FILTER

Alphabetical

REQUEST DEMO

GOLD SWATHMORE

Objectives
Botnet Operation and Sales, Financial gain

Aliases
Lunar Spider (CrowdStrike)

Tools

Cobalt Strike, GlobeImposter, Gozi, Gozi Trojan, IcedID, TrickBot, TrickBot

---

GOLD SWATHMORE is a financially motivated cybercriminal threat group that operates the IcedID (aka BokBot) malware since April 2017. This group previously operated the Catch malware (also known as Gozi Neverquest or Vawtrak) until the arrest of that malware's principal author in January 2017. IcedID, which its authors refer to internally as Anubis, was originally designed to facilitate financial fraud but is now used near exclusively to provide initial access to networks for post-intrusion style ransomware deployments. IcedID is modular malware that can retrieve additional plugins, such as those that provide a backconnect proxy or VNC access, to extend its capabilities. Typically new infections are immediately instructed to execute nearly a dozen system and network reconnaissance commands and transmit their output to C2 servers. This information is then used by GOLD SWATHMORE and its partners to select potential high-value targets and may prompt the execution of additional malware such as Cobalt Strike Beacon.

READ LESS