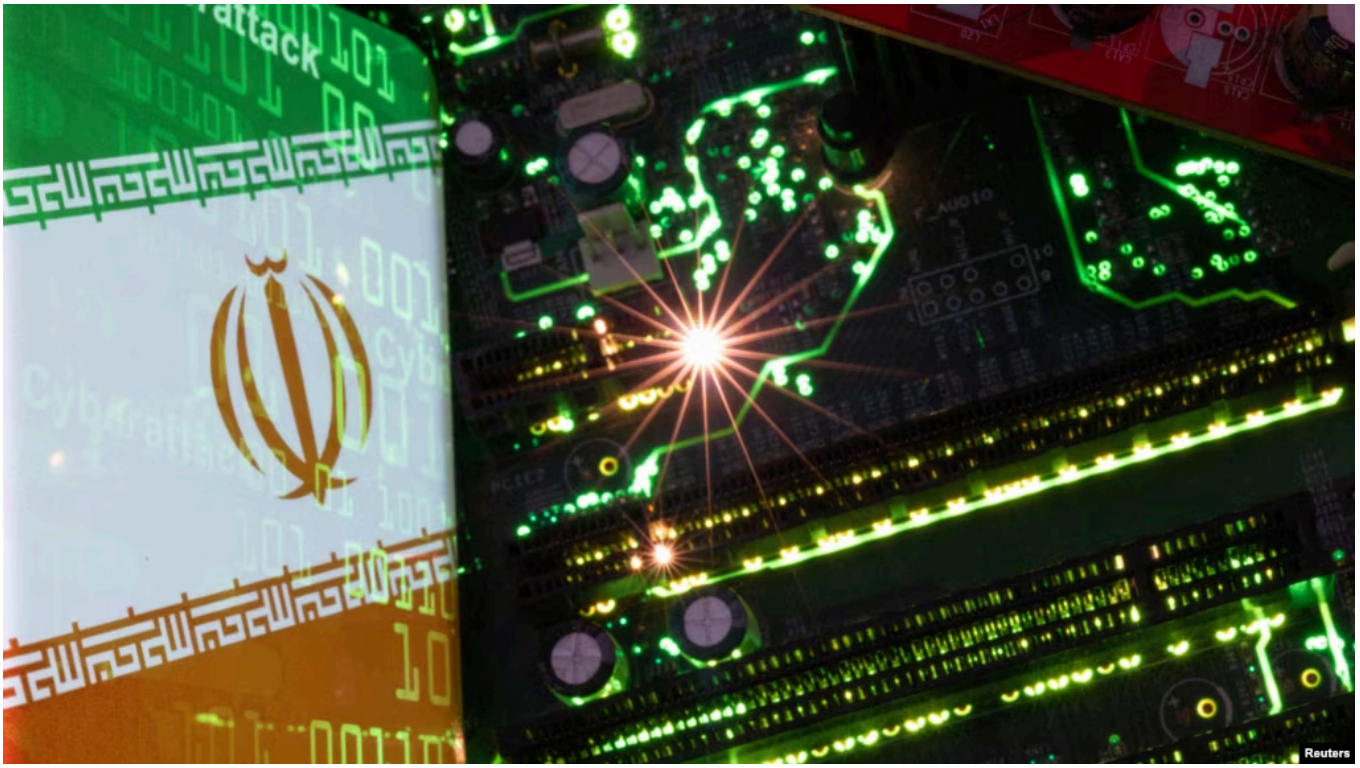
پاراگراف اول

پاراگراف اول؛ ایران از کُد تا بحران در قلب جنگ سایبری

محمد ضرغامی

۳ ساعت پیش



از نفوذ به سامانه‌های حساس و شبکه‌های نظارتی گرفته تا اختلال در خدمات بانکی و زیرساخت‌های حیاتی، فضای سایبری به یکی از مهم‌ترین میدان‌های رقابت و تقابل تبدیل شده است

کدها، بدافزارها و شبکه‌های رایانه‌ای در حال بازتعریف جنگ‌ها هستند؛ همپای موشک‌ها، تانک‌ها و جنگنده‌ها، درست جایی که نبردها در سکوت جریان دارد.

این جنگ پنهانِ زیرپوستی را می‌توان در تنش‌های اخیر میان ایران، اسرائیل و آمریکا دید.

از نفوذ به سامانه‌های حساس و شبکه‌های نظارتی گرفته تا اختلال در خدمات بانکی و زیرساخت‌های حیاتی، فضای سایبری به یکی از مهم‌ترین میدان‌های رقابت و تقابل تبدیل شده است. حمله‌هایی که گاه بدون شلیک حتی یک گلوله می‌توانند زندگی روزمره میلیون‌ها نفر را تحت تأثیر قرار دهند و اعتماد عمومی به خدمات حیاتی را بشکنند.

در برنامهٔ رادیویی «پاراگراف اول» با ممدو بابایی کارشناس امنیت سایبری و سامانه‌های بلادرنگ در هلند همراه با اشکان خسروپور خبرنگار حوزه فناوری اطلاعات و دسترسی به اینترنت در فرانسه به قلب یکی از

مهم‌ترین عرصه‌های نبرد عصر جدید سفر کرده‌ایم؛ جایی که جنگ در پشت خطوط کد و در اعماق شبکه‌ها جریان دارد.

پاراگراف اول؛ ایران از کُد ...
از رادیو فردا
SHARE EMBED
0:00 55:01

بازکردن در پنجره جدید

لینک مستقیم

به‌دنبال «شفافیت سایبری»

ممدو بابایی، «نبود شفافیت» را مهم‌ترین مشکل امنیت سایبری جمهوری اسلامی و آسیب‌پذیری زیرساخت‌های سایبری ایران می‌داند و معتقد است از آن‌جا که مشخص نیست تصمیم‌های کلان بر چه اساسی گرفته می‌شوند، قطع اینترنت هم بدون ارزیابی پیامدهای بلندمدتش به اجرا گذاشته شده است.

به باور آقای بابایی، قطع اینترنت ممکن است در دوره‌های بحرانی برخی مخاطرات را برای کوتاه‌مدت کاهش دهد، اما در بلندمدت مشکلات تازه‌ای ایجاد می‌کند.

او می‌گوید: زمانی که ارتباط با اینترنت برای مدت طولانی قطع می‌شود، سامانه‌های نرم‌افزاری امکان دریافت به‌روزرسانی‌های امنیتی را از دست می‌دهند و اگر در همان دوره آسیب‌پذیری تازه‌ای در یک سامانه عامل یا نرم‌افزار کشف شود، مدیران شبکه دیگر قادر به دریافت وصله‌های امنیتی نخواهند بود و همین مسئله یک حفره امنیتی جدید ایجاد می‌کند که می‌تواند بعداً مورد سوءاستفاده مهاجمان قرار گیرد.

به گفته آقای بابایی، کسانی که قصد نفوذ به زیرساخت‌های حیاتی یک کشور را دارند، لزوماً به اینترنت عمومی وابسته نیستند و مسیرهای متعدد دیگری برای دسترسی به این سامانه‌ها وجود دارد.

اما اشکان خسروپور، اولین مشکل امنیت سایبری در ایران را کمبود نیروهای متخصصی می‌داند که بتوانند در زمان وقوع بحران تصمیم‌های درست بگیرند.

به گفته آقای خسروپور، ایران در دهه‌های گذشته هزینه‌های زیادی برای خرید تجهیزات سخت‌افزاری پیشرفته انجام داده، اما پا به پای این موضوع، تربیت نیروی انسانی متخصص که بتواند از این تجهیزات بهره‌برداری مؤثر داشته باشد، کمتر مورد توجه قرار گرفته است.

اشکان خسروپور، ساختارهای استخدامی و گزینش در دستگاه‌های دولتی را هم دلیلی می‌داند که بر اساس آن بسیاری از نیروهای توانمند سایبری جذب این مجموعه‌ها نشوند.

این خبرنگار که در حوزه امنیت سایبری پژوهش می‌کند، از انجام حمله‌های سایبری فروردین ۱۳۹۷ یاد می‌کند که در آن‌ها، «اختلال‌های سراسری در سرویس اینترنت و سرویس‌های مراکز داده داخلی» رخ داد.

به گفته اشکان خسروپور، بررسی‌های بعدی نشان داد یکی از شرکت‌های معتبر بین‌المللی فعال در حوزه امنیت سایبری پیش از وقوع حمله، درباره وجود این آسیب‌پذیری هشدار داده و حتی راهکار برطرف کردن آن را نیز اعلام کرده بود، اما این موضوع در دستگاه‌های دولتی ایران جدی گرفته نشد.

«برتری در تهاجم سایبری، ضعف در دفاع»

ممدو بابایی ضمن مخالفت با گزاره «کمبود نیروی متخصص سایبری» در ایران، معتقد است برای اثبات این ادعا کافی است به فهرست «تحت تعقیب‌ترین مجرمان سایبری» در پایگاه اطلاع‌رسانی اف‌بی‌آی نگاهی کنیم.

به گفته این کارشناس امنیت سایبری، تعداد قابل توجهی از این متهمان ایرانی هستند؛ موضوعی که نشان می‌دهد دانش و توان فنی در ایران وجود دارد.

آقای بابایی مسئله اصلی را در نحوه استفاده از این ظرفیت می‌بیند و معتقد است جمهوری اسلامی از این توانمندی در «حوزه عملیات تهاجمی» بهره برده و در حوزه «دفاع سایبری و حفاظت از زیرساخت‌ها» از این ظرفیت استفاده مؤثری نکرده است.

ممدو بابایی با اشاره به الگوی حمله سایبری شهریورماه ۱۴۰۳ به تعدادی از بانک‌های ایرانی، می‌گوید که در آن حمله‌ها از روش «حمله زنجیره تأمین» استفاده شده بود؛ روشی که در آن مهاجم به جای حمله مستقیم به همه اهداف، ابتدا یکی از حلقه‌های اصلی زنجیره را هدف قرار می‌دهد.

به گفته آقای بابایی، در آن حمله هم رایانه‌های شرکت خصوصی «توسن» که خدمات نرم‌افزاری بانکی ارائه می‌دهد، هدف حمله قرار گرفت و مهاجمان از همین مسیر توانستند به داده‌های بانکی ایران دسترسی پیدا کنند و اطلاعات کاربران را سرقت کنند.

تخریب فیزیکی، ایجاد اختلال یا ضربه به اعتماد عمومی

از نگاه اشکان خسروپور، بخش قابل توجهی از حملات سایبری سال‌های گذشته در ایران بیش از آن‌که بر «تخریب فیزیکی و یا ایجاد اختلال» تمرکز داشته باشد، حمله‌هایی بوده که با هدف «افشای اطلاعات» صورت گرفته است.

آقای خسروپور در این‌باره به انتشار اسناد قضایی اشاره می‌کند که به گفته این خبرنگار اطلاعات تازه‌ای درباره شیوه‌های سرکوب جمهوری اسلامی، ساختارهای امنیتی و روش‌های اعمال محدودیت بر اینترنت در اختیار افکار عمومی قرار داده، اما از دیگر سو معتقد است که همه این اطلاعات الزاماً از طریق نفوذ غیرمجاز به سیستم‌های رایانه‌ای و شبکه‌ها به دست نیامده‌اند.

او در توضیح منظور خود با رجوع به تجربه شخصی‌اش می‌گوید سال‌ها پیش در برخورد با یکی از شرکت‌های خدمات‌دهنده تلفن‌های همراه در ایران دریافته بود که آن‌ها به حجم گسترده‌ای از اطلاعات کاربران، از جمله محل سکونت، الگوی تردد و دیگر داده‌های شخصی دسترسی دارند.

او این تجربه را نشانه‌ای می‌داند که بخش بزرگی از اطلاعات شهروندان، حتی پیش از حمله‌های سایبری، در اختیار نهادها و شرکت‌های مختلفی است که خود می‌تواند تهدیدی جدی برای حریم خصوصی باشد.

ممدو بابایی با تأکید بر نیاز به داشتن «اطلاعات فنی و مستندات لازم» برای قضاوت درباره یک حمله سایبری می‌گوید برای نتیجه‌گیری باید شواهد جرم‌شناسی دیجیتال، لاگ‌های سامانه‌ها، ترافیک شبکه و سایر داده‌های فنی در اختیار کارشناسان قرار گیرد.

او با این حال درباره حمله‌های سایبری خرداد ۱۴۰۵ معتقد است، بر «پایه شواهد موجود و نه نتیجه یک بررسی فنی کامل»، هدف اصلی مهاجمان «بیش از تخریب فنی، از بین بردن اعتماد عمومی به شبکه بانکی ایران» بوده باشد.

اشکان خسروپور هم مطرح شدن موضوعاتی از سوی برخی تصمیم‌گیران حکومتی در حوزه امنیت سایبری که چاره را در ایجاد محدودیت‌هایی برای فضای مجازی می‌بینند، فاقد تحلیل فنی دانسته و می‌گوید: بسیاری از حمله‌های مهم سال‌های اخیر در ایران علیه سامانه‌هایی انجام شده‌اند که اساساً به اینترنت عمومی متصل نبوده‌اند.

به گفته آقای خسروپور، این محدودیت‌ها سبب شده که کاربران به ابزارهایی برای دور زدن فیلترینگ فضای مجازی روی بیاورند.

نرم‌افزارهایی که می‌توانند دستگاه کاربران را به عضوی از یک «بات‌نت» تبدیل کنند؛ شبکه‌ای از دستگاه‌های آلوده که مهاجمان سایبری از آن برای اجرای حمله‌هایی نظیر «محروم‌سازی از خدمات توزیع‌شده یا دیداس (DDoS)» استفاده می‌کنند.

ممدو بابایی با اشاره به حملهٔ سایبری «استاکس‌نت» در شهریورماه ۱۳۸۹ آن را یکی از بهترین نمونه‌های تاریخ امنیت سایبری دانسته و معتقد است در آن زمان این بدافزار از نظر میزان پیچیدگی، بدون نیاز به اتصال مستقیم اینترنت توانست به هدف خود برسد.

به گفته آقای بابایی، این بدافزار سرعت چرخش سانتریفوژهای تأسیسات هسته‌ای ایران را افزایش می‌داد، اما هم‌زمان اطلاعات جعلی برای سامانه‌های کنترل ارسال می‌کرد تا کاربران تصور کنند همه چیز در وضعیت عادی قرار دارد.

او در ادامه به بررسی‌های انجام‌شده توسط شرکت امنیت سایبری «کسپرسکی» در مسکو و شرکت «نورتون لایف لاک» (سیمانتک) در کالیفرنیا اشاره کرده و می‌گوید که آن‌ها در یک مورد اتفاق نظر داشتند و آن این‌که اجرای عملیاتی با چنین سطحی از پیچیدگی، تنها از توان یک یا چند دولت برمی‌آید.

اشکان خسروپور هم تأکید می‌کند که بسیاری از حمله‌های سایبری جدید «فوری و لحظه‌ای» نیستند، بلکه به گفته او حاصل نفوذهای طولانی‌مدت و مرحله‌به‌مرحله‌اند که بدافزارها در آن‌ها مدت‌ها پیش از فعال‌سازی نهایی به‌صورت پنهان در شبکه باقی می‌مانند.

او استفاده گسترده از نرم‌افزارهای قفل‌شکسته، غیراصل و به‌روزنشده را یکی از عوامل اصلی ایجاد این آسیب‌پذیری می‌داند و می‌گوید: این حمله‌ها می‌توانند حتی از ساده‌ترین راه‌ها مانند «حافظه همراه» (Flash memory) آغاز شده و به‌تدریج کل شبکه را درگیر کنند.

این مطلب بخشی از:

ایران | امنیت سایبری | فراتر از خبر | پاراگراف اول

© ۲۰۲۶ تمام حقوق این وب‌سایت، بر اساس مقررات کپی‌رایت، برای رادیو فردا محفوظ است.