باسمه تعالی

گزارش فنی بدافزار
Andromeda

معرفی بدافزار

باتنت Andromeda که با نام Gamarue نیز شناخته شده، بات نتی است که بر اساس گزارش‌های ارائه شده توسط سامانه ملی مقابله با آسیب‌پذیری‌های شبکه و بات، در دو ماه اخیر بیش‌ترین میزان آلودگی را در ایران داشته است. این بدافزار از آیکون برنامه مشهور و پراستفاده SHAREit یعنی  استفاده کرده است؛ به این ترتیب در ظاهر از دید کاربر قانونی به نظر می‌رسد و امکان اجرا شدن آن توسط کاربر نیز افزیش می‌یابد. هدف اصلی این بدافزار توزیع سایرخانواده‌های بدافزاری بر روی ماشین‌های آلوده شده از طریق ارتباط با سرور کنترل و فرماندهی است. این بدافزار از روش‌های مختلفی برای مخفی ماندن و جلوگیری تحلیل شدن استفاده می‌کند.

نحوه شناسایی سیستم آلوده از طریق لاگ‌های شبکه

تمامی سیستم‌هایی از شبکه که با نام دامنه‌های زیر در ارتباط باشند:

- europe.pool.ntp.org
- microsoft.com
- id0000058.pulse-manager.pw
- id0000058.documents-ideas.pw
- id0000058.documents-freedom.pw
- ynvdudhnyxdvqlqab.com
- ynvdudh.msudate.pw

نحوه بررسی وجود آلودگی

۱. وجود کلید رجیستری HKLM\Software\Policies با مقدار is_not_vm.
۲. وجود فایلی به نام mshfnce.exe در ProgramData
۳. وجود کلید رجیستری

HKCU\Software\Microsoft\Windows NT\CurrentVersion\Windows\Load

که مقدار آن به فایل mshfnce تنظیم شده است.

۴. وجود کلید رجیستری HKLM\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\Run که مقدار آن به فایل mshfnce تنظیم شده است.

نحوه پاک‌سازی سیستم

۱. خاتمه‌دهی به پردازه msiexec.exe
۲. حذف فایل mshfnce.exe از ProgramData
۳. حذف کلیدهای رجیستری ایجاد شده
۴. منع ارتباط با دامنه‌های مورد استفاده برای سرورهای کنترل و فرمان.

نحوه بررسی پاک بودن سیستم

۱. نبود مقدار is_not_vm برای کلید رجیستری HKLM\Software\Policies
۲. نبود فایل mshfnce.exe در ProgramData (توجه شود که برای مشاهده این فایل باید ویژگی مشاهده فایل‌های مخفی را فعال نمود).
۳. نبود کلید رجیستری‌های ذکر شده
۴. نداشتن ارتباطات شبکه‌ای با سرورهای فرماندهی و کنترل.

توصیه‌های امنیتی برای پیشگیری از آلودگی

۱. خودداری از باز کردن مستندات الحاق شده به ایمیل‌های ناشناس و ...
۲. غیرفعال کرن ماکروها در مستندات
۳. استفاده از نرم‌افزارهای معتبر
۴. به‌روز بودن نرم‌افزار ضدبدافزار نصب شده بر روی سیستم
۵. مسدودسازی دسترسی به سرورهای فرماندهی و کنترل.