An Inside Look at the Conti Group | Deep Instinct

Published: 2023-12-12 · Archived: 2026-04-06 00:33:53 UTC

Ransomware is big business. In 2023, the average data breach cost organizations $4.45 million, while the average ransomware attack cost $4.54 million. For threat actor groups, there's profit to be made. The most successful ransomware groups feature sophisticated operational structures, running like a business with HR, finance, and all the support teams you'd find in a legitimate enterprise.

One of the most notable and well-documented threat groups is Conti, a Russian-affiliated organization formed in the late 2010s. While just one of many active threat groups, it was unique in its size, success (some estimates peg their earnings in the billions), and structure.

The now famous Conti Leaks in February 2022, which came from disaffected Ukrainian affiliates following the Russian invasion of Ukraine, exposed its organizational structure and techniques, which precipitated its demise.

How did the Conti group come to be, and what made it so successful? In this blog post, we'll take a brief look inside Conti – who they are, how they started, their notable successes, and ultimately, how they dissolved.

Who Was Conti?

Although a direct link was never made explicit, Conti had clear ties to Russia. Group members corresponded in Russian and publicly supported Russian geopolitical interests, particularly after the initial invasion of Ukraine.

According to the U.S. State Department, the group was responsible for more than a thousand attacks against the U.S. and international critical infrastructures. It targeted organizations and governments across the globe, including the Taiwanese chip manufacturer Advantech, Scotland's Environmental Protection Agency, and Bank Indonesia, among others.

Early builds of Conti were observed in late 2019. However, the first public report of Conti's ransomware didn't appear until mid-2020. The group was born from what most would consider a natural progression of the "big game hunting" methodology of the "TrickBot group" (a.k.a., ITG23, WizardSpider, FIN12, GOLD BLACKBURN, and DEV-0193).

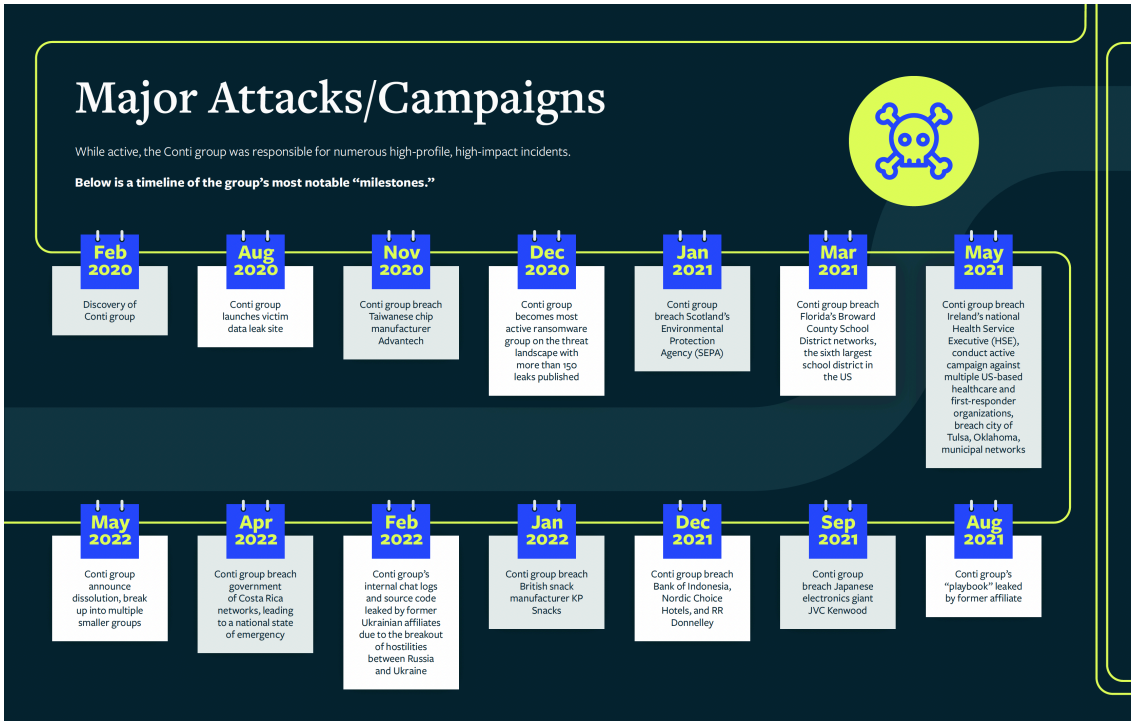

Figure 1-Conti Timeline

Conti's Tools and Techniques

Most ransomware can be categorized as fully automated or semi-automated. Fully automated ransomware carries out the infection, lateral movement, encryption, and exfiltration autonomously. In contrast, semi-automated ransomware requires an operator to carry out some of these steps using various tools. The Conti group belonged to the latter category.

Conti group's operators most often gained access to a victim's networks post-infection through malware operated by other groups with "friendly" relations to Conti, such as TrickBot, BazarLoader, Emotet, and IcedID.

Conti group's operators would hunt for and prioritize targets with elevated privileges, such as IT staff, system administrators, security professionals, or executives. Once a network was sufficiently compromised and access was obtained, Conti operators would shift their focus to data collection and exfiltration. After exfiltrating the data, the group delivered and executed its own malware, encrypting the victim's network.

Leaks That Lead to Conti's Eventual Downfall

When the group publicly declared its support for Russia in its war with Ukraine in February 2022, its troubles began. Conti's internal chat logs and source code were leaked by former Ukrainian affiliates after the breakout of hostilities between the two countries.

The published documents shed light on Conti's day-to-day operations. While most don't think of a ransomware threat group as a fully operating enterprise, that's exactly what the Conti Leaks showed. Based on research from Deep Instinct, Conti featured a robust organizational structure, with approximately 80-105 employees across HR, Finance, Reverse Engineering, Research, and OSINT teams.

The average monthly salary was $1,800 to $2,500 USD. Overall spending amounted to $140,000 to $165,000 for salaries and expenses per month, including transaction commissions and platform management (servers, proxy, recruitment). The evidence even showed that Conti, despite massive revenues, still suffered from cash flow issues in the same way you might see in any small tech startup.

Not only did the leaks reveal financials and team dynamics, but they also provided views into the group's "operational philosophy" including codified employee guides and working policies.

Pressure, Pursuit, and Breakup

Despite the leaks, Conti continued to orchestrate "numerous high-profile, high-impact incidents" after the onset of the Russia-Ukraine war. Unfortunately for Conti, the leaks put a target on their back and galvanized global law enforcement agencies to hunt its members.

Conti's attack against the Costa Rican government in April 2022 was the tipping point. This attack, which occurred roughly two weeks after a change of leadership, crippled Costa Rica's government and forced it to declare a state of emergency.

On August 11th, 2022, the U.S. State Department announced it had issued a $10 million USD reward for information that could lead to the identification of five key Conti members and their whereabouts.

With the February 2022 leak of internal chats and malware source code, the high-profile attack on the government of Costa Rica, and the considerable "bounty" on their heads from law enforcement, the group's leaders declared their "brand" had become "toxic" and ceased operations.

The Lessons from Conti

While Conti has disbanded, the bad actors and operators behind the group remain as active as ever, using increasingly sophisticated tools and techniques to attack vulnerable targets. Many of the group's former leaders and affiliates set up operations under new monikers, including HIVE, BlackBasta, BlackByte, AlphV/BlackCat, AvosLocker, Quantum, and Zeon/Royal Ransomware.

As they find success, their newly formed threat groups will grow, likely with improvements to their own security policies to prevent future leaks and stay under the radar from law enforcement authorities around the world.

As long as there is money to be made, threat actors will continue to build sophisticated operational structures to maximize profits. Competing threat groups have learned from Conti how to operate in an organized fashion, at scale, using their proven techniques and methodologies. The biggest lesson is clear: the next Conti is already out there.

Want to learn more about Conti, including member profiles and detailed internal chats? Check out our eBook, Threat Landscape Report Special Edition: Conti Group. In addition to an exploration of Conti's rise and eventual dissolution, its key figures, and major attacks, the eBook examines the exact tools and techniques Conti used to fuel their rise.
