Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-06 00:44:51 UTC

Home > List all groups > List all tools > List all groups using tool BLUEAGAVE

Tool: BLUEAGAVE

Names	BLUEAGAVE
Category	Malware
Type	Backdoor
Description	(Mandiant) FIN13 has also extensively deployed the PowerShell passive backdoor BLUEAGAVE on target hosts when establishing an initial foothold in an environment. BLUEAGAVE utilizes the HttpListener .NET class to establish a local HTTP server on high ephemeral ports (65510-65512). The backdoor listens for incoming HTTP requests to the root URI / on the established port, parses the HTTP request, and executes the URL encoded data stored within the 'kmd' variable of the request via the Windows Command Prompt (cmd.exe). The output of this command is then sent back to the operator in the body of the HTTP response. In addition, Mandiant has identified a Perl version of BLUEAGAVE which allows FIN13 to establish a foothold on Linux systems.
Information	<https://www.mandiant.com/resources/fin13-cybercriminal-mexico>

Last change to this tool card: 26 December 2021

Download this tool card in JSON format

All groups using tool BLUEAGAVE

Changed	Name	Country	Observed	
APT groups				
	FIN13	[Unknown]	2016	

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