Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 20:47:16 UTC

Tool: BISTROMATH

Names	BISTROMATH
Category	Malware
Type	Backdoor, Info stealer
Description	(US-CERT) This report looks at multiple versions of a full-featured RAT implant executable and multiple versions of the CAgent11 GUI implant controller/builder. These samples performs simple XOR network encoding and are capable of many features including conducting system surveys, file upload/download, process and command execution, and monitoring the microphone, clipboard, and the screen. The GUI controllers allow interaction with the implant as well as the option to dynamically build new implants with customized options. The implants are loaded with a trojanized executable containing a fake bitmap which decodes into shellcode which loads the embedded implant.
Information	<https://www.us-cert.gov/ncas/analysis-reports/ar20-045a>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.bistromath>
AlienVault OTX	<https://otx.alienvault.com/browse/pulses?q=tag:BISTROMATH>

Last change to this tool card: 24 April 2021

Download this tool card in JSON format

All groups using tool BISTROMATH

Changed	Name	Country	Observed	
APT groups				
	Lazarus Group, Hidden Cobra, Labyrinth Chollima		2007-May 2025	

1 group listed (1 APT, 0 other, 0 unknown)

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=63e35035-f269-4642-8038-f85b09fbe251