Shadow Banker Makes Glorious Return, Interviews Guy Exposing Conti Command & Control – Shadow Banker

By Written by Shadow Banker

Archived: 2026-04-05 13:16:00 UTC

*Author's note: Fantomas is a researcher**

So, it's been like three-and-a-half years since Shadow Banker published anything on their website. A lot of stuff happened and I'm not trying to go into any great detail about it, especially since there's actually some money on the line now. But the reason for this writeup is to discuss some recent developments in the **Conti** investigation. You know, the notorious and bygone Russia-nexus ransomware gang.

In 2022, the U.S. Department of State put a $10 million bag on the gang, seeking information on the owners, operators, and affiliates of the ransomware-as-a-service (RaaS) syndicate. Anyway, since some guy on the Ramp forum basically accused Shadow Banker of being the ransomware researcher **GangExposed**, an OSINT wizard who has been diligently deanonymizing top **Conti** members over the last two months, Shadow Banker had the bright idea of interviewing the mysterious ransomware investigator himself.

Fortunately, **GangExposed** graciously accepted Shadow Banker's interview request and agreed to answer about 10 questions pertaining to his background and recently obtained, high-confidence intel about Conti. Since April 19, some of the highlights from the researcher's doxxing campaign include releasing video footage taken on a private jet, chronicling Conti gang boss **Target**'s birthday getaway, exposing the operations of the gang's one-time Dubai operating post, and revealing the crypto money laundering front used by the group to disguise their source of income: the Russian Blockchain Life Forum.

GangExposed, who said he is a native Russian speaker, has high confidence that his attributions are accurate. "After I firmly verified my findings multiple times," he told me, "a few months ago, I launched a small but painful information attack in Telegram targeting some Conti members (**Target** and **Professor**). Out of desperation, they even tried to buy a Telegram exploit, offering $4 million for a zero-click vulnerability."

The researcher directed me to a Russian-language *Habr* article discussing this zero-day solicitation. "I also spoke with **Stern** (V*italy Kovalev, the gang's supreme leader who has also been previously sanctioned by the U.S. Treasury for his role in Trickbot malware distribution*), and he let it slip that he knows **Target** and **Professor** by their real names and admitted that he was Stern. I plan to publish this later too."

Most recently, the researcher exposed **Stern**'s "new face," which has allegedly undergone plastic surgery to help the suspected cybercriminal change his appearance.

But first, here is an overview on the **Conti** gang and why they are so uniquely exceptional in the history of the ransomware industry. According to the State Department's bounty page, the "Conti ransomware group has been responsible for hundreds of ransomware incidents" between 2019 and 2022. Following the February 2022 invasion of Ukraine, a Ukrainian affiliate, angered by the gang's public declaration of their allegiance to Russia, leaked a bunch of the syndicate's internal chat logs.

Through January 2022, the FBI estimated that **Conti** had successfully attacked over 1,000 organizations, generating ransom payouts "exceeding $150,000,000, making the Conti Ransomware variant the most damaging strain of ransomware ever documented," according to the State Department bounty page. In April 2022, **Conti** launched a ransomware attack "against the government of Costa Rica that severely impacted the country's foreign trade by disrupting its customs and taxes platforms," noted the State Department. The gang disbanded shortly after launching this attack, leading to the formation of various spinoffs.

According to research from cyber threat intelligence firm RedSense published in 2023, **Conti** operations reconstituted themselves via various RaaS offshoots, including Royal, Black Basta, Zeon, Silent Ransom Group, and AvosLocker. The following discussion will highlight **GangExposed**'s commentary on **Conti**'s command and control, as well as the researcher's technical background and experience.

SB: *Apart from the $10 million bounty, what made you want to expose Conti?*

GE: Honestly? I don't operate for medals or money. For me, this is sport — a challenge, a hunt. I've always found the myth of cybercriminal invincibility amusing. Especially when their leaders circle Western intelligence for years while agencies helplessly spin their wheels. I enjoy solving the toughest puzzles, dragging so-called anonymity experts into the spotlight, and proving there's no such thing as perfect obfuscation. Money is an illusion. Anonymity — that's real.

SB: *What is your technical background? Where are you from?*

GE: Surprisingly, I have no formal IT background. I'm not a "techie" in the usual sense. My arsenal includes classic intelligence analysis, logic, factual research, OSINT, stylometry, human psychology, and the ability to piece together puzzles others don't even notice. I'm a cosmopolitan nomad — many homes, no permanent base. I move between countries as needed. My privacy standards are often stricter than those of the very people I investigate.

SB: *Aren't you afraid Conti or Russian intelligence might retaliate and uncover your identity?*

GE: Honestly, no. Because anonymity isn't a costume — you don't just "put it on." It's a reflex, honed over years: think — delete, write — burn, meet — vanish. I've never had real social media, never used messengers where anyone called me by name. I haven't had a "real" name in years.
The lifestyle I lead would feel like torture to most "invisible" cybercriminals — but I'm used to it. Sure, nothing is 100% safe. But staying invisible to hunters who believe they themselves are invisible — that's the real thrill. I enjoy hunting the hunters.

SB: *Which cybercriminal forums do you visit?*

GE: I enjoy forums with rich data leaks — a treasure trove for stylometry. XSS, Exploit — those are classics, the gold standard for the underground service economy. You can sometimes spot the seedlings of new trends there. But the world doesn't revolve around legacy platforms — if those go offline, others will take their place. Always has, always will.

SB: *What are former Conti members doing now?*

GE: From what I know, some veterans have stepped away from direct attacks. Some are deep in crypto, some mentor younger players, some orbit blockchain startups as "consultants." I've pranked a few personally — including Stern, recently — and got some unexpected admissions Many handed down their methods and retreated into grey eminence roles. But that doesn't mean their influence has waned — it's just gone deeper underground.

SB: *Which sector do you think will be the main target for ransomware in the second half of 2025?*

GE: I won't pretend to be a prophet — let the big vendors publish their next reports; their predictions are usually close to the mark. It all depends on where the next big exploit hits, and where the defensive gaps are. That's where the next storm will land.

SB: *What TTPs will be popular among the next-gen RaaS groups?*

GE: Same story — only real-time analysis of fresh incidents can tell. I expect new and unexpected attack vectors to emerge soon. No wild speculation from me — let the latest breaches speak for themselves.

SB: *How important are platforms like XSS, Exploit, and Ramp to the ransomware economy?*

GE: Historically, these are the hubs where the entire shadow economy connects: reputation, escrow, services. Without them, ransomware would never have reached industrial scale. But if they vanished tomorrow, new alternatives would pop up within weeks. Supply follows demand — always.

SB: *What topics beyond Conti do you believe deserve deeper investigation?*

GE: Why have countries like the UAE become sanctuaries for cybercriminals from the post-Soviet space? There's plenty of solid data — but very few public investigations. How can we change that?
It's a subject worthy of a full-length exposé.

SB: *Are you tracking any other groups?*

GE: So far, my focus has been Conti. But this is just the beginning. Other targets are already in sight — and I promise, the next exclusives will be just as loud.
