گزارش

مجمع ایرانی دفاع از حقیقت

Iranian Council For
Defending The Truth

اسفند ۱۴۰۰

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 مطالب در محور های جنگ میان روسیه و اوکراین، ایالات متحده آمریکا و ارز های دیجیتال مورد طرح و بررسی قرار گرفته است.

در گرماگرم تنش ها در میدان جنگ نظامی میان روسیه و اوکراین شاهد درگیری های سایبری متعدد بین دوجبهه نیز بوده ایم. هر دو طرف اقدامات ویژه ای را برای برتری در نبرد سایبری علیه یکدیگر در پیش گرفته اند.

آمریکا در روز های گذشته متهم به برگزاری های کمپین های گسترده نظارت شده و نیز مشغول بررسی تهدیدات سایبری چین علیه خود بوده است.

در دنیای ارز های دیجیتال فرمان اجرایی جدیدی از سوی رییس جمهور آمریکا برای تنظیم مقررات این ارز ها به تصویب رسید که نوید بخش آینده ای روشن تر برای این ارز ها خواهد بود.

Iranian Council For
Defending The Truth

اخبار

۳

جنگ روسیه و اوکراین

کمپین DDoS روسیه

روسیه در اوایل فوریه یک سری حملات انکار سرویس توزیع شده (DDoS) علیه وب سایت های اوکراینی انجام داد. این حملات وب‌سایت‌های بانکی و دفاعی اوکراین را هدف قرار دادند و طبق گزارش‌ها توسط آژانس اطلاعات نظامی روسیه، GRU، راه‌اندازی شد. این حملات در حالی صورت گرفت که تنش بین اوکراین و روسیه افزایش یافت.

روسیه به صورت متناوب به حملات DDoS ادامه داده است و در هفته اول مارس، گروه‌های روسی از DanaBot، یک پلتفرم بدافزار به عنوان سرویس، برای انجام حملات DDoS علیه وب‌سایت‌های وزارت دفاع اوکراین استفاده می‌کنند. مشخص نیست که این گروه ها چه کسانی هستند و آیا با دولت روسیه مرتبط هستند یا خیر.

ارتش فناوری اطلاعات اوکراین

تلاش‌های اوکراینی در فضای مجازی از گروه‌های داوطلبی که از طریق رسانه‌های اجتماعی و کانال‌های تلگرامی هماهنگ شده‌اند، استفاده کرده است. ارتش فناوری اطلاعات اوکراین شاید یکی از بزرگترین تلاش‌های دولت اوکراین برای هماهنگ کردن اقدامات هکتیویست‌ها باشد. ارتش فناوری اطلاعات با ارسال اهداف مهم در یک کانال تلگرامی با صدها هزار عضو عمل کرده است، در حالی که افراد یا گروه ها از جزئیات ارائه شده برای حمله به اهداف مشخص شده استفاده می کنند. ارتش فناوری اطلاعات وب سایت های چندین بانک روسی، شبکه برق روسیه و سیستم راه آهن را هدف قرار داده و حملات DDoS گسترده ای را علیه سایر اهداف دارای اهمیت استراتژیک انجام داده است. به نظر می رسد بخش عمده ای از قدرت سایبری اوکراین از ارتش فناوری اطلاعات سرچشمه می گیرد.

حملات پارتیزان های سایبری بلاروس به سیستم های قطار

پارتیزان سایبری بلاروس، گروهی که در ژانویه در اعتراض به استقرار نیروهای روسیه در این کشور حملات سایبری را به سیستم‌های قطار بلاروس انجام داد، به نظر می‌رسد در ماه فوریه به کمپین خود علیه راه‌آهن بلاروس ادامه داده است. این حملات، وب‌سایت‌هایی را که برای خرید بلیط استفاده می‌شد، نابود کردند و ممکن است داده‌های رمزگذاری‌شده روی سیستم‌های سوئیچینگ و مسیریابی را داشته باشند، اگرچه مقیاس و شدت حملات فراتر از حذف وب‌سایت‌ها مشخص نبود.

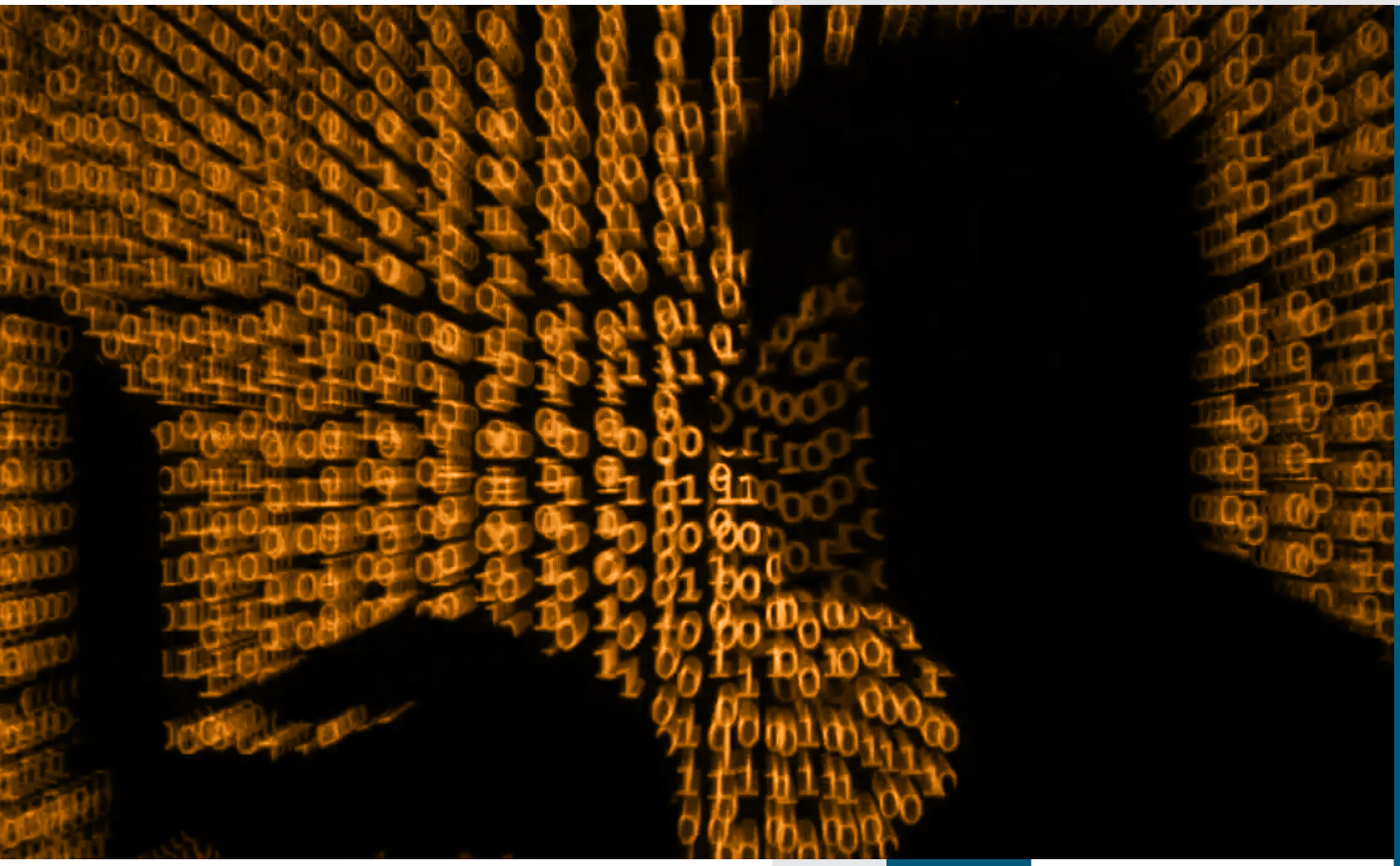
هدف قرار دادن ارتش اوکراین در تلاش های فیشینگ

UNC۱۱۵۱

در ۲۵ فوریه، تیم واکنش اضطراری کامپیوتری اوکراین، گروه هکری تحت حمایت دولت بلاروس UNC۱۱۵۱ را به تلاش برای هک کردن حساب‌های ایمیل پرسنل نظامی خود در یک حمله فیشینگ گسترده متهم کرد. هنگامی که هکرها به حساب‌های پرسنل نظامی نفوذ کردند، از دفترچه‌های آدرس در معرض خطر برای ارسال ایمیل‌های مخرب‌تر استفاده کردند. UNC۱۱۵۱ همچنین به طور بالقوه به یک کمپین فیشینگ دیگر با استفاده از ایمیل‌های نظامی اوکراینی به خطر افتاده برای هدف قرار دادن پرسنل دولت اروپایی که با بدافزار SunSeed به پناهندگان اوکراینی کمک می‌کنند، متصل است.

مقامات دولت اوکراین مظنون به عامل بلاروسی UNC۱۱۵۱ برای انجام یک حمله سایبری با هدف قرار دادن بیش از ۷۰ وب سایت دولتی در ۱۴ ژانویه هستند. هکرها وب سایت ها را تخریب کردند و پیام های تهدیدآمیزی از جمله "بترسید و انتظار بدترین ها را داشته باشید" را پیش از عبور نیروهای روسی از مرز به اوکراین ارسال کردند. گمان می رود که این حمله باعث انحراف از حملات مخرب تر شده باشد.

UNC۱۱۵۱ همچنین در اوایل ماه مارس شناسایی شد که یک کمپین فیشینگ را علیه دولت‌ها و ارتش‌های اوکراین و لهستان راه‌اندازی می‌کرد، اگرچه مشخص نیست که آیا آنها موفق به نفوذ به شبکه‌ای شده‌اند یا خیر.



گروه باج‌افزار Conti با لو رفتن گزارش‌های چت داخلی، با هک خود مواجه شد

پس از اعلام عمومی حمایت کونتی از حمله روسیه به اوکراین، هزاران چت داخلی این گروه توسط حساب توییتری به نام ContiLeaks منتشر شد. پیام‌های فاش شده بینشی از عملیات این گروه ارائه می‌دهند، همچنین قربانیان گزارش‌نشده قبلی و صدها آدرس بیت‌کوین را نشان می‌دهند که می‌توان از آنها برای ردیابی حملات گذشته سازمان استفاده کرد. این افشاگری‌ها همچنین تنش‌های داخلی در این گروه را که هم وابستگان روسیه و هم اوکراین را به کار می‌گیرند، نشان می‌دهد. در حالی که در مورد هویت افشاکننده اختلاف نظر وجود دارد، بسیاری از کارشناسان معتقدند که این یک محقق امنیتی اوکراینی است که از انتخاب کونتی برای حمایت از روسیه عصبانی شده است. پس از افشای اطلاعات، Conti مجبور شد به طور موقت سرورهای خود را خاموش و پاک کند، که باعث شد بسیاری امیدوار شوند که گروه در حال افول است. با این وجود، کارشناسان ادعا می کنند که Conti بازگشته است و تنها ده روز پس از افشای اولیه، حملاتی را به شرکت های آمریکایی انجام داده است.

خروج شرکت های اینترنتی از روسیه

از آنجایی که شرکت‌های بزرگ فناوری غربی مانند اپل، گوگل و اچ‌پی فعالیت خود را در روسیه قطع کردند، شرکت‌های چینی تا حد زیادی تصمیم گرفتند که باقی بمانند و از فرصت رشد سهم خود در بازار استفاده کنند. ویزا و مسترکارت از تعلیق خدمات در روسیه خبر دادند و بانک‌های بزرگ روسیه را به شراکت با سیستم پرداخت چینی UnionPay برای عملیات کارت سوق داد. معدود شرکت های چینی که خروج از بازار روسیه را انتخاب کرده اند با واکنش عمومی مواجه شده اند. دو ارائه‌دهنده خدمات اصلی اینترنت، Cogent Communications و Lumen، اعلام کردند که ارائه خدمات به شرکت‌ها و افراد را در روسیه نیز متوقف خواهند کرد. Cogent و Lumen خدمات اینترنتی را برای برخی از بزرگترین شرکت های اینترنتی در روسیه، از جمله موتور جستجوی Yandex و غول مخابراتی تحت حمایت دولتی Rostelecom ارائه می دهند و برای انتقال داده بین روسیه و سایر کشورها ضروری هستند.

کارشناسان می گویند ارتش اوکراین به فناوری تشخیص چهره دسترسی پیدا کرده است

پرش دیو و جفری دستین از رویترز گزارش دادند، وزارت دفاع اوکراین از شنبه شروع به استفاده از پایگاه داده شرکت تشخیص چهره Clearview AI از میلیاردها تصویر چهره کرد. مدیران شرکت گفتند که انتظار می رود سایر سازمان های دولتی اوکراین به زودی از این فناوری استفاده کنند.

این شرکت می گوید پایگاه داده آن دارای بیش از ۲ میلیارد تصویر از سایت شبکه اجتماعی روسی VKontakte است که به طور بالقوه به مقامات اوکراینی اجازه می دهد تا به سرعت نیروهای کشته شده و خرابکاران روسی را شناسایی کنند. با این حال، مشخص نیست که دقیقاً چگونه از این فناوری استفاده می کنند.

منتقدان می گویند این فناوری می تواند به غیرنظامیان آسیب برساند. گاهی اوقات به اشتباه افراد را شناسایی می کند و به عنوان مثال می تواند منجر به متهم شدن افراد نادرست به جاسوسی روسیه شود.

آنها ادعا کرده اند که هوش مصنوعی Clearview در مورد حفظ حریم خصوصی بد عمل می کند. این شرکت بدون رضایت سایت ها از سایت های رسانه های اجتماعی تصاویر می گیرد. متا مادر فیس بوک و سایر سایت ها از این شرکت خواسته اند که تصاویر خود را از پایگاه داده خود حذف کند. Clearview می گوید که مجموعه داده ها توسط اصلاحیه اول محافظت می شود.

ایالات متحده آمریکا

وزارت امنیت داخلی ایالات متحده به کمپین نظارت انبوه متهم شد

بر اساس نامه ای که سناتور ران وایدن در روز سه شنبه منتشر کرد، وزارت امنیت داخلی میلیون ها انتقال مالی بین افراد در ایالات متحده و مکزیک را زیر نظر داشت. وایدن و اتحادیه آزادی های مدنی آمریکا از این برنامه انتقاد کرده و آن را خلاف قانون اساسی و نقض حریم خصوصی خوانده اند. برنامه نظارتی که در سال ۲۰۱۹ آغاز شد و تا ژانویه ۲۰۲۲ ادامه یافت، شش میلیون رکورد از نقل و انتقالات پول بین آریزونا، کالیفرنیا، نیومکزیکو، تگزاس و مکزیک جمع آوری کرد. مجریان قانون فدرال، ایالتی و محلی همگی به سوابق دسترسی داشتند. این افشاگری در پی افشاگری های گذشته در مورد نظارت مالی در ایالات متحده است، مانند برنامه مخفیانه ای که در دولت بوش آغاز شد و به مقامات اجازه دسترسی به یک پایگاه بین المللی سوابق تراکنش های مالی شامل هزاران آمریکایی را داد.

مدیر دفتر اطلاعات ملی، آوریل هاینس می گوید که چین همچنان بزرگترین تهدید سایبری ایالات متحده است

آوریل هاینس در ارزیابی سالانه خود گفت که چین "گسترده ترین، فعال ترین و پایدارترین تهدید جاسوسی سایبری" را برای شبکه های ایالات متحده ایجاد می کند. در این گزارش آمده است که این کشور «تقریباً » قادر به انجام حملات سایبری است که به شبکه‌های زیرساختی حیاتی ضربه می‌زند.

این گزارش همچنین شامل ارزیابی از تهدیدات سایبری روسیه بود. هاینز در جریان یک جلسه کمیته اطلاعات مجلس نمایندگان در مورد تهدیدات با سایر مقامات ارشد اطلاعاتی صحبت کرد.

همچنین بر اساس این گزارش، کره شمالی «احتمالاً دارای تخصص» برای ایجاد اختلالات «موقتی و محدود» در شبکه‌های زیرساختی حیاتی ایالات متحده است. و ایران "بیشتر از گذشته مایل است تا کشورهایی با قابلیت های قوی تر" را در فضای سایبری هدف قرار دهد.


LITECOIN
LTC
LITECOIN

ارزهای دیجیتال

بایدن فرمان اجرایی جدیدی را برای تنظیم ارزهای دیجیتال امضا کرد

رئیس جمهور جو بایدن روز چهارشنبه فرمان اجرایی جدیدی را با هدف ارزهای دیجیتال اعلام کرد. این دستور به آژانس‌های فدرال شش ماه فرصت می‌دهد تا تأثیر ارزهای دیجیتال بر اقتصاد و محیط زیست را بررسی کنند. همچنین از وزارت دادگستری خواسته شد که ایجاد دلار دیجیتال را بررسی کند و اینکه آیا انجام این کار مستلزم تصویب قانونی توسط کنگره است یا خیر. بسیاری از شرکت‌های ارزهای دیجیتال از این فرمان اجرایی به عنوان یک پیروزی استقبال کردند، اما بدبینان ارزهای دیجیتال گفتند که این دستور گامی در جهت اشتباه است و مانع از تلاش‌ها برای توقف استفاده از ارزهای دیجیتال در جرم و جنایت می‌شود. ارزهای دیجیتال به کانون اصلی گفت و گوی تنظیم‌کننده‌های مالی و دادستان‌های ایالات متحده تبدیل شده‌اند و مقامات ایالات متحده در هفته گذشته تعدادی از اتهامات مربوط به سرقت ارزهای دیجیتال را افشا کرده‌اند.

ICDT.IR