Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-06 03:09:09 UTC

Tool: Godlua

Names	Godlua
Category	Malware
Type	Backdoor, Downloader
Description	(Qihoo 360) The file itself is a Lua-based Backdoor, we named it Godlua Backdoor as the Lua byte-code file loaded by this sample has a magic number of “God”. Godlua Backdoor has a redundant communication mechanism for C2 connection, a combination of hardcoded dns name, Pastebin.com, GitHub.com as well as DNS TXT are used to store the C2 address, which is not something we see often. At the same time, it uses HTTPS to download Lua byte-code files, and uses DNS over HTTPS to get the C2 name to ensure secure communication between the bots, the Web Server and the C2. We noticed that there are already 2 versions of Godlua Backdoor and there are ongoing updates. We also observed that attackers has been using Lua command to run Lua code dynamically and initiate HTTP Flood attacks targeting some websites.
Information	<https://blog.netlab.360.com/an-analysis-of-godlua-backdoor-en/>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/elf.godlua>

Last change to this tool card: 24 April 2021

Download this tool card in JSON format

All groups using tool Godlua

Changed	Name	Country	Observed	
Other groups				
	Rocke, Iron Group		2018-Apr 2021	

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