گزارش
مجمع ایرانی دفاع از حقیقت

Iranian Council For
Defending The Truth

فروردین ۱۴۰۱

امنیت سایبـــــری


بسم الله الرحمن الرحیم

فهرست

Iranian Council For
Defending The Truth

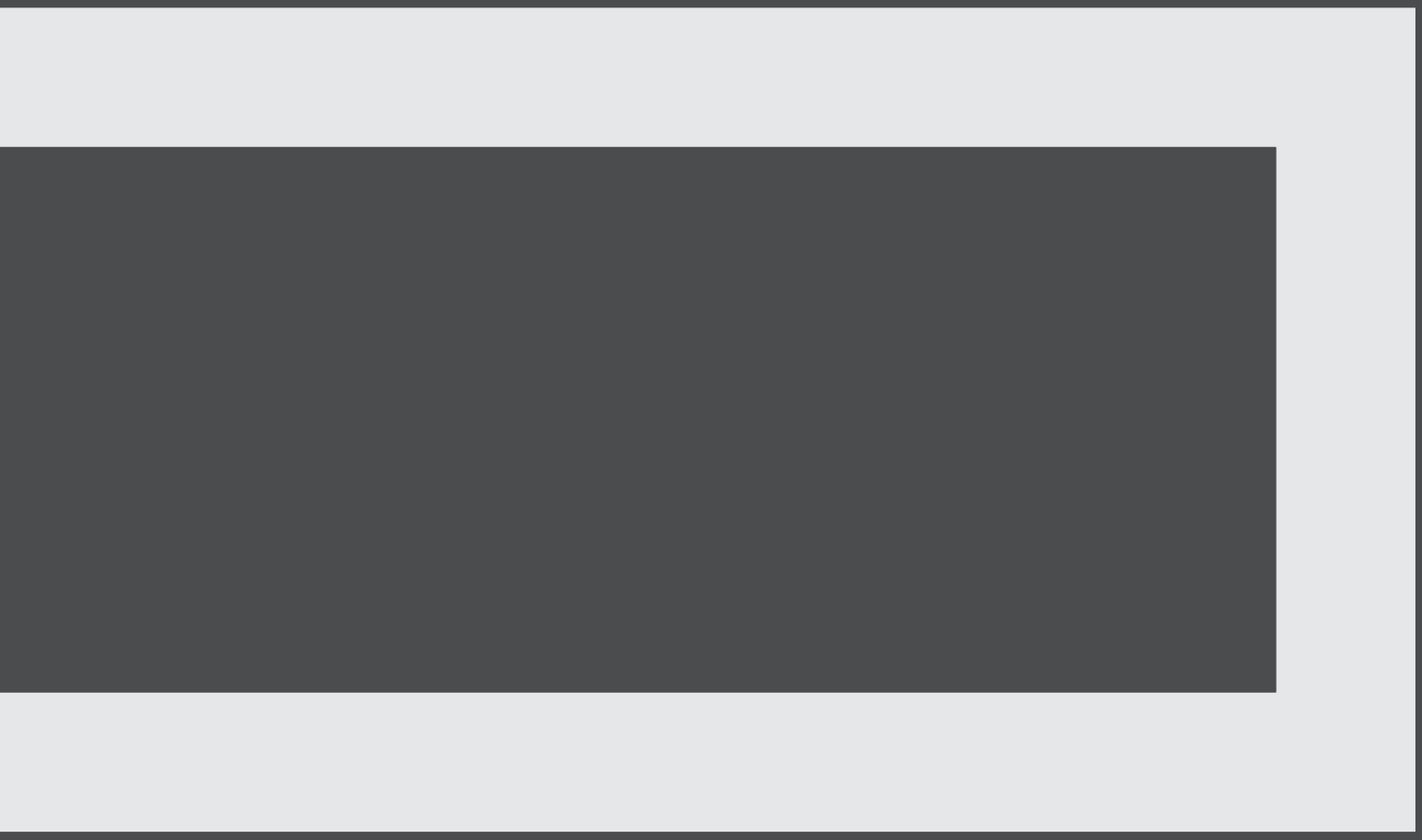
پیشگفتار

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 دیدبان سایبری در سه محور شامل ایالات متحده آمریکا، تنش بین روسیه و اوکراین، و سایبر بین الملل تهیه و منتشر شده است.

طی هفته گذشته بین آمریکا و اتحادیه اروپا توافقاتی در راستای ارتقای حفاظت از حریم خصوصی کاربران صورت گرفت. همچنین یک بازار غیرقانونی تبادلات مواد مخدر تحت تحریم های آمریکا قرار گفت.

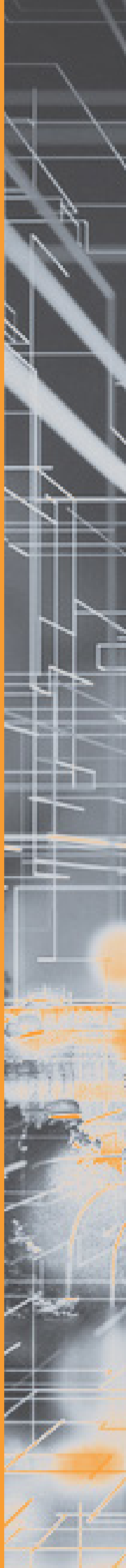
در تنش بین روسیه و اوکراین شاهد رویارویی همه جانبه بین دو طرف بوده ایم. هر طرف اقدام به به کارگیری روش هاُ، بد افزار ها و تکنیک های مختلف در حملات سایبری برای ضربه زدن بیش از بیش به طرف دیگر کرده است.

نهایتا در بخش سایبر بین الملل جدید ترین مصوبات سایبری در پارلمان استرالیا را بررسی کرده ایم.

Iranian Council For
Defending The Truth

اخبار

۳



ایالات متحده آمریکا

اتحادیه اروپا و ایالات متحده به توافق اولیه در مورد چارچوب حریم خصوصی داده های Trans-Atlacy می رسند

پس از دو سال مذاکره طولانی مدت، ایالات متحده و اتحادیه اروپا اعلام کردند ک به توافقنامه انتقال اطلاعات اولیه رسیدند. چارچوب حفظ حریم خصوصی داده های Trans-Atlantic، توافقنامه قبلی حریم خصوصی را جایگزین می کند که توسط بالاترین دادگاه اتحادیه اروپا در سال ۲۰۲۰ به دلیل نگرانی های مربوط به قانون نظارت بر حریم خصوصی شهروندان اروپایی مورد بررسی قرار گرفت.

توافق حاصله به دنبال اعلامیه هفته گذشته است که اعلام شد پارلمان اروپا به توافق در مورد قانون بازارهای دیجیتال نزدیک شده است، توافقی که طی آن به طور قابل توجهی بر کسب و کار شرکت های بزرگ فن آوری های آمریکایی مانند اپل و گوگل در اتحادیه اروپا تاثیر می گذارد.

دولت ایالات متحده یک بازار در دارک وب را تحریم کرد

تحریم‌های وزارت خزانه‌داری بر Hydra Market زمانی اعمال شد که مقامات آلمانی سرورهای سایت و حدود ۲۵ میلیون دلار ارز دیجیتال را توقیف کردند. وزارت دادگستری دیمیتری اولگوویچ پاولوف ۳۰ ساله ساکن روسیه را به توطئه برای توزیع مواد مخدر و ارتکاب پولشویی در مدیریت سرورهای هیدرا متهم کرد.

وزارت خزانه داری همچنین گارانتکس، یک صرافی ارز دیجیتال را که ابتدا در استونی ثبت شده بود اما بیشتر در داخل روسیه فعالیت می کرد، تحریم کرد. خزانه داری گفت که از بیش از ۱۰۰ میلیون دلار تراکنش غیرقانونی در سرورها، نزدیک به ۶ میلیون دلار مربوط به باج افزار باج افزار Conti و حدود ۲.۶ میلیون دلار مربوط به Hydra بوده است.

تنش‌های روسیه و اوکراین

نقش نوکیا در نظارت دیجیتال روسیه

شرکت مخابراتی فنلاندی نوکیا نقش مهمی در فعال ساختن ابزار نظارت دیجیتال روسیه، به عنوان سیستمی برای انجام فعالیت های تحقیقات و نظارت ایفا کرده است. دولت روسیه از نوکیا برای رهگیری ارتباطات و نظارت بر تماس های تلفنی، ایمیل ها و متون افراد در کشور استفاده می کند، از جمله مخالفان سیاسی مانند الکسی نالنی و بوریس نعمتوف. در حالی که نوکیا تکنولوژی رهگیری را ایجاد نمی کند، اما تجهیزات و خدماتی را ارائه می دهد که اهداف را به بزرگترین ارائه دهنده خدمات مخابراتی روسیه متصل می کند. اگرچه که در همین ارتباط نیویورک تایمز گزارش داده است که نوکیا به فروش روسیه به روسیه خاتمه داده است.

حمله سایبری در شرکت مخابراتی اوکراین

در روز دوشنبه هکرها به شرکت مخابراتی دولتی اوکراین حمله کردند و خدمات اینترنت را مختل کردند. در حالی که هنوز مشخص نیست که آیا فعالیت مخرب یک حمله انکار سرویس (DDOs) انجام شده یا یک نفوذ پیچیده تر بوده. سرویس پانزده ساعت پس از حمله اولیه بازسازی شد.

این اقدام به دنبال حملات ۲۴ فوریه به ارائه دهنده اینترنت ماهواره ای Viasat است. هفته گذشته، تحلیلگران اطلاعاتی آمریکایی نتیجه گرفتند که این حمله می تواند به خدمات جاسوسی نظامی روسیه، GRU نسبت داده شود، در همین ارتباط محققان سایبری معتقدند که بدافزار مورد استفاده در این حمله را شناسایی کرده اند.

کمپین DDOS روسیه

روسیه در اوایل ماه فوریه یک سری از حملات انکار دسترسی سرویس (DDOs) را علیه وب سایت های اوکراینی راه اندازی کرد. حملات جهت هدف قرار دادن وب سایت های بانکی و دفاعی اوکراین بود و گزارش شده که توسط آژانس اطلاعاتی روسیه، این حملات صوت گرفته است. این حملات به عنوان بخشی از تنش های بین اوکراین و روسیه قلمداد می شود.

روسیه همچنان به حملات DDOs به طور متناوب ادامه داده است، و در هفته اول ماه مارس، گروه های روسی با استفاده از Danabot، یک پلت فرم نرم افزارهای مخرب، برای راه اندازی حملات DDoS علیه وب سایت های وزارت دفاع اوکراین اقدام کرده اند.

هدف قرار دادن ارتش اوکراین در حملات فیشینگ

در ۲۵ فوریه، تیم واکنش اضطراری کامپیوتری در اوکراین، گروه هکری تحت حمایت دولت بلاروس UNC۱۱۵۱ را به تلاش برای هک کردن حساب‌های ایمیل پرسنل نظامی خود در یک حمله فیشینگ گسترده متهم کرد. هنگامی که هکرها به حساب‌های پرسنل نظامی نفوذ کردند، از دفترچه‌های ایمیل برای ارسال ایمیل‌های مخرب استفاده کردند. UNC۱۱۵۱ همچنین به یک کمپین فیشینگ دیگر با استفاده از ایمیل‌های نظامی اوکراینی برای هدف قرار دادن با بدافزار SunSeed متصل است.

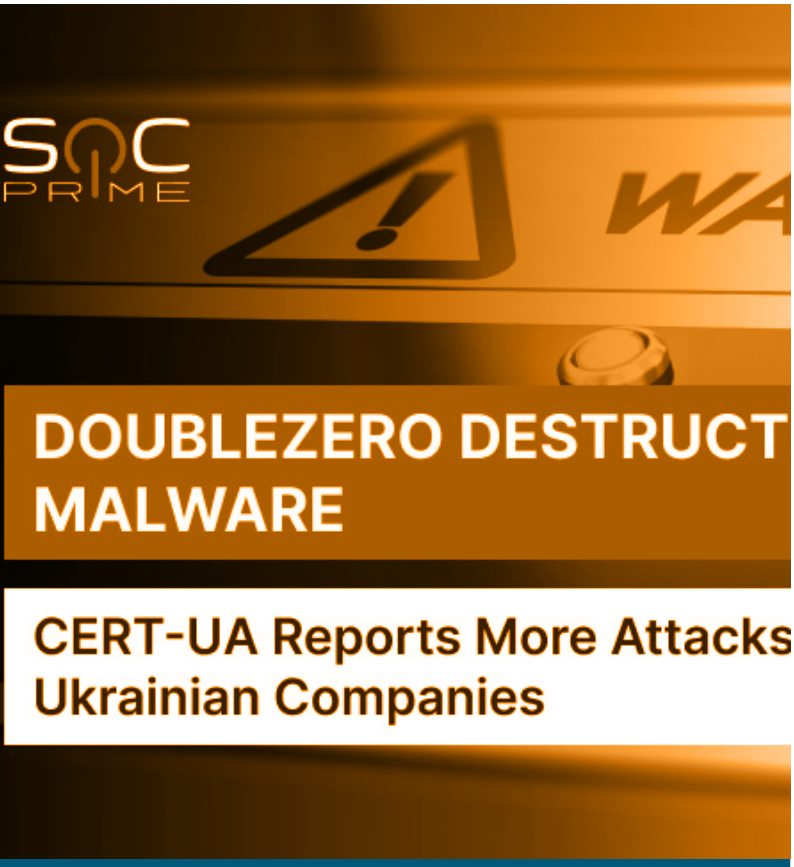
بدافزار CaddyWiper

محققان امنیتی در ۱۴ مارس یک بد افزار به نام CaddyWiper را شناسایی کردند که سیستم های اوکراینی را هدف قرار می دهد. این بدافزار به گونه ای طراحی شده است که به قربانی آسیب وارد کند و در عین حال دسترسی به شبکه آسیب دیده را حفظ کند.

قطعی ویاست

ارائه‌دهنده اینترنت ماهواره‌ای Viasat در ۲۴ فوریه، همان روزی که نیروهای روسیه به اوکراین حمله کردند، مورد حمله سایبری قرار گرفت که باعث قطع گسترده ارتباطات در سراسر اوکراین شد. Viasat تقریباً سه هفته پس از وقوع حمله همچنان برای بازگرداندن خدمات به بخش‌های آسیب‌دیده از کشور تلاش می‌کند. مقامات اوکراینی گفته اند که این حمله باعث "خسارت بزرگی در ارتباطات در همان ابتدای جنگ" شده است و آژانس امنیت ملی (NSA) تحقیقاتی را در مورد این هک اعلام کرده است.

بد افزار DoubleZero



اوکراین هشداری درباره نوع جدید بد افزار، با نام DoubleZero، که برای هدف قرار دادن نهادهای اوکراینی استفاده می شود، منتشر کرد. فعالیت این بدافزار برای اولین بار در ۱۷ مارس ۲۰۲۲ مشاهده شد، فعالیتی که طی آن عوامل تهدید حملات فیشینگ از آن برای ارائه بدافزاری استفاده کردند که محتوا را بازنویسی می کند و رجیستری ویندوز را قبل از خاموش کردن سیستم آلوده حذف می کند.

گروه ناشناس

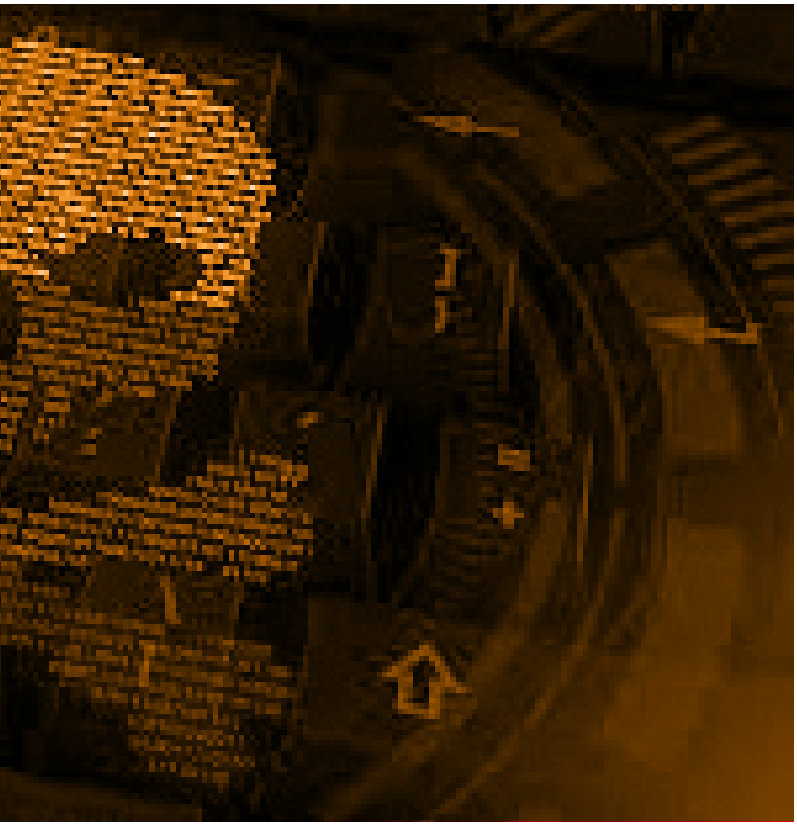
گروه ناشناس (Anonymous)، یک گروه غیرمتمرکز از هکتیویست ها، در ۱ مارس علیه دولت روسیه " اعلام جنگ " کرد و این گروه ادعا کرد که سایت هایی را که توسط رسانه های دولتی روسیه اداره می شد را غیرفعال کرده است. به نظر می رسد که Anonymous چندین بار در دو هفته گذشته رسانه های طرفدار روسیه را هدف قرار داده است. Anonymous همچنین مدعی شد که چندین پخش کننده اصلی روسیه از جمله کانال های تلویزیون دولتی روسیه ۲۴، کانال ۱، مسکو ۲۴ و سرویس های پخش Wink و Ivi را هک کرده است. جریان برنامه ها در این سرویس ها با کلیپ هایی از جنگ در اوکراین قطع شد.

ارتش فناوری اطلاعات اوکراین

ارتش فناوری اطلاعات اوکراین شاید یکی از بزرگترین تلاش‌های دولت اوکراین برای هماهنگ کردن اقدامات هکتیویست‌ها باشد. ارتش فناوری اطلاعات با ارسال اهداف مهم در یک کانال تلگرامی با صدها هزار عضو عمل کرده است.

ارتش فناوری اطلاعات وب سایت های چندین بانک روسیه، شبکه برق روسیه و سیستم راه آهن را هدف قرار داد و حملات DDoS گسترده ای را علیه سایر اهداف دارای اهمیت استراتژیک انجام داد. به نظر می رسد بخش عمده ای از قدرت سایبری اوکراین از ارتش فناوری اطلاعات سرچشمه می گیرد.

هکرها شرکت هوافضا و دفاعی دولتی روسیه Ros-tec را با حمله DDoS به وب سایت آن هدف قرار دادند . Rostec عامل این حادثه را «رادیکال‌های» اوکراینی و احتمالاً بخشی از ارتش فناوری اطلاعات، دانست و مدعی شد که از اواخر فوریه با حملات مستمری روبرو بوده است.



حملات پارتیزان های سایبری بلاروس به سیستم های قطار

پارتیـزان هـای سـایبری بـلاروس، گروهـی کـه در ژانویـه در اعتـراض بـه اسـتقرار نیروهـای روسـیه در ایـن کشـور حمـلات سـایبری را بـه سیسـتم‌های قطـار بـلاروس انجـام داد، بـه نظـر می‌رسـد در مـاه فوریـه بـه کمپیـن خـود علیـه راه‌آهـن بـلاروس ادامـه داده اسـت . ایـن حمـلات ، وب‌سـایت‌هایی را کـه بـرای خریـد بلیـط اسـتفاده می‌شـد، نابـود کردنـد و ممکـن اسـت داده‌هـای رمزگذاری‌شـده سیسـتم‌های مسـیریابی را داشـته باشـند، اگرچـه مقیـاس و شـدت حمـلات محتمـل و فراتـر از حـذف وب‌سـایت‌ها همچنـان مشـخص نیسـت.

بد افزار RURansom

ظهـور بدافـزار RURansom در ۱ مـارس ۲۰۲۲، نشـان دهنـده یکـی از اولیـن اسـتفاده هـا از بدافـزار توسـط هکـر هـای طرفـدار اوکرایـن اسـت و ممکـن اسـت نشـان دهنـده مرحلـه جدیـدی در کمپیـن سـایبری در حـال انجـام علیـه روسـیه باشـد. RURansom بـه عنـوان یـک بدافـزار عمـل مـی کنـد و بـه قربانیـان فرصتـی بـرای پرداخـت هزینـه بـرای رمزگشـایی سیسـتم هایشـان ارائـه نمـی دهـد. بـه نظـر مـی رسـد بدافـزار سیسـتم قربانـی را بـرای یـک آدرس IP روسـی بررسـی مـی کنـد و اگـر آن را پیـدا نکـرد، اجـرای آن را متوقـف مـی کنـد. بـه نظـر مـی رسـد کـه سـازندگان آن بـه طـور فعـال نسـخه هـای جدیـدی از آن را منتشـر مـی کننـد و ممکـن اسـت ایـن بدافـزار بـا گذشـت زمـان قـوی تـر شـود.

سایبر بین‌الملل

استرالیا قوانین جدید سایبری را اعلام می کند

پارلمان استرالیا مجموعه ای از قوانین سایبری را تصویب کرد که الزامات دقیق برای شرکت های استرالیایی را ایجاد می کند. این قوانین بر روی زیرساخت های اقتصادی و حیاتی متمرکز شده است. قوانین جدید در اصل بخشی از مجموعه های دیگری از قوانین متمرکز بر زیرساخت های حیاتی است که در سال ۲۰۲۱ اعمال شد، اما از بسته اصلی حذف شد تا دولت بتواند با صنعت خصوصی در ارتباط بماند. دولت همچنین یک صندوق جدید ۷.۵ میلیارد دلاری برای اداره سینگال استرالیا ارایه کرد، که به این اداره اجازه می دهد تا قابلیت های جدید سایبری را توسعه دهد و ۱۹۰۰ کارمند جدید را استخدام کند.

ICDT.IR