پایگاه اطلاع‌رسانی گرداب جهت افزایش آگاهی مخاطبان خود علی‌الخصوص پژوهشگران، مدیران و کارشناسان حوزه سایبری اقدام به ترجمه و انتشار این گزارش کرده است. بدیهی است محتوای این گزارش مورد تایید این نهاد نیست.

تیم بررسی تهدیدات سایبری در شرکت مایکروسافت در گزارشی به بررسی انواع جدید حملات سایبری منتسب به گروه‌های مرتبط با جمهوری اسلامی ایران پرداخته است. در این گزارش هدف اصلی عملیات‌های سایبری گروه‌های ایرانی را اقدامات تلافی‌جویانه در مقابل عملیات‌های سایبری دشمنان معرفی شده است که با توجه به سطح بسیار بالای پیچیدگی عملیات‌های سایبری دشمنان، گروه‌های ایرانی تلاش می‌کنند تا توانایی‌ها و ظرفیت‌های خود را به سطح دشمنان خود ارتقا دهند؛ تلاشی که تا حدی موفق ارزیابی شده است.
در ادامه گزارش با اشاره به رویدادهای سیاسی متناظر با رخدادهای سایبری تلاش داشته است تا تحلیلی از اقدامات احتمالی آتی گروه‌های سایبری ایرانی داشته باشد.

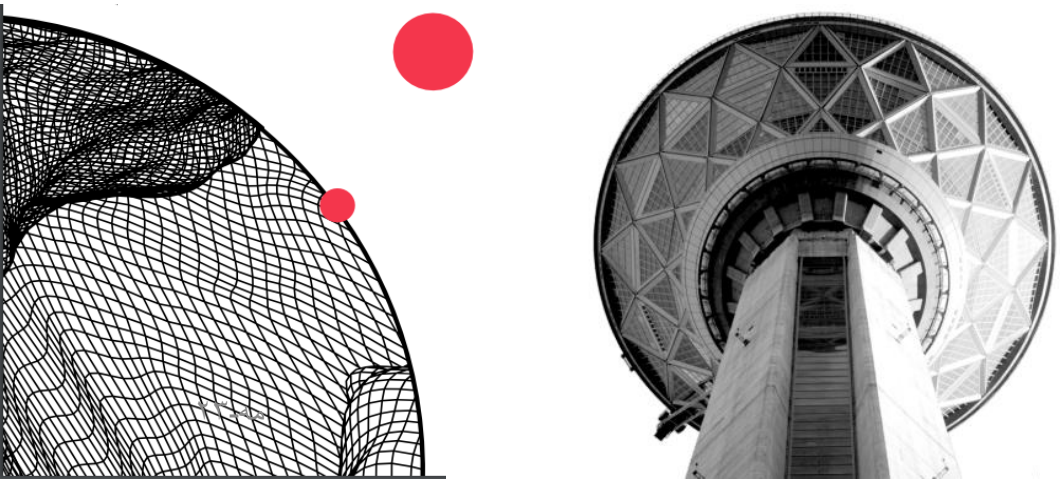
01010111 01101000 01101001
01101100 01100101 00100000
01110011 01100101 01100101
01101011 01101001 01101110
01100111 00100000 01101110
01100101 01110111 00100000
01100011 01111001 01100010
01100101 01110010 01100001
01110100 01110100 01100001
01100011 01101011 00100000
01100011 01100001 01110000
01100001 01100010 01101001
01101100 01101001 01110100
01101001 01100101 01110011

Microsoft

ایران برای اثرگذاری بیشتر به عملیات نفوذ سایبری روی می‌آورد

دوم مِی ۲۰۲۳

اطلاعات تهدیدات مایکروسافت



فهرست مطالب

معرفی

عاملان دولتی ایران برای رسیدن به تأثیرگذاری ژئوپلیتیک بیشتر، به مجموعه‌ی جدیدی از تکنیک‌های مدنظر با ترکیب عملیات سایبری و نفوذ - که ما به آن عملیات نفوذ سایبری می گوییم – روی آورده‌اند. از ژوئن ۲۰۲۲ چندین گروه دولتی ایرانی برای تقویت و پررنگ کردن اقدامات خود یا جبران کاستی‌ها در دسترسی به شبکه یا قابلیت‌های حمله سایبری خود، مرتباً از عملیات نفوذ سایبری استفاده کرده‌اند. اساساً آنها عملیات سایبری تهاجمی را با عملیات نفوذ چندجانبه ترکیب کرده‌اند تا تغییرات ژئوپلیتیکی را در راستای اهداف رژیم تقویت کنند. این اقدامات شامل عملیات‌هایی در سال جاری می‌شود که به دنبال تقویت مقاومت فلسطین، دامن زدن به اعتراضات شیعیان در بحرین و مقابله با عادی‌سازی روابط اعراب و اسرائیل بوده است.

افزایش همگرایی عملیات‌های سایبری و عملیات‌های نفوذ توسط گروه‌های ایرانی به دنبال حملات سایبری بسیار پیچیده‌ایست که از ژوئیه ۲۰۲۱ علیه ایران اتفاق افتاده است. احتمالاً ناتوانی ایران در انطباق با پیچیدگی برخی از حملات سایبری که با آن مواجه شده است، رژیم را بر آن داشته تا روش‌های نوآورانه‌ای را برای مقابله به مثل، برای همسویی با ترجیح آن‌ها در حوزه‌ی امنیت ملی (که انجام اقدامات تلافی‌جویانه‌ی متناسب و مستقیم است) به شیوه‌ای که متناسب به نظر می‌رسد بیابد .

احتمالاً عاملان تهدیدکننده‌ی ایرانی همزمان با بهبود بخشیدن توانایی‌های خود، در راستای انجام اقدامات تلافی‌جویانه‌ی متناسب، به دنبال تقویت تکنیک‌های سایبری و نفوذ خود برای رساندن خود به سطح حملات بسیار پیچیده‌ای هستند که با آن روبه‌رو هستند. بهبود مستمر در روش‌های تهاجمی سایبری عاملان تهدیدکننده‌ی ایرانی، گزینه‌های آن‌ها را برای هدف‌گیری، از جمله در برابر اهداف با مشخصات بالاتر، افزایش می‌دهد. همزمان تکنیک‌های جدید آن‌ها برای نفوذ به بسط، واقع‌گرایی و اثربخشی نهایی کمپین‌های آنها می‌افزاید. این گزارش بر دلایل احتمالی افزایش استفاده ایران از عملیات‌های نفوذ سایبری، تکنیک‌های مورد استفاده و تهدیدات محتملِ آتی تمرکز خواهد کرد.

این گزارش همچنین به‌روزرسانی شش ماهه‌ای درباره‌ی پیشرفت‌هایی که توسط عاملان تحت حمایت دولت ایران در عملیات‌های سایبری و روش‌های نفوذ از اواخر سال ۲۰۲۲ نشان داده شده است، ارائه می‌کند.

مایکروسافت به‌روزرسانی‌های شش ماهه را در خصوص ایران و سایر عاملان دولتی منتشر می‌کند تا به مشتریان خود و جامعه جهانی در مورد تهدید ناشی از چنین عملیات‌هایی هشدار دهد و بخش‌ها و مناطق خاصِ در معرض خطرِ بیشتر را شناسایی کند.

تعریف اصطلاحات کلیدی

عملیات نفوذ سایبری

عملیاتی که در آن تهاجم به شبکه‌ی کامپیوتری، با پیام‌رسانی و دامنه دادن به پیام‌ها به شیوه‌ای هماهنگ و تاثیرگذار ترکیب می‌شوند تا ادراکات، رفتارها یا تصمیمات مخاطبان هدف را به سمت پیشبرد منافع و اهداف یک گروه یا یک کشور تغییر دهد.

شخصیت سایبری

یک گروه یا فرد ساخته شده برای نمایش به عموم که مسئولیت عملیات سایبری را بر عهده می‌گیرد و در عین حال قابلیت انکار قابل قبولی را برای گروه یا کشور اصلی مسئول ایجاد می‌کند.

عروسک خیمه شب بازی

یک شخصیت آنلاین جعلی که از هویت ساختگی یا دزدیده شده به منظور فریب استفاده می‌کند.

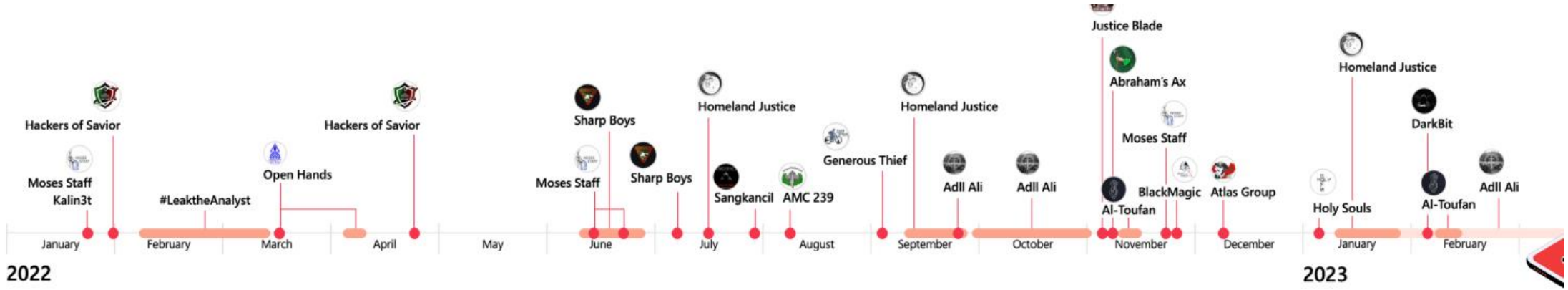
ایران عملیات نفوذ سایبری را شتاب می‌دهد

از ژوئن ۲۰۲۲ یکپارچه‌سازی عملیات‌های سایبری و نفوذ ایران سرعت گرفته است. در سال ۲۰۲۲ مایکروسافت ۲۴ عملیات نفوذ سایبری منحصر به فرد مرتبط با دولت ایران را شناسایی کرد – از جمله ۱۷ مورد از اواسط ژوئن – که در مقایسه با ۷ مورد در سال ۲۰۲۱ افزایش داشته است. (شکل ۱)

افزایش این عدد که ممکن است تا حدی به بهبود قابلیت‌های شناسایی ما نسبت داده شود، همزمان بوده با کاهش حملات باج‌افزارها یا پاک‌کن‌ها توسط گروه‌های مرتبط با بخش نظامی ایران و به‌ویژه سپاه پاسداران انقلاب اسلامی. همانطور که قبلاً گزارش شده بود، مایکروسافت از سال ۲۰۲۰ تا اواسط سال ۲۰۲۲ حملات بیشتری از این نوع را از سوی گروه‌های مرتبط با سپاه پاسداران و وزارت اطلاعات و امنیت شناسایی کرد. آخرین رشته عملیات‌های نفوذ سایبری سپاه پاسداران متمرکز بر حملات کم‌تاثیر و ساده‌ای همچون تغییر ظاهر وبسایت‌ها (Defacement) بود. اینگونه حملات سایبری زمان و منابع کمتری نیاز دارند و در روش‌های بسط چندجانبه نیازمند تلاش بیشتری هستند.

شکل ۱

جدول زمانی عملیات‌های نفوذ سایبری ایران نشان دهنده تطابق‌پذیری بیشتر است



در سال گذشته عملیات‌های نفوذ سایبری ایران، روایت‌هایی را در جهت تقویت مقاومت فلسطین، دامن زدن به اعتراضات شیعیان در کشورهای خلیج فارس، مقابله با عادی‌سازی روابط دیپلماتیک و اقتصادی اعراب با اسرائیل، ایجاد وحشت و ترس در میان اسرائیلی‌ها، و افشای فعالیت‌های فسادآمیز یا شرمسارکننده‌ی ایرانیانِ مخالف جلو برده‌اند.

همانطور که در ادامه بررسی می‌کنیم، برخی از عملیات‌ها چند روایت را دنبال کردند.

تقویت مقاومت فلسطین

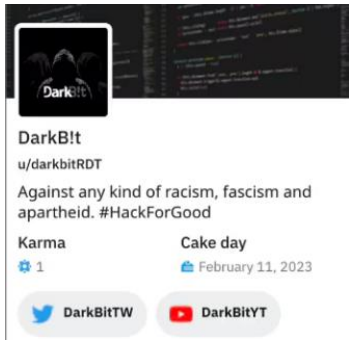
در اواسط فوریه، یک گروه احتمالاً ایرانی که ما با عنوان Storm-1084 (DEV1084) ردیابی می‌کنیم، حملات سایبری مخرب را با انتشار پیام‌هایی برای تشویق به پاسخ‌گویی به سیاست‌های اسرائیل در قبال فلسطینی‌ها ترکیب کرد. این گروه حملات خود را به‌عنوان باج‌افزار ارائه کرد و داده‌هایی را برای فروش در وب سیاه با استفاده از شخصیت سایبری DarkBit ارسال کرد که احتمالاً جهت افزایش قابلیت انکار از سوب ایران بوده است.

این باج‌افزار شامل یک یادداشت باج بود که از همان پیامی استفاده کرده بود که DarkBit در تلگرام قرار داده بود و در آن اسرائیل را «یک رژیم آپارتاید» نامیده بود که «باید بهای اشغالگری، جنایات جنگی علیه انسانیت و کشتار انسان‌ها» از جمله فلسطینیان را بپردازد. این نوع پیام‌ها سابقاً بین گروه‌هایی که طبق برآوردهای ما عملیات‌های نفوذ سایبری را از جانب سپاه پاسداران انجام می‌دهد دیده شده بود. (شکل ۳)

در ۷ آوریل یک عامل دولتی ایرانی دیگر که مرتبط با وزارت اطلاعات و امنیت است، احتمالاً دسترسی از راه دور را برای اجرای حملات Storm-1084 به دست آورد.

این عملیات همچنین ساختارها و محیط‌های ابری را هدف قرار داد و احتمالاً مستلزم زمان، منابع و مهارت‌های بیشتری نسبت به دیگر عملیات‌های اخیر سپاه پاسداران بود.

در این عملیات از تکنیک‌ها و ابزارهای گوناگون – از جمله برخی backdoorهای سفارشی شده– برای دسترسی، حفظ تداوم، افزایش نقاط برتری و اجرای حملات– استفاده شده بود.



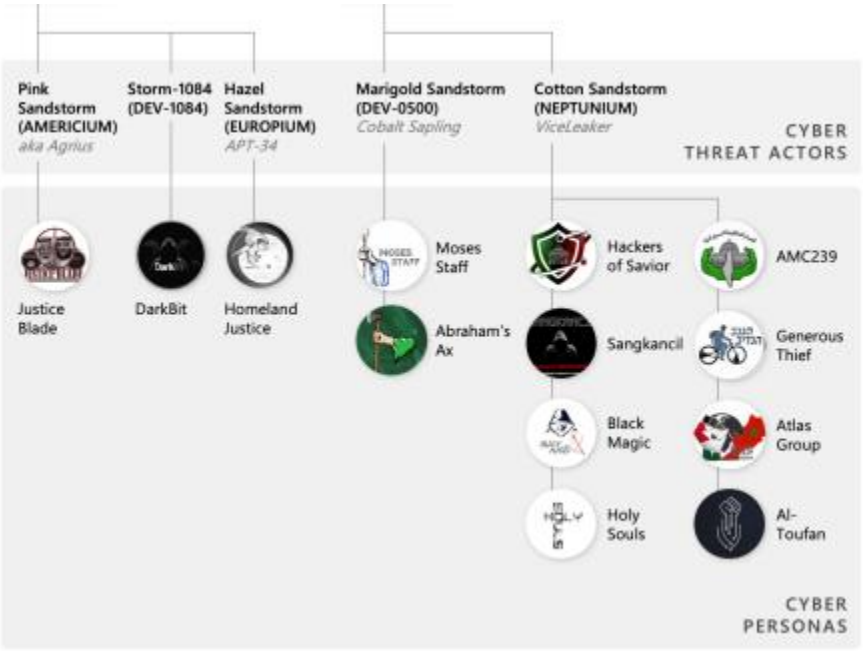
شکل ۲: حساب ردیت DarkBit که استفاده این گروه از توییتر و یوتیوب را نشان می‌دهد. DarkBit همچنین از طریق حساب‌های فیس‌بوک و تلگرام پیام ارسال کرد.

شکل ۳

عاملان دولتی ایران در اجرای عملیات‌های ترکیبی سایبری و نفوذ

سپاه پاسداران

وزارت اطلاعات



گروه‌های مرتبط با وزارت اطلاعات و سپاه پاسداران خود را برای بهره‌گیری از عملیات‌های نفوذ سایبری تطابق داده‌اند. در این گزارش از طبقه‌بندی جدید مایکروسافت برای نام‌گذاری عاملان تهدید استفاده می‌شود. برای اطلاع از جزئیات بیشتر در مورد طبقه‌بندی جدید و ارجاع متقابل به نام‌های قدیمی به وبلاگ و راهنمای مرجع ما مراجعه کنید.

شکل ۴

عملیات‌های نفوذ سایبری Cotton Sandstorm

شخصیت سایبری	Hackers of Savior	AMC239	Sangkancil	Generous Thief	Black Magic	Atlas Group	Holy Souls	الطوفان
آخرین عملیات	آوریل ۲۰۲۲	جولای ۲۰۲۲	آگوست ۲۰۲۲	سپتامبر ۲۰۲۲	نوامبر ۲۰۲۲	دسامبر ۲۰۲۲	ژانویه ۲۰۲۳	فوریه ۲۰۲۳
روش سایبری								
دزدی داده	✓	✓	✓	✓	✓		✓	✓
تغییر چهره‌ی وبسایت	✓	✓				✓	✓	✓
حمله‌ی انکار سرویس (DDoS)								✓
باج افزار					✓			
روش نفوذ								
نشت داده			✓	✓	✓		✓	
عروسک خیمه شب بازی		✓	✓	✓	✓	✓	✓	✓
جعل هویت قربانیان				✓	✓	✓	✓	✓
انتشار در گروه و صفحات شبکه‌های اجتماعی		✓	✓	✓	✓	✓	✓	✓
پیامک / ایمیل						✓		✓

مایکروسافت چنین ارزیابی می‌کند که اکثر عملیات‌های نفوذ سایبری ایران توسط Emennet Pasargad که ما آن را با عنوان Cotton Sandstorm ردگیری می‌کنیم اجرا می‌شود. این گروه یک عامل دولتی ایرانی است که به دلیل اقداماتش برای تضعیف روند انتخابات ریاست‌جمهوری ۲۰۲۰ آمریکا توسط وزارت خزانه‌داری ایالات متحده تحریم شده است. بر اساس ارزیابی ما Cotton Sandstorm در پشت صحنه‌ی تمام این ۸ شخصیت سایبری ساختگی که از ابتدای سال ۲۰۲۲ فعال بوده‌اند دخیل بوده یا مدیریت آن‌ها را بر عهده داشته است. همانطور که این نمودار نشان می‌دهد، تاکتیک‌ها، تکنیک‌ها و رویه‌های Cotton Sandstorm از اواسط ۲۰۲۲ توسعه و بهبود یافته است. ما بر اساس هم‌پوشانی قابل توجه میان تاکتیک‌ها، تکنیک‌ها و رویه‌های این گروه‌ها، آن‌ها را مرتبط با Cotton Sandstorm می‌دانیم. همچنین ما بر اساس اطلاعات منتشر شده از سوی دولت آمریکا، هم‌پوشانی بین قربانیان و سرنخ‌های فنی بین Cotton Sandstorm و عملیات‌های نفوذ، اطمینان بیشتری در انتساب فعالیت برخی شخصیت‌های سایبری به Cotton Sandstorm داریم. اطلاعات منتشرشده توسط برخی از شرکای تجاری نظیر شرکت Meta بر تقویت برآوردهای ما در ارتباط برخی از این شخصیت‌های سایبری با گروه Cotton Sandstorm تاثیرگذار بود.

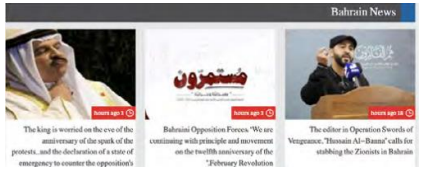
دامن زدن به اعتراضات شیعیان در بحرین

در اواسط فوریه، شخصیت سایبری الطوفان مدعی شد که چهره‌ی چندین وب سایت بحرینی و اسرائیلی را همزمان با دوازدهمین سالگرد آغاز تظاهرات سراسری ضددولتی در بحرین تغییر داده است. الطوفان که بر اساس ارزیابی ما توسط Cotton Sandstorm اداره می‌شود، وب‌سایت‌های خبری و دولتی بحرین را هدف قرار داد تا با دامن زدن به ناآرامی‌ها و برجسته کردن فقر و تورم، نارضایتی را در میان اکثریت شیعه‌ی بحرین که از نظر سیاسی قدرت کمتری دارند افزایش دهد. Cotton Sandstorm در ۱۱ فوریه در یک عملیات محتوای اصلی یک وب‌سایت خبری حامی دولت را با مقالاتی در انتقاد از رژیم و ترویج اعتراضات جایگزین کرد. سپس حساب‌های جعلی به زبان عربی (یا عروسک‌های خیمه شب بازی در رسانه‌های اجتماعی) خبر انجام این عملیات الطوفان را بسط دادند.

شکل ۵ سناریوی اجرای عملیات‌های نفوذ سایبری Cotton Sandstorm

حمله‌ی سایبری

تغییر چهره‌ی سایت های خبری دولتی



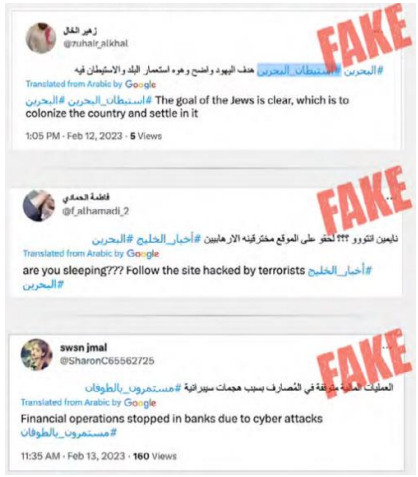
تغییر چهره‌ی سایت‌های اسرائیلی

اعلام عمومی

پست های توئیتری و تلگرامی الطوفان

بسط و دامنه دادن به پیام‌ها

پست‌های حساب‌های جعلی در توئیتر



هر دو عملیات Cotton Sandstorm در بحرین از یک سناریوی قابل پیش‌بینی برای عملیات نفوذ سایبری پیروی می‌کند که در جاهای دیگر نیز تکرار شده است. پس از یک **حمله‌ی سایبری** با پیچیدگی پایین (به عنوان مثال، تغییر چهره‌ی وب‌سایت)، یک شخصیت سایبری ساختگی خبر انجام حمله را در رسانه‌های اجتماعی **اعلام** کرده و پس از آن حساب‌های ساختگی به ظاهر نامرتبط، خبر حمله را به زبان مخاطب هدف بسط می‌دهد. همانطور که در عملیات الطوفان علیه انتخابات بحرین اتفاق افتاد، این گروه گاهی در مراحل اولیه‌ی بسط و دامنه دادن به خبر، از جعل هویت حساب‌های سازمان هدف یا یکی از مقامات ارشد آن سازمان برای ارتقای اعتبار این حمله سایبری استفاده می‌کند.

در ماه نوامبر، Cotton Sandstorm اولین عملیات نفوذ سایبری خود را علیه انتخابات پارلمانی بحرین، تحت پوشش الطوفان و با استفاده از سناریویی مشابه انجام داد. (شکل ۵)

این عملیات همچنین از طریق مشروعیت‌زدایی از انتخابات به دنبال برانگیختن اعتراض در میان شیعیان بحرین بود.

یک روز قبل از رای گیری ۱۲ نوامبر، الطوفان ادعا کرد که وب سایت پارلمان بحرین (nuwab.bh) را در حمایت از تحریم انتخابات و در پاسخ به «آزار و اذیت» مقامات بحرین مختل کرده است که احتمالاً اشاره‌ای به انحلال گروه‌های سیاسی شیعه توسط منامه دارد. اگرچه حملات سایبری توانست تنها به مدت زمان محدودی وب‌سایت پارلمان و یک سایت خبری را مختل کند،

Cotton Sandstorm به وسیله‌ی صدها اکانت جعلی توییتری و اینستاگرامی اقدام به دامنه دادن و برجسته کردن تأثیر حملات کرد. در واقع، برخی از این عروسک‌های خیمه شب بازی، هویت سازمان انتخابات پارلمانی بحرین و مدیر اجرایی آن را جعل کرده بودند و ادعا کردند که انتخابات ممکن است به تعویق بیفتد. سپس ده‌ها عروسک خیمه شب بازی اخبار جعلی تاخیر انتخابات را پخش کردند.

مقابله با عادی سازی روابط اعراب و اسرائیل

مطابق ارزیابی ما Cotton Sandstorm با استفاده از شخصیت سایبری گروه Atlas کارزار دیگری را برای مقابله با عادی‌سازی روابط اعراب و اسرائیل ترتیب داد. در ۱۰ دسامبر، گروه Atlas با تغییر چهره‌ی یک وب‌سایت خبری-ورزشی اسرائیلی، پیامی را منتشر کرد که در آن گفته بود اسرائیلی‌ها نه در جام جهانی قطر و نه در هیچ کشور مسلمان دیگری مورد استقبال قرار نخواهند گرفت. مشابه عملیات بحرین، Cotton Sandstorm اینجا هم از ده‌ها حساب جعلی برای پخش و برجسته‌سازی این خبر و تشدید احساسات ضداسرائیلی استفاده کرد. این عملیات نفوذ همزمان با مرحله‌ی یک‌چهارم نهایی جام جهانی و یک ماه پس از توافق اسرائیل و قطر برای برقراری پروازهای مستقیم برای بازی‌ها جام جهانی انجام شد.

شکل ۶: تصویری که گروه Atlas در حساب‌های رسانه های اجتماعی خود و در پیام های متنی با عنوان Sport5 منتشر کرد.

ایجاد وحشت در اسرائیل

در جمعه‌ی سیاه در اواخر نوامبر، یکی دیگر از شخصیت‌های سایبری که احتمالاً توسط Cotton Sandstorm اداره می‌شود با نام BlackMagic ادعا کرد که در حمله‌ای توانسته چهره‌ی ده‌ها وبسایت اسرائیلی را تغییر داده و اطلاعات باربری و داده‌های شخصی شرکت‌های حمل و نقل را به بیرون درز دهد. این گروه ویدئویی از یک اپراتور سایبری در حال تغییر مقصدها در گزارش‌های توزیع محصول یک شرکت حمل و نقل اسرائیلی را منتشر کرد. فقدانَ شواهد تأییدکننده مبنی بر اینکه این گروه بر فرآیند انتقال محموله‌های واقعی تأثیر گذاشته است، نشان می دهد که این عملیات نمونه دیگری از اقدامات Cotton Sandstorm برای استفاده از عملیات نفوذ برای مبالغه کردن در میزان تأثیرگذاری حملات سایبری خود است. این مورد مشابه ادعاهای نادرست در مورد آراء انتخابات ریاست جمهوری ۲۰۲۰ آمریکاست.

شکل ۷: پست تلگرامی BlackMagic از شرکت‌های خرده‌فروشی و لجستیک اسرائیلی که ادعا می‌کرد در کسب و کار آنها نفوذ کرده است.

این عملیات به دنبال ایجاد اختلال در حمل و نقل خرد، یا حداقل وانمود کردن به ایجاد چنین اختلالی بود که احتمالاً با هدف ایجاد وحشت در بین اسرائیلی ها دنبال شد. ما ارزیابی می‌کنیم که با درنظر گرفتن تشابهات فنی و استفاده از تاکتیک ها، تکنیک ها و رویه‌های مشابه، Cotton Sandstorm پشت شخصیت مجازی BlackMagic بود. یک باج‌افزار مرتبط با BlackMagic و یک ابزار تونل زنی مرتبط با Cotton Sandstorm که در این عملیات مورد استفاده قرار گرفت، روی یک IP میزبانی شد که طبق ارزیابی ما با Cotton Sandstorm مرتبط بود. آن‌ها در توئیتر و فیس‌بوک (در برخی موارد با استفاده مجدد از همان حساب‌های جعلی از کمپین‌های دیگر)، پیام‌هایی را با هدف تضعیف اعتماد به نهادهای اسرائیلی منتشر کردند. همچنین آن‌ها از حساب‌های توییتری استفاده کردند که به‌عنوان کسب‌وکارهای متخلف در اسرائیل شناخته می‌شدند.

شکل ۸: پست‌های ظاهراً اصیل در توییتر که به طور همزمان از حساب‌هایی که خود را به عنوان کسب‌وکارهای هدف قرار گرفته شده‌ی اسرائیلی معرفی می‌کردند ارسال شده است.

یکی دیگر از شخصیت‌های سایبری مرتبط با ایران، عصای موسی، تصاویر مداربسته‌ی یکی از بمب‌گذاری‌های ۲۳ نوامبر در یک ایستگاه اتوبوس اورشلیم را احتمالاً با هدف ایجاد ترس در بین اسرائیلی‌ها منتشر کرد. دسترسی این گروه به فیلم‌های حساس و انتشار آن در همان روز حملات، حاکی از مشارکت در برنامه‌ریزی حمله بَه غیرنظامیان است، اگرچه ممکن است ایرانی‌ها خود مسئول این بمب‌گذاری نبوده باشند. ارزیابی مایکروسافت این است که گروه عصای موسی توسط یک عامل دولتی ایرانی به غیر از عاملی که هدایت Cotton Sandstorm را بر عهده دارد، مدیریت می‌شود. ما این عامل را با عنوان Marigold Sandstorm ردگیری می‌کنیم. برخلاف رفتار معمول Cotton Sandstorm، مشاهده نشدَه که گروه عصای موسی از حساب‌های جعلی برای پخش و برجسته‌سازی اخبار اقدامات خود بهره برده باشد. همچنین هم‌پوشانی بین اهداف حملات گروه عصای موسی و Cotton Sandstorm دیده نشده است.

افشاگری درباره‌ی مخالفین

ایران آموخته است که از عملیات‌های نفوذ سایبری برای افشای اطلاعاتی بهره ببرد که به وسیله‌ی آن و با شرمسار کردن چهره‌های برجسته اپوزیسیون رژیم یا افشای روابط «فاسد» آن‌ها، شتاب اعتراضات سراسری را کاهش دهد. مدت کوتاهی پس از شروع اعتراضات ضددولتی در ایران در اواخر سپتامبر، یک شخصیت سایبری جدید به نام «عدل علی» که طبق برآورد ما از جانب ایران عمل می‌کند، شروع به درز دادن اطلاعاتی به منظور اتهام زدن به چند شخصیت برجسته‌ی اپوزیسیون ایران کرد.

اهداف آنها شامل پسر ارشد شاه سابق ایران و مسیح علینژاد، فعال سرشناس ایرانی-آمریکایی حقوق زنان بود. اولین پست‌های عدل علی از اسنادی استفاده می‌کرد که طبق ادعای آن‌ها پس از انجام یک عملیات سایبری علیه یک گروه جدایی‌طلب کرد - حزب کومه‌له - به دست آورده بودند. عدل علی به دنبال این بود که حزب کومه‌له را مسئول سازماندهی اعتراضات در ایران و شاید حتی حوادثی که منجر به دستگیری مهسا امینی شد جلوه دهد؛ حادثه‌ای که پس از فوت مهسا امینی هنگام بازداشت توسط پلیس امنیت اخلاقی ایران در سپتامبر ۲۰۲۲ موجب برانگیختن اعتراضات سراسری شد. عاملان مرتبط با دولت ایران، به شکل مداوم و در یک بازه‌ی زمانی نزدیک به یک ساله، مجموعه‌ای از حملات سایبری و عملیات‌های نفوذ را علیه دولت آلبانی (که در تیرانا پایگاهی را در اختیار مجاهدین خلق، یک گروه اپوزیسیون ایرانی، قرار داده است) را اجرا کردند. همانطور که مایکروسافت در ماه سپتامبر اعلام کرد، ما ارزیابی می‌کنیم که چندین عامل ایرانی مرتبط با وزارت اطلاعات ایران مسئول حمله‌ی اولیه برای حذف داده‌ها و سپس عملیات‌های رسانه‌ای متعاقب آن علیه تیرانا در تابستان ۲۰۲۲ بودند.

ایران با افشای فساد ادعایی رهبران سیاسی آلبانی و پیوندهای شرورانه بین مجاهدین خلق و تیرانا به دنبال بسط و گسترش روایت نفوذ خود بوده است. در ژانویه، شخصیت سایبری که مسئولیت این حملات را بر عهده گرفت یعنی Justice Homeland اطلاعات شخصی مشتریان بانکی را فاش کرده و ادعا کرد که مقامات آلبانیایی پول دریافتی از مجاهدین خلق را پولشویی کرده‌اند.

هکتیویست ها به اعتراضات ضدرژیم دامن می‌زنند

از ماه اکتبر، چندین گروه هکتیویست ضدرژیم، حملات سایبری و عملیات هک و افشای اطلاعات علیه ایران را برای دامن زدن به اعتراضات سراسری انجام داده‌اند. چندین گروه سایبری ضدرژیم (مثل لب‌دوختگان و عدالت علی) تمرکز خود را از سایر حوزه‌ها به اعتراضات تغییر دادند در حالی که گروه های جدیدی نیز ظاهر شدند (مانند بختک، بلک ریوارد ، هکرهای ZZA) که به طور خاص بر اعتراضات متمرکز بودند. همه گروه‌ها به شکل مستمر از شعارهای اعتراضات سراسری مانند #مهسا_امینی و «زن زندگی آزادی» استفاده می‌کردند.

گروه‌های سایبری که ادعا می‌کنند هکتیویست هستند، مانند بلک ریوارد، لب‌دوختگان، هکرهای ZZA و عدالت علی پایگاه‌های اطلاعاتی ایمیل‌های دولتی ایران را فاش کرده‌اند، وب‌سایت‌های مرتبط با دولت را هک کرده‌اند، پخش برنامه‌های تلویزیون دولتی ایران را هک و قطع کرده‌اند، و به طور کلی تلاش کرده‌اند که دولت ایران را شرمسار کنند. سایر فعالیت‌های سایبری ضدرژیم که پرکارتر بودند اما پیچیدگی کمتری داشتند شامل حملات انکار سرویس توزیع شده (DDoS) و هک و نشت داده‌های دولتی، حول گروه‌هایی با عنوان Anonymous و گروه‌های هکری با پشتوانه نامشخص متمرکز شده‌اند.

شخصیت های سایبری ضدرژیم

بلک ریوارد
افشای ارتباطات داخلی رسانه های مرتبط با دولت

بختک
انتشار اطلاعات لو رفته از مقامات سپاه و فساد رژیم

لب‌دوختگان
افشای اطلاعات در مورد عاملان سایبری ایرانی

Anonymous
هدف گرفتن وب سایت های مرتبط با رژیم

عدالت علی
تشدید فراخوان ها برای اعتراض، انتشار اطلاعات لو رفته مقامات رژیم

هکرهای ZZA
افشای سانسور رژیم، تلاش‌های نظارتی

استفاده از عملیات نفوذ سایبری برای یک ضربه‌ی تلافی‌جویانه‌ی بزرگتر

عملیات‌های نفوذ سایبری ایران در موارد متعدد به دنبال تلافی حملات سایبری یا عملیات‌های نفوذ سایبری‌ست که علیه ایران انجام گرفته است. در ماه سپتامبر، اطلاعات دوربین‌های مداربسته از گذرگاه‌های مرزی و پلیس آلبانی توسط گروه Homeland Justice به بیرون درز کرد، که طبق گزارش‌ها سیستم‌های آن هدف یک حمله‌ی سایبری قرار گرفته بود. ما حمله به سیستم اطلاعاتی تحت کنترل پلیس را به تلافی حمله‌ی پلیس آلبانیایی به سفارت ایران در تیرانا در روز قبل ارزیابی می‌کنیم. فیلم‌های منتشرشده‌ی دوربین مداربسته احتمالاً به دنبال تقلید از یک گروه ضدایرانی به نام «عدالت علی» بود که در سال ۲۰۲۱ فیلم‌هایی را از دوربین‌های مداربسته منتشر کرد که نشان‌دهنده‌ی اختلال در سیستم نظارت ویدئویی در زندان بدنام «اوین» در ایران به همراه پیامی تحقیرآمیز بود. (شکل ۹)

همانطور که تصاویر زیر نشان می‌دهد، عملیات سایبری ایران پیام واضحی در خود حمله ارسال نمی‌کند و نیاز به بررسی دقیق فیدهای دوربین‌های مداربسته برای اطلاع از تحت تاثیر قرار گرفتن عملیات ماموران مرزی دارد.

احتمالاً در برخی موارد، عملیات‌های نفوذ سایبری ایران به دنبال تلافی حملات سایبری بسیار پیچیده‌ای بود که ایران نمی‌توانست با آنها رقابت کند. هدف قرار دادن بخش حمل و نقل اسرائیل توسط Cotton Sandstorm در حملات BlackMagic یادآور حمله‌ای بود که در سال ۲۰۲۱ توسط یک گروه ضدایرانی به نام «گنجشک درنده» در ایران مورد هدف قرار گرفت. هدف عملیات نفوذ BlackMagic نیز همان چیزی بود که برخی از رهبران ارشد ایران آن را هدف حملات سایبری گنجشک درنده به جایگاه‌های سوخت ایران می‌دانستند: ایجاد خشم و بی نظمی. بر خلاف حمله‌ی سایبری در ایران که بر ایستگاه‌های سوخت در سراسر کشور تأثیر گذاشت، BlackMagic اقدامات ساده‌ای نظیر تغییر چهره وب‌سایت دسترسی به شبکه انجام داد و با انتشار یک ویدیوی احتمالاً دست‌کاری شده تلاش کرد میزان اثرگذاری حمله خود را قابل مقایسه با حمله به سیستم پخش سوخت ایران کند. (شکل ۱۰)

در فوریه ۲۰۲۲ Cotton Sandstorm تلاش کرد تا یک حمله‌ی سایبری علیه یک تأسیسات لجستیکی اسرائیل که پایانه‌های بنادر اصلی اسرائیل را اداره می‌کند، صورت دهد. این حمله‌ی سایبری احتمالاً به دنبال تلافی یک حمله‌ی سایبری بود که در ماه می ۲۰۲۰ علیه یک بندر بزرگ ایران انجام شده بود و برخی از مقامات دولت آمریکا و سایر دولت‌های خارجی انجام آن را به اسرائیل نسبت داده شده بودند. می‌توان گفت برخلاف حمله سایبری به بندر ایران که ترافیک دریایی و زمینی را متوقف کرد، حمله سایبری ایران به احتمال زیاد قبل از اجرای کامل شناسایی شد و تاثیر محدودی داشت که از مجبور شدن شرکت اسرائیلی به خاموش کردن تعدادی از سیستم‌های خود فراتر نرفت. به دلیل نبود تأثیر معنادار بر روند کار بنادر، Cotton Sandstorm به یک عملیات نفوذ تحت پوشش گروه Hackers of Savior متوسل شد تا با دسترسی به فیلم‌های دوربین مداربسته‌ی تأسیسات و انتشار آن‌ها، بین اسرائیلی‌ها ترس ایجاد کند.

شکل ۹: عدالت علی فیلم دوربین مداربسته را منتشر کرد که تجهیزات نظارتی هک شده در زندان بدنام اوین ایران را از سال ۲۰۲۱ نشان می‌دهد. متن آن چنین است: «زندان اوین لکه‌ای شرم‌آور بر عمامه سیاه و ریش سفید [رئیس‌جمهور] رئیسی است. اعتراضات گسترده تا آزادی زندانیان سیاسی.»

شکل ۱۰: عدالت وطن ویدئویی را در سپتامبر ۲۰۲۲ از فیلم دوربین مداربسته ایستگاه کنترل مرزی با صف‌های طولانی که در آن ماموران از تلفن‌های خود استفاده می‌کنند در حالی که تصویر رایانه‌ها پایین ظاهر می‌شوند، منتشر کرد.

روندهای آتی در روش‌های نفوذ

عاملان دولتی در ایران تکنیک‌های نفوذ خود را از طریق افزایش استفاده از عملیات نفوذ سایبری تقویت کرده‌اند. آنها دو روش جدید بسط را به جعبه ابزار خود اضافه کرده‌اند.

۱

استفاده از پیام کوتاه برای تماس با مخاطبان هدف

مایکروسافت در سه مورد در نیمه‌ی دوم سال ۲۰۲۲ چندین عامل ایرانی را شناسایی کرد که در حال تلاش برای استفاده از پیامک انبوه جهت تقویت و ایجاد اثرات روانی در عملیات نفوذ سایبری خود بودند. در این مسیر، Cotton Sandstorm حداقل در یک مورد در ماه دسامبر تا حدی موفق بوده است. به گفته اف‌بی‌آی از اوایل سال ۲۰۲۱ Cotton Sandstorm علاقه خود را به استفاده از سرویس‌های پیام کوتاه انبوه برای انتشار گسترده‌ی پیام‌های خود نشان داده بود.

شکل ۱۱: پست تلگرام گروه Atlas اسکرین‌شات‌هایی از پیامک‌هایی را که به اسم یک شبکه ورزشی اسرائیلی ارسال می‌کرد را نشان می‌دهد. لینک سمت چپ به صفحه وب Sport5 هدایت می‌شود. پیام سمت راست هشدار می‌دهد: «اگر زندگی خود را دوست دارید به کشورهای ما سفر نکنید»

در ماه دسامبر، Cotton Sandstorm پیام‌هایی ارسال کرد که ظاهراً از جانب شبکه Sport5 به اسرائیلی‌ها هشدار می‌داد که به کشورهای مسلمان سفر نکنند. یکی از این پیام‌ها شامل لینکی به صفحه‌ی وب تغییر یافته‌ی Sport5 بود. پیام‌های کوتاه احتمالاً برای اغراق‌آمیز کردن تأثیرات حمله سایبری و ایجاد وحشت در بین اسرائیلی‌ها بوده است. Sport5 تایید کرد که پیامک هایی شبیه آن برای هزاران نفر ارسال شده است. بر اساس گزارش‌های جداگانه‌ی مطبوعات اسرائیل، گیرندگان این پیامک‌ها شامل برخی از اسرائیلی‌هایی می‌شود که برای سفر به کشورهای عربی خلیج فارس برنامه‌ریزی کرده بودند.

الطوفان و Homeland Justice نیز ممکن است تلاش کرده باشند پیامک‌هایی ارسال کنند تا به ترتیب: خبر دروغ تعویق انتخابات پارلمانی بحرین در ماه نوامبر را نشان دهند و اطلاع‌رسانی حملات سایبری ایران در آلبانی را تقویت کنند. محدود بودن مخاطبانی که در هر دو مورد ادعای دریافت پیامک‌ها را داشتند، نشان می‌دهد که این کمپین‌ها یا از نظر دامنه محدود بوده یا توسط عروسک‌های خیمه شب بازی ساخته شده بودند.

۲

جعل هویت قربانیان برای افزایش اعتبار

اواخر سال گذشته، Cotton Sandstorm جعل هویت سازمان‌های قربانی یا شخصیت‌های برجسته در آن سازمان‌ها را آغاز کرد تا به تأثیرات حمله‌ی سایبری اعتبار بخشد. در ماه نوامبر، عملیات BlackMagic شامل جعل هویت چند خرده‌فروش اسرائیلی بود که این شخصیت سایبری ادعا می‌کرد آنها را هک کرده است. عملیات الطوفان جعل هویت یکی از مقامات سازمان انتخابات بحرین بود. به همین ترتیب در ژانویه عملیاتی که تحت عنوان شخصیت Holy Souls اجرا شد، از حساب‌های توئیتری جعلی به نام سردبیر مجله طنز فرانسوی شارلی ابدو استفاده کرد. همانطور که اغلب در مورد عروسک های خیمه شب بازی ایجاد شده توسط Cotton Sandstorm اتفاق افتاده بود، حساب‌های جعلی در هفته‌های منتهی به حمله‌ی سایبری یا نشت داده‌ها ایجاد شده بودند.

روندهای آتی در تهدیدات سایبری

عاملان دولتی در ایران در حالی که از نظر پیچیدگی اقدامات از همتایان روسی و چینی خود عقب هستند، ابزارها و تکنیک‌های جدیدی را به زرادخانه خود اضافه کرده‌اند. این پیشرفت مداوم در پیچیدگی، توانایی آن‌ها را برای دستیابی به اهداف خاص مورد نظر و حفظ تداوم در عین اجتناب از شناسایی عملیات افزایش می‌دهد؛ چالشی که آن‌ها احتمالاً در برخی از عملیات‌های نفوذ سایبری خود در سال ۲۰۲۲ با آن مواجه بودند.

۱

پذیرش سریع آسیب‌پذیری‌های روز N ام

عاملان دولتی ایران با فاصله‌ی زمانی کمتری از آسیب‌پذیری‌هایی که به تازگی گزارش شده‌اند استفاده می‌کنند. در ۱۹ ژانویه که کد اثبات مفهوم (POC) به طور عمومی منتشر شد، گروهی که ما تحت عنوان Mint Sandstorm ردگیری می‌کنیم، شروع به سوءاستفاده از یک آسیب‌پذیری اجرای کد از راه دور در Zoho ManageEngine– که مجموعه‌ای از محصولات مورد استفاده برای مدیریت IT سازمانی است – کردند. در فوریه، Mint Sandstorm از یک آسیب پذیری تازه فاش شده، تنها پنج روز پس از گزارش عمومی آن استفاده کرد. این یک آسیب‌پذیری از نوع اجرای کد از راه دور پیش از احراز هویت در یک برنامه انتقال فایل IBM بود. مایکروسافت مشاهده کرده است که عاملان دولتی در ایران همچنان به آسیب‌پذیری‌های قدیمی‌تر، از جمله Log4Shell، برای به خطر انداختن دستگاه‌های آسیب‌پذیر اعتماد می‌کنند. از آنجایی که این فعالیت معمولاً فرصت‌طلبانه و بدون تبعیض است، مایکروسافت توصیه می‌کند که سازمان‌ها به‌طور منظم آسیب‌پذیری‌ها را با کدهای در دسترس عموم، بدون توجه به مدت زمانی که کد اثبات مفهوم در دسترس بوده، اصلاح کنند.

۲

استفاده از وب‌سایت‌های قربانی برای زیرساخت فرماندهی و کنترل

از اواخر سال ۲۰۲۲، یک عامل ایرانی با نام Storm-0133 که طبق ارزیابی ما با وزارت اطلاعات ایران مرتبط است، از بدافزار سفارشی شده برای برقراری ارتباط بین یک وب‌سایت اسرائیلی که مورد هدف قرار گرفته بود با چندین شبکه قربانی دیگر در داخل اسرائیل استفاده کرد. این گروه مرتبط با وزارت اطلاعات، از وب‌سایت اصلی و در عین حال هک شده‌ی اسرائیلی برای فرماندهی و کنترل استفاده کرد که نشان‌دهنده بهبود امنیت عملیاتی است، زیرا این تکنیک تلاش‌های مدافعان را که اغلب از داده‌های موقعیت جغرافیایی برای شناسایی فعالیت‌های غیرعادی شبکه استفاده می‌کنند، پیچیده می‌کند. عملیات Storm-0133 منحصراً سازمان‌های اسرائیلی را هدف قرار داد و بر سازمان‌های دولتی محلی و شرکت‌هایی که در بخش‌های دفاعی، اسکان و مراقبت‌های بهداشتی خدمت می‌کردند، تأثیر گذاشت.

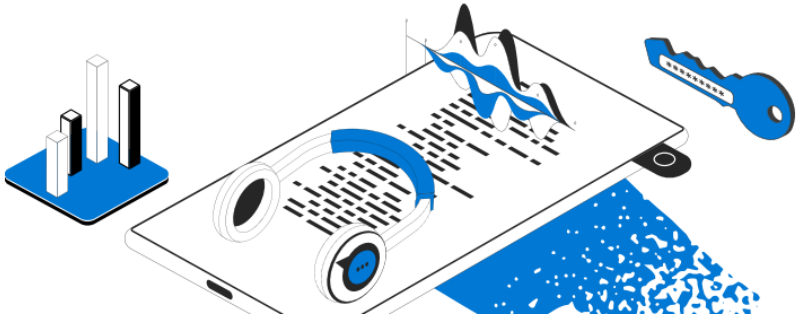
۳

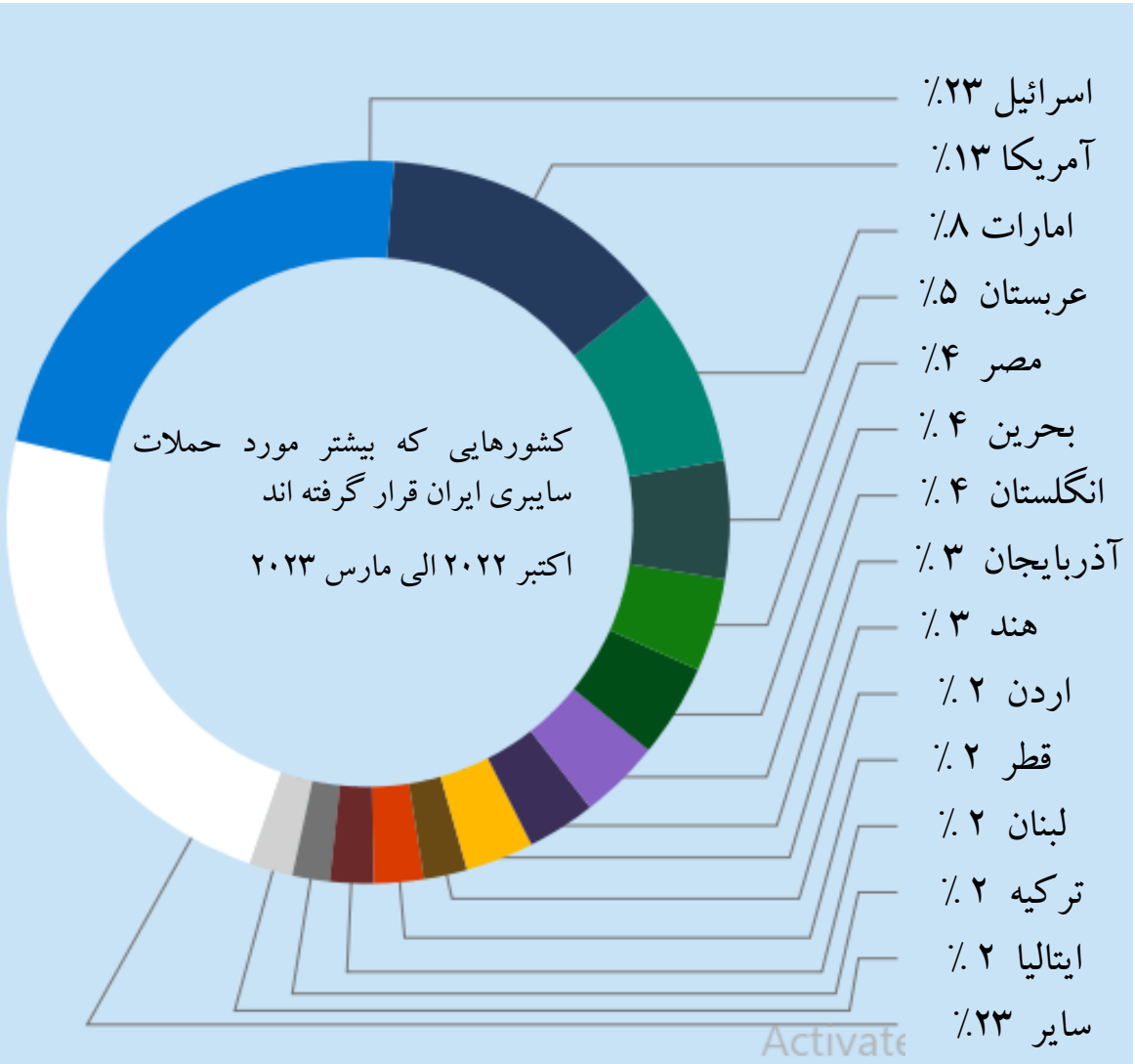
استفاده مستمر از ابزارهای سفارشی شده

گروه‌های مرتبط با سپاه پاسداران و وزارت اطلاعات در اوایل سال ۲۰۲۳ از ابزارهای سفارشی علیه اهداف مورد نظر خود استفاده کردند. حرکت از ابزارهای در دسترس عموم و اسکریپت‌های ساده به سمت توسعه و استفاده از کدهای سفارشی شده نشان می‌دهد که حداقل بخشی از افراد عامل حملات می‌توانند اقدامات پیچیده‌تر را انجام دهند. بدافزاری که Storm-0133 علیه سازمان‌های اسرائیلی استفاده کرد، یک بدافزار سفارشی بود که ما از آن به عنوان بدافزار Mango یاد می‌کنیم. بهره‌برداری Mint Sandstorm از آسیب‌پذیری CVE-2022-47986 همچنین شامل یک اسکریپت سفارشی PowerShell بود که با مبهم‌سازی داخلی برای مخدوش کردن اطلاعات قربانیان طراحی شده بود. Mint Sandstorm دو ابزار سفارشی دیگری را که مایکروسافت از سال ۲۰۲۲ شناسایی کرده است توسعه داده: Drokbk و Soldier (یک نوع پیچیده تر از Drokbk) این دو ایمپلنت‌های Backdoor هستند که اپراتورها از آنها برای ماندگاری در محیط‌های هدف و استقرار ابزارهای اضافی استفاده می‌کنند. این ابزارها از GitHub برای میزبانی یک چرخش دامنه استفاده می‌کنند، اقدامی که به اپراتورها اجازه می‌دهد تا به صورت پویا زیرساخت فرماندهی و کنترل خود را به‌روز کنند و به طور بالقوه از block list های ثابت پیاده‌سازی شده توسط مدافعان فرار کنند.

نگاهی به آینده

حملات سایبری و عملیات‌های نفوذ ایران احتمالاً بر تلافی‌جویی در برابر حملات سایبری خارجی و تحریک اعتراضات در داخل ایران متمرکز خواهد بود. اسرائیل و پس از آن آمریکا، احتمالاً در معرض بالاترین خطر برای چنین عملیات‌هایی در آینده هستند، به‌ویژه در کوتاه‌مدت و با توجه به نزدیک شدن ایران به عربستان سعودی و تغییرات دیپلماتیک در سایر کشورهای عربی خلیج فارس در ماه مارس. بر اساس داده‌های مایکروسافت اهداف مشترک عملیات سایبری ایران در سال گذشته، با افزایش هدف‌گیری اسرائیل در شش ماه گذشته همراه بوده است (نگاه کنید به شکل ۱۲). در ماه اکتبر، خامنه‌ای رهبر ایران و سازمان‌های اطلاعاتی ایران، اسرائیل و آمریکا را به تحریک اعتراضات در ایران متهم کردند و همچنین دیگر شخصیت‌های کلیدی رژیم، اسرائیل و ایالات متحده را مسئول حملات سایبری بزرگ علیه ایران دانستند.





شکل ۱۲: این نمودار نشان دهنده عملیات سایبری توسط عاملان تحت حمایت دولت ایران است. برگرفته از تله‌متری مایکروسافت از مشتریان خدمات آنلاین مایکروسافت

ایران در عملیات‌های خود علیه دولت آلبانی نشان داد که هدف دیگر این حملات اسرائیل بوده و یا در آینده خواهد بود. لوگوی گروه Homeland Justice، که آنها هم در یادداشت باج‌افزار و هم به طور منظم در پست‌های عمومی خود استفاده می‌کردند، یک عقاب بود که در حال شکار نشان گروه گنجشک درنده بود که درون ستاره داوود قرار داشت. (شکل ۱۳) گنجشک درنده حملات سایبری بسیار پیچیده‌ای را علیه ایران انجام داد که از جمله موجب تاخیر قطارها در ژوئیه ۲۰۲۱ و اختلال در پمپ‌های سوخت‌رسانی در سراسر کشور در اکتبر ۲۰۲۱ شده و در ژوئن ۲۰۲۲ از طریق دستکاری کنترل‌ها در تأسیسات یک کارخانه فولاد در ایران باعث آتش‌سوزی درآن شد.

شکل ۱۳: بنر Homeland Justice و تصویر باج‌افزار آن، یک عقاب است که نماد گنجشک درنده را در داخل ستاره داوود شکار می‌کند.

همچنین کشورهای عضو ناتو و اتحادیه اروپا ممکن است بیش از پیش در معرض عملیات‌های سایبری و نفوذ از جانب ایران باشند. خوی تهاجمی فزاینده‌ی عاملان ایرانی از سال ۲۰۲۱، از جمله اولین حمله سایبری ایران به طورِ مستقیم علیه یک دولت عضو ناتو (آلبانی) در ژوئیه ۲۰۲۲، نشان دهنده‌ی گسترش محدوده‌ی عملیاتی آن‌ها است و تهدیدی بزرگتر را در آینده برای اهداف کمتر متداول ایران همانند سایر اعضای ناتو نشان می دهد.

هدف قرار دادن مداوم آلبانی توسط ایران برای حملات سایبری و عملیات نفوذ، از جمله در زمان نگارش این مقاله، نشان می‌دهد که عاملان ایرانی از تعقیب متحدان ناتو منصرف نشده‌اند.

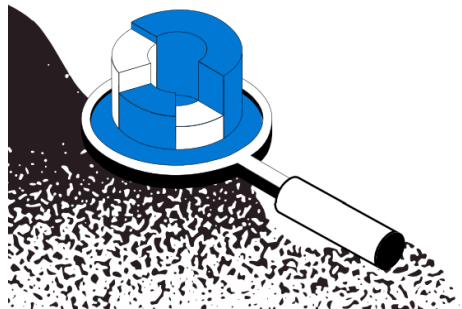
در واقع، همانطور که قبلاً نوشتیم، ایران در ژانویه یک عملیات نفوذ سایبری را به عنوان نوعی انتقام از یک مجله فرانسوی به دلیل برگزاری مسابقه کاریکاتورهایی که رهبر ایران را «مسخره» کرده و او را به عنوان نماد قدرت مذهبی عقب‌مانده و تنگ نظرو نابردبار نشان داده بود، انجام داد. این عملیات همچنین از دولت فرانسه انتقاد کرد و نشان داد که آنها بودجه‌ی مجله را تأمین می کنند.

در ماه نوامبر، Mint Sandstorm ایمیل‌های فیشینگ نیزه‌ای را به وزرای مرتبط با امنیت در کشورهای عمدتاً عضو ناتو در گروه مشاوره‌ی دفاعی اوکراین – که ظاهراً در مورد یک جلسه مجازی آتی بود – ارسال کرد. ایران احتمالاً در پی تحریم‌های اتحادیه اروپا علیه شرکت‌های ایرانی درگیر در تأمین پهپادها به روسیه و همچنین گزارش‌های مبنی بر تحویل سامانه‌های دفاع هوایی جدید به اوکراین برای مقابله با حملات موشکی و پهپادی، به دنبال اطلاعات بود.

سازمان‌های اطلاعاتی ایران سرویس‌های اطلاعاتی چندین کشور اروپایی را به همکاری با سیا در پروژه‌ی تحریک اعتراضات در ایران متهم کردند.

تلاش ایران برای انجام حملات سایبری با تاثیر بیشتر علیه فناوری عملیاتی

ایران احتمالاً به استفاده از توان جدید خود برای عملیات‌های نفوذ سایبری ادامه خواهد داد تا با فشار تهدیدات خارجی هم‌سطح شود. این کار تا حدی برای غلبه بر کمبودهایی که در قبال حملات خارجی از خود نشان داده دنبال می‌شود. در عین حال، عاملان سایبری ایران احتمالاً به دنبال قابلیت‌های بیشتر برای حملات سایبری هستند تا به هدف خود که دستیابی به توان انجام اقدام متقابل مطلوب رژیم است برسند. در واقع اشتباهات و کاستی‌های گاه به گاه نشان می‌دهد که ایران هنوز در حال تلاش برای ارتقای ظرفیت‌های خود است.



در اوایل آوریل ۲۰۲۳، یک گروه مرتبط با ایران به احتمال زیاد پشت یک حمله سایبری بود که کنترل‌کننده های آب در حداقل ده مزرعه‌ی اسرائیلی را از کار انداخت و تصویر کنترل‌کننده‌های PLC را با پیام «مرگ بر اسرائیل» جایگزین کرد. این تصویر مشابه تصویر مورد استفاده در حمله سایبری احتمالی ایران علیه «اسرائیل پست» در ژانویه ۲۰۲۲ بود، چند روز پس از آن که پخش یک شبکه دولتی ایران با پیام «مرگ بر خامنه‌ای» مختل شد.

قبل از حمله اخیر به سیستم آب‌رسانی اسرائیل، «اطلاعات تهدیدات مایکروسافت» یک عامل ایرانی را شناسایی کرد که در اواسط سال ۲۰۲۲ یک شرکت آب اسرائیلی را شناسایی و رابط‌های وب سیستم‌های کنترل صنعتی مستقر در اسرائیل را در دسامبر ۲۰۲۲ بررسی می‌کرد. نمی‌دانیم که آیا این کار توسط عاملی که در حمله اخیر نقش داشته است انجام شده بود یا خیر.

در ماه ژوئن، گروه عصای موسی خبر یک حمله سایبری را پخش کرد که در آن آژیرهای اضطراری حملات موشکی اسرائیل را با استفاده از نرم‌افزار تنظیم صدا روی پروتکل اینترنت (AoIP) به کار انداخت. نشانه‌ای برای مرتبط دانستن این حمله با گروه عصای موسی وجود ندارد.

اسناد طبقه‌بندی شده‌ای که توسط یک خبرگزاری انگلیسی در ژوئیه ۲۰۲۱ فاش شد نشان می‌دهد که در سال ۲۰۲۰ واحدی در سپاه پاسداران در حال انجام تحقیقاتی بر روی آسیب‌پذیری در سیستم‌های کنترل صنعتی و روش‌های تنظیم از راه دور کنترل پمپ‌های سوخت در پمپ بنزین‌ها و آبِ بالاست در کشتی‌های باری بوده است که می‌تواند باعث اختلال در عملیات کشتی شود.

شکل ۱۴: تصویر صفحه کنترل‌کننده‌ی سیستم آب‌رسانی از کار افتاده در مزارع اسرائیل، آوریل ۲۰۲۳

1. “Hackers Target Israeli TV/Radio Infrastructure,” 6 May 2021, al-sarira.com/2021/05/06/hackers-target-israeli-tv-radio-infrastructure/; “Listen: Hackers broke into 100 FM broadcasts” (machine translation from Hebrew), 6 May 2021, ice.co.il/media/news/article/819193; web.archive.org/web/20210616224505/https://www.hackersofsavior.com/eventitem.html
2. “Iran says retaliation will be proportionate and "against legitimate targets,"” 7 January 2020, cbsnews.com/news/iran-news-zarif-cbs-news-retaliation-qassem-soleimani-killingproportionate-legitimate-targets-today-2020-01-07/; “Iran warns of 'immediate counter-response' if US attacks its bases after strikes on Syria,” 25 March 2023, news.sky.com/ story/amp/iran-warns-of-immediate-counter-response-if-us-attacks-its-bases-after-strikes-on-syria-12842303; “Second US base hit in Syria following retaliatory strikes,” 24 March 2023, thehill.com/policy/defense/3916342-second-us-base-hit-in-syria-following-retaliatory-strikes/; “U.S. Responds to Attack That Killed U.S. Contractor in Syria ,” 24 March 2023, defense.gov/News/News-Stories/Article/Article/3341127/us-responds-to-attack-that-killed-us-contractor-in-syria/
3. This definition draws on elements of definitions of influence operations used by RAND, Recorded Future, and scholars at NATO’s Cooperative Cyber Defense Center of Excellence. “Foundations of Effective Influence Operations A Framework for Enhancing Army Capabilities,” 2009, rand.org/pubs/monographs/MG654.html; “Influence Cyber Operations: The Use of Cyberattacks in Support of Influence Operations,” ccdcoe.org/uploads/2018/10/Art-08-Influence-Cyber-Operations-The-Use-of-Cyberattacks-in-Support-of-InfluenceOperations.pdf
4. web.archive.org/web/20210509224051/https://hackersofsavior.com/Event_item.html; web.archive.org/web/20210616224505/https://www.hackersofsavior.com/event-item.html; moses-staff[.]se; eotp-us[.]ca
5. “Microsoft Digital Defense Report,” October 2022, microsoft.com/en-us/security/business/microsoft-digital-defense-report-2022. “Evolving trends in Iranian threat actor activity – MSTIC presentation at CyberWarCon 2021,” 16 November 2021, microsoft.com/en-us/security/blog/2021/11/16/evolving-trends-in-iranian-threat-actor-activity-msticpresentation-at-cyberwarcon-2021/
6. “Hackers Target Israeli TV/Radio Infrastructure,” 6 May 2021, al-sarira.com/2021/05/06/hackers-target-israeli-tv-radio-infrastructure/; “Listen: Hackers broke into 100 FM broadcasts” (machine translation from Hebrew), 6 May 2021, ice.co.il/media/news/article/819193; web.archive.org/web/20210616224505/https://www.hackersofsavior.com/eventitem.html
7. t[.]me/s/Saifal_Quds
8. “Israel’s cyber directorate issues annual warning ahead of Iran’s ‘Jerusalem Day,’” 24 April 2022, timesofisrael.com/israel-cyber-directorate-issues-annual-warning-ahead-of-iransjerusalem-day/
9. “MERCURY and DEV-1084: Destructive attack on hybrid environment,” 7 April 2023, microsoft.com/en-us/security/blog/2023/04/07/mercury-and-dev-1084-destructive-attackon-hybrid-environment/
10. “MERCURY and DEV-1084: Destructive attack on hybrid environment,” 7 April 2023, microsoft.com/en-us/security/blog/2023/04/07/mercury-and-dev-1084-destructive-attackon-hybrid-environment/
11. web.archive.org/web/20230212181234/https://www.facebook.com/profile.php?id=100090227412050; archive.is/9Ad5K; web.archive.org/web/20230213005442/https://www. youtube.com/@darkbitYT/about; web.archive.org/web/20230212213845/https://www.reddit.com/user/darkbitRDT/; web.archive.org/web/20230212181721/https://t.me/DarkBitChannel/7; iw6v2p3cruy7tqfup3y14dgt4pfibfa3ai4zgnu5df2q4hus3lm7c7ad[.]onion;
12. "Microsoft shifts to a new threat actor naming taxonomy," 18 April 2023, microsoft.com/en-us/security/blog/2023/04/18/microsoft-shifts-to-a-new-threat-actor-namingtaxonomy/; "How Microsoft names threat actors," 18 April 2023, learn.microsoft.com/en-us/microsoft-365/security/intelligence/microsoft-threat-actor-naming?view=o365- worldwide
13. “Treasury Sanctions Iran Cyber Actors for Attempting to Influence the 2020 U.S. Presidential Election,” 18 November 2021, home.treasury.gov/news/press-releases/jy0494; “Iranian Cyber Actors Responsible for Website Threatening U.S. Election Officials,” 23 December 2020, fbi.gov/news/press-releases/iranian-cyber-actors-responsible-for-websitethreatening-us-election-officials
14. “Iranian Cyber Group Emennet Pasargad Conducting Hack-and-Leak Operations Using False Flag Personas,” FBI Private Industry Notification, 20 October 2022, ic3.gov/Media/ News/2022/221020.pdf; “Context and Recommendations to Protect Against Malicious Activity by Iranian Cyber Group Emennet Pasargad,” FBI Private Industry Notification, 26 January 2022, ic3.gov/Media/News/2022/220126.pdf
15. “DRAFT WHITE PAPER: An Attribution model for influence operations,” 31 January 2023, blogs.microsoft.com/wp-content/uploads/prod/sites/5/2023/02/DTAC-AttributionFramework.pdf
16. web.archive.org/web/20230213170158/https://www.akhbar-alkhaleej.com/
17. “Bahrain dissolves main Shia opposition Al-Wefaq party,” 17 July 2016, aljazeera.com/news/2016/7/17/bahrain-dissolves-main-shia-opposition-al-wefaq-party; “Bahrain: Elections, But No Civic Space,” 10 November 2022, amnesty.org/en/documents/mde11/6124/2022/en/
18. “Israel reaches agreement with Qatar to allow direct flights during World Cup,” 10 November 2022, timesofisrael.com/israel-reaches-agreement-with-qatar-to-allow-directflights-during-world-cup/; “World Cup 2022: First ever Israel-Qatar flight lands in Doha,” 20 November 2022, middleeasteye.net/news/qatar-world-cup-first-ever-israel-flightdoha#
19. “Two Iranian Nationals Charged for Cyber-Enabled Disinformation and Threat Campaign Designed to Influence the 2020 U.S. Presidential Election,” 18 November 2021, justice. gov/opa/pr/two-iranian-nationals-charged-cyber-enabled-disinformation-and-threat-campaign-designed
20. “Israel purchase Bahraini island,” english.almayadeen.net/videos/israel-purchase-bahraini-island, “Bahrainis confident of toppling treasonous regime that sells islands to Israel,” kayhan[.]ir/en/news/112404/bahrainis-confident-of-toppling-treasonous-regime-that-sells%C2%A0-islands-to-israel, “Israel ‘buys island’ in Bahrain; activists call it ‘dangerous and worrying,’” 13 February 2023, parstoday[.]ir/en/news/west_asia-i195944; israel_'buys_island'_in_bahrain_activists_call_it_'dangerous_and_worrying', virustotal.com/gui/file/8f855ed4c2f17487bac5d5079437acd728ccd68d93b49ab2f5b6d6d2430da133/details
21. “Moses Staff Hackers Publish Footage of Jerusalem Explosion,” 25 November 2023, hackread.com/moses-staff-hackers-jerusalem-footage/; kan.org.il/Item/?itemId=138720
22. “Iranian Dissident Masih Alinejad Won't Be Silenced,” 2 March 2023, time.com/6259111/masih-alinejad/
23. t[.]me/adll_ali
24. “Microsoft investigates Iranian attacks against the Albanian government,” 8 Septermber, 2022, microsoft.com/en-us/security/blog/2022/09/08/microsoft-investigates-iranianattacks-against-the-albanian-government/
25. “Albanian PM says Iranian hackers hit country with another cyberattack,” 11 September 2022, therecord.media/albanian-pm-says-iranian-hackers-hit-country-with-anothercyberattack; twitter.com/ediramaal/status/1568920720658268165
26. “Albanian police force open Iranian Embassy after expulsions,” 8 September 2022, apnews.com/article/middle-east-iran-albania-tirana-5cd399beaa7381fd2c01ac6831fed208
27. “Iran Says Gas Stations Were Target Of Cyberattack To Foment Unrest,” 28 October 2021, iranintl.com/en/20211028778677
28. “‘Effect of cyber attack on Gold Bond will last for weeks,’ warns expert,” 1 February 2022, calcalistech.com/ctech/articles/0,7340,L-3928403,00.html
29. “Officials: Israel linked to a disruptive cyberattack on Iranian port facility,” 18 May 2020, washingtonpost.com/national-security/officials-israel-linked-to-a-disruptive-cyberattackon-iranian-port-facility/2020/05/18/9d1da866-9942-11ea-89fd-28fb313d1886_story.html
30. “‘Effect of cyber attack on Gold Bond will last for weeks,’ warns expert,” 1 February 2022, calcalistech.com/ctech/articles/0,7340,L-3928403,00.html
31. "Videos: When The Security of the Terrorists of Durres(MEK) is More Important than The Security of Your Own People,” 26 September 2022, justicehomeland[.]ru/videos-whenthe-security-of-the-terrorists-of-durresmek-is-more-important-than-the-security-of-your-own-people/
32. “Context and Recommendations to Protect Against Malicious Activity by Iranian Cyber Group Emennet Pasargad,” FBI Private Industry Notification, 26 January 2022, ic3.gov/ Media/News/2022/220126.pdf
33. "Messaging impersonating the sports channel are sent” (machine translation from Hebrew), 10 December 2022, sport5.co.il/articles.aspx?FolderID=10796&docID=422369
34. “The Arab world celebrates Morocco’s success in the World Cup – and in the meantime, the resident of Ashdod received threats in text messages.” 10 December 2022, ashdodi. com/hackers-are-threatening-an-ashdod-resident-not-to-fly-to-the-emirates/
35. reddit.com/r/albania/comments/w2y6wx/a_ju_erdhi_edhe_ju_a_jam_i_vetmi/
36. twitter.com/gerardbiard_; twitter.com/thierrykarsent
37. nvd.nist.gov/vuln/detail/CVE-2022-47966
38. cve.mitre.org/cgi-bin/cvename.cgi?name=2022-47986
39. “China-Brokered Deal Between Iran, Saudi Arabia Marks a New Middle East,” 11 March 2023, wsj.com/articles/china-brokered-deal-between-iran-saudi-arabia-marks-a-newmiddle-east-d1eaf94e; “Saudi Arabia, Iran Restore Relations in Deal Brokered by China,” 10 March 2023, wsj.com/articles/saudi-arabia-iran-restore-relations-in-deal-brokeredby-china-406393a1, “Senior Iranian Official Visits UAE on Heels of Saudi Deal,” 16 March 2023, voanews.com/a/senior-iranian-official-visits-uae-on-heels-of-saudi-deal-/7008237. html; “Iranian MP’s meet with Bahraini parliament speaker in Manama, 1st in years,” 14 March, 2023, ifpnews[.]com/iranian-mps-bahraini-parliament-speaker-manama-1st-years/
40. “Iran Says Israel, U.S. Likely Behind Cyberattack on Gas Stations,” 31 October 2021; bloomberg.com/news/articles/2021-10-31/iran-says-israel-u-s-likely-behind-cyberattack-ongas-stations; “Iran’s supreme leader breaks silence on protests, blames US,” 3 October 2022, apnews.com/article/iran-israel-middle-east-dubai-united-arab-emirates-25c14800 b5b145d850fe3181eb062664; “Tehran lashes out at Israelis’ support for Iranian protest movement,” 2 November 2022, mei.edu/publications/tehran-lashes-out-israelis-supportiranian-protest-movement; “Joint statement by intelligence ministry, IRGC: CIA project to destroy Iran defeated,” 28 October 2022, en.irna[.]ir/news/84926113/Joint-statement-byintelligence-ministry-IRGC-CIA-project-to
41. “Cyberattack forces Iran steel company to halt production,” 27 June 2022, apnews.com/article/technology-middle-east-iran-dubai-b0404963ae23e5008439a0b607952de1; “The Iran Steel Industry Cyber Attack Explained,” 7 July 2022, blog.scadafence.com/the-iran-steel-industry-cyber-attack-explained; “‘Cyber-attack’ hits Iran’s transport ministry and railways,” 11 July 2022, theguardian.com/world/2021/jul/11/cyber-attack-hits-irans-transport-ministry-and-railways
42. “#MULLAHSGETOUT : CHARLIE HEBDO’S INTERNATIONAL COMPETITION,” charliehebdo.fr/mullahsgetout-international-competition/
43. “EU agrees on new sanctions over Iranian drones in Ukraine,” 20 October 2022, aljazeera.com/news/2022/10/20/eu-agrees-new-sanctions-over-iranian-drones-in-ukraine; “Ukraine-bound NASAMS are in US hands now: Raytheon,” 25 October 2022, defensenews.com/pentagon/2022/10/25/ukraine-bound-nasams-are-in-us-hands-now-raytheon/
44. “Joint statement by intelligence ministry, IRGC: CIA project to destroy Iran defeated,” 28 October 2022, en.irna[.]ir/news/84926113/Joint-statement-by-intelligence-ministry-IRGCCIA-project-to
45. “Iranian hackers take responsibility for cyber attacks on Israeli sirens,” 22 June 2022, www.israelnationalnews.com/flashes/580076; “Cyberattack suspected behind false siren alerts in Jerusalem, Eilat,” 20 June 2022, timesofisrael.com/cyberattack-suspected-behind-false-siren-alerts-in-jerusalem-eilat/
46. “Iran’s Secret Cyber Files,” July 2021, news.sky.com/story/irans-secret-cyber-files-on-how-cargo-ships-and-petrol-stations-could-be-attacked-12364871