Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-06 00:17:41 UTC

Tool: LONGRUN

Names	LONGRUN
Category	Malware
Type	Backdoor, Info stealer, Exfiltration
Description	LONGRUN is a backdoor designed to communicate with a hard-coded IP address and provide the attackers with a custom interactive shell. It supports file uploads and downloads, and executing arbitrary commands on the compromised machine. When LONGRUN executes, it first loads configuration data stored as an obfuscated string inside the PE resource section. The distinctive string thequickbrownfxjmpsvalzydg is used as part of the input to the decoding algorithm. When the configuration data string is decoded it is parsed and treated as an IP and port number. The malware then connects to the host and begins interacting with it over a custom protocol.
Information	<http://contagiodump.blogspot.com/2013/03/mandiant-apt1-samples-categorized-by.html>

Last change to this tool card: 20 April 2020

Download this tool card in JSON format

All groups using tool LONGRUN

Changed	Name	Country	Observed	
APT groups				
	Comment Crew, APT 1		2006-May 2018	

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