رفتار شناسی بدافزار (Malware) قسمت ۱۱ : پیشرفت ویروس نویسی (نسخه PDF)

روند پیشرفت و توسعه فناوری ویروس نویسی

در روند پیشـرفت ویروس نویسـی ، ویروس ها سـعی بر آن داشـتند که توسط ویروس یابها شـناسایی نشوند. بطورمعمول ویروس یابها از روش یکسانی برای یافتن ویروس اسـتفاده می کنند و آن اینست که از رفتار ویروس الگوبرداری کرده و هرگاه ردی از این رفتار در سیسـتم دیده شد ، پی به ویروسی بودن سیستم برده و این ردپا می تواند عملکرد یک ویروس در یک مکان خاص و یا استفاده از یک تابع خاص و یا یا موارد مشابه باشد که ویروس یابها با بانک اطلاعاتی که در خود دارند و این علائم پی به ویروس و بدافزار می برند.

البته با توسـعه ویروس ها ، نحوه عملکرد آنها نیز تا حدی تغییر کرده به این صورت که ویروس ها دیگر عملکرد یکسانی در همه میزبان ها نداشـته و به همین جهت نمی توان الگوی ثابتی از رفتار آنها ترسـیم کرد. ولی آنچه که مسـلم است جنگی است بین ویروس ها و ویروس یابهـا همواره ادامه دارد و به نظر می رسـد که ویروس ها، یک گام جلوتر از ویروس یابها عمل می کننـدو شایـد این به این دلیل است که سازمانهای جاسوسی انگیزه بیشتری برای تخریب دارند و یا اینکه خود شرکتهای ویروسیاب همکاری ویژه ای با سازمانهای جاسوسی .

نمونه هایی از الگوریتم های ویروس های پیشرفته

ویروس های رمز شده

ویروس ها با رمزنگاری خود سـعی بر مخفی نگه داشـتن کدهای خود و همچنین قابل شناسایی نبودن دارند. در ویروس های تحت داسی، شناسایی ویروس با وجود کد ۱۳ و یا ۲۱ در برنامه، به راحتی می توان پی به ویروس برد(مقالات آموزشـی قبلی) ولی ویروس ها با توسعه خود و سعی بر رمزنگاری خودشان این امکان را از ویروس یابها گرفته اند که به راحتی شناسایی شوند.البته نکته دیگری که وجود دارد این است که وجود رمز بر روی کد ، خود شبه برانگیز است که موجب افزایش شک و تردید نسبت به فایل مربوطه مبنی بر اینکه ویروسی است می باشد.رمزنگاری در برخی ویروس ها به این صورت است که با عملگر xor کد را رمز و با همین عملگر و داشتن کلید ، مجدد از کد خارج می گردد.ضد ویروس ها برای **شناسایی در طی سه مرحله زیر عمل می کنند:**

- جستجوی روش رمزنگاری
- معکوس رمزنگاری را بر روی بدنه ویروس اعمال کنند
- بررسی وجود الگو در داده رمزبرداری شده

رمزنگاری بر روی بدنه ویروس ها می تواند به چندین روش باشد که متداولترین آنها به شرح زیر است:

- برنامه رمزگشا در بالای کد اصلی قرار دارد
- برنامه رمزگشا در پایین کد قرار دارد
- چنـدین رمزگشـا در ابتـدا یـا انتهـای بـدنه ویروس وجود دارد، به گونه ای که اول رمزگشای اولی کار می کنـد و رمزگشاهای بعـدی رمزبرداری می کند.

روش ترکیبی

برخی ویروس ها مانند فونو از طریق جابجا کردن حروف بطور مثال a با c و به همین ترتیب بر اساس یک الگوی خاص، عمل رمزگذاری را انجام دادهو یا ویروس چبا که از نام میزبان خود اسـتفاده کرده و عمل رمزنگاری را انجام می دهد و به همین ترتیب در میزبانهای مختلف بـا اسـتفاده از این الگوریتم ، رمزنگـاری مختلف انجـام می دهـد و یا ویروس کریپتو که از دو کلیـد عمومی و خصوصـی برای رمزنگاری و رمزگشایی استفاده می کند.

ویروس های چند شکلی ساده

ویروس نویسـان متوجه شدنـد در صورتیکه روش رمزنگاری درون ویروس جایگـذاری گردد، توسط ویروس یابها قابل شـناسایی هسـتند.به همین ترتیب ویروس ها، با نوشتن دو یا چند تایع برای یک رویه خود که با ورودی های یکسان، خروجی یکسان داده.

ویروس های چند شکلی

این نوع ویروسـها با اضافه کدن دسـتورات بی ارزش در داخل کد ویروس ، موجب سـردرگمی برای تحلیلگران را فراهم کرده و در واقع این کدهای اضافه جزء افزایش حجم فایل کاری دیگری نداشته و به این کد اصطلاحا زباله می گویند.

دستورات زباله چند گونه هستند که عبارت هستند از:

- دستور nop که ماهیتا هیچ کاری انجام نداده
- دستوراتی که خود دستور عملی را انجام می دهند ولی آرگومانهای آن تاثیری در اجرا ندارد
- دستورات mov eax geax
- دستوراتی که هم خود دستور و هم آرگومانهایش با معنی است ولی نسبت به برنامه هیچ تاثیری ندارد.

البته ابزارهایی مانند mte وجود دارد که تحت عنوان موتور ویروس ساز نام دارد با این توضیح که کافیست این موتور به عنوان یک شی به ویروس اضافه شده و موجب چند ریختی در ویروس شده.موتور ویروس یاب دیگر تحت عنوان موتور tpe که از موتور قبلی پیشرفته تر عمل کرده.ویروس hps یکی از ویروس های چند شکلی بود که از چندین روش رمزگذاری استفاده می کرد که برای هر فایل میزبانی متفاوت بود مانند رمزگذاری add و sub و dec و inc و not و xor که کلیدهای آن ۸و۱۶و۳۲ بیتی بوده.ویروس کوک نمونه دیگری از ویروس هـای چند شکلی است که از ماکرونویسـی در نرم افزارهای آفیس اسـتفاده می کردند که علاوه بر دسـتورات زباله از تغییر حروف بزرگ ب هکوچک و برعکس و تغییر نام متغیرها و تغییر اعداد شـمارش حلقه و ... اسـتفاده کرده.این نوع ویروس کند بوده.ویروس یابها در مواجه با این نوع ویروس ها باید از روشهای هوشمند و پیچیده استفاده کرده.

ویروسهای دگر شکلی

این نوع ویروس هـا رمزگـذاری یـا چندشـکلی عمل نکرده و این نوع ویروس رویکرد متفاوت از خود نشان می دهنـد در واقع در صورت و ظاهر مشابه ولی از نظر ژنتیکی تغییر می کنند.

نمونه های از ویروس های دگرشکلی

- **ویروس رج سواپ** ظاهر خود را تغییر نـداده ولی از نظر کـد بانیری تغییر می کند.این نوع ویروس سـعی می کند op code های متفاوتی را برای عملکرد های مشابه در نظر بگیرد.
- **ویروس بدبوی** خود را به چندین قسمت تقسیم کرده و از طریق پرش ، عمل جابجایی را انجام داده .
- **ویروس ایول** ساده ترین اعمال را به پیچیده ترین حالتها اجرا می کرد، این گونه ویروس با استفاده از اعمال ریاضی دستورات زباله و تغییر op-code ویروس دگرشکلی پیشرفته ای بسازند، در این روش op code ها تغییر می کند، رجیستری تغییر می کند، دستورات زباله اضافه شده و خود دستور عوض می گردد و همه اینها موجب پیچیدگی بیشتر در ویروس شده.

نتیجه: ویروس می توانـد با اسـتفاده از کلیه روشـها ، جایگشت های متفاوتی از آلودگی داشـته باشـند و ضد ویروس ها نمی توانند همه حالتهای آلودگی را شـناسایی کنند و برای هر کدام روشـی برای پاکسازی در نظر می گیرد.به همین دلیل ضد ویروس ها از روشـهایی مانند شبیه سازی دستورات برای شناسایی ویروس ها استفاده می کنند.

نویسنده : علیرضا(ARAF) - تحلیل بدافزار سعدی و زارع

منبع : ITPRO

مطلب اصلی