Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 13:50:23 UTC

Tool: GoldenEagle

Names	GoldenEagle
Category	Malware
Type	Reconnaissance, Backdoor, Info stealer, Exfiltration
Description	(Lookout) Among the aspects that make GoldenEagle particularly interesting is that the earliest test samples of this family appeared as early as 2012, making it one of the longest-running surveillanceware families we have observed to date. GoldenEagle code has been identified in an impressively large and diverse set of applications over the years. These samples can be divided into two major groups: those that exfiltrate data via HTTP and those that exfiltrate data via SMTP, i.e., by sending exfiltrated data in file attachments of emails to an attacker-controlled mailbox using innocuous-looking subjects and mail body content. The latter technique, while appearing in the early stages of GoldenEagle development, has resurfaced in samples signed and analysed in May 2020.
Information	<https://www.lookout.com/documents/threat-reports/us/lookout-uyghur-malware-tr-us.pdf>
MITRE ATT&CK	<https://attack.mitre.org/software/S0551/>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/apk.goldeneagle>
AlienVault OTX	<https://otx.alienvault.com/browse/pulses?q=tag:GoldenEagle>

Last change to this tool card: 30 December 2022

Download this tool card in JSON format

All groups using tool GoldenEagle

Changed	Name	Country	Observed
APT groups			

	Ke3chang, Vixen Panda, APT 15, GREF, Playful Dragon		2010-Oct 2024	

1 group listed (1 APT, 0 other, 0 unknown)

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=b36d7de7-3c91-4019-96b1-196c144c1e9f