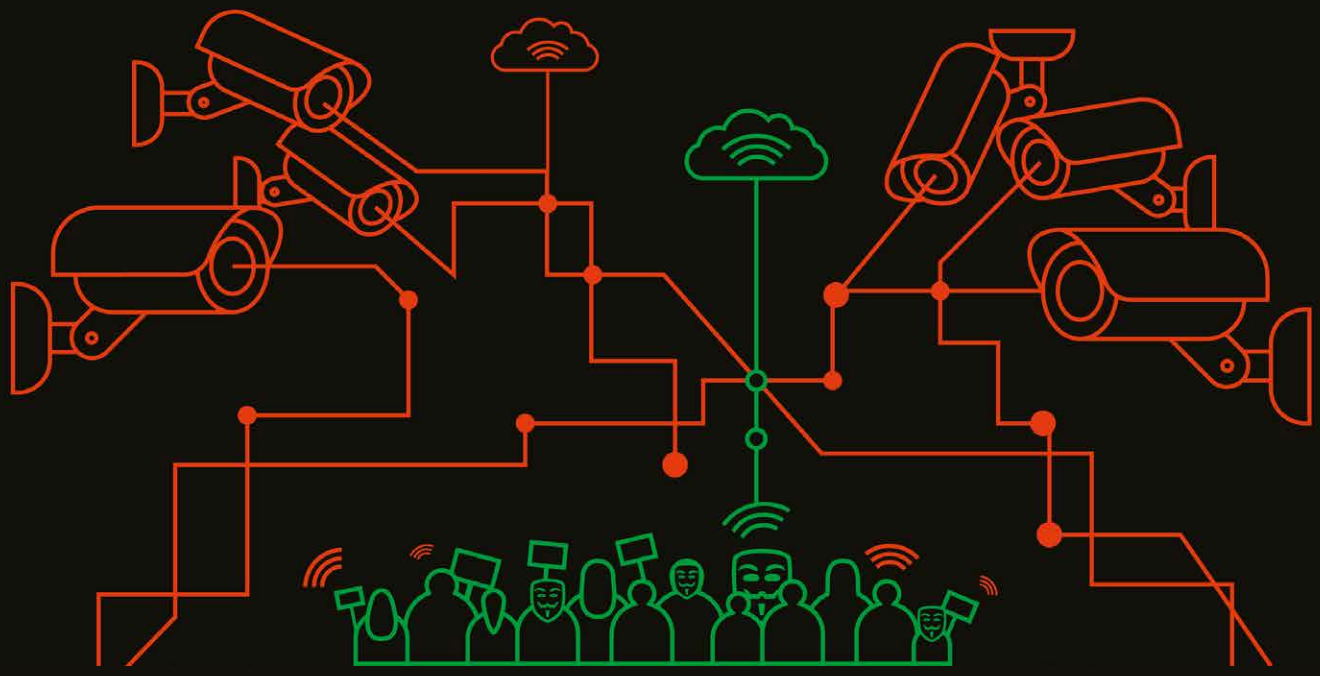


جمع‌بندی دیده‌بان هکری - تیر - آذر ۱۴۰۱

اعتراضات دموکراسی‌خواهی در میان نظارت دولتی و رقابت هکری

فیلتربان
ژانویه ـ مارس ۲۰۲۳

دومین گزارش دیده‌بان هَکری (هکرواچ) آخرین رویدادها و مسایل دنیای مجازی را در ایران بررسی می‌کند. فضای غالب بر این گزارش جنبش «زن، زندگی، آزادی» است که در اثر مرگ دلخراش ژینا مهسا امینی شکل گرفت. او زن جوان کُردی بود که در آبان ۱۴۰۱، به‌هنگامی که به جرم بدحجابی در بازداشت بود، جانش را از دست داد. گسترش اعتراضات در حالی بود که کنترل و نظارتِ دولت بر شهروندان و رقابت ژئوپلیتیک میان ایران و اسراییل دامنه‌ی وسیع‌تری پیدا کرد. گزارش کنونی بر دو موضوع متمرکز است: نخست، مروری خواهیم داشت بر ظرفیت‌های سایبری ایران برای هدف قرار دادن ناراضیان و حمله به شبکه‌هایی که علیه جمهوری اسلامی فعالیت دارند. به ویژه، آن بخش از ابزارهای نظارتی که دولت در همکاری با بخش خصوصی به آنها دست یافته است. این اطلاعات بر اساس افشاگری‌های تازه‌ی رسانه‌ها و هکرهای ناشناس تنظیم شده است.

دوم، دیده‌بان هکری به آسیب‌پذیری‌های سایبری دولت می‌پردازد که مواردی از آن را در یک سلسله حمله‌های هکریِ ظاهراً ارگانیک به شبکه‌های دولتی و سازمان‌های وابسته به آنها شاهد بوده‌ایم. تصویری که از این بررسی به دست می‌آید این است که دولت حاضر است به نام امنیت ملی دست به حمله‌هایی به دشمنان خود بزند که ریسک بالایی دارند. همزمان، منابعی که باید صرف امنیت و دفاع از شبکه‌های داخلی شود صرف این عملیات می‌شود. این سیاست باعث می‌شود شهروندان ایران به طور جمعی احساس ناامنی کنند.

پیش‌گفتار

در آبان ۱۴۰۱، به دنبال مرگ ژینا مهسا امینی دختر ۲۲ ساله‌ی کُرد در بازداشت گشت ارشاد، که به احتمال زیاد به دلیل رفتار خشن پلیس با او رخ داد، اعتراضات دموکراسی‌خواهی در ایران بالا گرفت. این اعتراض‌ها که نخست برای پاسخگویی دولت به مرگ ژینا، برابری جنسیتی، و احترام به حقوق زنان شکل گرفت به سرعت تبدیل به تجمع‌هایی با مطالبات درهم‌تنیده برضد رژیم شد که کنشگران قومیتی، دینی، برابری جنسیتی، حقوق کارگران، و جنبش دانشجویی را گرد هم آورد. از هنگام وقوع جنبش سبز در سال ۱۳۸۸، تظاهرات آزادی‌خواهانه به این وسعت در سراسر کشور بی‌سابقه بود، رویدادی که دنیا را شگفت‌زده کرد. دولت به سرعت در صدد خاموش‌کردن اعتراضات برآمد.

معترضان نه تنها در معرض بازداشت در خیابان بودند، بلکه دستگاه‌های نظارتی دولت امنیت فیزیکی و تماس‌های آنها را، چه در محل تظاهرات و چه خارج از آن، به خطر می‌انداختند. بسیاری از این معترضان پس از بازگشت به خانه دستگیر شدند، زیرا گوشی‌های همراه آنها به وسیله‌ی برج‌های مخابراتی ردگیری شده بود. عده‌ای دیگر از طریق شماره ثبت موبایل‌شان به دام افتادند، شماره‌هایی که دولت طی سالهای اخیر دست به جمع‌آوری آنها زده است. به هنگام اعتراض‌ها، جزییات بیشتری از قابلیت‌های نظارتیِ وسیع دولت آشکار شد که ناراضیان سیاسی، کنشگران اتنیکی و حقوق بشری، مجرمان احتمالی، و شهروندان عادی را هدف قرار می‌داد.

این ابزارهای وسیع نظارتی در همکاری با بخش خصوصی و چندین شرکتِ صوری فراهم شده‌اند که نیروهای امنیتی را علیرغم تحریم‌های شدید آمریکا از زیر ضربه خارج می‌کنند. گزارش کنونی سهم شرکت‌های خصوصی را در یاری رساندن به دولت برای سرکوب معترضان بررسی می‌کند.

طی دو دهه‌ی گذشته، جمهوری اسلامی بارها امنیت ملی را بهانه قرار داده تا ظرفیت‌های کنترل سایبری خود را بگستراند. از اواسط دهه‌ی ۷۰ شمسی، دولت به‌تدریج قابلیت‌های سایبری‌اش را چنان وسعت بخشیده که بتواند یک سیاست چندسویه را دنبال کند، یعنی همزمان نارضایتی داخلی را فرو بنشاند، سیاست‌های ژئوپولیتیکی منطقه را شکل دهد، و پاسخ دشمنان را هم بدهد ــ همه‌ی این‌ها با هزینه‌ی نسبتاً پایین! با این محاسبات، ایران چند گروه هکری را حمایت کرده و ظاهراً از هکرهای ناشناس کمک گرفته تا حمله‌هایی علیه ناراضیان داخلی و دشمنان خارجی مثل اسراییل، عربستان، و آمریکا، از طریق جاسوسی، خرابکاری، و باج‌گیری تدارک ببیند. این گزارش تعدادی از این گروه‌ها را بررسی می‌کند که علیه اهداف گوناگونی

مثل اقلیت‌های دینی، کسب و کارهای اسراییلی، حتی دولت آلبانی، دست به خرابکاری زده‌اند.

ایران، با وجود سرمایه‌گذاری‌های کلان برای عرضه‌ی خود به عنوان یک قدرت مهم سایبری، به شدت در برابر حمله‌های هکری آسیب‌پذیر است. هکرهای ناشناسی که در جامه‌ی ناراضیان سیاسی فعالیت دارند، به قصد جاسوسی یا خرابکاری، بارها شبکه‌های غیرنظامی ایران را هدف قرار داده‌اند. گرچه شناساییِ این هکرها با قطعیت ممکن نیست، دست‌کم در یک مورد در سال ۱۴۰۰، حمله به سیستم دیجیتال پمپ بنزین‌های ایران به اسراییل نسبت داده شده است. افزایش عملیاتِ امنیتی و خرابکارانه در فضای مجازی مطابق با تشدیدِ تنش میان دو کشور صورت می‌گیرد و باعث می‌شود شهروندان ایران نتوانند به نحو امن و آسوده به زیرساخت‌های دیجیتال کشور دسترسی داشته باشند.

اعتراضات اخیر در کشور این وضعیت را وخیم‌تر کرده است. ظاهراً در حمایت از معترضان، چندین گروه هکری به میدان آمدند، وبسایت‌های دولتی را پایین کشیدند، اسناد محرمانه را فاش ساختند، و برنامه‌هایی را که گفته می‌شد دولت برای سرکوب معترضان طرح ریخته برملا کردند. برخلاف حمله‌های پیشین که عموم مردم راا بدون استثنا هدف قرار می‌داد (مثل حمله به پمپ‌های بنزین)، حمله‌های اخیر فقط به قصد خرابکاری در نهادهای دولتی و افشاگری از مأموران آن صورت گرفت. این حمله‌ها همچون آینه شعارهای تظاهرکنندگان را بازتاب می‌داد و احساس اعتماد و همبستگی در میان آنان به وجود می‌آورد. در این افشاگری‌ها، به ویژه میزان همکاری رسانه‌های اصول‌گرا با دستگاه‌های نظامی و امنیتی روشن‌تر شد. درز بی‌سابقه‌ی اطلاعات باعث افشای مأموریت‌های فراقانونی ارگانهای گوناگون شد که سیستم نظارت و کنترل وسیعی را به خدمت می‌گیرد. در این گزارش به برخی از این ارگان‌ها و جزییات عملیات آنها می‌پردازیم.

اما شناسایی سررشته عملیات هکری همچنان محل مناقشه است. اگر احیانا ارتباطاتی با بازیگران دولتی، مثل اسراییل، شناسایی شود که از عملیات هکری برای برنامه‌های مخفیِ خود سود می‌گیرند، این امر می‌تواند در درازمدت به اعتماد معترضان و ایمنیِ دیجیتالِ آنها صدمه بزند. هرچه بیشتر عملیات هکری تبدیل به پوششی شود برای خسارت وارد کردن به شبکه‌های داخلی، به همان میزان نیز دولت ایران در صدد مقابله به مثل برخواهد آمد و طبعاً ناراضیان و معترضان را هم قربانی خواهد ساخت. این وضعیت به دولت این امکان را می‌دهد که به بهانه‌ی یک هکِ ساده‌ی به اصطلاح افشاگرانه، معترضان را به خاطر اخلال در نظم عمومی و تشویق خشونت مورد پیگرد قرار دهد. آنگاه خود دولت می‌تواند به همان تاکتیک هک کردن و «افشاگری» رو آورد و رهبران اپوزیسیون را تهدید کند و در میان معترضان بذر بی‌اعتمادی بیفشاند.

نشانه‌هایی مشاهده می‌شود که ایران خسارت ناشی از نشت اطلاعات را قبول کرده و در صدد ترمیم نهادهای حکومتی و حفاظت از افراد طرفدار رژیم برآمده است. اما هر درسی که آموخته می‌شود باید بدون تبعیض به نفع همه‌ی شبکه‌های داخلی به کار گرفته شود. وگرنه، خطر تشدید نابرابری در فضای مجازی و از طریق این فضا بیشتر می‌شود، و مردم برای حفاظت از داده‌های شخصی خود از ابتدایی‌ترین معیارهای امنیت سایبری محروم خواهند ماند. تخصیص ندادن بودجه و ارجح نبودن امنیت شبکه‌های داخلی باعث آسیب‌پذیری بیشتر در برابر تهدیدهای بازیگران دولتی و غیردولتی خواهد شد که بهای آنرا متاسفانه مالیات‌دهندگان خواهند پرداخت. حکمرانی

بد در زمینه‌ی امنیت سایبری عواقب وخیمی برای منابع عمومی و ایمنی جمعی به عنوان حقوق بنیادی بشری خواهد داشت.

توانایی‌های سایبری ایران
حمله‌های داخلی

تیر ۱۴۰۱ ـ اپلیکیشن «اهل بها» مربوط به آیین بهاییت

در تیرماه ۱۴۰۱، صاحب‌نظران امنیت سایبری در مورد ایمنی اپلیکیشن «اهل بها» به کاربران هشدار دادند. این نرم‌افزار نخستین بار در بهمن ۱۴۰۰ به وسیله‌ی یک کانال تلگرامی به همین نام در اختیار عموم قرار گرفت. این کانال اقلیت آیین بهایی را خطاب قرار داده و آنها را ترغیب به نصب اپلیکیشن «اهل بها» می‌کرد. اما این یک نرم‌افزار عادی نبود. «اهل بها» در فروشگاه‌های رایج مثل گوگل‌پلی عرضه نمی‌شد. این اپلیکیشن فقط به شکل یک فایل عظیم پنجاه گیگابایتی در قالب بسته‌ی اندرویدی (APK) در همان کانال تلگرامی قابل دانلود و نصب بود.

متخصصان امنیت سایبری با کاوش بیشتر کشف کردند که در کُدنویسی «اهل بها» یک روزنه‌ی عقبی تعبیه شده که از طریق آن می‌توان به داده‌های کاربران دسترسی پیدا کرد. این نرم‌افزار به دو آدرس اینترنتی یا آی‌پی مرتبط بود. نخستین آی‌پی به فهرست منوی اپلیکیشن (مثل دعا و مراسم مذهبی) وصل بود. اما دومین آی‌پی قادر به استخراج اطلاعات خصوصیِ کاربران بود که این اطلاعات را به یک سِرورِ ناشناس در یک کمپانی جعلی در لندن منتقل می‌کرد. همین آی‌پی پیوندهایی دارد با زیرساخت‌هایی که در عملیات سایبری دیگری به دست گروه هکری وابسته به حکومت ایران به نام «مادی واتر» در سال ۹۸ شمسی به اجرا گذاشته شد.

«مادی واتر» یک گروه جاسوسیِ سایبری است که دست‌کم از سال ۱۳۹۶ فعال بوده و سازمان‌های خصوصی و دولتی بسیاری را در خاورمیانه، آسیا، آفریقا، اروپا، و آمریکای شمالی هدف قرار داده است، از جمله سازمان‌های مخابراتی، دولت‌های محلی، نهادهای نظامی، و شرکت‌های نفت و گاز. در دی ماه ۱۳۹۹، فرماندهی سایبری وابسته به وزارت دفاع آمریکا گزارش داد که گروه «مادی واتر» وابسته به نهادهای امنیتی جمهوری اسلامی است.

تیر و مرداد ۱۴۰۱ ـ لب‌دوختگان

۲۵ تیر ۱۴۰۱، هکر ناشناسِ ضد دولت ایران به نام «لب‌دوختگان» نام دست‌کم پانزده نفر را فاش کرد که با دو شرکت جعلیِ وابسته به سپاه پاسداران کار می‌کردند. این فهرست بر اساس یافته‌های خبرنگار تحقیقی باب دیاچنکو به چنگ لب‌دوختگان افتاده بود.

در تاریخ ۴ اسفند ۱۴۰۰، باب دیاچنکو اطلاعاتی را به چاپ سپرد، با قسمت‌هایی که خط سیاه خورده بود، از یک دیتابیس یا مخزن اطلاعاتی بزرگ که داده‌های شخصی شهروندان ایران را ذخیره می‌کرد و از طریق حساب‌های کاربری شبکه‌های اجتماعی به شماره تلفن، اطلاعات ثبت‌نام رای دهندگان، مشخصات ثبت خودرو، مکان جغرافیایی گوشی همراه، و غیره دسترسی پیدا می‌کرد. این بانک اطلاعت روی سِروری میزبانی

می‌شد که در ایران بود (اکنون دیگر وجود ندارد) و وبسایت «secnerd[.]ir» را اداره می‌کرد. این سِرور به شهادت لب‌دوختگان با شرکتی به نام «تکنولوژی ناجی» در ارتباط است که از کمپانی‌های صوری وابسته به سپاه و متعلق به منصور احمدی است.[۱] لب‌دوختگان موفق شد یک شرکت صوری و بدلی دیگر وابسته به سازمان امنیت سپاه و خدمات سایبری آن کشف کند به نام «افکار سیستم» که مدیریت آن را احمد خطیبی به عهده داشت.

لب‌دوختگان اسنادی را به چاپ رساند که پیوند میان دو شرکت صوری و بازیگران سایبری وابسته به سپاه مثل «کوبالت میراژ»، «بچه گربه ملوس»[۲]، و «تانل‌ویژن» را نشان می‌داد. در سال‌های گذشته، این گروه‌ها در فعالیت‌های تخریبی سایبری مثل اخاذی در سراسر جهان دست داشته‌اند.

آبان ۱۴۰۱ ـ سیستم سیام (SIAM)

مورد بالا تنها باری نبود که مقامات ایرانی در ماه‌های اخیر مبادرت به نظارت وسیع شهروندان کردند. در آبان ۱۴۰۱، خبرگزاری «اینترسپت» گزارش مفصلی به چاپ رساند که یکی از ابزارهای هنوز ناشناخته‌ی سانسور حکومتی را به نام «سیستم سیام» افشا می‌کرد. این یک برنامه برای اینترنت است که از راه دور ارتباطات ماهواره‌ای را که در اختیار سازمان تنظیم مقررات و ارتباطات رادیویی (رگولاتوری) قرار می‌گیرد دستکاری می‌کند.

طبق اسناد محرمانه‌ی داخلی از «آریانتل»، یک اپراتور شبکه موبایل در ایران، که گفته می‌شود اینترسپت آنها را از یک هکر دریافت کرده، سیستم سیام این امکان را به اپراتورهای خود می‌دهد که به تلفن‌های مشتریان خود دسترسی یافته و کارکرد این گوشی‌ها را دستکاری کنند. این کار از طریق اخذ شماره‌ی تلفن (وصل به یک برج ارتباطاتی خاص) و انطباق دادن آن با شماره‌ی IMEI انجام می‌شود که یک زنجیره‌ی شماره‌ای منحصر به فرد است و هر گوشی در دنیا دارای یکی از این شماره‌های IMEI به طور اختصاصی است.

این نوع ردیابی باعث می‌شود روش‌های معمول حفظ حریم خصوصی مثل تعویض سیم‌کارت بی‌اثر شود، زیرا حتی بعد از عوض کردن سیم‌کارت، شماره‌ی IMEI ثابت می‌ماند و عوض نمی‌شود. گذشته از این، سیستم سیام قادر است سرعت ارتباط را از ۴G و ۳G به ۲G کاهش دهد، و با این کار از نقص‌های امنیتی ۲G استفاده کرده، پیام‌ها را رمزشکنی و حرکت افراد یا گروه‌ها را ردگیری کند، و ابرداده‌هایا داده‌های پنهان مربوط به تماس‌های افراد، از جمله پیام‌های کلامی و صوتی، پیامک‌ها، و حجم داده‌ها را استخراج کند.

به طور خلاصه، سیستم سیام یک سیستم دخالت و ردیابیِ قانونی است که دولت با کمک از آن می‌تواند هر زمان که لازم شد منتقدان و ناراضیان و اعتراضات را سرکوب

---

۱ در ماه مه ۲۰۲۲، دو ماه قبل از لب‌دوختگان، یک وب‌سایت متن باز به نام «داعش‌هانتر» (شکارچی داعش) مدعی شد میان وبسایت «SECNERD» و منصور احمدی و شرکت صوری‌اش «ناجی تکنولوژی» ارتباط وجود دارد.

۲ «بچه گربه ملوس» دارای تاریخچه‌ی بلندی از حمله‌های سایبری است علیه کنشگران سیاسی، تحلیلگران، و سایر کارشناسان منطقه‌ای. اخیراً کشف شد که این گروه در لباس مبدل به نام نویسندگان مشهور یا رهبران اندیشکده‌ها خود را جا زده و سعی در استخراج اطلاعات از متخصص منطقه‌ای کرده است.

کند. باید دانست که این سیستم کاملاً متفاوت است از روش‌های استاندارد و قانونیِ رهگیری که تشکیلات ۳GPP و کمیته‌های استاندارد ETSI وضع کرده‌اند. این استانداردها در مورد روندها و تبادل‌هایی است که قانوناً تعریف شده و به منظور صدور مجوزهای قانونی، فعال کردن رهگیری ارتباطی، و ارائه‌ی محتوا به مراجع قانونی است.

مهر ۱۴۰۱ ـ گربه خانگی

سیستم سیام تنها ابزاری نیست که با آن جمهوری اسلامی از شهروندان جاسوسی می‌کند. در مهرماه ۱۴۰۱، پژوهشگران شرکت امنیت سایبری ESET بدافزار «گربه خانگی» را ردیابی کردند. گربه خانگی یک بازیگر سایبری وابسته به دولت است که لااقل از سال ۱۳۹۴ به جاسوسی از شهروندان ایرانی پرداخته است.

«گربه خانگی» ایرانیان و گروه‌های ضددولتی در خاورمیانه را هدف می‌گیرد و گوشی‌های آنها را زیر نظارت می‌آورد. شرکت امنیت سایبری «چک پوینت» موفق شد یک کارزار گسترده‌ی جاسوسی از طرف گربه خانگی را در سال ۱۳۹۶ کشف کند که ایرانیانی که اصلیت کُردی یا تُرکی داشتند، و در مواردی هواداران داعش را هدف قرار داده بود. این عملیات جاسوسی از سال ۱۳۹۴ با استفاده از بدافزارهای اندرویدی توانسته به فهرست آشنایان، سابقه تماس‌های تلفنی، پیامک‌ها، و داده‌های دیگر دسترسی پیدا کند. از خرداد ۱۴۰۰، گربه خانگی دست به توزیع یک بدافزار به نام «فربال» یا گوی پشمالو (FurBall) زده است که به شکل تقلبی در پوشش ظاهریِ یک اپلیکیشن ویژه‌ی ترجمه در سیستم عامل اندروید به نام «سرای مقاله» (sarayemaghale.apk) ظاهر می‌شود تا کاربران مقاله‌ها و کتاب‌های ترجمه شده از انگلیسی به فارسی را دانلود کنند. (نگاه کنید به تصویر ۱ برای مقایسه سایت اصلی با سایت بدلی)

وب‌سایت تقلبی یک اپلیکیشن اندرویدی را برای دانلود در دسترس قرار می‌داد، اما به جای رجوع دادنِ کاربران به فروشگاه گوگل‌پلی، این نرم‌افزار مستقیماً از سِرور جاسوس دانلود می‌شود. در مهر ۱۴۰۱ پژوهشگران شرکت ای‌اس‌ای‌تی (ESET) نسخه‌ی جدیدی از این بدافزار را شناسایی کردند که دستورات کمتری برای دانلود داشت و فقط دسترسی به لیست آشنایان را تقاضا می‌کرد. نسخه‌ی اصلی و پیشین این اپلیکیشن علاوه بر فهرست آشنایان، دسترسی به پیامک‌ها، مکان جغرافیاییِ گوشی، رکورد تماس‌های تلفنی، و داده‌های ذخیره در حافظه را هم طلب می‌کرد. تغییرات در نسخه‌ی

تصویر ۱ ـ شباهت بسیار میان وبسایت گربه خانگی (چپ) و وبسایت حقیقی (راست). منبع: ای‌اس‌ای‌تی (ESET)

تازه‌تر به احتمال زیاد به قصد رد گم کردن و مهندسی اجتماعی بیشتر، از راه شکار پیامک‌های کاربر به واسطه آشنایان بوده است.

حمله‌های بین‌المللی

تیر ۱۴۰۱ ـ حمله به هدف‌های اسراییلی

در تابستان ۱۴۰۱، چندین نهاد خصوصی و دولتی در اسراییل هدف حمله‌های سایبری قرار گرفتند که جای پای فعالیت‌های جمهوری اسلامی در آنها نمایان بود. در تیرماه، یک گروه هکری به نام الطاهره که خود را عراقی معرفی می‌کرد چندین حمله به وبسایت‌های تجاری و دولتی در اسراییل را به گردن گرفت، از جمله حمله به شهرداری تل‌آویو و سیستم مسافربری کشور. سپس در مرداد، گروه هکری ایرانی جیوه یا «مرکوری» که همان «مادی واتر» باشد مورد ردیابی قرار گرفت و معلوم شد این گروه با استفاده از آسیب‌پذیری‌های نرم‌افزار «لاگ۴جی۲» (Log4j۲)[۳] به سازمان‌های اسراییل حمله کرده است. این نرم‌افزار را برنامه‌نویسان برای توسعه‌ی کُدنویسی به کار می‌گیرند.

مرکوری (مادی واتر)

در مرداد ماه ۱۴۰۱، مرکز تهدیدات امنیت سایبری مایکروسافت (MSTIC) موفق به ردگیری عامل تهدید هکری ایرانی «مرکوری» (یا همان مادی واتر) شد که از ضعف‌های امنیتی نرم‌افزار «لاگ۴جی۲» (Log4j2) که در چند اپلیکیشن به کار رفته سو استفاده می‌کند. این اپلیکیشن‌ها به وسیله‌ی شرکت «سیس‌اید» (SysAid) که یک شرکت مدیریت فناوری اینترنتی جهانی است، عرضه و مدیریت می‌شد. مادی واتر از این آسیب‌پذیری‌ها در ابزارهای شرکت «سیس‌اید» به قصد دسترسی به هدف‌های اسراییلی استفاده برد.

مادی‌واتر بعد از اینکه به قربانی‌اش دسترسی پیدا می‌کند، ارتباط را حفظ کرده، مشخصات کاربر را ردیف می‌کند و سپس با استفاده از ابزارهای هکری رایج و آنهایی که خودش به همراه دارد، و همچنین ابزارهای مربوط به سیستم عامل، سعی می‌کند تا به سهولت درون سازمان مورد هدف به گردش بپردازد. (نگاه کنید به تصویر ۲)

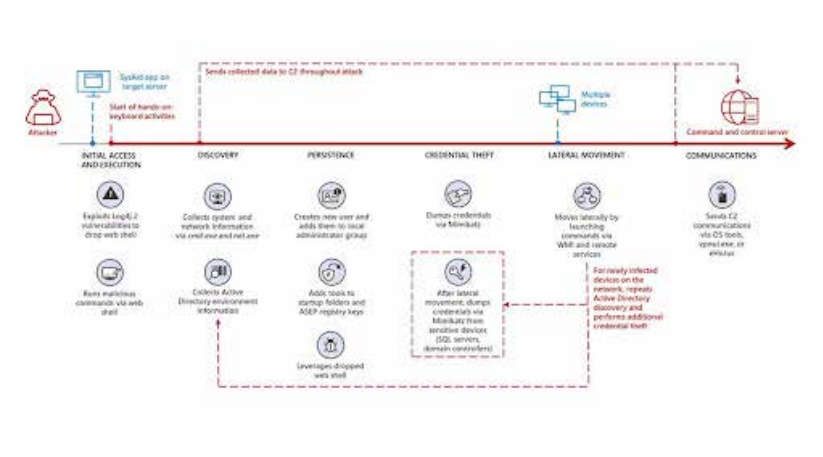
الطاهره

شرکت مسافربری شهری ان‌تی‌اِ (NTA)

۱۳ تیر ۱۳۴۱، کانل تلگرامی «الطاهره» (در عربی به معنی پاک و طاهر)، یک گروه هکری کمترشناخته‌شده که خود را عراقی معرفی می‌کند، اخبار و اسکرین‌شات‌هایی از یک «حمله»ی سایبری به «متروی تل‌آویو» منتشر کرد و مسؤلیت آنرا هم به عهده گرفت.

---

۳ «Log۴J» یک فریم‌وُرک یا چارچوب به منظور کُدنویسی است که شرکت آپاچی آنرا ساخته و نرم‌افزارهای مختلفی آنرا به قصد برنامه‌نویسی به کار گرفته‌اند. در آذر ۱۴۰۰، شرکت آپاچی در مورد آسیب‌پذیری‌های لاگ۴جی هشدار داد و گفت برخی از بدافزارها از این ضعف‌ها برای به دست گرفتن فرمان سیستم‌های متعدد استفاده می‌کنند. حدوداً در همان زمان، معلوم شد که بازیگر هکری ایرانی به نام «بچه گربه ملوس» با استفاده از ابزارهای متن باز (کُدنویسی غیرتجاری و در دسترسی همگانی) سعی دارد از آسیب‌پذیری‌های لاگ۴جی سواستفاده کند. این نشان می‌داد که این گروه به سرعت دست به کار شده بود. نسخه‌ی جدید فریم‌ورک آپاچی به نام لاگ۴جی۲ با کارکردهای جدید مشکلات نسخه‌ی قبلی را برطرف کرده است.



تصویر ۲ ـ زنجیره‌ی مورد حمله‌ی مرکوری (مادی واتر). منبع: مایکروسافت

پیام‌های الطاهره بسیار به پیام‌های میلیشیای حشدالشعبی یا مقاومت اسلامی عراق شباهت دارد که یک واحد نیروی قدس، وابسته به سپاه پاسداران جمهوری اسلامی ایران است.

به فاصله‌ی کوتاهی پس از اعلام حمله‌ی الطاهره، صابرین نیوز، خبرگزاری وابسته به میلیشیای حشدالشعبی نزدیک به نیروی قدس سپاه، به اتفاق حساب‌های توییتری نزدیک به ایران و «مقاومت اسلامی»، خبر حمله به اسراییل را پخش و تبلیغ کردند. آنها ادعا کردند که حمله‌ی سایبری باعث اختلال در سیستم‌های عامل متروی تل‌آویو، مانیتورهای کنترل، و سِروِرهای آن شده است. پس از چند ساعت، پرس تی‌وی، رسانه‌ی انگلیسی‌زبان و رسمی جمهوری اسلامی، و فارس نیوز نزدیک به دولت هم این خبر را پوشش دادند.

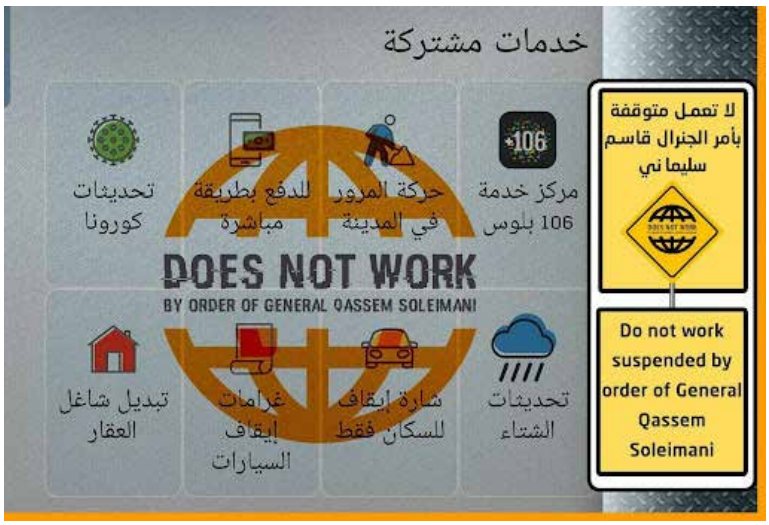
اما بعدتر معلوم شد که این اخبار همه یک کارزار گمراه کننده و شاید به کلی کذب باشند. تل‌آویو سیستم مترو ندارد. فقط یک سیستم کوچک ریلی در دست ساختمان وجود دارد که به وسیله‌ی شرکت دولتی ان‌تی‌اِ (NTA) اداره می‌شود و فعالیت‌های آن در اسراییل موضوع یک جدل سیاسی بوده است. حمله‌ی ادعایی الطاهره به نظر می‌رسد فقط یک حمله‌ی محدود «دی‌داس» (DDoS) یا رد-سرویس به وبسایت ان‌تی‌ا و آی‌پی‌های مرتبط با آن بوده است.[۴]

شهرداری تل‌آویو

در تیرماه ۱۴۰۱، گروه الطاهره به حمله‌های دی‌داس علیه اسراییل ادامه داد. ۲۰ تیر، گروه ادعا کرد به وبسایت شهرداری تل‌آویو حمله کرده و با پیامی در دفاع از قاسم سلیمانی در صفحه اول این وبسایت، ظاهر آن را تغییر داده است.. این پیغام تلافی‌جویانهز اشاره‌ای بود به مشارکت اسراییل در حمله‌ی پهپادی آمریکا به سلیمانی و هم‌رزم عراقی‌اش ابومهدی ال‌مهندس.

بار دیگر کانال تلگرامی صابرین نیوز وابسته به حشدالشعبی خبر را تبلیغ و پخش کرد و مدعی شد که یک حمله‌ی سایبری از عراق «شبکه‌های کامپیوتری شهرداری تل‌آویو» را هدف قرار داده است. رسانه‌های تندرو ایران مثل خبرگزاری تسنیم وابسته به سپاه،

۴ حمله‌ی دی‌داس با ارسال همزمان تقاضاهای بسیار به یک وبسایت و سنگین کردن ترافیک آن باعث کندی و سپس آفلاین شدن آن وبسایت می‌شود، اما در این نوع حمله اطلاعات به سرقت نمی‌رود.



تصویر ۳ ـ حمله‌ی گروه هکری الطاهره به وبسایت شهرداری تل‌آویو در ۲۰ تیر ۱۴۰۱.
منبع: کانال تلگرامی الطاهره

و المیادین لبنان که حامی حکومت ایران است هم این خبر را با آب و تاب نقل کردند. ۲۳ تیرماه، الطاهره با حمله‌ای مشابه وبسایت شهرداری اورشلیم (بیت‌المقدس) را هدف گرفت اما پوشش خبری این‌بار چندان وسیع نبود.

وبسایت‌های دولتی و تجاری

۲۶ تیر ۱۴۰۱، گروه الطاهره اعلام کرد به تلافی بمباران نوار غزه در روز قبل و سایر عملیات اسراییل، وزارت بهداشت این کشور را هک کرده است. اسراییل در تاریخ ۲۵ تیرماه و در پاسخ به حملات موشکی به مناطق مسکونی این کشور از خاک فلسطین، دوبار غزه را هدف حملات موشکی خود قرار داده بود.وزارت بهداشت اسراییل اعلام کرد قطع دسترسی به وب‌سایت این وزارت فقط منحصر به خارج است و ساکنان داخل کشور می‌توانند از سایت بازدید کنند.

۴ مرداد ۱۴۰۱، گروه الطاهره اعلام کرد تعداد ۱۹ وب‌سایت تجاری اسراییلی را هک کرده، صفحه نخست آنها را تغییر داده، و تصویر قاسم سلیمانی را به نمایش گذاشته است. خبرگزاری‌های فارس و تسنیم از این خبر استقبال کردند و توانایی‌های گروه هکری عراقی را به رخ خوانندگان کشیدند.

خاستگاه گروه هکری الطاهره و کارزارهایی که صابرین نیوز وابسته به حشدالشعبی، به نفع این گروه به راه انداخت با انگیزه‌های اعلام شده‌ی آنکه انتقام از قتل قاسم سلیمانی و المهندس است، همخوانی دارد. اما عراق سابقه‌ی چندانی در حمله‌های سایبری ندارد و این واقعیت مساله‌ی خاستگاه واقعی الطاهره را به میان می‌کشد. از جمله آموزش و حمایت مادی از سوی جمهوری اسلامی ایران، به عنوان حامی اصلی حشدالشعبی، یا این احتمال که الطاهره از ابتدا یک گروه هکری ایرانی بوده که پشت نقاب رزمندگان مقاومت عراقی فعالیت می‌کند.

در همان حال که منشا دقیق الطاهره و رابطه‌اش با بازیگران هکری ایرانی هنوز ناروشن است، پوشش گسترده‌ی خبری از فعالیت‌های الطاهره احتمال پیوند میان این گروه‌ها را بیشتر می‌کند. در گذشته، ایران زیر نام‌های جعلی مثل ارتش سایبریِ یمن دست به عملیات هکری می‌زد تا منشا واقعیِ این کارازهای سایبری ناشناخته بماند. احتمال دارد

که الطاهره نیز یکی از تازه‌ترین جبهه‌های سایبری جمهوری اسلامی علیه رقیبانش در منطقه باشد.

تیر ۱۴۰۱ ـ حملات علیه دولت آلبانی

۲۴ تیر ۱۴۰۱، هکرهای وابسته به حکومت ایران دست به یک حمله‌ی مخرب علیه دولت آلبانی زدند و وبسایت‌های دولتی و خدمات عمومی را مختل کردند. علاوه بر این، یک ماه پیشتر و در اواخر اردیبهشت، هکر دیگری که همزمان از سوی ایران حمایت می‌شد اطلاعات محرمانه‌ی حساسی را به بیرون درز داده بود. این اطلاعات از طریق چندین وب‌سایت و رسانه‌ی گوناگون به بیرون درز کرد. دولت آلبانی مجبور شد موقتاً سیستم‌های دولتی را تعطیل کند که شامل خدمات عمومی آنلاین و وبسایت‌های دولتی می‌شد.

این حمله‌ها یک هفته قبل از نشست سالانه «همایش جهانی ایران آزاد» که سازمان مجاهدین خلق تدارک دیده بود اتفاق افتاد. همایش، که قرار بود در روزهای یکم و دوم مردادماه در شهر مانز، ناحیه‌ی دروس، در آلبانی برگزار شود، به دلیل احتمال حمله‌ی تروریستی در ۳۰ تیر کنسل شد. این همایش هر سال به منظور گردهمایی اعضای سازمان مجاهدین و متحدان آنها علیه جمهوری اسلامی تشکیل می‌شود.

سازمان مجاهدین که برنامه سرنگونی رژیم تهران را دارد پیش از سال ۱۳۹۱ از طرف وزارت امور خارجه‌ی آمریکا به عنوان یک تشکیلات تروریستی شناخته می‌شد. اکنون این گروه در قرارگاه اشرف ۳ واقع در شهر مانز، در سی کیلومتری غرب تیرانا پایتخت آلبانی مستقر شده است.

در ۳۱ تیر ۱۴۰۱، یک گروه هکری به نام «عدالت وطن» که مدعی است به وسیله‌ی شهروندان آلبانیایی مخالف دولت این کشور اداره می‌شود اعلام کرد وبسایت‌های دولتی را هک کرده است. گروه یک ویدیوی اخاذی سایبری بر روی وب‌سایتی با دامنه‌ی «homelandjustice.ru.» (ru) و در کانال تلگرامی خود منتشر کرد.[۵] این گروه همچنین اسنادی را منتشر کرد که گفته می‌شود متعلق به دولت آلبانی است و در آنها مجوزهای اقامت اعضای سازمان مجاهدین خلق و اطلاعات شخصی آنها درج شده بود.

لوگوی گروه هکری «عدالت وطن» یک عقاب را در حال شکار نماد گروه هکری «گنجشک درنده» در داخل یک ستاره داوود نشان می‌دهد. (تصویر ۴) این لوگو نشانه‌ای است که حمله به دولت آلبانی به عنوان حامی سازمان مجاهدین، به تلافی عملیات «گنجشک درنده» علیه جمهوری اسلامی ایران صورت گرفته است. ثابت شده که دولت اسراییل، دست‌کم در یکی از عملیات‌های گنجشک درنده مشارکت داشته است. از تاریخ تیرماه ۱۴۰۱، گنجشک درنده مسؤلیت چند حمله‌ی پر سروصدا علیه نهادهای وابسته به دولت ایران را به عهده گرفته است. از جمله‌ی این عملیات، حمله به جایگاه‌های سوخت (پمپ‌های بنزین) در آبان ۱۴۰۰، حمله به مجموعه‌ی فولاد در تیرماه ۱۴۰۱، و اختلال در برنامه‌ی تلویزیونی صدا و سیما با نصب تصاویر رهبران سازمان مجاهدین خلق در بهمن ۱۴۰۰ بود.

---

۵ وبسایت اصلی و کانال تلگرامی اکنون از دسترس خارج شده‌اند. آرشیو اینترنت تعدادی از صفحه‌های وبسایت را بایگانی کرده و نسخه‌ای هم از کپیِ کانال تلگرامی موجود است که در تاریخ ۳۱ اوت ۲۰۲۲ ایجاد شده است.

تصویر ۴ ـ بنر گروه هکری عدالت وطن و تصویر بدافزار اخاذی آن

هکرهای ایرانی و عملیات اطلاعاتی به نفع دولت ایران اغلب اوقات با بدافزارها، پیام‌های خصمانه، و حتی اسناد جعلی، سازمان مجاهدین خلق را هدف می‌گیرند. اما تازه‌ترینِ این حمله‌ها محدوده‌یجغرافیایی عملیات سایبری ایران را وسیع‌تر کرده و یک دولت عضو پیمان نظامی ناتو را هدف قرار داده است. این می‌تواند نشانگر افزایش خطر پذیری جمهوری اسلامی در موقع ضرورت و در برابر تهدید منافع ملی و ژئوپولیتیک خود باشد.

کمپانی مایکروسافت درشهریور ۱۴۰۱، پس از بررسی حمله‌های ایران به آلبانی، با اطمینان اعلام کرد که دست‌کم چهار هکر در این عملیات دست داشتند که هریک وظیفه‌ی متفاوتی به عهده داشته است. این چهار بازیگر هکری با فرستادن بدافزارهای اخاذی، پاک کردن و از میان بردن داده‌ها بر روی سیستم‌های مورد حمله، و کاوش در زیرساخت‌های این سیستم‌ها، اطلاعات آنها را دزدیده و به بیرون درز دادند. مایکروسافت همچنین با کمی احتیاط چنین برآورد کرد که این هکرها در رابطه با «ایوروپیوم» هستند که وابسته به وزارت اطلاعات و امنیت ایران است و با نام‌های دیگرش «اویل ریگ» (OilRig) و «آ پ ت ۳۴» (APT ۳۴) یک بازیگر شناخته‌شده‌ی تهدیدهای هکری به شمار می‌رود.

در جواب این حمله‌ها، در ۱۶ شهریور ۱۴۰۱ آلبانی روابط دیپلماتیک خود را با ایران قطع کرد. این نخستین بار در دنیا بود که یک کشور به خاطر حمله‌های سایبری ارتباط خود را با کشوری دیگر پایان می‌داد. دولت آلبانی دستور داد ظرف ۲۴ ساعت دیپلمات‌های سفارت ایران خاک این کشور را ترک کنند. ایالات متحده از این تصمیم حمایت کرد و به نوبه‌ی خود وزارت اطلاعات و نیروهای امنیتی ایران را به دلیل مبادرت به حمله‌های سایبری به یک کشورِ متحد و عضو ناتو، در لیست تحریم‌های خود قرار داد. دولت ایران این اتهام را اکیداً رد کرد و به بستن سفارت‌خانه‌اش معترض شد. اما بلافاصله بعد از قطع روابط دیپلماتیک، نخست‌وزیر آلبانی ادی راما فاش کرد که همان هکرها بار دیگر سیستم‌های دولتی را در۱۸ شهریور ماه مورد حمله قرار داده‌اند. این حمله‌های جسورانه نشانگر آن است که جمهوری اسلامی حاضر است دست به اقدامات مخاطره‌آمیزی زده و در مسیر عملیات خرابکارانه‌ی سایبری همچنان به جلو بتازد.

آسیب‌پذیری‌های سایبری ایران

با وجود آنکه ایران تلاش می‌کند خود را به عنوان یک قدرت سایبری به دنیا معرفی کند، شبکه‌ها، زیرساخت‌ها، و اسرار دولتیِ آن همچنان در معرض حمله‌های متعددی قرار دارد.. این حمله‌های سایبری نشان می‌دهد ایران در حفاظت از سیستم‌های شبکه‌ی کامپیوتری خود، حتی در بالاترین سطح حکومت، ناتوانی‌های جدی داشته است. دست‌کم از سال ۱۴۰۰ به این طرف، به طور مداوم ایران با حمله‌های هکری‌ای درگیر بوده که با نفوذ در سیستم‌ها، اطلاعات را دزدیده و به بیرون منتقل کرده‌اند و در مواردی هم دست به خرابکاری زده‌اند. این حمله‌ها به هنگام خیزش «زن، زندگی، آزادی» شدت گرفتند.

با ادامه‌ی اعتراضات و تحمیل محدودیت اینترنتی به دست دولت، گروه‌های هکری متعددی با استفاده از پلتفرم‌هایی نظیر سیگنال و تلگرام، حتی «دارک وب» یا وب ناشناس و تاریک، به کمک معترضان آمدند. این عملیات به شکل‌های گوناگون صورت گرفت، مثل درز دادن اطلاعات از نهادهای مهم مثل سپاه پاسداران و متحدانش، افشای داده‌های شخصی از کارکنان دولتی که در سرکوب‌ها مشارکت داشتند، و توزیع فیلترشکن برای دسترسی به اینترنت. اما این اقدامات فقط به معنی افزایش تعداد حمله‌های هکری علیه شبکه‌های ایران نبود، بلکه شمار گروه‌ها و بازیگران عرصه‌ی هکری هم در این بازه زمانی وسعت گرفت.

آر- تو- اُ (R2O)

این گروه که با نام انگلیسی «شورش برای براندازی» (Revolt to Overthrow) یا آرتواُ (R2O) شناخته می‌شود پیش از این چندین وب‌سایت دولت ایران را تغییر صورت داد، پیام‌های مدافع مجاهدین خلق را در آنها به نمایش گذاشت، و اسناد محرمانه‌ای را به خارج درز داد. همچنین به سیستم‌های ارسال پیامک و تلویزیون‌های مداربسته‌ی شهرداری تهران حمله کرد. در تیرماه ۱۴۰۱ شش وب‌سایت و ۴۴ سرور متعلق به سازمان فرهنگ و ارتباطات اسلامی را هک کرد و گفته شد که بیش از ۱۲۰۰۰ سند را ربود.

سازمان فرهنگ و ارتباطات ماموریت چاپ و پخش پروپاگاندا و تبلیغات اسلامی را به عهده دارد. در مهرماه ۱۴۰۱، آرتواُ، به تلافیِ سرکوب معترضان و دادگاه‌های فرمایشیِ آنها، به سِرورهای قوه قضاییه حمله برد و سپس دست به انتشار اسامی و مشخصات ۶۳۰۰۰ پرسنل قوه قضاییه زد. بار دیگر، وب‌سایت پژوهشکده امام خمینی و انقلاب اسلامی را هک کرد و تصاویر و شعارهای مجاهدین خلق را در صفحه نخست آن به نمایش گذاشت..

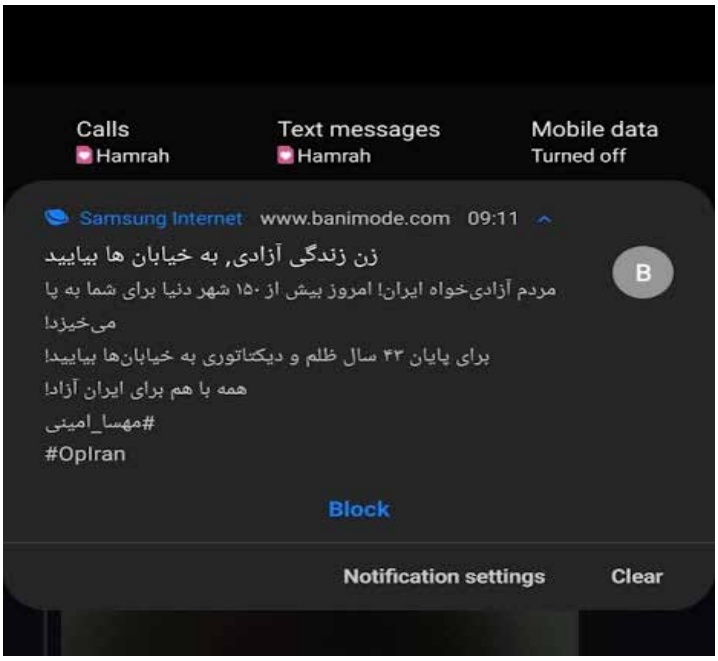
ناشناس (Anonymous)

مجموعه‌ی هکری «ناشناس» یا «انانیمُس» بعد از اعتراضات زن، زندگی، آزادی، بار دیگر به میدان مبارزه بازگشت.[۶] در ابتدای اعتراضات، «ناشناس» که به خاطر عملیاتش

---

۶ این نخستین بار نبود که «ناشناس» دولت ایران را هدف قرار می‌داد. در اعتراضات جنبش سبز در سال ۱۳۸۸، که آغازش مخالفت با انتخابِ مجدد محمود احمدی‌نژاد به ریاست جمهوری بود، «ناشناس» نخستین سناریوی «عملیات ایران» یا «آپ‌ایران» (OpIran) را به اجرا گذاشت که عبارت بود از یک سلسله حمله‌های دی‌داس به وبسایت‌ها و سازمان‌های دولتی یا وابسته به دولت. در بهمن ماه ۱۳۹۸ (فوریه ۲۰۱۱)، ایرانیان در حمایت از بهار عربی به خیابان آمدند، اما دولت تظاهرات آنها را با سرکوب و بازداشت‌های جمعی پاسخ داد. در واکنش به سرکوب، عملیات «آپ‌ایران» از سر گرفته شد و وبسایت‌های دولتی،

در جنبش «اشغال وال‌استریت» و بهار عربی شناخته شده بود، وعده داد که به یاریِ معترضان ایران بر خواهد خاست. روز ۲۹ شهریور ۱۴۰۱، شخصی که نقاب گای فاوکس را بر چهره داشت در یک ویدیو ظاهر شد و اعلام کرد عملیات «آپ‌ایران» (#OpIran) آغاز شده، و وعده داد که دولت ایران را به تعطیلی خواهد کشاند.
از زمان پخش آن ویدیو در یوتیوب تاکنون، گفته می‌شود که «ناشناس» موفق



تصویر ۵ ـ یکی از پیامک‌هایی که از مردم برای شرکت در تظاهرات ضد رژیم دعوت می‌کند. این پیامک، از جانب لباس‌فروشیِ آنلاین «بانی‌مُد» و از طریق شرکت نجوا به گوشی‌های همراه فرستاده شد.

شده بیش از هزار دوربین مداربسته را در سراسر ایران هک کند و حمله‌های متعدد دی‌داس (کند کردن و پایین کشیدن وبسایت‌ها با انبوه تقاضاهای همزمان) به ارگان‌های دولتی را سازمان داد؛ بانک مرکزی ایران، وبسایت‌های رسمی کابینه از جمله وبسایت رییس جمهور (president.ir)، پایگاه رسمی رهبر نظام علی خامنه‌ای[۷]، و وب‌سایت شرکت مخابرات ایران از جمله این وبسات‌ها بودند. همچنین به نظر می‌رسد «ناشناس» تحت نام و هشتک‌های «آپ‌ایران» (#OpIran) و #مهسا_امینی، موفق به درز اطلاعات بانکی کارمندان دولت و شماره تلفن اعضای مجلس شده، همه در راه مبارزه برای انقلاب ژینا امینی.

در میان عملیات «ناشناس» در ماه‌های گذشته، دو مورد دارای اهمیت است. روز ۹ مهر ۱۴۰۱، بسیاری از شهروندان ایران پیامکی دریافت کردند که آنها را برای تظاهرات خیابانی علیه رژیم دعوت می‌کرد. «ناشناس» ادعا کرد که شرکت «نجوا»، که یک کمپانی خدمات بازاریابی است، را هک کرده و از طریق این شرکت پیامک‌ها را به مردم ارسال داشته است. مشتریان نجوا برای بازاریابی را شرکت‌های متعددی تشکیل

از جمله پایگاه رئیس جمهور و سایت رهبر نظام علی خامنه‌ای زیر حمله‌های دی‌داس رفت. کمی دیرتر در همان سال، در سالگرد انتخابات ۸۸، «ناشناس» بیش از ده هزار ایمیل از وزارت امور خارجه به بیرون درز داد که در آنها تقاضای اخذ ویزا و تصاویر متقاضیان غیرایرانی بود. این رویدادهای هکری در آن زمان چندان جلب توجه نمی‌کرد. برای اطلاعات بیشتر به «دی‌اف‌آر لَب» (DFRLab) رجوع کنید.

۷ یک گروه هکری اسراییلی به نام «ارتش راهزنان» نیز، همزمان و در همان روز حمله‌های «ناشناس»، اعلام کرد که طی «دو روز حمله‌های سخت» دی‌داس، سایت خامنه‌ای را هدف قرار داده است. (۲۲ سپتامبر ۲۰۲۲)

می‌دهند که شامل خبرگزاری فارس و زنجیره‌ای از فروشگاه‌های لباس (مثل «بانی مُد») می‌شود. «ناشناس» پس از آنکه کنترل سِرورهای شرکت نجوا را به دست گرفت، از جانب این شرکت‌های طرف معامله‌ی نجوا، پیامک‌های تلفنی به تعداد زیادی از صاحبان گوشی همراه فرستاد. شرکت نجوا تأیید کرد که امنیت خدمات دیجیتالی‌اش به خطر افتاده و به مدت چند ساعت سِرورهای خود را خاموش کرد.

تصویر ۵ ـ یکی از پیامک‌هایی که از مردم برای شرکت در تظاهرات ضد رژیم دعوت می‌کند. این پیامک، از جانب لباس‌فروشیِ آنلاین «بانی‌مُد» و از طریق شرکت نجوا به گوشی‌های همراه فرستاده شد.

مورد دوم از عملیات مهم «ناشناس» این بود که در ۲۱ مهر ۱۴۰۱ هشدار داد روی تلفن موبایل معترضانی که مدتی در بازداشت به سر برده و آزاد شده‌اند یک بدافزار اندروید نصب شده است. «ناشناس» ادعا کرد که بدافزاری به نام «ال‌تری‌مان» (L۳MON) با نصب یک برنامه‌ی کامپیوتریِ کنترل از راه دور می‌تواند به اطلاعات شخصیِ صاحب گوشی دسترسی پیدا کند، از جمله به عکس‌ها، شماره تلفن‌ها، و پیامک‌های کسی که گوشی به او تعلق دارد. «ناشناس» به معترضان توصیه کرد که ۱- گوشی‌های خود را به خیابان نبرند و ۲- فرض را بر این بگذارند که به محض دستگیر شدن و ضبط گوشی‌های همراه، مأموران در خفا این موبایل‌ها را با بدافزارهای خطرناک آلوده کرده‌اند. در چنین صورتی، «ناشناس» پیشنهاد داد که کاربران گوشی خود را به تنظیمات کارخانه برگردانند و به فهرست مخاطبین خود نیز اطلاع دهند که ممکن است در معرض شناساییِ هکرهای دولتی قرار گرفته باشند.

یک مورد دیگر از عملیات مهم «ناشناس» این بود که در ۱۲ آبان ۱۴۰۱ مجموعه‌ای از اسناد هک‌شده متعلق به «کارگروه تعیین مصادیق محتوای مجرمانه» را منتشر کرد. این کارگروه نهادی وابسته به دادستانی کل کشور است که تصمیم می‌گیرد کدام وبسایت‌ها و محتوای آنلاین باید سانسور شود. ایمیل‌های هک شده اما نشان می‌داد که حوزه‌ی وظایف این کارگروه در نظارت بر محتوای اینترنت بسیار وسیع‌تر از آن‌چیزی است که می‌دانیم.

برای مثال، در یکی از ایمیل‌های هک شده از سال ۱۴۰۰، کارگروه به مدیران شرکت خدمات ویدیویی آپارات (معادل یوتیوب در ایران) دستور می‌دهد «مشخصات هویتی و دسترسی ثبت‌کننده»ی یکی از مشتریان آپارات را در اختیار کارگروه بگذارد، بدون آنکه دلیلی برای این تقاضا ارایه دهد. پس از چند روز آپارات از این دستور اطاعت کرد و اطلاعات ایمیلی و آی‌پی‌های صاحب حساب کاربری را تسلیم کارگروه تعیین مصادیق محتوای مجرمانه کرد.

در یک ایمیل دیگر از سال ۱۳۹۹، یک سال قبل از ریاست جمهوری ابراهیم رئیسی، فاش می‌شود که او در مقام رئیس قوه قضاییه، حامی سرسخت فیلترینگ و سرکوب فیلترشکن‌ها، و سانسور رسانه‌های اجتماعی و پیام‌رسان‌هایی است که هنوز مسدود نشده بودند (مانند اینستاگرام و واتس‌اپ). افشای این حقیقت با ادعاهای رییسی به هنگام کارزار انتخاباتی در تضاد بود؛ او ظاهراً از پلتفرم‌هایی مثل اینستاگرام حمایت می‌کرد و وجود آنها را برای اقتصاد و ایجاد اشتغال مهم عنوان می‌کرد.

بلک ریوارد (Black Reward)

بین شهریور تا آذر ۱۴۰۱ چندین گروه هکری پا به میدان گذاشتند و این روند با گسترش اعتراضات سرعت بیشتری به خود گرفت. «بلک ریوارد» یکی از این گروه‌های هکری بود. روز سوم مهرماه، به تلافی سرکوب تظاهرکنندگان، بلک ریوارد اعلام کرد که اطلاعات سرورهای بنیاد مسکن انقلاب اسلامی و وبسایت‌های وابسته به آن را که «بخشی از شبکه فساد اقتصادی افراد وابسته به بیت و سپاه» هستند هک کرده و اطلاعات آن را از میان برده است. ۲۷ مهر، بلک ریوارد ایمیل‌های داخلی «پِرس تی‌وی» (بازوی بین‌المللی صدا و سیما) را به خارج درز داد. این ایمیل‌ها عملیات پرس‌تی‌وی و طرز کار داخلی‌اش را افشا کرد، از صورت‌حساب‌های پرداخت‌نشده‌ی ۱۸۰۰۰ دلاری گرفته تا شکایت‌های مسؤلان بالای رژیم از بخشِ عربی تلویزیون آرتی (RT)، شبکه تلویزیونی وابسته به روسیه، به دلیل پوشش خبریِ انتقادی از ایران.[۸]

در روزهای بعد، «بلک ریوارد» دست به انتشار مجموعه‌ای از اطلاعات محرمانه زد از جمله اطلاعات متعلق به سازمان انرژی اتمی ایران به حجم ۵۰ گیگابایت، یک سری اسناد محرمانه از سازمان فرهنگ و ارتباطات اسلامی[۹] (همان سازمانی که گروه هکری «آرتواُ» هم آن را در شهریور هک کرده بود)، مجموعه‌ای از داده‌های شرکت ملی نفت و گاز و ده‌ها پیمانکار خصوصی وابسته به آن، و اطلاعاتی از قرارگاه مرکزی خاتم‌الانبیا وابسته به سپاه پاسداران.

به دنبال گسترش اعتراضات، بلک ریوارد به تنهایی ظرف چند هفته بیشتر از هر گروه و بازیگر هکریِ دیگر موفق شد اطلاعات محرمانه‌ی دولتی را به بیرون درز دهد. نه تنها حجم زیاد اینِ داده‌ها، بلکه ماهیت و محتوای آنها بود که نام بلک ریوارد را برجسته کرد.

تصویر ۶ ـ گروه هکری تپندگان پایگاه اینترنتی دانشگاه الزهرا در تهران را در تاریخ ۲۱ مهر ۱۴۰۱ هک کرد و آن را به این شکل تغییر صورت داد.

۸ ظاهراً در ارتباط با پوشش خبری آرتی از اعدام نوید افکاری در سال ۱۳۹۹.

۹ یکی از سندهای درز کرده نشان می‌دهد در سال ۱۴۰۰تقاضایی برای مبلغ ۳۰۰۰۰۰ (سیصدهزار) یورو از بودجه دولتی شده تا مبالغی به دفترهای محلی این سازمان در خارج کشور پرداخت شود، یعنی دفاتر سازمان فرهنگ و ارتباطات اسلامی در کشورهای تانزانیا، آفریقای جنوبی، الجزایر، اوگاندا، قطر، سوریه، عراق، کویت، کنیا، و تونس. این فقط یک تصویر کوچک از شبکه‌ی جهانی جمهوری اسلامی برای عملیات مؤثر تبلیغاتی و سیاسی است.

۴ آذر ۱۴۰۱، بلک ریوارد صفحه‌ی اول وبسایت خبرگزاری فارس وابسته به سپاه را هک کرد و تغییر صورت داد و تصویری تار از یک زن معترض که روسری خود را تکان می‌دهد بر آن نقش زد، حرکتی که نماد جنبش زن، زندگی، آزادی است. چهار روز بعد در ۸ آذر بلک ریوارد یک بولتن داخلی از خبرگزاری فارس را منتشر کرد که این خبرگزاری در باره‌ی اعتراضات برای مقامات بالای سپاه فراهم کرده بود.

بولتن فارس یک سند بحث‌انگیز بود که ظاهراً از روی سرور این خبرگزاری چند روز پیش‌تر ربوده شده بود. این بولتن نشان می‌داد رژیم چه تصوری از اعتراضات دارد و چگونه خبرها را به نفع خود دستکاری می‌کند. مثلاً، بولتن اظهار می‌داشت که علی خامنه‌ای نسبت به عملکرد رئیس جمهور ابراهیم رئیسی و فرماندهان نیروی انتظامی به دلیل بی‌کفایتی در فرونشاندن اعتراضات اظهار نارضایی کرده است. در همان حال، رهبر نظام خواسته بود به جای دستگیری مولوی عبدالحمید، رهبر دینی سُنی در سیستان و بلوچستان که مدافع اعتراضات بود، با او با احتیاط بیشتری رفتار کنند. بولتن داخلی خبرگزاری فارس نشان از راز سرگشاده‌ای داشت که مردم سال‌ها ظن آن را داشتند؛ این واقعیت که رسانه‌های اصول‌گرا نقش فعالی در دستگاه امنیتی رژیم و به ویژه اطلاعات سپاه، بازی می‌کنند. کارکنان این خبرگزاری‌ها اخبار آخرین تحولات اجتماعی و اقتصادی را همراه با تحلیل وقایع به اطلاع فرماندهان ارشد سپاه می‌رسانند تا آنها به نوبه‌ی خود در برابر رویدادهای حساس مثل اعتراضات مردمی آماده‌ی برخورد باشند.

تا اواسط دی‌ماه گروه بلاک ریوارد توانست چندین دسته از اسناد مربوط به خبرگزاری فارس را منتشر کند نظیر سندهای داخلی، قبض پرداخت‌های نجومی به مدیران ارشد، مصاحبه‌های حساس سیاسی که ضبط شده اما هرگز منتشر نشده بودند، و یک فایل صوتی از یک ملاقات مقامات تندرو رژیم که در آن راجع به اعتراضات و راه‌های احتمالی مقابله با مردم صحبت می‌کنند. یکی از خبرهای فاش شده در این ملاقات این بود که دولت قطر حاضر شده بود اطلاعات مربوط به گذرنامه‌های شرکت‌کننده در جام جهانی ۲۰۲۲ به میزبانی قطر را در اختیار مقامات ایرانی قرار دهد و به آنها قول می‌دهد با تظاهرکنندگان ضد رژیم در بازی‌های جام جهانی به شدت برخورد کند.

تپندگان

روز ۲۱ مهر ۱۴۰۱، یک گروه هکری به نام «تپندگان» به وبگاه دانشگاه الزهرا نفوذ کرد. این دانشگاه دخترانه به خاطر سابقه‌ی تاریخی‌اش در تحمیل سرسختانه‌ی قواعد حجاب و شرایط دشوار پذیرش شهرت دارد. تپندگان وب‌سایت الزهرا را تغییر صورت داد و فراخوانی به تظاهرات سراسری همراه با دستورات لازم به چاپ رساند (تصویر ۶).

در ۸ آذر، تپندگان اطلاعات کلیدی‌ای راجع به دست‌کم دو پیمانکار سپاه پاسداران منتشر کرد که وظیفه‌ی آنها فراهم کردن تسهیلات برای نیروی قدس سپاه در کشور سوریه برای همکاری با رژیم بشار اسد است. در این اسناد گفته می‌شود که شرکت‌های تجاری نظیر «میلاد» و «گروه ویژه سورین» به عنوان واسطه‌ی نیروی قدس در سوریه به کار مشغول هستند و خدمات امنیتی و ساختمانی در شهرهای مختلف آن کشور را به عهده دارند.

براندازان

۱۱ آبان ۱۴۰۱، یک گروه هکری کم‌تر شناخته‌ی دیگر به نام «براندازان» هم نظیر گروه هکری پیشین به دانشگاه الزهرا شبیخون زد و اطلاعات داخلی آن را به خارج درز داد. این سندها عمدتاً تصویری از پشت صحنه‌ی تصمیمات و سیاست‌های دانشگاه از زمان اعتراضات را به دست می‌دهد. از جمله در یکی از این اسناد تقاضای پاداش برای گارد امنیتی دانشگاه شده تا روحیه‌ی آنها برای سرکوب اعتراضات دانشجویی تقویت شود. به هنگامی که دانشجویان سراسر کشور آماده‌ی اعتصابات سراسری در ۱۶ آذر (روز دانشجو) می‌شدند، گروه «براندازان» به بیش از صد آدرس اینترنتی متعلق به ۱۶ دانشگاه، از جمله الزهرا، شبیخون زده و آنها را هک کردند.

«براندازان» وعده داد که در روزهای آینده اسنادی به حجم ۸ گیگابایت از دانشگاه‌ها منتشر خواهد کرد، بدون آنکه اطلاعات شخصی دانشجویان لو برود. اما از آن تاریخ تاکنون کانال تلگرامیِ این گروه مطلب تازه‌ای منتشر نکرده است.[۱۰]

نتیجه

از شهریور ۱۴۰۱ به این سو جمهوری اسلامی به اسم امنیت ملی به فعالیت‌های مخرب سایبری علیه دشمنان خود ادامه داده است. هدف این اقدامات تابع الگوی همیشگی بوده است: ناراضیان سیاسی در داخل و خارج از کشور از یک سو، و دشمنان خارجی که دولت ایران از نظر تاریخی و ایدئولوژیک با آنها ستیز دارد از سوی دیگر. کشور اسراییل یک نمونه‌ی بارز است. هکرهای وابسته به ایران با حمله‌های اخلال‌گرانه اما نه چندان پیشرفته، مثل تهاجم‌های دی‌داسی، همچنان نهادهای تجاری اسراییل را هدف گرفتند. اما یک تحول عمده در این الگو روی داد و آن جسارت ایران در عملیات سایبری علیه پیمان نظامی ناتو بود که به شکل حمله‌های چندمرحله‌ای، فرستادن بدافزارهای اخاذی، و هک و نشت اطلاعات علیه دولت آلبانی صورت گرفت که عضو این پیمان نظامی است. این عملیات ریشه‌های داخلی داشت، یعنی حمایت دولت آلبانی از سازمان مجاهدین خلق. با این حال، این عملیات می‌تواند به عنوان نخستین گام آمادگی جمهوری اسلامی برای خطر پذیری بیشتر و تغییر دادن مسیر فعالیت‌های سایبری در آیندهٔ به قصد تغییر موازنه در رقابت‌های ژئوپلیتیک منطقه تعبیر کرد.

این گزارش همچنین به گسترش فعالیت سایبری جمهوری اسلامی برای نظارت بر شهروندان خود پرداخت. هرچند دولت به بهانه‌ی امنیت ملی به توجیه سیستم‌هایی مثل «سیام» می‌پردازد، اما استفاده‌ی گسترده از چنین سیستم‌هایی از اهداف عنوان شده برای آن‌ها به مراتب فراتر می‌رود. در این سیاست‌های سایبری که به بهانه‌ی حاکمیت قانون، تمام گروه‌ها اعم از مجرمان قانون‌شکن، ناراضیان سیاسی و یا کنشگران قومیتی و حقوق بشری را به طور یکسان و بی‌توجه به تفاوت‌ها هدف قرار میدهد، نشانی از اصول ضرورت و تناسب دیده نمی‌شود.

. کارنامه‌ی منفی ایران در نقض حقوق بشر همراه با قابلیت‌های خطرناک سایبری‌اش باعث افزایش نگرانی درباره‌ی نقش دستگاه‌های نظارتی دیجیتالی و سانسور آنلاین در سرکوب حقوق شهروندان می‌شود.

---

۱۰ براندازان همچنین در ۱ آذرماه وبسایت دولتی دیوان محاسبات کشور را تغییر صورت داد، که ظاهرا به تلافی سرکوب اعتراضات در کردستان و سیستان و بلوچستان انجام شد.

با وجود اینکه ایران تلاش می‌کند خود را به عنوان یک قدرت مهم سایبری به دنیا عرضه کند، خودش در برابر حمله‌های سایبری به شبکه‌ها و زیرساخت‌های کشور و نشت اسرار دولتی به شدت آسیب‌پذیر است. حمله‌های سایبری گروه‌های هکری به نهادهای داخلی از هنگام وقوع جنبش زن، زندگی، آزادی، شدت بیشتری گرفته است. این حمله‌ها ضعف دولت را در محافظت از سیستم‌ها و شبکه‌ی کامپیوتری کشور، حتی در بالاترین سطوح دولتی، آشکار می‌کند. این وضعیت یک مساله‌ی استراتژیک را در مقابل دولت قرار می‌دهد. حکومت ایران نیازمند برقراری توازن میان منابع خود است که چه میزان از آنها را صرف امنیت شبکه‌های داخلی کند و چه مقدار را به عملیات سایبری خرابکارانه اختصاص دهد. تا این لحظه، حکومت دایماً سیاست دوم را در پیش گرفته و آنرا بر امنیت شبکه‌های داخلی که خواست مالیات‌دهندگان است ارجح شمرده است. باید منتظر شد و دید آیا ایران حاضر خواهد شد پس از تحمل خسارت‌های زیاد از حمله‌های سایبری، سیاست خود را عوض کند و در جهت حکمرانی دیجیتال پایدار دست به کار شود. ما در گزارش‌های آینده‌ی دیده‌بان هکری این تحولات را دنبال خواهیم کرد. ///