# New Godlua Malware Evades Traffic Monitoring via DNS over HTTPS

By Sergiu Gatlan

Published: 2019-07-03 · Archived: 2026-04-05 13:16:05 UTC

A Lua-based backdoor malware capable of targeting both Linux and Windows users while securing its communication channels via DNS over HTTPS (DoH) was discovered by researchers at Network Security Research Lab of Qihoo 360.

By using DoH to encapsulate the communication channels between command-and-control servers, the infected machines, and the attacker-controlled servers within HTTPS requests, the malware dubbed Godlua manages to block researchers from analyzing its traffic.

Godlua's main function seems to be that of a DDoS bot and it was already seen in action when its masters launched an HTTP flood attack against the liuxiaobei[.]com domain, as observed by the Qihoo 360 researchers.


DIE LINKE.
0:00

Until now, two samples of the Godlua backdoor have been found, with one of them targeting only Linux boxes (version 201811051556) while the other is also able to infect Windows computers, has more built-in commands, and supports more CPU architectures (version 20190415103713 ~ 2019062117473)

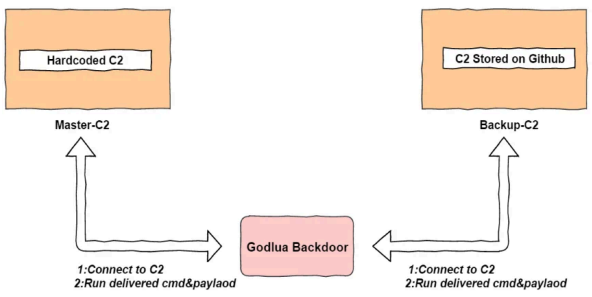
| Version | Platform | CPU Architecture | Control Implementation | Command |
|---|---|---|---|---|
| 201811051556 | Linux | x86, x86-64 | C | cmd_call,cmd_shell |
| 20190415103713 ~ 20190621174731 | Linux, Windows | x86, x86-64, arm, mipsel | Lua | lua,shell,shell2,proxy,upgrade |

**Godlua versions**

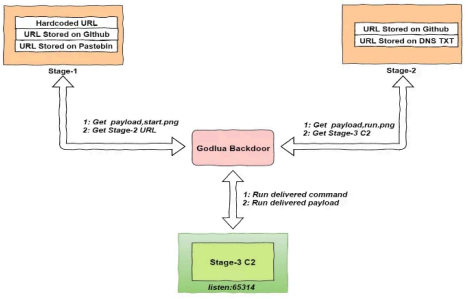
While Godlua version 201811051556 is currently not being updated anymore, the second sample is actively being updated by its developers which might be the reason behind its extra features and multi-platform support.

The version that focuses only the Linux platform can receive only two types of instructions from its command and control (C2) server, allowing the attackers to run custom files and to execute Linux commands.

The second variant comes with support for five C2 commands and it "downloads many Lua scripts when executing, and the scripts can be broken down to three categories: execute, auxiliary, and attack."




Version 1 C2 redundant mechanism




Version 2 C2 redundant mechanism

Even though a number of Linux machines were found to have been infected with the Godlua backdoor using a Confluence exploit for CVE-2019-3396, the Qihoo 360 researchers are still looking for additional infection vectors.

## DNS over HTTPS used to secure C2 traffic

Although quite new, the DoH protocol is a proposed standard as of October 2018 and it is already supported by quite a long list of publicly available DNS servers, as well as web browsers like Google Chrome and Mozilla Firefox.

DoH increases DNS queries' privacy by enveloping them within HTTPS communication channels which effectively blocks both eavesdropping and DNS data manipulation by third parties between the client and the DNS server.

DNS over HTTPS Request

**DNS over HTTPS Request**

By abusing the DoH protocol, the Godlua malware hides the URLs of the C2 servers used during the later stages of the infection process from prying eyes, URLs that it gets from the DNS TXT record of a domain it collects during the first stage.

Godlua is the first observed malware that makes use of the DNS over HTTPS protocol to conceal part of its C2 infrastructure from analysts and anti-malware analysis tools according to Cisco Talos threat researcher Nick Biasini.

More details on how this malware communicates with its C2 infrastructure and indicators of compromise (IOCs) are provided by the Qihoo 360's research team in their Godlua backdoor analysis.

---

Source: https://www.bleepingcomputer.com/news/security/new-godlua-malware-evades-traffic-monitoring-via-dns-over-https/