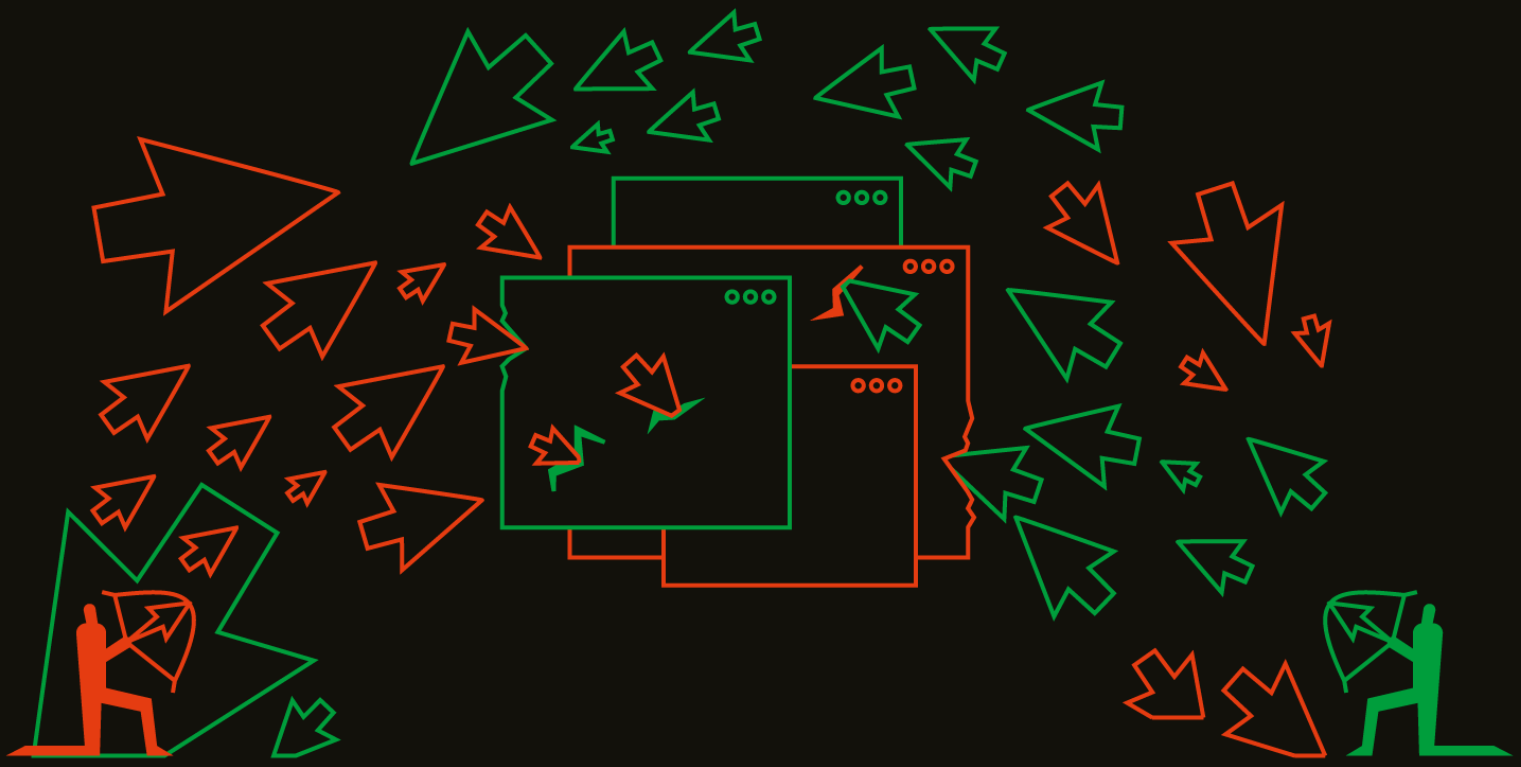

جمع‌بندی هکر بان

جنگ سایبری مخفیانه میان ایران و اسراییل و برآیندهای آن برای حقوق دیجیتال

فیلتربان
ژانویه ـ ژوئن ۲۰۲۲
دی ۱۴۰۰ ـ تیر ۱۴۰۱

در سال گذشته، تنش پیرامون برنامه‌ی هسته‌ای ایران به طرز بی‌سابقه‌ای به فضای مجازی کشیده شد و نزاعِ دوطرفه‌ی بی‌پایانی را با دولت اسراییل به دنبال داشت. گروه‌های هکری ظاهراً ناشناس، در لباس ناراضیان و مخالفانِ نظام، بارها نهادهای دولت ایران را آماج حمله‌های جاسوسی و خرابکارانه قرار دادند. تنش‌ها محدود به این نیست که هر یک دیگری را به سازماندهی حمله‌های سایبری علیه خود متهم می‌کند. تا این تاریخ، نیویورک‌تایمز به نقل از دو مقام آمریکایی تایید کرده است که دست‌کم یکی از این حمله‌های سایبری ــ حمله به پمپ بنزین‌های ایران در آبان ۱۴۰۰ ــ به‌دست اسرائیل صورت گرفته است.[۱] در مورد ارتباط حمله‌های سایبری نهادهای اسرائیلی با

۱ https://www.nytimes.com/2021/11/27/world/middleeast/iran-israel-cyber-hack.html

ایران نیز گمانه‌زنی‌هایی وجود دارد[۲]. سرعت فزاینده‌ی این رویدادها سبب آفتابی شدن هرچه بیشترِ خصومت‌های دیرینه در فضای مجازی از طریق رویارویی سایبری است. حمله‌های سایبریِ اخیر آسیب‌پذیری ایران را در این عرصه نمایان‌تر کرده است. یک گزارش اطلاعاتی مَربوط به تهدیدهای سایبری به دست فیلتربان رسیده که برای شهرداری تهران تهیه شده و در آن جزییات یک بدافزار که شهرداری را هدف قرار داده توصیف شده است. این گزارش نشان‌دهنده‌ی پیشرفت نهادهای دولتی در تحقیق و پاسخگویی به حمله‌های سایبری است، اما هنوز جای خالی برخی از ویژگی‌های کلیدی در آن محسوس است؛ یعنی ویژگی‌هایی که لازمه‌ی صلاحیت کامل در تجزیه و تحلیل حمله‌ها و تدارک دفاع استراتژیک هستند.

پرسش‌های تازه‌ای در باره‌ی توانایی جمهوری اسلامی در رسیدگی به کمبودهای موجود در فناوری و سیاستگذاریِ امنیت سایبری مطرح شده است؛ از جمله، پیامدهای سرمایه‌گذاری‌های نابرابر در شبکَه ملی اطلاعات و ظرفیت‌های تهاجمی[۳] در مقایسه با سرمایه‌گذاری در ظرفیت‌های دفاعی برای حفاظت از شبکه‌های داخلی، زیرساخت‌ها، و حریم خصوصی و امنیت کاربران.

شبکه ملی اطلاعات با سرمایه‌گذاری بیش از ۶ میلیارد دلار، پرخرج‌ترین پروژه ملی مخابراتی در تاریخ جمهوری اسلامی محسوب می‌شود.[۴] هدف اصلی این شبکه این است که تا جای ممکن نیاز به پلتفرم‌های خارجی و دروازه‌های اینترنت بین‌المللی را در کشور کاهش دهد. با این هدف، جمهوری اسلامی حدود یک میلیارد و پانصد هزار دلار خرج تولید موتورهای جستجوگر داخلی کرده و صدها هزار دلار برای کمک به توسعه‌ی انواع نرم‌افزارها برای پیام‌رسانی، پخش ویدیویی، بانکداری و سرویس‌های دیگر هزینه کرده است. تا این تاریخ هیچ یک از این پلتفرم‌ها موفق نشده جای همتاهای بین‌المللی که محبوب‌تر و امن‌تر هستند را بگیرد.

حمله‌های سایبری اخیر به زیرساخت‌های ایران، حاصل این سرمایه‌گذاری‌های کلان را به آزمون گذاشت و این نکته را برجسته کرد که تمرکز بیش از اندازه در این شبکه، بدون توجه کافی به امنیت سایبریِ آن و تاثیرش بر زندگی روزمره، بسیار چالش‌برانگیز است. اکثر انتقادهایی که از شبکَه ملی اطلاعات شده پیرامون اثرات آن بر حق آزادی بیان و دسترسی به اطلاعات بوده است. اما رویدادهای اخیر مسأله‌ی مهم اما کمتر پژوهش شده‌ی حقوق بشر و حکمرانی دیجیتال را در بستر آسیب‌پذیری‌های مهم امنیت سایبری در شبکه‌ی ملی پیش می‌گذارد.

سازمان پدافند غیرعامل در سال ۱۳۸۲ (۲۰۰۳ میلادی) به منظور حفاظت از شبکه‌های غیرنظامی شکل گرفت تا اقدامات دفاعی از شبکه‌های داخلی را هدایت کرده و با تهدیدهای خارجی مقابله کند. با این وجود، این سازمان از ابتدای تاسیس به خاطر ضعف‌های مهم امنیتی مورد انتقاد قرارگرفت. از این جمله می‌توان به حمله ویروس «استاکس‌نت» به نیروگاه هسته‌ای نطنز در سال ۱۳۸۹ و یک سلسله آتش‌سوزی با

---

۲ https://www.cybereason.com/blog/research/strifewater-rat-iranian-apt-moses-staff-adds-new-trojan-to-ransomware-operations

۳ ظرف بیش از یک دهه، ایران در کنار چین، روسیه، و کره شمالی، تبدیل به یکی از بازیگران کلیدی تهدیدهای سایبری شده است. از سال ۲۰۰۹ تا ۲۰۱۹، ایران هفت کشور را هدف ۳۱ حمله سایبری قرار داد که ۴۲% آنها معطوف به ایالات متحده بود. برای اطلاعات بیشتر رجوع کنید به: https://www.privacyaffairs.com/geopolitical-attacks/

۴ https://cyber.harvard.edu/node/100145

جدول ۱: ده کشور که بیشترین در صد میزان آلودگی ویروسی در گوشی‌های همراه را داشته‌اند.

	کشور	٪ - درصد آلودگی
۱	ایران	۳۵.۲۵
۲	چین	۲۶.۸۵
۳	یمن	۲۱.۲۳
۴	عمان	۱۹.۰۱
۵	عربستان سعودی	۱۵.۸۱
۶	الجزایر	۱۳.۸۹
۷	آرژانتین	۱۳.۵۹
۸	برزیل	۱۰.۸۰
۸	اکوادور	۱۰.۶۴
۱۰	مراکش	۱۰.۵۶

منشا نامعلوم[۵] در پالایشگاه‌های نفت و گاز در ۱۳۹۵ اشاره کرد. در حالی‌که این انتقادها همچنان بی‌پاسخ مانده‌اند، سردار غلامرضا جلالی رئیس سازمان پدافند غیرعامل تمایل خود را به توسعه یک شبکه ملی اطلاعات[۶] ابراز کرده و پیشنهاد داده است که برای دور زدن تحریم‌های آمریکا از رمزارز یا پول دیجیتالی استفاده شود.[۷]

پس از متحمل شدن حمله‌های متعدد سایبری، که گفته می‌شود از جانب اسراییل صورت گرفته، در خرداد ۱۴۰۱ مجلس خواهان تغییرات ساختاری و بودجه‌ی جدید برای سازمان پدافند غیرعامل شد[۸] تا مقاومت زیرساخت‌های حیاتی و شبکه‌های غیرنظامی بهبود یابد. در طرح جدید مجلس همه دستگاه‌های اجرایی کشور ملزم می‌شوند یک درصد از اعتبارات خود را به سازمان پدافند غیرعامل تخصیص دهند.[۹] با آنکه این طرح نشان از رویکرد جدیدی به مسایل امنیت سایبری دارد، به نظر می‌رسد برای رسیدن به هدفش راهی طولانی در پیش داشته باشد. . سازمان پدافند غیرعامل با توجه به کارنامه‌ی منفی‌اش و بی‌اعتنایی به رویکرد حقوق بشری، ایمنی مدنی و امنیت سایبری، به هیچ وجه صلاحیت رهبری این برنامه‌ها را ندارد.

در گزارشی که شرکت امنیت سایبری روسی «کاسپرسکی» [۱۰] در ژوییه ۲۰۲۲ منتشر کرد،

۵ https://www.radiofarda.com/a/f35_oil_indu_fire_ladan_salami/28057862.html

۶ https://www.alef.ir/news/3980918054.html?show=text

۷ https://en.mehrnews.com/news/139158/Iran-could-turn-to-cryptocurrencies-to-evade-some-sanctions

۸ https://bit.ly/3zgOsiJ

۹ https://bit.ly/3Je7jj2

۱۰ https://securelist.com/it-threat-evolution-in-q1-2022-mobile-statistics/106589

به قابلیت امروز دفاع سایبری ایران اشاره‌ی مختصری شده است. طبق این گزارش که می‌گوید بیش از ۳۵ درصد کاربران گوشی همراه در کشور گرفتار بدافزار شده‌اند، ایران در صدر فهرست کشورهایی قرار می‌گیرد که بیشترین میزان آلودگی ویروسی را تجربه می‌کنند، حتی بیشتر از کشور چین.

ایران علاوه بر اینکه امنیت شبکه‌ها را قربانی سانسور و متمرکز کردن امور کرده، در زمینه‌ی امنیت سایبری نیز از تخصص کافی بی‌بهره است. اینجا مجموعه‌ای از عوامل - از جمله رقابت نهادهای دولتی با بخش خصوصی در جذب استعدادهای فناوری اطلاعات و امنیت سایبری در دهه‌ی گذشته[۱۱] - دست به دست هم داده‌اند به گفته‌ی منابع آگاه، نرخ گردش استعدادهای فناوری در بخش خصوصی چنان بالا است که برخی از معروف‌ترین برندها در کمتر دو سال، سه نسل از مهندسان این حوزه را به کار گرفته و از دست داده‌اند. روند مهاجرت این استعدادها به کمپانی‌های اروپایی، آمریکای شمالی و استرالیایی همچنان ادامه دارد.

در حالی که مذاکرات هسته‌ای میان ایران و قدرت‌های بزرگ ادامه دارد، به احتمال زیاد فضای تنش‌آمیزِ ژئوپولیتیک به همین صورت باقی خواهد ماند. ارجحیت‌های جمهوری اسلامی در زمینه‌ی جاسوسی و خرابکاری (عمدتاً علیه اسراییل) محتملاً تغییر چندانی نخواهد کرد. اما نزاع میان ایران و اسراییل به طور فزاینده‌ای در جنگ‌های سایبری انعکاس می‌یابد که در آنها شبکه‌های غیرنظامی بیشترین آسیب را خواهند دید. فقدان سرمایه‌گذاری و تخصص در بخش دولتی کماکان شبکه‌های غیرنظامی و زیرساخت‌های حیاتی ایران را در معرض حمله‌های بیشتر قرار خواهد داد. فقط تغییرات ساختاری در سیاستگذاری و اقدامات امنیت سایبری می‌تواند در این وضعیت تغییر به وجود آورد. این وضعیت باعث می‌شود وعده‌ی دیرینه‌ی حکمرانی دیجیتال برای تسهیل امور دولتی و خدمات شهروندی تحقق پیدا نکند. در میان حمله‌های سایبری اخیر، آنها که نهادهای دولتیِ مسئول رسانه‌ها را هدف می‌گیرند مشکلات را دوچندان کرده و کسب مجوز برای محصولات فرهنگی و ترخیص آنها را طولانی‌تر می‌کنند. حمله به شبکه‌های غیرنظامی، مثل هدف گرفتن پمپ‌بنزین‌ها، وضعیت خطیر اقتصادی با جمعیت رانده شده زیر خط فقر را از همین که هست هم بدتر می‌کند. حملات سایبری هرگز تا این اندازه به حقوق اقتصادی و انسانی گره نخورده بوده است.

دولت ایران اگر بخواهد می‌تواند با سرمایه‌گذاری در امنیت سایبری و بالا بردن مقاومتِ شبکه‌های غیرنظامی بر این مشکلات غلبه کند. اما بیشتر سرمایه‌گذاری دولتی تاکنون، بدون توجه به امنیت سایبری، صرف ظرفیت‌های تهاجمی علیه دشمنان رژیم و گسترش شبکه ملی اطلاعات شده است. چنانچه ارجحیت‌های رژیم تغییر نیابد، شبکه‌های غیرنظامی و حقوق بشر کماکان قربانی خصومت‌های سیاسی میان ایران و رقیبان‌اش خواهد شد.

هکر بان چیست؟

آنچه می‌خوانید نخستین گزارش از سلسله جستارهای هکر بان است که از این پس به طور منظم منتشر خواهد شد. در این گزارش‌ها، فیلتربان حمله‌های سایبری را ــ چه از

سوی ایران و چه از طرف بازیگران سیاسی مخالفش ــ رصد می‌کند.

ما امیدواریم بتوانیم با بررسی روندهای امنیت سایبری، چشم‌انداز دایماً در حال تغییرِ فضای مجازی در ایران را پیگیری کنیم، منطق فعالیت‌های سایبری تهاجمی یا دفاعی را دریابیم، و تصویر جامعی از نزاع‌های سایبری در خاورمیانه را ترسیم کنیم.

هکر بان دو بار در سال منتشر خواهد شد و هربار مهمترین روندهای شش ماه قبل را گزارش خواهد کرد. نخستین گزارش دربرگیرنده‌ی مهم‌ترین رویدادهای نیمه‌ی اول سال ۲۰۲۲ (۱۱ دی ۱۴۰۰ تا ۱۰ تیر ۱۴۰۱) است.

دو موضوع مهم در فاصله‌ی دسامبر گذشته تا ژوئن ۲۰۲۲ (دی ۱۴۰۰ تا تیر ۱۴۰۱) عبارت‌اند از (۱) ادامه‌ی حمله‌های سایبری جمهوری اسلامی علیه ایرانیان خارج از کشور به شکل «فیشینگ» (دزدی هویت از طریق جلب اعتماد)، جعل هویت، و خرابکاری در اکانت‌ها، و (۲) افزایش حمله‌های هکرها با آماج ایران و اسراییل، و اتهام‌های دوجانبه‌ی این دولت‌ها به یکدیگر.

در حالیکه جمهوری اسلامی به مذاکرات هسته‌ای با قدرت‌های جهانی ادامه می‌دهد ــ و مخالفت شدید اسراییل با هر نوع توافق ادامه می‌یابد ــ حمله‌های سایبری فزونی گرفته و همچون امتداد تنش‌های ژئوپولتیک میان دو دولت عمل می‌کند.

دسامبر ۲۰۲۱
(۱۰ آذر تا ۱۰ دی ۱۴۰۰)

در دسامبر ۲۰۲۱ چند روز پس از هشدار آپاچی (وب سِرور) در مورد آسیب‌پذیری «لاگ۴ج» (Log4j)[۱۲] ــ یک چارچوب کدنویسی برای استفاده در نرم‌افزارهای مختلف ــ معلوم شد که هکرهای وابسته به دولت ایران در حمله‌های سایبری خود از این آسیب‌پذیری استفاده کرده‌اند.[۱۳] به طور مشخص، تهدید مداوم پیشرفته ۳۵ (APT35)[۱۴] که به نام‌های بچه‌گربه‌ی دوست‌داشتنی (TS453، Charming Kitten)، و فسفر شناخته می‌شود، فقط با به‌کار گرفتن ابزارهای مقدماتی کدنویسی رایج از این آسیب‌پذیری سوءاستفاده می‌کرد. این نشان می‌داد هکرها خیلی سریع دست به کار شده و از آسیب‌پذیری مذکور بهره گرفتند.

تحقیق فیلتربان نشان می‌دهد که سازمان‌های جامعه مدنی بیشتر از دیگران در معرض حمله‌های APT35 هستند، به ویژه آنها که هنوز از نسخه‌های قدیمی نرم‌افزار VMWare (یک سرویس رایانه‌ای ابری) و وب‌سِرورهایی که از آسیب‌پذیری «لاگ۴ج» صدمه دیدند، استفاده می‌کنند.

---

۱۲ https://logging.apache.org/log4j/2.x/security.html

۱۳ https://research.checkpoint.com/2022/apt35-exploits-log4j-vulnerability-to-distribute-new-modular-powershell-toolkit/

۱۴ https://www.cfr.org/cyber-operations/charming-kitten

تصویر ۱ ـ هک و تغییر چهره‌ی پایگاه توانا بر روی فوروم «زون اچ»، ۸ بهمن ۱۴۰۰

APT35 تاریخچه‌ای طولانی در استفاده از نرم‌افزارهای جاسوسی، فیشینگ، و مهندسی اجتماعی به قصد نظارت و رصد کردن دارد. این گروه با سپاه پاسداران انقلاب که در سراسر کشور نفوذ کرده، همکاری دارد . گرچه اولین بار نبود که گروه‌های ایرانی در صدد نفوذ در شبکه‌های سازمان‌های جامعه مدنی برآمدند، اما این مورد جدید نشان از پشتکار آنها در سوءاستفاده از آسیب‌پذیری‌های شناخته شده دارد.

ژانویه ۲۰۲۲
(۱۱ دی تا ۱۲ بهمن ۱۴۰۰)

۷ بهمن ۱۴۰۰، یک گروه هکری ناشناس به کانال یک صدا و سیما[۱۵] شبیخون زد و به مدت کوتاهی تصویرهای رهبران سازمان مجاهدین خلق را ور ر پرده‌ی این شبکه نشان داد. مجاهدین، که خواهان سرنگونی جمهوری اسلامی هستند، مسئولیت این حمله را به عهده نگرفتند. بعید نیست این حمله، با وجود بُرد محدود و پوشش خبریِ کمی که گرفت، بر رویدادهای بعدی تأثیر گذاشته باشد، از جمله حمله‌ای که به یکی از سازمان‌های جامعه مدنی تبعیدی صورت گرفت.

۸ بهمن ۱۴۰۰، دست‌کم سه وبسایت وابسته به «آموزشکده الکترونیکی توانا برای جامعه مدنی» آماج حمله سایبری قرار گرفت و تصویرهای تحقیرآمیزی از رهبران سازمان مجاهدین خلق بر صفحات آنها ظاهر شد. در اطلاعیه هکرها ادعا شد که توانا

۱۵ https://twitter.com/radiofarda_/status/1486679822856245250?s=21&t=LoFLjKLn6JM1-xBwdEjuhg

تصویر ۲ ـ عصای موسی اعلام می‌کند که دوربین‌های مداربسته‌ی اسراییل را هک کرده است.

«مرکز فنی عملیات سایبری مجاهدین خلق» است و میان حمله‌ی سایبری به صدا و سیما در روز قبل با آموزشکده توانا ارتباط‌هایی وجود دارد.

همان اطلاعیه در یک فروم مربوط به حمله‌های سایبری به نام «زون اچ» (Zone-H) هم پست شد که وعده می‌داد به زودی دست به افشاگری در مورد اعضای توانا خواهد زد (تصویر ۱). روز ۷ بهمن ۱۴۰۰ یک هکر که خودش را «کالین۳ت» (Kalin3t) می‌نامد در کانال تلگرام خود[۱۶] (kalin3t hacker) یک ویدیوی یک دقیقه‌ای از کسانی که عضو رسمی توانا هستند را پست کرد. پست قبلی همین گروه در ۱۶ بهمن، با حمله به یکی از تجمعات مجاهدین، گفت به زودی اطلاعات محرمانه‌ای از مجاهدین پخش می‌کند. معلوم شد این اطلاعات همان مشخصات شخصی کاربران آموزشکده توانا است.
طی سال‌های متمادی جمهوری اسلامی طیف گسترده‌ای از گروه‌های مخالف خود را منافق و وابسته به سازمان مجاهدین قلمداد کرده‌است هرچند گرایش سیاسی، فعالیت‌ها و تاریخچه‌ی آنها از هم متفاوت است. نسبت وابستگی توانا به مجاهدین هم از همین قماش اتهام‌ها به نظر می‌رسد.

تحقیق فیلتربان نشان می‌دهد که پیش از حمله به سایت توانا و نشت اطلاعات آن، دست‌کم دو کارمند این سازمان اعلام کرده بودند که هویت آنها در «اسکایپ» جعل شده است.

این دو کارمند هشدار دادند که بعضی از حساب‌های جعلی با کسانی که در لیست مخاطبان آنها هستند ارتباط برقرار می‌کنند و از این طریق شماره تلفن و اطلاعات بانکی را می‌گیرند، همچنین دست به توزیع فایل‌های خطرناک می‌زنند. روشن نیست که تا چه حد این رویداد با حمله سایبری به توانا مرتبط بوده باشد. در مورد ارتباط آن با «کالین۳ت» و کانال تلگرام او هم اطلاعاتی در دست نیست.

۱۶ https://twitter.com/radiofarda_/status/1486679822856245250?s=21&t=LoFLjKLn6JM1-xBwdEjuhg

تصویر ۳ ـ توییت سپاه پاسداران همان شبی که سایت‌های اسراییل هدف حمله سایبری قرار گرفتند.

روز ۸ بهمن فقط توانا نبود که مورد حمله قرار گرفت. یک گروه هکری به نام «عصای موسی» (Moses Staff) ویدیو کلیپ‌هایی از دوربین‌های مداربسته‌ی خیابانی در اسراییل بر روی وبسایت خود گذاشتند.[۱۷] در بیانیه‌ای با عنوان «ما شما را با چشمان خودتان می‌بینیم . . .» ، این گروه هکری ادعا می‌کرد این ویدیوها فقط بخش کوچکی از عملیات بزرگتر جاسوسی است که دستگاه‌های امنیتیِ اسراییل را هدف گرفته است. در ادامه همان تهدیدهای قدیمی ایران برای حملهِ به اسراییل تکرار شده است. خبرگزاری فارس وابسته به سپاه در گزارشی راجع به این موضوع، این اقدامات را به گروه «عصای موسی» نسبت داد، بدون آنکه اطلاعات بیشتری در مورد این گروه هکری، ساختار و وابستگی آن ارائه کند.[۱۸] در آبان ۱۴۰۰، خبرگزارس فارس به فعالیت‌های دیگر گروه عصای موسی پرداخته بود، از جمله هک کردن نقشه‌های سه بعدی و تصاویر زیرساخت‌های مهم اسراییل، سرقت اسناد مالی سه بنگاه مهندسی اسراییلی[۱۹] و حمله نفوذی به وزارت دفاع اسراییل و نشت اطلاعات شخصی کارکنان نظامی و سرقت مدارک محرمانه‌ی دیگر.[۲۰]

شرکت امنیت سایبری «سایبریزن» که اسراییلی است حدس می‌زند که «عصای موسی» برای جمهوری اسلامی ایران کار می‌کند. این گمانه‌زنی بر اساس سرنخ‌های ایدئولوژیک و همسویی آن با منافع ژئوپولیتیک جمهوری اسلامی صورت گرفته است.[۲۱]

۱۷ https://moses-staff.se/we-see-with-your-eyes

۱۸ https://bit.ly/3lAr4ka

۱۹ https://bit.ly/3z14VlQ

۲۰ https://bit.ly/3o1YwH6

۲۱ https://www.cybereason.com/blog/research/strifewater-rat-iranian-apt-moses-staff-adds-new-trojan-to-ransomware-operations#:~:text=Over%20the%20past%20months%2C%20the,by%20leaking%20sensitive%2C%20stolen%20data

مارس ۲۰۲۲
(۱۰ اسفند ۱۴۰۰ تا ۱۲ فروردین ۱۴۰۱)

۲۳ اسفند ۱۴۰۰، یک هفته قبل از تعطیلات عید نوروز، یک گروه هکری که خود را «قیام تا سرنگونی» می‌نامد در توییتر اعلام کرد اقدام به هک ۶۲ دامنه و وبسایت وابسته به وزارت فرهنگ و ارشاد اسلامی کرده، ۷۷ وب‌سِرور را پایین کشیده، و ۲۸۰ دستگاه رایانه‌ای را از کار انداخته است.[۲۲]

مشابه با هک کا ۴۳۰۰ نال یک صدا و سیما، اینجا هم تصویرهای رهبران سازمان مجاهدین همراه با حمله‌های لفظی به آیت‌الله علی خامنه‌ای بر وبسایت‌ها ظاهر شد. این خبر نخست از سوی ایسنا منتشرشد که نوشت هیچ مقام وزارت ارشاد تا کنون آن را تأیید نکرده است.[۲۳]

همان روز، موجی از حمله‌های دی‌داس (DDoS) که با انبوه تقاضاهای همزمان، سرورها را زیر بار سنگین پایین می‌کشند، چندین وبسایت دولت اسراییل را که از دامنه‌ی «.gov.il» استفاده می‌کنند مثل وزارت‌های بهداشت، دادگستری، رفاه اجتماعی، و دفتر نخست وزیر، مورد حمله قرار دادند.[۲۴]

یک گروه هکری به نام «سایه سیاه» (Black Shadow) که سابقه‌ی استفاده از باج‌افزار را دارد،[۲۵] خود را مسئول این حمله‌ها معرفی کرد. این گروه قبلًا به شرکت‌های اسراییلی، از جمله یک شرکت میزبان خدمات اینترنتی و یک شرکت دوست‌یابی اقلیت‌های جنسی،[۲۶] حمله کرده بود. گفته می‌شود آن حمله‌ها به تلافی حمله‌ی سایبری به پمپ‌بنزین‌های ایران و فلج کردن چهار هزارو سیصد ایستگاه پمپ بنزین در اکتبر ۲۰۲۱ بود که احیای سرویس بنزین چندین روز طول کشید. آن حمله طبق گفته‌ی دو کارمند وزارت دفاع آمریکا به دست اسراییل انجام شده بود.[۲۷]

کمی پیش‌تر از آنکه خبر حمله‌ی سایبری به وبسایت‌های اسراییلی اعلام شود، حساب توییتری سپاه پاسداران مرموزانه تهدید کرده بود که «رژیم صهیونیستی امشب را هیچ‌گاه فراموش نخواهد کرد»، که با هشتگ #این_تازه_شروع_ماجراست همراه بود. به فاصله‌ی چند دقیقه، حساب‌های کاربری مدافع سپاه شروع به تکثیر این توییت کردند و حتی پیش از اینکه دولت اسراییل رسماً حمله را اعلام کند، خبر هک کردن سایت‌های اسراییلی را منتشر کردند. حساب‌های وابسته به سپاه حمله‌ی سایبری مذکور را «نخستین ضربه» نامیدند؛ به این معنی که بازهم دست به حمله خواهند

---

۲۲ https://twitter.com/GhiamSarnegouni/status/1503259362944507907

۲۳ https://bit.ly/3NYK4dq

۲۴ https://www.haaretz.com/israel-news/tech-news/2022-03-15/ty-article/.premium/cyber-attack-on-israel-biggest-attack-ever-or-iranian-propaganda/00000180-5bba-db1e-a1d4-dffbfa970000

۲۵ https://securityaffairs.co/wordpress/124000/hacking/black-shadow-hacked-cyberserve.html

۲۶ https://www.cyberscoop.com/hack-and-leak-group-black-shadow-keeps-targeting-israeli-victims/

۲۷ ر. ک. پانوشت ۱

تصویر ۴ ـ هک کردن سایت‌های شهرداری تهران، ۱۲ خرداد، منبع: حساب توییتری قیام تا سرنگونی

تصویر ۵ ـ وبسایت شهرداری تهران قبل و بعد از حمله سایبری قیام تا سرنگونی
(منبع: توییتر قیام تا سرنگونی)

زد.[۲۸] همان شب، سپاه پاسداران اعلام کرد که رهبر یک گروه وابسته به موساد (سازمان امنیت اسراییل) را دستگیر کرده است. سپاه ادعا کرد این گروه قصد خرابکاری در تأسیسات هسته‌ای فُردو را داشته است.[۲۹]

۲۸ https://twitter.com/matinmoraveji/status/1503428748418375683?s=21&t=ylr8F37pYsiE4MB4tjRmDQ

۲۹ https://twitter.com/sepah_fa/status/1503432110404784134?s=21&t=ylr8F37pYsiE4MB4tjRmDQ

تصویر ۶ ـ نموداری از حمله‌های سایبری گروه «عصای موسی» به هدف‌های اسراییلی. این نمودار از سوی چند اکانت توییتری هوادار رژیم اسلامی در خرداد ۱۴۰۱ منتشر شد.

آوریل ۲۰۲۲
(۱۲ فروردین تا ۱۱ اردیبهشت ۱۴۰۱)

۵ اردیبهشت، گروه هکری «قیام تا سرنگونی» برای نخستین بار پس از هک کردن وزارت فرهنگ در اسفند سال گذشته، دوباره پا به صحنه گذاشت. این بار هدف حمله ۴۹ دامنه وابسته به وزارت کشاورزی ایران بود. وبسایت‌های هک شده باز هم مثل گذشته تصویر رهبران سازمان مجاهدین را به نمایش گذاشته و خواهان مرگ خامنه‌ای شدند.[۳۰] همچنین تعدادی از اسناد محرمانه‌ی دولتی که از شبیخون به شبکه وزارت کشاورزی به دست آمده بود نیز به وسیله‌ی این گروه هکری به بیرون درز کرد.[۳۱]

۳۰ https://twitter.com/ghiamsarnegouni/status/1518500745406029825?s=21&t=u-ib7_STQ6XC7zLASdUNYQ

۳۱ https://twitter.com/GhiamSarnegouni/status/1518544409268211713

این حمله ظاهراً به جبران سرکوب تظاهرات کشاورزانِ اصفهان صورت گرفت. کشاورزان اصفهانی ابتدا در آبان ۱۴۰۰ به طور مسالمت‌آمیز دست به تظاهرات زدند و به شدت به دست نیروهای امنیتی سرکوب شدند. در فروردین ۱۴۰۱ دست‌کم در دو نوبت تظاهراتی برگزار شد که خواهان پاسخگویی مقامات محلی، به خاطر سوء مدیریت منابع آبی و تاثیر منفی آن بر اقتصاد کشاورزی شد.

ژوئن ۲۰۲۲
(۱۱ خرداد تا ۱۰ تیر ۱۴۰۱)

گروه «قیام تا سرنگونی» در این ماه نیز به فعالیت‌های خود ادامه داد. این بار وبسایت و پورتال پیامک‌رسانی شهرداری تهران را هدف گرفت، همچنین بیش از پنجاه هزار دوربین مداربسته در اطراف شهر،[۳۲] از جمله در محل مزار روح‌الله خمینی، بنیانگذار نظام را هک کرد.[۳۳] این حمله‌ها روز تعطیل ۱۲ خرداد، سالروز مرگ خمینی، صورت گرفت. مشابه حمله‌های سایبری پیشین، تصویرهای رهبران مجاهدین و پیام‌های ضدرژیم صفحات هک شده را مزین کرد.

رسانه‌های داخلی این واقعه را گزارش دادند و برخی به نقل از مقامات شهرداری گفتند موساد مسئول این حمله بوده است.[۳۴] دو هفته بعد، خبرگزاری فارس مدعی شد در رابطه با این حمله دست‌کم یک نفر وابسته به سازمان‌های جاسوسی بیگانه دستگیر شده است.[۳۵] فیلتربان سندی به دست آورده که حاوی گزارش امنیتی به شهرداری متعاقب این حمله بوده و در آن جزییات نرم‌افزار مورد استفاده هکرها را شرح داده است.

باید اضافه کرد که استفاده‌ی مدام از نام سازمان مجاهدین خلق به عنوان مسئول اصلی حمله‌های اخیر چندان مجاب‌کننده نیست. دلیل آن است که سازمان مجاهدین در گذشته چندان از خود توانایی بالای فعالیت‌های سایبری نشان نداده و در این زمینه تاریخ بلندی ندارد. خود سازمان مجاهدین نیز رسماً مسئولیت این حمله‌ها را به عهده نگرفته است.

در پاسخ به این حمله‌ها، گروه هکری «عصای موسی» به سه شرکت برق و انرژی در اسراییل، از جمله شرکت برق اسراییل (IEC) حمله کرد.[۳۶]

۲۵ خرداد، همان گروه که دوربین‌های مداربسته‌ی اسراییل را هک کرده بود، اعلام کرد که «این تازه شروع ماجراست» و وعده داد که «منتظر حملات ترکیبی باشید.»[۳۷] یک

---

۳۲ https://twitter.com/ghiamsarnegouni/status/1532396522171777027?s=21&t=uwHhq95PmXaBvQFFR17qeg

۳۳ https://twitter.com/ghiamsarnegouni/status/1532276891100532738?s=21&t=R860snG2h_T-sAzvCbiiVg

۳۴ https://bit.ly/3zjedjH

۳۵ https://bit.ly/3cf8PEX

۳۶ https://moses-staff.se/israeli-power-companies/

۳۷ https://twitter.com/staffofmoses1/

هفته بعد، گروه عصای موسی فهرستی از شماره تلفن‌هایی که ادعا می‌کرد به سران بالای ارتش اسراییل تعلق دارد، از جمله تلفن سخنگوی ارتش اسراییل، را منتشر کرد.[۳۸] در یک حمله‌ی سایبری جداگانه، سیستم اخطار شهرداری که در اورشلیم و عیلات آژیر حمله موشکی را به صدا در می‌آورد هدف قرار گرفت اما طبق گزارش رسانه‌های اسراییلی، این حمله موفق به نفوذ در زیرساخت‌های مهم ارتش اسراییل نشد.[۳۹]

پس از گذشت چند روز، این بار نوبت ایران بود که هدف حمله متقابل قرار گیرد. روز ۶ تیر ۱۴۰۱، یک گروه هکری به نام «گنجشک درنده» مسئولیت خرابکاری در یک مجتمع فولاد ایرانی را به عهده گرفت. در این حمله به ماشین‌آلات این مجتمع خسارت‌های فیزیکی وارد آمد که به وسیله‌ی دوربین‌های امنیتی ضبط شده است.[۴۰]

گنجشک درنده توضیح داد که این حمله به تلافی حمله‌های سایبری جمهوری اسلامی و ادامه فعالیت مجتمع فولاد علی‌رغم تحریم‌های اقتصادی صورت گرفته است. مقامات دولت ایران گفتند خسارت جزیی بوده و تهدیدها خنثی شده است. این گروه هکری قبلاً به پمپ بنزین‌ها،[۴۱] خطوط راه آهن سراسری،[۴۲] و وزارت خانه‌سازی و طراحی شهری حمله کرده بود.[۴۳]

۷ تیر ۱۴۰۱، بیش از ۲۰ اداره، هتل، و مراکز استراحت مورد حمله‌ی سایبری قرار گرفتند، از جمله وبسایت‌های این هتل‌ها می‌توان به موارد زیر اشاره کرد: hotels4u.co.il, hotels.co.il, isrotel.com, minihotel.co.il, trivago.co.il and danhotels.com یک گروه هکر ایرانی به نام «پسران تیزهوش» (ظاهراً به تأثیر از نام «پسران پرافتخار آمریکایی»[۴۴]) مسئولیت این حمله‌ها را به عهده گرفت و دست به انتشار اطلاعات شخصی بیش سیصدهزار اسراییلی زد که اسامی و مشخصات آنها را از سایت‌های توریستی اسراییلی به سرقت برده بود. این اطلاعات شامل شماره هویت ملی، آدرس، اطلاعات کارت اعتباری و اقلام دیگر می‌شد.[۴۵]

---

status/1539594882620297216?s=21&t=IXOXImGJRQGEitpUeeJe1Q

۳۸ https://twitter.com/staffofmoses1/status/1539591537453146112?s=21&t=HZbvjrnfvIGzRy8DseECQQ

۳۹ https://www.israeltoday.co.il/read/iranian-cyber-attackers-trying-and-so-far-failing-to-create-panic-in-israel/

۴۰ https://t.me/GonjeshkeDarand/20

۴۱ https://twitter.com/gonjeshkedarand/status/1452992555361214474?s=21&t=h7MR0r1rxV9dUW9utmxHCw

۴۲ https://twitter.com/gonjeshkedarand/status/1452876401804288001?s=21&t=h7MR0r1rxV9dUW9utmxHCw

۴۳ https://twitter.com/gonjeshkedarand/status/1452879508214886406?s=21&t=h7MR0r1rxV9dUW9utmxHCw

۴۴ https://www.splcenter.org/fighting-hate/extremist-files/group/proud-boys

۴۵ https://m.jpost.com/israel-news/article-710973/amp

قبلاً در آذر ۱۴۰۰، گروه پسران تیزهوش دو وبسایت اسراییلی که ویژه راه‌پیمایی و ورزش بود را هک کرده و اطلاعات شخصی بیش از صدهزار کاربر - از جمله آدرس ایمیل، آدرس منزل، عکس‌های خانوادگی، و شماره تلفن - را به بیرون درز داده بود. این گروه هکری بعداً اطلاعات بیش از سه میلیون نفر را برای فروش عرضه کرد بدون آنکه مشخصاً پولی دراین‌باره درخو است کند.[۴۶]

نتیجه

نیمه‌ی نخست سال ۲۰۲۲ مملو از حمله‌های سایبری، همسو با منافع ژئوپولیتیک ایران و اسراییل بود. بالا رفتن تعداد این حمله‌ها، دامنه‌ی نفوذ و تنوع هدف‌های آنها بسیار قابل توجه است. در حالیکه هریک از این دو دولت دیگری را متهم به فعالیت‌های خرابکارانه می‌کند، هیچ بیانیه و انتساب رسمی از سوی هیچ‌کدام صادر نشده است.

با این حال، تجزیه و تحلیل فنی این حمله‌ها به ما می‌گوید که هکرهای «سایه سیاه» و «عصای موسی» به ایران تعلق دارند. انتساب حمله‌هایی که به نهادهای ایرانی شده دشوارتر است، اما دست‌کم به شهادت دو کارمند آمریکایی در گزارش نیویورک تایمز، اسراییل مسئول حملات سایبری «گنجشک درنده» به سیستم پمپ بنزین‌های ایران بود. این نشانه‌ها تصویری پیچیده از تشدید عملیات امنیتی و اقدامات خرابکارانه از طریق فضای مجازی ترسیم می‌کنند که با افزایش تنش‌های سیاسی میان دو دولت همخوانی دارد.

در حالی که جامعه بین‌الملل در جستجوی راه حل دیپلماتیک برای برنامه هسته‌ای ایران است، اسراییل همچنان هشدار می‌دهد که یک ایران اتمی برای آینده منطقه و جهان خطرناک است. در پاسخ، ایران اسراییل را به کارشکنی در مذاکرات هسته‌ای متهم کرده و این کشور را به «انتقام سخت» تهدید می‌کند. این دعواهای سایبری در سطوح پایین، در مقایسه با احتمال جنگ واقعی با عواقب به شدت سهمگین میان دو دولت، بدیل کم‌هزینه‌تری محسوب می‌شود. فعلاً کارکرد اصلی حمله‌های سایبری ایجاد نوعی بازدارندگی است.

تا این تاریخ، حمله‌های سایبری به نهادهای ایران سیستماتیک‌تر و سازمان‌داده‌شده‌تر شده‌اند. ترکیب خرابکاری و جاسوسی حاکی از دست‌اندرکار بودن سازمان‌های امنیتی در طراحی و اجرای حمله‌های اخیر علیه ایران است. استفاده‌ی مدام از نام مجاهدین خلق برای استتار عاملان اصلی نشان می‌دهد هر نیرویی که پشت این حمله‌هاست فهم درستی از اپوزیسیون ایران دارد و با زبان و تبلیغات جمهوری اسلامی علیه آنها آشناست. اما انتساب مسئولیت به مجاهدین عواقب خطیری برای آزادی‌های مدنی و سیاسی در ایران دارد. چنین انتسابی به تبلیغات دولتی دامن می‌زند که طبق آن گروه‌های مخالف را همچون یک تهدید وجودی برای رژیم قلمداد می‌کند و در نتیجه دور باطل سرکوب علیه ناراضیان مدنی تکرار می‌شود. این نیز به نوبه‌ی خود به حملات سایبری دولت علیه سازمان‌های جامعه مدنی می‌انجامد؛ همانطور که در مورد آموزشکده توانا شاهدش بودیم.

---

۴۶ https://m.jpost.com/business-and-innovation/tech/hackers-attack-israeli-hiking-websites-leak-personal-information-689128/amp

در مقابل، حمله به شبکه‌های اسراییل از درجه پیچیدگی کمتری برخوردار هستند و عمدتاً به قصد اخلال و ایجاد هراس عمومی عمل می‌کنند (مثل فعال کردن آژیرهای خطر یا هک کردن دوربین‌های مداربسته). اما هکرهای وابسته به دولت ایران پشتکار دارند و تاکتیک‌های خود را مدام بهبود می‌بخشند و آسیب‌پذیری‌های جدیدی کشف می‌کنند تا حمله‌های بعدی خود را از آن طریق عملی سازند. در حالیکه مذاکرات هسته‌ای ادامه دارد و تنش میان ایران و اسراییل بالا می‌گیرد، به احتمال زیاد حمله‌های سایبری متقابل هم گسترش می‌یابند و متحول می‌شوند. مهمتر اینکه، این جدل‌های سایبری در فضای مجازی تأثیر منفی خود را بر شهروندان عادی گذاشته و به حقوق بشر در سطوح مختلف آسیب می‌زند. با توجه به فقدان تخصص لازم و اولویت نداشتن ایمن‌سازی شبکه‌های غیرنظامی برای دولت، به احتمال زیاد این شبکه‌ها همچنان در معرض حمله‌های سایبری بیشتری قرار خواهند گرفت. ما در گزارش‌های آینده‌ی هکر بان این روندها را پوشش خواهیم داد.