LevelBlue - Open Threat Exchange

By caralin0702

Archived: 2026-04-05 12:37:20 UTC

- Created 7 years ago
- Modified 6 years ago by AlienVault
- Public
- TLP: White

FileHash-MD5: 5 | **FileHash-SHA1:** 1 | **FileHash-SHA256:** 1 | **URL:** 2 | **Domain:** 9 | **Hostname:** 1

During the period of March to May 2019, Morphisec Labs observed a new, highly sophisticated variant of the ShellTea / PunchBuggy backdoor malware that attempted to infiltrate a number of machines within the network of a customer in the hotel-entertainment industry. It is believed that the malware was deployed as a result of several phishing attempts.

Source: https://otx.alienvault.com/browse/pulses?q=tag:PunchBuggy