



## October 2023

---

Updates released in October of 2023 to Cisco cloud-based machine learning global threat alerts:

- [Additional Threat Detections, on page 1](#)

### Additional Threat Detections

We've added a new threat detection to our portfolio:

- DarkGate Loader

We've also updated indicators for our existing threat detections.

#### **DarkGate Loader**

DarkGate Loader, also called MehCrypter, is a variant of QakBot. The loader is distributed by a phishing campaign ([T1566](#)) which abuses Microsoft Teams messages to send malicious attachments that install the DarkGate Loader. Once the malware is executed on the endpoint ([T1204.002](#)), there can be various malicious activities like remote access ([T1219](#)), cryptocurrency mining ([T1496](#)), keylogging ([T1056.001](#)), clipboard stealing, and information stealing.

To see if Dark Gate Loader has been detected in your environment, click [DarkGate Loader Threat Detail](#) to view its details in global threat alerts.

