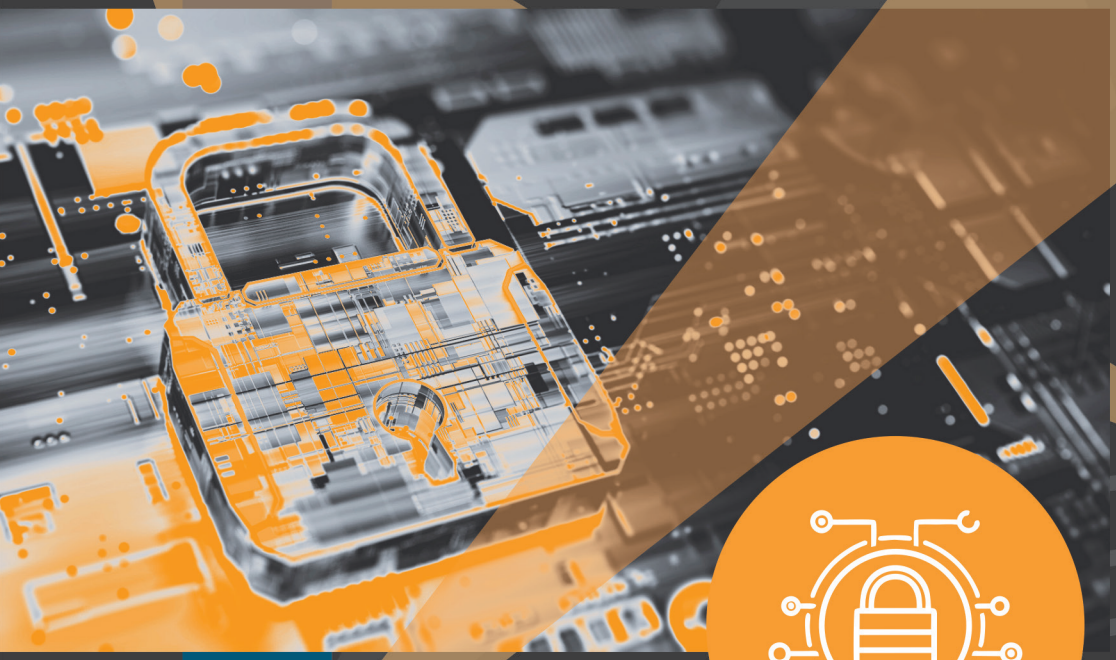
گزارش

مجمع ایرانی دفاع از حقیقت

Iranian Council For
Defending The Truth

خرداد ۱۴۰۰



امنیت سایبـــــری


بسم الله الرحمن الرحیم

فهرست

Iranian Council For
Defending The Truth

مقدمه

۱

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 از طرفی، به اعتراف مسئولین امریکایی بخش سایبری ایران از این توانایی برخوردار است که در تقابل با ایالات متحده از همین ضعف‌ها بهره‌برداری کند و به دشمن ضربه بزند. در نتیجه ما می‌توانیم زمین بازی را به نفع خود تغییر داده 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 این حوزه از مسائل بتوانند نسبت به وضعیت ایالات متحده از نگاهی جامع، کلان و به‌روز برخوردار شوند.

دیدکلی

رشد روزافزون عملیات‌های باج‌افزاری در جهان، نگرانی‌های قابل توجهی را در خصوص نحوه مقابله با آنها در میان کارشناسان و مقامات امنیتی بر انگیخته است. مقامات و مسئولین امریکایی که کشورشان را آماج اصلی این حملات یافته اند، تنظیم و اصلاح مقررات را در اولویت قرار داده اند. نکته محوری قانون‌های جدید، افزایش سرمایه گذاری‌های فدرال و بروزرسانی الزامات حفاظتی و امنیتی هم برای بخش دولتی و هم برای بخش خصوصی است. یکی از مهم‌ترین رخدادهای این هفته مربوط به مصادره باج پرداخت شده از سوی شرکت خط لولهColonial به هکرها توسط وزارت دادگستری امریکا بود. این اقدام چشم‌انداز جدیدی را در مقابله با باج‌افزارها در برابر کارشناسان امنیت سایبری گشود.

Iranian Council For
Defending The Truth

اخبار

۲

تغییر رویکرد فیس‌بوک در سانسور محتواهای مربوط به ویروس کرونا

به دنبال اتهامات مداخله روسیه در انتخابات ۲۰۱۶، شرکت‌های رسانه‌های اجتماعی تحت فشار قانون‌گذاران امریکایی قرار گرفتند تا اطلاعات گمراه‌کننده و نادرست را حذف و تعدیل نمایند.

هفته گذشته فیسبوک اعلام نمود که رویکرد این شرکت در قبال مطالب مرتبط با کوید ۱۹ تغییر نموده است. فیسبوک در شرایطی چنین تصمیمی را اتخاد کرده که شرکتهای رسانه های اجتماعی با فشار شدید برای تعدیل پست‌های مرتبط با ویروس کرونا مواجه هستند.

به مدت ۴ ماه فیسبوک هر گونه محتوایی که مدعی نشت ویروس کرونا از آزمایشگاهی در ووهان چین بود، سانسور می‌نمود، اما اکنون فیسبوک موضع خود را عکس نموده است. بنابراین فیسبوک دیگر این جملات که "COVID-۱۹ توسط انسان ساخته یا به وجود آمده است" حذف نمی کند. نماینده فیسبوک در واکنش به سوال خبرنگاران مشخص نکرد که چه تعداد از این گونه پست ها تا کنون حذف شده است. در این میان برخی از کارشناسان رسانه‌ای ادعا نموده اند که این شرکت بیش از ۱۸ میلیون پست را که کوید ۱۹ و سیاست های غلط در باره واکسن را مورد تهاجم قرار داده حذف کرده است.

در پی همه‌گیری کرونا، فشار سیاستمداران به خصوص دموکراتها برای ارتقای سیستم‌های تعدیل محتوا در رسانه‌های اجتماعی افزایش یافت؛ در سوی مقابل جمهوریخواهان نسبت به این مسئله اعتراض نمودند و ادعا کردند شرکتهای فناوری و سیستم‌های بررسی واقعیت (Fact Checking) مغرضانه عمل می‌کنند. شماری از قانونگذاران امریکایی، شرکتهای فناوری را تهدید به تدوین مقرراتی نموده اند که مصونیت‌های مسئولیت‌پذیری پلتفرم‌ها را کاهش می دهند؛ در صورتی که با ادعاهای دروغ در فضای مجازی مقابله نکنند.

توییتر می‌گوید از زمان آغاز همه‌گیری تاکنون بیش از ۸۴۰۰ توییت را حذف کرده و میلیون‌ها حساب را از زمان ارائه دستورالعمل‌های ویروس کرونا به چالش کشیده است. این دستورالعمل‌ها شامل منع انتساب همه‌گیری به "توطئه ای عمدی توسط نیروهای مخرب و / یا قدرتمند می‌شود."

اما این شرکت مشخص نکرده است که ادعاهای مربوط به این که مبدأ این ویروس یک آزمایشگاه است را حذف کرده یا نه.

شرکتهای فناوری که مدتهاست از ورود به کار بررسی واقعیت امتناع می ورزند، نوید یک رویکرد تهاجمی‌تر در سالهای آینده را داده‌اند. برای مثال فیسبوک دیگر فقط اطلاعات غلط راجع به واکسن‌های کرونا را سانسور نمی‌کند و اعلام کرده است ادعاهای غلط درباره عوارض جانبی و دیگر واکسن ها مثل ادعای این که واکسیناسیون کودکان منجر به اوتیسم می‌شود ، حذف می‌کند.

برخی از نظریه پردازان توطئه ادعا کرده اند که چینی ها عمدا ویروس کرونا را مهندسی کرده اند تا به عنوان سلاح بیولوژیک استفاده شود. هیچ مدرک رسمی مبنی بر این که ویروس به طور هدفمند ایجاد شده یا از نظر ژنتیکی در آزمایشگاه تغییر داده شده است وجود ندارد و بسیاری از کارشناسان می‌گویند ویژگی های ویروس این موضوع که ویروس ساختگی باشد بعید می‌سازد . حتی طرفداران فرضیه "نشت ویروس از آزمایشگاه"، به شدت منکر نظریه هایی هستند که ویروس را نوعی اسلحه زیستی مهندسی شده می‌پندارند.

حملات باج افزار، امنیت سایبری را در کانون توجه قرار داده است

در پی موج حملات پرهزینه و مخل کننده باج افزاری، تقریبا تمام قسمت‌های مختلف دولت فدرال درگیر شده‌اند. در این حملات هکرها، رایانه‌های قربانیان را مسدود نموده و تقاضای غرامت می‌کنند. حملات باج‌افزاری اخیر نشانگر وضعیت غیرقابل قبول از آسیب‌پذیری زیرساخت‌های حیاتی کشور امریکا است.

وضعیت پیش آمده سبب شده تا نگاه به مسئله باج‌افزارها به عنوان یک مسئله جنایی مزاحم تغییر یافته و به یکی از مسائل حیاتی امنیت ملی تبدیل شود. در واقع، مقامات کاخ سفید در حال بحث در مورد حملات باج افزار علیه صنایع مهم هستند که میتواند به قدری مخرب باشند که پیامد های جهانی داشته باشند. در همین راستا کاخ سفید صدور مجموعه ای از الزامات جدید امنیت سایبری برای خطوط لوله گاز را آغاز کرده است . هم چنین رئیس جمهور بایدن متعهد شده با ولادیمیر پوتین رئیس جمهور روسیه در اجلاس این ماه سران جی۷ در مورد باندهای باج افزاری که در خاک روسیه فعالیت می‌کنند، مذاکره نماید.

مقامات کاخ سفید در تلاش اند تا سایر سیاستمداران ایالت متحده را متقاعد سازند که اقدامات بیشتری در زمینه شفافیت مبادلات ارزهای رمزنگاری شده و این که پرداخت‌های باج افزاری بررسی شوند، احتیاج است. هدف آنها این است که از این مبادلات برای کشف گیرندگان باج‌ها استفاده نمایند و ردیابی گیرندگان باج‌ها برای مسئولین اجرای قانون تسهیل شود.

وزارت دادگستری این کشور ضمن تاکید بر این که شرکتها از پرداخت باج تا حد ممکن پرهیز کنند، از شرکتهای امریکایی خواسته است جهت پیشگیری از تکرار باج‌گیری، هنگام پرداخت باج به دولت اطلاع دهند.

وزارت دادگستری امریکا تحقیقات مربوط به باج‌افزارها را هم سطح با تحقیقات تروریسم قرار داده است.


RANSOMWARE


COLONIAL PIPELINE CO
213

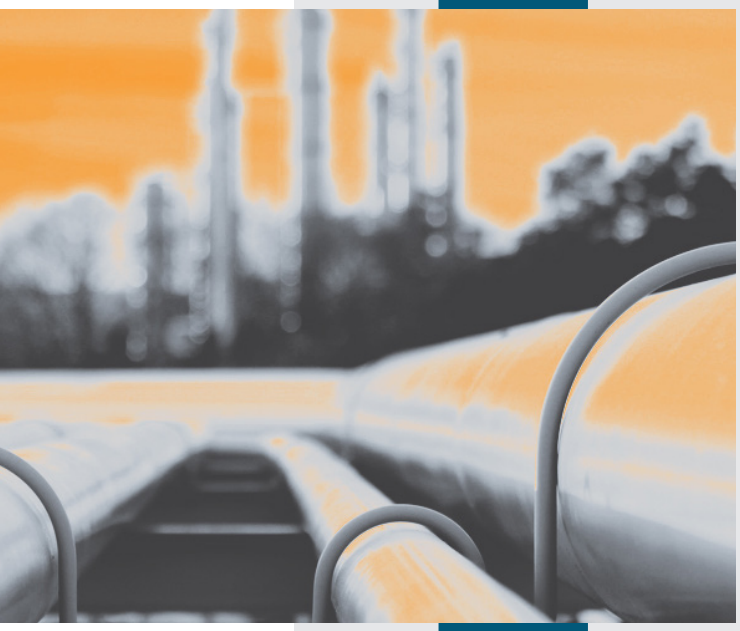
مبارزه وزارت دادگستری با هکرهای خط لوله COLONIAL

بیش از ۲ میلیون دلار از هکرهای باج افزارهای Colonial Pipeline توسط وزارت دادگستری مصادره شد. این اقدام یکی از مهم‌ترین ضربات وارده علیه جرایم سایبری سازمان یافته تا این زمان است. گرچه اقدامات قبلی مجریان قانون در امریکا، کسب و کار مجرمان سایبری را سخت کرده است ؛ اما به ندرت شرایطی را ایجاد کرده اند که این جنایات چندان سودآور نباشند.

اقدام وزارت دادگستری در واقع سود حاصل از هدیه ۴.۴ میلیون دلاری را که شرکت خط لوله با بیت‌کوین برای باز کردن قفل سیستم های رایانه‌ای خود پرداخت ، از بین برد. مابه التفاوت بین ۴.۴ میلیون دلار باج و ۲.۳ میلیون دلار توقیف شده اساساً به دلیل افت قیمت بیت کوین وهزینه پردازش نسخه باج افزار است.

این وزارتخانه تمام جزئیات عملیات را فاش نکرد ولیکن مدعی شد از روشی استفاده نموده که می تواند مجدداً آن را تکرار کند تا کلید کیف پول بیت‌کوین هکرها را بدست آورد و پول را از آن خارج نماید.

کارشناسان معتقدند مصادره باج Colonial به تنهایی برای دور کردن هکرها از چنین اهدافی کافی نخواهد بود ، اما این می تواند یک آغاز باشد. بابی چسنی ، مقام سابق وزارت دادگستری، نیز در این خصوص گفت: اگر وزارت دادگستری بتواند در چنین موارد برجسته‌ای مرتبا باج ها را پس بگیرد ، این امر حداقل می تواند برخی از باندهای باج افزار را متقاعد کند که بر روی قربانیانی تمرکز کنند که توجه پلیس و مردم را به خود جلب نمی‌کنند. در صورتی که هکرها از کسب درآمد از چنین اقداماتی ناامید شوند، یکی از اصلی‌ترین مشوق‌های خود را از دست خواهند داد.



هکرها اطلاعات حساس یک شرکت خط لوله دیگر را به سرقت بردند.

تیم هکرهای زینگ ده ها هزار پرونده سرقت شده از شرکت LineStar Integrity Services که به شرکتهای خط لوله خدمات ارائه می دهد، در اینترنت منتشر نمودند. محققان امنیتی می گویند ، داده های فاش شده می تواند شرکت های خط لوله را در برابر حملات جدی سایبری آسیب پذیر کند.

برت کالوو ، محقق Emsisoft گفت: "اگر شما بخواهید داده های یک شرکت خط لوله را بدزدید ، کافی است تا یک ایمیل فیشینگ نسبتاً معمولی به یک شرکت خط لوله دیگر ارسال کنید تا به مقصود خود برسید."

جاسوسی FBI از مجرمان با استفاده از نرم‌افزاری به نام ANOM

مجرمـان در سراسـر جهـان از تلفـن هـای هوشـمند ویـژه ای بـرای برقـراری ارتبـاط اسـتفاده مـی کننـد؛ بـا ایـن وجـود اف‌بـی‌آی توانسـته اسـت کـه مکالمـات آنهـا را شـنود کنـد. FBI بـه طـور مخفیانـه بـر روی تلفن‌هـای مجرمـان نرم‌افـزاری بـه نـام Anom را بارگـذاری نمـوده کـه بـه آنهـا اجـازه مـی‌داده مکالمـات جنایتـکاران را بـه مـدت ۳ سـال زیـر نظـر داشـته باشـند. در پایـان ایـن عملیـات ۸۰۰ نفـر دسـتگیر شـدند.

ژان فیلیـپ لکوفـه ، معـاون مدیـر اجرایـی عملیـات یوروپـول ، گفـت ایـن عملیـات "یکـی از بزرگتریـن و پیچیده‌تریـن عملیـات هـای اجـرای قانـون تاکنـون در مبـارزه بـا فعالیـت هـای مجرمانـه رمزگـذاری شـده اسـت." علیرغـم رمزگـذاری پیـام هـا ، آن پیـام هـا مسـتقیماً بـرای عوامـل اجـرای قانـون نیـز ارسـال مـی شـدند.

پرداخت باج به هکرها توسط بزرگترین شرکت تأمین و تولید گوشت در امریکا

JBS برای کمک به راه اندازی عملیات های فرآوری گوشت خود ، ۱۱ میلیون دلار باج به هکرها پرداخت کرد .

آندره نوگیرا ، مدیر اجرایی JBS ایالات متحده گفت ، این شرکت پس از آنکه اکثر کارخانه های JBS مجدد آنلاین شدند ، باج را پرداخت نموده است. وی گفت که این شرکت برای محافظت از کارخانه های JBS در برابر اختلالات بعدی و محدود کردن اثرات پایین دستی بر شرکت ها و کشاورزانی که به محصولات آن اعتماد می کنند ، این باج را پرداخت نمود.

نوگیرا گفت: "پرداخت پول به مجرمان بسیار دردناک بود ، اما ما کار درستی برای مشتریان خود انجام دادیم."

ارسال پست‌های تفرقه انگیز به آمریکایی‌های راستگرا توسط یک گروه مرتبط با روسیه

محققان شرکت تجزیه و تحلیل شبکه Graphika اعلام کردند: این کمپین با تقریباً ۲۰ حساب که بیشتر پس از انتخابات سال ۲۰۲۰ ایجاد شده اند ، وسعت یافته است. افراد پشت این کمپین در شبکه های اجتماعی جناح راست مانند Gab و Parler فعالیت می کنند. حساب های روسی به منظور تحقیر رئیس جمهور بایدن چنین اقدامی را نموده اند.

در گزارش این شرکت امنیتی آمده است: بازیگران مظنون روسی پس از اخلال در فعالیتهای قبلی‌شان پیش از انتخابات ۲۰۲۰ آمریکا ، تلاش خود را برای هدف قرار دادن مخاطبان راست افراطی آمریکا دو برابر کردند.“ ”حضور مستمر بازیگران سیاسی در سیستم عامل‌های جایگزین که فاقد سیاست‌های دقیق در مورد مداخلات خارجی هستند ، به آنها امکان ایجاد خط مستقیم ارتباطی با این جوامع را می دهد و از این طریق می‌توانند محتوای سیاسی سفارشی را ارائه دهند.“


eselected mirror modifier
r_ob
difier ob is the active ob


mirror_mod.use_y = True
mirror_mod.use_z = False
elif operation == "MIRROR_Z":
mirror_mod.use_x = False
mirror_mod.use_y = False
mirror_mod.use_z = True
#selection at the end -add back the d
mirror_ob.select= 1
modifier_ob.select=1
bpy.context.scene.objects.active = modifi
print("Selected" + str(modifier_ob)) # mo
mirror_ob.select = 0

سنا لایحه گسترده ای را برای تقویت فناوری ایالات متحده در مقابله با چین تصویب کرد

طبق این مصوبه ۵۰ میلیارد دلار سرمایه‌گذاری در صنعت تراشه‌های نیمه‌هادی از سوی دولت فدرال انجام خواهد شد. این لایحه در حالی مطرح گردیده که تسلط چین در فن آوری های نسل بعدی می تواند دولت و شرکت های ایالات متحده را نسبت به جاسوسی دیجیتال از جانب پکن بسیار آسیب پذیرتر کند.

در حال حاضر بسیاری از شرکت ها، تراشه‌های نیمه هادی را از چین تهیه می کنند و این لایحه می تواند مزیتی برای شرکت های نیمه هادی ایالات متحده باشد. این بودجه در حالی است که کمبود تراشه جهانی باعث آزار کسب و کارهای ایالات متحده از خودروسازان گرفته تا ماشین های شست و شوی سگ شده است.

از مفاد دیگر این لایحه آن است که یک اداره جدید فناوری و نوآوری در بنیاد ملی علوم تاسیس می‌شود. رئیس این اداره بر بودجه تحقیقاتی در زمینه هوش مصنوعی و علوم کوانتومی متمرکز خواهد بود.

تصویبت این لایحه مورد ستایش شرکت‌های سازنده چیپ‌ست های نیمه‌هادی قرار گرفت. رئیس‌جمهور بایدن در بیانیه ای تصویب این لایحه را توسط سنا ستود و گفت دولت او با نمایندگان مجلس همکاری خواهد کرد تا مطمئن شود که این قانون به سرعت به میز او می رسد.

لغو تحریم‌های ترامپ و جایگزین ساختن ممنوعیت‌های جدید علیه نرم‌افزارهای چینی

بایدن ممنوعیت های ترامپ برای TikTok و سایر برنامه های چینی را لغو کرد و پس از بررسی‌های امنیتی جدید، آنها را جایگزین خواهد کرد. دستور اجرایی که بایدن امضا کرد می تواند گام های جدیدی برای محدود سازی این اپلیکیشن ها ایجاد کند.

یک مقام ارشد دولت گفت: "دولت متعهد است که بابت حفاظت از داده های آمریکایی ها در برابر برنامه های خارجی مخاطره آمیز در سراسر کشور اطمینان حاصل کند ... از جمله برنامه های بزرگ و محبوب." "من فکر می کنم طیف گسترده ای از اقدامات وجود دارد که می توان در مورد آنها مذاکره نمود یا اجرایی شوند تا اطمینان حاصل شود که داده های آمریکایی ها به طور کامل حراست می شود."

دولت بایدن ممنوعیت سرمایه‌گذاری ایالات متحده در شرکت های چینی را به سایر شرکتهای بخش نظارت تعمیم داد.

دستورالعمل اجرایی صادر شده در روز پنجشنبه "مانع از سرمایه گذاری ایالات متحده در حمایت از بخش دفاعی چین می شود. در عین حال توانایی دولت ایالات متحده برای مقابله با تهدیدات شرکت‌های چینی فن‌آوری نظارت که - چه در داخل و چه در خارج از چین - به نظارت بر اقلیت های مذهبی یا قومی کمک می‌کنند یا به طریقی دیگر، سرکوب و نقض حقوق بشر را تسهیل می کند، گسترش می‌یابد. "

این دستور مرجع متصدی تحریم‌ها را از پنتاگون به وزارت خزانه داری تغییر داده است.


Data Breach
Cyber Attack
System Safety Compromised

هک دولت روسیه

به گفته یک شرکت امنیت سایبری ، هکرهای مرتبط با چین در پشت کارزاری قرار دارند که دولت روسیه را هدف قرار داده است.

گمانه زنی های اولیه این نظریه را مطرح نمود که یک دولت غربی مانند ایالات متحده عامل حمله است. از آن جایی که این حمله اندکی پس از آن رخ داد که که دولت بایدن روسیه را مسئول حمله سایبری SolarWinds دانست ؛ این استدلال مورد استقبال قرار گرفت. با این حال شواهد قوی حاکی از آن است که هکرهای مرتبط با چین در واقع عامل این حمله بوده اند.

بدافزار مورد استفاده در این حمله نسخه‌ای از نرم افزاری است که توسط یک گروه مرتبط با چین استفاده می شود. این نرم افزار این کمپین را به یک گروه هکری پیوند می دهد که از نظر تاریخی سازمان های روسیه و آسیا را هدف قرار داده است.

Iranian Council For
Defending The Truth

اخبار کوتاه

۳


U. S.
CYBER
COMMAND
NATIONAL
SECURITY
AGENCY
CENTRAL
SECURITY
SERVICE

- آژانس امنیت زیرساخت و امنیت سایبری وزارت امنیت داخلی در حال راه اندازی برنامه‌ای است که از محققان خارجی برای جستجوی اشکالات رایانه ای در وب سایت های خود دعوت می کند. این برنامه با مدیریت Bugcrowd و Endyna بخشی از مأموریت دولت است که باعث می شود هکرهای قانونی بتوانند چنین اشکالاتی را در وب سایتهای دولتی آسان تر فاش کنند.

ICDT.IR