باسمه‌تعالی

گزارش فنی باج‌افزار
Crypton

معرفی بدافزار

باج‌افزار Crypton نسخه جدیدی از خود را در ماه مه سال جاری میلادی منتشر کرده که از طریق سرویس‌های آسیب‌پذیر remote desktop خود را به سیستم قربانیان می‌رساند. گزارش‌های ناشی از آلودگی کاربران ایرانی به این باج‌افزار نشان از لزوم آگاهی رسانی و پیشگیری در برابر این باج‌افزار دارد.

نحوه شناسایی سیستم آلوده از طریق لاگ‌های شبکه

تمامی سیستم‌هایی از شبکه که با آدرس زیر در ارتباط باشند:

http://auth-rambler.com/krya18/index_shell.php

نحوه بررسی وجود آلودگی

۱. وجود کلید رجیستری زیر در سیستم:

HKEY_CURRENT_USER\Software\Microsoft\CurrentVersion\Run\ZXKmUvnudOMimWHm

۲. وجود کلید رجیستری HKLM\SOFTWARE\ZXKmUvnudOMimWHm همراه با مقادیر زیر در سیستم:

- HKLM\SOFTWARE\ ZXKmUvnudOMimWHmd
- HKLM\SOFTWARE\ ZXKmUvnudOMimWHmn
- HKLM\SOFTWARE\ ZXKmUvnudOMimWHmp
- HKLM\SOFTWARE\ ZXKmUvnudOMimWHms
- HKLM\SOFTWARE\ ZXKmUvnudOMimWHmu
- HKLM\SOFTWARE\ ZXKmUvnudOMimWHmv

۳. وجود mutex ای به نام ZXKmUvnudOMimWHm در سیستم

نحوه پاک‌سازی سیستم

در صورتی که در سیستم یکی از علائم فوق مشاهده شد اما هنوز اطلاعات کاربر رمز نشده باشد، باید ابتدا به پردازه اصلی بدافزار خاتمه داد. برای این کار باید:

۱. در کلید رجیستری run درایه با نام ZXKmUvnudOMimWHm را یافت. مقدار تنظیم شده در این درایه مسیر فایل اجرایی باج‌افزار را نشان می‌دهد. سپس بایستی پردازه با این نام را در سیستم خاتمه داد و فایل اجرایی مذکور و درایه ZXKmUvnudOMimWHm در کلید رجیستری را حذف نمود.
۲. بایستی کلید رجیستری HKLM\SOFTWARE\ZXKmUvnudOMimWHm را حذف نمود.
۳. بایستی ارتباطات به آدرس auth-rambler.com را مسدود نمود.

نحوه بررسی پاک بودن سیستم

۱. وجود نداشتن درایه‌ای با نام ZXKmUvnudOMimWHm در کلید رجیستری run
۲. وجود نداشتن کلید رجیستری HKLM\SOFTWARE\ZXKmUvnudOMimWHm
۳. نداشتن ارتباط با دامنه auth-rambler.com

توصیه‌های امنیتی برای پیشگیری

۱. امن‌سازی سرویس remoot desktop
۲. خودداری از باز کردن مستندات الحاق شده به ایمیل‌های ناشناس و ...
۳. به‌روز بودن نرم‌افزار ضدبدافزار نصب شده بر روی سیستم
۴. ذخیره پشتیبان‌های سیستم در مکانی خارج از سیستم