بات نت و یا زامبی در سیستم های کامپیوتری چیست؟

بات نت به مجموعه ای از رایانه های آلوده گفته می شود که توسط یک رایانه آلوده تشکیل شده اند. به هریک از آن رایانه های آلوده که توانایی آلوده کردن بقیه رایانه ها را نیز دارد بات گفته می شود (البته گاهی نیز زامبی خوانده می شوند) درواقع بات مخفف روبات می باشد.

هنگامی یک رایانه به بات تبدیل می شود که یک مجرم اینترنتی شروع به پخش کردن نرم افزارهای مخرب در سراسر جهان می کند. این نرم افزار های مخرب که بدافزار نیز خوانده می شود, رایانه های سالم را به بات تبدیل میکنند. به‌طور معمول مجرمان اینترنتی از این بات ها استفاده می کنند تا با آلوده کردن تعداد زیادی از رایانه های سالم یک شبکه یا همان بات نت را تشکیل دهند.

چند توصیه واضح و کاربردی برای جلوگیری از بات نت ها!

۱- حتما لاگهای سیستم خود را نگاه کنید

۲- مصرف پهنای باند را در شبکه بررسی نمایید

۳-آگاهی و دانش کاربران را افزایش دهید. به آنها بگویید که پیوستهای ناشناس یا ناخواسته را باز نکنند، روی لینکهای داخل ایمیلها کلیک نکنند، و به هر لینک غیر عادی که میبینند فکر کنند.

۴- مراقب این پورتها باشید.

اگرچه botnet های اخیر می توانند از هر پورتی که مدیر شبکه باز گذاشته باشد ارتباط برقرار کنند، ولی اغلب botnet ها هنوز با استفاده از IRC یعنی پورت شماره ۶۶۶۷ یا سایر پورتهایی با شماره های بزرگ و فرد (مانند ۳۱۳۳۷ و ۵۴۳۲۱) ایجاد ارتباط می کنند. تمامی پورتهای بالای ۱۰۲۴ باید در مورد ارتباطات ورودی و خروجی مسدود باشند، مگر اینکه سازمان شما یک برنامه خاص یا نیاز خاصی برای باز کردن یک پورت داشته باشد. حتی در چنین حالتی نیز شما می-توانید با استفاده از سیاستهایی مانند بستن پورت در

ساعتهای غیر کاری یا رد کردن تمامی ارتباطات به جز ارتباطاتی که از IP های قابل اعتماد ایجاد شده اند، احتیاط لازم را به عمل آورید.

۵- و در آخر از آنتی ویروسهای به روز، نصب فایروال، استفاده از کلمات عبور مناسب، به روز نگه داشتن نرم افزارها، و رعایت جوانب احتیاط در هنگام استفاده از ایمیل و مرورگرهای وب و از این دسته توصیه های امنیتی غافل مشوید