چهار شنبه 22 آذر 1391 - 09:58

نبرد در دنياي صفر و يك

يونانيها با لشكري متحد براي تسخير شهر تروا بر آستانه دروازههاي اين شهر باستاني صفآرايي كرده بودند.

جام جم آنلاين: يونانيها با لشكري متحد براي تسخير شهر تروا بر آستانه دروازههاي اين شهر باستاني صفآرايي كرده بودند. نبردي كه بيشتر براي طرفين جنبه حيثيتي داشت به معركهاي از نبرد ميان قهرمانان و حتي ساكنان افسانهاي كوه المپ بدل شده بود. حضور قهرماناني مانند اوليس و آشيل نيز باعث نشد تا دروازههاي مستحكم شاه پريام روي مهاجمان باز شود.

يونانيان كه با 1000 كشتي به تروا حمله كرده بودند ده سال پشت دروازههاي تروا زمينگير شدند. سرانجام اين اوليس بود كه چاره كار را شناخت. به پيشنهاد او اسبي عظيم و چوبي و ميان تهي ساخته شد. گروهي از بهترين جنگاوران در دل آن پنهان شدند و كشتيهاي يونان به ظاهر خسته از نبردي بيحاصل بادبان برافراشتند و ساحل را ترك كردند. ترواييها شادمان از پيروزي حاصل از مقاومت ده ساله و بيتوجه به اندرزهاي پيشگويان، اسب را هديه يونانيها و دليلي بر شكست آنها دانستند و آن را به ميدان شهر بردند. آنها پس از ده سال جنگ، محاصره، بدبختي و وحشت تا نيمههاي شب به پايكوبي و جشن پيروزي پرداختند. نيمهشب كه ترواييها براي اولين بار پس از ده سال آسوده در خواب بودند، سربازان يوناني از دل اسب بيرون آمدند و دروازههاي مستحكم تروا را گشودند. سربازان به ظاهر سفر كرده يوناني از كمينگاه خود به درون شهر حمله كردند و تروا سقوط كرد. شهري كه ده سال دروازههاي خود را بر حملات فيزيكي دشمنانش بسته نگه داشته بود اسير نيرنگ و حيلهاي شد و سقوطش را به چشم ديد.

داستان تروا و اسب معروف او مربوط به دوراني است كه تاريخ و اسطوره در هم آميختهاند؛ ردپاي حقيقت در سايههاي افسانه پنهان شده است. هزاران سال بايد از آن نبرد ميگذشت تا انسان مدرن كه افتخارش كشتن اسطورههاي باستاني بود شاهد سقوط دوباره باورهاي مدرنش به دست اسبهاي تروا باشد. امروز اسبهاي تروا بازيگران اصلي نبردهاي مدرني را شكل دادهاند كه جايگزين نبردهاي سنتي شدهاند.

اسب تروايِ ديجيتالي

اسب تروا يا تروجان هورس، در زبان امروزه ما بيشتر از آنكه اشاره به آن داستان افسانهاي داشته باشد واقعيتي عيني را هدف قرار داده است. در دوراني كه روز به روز زندگي و همه ساختارهاي نظامي، سياسي، فرهنگي، تجاري و اقتصادي بر دادههاي ديجيتال و شبكههاي كامپيوتري استوار است، نرمافزارهاي مخربي وجود دارند كه بدون دعوت شما و معمولا پنهان در دل برنامهاي خوش ساخت و جذاب (همانند همان اسب معروف) وارد حريم ديجيتال شما ميشود و هنگامي كه انتظار نداريد از دل آن بيرون ميآيد و زمام اين شهر الكترونيك را به دست ميگيرد.

بطور خاصتر اسبهاي تروا در حقيقت گونهاي از بدافزارها هستند. اينها كدهاي كامپيوتري بوده كه هكرها براي نفوذ به سيستمهاي كامپيوتري طراحي ميكنند. معمولا اين برنامهها در قالب ايميلهاي تبليغاتي، صفحات خاصي از وب يا نرمافزارهاي مختلف پنهان ميشوند. زماني كه شما آن برنامه را اجرا ميكنيد اين كد فعال شده و در سيستم شما خانه ميكند و بنا بر نوع طراحي، فعاليت خود را آغاز ميكند. بسياري از اسبهاي تروا براي دزديدن كلمات عبور كاربران، از كار انداختن رايانه هدف، فراخواني برنامهاي خاص در زمان مشخص، ارسال هرزنامه از رايانه شما به ديگران، جمعآوري دادههاي ذخيرهشده در كامپيوتر، تهيه تصويري از صفحات كاربري كاربران و ثبت دادههاي آنها و ارسال به هكرها، طراحي ميشوند. در مقابل اين گروههاي طراح، شركتهاي امنيت رايانهاي نظير طراحان ضد ويروسها بطور منظم اين نرمافزارهاي جديد را زير نظر ميگيرند تا برنامه مقابله با آنها را نيز طراحي كرده و در اختيار مشتريان قرار دهند. تا مدتها اين تروجانها و ويروسها (ويروسها البته ساختار فني متفاوتي از اسبهاي تروا دارند) براي سرقت اطلاعات شخصي و در نهايت در نبرد ميان شركتهاي تجاري براي جاسوسي صنعتي يا از كار انداختن امكانات رقيب به كار گرفته ميشد، اما با افزايش وابستگي ما به دنياي شبكه نقش اين بدافزارها و بازه اقدام آنها نيز توسعه پيدا كرد. امروز همه ما از سيستمهاي آنلاين بانكي استفاده ميكنيم و احتمالا هر كدام از ما دهها نام كاربري و رمز عبور داريم. بيشتر اين موارد نه تنها روي كامپيوترهاي شخصي، كه روي تبلتها و گوشيهاي هوشمند ذخيره شده است. رشد شبكههاي اجتماعي از سوي ديگر باعث شده است حضور آنلاين و ديجيتال ما به اندازه حضور فيزيكي ما در دنياي واقعي پررنگ شود. به اين ترتيب، هككردن يك گوشي تلفن هوشمند عملا ميتواند تمام جزئيات و روش زندگي يك نفر را در اختيار هكر قرار دهد. از دوستان و آشنايان و رمزهاي يك نفر گرفته تا غذاي مورد علاقه و

حتي احساساتي كه او در محيط‌هايي مانند توئيتر، فيس‌بوك يا گوگل پلاس با ديگران به اشتراك مي‌گذارد.

دولت الكترونيك و خطرات فزاينده

امروزه دولت‌هاي جهان و سازمان‌هاي بين‌المللي يا الكترونيك شده‌اند يا به سمت الكترونيك شدن پيش مي‌روند. ديگر كسي نامه‌نگاري سنتي را به صرفه نمي‌داند و ترجيح مي‌دهد از پست الكترونيك استفاده كند. ما از طريق نرم‌افزارها و اپليكيشن‌هاي نصب شده روي سيستم‌هاي خود، كنفرانس‌هاي تصويري برگزار مي‌كنيم و سياستمداران نيز از اين قانون مستثني نيستند. زيرساخت‌هاي مهم كشورها نيز به ناچار به شبكه‌هاي آنلاين متصلند يا توسط سيستم‌هاي رايانه‌اي كنترل مي‌شوند. همين موضوع باعث شده است تا مفهوم نبردهاي مهم به طور چشمگيري تغيير كند. امروزه شبكه‌اي بزرگ از كامپيوترها در يك كشور، صنعت، تجارت و سياست آن كشور را كنترل مي‌كنند؛ شبكه‌اي كه اگر از آن خوب مراقبت نشود، مي‌تواند بسادگي مورد حمله سايبري قرار گيرد.

اگر داستان‌هاي علمي تخيلي را دنبال كنيد آنها از زماني صحبت مي‌كردند كه نبردها ديگر از عرصه ميدان‌هاي جنگ جمع مي‌شوند و قدم به دنياي ديجيتال مي‌گذارند. اگر قرار است دو كشور در مقابل هم صف‌آرايي كنند، با توجه به اين‌كه عمده تاسيسات زيرساختي آنها مبتني بر بسترهاي ديجيتال است، اين امكان وجود دارد كه به جاي حمله نظامي به اهداف مهم، آنها را مورد حمله سايبري قرار داد. امروز اين دوران آغاز شده است و جالب اين‌كه كشور ما در ميانه اين نبرد قرار دارد.

استاكس‌نت؛ هوشمند و مخرب

دو نمونه از مهم‌ترين ويروس‌هاي مخرب كه احتمالا با حمايت‌هاي دولتي طراحي شده و اهداف كلان و زيرساخت‌هاي يك كشور ديگر را هدف گرفته‌اند و عملا پرچمدار جنگ سايبري قرن 21 بودند هدفشان را در ايران جستجو مي‌كردند.

ويروس مخرب استاكس‌نت، نمونه اول اين موارد بود. پيش از اين ويروس‌ها براي شناسايي و جاسوسي و حتي خرابكاري در سيستم‌هاي صنعتي به كار گرفته شده بودند، اما اين ويروس بسيار پيچيده كه سال 2010 شناسايي شد، اولين موردي بود كه بنابر نظر كارشناسان و متخصصان و محافل رسانه‌اي از سوي يك كشور و با هدف حمله به تاسيسات زيرساختي كشور ديگري ساخته شده بود. بعدها معلوم شد يكي از اهداف اصلي اين ويروس سامانه‌هاي كنترل نيروگاه اتمي بوشهر بوده است.

شناسايي اين ويروس و آشكار شدن عملكردش باعث شد بسياري آن را نقطه شروع علني جنگ‌هاي سايبري در نظر بگيرند.

اين ويروس اين توانايي را داشت كه در سيستم‌هاي هدف نفوذ كرده و بطور هوشمند و در حالي كه خود را در زير لايه‌هاي مختلف پنهان مي‌كند كنترل بخش‌هاي حياتي را در نظر بگيرد. اين ويروس مي‌توانست داده‌هاي واقعي سيستم را پنهان كرده و به جاي آن داده‌هاي اشتباهي را به سيستم‌هاي كنترل ارسال كند، امري كه در برخي موارد مي‌تواند به از بين رفتن يك تاسيسات عظيم منجر شود. يك سيستم بسيار ساده را تصور كنيد كه شامل يك ظرف فشار (مانند يك ديگ زودپز) يك فشار سنج و يك سيستم قطع‌كننده منبع انرژي است. در اين مثال فرض كنيد فشارسنج درون محفظه فشار قرار دارد و هرگاه فشار از حد ايمني بالاتر رفت سيستم كنترل منبع گرما دهنده زير اين منبع (مثلا اجاق گاز) را خاموش مي‌كند. اگر واسطه‌اي در اين بين قرار بگيرد و به جاي دماي واقعي ديگ عدد اشتباه و بسيار پايين‌تري را به سيستم كنترل ارسال كند، واحد قطع‌كننده عملا متوجه گذشتن دما و فشار از آستانه خطر نمي‌شود و اجاق را خاموش نمي‌كند. افزايش فشار ممكن است به انفجار ديگ شما منجر شود. اين مثال را در مقياس صنعتي بزرگ كنيد تا متوجه شويد چنين كرم رايانه‌اي مخربي تا چه حد مي‌تواند خطرناك باشد. در واقع چنين ويروس‌هايي مي‌توانند كار بمباران يكي از زيرساخت‌ها را انجام دهند. اگرچه استاكس‌نت به سرعت شناسايي و جلوي عمليات مخربش گرفته شد، اما اين ويروس نشان مي‌داد عصر جديد آغاز شده است. جنگ‌ها ديگر بدون سر و صدا و بدون اعلام قبلي و در جايي كه انتظارش را نداريم آغاز مي‌شوند.

رقص مرگبار شعله

نمونه دوم حتي از نمونه اول سهمناك‌تر بود؛ ويروسي كه به نام شعله معروف شده است. خبر كشف اين ويروس بيست و هشتم مي2012 همزمان از سوي مركز واكنش اضطراري مسائل كامپيوتري ايران، آزمايشگاه موسسه مبارزه با تهديدات كامپيوتري كاسپراسكاي و آزمايشگاه CrySys وابسته به دانشگاه بوداپست اعلام شد.

اين تهديد رايانه‌اي نيز در واقع يك اسب تروا‌ي ويژه بود. بررسي‌ها نشان داد كه ورودي اين اسب تروا مي‌تواند درگاه يو اس بي يا روش‌هاي ديگر ورودي باشد. اين نرم‌افزار پس از ورود به سيستم و پنهان شدن در آن مي‌تواند عمليات جاسوسي خود را آغاز كند. نخستين بار پس از هشدارهاي وزارت نفت ايران اين ويروس ردگيري و شناسايي شد.

اين ويروس اين قابليت را داشت كه از صفحات فعال كامپيوتر عكسبرداري كند، رمزهاي كدگذاري شده را سرقت كرده، ميكروفن‌هاي كامپيوتر را به صورت خودكار روشن و اقدام به شنود كند و حتي از طريق كامپيوتري كه در آن منزل كرده است ابزارهايي كه به فناوري ارتباطي بلوتوث مجهز بوده و در بازه دستگاه آلوده قرار دارد نيز فعال و اطلاعات آنها را سرقت كند. بررسي‌ها نشان داد كه به احتمال زياد اين ويروس نيز از طريق سازندگان استاكس‌نت طراحي و ساخته شده است.

اگرچه اين بار نيز مظنون اصلي به نوشته روزنامه‌هاي آمريكايي دولت اين كشور بود، اما خطرات بالقوه اين ويروس كه احتمالا از سال 2010 و همزمان با استاكس‌نت در شبكه‌هاي مختلف نفوذ كرده است به قدري بود كه رئيس‌جمهور آمريكا به سازمان‌هاي دولتي اين كشور توصيه كرد براي مقابله با اين ويروس آماده باشند. البته باراك اوباما تنها كسي نبود كه در اين باره هشدار مي‌داد.

براي اولين بار در تاريخ، سازمان ملل متحد در باره خطرات بالقوه اين ويروس به كشورهاي عضو هشدار داد و با اشاره به خطرات بالقوه‌اي كه اين ويروس مي‌تواند در پي داشته باشد از آنها خواست اين موضوع را در اولويت قرار داده و به بررسي ايمني سيستم‌هاي خود بپردازند.

به اين ترتيب نبرد رسمي و علني سايبري مدتي است آغاز شده است، اما در اين بين تنها دولت‌ها و تاسيسات زيرساختي نيستند كه در خطر قرار دارد. اگر هشدارها و احتياط‌هاي لازم به عمل نيايد ممكن است گوشي تلفن شما، رمزهاي بانكي، مكالمات يا پيام‌هاي شما نيز از سوي افراد سودجو مورد سوءاستفاده قرار گيرد. به اين ترتيب اسب افسانه‌اي تروا اين روزها بيش از هر زماني در تاخت و تاز اطراف ماست.

غارنشين يا سفر به فضا؟

در اين شرايط شايد بسياري فكر كنند فناوري جامعه را ناامن‌تر كرده و خطرات اطراف ما را افزايش داده است، اما واقعيت اين است كه اين ساده‌دلانه‌ترين برداشت از وضع موجود است. فناوري و پيشرفت آن موضوع واقعي و ضروري است و مواجهه با خطرات رشد فناوري به معني غلط بودن استفاده از آنها و ضرورت بازگشت به دوران غارنشيني نيست. واقعيت اين است كه انقلاب فناوري ديجيتال زندگي ما را به مرحله نويني وارد كرده است و ما سطح و سبكي از زندگي را تجربه مي‌كنيم كه پيش از اين وجود نداشته است. ورود الزامي ما به اين سطح جديد به قدري سريع رخ داده كه بسياري از ما هنوز اگرچه كاربران اين سيستم‌ها هستيم، اما تفكرمان را متناسب با آن اصلاح نكرده‌ايم. متاسفانه و بويژه در سال‌هاي اخير موجي از فناوري هراسي يا تكنوفوبيا در بين جوامع مختلف و از جمله كشور ما تبليغ مي‌شود. چنين كاري نه چرخ‌هاي زمان را به عقب بازمي‌گرداند و نه نيازهاي ما به فناوري روز را كاهش مي‌دهد. تنها راه مقابله با چنين تهديدهايي ـ حداقل در سطح عمومي و فردي ـ آشنا كردن مردم با فناوري و پرهيز از ترساندن آنها از دنياي مدرن است. در سطح كلان نيز همان‌گونه كه هر دوره‌اي با پيشرفت ابزارهاي مبارزه و جاسوسي، طرح‌ها و سيستم‌هاي پدافندي مناسب آن طراحي شده است اين بار نيز همين روند در دستور كار همه كشورها قرار دارد.

اگرچه اسب‌هاي تروا اين روزها از كامپيوترهاي به ظاهر خاموش در محرمانه‌ترين جلسات، تا دل صنايع يا حتي جيب لباس شما ممكن است جولان بدهند، اما نبايد فراموش كرد آنچه باعث سقوط شهر تروا پس از مقاومتي ده ساله شد، اسب تروا نبود، بلكه شهروندان ترواييِ بودند كه اسب را هديه‌اي فرض كردند و درهاي دژ مستحكم خود را در برابر آن باز كردند و آن را به ميانه شهر آوردند. سپس بناي سرخوشي و بي‌خيالي و عشرت در پيش گرفتند و در كنار تهديد پنهان آسوده سر به بالين نهادند. راه‌حل سقوط تروا خراب كردن شهر تروا نبود، تنها لازم بود بيشتر مواظب هديه مشكوك دشمنانشان باشند.

پوريا ناظمي / جام‌جم