گزارش

مجمع ایرانی دفاع از حقیقت

Iranian Council For
Defending The Truth

بهمن 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

این شماره از گزارش امنیت سایبری ICDT، طبق روال سابق سعی نموده تا گزارش خود را متنوع‌تر و تحلیلی‌تر از قبل نماید. به همین جهت موضوعات گسترده‌تری در این شماره پوشش داده شده است. گزارش این هفته امنیت سایبری تحت عناوین: ایالات متحده، اوکراین، ناامنی سایبری، پگاسوس و فناوری‌های نوین فراهم شده است.

حملات سایبری در چند هفته اخیر مجدداً فزونی یافته است. برخی از آنها ناشی از بحران اوکراین و درگیری روسیه با ناتو می‌باشد و بخشی دیگر حملات باندهای خلافکار هکری غیردولتی هستند که اقدام به باج‌گیری می‌کنند. طی چند ماه اخیر گروه‌های هکری، صرافی‌های ارزهای دیجیتال را مورد توجه قرار داده و آنها را به آسانی هدف گرفته و مبالغ گزافی را به جیب زده‌اند.

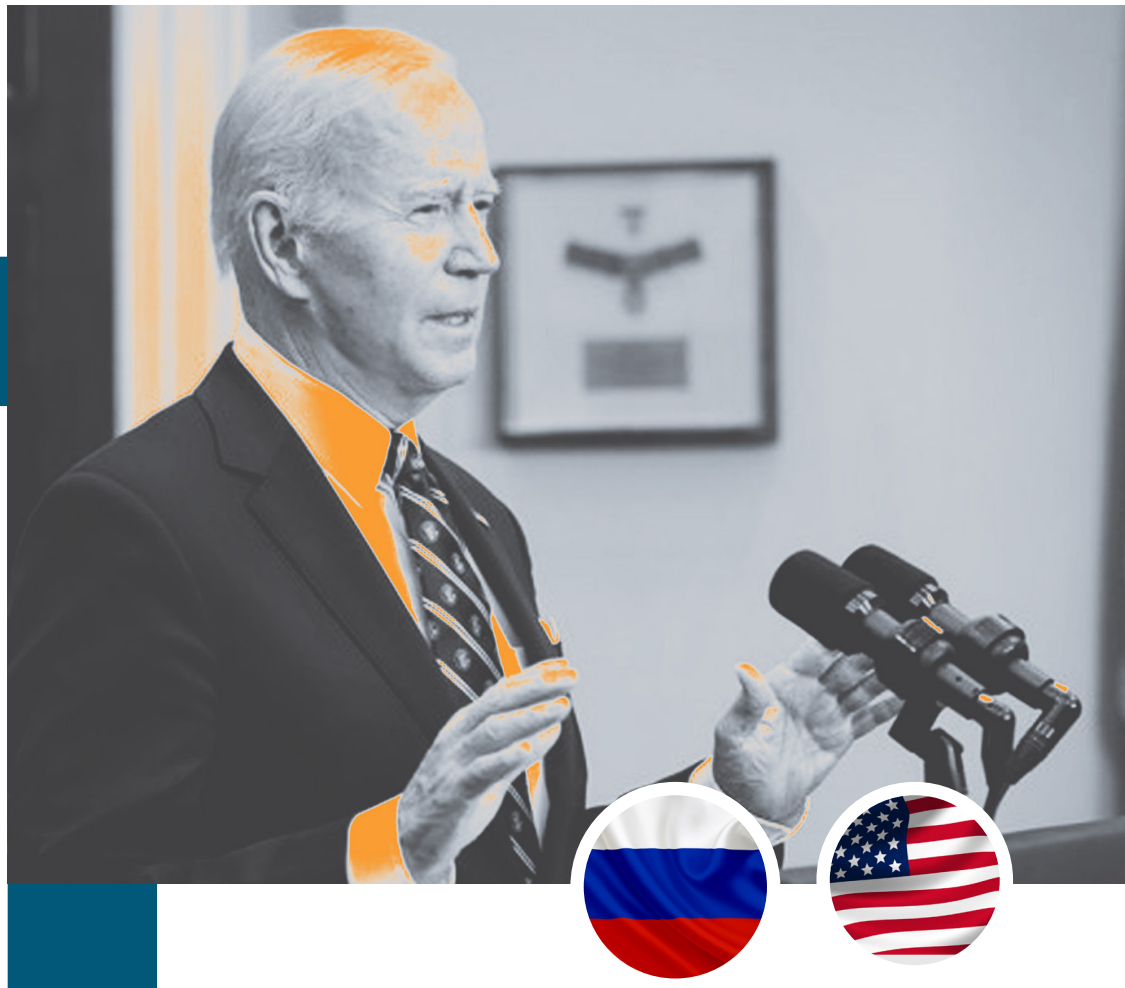
اخبار به کارگیری جاسوس‌افزار پگاسوس توسط دولت‌های مختلف از جمله اسرائیل و مجارستان در مدت اخیر مجدداً مطرح و مورد بررسی قرار گرفت.

Iranian Council For
Defending The Truth

اخبار

۳

ایالات متحده



دولت بایدن در حال بررسی تحریم هایی با هدف فلج کردن بخش فناوری روسیه است

هدف این است که در صورت حمله روسیه به اوکراین، جریان نیمه هادی ها و سایر اجزای حیاتی به صنایع پیشرفته مانند هوش مصنوعی و محاسبات کوانتومی قطع شود.

دولت ایالات متحده تنها یک بار قبلاً چنین کنترل صادرات گسترده ای را اعمال کرده است، زمانی که غول فناوری چینی هوآوی را به اتهام کمک به جاسوسی چین هدف قرار داد. به گفته تحلیلگران، در سال گذشته در اثر این تحریم‌ها برای اولین مرتبه درآمد شرکت هواوی تنزل یافت.

این تحریم ها به دنبال آن است که شرکت های خارجی را از صادرات تکنولوژی و فناوری به روسیه در صورت اتکا به قطعات آمریکایی منع کند. این حرکت بسیار قدرتمندی است زیرا "کمتر نیمه هادی روی کره زمین وجود دارد که با ابزارهای ایالات متحده ساخته نشده یا با نرم افزار ایالات متحده طراحی نشده باشد."

این اقدام می‌تواند با بادهای مخالفی از جانب منافع تجاری آمریکایی ها و اروپاییان مواجه شود چرا که آنها می ترسند از این که به کارگیری کنترل‌های صادراتی منجر به اقدامات تلافی جویانه روسیه در حوزه‌های دیگر شود - و در نهایت باعث شود شرکت‌های خارجی به دنبال طرح خارج نمودن فناوری ایالات متحده از محصولات خود باشند.

استفاده هدفمند از کنترل‌های صادراتی می‌تواند به ارتش روسیه که از یک تراشه طراحی داخل به نام Elbrus که توسط TSMC در تایوان تولید می‌شود، ضربه بزند. کوستاس تیگوس، کارشناس الکترونیکی در ارائه‌دهنده اطلاعات دفاعی گروه جینز، می‌گوید:« اگر دولت ایالات متحده TSMC را با موفقیت، همان طور که در تامین هوآوی محدود کرد، از تامین این تراشه‌ها برای روسیه منع کند "اثر مخربی" بر روسیه خواهد گذاشت.»

نظر کارشناسان سایبری امریکا در مورد اولویت تهدید خارجی: اول روسیه بعد چین

طبق آخرین نظرسنجی واشنگتن پست از یک گروه کارشناسان امنیت سایبری، کارشناسان تقریباً به طور مساوی در مورد اینکه آیا چین یا روسیه خطرناک‌ترین دشمن سایبری ایالات متحده هستند تقسیم شده‌اند.

نتیجه نظرسنجی منعکس کننده یک دهه حملات به شدت مخرب هر دو کشور است، از جمله دزدی چین از اطلاعات سری شرکتها که میلیاردها دلار را از اقتصاد ایالات متحده ربوده و هک های مورد حمایت کرملین که ارزش های سیاسی امریکا را تضعیف نموده و گنجینه های اسرار دولت را به خطر انداخته است.

جزئیات:

• از ۹۶ پاسخ دهنده، ۴۰ نفر روسیه را به عنوان تهدید بزرگ توصیف کردند در حالی که ۳۹ نفر چین را در آن موقعیت قرار دادند.

• بقیه از دشمن دیگری به عنوان تهدید اصلی نام بردند - از جمله تعداد زیادی ایالات متحده را بدترین دشمن خود در فضای سایبری معرفی نموده اند.

بسیاری از کارشناسان روسیه را به‌عنوان تهدید کوتاه‌مدت بسیار خطرناک‌تر توصیف کردند، اما هشدار دادند که رقابت سایبری چین در بلندمدت هراسناک‌تر است.

کیتی نیکلز، مدیر اطلاعاتی شرکت امنیت سایبری Red Canary، گفت: «وقتی خطر به عنوان داشتن بیشترین پتانسیل برای آسیب رساندن به افراد و سازمان‌ها در ایالات متحده تعریف شود، پاسخ روسیه است. اما اگر عامل خطرناک به صورت دارنده بیشترین پتانسیل جهت تهدید نقش استراتژیک ایالات متحده به عنوان یک قدرت بزرگ پایدار تعریف شود، پاسخ چین است.»

مایکل دانیل، مدیر سایبری کاخ سفید در دوران دولت اوباما، به کمک یک قیاس پاسخ داد: "روسیه همانند یک طوفان است، در حالی که چین مانند تغییرات آب و هوایی (تدریجی) است.

به عبارت دیگر، روسیه می‌تواند آسیب‌های ناگهانی و غیرقابل پیش‌بینی ایجاد کند، اما چین یک تهدید استراتژیک بلندمدت است."

برای کارشناسانی که چین را بزرگ‌ترین تهدید می‌دانستند، اظهارنظر رایج این بود که رهبران چینی سرقت و هک داده‌های دیجیتال را ابزاری برای رسیدن به موقعیت ابرقدرت جهانی می‌دانند.

نورما کرایم، کارشناس سیاست سایبری در Van Scoyoc Associates گفت:« [چین] یک برنامه ۱۰۰ ساله برای ابرقدرت شدن دارد. امنیت سایبری ساده‌ترین و موذی‌ترین ابزار برای دستیابی به این هدف است.»

ساموئل ویسنر، یکی از همکاران فناوری در شرکت میتر، می‌گوید: «چین از فضای سایبر به عنوان ابزاری برای تغییر شکل نظام بین‌الملل مطابق با ایدئولوژی و منافع و دیدگاه جهانی خود استفاده می‌کند.»

کارشناسانی که می‌گفتند روسیه تهدید بزرگ‌تر است، هشدار دادند که این کشور تمایل بیشتری به ریسک‌پذیری و عبور از خطوط قرمز در فضای سایبری دارد - نظیر دخالت این کشور در انتخابات ۲۰۱۶.

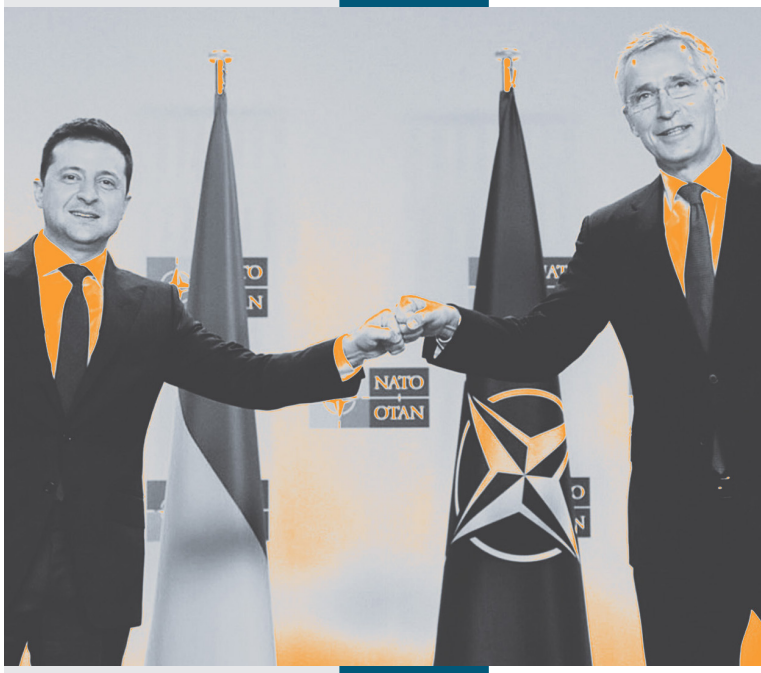
جوزفین وولف، استادیار سیاست امنیت سایبری در دانشکده حقوق و دیپلماسی فلچر در دانشگاه تافتس، گفت: «روسیه در آنچه در فضای سایبری تلاش می‌کند جسورترین - یا به عبارت دیگر، بی‌ملاحظه‌ترین - است و به نظر کمترین ترس از پیامدهای مخرب را دارد.»

چندین کارشناس نیز اظهار داشتند : به استناد حفاظت های ضعیف و مقررات قدیمی که کشور را در برابر حملات آسیب پذیرتر می کند، ایالات متحده در واقع بدترین دشمن خود در فضای سایبری است.

الیزابت وارتون، معاون عملیات در شرکت امنیت سایبری SCYTHE، گفت: «تلاطم فعلی سیاست‌های قانونی و مقررات منسوخ، تهدید داخلی بزرگتری برای امنیت سایبری کارآمد در ایالات متحده نسبت به یک دولت دشمن و خارجی است».

اوکراین

ناتو و اوکراین برای همکاری سایبری عمیق تر به توافق رسیدند



ناتو پس از حمله مخرب علیه کیف که بیش از ۷۰ وب سایت دولتی هک شدند، به سرعت با اوکراین قراردادی امضا کرد تا حمایت سایبری خود را تقویت کند. مهاجمین به سیستم‌های رایانه‌ای دولت اوکراین نفوذ کرده بودند و بدافزار مخفی 'wiper' در این حمله نصب شده بود.

به نظر می‌رسد که این بدافزار پیش از آن که کد مخرب خود را در شبکه‌ها آزاد کند، برای ماه‌ها در برخی از سیستم‌ها به طور ساکت و خاموش قرار داده شده بود.

این حملات نگرانی هایی را ایجاد کرده است مبنی بر این که روسیه در حال برنامه‌ریزی برای حمله نظامی است و به گفته وزارت توسعه دیجیتال اوکراین "همه شواهد نشان می دهد که روسیه پشت این حمله سایبری است." کرملین دخالت روسیه را رد کرده است.

نفوذها به شبکه اوکراین زمانی کشف شد که ده‌ها سازمان دولتی به طور ناگهانی در یک کمپین de-facement (تخریب چهره) مورد هدف قرار گرفتند. در این حملات هکرها صفحه اصلی وب حدود ده سایت را با یک پیام سیاسی جایگزین کردند. در همان روزی که خرابی ها رخ داد، مایکروسافت کد پاک کن مخربی را در سیستم تعداد معدودی از نهادها در اوکراین کشف کرد، این کد در سازمان های دولتی و حداقل یک شرکت فناوری اطلاعات وجود داشت که اکنون گمان می رود شرکت توسعه نرم افزار و وب سایت اوکراینی به نام Kitsoft باشد.

ژنرال امنیتی ناتو، ینس استولتنبرگ، گفت که کارشناسان از قبل با اوکراین برای مقابله با این حملات سایبری اخیر کار می کردند.

توافقنامه جدید با اوکراین همکاری سایبری را

افزایش می‌دهد و به اوکراین اجازه دسترسی به پلت فرم اشتراک‌گذاری اطلاعات بدافزاری ناتو را می‌دهد و مشخص می‌کند که در کجا ممکن است به آموزش پرسنل اوکراینی نیاز باشد. حملات سایبری اخیر به اوکراین در حالی رخ داد که تنش‌ها بین مسکو و غرب به دلیل تجمع حدود ۱۰۰۰۰۰ سرباز در مرز که دلالت بر برنامه‌ریزی روسیه برای تهاجم جدید به همسایه خود را دارد، افزایش یافته است. متحدان غربی هشدار داده‌اند که پیش از حمله زمینی به اوکراین ممکن است حمله هکری برای از بین بردن زیرساخت های کلیدی در اوکراین مقدم شود.

مایکروسافت می‌گوید که این بدافزار زمانی که دستگاه آسیب‌دیده خاموش شود، اجرا می‌شود و خود را به‌عنوان باج‌افزار پنهان می‌کند. لکن این بدافزار مکانیسم باجگیری ندارد و به قصد تخریب و غیرفعال کردن دائمی دستگاه‌های هدف در نظر گرفته شده است. مایکروسافت این بدافزار را نوعی پاک‌کننده MBR (Master Boot Record) هارد دیسک شناسایی نموده است.

مسکو و ناتو در گفتگوهای سطح عالی هفته گذشته نتوانستند پیشرفتی برای کاهش تنش بر سر اوکراین داشته باشند. کرملین مجموعه ای از خواسته ها را به ناتو و ایالات متحده ارائه کرده است، از جمله رد عضویت اوکراین در این ائتلاف.

ینس استولتنبرگ، دبیرکل ناتو گفت که کارشناسان ناتو و اعضای آن از قبل در صحنه حضور داشتند و با اوکراین برای مقابله با آخرین حمله سایبری همکاری می کردند. روابط بین ناتو و اوکراین به اوایل دهه ۱۹۹۰ باز می گردد. همکاری آنها در طول زمان عمیق‌تر شده و برای دو طرف نیز سودمند بوده است. اوکراین به طور فعال در عملیات‌ها و مأموریت‌های ناتو مشارکت می‌کند.

نگرانی‌های سایبری به خاطر پیش بینی تهاجم روسیه به اوکراین افزایش یافته است

به سبب بیم از تهاجم روسیه به اوکراین، نگرانی ها در مورد چگونگی وقوع چنین درگیری در فضای سایبری نیز افزایش یافته است.

وزارت امنیت داخلی امریکا ۲۴ ژانویه هشدار داد که به دنبال هجوم روسیه به اوکراین و تشدید ضربات متقابل میان ایالات متحده یا ناتو با روسیه، احتمال انجام حملات سایبری علیه اهداف امریکایی نیز وجود دارد.

این وزارتخانه در اطلاعیه به بخش صنعت و دولت‌های ایالتی و محلی هشدار داد که چنین حملاتی می‌تواند از حملات نسبتاً بی‌ضرری که هدف آنها آسیب به وب‌سایت‌ها باشد تا حملات بسیار جدی‌تر که هدف آنها صدمه به زیرساخت‌های حیاتی مانند فرودگاه‌ها و تأسیسات انرژی است.

این هشدار پس از سلسله حملات سایبری مخرب علیه کامپیوترهای دولتی و صنعتی داخل اوکراین منتشر شد که شباهت هایی به عملیات های قبلی تحت حمایت دولت روسیه داشت. بایدن هشدار داده است که این احتمال وجود دارد ایالات متحده با حملات سایبری تلافی جویانه به حملات سایبری روسیه علیه اوکراین پاسخ دهد.

وزارت امور خارجه ایالات متحده اخیراً به خانواده های دیپلمات ها دستور داد تا سفارت ایالات متحده در پایتخت اوکراین را به دلیل تهدید به اقدام نظامی روسیه ترک کنند.

اگر تهاجمی رخ دهد، هک احتمالا نقش مهمی ایفا می کند. کارشناسان جنگ سایبری سال‌هاست که هشدار می دهند هک نقش برجسته‌تری در درگیری‌های نظامی متعارف بازی خواهد کرد. به عنوان مثال، کشورها ممکن است سیستم های ارتباطاتی و انرژی را هک کنند تا توانایی دشمنان خود را جهت پاسخ نظامی تضعیف نموده یا شهروندان را بترسانند و حمایت سیاسی آنان از دولت را کاهش دهند.

روسیه در تهاجم سال ۲۰۰۸ به گرجستان و حمله به کریمه در سال ۲۰۱۴، حملات سایبری را با عملیات نظامی به هم پیوند زد. روسیه همچنین زمانی که برق هزاران شهروند اوکراینی را در سال ۲۰۱۵ قطع کرد، جدی ترین حمله شناخته شده را علیه یک سیستم انرژی انجام داد.

حملات سایبری روسیه می تواند با هدف افزایش هزینه های سیاسی برای ایالات متحده و متحدان ناتو انجام شود تا احتمال عکس العمل نشان دادن به تهاجم روسیه را کاهش دهد.

تنش ها با حمله سایبری که سیستم های ریلی بلاروس را هدف قرار داد، شدت گرفت

گروه هکتیویست بلاروسی "پارتیزان های سایبری" مسئولیت این حمله را بر عهده گرفت و گفت که هدف ممانعت از حمل و نقل نیروهای روسی و استفاده از خدمات ریلی داخلی این کشور بود. بلاروس متحد مسکو می باشد.

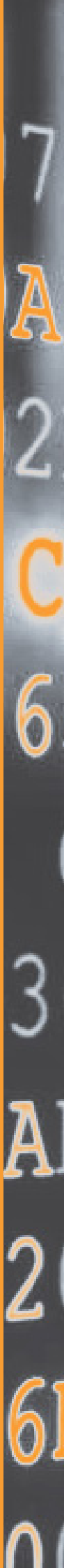
این گروه در توییتی متعهد شد که اگر رهبران دولت مانع از ورود نیروهای روسیه به خاک بلاروس شوند و ۵۰ زندانی سیاسی را آزاد کنند، حمله خود را متوقف خواهد کرد.

به نظر می رسد هک پارتیزان های سایبری به طور ناخواسته فروش بلیط‌های قطار را نیز مختل کرده است. این گروه گفته است قصد ایجاد اختلال در خدمات مسافربری عادی را ندارد و در تلاش است تا این مشکل را برطرف کند.

اگرچه به ظاهر خطای جزئی رخ داده اما این خطا نشان می دهد که چگونه اشتباهات در عملیاتهای سایبری می تواند منجر به عواقب شدید و ناخواسته شود - اتفاقی که می تواند شدیداً در طول یک درگیری نظامی داغ، آسیب‌زا باشد ؛ به خصوص زمانی که دیگر بعید به نظر می رسد دشمنان حرف یکدیگر را در مورد غیرتعمدی بودن حادثه قبول کنند.


Data Breach
yber Attack
System Safety

ناامنی سایبری

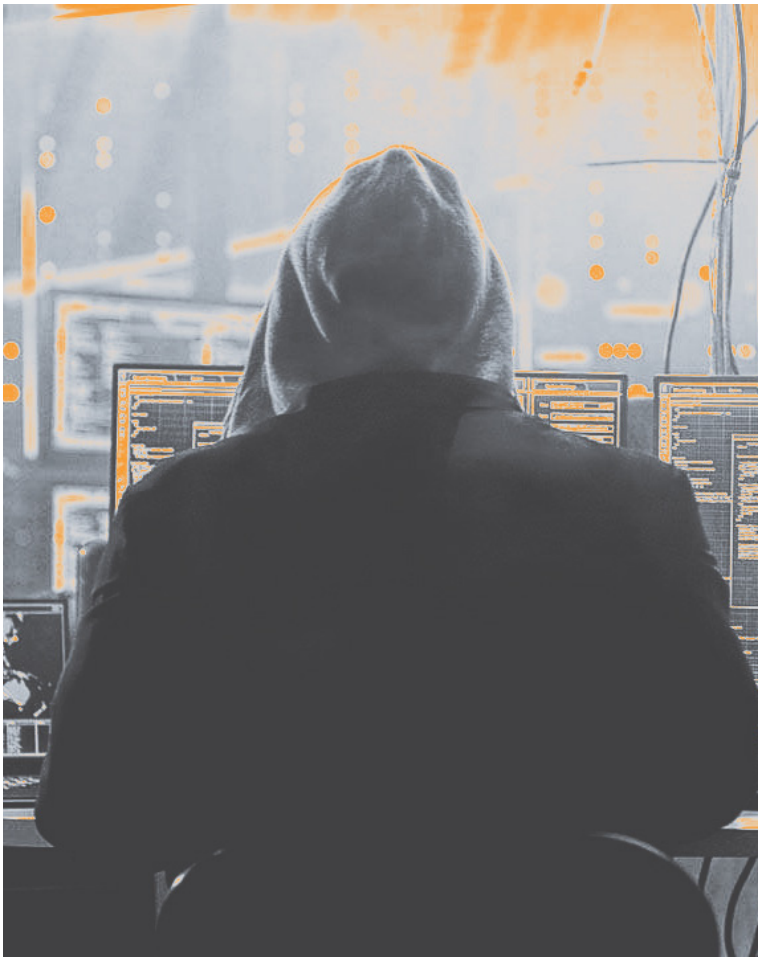


هکرها اطلاعات حساس بیش از ۵۰۰۰۰۰ نفر را از کمیته بین المللی صلیب سرخ سرقت کردند

کمیته بین المللی صلیب سرخ (ICRC) گفت که قربانیان شامل "بیش از ۵۱۵۰۰۰ نفر، از جمله افرادی که به دلیل درگیری، مهاجرت و بلایای طبیعی از خانواده های خود جدا شده اند، افراد ناپدید شده و خانوادههای آنها، و افراد در حبس می باشند."

این گروه بشردوستانه از هکرها درخواست کرد که "کار درست را انجام دهند" و "این داده ها را به اشتراک نگذارند، نفروشند، افشا نکنند و یا از آنها استفاده دیگری نکنند."

کمیته بین‌المللی صلیب سرخ هیچ نشانه‌ای مبنی بر اینکه چه کسی این حمله سایبری را انجام داده است، ندارد. "هنوز هیچ نشانه ای مبنی بر افشای اطلاعات به خطر افتاده یا به اشتراک گذاری عمومی وجود ندارد."



تأیید حمله هکری کره شمالی به کاربران از طریق آپدیت ویندوز!

ظاهراً هکرهای کره شمالی موفق شده‌اند با استفاده از سرویس آپدیت ویندوز و سرورهای گیت‌هاب به روش جدیدی برای نفوذ به سیستم کارمندان سازمان‌ها و ادارات دست یابند.

بر اساس اعلام شرکت امنیتی Malwarebytes، یک گروه از هکرهای کره شمالی از سرویس آپدیت ویندوز برای استقرار کدهای مخرب خود استفاده کرده و از سرورهای Github به عنوان سرور فرمان و کنترل حملات خود بهره می‌برند.

هفته گذشته، تیم امنیتی Malwarebytes دو فایل Word آلوده را شناسایی کرده که محتوای جعلی آن به استخدام در شرکت لاکهید مارتین مربوط می‌شد. ظاهرا هدف این گروه هکری نفوذ به نهادهای مرتبط با صنایع دفاعی و هوافضا و سرقت اطلاعات آنها بوده است.

هکرها مجموعه ای از کدهای مخرب را در اسناد Word تعبیه کرده‌اند که پس از فعال شدن به سیستم نفوذ کرده و بلافاصله کدها را در رایانه قربانی قرار می‌دهد تا پس از راه اندازی مجدد رایانه ویروس از کار نیفتد.

جالب اینجاست که بخشی از این فرآیند با بهره‌گیری از سرویس Windows Update انجام شده و از این سرویس برای نصب یک DLL مخرب استفاده می‌شود. این مراحل به صورت بسیار هوشمندانه‌ای انجام شده تا سیستم‌های امنیتی ویندوز متوجه این مشکل نشوند.

Malwarebytes گزارش داده گروه هکریLazarus بیش از یک سال است که از این استراتژی استفاده می‌کند. در این روش کارمندان سازمان‌ها و ادارات قربانی این حمله فکر می‌کنند که یک فرصت شغلی بسیار عالی به آنها پیشنهاد شده است. اما متوجه نیستند که همه اینها یک نمایش برای سرقت اطلاعات حساس از سازمان‌هایی است که در آن مشغول به کار هستند.

ظاهراً این گروه هکری پس حمله موفقیت آمیز خود به ده‌ها شرکت و سازمان جهانی در سال گذشته، تحت رصد شرکت‌های بزرگ امنیتی مانند Malwarebytes،ESET و MacAfee قرار گرفته است.

مدیر عامل Crypto.com تأیید کرد که صدها حساب هک شده اند

مدیرعامل صرافی Crypto.com، کریس مارشالک، سرانجام تأیید کرد که صدها حساب کاربری واقعاً توسط هکرها در معرض خطر قرار گرفته و در نتیجه آن وجوه به سرقت رفته است؛ اگرچه جزئیات روش نقض دقیقا نامشخص است.

Marszalek در مصاحبه آنلاین با بلومبرگ، وقوع این هک را تایید کرد و اظهار داشت که حدود ۴۰۰ حساب مشتری به خطر افتاده است. او همچنین به بلومبرگ گفت از زمانی که حمله برای اولین بار علنی شد، هیچ گونه دسترسی فراتری از سوی تنظیم کننده ها دریافت نکرده است، اما در صورت انجام تحقیقات رسمی، اطلاعاتی را به اشتراک خواهد گذاشت.

بیانیه های قبلی Marszalek و سایر مکاتبات با Crypto.com به دلیل ابهام و نامشخص بودن مورد انتقاد قرار گرفته است. پیام‌های رسمی این شرکت از یک «حادثه امنیتی» نام برد و در یک پست اولیه توییتری فقط اشاره شد که تعداد کمی از کاربران «فعالیت مشکوکی در حساب‌هایشان گزارش شده است».

مدت کوتاهی پس از آن، شرکت امنیتی PeckShield توئیتی منتشر کرد که در آن ادعا کرد، در حقیقت، ضرر Crypto.com به حدود ۱۵ میلیون دلار ETH بالغ شده است و به Tornado Cash فرستاده شده است تا "شسته شود". Tornado Cash یک ابزار حفظ حریم خصوصی ارزهای دیجیتال است که به عنوان «میکسر» شناخته می‌شود و می‌تواند مقصد نهایی اتریومی را که به آن ارسال می‌شود پنهان کند: سرویسی که کاربردهای قانونی دارد اما به راحتی می‌توان از آن برای شستشوی درآمدهای حاصل از سرقت و سایر جرایم مرتبط با رمزنگاری استفاده کرد.

از آنجایی که تعداد کاربران صنعت ارزهای دیجیتال همچنان در حال رشد است، صرافی های دیجیتال یکی از با ارزش ترین اهداف برای هدف قرار گرفتن از جانب هکرها هستند. به گفته NBC News، بیش از ۲۰ هک مبادله ای در طول سال ۲۰۲۱ وجود داشته که در آن هکر با بیش از ۱۰ میلیون دلار سود از مخمصه گریخته است. در شش مورد بیش از ۱۰۰ میلیون دلار عایدی برای هکرها داشته است.

هکرهای چینی شرکت های داروسازی و فناوری آلمان را هدف قرار می دهند

اداره فدرال حفاظت از قانون اساسی آلمان (BfV) روز چهارشنبه اعلام کرد گروه هکری چینی APT۲۷ که مدتها مظنون به انجام حملات به آژانس های دولتی غربی بود، شروع به هدف قرار دادن شرکت‌های آلمانی در بخش هایی مانند داروسازی و فناوری کرده است.

BfV در بخشنامه‌ای به شرکت‌ها گفت: علاوه بر سرقت اسرار تجاری و دارایی‌های معنوی، هکرها ممکن است سعی داشته باشند به درون شبکه‌های مشتریان و ارائه دهندگان خدمات رخنه کنند تا به طور همزمان به چندین شرکت نفوذ نمایند.

در گزارش سالانه خود از سال ۲۰۱۹، BfV اشاره کرده بود که نام اختصاری این گروه APT ۲۷ نام مستعار یک گروه هکر چینی است که به نام "پاندای سفیر" نیز شناخته می شود و گفته می شود سفارتخانه‌های خارجی و بخش‌های حیاتی را هدف قرار می دهد.

سال گذشته، ایالات متحده و متحدانش، چین را به انجام یک سلسله عملیات‌های جاسوسی سایبری در سطح جهانی متهم کردند. چین نیز در پاسخ، این اتهامات را رد کرده است.

یک گروه باج افزاری می گوید که وزارت دادگستری فرانسه را هک کرده است

هکرها تهدید کرده‌اند که «تمام داده‌های موجود» را ظرف دو هفته منتشر خواهند کرد. تنها یک روز پس از آن که یک حسابرس مستقل فرانسوی گفت که این وزارتخانه پیشرفت‌هایی در زمینه امنیت سایبری داشته است، اما هنوز کارهای قابل توجهی برای انجام دادن دارد؛ هکرها مسئولیت این رخنه را بر عهده گرفتند.

وزارت دادگستری گفت که از ادعای این گروه آگاه است و تحقیقات را آغاز کرده.

گروه باج افزاری معروف به LockBit همچنین با هک هایی مرتبط است که شرکت های بزرگی مانند شرکت دانمارکی توربین بادی Vestas و شرکت مشاوره Accenture را هدف قرار می دهد. این باند به "تهدید به انتشار داده‌ها در صورت عدم برآورده شدن درخواست‌های باج" معروف است.

مقامات ایران در حال بررسی هک تلویزیون دولتی هستند

کانال تلویزیونی هک شده رهبران گروه اپوزسیون در تبعید مجاهدین خلق (مجاهدین خلق) را به تصویر می کشد. یک سخنگوی دولتی گفت که مجاهدین خلق پشت این هک "بسیار دقیق" بوده است.

شاهین قبادی، سخنگوی مجاهدین خلق، مسئولیت مستقیم این رخنه را برعهده نگرفت و گفت که به نظر می‌رسد این کار توسط «حامیان مجاهدین خلق و واحدهای مقاومت در ایستگاه‌های رادیویی و تلویزیونی رژیم» انجام شده باشد.

سازمان مجاهدین خلق به دلیل عملیات های سایبری و دیگر عملیاتهایش شدیداً تحت نظر قرار گرفته است. فیس بوک ترول های مرتبط با این گروه را که عمدتاً در آلبانی مستقر هستند حذف کرده است. اینترسپت گزارش داد که یک منتقد معروف توییتری ایران در واقع یک شخصیت ساخته شده توسط مجاهدین خلق است (حشمت علوی). دولت اوباما در سال ۲۰۱۲ این گروه را از فهرست دولتی سازمان های تروریستی حذف کرد.

پگاسوس

جلسه استیضاح در مورد استفاده پلیس از جاسوس افزار Pegasus گروه NSO

اعضای کمیته امنیت عمومی پارلمان اسرائیل پس از گزارش هایی مبنی بر استفاده از پگاسوس برای هک غیرقانونی شهروندان اسرائیلی، از پلیس اسرائیل خشمگین شدند.

قانونگذاران پس از جلسه استماع گزارش‌ها پلیس اسرائیل را "سازمانی جنایتکار" خطاب کردند و خواستار وضع قوانین جدید و تفحص پارلمانی و پیوند دادن این جاسوسی به نخست وزیر سابق اسرائیل بنیامین نتانیاهو شدند؛ گرچه نتانیاهو در این پرونده ها به تخلف متهم نشده است.

عمر بارلف، وزیر امنیت عمومی به وزارتخانه خود گفته است که قوانین شنود این کشور را بررسی کنند. او گفت که "در صورت لزوم" قانون جدیدی پیشنهاد خواهد کرد. بارلف قبلا گفته بود که هیچ مدرکی دال بر تخلف پلیس وجود ندارد. پلیس اسرائیل از پذیرش ادعاهای نشریه Calcalist که در ابتدا این اتهامات را مطرح کرده بود، خودداری نموده است.

قانونگذاران اسرائیلی به فکر اصلاح مقررات نظارت سایبری این کشور هستند

تایمز اسرائیل گزارش داد که این اقدام در پی افشاگری‌هایی انجام می‌شود که پلیس اسرائیل را متهم به استفاده از نرم‌افزار جاسوسی Pegasus شرکت NSO برای جاسوسی از رهبران معترض، شهرداران و مقامات دولتی سابق بدون تأیید دادگاه‌های اسرائیل می‌کند.

مقامات قوه قضائیه اسرائیل و دو کمیته پارلمانی در حال بررسی فناوری پیشرفته نظارتی این کشور هستند. پلیس اسرائیل استفاده نادرست از این نرم افزارهای جاسوسی را رد کرده است.

طبق آخرین افشاگری: در سال‌های اخیر، یک واحد پلیس اسرائیل متهم است «حداقل سه هکر خارجی را به عنوان پیمانکاران پولی به منظور کمک برای جمع‌آوری اطلاعات و کشف پرونده‌های جنایی به کار گرفته است».

هکرها «به شبکه‌های وای‌فای خصوصی نفوذ نموده، فیلم‌های ضبط شده را از دوربین‌های امنیتی متعلق به شرکت‌های خصوصی دانلود کرده، [و] به فایل‌های بیمه، و همچنین تلفن‌هایی که پلیس نمی‌توانست با Pegasus آن‌ها را هک کند، رخنه می‌کردند». پلیس اسرائیل به Calcalist گفت که ادعاهای این گزارش "نادرست" است و آنها طبق قانون عمل می کنند.


NSO GROUP

مدافعان حقوق مدنی و روزنامه نگاران مجارستانی درگیر چالش های حقوقی به خاطر استفاده این کشور از جاسوس افزار Pegasus هستند

اتحادیه آزادی‌های مدنی مجارستان (HCLU) قصد دارد شکایت‌هایی را تنظیم و برای تنظیم‌کننده‌های داده و مقاماتی که بر سرویس‌های امنیتی مجارستان نظارت دارند، ارسال کند. اگر این کار به جایی نرسد، این گروه - که وکالت چهار نفر را که توسط نرم افزار جاسوسی Pegasus گروه NSO هدف قرار گرفته اند برعهده دارد- به اقدامات قانونی متوسل می شود.

در مجارستان، قربانیان پگاسوس شامل دو روزنامه‌نگار و یک تاجر هستند که نمی‌خواستند هویتشان فاش شود. منتقدان، استفاده از پگاسوس در مجارستان را با گذشته کمونیستی این کشور مقایسه کرده اند. ویکتور اوربان، نخست وزیر جناح راست این کشور، متهم به حرکت به سمت استبداد و تضعیف دموکراسی مجارستان شده است.

استفاده این کشور از پگاسوس توجه خاصی را به خود جلب کرده است زیرا مجارستان یکی از اعضای اتحادیه اروپا است.

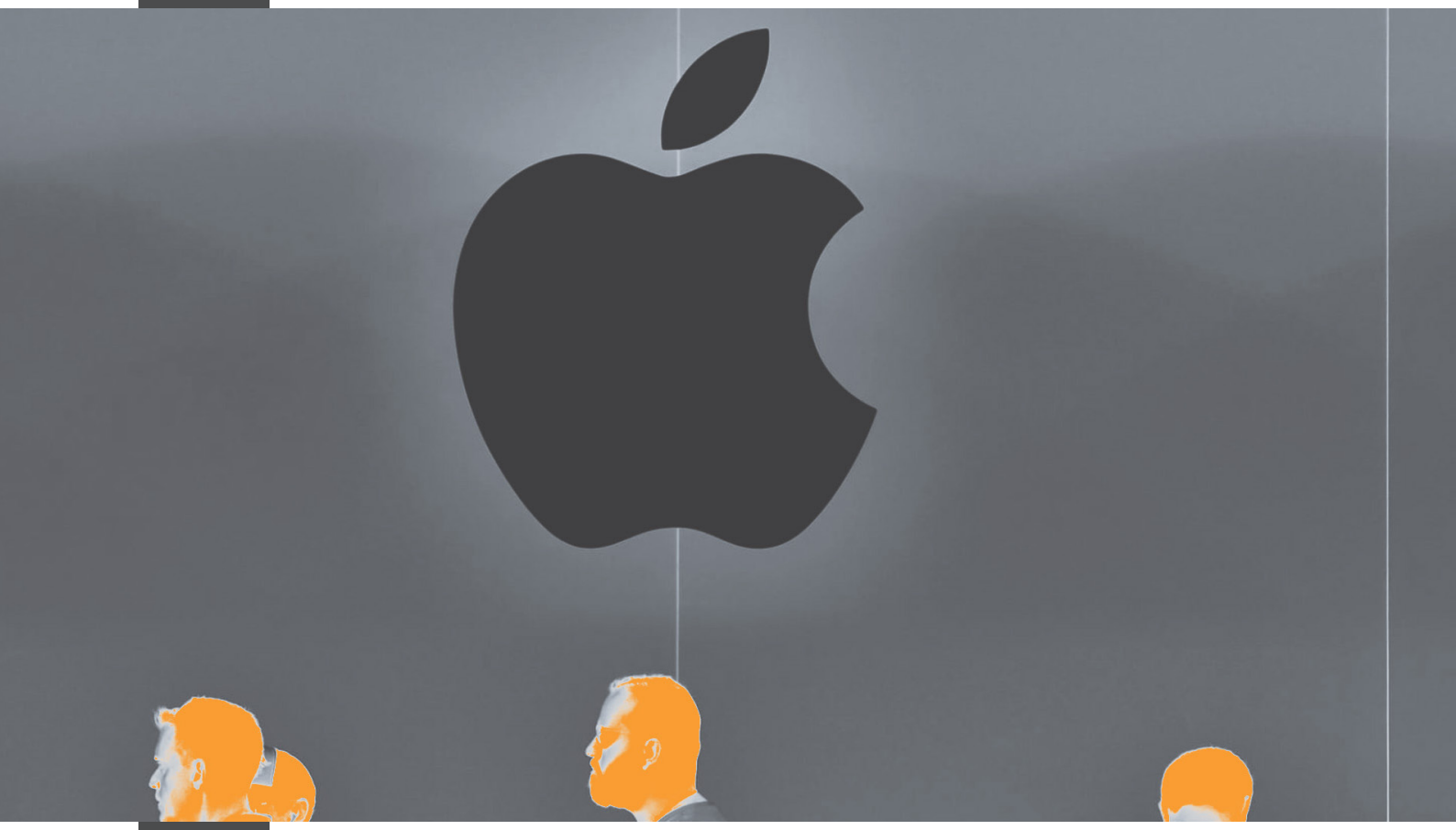
این نهاد مدنی «تعداد زیادی از شکایت‌ها» را به نمایندگی از طیف گسترده‌ای از بازیگران جامعه مدنی و روزنامه‌نگارانی که به گفته HCLU در معرض نظارت قرار دارند، به دادگاه حقوق بشر اروپا خواهد برد.

HCLU همچنین به نمایندگی از آدرین بودوین، فعال دانشجویی بلژیکی-کانادایی که در مجارستان تحصیل می‌کرد و مورد هدف پگاسوس قرار گرفت، شکایتی را به کمیسیون اروپا ارائه می کند. این گروه می‌گوید اقدام مجارستان ناقض قوانین اتحادیه اروپا است.

NSO هویت مشتریان خود را فاش نمی‌کند، اما یکی از کارمندان سابق NSO به شرط ناشناس ماندن سال گذشته در این خصوص به واشنگتن پست گفته بود: دولت مجارستان یکی از مشتریان NSO است.

دولت مجارستان می‌گوید هنگام استفاده از فناوری های نظارتی از قانون پیروی نموده است.

فناوری نوین



افزایش تکاپوی اپل برای ورود به دنیای متاورس

کمپانی اپل در جدیدترین گزارش مالی خود عنوان کرد در یک سال اخیر بیش از ۱۶۵ میلیون کاربر به عضویت سرویس‌های خدماتی این شرکت درآمده و به کاربران اپل اضافه شده‌اند. این تعداد مجموع تمام کاربران جدید سرویس‌های اپل از قبیل Arcade، Music، iCloud و Apple TV+ را در سراسر جهان نشان می‌دهد. مدیر مالی اپل، «لوکا میستری» ، در این مورد گفت:« ما در سه‌ماهه‌ی نهایی سال ۲۰۲۱ در تمام بخش‌های خدماتی خود در سرتاسر جهان رکورد زده‌ایم. در نتیجه می‌توان گفت که در سه‌ماهه‌ی اخیر بهتر از آنچه در ابتدا انتظار می‌رفت عمل کردیم.»

تعداد کاربران سرویس‌های اپل (Paid Subscribers) هم‌اکنون به عدد ۷۸۵ میلیون رسیده است که حدود ۱۶۵ میلیون از آن‌ها مربوط به یک سال اخیر هستند.

در همین ارتباط مدیر عامل اپل، آقای تیم کوک، از علاقه‌ی اپل به سرمایه‌گذاری در متاورس سخن گفت و مدعی شد سرمایه‌گذاری که اپل هم‌اکنون در حوزه‌ی AR انجام داده است، نشان‌گر این موضوع است. البته آقای کوک در پاسخ خود از کلمه‌ی «متاورس» استفاده نکرد و با اشاره به حضور بیش از ۱۴,۰۰۰ اپلیکیشن AR در اپ استور به پاسخ خود پایان داد.

مدیر عامل سرشناس اپل در ادامه اظهار داشت فضای متاورس پتانسیل بالایی برای خلاقیت دارد و شرکت اپل نیز بسته به این پتانسیل در حوزه‌ی مزبور سرمایه‌گذاری خواهد کرد. اگر به خاطر داشته باشید اپل با افزودن حسگر LiDAR به گوشی‌های آیفون ۱۲ پرو و سپس حضور آن در آیپد پروها علاقه‌مندی خود به عرصه‌ی فناوری‌های واقعیت افزوده را مشخص کرد. از این روز انتظار می‌رود با اوج‌گیری متاورس، فعالیت اپل نیز در این حوزه افزایش یابد.

تفاوت "رمزریال" با سایر رمزارزها چیست؟

معاون فناوری‌های نوین بانک مرکزی اعلام کرد «رمز ریال» شباهتی به "بیت کوین" نداشته و صرفا ابرازی برای مبادله و پرداخت است. به گفته وی انتشار «رمزریال» در انحصار بانک مرکزی بوده و بحث استخراج و سرمایه‌گذاری درباره آن معنایی ندارد.

«مهران محرمیان» به تشریح تفاوت "رمز ریال" با سایر رمزارزهای شناخته شده همانند بیت کوین پرداخت و گفت:« رمز ریال یک رمزارز جهان روا مانند بیت کوین که پشتوانه ندارد، نبوده و همچنین خبری از استخراج آن نیست».

به گفته وی انتشار "رمز ریال" همانند اسکناس در انحصار بانک مرکزی است و بحث سرمایه گذاری در آن وجود ندارد:«کسی روی پول سرمایه‌گذاری نمی‌کند، بلکه تنها یک ابزار پرداخت است».

محرمیان با بیان اینکه مردم با مراجعه به بانک می‌توانند به ازای پولی که در بانک دارند، "رمز ریال" دریافت کنند، اعلام کرد سقف دریافت "رمز ریال" بسته به اینکه کیف پول الکترونیکی تجاری یا غیر تجاری باشد متفاوت است.

او در پاسخ به این سوال که رمز پول بانک مرکزی از چه زمانی در دسترس قرار خواهد گرفت، گفت:« "رمزریال" از ابعاد فنی، اقتصادی، نظارتی، ارزی، ریالی و به خصوص حقوقی مورد بررسی قرار گرفته است. بعد از ابلاغ مصوبه رمزپول ملی به شورای پول و اعتبار ظرف چند ماه آینده آن را به صورت آزمایشی اجرا خواهیم کرد.»

معاون فناوری‌های نوین بانک مرکزی در ادامه کاربرد "رمز ریال" را شفاف کرده و گفت:« در حال حاضر کارت‌های بانکی ابزاری برای دسترسی به پولی است که در بانک قرار دارد. یعنی این کارت تنها دسترسی الکترونیکی به پول داخل بانک را ایجاد کرده و اگر روزی بانک مورد نظر ورشکست شود، افراد دیگر به پولشان دسترسی نخواهند داشت. در حالی که با رمز ریال، بانک به عنوان

واسط حذف شده و افراد پولشان را در گوشی خود نگه‌داری می‌کنند.»

او با تاکید بر بحث نظارتی در پروژه رمز ریال، ردیابی پول را یکی از فواید آن برشمرده و اظهار داشت در صورت نفوذ به گوشی افراد و جا به جایی بدون اطلاع رمز ریال، امکان ردیابی پول وجود خواهد داشت.

محرمیان در ادامه اعلام کرد پروژه رمز ریال باعث تبدیل اسکناس به "open money" و پول قابل برنامه‌نویسی خواهد شد که فضای نوآورانه‌ای را ایجاد خواهد کرد:« از مزیت‌های این اتفاق امکان رهگیری استفاده از تسهیلات بانکی است تا افراد و شرکت‌ها، وام را در جای دیگری خرج نکنند. همچنین با تعیین ضابطه هنگام بستن قرارداد و انتقال پول، می‌توان میزان جریمه فسخ قرارداد را تعیین کرد تا در صورت وقوع آن، مبلغ جریمه به طور خودکار از حساب طرف مقابل برداشت شود.»

ICDT.IR