شنبه 12 شهريور 1390 - 13:26

جنگ سايبري ،جانشين جنگ سرد مي‌شود

بتازگي يكي از متخصصان ضدتروريسم ايالات متحده هشدار داد جنگ سرد در حال تغيير چهره و تبديل به جنگ كدهاست به گونه‌اي كه ممكن است ...

جام جم آنلاين: بتازگي يكي از متخصصان ضدتروريسم ايالات متحده هشدار داد جنگ سرد در حال تغيير چهره و تبديل به جنگ كدهاست به گونه‌اي كه ممكن است تا چند وقت ديگر، سلاح‌هاي سايبري با توفاني از پيامدهاي مخرب شروع به حركت ويرانگر خود كند.
طبق گفته‌هاي كوفر بلك ـ كه قبل از تبديل شدن به يك مشاور خصوصي به مدت 28 سال در سازمان‌هاي امنيتي خدمت كرده ـ كشورهاي مختلف حملات آنلاين جديدي را طراحي و اجرا كرده‌اند و برخي گروه‌هاي افراطي، حملات سايبري را به تاكتيك‌هايشان افزوده‌اند.

ما پيش از اين جنگ سرد و مبارزه جهاني با تروريسم را تجربه كرده‌ايم و اكنون با جنگ سايبري (كدها و اطلاعات) روبه‌رو هستيم. در اين ميان مي‌توان به گروه‌هاي تروريستي اشاره كرد كه در آينده نزديك به دنياي سايبري قدم خواهند گذاشت.

شايد استفاده از متخصصان امنيت كامپيوتر براي تقويت دفاع عليه حملات سايبري و غلبه بر چالش تشخيص مجرمان، يك راهكار مناسب باشد.

تشخيص هويت شخص يا گروهي كه پشت حملات سايبري قرار دارد بسيار ضروري به نظر مي‌رسد چنان كه دولت‌ها در حال سنجش امكانات دفاع در برابر تاخت و تازهاي دنياي مجازي هستند بنابراين انجام يكسري عمليات هك پيچيده كه اخيرا توسط شركت ارائه‌كننده محصولات امنيتي مك آفي ارائه شده چندان عجيب نيست.

به گفته شركت مك آفي، اتحاديه اروپا و كميته ملي المپيك اهدافي هستند كه در معرض حملات شديد سايبري قرار دارند و به نظر مي‌رسد چين يكي از مظنونان چنين حملاتي است.

شركت مك آفي در گزارشي به شناسايي 72 قرباني در 14 كشور اشاره مي‌كند كه در عملياتي تحت عنوان shady RAT مورد حمله قرار گرفته‌اند كه سوابق آن به سال 2006 باز مي‌گردد.

ديميتري الپروويچ، نايب‌رئيس مك آفي در برنامه‌اي كه دولت‌هاي كانادا، كره جنوبي، آمريكا، هند، تايوان، ويتنام، انجمن ملل جنوب شرق آسيا، كميته ملي المپيك، آژانس ضددوپينگ جهاني و 12 پيمانكار بخش دفاعي آمريكا در آن حضور داشتند، به شرح اين عمليات پرداخت.

الپروويچ معتقد است هدف از حملات ناگهاني به پيمانكاران بخش دفاعي ايالات متحده، تكنولوژي‌ها و طرح‌هاي حساس نظامي است.

الپروويچ معتقد است بر اساس هدف، اندازه و نقش چنين عملياتي نمي‌توان گفت تنها يك منظور اقتصادي پشت چنين عملياتي نهفته است بلكه مقاصد سياسي، نظامي و ملي را در بر مي‌گيرد، اما نمي‌توان انگشت اتهام را به سوي شخص يا گروه خاصي گرفت.

جيمز لويس يكي از متخصصان امنيت سايبري در مركز مطالعات ملي و استراتژيك مي‌گويد اگرچه شواهد و مدارك نهايي و قطعي در دست نيست، اما يكي از مظنونان چنين حملاتي عليه ما مي‌تواند كشور چين باشد.

ارزيابي تهديدها و حملات سايبري كم‌كم پا به دنياي ما خواهد گذاشت؛ اما يكي از مشكلات بزرگ، تاخير در ارزيابي چنين حملاتي مي‌تواند باشد.

يكي ديگر از مشكلات، نسبت دادن اين حملات به شخص يا گروه خاص است، چرا كه هكرها با استفاده از تاكتيك‌هاي خاص نظير استفاده از سرور ديگر كشورها يا استفاده از ويروس‌هاي كامپيوتري، كامپيوتر ديگران را بدون اين كه مالك آن اطلاعي داشته باشد به پايگاهي براي حملات سايبري تبديل مي‌كنند.

همكاري بين گروه‌هاي مختلفي كه نقش حاكميتي، نظارتي و مديريتي در اينترنت دارند مي‌تواند امكان مخفي شدن را براي هكرها سخت‌تر كند.