سیستم تشخیص رفتار بدافزار با استفاده از تکنیک‌های استخراج گراف

فاطمه دباغی زرندی[۱]، سوده حسینی [۲]، فهیمه دباغی زرندی [۳]

[۱]دانشگاه شهید باهنر کرمان، dabaghi.fateme@gmail.com
[۲]دانشگاه شهید باهنر کرمان، so_hosseini@uk.ac.ir
[۳]دانشگاه ولی‌عصر(عج) رفسنجان، f.dabaghi@vru.ac.ir

چکیده

با توجه به رشد روز افزون کدهای مخرب در سال‌های اخیر، تشخیص بدافزار به یک موضوع مهم تبدیل شده است. در این راستا، بسیاری از محصولات تشخیص بدافزار، از الگوریتم‌های مبتنی بر امضا استفاده می‌کنند که به دلیل متکی بودن این محصولات بر فایل هش و بایت امضا مشکل‌ساز می‌باشند و در مقابله با تکنیک‌های مبهم‌سازی مخرب‌ها، دارای ضعف می‌باشند. از طرف دیگر برای یک حمله کننده تغییر اساسی در رفتار یک بدافزار، سخت‌تر از تغییر در ساختار دستوری آن می‌باشد. بر این اساس تکنیک‌های تشخیص مبتنی بر رفتار یک راه حل امیدبخش برای حل مشکل مبهم‌سازی می‌باشند. در این مقاله یک روش جدید استخراج گراف برای تشخیص انواع بدافزارها با استفاده از تجزیه و تحلیل ایستا ارائه می‌شود. این روش از امضای معنایی به جای امضای دستوری استفاده می‌کند. بنابراین این امکان را به وجود می‌آورد که به وسیله تشخیص نمایه‌های مختلف رفتار مخرب، با تکنیک‌های مبهم‌سازی حمله کننده مقابله کند. علاوه بر این، روش پیشنهادی به دلیل استخراج دقیق الگوهای رفتاری در تشخیص بدافزارها کارایی بالایی دارد و در مقایسه با سایر روش‌ها، مثبت کاذب کمتری تولید خواهد کرد.

واژه های کلیدی

تشخیص بدافزار، تحلیل ایستا، کد مبهم‌سازی، کدگراف، خوشه‌بندی گراف

مقدمه

برای ایجاد امنیت کامل در یک سیستم کامپیوتری علاوه بر دیوار آتش[۱] و دیگر تجهیزات جلوگیری از نفوذ، سیستم‌های دیگری به نام سیستم‌های تشخیص نفوذ (IDS[۲]) مورد نیاز می باشند تا بتوانند در صورتی که نفوذگر از دیواره آتش، آنتی ویروس و دیگر تجهیزات امنیتی عبور کرد و وارد سیستم شد آن را تشخیص داده و چاره‌ای برای آن بیاندیشند.

سیستم‌های تشخیص نفوذ برای کمک به مدیران امنیتی سیستم در جهت کشف نفوذ و حمله به کار گرفته شده‌اند. هدف یک سیستم تشخیص نفوذ تنها جلوگیری از حمله نیست بلکه باید به کشف و احتمالا شناسایی حملات و تشخیص اشکالات امنیتی در سیستم یا شبکه‌ی کامپیوتری و اعلام آن به مدیر سیستم نیز بپردازد. سیستم‌های تشخیص نفوذ در کنار دیواره‌های آتش و به صورت مکمل امنیتی برای‌آن‌ها مورد استفاده قرار می‌گیرند.

امروزه دو روش اصلی برای تشخیص نفوذ به شبکه ها مورد استفاده قرار می‌گیرد [۱].

۱) تشخیص رفتار غیر عادی[۳]
۲) تشخیص مبتنی بر امضا[۴] یا تطبیق الگو

روش اول مبتنی بر تعیین میانگین انواع فعالیت‌ها بر روی شبکه است. مثلا چند بار یک دستور مشخص توسط یک کاربر در یک تماس با یک میزبان[۵] اجرا می‌شود. لذا در صورت بروز یک نفوذ امکان تشخیص آن به علت مخالف معمول بودن آن وجود دارد. اما بسیاری از حملات به گونه‌ای هستند که نمی‌توان به راحتی و با کمک این روش آن‌ها را تشخیص داد [۱].

روش دوم که در بیشتر سیستم‌های موفق تشخیص نفوذ به کار گرفته می‌شود، IDS مبتنی بر امضا یا تطبیق الگو است. منظور از امضا مجموعه قواعدی است که یک حمله‌ی در حال انجام را تشخیص می‌دهد. سیستمی که قرار است نفوذ را تشخیص دهد، با مجموعه‌ای از قواعد بارگذاری می‌شود. هر امضا دارای اطلاعاتی است که به سیستم نشان می‌دهد در داده‌های در حال عبور باید به دنبال چه فعالیت‌هایی بگردد. هرگاه ترافیک در حال عبور با الگوی موجود در امضا تطبیق کند، پیغام اخطار تولید می‌شود و مدیر شبکه را از وقوع یک نفوذ آگاه میکند. در بسیاری از موارد، علاوه برآگاه کردن مدیر شبکه، اتصال مرتبط با نفوذگر را راه اندازی مجدد می‌کند و یا با کمک یک دیوارآتش و انجام عملیات کنترل دسترسی با نفوذ بیشتر مقابله می‌کند [۱].

با توجه به متداول بودن و دقیق‌تر بودن تشخیص نفوذ مبتنی بر امضا، در این مقاله روی این روش تمرکز خواهیم کرد.

[1] Firewall
[2] Intrusion Detection System
[3] Anomaly Detection
[4] Signature-Based Detection
[5] Host