جبهه مقاومت در حمایت از غزه متوقف نخواهد شد

سیدحسن نصرالله، دبیرکل حزب‌الله لبنان در واکنش به حملات تروریستی رژیم اسرائیل و تحولات منطقه روز پنجشنبه سخنرانی کرد. او شهات تعدادی از نیروهای مقاومت در جبهه نبرد با دشمن را تسلیت گفت و از بیمارستان‌ها و پزشکان و همچنین کشورهایی که کمک‌های خود را به لبنان ارسال کردند، تشکر کرد. نصرالله گفت: «دشمن صهیونیستی هزاران دستگاه پیام‌رسان را هدف قرار داد و تمام قوانین و خطوط قرمز را زیر پا گذاشت. دشمن با یک ابزار غیرنظامی نه‌تنها نیروهای حزب‌الله بلکه مردم عادی را نیز هدف قرار داد.» سیدحسن نصرالله گفت: «این جنایت در تاریخ درگیری با دشمن بی‌سابقه بود. حتی می‌توان گفت این جنایت در جهان نیز بی‌سابقه است.» دبیرکل حزب‌الله لبنان گفت: «این واقعیت که دشمن با اتکا به غرب از توانمندی تکنولوژی برخوردار است غیرقابل انکار است؛ اما با تمام اطمینان می‌گویم این ضربه قوی ما را از مسیر خود متوقف نمی‌کند بلکه ما قدرتمندتر در مقابل آنها خواهیم ایستاد.» سیدحسن نصرالله در ادامه به سالگرد عملیات «طوفان الاقصی» اشاره کرد و افزود: «یک روز پس از آغاز عملیات «طوفان الاقصی» جبهه مقاومت در لبنان فعالیت خود را آغاز کرد و تا امروز هم حمایت از مردم فلسطین ادامه داشته است.»

دبیرکل حزب‌الله در ادامه سخنرانی خود اظهار داشت: «وقتی دشمن می‌گوید آنچه در شمال می‌گذرد، اولین شکست تاریخی «اسرائیل» است، دلیل دیگری بر کارآمدی جبهه ماست. تمام نظامیانی که دشمن به شمال منتقل کرده است تایید می‌کند که او در این جبهه با تهدید واقعی روبه‌رو است.» سیدحسن نصرالله گفت: «جبهه لبنان، یکی از مهمترین عوامل فشار بر دشمن است و یکی از مهمترین ابزارهای مذاکره است که در اختیار گروه‌های مقاومت فلسطین قرار دارد.» نصرالله تأکید کرد: «به‌رغم تمام فداکاری‌ها و جانفشانی‌ها و به‌رغم تمام تبعات و پیامدها، مقاومت از یاری رساندن به غزه و کرانه باختری منصرف نخواهد شد. به‌نتانیاهو و گالانت و همه اشغالگران قویاً می‌گویم جبهه مقاومت در حمایت از غزه متوقف نخواهد شد.» او در ادامه سخنرانی خود اشاره کرد: «انفجارهای اخیر هیچ تاثیری بر ساختار مقاومت نداشت. دشمن بر این باور است که از نظر تکنولوژی برتر است، اما کاری که او با انفجارها انجام داد نشان داد که او بسیار کودن است.» نصرالله همچنین گفت: «اقدامات رژیم اشغالگر روند آواره کردن صهیونیست‌ها را افزایش داده و فرصت بازگرداندن آنان را محال می‌کند. پیشنهاد فرمانده احمق منطقه‌شمالی در ایجاد کمربند امنیتی، امیدواریم عملی شود و آن را فرصتی تاریخی می‌دانیم و تاثیرات زیادی بر نبرد خواهد داشت. اگر دشمن کمربند امنیتی ایجاد کند باید بداند که همین کمربند امنیتی به دامی تبدیل خواهد شد که خودش در آن گرفتار می‌شود.»

دو فرمانده ارشد حزب‌الله کشته شدند

در جریان حملات هوایی اسرائیل در ۳۰ شهریور به ضاحیه در جنوب بیروت، ابراهیم عقیل، یکی از رهبران ارشد نظامی گروه حزب‌الله و چندین نفر از فرماندهان گردان رضوان کشته شدند. حزب‌الله هم با انتشار بیانیه‌ای ترور ابراهیم عقیل را تایید کرد. علاوه بر او رسانه‌های نزدیک به حزب‌الله تصویر ۱۲ عضو از «یگان رضوان» را که آنها را فرمانده خطاب کرده بود منتشر کردند. احمد وهبی، دومین فرمانده ارشد حزب‌الله است که در حمله هوایی اسرائیل کشته شده است.

ابراهیم عقیل ملقب به «حاج تحسین» از فرماندهان نظامی بود که پس از شهادت «فواد شکر» به‌عنوان مرد شماره دو حزب‌الله و همچنین فرمانده نیروی رضوان، نیروی نخبه و رئیس دایره عملیات نظامی ویژه حزب‌الله شناخته می‌شود. پیشتر آمریکا برای پیدا کردن عقیل جایزه ۷ میلیون دلاری تعیین کرده بود. عقیل همچنین عضو مجلس جهادی حزب‌الله بود که پیشینه‌ای طولانی در فعالیت‌های مبارزاتی و سازمانی داشت. از عقیل به‌عنوان یکی از بنیانگذاران حزب‌الله و از جمله شخصیت‌هایی یاد می‌شود که از زمان تاسیس حزب‌الله در اوایل دهه ۱۹۸۰ در تمام عملیات‌های این گروه مشارکت داشته است. از او به‌عنوان مغز متفکر بسیاری از عملیات‌های نظامی بزرگ حزب‌الله علیه اسرائیل از جمله نبردهای آزادسازی جنوب لبنان در سال ۲۰۰۰ یاد می‌شود. او همچنین در جنگ ۳۳ روزه نیز نقش‌های بسیار مهمی ایفا کرد. عقیل همچنین بر توسعه سیستم موشکی و تجهیزات نظامی حزب‌الله نظارت داشت.

نگاه پژوهشگر

تکنولوژی د

نگاه تکنیکال به حمله سایبری روی پیجرهای نظامی: ا

عکس: Reuters

علی امیری
دانشیار گروه کامپیوتر دانشگاه زنجان

در دنیای امروز که فناوری اطلاعات و ارتباطات به‌بخش جدایی‌ناپذیر تمام سازمان‌ها، صنایع و کسب و کارها تبدیل شده است، امنیت سایبری (به‌عنوان مجموعه‌ای از تکنیک‌ها و فرآیندها و اقدامات برای حفاظت از سیستم‌های کامپیوتری، شبکه‌ها، انواع سخت‌افزارهای برنامه‌پذیر، داده‌ها و اطلاعات در سیستم‌های فناوری اطلاعات و سیستم‌های کنترل صنعتی در مقابل حملات سایبری مختلف، دسترسی غیرمجاز، خرابی‌ها و سرقت‌ها) یکی از حیاتی‌ترین مباحثی است که نیازمند توجه جدی دولت‌ها است. از اینرو، دولت‌های مختلف در سراسر جهان برای مقابله با تهدیدات سایبری و حفاظت از زیرساخت‌های حساس خود، چارچوب‌های قانونی و مقررات سختگیرانه‌ای را برای الزامات امنیت سایبری وضع کرده‌اند. این قوانین معمولاً شامل استانداردها، سیاست‌ها، ومقرراتی هستند که سازمان‌ها و شرکت‌ها باید برای حفاظت از داده‌ها و سیستم‌های خود رعایت کنند. به‌عنوان مثال، ایالت متحده آمریکا در سال ۲۰۱۱ قانونی وضع نموده است که طی آن به هیچ پروژه‌ای بدون تکمیل مطالعات امنیت سایبری و رعایت الزامات، سیاست‌ها و رویه‌های کنترلی امنیت سایبر-فیزیکی اجازه اجاره داده نمی‌شود.

در ایران تجربه‌های عملی در اجرای پروژه‌های مرتبط با امنیت سایبری نشان می‌دهد متاسفانه بسیاری از مدیران در صنایع حساس مانند انرژی و زیرساخت‌های حیاتی هنوز درکی کامل از اهمیت و ضرورت امنیت سایبری نداشته و اغلب آن را به‌عنوان یک مقوله جانبی و تشریفاتی تلقی کرده و توجه به این حوزه را یک هزینه اضافی و غیرضروری نگاه می‌کنند. اما واقعیت این است که بی‌توجهی به امنیت سایبری به معنای قرار دادن سازمان‌ها در معرض تهدیدات مداوم و پرهزینه است. این تهدیدات می‌توانند به شکل‌های مختلف بروز کنند و هزینه‌های بسیار بالایی را در سطح مخاطرات امنیت ملی به کشورها تحمیل نمایند.

حمله سایبری اخیر رژیم صهیونیستی بر روی پیجرها و دستگاه‌های بی‌سیم حزب‌الله در لبنان نشان داد که فراتر از تجهیزات مبتنی بر IP، حتی تجهیزاتی که از طریق فرکانس‌های رادیویی خاص و امن استفاده می‌کنند نیز می‌تواند هدف حمله قرار گیرد و هزینه‌های جبران‌ناپذیری را به دولت‌ها تحمیل نماید.

از این رو این یادداشت ضمن تشریح فنی پیجرها و ساختار شبکه ارتباطی و سناریوهای حمله و اقدامات لازم برای مقابله با این حملات، به ضرورت نگاه جدی به مقوله امنیت سایبری در کشور و به‌ویژه در زیرساخت‌های حیاتی تاکید کرده و هزینه‌کرد در این مقوله را سرمایه‌گذاری برای کشور تلقی می‌کند و از تصمیم‌گیران و دولت‌مردان می‌خواهد با نگاه ویژه‌تری این مقوله را در کشور دنبال کنند.

پیجرها: نحوه عملکرد و ساختار ارتباطی

پیجرها دستگاه‌های ارتباطی قابل حمل و کم‌حجمی هستند که به کاربران امکان ارسال و دریافت پیام‌های متنی یا هشدارهای فوری را می‌دهند. این دستگاه‌ها به‌طور گسترده در کاربردهای حساس، به‌ویژه در شرایط بحرانی یا محیط‌های با دسترسی محدود به شبکه‌های ارتباطی بزرگ‌تر، استفاده می‌شوند.

پیجرها به‌دلیل نیاز به امنیت، مقاوم بودن در برابر اختلالات، اغلب از پروتکل‌های ارتباطی مبتنی بر امواج رادیویی مانند POCSAG و FLEX استفاده می‌کنند. معمولاً امنیت در این پروتکل‌ها محدود بوده و ضروری است در کاربردهای حساس از رمزنگاری‌های سفارشی و مدیریت کلید استفاده شود. از نظر ساختار ارتباطی، این پیجرها معمولاً در قالب یک شبکه خصوصی رادیویی، پیام‌ها را به‌صورت متمرکز یا توزیع‌شده از طریق شبکه‌های رادیویی خاص ارسال می‌کنند. پیام‌های ارسالی به‌دلیل حساسیت بالا بایستی با روش‌های رمزنگاری سفارشی (مانند AES یا DES) رمزنگاری و ارسال شوند. این رمزنگاری‌ها معمولاً هم در سطح پیام‌های ارسالی و هم در سطح فرکانس رادیویی اعمال می‌شوند. علاوه بر این، در این سیستم‌ها معمولاً از مکانیزم‌های احراز هویت پیشرفته برای اطمینان از اینکه پیام فقط به پیجرهای مجاز ارسال می‌شود، استفاده می‌کنند که شامل کلیدهای مشترک یا سیستم‌های احراز هویت چندلایه می‌باشند.

از نظر مدل ارتباطی، معمولاً ارتباطات در پیجرها یک‌طرفه است. به این معنی که پیجرها تنها می‌توانند پیام را دریافت کنند و قادر به ارسال پیام نیستند. البته در برخی سیستم‌های پیشرفته‌تر ممکن است به پیجرها اجازه ارسال تایید دریافت پیام یا پیام‌های مختصر بازگشتی داده شده باشد. به‌طور کلی مدل ارتباطی شامل مراحل زیر است:

الف) ارسال پیام رمزنگاری‌شده از مرکز کنترل یا فرستنده مرکزی

ب) انتشار پیام از طریق ایستگاه‌های رادیویی با استفاده از باند فرکانسی خاص

ج) دریافت پیام توسط پیجرها، رمزگشایی پیام و نمایش آن به کاربر

د) در برخی سیستم‌ها ارسال تاییدیه دریافت پیام

البته در برخی سازمان‌های مدرن، از سیستم‌های ارتباطی مبتنی بر IP و شبکه‌های ماهواره‌ای استفاده می‌شود که نیازمند وجود زیرساخت‌های ارتباطی پیشرفته‌تر و سطح امنیت بالای سایبری است.

انواع حملات سایبری روی پیجرها

حملات سایبری به پیجرها، به‌ویژه در کاربردهای حساس، می‌تواند به چندین شکل و در سناریوهای مختلف رخ دهد. در زیر به تفصیل برخی از مهم‌ترین سناریوهای حمله سایبری به پیجرها توضیح داده شده است:

پیجرها به‌دلیل نیاز به امنیت، مقاوم بودن در برابر اختلالات، اغلب از پروتکل‌های ارتباطی مبتنی بر امواج رادیویی مانند POCSAG و FLEX استفاده می‌کنند. معمولاً امنیت در این پروتکل‌ها محدود بوده و ضروری است در کاربردهای حساس از رمزنگاری‌های سفارشی و مدیریت کلید استفاده شود. از نظر ساختار ارتباطی، این پیجرها معمولاً در قالب یک شبکه خصوصی رادیویی، پیام‌ها را به‌صورت متمرکز یا توزیع‌شده از طریق شبکه‌های رادیویی خاص ارسال کنند

حملات استراق سمع[1]

در این نوع حمله، مهاجم با استفاده از تجهیزات رادیویی می‌تواند به‌سادگی پیام‌های ارسالی به پیجرها را شنود کند. این حملات زمانی محتمل است که پیام‌ها به صورت رمزنگاری نشده یا با رمزنگاری ضعیف ارسال شوند. پروتکل‌های قدیمی‌تر مانند POCSAG و FLEX در برابر این نوع حمله آسیب‌پذیرتر هستند، به‌ویژه اگر از رمزنگاری استفاده نشده باشد. معمولاً از روش‌هایی مانند الف) استفاده از رمزنگاری قوی برای پیام‌های ارسالی. ب) بهره گیری از فرکانس‌های جهش‌یاب[2] (دشوار نمودن شنود ارتباطات) برای جلوگیری از این حمله استفاده می‌شود.

حملات دستکاری پیام[3]

در حملات دستکاری پیام، مهاجم می‌تواند پیام‌ها را در مسیر انتقال تغییر دهد یا پیام‌های جعلی ارسال کند. در سیستم‌های پیجر رادیویی، به‌ویژه اگر مکانیسم‌های احراز هویت قوی برای فرستنده وجود نداشته باشد، مهاجم می‌تواند پیام‌های کاذب یا اشتباه را به پیجرها ارسال کند و باعث ایجاد سردرگمی یا اختلال در عملکرد عملیاتی شود. برای جلوگیری از این حمله از رویکردهای الف) احراز هویت قوی برای تأیید منبع پیام، و ب) استفاده از امضای دیجیتال یا تکنیک‌های رمزنگاری برای اطمینان از صحت پیام استفاده می‌شود.

حملات منع سرویس[4]

در این سناریو، مهاجم با ایجاد تداخل رادیویی[5] یا ارسال پیام‌های مکرر و حجیم، می‌تواند سیستم‌های پیجر را از کار بیاندازد یا به اصطلاح بلاک کند. این حمله می‌تواند باعث شود پیجرها پیام‌های اصلی را دریافت نکنند یا به شدت کُند شوند. استفاده از تجهیزات جمر رادیویی برای ایجاد اختلال در فرکانس‌های مورد استفاده پیجرها و جلوگیری از دریافت پیام‌های حساس، و یا ارسال تعداد زیادی پیام بی‌فایده به سیستم‌های پیجر برای اشباع کانال‌های ارتباطی نمونه‌هایی از سناریوهای این نوع حمله هستند. راهکارهایی مانند الف) استفاده از تکنولوژی جهش فرکانس و تکنیک‌های طیف گسترده[6] برای کاهش احتمال تداخل رادیویی، ب) پیاده‌سازی مکانیزم‌های کنترل جریان داده‌ها برای جلوگیری از اشباع شدن کانال‌های ارتباطی می‌توانند برای جلوگیری از این حملات مورد استفاده قرار گیرند.

حملات بازیابی پیام‌های قدیمی[7]

در حملات بازپخش، مهاجم پیام‌هایی که قبلاً ارسال شده را دریافت و دوباره ارسال می‌کند. این نوع حمله می‌تواند باعث شود که پیجرها دوباره به پیام‌هایی که در گذشته ارسال شده‌اند واکنش نشان دهند. استفاده از زمان‌بندی معتبر برای پیام‌ها (مانند timestamps) که پیام‌های قدیمی را رد می‌کند، پیاده‌سازی نرم‌افزارهای ضدبازپخش که پیام‌های تکراری را تشخیص و مسدود می‌کنند، می‌توانند برای جلوگیری از این حملات مورد استفاده قرار گیرند.

حملات جابه‌جایی فرکانس[8]

مهاجم ممکن است فرکانس‌هایی که برای ارسال پیام به پیجرها استفاده می‌شود را پیدا کرده و آن‌ها را تغییر دهد یا از آن‌ها برای ارسال پیام‌های خود استفاده کند. این حمله می‌تواند باعث قطع ارتباطات یا ارسال پیام‌های جعلی به پیجرها شود. با استفاده از تکنیک‌های فرکانس پویا یا جهش فرکانس برای تغییر مداوم فرکانس ارتباطات، یا استفاده از رمزنگاری فرکانسی تا مهاجم نتواند به سادگی فرکانس‌های مورد استفاده را پیدا کند، می‌توان از این حمله سایبری جلوگیری کرد.

حملات مبتنی بر تداخل فرکانس[9]

این نوع حمله معمولاً از تجهیزات Jammer برای ایجاد تداخل در فرکانس‌های رادیویی مورد استفاده پیجرها قرار می‌گیرد. این تداخل می‌تواند باعث قطع کامل ارتباطات یا کاهش کیفیت ارتباطات شود. استفاده از سیستم‌های رادیویی مقاوم در برابر تداخل مانند طیف گسترده یا سیستم‌های فرکانس جهشی که احتمال موفقیت جمرها را کاهش می‌دهد، یا استفاده از آنتن‌های جهت‌دار که حساسیت به تداخل رادیویی را کاهش می‌دهند، راهکارهای مؤثری برای مقابله و جلوگیری از این حملات به شمار می‌رود.

حملات هویت‌دزدی[10]

در این سناریو، مهاجم با جعل هویت فرستنده پیام‌ها می‌تواند به پیجرها پیام‌های جعلی ارسال کند. این حمله می‌تواند باعث شود پیجرها پیام‌هایی از منابع جعلی دریافت کنند و اطلاعات نادرست را به کاربران ارائه دهند. با استفاده از راهکارهایی مانند پیاده‌سازی احراز هویت دوطرفه بین فرستنده و گیرنده برای اطمینان از صحت هویت فرستنده، یا استفاده از امضاهای دیجیتال در پیام‌ها که به پیجرها اجازه می‌دهد تا از صحت پیام اطمینان حاصل کنند، می‌توان از این حملات جلوگیری نمود.

حملات مهندسی اجتماعی[11]

مهاجم می‌تواند از طریق مهندسی اجتماعی و با فریب کاربران پیجر، اطلاعات حساس را به‌دست آورد یا آن‌ها را به انجام عملیاتی خاص ترغیب کند. در این سناریو، نقطه‌ضعف سیستم امنیتی نه در تکنولوژی، بلکه در تعاملات انسانی و فریب‌کاری قرار دارد. به‌عنوان سناریویی از این حمله، مهاجم با ارسال پیام جعلی به کاربر پیجر (مثلاً پیام اضطراری از سوی فرماندهی) او را به اقدام اشتباه یا افشای اطلاعات حساس ترغیب می‌کند. راهکارهایی مانند آموزش افزایش آگاهی امنیتی در کاربران پیجر و آشنا کردن آن‌ها با حملات مهندسی اجتماعی، و پیاده‌سازی مکانیزم‌های تأیید هویت و منبع پیام‌ها به‌صورت دقیق و قابل اعتماد می‌توانند برای مقابله با این نوع حملات مورد استفاده قرار گیرند.

سناریوهای حمله سایبری روی باتری‌های لیتیومی

واقعیت این است که حمله سایبری به یک پیجر یا هر دستگاه الکترونیکی که از باتری‌های لیتیومی استفاده می‌کند، به‌طور مستقیم برای «انفجار باتری» چالش‌برانگیز و پیچیده است. از نظر فنی، انفجار باتری از طریق حمله سایبری به دلایل زیر بسیار دشوار است:

- سیستم‌های حفاظتی سخت‌افزاری: باتری‌های لیتیومی معمولاً دارای مدارهای حفاظتی هستند که از شارژ بیش از حد یا تخلیه کامل جلوگیری می‌کنند. حتی اگر مهاجم به سیستم نرم‌افزاری نفوذ کند، مدارهای سخت‌افزاری معمولاً از رخ دادن شرایط خطرناک جلوگیری می‌کنند.
- نیاز به نفوذ به سطح پایین سخت‌افزار: برای اجرای حملاتی که بتواند باتری را منفجر کند، مهاجم باید به سطح پایین‌تری از سخت‌افزار (مانند سیستم‌های مدیریت انرژی یا BMS) دسترسی داشته باشد. این کار نیازمند دسترسی فیزیکی یا دسترسی به نرم‌افزارهای سیستمی است که معمولاً بسیار محافظت شده‌اند.

با این حال، در تئوری امکان وقوع این اتفاق در شرایط خاص وجود دارد، اما نیازمند مجموعه‌ای از شرایط و آسیب‌پذیری‌های سخت‌افزاری و نرم‌افزاری است. در ادامه توضیح داده می‌شود که چگونه یک حمله سایبری ممکن است منجر به تخریب یا حتی انفجار باتری لیتیومی در پیجر شود.

باتری‌های لیتیوم به دلیل ویژگی‌هایی مانند تراکم انرژی بالا و