خبر

۱۲ هزار گوشی موبایل قاچاق با اقدام سامانه همتا خاموش شد

ایسنا: رئیس انجمن واردکنندگان موبایل، تبلت و لوازم جانبی، از خاموش‌شدن ۱۲ هزار دستگاه موبایل در پی واردات گوشی‌های لوکس به جای گوش‌های ارزان‌قیمت خبر داد. این خاموشی از سوی «همتا» انجام شده است. همچنین تاکنون ۱۱ نفر ممنوع‌الخروج شده‌اند. مهدی اسدی در این زمینه گفت: «متأسفانه تعداد محدودی شرکت واردکننده از اوایل سال که البته شاید از سال گذشته هم این‌طور بوده، این کالاهای گران‌قیمت را به اسم کالاهایی مثل شیائومی و سامسونگ که ارزان‌تر هستند، وارد کرده‌اند. درواقع بازار و سامانه را دور زده‌اند و کالاهای مذکور را آورده‌اند؛ اما در اصل آیفون وارد کرده‌اند». رئیس انجمن واردکنندگان موبایل ادامه داد: «با توجه به شرایط پیش‌آمده، سامانه همتا تا زمان مشخص‌شدن وضعیت، ۱۲ هزار دستگاه را خاموش کرده است و ما پیگیری می‌کنیم تا این کالاها را که در دست مردم و فروشگاه‌هاست، روشن کنند تا تخلف برای واردکننده باشد و مردم متضرر نشوند». اسدی در ادامه درباره سوءاستفاده گروه واردکننده عنوان کرد: «به‌عنوان مثال برای یک گوشی که ۳۸ میلیون تومان هزینه یا سود بازرگانی و گمرکی داشته است، مبلغ کمتری در حدود ۵۰۰ تا ۷۰۰ هزار تومان پرداخت می‌کرده‌اند و ۳۸ میلیون پول دولت و سود اضافی به جیب این افراد طماع می‌رفته که خوشبختانه این موضوع مشخص شد و نهادهای نظارتی و امنیتی به طور جدی و هماهنگ پیگیر هستند». اسدی در پاسخ به این سؤال که قاچاقچیان چگونه سامانه همتا را دور زده‌اند؟ توضیح داد: «درواقع این افراد به نوعی سرقت کرده‌اند. اتفاق بسیار تلخی است. در سامانه‌ها طی فرایندهای مختلف شما متوجه باگ می‌شوید و این افراد هم تست کرده و فهمیده‌اند و در نهایت سوءاستفاده شده است. متأسفانه صنعت ما صدمات شدیدی در برند آیفون دید. شش ماه است هیچ‌یک از شرکت‌های ما سود نگرفته‌اند و این افراد ۳۸ میلیون جلو بودند و باقی شرکت‌ها ضرر می‌کردند». اسدی تأکید کرد که با توجه به تضییع حقوق مصرف‌کنندگان و آسیب به وجاهت صنف و منافع ملی، این موضوع از طریق سه قوه قضائیه، مجریه و مجلس در حال پیگیری است. او در ادامه خاطرنشان کرد که فعلا در واردات آیفون ۱۷ مشکلی وجود ندارد. او با اشاره به ممنوع‌الخروجی مدیرانی که در واردات اخیر نقش داشته‌اند، عنوان کرد که براساس اخبار غیررسمی گویا برخی از این مدیران از کشور خارج شده‌اند، اما حدود ۱۱ نفر در زمینه این پرونده شناسایی شده‌اند. رئیس انجمن واردکنندگان موبایل در ادامه بیان کرد که برای جلوگیری از تکرار این اتفاق قرار است بین بخش خصوصی، انجمن موبایل و کمیسیون اصناف موبایل و بخش‌های حاکمیتی و دولتی کمیته‌ای برگزار شود تا جلوی این اتفاقات و باگ‌های سامانه‌ای گرفته شود.

معاون شرکت مخابرات ایران پاسخ داد

چرا پرداخت‌کنندگان قبوض تلفن ثابت بدهکار شدند؟

ایسنا: در پی اعلام برخی مشترکان مبنی بر ثبت بدهی پیشین پس از پرداخت هزینه تلفن ثابت، معاون ارتباطات شرکت مخابرات ایران گفت: ممکن است مشترکانی که از طریق اپلیکیشن‌ها و روش‌های غیرمستقیم به پرداخت قبوض اقدام می‌کنند، با توجه به سیاست بانک‌ها، پرداختی آنها ۲۴ تا ۷۲ ساعت بعد برای وصول به مخابرات اعلام شود. برخی مشترکان اعلام کرده‌اند که با وجود پرداخت هزینه تلفن ثابت، برای آنها بدهی پیشین لحاظ شده و پرداخت‌های ماه قبل نیز محاسبه نشده است. در این راستا، داود زارعیان، معاون ارتباطات شرکت مخابرات ایران، درباره چرایی این موضوع اظهار کرد: پرداخت قبض از کانال‌های مختلفی امکان‌پذیر است که بعضی از آنها از طریق روش‌های مستقیم مانند تلفن ۲۰۰۰، اپلیکیشن مخابرات و ۲۰۲۰*# انجام می‌شود، بنابراین وقتی مشترک از این روش‌ها پرداخت می‌کند، بلافاصله سیستم ثبت و صورت‌حساب او صفر می‌شود که در حال حاضر بخش زیادی از مشترکان از این طریق قبض خود را پرداخت می‌کنند. او افزود: دسته دوم کسانی هستند که از طریق سایر اپلیکیشن‌ها یا روش‌های پرداخت مانند اپلیکیشن سایر بانک‌ها یا آپ، قبض خود را پرداخت می‌کنند. معمولا در این روش‌ها ممکن است سیاست بانک‌ها متفاوت باشد و برخی تا ۲۴ ساعت و برخی دیگر تا ۷۲ ساعت بعد به مخابرات اعلام کنند؛ اما آنچه مسلم است، این بوده که روش‌های پرداخت از دو روش دیگر خارج نیست و در دیرترین زمان ممکن ۷۲ ساعت و در بهترین حالت ممکن کمتر از یک دقیقه در سیستم، صورت‌حساب مخابرات اعمال می‌شود. معاون ارتباطات شرکت مخابرات ایران گفت: البته گاهی اوقات ممکن است تعداد محدودی کمتر از یک درصد مواردی هم وجود داشته باشد که به دلیل اختلال در سیستم بانکی یا یک اپلیکیشن این وصولی چند روز و بیشتر از ۷۲ ساعت طول بکشد، اما در نهایت وصولی به مخابرات اعلام می‌شود. همچنین قبض‌های صادره در دوره بعد براساس همین اعلام وصولی است که از طریق بانک‌ها به طرف مخابرات ارسال می‌شود. زارعیان گفت: در حال حاضر مشکلی در این زمینه نداریم، اما ممکن است آن دسته از مشترکانی که کمتر از ۷۲ ساعت قبل از صدور قبض، پرداخت داشتند، در صورت‌حساب دوره‌های‌شان بدهی اعلام شود که این هم ایرادی نیست و مشترک در دوره بعدی بستانکار می‌شود. او در پایان تشریح کرد: مشترکان برای انجام پیگیری‌های لازم می‌توانند با شماره ۲۰۲۰ تماس بگیرند، ضمن اینکه از طریق مخابرات من هم می‌توانند میزان بدهی خود را مشاهده کنند تا مطمئن شوند بدهکار هستند یا نیستند.

یادداشت

به این مردم اعتماد کنید

ادامه از صفحه اول

تجاوز اسرائیل به قطر شمار بیشتری از شهروندان ناراضی و معترض کشور ما را از تخیلات و تصورات القایی درباره منشأ و مقصود حمله اسرائیل به ایران رها کرد. حس همدلی و همدردی با مردم قطر و با مردم سایر کشورهایی که در معرض تجاوز و بمباران اسرائیل قرار دارند، در وجود مردم ایران رو به افزایش است.

اینکه تا این لحظه برخلاف کشورهای همسایه در کشور ما هیچ موجی از همدردی با قطر سامان داده نشده، به این دلیل نیست که این حس همبستگی و همدردی با قطر در ایران وجود ندارد؛ بی‌اعتمادی و واهمه جناح‌هایی از مردم خویش منشأ اصلی این سکوت و سردی است. این روحیه هفته گذشته کنسرت شجریان را لغو کرد و این هفته از موج همراهی و همبستگی مردمی با مردم قطر هراسید.

ایران در چشم جهانیان، به‌ویژه در چشم مردم عاصی اسرائیل، ایران دیگری بود، هرگاه روز جمعه گذشته بانگ هلهله و شادی مردم در میدان آزادی فلک را سقف می‌شکافت و این جمعه موج جمعیت، از هر قشر و طایفه‌ای، با سه پرچم ایران، قطر و فلسطین سراسر خیابان انقلاب را تزیین می‌کرد.

راه‌حل پیشنهادی تعویض پلاک خودروها با اعداد لاتین کارشناسی‌شده نیست

ادامه از صفحه اول

مسئول هزینه‌های فراوانی که از این راه به کشور وارد شده -و البته این هزینه‌ها به تضعیف زبان ملی و تمدنی فارسی نیز منجر شده و نوعی فرهنگ‌سازی علیه زبان تمدنی و تاریخی فارسی صورت گرفته- چه کسی یا کسانی خواهد بود؟ به مسئولان پلیس راهور پیشنهاد می‌کنم با تأمل بیشتر و کار مطالعاتی و کارشناسی براساس توجه به میراث تمدنی و ملی به تدبیر مسائل پیش‌روی بپردازند و متوجه هزینه‌های هر نوع تصمیم غیرکارشناسی باشند.

درز اسناد جدید نشان می‌دهد

صادرات سیستم فیلترینگ چینی به دنیا

تحلیلگران می‌گویند سیستم نظارتی که شرکت چینی Geedge می‌فروشد، قدرتی ترسناک به دولت‌ها برای محدودیت دسترسی به اینترنت می‌دهد که واقعا هیچ‌کس نباید داشته باشد

سایه فرنود

شنیدن خبرهایی از اینکه چین با کمک ابزارهای پیشرفته، فیلترینگی بسیار پیچیده در اینترنت ایجاد کرده که کاربران به‌راحتی نمی‌توانند به سرویس‌ها و وب‌سایت‌های خارجی دسترسی داشته باشند، حتی به کمک فیلترشکن، همیشه برای کاربران خارجی ازجمله ما ایرانیان ترسناک بوده است. حالا خبرهایی درز کرده که این کشور با کمک پدر سازنده «فایروال بزرگ چین» ابزارها پیشرفته‌تری برای کنترل کاربران در سراسر دنیا ساخته و آن را به برخی کشورهای آسیایی و آفریقایی نیز صادر کرده است. این ابزار کنترلی با الگوبرداری از دیوار آتش بزرگ چین، فناوری‌ای به دولت‌های سراسر جهان صادر می‌کند که امکان ردیابی لحظه‌ای ترافیک اینترنت، مسدودسازی وب‌سایت‌ها و ابزارهای فیلترشکن و جاسوسی از کاربران خاص را فراهم می‌کند.

از سوی دیگر این سیستم نه‌تنها بر کل ترافیک نظارت دارد، بلکه می‌تواند کاربران مشکوک را شناسایی کرده، موقعیت جغرافیایی آنها را ردیابی کند و محدوده‌های جغرافیایی خاصی (geofences) برای محدودکردن فعالیت‌شان تعریف کند.

علاوه بر این، ویژگی‌ای به نام «امتیاز اعتبار فردی» در این سیستم نظارتی در حال توسعه است که کاربران را ارزیابی می‌کند؛ به این صورت که هر کاربر یک امتیاز پایه ۵۵۰ دارد و تنها با تأیید هویت شامل شماره ملی، داده‌های تشخیص چهره و سوابق شغلی، امکان دسترسی به اینترنت بالاتر می‌رود. اگر این امتیاز به ۶۰۰ نرسد، کاربر عملا دسترسی به اینترنت نخواهد داشت. این درز عظیم اسناد، تصویر ترسناکی از کنترل دیجیتال و سانسور جهانی براساس یک فرمول چینی ارائه می‌دهد که آزادی آنلاین را در معرض تهدید جدی قرار داده است.

صادرات سانسور از نوع چینی

درز اطلاعاتی شامل بیش از صد هزار سند نشان می‌دهد که یک شرکت چینی کمترشناخته‌شده به‌طور مخفیانه سیستم‌های سانسور دیجیتال را که به نظر شبیه دیوار آتش بزرگ چین (Great Firewall) طراحی شده‌اند، به دولت‌های سراسر جهان فروخته است. اطلاعات درز کرده نشان می‌دهد که چگونه چین با راه‌اندازی یک سیستم پیچیده این امکان را به مشتریانش در سراسر دنیا می‌دهد تا به شکل آنلاین اطلاعات ردوبدل‌شده در اینترنت را زیر نظر داشته باشند و برخی وب‌سایت‌ها و ابزارهای فیلترشکن را نیز مسدود و از افراد خاصی نیز جاسوسی کنند.

Geedge Networks، شرکتی که در سال ۲۰۱۸ تأسیس شد و «پدر» زیرساخت سانسور دیجیتال گسترده چین یکی از سرمایه‌گذارانش است، خود را به عنوان ارائه‌دهنده خدمات نظارت شبکه اینترنت معرفی می‌کند. طبق اسنادی که بخشی از آن را وب‌سایت wired (یک نشریه آنلاین در زمینه فناوری و امنیت سایبری) منتشر کرده، این شرکت ابزارهای امنیت سایبری در سطح تجاری را برای «دستیابی به دید کامل و کاهش خطرات امنیتی» به مشتریان خود ارائه می‌دهد. در واقع، اسناد منتشرشده نشان می‌دهد که این شرکت یک سیستم پیچیده راه‌اندازی کرده است که به مشتریانش امکان می‌دهد اطلاعات آنلاین را زیر نظر داشته باشند، برخی وب‌سایت‌ها و ابزارهای VPN را مسدود کنند و از افراد خاص جاسوسی کنند.

پژوهشگرانی که اسناد لورفته را بررسی کرده‌اند، دریافته‌اند که این شرکت قادر است قابلیت‌های پیشرفته نظارتی را در قالب ابزارهایی عرضه کند که عملا یک نسخه تجاری‌شده از دیوار آتش بزرگ چین یا Great Firewall است؛ راه‌حل کاملی که شامل سخت‌افزاری است که می‌تواند در هر مرکز داده مخابراتی نصب شود و نرم‌افزاری که توسط مأموران دولتی محلی اداره می‌شود. اسناد همچنین به عملکردهای مورد نظر اشاره دارند که شرکت روی آنها کار می‌کند، مانند حملات سایبری به‌عنوان خدمت (cyberattack-for-hire) و محدودسازی جغرافیایی کاربران (geofencing). طبق اسناد لورفته، Geedge در حال حاضر در قزاقستان، اتیوپی، پاکستان، میانمار و همچنین یک کشور دیگر که هویتش مشخص نیست، فعال شده است. یک آگهی شغلی عمومی نشان می‌دهد که Geedge همچنین به دنبال مهندسانی است که بتوانند برای کارهای مهندسی به کشورهای دیگر سفر کنند.

مارلا ریورا، پژوهشگر فنی در InterSecLab، یک مؤسسه جهانی تحقیقات دیجیتال و جرم‌شناسی در مورد سیستم شرکت Geedge Networks می‌گوید: «این مانند شنود قانونی نیست که هر کشوری انجام می‌دهد، ازجمله دموکراسی‌های غربی. علاوه بر سانسور گسترده دیجیتال، این سیستم به دولت‌ها اجازه می‌دهد افراد خاص را براساس فعالیت‌هایشان در وب‌سایت‌ها هدف قرار دهند، مانند بازدید از یک دامنه مشخص». ریورا تأکید می‌کند: «سیستم نظارتی که Geedge می‌فروشد، قدرتی به دولت می‌دهد که واقعا هیچ‌کس نباید داشته باشد. این بسیار ترسناک است».

سانسوری و اقتدارگرایی دیجیتال به‌عنوان یک خدمت

طبق اسنادی که بخش‌هایی از آنها منتشر شده، در مرکز ارائه خدمات Geedge، ابزار دروازه‌ای به نام TSG (Tiangou Secure Gateway) قرار دارد که طراحی شده تا در مرکز داده‌ها (دیتاسنترها) نصب شود و می‌تواند برای پردازش، تحلیل و مسدودکردن ترافیک اینترنت یک کشور کامل مقیاس‌پذیر باشد. پژوهشگران می‌گویند که هر بسته ترافیک اینترنتی که از طریق این سیستم عبور می‌کند، امکان اسکن، فیلتر یا توقف کامل را دارد. علاوه بر نظارت بر کل ترافیک، اسناد نشان می‌دهند که سیستم همچنین امکان ایجاد قوانین اضافی برای کاربران خاص که مشکوک تلقی می‌شوند و جمع‌آوری فعالیت‌های شبکه‌ای آنها را فراهم می‌کند.

طبق اسناد لورفته، برای ترافیک اینترنت رمزنگاری‌نشده، سیستم قادر است اطلاعات حساس مانند محتوای وب‌سایت‌ها، رمز عبورها و ضمیمه‌های ایمیل را رهگیری کند. اگر محتوا به‌طور صحیح از طریق پروتکل Transport Layer Security رمزنگاری شده باشد، سیستم از بازرسی عمیق بسته‌ها (DPI) و تکنیک‌های یادگیری ماشین برای استخراج متادیتا از ترافیک رمزگذاری‌شده و پیش‌بینی اینکه آیا از ابزاری برای دورزدن سانسور مانند VPN استفاده می‌شود یا خیر، بهره می‌برد. اگر سیستم نتواند محتوای ترافیک رمزگذاری‌شده را تشخیص دهد، می‌تواند آن را به‌عنوان مشکوک علامت‌گذاری کرده و برای مدت مشخصی مسدود کند. یک اسکرین‌شات از داشبورد Geedge برای میانمار نشان می‌دهد که سیستم به‌طور هم‌زمان ۸۱ میلیون اتصال اینترنتی را نظارت می‌کند. سایر اسناد نشان می‌دهند که تا فوریه ۲۰۲۴، تجهیزات Geedge در ۲۶ مرکز داده در ۱۳ ارائه‌دهنده خدمات اینترنتی میانمار نصب شده بود. Frontiir، اپراتور محلی مخابرات میانمار، قبلا انکار کرده بود که «چیزی مرتبط با نظارت ساخته، برنامه‌ریزی یا طراحی کرده باشد»، اما در لورفتن اسناد مشخص شد تجهیزات Geedge را در مرکز داده خود نصب کرده است. Investcom، یک اپراتور مشترک میان شرکت‌های برمه‌ای و لبنانی، گفته بود که «از ادعاهایی مربوط به فناوری‌های شخص ثالث در میانمار مطلع است»، اما در پاسخ کتبی به پژوهشگران Justice for Myanmar از «تأیید یا انکار وجود سیستم‌های شخص ثالث» خودداری کرده است.

Geedge یک راه‌حل جامع سانسور می‌فروشد، شامل سخت‌افزار کنترل دروازه اینترنت. طبق گفته InterSecLab، Geedge در ابتدا از تجهیزات برندهای غربی مانند HP و Dell استفاده می‌کرد، اما بعدها به استفاده از سخت‌افزار تولیدشده توسط شرکت‌های چینی روی آورد تا تحت تأثیر تحریم‌های احتمالی قرار نگیرد. Cyber Narrator یکی دیگر از محصولات بنیادین Geedge است؛ رابط کاربری اصلی که به مشتریان دولتی غیرفنی امکان می‌دهد بر داده‌هایی که از پروتکل Tiangou Secure Gateway استفاده می‌کنند، نظارت کنند. در اسکرین‌شات‌های سیستم موجود در لورفتن اسناد، اپراتورهای Cyber Narrator می‌توانند موقعیت جغرافیایی هر کاربر اینترنت موبایل را براساس ارتباطات سرویس سلولی مشاهده کنند و همچنین تحلیل کنند که آیا کاربر از طریق خدمات VPN به اینترنت متصل شده است یا خیر. در اسناد منتشرشده مشخص شده که در میانمار، Geedge ۲۸۱ ابزار VPN محبوب را همراه با مشخصات فنی، قیمت اشتراک و امکان استفاده از آنها در این کشور مشخص کرده است. همچنین یک سند جداگانه ۵۴ اپلیکیشن را به عنوان اولویت بالاتر برای مسدودسازی مشخص کرده است. فهرست اولویت‌بندی ابزارها عمدتا خدمات تجاری محبوب مانند ExpressVPN و همچنین Signal، اپلیکیشن پیام‌رسان رمزگذاری‌شده را شامل می‌شود.

مشتریانی بیشتر در آسیا و آفریقا

در حالی که اسناد لورفته شامل هیچ رکوردی از قراردادهای تجاری نیست، اما مشتریان را با نام‌های رمزگذاری‌شده مرموز مورد بحث قرار می‌دهد. پژوهشگران توانستند چهار مورد از مشتریان دولتی خارجی را با بررسی اسناد لورفته، جست‌وجوی مکان‌های جغرافیایی مراکز داده، ردیابی سوابق حمل‌ونقل بین‌المللی از Geedge به سایر کشورها و استناد به گزارش‌های پیشین درباره مشارکت شرکت‌های چینی در فروش نرم‌افزار سانسور، مشخص کنند: قزاقستان، پاکستان، اتیوپی و میانمار.

همچنین اشاره‌ای به مشتری با کدی مشخص وجود دارد، اما شواهد کافی برای تعیین اینکه به چه چیزی اشاره دارد موجود نیست. به باور تحلیلگران تلاش‌های عمومی Geedge برای استخدام ممکن است اطلاعات بیشتری درباره برنامه‌های احتمالی توسعه آن ارائه دهد. در یک پلتفرم استخدام ثالث در چین، Geedge در حال استخدام یک مهندس ارشد عملیات و نگهداری در خارج از کشور است تا سیستم‌ها را در «کشورهای کمربند و جاده» مدیریت کند. آگهی شغلی می‌گوید ممکن است نیاز باشد سه تا شش ماه خارج از چین بگذرانند و به کشورهای پاکستان، مالزی، بحرین، الجزایر و هند سفر کنند.

به‌طور جداگانه، در ماه مارس، شرکت همچنین در حال استخدام مترجمان اسپانیایی‌زبان و فرانسوی‌زبان بود که بتوانند از کسب‌وکارهای بین‌المللی Geedge پشتیبانی کنند.

پژوهشگران معتقدند برخی از کارکنان Geedge قادرند به اطلاعات رهگیری‌شده توسط مشتری دسترسی داشته باشند که این می‌تواند یک خطر امنیت ملی برای دولت‌های مشتری باشد. تجربه Geedge در پاکستان همچنین نشان می‌دهد که این شرکت در حال ساخت محصولات براساس سخت‌افزارهای قابل تعامل با تجهیزات دیگر است تا برای مشتریان مختلف جذاب باشد. پیش از ورود Geedge به پاکستان، این کشور با Sandvine، یک شرکت کانادایی که تجهیزات بازرسی عمیق بسته‌ها (DPI) تأمین می‌کرد، همکاری کرده بود، اما این شرکت به دلیل تحریم‌های آمریکا از پاکستان خارج شد. وقتی Sandvine رفت، سخت‌افزار آن در مراکز داده پاکستانی باقی ماند. طبق اسناد لورفته، شرایط برای ورود Geedge مهیا بود و در نهایت توانست زیرساخت موجود را بازطراحی و تقویت کند.

پژوهشگران هشدار می‌دهند هیچ مستند واقعی در لورفتن اسناد وجود ندارد که ثابت کند سیستم Geedge مسئول سانسور اینترنتی در کشور خاصی است، اما تغییرات کلیدی عملیاتی در لاگ‌های فنی Geedge با رویدادهای قابل توجه هم‌زمان است. برای مثال، در اتیوپی، سیستم از حالتی که ترافیک را به صورت منفعل نظارت می‌کرد به حالتی که می‌تواند به‌طور فعال ترافیک را متوقف کند تغییر یافت؛ «فقط چند روز قبل از خاموشی اینترنت در فوریه ۲۰۲۳»، به گفته ریورا. در مجموع، لورفتن اسناد نشان می‌دهد که ۱۸ بار سیستم دروازه Geedge در اتیوپی از نظارت منفعل به دخالت فعال تغییر حالت داده که باعث کندشدن خدمات شده است.

از سوی دیگر اسناد نشان می‌دهد، سرویس VPN کانادایی Psiphon می‌تواند هدف سیستم Geedge باشد.

بازگشت به خانه

اسناد نشان می‌دهند Geedge فقط در حال صادرات سانسور دیجیتال چینی به خارج نیست، بلکه درس‌های آموخته‌شده در خارج را به داخل بازمی‌گرداند تا کنترل داخلی را بهبود دهد. سال‌ها پس از فروش فناوری‌های نظارتی به سایر کشورها، Geedge شروع به هدف‌گیری دولت‌های استانی چین نیز کرد تا نیازهای منحصربه‌فرد آنها را پوشش دهد. اولین مقصد: شین‌جیانگ. این منطقه که میزبان میلیون‌ها مسلمان اویغور است، در دهه گذشته شاهد نظارت دیجیتال گسترده توسط دولت چین بوده است.

هم‌زمان، طبق اسناد لورفته، Geedge پروژه‌های پایلوتی را در دو استان چینی دیگر، فوجیان و جیانگ‌سو نیز اجرا کرده است. اسکرین‌شات‌ها و سایر اسناد این پروژه‌ها نشان می‌دهند که تمرکز سیستم بر شناسایی وب‌سایت‌های کلاهبرداری مالی بوده که بیشتر در استان‌های ساحلی شرقی چین رخ می‌دهد.

علاوه بر جمع‌آوری اطلاعات ترافیک اینترنت به صورت گسترده و فردی، پروژه Geedge برخی قابلیت‌های آزمایشی را هم بررسی می‌کرد. اسناد لورفته نشان می‌دهد Geedge می‌خواست قابلیت Cyber Narrator را به‌روزرسانی کند تا:

۱. ارتباطات کاربران را تحلیل کند و براساس اپلیکیشن‌هایی که استفاده می‌کنند، افراد را گروه‌بندی کند.

۲. موقعیت جغرافیایی کاربران را از طریق ایستگاه‌های سلولی موبایل مشخص کند.

۳. برای برخی کاربران، محدوده‌های جغرافیایی خاص (geofences) ایجاد شود تا فعالیت‌های آنها محدود یا کنترل شود.

یک ویژگی نمونه دیگر که در اسناد لورفته به دست آمده، امتیاز اعتبار فردی است. در این ویژگی، هر کاربر اینترنتی یک امتیاز پایه ۵۵۰ دریافت می‌کند که با احراز هویت اطلاعات شخصی شامل شماره ملی، داده‌های تشخیص چهره و جزئیات شغلی قابل افزایش است. اگر امتیاز اعتبار کاربر بالای ۶۰۰ نشود، امکان دسترسی به اینترنت نخواهد داشت.

هنوز نامشخص است که آیا این ویژگی‌ها واقعا اجرائی شده و در سیستم‌های نظارتی Geedge در چین و خارج از کشور گنجانده شده‌اند یا خیر.

تلاش مداوم Geedge برای کشف اطلاعات از افراد به باور تحلیلگران بسیار نگران‌کننده است؛ زیرا شرکت قابلیت تزریق بدافزار به ترافیک اینترنت کاربران را نیز دارد. Lea Horne، پژوهشگر دیگری از InterSecLab در این مورد گفته است: «این روش کار را بسیار آسان‌تر می‌کند تا بتوان فرد خاصی را هدف قرار داد. در واقع به‌جای حدس‌زدن اینکه کاربر چه وب‌سایتی را بازدید می‌کند و اینکه این وب‌سایت آیا ازپروتکل HTTPS استفاده می‌کند یا خیر، می‌توانید تمام فعالیت‌های اینترنتی گذشته او را بررسی، یک وب‌سایت که معمولا از اتصال امن استفاده نمی‌کند پیدا و دفعه بعد که کاربر به آن وب‌سایت مراجعه می‌کند، بدافزار تزریق کنید». به باور او حتی اگر بعضی از این ویژگی‌ها هنوز در چین در حال آزمایش باشند، وقتی فناوری کامل و آماده شود، هر مشتری خارجی می‌تواند با یک به‌روزرسانی ساده نرم‌افزاری همان قابلیت‌ها را در سیستم خود فعال کند؛ این یعنی خطر کامل برای آزادی دسترسی به اینترنت.

جعبه‌ابزار

آموزش برنامه‌نویسی به‌زبان ساده

وقتی به فهرست بلندبالای اپلیکیشن‌ها نگاه می‌کردم، یک عنوان نظرم را جلب کرد؛ «آموزش برنامه‌نویسی» و این سؤال ایجاد شد که چگونه می‌توان با اپلیکیشن و بدون نیاز به لپ‌تاپ و کامپیوتر برنامه‌نویسی یاد گرفت و آن‌طور که از نظرات مردم مشخص بود چنین کاری امکان‌پذیر است. فقط باید اپلیکیشن «فینکا؛ آموزش برنامه‌نویسی» را نصب کنید. در اولین قدم برای استفاده از این اپلیکیشن از شما چند سؤال پرسیده می‌شود؛ اینکه چقدر با برنامه‌نویسی آشنایی دارید، چندساله هستید و به چه کاری مشغول هستید، در مورد اینکه از برنامه‌نویسی چه چیزی را دوست دارید یاد بگیرید «مفاهیم پایه و اصول برنامه‌نویسی، طراحی سایت، هوش مصنوعی، تحلیل داده، هک و امنیت، برنامه‌نویسی سخت‌افزار» و در طول روز چقدر می‌توانید برای آموزش وقت بگذارید. بعد از اینکه به این سؤالات پاسخ دادید، دوره مناسب به شما معرفی می‌شود. آن دوره یک درس‌نامه و یک تمرین دارد. در بخش درس‌نامه از صفر و به زبان ساده به شما برنامه‌نویسی آموزش داده می‌شود. وقتی آموزش هر بخش به پایان رسید، تمرینی متناسب با آن بخش خواهید داشت تا به صورت عملی هم آموزش ببینید. دوره‌های اولیه رایگان هستند و برای استفاده از سایر قسمت‌ها باید اشتراک خریداری کنید. در اپلیکیشن فینکا، علاوه بر دوره‌های آموزشی، قسمت گفت‌وگو هم می‌بینید که می‌توانید با کاربران و استادان مکالمه برقرار کنید و اگر سؤالی داشتید بپرسید و آنها شما را راهنمایی خواهند کرد. فینکا یک مدرسه دیجیتال برای آموزش مهارت‌های جدید است. این تیم در تلاش است تا یک‌سری مهارت‌هایی را که در مدارس به آنها پرداخته نمی‌شود، در قالب آموزش‌های جذاب به بچه‌ها آموزش دهد.

کتابخانه

تأثیرات متقابل سینما و گیم

در سال‌های اخیر شاهد ساخت فیلم‌ها و سریال‌های بسیار براساس بازی‌های ویدئویی بودیم. آخرین سریالی که در این زمینه دیدم، آخرین بازمانده از ما (the last of us) بود. سریالی که بسیاری آن را بهترین اقتباس از یک بازی ویدئویی نامیدند. البته در این سال‌ها بسیاری از این نوع فیلم‌ها هم اقتباس‌های ضعیفی بودند، اما در کل بازی توانسته تأثیر بسیاری روی سینما بگذارد، با اینکه سن سینما بیشتر از گیم است و شاید فکر می‌کردیم باید تأثیرات از سینما به بازی باشد، اما بازی هم در تغییر شکل سینمای معاصر دخیل بوده است. جاسمین کالی، در کتاب خود به نام «از گیم تا فیلم» به بررسی تأثیر نقش بازی در دگرگونی‌های شکلی سینمای امروز می‌پردازد. از گیم تا فیلم نخستین کتابی است که در حوزه تأثیرات متقابل گیم و سینما به فارسی ترجمه می‌شود. آن‌طور که در این کتاب آمده است: «در چند دهه گذشته دو صنعت مهم گیم (بازی) و سینما پیشرفت‌های وسیعی داشته‌اند و تحت تأثیر این پیشرفت‌ها هر دو حوزه تعاملات و تأثیرات متقابلی روی یکدیگر داشته‌اند. اقتباس‌های داستانی متقابلی که گیم‌ها و فیلم‌ها از یکدیگر داشته‌اند تا پیشرفت‌های گرافیکی و نزدیک‌ترشدن رابط‌های کاربری هر دو حوزه و شیوه‌های تماشای دوبعدی و سه‌بعدی در سینما و بازی همه و همه از تأثیر و تعامل این دو صنعت بر یکدیگر حکایت می‌کنند». در کتاب از گیم تا فیلم همچنین به تفاوت فیلم و گیم هم پرداخته می‌شود. از تفاوت‌های این دو می‌توان به تعاملی‌بودن آنها اشاره کرد. یعنی فیلم‌ها تماشا می‌شوند و با کاربران تعاملی ندارد، اما در گیم، تعامل بین کاربران صورت می‌گیرد. کالی در فصل اول این کتاب رویکردهای تازه و در حال تحول نسبت به حضور کامپیوترها و گیم‌های کامپیوتری در روایت‌های سینمایی را بررسی می‌کند. فصل دوم با نحوه نمایش گیم‌ها در روایت‌های سینمایی آغاز می‌شود و در ادامه بررسی می‌کند که گیم از نظر ساختاری چه تأثیراتی بر سینما داشته است. جاسمین کالی، نویسنده، کارگردان انیمیشن، فیلم‌نامه‌نویس و تهیه‌کننده تلویزیونی اهل کشور کرواسی است. او مدرک دکترای خود را در رشته فیلم‌نامه‌نویسی تعاملی از دانشگاه دوبلین دریافت کرد و سپس به تحقیق و نوشتن درباره مطالعات دیجیتال به‌ویژه رابطه سینما و بازی‌های کامپیوتری پرداخت.