گزارش

مجمع ایرانی دفاع از حقیقت

Iranian Council For
Defending The Truth

فروردین ۱۴۰۱

امنیت سایبـــــری


بسم الله الرحمن الرحیم

فهرست

۱ **پیشگفتار**
۲ **مقدمه**
۳ **اخبار**

۱۶ وزارت امور خارجه دفتر جدید فضای مجازی و سیاست دیجیتال را افتتاح کرد
۱۷ جنجال بر سر نظارت شبکه های اجتماعی توسط FBI
۱۸ ایالات متحده و شرکای آن، بات نت روسیه را مختل می کنند
۱۹ دولت ایالات متحده یک توسعه دهنده بدافزار روسی را تحریم می کند

۲۲ مایکروسافت هکرهای روسی را که سازمان‌های اوکراینی، آمریکایی و اروپایی را هدف قرار می‌دهند، مختل می‌کند
۲۳ دولت بایدن به شرکت‌ها در مورد کسپرسکی هشدار داد

۲۶ عدم موفقیت T-Mobile در تلاش باز خرید اطلاعات مشتریان
۲۶ چین به عنوان یک خروجی قوی برای اطلاعات نادرست روسیه عمل می کند

۳۱ هوش مصنوعی Clearview فراتر از مشتریان دولتی است

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

این شماره از دیدبان سایبری در چهار محور شامل ایالات متحده آمریکا، تنش بین روسیه و اوکراین، سایبر بین الملل و تازه های سایبری تهیه و منتشر شده است. در هفته ای که گذشت درآمریکا دفتری برای آمادگی در برابر تهدیدات سایبری از جمله روسیه، افتتاح شد و نیز تحریم هایی علیه توسعه دهندگان ویروس های روسی انجام گرفت. همچنین جنجال های زیادی در مورد استفاده ی اف بی ای از ابزار های نظارت در شبکه های اجتماعی بوجود آمده است. اما در ادامه تنش بین روسیه و اوکراین این بار مایکروسافت دست به اقدام زده و زیرساخت های ارتباطی روسی که جهت عملیات های سایبری استفاده می شده اند را محدود کرده همچنین از طرفی دولت بایدن هشدار به استفاده از ضدویروس روسی کسپراسکی داده است. در بخش تهدیدات سایبری و تازه های سایبری میخوانیم که چین به عنوان نماینده روسیه در انتشار اطلاعات غلط استفاده شده، شرکت تی موبایل نتوانسته اطلاعات هک شده مشتریانش از هکر ها را بازیابی کند و نیز شرکت کلیر ویو به دنبال مشتریان خصوصی بوده است.

Iranian Council For
Defending The Truth

اخبار

۳

ایالات متحده آمریکا

وزارت امور خارجه دفتر جدید فضای مجازی و سیاست دیجیتال را افتتاح کرد

وزارت امور خارجه آمریکا در اوایل این هفته دفتر جدیدی برای فضای مجازی و سیاست دیجیتال راه اندازی کرد. افتتاح این دفتر با تمرکز دولت بایدن بر دیپلماسی سایبری هماهنگ است و همزمان با نگرانی های فزاینده در مورد حملات سایبری روسیه است. این به دنبال هشدارهای کاخ سفید در مورد افزایش خطرات حملات سایبری روسیه در زیرساخت های حیاتی ایالات متحده و سایر بخش ها است. این دفتر بر توزیع کمک های سایبری به کشورهای خارجی، تنظیم استانداردهای بین المللی به عنوان بخشی از نهادهایی مانند اتحادیه بین المللی مخابرات، و ارتقای حقوق و آزادی های دیجیتال تمرکز خواهد کرد. این دفتر قرار است به باج‌افزار، مقررات فضای سایبری و جایگزین‌های فناوری 5G چینی بپردازد.

جنجال بر سر نظارت شبکه های اجتماعی توسط FBI

اف‌بی‌آی در حال سرمایه‌گذاری در فناوری نظارت بر رسانه‌های اجتماعی است و ۲۷ میلیون دلار برای قراردادی با شرکت نرم‌افزاری Babel Street هزینه کرده است. این توافق باعث نگرانی قانونگذاران دموکرات و جمهوری خواه در مورد خطر نظارت و سانسور دولت شده است. FBI از این خرید دفاع کرده است و ادعا می کند که این ابزار تنها با انجام حدود ۲۰۰۰۰ جستجوی کلمه کلیدی در ماه، اطلاعات در دسترس عموم را بررسی می کند.

در نوامبر ۲۰۲۱، بحث مشابهی بر سر قرارداد خزانه داری ایالات متحده با Babel Street به وجود آمد. این قرارداد شعبه اجرای تحریم‌ها و خدمات درآمد داخلی را قادر می‌سازد تا به داده‌های مکان و سایر اطلاعات جمع‌آوری‌شده در اپلیکیشن‌های گوشی‌های هوشمند بدون هیچ گونه محدودیتی در روند قانونی دسترسی داشته باشند. گمرکات و حفاظت مرزی، سرویس مخفی، و اداره مهاجرت و گمرک ایالات متحده نیز در گذشته ابزارهایی را از Babel Street خریداری کرده اند.

ایالات متحده و شرکای آن، بات نت روسیه را مختل می کنند

وزارت دادگستری اعلام کرد که با آژانس‌های امنیتی ایالات متحده و بریتانیا در ایجاد اختلال در باتنت بزرگ جهانی که توسط بازیگر روسی Sandworm ایجاد شده بود، همکاری کرده است. این بات نت، معروف به Cyclops Blink، حداقل از ژوئن ۲۰۱۹ فعال بوده و هزاران دستگاه را آلوده کرده است، اما احتمالاً در هیچ حمله ای استفاده نشده است. وزارت دادگستری دستورات دادگاه را برای قطع ارتباط بسیاری از سرورهای فرمان و کنترل جهانی که توسط Sandworm برای هدایت باتنت استفاده می‌شد، تضمین کرد و FBI این بدافزار را در برخی موارد بدون تأیید صاحب دستگاه از دستگاه‌های آلوده حذف کرد. ایالات متحده قبلاً باتنت‌های Sandworm را مختل کرده است، از جمله در سال ۲۰۱۸ که FBI باتنت VPNFilter را حذف کرد.

دولت ایالات متحده یک توسعه دهنده بدافزار روسی را تحریم می کند

این تحریم ها یک هفته پس از افشای کیفرخواستی از سوی وزارت دادگستری صورت گرفت که محققی به نام گلادکیخ را متهم به توسعه بدافزاری کرد که یک کارخانه پتروشیمی عربستان را در سال ۲۰۱۷ هدف قرار داد. وزارت خزانه داری گلادکیخ را به همراه مؤسسه تحقیقاتی روسیه که در آن کار می کرد، تحریم کرد. وزارت خزانه داری آمریکا می گوید: گلادکیخ، نقش مهمی در حمله سایبری بدافزار تریتون در آگوست ۲۰۱۷ ایفا کرد. دولت ایالات متحده برای اطلاعات در مورد گلادکیخ تا ۱۰ میلیون دلار جایزه تعیین کرده است.

تنش روسیه و اوکراین

مایکروسافت هکرهای روسی را که سازمان‌های اوکراینی، آمریکایی و اروپایی را هدف قرار می‌دهند، مختل می‌کند

مایکروسافت کنترل دامنه های اینترنتی مورد استفاده گروهی از هکرهای جاسوسی ارتش روسیه را برای هدف قرار دادن سازمان های رسانه ای اوکراینی و همچنین موسسات دولتی و اتاق های فکر در ایالات متحده و اروپا به دست گرفت. به گفته مایکروسافت، دادگاه روز چهارشنبه به شرکت اجازه داد تا کنترل دامنه ها را در دست بگیرد. گروه هک Strontium که به گفته مایکروسافت پشت این کمپین بود، بیشتر با نام Fancy Bear شناخته می شود. دولت ایالات متحده این گروه را متهم به ارتباط با یک واحد اطلاعاتی نظامی روسیه کرده و گفته است که مسئول برخی از کمپین های مداخله در انتخابات بوده است.

دامنه‌های ضبط شده قبلاً برای حمله به چندین آژانس دولتی اوکراین، اتحادیه اروپا (EU) و ایالات متحده و تعداد کمی از اندیشکده‌های سیاست خارجی استفاده شده بود. مایکروسافت اعلام کرد که معتقد است از این دامنه ها به عنوان بخشی از تلاش برای ایجاد دسترسی طولانی مدت به سیستم های هدفمند و سرقت داده های حساس استفاده می شود. APT۲۸ به دلیل تعدادی از هک‌های پرمخاطب متهم شده است، اما شاید بیشتر به خاطر نقشش در دخالت در انتخابات ۲۰۱۶ مشهور است. مایکروسافت گفت: «ما معتقدیم که استرانسیوم تلاش می‌کرد تا دسترسی طولانی‌مدت به سیستم‌های اهداف خود ایجاد کند و پشتیبانی تاکتیکی برای تهاجم فیزیکی و استخراج اطلاعات حساس فراهم کند. ما به دولت اوکراین درباره فعالیت‌هایی که شناسایی کرده‌ایم و اقداماتی که انجام داده‌ایم اطلاع داده‌ایم.»

دولت بایدن به شرکت‌ها در مورد کسپرسکی هشدار داد

مقامات دولتی یک روز پس از تهاجم روسیه به اوکراین به شرکت های آمریکایی هشدار دادند که مقامات روسیه می توانند «نرم افزار طراحی شده توسط شرکت امنیت سایبری روسیه کسپرسکی را برای آسیب رساندن دستکاری کنند». مشخص نیست که آیا اطلاعات جدید یا یک حادثه باعث این سخنان شده است.

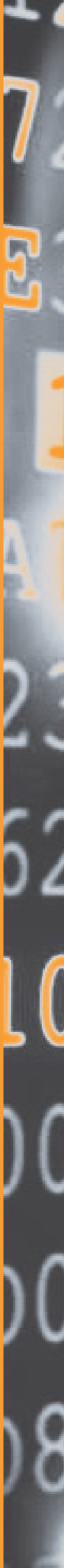
کسپرسکی خود را بزرگترین شرکت امنیت سایبری خصوصی در جهان می نامد. جامعه اطلاعاتی ایالات متحده سال ها استدلال می کرد که مسکو می تواند از این نرم افزار به عنوان ابزار جاسوسی استفاده کند. این شرکت بارها این اتهامات را رد کرده است.

آژانس‌های امنیتی مجموعه‌ای از جلسات توجیهی امنیتی سایبری را پیرامون ممنوعیت دولت ترامپ از نرم‌افزار کسپرسکی از شبکه‌های آژانس‌های غیرنظامی در سال ۲۰۱۷ انجام دادند. در هفته های اخیر وال استریت ژورنال گزارش داد که دولت ایالات متحده در نظر گرفته است که آزمایشگاه های کسپرسکی را تحریم کند، اگرچه ظاهراً این ایده متوقف شده است. کمیسیون ارتباطات فدرال این شرکت را یک تهدید امنیت ملی تلقی کرد، به این معنی که نمی توان از یارانه های فدرال برای خرید خدمات آن استفاده کرد.

یکی از سخنگویان کسپرسکی به رویترز گفت که جلسات توجیهی بیشتر به شهرت کسپرسکی آسیب می رساند بدون اینکه به شرکت فرصت پاسخگویی مستقیم به چنین نگرانی هایی را بدهد و عادلانه نیست.


Data Breach
Cyber Attack
System Sa

تهدیدات سایبری



عدم موفقیت T-Mobile در تلاش باز خرید اطلاعات مشتریان

هکرها برای دسترسی به اطلاعات دزدیده شده ۶ بیت کوین یا حدود ۲۷۰۰۰۰ دلار درخواست کردند. این معامله در نهایت به ضرر شرکت شکست خورد و جنایتکاران علیرغم اینکه در مجموع ۲۰۰۰۰۰ دلار به آنها داده شده بود ، به فروش داده‌ها ادامه دادند. اما این اخبار برخی از تاکتیک‌های بحث‌برانگیز را آشکار می‌کند که ممکن است توسط شرکت‌ها در واکنش به نقض داده‌ها، یا برای کاهش نشت اطلاعات دزدیده شده یا در تلاش برای شناسایی افرادی که به شبکه‌های آنها نفوذ کرده‌اند، استفاده کنند.

چین به عنوان یک خروجی قوی برای اطلاعات نادرست روسیه عمل می کند

الیزابت دووسکین گزارش می‌دهد که موفقیت روسیه در انتشار روایت‌های گمراه‌کننده از طریق نیابت‌ها و متحدان، توانایی غول‌های فناوری و دولت‌های غربی را برای مهار تبلیغات و انتشار محتوای غلط مورد تهدید قرار داده است. این مساله به کرملین این امکان را داد که به طور مؤثری از ممنوعیت هایی که به منظور محدود کردن گسترش تبلیغات روسیه است، فرار کند. چینی ها مخاطبان زیادی دارند. تنها در فیس بوک، رسانه های چینی بیش از ۱ میلیارد دنبال کننده دارند - بسیار بیشتر از مجموع ۸۵ میلیون دنبال کننده که کانال های اصلی روسیه دارند.

فیس بوک در پاسخ به سوالی درباره نحوه رسیدگی به این موضوع، نمونه هایی از بررسی حقایق در مورد محتوای گمراه کننده طرفدار روسیه را از رسانه های دولتی چین به اشتراک گذاشت. این شرکت به سوالاتی در مورد اینکه آیا حساب های رسانه دولتی چین را محدود کرده است یا قصد انجام این کار را دارد، پاسخی نداد.


(0,1)
M = 0.046765 / 3 0L
n (B) + n (C)-n (B∩C)
02602
989769
948
CH
CH
HO
H
H
y = ax +

تازه‌های سایبری

هوش مصنوعی Clearview فراتر از مشتریان دولتی است

شرکت تشخیص چهره Clearview AI در حال گسترش فراتر از مشتریان معمولی بخش دولتی خود است و قصد دارد تا محصولات خود را به بانک ها و سایر مشاغل بخش خصوصی عرضه کند. مدیرعامل شرکت فاش کرد که این شرکت برنامه هایی برای رقابت با شرکت های فناوری بزرگ مانند آمازون و مایکروسافت برای ایجاد ابزارهای تأیید هویت مشتری با استفاده از فناوری تشخیص چهره دارد. Clearview AI الگوریتم های پیشرفته تشخیص چهره خود را در دسترس مشتریان بخش خصوصی قرار می دهد. با این حال، این شرکت گفت که مجموعه بیست میلیارد تصویری که برای مطابقت دادن افراد با پروفایل های آنلاین استفاده می شود، محدود به استفاده از اجرای قانون خواهد شد. Clearview AI نیز اخیرا خدمات خود را به عملیات نظامی گسترش داده است. این شرکت پس از اینکه اوکراین شروع به استفاده از فناوری تشخیص چهره خود برای شناسایی سربازان روسی در طول درگیری کرد، خبرساز شد.

ICDT.IR