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

وقوع بزرگترین هک شناسایی شده در پلتفرم ارزهای دیجیتال سبب شد تا بار دیگر بحث در مورد مخاطراتی که گسترش استفاده از آنها با خود به همراه دارد مورد بحث محافل آکادمیک قرار گیرد. این اتفاق فقدان امنیت در این بخش را کاملاً عیان ساخت.

یکی دیگر از جنجالی‌ترین اخبار سایبری هفته گذشته آشکار شدن حملات سایبری چین به زیرساخت‌های اسرائیل بود که با پوشش هکرهای ایرانی انجام می‌شد.

Iranian Council For
Defending The Truth

اخبار

۳

امنیت سایبر آمریکا

اقدام شرکت اَپل علیه پورنوگرافی کودکان؛ تغییر به نفع تقاضاهای آژانس‌های امنیتی و انتظامی امریکا

جدالی هفت ساله میان تکنسین‌ها و سازمان‌های انتظامی و امنیتی امریکا بر سر دسترسی بدون اطلاع به محتویات دستگاه‌ها و پلتفرم‌های اجتماعی وجود دارد. در این کشمش چندین ساله عمدتاً FBI و وزارت دادگستری امریکا خواهان دسترسی ویژه پلیس به ارتباطات رمزگذاری شده بوده‌اند. آنها می‌گویند چنین دسترسی با صدور حکم قانونی برای جلوگیری از تروریست‌ها، مبارزه با پورنوگرافی کودکان و سایر جرائمی که به صورت آزادانه و آنلاین فعالیت می‌کنند، ضروری است.

در طرف مقابل، تکنسین‌ها تقریباً به اجماع بر این باور هستند که ایجاد چنین درب پشتی بر محتویات رمزگذاری شده ، همه کاربران را در خطر هک شدن قرار می دهد و این توافقات ارزش چنین ریسکی را ندارد.

اما اکنون در این کشمکش دشوار، سیستم اپل قصد دارد اقدام ماهرانه‌ای را انجام دهد به این نحو که رایج‌ترین تصاویر پورنوگرافی به اشتراک گذاشته شده مربوط به کودکان را گزارش کند.

این سیستم همچنان مورد انتقاد اکثریت قریب به اتفاق تکنسین‌ها و متخصصان حفظ حریم خصوصی است. آنها معتقدند این شیوه بیش از حد تهاجمی است و هشدار می‌دهند که می‌تواند سراشیبی هموواری را به سوی نظارت بیشتر دولتی ایجاد کند.

از طرفی این راهکار جدید اَپل مورد تمجید افرادی است که آن را مصالحه‌ای معقول در جهت مبارزه با گسترش چنین تصاویری می‌دانند.

در شیوه‌ی مدنظر اپل، تصاویر واقعی بررسی نمی‌شوند بلکه اثرانگشت‌های دیجیتالی مربوط به آنها یا به عبارت تخصصی‌تر، هَش‌ها بررسی می‌شوند. این برنامه هش‌های عکس را در تلفن‌ها و تبلت‌ها قبل از بارگذاری در iCloud اسکن می‌کند تا ببیند آیا با هش‌های شناخته شده مرتبط با پورنوگرافی کودکان مطابقت دارد یا خیر. اپل نه به عکس‌ها نگاه می کند و نه اطلاعاتی در مورد عکس‌هایی که با امضای دیجیتال مطابقت ندارند جمع آوری می کند.

اگر تعداد تطابقت ها از یک آستانه مشخص عبور کند ، اپل اطلاعات مربوط به کاربر را به "مرکز ملی کودکان مفقودالاثر و استثمار شده" ارسال می کند ، که احتمالاً این اطلاعات را با ماموران قانون به اشتراک می گذارد.

اپل در یک مقاله فنی می گوید که این آستانه را به اندازه کافی بالا قرار داده است به طوری که تقریباً ۱ در ۱ تریلیون این احتمال وجود دارد که

فردی به دلیل داشتن پورنوگرافی کودکان به اشتباه متهم شود. این شرکت گفته است که از هرگونه درخواست دولتی برای جستجوی موارد دیگری به جز پورنوگرافی کودکان خودداری می‌کند.

با این حال ، اکثر تکنسین‌ها و حامیان حریم خصوصی به شدت با سیستم اپل مخالف هستند. برخی نگران‌اند که این روش به مرور بی‌اثر شود چرا که افراد خطاکار می‌توانند به انجام فعالیت‌های خود در پلتفرم‌ها و بسترهایی که رمزنگاری در برابر ماموران قانون را حفظ نموده‌اند، ادامه دهند. هم‌چنین این سیستم احتیاج دارد تا کاربران به اپل اعتماد کنند که این شرکت از این فناوری سوء استفاده نخواهد کرد و چیزهایی را فراتر از پورنوگرافی کودکان جستجو نمی‌کند. برخی دیگر نگران هستند که این امر اسکن تلفن‌ها در کشورهای سرکوب‌گر نظیر چین را تسهیل نماید.

جاناتان مایر ، استاد علوم کامپیوتر در دانشگاه پرینستون گفت:« هنگامی که اپل برنامه های VPN را از App Store در چین حذف کرد، "تیم کوک " گفت در هر جایی که ما تجارت می کنیم تابع قانون هستیم. اگر چین یا کشور غیر دموکراتیک دیگری بخواهد که اپل از این سیستم برای نظارت یا سانسور نامشروع استفاده کند ، چه اتفاقی می افتد؟ »


You
Tube

پلتفرم‌های گوناگون

بزرگترین هک ارزهای رمزنگاری‌شده

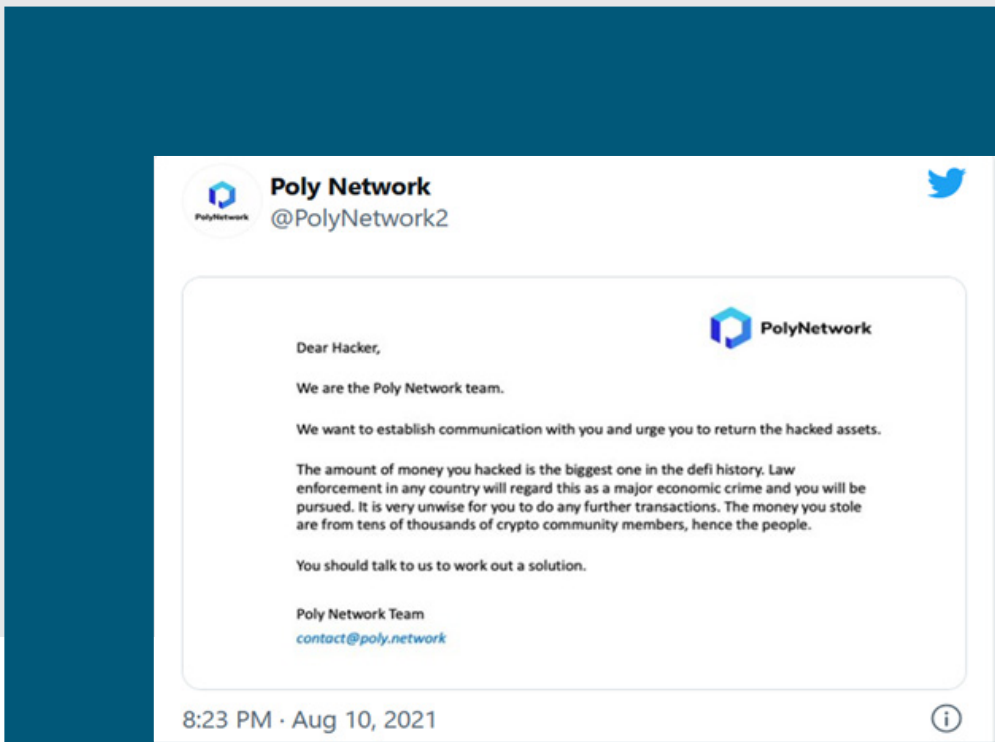
هفته گذشته یک هکر ناشناس بیش از ۶۰۰ میلیون دلار از پلتفرم مالی غیرمتمرکز Poly Network سرقت کرد اما اندکی پس از افشای آن، تقریباً تمام این پول را پس داد. ظاهراً این هکر یا گروه هکری، پاداش نیم میلیون دلاری را که Poly Network برای افشای آسیب‌پذیری امنیتی خود ارائه کرده بود، نیز رد کرده‌اند.

طبق وب سایت Poly Network ، این پلتفرم به کاربرانش این امکان را می‌دهد تا دارایی‌های رمزنگاری شده را در بلاک چین‌های مختلف معامله کنند. تحت پوشش، Poly Network این تراکنش‌ها با استفاده از اسکریپت‌هایی به نام "Contracts" انجام می‌شود.

سخنگوی Poly Network گفت: "هکر از یک آسیب پذیری ، به نام _executeCrossChainTx که عملکرد بین فرمانهای Contract را مدیریت می‌کند، سوء استفاده کرده است." در این حمله هکری، مهاجمان با استفاده از فرمان‌های مکرر به Contract مورد حمله ، توانستند وجوه Poly Network را جمع آوری کرده و سپس آنها را به کیف پول‌های تحت کنترل خود منتقل نمایند.

پس از کشف این حمله ، شرکت Poly Network این حادثه را برای عموم فاش کرد و ضمن تقاضای کمک از جامعه ارزهای رمزپایه، از پلتفرم‌های استخراج و صرافی‌ها درخواست نمود تا حرکات هکرها را ردیابی کرده و حساب های آنها را مسدود کنند.

در توییتر ، شرکت‌هایی مانندOKEx ، Tether، Huobi و Binance اعلام کردند که موفق شده‌اند بخش کوچکی از دارایی‌های سرقت شده را مسدود نمایند. در همین حال ، Poly Network نامه‌ای در صفحه توییتر خود منتشر و از هکر خواست قبل از تشدید حادثه ، وجوه را پس دهد. هکرها در گذشته برای جلوگیری از تعقیب قانونی وجوه سرقت شده را به پلتفرم‌های ارزهای رمزنگاری شده تبدیل می‌ساختند، به همین خاطر نامه‌ی این شرکت فعال در زمنیه ارزهای دیجیتال مورد تمسخر قرار گرفت و به موضوعی پرطرفدار در توییتر مبدل شد.



شرکت امنیت بلاک‌چین Xiamen Slowmist Technology ، اعلام کرد آدرس IP و اطلاعات ایمیل هکر را کشف کرده است. این شرکت در یک پست وبلاگی نحوه انجام این حمله توسط هکر را توضیح داد. Slowmist نتیجه گرفت که مجرمان سایبری از یک نقطه آسیب پذیر در کدهای Poly Network استفاده نموده‌اند که در آن هکرها می‌توانند بدون شناسایی ، ارزهای رمزنگاری شده را برای یکدیگر ارسال کنند.

هنوز انگیزه هکرها از این رویداد مشخص نشده است. به گفته کارشناسان خرج کردن مبالغ سرقت شده برای هکر بسیار دشوار بوده؛ از طرفی به این دلیل که تراکنش‌های بلاک‌چین به صورت عمومی ثبت می‌شوند، پولشویی پولها را نیز دشوار می‌نموده است به همین خاطر شاید ارزها بازگردانده شده‌اند.

تحلیلگران بلاکچین می‌گویند هکرها در پیام‌هایی اذعان داشته‌اند که "برای سرگرمی" به Poly Network نفوذ کرده‌اند و می خواستند آسیب پذیری در این سیستم را "آشکار" کنند.

فیس‌بوک ده‌ها حساب مرتبط با کوشش روسیه در ایجاد شک در مورد واکسن‌های کرونا را حذف کرد

CyberScoop اعلام نمود که این حساب‌ها سعی می‌کردند اینفلوئنسرهای اینستاگرام ، TikTok و YouTube را متقاعد کنند که واکسن کرونای Pfizer ایمن نیست. فیس‌بوک گفت ، اما اینفلوئنسرها در اوایل امسال عملیات را شناسایی و افشا کردند.

بِن نیمو ، مقام اطلاعاتی تهدیدات فیس بوک گفت:« در واقع ، این نه فقط یک عملیات نفوذ بلکه یک عملیات بر روی عوامل اثرگذار بود. از قضا ، این عملیات به دنبال بی آبرو کردن Pfizer بود.»

یک کمپین مشابه دیگر نیز واکسن AstraZeneca را هدف قرار داده است و در مِیم‌ها و پست‌ها نشان می‌داد که این واکسن می‌تواند افراد واکسینه شده را به شامپانزه تبدیل کند. به گفته فیس بوک ، این بخش از عملیات‌های اطلاعاتی در گذشته مورد توجه قرار نگرفته است.

امنیت سایبر بین‌الملل

جاسوسان سایبری چینی با پوشش هکرهای ایرانی زیرساخت‌های اسرائیل را هدف قرار داده‌اند

یک گروه جاسوسی سایبری چینی در کمپینی که در ژانویه ۲۰۱۹ آغاز شد ، سازمان‌های اسرائیلی را هدف قرار داده و طی آن این گروه اغلب از علائم دروغین برای مبدل شدن به عنوان یک عامل تهدید کننده ایرانی استفاده می‌کرده است.

در گزارشی که توسط شرکت امنیتی Mandiant منتشر شده ، این حملات نهادهای دولتی اسرائیل، شرکت‌های فناوری اطلاعات و سرویس‌دهندگان مخابرات رژیم صهیونیستی را هدف قرار داده است.

مهاجمان که به گفته Mandiant با کد رمز UNC۲۱۵ ردیابی شده اند ، معمولاً با هدف قرار دادن سرورهای تعمیر نشده Microsoft SharePoint به خاطر آسیب‌پذیری CVE-۲۰۱۹-۰۶۰۴ توانسته‌اند به سازمان‌ها نفوذ کنند.

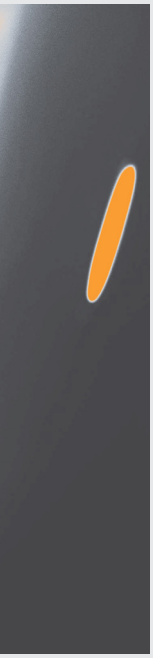
این گروه هکری اقدامات متعددی را برای پنهان کردن نفوذ خود و به حداقل رساندن شواهد قانونی در شبکه قربانی انجام می‌داده ، مانند حذف اثرات ایجاد شده در اثر بدافزار در صورت عدم نیاز و استفاده از نرم افزارهای قانونی برای انجام عملیات تخریبی.

علاوه بر این ، این گروه از علائم دروغین در داخل کد منبع بدافزار خود استفاده کرده تا هویت واقعی خود را مخفی کند.

Mandiant اعلام نمود UNC۲۱۵ اغلب از مسیرهای پرونده‌ای استفاده نموده که از ایران نام می‌برد (به عنوان مثال: C:\Users\Iran) یا پیام‌های خطا که به زبان عربی نوشته شده است (یعنی "ضائع" - که به معنی: گم شده یا مفقود شده است)

علاوه بر این ، حداقل در سه مورد ، UNC۲۱۵ از یک ابزار هک ایرانی استفاده کرد که در سال ۲۰۱۹ در تلگرام فاش شد (یعنی پوسته وب SEASHARPEE).

آمریکا به برزیل در خصوص تأمین تجهیزات ۵G از شرکت هوآوی هشدار داد



جیک سالیوان ، مشاور امنیت ملی ایالات متحده ، هفته گذشته در سفر خود به این کشور نگرانی هایش را درباره تجهیزات هوآوی در شبکه مخابراتی ۵G برزیل ابراز داشت ، اما برزیل هیچ قولی در مورد عدم استفاده از محصولات این شرکت چینی نداد.

خوان گونزالس مدیر ارشد "شورای امنیت ملی در نیمکره غربی" ، گزارش‌هایی را که مدعی بودند ایالات متحده در ازای همکاری برزیل در زمینه تجهیزات ۵G ساخته شده توسط شرکت هوآوی به این کشور پیشنهاد نموده که برای مشارکت این کشور در ناتو از برزیل حمایت خواهد کرد، قویاً رد نمود و گفت که این دو موضوع به هم مربوط نیستند.

گونزالس افزود: "ما همچنان در مورد نقش احتمالی هواوی در زیرساخت‌های مخابراتی برزیل نگرانی داریم" و افزود که هواوی با چالش‌های بزرگی در زنجیره تامین نیمه هادی‌های خود مواجه است که مشتریان بین المللی را "بدون کمک" رها خواهد کرد.

وی گفت که برزیل در قبال هواوی هیچ تعهدی نداده است و افزود که مقامات آمریکایی از برزیل و آرژانتین خواسته اند در این حوزه صنایع بومی ایجاد کنند.

ایالات متحده با استفاده برزیل از هواوی به دلایل امنیتی مخالف است ، اگرچه شرکت‌های مخابراتی برزیل پیش از این شبکه‌هایی با قطعات چینی راه اندازی نموده‌اند.

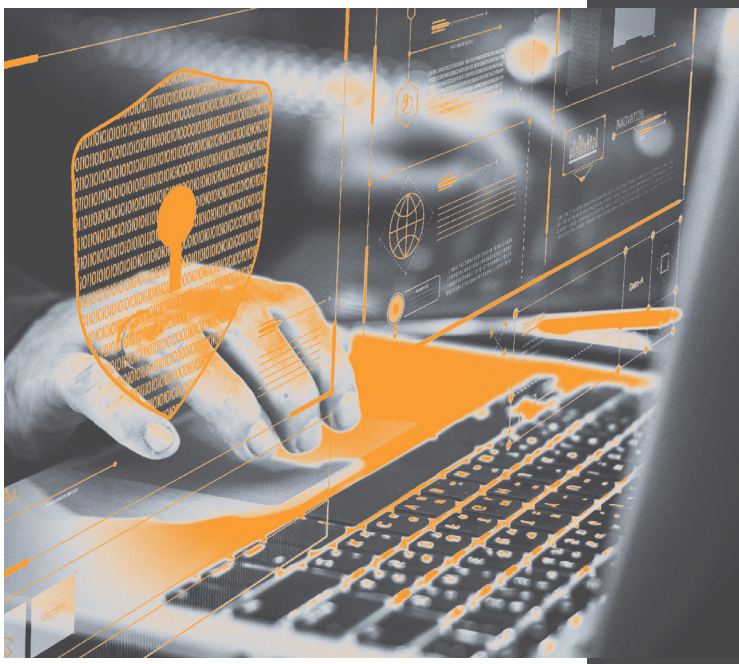
همکاری سرویس‌های اطلاعاتی روسیه با گروه‌های باج افزاری

بـر اسـاس تحقیقـات جدیـد شـرکت امنیت سـایبری Analyst۱ ، سـرویس‌های اطلاعاتـی روسـیه بـا گروه‌هـای برجسـته بـاج افـزار بـا هـدف اخـلال در دولـت ایالات متحـده و سـازمان‌های وابسـته به این کشـور همـکاری می‌کننـد.

تحلیلگـران امنیتـی ایـن شـرکت در ایـن گـزارش ادعا کردنـد کـه دو اداره جاسوسـی روسـیه - FSB و SVR - بـا افـرادی در "چندیـن تشـکیلات جرائـم سـایبری" همـکاری داشـته‌اند. ایـن تحقیقـات نشـان می‌دهـد کـه ایـن مجرمـان سـایبری بـه سـرویس اطلاعاتـی روسـیه در توسـعه و اسـتقرار بدافزارهـای سفارشـی کمـک نموده‌انـد تـا شـرکت‌های آمریکایـی خدمـات دهنـده بـه مشـتریان نظامی ایـالات متحـده را هدف قـرار دهند.

بـه گفتـه Analyst۱ ، گروه‌هـای هکـری از انـواع باج‌افـزار Ryuk بـه نـام "Sidoh" -کـه بـرای حملـه بـه شـرکت‌های بـزرگ و بـه طـور خـاص برای جاسوسـی اسـتفاده می‌شـود، بهـره جسـته‌اند. ایـن کـد بیـن ژوئـن ۲۰۱۹ و ژانویـه ۲۰۲۰ راه انـدازی شـد و در پـس زمینـه دسـتگاه‌های ویندوز پنهـان می‌گردد و بی سـر و صـدا کلیدهـا و اسـناد حسـاس را از دسـتگاه هدف برداشـت می‌کنـد.

یکـی از حمـلات توصیـف شـده در گـزارش توسـط گروهـی به نام EvilCorp در اکتبر ۲۰۲۰ اجرا شـد. گروه دیگـری که بـه عنـوان SilverFish شـناخته می‌شـوند ، تنهـا دو مـاه بعـد با اسـتفاده از زیرسـاخت‌های فنی مشـابه ، ابزارهـای هـک و اسـکریپت هـای مخـرب ، همـان قربانـی را هـدف قـرار دادنـد. ایـن گروه‌هـا بـرای پنهـان کـردن فعالیـت خـود از تکنیکـی بـه نام "fronting domain" استفاده کرده‌اند.



مظنون جاسوسی برای روس‌ها بازداشت شد

دادستان‌های فدرال آلمان گفتند که این فرد با نام دیوید اس، در سفارت انگلیس در برلین کار می‌کرد و این طور به نظر می‌رسد که در آنجا اسناد الکترونیکی سایبری ، جزئیات شبکه Wi-Fi داخلی و کاغذهای محرمانه را به عوامل اطلاعاتی روسیه در ازای "مقدار نامعلومی پول" منتقل کرده است.

این شهروند انگلیسی در ۱۰ آگوست در پوتسدام دستگیر شد و خانه و محل کار وی در چارچوب تحقیقات مشترک بین "فرماندهی مبارزه با تروریسم پلیس بریتانیا" و همتایان آلمانی آنها مورد بازرسی قرار گرفت. در این گزارش آمده است که اتهامات وی مربوط به مشارکت در فعالیت جاسوسی براساس قوانین آلمان است. مقامات آلمانی مسئولیت این پرونده را در حال حاضر در اختیار دارند.

این بریتانیایی ۵۷ ساله نه تنها دیپلمات نیست بلکه یک نگهبان امنیتی از طرف یک شرکت خصوصی است که در سفارت برلین کار می‌کند و بنابراین مصونیت دیپلماتیک ندارد. وی مظنون است که حداقل از نوامبر ۲۰۲۰ با سازمان اطلاعاتی روسیه همکاری داشته و اسنادی را که در طول کار خود به دست آورده به واسطه این سازمان منتقل کرده است.

دولت اسلواکی برای ماه‌ها هدف جاسوسان سایبری روسیه بوده است

این هفته شرکت‌های امنیتی ESET و IstroSec در اسلواکی اعلام کردند که یک گروه جاسوسی سایبری روسی مرتبط با نیروهای اطلاعاتی روسیه ، دولت اسلواکی را برای چندین ماه‌ها هدف قرار داده است.

این حملات به گروهی معروف به دوک‌ها ، نوبلیوم یا APT۲۹ نسبت داده شد که سازمان‌های امنیت سایبری ایالات متحده و برخی کشورهای دیگر رسماً به سرویس اطلاعات خارجی روسیه ، معروف به SVR مرتبطه دانسته‌اند.

ESET و IstroSec گفتند هکرهای SVR اخیراً چندین کمپین فیشینگ را بین فوریه تا ژوئیه ۲۰۲۱ سازماندهی کرده‌اند که مقامات اسلواکی را هدف قرار داده است.

عملیات‌کنندگان SVR برای دیپلمات‌های اسلواکی ایمیل‌هایی ارسال می‌کردند و خود را به عنوان مقام امنیت ملی اسلواکی (NBU) معرفی می‌نمودند. سپس به همراه اسنادِ ضمیمه شده به ایمیل‌ها (معمولاً یک فایل تصویری ISO)، یک درب پشتی Cobalt Strike را در سیستم‌های آلوده بارگیری و نصب می‌نمودند.

شرکت ESET مدعی است در این کمپین‌های فیشینگ دیپلمات‌های بیش از ۱۳ کشور اروپایی هدف قرار گرفته‌اند. بر اساس گزارش ESET ، به نظر می رسد که همه حملات از یک تاکتیک (ایمیل-> تصویر دیسک ISO -> فایل میانبر LNK -> Cobalt Strike backdoor) پیروی می‌کنند ؛ تاکتیکی که در دو گزارش اوایل امسال از Volexity و Microsoft نیز توضیح داده شد. در برخی از این حملات ، گروه جاسوسی روسیه همچنین برای آلوده نمودن دیپلمات‌هایی که ایمیل‌های خود را بر روی گوشی‌های آیفون خود می‌خوانند ، به یک آسیب‌پذیری از پیش ناشناخته Safari iOS متکی بودند.

ICDT.IR