گزارش «شرق» از حمله‌های هکری علیه نهادها و ارگان‌های کشور

«هکتیویسم»، تهدیدی برای تهران؟

شرق: در کنار اوج‌گیری تحریم‌ها، تحرکاتی برای اجماع‌سازی علیه تهران، تشدید فشار سیاسی و دیپلماتیک، پررنگ‌ترشدن تلاش برای انزواسازی ایران و... به نظر می‌رسد اکنون جنگ سایبری و مشخصا جنگ هکری علیه ایران نیز در حال انجام است که سرفصل نوینی از تقابلات را ذیل عنوان «هکتیویسم» در بستر فضای صفر و یک شکل داده است.

در تازه‌ترین مورد گروه هکری موسوم «بلک ریوارد» (پاداش سیاه) مدعی شده بود با رخنه اطلاعاتی به شرکت مادر نیروگاه هسته‌ای بوشهر (یکی از زیرمجموعه‌های شرکت مادرتخصصی تولید و توسعه انرژی اتمی ایران) به اسناد و اطلاعاتی از جزئیات فعالیت‌های هسته‌ای ایران دست یافته است. در اسناد جدیدی که این گروه منتشر کرده است، عکس‌ها و نقشه‌هایی از تأسیسات هسته‌ای، قراردادهای میان نیروگاه بوشهر و شرکت‌های دیگر، فیش‌های پرداخت و اسناد مربوط به ارزیابی ایمنی تأسیسات دیده می‌شود. گروه بلک ریوارد پیش از انتشار اسنادی که ادعا کرده بود با رخنه به شرکت مادرتخصصی تولید و توسعه انرژی اتمی ایران به دست آورده است، در یک تهدید، پیامی در شبکه‌های اجتماعی منتشر کرد و خواهان آزادی زندانیان سیاسی شد.

این گروه روز شنبه (۳۰ مهرماه) در پایان ضرب‌الاجل یک‌روزه خود به مقامات ایران، با انتشار پیام جدیدی در حساب تلگرام خود، ۵۰ گیگابایت از اسناد هک‌شده این شرکت را منتشر کرد. پیرو این اقدام گروه هکری بلک ریوارد، دیروز یکشنبه اداره کل دیپلماسی عمومی و اطلاع‌رسانی سازمان انرژی اتمی ایران در بیانیه‌ای اعلام کرد که مطالب منتشرشده در فضای مجازی مبنی بر نفوذ به سرور پست الکترونیک شرکت تولید و توسعه انرژی اتمی با هدف جلب توجه عموم و فضاسازی‌های رسانه‌ای صورت گرفته است.

در این بیانیه عنوان شده است: «براساس گزارش دریافتی از واحد فناوری اطلاعات شرکت مادرتخصصی تولید و توسعه انرژی اتمی، دسترسی غیرمجاز از مبدأ یک کشور خارجی مشخص، به سامانه پست الکترونیک این شرکت منجر به انتشار محتوای برخی از پست‌های الکترونیکی در فضای مجازی شد. در پی این امر، واحد فناوری اطلاعات شرکت تولید و توسعه انرژی اتمی براساس ترتیبات پیش‌بینی‌شده و در کوتاه‌ترین زمان ممکن ضمن انجام اقدامات لازم و پیشگیرانه، موضوع را از ابعاد مختلف مورد بررسی قرار داد و گزارش اولیه خود را به مسئولان سازمان انرژی اتمی ارائه داد».

این اعلامیه ضمن تأکید بر اینکه محتوای موجود در ایمیل‌های کاربران حاوی پیام‌های فنی و تبادلات معمول و جاری روزمره است، تصریح کرد: «هدف از انجام این‌گونه تلاش‌های غیرقانونی که از روی استیصال انجام می‌شود، به منظور جلب توجه عموم، فضاسازی‌های رسانه‌ای و عملیات روانی بوده و فاقد هرگونه ارزش دیگری است».

از تپندگان تا بلک ریوارد، انانیموس، عدالت علی و...

اگرچه به گواه برخی تحلیل‌ها اولین حمله هکری علیه ایران به ژوئن ۲۰۱۰ بازمی‌گردد؛ حمله‌ای که به وسیله ویروس استاکس نت و با هدف حمله به تأسیسات هسته‌ای نطنز با مشارکت آمریکا و اسرائیل طراحی شد و در ۱۲ سال گذشته هم این جنگ هکری و حملات سایبری با شدت و ضعف ادامه دارد؛ اما در چند سال اخیر عملا این جنگ و هکتیویسم به سرفصل جدید و جدی برای تقابل با ایران بدل شده است.

گروه هکری بلک ریوارد پیش از این رخنه به شرکت مادرتخصصی تولید و توسعه انرژی اتمی ایران، هک ایمیل کارکنان دانشگاه الزهرا و حمله سایبری به پرس‌تی‌وی و ارسال ایمیلی با عنوان «زن، زندگی، آزادی» را به کارمندان و پرسنل این شبکه انگلیسی‌زبان جمهوی اسلامی ایران هم در کارنامه خود دارد؛ اما به جز پاداش سیاه، گروه‌های دیگری هم طی اعتراضات یک ماه اخیر و پیش از آن هم حملاتی را علیه مراکز و نهادهای ایران شکل دادند که حتی در موارد شدت آثار این حملات سایبری به تغییر مقامات و مسئولان کشور منجر شد که یک نمونه آن برکناری محمدمهدی حاج‌محمدی، رئیس سابق سازمان زندان‌ها و اقدامات تأمینی و تربیتی کشور است که در پی حمله سایبری گروه عدالت علی در مرداد ماه سال گذشته به دوربین‌های زندان اوین صورت گرفت.

افزون بر آن گروه هکری «عدالت علی» ۱۲ بهمن سال گذشته در حساب توییتری خود صورت‌جلسه یک نشست قرارگاه ثارالله درباره وضعیت اقتصادی و به‌ویژه پیامدهای حذف ارز ترجیحی را منتشر کرد که روی آن مهر «خیلی محرمانه» خورده و گزارشی از جلسه ۳۰ آبان سال قبل است. همچنین در تاریخ ۲۹ شهریور ۱۴۰۱ این گروه توانست وب‌سایت ستاد امر به معروف را هک کند. در تاریخ ۱۲ بهمن ۱۴۰۰ تلویزیون اینترنتی ایران موسوم به تلوبیون هم به دست این گروه هک شد. به تاریخ ۱۸ بهمن ۱۴۰۰ مجددا رسانه‌ها خبر هک‌شدن دوربین‌های زندان قزلحصار از سوی این گروه را منتشر کردند. البته همراه با این فیلم گفته می‌شود اسنادی شامل اسامی برخی از بازداشت‌شدگان آبان ۹۸ و اتهامات واردشده به آنها منتشر شد.

ساعت ۹:۳۳ شنبه‌شب (۱۶ مهر ۱۴۰۱) و در جریان اعتراضات چند هفته اخیر هم شبکه خبر و شبکه یک صداوسیمای ایران برای لحظاتی هک شد که برخی منابع خبری این هک را به گروه عدالت علی ارتباط می‌دهند. این حمله سایبری هم نهایتا به برکناری معاون توسعه و فناوری رسانه منجر شد؛ اقدامی که سرنوشتی مشابه با محمدمهدی حاج‌محمدی، رئیس سابق سازمان زندان‌ها را برای رضا علیدادی رقم زد. تنها گروه هکری عدالت علی نبود که در جریان اعتراضات یک ماه اخیر وارد جنگ سایبری با ایران شد. به طور مشخص از نیمه‌شب سی‌ام شهریورماه گروه هکری انانیموس پیام تهدیدآمیزی خطاب به سایت‌های دولتی ایران نوشت و در ادامه تصویری را منتشر کرد و مدعی شد که سایت رسمی دولت از دسترس خارج شده است. پس از این حمله سایبری، گروه انانیموس در یکی از پیام‌های معروفش با رمز «MahsaAmini» خطاب به ایران نوشت: «ما اینجاییم، ما با شما هستیم... منتظر ما باشید».

با این تهدید، درگاه ملی دولت هوشمند به همراه سایت صداوسیما و سایت بانک مرکزی مورد حمله هکرهای منسوب به این گروه قرار گرفت. اینها علاوه بر آن است که این گروه هکری اسکرین‌شات صفحه و آی‌پی‌های مختلفی را هم که برای ورود به این سایت تلاش کرده بودند، منتشر کرد. البته اخباری هم مبنی بر هک بخشی از اطلاعات خبرگزاری فارس منتشر شد. باوجوداین این گروه هکری در این زمینه موضعی نگرفت. افزون بر اینها بانک ملی ایران، وزارت اقتصاد، وزارت نفت، اپراتور همراه اول، سایت رهبر انقلاب و... هم مورد حمله هکری انانیموس قرار گرفتند. البته گروه هکری انانیموس در توییتی هم مدعی شد که ۳۰۰ دوربین در ایران را هک کرده است. این گروه اطلاعات بیشتری در این زمینه نداد.

با نگاهی به این مجموعه حملات سایبری منسوب به انانیموس به نظر می‌رسد نمی‌توان همه آنها را درست دانست؛ کمااینکه مرکز ملی فضای مجازی در اطلاعیه‌ای اعلام کرد که ادعاهای اخیر گروه انانیموس درباره حملات سایبری به سایت‌های دولتی کشور مانند مجلس شورای اسلامی، وزارت امور اقتصاد و دارایی، وزارت نفت یا اپراتور همراه اول صحت نداشته و تکذیب می‌شود. مضافا بانک ملی و نیز سخنگوی هیئت‌رئیسه مجلس یازدهم (سیدنظام‌الدین موسوی) هم از اساس حمله سایبری انانیموس را رد کردند. روابط‌عمومی بانک مرکزی نیز اعلام کرد: «مشکل پیش‌آمده ناشی از هک تنها یک اختلال فنی و قابل رفع است». با این همه تعدادی از این حملات ادعایی هم صحت داشتند که به اذعان سخنگوی مرکز ملی فضای مجازی، مواردی که بعضا به دلیل هک دچار مشکل شده‌اند در کوتاه‌ترین زمان ممکن برطرف شد.

البته پیش‌تر از عدالت علی، بلک ریوارد و انانیموس، گروه هکری «تپندگان» در فاصله یک‌ساله بین ۹۷ تا ۹۸ توانست شش حمله هکری را انجام دهد که نخستین مورد آن هک‌شدن فرودگاه بین‌المللی شهید هاشمی‌نژاد مشهد بود و بعد از آن هک‌شدن فرودگاه بین‌المللی شهید مدنی تبریز، حمله سایبری به شهرداری تهران، صداوسیمای ایران، سفارت ایران در برلین، هک‌شدن مجدد فرودگاه مشهد و حمله به سایت سازمان تأمین اجتماعی در سال ۹۸ از سوی همین گروه انجام شد.

هکتیویسم و ضرورتی که مغفول مانده است

عملیات سایبری و آمادگی‌هایی که برخی کشورها کسب کرده‌اند، مؤید آن است که رقابت تسلیحات سایبری آغاز شده است، ضمن آنکه شدت تأثیرگذاری حملات هکری نشان‌دهنده عمق ورود فضای سایبری به عملکردهای راهبردی دولت‌هاست. مسئله فوق در عین حال مبین آن است که چنین حملاتی با ماهیت استراتژیک، احتمالا در مرکز امنیت ملی هر کشوری قرار دارند.

با این حال امروزه دیگر جنگ سایبری و حملات هکری، نه از سوی دولت‌ها، بلکه به‌وسیله گروه‌های هکری صورت می‌گیرد که هر روز بر تعداد آنها افزوده می‌شود. شاید دراین‌بین این‌گونه به نظر آید که عمده این گروه‌ها از حمایت و پشتیبانی مالی و فنی کشورهای منطقه‌ای و فرامنطقه‌ای با هدف حمله به ایران برخوردارند هستند؛ اما نباید این گزاره را نادیده گرفت که اساسا گروه‌ها و حملات هکری امروزه ماهیتی متفاوت از گذشته پیدا کرده‌اند و گاهی مستقل از دولت‌ها و جریان‌های سیاسی و با اهداف خاص خود عمل می‌کنند؛ حتی در کشورهای اروپایی و ایالات متحده نیز گروه‌های هکری داخلی اقدام به حملاتی علیه اماکن، تأسیسات و نهادهای حساس با اهداف مختلف کرده‌اند.

در همین زمینه اسناد منتشرشده در مؤسسه امنیتی «سایبرپروف» (cyberproof) نشان می‌دهد بیشترین تعداد حمله‌های سایبری در سال ۲۰۲۱ در کشورهای چین، آمریکا و برزیل به وقوع پیوسته است. پس از این سه کشور هند، آلمان، ویتنام، تایلند، روسیه، اندونزی و هلند بیشترین میزان حمله از سوی هکرها در سال ۲۰۲۱ را تجربه کرده‌اند. البته همیشه بیشترین میزان حمله سایبری به سایت‌های دولتی و شخصی در یک کشور به معنای بالاترین حجم آسیب به آن کشور خاص نیست، به طوری که در سال ۲۰۲۱ کشور کره جنوبی ۷۲ میلیارد دلار بر اثر جرائم سایبری متضرر شده و پس از این کشور آمریکا با ضرر چهارمیلیاردو صد میلیون دلاری در جایگاه دوم قرار دارد.

با استناد به همین آمارها درخصوص میزان خسارات حملات سایبری به دو کشور کره جنوبی و آمریکا روشن است که این حملات مشخصا از نظر مالی چه هزینه گرافی را برای کشورها به دنبال خواهد داشت. همین هزینه‌ها و بار مالی حملات سایبری سبب شده است تا این مقوله به سرفصل نوینی از جنگ ترکیبی امروز علیه ایران بدل شود؛ چراکه هزینه صدمات مستقیم و غیرمستقیم این حملات در کوتاه و بلندمدت، به اندازه هزینه حاصله از حملات هوایی یا موشکی زیاد است. بنابراین در این صحنه پیچیده «هکتیویسم» باید نهادها ذی‌ربط توانایی‌های تهاجمی و تدافعی خود را به طور هم‌زمان و مستمر ارتقا دهند.