بررسی حملات امنیتی شاخص در سامانه‌های کنترل صنعتی: از سال ۲۰۰۰ تا کنون

راضیه اسکندری* و الهه معتمدی

گروه مهندسی کامپیوتر، دانشکده فنّی و مهندسی، دانشگاه شهرکرد، شهرکرد، ایران

چکیده

استفادهٔ گسترده از فناوری اطلاعات و ارتباطات در سامانه‌های کنترل صنعتی، این سامانه‌ها را در معرض حملات سایبری قرار داده است. با توجه به این‌که قدم نخست در ارائهٔ راه‌حل امنیتی، شناخت تهدیدها و آسیب‌پذیری‌های یک سامانه است، در این مقاله مروری کلّی بر امنیت سامانه‌های کنترل صنعتی و تبیین حملات سایبری از گذشته تا به حال خواهیم داشت. در راستای ارزیابی بهتر ریسک در حملات، در این مقاله ملاک‌های هدف حمله، منطقهٔ حمله، روش و تأثیر حمله را بررسی کرده و در تحلیل امنیتی سایبری مرتبط با زیرساخت‌های حیاتی و سامانه‌های اسکادا، این حوادث را بر مبنای پارامترهای یادشده نمایه‌سازی می‌کنیم. این نمایه‌سازی، دید روشنی از مهم‌ترین حوادث امنیتی مطرح در سامانه‌های اسکادا فراهم کرده و در تبیین راه‌بردهای مناسب جهت پیش‌گیری و مقابله با حملات امنیتی، مفید واقع خواهد شد.

واژگان کلیدی: سامانه‌های اسکادا، امنیت سایبری، حملات سایبری، ارزیابی ریسک.

۱- مقدّمه

اصطلاح کلی سامانه کنترل صنعتی برای توصیف چندین نوع سامانه، نظیر DCS (سامانه‌های کنترل توزیع‌شده[1])، اسکادا (کنترل نظارت و اکتساب داده[2])، IAS (سامانه اتوماسیون صنعتی[3])، IACS (اتوماسیون صنعتی و سامانه‌های کنترل[4]) یا حتی گاهی برای توصیف PLC (کنترل کنندهٔ منطقی قابل برنامه‌ریزی[5]) استفاده می‌شود. سامانهٔ کنترل صنعتی، مجموعه‌ای از تجهیزات و زیرسامانه‌های به‌هم پیوسته برای اجرای سه عمل اصلی اکتساب[6]، کنترل و نظارت[7] است. سامانه‌های کنترل صنعتی نتایج اندازه‌گیری‌های حس‌گرها و داده‌های عملیاتی را از زمینهٔ پردازش، خودپردازش و تحلیل جمع‌آوری کرده و برای اپراتور سامانه به نمایش در آورده و منطق کنترل را در دستگاه‌های کنترل محلی یا از راه دور اجرا می‌کند [۱].

ICS، فرآیندهای نظارت و کنترل را در صنایع مختلفی مانند تولید برق، انتقال و توزیع، تولید مواد شیمیایی، نفت و گاز، پالایش[8] آب و شیرین‌کردن آب، به‌هم مرتبط می‌سازد. با توجه به نقش برجستهٔ سامانه‌های کنترل صنعتی در کنترل و پایش زیرساخت‌های حیاتی و صنایع مهم یک کشور، پرداختن به ایمن‌سازی آن‌ها به یک اولویت ملّی مهم در هر کشوری تبدیل شده است [۳ و۲].

زیرساخت‌های حیاتی سایبری، به‌دلیل استفادهٔ فزاینده از سامانه‌های فناوری اطلاعات و ارتباطات با چالش‌های امنیتی بزرگی مواجه شده است؛ چون این سامانه‌ها در ابتدا به شبکه متصل نبودند، امنیت را تنها به واسطه ایزوله‌بودن فراهم می‌کردند؛ اما در حال حاضر نه‌تنها به‌صورت برخط در دسترس هستند، بلکه برای کارکرد بهینه و مطمئن خود به این ارتباط وابسته‌اند. اتصال به شبکه مانند یک شمشیر قدرتمند دو لبه عمل می‌کند که هم می‌تواند منجر به افزایش بهره‌روی و هم منجر به تهدیدات امنیتی شود [۴].

راه‌حل‌های سنّتی امنیت IT، موفق نشدند که ارتباط بین اجزای فیزیکی و سایبری ICS را مدیریت کنند[۵].

[1] Distributed Control System
[2] Supervisory Control And Data Aquisition
[3] Industrial Automation System
[4] Industrial Automation And Control Systems
[5] Programmable Logic Controller
[6] Acquisition
[7] Supervision
[8] Monitoring

* نویسندهٔ مسؤول

براساس مستند NIST SP 800-82، امنیت ICS از منظرهای زیر با امنیت سامانه‌های متداول IT متفاوت است[۲]:

۱) هدف اصلی ICS، حفظ یک‌پارچگی فرآیند صنعتی است؛
۲) فرآیندهای ICS پی‌درپی هستند و ازاین‌رو باید دسترسی‌پذیری بالایی داشته باشند (۲۴ساعت شبانه‌روز)؛ وقفه‌های غیرمنتظره باید برای تصحیح، برنامه‌ریزی و زمان‌بندی شوند.
۳) در یک ICS، تعاملات با فرآیندهای فیزیکی، متمرکز و اغلب پیچیده است؛
۴) ICS، فرآیندهای صنعتی خاصی را هدف می‌گیرد و ممکن است منابع لازم برای قابلیت‌های اضافی مانند امنیت را نداشته باشد؛
۵) در ICS، پاسخ به‌موقع به واکنش انسان و حس‌گرهای فیزیکی بسیار مهم است؛
۶) ICS از پروتکل‌های ارتباطی اختصاصی برای کنترل دستگاه‌های field استفاده می‌کند؛
۷) قطعات ICS به‌ندرت جایگزین می‌شوند (۱۵-۲۰ سال یا بیشتر کار می‌کنند)؛
۸) اجزای ICS، توزیع‌شده و مجزا هستند و ازاین‌رو دسترسی فیزیکی برای تعمیر و ارتقای آن‌ها دشوار است.

در مستند NIST SP 800-82 خلاصه‌ای از بهترین تجارب عملی و فناوری‌های توصیه‌شده در حیطهٔ وسیعی از راه‌حل‌های امنیتی آورده شده است [۲].

حمله به ICS ها به‌سرعت در حال وقوع و هزینهٔ این حملات برای دولت‌ها و صنایع قابل‌توجه است [۶]. اداره حسابداری دولتی ایالات‌متحده عنوان کرده است که حملات سایبری به زیرساخت‌های حیاتی و سامانه‌های فدرال بین سال‌های ۲۰۰۶ تا ۲۰۱۲ به ۷۸۲ درصد افزایش یافت [۷] . اگرچه این ارقام در حال حاضر منسوخ شده‌اند، اما نشان‌گر آغاز یک روند خطرناک حمله به زیرساخت‌های حیاتی هستند. هزینه حملات سایبری به زیرساخت‌های نفت و گاز برای شرکت‌ها معادل ۱,۸۷ بیلیون دلار در سال ۲۰۱۸ تخمین زده می‌شود [۸] .

ساختار این مقاله به این صورت است: در بخش ۲، به تشریح سامانه‌های کنترل صنعتی پرداخته شده و چالش‌های مطرح در امنیت آنها نیز در بخش ۳ مطرح شده است. بخش ۴ به موضوع انتخاب پایگاه دادهٔ مورد بررسی در این مقاله می‌پردازد. در ادامه، در بخش ۵ روشی برای نمایه‌سازی حملات برای تحلیل وقایع در این مقاله شرح داده شده است. حملات مورد بررسی در بخش ۶ تشریح شده‌اند. در انتها در بخش ۷ و ۸ تحلیل رخدادهای امنیتی و جمع‌بندی آنها ذکر شده است.

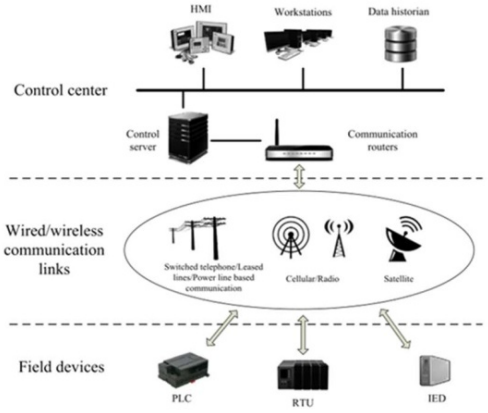
۲- سامانه‌های کنترل صنعتی

بر اساس مرجع [۹]، معماری کلی ICS در شکل (۱) نشان داده شده است. اجزای اصلی ICS عبارت‌اند از:

- کنترل‌کنندهٔ منطقی قابل‌برنامه‌ریزی[1] (PLC): PLC، یک رایانهٔ دیجیتال است که برای پردازش‌های الکترومکانیکی صنعتی خودکار استفاده می‌شود. PLCها حالت دستگاه‌های خروجی را بر اساس سیگنال‌های دریافت‌شده از حس‌گرها و برنامه‌های ذخیره‌شده کنترل می‌کنند. PLCها در شرایط سخت محیطی مانند ارتعاشات بالا و سروصدای زیاد عمل می‌کنند[۱۰]. PLCها تجهیزات مستقل و فرآیندهای تولید گسسته را کنترل می‌کنند.
- سامانهٔ کنترل توزیع‌شده[2] (DCS): DCS یک سامانهٔ کنترل خودکار است که در آن عناصر کنترل در سراسر سامانه توزیع شده‌اند [۱۱]. کنترل‌کننده‌های توزیع‌شده به‌منظور تأمین نظارت از راه دور فرایندها، به شبکه متصل می‌شوند. اگر بخشی از سامانهٔ کنترل از کار بیافتد، DCS هم‌چنان فعال می‌ماند. DCSها اغلب در فرایندهای پیوسته[3] و دسته‌ای[4] تولید می‌شوند که نیاز به کنترل و ارتباط پیشرفته با دستگاه‌های هوشمند field دارند.
- کنترل نظارت و اکتساب داده[5] (اسکادا) :اسکادا یک سامانهٔ رایانه‌ای است که برای نظارت و کنترل فرایندهای صنعتی استفاده می‌شود. اسکادا سایت‌های field را که در یک منطقه وسیع جغرافیایی پخش شده‌اند، نظارت و کنترل می‌کند. سامانه‌های اسکادا اطلاعات را به‌صورت بی‌درنگ از مکان‌های دور جمع‌آوری می‌کند؛ سپس تصمیمات نظارتی برای تنظیم کنترل‌ها انجام می‌شود.
- همان‌طورکه در شکل (۱) نشان داده شده است، داده‌های فرایند صنعتی که در سایت‌های راه دور جمع‌آوری می‌شوند، توسط دستگاه‌های field مانند پایانهٔ از راه دور[6] (RTU)، دستگاه‌های الکترونیکی هوشمند[7] (IED) و کنترل‌کنندهٔ منطقی قابل برنامه‌ریزی (PLC)، از طریق پیوندهای سیمی و بی‌سیم، به مرکز کنترل ارسال می‌شود. سرویس‌دهندهٔ کنترل، مشتریان را برای دسترسی به

[1] Programmable Logic Controller
[2] Distributed Control System
[3] Continuous
[4] Batch
[5] Supervisory Control And Data Acquisition
[6] Remote Terminal Unit
[7] Intelligent Electronic Device

داده‌ها با استفاده از پروتکل‌های استاندارد، مجاز می‌کند. رابط کاربری انسان-ماشین (HMI)، داده‌های پردازش شده را با پرس‌وجو از داده‌های زمان‌بندی‌شدهٔ انباشته‌شده در نرم‌افزار تاریخ نگار داده[1]، به یک اپراتور انسانی ارائه می‌کند. داده‌های جمع‌آوری‌شده، تجزیه و تحلیل می‌شوند و دستورهای کنترل به کنترل‌کننده‌های از راه دور ارسال می‌شود.



(شکل-۱): ساختار کلی ICS

این معماری از پروتکل‌های TCP/IP، UDP و سایر پروتکل‌های ارتباطی مبتنی بر IP به‌علاوهٔ پروتکل‌های صنعتی نظیر Modbus TCP، Modbus روی TCP یا Modbus روی UDP، پشتیبانی می‌کند. هر یک از این موارد از طریق شبکه‌های سلولی[2]، رادیویی یا ماهواره‌ای خصوصی[3] می‌توانند کار کنند. انتخاب نحوهٔ ارتباط، به چندین عامل بستگی دارد که عبارتند از: میزان دور بودن[4]، ارتباطات موجود در مکان‌های دور، زیرساخت‌های ارتباطی موجود، فرکانس نمونه‌برداری[5] و نرخ داده. این عوامل تصمیم نهایی در مورد معماری اسکادا را تحت تأثیر قرار می‌دهد[۹].

همان‌طورکه در [۱۲] عنوان شده، تعداد پروتکل‌های ارتباطی که در سامانه‌های کنترل صنعتی استفاده شده، بسیار زیاد است(حدود ۱۵۰ تا ۲۰۰ پروتکل). متداول‌ترین آنها عبارتند از: Ethernet/IP، DeviceNet، ControlNet، PROFIBUS، MODBUS، DNP3 و Foundation Fieldbus.

آسیب‌پذیری‌های این پروتکل‌ها در منابع متعددی مورد بررسی قرار گرفته است [۲۰].

در عین گستردگی پروتکل‌های استفاده‌شده در سامانه‌های کنترل صنعتی، با گستردگی استانداردهای ارتباط امن در این سامانه‌ها نیز مواجه هستیم. در [۱۳] به استانداردهای ارتباطاتی اسکادا که توسط چند سازمان ملّی ایجاد شده، اشاره شده است. این استانداردهای ارتباطی عبارتند از:

الف) IEEE C37.1: این استاندارد در سال ۲۰۰۸ و به‌عنوان نمونهٔ اولیه برای سامانه‌های اتوماسیون اداری مورد استفاده برای اسکادا و کنترل اتوماسیون آن در آمریکا طراحی شده است [۱۴] و در حال حاضر چهار نسخه دارد که عبارتند از؛ ANSI / IEEE C37.1-1979، ANSI / IEEE C37.1-1987 و IEEE Std.C37.1-1994 و IEEE Std.C37.1-2007.

ب) IEEE Std. 999-1992: این استاندارد مجموعه تجارت موفق و توصیه شده برای ارتباطات در اسکاداست [۱۵].

ج) NCS TIB 04-1: سامانهٔ ارتباطات ملّی [6] (NCS)در سال ۲۰۰۴، یک بولتن اطلاعات فنّی برای سامانه‌های اسکادا منتشر کرده است که گزارش‌های مروری اخیر را در مورد معماری‌ها و پروتکل های اسکادا در خصوص ارتباطات پوشش می‌دهد [۱۶].

به غیر از استانداردهای ملّی یادشده، پژوهش‌گران بسیاری، فناوری‌های ارتباطی جدیدی را برای سامانهٔ ارتباطی اسکادا پیشنهاد کرده‌اند. همچنین روش‌های ارتباطی پیشرفته برای تطابق با زیرساخت‌های ارتباطی موجود در اسکادا پیشنهاد شده است.

۳- امنیت سامانه‌های کنترل صنعتی

شبکه‌های ICS بسیار متفاوت از شبکه‌های IT هستند؛ زیرا در هر کدام پارامترهای زیر متفاوت است [۱۷]:

- نیازمندی‌های کارکردی؛
- نیازمندی‌های قابلیت اطمینان؛
- سیستم‌عامل‌ها و برنامه‌های کاربردی؛
- اهداف مدیریت ریسک؛
- معماری‌های امنیتی؛
- اهداف امنیتی

در شبکه‌های ICS اولویت نخست دردسترس‌بودن خدمات شبکه است؛ درحالی‌که در شبکه‌های IT، اولویت نخست، محرمانگی است. علاوه‌براین، مرکز شبکه‌های IT، یک اتاق رایانه‌ای امن و کنترل‌شده است که به‌عنوان مرکز داده با تجهیزات مدرن استاندارد طراحی می‌شود. درحالی‌که مرکز تمام شبکه‌های ICS اغلب در کارخانه قرار دارد که بیش‌تر

[1] Data Historian
[2] Cellular
[3] Private Radio Or Satellite Networks
[4] Remoteness
[5] Polling Frequency
[6] National Communication System

اوقات یک محیط خطرناک است و تجهیزات آن‌ها میانگین عمر بیش از ۱۰ سال دارند.

به‌عنوان دلایل اصلی هک‌شدن بسیاری از دستگاه‌های صنعتی، موارد زیر در مرجع [۱۸] بیان شده است:

الف) در بسیاری از محیط‌های صنعتی، دستگاه‌ها برای هفته‌ها یا ماه‌ها بدون هیچ‌گونه به‌روزرسانی امنیتی یا حتی وجود ابزارهای ضدویروس اجرا می‌شوند.

ب) بسیاری از کنترل‌کننده‌هایی که در شبکه‌های ICS استفاده می‌شوند، به‌نحوی طراحی شده‌اند که در طراحی آن‌ها دید امنیتی، جایگاهی نداشته است. درنتیجه این کنترل‌کننده‌ها می‌توانند توسط ترافیک شبکه‌ای نادرست و یا حتی حجم بالای ترافیک درست، مختل شوند.

ج) بسیاری از شبکه‌های ICS مسیرهای دسترسی متعددی دارند که از طریق آن تهدیدهای امنیتی سایبری می‌توانند اعمال شوند و اقدامات امنیتی سایبری را دور بزنند. نمونه‌های متداول این امر این است که لپ‌تاپ‌ها پیوسته به داخل و خارج از شبکه وارد و خارج می‌شوند یا فلش‌های USB که در رایانه‌ها بدون این‌که به لحاظ وجود بدافزار بررسی شوند، استفاده می‌شوند.

د) بسیاری از شبکه‌های ICS همچنان به‌عنوان یک شبکهٔ بزرگ مسطح، پیاده می‌شوند که هیچ‌گونه ایزوله‌سازی فیزیکی یا مجازی بین شبکه‌های غیر مرتبط وجود ندارد. این امر به گسترش سریع نرم‌افزارهای مخرب حتی در سایت‌های راه دور کمک می‌کند.

وضعیت کنونی امنیت سایبری در سامانه‌های کنترل صنعتی ناامیدکننده و قابل قیاس با وضعیت امنیت سایبری در پانزده سال پیش است [۱۹].

مرجع [۲۰] چارچوب بسیار مفیدی را درخصوص زمینه‌های مطالعاتی باز امنیت سایبری سامانه‌های کنترل صنعتی، ارائه کرده است. در این پژوهش، آسیب‌پذیری‌های سامانهٔ کنترل صنعتی به شش دسته تقسیم‌بندی می‌شوند:

۱. آسیب‌پذیری‌های تجهیزات فیلد؛
۲. آسیب‌پذیری‌های شبکه ارتباطی تجهیزات فیلد؛
۳. آسیب‌پذیری‌های کنترل‌کننده‌های محلی مانند RTU و PLC؛
۴. آسیب‌پذیری‌های پروتکل‌های ارتباطی شبکه کنترل؛
۵. آسیب پذیری‌های شبکه LAN کنترلی؛
۶. آسیب‌پذیری‌های شبکه‌های همکار و مالی– تجاری

مرجع [۲۱] آسیب‌پذیری‌های این سامانه‌ها را به شیوهٔ مناسبی معرفی کرده است.

امن‌سازی سامانه‌های کنترل صنعتی نیازمند توجه دقیق به استانداردهای امنیتی خاص سامانه‌های اسکادا است. ژو و همکاران در سال ۲۰۱۷ بررسی جامعی درخصوص تمامی استانداردهای امنیتی سامانه‌های کنترل صنعتی انجام داده‌اند. در این بررسی از بین بیش از چهل استاندارد صادرشده توسط کشورها و مؤسسه‌های مختلف، پانزده استاندارد انتخاب و مقایسه شده است. ملاک انتخاب این پانزده استاندارد سه مورد زیر بوده است:

۱) استاندارد توسط مؤسسات بین‌المللی یا نهادهای دولتی صادر شده باشد؛
۲) استاندارد به‌طور مشخص متمرکز بر امنیت سامانه‌های اسکادا باشد نه یک استاندارد کلّی؛
۳) استاندارد به‌روز بوده و از اعتبار و شهرت کافی برخوردار باشد [۲۲].

این استانداردها در شکل (۲) به‌تفکیک سال انتشار، نشان داده شده است. از آن‌جایی‌که بررسی این استانداردها در چارچوب این مقاله نمی‌گنجد، جهت مطالعه بیشتر به مرجع [۲۲] مراجعه شود.

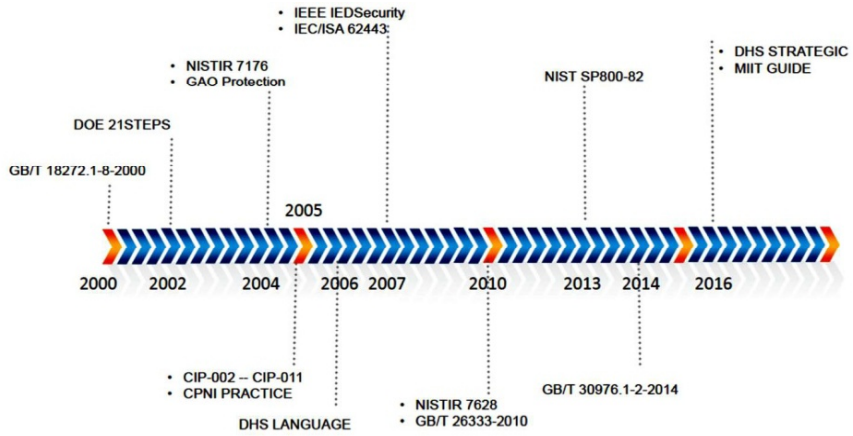
ازآن‌جایی‌که نخستین قدم برای جلوگیری از حملات به‌عنوان یک ریسک، شناخت ریسک بر اساس پارامترهای میزان تکرار و میزان اثر تخریبی حملات است، در این مقاله بر آن شدیم تا به بررسی حوادث رخداده در سامانه‌های کنترل صنعتی، بپردازیم.

۴- پایگاه دادهٔ حملات سامانه‌های کنترل صنعتی

در اوایل سال ۲۰۰۱، از سوی یکی از مراکز مهم پالایش نفت، از یک گروه پژوهشی امنیتی در مؤسسهٔ فناوری بریتیش کلمبیا (BCIT) خواسته شد تا امنیت سامانه‌های کنترل آن‌ها را مورد بررسی قرار دهند [۲۳]. در جریان این مطالعه معلوم شد که اطلاعات دقیق در مورد سابقهٔ حملات سایبری در صنایع اسکادا به‌طوری‌که امکان ارزیابی دقیق ریسک را فراهم کند، در دسترس نیست.

برای رفع این کمبود، نویسندگان پایگاه داده[1] ISID را با کمک جاستین لاو از شرکت PA Consulting تأسیس کردند. ISID به‌عنوان یک مخزن برای جمع‌آوری، تجزیه و تحلیل و به‌اشتراک‌گذاری اطلاعات باارزش در مورد حوادث امنیتی سایبری صنعتی که به‌طور مستقیم بر سامانه‌های کنترل، تولید و کنترل فرایند اسکادا تأثیر می‌گذارد، در نظر گرفته شده است.

[1] The Industrial Security Incident Database



(شکل-۲): استانداردهای امنیتی سامانه‌های کنترل صنعتی بر حسب سال انتشار آنها [۲۲].

حوادث جمع‌آوری‌شده در این پایگاه داده، یا از طرف سازمان‌ها به‌طور داوطلبانه و با ارسال فرم گزارش‌دهی جمع‌آوری شده و یا گزارش جمع‌آوری‌شده توسط کارکنان ISID از منابع عمومی مانند اینترنت، بحث‌های کنفرانس‌های امنیتی اسکادا / صنعت سایبری و انتشارات مربوطه صنعتی حاصل شده است. تمامی حوادث ثبت‌شده توسط پژوهش‌گران ISID بررسی و تأیید شده است. ازآن‌جایی‌که بسیاری از حملات این پایگاه داده، تکرار حملات قبلی در صنایع مختلف یا کشورهای مختلف‌اند، و هدف این مقاله بررسی حملات جدید و چالش‌های بزرگ امنیتی در دنیا بوده است، در این مقاله از آمارها و ارقام این پایگاه داده استفاده نشد. علاوه‌براین، همان‌طور که در مرجع [۲۴] اشاره شده است، پژوهش‌ها پس از حادثه در زمینهٔ حملات واقعی، منابع ارزشمندی هستند. گزارش رولف لانگر[1] در مورد بدافزار استاکس‌نت[2] شناخته‌شده در مرجع [۲۵] ، که هدف‌قراردادن تأسیسات هسته‌ای ایران بود، نمونهٔ خوبی از چنین منابعی است. این منابع دارای مزیتی هستند که بر حملات واقعی و موفقیت‌آمیز قرار می‌گیرند و در آن‌ها به تجزیه و تحلیل کامل حوادث پیچیده پرداخته که اغلب توسط مراجع دولتی پشتیبانی مالی می‌شوند [۲۴]؛ لذا به جای پروفایل‌های ساده‌تر حملات در پایگاه داده ISID، ما در این مقاله به بررسی حملات شاخصی که در منابع پژوهشی به آن‌ها پرداخته شده است و تحلیل امنیتی شده‌اند، خواهیم پرداخت.

۵- نمایه‌سازی حملات

در این مقاله بر اساس نمایه‌سازی[3] ارائه‌شده توسط کاجرلند[4] در مرجع [۲۶]، رخدادهای امنیتی اسکادا را بر اساس ملاک‌های «هدف حمله»، «منطقهٔ جغرافیایی مورد حمله»، «روش حمله»، «تأثیر حمله» نمایه می‌کنیم.

در این روش نمایه‌سازی، منظور از بیان هدف حمله، مشخص‌کردن این است که سامانه‌های قربانی چه نوع دستگاه‌هایی را شامل می‌شوند. منطقهٔ جغرافیایی مورد حمله، مشخص‌کنندهٔ این است که هدف حمله یک نهاد دولتی، خصوصی یا مربوط به چه دامنه‌ای است. این امر می‌تواند به تحلیل انگیزهٔ مهاجم که سیاسی، مالی، مخرب و غیره است، کمک کند. همچنین می‌توان با تحلیل هدف حمله و منطقهٔ جغرافیایی مورد حمله، در مورد علایق مهاجمان بیشتر دانست.

روش حمله، اطلاعاتی راجع به ابزارهای مورد استفادهٔ مهاجم و نقطهٔ دسترسی فراهم می‌کند و می‌تواند یکی از یازده مورد زیر باشد:

۱- سوءاستفاده از منابع - استفاده غیرمجاز از منابع، برای مثال ذخیره فایل‌های غیرمجاز بر روی سرور و استفاده از این سایت به‌عنوان یک گام برای فعالیت‌های غیرمجاز بیشتر؛
۲- سوءاستفاده از دسترسی غیرمجاز به کاربر؛
۳- سوءاستفاده از دسترسی غیرمجاز به *root*؛
۴- مهندسی اجتماعیِ دست‌یابی غیرمجاز به اطلاعات ممتاز از طریق فریب انسان‌ها؛
۵- کد مخربِ ویروس؛
۶- کد مخربِ تروجان؛
۷- کد مخربِ کرم‌واره؛
۸- سوءاستفاده از آسیب‌پذیری‌های وب؛
۹- پویش سایت و مشاهدهٔ خدمات در دسترس برای تعیین آسیب‌پذیری‌های موجود جهت سوءاستفاده؛

[1] Rolf Langer
[2] Stuxnet
[3] Profiling
[4] Kjaerland

۱۰- ممانعت از سرویس قطع برنامه یا کل سامانه؛
۱۱- شکست‌های سامانه‌ای دیگرِ حادثه‌هایی ناشی از ضعف در طراحی یا موارد ناشناخته‌ها دیگر؛

بر اساس نمایه‌سازی ارائه‌شده توسط کاجرلند، تأثیر یک حمله، نشان‌دهندهٔ نتیجهٔ نهایی یک حمله است و می‌تواند یکی از موارد زیر باشد:

۱- اختلال[1]- دسترسی تغییر و یا حذف دسترسی قربانی به اطلاعات یا حذف خود اطلاعات. مانند حملهٔ انکار سرویس
۲- خراب‌کاری[2]- تغییر فایل‌ها و یا اطلاعات فایل‌های قربانی
۳- تخریب[3] - حذف فایل‌ها یا حذف اطلاعات قربانی. تخریب ممکن است، شامل اختلال یا خراب‌کاری باشد.
۴- افشا[4] - نمایش غیرمجاز اطلاعات. اطلاعاتی که خود ممکن است، منجر به حملات بیشتر شود؛ مانند بارگیری فایل رمز عبور.
۵- مرگ – ازدست‌دادن زندگی انسانی.
۶- ناشناخته – حملات با اطلاعات ناکافی برای طبقه‌بندی.

کاجرلند نشان داد که جنبه های حوادث سایبری (شامل هدف حمله، روش و تأثیر و منطقه آن) می توانند در کشف هدف حملات، از طریق طبقه‌بندی وقایع استفاده شوند [۲۶]. با استفاده از ویژگی‌های حمله و اطلاعاتی در مورد روش عملیات، می‌توان در مورد مهاجم و انگیزهٔ حمله نتیجه‌گیری بهتری کرد. این نوع نمایه‌سازی جنایی، در بسیاری از زمینه‌ها مانند آتش‌سوزی، سرقت، تروریسم و غیره انجام شده است.

در مواردی که داده‌ها به‌صورت دودویی باشند (یعنی یا متغیر جرم وجود دارد یا ندارد)، تجزیه و تحلیل داده‌های جرایم از طریق روش‌های پوسته‌بندی چندبعدی[5](MDS) ، مانند کوچک‌ترین تجزیه و تحلیل فضایی[6] (SSA) و تجزیه و تحلیل مقیاس چندگانه[7](MSA) ، را می‌توان به کار برد. همچنین تجزیه و تحلیل داده‌های این نمایه‌سازی، می‌تواند روشن‌گر روابط کمی بین متغیرها را از طریق ضریب بیگانگی[8] یا سایر معیارهای همبستگی نشان دهد [۲۶].

در ادامه حملات مهم به سامانه‌های اسکادا بررسی و بر اساس پارامترهای یادشده، نمایه‌سازی خواهد شد.

۶- بررسی تاریخچهٔ حملات به سامانه‌های اسکادا

[1] Disrupt
[2] Distort
[3] Destruct
[4] Disclosure
[5] Multidimensional Scaling
[6] Smallest Space Analysis
[7] Multiple Scaling Analyses
[8] coefficient of alienation

۶-۱- حمله به سامانهٔ اپراتور کالیفرنیا

سال حمله: ۲۰۰۱
هدف حمله: شبکه‌های اتوماسیون صنعتی PCS
منطقهٔ جغرافیایی مورد حمله: کالیفرنیا

مهاجمان در ماه مه سال ۲۰۰۱ قادر به دسترسی به یکی از شبکه‌های رایانه‌ای در سامانه اپراتور مستقل کالیفرنیا[9] (Cal-ISO) شدند. Cal-ISO دارای کنترل سلسله‌مراتبی روی تعداد زیادی از شبکه‌های PCS[10] بود. این شبکه‌های PCS به‌نوبهٔ خود توسط سازندگان خود اداره می‌شد. اگرچه این هکرها در نفوذ به شبکه‌های PCS ناموفق بودند، اما بااین‌وجود بیش از دو هفته کنترل Cal-ISO را در دست داشتند [۲۷]. این حمله به‌عنوان "مهم‌ترین حادثهٔ تروریسم داخلی شبکه در ایالات متحده" تا آن زمان شناخته شد. در مرجع [۲۷] آسیب‌پذیری‌هایی که در ارزیابی Sandia از شبکه‌های PCS، دیده می شوند، نیز ذکر شده است. این آسیب‌پذیری‌ها در دسته‌بندی‌های زیر بررسی شده‌اند: (۱) داده‌ها (۲) مدیریت امنیت، (۳) معماری، (۴) شبکه و (۵) بسترهای نرم‌افزاری برای کمک به تعیین استراتژی‌های بهینهٔ دفاعی. هر PCS خاص به‌طورمعمول زیرمجموعه‌ای از این آسیب‌پذیری‌ها را دارد، اما ممکن است، برخی مشکلات اضافی منحصربه‌فرد را نیز داشته باشد.

روش حمله: دسترسی غیرمجاز به root
تأثیر حمله: ناشناخته

۶-۲- حمله به شبکهٔ تأسیسات هسته‌ای Davis Besse

سال حمله: ۲۰۰۳
هدف حمله: تأسیسات هسته‌ای
منطقهٔ جغرافیایی مورد حمله: ایالت اوهایوی آمریکا
شرح حمله: کرم SQL Slammer به شبکه‌های نیروگاه هسته‌ای Davis Besse در اوهایو نفوذ کرد. ممانعت از خدمات در اثر سیلاب بسته‌های ارسالی در شبکه، شگرد این کرم‌واره محسوب می‌شود. بر اثر این حمله سامانهٔ نظارتی برای حدود پنج ساعت و رایانه پردازش تأسیسات، حدود شش ساعت از کار افتادند. همچنین ارتباطات شبکه‌های کنترل دست‌کم پنج تأسیسات دیگر را با انتشار سریع مختل کرد [۲۸].
مهم‌ترین عملیات انجام‌شده: کندکردن شبکه
روش حمله: کرم‌واره، ممانعت از سرویس
تأثیر حمله: اختلال

۶-۳- حمله ویروس Sobig به شرکت CSX

سال حمله: ۲۰۰۳

[9] California Independent System Operator
[10] Process Control System
نام دیگری برای اتوماسیون شبکه‌های صنعتی است

هدف حمله: سامانه‌های قطار

منطقهٔ جغرافیایی مورد حمله: فلوریدا آمریکا

در یک مورد مشابه با کرم SQLSlammer، در سال ۲۰۰۳، یک ویروس رایانه‌ای به نام Sobig گزارش داده شد. این ویروس سامانه‌های سیگنالینگ قطار را در فلوریدا تعطیل کرد. این ویروس یکی از سریع‌ترین ویروس‌های پیوست‌شده به رایانامه در آن زمان بود. این ویروس، سامانه‌های سیگنالینگ، dispatching و سایر سامانه‌ها را در شرکت CSX خاموش می‌کرد؛ شرکت CSX یکی از بزرگ‌ترین شرکت‌های حمل‌ونقل در ایالات‌متحده بود. گرچه این ویروس منجر به هیچ حادثه‌ای نشد، اما قطارها به تأخیر افتادند [۲۹].

مهم‌ترین عملیات انجام‌شده: ارسال spam از طریق رایانامه

روش حمله: ویروس

تأثیر حمله: اختلال

۶-۴- حمله کرم‌واره slammer به تأسیسات برق

سال حمله: ۲۰۰۳

هدف حمله: تأسیسات برق

منطقهٔ جغرافیایی مورد حمله: آمریکای شمالی

شرح حمله: شورای تجهیزات آمریکای شمالی[1] (NREC) اثرات کرم‌واره slammer را بر تأسیسات برقی مورد استفاده در آمریکای شمالی گزارش داد. این کرم‌واره از طریق یک اتصال VPN به شبکه شرکتی وارد شد و درنهایت به شبکهٔ کنترل نظارت و کسب داده (اسکادا) رسید و یک سرور را در شبکه کنترل مرکزی که MS-SQL را اجرا می‌کرد، آلوده ساخت. ترافیک کرم‌واره، ترافیک اسکادا را مسدود کرد که درنتیجه این حمله باعث یک خاموشی سراسری شد [۳۰].

روش حمله: کرم‌واره، ممانعت از سرویس، دسترسی غیرمجاز به کاربر

تأثیر حمله: اختلال

۶-۵- حمله گسترده کرم‌واره Slammer

سال حمله: ۲۰۰۳

هدف حمله: بانک‌ها، تأسیسات هسته‌ای، فرودگاه‌ها، اورژانس و...

منطقهٔ جغرافیایی مورد حمله: در بسیاری از مناطق نفوذپذیر دنیا

شرح حمله: کرم slammer ممانعت از سرویس در شبکه را با استفاده از ارسال سیلاب بسته‌ها در شبکه در پی دارد. پس از حمله به تأسیسات برق، در همان سال یک حملهٔ گسترده با استفاده از این کرم‌واره طراحی شد که در کمتر از ده دقیقه، به بیش از نوددرصد از سامانه‌های آسیب‌پذیر دنیا در صنایع مختلف نفوذ کرد و باعث ازکارافتادن شبکهٔ بانک‌ها، ATMها، لغو پروازها، اورژانس‌های پزشکی و نیروگاه‌های هسته‌ای شد [۳۱-۳۳].

روش حمله: کرم‌واره، ممانعت از سرویس

تأثیر حمله: اختلال

۶-۶- حمله به سامانه‌های کنترل ترافیک هوایی

سال حمله: ۲۰۰۴

هدف حمله: سامانه کنترل ترافیک هوایی

منطقهٔ جغرافیایی مورد حمله: کالیفرنیای جنوبی

شرح حمله: به‌طورتقریبی به اندازهٔ ۳,۵ ساعت رادیو و صفحات رادار سامانهٔ کنترل ترافیک هوایی بدون هیچ هشدار قبلی از کار افتاد. اطلاعات بیشتری در مورد این حمله منتشر نشده و روش حمله ناشناخته باقی مانده است [۳۴].

روش حمله: ناشناخته

تأثیر حمله: اختلال

۶-۷- حمله باران تیتان

سال حمله: ۲۰۰۴

هدف حمله: ناسا و سامانهٔ امنیت نظامی

منطقهٔ جغرافیایی مورد حمله: آمریکا

شرح حمله: باران تیتان[2]، نامی است که توسط FBA به حملاتی که هدف آن‌ها ضربه‌زدن به ناسا و در کل امنیت نظامی آمریکا- به عنوان بزرگ‌ترین سازنده تسلیحات جهان- بوده است، داده شد. در این حمله، علاوه‌بر لورفتن اطلاعات بسیار حساس، سامانه‌ها تبدیل به ماشین‌های Zombie می‌شدند که هک‌کردن آن‌ها در آینده بسیار راحت‌تر می‌شد؛ باران تیتان یکی از بزرگ‌ترین حملات سایبری تاریخ است که به‌احتمال توسط هکرهای چینی و با هدف سیاسی/اقتصادی انجام گرفته است. گرچه این حمله شبکه‌های محافظت‌نشدهٔ نظامی را هدف قرار داد، ولی اطلاعات حساسی در این شبکه‌ها به‌دست آمد[۳۵]. اطلاعات بیشتری راجع به روش حمله منتشر نشده است[۳۵و۵۹].

روش حمله: ناشناخته

تأثیر حمله: افشا، اختلال

[1] The North American Equipment Council

[2] Titan Rain

۶-۸- حملهٔ کرم‌واره sasser

سال حمله: ۲۰۰۴

هدف حمله: مراکز مهم دولتی، نظامی، خدماتی و درمانی

منطقهٔ جغرافیایی مورد حمله: به‌طورتقریبی تمام دنیا!

شرح حمله: جاشان هیجده‌ساله، کرم‌واره sasser را منتشر کرد؛ این کرم‌واره رایانه‌ای، ده‌ها میلیون رایانه را در سرتاسر جهان آلوده ساخت. گزارش‌ها حاکی از آن بود که هفتاددرصد رایانه‌ها و سامانه‌های آلودهٔ جهان در نیمهٔ نخست سال ۲۰۰۴ به این کرم‌واره مبتلا شده‌اند. بیش‌ترین سطح صدمات این کرم‌واره، زمانی بود که سامانه‌های رایانه‌ای خطوط هوایی دلتا به این کرم آلوده و غیرفعال شدند و درنتیجه بسیاری از پروازها لغو شد. بعد از پخش‌شدن کرم‌واره، بیشتر بیمارستان‌های دنیا اعلام مشکل کردند. همچنین نیروی ساحلی انگلستان و سامانه‌های نظامی این کشور از کار افتادند [۳۶].

مهم‌ترین عملیات انجام شده: تکثیر خود در شبکه و مختل کردن شبکه

روش حمله: کرم‌واره

تأثیر حمله: اختلال

۶-۹- حمله به سامانه تصفیه آب

سال حمله: ۲۰۰۶

هدف حمله: سامانه تصفیه آب

منطقهٔ جغرافیایی مورد حمله: هاریسبرگ

شرح حمله: یک هکر خارجی از طریق اینترنت به امنیت یک کارخانه تصفیه آب نفوذ کرد. مهاجم نرم‌افزارهای مخربی را کشف کرد که قادر به تأثیرگذاری روی عملیات تصفیه آب بود و منجر به هدایت آب آلوده به بخش‌هایی از شهر شد.

روش حمله: کد مخرب، بهره‌برداری از آسیب‌پذیری وب

تأثیر حمله: مرگ

۶-۱۰- حملهٔ Aurora

سال حمله: ۲۰۰۷

هدف حمله: زیرساخت برق

منطقهٔ جغرافیایی مورد حمله: آمریکای شمالی

شرح حمله: در سال ۲۰۰۷، آزمایشگاه ملّی آیداهو حملهٔ آئورو[1] را انجام داد، تا نشان دهد چگونه یک حملهٔ مجازی می‌تواند اجزای فیزیکی شبکه برق را از بین ببرد. مهاجم، دسترسی به شبکه کنترل‌کننده یک ژنراتور دیزل را به‌دست آورد. در این حمله، یک برنامهٔ رایانه‌ای مخرب بهسرعت به بازکردن و بستن مدارهای ژنراتور، خارج از فاز بقیهٔ شبکه و به‌صورت ناهمگون پرداخت [۳۷]. این عمل منجر به انفجار دیزل ژنراتور شد که یک میلیون دلار خسارت وارد کرد. ازآن‌جایی‌که بیش‌تر تجهیزات شبکه از پروتکل‌های ارتباطی قدیمی استفاده می‌کنند که امنیت را در نظر نمی‌گیرند، این آسیب‌پذیری بسیار نگران‌کننده است [۳۸].

روش حمله: کد مخرب، سوءاستفاده از دسترسی غیرمجاز

تأثیر حمله: اختلال

۶-۱۱- حمله به TCAA

سال حمله: ۲۰۰۷

هدف حمله: شرکت برق

منطقهٔ جغرافیایی مورد حمله: کالیفرنیا

یک سرپرست پیشین برق در مؤسسهٔ TCAA[2]، نرم‌افزار غیرمجازی را در سامانهٔ اسکادای این شرکت نصب کرد. این کارمند بعد از هفده سال کار در این مؤسسه، روزی که اخراج شد، این نرم‌افزار را نصب کرد. هیچ گزارش فنّی‌ای در مورد تجزیه و تحلیل این نرم‌افزار غیرمجاز به‌صورت عمومی منتشر نشد؛ لذا جزئیات نرم‌افزار غیرمجاز علنی نشد و نمی‌دانیم آیا خسارتی ایجاد شده یا خیر [۲۸].

روش حمله: سوءاستفاده از منابع

تأثیر حمله: ناشناخته

۶-۱۲- حملهٔ کرم‌واره AGENT.BTZ

سال حمله: ۲۰۰۸

هدف حمله: ماشین‌های نظامی

منطقهٔ جغرافیایی مورد حمله: آمریکا

شرح حمله: با کمک کرم‌وارهٔ AGENT.BTZ، ماشین‌های ارتش آلوده شدند. نقص فنّی CENTOMS به‌طور گسترده در رسانه‌ها منتشر شد؛ اما جزئیات خسارات و هدف حمله مبهم باقی ماند[۳۹].

روش حمله: کرم‌واره

تأثیر حمله: ناشناخته

۶-۱۳- حمله به سامانهٔ کنترل خط لوله

سال حمله: ۲۰۰۸

هدف حمله: سامانهٔ کنترل خط لوله

منطقهٔ جغرافیایی مورد حمله: ترکیه

[1] Aurora

[2] Tehama Colusa Canal Authority

شرح حمله: مهاجمان با استفاده از آسیب‌پذیری‌های نرم‌افزار "ارتباطات بی‌سیم به دوربین"، وارد سامانه شده و سپس به شبکهٔ داخلی وارد شدند. مهاجمان به واحدهای مورد استفاده برای هشدار عملکرد بد و نشتی‌ها به اتاق کنترل، رخنه کرده و PLC های موجود در دریچه‌ها را دست‌کاری کردند تا افزایش فشار در خط لوله باعث انفجار شود. بیش از سی‌هزار بشکهٔ نفت در یک ناحیه بالای سفره آب زیرزمینی، ریخته شد. علاوه‌براین در تعرفه‌های حمل‌ونقل پنج‌میلیون دلار در روز متحمل هزینه شد [۸].

روش حمله: سوءاستفاده از دسترسی غیرمجاز

تأثیر حمله: اختلال

۶-۱۴- حملهٔ کرم‌واره AHACK

سال حمله: ۲۰۰۸

هدف حمله: صنایع استیل

منطقهٔ جغرافیایی مورد حمله: برزیل

شرح حمله: این حمله بر اثر خراب‌کاری کرم‌واره AHACK انجام شد که در آن یک پیمان‌کار اسبق، به‌وسیله مودم 3G ، توانست به اینترنت درون نیروگاه، دسترسی پیدا کرده و کورهٔ برق و انفجار را با کرم‌واره AHACK آلوده سازد. سیل بسته‌های ناخواسته، باعث شد ارتباط بین PLCها و ایستگاه‌های نظارتی ناپایدار شده و دسترسی به این سامانه‌ها از بین برود. این کرم‌واره سامانه‌عامل ویندوز در برخی از ماشین‌آلات را نیز از کار انداخت و در سراسر شبکهٔ اتوماسیون نیروگاه، گسترش یافت. ازدست‌دادن کنترل سامانه‌ها، باعث راه‌اندازی مجدد سامانه‌های اسکادا شد. این کرم‌واره باعث ازبین‌رفتن تولید / عملیات و درنهایت زیان مالی شد [۴۰].

روش حمله: کرم‌واره، ممانعت از سرویس، سوءاستفاده از دسترسی کاربر

تأثیر حمله: اختلال

۶-۱۵- آزمون نفوذپذیری اسکادا در صنعت برق

سال حمله: ۲۰۱۰

هدف حمله: صنعت برق

منطقهٔ جغرافیایی مورد حمله: ایالت تگزاس

شرح حمله: این عملیات پژوهشی بر امنیت شبکه‌های صنعتی بود. آزمون نفوذپذیری به‌طورتقریبی روی یکصد دستگاه تولید برق انجام شد که بیش از ۳۸۰۰۰ مورد آسیب‌پذیری و هشدار امنیتی را نتیجه داد [۴۱]. برای نمونه، جدول (۱) فهرست خلاصه‌ای از این آسیب‌پذیری‌ها را نشان می‌دهد.

روش حمله: پویش همه‌جانبهٔ سایت

تأثیر حمله: ناشناخته

(جدول-۱): فهرست آسیب‌پذیری‌های سامانه‌های کنترل صنعتی تولید برق در تگزاس

آسیب پذیری‌های اسکادا بسته به مکان در شبکه	درصد	تعداد
Level 5 - Internet DMZ zone	%16.9	6561
Level 4 - Enterprise LAN zone	%24.7	9567
Level 3 - Operations DMZ	%46.3	17957
Level 2 - Supervisory HMI LAN	%11.8	4554
Level 1 - Controller LAN	%0.3	105
Level 0 - Instrumentations bus network	%0.0	0
Totals	%100.0	38744

شایع‌ترین آسیب‌پذیری مربوط به اشکال در پیکره‌بندی بوده است. جزئیات آسیب‌پذیری‌های یادشده در پیوست سند [۴۱] آورده شده است. هم‌چنین عنوان شده است آنقدر آسیب‌پذیری‌های قدیمی در سامانه‌های اسکادا وجود دارد که مهاجم نیازی به نوشتن حملات روز-صفر[1] نیز نخواهد داشت!

۶-۱۶- حمله به صنعت استیل

سال حمله: ۲۰۱۰

هدف حمله: صنایع استیل

منطقهٔ جغرافیایی مورد حمله: آمریکا

شرح حمله: در سال ۲۰۱۰ صنعت استیل در آمریکا در حال رقابت تجاری تنگاتنگی با شرکت‌های استیل چینی بود. در این زمان تعدادی رایانامه به کارمندان شرکت «استیل آمریکا» ارسال شد که برخی از این رایانامه‌ها موجب نصب یک بدافزار روی رایانه‌های این شرکت شدند. سه روز بعد، مشخصات کلیه رایانه‌های موجود در شبکهٔ شرکت، به دست شرکت چینی رقیب ونگ (Wang) افتاده بود. از جمله این رایانه‌ها، سامانه‌هایی بودند که دسترسی مستقیم به تأسیسات شرکت را کنترل می‌کردند و همچنین دستگاه‌های قابل‌حملی که به شبکه داخلی دسترسی داشتند. پس از آن شرکت «ونگ» توانست قدم‌هایی در راستای مشخص‌کردن و بهره‌برداری از نقاط ضعف سرورهای آن شرکت، بردارد [۴۲].

[1] Zero-day exploits

روش حمله: مهندسی اجتماعی، تروجان، سوءاستفاده از دسترسی کاربر

تأثیر حمله: افشا، اختلال

۶-۱۷- حمله کرم Stuxnet

سال حمله: ۲۰۱۰

هدف حمله: تأسیسات هسته‌ای

منطقهٔ جغرافیایی مورد حمله: ایران

شرح حمله: کرم رایانه‌ای stuxnet که حاوی بدنه پیام مخربی است و با الگوی نامشخصی پخش می‌شود، برای هدف‌گرفتن سامانه‌های اسکادا در نطنز طراحی شد. این کرم‌واره از چهار آسیب‌پذیری روز صفر[1]، استفاده می‌کرد. بنابراین زمان زیادی برای توسعهٔ Patch و اصلاح سامانه‌ها وجود نداشت. این کرم‌واره، از طریق فلش درایو USB آلوده، به سامانهٔ هدف معرفی شد و از گذرواژه‌های پیش‌فرض سیستم‌عامل ویندوز که از Wincc یا PCS7 استفاده می‌کردند، بهره‌برداری کرد؛ سپس Stuxnet با آلوده‌کردن درایوهای قابل‌حمل، رونوشت-کردن خود در منابع مشترک شبکه و هم‌چنین بهره‌برداری از آسیب‌پذیری‌های موجود، به‌صورت مخفیانه در شبکه منتشر شد. درایورهای استفاده‌شده در حملات این کرم‌واره، درایورهای تبدیل فرکانس Fararo Paya ایران و Vacon فنلاند بودند که در سانتریفیوژهای اورانیوم ۲۳۵ مورد استفاده قرار می‌گرفتند. از طریق این کرم‌واره، دستور اتصال به سرویس‌دهندهٔ فرمان و کنترل خارجی به رایانه‌های آلوده داده شد؛ سپس این کد مخرب، سرویس‌دهندهٔ مرکزی PLCها را دوباره برنامه‌ریزی کرد تا عملیات سانتریفیوژ را به‌نحوی تغییر دهد که خودشان را به‌واسطهٔ PLCهای آسیب‌دیده، نابود کنند؛ یعنی با تغییردادن فرکانس واردشده به درایورها و تغییر سرعت مداوم آن‌ها بین سرعت بیشینه و کمینه‌ای که برای کار با این سرعت‌ها طراحی نشده بودند. این کرم PLC های موجود در چهارده سایت صنعتی را در ایران آلوده کرد؛ از جمله کارخانه غنی‌سازی اورانیوم. همچنین این کرم‌واره سانتریفیوژها را نابود ساخت [۴۵-۴۳].

روش حمله: کرم‌واره، دسترسی غیرمجاز به root، تروجان

تأثیر حمله: اختلال، خراب‌کاری

۶-۱۸- حمله اژدهای شب[2]

سال حمله: ۲۰۱۱

هدف حمله: شرکت‌های نفتی، پتروشیمی و انرژی

منطقهٔ جغرافیایی مورد حمله: بین‌المللی

شرح حمله: در ماه فوریه ۲۰۱۱، McAfee گزارش داد که پنج شرکت انرژی و نفت جهانی با چندین حمله شامل حملات مهندسی اجتماعی، تروجان‌ها و Exploitهای مبتنی بر ویندوز مورد هدف قرارگرفته‌اند. اشاره شده که این حمله از مبدأ چین بوده، اما مهاجمان ممکن است، به‌سادگی از ابزار چینی استفاده کرده و رایانه‌های چینی را به‌خطر انداخته‌اند تا هویت خود را پنهان کنند.

اگرچه این حمله منجر به خراب‌کاری نشد، ولی باعث سرقت اطلاعات حساس شد. این حمله با تزریق SQL در سرورهای وب شرکت‌های بزرگ آغاز شد تا پس از آن از این سرورها برای دسترسی به سرورهای اینترنت استفاده شود. مهاجمان، نام کاربری و رمز عبور زیادی را به‌دست آوردند که امکان نفوذ بیشتر به رایانه‌های شخصی و سرورها را فراهم می‌کرد. گرچه سامانه‌های کنترل صنعتی شرکت‌های هدف تحت تأثیر این حمله قرار نگرفتند، اما با توجه به طراحی و عملکرد این سامانه‌ها ممکن است، اطلاعاتی استخراج شده باشد که بعدها از آن استفاده شود [۴۶و۲۹].

روش حمله: مهندسی اجتماعی، تروجان، افزایش دسترسی به دسترسی root

تأثیر حمله: افشا

۶-۱۹- حمله ویروس DUQU

سال حمله: ۲۰۱۱

هدف حمله: سامانه‌های کنترل صنعتی

منطقهٔ جغرافیایی مورد حمله: فرانسه، هلند، سوئیس، اوکراین، هند، ایران، سودان، ویتنام، انگلیس، اتریش، مجارستان و اندونزی

شرح حمله: حمله به این مناطق از نوع ویروس DUQU بود. DUQU ویروسی است از نوع تروجان که کدهای اصلی آن به‌طورکامل مشابه ویروس استاکس‌نت بود و می‌توانست با جمع‌آوری اطلاعات سامانه‌ها و مجتمع‌های صنعتی، زمینه را برای دراختیارگرفتن کنترل آن‌ها از راه دور فراهم کند. DUQU می‌تواند با استفاده از یک نقص امنیتی ویندوز در یک رایانه نفوذ کرده و در یک فایل WORD مخفی شود. درحقیقت این حمله مقدمه‌ای برای حمله‌های بزرگ‌تر بوده است؛ چون DUQU قابلیت تکثیر خود را نداشت و بدنهٔ آن حاوی هیچ Payload ای نبود [۴۷].

روش حمله: تروجان

تأثیر حمله: افشا

[1] Zero-Day Vulnerability

[2] Night Dragon

۶-۲۰- حملهٔ بدافزار Shamoon

سال حمله: ۲۰۱۲

هدف حمله: شرکت‌های نفت و گاز و انرژی

منطقهٔ جغرافیایی مورد حمله: عربستان صعودی

شرح حمله: این حمله توسط بدافزار Shamoon انجام گرفت. این بدافزار توانایی انتشار را از طریق بهره‌برداری از فضای دیسک سختی که بین سامانه‌های شبکه اشتراک گذاشته شده است، دارد. این بدافزار پس از آلوده‌سازی سامانه، فایل‌های خاصی از سامانه را به مهاجم می‌فرستد و سپس اقدام به پاک‌کردن این فایل‌ها می‌کند. درنهایت این بدافزار master boot record را بازنویسی می‌کند تا فرایند راه‌اندازی آیندهٔ سامانه با مشکل روبه‌رو شود. این بدافزار، رکورد راه‌انداز اصلی[1] (MBR) سامانه، جداول پارتیشن و فایل‌های دادهٔ تصادفی دیگری را به‌نحوی هدف می‌گرفت که سامانه از کار می‌افتاد. این کد مخرب توانست سی‌هزار رایانه و لپ‌تاپ شرکت آرامکو را آلوده کند و به‌احتمال درکل ۵۵۰۰۰ رایانه صنعتی را آلوده کرد. گروهی تحت عنوان "Cutting Sword of Justice" مسئولیت این حمله را به عهده گرفتند [۴۸].

روش حمله: سوءاستفاده از منابع، کد مخرب

تأثیر حمله: اختلال، افشا

۶-۲۱- حمله ویروس Flame

سال حمله: ۲۰۱۲

هدف حمله: سامانه‌های تأسیسات صنعتی

منطقهٔ جغرافیایی مورد حمله: خاورمیانه و شمال آفریقا

شرح حمله: محققان اخیراً بدافزاری در ایران، لبنان، سوریه، سودان، کرانه غربی و دیگر مکان‌های خاورمیانه و شمال آفریقا کشف کرده‌اند که دست‌کم به مدت دو سال در حال فعالیت بوده است. این حمله با کمک ویروسی به نام شعله[2] انجام شده که توسط همان گروه پشتیبان استاکس‌نت نوشته شده است. آمریکا و اسرائیل به‌طور مشترک این ویروس را با هدف تخریب سایبری هوشمند ساختند تا پیشرفت برنامه هسته‌ای ایران را به تعویق بیندازند. این ویروس امکان عکس‌گرفتن از صفحه نمایش‌گر، ذخیره‌سازی صدا، متون تایپ‌شده و ترافیک شبکه را داشت. همچنین می‌توانست مکالمات اسکایپ را ذخیره کند. همچنین ماژول بلوتوث سامانه را روشن کرده، اطلاعات اشخاص را از دستگاه‌های نزدیک که بلوتوث روشن دارند، دریافت کند. ویروس Flame این داده‌ها را به همراه اسناد و فایل‌های ذخیره‌شدهٔ مهم روی سامانهٔ آلوده، به یکی از چندین سروری که در سراسر جهان پراکنده بودند، ارسال می‌کرد. همچنین از این سرورها، دستورهایی برای فعالیت‌های بعدی خود دریافت می‌کرد. یکی از این دستورها، دستور «Kill» بود که با اجرای این دستور، هیچ ردپایی از این ویروس در سامانه باقی نمی‌ماند؛ این بدافزار، روی سامانه‌هایی با سیستم‌عامل ویندوز عمل می‌کرد و از طریق شبکه داخلی یا از طریق USB امکان انتشار داشت. درواقع هدف حملهٔ این ویروس طراحی‌ها، برنامه‌ریزی‌ها، و داده‌های ارزشمندی بود که در سامانه‌های تأسیسات صنعتی بزرگ ایران به‌طور محرمانه نگهداری می‌شد.

تجزیه و تحلیل‌های اولیه نشان می‌داد که این برنامه در درجهٔ نخست برای جاسوسی از کاربران رایانه‌های آلوده و سرقت اطلاعات، از جمله اسناد، مکالمات ضبط‌شده و عمل فشردن کلید است. این بدافزار، بعدازاین‌که اتحادیه بین‌المللی ارتباطات سازمان ملل[3] از پژوهش‌گران خواست تا گزارش‌های ارسالی به این سازمان در ماه آوریل را تحلیل کنند، کشف شد و گزارش شد که رایانه‌های متعلق به وزارت نفت ایران و شرکت ملّی نفت ایران با نرم‌افزارهای مخرب که اطلاعات را از سامانه‌ها سرقت و حذف می‌کنند، آلوده شده است [۴۹].

روش حمله: کرم‌واره

تأثیر حمله: افشا، تخریب

۶-۲۲- حمله Wiper

سال حمله: ۲۰۱۲

هدف حمله: شرکت‌های نفت و گاز و انرژی، نهادهای وابسته به دولت، سازمان‌های دیپلماتیک و سفارت‌خانه‌ها، مراکز پژوهشی و دانشگاه‌ها، شرکت‌های خاص غیردولتی

منطقهٔ جغرافیایی مورد حمله: ایران

شرح حمله: این حمله با کمک بدافزار Wiper صورت گرفت. این بدافزار به‌محض اجرا در همان بار نخست هیچ داده‌ای را سالم نمی‌گذاشت و همهٔ اطلاعات سامانه را پاک می‌کرد که منجر به توقف کار وب‌سایت‌های وزارت نفت و نهادهای وابسته شد. جزئیات بیشتر این رویداد منتشر نشده است [۵۰].

روش حمله: کد مخرب

تأثیر حمله: تخریب

۶-۲۳- حمله بدافزار The Mask

سال حمله: ۲۰۱۳

هدف حمله: شرکت‌های نفت و گاز و انرژی، نهادهای وابسته به دولت، سازمان‌های دیپلماتیک و سفارتخانه‌ها، مراکز پژوهشی و دانشگاه‌ها، برخی شرکت‌های غیردولتی

[1] Master Boot Record
[2] Flame
[3] United Nations International Telecommunications Union

منطقهٔ جغرافیایی مورد حمله: شماری از کشورها

شرح حمله: حمله با بدافزار The Mask انجام گرفت که یک سارق اطلاعات محسوب می‌شود و کار آن جاسوسی سایبری است. طراحان این بدافزار از مجموعه‌ای از ابزارهای متنوع استفاده کرده‌اند. این بدافزار شامل مجموعه‌ای از rootkit و boot kit است که برای سیستم‌عامل‌های مختلف از جمله Mac OS X، نسخه‌های مختلف لینوکس و به‌احتمال برای اندروید و iPad/iPhone قابل‌استفاده‌اند. به‌علت حرفه‌ای‌بودن بسیار زیاد این بدافزار و رویه‌های عملیاتی خاص و پیشرفته، احتمال می‌رود این بدافزار توسط مراکز مورد حمایت دولتی ساخته شده باشد [۵۱].

روش حمله: کد مخرب

تأثیر حمله: اختلال، افشا

۶-۲۴- حمله بدافزار MiniDuke

سال حمله: ۲۰۱۳

هدف حمله: سازمان‌های دولتی و نهادهای مالی کشورها

منطقهٔ جغرافیایی مورد حمله: کشورهای اروپایی، اوکراین، بلژیک، پرتغال، رومانی، جمهوری چک، ایرلند و...

شرح حمله: بدافزار MiniDuke مأمور این حمله بود که یک بدافزار سارق اطلاعات است. پس از این‌که داده‌ها از ماشین آلوده جمع‌آوری شدند، این داده‌ها به قطعات بسیار کوچک شده و به‌صورت رمزشده منتقل می‌شدند. داده‌های منتقل‌شده، در سمت مهاجمان، رمزگشایی می‌شوند، از بسته‌های داده استخراج و سپس قطعات مرتبط با یکدیگر ترکیب شده و دادهٔ اصلی را می‌ساختند [۵۲].

روش حمله: کد مخرب

تأثیر حمله: افشا

۶-۲۵- حمله بدافزار Red October

سال حمله: ۲۰۱۳

هدف حمله: حمله به مراکز دیپلماتیک، دولتی و علمی در کشورهای مختلف

منطقهٔ جغرافیایی مورد حمله: در حدود ۳۹ کشور از جمله کشورهایی که در گذشته عضو اتحادیه جماهیر شوروی بوده‌اند، کشورهای اروپای شرقی و برخی کشورهای آسیای میانه

شرح حمله: در این حملات بدافزار Red October نقش اساسی داشت. هدف این بدافزار، جمع‌آوری اطلاعات از سازمان‌های مورد نفوذ، شامل تمامی تجهیزات آن‌ها از جمله رایانه‌ها، دستگاه‌های تلفن همراه شخصی و تجهیزات شبکه بود. روش کار این بدافزار، ارسال رایانامه‌هایی حاوی اسناد ضمیمه‌شده‌ای بود که آسیب‌پذیری‌های word و excel را مورد سوءاستفاده قرار می‌دادند. طراحان این بدافزار، برای کنترل شبکه‌ای از ماشین‌های آلوده و همچنین کنترل و بازیابی داده‌های قربانیان، بیش از شصت دامنهٔ اینترنتی و چندین سرور میزبان محلی را در کشورهای مختلف ایجاد کردند. اطلاعات به‌سرقت‌رفته از قربانیان، اطلاعات سطح بالا و طبقه‌بندی‌شده‌ای بوده و شامل داده‌های جغرافیایی-سیاسی است که می‌تواند توسط دولت‌های ملّی مورد استفاده قرار گیرد [۵۳].

روش حمله: مهندسی اجتماعی، کد مخرب، سوءاستفاده از دسترسی کاربر

تأثیر حمله: افشا

۶-۲۶- حمله HAVEX

سال حمله: ۲۰۱۴

هدف حمله: سازمان‌های بخش انرژی

منطقهٔ جغرافیایی مورد حمله: تعدادی از شرکت‌های اروپایی

شرح حمله: در سال ۲۰۱۴ بدافزار HAVEX سامانه‌های صنعتی اسکادا و سامانه‌های ICS را آلوده کرد. این بدافزار به‌احتمال قادر به غیرفعال‌کردن سدهای آبی، بارگیری نیروگاه‌های هسته‌ای، و حتی شبکهٔ برق کشور تنها با فشردن یک کلید است. در این بدافزار علاوه‌بر روش‌های انتشار قدیمی مانند رایانامه‌های اسپم، از روش هک‌کردن وب‌سایت‌های شرکت‌های نرم‌افزاری و انتظار برای نصب نسخه‌های تروجان، استفاده شده است. تولیدکنندهٔ ماشین‌آلات صنعتی و دو سازمان آموزشی در فرانسه و شرکت‌های آلمانی، مورد هدف جاسوسی این بدافزار قرار گرفتند [۵۴].

روش حمله: کد مخرب، سوءاستفاده از آسیب‌پذیری وب، تروجان

تأثیر حمله: افشا

۶-۲۷- حملهٔ بدافزار BlackEnergy

سال حمله: ۲۰۱۵

هدف حمله: خطوط انتقال برق

منطقهٔ جغرافیایی مورد حمله: اوکراین

شرح حمله: یک حمله تأییدشده در سال ۲۰۱۵ به خطوط انتقال برق اوکراین اتفاق افتاد که ۵۷ ایستگاه برق در غرب اوکراین را به خاموشی مطلق فرو برد. در نخستین بررسی،

مشخص شد در سامانهٔ نظارتی یکی از شرکت‌های آسیب‌دیده، خللی رخ داده است که بعداً معلوم شد در نتیجهٔ حملهٔ هکر به سامانه‌های کنترل صنعتی بوده است و درنهایت، وقوع این حمله در ژانویه ۲۰۱۶ توسط CERT –UA تأیید شد. این حمله، بسیار پیچیده و با طراحی خیلی خوب بود، و در سه مرحله انجام شد:

در گام نخست آلوده‌کردن سامانه‌ها از طریق ارسال یک فایل word آلوده به ماکروهای مخرب از طریق رایانامه.

گام دوم جلوگیری از حذف و بازیابی فایل‌ها با پاک‌کردن فایل‌های سامانه‌ای از روی سامانهٔ کنترل.

و درنهایت، مهاجمان با تماس‌های تلفنی جعلی به مرکز سرویس‌های مشتریان شرکت‌های مختلف تولید قدرت (برق)، باعث شدند تا شرکت‌ها در بررسی و پیداکردن دلیل اصلی مشکل به تأخیر بیفتند. بدافزار استفاده‌شده در این حمله به خانواده بدافزارهای BlackEnergy متصل می‌شود [۵۵].

در این حمله مهاجمان، رایانامه‌های فیشینگ حاوی کدهای مخرب بهره‌بردار را برای کارکنان شبکه اداری و شرکت‌های برق ارسال کردند. به‌محض‌اینکه اولین رایانه‌ها آلوده شدند، مهاجمان توانستند منبع برق را مختل کرده و تمام دسترسی راه دور به شبکه را قطع کنند. این کار با از بین بردن نرم‌افزار بخصوصی در شرکت و خراب‌کردن Boot Sector سامانه، انجام شد که امکان مدیریت و تعمیر سامانه را از راه دور غیرممکن می‌ساخت [۵۶].

روش حمله: مهندسی اجتماعی، کد مخرب

تأثیر حمله: اختلال، تخریب

۶-۲۸- حملهٔ کرم‌وارهٔ Kido

سال حمله: ۲۰۱۶

هدف حمله: نیروگاه هسته‌ای

منطقهٔ جغرافیایی مورد حمله: آلمان

در پایان آوریل ۲۰۱۶ شرکت اپراتور نیروگاه هسته‌ای Gundremmingen گزارش داد که سامانهٔ کنترل این شرکت که مسئول بارگیری سوخت هسته‌ای است، به کرم‌وارهٔ Kido آلوده شده است. (این کرم‌واره Conficker نیز نامیده می‌شود) خوشبختانه کرم، بر فرایند فناورانه تأثیر نگذاشت و به نیروگاه آسیب نرساند [۵۶].

هرچند منشأ این کرم واره اعلام نشده است، اما گفته شد که حدود هیجده فلش USB که در شبکه‌های اداری استفاده می‌شدند، به این کرم‌واره آلوده شده‌اند. اعلام شد که این کرم‌واره هیچ آسیبی نمی‌تواند به‌وجود آورد؛ چون تمام سامانه‌های حیاتی کنترل ایزوله شده‌اند. هم‌چنین برای جلوگیری از حملات انکار سرویس، معماری کل سامانه دارای افزونگی است، لذا امکان دست‌کاری و تغییر وجود ندارد.

روش حمله: کرم‌واره

تأثیر حمله: بدون تأثیر

۶-۲۹- کرم‌واره PLC-based

سال حمله: ۲۰۱۶

هدف حمله: محصولات شرکت زیمنس

منطقهٔ جغرافیایی مورد حمله: کل دنیا

در آگوست ۲۰۱۶ در کنفرانس Black Hat 2016، یک کرم‌واره مبتنی بر PLC توسط پژوهش‌گران گروه امنیتی OpenSource Security ارائه شد. این کرم‌واره تنها به قصد این‌که یک برنامه PLC ای باشد که قادر به شناسایی کنترل‌کننده‌های منطقی قابل‌برنامه‌ریزی (PLC) در شبکه بوده و از یک PLC به دیگری پخش شود، نوشته شد تا به‌عنوان اثبات ادعای امکان وجود این کرم‌واره‌ها باشد. همچنین این کد مخرب قادر به کنترل و دست‌کاری ورودی و خروجی PLC بوده، می‌تواند باعث ممانعت از سرویس PLC شده، به سرورهای فرماندهی متصل شده و آن‌ها را کنترل کند یا به‌عنوان یک پروکسی برای انتشار حمله، از آن استفاده شود [۵۶].

جالب‌ترین بخش این کد مخرب با هدف اثبات مفهوم[1] (PoC)، روش‌هایی است که برای آلوده‌کردن یک PLC مورد استفاده قرار گرفت. PoC برای کنترل‌کننده‌های Siemens S7-1200 نوشته شد که دارای ویژگی حفاظت دسترسی هم هستند. این ویژگی، درصورت فعال‌بودن، اجازه می‌دهد تا رمز عبور موردنیاز برای دسترسی به PLC با استفاده از پروتکل S7CommPlus تنظیم شود. بنابراین PLC را از هر عملیات غیرمجاز خواندن یا اصلاح غیرمجاز کد PLC ، مصون می‌دارد. اما به‌طور پیش‌فرض، ویژگی حفاظت از دسترسی غیرفعال است. اگر این ویژگی فعال باشد، تنها راه ممکن برای یک کرم در راستای آلوده‌کردن PLC این است که حملهٔ همه‌جانبه‌ای بر رمز عبور انجام دهد یا رمز عبور را شنود کرده یا به‌نحو دیگری برباید [۵۶].

درس مهمی که این کرم‌واره بر آن تأکید داشت، این بود که دستگاه‌های PLC آسیب‌پذیرتر هستند (به‌خصوص نسبت به حملات ممانعت از سرویس)؛ زیرا ازآن‌جایی‌که انتظار

[1] Proof of Concept

نمی‌رود هیچ‌کس به‌جز سامانه‌های اسکادا با آن‌ها ارتباط برقرار کند، بنابراین در زمینهٔ حفاظت از دسترسی‌های غیرمجاز، ورودی‌های بد و یا دست‌کاری های مخرب هیچ راه‌کاری اندیشیده نشده است [۵۶].

روش حمله: کرم‌واره، ممانعت از سرویس

تأثیر حمله: اختلال، تخریب، خراب‌کاری

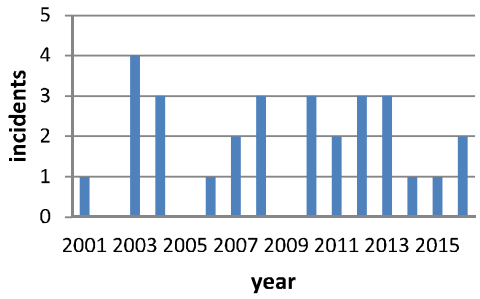
۶-۳۰- جمع‌بندی و تحلیل رخدادهای امنیتی

جهت انجام تحلیل رخدادهای امنیتی، خلاصه‌ای از حملات بررسی‌شده در این مقاله، در جدول (۲) آمده است. نمایه‌سازی بر اساس پارامترهای مهم حمله، می تواند دید روشن‌تری از مهم‌ترین حوادث امنیتی مطرح در سامانه‌های اسکادا فراهم کرده و در تبیین راه‌بردهای مناسب جهت پیش‌گیری و مقابله با حملات امنیتی، مفید واقع شود. همان‌طورکه درقبل اشاره شد، با استفاده از ویژگی‌های حمله و اطلاعاتی در مورد روش عملیات، می‌توان در مورد مهاجم و انگیزهٔ حملهٔ بیشتر نتیجه‌گیری کرد.

کاجرلند نشان داد که تجزیه و تحلیل داده‌های این نمایه‌سازی، می‌تواند روشن‌گر روابط کمّی بین متغیرها را از طریق ضریب بیگانگی یا سایر معیارهای همبستگی نشان دهد. همان‌طورکه درقبل بیان شد، در این مقاله به جای بررسی پروفایل‌های ساده‌تر و تکراری حملات در پایگاه داده ISID، تنها به بررسی حملات شاخصی که از نظر تئوری حمله دارای ارزش ویژه بوده‌اند و در منابع پژوهشی به آن‌ها پرداخته شده، بسنده شده است؛ لذا با توجه به محدودبودن داده‌های این پژوهش، روش‌های همبستگی و... قابل اعمال نبوده و به بررسی آماری ساده پرداخته خواهد شد.

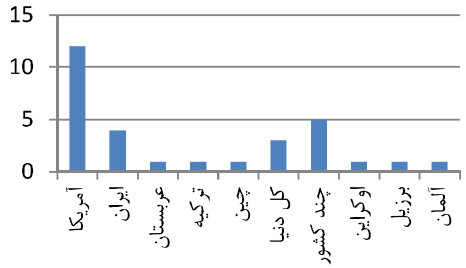
شکل (۳)، فراوانی رخدادهای وقایع امنیتی مهم بررسی‌شده را نشان می‌دهد. گفتنی است، ازآن‌جایی‌که این مقاله محدود به بررسی "تمامی وقایع بسیار مهم" امنیتی است که در مقالات دانشگاهی، مورد تحلیل قرارگرفته و از سایر وقایعی که به‌دلیل تکراری‌بودن یا نداشتن ایدهٔ نو در حمله، در مقالات مورد بررسی قرر نگرفته‌اند، چشم‌پوشی شده است؛ لذا شکل (۳)، نشان‌دهندهٔ افزایش یا کاهش تعداد وقایع امنیتی نخواهد بود. لازم به ذکر است که با توجه به گزارش‌های سرویس امنیتی IBM، تعداد حملات سایبری ICS در سال ۲۰۱۶ در مقایسه با سال ۲۰۱۵، ۱۱۰ درصد افزایش یافته است[۵۷]. هم‌چنین براساس اطلاعات ICS CERT ایالات متحده در سال ۲۰۱۵، ۴۲۷ مورد گزارش آسیب‌پذیری صورت گرفته است که در مقایسه با ۲۴۵ گزارش آسیب‌پذیری دریافت‌شده در سال ۲۰۱۴ رشد قابل ملاحظه‌ای داشته است [۵۶].

طبق اطلاعات ICS CERT ایالات متحده، حدود ۲۵ درصد از این حملات، ناشی از اعتبارسنجی نامناسب ورودی است و ۲۷ درصد به‌دلیل کنترل دسترسی‌های نامناسب. دسته‌های مهم دیگر حملات مربوط به پیکربندی نادرست و خطاهای عملیاتی می‌شوند که متأسفانه اغلب توسط فروشندگان دستگاه‌های اسکادا انکار می‌شوند.



(شکل-۳): تعداد رخداد حملات بررسی‌شده اسکادا بعد از سال ۲۰۰۰

آسیب‌پذیری‌هایی مانند نام‌کاربری و گذرواژه پیش‌فرض، تنظیمات امنیتی پیش‌فرض (که اغلب به‌صورت غیرفعال هستند)، API های پنهان یا کارکردهای مستندسازی‌نشده، بسیار خطرناک هستند؛ زیرا دسترسی گسترده‌ای به یک سامانهٔ کنترلی فراهم می‌کنند؛ اما نیاز به مهارت‌های فنّی بالا نیز ندارند [۵۶].

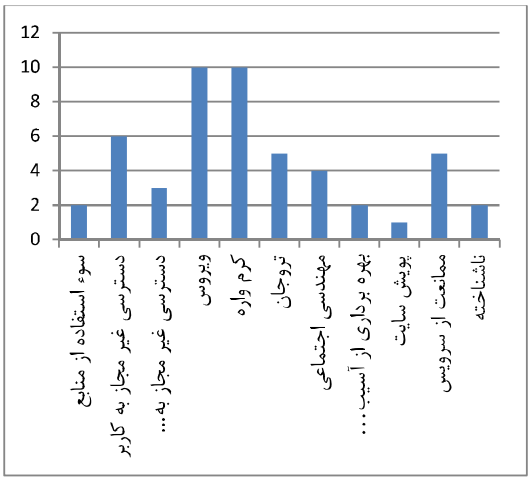


(شکل-۴): نمودار فراوانی حملات بررسی شده بر اساس کشور مورد حمله

سؤال بعدی این است که هدف از این حملات شاخص و طراحی‌شده، حمله به زیرساخت‌های حیاتی چه کشورهایی است؟ به این منظور فراوانی کشورهای مورد حمله، در شکل

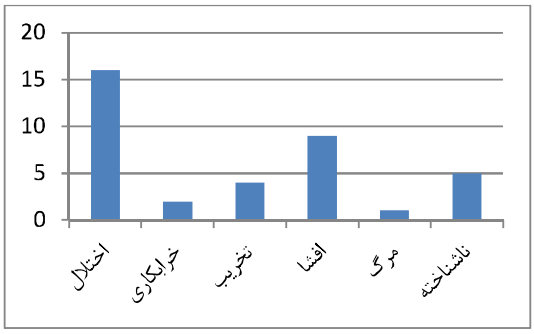
(۴) نمایش داده شده است. همان‌طورکه در این شکل دیده می‌شود، آمریکا نخستین هدف مهاجمان سامانه‌های کنترل صنعتی بوده است. به‌طور اخص، کشور دومی که شاهد بیشترین حملات بوده، ایران است. این نمودار، اهمیت توجه به امنیت زیرساخت‌های حیاتی کشورمان را نشان می‌دهد.

همان‌طور که در شکل (۵) مشاهده می‌شود، کدهای مخرب شایع‌ترین روش حمله به سامانه‌های کنترل صنعتی در سال‌های بعد از سال ۲۰۰۰ بوده است (به‌ترتیب، حملات ویروس ۱۰ مورد، کرم واره ۱۰ مورد و تروجان ۵ مورد و در مجموع ۲۵ مورد)، سوءاستفاده از دسترسی کاربر و دسترسی root در جایگاه بعدی قرار می‌گیرد (به‌ترتیب ۶ و ۳ مورد و درمجموع ۹ مورد). به‌عنوان شایع‌ترین روش حمله در درجهٔ سوم و چهارم، می‌توان به روش‌های ممانعت از سرویس مهندسی اجتماعی، با تکرار به‌ترتیب ۵ و ۴ مورد اشاره کرد. درنهایت، سوءاستفاده از منابع، بهره‌برداری از آسیب‌پذیری وب، پویش سایت و حملات ناشناخته نیز به‌ترتیب تکرار ۲، ۲، ۱، ۲ را داشته‌اند.



(شکل-۵): تعداد رخداد حملات بررسی‌شده اسکادا بعد از سال ۲۰۰۰ برحسب روش حمله

در شکل (۶) به بررسی تأثیر این حملات پرداخته‌ایم. همان‌طورکه در شکل مشاهده می‌شود، بیشتر حملات مربوط به ایجاد اختلال در عملیات بوده است. در ۹ مورد داده‌های حیاتی افشا شده‌اند، در چهار مورد داده‌ها تخریب شده‌اند، دو مورد مربوط به خراب‌کاری و تغییر دسترسی‌ها بوده، یک مورد پیامد انسانی داشته و در مورد پنج رخداد دیگر اطلاعاتی در دست نیست.



(شکل-۶): نمودار فراوانی حملات بررسی شده اسکادا بعد از سال ۲۰۰۰ برحسب اثر حمله

با توجه به کامل‌نبودن مجموعه دادهٔ حملات، بایست در تفسیر ارقام بالا دقت شود. حوادث پوشش‌داده‌شده، تنها برخی از حملات قابل مشاهده و مستندشده تاکنون بوده‌اند که ملاک جمع‌آوری آنها میزان اهمیت رخداد و نوبودن روش‌های به‌کار گرفته‌شده در آن حمله بوده است.

۷- پیشنهاد کارهای آینده

شناخت ماهیت حملات اسکادا و نحوهٔ تکامل آن‌ها در گذر زمان، می‌تواند به توسعه روش‌های مقابله با حملات کمک کند؛ اما کامل‌کردن فهرست حملات رخ‌داده در سامانه‌های کنترل صنعتی، در قالب یک مقاله نخواهد گنجید. برای مثال پایگاه داده RISI شامل بیش از ۱۲۰ مورد از چنین حوادثی، تنها در سال ۲۰۰۵ بوده است [۵۸]. همچنین به‌دلایل سیاسی، جزئیات زیادی در مورد رویدادهای بزرگ امنیتی رخ داده در سامانه‌های کنترل صنعتی منتشر نشده است.

بررسی ما نشان داد که وجود پایگاه داده‌ای جامع از حوادث سامانه‌های کنترل صنعتی که با استفاده از یک اصطلاحات استاندارد و داده‌های قابل اندازه‌گیری برای تعیین شدت فراهم شده باشد، بسیار مورد نیاز است و در حال حاضر نبود چنین پایگاه داده‌ای تحلیل حوادث را بسیار دشوار کرده است. توصیه می‌شود که این پایگاه داده، تا جای ممکن شامل ارجاعات به مقالات پژوهشی‌ای که تفسیر یک حادثه را ارائه می‌دهند، نیز باشد.

(جدول-۲): خلاصه حملات بررسی‌شده به سامانه‌های اسکادا از سال ۲۰۰۰ به بعد

ردیف	سال	نام حمله	هدف حمله	کشور مورد حمله	روش حمله	تأثیر حمله
۱	۲۰۰۱	حمله به سامانهٔ اپراتور کالیفرنیا	شبکه‌های اتوماسیون صنعتی PCS	آمریکا	دسترسی غیرمجاز به root	ناشناخته
۲	۲۰۰۳	حمله به شبکهٔ تأسیسات هسته‌ای Davis Besse	تأسیسات هسته‌ای	آمریکا	کرم‌واره، ممانعت از سرویس	اختلال
۳	۲۰۰۳	حمله ویروس Sobig به شرکت CSX	سامانه‌های قطار	آمریکا	ویروس	اختلال
۴	۲۰۰۳	حملهٔ کرم‌واره slammer به تأسیسات برق	تأسیسات برق	آمریکا	کرم‌واره، ممانعت از سرویس، دسترسی غیرمجاز به کاربر	اختلال
۵	۲۰۰۳	حملهٔ گستردهٔ کرم‌وارهٔ Slammer	بانک‌ها، تأسیسات هسته‌ای، فرودگاه‌ها، اورژانس و...	کل دنیا	کرم‌واره، ممانعت از سرویس	اختلال
۶	۲۰۰۴	حمله به سامانه‌های کنترل ترافیک هوایی	سامانه کنترل ترافیک هوایی	آمریکا	ناشناخته	اختلال
۷	۲۰۰۴	باران تیتان	ناسا و سامانه امنیت نظامی	آمریکا	ناشناخته	اختلال، افشا
۸	۲۰۰۴	حملهٔ کرم‌وارهٔ sasser	مراکز مهم دولتی، نظامی، خدماتی و درمانی	کل دنیا	کرم‌واره	اختلال
۹	۲۰۰۶	حمله به سامانهٔ تصفیهٔ آب	سامانه تصفیه آب شهر	آمریکا	کد مخرب، بهره‌برداری از آسیب‌پذیری وب	مرگ
۱۰	۲۰۰۷	حملهٔ Aurora	زیرساخت برق در رسانه‌های عمومی	آمریکا	کد مخرب، سوءاستفاده از دسترسی غیرمجاز	اختلال
۱۱	۲۰۰۷	حمله به TCAA	شرکت برق	آمریکا	سوءاستفاده از منابع	ناشناخته
۱۲	۲۰۰۸	حملهٔ کرم‌وارهٔ AGENT.BTZ	ماشین‌های نظامی ارتش	امریکا	کرم‌واره	ناشناخته
۱۳	۲۰۰۸	حمله به سامانهٔ کنترل خط لوله	سامانه کنترل خط لوله	ترکیه	سوءاستفاده از دسترسی غیرمجاز	اختلال
۱۴	۲۰۰۸	حملهٔ کرم‌وارهٔ AHACK	اتوماسیون صنعت استیل	برزیل	کرم‌واره، ممانعت از سرویس، سوءاستفاده از دسترسی کاربر	اختلال
۱۵	۲۰۱۰	آزمون نفوذپذیری اسکادا در صنعت برق	صنعت برق	آمریکا	پویش همه‌جانبه سایت	ناشناخته
۱۶	۲۰۱۰	حمله به صنعت استیل	صنعت استیل	آمریکا	مهندسی اجتماعی، تروجان، سوءاستفاده از دسترسی کاربر	افشا، اختلال
۱۷	۲۰۱۰	حملهٔ کرم Stuxnet	نرم‌افزارها و تجهیزات صنعتی تأسیسات هسته‌ای	ایران	کرم‌واره، دسترسی غیرمجاز به root، تروجان	اختلال، خراب‌کاری
۱۸	۲۰۱۱	حملهٔ اژدهای شب	شرکت‌های نفتی، پتروشیمی و انرژی	چین	مهندسی اجتماعی، تروجان، سوءاستفاده از دسترسی root	افشا
۱۹	۲۰۱۱	حملهٔ ویروس DUQU	سامانه‌های کنترل صنعتی	چندین کشور از جمله ایران	تروجان	افشا
۲۰	۲۰۱۲	حملهٔ بدافزار Shamoon	شرکت‌های نفت و گاز و انرژی	عربستان صعودی	سوءاستفاده از منابع، کد مخرب	اختلال
۲۱	۲۰۱۲	حملهٔ Flame	سامانه‌های تأسیسات صنعتی	ایران	کرم‌واره	افشا، تخریب
۲۲	۲۰۱۲	حملهٔ Wiper	چندین شرکت مهم دولتی و غیردولتی	ایران	کد مخرب	تخریب
۲۳	۲۰۱۳	حملهٔ بدافزار Mask The	چندین شرکت مهم دولتی و غیردولتی	چندین کشور	کد مخرب	اختلال، افشا
۲۴	۲۰۱۳	حملهٔ بدافزار MiniDuke	سازمان‌های دولتی و نهادهای مالی کشورها	کشورهای اروپایی	کد مخرب	افشا
۲۵	۲۰۱۳	حملهٔ بدافزار October Red	مراکز دیپلماتیک، دولتی و علمی در کشورهای مختلف	چندین کشور	مهندسی اجتماعی، کد مخرب، سوءاستفاده از دسترسی کاربر	افشا

۲۶	۲۰۱۴	حملهٔ HAVEX	سازمان‌های بخش انرژی	شرکت‌های اروپایی	کد مخرب، سوءاستفاده از آسیب‌پذیری وب، تروجان	افشا
۲۷	۲۰۱۵	حملهٔ بدافزار BlackEnergy	خطوط انتقال برق	اوکراین	مهندسی اجتماعی، کد مخرب	اختلال، تخریب
۲۸	۲۰۱۶	حملهٔ کرم‌وارهٔ Kido	نیروگاه هسته‌ای	آلمان	کرم‌واره	بدون تأثیر
۲۹	۲۰۱۶	کرم‌وارهٔ PLC-based	محصولات شرکت زیمنس	کل دنیا	کرم‌واره، ممانعت از سرویس	اختلال، تخریب، خراب‌کاری

فهرست اختصارات

CS سامانهٔ ارتباطی[1]

DoS حمله ممانعت از سرویس[2]

ERP سامانهٔ برنامه‌ریزی منابع سازمانی[3]

ICT فناوری اطلاعات و ارتباطات[4]

RTU واحد پایانهٔ از راه دور[5]

DMS سامانهٔ مدیریت توزیع[6]

EMS سامانهٔ مدیریت انرژی[7]

ICS سامانه‌های اطلاعاتی و ارتباطی[8]

IED دستگاه الکترونیکی هوشمند[9]

۸- مراجع

[1] Drias, Z., Serhrouchni, A. and Vogel, O., 2015, August. Analysis of cyber security for industrial control systems. In Cyber Security of Smart Cities, Industrial Control System and Communications (SSIC), 2015 International Conference on (pp. 1-8). IEEE.

[2] K. Stouffer, J. Falco, and K. Scarfone, "Guide to industrial control systems (ICS) security," NIST Special Publication 800-82, 2011.

[3] E. Hayden, M. Assante, and T. Conway, "An abbreviated history of automation & industrial controls systems and cybersecurity," 2014.

[4] Miller B, Rowe D. A survey SCADA of and critical infrastructure incidents. InProceedings of the 1st Annual conference on Research in information technology 2012 Oct 11 (pp. 51-56). ACM.

[5] Weiss J. Assuring industrial control system (ICS) cyber security. Center for Strategic and International Studies. 2008..

[6] R. Anderson et al., "Measuring the cost of cybercrime," in The Economics of Information Security and Privacy. Berlin, Germany: Springer-Verlag, 2013, pp. 265–300.

[7] Flowers A, Zeadally S. US policy on active cyber defense. Journal of Homeland Security and Emergency Management. 2014 Apr 1;11(2):289-308.

[8] Willis Group, "Energy market review 2014 Cyberattacks: Can the market respond?" 2014.

[9] S. McLaughlin, C. Konstantinou, X. Wang, L. Davi, A. R.Sadeghi, M. Maniatakos, and R. Karri, "The cybersecurity landscape in industrial control systems," Proceedings of the IEEE, vol. 104, no. 5, pp. 1039–1057, May 2016.

[10] Webb JW, Reis RA. Programmable logic controllers: principles and applications. Prentice Hall PTR; 2002 Mar 1.

[11] Murayama T. Distributed Control System. InAdvanced Robotics, 1991.'Robots in Unstructured Environments', 91 ICAR., Fifth International Conference on 1991 Jun 19 (pp. 1501-1504). IEEE.

[12] Igure, V.M., Laughter, S.A. and Williams, R.D., 2006. Security issues in SCADA networks. Computers & Security, 25(7), pp.498-506.

[13] Gao, J., Liu, J., Rajan, B., Nori, R., Fu, B., Xiao, Y., Liang, W. and Philip Chen, C.L., 2014. SCADA communication and security issues. Security and Communication Networks, 7(1), pp.175-194.

[14] "IEEE Standard for SCADA and automation systems," IEEE Std C37.1-2007 (revision of IEEE Std C37.1-1994). 2008; c1–133.

[15] "IEEE recommended practice for master/remote supervisory control and data acquisition (SCADA) communications," IEEE Std. 999–1992, p. 0_1, 1993

[16] Tib N. 04-1, Technical Information Bulletin 04–1,National Communications System, SCADA Systems.October, 2004

[1] Communication System
[2] Denial-Of-Service
[3] Enterprise Resource Planning
[4] Information And Communication Technology
[5] Remote Terminal Unit
[6] Distribution Management System
[7] Energy Management System
[8] Information And Communication Systems
[9] Intelligent Electronic Device

[17] Benias N, Markopoulos AP. A review on the readiness level and cyber-security challenges in Industry 4.0. InDesign Automation, Computer Engineering, Computer Networks and Social Media Conference (SEEDA-CECNSM), 2017 South Eastern European 2017 Sep 23 (pp. 1-5). IEEE.

[18] Zhu B, Joseph A, Sastry S. A taxonomy of cyber attacks on SCADA systems. InInternet of things (iThings/CPSCom), 2011 international conference on and 4th international conference on cyber, physical and social computing 2011 Oct 19 (pp. 380-388). IEEE.

[19] Senate US. Control Systems Cyber Security—The Current Status of Cyber Security of Critical Infrastructures,2009.

[۲۰] احمد افشـــار، عاطفه ترمه چی، عارفه گلشـــن، آزاده آقائیان، حمیدر ضا شهریاری، مروری بر امنیت سایبری سامانه‌های کنترل صنعتی، مجله کنترل، جلد ۸، شماره ۱، بهار ۱۳۹۳، صفحه ۴۵-۳۱.

[۲۱] اف شار، ترمه چی، گل شن، آقائیان، شهریاری، سلیمانی، ارائه یک مدل مفهومی جامع برای آســـیب‌پذیری‌های ســـامانه کنترل واحدهای صـــنعتی و زیرســـاخت‌های حیاتی. فصـــل‌نامه پدافند غیرعامل; ســـال ۶، شـــماره ۴ (۱۳۹۴): زمستان ۹۴

[22] Zhou, X., Xu, Z., Wang, L. and Chen, K., 2017, April. What should we do? A structured review of SCADA system cyber security standards. In Control, Decision and Information Technologies (CoDIT), 2017 4th International Conference on (pp. 0605-0614). IEEE.

[23] Byres E, Leversage D, Kube N. Security incidents and trends in SCADA and process industries. Ind Ethernet B [Internet]. 2007;39:12–20

[24] Rosa, L., Cruz, T., Simões, P., Monteiro, E. and Lev, L., Attacking SCADA systems: A practical perspective. In Integrated Network and Service Management (IM), 2017 IFIP/IEEE Symposium on (pp. 741-746). IEEE.

[25] R. Langner, "To kill a centrifuge a technical analysis of what stuxnet's creators tried to achieve," Technical report ,The Langner Group, November 2003.

[26] Kjaerland, M. A taxonomy and comparison of computer security incidents from the commercial and government sectors. Computers & Security. 25, 7 (Oct. 2006), 522–538.

[27] Stamp J, Dillinger J, Young W, DePoy J. Common vulnerabilities in critical infrastructure control systems. SAND2003-1772C. Sandia National Laboratories. 2003 May 22.

[28] Remenyi, E. by D.D. et al. Proceedings of the 5th European Conference on Information Warfare and Security: National Defense College, Helsinki, Finland, 1 - 2 June 2006.

[29] Nicholson A, Webber S, Dyer S, Patel T, Janicke H. SCADA security in the light of Cyber-Warfare. Computers & Security. 2012 Jun 1;31(4):418-36.

[30] Kuvshinkova S. SQL Slammer worm lessons learned for consideration by the electricity sector. North American Electric Reliability Council. 2003 Jun;1(2):5.

[31] Moore D, Paxson V, Savage S, Shannon C, Staniford S, Weaver N. The spread of the sapphire/slammer worm, 2003. URL: http://www.caida.org/outreach/papers/2003/sapphire/sapphire. html. 1999.

[32] Serazzi G, Zanero S. Computer virus propagation models. In Performance Tools and Applications to Networked Systems 2004 (pp. 26-50). Springer, Berlin, Heidelberg.

[33] ISS Security Brief: Microsoft SQL Slammer Worm Propagation". ISSForum. 25 January 2003. Retrieved 2008-II-29.

[34] http://articles.latimes.com/2004/sep/15/local/me-faa15.

[35] Thornburgh, N. Inside the Chinese Hack Attack. Times, 2005, August; 25.

[36] Acohido B, Swartz J. Unprotected PCs can be hijacked in minutes. USA Today. 2004 Nov 30;29.

[37] Meserve J. Mouse click could plunge city into darkness, experts say. CNN. com. 2007 Sep 27;27.

[38] Security Matters, "The Aurora attack."[Online]. Available:http://www.secmatters.com/casestudy 10.

[39] Messick G. Cyber War: Sabotaging the System, 2009.

[40] http://www.risidata.com/Database/country/asc.

[41] J. Pollet, Red Tiger, Electricity for free? The dirty underbelly of SCADA and smart meters, in: Proc. 2010 BlackHat Technical Conference, Las Vegas, NV, July 2010.

[42] http://free-automation.com.

[43] T. M. Chen and S. Abu-Nimeh, "Lessons from Stuxnet," Computer, vol. 44, no. 4, pp. 91–93, 2011.

[44] Kushner D. The real story of stuxnet. IEEE Spectrum. 2013 Mar 1;50(3):48-53.

[45] M. B. Line, A. Zand, G. Stringhini, and R. Kemmerer, "Targeted attacks against industrial control systems: Is the power industry prepared?" in Proc. 2nd Workshop Smart Energy Grid Security, 2014, pp. 13–22.

[46] Global Energy Cyberattacks: "Night Dragon," McAfee Foundstone Professional Services and McAfee Labs, Santa Clara, CA, February 10, 2011.

[47] Zetter K. Son of Stuxnet found in the wild on systems in Europe. Threat Level. 2011.

[48] Stouffer K, Falco J, Scarfone K. Guide to industrial control systems (ICS) security. NIST special publication. 2011 Jun;800(82):16-.

[49] Zetter K. Flame" spyware infiltrating Iranian computers. CNN. Com , 2012.

[50] Erdbrink T. Facing Cyberattack, Iranian Officials Disconnect Some Oil Terminals From Internet. The New York Times. 2012 Apr 23.

[51]https://apt.securelist.com(accessdate:03/04/2018).

[52]https://news.asis.io/content.(accessdate:03/04/2018).

[53] The "Red October" Campaign - An Advanced Cyber Espionage Network Targeting Diplomatic and Government Agencies". Kaspersky Lab. 3 Mar 2014.

[54] Walker D. Havex malware strikes industrial sector via watering hole attacks. SC Magazine. 2014 Jun.

[55] Kovacs E. BlackEnergy Malware Used in Ukraine Power Grid Attacks. SecurityWeek, www. security-week. com. 2016;4(01).

[56] David Emm, Roman Unuchek, Kirill Kruglov, "Kaspersky Security Bulletin 2016, REVIEW OF THE YEAR," Kaspersky Lab, 2016.

[57] Alvarez M, Bradley N, Cobb P, Craig S, Iffert R, Kessem L, Kravitz J, McMillen D, Moore S. IBM X-Force Threat Intelligence Index 2017 The Year of the Mega Breach. IBM Security,(March). 2017:1-30.

[58] Turk RJ. Cyber incidents involving control systems. Idaho National Laboratory (INL); 2005 Oct 1.

[59] Athina Karatzogianni, Cyber-Conflict and Global Politics, Routledge, 2008

راضیه اسکندری فارغ‌التحصیل کارشناسی ارشد رشته فناوری اطلاعات گرایش امنیت اطلاعات دانشگاه صنعتی امیرکبیر و عضو هیئت علمی دانشکده فنّی مهندسی دانشگاه شهرکرد است. زمینه‌های تحقیقاتی ایشان در زمینه شبکه‌های کامپیوتری و امنیت اطلاعات و حوزه‌های مربوطه است. در سال‌های اخیر، وی رهبری یا مشارکت در بسیاری از برنامه‌های ملّی ، استانی برای پژوهش و توسعه امنیتی را بر عهده داشته است. این پروژه‌ها دستاوردهای قابل توجهی را به‌دست آورده‌اند و بسیاری از آنها برای توسعه برنامه‌های امنیتی در مرکز ماهر مورد استفاده قرار گرفته‌اند.

الهه معتمدی فارغ‌التحصیل کارشناسی رشته مهندسی کامپیوتر در دانشگاه شهرکرد است. زمینه‌های پژوهشی مورد علاقه ایشان در زمینه سیستم‌های اسکادا است