گزارش

مجمع ایرانی دفاع از حقیقت

Iranian Council For
Defending The Truth

مرداد ۱۴۰۰

امنیت سایبـــــری


بسم الله الرحمن الرحیم

فهرست

Iranian Council For
Defending The Truth

پیشگفتار

۱

پیشگفتار

مجمع ایران 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 سوءتفاهم ها 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

گزارش این هفته در چهار دسته کلی امنیت سایبر امریکا، شبکه‌های اجتماعی، فضای مجازی بین الملل و ناامنی سایبری اخبار این حوزه را پوشش داده است. برخلاف هفته‌های قبلی که حملات سایبری و نقض قوانین فضای سایبر سر و صدای گسترده‌ای به پا می‌نمود، هفته گذشته به آرامی سپری شد و کارشناسان فرصت یافتند تا نتایج بررسی‌های تخصصی و عیب‌یابی‌هایشان را منتشر کنند. برگزاری کنفرانس بزرگ امنیت‌سایبر Black Hat در امریکا یکی از مهم‌ترین رویدادهای این حوزه بود.

Iranian Council For
Defending The Truth

اخبار

۳

امنیت سایبر آمریکا

گزارش سنا از وضعیت ضعیف حفاظت سایبری دولت آمریکا

در سال ۲۰۱۹ گزارشی از مجلس سنا خطاهای امنیت سایبری خطرناک در ۸ سازمان دولتی را نشان داد؛ از جمله اشکالات رایانه‌ای تعمیر نشده و اطلاعات شخصی شهروندان که در معرض خطر هک قرار دارند. با وجود گذشت دو سال از آن گزارش ولی اوضاع هنوز بهبود چندانی نیافته است.

در به روزرسانی ۲۰۲۱ این گزارش توسط کمیته امنیت داخلی مجلس سنا آمده است که هفت مورد از هشت سازمان یاد شده طی دو سال گذشته حداقل بهسازی‌ها را انجام داده اند. فقط وزارت امنیت داخلی ، که شامل آژانس امنیت سایبری دولتی است ، به طور قابل توجهی بهتر عمل نموده است. این یافته‌ها عمدتاً از گزارشات ناظران داخلی خود آژانس‌ها جمع آوری شده است.

در این گزارش آمده است:«علیرغم سال‌ها هشدار از سوی دولت اما این ادارات آمادگی کافی برای مقاومت در برابر هک های روسیه ، چین و جاهای دیگر را ندارند. از آنجایی که هکرها چه آنهایی که تحت حمایت دولت‌ها هستند و چه سایرین به طور فزاینده‌ای پیچیده و مقاوم شده‌اند ، کنگره و قوه مجریه نمی‌توانند اجازه دهند [اطلاعات هویتی شخصی] و اسرار امنیت ملی همچنان آسیب پذیر باقی بمانند.»

سناتورهای هدایت کننده این بازرسی در نظر دارند تا قبل از پایان سال ۲۰۲۲ قانونی را برای رسیدگی به بسیاری از مشکلات ، از جمله بازنویسی قانون اصلی امنیت سایبری دولت و قانون مدیریت امنیت اطلاعات فدرال ، معرفی کنند.

این گزارش مملو از مثالهای نگران کننده است:

• در حین یک هک تمرینی، محققان توانستند به صدها سند حاوی اطلاعات شخصی افراد از وزارت آموزش و پرورش ، از جمله ۲۰۰ شماره کارت اعتباری دسترسی پیدا کنند. کارکنان بخش فناوری اطلاعات آنها را مسدود نکرده و حتی متوجه آن نشده اند.

• اداره تأمین اجتماعی به اندازه کافی از اطلاعات شخصی افراد محافظت نمی‌کرد و هنوز الزامات امنیت رایانه‌ای را که در سال ۲۰۱۵ مقرر شده بود، اجرا نکرده بود.

• هـزاران شـاهد مثـال وجـود داشـت کـه در آن کارکنـان وزارت امـور خارجـه، ایـن سـازمان را بـرای مـدت زمـان زیـادی تـرک کـرده بودنـد ، امـا ایـن وزارتخانـه حسـاب‌های دیجیتالـی آنهـا را غیرفعـال نکـرده بـود - برخـی از آنهـا بـه اطلاعـات طبقـه بنـدی شـده دسترسـی داشـتند. آن حسـاب‌های فعـال امـا بـدون نظـارت می‌تواننـد معـدن طـلا بـرای هکرهایـی باشـد کـه سـعی مـی کننـد بـه سیسـتم‌ها و اطلاعـات رایانـه‌ای دسترسـی مخفـی داشـته باشـند.

• بـازرس کل وزارت حمـل و نقـل نزدیـک بـه ۱۵۰۰۰ دسـتگاه IT، از جملـه بیـش از ۷۰۰۰ تلفـن را پیـدا کـرد کـه توسـط کارکنـان و پیمانـکاران مـورد اسـتفاده قـرار می‌گرفـت و ایـن اداره هیـچ بایگانـی و مدرکـی در مـورد آنهـا نداشـت.

ایـن گزارش همچنین مشـکلات امنیت سـایبری اساسـی و بی‌شـماری از جملـه عـدم موفقیـت سـازمان‌ها در رمزنـگاری داده‌هـا ، عـدم الـزام کارکنـان به تأییـد هویت خـود بـه روش‌هـای ترکیبـی در هنـگام دسترسـی بـه حسـاب‌های حسـاس و جلوگیـری از دسترسـی کارکنـان بـه داده‌هایـی کـه هیـچ کاربـردی ندارنـد را شناسـایی نمـوده اسـت.

روابط میان دولت امریکا با گروهی از هکرها

در کشور امریکا، دولت به منظور یافتن باگ‌ها و اشکالات سایبری با برخی از هکرها همکاری می‌کند. این هکرها در ادبیات رسانه‌ای به آنها هکرهای اخلاقی گفته می‌شود. به عبارتی یک هکر اخلاقی ، که به آن هکر کلاه سفید نیز گفته می‌شود ، یک متخصص امنیت اطلاعات (infosec) است که از طرف صاحبان سازمان‌ها و با مجوز آنها به یک سیستم رایانه‌ای ، شبکه ، نرم‌افزار یا سایر منابع کامپیوتری آنها نفوذ می‌کند.

کارشناسان سایبری در مورد اینکه آیا روابط پیچیده بین دولت ایالات متحده و هکرهای اخلاقی در دو سال گذشته بهبود یافته است اختلاف نظر دارند.

طی آن سال‌ها مجموعه‌ای از برنامه‌ها اجرایی گردید که از هکرهای اخلاقی برای جستجوی اشکالات در سیستم‌های رایانه‌ای دولتی دعوت می‌کرد و هم چنین حکم فوت العاده‌ای از سوی دادگاه عالی تعیین می‌نمود که دادستان‌ها چه موقع می‌توانند علیه محققان امنیتی که "شرایط خدمات محصولات فناوری" را نقض نموده اند، تشکیل پرونده قضایی دهند.

به گفته کارشناسان استقبال دونالد ترامپ از نظریه های توطئه مربوط به امنیت سایبری ، تقلب در انتخابات و سایر موضوعات باعث بدبینی گسترده به جامعه هکرها شد. پل روزنزویگ ، یکی از مقامات وزارت امنیت داخلی در دولت جورج دبلیو بوش که اکنون "موسسه مشاوره شاخه سرخ" را اداره می کند ، می گوید: "به طور کلی ، این روزها به دولت کمتر اعتماد می شود." "احساس من این است که روابط اکنون ضعیف تر است ، نه قوی تر."

این رابطه در سال ۲۰۱۳ پس از افشاگری های ادوارد اسنودن در مورد جاسوسی گسترده آژانس امنیت ملی به سطح پایینی رسید؛ اما به تدریج روابط میان دو طرف ترمیم شد. به گفته کارشناسان علت این امر به درک متقابل بین دولت و متخصصان بیرونی بر می‌گردد مبنی بر این که هر دوی آنها به این باور رسیده اند که برای محافظت از کشور در برابر حملات سایبری ضروری هستند.

نماینده جیم لانگوین ، یکی از بنیانگذاران گروه امنیت سایبری کنگره ، گفت:«کشور ما به همه کمک‌هایی که می‌توانیم برای بهبود دفاع سایبری خود داشته باشیم نیاز دارد. امیدوارم دولت ایالات متحده به یافتن راه هایی برای همکاری با جامعه هک اخلاقی ادامه دهد تا از مهارت‌های آنها استفاده کرده و اینترنت را به مکانی امن‌تر تبدیل کند.»

بسیاری از کسانی که می گویند روابط با دولت بهبود نیافته است بیشتر تقصیرها را بر گردن ترامپ می اندازند. جف ماس ، بنیانگذار کنفرانس های Def Con و Black Hat گفت:« سوء استفاده های دولت قبلی حیثیت بسیاری از آژانس هایی را [که] هکرها با آنها همکاری می نمودند مانند DOJ ، FBI و DHS لکه دار نمود. محققان می‌خواهند بدانند که از کار آنها سوء استفاده نمی‌شود. ... زمان می‌برد تا دولت جدید بتواند با شفافیت و مسئولیت پذیری بیشتر این اعتماد را جبران کند.»

تعیین مقررات برای ارزهای دیجیتال

گری جنسلر ، رئیس کمیسیون بورس و اوراق بهادار گفت: در پی افزایش باج افزارها تعیین مقررات برای ارزهای رمزپایه لازم است.

جنسلر از تنظیم کننده‌های مقررات برای اوراق بهادار تقاضا نموده است "از همه اقتدارشان در هر جایی که می‌توانند" در مورد ارزهای رمزنگاری شده استفاده کنند. جنسلر طی سخنرانی خود، حمایت از سرمایه گذاران ارزهای رمزنگاری شده را با "غرب وحشی" مقایسه کرد. او گفت که ارزهای رمزنگاری شده بیشتر برای نقض قوانین و اخاذی از قربانیان باج افزارها استفاده می شوند تا ابزاری برای تبادل مالی.

قانونگذاران و مقامات ارشد دولت بایدن به دنبال این هستند که استفاده هکرهای باج افزار از ارزهای رمزنگاری شده برای اخاذی قربانیان سخت‌تر شود. در همین راستا، کاخ سفید به یک استاندارد بین المللی برای گزارش معاملات مشکوک و بزرگ احتیاج دارد. گری پیترز ، رئیس کمیته امنیت داخلی سنای آمریکا نیز در حال بررسی استفاده از ارزهای رمزنگاری شده در طرح‌های باج افزار است.


You
Tube

شبکه‌های اجتماعی

طرفداران داعش با تبلیغات گسترده به شبکه‌های اجتماعی حامی ترامپ هجوم آوردند

GETTR ، پلتفرم جدیدی است که توسط اعضای حلقه نزدیک رئیس جمهور سابق راه اندازی گردید و در حال حاضر مملو از فیلم های سربریدن و محتواهای خشن و افراطی شده است.

بر اساس بررسی POLITICO از فعالیت‌های آنلاین در این پلتفرم نوپا ، تنها چند هفته پس از راه اندازی این شبکه اجتماعی حامی ترامپ، GETTR غرق در تبلیغات تروریستی توسط حامیان داعش شده است.

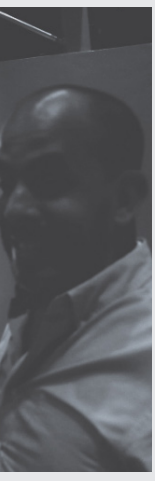
این شبکه اجتماعی مجموعه‌ای از مطالب مرتبط با تروریست‌های داعش را به طور واضح نشان می‌دهد ، از جمله فیلم‌های گرافیکی سر بریدن ، میم های وایرال خشونت‌آمیز و همین طور میم های یک جنگ جو اعدام کننده ترامپ با یک لباس نارنجی مشابه آنچه در گوانتانامو استفاده می شد.

تکثیر سریع چنین مطالبی، GETTR را در موقعیت ناخوشایندی به دلیل ایجاد پناهگاهی امن برای افراط گرایان جهادی به صورت آنلاین قرار داده ، زیرا این پلتفرم تلاش می‌کند خود را به عنوان گزینه جایگزین سایت‌هایی مانند فیس‌بوک و توییتر برای MAGAها معرفی کند که حافظ آزادی بیان است.

این امر بر چالش‌های پیش روی ترامپ و پیروانش در پی ممنوعیت حضور وی در شبکه‌های اجتماعی اصلی پس از شورش‌های ۶ ژانویه در کاپیتول هیل تأکید می‌کند.

چند روز پس از راه اندازی GETTR در ۱ ژوئیه ، حامیان داعش از پیروان خود در سایر شبکه‌های اجتماعی خواستند تا در شبکه حامی ترامپ ثبت نام کنند ، با این انگیزه که "مستقیماً با ملت MAGA " مبارزه کنند .

سرانجام برخی از پست‌های جهادی‌ها در GETTR از اوایل ژوئیه حذف شدند و مشخص شد که پلتفرم حامی ترامپ حداقل برخی اقدامات را برای حذف مواد مضر انجام می‌دهد.



سناتورها خواهان توضیح فیس‌بوک درباره نحوه تأثیر محصولاتش بر سلامت روانی کودکان شدند

دو قانونگذار برجسته از هیئت حمایت از حقوق مصرف کنندگان در کمیته تجارت سنا می گویند فیس بوک باید تحقیقات داخلی در مورد نحوه تأثیرگذاری سیستم عامل ها و محصولاتش بر کاربران جوان را تحویل دهد. رئیس کمیته فرعی ، سناتور ریچارد بلومنتال و مارشا بلکبرن ، جمهوری خواه ارشد این هیئت ، در نامه‌ای به مارک زاکربرگ ، مدیرعامل فیس‌بوک گفتند که آنها "نگرانی های جدی" در مورد اینستاگرام ویژه کودکان دارند.

قانونگذاران دو هفته به فیس بوک مهلت دادند تا داده ها را به اشتراک بگذارند. آنها همچنین تقاضا نمودند فیس بوک یک "مدیر ارشد" را در اختیار داشته باشد تا در جلسه سپتامبر در این مورد شهادت دهد.

استفانی اوتوی ، سخنگوی فیس بوک در بیانیه‌ای گفت:« ما از همکاری سازنده با سناتورها بلومنتال و بلکبرن برای حفظ امنیت جوانان در اینترنت استقبال می‌کنیم.» اوتوی گفت:« برای افراد زیر ۱۳ سال ، واقعیت این است که آنها از قبل در فضای مجازی حاضر هستند ، بنابراین ما برای آنها تجربه‌ای متناسب سن شان را مهیا می‌کنیم که توسط والدین مدیریت می‌شود.»

برنامه‌های این شرکت برای راه اندازی اینستاگرام مخصوص کودکان نیز با بررسی دادستان‌های کل کشور روبرو شده است ، آنها در نامه‌ای در ماه مه به زاکربرگ نوشتند که چنین پلتفرمی مضر خواهد بود. این شرکت می‌گوید این پلتفرم به والدین کنترل‌های بیشتری می‌دهد و تبلیغات را برای کودکان زیر ۱۳ سال نشان نمی‌دهد.

پروپاگاندای روسیه، واکسن‌ها و دولت بایدن را هدف قرار می‌دهد

شرکت Graphika که کمپین های نشر اطلاعات غلط را در اینترنت ردیابی می‌کند، در یکی از تالارهای گفت‌وگو جناح راست کاریکاتوری را یافته که دولت بایدن-هریس را متهم به واکسیناسیون اجباری می‌کند و از این طریق در تلاش است تا فرایند ایمن‌سازی مردم را تضعیف نماید.

نیویورک تایمز گزارش می‌دهد بنا به گفته "مرکز مشارکت جهانی وزارت خارجه امریکا" ، کشورهای روسیه و چین برای تبلیغ واکسن های خود از پیام هایی که برنامه های واکسیناسیون آمریکایی و اروپایی را تضعیف می‌کند ، استفاده کرده اند. اما مسکو علاوه بر پیام‌های بازگانی واضح برای تبلیغ واکسن های خود ، نظریه‌های توطئه را نیز گسترش داده است. سال گذشته ، این وزارتخانه درباره نحوه استفاده روسیه از وب‌سایت‌های حاشیه‌دار برای ترویج تردید در مورد واکسیناسیون هشدار داد.

به گفته مقامات دولتی امریکا و کارشناسان خارجی، تعیین میزان اطلاعات غلطی که در هر زمان توسط روس‌ها یا دیگر قدرت های متخاصم تولید می‌شود دشوار است. به گفته کارشناسان، ظهور نوع دلتا ویروس کرونا - و تغییر توصیه های علمی در مورد نحوه دفاع در برابر یک نوع عفونی و نیاز به شات‌های تقویت کننده یا ماسک - فضایی را ایجاد کرده است که اطلاعات غلط به راحتی نشر می‌یابد.

لیزا کاپلان ، مدیر اجرایی گروه Alethea ، که به شرکت‌ها در برابر اطلاعات غلط کمک می‌کند، می‌گوید: "اطلاعات غلط در خلاء اطلاعات رشد می‌کند." "در آن زمان است که اطلاعات غلط واقعاً می‌تواند جا بیفتد. و چون می‌دانم که روس‌ها معمولاً در چنین موقعیت‌هایی چگونه نقش‌آفرینی می‌کنند ، تعجب نمی‌کنم که آنها سعی کنند از این موقعیت استفاده ببرند. "

مقامات وزارت خارجه ایالات متحده این هفته گفتند که کمپین‌های نشردهنده اطلاعات گمراه کننده روسی و چینی تلاش کرده‌اند تا عوارض جانبی احتمالی واکسن‌های Pfizer و Moderna را بزرگنمایی کنند و نشان دهند که فناوری mRNA آزمایش نشده یا خطرناک است.

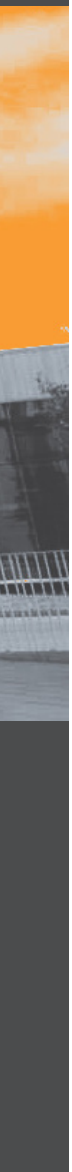
به گفته برخی مقامات و کارشناسان خارجی ، در هفته‌های اخیر ماهیت کمپین‌های نشر اطلاعات نادرستِ روسیه نیز تغییر کرده است. پست‌های اخیر که اطلاعات نادرست را منتشر می‌کنند نشان می‌دهد که دولت بایدن قصد دارد آمریکایی‌ها را مجبور به دریافت واکسنهایی کند که در برابر ویروس کرونا شکست می‌خورند.

با توجه به اختلافات عمیق بر سر واکسیناسیون که قبلاً در ایالات متحده و اروپا وجود داشت، سنجش تأثیر کمپین‌های مروج اطلاعات نادرست دشوار است. سوء استفاده از شکاف بین آمریکاییها یک تاکتیک معمولی روسیه است. حتی در تالارهای گفتگوی افراطی راست گرا، برخی از کاربران منشأ روسی کاریکاتورهای مسخره کننده دولت بایدن را متوجه شده اند؛ هرچند انتشار پست ها همچنان ادامه دارد.

تنها نحوه پیام رسانی روس‌ها در سایت‌های راست افراطی تغییر نکرده است. موسسه "اتحاد برای تأمین دموکراسی"، یک گروه غیرانتفاعی متمرکز بر نشر اطلاعات غلط، متوجه تغییر در آنچه رسانه‌های دولتی روسیه تولید کرده‌اند نیز شده ا ست .

پیش از این، انجمن هایی مانند RT (یک شبکه انگلیسی زبان تحت حمایت کرملین) بر تبلیغ واکسن روسیه و تحقیر واکسن‌های غربی متمرکز بودند. برت شفر ، کارشناس اطلاعات غلط در موسسه "اتحاد برای تأمین دموکراسی" گفت: اما اخیراً ، رسانه های دولتی روسیه "واقعاً به بحث‌های جنگ فرهنگی در مورد واکسن و دستور ماسک متمایل شده اند.

فضای مجازی بین‌الملل



پکن در واکنش به تحریم هوآوی توسط غربی‌ها، شرکت‌های اریکسون و نوکیا را محدود می‌کند

ایالات متحده و بسیاری از متحدانش استفاده از تجهیزات سلولی تلفن همراه ۵G ساخته شده توسط شرکت Huawei را محدود کرده اند. پکن نیز در واکنش به این اقدام قصد دارد تا همین کار را با رقبای غربی هواوی انجام دهد. در این راستا، شرکت "مخابرات بی‌سیم چین" فروش تجهیزات به هواوی را افزایش داده و در مقابل تجارت با اریکسون سوئد را کاهش خواهد داد.

یک رسانه دولتی در چین از دست دادن سهم بازار اریکسون را تلافی تصمیم سوئد مبنی بر ممنوعیت شرکت هواوی و ZTE Corp. چین از شبکه‌های ۵G خود دانست.

فضای محتوایی وب را می‌توان به طور کلی به دو جهان مجزا تحت رهبری چین و آمریکا تقسیم نمود. همین دسته‌بندی نیز در مورد زیرساخت‌های وب صادق است. بازار ۳۵ میلیارد دلاری جهانی تجهیزات سلولی را می‌توان به سه بخش تقریباً مساوی تقسیم کرد: چین ، ایالات متحده و بقیه جهان. چین اساساً به تجهیزات داخلی متکی است. ایالات متحده هم عملاً هواوی ، بزرگترین سازنده تجهیزات تلفن همراه در جهان را به دلیل نگرانی‌هایی مبنی بر اینکه پکن از این شرکت برای جاسوسی استفاده می‌کند ، از شبکه‌های بزرگ نت منع نموده است. شرکت هوآوی و چین این اتهامات را بی‌اساس دانسته اند.

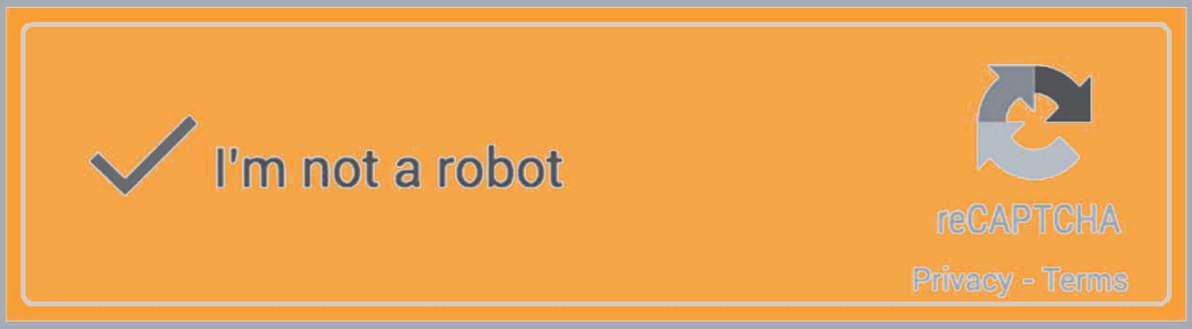
بخش بزرگی از بقیه جهان از رهبری واشنگتن در فضای سایبر پیروی می‌کنند البته استثنائات بزرگی مانند آلمان نیز وجود دارد. به گفته شرکت تحقیقاتی Dell'Oro Group ، کشورهایی که محدودیت‌هایی را علیه هواوی وضع کرده اند یا در نظر دارند تا وضع کنند، بیش از ۶۰ درصد بازار تجهیزات تلفن همراه جهان را تشکیل می‌دهند.

سیمون لئوپولد ، تحلیلگر مخابرات در موسسه ریموند جیمز می گوید: "با توجه به مسیر فعلی ، به نظر می رسد صنعت مخابرات بین شرق و غرب قطبی تر شده است."

در سال ۲۰۲۰ ، سوئد فراتر از همتایان اروپایی‌اش به طور صریح هواوی و ZTE را از تأمین شبکه های ۵G خود تحریم کرد. سایر کشورهای اروپایی شرکت های چینی را بدون نام بردن محدودیت‌هایی برایشان وضع نموده اند. مقامات چینی به این کشور منطقه اسکاندیناوی هشدار دادند که می‌توانند به واسطه اریکسون تصمیم سوئد را تلافی نمایند.


ERICSSON
Ericsson Group
Headquarters

ناامنی سایبری


I'm not a robot
reCAPTCHA
Privacy - Terms

هکرها از اصول فنی CAPTCHA برای کلاهبرداری از کاربران ایمیل استفاده می‌کنند

گزارش جدید شرکت امنیتی Proofpoint نشان می دهد که کاربران ایمیل بیشتری در سال ۲۰۲۰ دچار کلاهبرداری با استفاده از فناوری CAPTCHA شدند.

این تکنیک که از یک پازل بصری برای کمک به تأیید صحت رفتار انسان استفاده می‌کند ، در سال ۲۰۲۰ در مقایسه با سال ۲۰۱۹ ، پنجاه برابر بیشتر کلیک دریافت کرد. محققان خاطرنشان نمودند که این هنوز تنها ۵ درصد نرخ پاسخ کلی است. در مقام مقایسه، از هر پنج کاربر، یک نفر بر روی ایمیل‌های پیوست‌داری که بدافزارها را به صورت پاورپوینت مایکروسافت یا صفحات گسترده Ex-cel پنهان می‌کنند کلیک کرده‌اند. کمپین‌هایی که از فایل‌های ضمیمه برای مخفی کردن بدافزارها استفاده می‌کنند، یکی از هر چهار حمله سایبری را تشکیل می دادند که توسط محققان Proofpoint زیر نظر قرار گرفتند.

محققان دریافتند که کمیت همچنان در حملات ایمیل به کیفیت کمک می‌کند. Proofpoint دریافت که بیشترین تعداد کلیک از طرف یک عامل تهدید، مرتبط با بات نت Emotet بوده است. در این گزارش آمده است: "این آمار نشان دهنده اثربخشی آنها و حجم زیاد ایمیل‌هایی است که در هر کمپین ارسال کرده اند."

محققان امنیت سایبری همچنین می‌گویند که شرکت‌ها نباید اصول اولیه سایبری را در مبارزه با باج افزار دست کم بگیرند. هکرها برای توزیع بدافزار اصلی و اولیه که بعداً برای بارگیری باج افزارها استفاده می شود به ایمیل روی خواهند آورد، به جای این که از ایمیل‌های فیشینگ به عنوان مسیر حملات آغازین استفاده نمایند. در سال ۲۰۲۰، Proofpoint چهل و هشت (۴۸) میلیون ایمیل را شناسایی کرد که حاوی بدافزارهایی بود که برای راه اندازی باج افزار استفاده می شد. تهدیدهای اصلی شناسایی شده توسط Proofpoint شامل نام هایی مانند Dridex ، The Trick و Qbot بود.

ICDT.IR