Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-02 11:16:04 UTC

Tool: FOXGRABBER

Names	FOXGRABBER
Category	Malware
Type	Credential stealer
Description	(FireEye) FOXGRABBER is a command line utility used to harvest FireFox credential files from remote systems. It contains the PDB path: C:\Users\kolobko\Source\Repos\grabff\obj\Debug\grabff.pdb. FOXGRABBER has also been observed in DarkSide ransomware intrusions.
Information	<https://www.fireeye.com/blog/threat-research/2021/04/unc2447-sombrat-and-fivehands-ransomware-sophisticated-financial-threat.html>

Last change to this tool card: 15 May 2021

Download this tool card in JSON format

All groups using tool FOXGRABBER

Changed	Name	Country	Observed	
APT groups				
	Carbanak, Anunak		2013-Apr 2023	
	UNC2447	[Unknown]	2020	

2 groups listed (2 APT, 0 other, 0 unknown)