بسمه تعالی

ابزارهای رمزگشایی و بازیابی اطلاعات برای برخی از باج افزارها

فهرست مطالب

۱ مقدمه

باج‌افزار یکی از بدافزارهایی است که می‌تواند رایانه‌ها را آلوده کند. این نوع بدافزار، فایل‌های رایانه را رمزگذاری و قفل می‌کند و تنها راه دسترسی به آن‌ها پرداخت باج به هکر است. خوش‌بختانه، امروزه لیستی از ابزارهای رمزگشایی باج‌افزار برای ویندوز ۱۰ وجود دارد که به قربانی کمک می‌کند تا این مشکل را رفع کند. در ادامه، ابزارهای رمزگشای باج‌افزار برای ویندوز ۱۰ شرح داده خواهد شد.

۲ ابزارهای رمز گشایی وبازیابی اطلاعات برای برخی از باج افزار ها

برای حذف باج‌افزار از رایانه، ابتدا باید نوع باج‌افزاری که رایانه را آلوده کرده است، شناسایی شود. برای این منظور، می‌توان از خدماتی هم‌چون شناسه‌ی باج‌افزار، برای شناسایی باج‌افزار استفاده کرد. پس از شناسایی نوع باج‌افزار، می‌توان آن را با یکی از ابزارهای زیر از بین برد.

۲-۱ رمزگشای باج‌افزار AutoLocky

رمزگشای AutoLocky برای از بین بردن باج‌افزار AutoLocky استفاده می‌شود. اگر رایانه‌ای آلوده به این باج‌افزار شود، نام فایل‌های آن رایانه به "*.Locky" تغییر می‌یابد و رمزگذاری می‌شود. با استفاده از رمزگشای Autolocky می‌توان به حذف این نرم‌افزار مخرب امیدوار بود.

۲-۲ رمزگشای Jigsaw

باج‌افزار Jigsaw در صورت عدم پرداخت باج به هکر، تمامی فایل‌ها را حذف خواهد کرد. اما با ابزاری مانند رمزگشای Jigsaw می‌توان این نرم‌افزار را به راحتی از رایانه حذف کرد.

۲-۳ رمزگشای باج‌افزار کسپرسکی

این ابزار توسط شرکت آنتی‌ویروس کسپرسکی منتشر شده و می‌تواند هر دو باج‌افزار CoinVault و Bitcryptor را از رایانه حذف کند. کسپرسکی ابزارهای مختلف دیگری هم‌چون XoristDecryptor، ScatterDecryptor و RakhniDecryptor را نیز برای حذف باج‌افزارها منتشر کرده است که می‌توان آن‌ها را از وب‌سایت کسپرسکی دانلود کرد.

۲-۴ رمزگشای RannohDecryptor

کسپرسکی، رمزگشای RannohDecryptor را برای باج‌افزار CryptXXX منتشر کرده است. بنابراین اگر رایانه‌ای آلوده به چنین باج‌افزاری شود، باید از این ابزار استفاده کرد.

۲-۵ کسپرسکی WindowsUnlocker

باج‌افزار خاصی می‌تواند به طور کامل مانع از دسترسی به رایانه شود. اما خوش‌بختانه ابزارهایی هم‌چون کسپرسکی WindowsUnlocker می‌توانند این مشکل را رفع کنند. برای حذف باج‌افزار با استفاده از این ابزار، تنها باید فایل ".iso" را دانلود کرد و از آن برای ساخت یک درایو حافظه‌ی فلش قابل راه‌اندازی[۱] استفاده کرد. پس از آن باید رایانه‌ی خانگی را از این درایو راه‌اندازی کرد و با توجه به دستورالعمل، عمل کرد.

۲-۶ رمزگشای HitmanPro.Kickstart

HitmanPro.Kickstart ابزار دیگری برای دستیابی به رایانه است، حتی اگر رایانه به طور کامل مسدود شده باشد. تنها لازم است این رمزگشا در درایو حافظه‌ی فلش قرار گیرد و رایانه راه‌اندازی شود. سپس برنامه به طور خودکار باج‌افزار را حذف خواهد کرد.

۲-۷ ابزار ضدباج‌افزاری Trend Micro

همانند دو باج‌افزار قبلی، ابزار ضدباج‌افزاری Trend Micro می‌تواند برای دستیابی به رایانه و حذف باج‌افزار با راه‌اندازی از یک درایو حافظه فلش استفاده شود.

۲-۸ ابزار رمزگشای Cisco TelsaCrypt

Cisco نیز ابزار رمزگشای خود را برای باج‌افزار منتشر کرده است و این ابزار برای حذف TelsaCrypt طراحی شده است. ابزار رمزگشای TelsaCrypt به صورت یک ابزار خط فرمان منتشر می‌شود و به قربانی برای حذف این باج‌افزار از یارانه‌ی خانگی کمک می‌کند.

---

[۱] Bootable

۹-۲ ابزار رمزگشای باج‌افزار Operation Global III

باج‌افزار خاصی فایل‌ها را رمزگذاری خواهد کرد و پسوند آن‌ها را به ".exe" تغییر خواهد داد. در صورت برخورد با چنین مشکلی، می‌توان از ابزار Operation Global III استفاده کرد.

۱۰-۲ ابزار رمزگشایی باج‌افزار Petya

گاهی اوقات باج‌افزار، رکورد Master Boot را تغییر خواهد داد و مانع از راه‌اندازی به Windows یا Safe Mode می‌شود. یکی از باج‌افزارهایی که چنین کاری را انجام می‌دهد، باج‌افزار Petay است، اما می‌توان آن را به راحتی با استفاده از ابزار رمزگشایی باج‌افزار Petya حذف کرد.

۱۱-۲ رمزگشاهای باج‌افزار HydraCrypt و UmbreCrypt

در صورت آلوده شدن رایانه‌ی خانگی به باج‌افزار HydraCrypt و UmbreCrypt، باید آن را با استفاده از رمزگشاهای باج‌افزار HydraCrypt و UmbreCrypt حذف کرد.

۳ نتیجه‌گیری

ابزارهای فراوانی برای حذف انواع باج‌افزار وجود دارد. نویسندگان رمزگشاهای باج‌افزار امیدوارند که این ابزارها مفید واقع شوند و قربانیان بتوانند بدون پرداخت باج، باج‌افزار را از رایانه‌های خود حذف کنند.