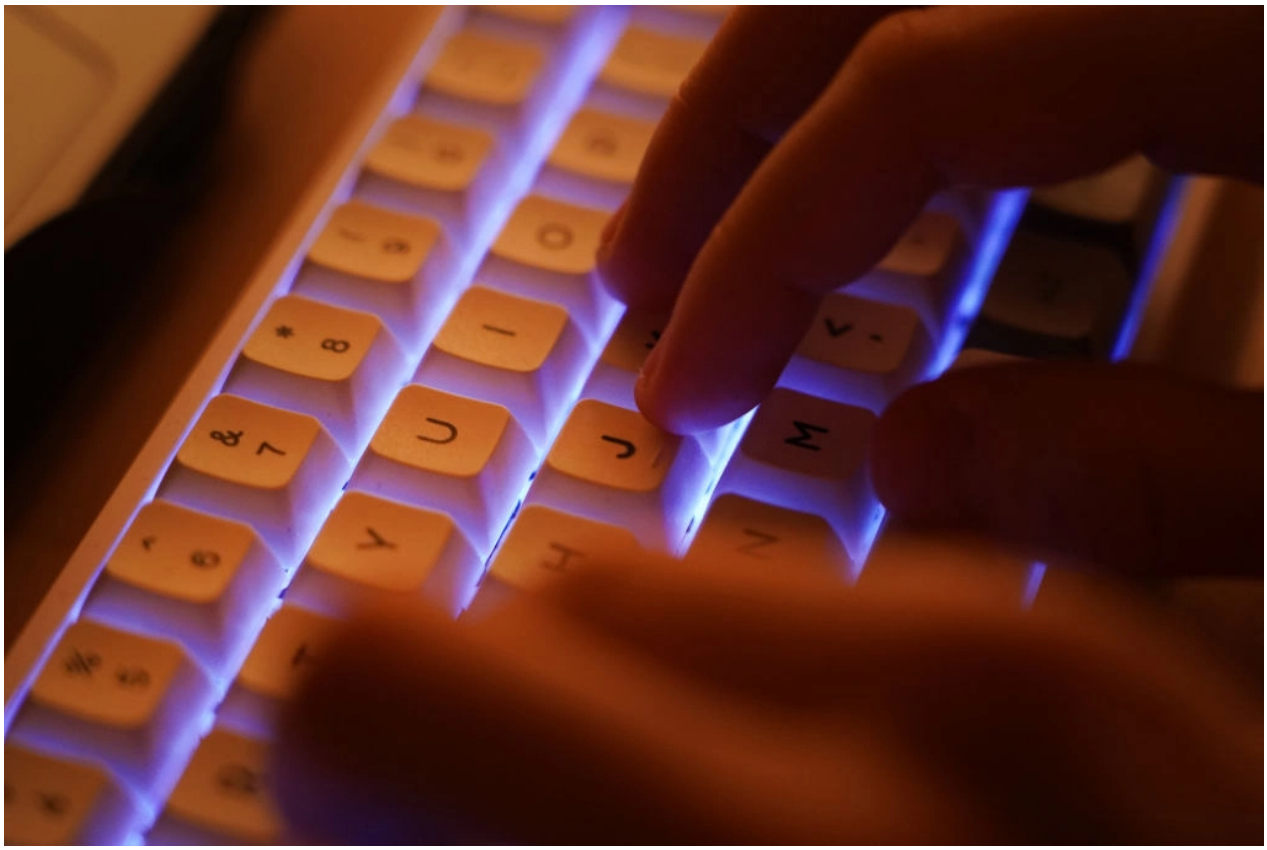
POLITICO

Shadowboxing and geopolitics on the dark web

The takedown of a Russian darknet marketplace exposed cracks within the cyber-criminal underworld — and the global effort to shut down these digital black markets.



Domestically, federal agencies have yet to settle on a cohesive strategy to tackle cyber-criminal activity on the dark web because the traditional methods to "follow the money" are increasingly hard in a cryptocurrency-dominated world. | Sean Gallup/Getty Images

By **MOHAR CHATTERJEE**
12/11/2022 04:00 PM EST

When Russia invaded Ukraine in February, a notorious cyber-criminal group called Conti declared its "full support" for President Vladimir Putin. Three days later, a pro-Ukraine member of Conti leaked logs detailing the group's plans to follow that up with action, saying Conti's leaders had "lost all their shit."

The logs revealed a startling new dimension to the evolution of one of the world's biggest cyber-criminal collectives: These groups were splintering along geopolitical lines — nationalist agendas were infiltrating a cybercrime operation that had, until now, been ruthlessly profit-driven.

And that's making the shadowy world of the so-called darknet marketplaces — where criminals trade in computer hacking tools, stolen data, narcotics and money-laundering services — even more dangerous and difficult to rein in. Cyber-criminal groups are abandoning rules that governed these marketplaces and using the malware they trade on these platforms to go after more sensitive computing systems connected to critical infrastructure and government services of the countries they deem enemies.

"You've got kind of an ideological cyber operation occurring between what I would call willing participants," said Adam Meyers, senior vice president for intelligence at cybersecurity technology company CrowdStrike. "We're seeing the proliferation of offensive cyber operations to more and more nation-states."

Want to know more about the efforts to police darknet marketplaces? We've got a 10-episode podcast for you. For the debut of the POLITICO Tech podcast, Mohar Chatterjee digs deeper with the regulators, enforcers and lawmakers trying to rein in this corner of the dark web. Check it out here.

In September, researchers from Google and IBM noted the same dynamic. Conti's hacking tools were being used in cyberattacks against Ukraine in what the researchers called an "unprecedented blurring of lines."

On the dark web, this new environment arose, in part, due to a law enforcement success: In April, German authorities shut down Hydra — at the time, the world's oldest and largest darknet marketplace, and one of the places where Conti bought and sold data and hacking tools, according to the logs.

Groups like Conti had always been relatively platform agnostic, willing to make

the jump to the next big platform and go on with their business. When the FBI shut down Silk Road, the world's first modern darknet marketplace, in October 2013, that paved the road for AlphaBay, a darknet market that grew to be 10 times bigger than its predecessor.

But when Hydra disappeared, its former administrators quickly filled the void with a multiple new, smaller darknet marketplaces and forums, setting the stage for what András Tóth-Czifra, a senior analyst at the cyber threat intelligence firm Flashpoint, calls a "war of the marketplaces" on the Russian-language darknet.

And those marketplaces are not just in conflict with the law, they are in ideological conflict with each other, divided along pro-Kremlin and pro-Ukraine lines.

Washington is worried about these groups, but also struggling to find solutions.

Rep. Jim Himes (D-Conn.), who chairs the House subcommittee on national security, international development and monetary policy, said that the criminals who make use of darknets are particularly dangerous because they need relatively few resources to hack and compromise massive computing systems in the U.S.

Mariam Zuhaib/AP Photo

“It is the ultimate asymmetric threat,” Himes said.

And regulation is especially difficult when we’re talking about the technologically complex world of the dark web, he says.

“Everybody understands bridges, right? Nobody understands Monero,” Himes said, referring to the hard-to-track cryptocurrency that’s becoming the default for darknet marketplaces.

And police and law enforcement agencies are also still playing catch-up, operating with significant technological and diplomatic handicaps that hinder efforts to take down vast, decentralized cyber-criminal operations.

At the same time, the cyber criminals on these platforms are constantly improving their operational security. Many newer marketplaces have mandated the use of Monero and increasingly use encrypted communication tools.

The geopolitics of cybercrime

The Conti leak was only the first political standoff between these gangs on new marketplaces after Hydra’s fall.

In August, outspoken pro-Kremlin hacktivist group Killnet attacked a pro-Ukraine

darknet discussion forum called RuTor, claiming it was run by the Ukrainian Secret Service agents.

Flashpoint's Tóth-Czifra said that's the kind of action that had, so far, been all but forbidden in the cyber-criminal underworld — attacking a darknet actor affiliated with a former Soviet country. Alphabay, for example, has guidelines saying the platform prohibits any activity directed against Russia, Belarus, Kazakhstan, Armenia or Kyrgyzstan.

That's partly because there's always been a somewhat political dimension to keeping darknet marketplaces running, and that's often involved making nice with governments that will be lax with enforcement.

"What Russia and some other countries do is look the other way," Himes said, describing gangs like Conti as "quasi-state actors" that governments allow to operate because their attacks on rival countries fulfill those governments' political aims.

Before Russia invaded Ukraine, there'd been at least a few overtures between the U.S. and Russia to tackle transnational cybercrime. In July 2021, President Joe Biden held a phone call with Putin to try to convince him to crack down on hacking collectives based in Russia. While Biden threatened to take "any necessary action" to protect U.S. critical infrastructure, he also said the two countries had set up lines of communication about the issue.

But the last time Russian agents even nominally cooperated with their American counterparts on a darknet law enforcement operation was in April — 10 days after the Hydra bust and less than two months after the Ukraine invasion. Russian authorities arrested Dmitry Pavlov on charges of large-scale drug trafficking. Pavlov admitted to providing servers for rent as an intermediary, but denied direct involvement in the site's administration.

At the same time, the criminal gangs that use these marketplaces are getting more brazen, using the hacking tools they buy on the platforms for cyberattacks against bigger targets that could hobble governments.

By 2017, CrowdStrike's Meyers saw the emergence of "what we call big game hunting or enterprise ransomware" — referring to tools hackers use to block access to a computer system until they get a payment. These cyber-criminal actors had figured out they would get better compliance for their ransom demands if their target's cost of going offline even for a few hours is steep, or if the compromised data is particularly sensitive. "That's really the sweet spot that they're looking for," said Meyers.

Flashbpoint's Tóth-Czifra said these higher-profile attacks meant they were also less worried about governments coming after them.

"We thought that they would not target critical infrastructure or industrial systems because of the fear of retaliation. And then Colonial Pipeline happened," he said, referring to the May 2021 cyberattack by an Eastern European group called DarkSide on a major East Coast fuel pipeline that forced the company to stop operations for six days. DarkSide said the attack was not political.

The problem with regulation and enforcement

On the day Hydra fell, Treasury Secretary Janet Yellen issued an ominous warning to the platform's users. "You cannot hide on the darknet or their forums, and you cannot hide in Russia or anywhere else in the world," Yellen said. "In coordination with allies and partners, like Germany and Estonia, we will continue to disrupt these networks."

Yet most of Hydra's cyber-criminal user base — vendors, buyers and administrators — have thus far escaped prosecution.

Critics say that's because law enforcement has been slow to adapt and coordination between agencies and among governments has been scattershot at best.

Domestically, federal agencies have yet to settle on a cohesive strategy to tackle cyber-criminal activity on the dark web — even for illicit drugs, one of the areas where law enforcement has focused intense effort.

That's because the traditional methods to "follow the money" are increasingly hard in a cryptocurrency-dominated world.

Former DEA agent Elizabeth Bisbee has been pushing since 2015 for federal law enforcement to learn how to monitor cryptocurrency transactions — one of the main methods of payment on these marketplaces — in drug investigations.

Bisbee, who now heads U.S. investigations at the private blockchain analysis firm Chainalysis, said internal advocacy for more cyber support in DEA investigations during her tenure at the agency were "met with hesitation."

In a traditional law enforcement environment, concepts like digital payments and cryptocurrency are still unfamiliar, she said. Bisbee recalled the statements she'd often hear from law enforcement agents struggling to adapt: "We run phone numbers, we do surveillance on the street. What do you mean, we now have to do surveillance on a computer? What does that even mean?"

Investigators sometimes lean on traditional techniques, like analyzing phone call records on individual darknet market vendors when they attempt to cash out their cryptocurrency gains.

But that has its drawbacks. It takes a lot of hours to track down a single vendor using traditional investigative techniques. Hydra had more than 19,000 active

vendors when its servers were seized.

Because of technological challenges and the cross-jurisdictional nature of these investigations, it can take years to coordinate a multinational law enforcement operation to take down a cyber-criminal operation on the darknet. Hydra ran unfettered for seven years before its servers were seized.

There has been progress in recent years. In the U.S., the DEA has created a number of initiatives to tackle the online drug trade, including a Joint Criminal Opioid Darknet Enforcement team formed in 2018. That same year, the DOJ led a multi-agency team that took down a massive darknet marketplace where child pornography was sold. And on the international front, the United States signed an international law enforcement cooperation protocol to combat cybercrime in May, after nearly four years of negotiation by the DOJ and the State Department.

But the global network of cyber criminals has upped its game too.

In addition to use of cryptocurrencies like Monero and stronger encryption, the new darknet marketplaces are turning to built-in cryptocurrency "mixers" that increase user anonymity by obscuring the origins of payments.

And a lack of regulation continues to help darknet marketplace trading. Regulations on cryptocurrency vary widely around the world, meaning marketplaces can move to a new country whenever one cracks down. And the backlash against the August 2022 sanction of one of these mixers — Tornado Cash — has highlighted how difficult it is to regulate technologies supporting user anonymity.

While federal regulators puzzle out how to regulate the blockchain, Monero announced encryption upgrades in August to improve user anonymity.

Adjusting to a changed landscape

So this newest generation of darknet marketplaces are sprawling cyber-criminal enterprises with murky, nationalistic motivations that have learned from the operational security mistakes of their predecessors.

And they're only getting more active. In the first half of 2022 alone, more than 236 million ransomware attacks were reported across the globe.

"You have to understand that you are a target, whether it be from an organized cyber-criminal group, from ransomware, or from a nation-state trying to steal your intellectual property," said Keith Mularski, a former FBI cyber investigator.

And as these groups' motivations change, the approaches to cracking down on them likely will have to as well.

At the end of the day, the key to tackling these shadowy cyber threats, Mularski said, is to understand the "person at the end of that keyboard."

Related Tags

Cybersecurity **Russia** **cryptocurrency** **Technology** **National Security** **Cyberattack** **Hackers** **Malware** **Ukraine** **Ransomware** **Jim Himes** **Russia's War on Ukraine**