

# LevelBlue - Open Threat Exchange

By TheNewRaikage

Archived: 2026-04-05 12:40:40 UTC



**[Threat Research | FireEye Inc](#)**

Find out more about FireEye.com, the world's leading cyber security company, which provides security services to more than 1.5 million customers across the globe, and offers a wide range of products and services.

- 17 Subscribers



- 95 Subscribers



## [U.S. Government Targeted in Spear-Phishing Attacks](#)

**FileHash-SHA256:** 19 | **Email:** 2 | **Hostname:** 5

Between July and October 2019, Unit 42 observed several malware families typically associated with the Konni Group used to primarily target a US government agency, using the ongoing and heightened geopolitical relations issues surrounding North Korea to lure targets into opening malicious email attachments. The malware families used in this campaign consisted mainly of malicious documents featuring CARROTBAT downloaders with SYSCON payloads, but also included a new malware downloader Unit 42 has dubbed CARROTBALL.

- 373,890 Subscribers

---

Source: <https://otx.alienvault.com/browse/pulses?q=tag:carrotball>