Conti Ransomware Group Diaries, Part IV: Cryptocrime

Published: 2022-03-08 · Archived: 2026-04-05 16:27:05 UTC

Three stories here last week pored over several years' worth of internal chat records stolen from the **Conti** ransomware group, the most profitable ransomware gang in operation today. The candid messages revealed how Conti evaded law enforcement and intelligence agencies, what it was like on a typical day at the Conti office, and how Conti secured the digital weaponry used in their attacks. This final post on the Conti conversations explores different schemes that Conti pursued to invest in and steal cryptocurrencies.

When you're perhaps the most successful ransomware group around — Conti made $180 million last year in extortion payments, well more than any other crime group, according to **Chainalysis** — you tend to have a lot digital currency like Bitcoin.

This wealth allowed Conti to do things that regular investors couldn't — such as moving the price of cryptocurrencies in one direction or the other. Or building a cryptocurrency platform and seeding it with loads of ill-gotten crypto from phantom investors.

One Conti top manager — aptly-named "**Stern**" because he incessantly needled Conti underlings to complete their assigned tasks — was obsessed with the idea of creating his own crypto scheme for cross-platform blockchain applications.

"I'm addicted right now, I'm interested in trading, defi, blockchain, new projects," Stern told "**Bloodrush**" on Nov. 3, 2021. "Big companies have too many secrets that they hold on to, thinking that this is their main value, these patents and data."

In a discussion thread that spanned many months in Conti's internal chat room, Stern said the plan was to create their own crypto universe.

“Like Netherium, Polkadot and Binance smart chain, etc.,” Stern wrote. “Does anyone know more about this? Study the above systems, code, principles of work. To build our own, where it will already be possible to plug in NFT, DEFI, DEX and all the new trends that are and will be. For others to create their own coins, exchanges and projects on our system.”

It appears that Stern has been paying multiple developers to pursue the notion of building a peer-to-peer (P2P) based system for “smart contracts” — programs stored on a blockchain that run whenever predetermined conditions are met.

It’s unclear under what context the Conti gang was interested in smart contracts, but the idea of a ransomware group insisting on payments via smart contracts is not entirely new. In 2020, researchers from **Athens University School of Information Sciences and Technology** in Greece showed (PDF) how ransomware-as-a-service offerings might one day be executed through smart contracts.

Before that, **Jeffrey Ladish**, an information security consultant based in Oakland, Calif., penned a two-part analysis on why smart contracts will make ransomware more profitable.

“By using a smart contract, an operator can trustlessly sell their victims a decryption key for money,” Ladish wrote. “That is, a victim can send some money to a smart contract with a guarantee that they will either receive the decryption key to their data or get their money back. The victim does not have to trust the person who hacked their computer because they can verify that the smart contract will fairly handle the exchange.”

The Conti employee “**Van**” appears to have taken the lead on the P2P crypto platform, which he said was being developed using the Rust programming language.

“I am trying to make a p2p network in Rust,” Van told “**Demon**” on Feb. 19, 2022 [Demon appears to be one of Stern’s aliases]. “I’m sorting it out and have already started writing code.”

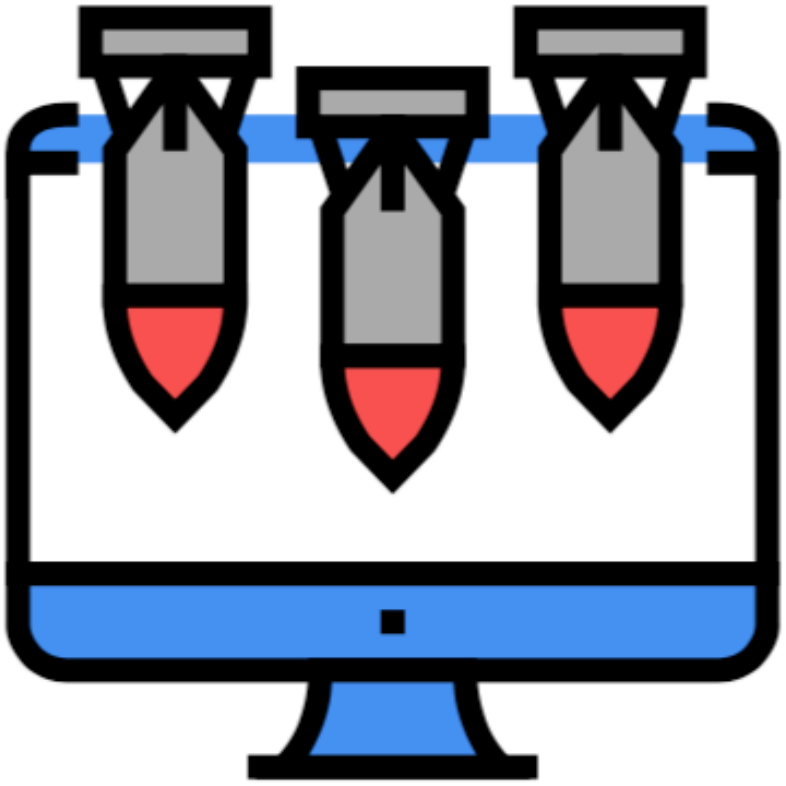
“It’s cool you like Rust,” Demon replied. “I think it will help us with smart contracts.”

Stern apparently believed in his crypto dreams so much that he sponsored a $100,000 article writing contest on the Russian language cybercrime forum Exploit, asking interested applicants to put forth various ideas for crypto platforms. Such contests are an easy way to buy intellectual property for ongoing projects, and they’re also effective recruiting tools for cybercriminal organizations.

“Cryptocurrency article contest! [100.000$],” wrote mid-level Conti manager “Mango,” to boss Stern, copying the title of the post on the Exploit forum. “What the hell are you doing there…”

A few days later Mango reports to Stern that he has “prepared everything for both the social network and articles for crypto contests.”

DISTRIBUTED DENIAL OF DISCORD?



On June 6, 2021, Conti underling "**Begemot**" pitched Stern on a scheme to rip off a bunch of people mining virtual currencies, by launching distributed denial-of-service (DDoS) attacks against a cryptocurrency mining pool.

"We find young forks on exchanges (those that can be mined), analyze their infrastructure," Begemot wrote.

Begemot continues:

> "Where are the servers, nodes, capitalization, etc. Find a place where crypto holders communicate (discord, etc.). Let's find out the IP of the node. Most likely it will be IPv6. We start ddosing. We fly into the chat that we found earlier and write that there are problems, the crypt is not displayed, operations are not carried out (because the crypt depends on mining, there will really be problems). Holders start to get nervous and withdraw the main balance. Crypto falls in price. We buy at a low price. We release ddos. Crypto grows again. We gain. Or a variant of a letter to the creators about the possibility of a ransom if they want the ddos to end. From the main problem points, this is the implementation of Ipv6 DDoS."

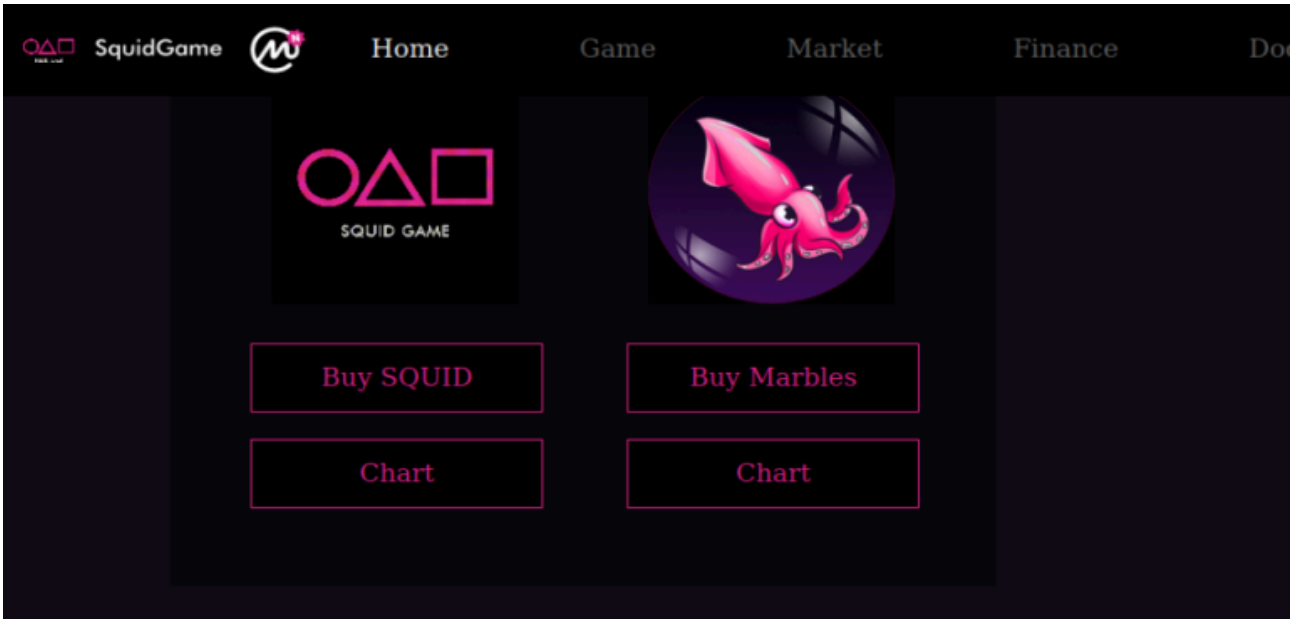
Stern replies that this is an excellent idea, and asks Begemot to explain how to identify the IP address of the target.

SQUID GAMES

It appears Conti was involved in "**SQUID**," a new cryptocurrency which turned out to be a giant social media scam that netted the fraudsters millions of dollars. On Oct. 31, 2021, Conti member "**Ghost**" sent a message to his colleagues that a big "pump" moneymaking scheme would be kicking off in 24 hours. In crypto-based pump-and-dump scams, the conspirators use misleading information to inflate the price of a currency, after which they sell it at a profit.

"The big day has arrived," Ghost wrote. "24 hours remaining until the biggest pump signal of all time! The target this time will be around 400% gains possibly even more. We will be targeting 100 million $ volume. With the bull market being in full effect and volumes being high, the odds of reaching 400% profit will be very high once again. We will do everything in our power to make sure we reach this target, if you have missed our previous big successful pumps, this is also the one you will not want to miss. A massive pump is about to begin in only 24 hours, be prepared."

Ghost's message doesn't mention which crypto platform would be targeted by the scam. But the timing aligns with a pump-and-dump executed against the SQUID cryptocurrency (supposedly inspired by the popular South Korean Netflix series). SQUID was first offered to investors on Oct. 20, 2021.



The now-defunct website for the cryptocurrency scam SQUID.

As *Gizmodo* first reported on Nov. 1, 2021, just prior to the scam SQUID was trading at just one cent, but in less than a week its price had jumped to over $2,856.

Gizmodo referred to the scam as a "rug pull," which happens when the promoter of a digital token draws in buyers, stops trading activity and makes off with the money raised from sales. SQUID's developers made off with an estimated $3.38 million (£2.48m).

"The SQUID crypto coin was launched just last week and included plenty of red flags, including a three-week old website filled with bizarre spelling and grammatical errors," Gizmodo's **Matt Novak** wrote. "The website, hosted

at SquidGame.cash, has disappeared, along with every other social media presence set up by the scammers.”
