Trickbot in Light of Trickleaks Data

nisos.com/research/trickbot-trickleaks-data-analysis/

August 30, 2023

Threat Analysis

by Vincas Čižiūnas | Aug 30, 2023 | Blog, Research

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.

OVERVIEW

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. ***(See source 1 and 2 in appendix)***

In May 2022, the Twitter handle @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.” Nisos examined chat logs that were leaked by the trickleaks Twitter account for ties between Trickbot and the Russian Government.

Trickbot actor bentley is 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. ***(See source 3 and 4 in appendix)***

REACTION TO OCTOBER 2021 ARRESTS

In October 2021, alleged Trickbot actors Alla Witte and Vladimir Dunaev appeared in a US Federal Court in the Northern District of Ohio. After subsequent media reports on 1 November, some of the actors discovered that they were locked out of some of the group’s cryptocurrency wallets, presumably due to blacklisting. (See source 5 in appendix) Two of the actors, brooks—who is involved in systems testing—and silver (see source 6 in appendix)—an apparent senior member of the gang—engaged in a conversation on their chat platform regarding the news.

Brooks expressed his fear that the crypto-wallet failures were due to exposure presumably from recent arrests. Silver reassured brooks that their key leaders have not been exposed and that while there “will be problems..[the Russian government] will excuse” them. The Russian Ministry of Internal Affairs will expect a payoff, but that the other government agencies, the FSB and SVR are “for…[them] or neutral.”

STERN AND THE FSB

Later in the month, Trickbot actors manuel ***(see source 7 in appendix)*** and angelo discussed Stern, often referred to simply as "S," who is the leader of the Conti and Trickbot ransomware gang. Specifically, they discussed their leader Stern's behavior, with angelo noting that Stern did not seem to be handling the stress. ***(See source 8 in appendix)*** Manuel provided some context, indicating that he thought that their boss "has been doing this since 2000." Angelo agreed that he was "the link between us and the ranks/head of department type at FSB," to which manuel agreed and proposed the possibility that Stern may just have been a "target," an operative in a controlled relationship with the organization. Their conversation then turned toward working harder to keep their boss happy.

JABBER ADDRESS FOR BENTLEY

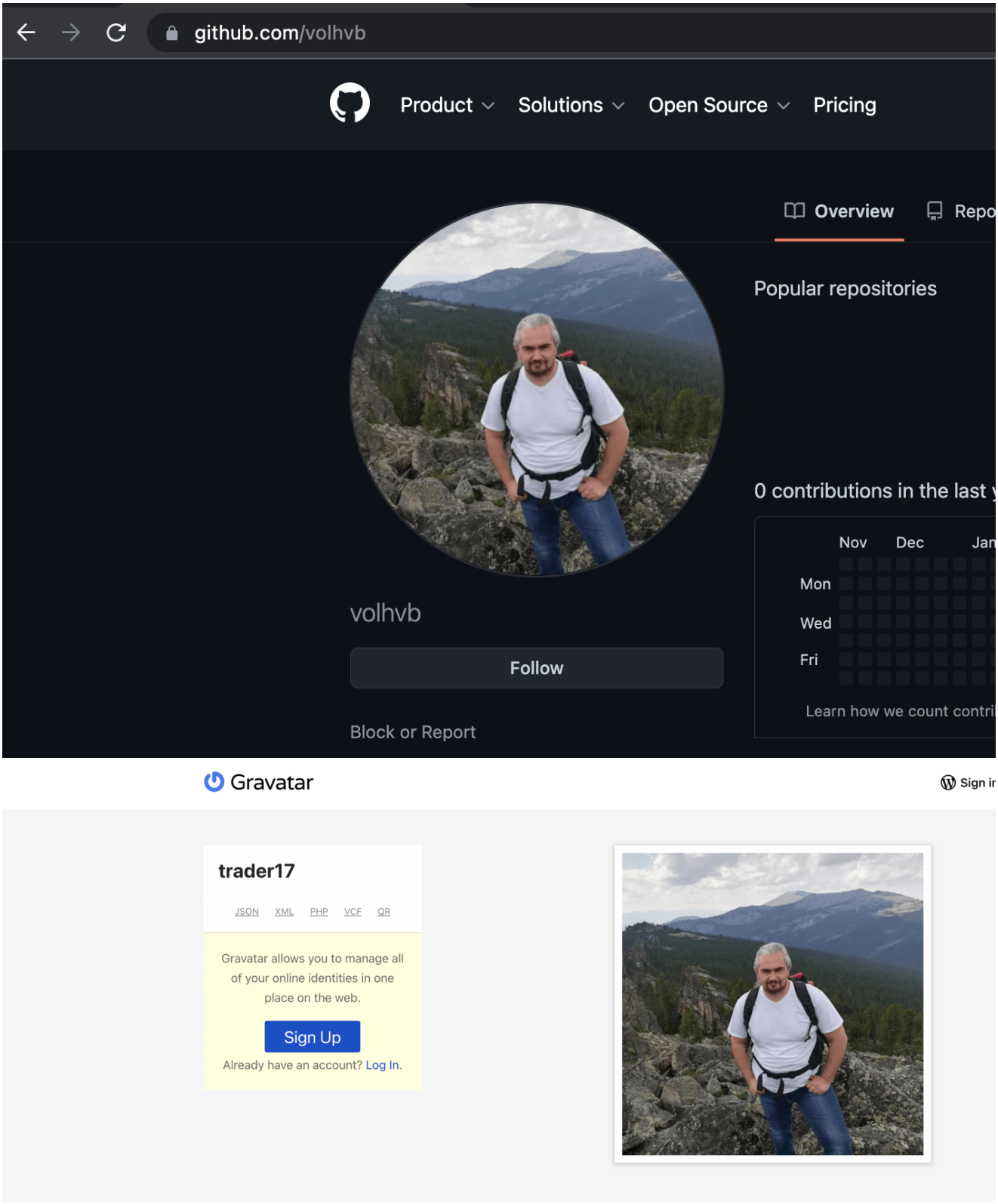
On 22 June 2020, an actor named "defender" requested an external jabber address of actor bentley. Bentley provided the username volhvb@exploit.im. Nisos identified a gmail address, volhvb@gmail[.]com that belongs to a Степка Розин (Stepka Rosin). This name is associated with a YouTube user Mrvolhvb, whose videos primarily feature Russian cryptocurrency market trading. Mrvolhvb posted a video where he is logged into his jabber volhvb account using the raidcall jabber client.

Picture 1: volhvb logged into raidcall Jabber client ***(See source 9 in appendix)***

MAKSIM SERGEEVICH GALOCHKIN

The volhvb@gmail.com address has an adobe.com account that is associated with a phone number that ends in 58. Nisos data sources further tie this email address to Russian mobile phone number +79134448958 and the name Maksim Sergeevich Galochkin. In addition, this email address is associated with a github account, volhvb, that contains a picture of Mr. Galochkin.

Nisos data sources also tie email volhvb@live.ru to Galochkin and the phone number +79134448958. This email was used to register gravatar account http://en.gravatar.com/trader17 with a photo that matches the profile image on his github.



Pictures 2 & 3: Mr. Galochkin's github and gravatar accounts

To obtain the complete research report, including endnotes, please click the button below.

DOWNLOAD PDF

DISCLAIMER:

The reporting contained herein from the Nisos research organization consists of analysis reflecting assessments of probability and levels of confidence and should not necessarily be construed as fact. All content is provided on an as-is basis and does not constitute professional advice, and its accuracy reflects the reliability, timeliness, authority, and relevancy of the sourcing underlying those analytic assessments.

About Nisos®

Nisos is The Managed Intelligence Company®. Our analyst-led intel investigations, assessments, and monitoring services empower your security, intelligence and trust and safety teams. We provide accurate, customized intelligence that guides your security and risk decisions – protecting your organization, assets, and people. Learn more at nisos.com.