، در این رتبه‌بندی در جایگاه هفتم قرار گرفته است.

جدول ۴-۱ کشورهایی که بالاترین درصد رایانه‌های ICS موردحمله قرارگرفته را در نیمه‌ی اول سال ۲۰۱۷ دارا بودند

	کشور	درصد سامانه‌های موردحمله قرارگرفته
۱	ویتنام	٪۷۱
۲	الجزیره	٪۶۷/۱
۳	مراکش	٪۶۵/۴
۴	اندونزی	٪۵۸/۷
۵	چین	٪۵۷/۱
۶	هند	٪۵۶/۰
۷	**ایران**	**٪۵۵/۳**
۸	عربستان سعودی	٪۵۱/۸
۹	مصر	٪۵۱/۶
۱۰	پرو	٪۵۰/۸
۱۱	تایلند	٪۴۷/۸
۱۲	مالزی	٪۴۷/۲
۱۳	اوکراین	٪۴۶/۳
۱۴	پرتغال	٪۴۶/۱
۱۵	قزاقستان	٪۴۵/۹

٤-٤ بدافزار در سامانه‌های خودکارسازی صنعتی

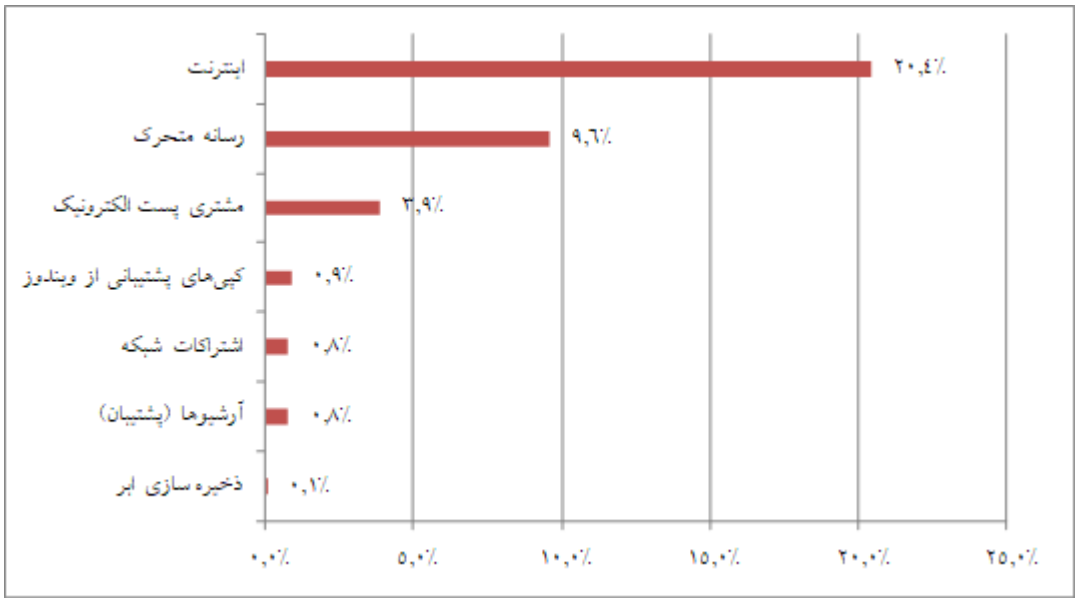
شبکه‌های صنعتی ازلحاظ موارد استفاده و فن‌آوری‌های مورداستفاده، شباهت زیادی به شبکه‌های شرکت‌های بزرگ دارند. درنتیجه، چشم‌انداز تهدید برای سامانه‌های صنعتی، شبیه به چشم‌انداز تهدید برای سامانه‌های شرکت‌های بزرگ است.

در نیمه‌ی اول سال ۲۰۱۷، حدود ۱۸۰۰۰ بدافزار بهبودیافته، متعلق به بیش از ۲۵۰۰ خانواده‌ی مختلف، در سامانه‌های خودکارسازی (اتوماسیون) صنعتی شناسایی شدند.

آن دسته از نرم‌افزارهای مخربی که به رایانه‌های شرکت‌های تجاری حمله می‌کنند، به رایانه‌های ICS نیز مرتبط هستند، ازجمله جاسوس‌افزار (Trojan-Spy و Trojan-PSW)، باج‌افزار (Trojan-Ransom) و برنامه‌ی Wipertype (KillDisk) که رایانه را غیرقابل استفاده می‌کند و اطلاعات را از دیسک سخت پاک می‌کند. چنین برنامه‌هایی، تهدیدی جدی برای رایانه‌های ICS هستند؛ زیرا آلوده‌شده با چنین نرم‌افزارهای مخربی می‌تواند منجر به ازدست‌رفتن کنترل یا خراب شدن فرایندهای صنعتی شود.

٤-٥ منابع آلوده‌کننده سامانه‌های خودکارسازی صنعتی

در نیمه‌ی اول سال ۲۰۱۷، تلاش برای دانلود نرم‌افزارهای مخرب از طریق اینترنت یا دسترسی به منابع وب مخرب و ماحیگیری شناخته‌شده، در ۲۰/۴ درصد از رایانه‌های ICS مسدود شد (نمودار ۴-۳).



نمودار ۴-۳ منابع اصلی تهدید مسدودشده در رایانه‌های ICS در نیمه‌ی اول سال ۲۰۱۷

برای رایانه‌هایی که بخشی از زیرساخت‌های صنعتی هستند، اینترنت به‌عنوان منبع اصلی آلودگی باقی می‌ماند. عوامل مشارکتی شامل رابط‌های بین شبکه‌های شرکتی و صنعتی، قابلیت دسترسی محدود به اینترنت از شبکه‌های صنعتی و اتصال رایانه‌ها در شبکه‌های صنعتی به اینترنت از طریق اپراتورهای تلفن همراه (با استفاده از تلفن‌های همراه، مودم‌های USB و/یا مسیریاب‌های وای‌فای با پشتیبانی LTE/3G) است. پیمانکاران، توسعه‌دهندگان و مدیران سامانه که به‌طور خارجی (مستقیم یا از راه دور) به شبکه‌ی کنترل متصل می‌شوند، اغلب دسترسی به اینترنت نامحدود دارند. رایانه‌های این دسته از افراد، در گروه خطرناک قرار دارند و می‌توانند توسط نرم‌افزارهای مخرب به‌عنوان کانالی برای نفوذ به شبکه‌های صنعتی شرکت‌های تحت پوشش آن‌ها مورداستفاده قرار گیرند.

نرم‌افزارهای مخرب در ۹/۶ درصد از رایانه‌های ICS، در هنگام اتصال رسانه‌های قابل‌حمل به آن‌ها شناسایی شدند. بدافزارهایی که از طریق رسانه‌های قابل‌حمل و پوشه‌های شبکه گسترش می‌یابند، اغلب فایل‌های مجاز را آلوده می‌کنند یا از نام‌هایی شبیه به این فایل‌های مجاز استفاده می‌کنند (این رفتار، ویژگی بسیاری از ویروس‌ها و کرم‌ها است). فایل‌های مخرب با اسامی مشابه به فایل‌های مجاز می‌توانند در آرشیو داده‌های امن ایجادشده توسط کاربران (این آرشیوها در ۰/۸ درصد از رایانه‌ها شناسایی‌شده‌اند) و پشتیبان فایل سیستم ایجادشده توسط سیستم‌عامل (۰/۸ درصد) جای گیرند.

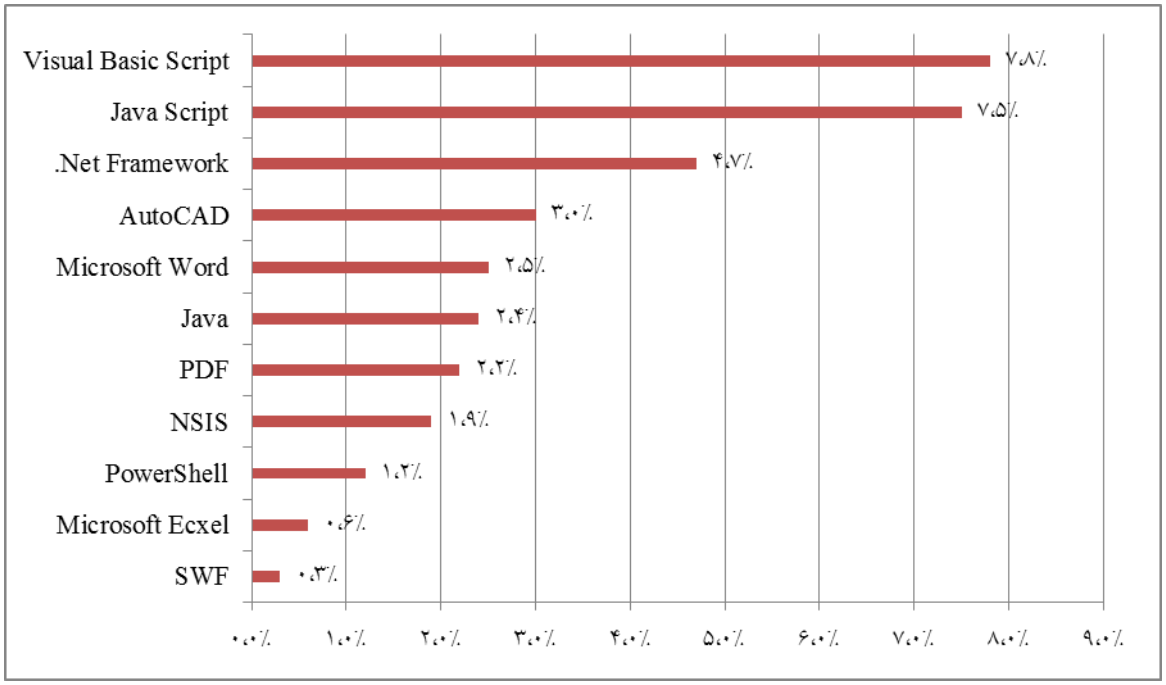
پیوست‌های نامه‌های الکترونیکی و اسکریپت‌های مخرب که در صندوق‌های نامه‌های الکترونیکی تعبیه شده بودند، در ۳/۹ درصد از رایانه‌های ICS مسدود شدند. در رتبه‌بندی کسپرسکی، مشتریان نامه الکترونیکی در رتبه‌ی سوم قرار دارند. مهاجمان در اغلب موارد، نامه‌های الکترونیکی را با پیوست‌های مخرب در فرمت‌های اداری مانند MS Office و PDF توزیع می‌کنند.

در ۰/۱ درصد از رایانه‌های ICS، نرم‌افزارهای مخرب در پوشه‌های محلی سرویس‌های ذخیره‌سازی ابر یافت می‌شوند که به‌طور خودکار با رایانه به اینترنت متصل می‌شوند. اگر ذخیره‌سازی ابر آلوده باشد (از طریق هر یک از رایانه‌هایی که به آن دسترسی دارند)، فایل‌های مخرب به‌صورت خودکار به تمام دستگاه‌های متصل به ذخیره‌سازی ابر منتقل می‌شوند.

٦-٤ بسترهای مورداستفاده توسط بدافزار

بدافزارها در قالب ویندوز (Win32 / Win 64)، فایل‌های اجرایی بیش از ۵۰ درصد از تمام رایانه‌های موردحمله را مسدود کردند. بازیگران تهدید اغلب به‌جای ایجاد فایل اجرایی، قابلیت‌های مخرب را با

استفاده از زبان اسکریپتی که ممکن است قبلاً توسط مترجم‌هایی روی رایانه‌ی قربانی نصب شده باشند، اجرا می‌کنند. رتبه‌بندی سیستم‌عامل‌های اصلی بدافزار، ازجمله ویندوز، در نمودار ۴-۴ ارایه شده است.



نمودار ۴-۴ بسترهای مورداستفاده‌ی بدافزار

باید توجه داشت که مهاجمان اغلب از بارگذارهای کوچک نوشته‌شده در جاوا اسکریپت، Visual Basic Script یا Powershell استفاده می‌کنند که با استفاده از پارامترهای خط فرمان برای مترجمان مربوطه راه‌اندازی می‌شوند.

۵ توصیه‌های پیشنهادی

برای جلوگیری از چنین اتفاقاتی در آینده و حفاظت از حملات هدفمند علیه شبکه‌های صنعتی، مجموعه‌ای از اقدامات طراحی‌شده برای اطمینان از امنیت محدوده‌ی داخلی و خارجی شبکه‌های صنعتی ارایه شده است.

اول از همه، برای ارایه‌ی مدیریت ایمنی از راه دور سامانه‌های خودکارسازی و انتقال داده‌ها بین یک شبکه‌ی صنعتی و دیگر شبکه‌ها، دسترسی بین سامانه‌هایی که بخشی از شبکه‌های مختلف یا دارای سطوح اعتماد متفاوت هستند، باید به حداکثر دسترسی ممکن محدود شود:

- سامانه‌هایی که دائماً یا به‌طور منظم با شبکه‌های خارجی ارتباط دارند (دستگاه‌های تلفن همراه، متصل‌شونده‌های VPN، کارگزارهای پایانه و غیره) باید در یک بخش جداگانه (منطقه‌ی نظامی[۴]) از شبکه‌ی صنعتی قرار گیرند.
- سامانه‌ها در منطقه‌ی نظامی باید به زیرشبکه‌ها یا زیرشبکه‌های مجازی (VLAN)، با دسترسی محدود بین زیرشبکه‌ها (فقط ارتباطات لازم، مجاز هستند) تقسیم شوند.
- همه‌ی تبادل اطلاعات لازم بین شبکه‌ی صنعتی و جهان خارج، باید از طریق DMZ (منطقه غیرنظامی) انجام شود.
- در صورت لزوم، کارگزارهای پایانه را می‌توان در DMZ مستقر کرد تا روش اتصال معکوس (از شبکه‌ی صنعتی به DMZ) را فعال کند.
- در صورت امکان، دسترسی از DMZ به شبکه‌ی صنعتی باید مسدود شود.
- اگر فرایندهای کسب‌وکار سازمانی با ارتباط یک‌طرفه سازگار باشد، توصیه می‌شود که از دیودهای داده استفاده شود.

لازم به ذکر است که چشم‌انداز تهدید برای سامانه‌های خودکارسازی صنعتی، به‌طور مداوم در حال تغییر است و آسیب‌پذیری‌های جدید، هم در نرم‌افزار کاربردی وهم در نرم‌افزار صنعتی یافت می‌شود.

برای حفاظت در برابر تهدیدات ناشناخته، ازجمله تهدیدهای هدفمند، توصیه می‌شود تا موارد زیر اجرا گردد:

- فهرست سرویس شبکه‌ی در حال اجرا تهیه شود. در صورت امکان، سرویس‌های شبکه‌ی آسیب‌پذیر (مگر اینکه این امر به تداوم فرایندهای صنعتی آسیب برساند) و سایر خدماتی که مستقیماً برای عملیات سیستم خودکارسازی لازم نیستند، متوقف شوند. باید بر روی خدماتی که دسترسی از راه دور به اشیاء سیستم فایل مانند SMB، CIFS و/ یا NFS (که در مواردی حملات آسیب‌پذیری را در لینوکس مورداستفاده قرار می‌دهند) فراهم می‌آورند، تأکید ویژه‌ای شود.
- از بین بردن هرگونه ارتباط شبکه با شبکه‌های اطلاعاتی دیگر و مجاور آن‌که توسط فرایندهای صنعتی موردنیاز نیست.

---

[۴] Demilitarized zone (DMZ)

- تأیید امنیت دسترسی از راه دور به شبکه‌ی صنعتی؛ تأکید ویژه بر اینکه آیا مناطق نظامی در مطابقت با نیازهای امنیتی IT تنظیم شده‌اند یا خیر. به حداقل رساندن یا به‌طور کامل از بین‌بردن استفاده از ابزارهای مدیریت از راه دور (مانند RDP یا TeamViewer).
- اطمینان از به روزرسانی ابزارهای فراهم کننده‌ی امنیت همچون پایگاه داده‌های امضا[۵]، سامانه‌های تشخیص و الگوریتم‌های تصمیم‌گیریِ راه‌حل‌های امنیتی. بررسی اینکه تمام اجزای حفاظت اصلی فعال هستند و پوشه‌های نرم‌افزار ICS از محدوده‌ی حفاظت خارج نمی‌شوند.
- بررسی خط‌مشی‌ها و شیوه‌های مربوط به استفاده از رسانه‌های متحرک و دستگاه‌های قابل‌حمل؛ دستگاه‌های مسدودکننده‌ای که دسترسی غیرمجاز به شبکه‌های خارجی و اینترنت را از اتصال به میزبان در شبکه‌ی صنعتی فراهم می‌کنند. هر جایی که امکان دارد، درگاه‌های مربوطه را غیرفعال می‌کنند یا کنترل دسترسی به این درگاه‌ها باید با استفاده از ابزارهای تخصصی به‌خوبی پیکربندی شوند.
- استقرار ابزارهایی که نظارت بر ترافیک شبکه و تشخیص حملات سایبری را در شبکه‌های صنعتی انجام می‌دهند. در اغلب موارد، در چنین اقداماتی نیازی به تغییرات در اجزای ICS یا پیکربندی آن‌ها نیست و می‌توانند بدون توقف عملیات انجام شوند.

۶ نتیجه‌گیری

ظهور سامانه‌های صنعتی و اتصال آن‌ها به شبکه‌ی جهانی، تاثیر شگرفی در توسعه‌ی فرآیندهای کنترلی زیرساخت‌های حیاتی کشورها، به‌ویژه نظارت و کنترل تجهیزات از راه دور داشته است. این پیشرفت و توسعه، آسیب‌پذیری‌های جدیدی را نیز به همراه داشته که بحث امنیت سایبری سامانه‌های کنترل صنعتی را به چالش کشیده است. ازاین‌رو، شناخت کامل بسترها و بخش‌های آسیب‌پذیر و همچنین تهدیدات ناشی از آن‌ها امری لازم و ضروری است. پس از شناخت بخش‌های آسیب‌پذیر سامانه‌های صنعتی، بررسی راهکارهای تدافعی و بهبود سطح ایمنی، ازجمله اقداماتی است که در کاهش تهدیدات و خطرات احتمالی نقش بسزایی دارد.

---

۵ Signature database

در این گزارش تهدیدات مربوط به سامانه‌های کنترل صنعتی که در نیمه اول سال ۲۰۱۷ صورت گرفته بود، با هدف شناخت آن‌ها و جلوگیری از وقوع تهدیدات مشابه مطرح شد. همچنین بررسی شد که سامانه‌های کنترل صنعتی در کدام صنایع و در چه کشورهایی بیشتر توسط باج‌افزارهای رمزگذاری آلوده‌شده‌اند؛ و در نهایت برای جلوگیری از این نوع تهدیدات توصیه‌هایی ارایه شده است.