Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 20:04:06 UTC

Description(Group-IB) In mid-September 2023, during routine monitoring of adversary infrastructure, Group-IB's Threat Intelligence unit identified a command and control (C&C) server that was hosting several tools. Notably, none were custom-made. The entire toolset was based on publicly available open-source instruments used for pentesting purposes. After examining the toolset in more detail, it became clear that the tools were most likely associated with a threat actor executing one of the oldest attack methods: SQL injections.

While delving deeper into the malicious infrastructure, Group-IB researchers identified the threat actor's first targets, predominantly linked to the gambling industry. This prompted the Threat Intelligence unit to name the threat actor GambleForce (tracked under the name EagleStrike GambleForce in Group-IB's Threat Intelligence Platform). Since it appeared in September 2023, GambleForce has targeted more than 20 websites (government, gambling, retail, and travel) in Australia, China, Indonesia, the Philippines, India, South Korea, Thailand, and Brazil.

Despite using very basic attack methods, the threat actor has managed to successfully attack six companies in Australia (travel), Indonesia (travel, retail), the Philippines (government), and South Korea (gambling), which shows just how vulnerable many organizations are against rudimentary but clearly dangerous SQL injection attacks.

In some instances, the attackers stopped after performing reconnaissance. In other cases, they successfully extracted user databases containing logins and hashed passwords, along with lists of tables from accessible databases. Rather than looking for specific data, the threat actor attempts to exfiltrate any available piece of information within targeted databases, such as hashed and plain text user credentials. What the group does with the stolen data remains unknown so far.
