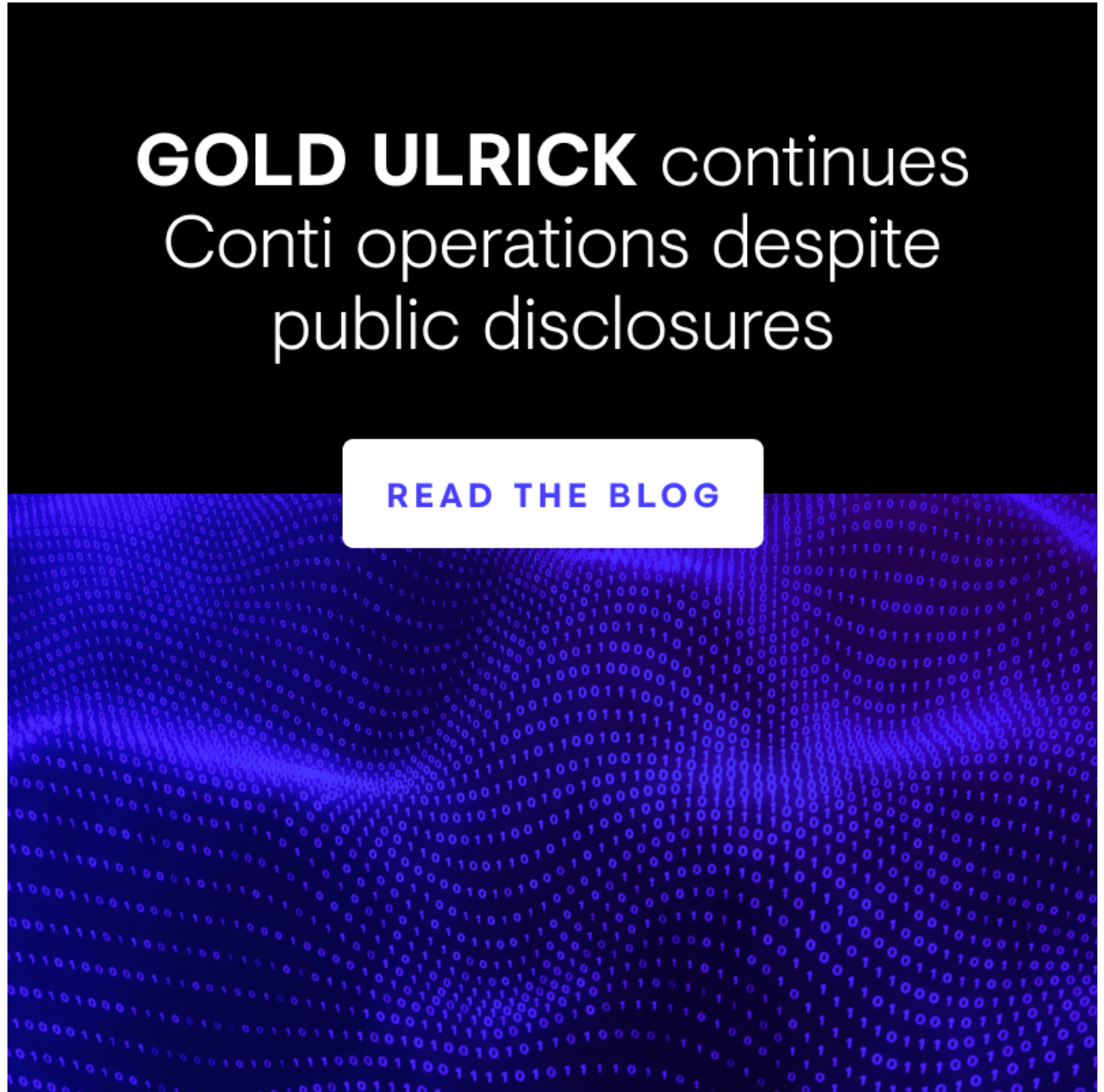


GOLD ULRICK Continues Conti Operations Despite Public Disclosures

secureworks.com/blog/gold-ulrick-continues-conti-operations-despite-public-disclosures

Counter Threat Unit Research Team



GOLD ULRICK continues
Conti operations despite
public disclosures

[READ THE BLOG](#)

Secureworks® Counter Threat Unit™ (CTU) researchers analyzed how the GOLD ULRICK threat group, which operates the Conti name-and-shame ransomware scheme, has adapted in response to the public disclosure of a significant amount of GOLD ULRICK communications and operational details. CTU™ analysis indicates that the group is returning to the levels of activity that represented a peak in 2021.

The Conti leak site listed an average of 43 victims per month in 2021. Despite a drop following the Colonial Pipeline attack and a peak of 95 victims listed in November, the rate of naming victims was fairly consistent. The decreased activity in December 2021 and January 2022 across all name-and-shame ransomware groups was likely due to a holiday break. The number of victims added to the Conti leak site increased in February 2022. On February 27, the @ContiLeaks Twitter persona began leaking GOLD ULRICK data and communications. Despite these public disclosures, the number of Conti victims posted in March surged to the second-highest monthly total since January 2021 (see Figure 1).

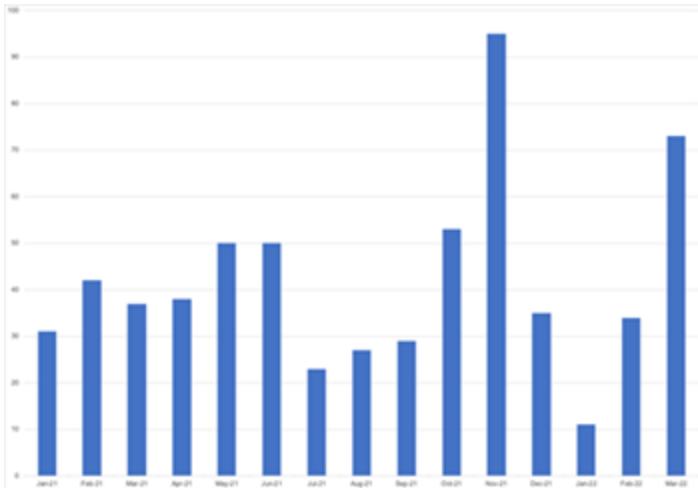


Figure 1. Number of new victims added to the Conti leak site per month between January 2021 and March 2022. (Source: Secureworks)

Although these types of leaks could have prompted some threat groups to modify their communication methods or tooling, GOLD ULRICK appears to have continued and even increased the tempo of its operations without disruption. GOLD ULRICK member 'Jordan Conti' confirmed this continuation and the minimal impact of the disclosures in a March 31, 2022 post on the RAMP underground forum (see Figure 2). CTU researchers previously observed this persona advertising Conti, providing updates on takedown efforts, and recruiting affiliates.

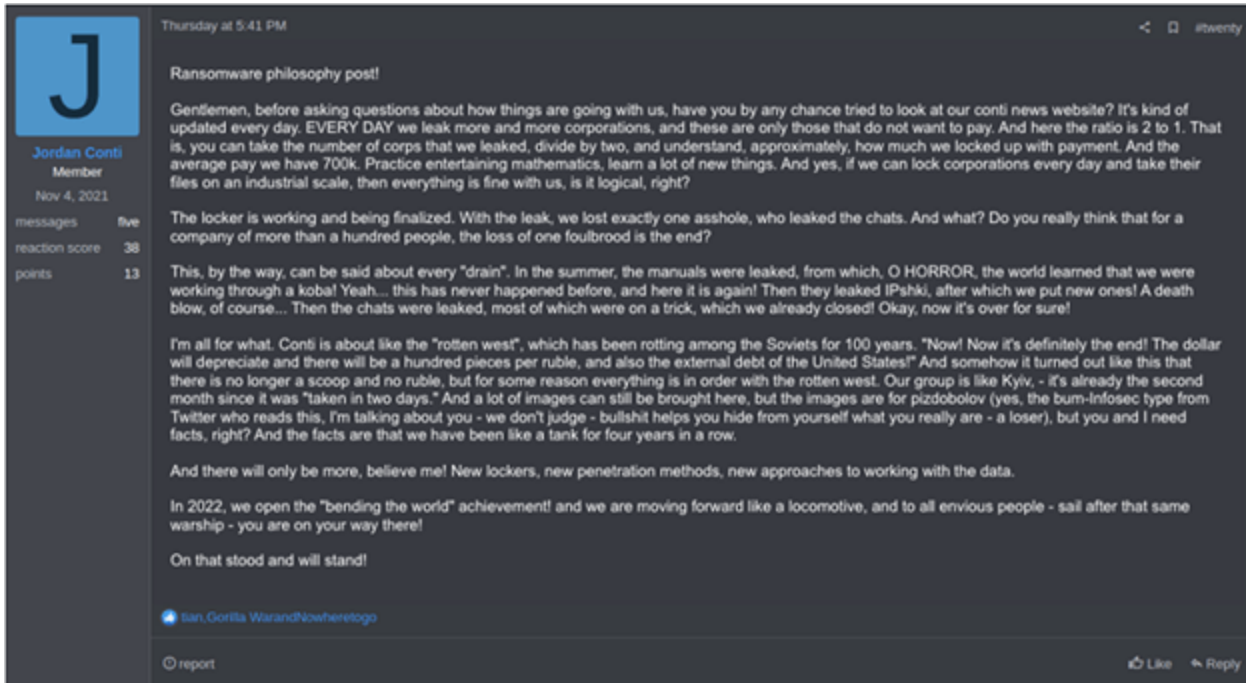


Figure 2. RAMP forum post by a GOLD ULRICK member (translated from Russian). (Source: Secureworks)

The March 31 post claims that the Conti leak site only lists victims that have not paid the ransom and that twice that number have been compromised. It suggests that Conti has a 50% payment success rate with an average payout of '700k'. The currency is not specified but is likely to be U.S. dollars. CTU researchers are unable to verify these claims, but it is reasonable to assume that the leak site does not list all victims.

'Jordan Conti' indicates that GOLD ULRICK continues to evolve its ransomware, intrusion methods, and approaches to working with data. The Conti leak site added 11 victims in the first four days of April. If GOLD ULRICK operations continue at that pace, the group will continue to pose one of the most significant cybercrime threats to organizations globally.

To learn more about how ransomware groups adapt, read our [Ransomware Evolution](#) analysis and watch our [Ransomware Trends: The Evolution of Threat](#) webinar.

If you need urgent assistance with an incident, contact the [Secureworks Incident Response team](#).