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

شماره حاضر از دیدبان سایبری در چهار محور شامل ایالات متحده آمریکا، تنش بین روسیه و اوکراین، سایبر بین الملل و حملات سایبری تهیه و منتشر شده است.

در روزهای گذشته در آمریکا گزارشی توسط اف بی آی منتشر شد، مبنی بر افزایش قابل توجه جرایم و حملات سایبری در این کشور. مقامات آمریکایی و اروپایی توافقات سایبری جدیدی با هم داشتند و آمریکا به دنبال محدود کردن تعدادی از گروه های هکری مخالف خود بوده است. در تنش بین روسیه و اوکراین زیرساخت های مهمی از اوکراین مورد حمله سایبری روسیه قرار گرفته است. در سوی دیگر جبهه کمک های ناتو کمک زیادی به اوکراین در بخش جنگ فناوری ها در میدان نبرد کرده است. در سایبر بین الملل شاهد بررسی قوانین جدید در اروپا و نیز بررسی شرایط آینده هوآوی در بازار تکنولوژی هستیم و در بخش حملات سایبری جدید ترین حمله علیه رییس موساد را مورد بررسی قرار دادیم.

Iranian Council For
Defending The Truth

اخبار

۳

ایالات متحده آمریکا

گزارش FBI افزایش جرایم سایبری را نشان می دهد

در گزارش سالانه جرایم اینترنتی، FBI فاش کرد که بیش از ۸۰۰۰۰۰ شکایت از جرایم سایبری در سال ۲۰۲۱ دریافت کرده است. بر اساس این گزارش، تخمین زده می شود که خسارات احتمالی ناشی از جرایم سایبری بالغ بر ۶.۹ میلیارد دلار باشد که نشان دهنده افزایش ۶۴ درصدی نسبت به سال ۲۰۲۰ است. این گزارش همچنین به برخی از موارد اشاره کرد. پرهزینه ترین کلاهبرداری ها، که شامل به خطر افتادن ایمیل های تجاری، طرح های سرمایه گذاری، طرح های عاشقانه، نقض اطلاعات شخصی و کلاهبرداری در املاک و مستغلات می شود. اگرچه باجافزار پس از هک Colonial Pipe-line در سال گذشته توجه ملی را به خود جلب کرد، اما تنها ۳۷۲۹ شکایت و ضرر ۴۹ میلیون دلاری را به خود اختصاص داد. این تعداد کم ممکن است تا حدی به دلیل گزارش ناکافی باشد، که ممکن است مربوط به گذشته باشد زیرا یک قانون جدید فدرال موظف می‌کند که کسب‌وکارها نقض‌های دیجیتال را به دولت افشا کنند.

گزارش چینی مدعی است که ایالات متحده رسانه های اجتماعی و ایمیل کاربران را هک می کند

Qihoo ۳۶۰، یک شرکت امنیت سایبری چینی، اوایل این هفته اعلام کرد که مجموعه‌ای از ابزارهایی را شناسایی کرده است که گفته می‌شود توسط آژانس امنیت ملی ایالات متحده (NSA) برای هدف قرار دادن ایمیل کاربران چینی و اطلاعات رسانه‌های اجتماعی استفاده می‌شود. ظاهراً این ابزار می تواند برای نظارت بر بیشتر ارتباطات و فعال کردن میکروفون یا دوربین رایانه استفاده شود. برخی از شرکت‌ها و آژانس‌های امنیت سایبری چین اخیراً ابزارهای جاسوسی NSA را به صورت عمومی منتشر کرده‌اند. مرکز ملی واکنش اضطراری ویروس های کامپیوتری گزارشی منتشر کرد مبنی بر اینکه یک تروجان لینوکس مورد استفاده NSA را کشف کرده است که NOPEN نام دارد. با این حال، NOPEN تقریبا شش سال قبل به عنوان بخشی از افشاگری Shadow Brokers فاش شده بود.

عملیات Bridgestone در ایالات متحده با حمله اخیر باج افزار بسته شد

رویترز توضیح می‌دهد که چگونه حمله اخیر باج‌افزار علیه شرکت تابعه شرکت بریجستون در ایالات متحده منجر به تعطیلی یک هفته‌ای شبکه کامپیوتری و تولید در کارخانه‌های آن در آمریکای شمالی و میانه شد. بریجستون تایرها و سایر قطعات را برای خودروسازان مختلف از جمله تویوتا تامین می‌کند که اخیراً تحت تأثیر حملات مشابه علیه تامین‌کننده دیگری قرار گرفته است.

مقامات آمریکایی و اروپایی به یک توافق اولیه برای حفظ حریم خصوصی داده ها دست یافتند

دانیل مایکلز و سام شچنر از وال استریت ژورنال گزارش دادند که چارچوب حریم خصوصی داده های ترانس آتلانتیک اجازه می دهد تا داده های مربوط به اروپایی ها در ایالات متحده ذخیره شود. این معامله سعی می‌کند با راه‌اندازی یک فرآیند استیناف اروپایی که شامل یک دادگاه مستقل بررسی حفاظت از داده‌ها است، نگرانی‌های حقوقی اروپا را کاهش دهد. دادگاه قدرت صدور احکام لازم الاجرا را خواهد داشت. این معامله برای شرکت‌های بزرگ فناوری که به دلیل انتقال داده‌هایشان به ایالات متحده مورد هدف تنظیم‌کنندگان حریم خصوصی اروپایی قرار گرفته‌اند، مهم است. مایکلز و شچنر می نویسند که مقامات اروپایی و آمریکایی گفتند که "دادگاه جدید حفاظت از داده های ایالات متحده، همراه با تعهد به محدود کردن جمع آوری اطلاعات سیگنال های نامتناسب، از طریق یک فرمان اجرایی ایالات متحده ایجاد خواهد شد."

دولت ایالات متحده در حال بررسی تحریم باند Trickbot است

رابرت مک میلان، کوین پولسن و داستین ولز از وال استریت ژورنال گزارش دادند که تحریم‌ها علیه این گروه، پرداخت باج را برای سازمان‌های آمریکایی غیرقانونی می‌سازد. هکرها و افراد وابسته به آنها از سال ۲۰۱۸ با هدف قرار دادن بیمارستان ها، مدارس و دولت ها در سراسر ایالات متحده صدها میلیون دلار درآمد کسب کرده اند.

یک محقق اوکراینی گفت که آنها به سرورهای گروه نفوذ کرده و ماه گذشته داده ها را به صورت آنلاین ارسال کردند. آنها می نویسند: «بیش از ۲۰۰۰۰۰ پیام رد و بدل شده توسط ۴۵۰ مدیر، کارکنان و شرکای تجاری Trickbot از ژوئن ۲۰۲۰ نشان می دهد که یک سندیکای جنایی سازمان یافته با ارتباطات احتمالی با آژانس های اطلاعاتی روسیه وجود دارد.

تنش‌های روسیه و اوکراین

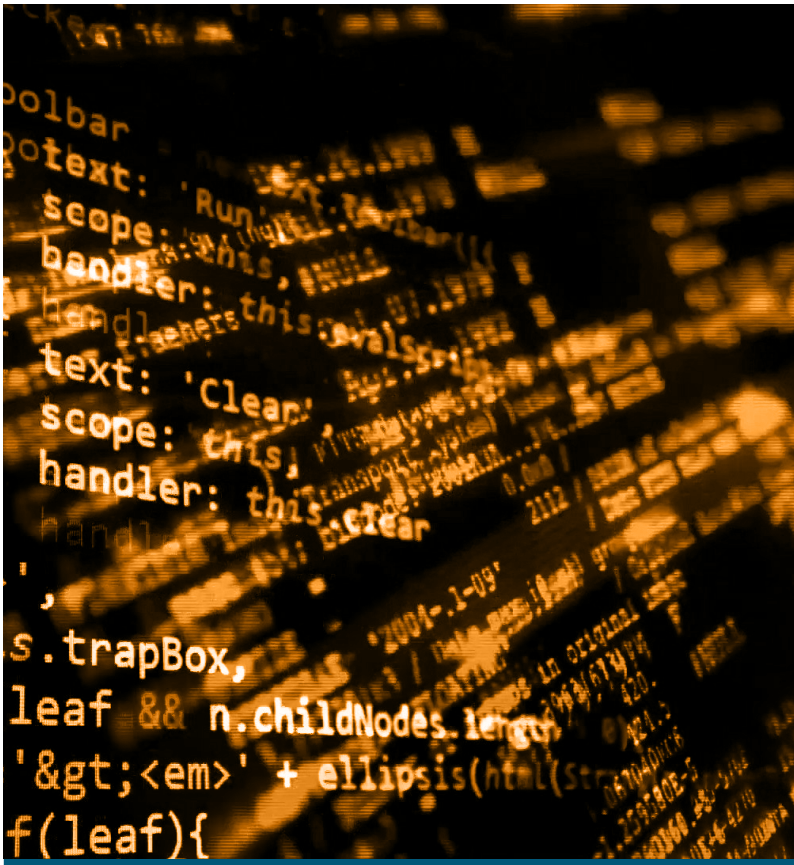
یک شرکت مخابراتی بزرگ اوکراینی در یک "حمله سایبری گسترده" هدف قرار گرفت

حمله سایبری آشکار به ارائه دهنده خدمات اینترنت و تلفن اوکراین Ukrtelecom باعث یکی از گسترده ترین قطعی اینترنت در اوکراین از زمان تهاجم روسیه در ماه گذشته شد. مقامات اوکراینی اشاره کردند که روسیه در پشت این حمله سایبری قرار دارد و گفتند Ukrtelecom در تلاش است تا دوباره آنلاین شود. گریت دی وینک، ریچل لرمن و کت زاکرزوسکی گزارش دادند، علیرغم اختلال در سرویس Ukrtelecom و حمله سایبری به ارائه‌دهنده اینترنت ماهواره‌ای Viasat در ابتدای جنگ، هک‌هایی که زیرساخت‌های مخابراتی اوکراین را هدف قرار می‌دهند، کوچک‌تر و کمتر مخرب‌تر از آن چیزی است که بسیاری از کارشناسان انتظار داشتند. شبکه ها با کمک مهندسان و برنامه های پشتیبان مقاوم باقی مانده اند.

استفاده نیروهای روسی از تجهیزات ناامن آنها را در برابر هدف قرار دادن آسیب پذیر می کند

الکس هورتون و شین هریس گزارش می دهند که سربازان روسی به دلیل نظم نابرابر، فقدان برنامه ریزی برای یک جنگ طولانی و حملات روسیه به زیرساخت های ارتباطی اوکراین که نیروهای روسی نیز به آن متکی هستند، از فناوری ارتباطات ایمن استفاده نمی کنند. کوستاس تیگوس، کارشناس نظامی روسی در شرکت تحلیل دفاعی Janes Group، گفت، شواهدی وجود دارد که نشان می‌دهد ایالات متحده و متحدانش در ناتو به نیروهای اوکراینی تجهیزاتی داده‌اند که می‌توانند ارتباطات روسیه را قطع کنند و به آنها اجازه دهد پست‌های فرماندهی روسیه را هدف قرار دهند. او گفت: «با تخریب گره‌های ارتباطی روسیه، اوکراینی‌ها می‌توانند بر دشمنان خود فشار بیاورند تا از تجهیزات کم‌ایمن استفاده کنند و این احتمال را افزایش می‌دهد که مکالمات آنها شنود شود یا مواضع آنها تضعیف شود.

ایالات متحده و بریتانیا در مورد حملات سایبری احتمالی روسیه هشدار دادند



با ادامه حملات سایبری روسیه و اوکراین به عنوان بخشی از جنگ بین مسکو و کیف، رهبران بریتانیا و آمریکا هشدارهایی را در مورد حملات روسیه به اهداف غربی منتشر کردند. رئیس جمهور بایدن در بیانیه ای در روز دوشنبه شرکت ها را تشویق کرد تا در دفاع سایبری خود هوشیار باشند و به اطلاعاتی اشاره کرد که نشان می دهد دولت روسیه در حال بررسی حملات سایبری است. FBI همچنین هشداری درباره اسکن‌های روسی از شبکه‌های شرکت‌های انرژی آمریکایی صادر کرد و از شرکت‌ها خواست تا ترافیک شبکه را برای آدرس‌های IP مخرب روسیه بررسی کنند. مرکز ملی امنیت سایبری بریتانیا روز سه‌شنبه هشدار پرزیدنت بایدن را تکرار کرد و بیانیه‌ای را منتشر کرد که در آن بر اهمیت اقدامات امنیتی در مواجهه با حملات احتمالی تأکید کرد.

سایبر بین‌الملل


HUAWEI
HUAWEI

مدیر مالی هوآوی اعلام کرد در حال ارزیابی تحریم‌های روسیه است

هوآوی، بزرگترین فروشنده تجهیزات مخابراتی جهان از نظر فروش، می گوید هنوز در حال ارزیابی واکنش خود به تحریم های غرب علیه روسیه است. ارائه گزارش مالی غول فناوری چینی اولین حضور عمومی منگ وانژو، مدیر اجرایی هوآوی از زمان آزادی وی از کانادا در ماه سپتامبر بود.

بازداشت منگ در کانادا به درخواست مقامات ایالات متحده در دسامبر ۲۰۱۸ باعث یک گروگان گیری شد که طی آن چین دو شهروند کانادایی، مایکل کووریگ و مایکل اسپاور را بازداشت و آنها را به جاسوسی متهم کرد. منگ در ایالات متحده به اتهامات کلاهبرداری مربوط به نمایندگی او از رابطه هواوی با یک شرکت وابسته که در ایران فعالیت می کند، متهم شد و او خود را بی گناه دانست.

جنگ در اوکراین باعث عدم اطمینان بیشتر هواوی شده است. هواوی روز دوشنبه اعلام کرد که درآمد آن در سال ۲۰۲۱ نسبت به سال قبل ۲۸.۶ درصد کاهش یافته است، زیرا کسب و کار گوشی های هوشمند Honor خود را به دلیل عدم عرضه تراشه تحت تحریم های ایالات متحده فروخته است. اما این شرکت گفت که سود آن به لطف فروش بخشی از کسب و کار و عوامل دیگر، از جمله «بهینه سازی ترکیب محصول ما»، ۷۵.۹ درصد افزایش یافت. دولت ایالات متحده استدلال کرده است که هوآوی یک خطر امنیت ملی است و می تواند توسط دولت چین برای جاسوسی از آمریکایی ها استفاده شود. این شرکت با این ادعاها مخالفت می کند.

پارلمان اروپا در مورد قانون رقابت دیجیتال بزرگ به توافق نزدیک می شود

انتظار می‌رود پارلمان اروپا در هفته آینده قانون رقابت دیجیتالی جدید، قانون بازارهای دیجیتال را نهایی کند. این قانون، در صورت تصویب، یکی از بزرگ‌ترین تغییرات در مقررات دیجیتال از زمان تصویب مقررات عمومی حفاظت از داده‌های اتحادیه اروپا (GDPR) در سال ۲۰۱۸ خواهد بود.

لابی‌گران صنعت فناوری و برخی از قانون‌گذاران آمریکایی می‌گویند که این قانون به‌طور ناعادلانه شرکت‌های فناوری ایالات متحده را از طریق مقرراتی که تنها شرکت‌هایی با ارزش بازار ۸۲ میلیارد دلار را تحت تأثیر قرار می‌دهد، هدف قرار می‌دهد. این لایحه به طور قابل توجهی مدل های تجاری شرکت های فناوری بزرگ مانند اپل و گوگل در اتحادیه اروپا را تغییر می دهد و مزایای عمده ای برای رقبای کوچکتر ایجاد می کند.


Data Breach
Cyber Attack
System Sa

حملات سایبری

رئیس موساد اسرائیل و همسرش هدف حمله هکرها قرار گرفتند

هکرهایی که ظاهراً با ایران ارتباط دارند اسناد متعلق به دیوید بارنیا، رئیس موساد را در یک کانال تلگرامی ناشناس به نام «دست‌های باز» منتشر کردند. این مطالب شامل عکس ها و فیلم های شخصی، بلیط هواپیما و کارت شناسایی رئیس بود. بارنیا هک شدن دستگاه‌هایش را تکذیب کرد و مدعی شد که این حمله تنها تلفن قدیمی همسرش را نقض کرده است و به اطلاعات حساس مربوط به امنیت دولتی دسترسی پیدا نکرده است. هکرها با انتشار اسناد اضافی، از جمله فرم‌های مالیاتی بارنیا از سال ۲۰۲۰، به این انکار پاسخ دادند. این حمله به دنبال حمله گسترده انکار سرویس (DDoS) در هفته گذشته علیه یک ارائه‌دهنده مخابرات اسرائیلی است که چندین سایت دولتی را آفلاین کرد.


2021

ICDT.IR