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

شماره کنونی دیدبان سایبری در محور های ایالات محتده آمریکا، تهدیدات سایبری، سایبر بین الملل و مناقشه روسیه و اوکراین تهیه و تنظیم شده است.

در روز های اخیر مجلس سنای آمریکا قانون جدیدی را برای افزایش توان بازدارندگی خود در عرصه امنیت سایبری به تصویب رسانده است.

در مورد تهدیدات سایبری اخیریک بد افزار پیشرفته ی چینی در حملات چند روز گذشته و در آزمایش‌های سایبری مشاهده شده که توان تخریبی بالایی را از خود نشان داده است. همچنین گروهی از هکرها به اطلاعات مهمی از شرکت های فناوری مانند سامسونگ دسترسی پیدا کرده اند.

مناقشات روسیه و اوکراین شاهد صحنه های دیگری در عرصه های سایبری بوده است. اینترنت روسیه در حال محدود شدن بوده و بسیاری از بزرگترین شرکت های خدمات دهنده ی اینترنت ارایه خدمات خود به روسیه را کاهش داده یا قطع کرده اند. حملات هکری بین دو طرف نیز ادامه دارد.

Iranian Council For
Defending The Truth

اخبار

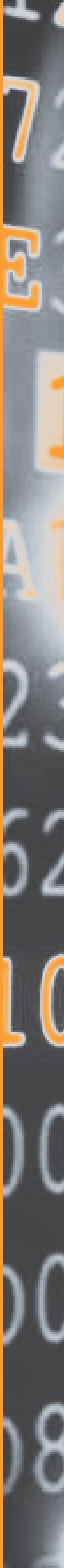
۳

ایالات متحده آمریکا

سنا قانون تقویت امنیت سایبری آمریکا را تصویب کرد

سنا اوایل این هفته قانون تقویت امنیت سایبری آمریکا را تصویب کرد . این لایحه به اتفاق آرا به تصویب رسید، این قانون الزامات گزارش دهی را برای آژانس های فدرال، که اکنون ملزم به گزارش حملات سایبری به آژانس امنیت سایبری و امنیت زیرساخت فدرال (CISA) هستند، گسترش می دهد. این لایحه همچنین تعریف زیرساخت های حیاتی را گسترده تر می کند و شرکت هایی را که تحت این تعریف قرار می گیرند ملزم می کند حملات سایبری را به CISA نیز گزارش دهند. گروه‌های زیرساختی حیاتی هم اکنون موظفند حملات سایبری را ظرف هفتاد و دو ساعت پس از شناسایی و پرداخت‌های باج‌افزاری را ظرف بیست و چهار ساعت پس از انجام آن گزارش کنند.

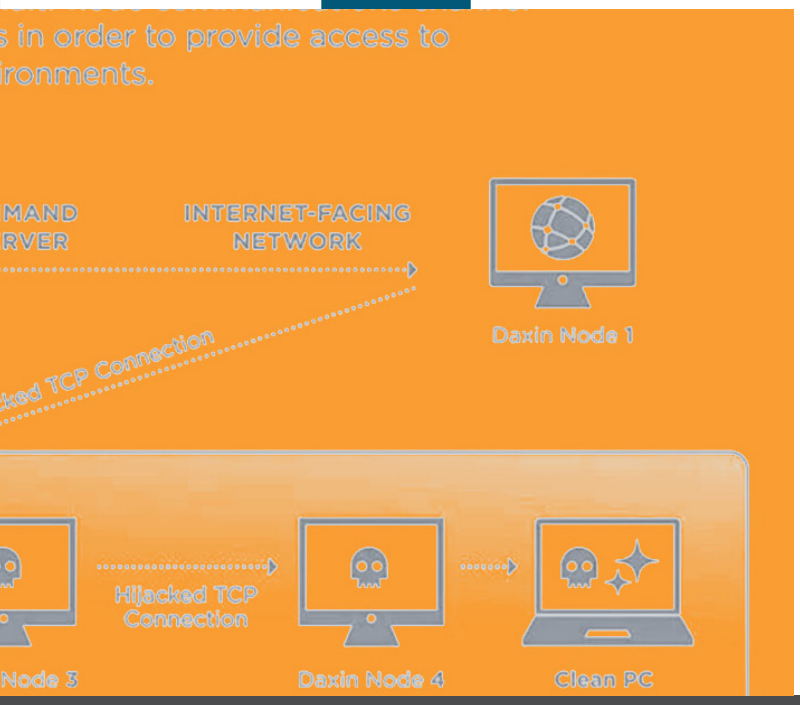

Data Breach
Cyber Attack
System Sa



تهدیدات سایبری

ابزار جدید و بسیار پیشرفته جاسوسی سایبری چینی شناسایی شد

گزارش سیمانتک که روز دوشنبه منتشر شد نشان داد بدافزار بسیار پیچیده ای توسط عوامل مرتبط با چین برای انجام کمپین های جاسوسی مستقر شده است. این بدافزار که Daxin نام دارد، به عنوان یک درپشتی مخفیانه عمل می‌کند و در حملاتی که به دولت‌های منتخب و زیرساخت‌های حیاتی هدایت می‌شوند، استفاده شده است. داکسین با ربودن سرویس‌های قانونی که قبلاً روی دستگاه‌های آلوده اجرا می‌شدند به منظور پنهان کردن ارتباطات خود در ترافیک عادی شبکه، بر قابلیت‌های پیشرفته تشخیص تهدید غلبه می‌کند. در حالی که آخرین حمله Daxin در نوامبر ۲۰۲۱ رخ داد، شواهدی وجود دارد که نشان می‌دهد این بدافزار در اوایل سال ۲۰۱۳ کار می‌کرده است. در نوامبر ۲۰۱۹، یک عامل تهدید چینی تلاش ناموفقی برای استقرار Daxin علیه یک شرکت فناوری اطلاعات داشت. داکسین، یکی از ابزارهای قدرتمندی است که در سال گذشته با چین مرتبط شده است و قابلیت‌های رو به رشد سایبری این کشور را برجسته می‌کند.



یک گروه هکر در حال انتشار اطلاعات حساس در مورد شرکت های بزرگ فناوری است

که گروه هک $Lapus در روزهای اخیر اطلاعات اختصاصی سامسونگ و انویدیا را فاش کرده است. این گروه می گوید که داده های بسیار حساس از هر دو شرکت از جمله کد منبع داخلی را فاش کرده است. مشخص نیست این گروه هکر چگونه و چه زمانی اطلاعات را به سرقت برده یا در ازای عدم انتشار اطلاعات خود از سامسونگ باج می خواهد.

این گروه به طور علنی تهدید کرد که اگر انویدیا نرم‌افزار خود را برای رفع محدودیت‌های استخراج ارزهای دیجیتال، که به منابع رایانه‌ای فشرده نیاز دارد، به‌روزرسانی نکند، داده‌های مربوط به فناوری را منتشر خواهد کرد.

مشخص نیست که چرا هکرها چنین تقاضایی را مطرح کردند، اگرچه آنها گفتند که این کار را برای "کمک به" جوامع ماینینگ و بازی انجام دادند و پس از اینکه شرکت از مذاکره امتناع کرد، شروع به انتشار داده ها کردند.

هکرها در حال حاضر از اطلاعات لو رفته انویدیا به عنوان بخشی از حملات خود استفاده می کنند. آنها اساسا از ابزارهای شرکت استفاده می کنند تا ابزارهای هک را شبیه نرم افزارهای قانونی جلوه دهند، به گونه ای که ممکن است از ابزارهای تشخیص ویروس پیشی بگیرد. این شرکت گفت که انویدیا در حال بررسی این حادثه است و عملیات تجاری آن بدون وقفه ادامه دارد. سامسونگ به درخواست ها برای اظهار نظر پاسخ نداد.

سایبر بین‌الملل

گوگل غول سایبری Mandiant را به قیمت ۵.۴ میلیارد دلار خریداری خواهد کرد

Mandiant اغلب تحقیقاتی را در مورد هکرهای دولتی از کشورهایی مانند چین و روسیه منتشر می کند. رویترز گزارش می دهد که این معامله یک موهبت بزرگ برای تجارت رایانش ابری گوگل است. گوگل گزارش می دهد که بخش ابری گوگل سالانه حدود ۱۹ میلیارد دلار درآمد دارد اما همچنان ضرر می کند.

این گزارش تقریبا یک ماه پس از گزارش بلومبرگ منتشر شد که مایکروسافت در حال مذاکره برای خرید Mandiant است. مایکروسافت و گوگل دارای تقسیمات ابری قابل توجهی هستند. مایکروسافت بیش از یک هفته پیش از مذاکرات برای این شرکت خارج شد.

Mandiant با انتشار گزارشی مهم در سال ۲۰۱۳ در مورد APT۱، که جزئی ترین گزارش عمومی از هک مورد حمایت دولت چین در آن زمان بود، به رسمیت شناخته شد. شرکت های برتر امنیت سایبری اکنون چنین گزارش هایی را به عنوان بخشی از اقدامات استاندارد خود منتشر می کنند. FireEye Mandiant را در سال ۲۰۱۳ خرید، اما Mandiant سال گذشته به یک شرکت جداگانه تبدیل شد. FireEye با McAfee Enterprise ترکیب شده و شرکت امنیت سایبری Trellix را تشکیل داده است. این شرکت در بیانیه‌ای اعلام کرد: «بیش از ۶۰۰ مشاور Mandiant در حال حاضر به هزاران نقض امنیتی هر سال پاسخ می‌دهند»

شرکت مخابراتی سوئدی اریکسون با رسوایی فساد جدیدی روبرو شد

اسناد فاش شده از تحقیقات داخلی شرکت مخابرات سوئدی اریکسون، سوء رفتار در معاملات تجاری عراق را فاش کرد. این گزارش جزئیات رشوه، کلاهبرداری و اختلاس شرکتی در عراق را ارایه کرده و نشان می دهد که چگونه وجوه پرداختی به ستیزه جویان برای قراردادهای حمل و نقل ممکن است در اختیار داعش قرار گرفته باشد. این گزارش همچنین اشاره می‌کند که چگونه شبه‌نظامیان پیمانکاران اریکسون را پس از اینکه شرکت تصمیم گرفت آنها را به قلمرو تحت کنترل جنگجویان داعش بفرستد، ربودند. این اولین بار نیست که اریکسون با اتهامات فساد روبرو می شود. در سال ۲۰۱۹، اریکسون ۱.۰۶ میلیارد دلار برای حل و فصل اتهامات مربوط به رشوه توسط وزارت دادگستری ایالات متحده پرداخت کرد که در اکتبر ۲۰۲۱ توسط دادستان ها به نقض توافقنامه متهم شد.


ERICSSON
Ericsson Group
Headquarters
21

تنش‌های روسیه و اوکراین


LinkedIn
foursquare
skype
LIVEJOUR
vime
Tube
facebook
g+
Blogger
my
twitter
flickr

شرکت‌های رسانه‌های اجتماعی با تمرکز روسیه بر کمپین‌های اطلاعات نادرست سرکوب می‌شوند

بسیاری از پلتفرم‌های رسانه‌های اجتماعی با افزایش قابل توجه کمپین‌های اطلاعات نادرست روسی، به فعالیت رسانه‌های روسی در سایت‌های خود می‌پردازند. فیس‌بوک، تیک تاک و یوتیوب اعلام کردند که رسانه‌های دولتی روسیه را از پلتفرم‌های خود در اروپا منع می‌کنند، در حالی که توییتر ترجیح داده است برچسب‌های مشاوره‌ای را برای پست‌هایی با پیوند به منابع رسانه دولتی روسیه منتشر کند. علاوه بر این، متا شروع به ارائه خدمات پیام رسانی مستقیم رمزگذاری شده اینستاگرام در روسیه و اوکراین کرده است. بنا بر گزارش‌ها، رهبران اوکراین از اپل، متا و گوگل درخواست کرده‌اند که خدمات خود را در داخل روسیه محدود کنند و این بحث را در مورد اینکه آیا چنین اقدامی با از بین بردن راه‌های مخالفت آنلاین، رژیم را تقویت می‌کند یا خیر، ایجاد کرد. رهبران اوکراین همچنین نامه‌ای به شرکت بین‌المللی برای نام‌ها و شماره‌های اختصاص‌یافته که دسترسی به دامنه‌ها را کنترل می‌کند، ارسال کردند و درخواست کردند که دامنه‌های اینترنتی روسی، .ru و .su، به طور کامل از سرورهای نام دامنه جهانی جدا شوند و عملاً کل دامنه منزوی شود. برخی از محققان گفتند که این اقدام احتمالاً با منزوی کردن شهروندان روس از منابع اطلاعاتی تحت کنترل غیردولتی، به برنامه‌های پوتین کمک می‌کند.

اطلاعات منبع باز نقش کلیدی در مناقشه روسیه و اوکراین دارد

تحقیقات منبع باز (OSINT) ثابت کرده است که ابزار بسیار مفیدی است زیرا محققان تلاش می کنند تا در مورد مناقشه در حال تغییر در اوکراین به روز بمانند. پست‌های رسانه‌های اجتماعی که فعالیت در اوکراین را مستند می‌کنند، به تحلیلگران OSINT این امکان را می‌دهد تا عملیات نیروهای روسی را موشکافی کنند و اطلاعات نادرست منتشر شده توسط خبرگزاری‌های تحت حمایت دولت روسیه را به‌موقع از بین ببرند. توییتر به ویژه منبع پرکار OSINT بوده است، با حساب‌هایی مانند اوکراین Weapons Tracker که هر ساعت به‌روزرسانی‌های مربوط به درگیری را ارسال می‌کند. با این حال، توییتر با چالش هایی در ایجاد تمایز بین OSINT و اطلاعات نادرست مواجه شده است و روز سه شنبه اعتراف کرد که به اشتباه حساب های برخی از خبرنگاران OSINT را تعلیق کرده است.

قبل از حمله روسیه به اوکراین، هکرها به بیش از ۲۰ شرکت گاز طبیعی نفوذ کردند

Resecurity گفت که برخی از هکرهای دخیل در این کمپین توسط سایر محققان سایبری با گروه های هکر روسی مرتبط شده اند، اما این شرکت از بیان اینکه این حمله یک عملیات روسی بوده است خودداری کرد. ژن یو، مدیر اجرایی امنیت، گفت که فکر می‌کند هکرهای دولتی پشت این حملات بوده‌اند، اما از اظهارنظر بیشتر خودداری کرد. Resecurity متوجه شد که هکرها سعی می‌کردند نام‌های کاربری و رمز عبور کارمندان شرکت‌های بزرگ گاز طبیعی ایالات متحده را بخرند و پیشنهاد پرداخت را داشتند.

روسیه و بلاروس حملات فیشینگ را با هدف اوکراین آغاز کرده اند

گوگل اعلام کرد هکرهای نظامی روسیه سعی کردند شهروندان اوکراینی را فریب دهند تا مدارک خود را در آستانه تهاجم روسیه به این کشور تحویل دهند. بلاروس، در عین حال، هم اوکراینی ها و هم ارتش لهستان را در کمپین های فیشینگ هدف قرار داده است.

این شرکت گفت: «گروه تحلیل تهدیدات گوگل این تلاش ها را ردیابی کرد و به صدها نفر هشدار داد که توسط یک دولت هدف قرار گرفته اند. مشخص نیست که آیا هیچ یک از تلاش‌ها موفق بوده است یا خیر، زیرا هدف آنها حساب‌های ایمیل گوگل نبوده است.

حملات یک گروه مرتبط با دولت بلاروس به نام Ghostwriter همگی در هفته گذشته رخ داده است. گوگل گفت که طی دو هفته گذشته، یک گروه هکر کرملین معروف به Fancy Bear کمپین های فیشینگ بزرگی را علیه کاربران Ukr.net، یک سازمان رسانه ای اوکراینی، راه اندازی کرده است.


CYBER
DATA

اینترنت روسیه در حال تغییر به سمت داخل است

سانسورچیان روسی فیس بوک را ممنوع کرده و دیگر سرویس های رسانه های اجتماعی ایالات متحده را خفه کرده اند. ارائه دهنده خدمات اینترنتی Cogent Communications نیز روابط خود را با مشتریان روسی قطع کرده است. مایکروسافت و اپل نیز فروش در روسیه را ممنوع کرده اند.

روی هم رفته، این تحولات ردیابی جنگ در اوکراین را برای روس‌ها سخت‌تر می‌کند و این کشور را به اینترنت کاملاً منزوی نزدیک‌تر می‌کند.

تحلیلگران می گویند که حرکت کوجنت بسیار مهم بود. داگ مادوری، تحلیلگر می‌نویسد: « در تاریخ اینترنت بی‌سابقه است یک شرکت حامل اصلی مشتریان خود را در کشوری به بزرگی روسیه قطع کند.

دیو شفر، مدیر اجرایی، گفت، نگرانی اصلی این بود که دولت روسیه از شبکه‌های کوجنت برای انجام حملات سایبری یا ارائه تبلیغاتی که اوکراین را هدف قرار می‌دهد استفاده کند.

وزیر تحول دیجیتال اوکراین، میخایلو فدور می نویسند، در ابتدا شرکت های مصرف کننده محبوب مانند اپل، فیس بوک و گوگل را تحت فشار قرار دادند تا خدمات را از روسیه خارج کنند. اکنون او توجه خود را به شرکت‌هایی معطوف کرده است که خود اینترنت را به کار می‌اندازند و از شرکت‌هایی مانند آمازون و کلودفلر می‌خواهد که ارائه خدمات در روسیه را متوقف کنند. با تشدید جنگ و تحریم های بین المللی، اشکال دیگری از قطع ارتباط احتمالی وجود دارد.

هک یک شرکت اینترنتی ماهواره ای که به اوکراین خدمات رسانی می کند

مقامات آلمانی می گویند که حمله سایبری که ویاسات را هدف قرار داد می تواند مربوط به حمله روسیه به اوکراین باشد که ارتش آن از این فناوری استفاده می کند. این هک باعث شد مشتریان Viasat اینترنت خود را در ۲۴ فوریه، همزمان با حمله روسیه از دست بدهند. این هک همچنین از اتصال هزاران توربین بادی آلمانی به اینترنت جلوگیری کرده است. این امر اپراتورها را از کنترل توربین ها از راه دور مسدود می کند. جزئیات این حمله سایبری کم کم آشکار شد. ژنرال میشل فریدلینگ، که فرماندهی فضایی فرانسه را رهبری می‌کند، تأیید کرد که این شرکت مورد حمله سایبری قرار گرفته است. Viasat قبلاً گفته بود که یک "رویداد سایبری" را تجربه کرده است، اما جزئیات کمی ارائه کرد و گفت که در حال "کمک کردن" به تحقیقات است.

Cloudflare همچنان در روسیه می ماند

Cloudflare که به محافظت از شرکت‌ها در برابر حملات انکار سرویس کمک می‌کند، درخواست‌ها برای کنار گذاشتن همه مشتریان روسی خود را رد کرد و گفت که «روسیه به دسترسی بیشتر به اینترنت نیاز دارد، نه کمتر»

این اقدام در حالی صورت می‌گیرد که چندین شرکت فناوری دیگر روابط خود را با روسیه قطع کرده‌اند و بسیاری از آنها به نگرانی در مورد نقض تحریم‌های غرب اشاره می‌کنند. دو منبع امنیتی گفتند که Cloudflare می گوید که مشتریان جدید روسی را قبول نمی کند. یک سخنگو گفت که این شرکت در حال بررسی روابط موجود خود به صورت موردی است.

در اخبار دیگر Cloudflare - همراه با CrowdStrike و Ping Identity - برنامه‌ای را برای اعطای چهار ماه از خدمات خود به بیمارستان‌های ایالات متحده و همچنین تاسیسات برق و آب اعلام کرد.

هدف افزایش حفاظت از امنیت سایبری برای آسیب‌پذیرترین بخش‌هایی است که برای زندگی روزمره حیاتی هستند. متیو پرنس، مدیرعامل کلودفلر گفت: «در حال حاضر فقط بیمارستان ها تحت خدمات ما هستند. ما این فهرست را با مشورت با کارشناسان صنعت و دولت تهیه کردیم تا از آسیب پذیرترین بخش ها محافظت کنیم. در صورت نیاز ممکن است در آینده به بخش‌های دیگر گسترش پیدا کنیم.»

ICDT.IR