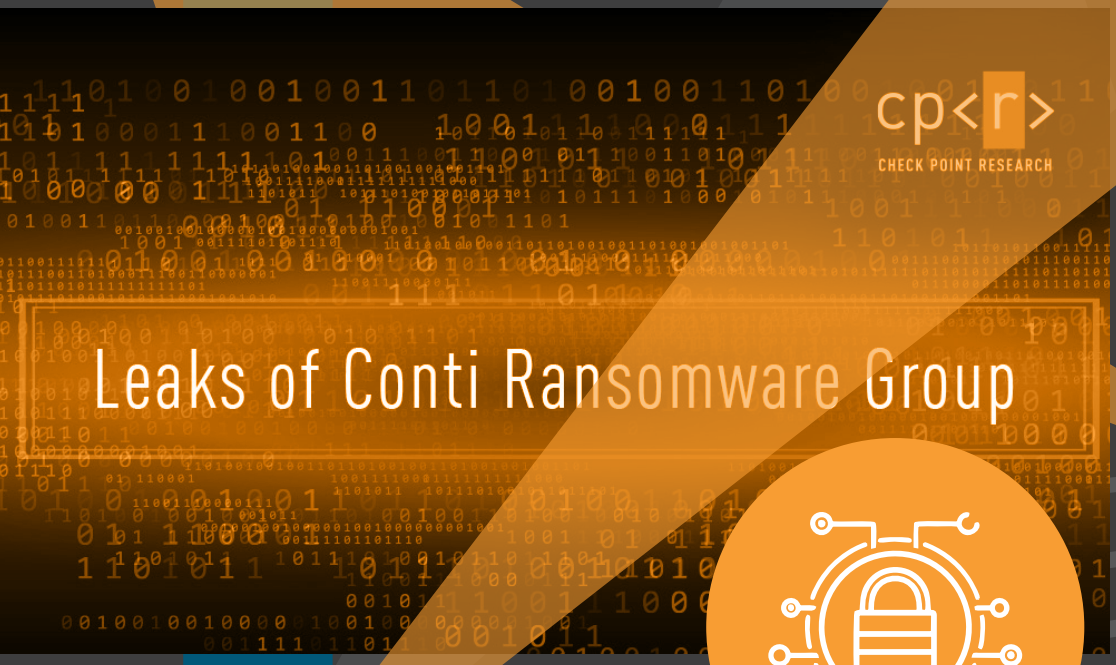
گزارش
مجمع ایرانی دفاع از حقیقت

Iranian Council For
Defending The Truth

فروردین ۱۴۰۱



امنیت سایبـــــری


بسم الله الرحمن الرحیم

فهرست

Iranian Council For
Defending The Truth

پیشگفتار

۱

پیشگفتار

مجمع ایرانی دفاع از حقیقت مادام همه تلاش خود را انجام می‌دهد که با به کارگیری شبکه‌ای از نخبگان در حوزه‌های مختلف سیاسی و شناختی گامی در جهت جلوگیری از ایجاد سوءتفاهم بردارد. در همین خصوص ما در مجمع ایرانی دفاع از حقیقت رسالت خود میدانیم تا با تهیه دیدبان‌هایی از موضوعاتی که به عنوان کارویژه برای خود انتخاب کرده‌ایم، چشم اندازی از مسیر را ارائه داده و در صورت توان پیشنهاداتی نیز برای کاهش این سوءتفاهم‌ها در آنان جای دهیم. ناگفته نماد که این دیدبان خود بخشی از راه حل کاهش سوءتفاهم است.

مجمع ایرانی دفاع از حقیقت
میز مطالعات امنیت

Iranian Council For
Defending The Truth

مقدمه

۲

مقدمه

اطلاع از اخبار و وضعیت فضای سایبر در ایالات متحده این امکان را فراهم می‌سازد تا با مسائل و مشکلات این حوزه سریع‌تر آشنا شده و هم‌چنین پیش از این که کشور ما نیز به آن مصائب و دشواری‌ها دچار گردد، راهکارهای اصلاحی را پیش‌بینی نماییم. از طرفی، با توجه به این که در اظهارات عمومی و جلسات رسمی مقامات این کشور برخی از نقاط ضعف دشمن در زمینه سایبری و فناوری‌های نوین بیان می‌گردد و با توجه به این نکته که بخش سایبری ایران توانایی آن را دارد که در تقابل با ایالات متحده از همین ضعف‌ها بهره‌برداری کند و به دشمن ضربه بزند؛ فلذا می‌توانیم از نقاط ضعف حریف استفاده نماییم و زمین بازی را به نفع خود تغییر دهیم و در موضع آفندی قرار بگیریم.

این تذکر ضروری است که با توجه به پیشگامی کشور امریکا در عرصه تکنولوژی، بررسی پیشرفت‌ها و برنامه‌ریزی‌های کلان این کشور در زمینه فناوری پیش‌بینی مقصد نهایی مسیر تکنولوژی در آینده را ممکن می‌سازد.

در بولتنی که در اختیار دارید اهم اخبار و اتفاقات کلان حوزه سایبر، تکنولوژی و فناوری‌های نوین جمع‌آوری شده است تا مخاطبین و فعالین در این زمینه بتوانند نسبت به وضعیت ایالات متحده از نگاهی جامع، کلان و به‌روز برخوردار شوند.

دیدکلی

در این شماره از دیدبان سایبری ذیل محور های ایالات متحده آمریکا، تنش روسیه و اوکراین، تهدیدات سایبری و سایبر بین الملل، خبر هایی در مورد رخداد های مهم سایبری در هفته گذشته میخوانیم.

در آمریکا یک بد افزار جدید که به سیستم های کنترل صنعتی حمله می کند شناسایی شده، همچنین تحقیقاتی توسط NSA برای شناسایی عوامل حمله به وایاست صورت گرفته است. در جریان تنش های بین روسیه و اوکراین جزییاتی در مورد حملات به شبکه برق اوکراین توسط هکر های روسی منتشر شده همچنین کلیپی از زلنسکی که با فناوری جعل عمیق ساخته و در شبکه های اجتماعی منتشر شده خبر ساز شده است. در بخش تهدیدات سایبری از خنثی شدن حملات هکری چینی ها به اهداف هندی صحبت می کنیم و نیز خبر هایی از هک موبایل برخی مقامات اروپایی با بدافزار اسراییلی. نهایتا در بخش سایبر بین الملل نگاهی به افزایش استفاده از وی پی ان در روسیه و سرمایه گذاری اینتل در اروپا و نیز أقامه ی دعوا علیه شرکت متا توسط تنظیم کننده ی آفریقایی داریم.

Iranian Council For
Defending The Truth

اخبار

۳

ایالات متحده آمریکا

بدافزار جدید سیستم کنترل صنعتی در ایالات متحده شناسایی شد

تنها چند روز پس از خبر تلاش برای استفاده از نوع جدیدی از بدافزار Industroyer، هشداری از سوی آژانس امنیت سایبری و امنیت زیرساخت ایالات متحده منتشر شد: برخی از هکر ها توانایی دسترسی کامل به سیستم کنترل صنعتی دارند.

آژانس امنیت سایبری و امنیت زیرساخت اعلام کرد که یک تهدید پیشرفته را شناسایی کرده است که سیستم‌های کنترل صنعتی را با یک ابزار بدافزار جدید به نام‌های PIPEDREAM و INCONTROLLER توسط شرکت‌های مختلف امنیت سایبری هدف قرار می‌دهد. این بدافزار می‌تواند برای وارد کردن آسیب‌های فیزیکی به فرآیندهای صنعتی، از جمله مواردی که توسط تأسیسات گاز طبیعی مایع استفاده می‌شود و مقامات معتقدند هدف بدافزار بوده است ، استفاده شود. هکرها قبلاً سیستم‌های کنترل صنعتی را برای ایجاد آسیب فیزیکی دستکاری کرده‌اند که معروف‌ترین آن از طریق بدافزار استاکس‌نت است که علیه تأسیسات هسته‌ای نطنز در ایران راه‌اندازی شده است. دولت بایدن چندین هشدار درباره احتمال حملات سایبری مخرب روسیه علیه زیرساخت های حیاتی ایالات متحده از زمان تهاجم روسیه به اوکراین صادر کرده است.

NSA تحقیقات سایبری در مورد هک Viasat را اعلام کرد

آژانس امنیت ملی (NSA) اعلام کرد که در حال بررسی یک حمله سایبری به ارائه‌دهنده اینترنت ماهواره‌ای Viasat است که باعث قطع ارتباط در سراسر اوکراین در ۲۴ فوریه، همان روزی که نیروهای روسیه به این کشور حمله کردند، است. این قطعی در سراسر شبکه‌های Viasat در اروپا ادامه دارد، و بسیاری از مناطق هنوز اتصال کم یا بدون اتصال هستند. اگر قطعی Viasat به عنوان یک عملیات سایبری روسیه تایید شود، یکی از موثرترین استفاده از حملات سایبری در جنگ تا کنون خواهد بود. مقامات اوکراینی گفته‌اند که این قطعی باعث "خسارت بزرگی در ارتباطات در همان ابتدای جنگ" شده است، اگرچه آنها در دو هفته پس از تهاجم عملیات بازیابی را انجام دادند.

تنش روسیه و اوکراین

روسیه شبکه برق اوکراین را هدف قرار داده است

تیم واکنش اضطراری کامپیوتری اوکراین (CERT-UA) و شرکت امنیت سایبری ESET فاش کردند که هکرهای Sandworm مرتبط با روسیه، جایگاه های برق فشار قوی در اوکراین را با بدافزار هدف قرار داده‌اند. مهاجمان پست‌های برق را با نوع جدیدی از بدافزار Industroyer به نام Industroyer هدف قرار دادند که با سیستم‌های کنترل صنعتی که جریان نیرو را مدیریت می‌کنند تعامل دارد. این حمله یادآور کمپین های سال ۲۰۱۵ و ۲۰۱۶ است که توسط Sandworm انجام شده است که در آن مهاجمان از بدافزار Industroyer برای ایجاد خاموشی در کیف استفاده کردند. در حالی که مقامات اوکراینی ادعا کردند در این مورد آسیبی به شبکه برق وارد نشده است، برخی گزارش‌ها از آسیب در پست‌های برق حکایت می کنند. شواهدی وجود دارد مبنی بر اینکه هکرها ممکن است در اوایل فوریه به سیستم های هدف نفوذ کرده باشند و برای حملات برنامه ریزی شده در آوریل در کمین نشسته باشند. هکرها همچنین چندین گونه از بدافزار ، از جمله CaddyWiper، را در سیستم های دیگر مستقر کردند.

هکرها از کد باج افزار Conti برای حمله به اهداف در روسیه استفاده می کنند

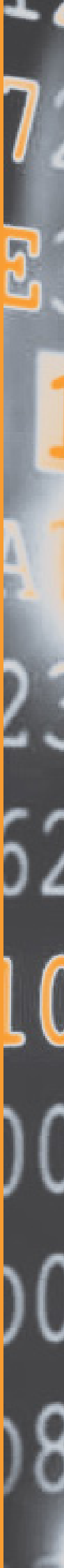
یک گروه هکر، معروف به NB۶۵، شروع به استفاده از کد ایجاد شده توسط گروه باج افزار Conti برای حملات باج افزار علیه شرکت های روسی کرد. کد Conti در ماه مارس توسط یک محقق امنیتی که از موضع این گروه در قبال جنگ در اوکراین ناراضی بود فاش شد. NB۶۵ چندین هدف برجسته در روسیه، از جمله ایستگاه های تلویزیونی و رادیویی دولتی را مورد حمله قرار داده است، اما تغییر به استفاده از باج افزار Conti یک اقدام جدید است. NB۶۵ می گوید انگیزه عملیات های آنها حمله روسیه به اوکراین است و ادعا می کند که هر باج پرداختی به سازمان های کمک در اوکراین اهدا خواهد شد. در حالی که روسیه یک هدف سنتی برای باج افزارها نبوده است، جنگ در اوکراین ظاهرا محاسبات برخی گروه ها را تغییر داده است.

دیپ فیک تسلیم شدن زلنسکی در شبکه‌های اجتماعی دست به دست می‌شود

دیپ‌فیک ولودیمیر زلنسکی، رئیس‌جمهور اوکراین این هفته در یک وب‌سایت شبکه خبری اوکراینی که هک‌شده بارگذاری شد و از طریق رسانه‌های اجتماعی توزیع شد. این ویدئو نسخه جعلی زلنسکی را نشان می دهد که از سربازان اوکراینی می خواهد تسلیم شوند و سلاح های خود را زمین بگذارند. زلنسکی تکذیبیه ی این ویدئو را منتشر کرد و فیس‌بوک و اینستاگرام کپی‌هایی را که در فضای مجازی پخش می‌شد را حذف کردند. هک دیپ‌فیک و مرتبط با آن نشان‌دهنده خطر فزاینده تلاش‌های انتشار اطلاعات نادرست برای تأثیرگذاری بر مردم در طول درگیری و تنش است.


Data Breach
Cyber Attack
System Sa

تهدیدات سایبری



هند مدعی است که حمله سایبری چین را خنثی کرده است

تحلیلگران امنیت سایبری یک گروه چینی را که اجزای شبکه برق هند را هدف قرار داده است شناسایی کردند. یک عامل احتمالاً تحت حمایت دولت از بدافزار ShadowPad برای دسترسی به شبکه‌های مراکز ارسال بار دولتی هند که مسئول عملیات کنترل شبکه و ارسال برق هستند، استفاده کرده است. مراکز مورد هدف بیشتر در شمال هند و در نزدیکی مرز مورد مناقشه لداخ قرار داشتند.

عامل چینی RedEcho در گذشته سازمان‌های بخش برق هند را هدف قرار داده است، اما مشخص نیست که آیا این گروه پشت کمپین اخیر است یا خیر. یک روز پس از انتشار جزئیات این کمپین، هند مدعی شد که حداقل دو حمله را خنثی کرده است. ژائو لیجیان، سخنگوی وزارت امور خارجه چین، اتهامات مربوط به دست داشتن دولت چین در پشت این حملات را رد کرد.

مقامات اتحادیه اروپا با نرم افزارهای جاسوسی اسرائیل هدف قرار گرفتند

ظاهراً از ابزارهای گروه NSO برای هدف قرار دادن حداقل پنج مقام و کارمند ارشد در کمیسیون اروپا بین فوریه تا سپتامبر ۲۰۲۱ استفاده شده است. هنگامی که اپل در ماه نوامبر به کاربران آیفون هشدار داد که ممکن است قربانی یک کمپین هک توسط دولت شوند، به مقامات هشدار داده شد. دستگاه‌های این مقامات به بدافزار ForcedEntry آلوده شده‌اند که در گذشته با چندین فروشنده نرم‌افزار جاسوسی اسرائیلی مانند NSO Group و QuaDream مرتبط بوده است، اگرچه NSO Group هرگونه دخالت در این حادثه را رد کرده است. هنوز مشخص نیست چه کسی پشت این کمپین بوده است. این افشاگری یک هفته قبل از راه اندازی کمیته تحقیق در ۱۹ آوریل توسط پارلمان اروپا که وظیفه بررسی استفاده از نرم افزارهای نظارتی در کشورهای عضو را دارد، منتشر شد.


NSO GROUP

سایبر بین‌الملل

استفاده از VPN روسی در دو هفته گذشته افزایش یافته است

بارگیری‌های شبکه خصوصی مجازی (VPN) که به کاربران اجازه می‌دهد کنترل‌های اینترنت را دور بزنند، طی دو هفته گذشته نزدیک به دو هزار درصد در فدراسیون روسیه افزایش یافته است. این افزایش زمانی اتفاق می‌افتد که روسیه به طور فزاینده‌ای کنترل‌های شدید اینترنت را اعمال کرده و رسانه‌های اجتماعی مانند فیس‌بوک، توییتر و اینستاگرام را مسدود کرده است. مقامات روسی در گذشته تلاش کرده اند خدمات محبوب VPN را ممنوع کنند، اما نتوانسته اند دسترسی را به طور کامل قطع کنند. با عمیق تر شدن انزوای اینترنت در روسیه، بسیاری نگران هستند که شهروندان روسی دسترسی به اطلاعات قابل اعتماد را از دست بدهند. با این حال، به نظر می رسد که VPN ها ممکن است یکی از مسیرهای جریان اطلاعات به داخل و خارج از کشور باشند.

اینتل ۳۶ میلیارد دلار در کارخانه‌های تولید تراشه در اروپا سرمایه‌گذاری می‌کند

شرکت سازنده نیمه هادی ایالات متحده اینتل از سرمایه گذاری ۳۶ میلیارد دلاری در ساخت نیمه هادی ها و تأسیسات تحقیق و توسعه در سراسر اروپا خبر داد. این اعلام در حالی منتشر می شود که اینتل تولید مسیر آینده خود را به سمت ایالات متحده و اروپا تغییر می دهد.

سرمایه گذاری جدید اینتل در چندین کارخانه از جمله دو کارخانه جدید نیمه هادی در آلمان و یک سایت تحقیق و توسعه جدید در فرانسه خواهد بود. تحولات جدید در اروپا در نهایت می تواند منجر به هزینه بیش از ۹۰ میلیارد دلاری اینتل برای افزایش تولید نیمه هادی در این قاره شود.

تنظیم کننده آفریقای جنوبی متا را به دادگاه کشاند

کمیسیون رقابت آفریقای جنوبی (CC)، قدرتمندترین تنظیم کننده ضد انحصار این کشور، اعلام کرد که متا پلتفرم، شرکت مادر فیس بوک و واتس اپ را به دلیل سوء استفاده از موقعیت خود به عنوان رهبر بازار به دادگاه ارجاع می دهد. این شکایت حول رفتار متا با GovChat است، GovChat یک سرویس پیام رسانی است که توسط دولت برای برقراری ارتباط در مورد مسائل مدنی استفاده می شود. CC ادعا می کند که فیس بوک به طور ناعادلانه دسترسی GovChat به داده ها را محدود کرده است، در حالی که متا می گوید که این محدودیت ها پس از نقض GovChat از شرایط و ضوابط خدمات متا اعمال شده است. تلاش‌های ضد انحصار آفریقای جنوبی جدیدترین موارد در ردیف شکایت‌های ضدانحصار علیه متا و سایر شرکت‌های فناوری در ایالات متحده و خارج از کشور است.

ICDT.IR