Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-06 03:27:16 UTC

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

Tool: CostaBricks

Names	CostaBricks
Category	Malware
Type	Loader
Description	(BlackBerry) The loader used with 32-bit backdoors is more technically compelling. It implements a simple custom-built virtual machine mechanism that will execute an embedded bytecode to decode and inject the payload into memory. This attempt at obfuscation, although not new, is rather uncommon in relation to targeted attacks. Code virtualization has been most prevalent in commercial software protectors which use much more advanced solutions; simpler virtual machines are sometimes also featured in off-the-shelf malicious packers used by widespread financial crimeware. This particular implementation, however, is unique (there are just a handful of samples in the public domain) and seems to be used only with SombRAT payloads – which makes us believe it is a custom-built tool that is private to the attackers.
Information	<https://blogs.blackberry.com/en/2020/11/the-costaricto-campaign-cyber-espionage-outsourced>
MITRE ATT&CK	<https://attack.mitre.org/software/S0614/>

Last change to this tool card: 30 December 2022

Download this tool card in JSON format

All groups using tool CostaBricks

Changed	Name	Country	Observed	
APT groups				
	CostaRicto	[Unknown]	2017	

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

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=3d97f5f2-fffb-4fac-9248-9c8f531d8cc7