امنیت سایبری

آمریکا، بریتانیا و هلند درباره عملیات سایبری حکومت ایران علیه مخالفانش هشدار دادند

رادیو فردا

۶ دقیقه پیش

ایالات متحده، انگلیس، و هلند روز سه‌شنبه ۲۴ شهریور در یک هشدار مشترک امنیت سایبری، جزئیات جاسوس‌افزاری را منتشر کردند که به گفته آنها عوامل مرتبط با حکومت ایران از آن برای هدف قرار دادن مخالفان، فعالان و روزنامه‌نگاران استفاده می‌کنند.

مرکز ملی امنیت سایبری بریتانیا اعلام کرد عوامل سایبری مرتبط با دولت ایران از خانواده‌ای از جاسوس‌افزارها موسوم به «CHOSEN BRICK» برای سرقت ایمیل‌ها، پیام‌ها و دیگر اطلاعات حساس از طریق کارزارهای «فیشینگ هدفمند» در بستر پیام‌رسان‌هایی مانند واتس‌اپ و تلگرام استفاده کرده‌اند.

پل چیچستر، مدیر عملیات مرکز ملی امنیت سایبری بریتانیا، در بیانیه‌ای گفت: «جزئیات این کارزار سایبری نشان می‌دهد ایران چگونه بی‌رحمانه از نظارت دیجیتال برای سرکوب منتقدان حکومت استفاده می‌کند؛ ایمیل‌ها و پیام‌ها را به سرقت می‌برد و به دستگاه‌های افراد دسترسی پیدا می‌کند.»

خبرگزاری رویترز می‌گوید سفارت ایران در لندن به درخواست برای اظهارنظر دربارهٔ این گزارش پاسخ نداد.

بر اساس این هشدار، این بدافزار می‌تواند اطلاعات فهرست مخاطبان، ایمیل‌ها و حساب‌های شبکه‌های اجتماعی را جمع‌آوری کند، از محتوای صفحه نمایش دستگاه‌ها تصویربرداری کند و به میکروفون آنها دسترسی پیدا کند.

مرکز ملی امنیت سایبری بریتانیا همچنین اعلام کرد اطلاعات شخصی برخی قربانیان بعدتر در وب‌سایت‌های افشای اطلاعات طرفدار ایران منتشر شده است.

این هشدار یک روز پس از آن منتشر شده که خبرگزاری فارس، نزدیک به سپاه پاسداران، از راه‌اندازی سامانه‌ای با عنوان «علاج» خبر داد که هدف آن به نوشته این خبرگزاری «شناسایی و مجازات خائنان خارج نشین» است.

قوه قضائیه جمهوری اسلامی نیز روز دوشنبه اعلام کرد در ماه‌های گذشته ۲۴۰ فقره از اموال و دارایی‌های شهروندان ایرانی را توقیف و ۱۸۲ حساب بانکی متعلق به آنان را مسدود کرده و خبر داد بخشی از اموال توقیف‌شده متعلق به خبرنگاران شبکه‌هایی چون ایران اینترنشنال و من‌وتو و دیگر رسانه‌های فارسی‌زبان و «چهره‌های سرشناس» ساکن خارج از کشور است.

به گفته مرکز ملی امنیت سایبری بریتانیا، مهاجمان وابسته به حکومت ایران اغلب در پیام‌رسان‌ها خود را به‌عنوان افرادی مورد اعتماد قربانیان معرفی می‌کردند و شیوه ارتباط خود را متناسب با هر هدف تغییر می‌دادند.

در برخی موارد نیز، مهاجمان از اسناد جعلی، از جمله نتایج ساختگی آزمایش‌های ام‌آرآی، برای متقاعد کردن قربانیان به دانلود بدافزار استفاده کرده‌اند.

مرکز ملی امنیت سایبری بریتانیا، پلیس فدرال آمریکا، اف‌بی‌آی، و سرویس اطلاعاتی هلند در این هشدار مشترک اعلام کردند که ایران «تقریباً به‌طور قطعی» از عملیات سایبری برای کمک به سرکوب افرادی که آنها را تهدید می‌داند، استفاده می‌کند.

در هشدار اف‌بی‌آی آمده است که این گزارش به‌روزرسانی هشدار دیگری است که در مارس منتشر شده بود و در آن درباره تلاش‌های وزارت اطلاعات ایران برای استفاده از این بدافزار به‌منظور جمع‌آوری اطلاعات درباره اهداف خود هشدار داده شده بود؛ اطلاعاتی که بعداً توسط هکری با نام مستعار «هاندالا هک» در اینترنت منتشر شده است.

گروه یا هویت سایبری «هاندالا» از زمان آغاز جنگ ایران، چندین شرکت و فرد آمریکایی را هدف حملات خود قرار داده است. از جمله این حملات می‌توان به یک حمله سایبری مخرب علیه شرکت «استرایکر»، تأمین‌کننده تجهیزات و خدمات پزشکی مستقر در ایالت میشیگان، در ماه مارس اشاره کرد.

این گروه همچنین در اواخر همان ماه، ایمیل‌های شخصی کش پاتل، رئیس اف‌بی‌آی، را افشا کرد.

بیشتر در این باره:

گزارش آنتروپیک از نقش هوش مصنوعی در عملیات تبلیغاتی و امنیتی نهادهای مرتبط با ایران

شرکت آمریکایی «آنتروپیک»، سازندهٔ مدل هوش مصنوعی «کلود»، روز ۱۹ شهریور در گزارشی از برخی فعالیت‌های سایبری مرتبط با جمهوری اسلامی پرده برداشت که یکی از آنها ساخت افزونه‌ای مخرب برای

مرورگر فایرفاکس برای جمع‌آوری گستردهٔ هویت کاربران شبکه‌های اجتماعی بود.

این شرکت گفت این مرکز وابسته به حکومت ایران که در شهر قم مستقر بود، ابزارهای دیگری برای مرتبط کردن شمارهٔ تلفن با هویت افراد، صفحات فیشینگ شمارهٔ ملی و گزارش انبوه حساب‌های تلگرامی نیز در این مجموعه ساخته شده بود.

این مطلب بخشی از:

بایگانی | امنیت سایبری | گزارش‌های خبری
