

بسمه تعالی

راهنمای ابزار شناساگر افتا

این ابزار جهت شناسایی بدافزار و وب‌شل طراحی شده است. در راستای اجرای بهینه و دریافت خروجی قابل استناد مراحل زیر اجرا شود. قابل ذکر است که این ابزار بر روی تمامی سرورهای سازمانی می‌بایست اجرا شود.

- ۱- Hash محتوای پوشه دریافت‌شده، مطابق مراحل زیر محاسبه و با مقدار درج شده در جدول ۱ مقایسه شود.
- a. دستور PowerShell زیر در مسیر فایل شناساگر اجرا شود.

Get-FileHash -Algorithm MD5*

خروجی مشابه تصویر زیر خواهد بود:

Algorithm	Hash	Path
MD5	A1A268C7EDF122D89587E2D692435DFC	C:\Afta_Detector_v1.6\Afta_Detector_v1.6.exe
MD5	B3C9BD5F2D5E4C99278CF4C608CD03F4	C:\Afta_Detector_v1.6\Hash-Files.txt
MD5	0F1B33952D5CB27FFC0FCBEF732E6298	C:\Afta_Detector_v1.6\Help.pdf

شکل ۱: خروجی دستور محاسبه Hash فایل

- b. مقدار خروجی Hash محاسبه شده با جدول زیر مقایسه شود.

جدول ۱: مقدار Hash فایل شناساگر افتا

نام فایل	مقدار Hash
Afta Detector v1.6.exe	A1A268C7EDF122D89587E2D692435DFC

- ۲- در صورت تطبیق کامل مقدار محاسبه شده، ادامه مراحل انجام شود. در غیر اینصورت به حوزه مربوطه اطلاع رسانی شود.
- ۳- فایل AFTA Detector V1.6.exe با دسترسی Run as administrator اجرا شود.
- ۴- با انتخاب گزینه "انتخاب مسیر"، مسیر مدنظر انتخاب شود. مسیر پیشنهادی شامل موارد زیر است:
- مسیر اصلی سیستم عامل (مانند C:\)
 - مسیر اصلی سرویس IIS و مسیری که محتوای وب در آن قرار دارد.
- ۵- دکمه "اجرا" انتخاب شود. پس از اتمام جستجو، ۲ فایل با فرمت csv و zip و با نام result ایجاد می‌گردد. فایل result.csv جهت مشاهده خروجی پویشرگ توسط سازمان است.
- ۶- فایل result.zip توسط ایمیل سازمانی و یا داخلی به آدرس ایمیل csirt@aftasec.ir ارسال گردد. در عنوان ایمیل ارسالی درج نام سازمان الزامی است.