Secret Chats Show How Cybergang Became a Ransomware Powerhouse

nytimes.com/2021/05/29/world/europe/ransomware-russia-darkside.html

Andrew E. Kramer, Michael Schwirtz, Anton Troianovski May 29, 2021

Continue reading the main story

MOSCOW — Just weeks before the ransomware gang known as DarkSide attacked the owner of a major American pipeline, disrupting gasoline and jet fuel deliveries up and down the East Coast of the United States, the group was turning the screws on a small, family-owned publisher based in the American Midwest.

Working with a hacker who went by the name of Woris, DarkSide launched a series of attacks meant to shut down the websites of the publisher, which works mainly with clients in primary school education, if it refused to meet a $1.75 million ransom demand. It even threatened to contact the company's clients to falsely warn them that it had obtained information the gang said could be used by pedophiles to make fake identification cards that would allow them to enter schools.

Woris thought this last ploy was a particularly nice touch.

"I laughed to the depth of my soul about the leaked IDs possibly being used by pedophiles to enter the school," he said in Russian in a secret chat with DarkSide obtained by The New York Times. "I didn't think it would scare them that much."

DarkSide's attack on the pipeline owner, Georgia-based Colonial Pipeline, did not just thrust the gang onto the international stage. It also cast a spotlight on a rapidly expanding criminal industry based primarily in Russia that has morphed from a specialty demanding highly sophisticated hacking skills into a conveyor-belt-like process. Now, even small-time criminal syndicates and hackers with mediocre computer capabilities can pose a potential national security threat.

Image
Motorists lining up for gas at a Costco filling station in North Carolina amid the panic that followed DarkSide's ransom attack on Colonial Pipeline.Credit...Travis Long/The News & Observer, via Associated Press

Where once criminals had to play psychological games to trick people into handing over bank passwords and have the technical know-how to siphon money out of secure personal accounts, now virtually anyone can obtain ransomware off the shelf and load it into a compromised computer system using tricks picked up from YouTube tutorials or with the help of groups like DarkSide.

"Any doofus can be a cybercriminal now," said Sergei A. Pavlovich, a former hacker who served 10 years in prison in his native Belarus for cybercrimes. "The intellectual barrier to entry has gotten extremely low."

A glimpse into DarkSide's secret communications in the months leading up to the Colonial Pipeline attack reveals a criminal operation on the rise, pulling in millions of dollars in ransom payments each month.

DarkSide offers what is known as "ransomware as a service," in which a malware developer charges a user fee to so-called affiliates like Woris, who may not have the technical skills to actually create ransomware but are still capable of breaking into a victim's computer systems.

DarkSide's services include providing technical support for hackers, negotiating with targets like the publishing company, processing payments, and devising tailored pressure campaigns through blackmail and other means, such as secondary hacks to crash websites. DarkSide's user fees operated on a sliding scale: 25 percent for any ransoms less than $500,000 down to 10 percent for ransoms over $5 million, according to the computer security firm, FireEye.

As a start-up operation, DarkSide had to contend with growing pains, it appears. In the chat with someone from the group's customer support, Woris complained that the gang's ransomware platform was difficult to use, costing him time and money as he worked with DarkSide to extort cash from the American publishing company.

“I don’t even understand how to conduct business on your platform,” he complained in an exchange sometime in March. “We’re spending so much time when there are things to do. I understand that you don’t give a crap. If not us, others will bring you payment. It’s quantity not quality.”

The Times gained access to the internal “dashboard” that DarkSide customers used to organize and carry out ransom attacks. The login information was provided to The Times by a cybercriminal through an intermediary. The Times is withholding the name of the company involved in the attack to avoid additional reprisals from the hackers.

Read More on the World of Cryptocurrencies

- **A Perfect Storm:** A steep sell-off that gained momentum this week is illustrating the dangers of cryptocurrencies.
- **Understand a $40 Billion Crash:** A trash-talking South Korean entrepreneur hyped the Luna and TerraUSD cryptocurrencies. Then, their failures have devastated traders.
- **Celebrity Endorsements:** Matt Damon, Reese Witherspoon and others have been criticized for hyping virtual currency without highlighting the risks.
- **Crypto Emperor:** Sam Bankman-Fried, a studiously disheveled billionaire, is hoping to put a new face on the still-chaotic world of digital assets.
- **Crypto Critic:** The actor Ben McKenzie, best known for “The O.C.,” has become an outspoken skeptic of digital currencies. Who’s listening?

Access to the DarkSide dashboard offered an extraordinary glimpse into the internal workings of a Russian-speaking gang that has become the face of global cybercrime. Cast in stark black and white, the dashboard gave users access to DarkSide’s list of targets as well as a running ticker of profits and a connection to the group’s customer support staff, with whom affiliates could craft strategies for squeezing their victims.

Image
A screenshot of the rules on the website of DarkSide.
The dashboard was still operational as of May 20, when a Times reporter logged in, even though DarkSide had released a statement a week earlier saying it was shutting down. A customer support employee responded almost immediately to a chat request sent from Woris’s account by the Times reporter. But when the reporter identified himself as a journalist the account was immediately blocked.

Even before the attack on Colonial Pipeline, DarkSide’s business was booming. According to the cybersecurity firm Elliptic, which has studied DarkSide’s Bitcoin wallets, the gang has received about $15.5 million in Bitcoin since October 2020, with another $75 million going to affiliates.

The serious profits for such a young criminal gang — DarkSide was established only last August, according to computer security researchers — underscore how the Russian-language cybercriminal underground has mushroomed in recent years. That growth has been abetted by the rise of cryptocurrencies like Bitcoin that have made the need for old-school money mules, who sometimes had to smuggle cash across borders physically, practically obsolete.

In just a couple of years, cybersecurity experts say, ransomware has developed into a tightly organized, highly compartmentalized business. There are certain hackers who break into computer systems and others whose job is to take control of them. There are tech support specialists and experts in money laundering. Many criminal gangs even have official spokespeople who do media relations and outreach.

In many ways, the organizational structure of the Russian ransomware industry mimics franchises, like McDonald's or Hertz, that lower barriers to entry and allow for easy duplication of proven business practices and techniques. Access to DarkSide's dashboard was all that was needed to set up shop as an affiliate of DarkSide and, if desired, download a working version of the ransomware used in the attack on Colonial Pipeline.

Image
The ransomware industry is growing explosively in Russia, in part because the authorities there have made it clear that they will rarely prosecute people for cybercrimes outside Russia.Credit...Sergey Ponomarev for The New York Times
While The Times did not acquire that software, the publishing company offered a window into what it was like to be the victim of an attack by DarkSide ransomware.

The first thing the victim sees on the screen is a ransom letter with instructions and gentle threats.

"Welcome to DarkSide," the letter says in English, before explaining that the victim's computers and servers had been encrypted and any backups deleted.

To decrypt the information, victims are directed to a website where they must enter a special pass key. The letter makes clear that they can call on a tech support team if they should run into any problems.

"!!! DANGER !!! DO NOT MODIFY or try to RECOVER any files yourself," the letter says. "We WILL NOT be able to RESTORE them."

The DarkSide software not only locks victims' computer systems, it also steals proprietary data, allowing affiliates to demand payment not only for unlocking the systems but also for refraining from releasing sensitive company information publicly.

In the chat log viewed by The Times, a DarkSide customer support employee boasted to Woris that he had been involved in more than 300 ransom attacks and tried to put him at ease.

“We’re just as interested in the proceeds as you are,” the employee said.

Together, they hatched the plan to put the squeeze on the publishing company, a nearly century-old, family-owned business with only a few hundred employees.

In addition to shutting down the company’s computer systems and issuing the pedophile threat, Woris and DarkSide’s technical support drafted a blackmail letter to be sent to school officials and parents who were the company’s clients.

“Dear school staff and parent,” the letter went, “have nothing personal against you, it is only business.” (A spokesman for the company said that no clients were ever contacted by DarkSide, but several employees were.)

On top of this, using a new service that DarkSide introduced in April, they planned to shut down the company’s websites with so-called DDOS attacks, in which hackers overload a company’s network with fake requests.

Image
President Biden said it did not appear that the Russian state was involved in the attack on Colonial Pipeline, but stressed that the Kremlin has a responsibility to prosecute cybercrimes committed by groups within its borders. Credit...Doug Mills/The New York Times
Negotiations over the ransom with DarkSide lasted for 22 days and were carried out over email or on the gang’s blog with a hacker or hackers who spoke only in mangled English, said the company’s spokesman. Negotiations broke down sometime in March over the company’s refusal to pay the $1.75 million ransom. DarkSide, it seems, was livid and threatened to leak news of the ransomware attack to the news media.

Expand Your Cryptocurrency Vocabulary

Card 1 of 9
A glossary. Cryptocurrencies have gone from a curiosity to a viable investment, making them almost impossible to ignore. If you are struggling with the terminology, let us help:

Bitcoin. A Bitcoin is a digital token that can be sent electronically from one user to another, anywhere in the world. Bitcoin is also the name of the payment network on which this form of digital currency is stored and moved.

Blockchain. A blockchain is a database maintained communally and that reliably stores digital information. The original blockchain was the database on which all Bitcoin transactions were stored, but non-currency-based companies and governments are also

trying to use blockchain technology to store their data.

Cryptocurrencies. Since Bitcoin was first conceived in 2008, thousands of other virtual currencies, known as cryptocurrencies, have been developed. Among them are Ether, Dogecoin and Tether.

Coinbase. The first major cryptocurrency company to list its shares on a U.S. stock exchange, Coinbase is a platform that allows people and companies to buy and sell various digital currencies, including Bitcoin, for a transaction fee.

DeFi. The development of cryptocurrencies spawned a parallel universe of alternative financial services, known as Decentralized Finance, or DeFi, allowing crypto businesses to move into traditional banking territory, including lending and borrowing.

NFTs. A "nonfungible token," or NFT, is an asset verified using blockchain technology, in which a network of computers records transactions and gives buyers proof of authenticity and ownership. NFTs make digital artworks unique, and therefore sellable.

Web3. The name "web3" is what some technologists call the idea of a new kind of internet service that is built using blockchain-based tokens, replacing centralized, corporate platforms with open protocols and decentralized, community-run networks.

DAOs. A decentralized autonomous organization, or DAO, is an organizational structure built with blockchain technology that is often described as a crypto co-op. DAOs form for a common purpose, like investing in start-ups, managing a stablecoin or buying NFTs.

"Ignoring is very bad strategy for you. You don't have much time," DarkSide wrote in an email. "After two days we will make you blog post public and send this news for all big mass media. And everyone will see you catastrophic data leak."

For all the strong-arm tactics, DarkSide was not completely without a moral compass. In a list of rules posted to the dashboard, the group said any attacks against educational, medical or government targets were forbidden.

In its communications, DarkSide tried to be polite, and the group expected the same of the hackers using its services. The group, after all, "very much treasures our reputation," DarkSide said in one internal communication.

"Offending or being rude to targets for no reason is prohibited," DarkSide said. "We aim to make money through normal and calm dialogue."

Another important rule adopted by DarkSide, along with most other Russian-speaking cybercriminal groups, underscores a reality about modern-day cybercrime. Anyone living in the Commonwealth of Independent States, a collection of former Soviet republics, is strictly off limits to attacks.

Cybersecurity experts say the “don’t work in .ru” stricture, a reference to Russia’s national domain suffix, has become de rigueur in the Russian-speaking hacking community, to avoid entanglements with Russian law enforcement. The Russian authorities have made it clear they will rarely prosecute cybercriminals for ransomware attacks and other cybercrimes outside Russia.

As a result, Russia has become a global hub for ransomware attacks, experts say. The cybersecurity firm Recorded Future, based outside Boston, tracks about 25 ransomware groups, of which about 15 — including the five biggest — are believed to be based in Russia or elsewhere in the former Soviet Union, said a threat intelligence expert for the firm, Dmitry Smilyanets.

Mr. Smilyanets is himself a former hacker from Russia who spent four years in federal custody for cybercrimes. Russia in particular has become a “greenhouse” for cybercriminals, he said.

“An atmosphere was created in Russia in which cybercriminals felt great and could thrive,” Mr. Smilyanets said. “When someone is comfortable and confident that he won’t be arrested the next day, he starts to act more freely and more brazenly.”

Russia’s president, Vladimir V. Putin, has made the rules perfectly clear. When the American journalist Megyn Kelly pressed him in a 2018 interview on why Russia was not arresting hackers believed to have interfered in the American election, he shot back that there was nothing to arrest them for.

“If they did not break Russian law, there is nothing to prosecute them for in Russia,” Mr. Putin said. “You must finally realize that people in Russia live by Russian laws, not by American ones.”

Image
When Megyn Kelly asked President Vladimir V. Putin of Russia why his country was not arresting hackers believed to have interfered in the American election, he said that under Russian law there was nothing to prosecute them for.Credit...Alexei Druzhinin/Agence France-Presse — Getty Images

After the Colonial attack, President Biden said that intelligence officials had evidence the hackers were from Russia, but that they had yet to find any links to the government.

“So far there is no evidence based on, from our intelligence people, that Russia is involved, though there is evidence that the actors, ransomware, is in Russia,” he said, adding that the Russian authorities “have some responsibility to deal with this.”

This month, DarkSide’s support staff scrambled to respond to parts of the system being shut down, which the group attributed, without evidence, to pressure from the United States. In a posting on May 8, the day after the Colonial attack became public, the DarkSide staff appeared to be hoping for some sympathy from their affiliates.

“There is now the option to leave a tip for Support under ‘payments,’” the posting said. “It’s optional, but Support would be happy :).”

Days after the F.B.I. publicly identified DarkSide as the culprit, Woris, who had yet to extract payment from the publishing company, reached out to customer service, apparently concerned.

“Hi, how’s it going,” he wrote. “They hit you hard.”

It was the last communication Woris had with DarkSide.

Days later, a message popped up on the dashboard saying the group was not exactly shutting down, as it had said it would, but selling its infrastructure so other hackers could carry on the lucrative ransomware business.

“The price is negotiable,” DarkSide wrote. “By fully launching an analogous partnership program it’s possible to make profits of $5 million a month.”

Oleg Matsnev contributed reporting.