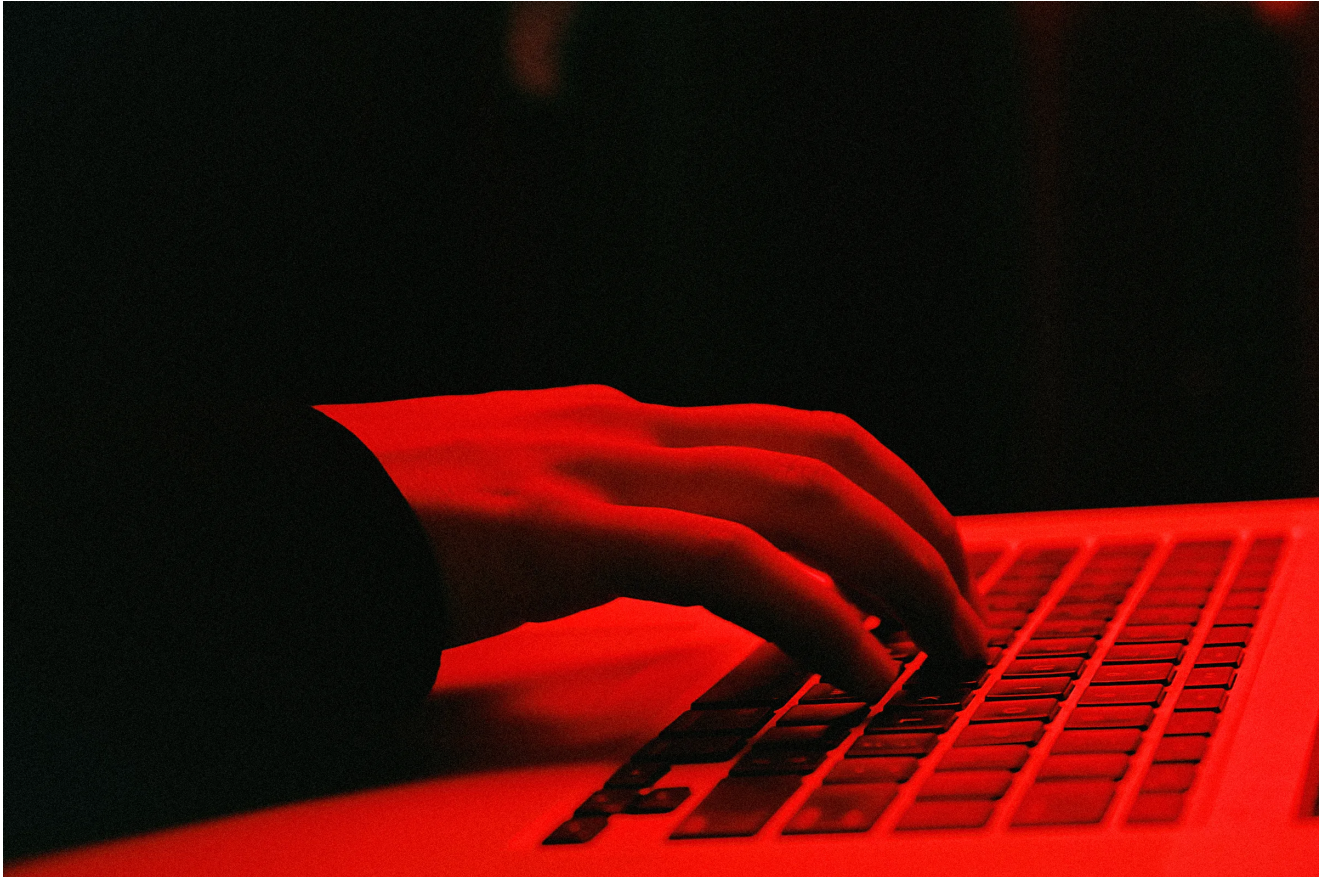


Inside Trickbot, Russia's Notorious Ransomware Gang

 [wired.com/story/trickbot-malware-group-internal-messages/](https://www.wired.com/story/trickbot-malware-group-internal-messages/)

Matt Burgess

February 1, 2022



When the phones and computer networks went down at Ridgeview Medical Center's three hospitals on October 24, 2020, the medical group resorted to a Facebook post to warn its patients about the disruption. One local volunteer-run fire department said ambulances were being diverted to other hospitals; officials reported patients and staff were safe. The downtime at the Minnesota medical facilities was no technical glitch; reports quickly linked the activity to one of Russia's most notorious ransomware gangs.

Thousands of miles away, just two days later members of the Trickbot cybercrime group privately gloated over what easy targets hospitals and health care providers make. "You see, how fast, hospitals and centers reply," Target, a key member of the Russia-linked malware gang, boasted in messages to one of their colleagues. The exchange is included in previously unreported documents, seen by WIRED, that consist of hundreds of messages sent between Trickbot members and detail the inner workings of the notorious hacking group. "Answers from the rest, [take] days. And from the ridge immediately the answer flew in," Target wrote.

As Target typed, members of Trickbot were in the middle of launching a huge wave of ransomware attacks against hospitals across the United States. Their aim: to force hospitals busy responding to the surging Covid-19 pandemic to quickly pay ransoms. The series of attacks prompted urgent warnings from federal agencies, including the Cybersecurity and Infrastructure Security Agency and the Federal Bureau of Investigation. “Fuck clinics in the usa this week,” Target said as they gave the instruction to start targeting a list of 428 hospitals. “There’s gonna be a panic.”

The documents seen by WIRED include messages between senior members of Trickbot, dated from the summer and autumn of 2020, and expose how the group planned to expand its hacking operations. They lay bare key members’ aliases and show the ruthless attitude of members of the criminal gang.

The messages were sent in the months before and shortly after US Cyber Command disrupted much of Trickbot’s infrastructure and temporarily stopped the group’s work. Since then the group has scaled up its operations and evolved its malware, and it continues to target businesses around the world. While Russia’s Federal Security Service has recently arrested members of the REvil ransomware gang—following diplomatic efforts between presidents Joe Biden and Vladimir Putin—Trickbot’s inner circle has so far been left relatively unscathed.

“They’re trying to infect as many people as possible.”

Limor Kessem, IBM Security

The Trickbot group evolved from the banking trojan Dyre around the end of 2015, when Dyre’s members were arrested. The gang has grown its original banking trojan to become an all-purpose hacking toolkit; individual modules, which operate like plugins, allow its operators to deploy Ryuk and Conti ransomware, while other functions enable keylogging and data collection. “I don’t know any other malware families that have so many modules or extended functionalities,” says Vlad Pasca, a senior malware analyst at security company Lifars who has decompiled Trickbot’s code. That sophistication has helped the gang, also known as Wizard Spider, collect millions of dollars from victims.

A core team of around half a dozen criminals sits at the heart of Trickbot’s operations, according to the documents reviewed by WIRED and security experts who track the group. Each member has their own specialities, such as managing teams of coders or heading up ransomware deployments. At the head of the organization is Stern. (Like all the monikers used in this story, the real-world name, or names, behind the handles are unknown. They are, however, the identities the group uses when talking to each other.)

“He is the boss of Trickbot,” says Alex Holden, who is CEO of cybersecurity firm Hold Security and has knowledge of the workings of the gang. Stern acts like a CEO of the Trickbot group and communicates with other members who are at a similar level. They may

also report to others who are unknown, Holden says. “Stern does not get into the technical side as much,” he says. “He wants reports. He wants more communication. He wants to make high-level decisions.”

On August 20, 2020, the chat logs—provided by a cybersecurity source with knowledge of the group—show Target briefing Stern on how the group would expand in the coming weeks. “There will be 6 offices for sure and 50-80 people by the end of September,” Target said in one of a flurry of 19 messages. These offices are believed to be based in Russia’s second-largest city, Saint Petersburg. Kimberly Goody, director of cybercrime analysis at security firm Mandiant, says the group “most likely” has a significant presence there. Current estimates say Trickbot has anywhere from 100 to 400 members, making it one of the largest cybercrime groups in existence.

Messages between Target and Stern show that in mid-2020 the group was spending money on three main areas. Two offices—“one main and one new for training”—were being used for the current operators’ expenses and expansion. “Hacker offices,” where 20-plus people worked, would be used for interviews, equipment, servers, and hiring, Target said. And finally, there would be an office for “programmers” and their equipment. “A good team leader has already been hired, and he will help gather the team,” Target continued. “I’m sure that everything will pay off, so I’m not nervous.”

Throughout the conversations viewed by WIRED, the group makes various references to “senior managers” working as part of Trickbot and its businesslike structure. “There is generally a core team of developers,” Goody explains. “There’s a manager who oversees development work, and they have coders that work under them on specific projects.” Members of the group are encouraged to propose ideas, such as new scripts or malware, that developers could work on, Goody says, and generally the lower-level workers don’t talk to their senior colleagues. Most of the group’s internal conversations, according to various sources—including US court documents—happen through instant messages on Jabber servers.

A gang member going by the moniker Professor oversees much of the ransomware deployment work, Goody says. “Professor, who we believe also goes by the name Alter, seems to be a relatively significant player in terms of managing these specific ransomware deployment operations,” Goody says, “as well as requesting development of specific tools that would help enable those.” She adds that Professor has been linked to Conti ransomware operations in the last year and “appears to lead multiple sub-teams or has multiple team leaders” that report to them.

That wouldn’t be the only working relationship Trickbot’s team has with outside parties. In the conversations seen by WIRED, Target says the group will “learn to collaborate” with those behind the Ryuk ransomware, indicating that the two organizations are largely separate. And while the Trickbot group hasn’t been linked to hacking operations run by the Russian state—such as the activities of Sandworm—the core members of the gang make reference to

Kremlin-backed activities. Stern mentioned setting up an office “for government topics” in July 2020. In response, Professor said the hacking group Cozy Bear is “working their way down the list” of potential Covid-19 targets.

In one set of internal conversations, Target answers questions from a group member who is concerned about being caught. The person is worried that colleagues could expose their locations, through leaking their IP addresses, when they don’t use a VPN to mask their whereabouts. Target says IP address exposure shouldn’t be a problem: “Here it is guaranteed that no one will touch you and you are probably not going to fly somewhere anyway.”

Prior to the REvil arrests, the Kremlin and Russian authorities spent years allowing ransomware groups believed to be based in the country to operate with relative impunity. “There seems to be very deliberate separation and non-attacks of any Russian interests by Trickbot, Ryuk, Emotet, and Conti because they don’t want confrontation with the government,” Holden says. However, not all of Trickbot’s members are in Russia. The conversations among the group viewed by WIRED reveal at least two members appear to be based in Belarus—during the summer of 2020 when Belarus shut down the internet Stern said that one member, a coder called Hof, would not be online until “the internet problem in Belarus is solved.”

These exchanges likely comprise only a small element of the group’s interactions. Some details of TrickBot’s inner workings were also revealed in June and October 2021, when the US Department of Justice unsealed and unredacted charges against two alleged Trickbot members, Alla Witte and Vladimir Dunaev. The indictment, which also covers other unnamed members of the Trickbot group, focuses on the group’s hacking and money laundering but also provides snippets of conversations. Goody says some private communication channels can contain dozens of members of the group.

Coders and developers recruited by Trickbot are drawn in from job postings on dark web forums but also on open web Russian-language freelancer websites, the DOJ indictment says. While many of the job ads are hiding in plain sight, they don’t explicitly say successful applicants will be working for one of the world’s most ruthless cybercriminal groups. One job ad the indictment points to calls for someone who is an experienced reverse engineer and knows the coding language C++. The ad, which has long-since expired, says the job was focused around web browsers on Windows, involved working remotely, and had a budget of \$7,000. A long-term position would potentially be possible if the work was completed successfully, the ad says.

Holden says Trickbot uses multiple layers during its hiring process in an effort to weed out those without the technical skills needed, and also cybersecurity companies trying to gather intelligence. Anyone applying for work has to pass an initial screening before moving on to

tough skills tests, he says. “The questions are very complex technologically,” he explains. Goody adds that penetration testers working for the group can be paid \$1,500 per month, plus a cut of ransoms that are paid.


During the recruitment process, Holden says, it is “acknowledged” that these aren’t everyday roles. Holden says he has seen ads that tell potential recruits they will be working for a startup involved in bug bounties, and that most of its funding comes from abroad. “The majority understand that this is blackhat and asking for the commercial target,” Trickbot conversations within the DOJ indictment say, referring to criminal hacking activities. “We need to stop communicating with idiots.”

The two alleged members of Trickbot named by the DOJ—Witte and Dunaev—were arrested by law enforcement outside of Russia. Witte, a 55-year-old Latvian national who lived in Suriname, was arrested in June 2021 while traveling to Miami and is charged with 19 counts that range from identity theft to bank fraud. She’s accused of being one of Trickbot’s malware developers and allegedly exposed herself after hosting Trickbot’s malware on her personal domain name. Dunaev, 38, was extradited from the Republic of Korea to Ohio in October 2021 and is also accused of developing Trickbot’s malware.

Despite the arrests and wider ransomware crackdowns in Russia, the Trickbot group has not exactly gone into hiding. Toward the end of last year, the group boosted its operations, says Limor Kessem, an executive security advisor at IBM Security. “They’re trying to infect as many people as possible by contracting out the infection,” she says. Since the start of 2022, the IBM security team has seen Trickbot increase its efforts to evade security protections and conceal its activity. The FBI also formally linked the use of the Diabol ransomware to Trickbot at the beginning of the year. “Trickbot doesn’t seem to be targeting very specifically; I think what they have is numerous affiliates working with them, and whoever brings the most money is welcome to stay,” Limor says.

Holden too says he has seen evidence that Trickbot is ramping up its operations. “Last year they invested more than \$20 million into their infrastructure and growth of their organization,” he explains, citing internal messages he has seen. This money, he says, is being spent on everything Trickbot does. “Staffing, technology, communications, development, extortion” are all getting extra investment, he says. The move points to a future where—after the takedown of REvil—the Trickbot group may become the primary Russia-linked cybercrime gang. “You expand in the hope of getting that money back in spades,” Holden says. “It’s not like they are planning to close the shop. It’s not like they are planning to downsize or run and hide.”

More Great WIRED Stories

-  The latest on tech, science, and more: [Get our newsletters!](#)
- The quest to trap CO₂ in stone—and [beat climate change](#)
- The trouble with [Encanto](#)? It twerks too hard

- Here's how [Apple's iCloud Private Relay](#) works
- This app gives you a tasty way to [fight food waste](#)
- [Simulation tech](#) can help predict the biggest threats
- 👁 Explore AI like never before with [our new database](#)
- ✨ Optimize your home life with our Gear team's best picks, from [robot vacuums](#) to [affordable mattresses](#) to [smart speakers](#)