Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 16:27:02 UTC

Tool: HALFBAKED

Names	HALFBAKED VB Flash
Category	Malware
Type	Reconnaissance, Backdoor, Info stealer
Description	(FireEye) The HALFBAKED malware family consists of multiple components designed to establish and maintain a foothold in victim networks, with the ultimate goal of gaining access to sensitive financial information. This version of HALFBAKED connects to the following C2 server: hxxp://198[.]100.119.6:80/cd hxxp://198[.]100.119.6:443/cd hxxp://198[.]100.119.6:8080/cd This version of HALFBAKED listens for the following commands from the C2 server: • info: Sends victim machine information (OS, Processor, BIOS and running processes) using WMI queries • processList: Send list of process running • screenshot: Takes screen shot of victim machine (using 58d2a83f777688.78384945.ps1) • runvbs: Executes a VB script • runexe: Executes EXE file • runps1: Executes PowerShell script • delete: Delete the specified file • update: Update the specified file
Information	<https://www.fireeye.com/blog/threat-research/2017/04/fin7-phishing-lnk.html>
MITRE ATT&CK	<https://attack.mitre.org/software/S0151/>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/vbs.halfbaked>
AlienVault OTX	<https://otx.alienvault.com/browse/pulses?q=tag:halfbaked>

Last change to this tool card: 23 April 2020

Download this tool card in JSON format

All groups using tool HALFBAKED

Changed	Name	Country	Observed	
APT groups				
	Carbanak, Anunak		2013-Apr 2023	
	FIN7		2013-Jul 2024	

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

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=7c520285-abe4-4a29-afc3-47ae713edd82