تحلیل بدافزار Bankpatch با هدف سرقت مشخصات بانکی و ارائه راهکارهای مقابله با آن

معرفی بدافزار

بدافزار Bankpatch یک تروجان بانکی پیشرفته است که برای اولین بار در سال ۲۰۰۷ کشف شده و فعالیت آن تا امروز نیز ادامه دارد. توسعه‌دهندگان این بدافزار هنوز هم آن را به‌روزرسانی کرده و افزونه‌های جدیدی برای این بدافزار تولید می‌کنند. به عنوان مثال هر روز افزونه‌های جدیدی از این بدافزار کشف می‌شوند که هدفشان سرقت مشخصات بانکی مشتریان مجموعه جدیدی از بانک‌های هدف است.

قربانیان غالباً از طریق روش‌های معمول انتشار بدافزار مانند بازدید از سایت‌هایی که از آسیب‌پذیری مرورگر کاربر و افزونه‌های آن (علی‌الخصوص Internet Explorer) سوء استفاده می‌کنند و یا از اجرای فایل‌هایی آلوده می‌شوند که به ظاهر سالم به نظر می‌رسند.

معمولاً Bankpatch فعالیت‌های خود را از طریق تزریق کد در پروسه‌های دیگر علی‌الخصوص پروسه‌های اساسی ویندوز به انجام می‌رساند. این کار سبب می‌شود تشخیص و پاک‌سازی سیستم‌های آلوده بسیار دشوارتر شود.

شناسایی سیستم آلوده از طریق لاگ‌های شبکه

تمامی سیستم‌هایی که نام‌های دامنه زیر را Resolve کرده باشند، آلوده هستند:

- oqorierihon.com
- banking-finanzportal.com
- security-validate-chek.net
- securityanaliz.ru
- stoneseal.eu
- securitycheck.com

بررسی وجود آلودگی

۱. وجود زیرکلیدهای ins، del، vendor، prd، proxy در کلید زیر از رجیستری ویندوز:

HKLM\Software\Microsoft\Windows\CurrentVersion\Internet Settings\

۲. وجود فولدرهایی با نام xmldm یا kock در مسیر Windows\system32

۳. وجود فایلی با نام appconf32.exe در مسیر Windows\system32

۴. وجود Mutexهایی با نام SearchBinary و Updateappconf32 بر روی سیستم

۵. وجود Internet Zone شماره ۳ بر روی Internet Explorer

۶. عدم امکان فعال‌سازی قابلیت به‌روزرسانی خودکار بر روی Firefox

۷. وجود نام appconf32.exe در مقادیر کلیدهای زیر از رجیستری:

- HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\Userinit
- HKCU\Software\Microsoft\Windows\CurrentVersion\Run

نحوه پاک‌سازی سیستم

۱. حذف فایل appconf32.exe از مسیر Windows\system32

۲. حذف مقدار appconf32.exe از کلیدهای زیر در رجیستری ویندوز:

- HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\Userinit
- HKCU\Software\Microsoft\Windows\CurrentVersion\Run

۳. راه اندازی مجدد سیستم

بررسی پاک بودن سیستم

۱. نبود فایلی با نام appconf32.exe در مسیر Windows\system32
۲. در حال اجرا نبودن پروسه‌ای با این نام بر روی سیستم
۳. نبود ارتباط با نام‌های دامنه یاد شده بر روی سیستم
۴. نبود کلیدهای یاد شده در رجیستری ویندوز

توصیه‌های امنیتی برای پیشگیری

۱. خودداری از اجرای فایل‌های ناشناس (کرک‌های ارایه شده برای نرم‌افزارها توسط تیم‌های ناشناس، فایل‌های دریافتی از اشخاص ناشناس، فایل‌های الحاق شده به ایمیل‌های ناشناس و ...)
۲. به‌روز بودن نرم‌افزار ضدبدافزار نصب شده بر روی سیستم
۳. استفاده از مرورگرهای امن و به‌روز