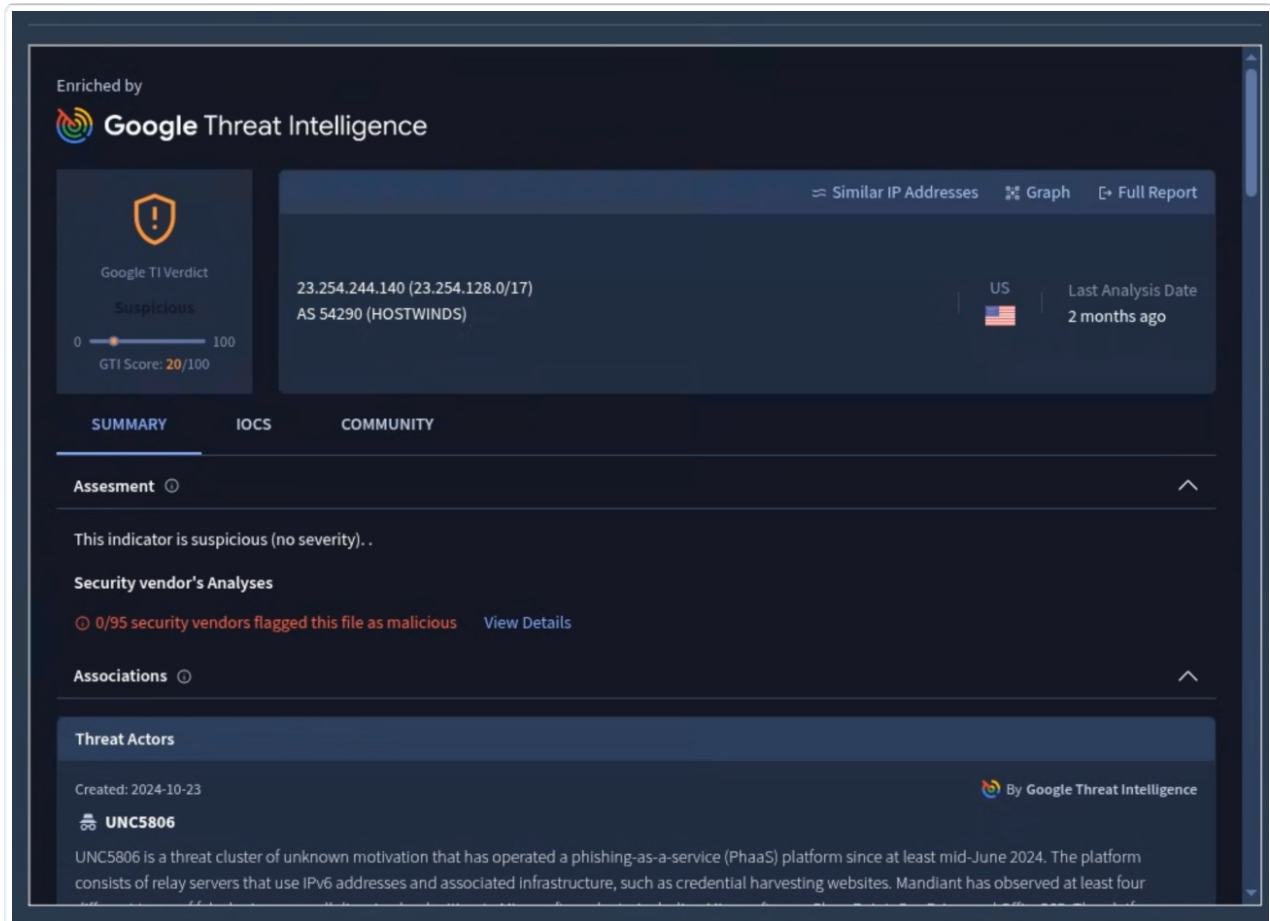


OCTOBER 9, 2025 MANDIANT THREAT DEFENSE RELEASE

Investigations contain links to Google Threat Intelligence context for entities (IP addresses, Domains, URLs, and SHA256 file hashes). This information is located in the evidence section of an Investigation and applies to all Investigations. In the Managed Defense portal, click the Google Threat Intelligence icon next to an entity to display a summary of the threat actor, malware family, and verdicts from engine vendors and sandboxes.

For more information, see [Working with Investigations \(https://docs.mandiant.com/home/mh-working-with-investigations\)](https://docs.mandiant.com/home/mh-working-with-investigations).



The screenshot displays the Google Threat Intelligence enrichment interface. At the top, it is labeled "Enriched by Google Threat Intelligence". The main content area shows a "Google TI Verdict" of "Suspicious" with a "GTI Score: 20/100". The IP address "23.254.244.140 (23.254.128.0/17)" is associated with "AS 54290 (HOSTWINDS)" and is located in the "US". The "Last Analysis Date" is "2 months ago". Below this, there are tabs for "SUMMARY", "IOCS", and "COMMUNITY". The "Assesment" section indicates "This indicator is suspicious (no severity)". The "Security vendor's Analyses" section shows "0/95 security vendors flagged this file as malicious". The "Associations" section is currently empty. The "Threat Actors" section identifies "UNC5806" as a threat cluster of unknown motivation that has operated a phishing-as-a-service (PhaaS) platform since at least mid-June 2024. The platform consists of relay servers that use IPv6 addresses and associated infrastructure, such as credential harvesting websites. Mandiant has observed at least four...