Trickbot in Light of Trickleaks Data

By Vincas Čižiūnas

Published: 2023-08-30 · Archived: 2026-04-06 00:59:55 UTC

EXECUTIVE SUMMARY

Attribution work by its very nature is challenging and dependent on the timeliness and accuracy the data researchers initially have on the unknown actor. The challenge is to increase confidence in the accuracy of any additional selectors by corroborating them with the primary selector and other data points found during an investigation.

In February 2023, the US Treasury Department and Secret Service named Vitaly Kovalev as the ransomware actor user of the handle “bentley,” based on activity using that handle in 2009 and 2010.

In May 2022, a Twitter account known as @trickleaks released chat logs claiming to be from the ransomware actor group Trickbot, along with several dossiers profiling the individual actors, including one using the handle “bentley.” The report that follows will provide an alternate possibility of the true identity for the threat actor known as “bentley” based on the more recent TrickLeaks release. Nisos examined chat logs, dated June 2020 to November 2021, from the Trickleaks breach data set to identify any ties between Trickbot actors and the Russian government. For context, similar to ContiLeaks, TrickLeaks provided intimate details about the TrickBot gang; however, where the majority of the data contained with the ContiLeaks disclosure focused on source code, the TrickLeaks disclosure included identity and account related personal information of the actual Trickbot members. While analysts did not identify a direct link between Trickbot actors and the Russian government, multiple Trickbot actors, including “silver,” “manuel” (aka “bentley,” “max17,” and “volhvb”), and “angelo” likely believed that the FSB and/or SVR supported them and that their leadership had FSB ties.

Additionally, actor bentley is believed to be a senior member of the Trickbot group performing human resources-related roles, such as payments for the group, and subscriptions needed to conduct ransomware attacks. He was also charged with “crypting” the group’s malware—ensuring that it goes undetected by all or at least most antivirus products on the market. Nisos determined that bentley, who revealed his username as volhvb@exploit[.]im for the popular exploit.im jabber service, is currently identifiable as Maksim Sergeevich Galochkin. Nisos further identified that Galochkin changed his name from Maksim Sergeevich Sipkin, and that he has significant financial debt as of 2022. In 2010, Sipkin was an active member of the “Solidarity” in Khakassia, a group associated with the assassinated Russian opposition leader, Boris Nemtsov.

Nisos cannot rule out the possibility that both individuals were users of the handle at different times.
