

MATT BURGESS SECURITY MAR 16, 2022 7:00 AM

The Workaday Life of the World's Most Dangerous Ransomware Gang

A Ukrainian researcher leaked 60,000 messages from inside Conti. Here's what they reveal.



ILLUSTRATION: ELENA LACEY; GETTY IMAGES

THE CONTI RANSOMWARE gang was on top of the world. The sprawling network of cybercriminals extorted \$180 million from its victims last year, eclipsing the earnings of all other ransomware gangs. Then it backed Vladimir Putin's invasion of Ukraine. And it all started falling apart.

Conti's implosion started with a single post on the group's website, usually reserved for posting the names of its victims. Hours after Russian troops crossed Ukrainian borders on February 24, Conti offered its "full support" to the Russian government and threatened to hack critical infrastructure belonging to anyone who dared to launch cyberattacks against Russia.

But while many Conti members live in Russia, its scope is international. The war has divided the group; privately, some had railed against Putin's invasion. And while Conti's ringleaders scrambled to retract their statement, it was too late. The damage had been done. Especially because the dozens of people with access to Conti's files and internal chat systems included a Ukrainian cybersecurity researcher who had infiltrated the group. They proceeded to rip Conti wide open.

On February 28, a newly created Twitter account called @ContiLeaks released more than 60,000 chat messages sent among members of the gang, its source code, and scores of internal Conti documents. The scope and scale of the leak is unprecedented; never before have the daily inner workings of a ransomware group been laid so bare. "Glory to Ukraine," @ContiLeaks tweeted.

The leaked messages, reviewed in depth by WIRED, provide an unrivaled view into Conti's operations and expose the ruthless nature of one of the world's most successful ransomware gangs. Among their revelations are the group's sophisticated businesslike hierarchy, its members' personalities, how it dodges law enforcement, and details of its ransomware negotiations.

"We see the gang progressing. We see the gang living. We see the gang committing crimes and changing over the course of several years," says Alex Holden, whose company Hold Security has tracked Conti members for most of the last decade. Holden, who was born in Ukraine but lives in America, says he knows the cybersecurity researcher who leaked the documents but says they are staying anonymous for safety reasons.

The Conti ransomware gang runs like any number of businesses around the world. It has multiple departments, from HR and administrators to coders and researchers. It has policies on how its hackers should process their code, and shares best practices to keep the group's members hidden from law enforcement.

At the top of the business is Stern, who also goes by Demon and acts as the CEO—Conti members call Stern the “big boss.” All Conti members have pseudonymous usernames, which can change. Stern regularly chases people on their work and wants to account for their time. “Hello, how are you doing, write the results, successes or failures,” Stern wrote in one message sent to more than 50 Conti members in March 2021.

The Conti chat logs span two years, from the start of 2020 until February 27, 2022—the day before the messages leaked. In February WIRED reported on a small number of the messages, after they were provided by another source. The conversations are fragmented—think of taking your WhatsApp or Signal messages out of context—and were released in their original Russian form. WIRED reviewed a machine-translated version of the messages.

Some of the most revealing discussions take place between Stern and Mango, who acts as a general manager within Conti. Mango frequently launches into long monologues in private chats to Stern, either bemoaning team members or providing Stern with updates on the group’s projects. “They seem to be responsible for procuring different tools for different departments and making sure that the employees are being paid,” says Kimberly Goody, director of cybercrime analysis at security firm Mandiant.

The main Conti team consisted of 62 people, Mango told Stern in the middle of 2021. The exact number of Conti members fluctuates over time—at some points reaching around 100—as people join and leave the group. In one instance Stern says they are thinking of recruiting 100 more participants. “The group is so big that there are still middle managers,” group member Revers tells Meatball in June 2021.

Potential workers are funneled into Conti’s recruitment system from hacker forums and also legitimate job websites across the web. There’s even something of an onboarding process: When one new member joins the group they’re introduced to their team leader who will dish out their tasks. “I will hold a planning meeting in the evening and appoint you to the team,” Revers says in another message.

“What could be striking at first glance is the size, structure, and hierarchy of the organization,” says Soufiane Tahiri, a security researcher who has been

reviewing the documents. “They operate pretty much like a software development company, and contrary to popular belief it seems that many coders have salaries and do not take part in the paid ransom.”

Rank-and-file programmers are paid around \$1,500 to \$2,000 per month for their work, but those negotiating ransom payments can take a cut of the profits. The group even claimed to have an unnamed journalist on its payroll in April 2021, who would get a 5 percent cut by helping put pressure on victims to pay up. “We have salaries on the 1st and 15th, usually 2 times a month,” Mango tells one member of the group. Sometimes Conti members ask for extra money due to family problems—one claims they need more because their mother suffered from a heart attack—or because they’re cash-strapped.

Money is a frequent subject of discussion within Conti—both a personal and group level. They debate the ransoms, often into millions of dollars, that they plan to charge businesses for providing them with decryption keys for their files. They discuss budgets available for buying equipment and the expenses of running physical offices and servers. “They also share a Google doc spreadsheet that contains a list of expenses,” Goody says of one instance.

But some Conti members display the bombast of cybercriminals caught driving luxury cars and storing piles of cash. Bio brags they have “80k” in their bank account and that they’ve “earned more this month with you than in 10 years.” They quickly backtrack, saying they probably exaggerated. On another occasion Skippy says they purchased a 27-inch iMac with their earnings —“wanted all my life.”

Skippy was also excited about taking a holiday from work. In November 2021 they said they planned to fly abroad in the new year but were warned by Mango they could be arrested. “It’s up to you, of course, but I wouldn’t fly abroad,” Mango said. Skippy replied asking if they are meant to “sit in Russia” for the rest of their life. Mango advised making sure their phone is “clean” and not taking their laptop. On other occasions, gang members ask their superiors if the holiday they requested has been approved and if they can finish early.

“We found through our logs that they have the full plethora of manuals of how they should maintain team spirit,” says Vitali Kremez, the CEO of security company AdvIntel. Kremez’s research is name-checked by Conti multiple times

throughout the chats. “They are not just making money, they are thinking about people and how to be more successful in the environment they have created.”

Many of the conversations are dull, daily chatter as group members become acquainted and even friendly with each other. On New Years Eve 2021 some wished each other the best for 2022; members tell others they have caught Covid-19; they have issues with connectivity ("damn sorry my internet is dead"); and they bond with conversations about their partners or exes. The water cooler conversations are a stark contrast to Conti's dark work.

Despite some camaraderie, staff turnover is high. Members appear to frequently leave, which necessitates constant recruitment. As WIRED previously reported, during 2020 the Conti members, as part of the wider Trickbot cybercrime gang, discussed opening six offices in St. Petersburg for new recruits. In July 2021, Mango messaged Stern and said they were interested in moving onto Moscow “time” and starting a new company. Echoing the rise in remote working over the last two years, Stern replied: "now it's better to manage the team from a laptop."

Most of the leaked Conti chat messages are DMs sent with Jabber, but the group coordinates attacks using Rocket.Chat, a slack-style platform that can be easily encrypted. Like Slack or Microsoft Teams, Rocket.Chat lists a group's channels down a left-hand panel.

“There were channels created specifically for potential victims or infected victims,” says Émilio Gonzalez, a Canadian security researcher who studied the Conti files and re-created the group's Rocket.Chat conversations. Companies are listed as “dead” or “done” in channel names. Each channel has two to four participants with different levels of seniority and responsibilities, Gonzalez says. “The conversation usually starts with credentials or access to a specific machine on the network of the victim.” The attacks then progress from there. A review of February 2022 RocketChat messages by The Intercept shows the group discussing drug use and child sexual abuse content in general channels, and making anti-Semitic comments about Ukrainian president Volodymyr Zelensky.

Beyond its chat messages, Conti uses common tools to organize. The team regularly references the Tor browser for getting online and GPG and ProtonMail

for encrypted emails, uses Privnote for self-destructing messages, and shares files through [file.io](#), [qaz.im](#), and Firefox's discontinued Send service. They also use databases, such as Crunchbase, to gather intelligence on the businesses they want to target.

Within Conti's organizational structure is a team dedicated to open source intelligence that includes learning about potential threats. The group tried to purchase antivirus systems from security companies to test their malware against—creating [fake companies to do so](#). They circulate YouTube videos about the latest security research, watch what researchers say about them, and share news articles about the group. (One Conti member sent Stern a Russian summary of [WIRED's February story about the Trickbot group](#) the day after it was published).

THE CONTI FILES

The Big, Baffling Crypto Dreams of a \$180 Million Ransomware Gang

MATT BURGESS

RANSOM NOTES

Leaked Ransomware Docs Show Conti Helping Putin From the Shadows

MATT BURGESS




As with any workplace, Conti members get frustrated with their colleagues. People don't reply to messages, they vanish while working ("he went to get a haircut"), and they complain about long working hours. "For my part, I do not agree with the idea that I should be in touch 24 hours," Driver complained in March 2021. Working all hours of the day "is a direct path to burnout," they said.

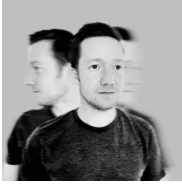
The gang fines members who underperform or don't show up for work, [analysis of the chats](#) by security firm CheckPoint shows. "I have 100 people here, half of them, even 10 percent, do not do what they need," Stern said to Mango in the summer of 2021. "And they only ask for money, because they think that they are fucking useful." At another point, Stern scolds one person: "everyone works except for you."

The Conti member Dollar is a particular pain. On January 20, 2022, the handle Cyberganster launched into a tirade about Dollar to Mango. “Let's get the dollar out of the game,” Cyberganster writes. “He is a fucked up bastard.” It’s claimed that Dollar targeted hospitals with the group’s ransomware despite being told not to. Conti members say they have a rule of not attacking hospitals or medical centers, although a May 2021 attack against [Ireland’s health service](#) [cost](#) the organization \$600 million to recover from. Six days after the complaint from Cybergangster, Mango confronts Dollar. “You really [are] more problems than good,” one message in a series of 11 says. Mango says “everyone constantly complains about you and gets angry” and accuses Dollar of spoiling the gang’s “reputation” by targeting hospitals.

Despite their everyday work life being exposed, the Conti group hasn’t gone away. But the messages include a trail of personal details, such as the handles they use online, Bitcoin addresses, and email addresses. “If this information is true, it definitely makes life easier for law enforcement,” says Tahiri. “By dismantling the group behind Trickbot/Conti we can be sure that the whole infrastructure will suffer.” It’s something the group’s members are well aware of: “We are already in the news,” read one of the last messages sent before the leak.

More Great WIRED Stories

-  The latest on tech, science, and more: [Get our newsletters!](#)
- [How Telegram](#) became the anti-Facebook
- [Wind turbines](#) could mess with ships' radar signals
- The governor of Colorado is high on [blockchain](#)
- The age of [everything culture](#) is here
- An internet troll targets [nonalcoholic spirits startups](#)
-  Explore AI like never before with [our new database](#)
-  Torn between the latest phones? Never fear—check out our [iPhone buying guide](#) and [favorite Android phones](#)



[Matt Burgess](#) is a senior writer at WIRED focused on information security, privacy, and data regulation in Europe. He graduated from the University of Sheffield with a degree in journalism and now lives in London. Send tips to Matt_Burgess@wired.com.

SENIOR WRITER



TOPICS HACKING RUSSIA UKRAINE RANSOMWARE

MORE FROM WIRED

Russia Is Leaking Data Like a Sieve

Ukraine claims to have doxed Russian troops and spies, while hackers are regularly leaking private information from Russian organizations.

MATT BURGESS

The Best Password Managers to Secure Your Digital Life

Keep your logins locked down with our favorite apps for PC, Mac, Android, iPhone, and web browsers.

SCOTT GILBERTSON

The Bitcoin Bust That Took Down the Web's Biggest Child Abuse Site

They thought their payments were untraceable. They couldn't have been more wrong. The untold story of the case that shredded the myth of Bitcoin's anonymity.

ANDY GREENBERG

Proton Is Trying to Become Google—Without Your Data

The encrypted-email company, popular with security-conscious users, has a plan to go mainstream.

GILAD EDELMAN

Ice Cream Machine Hackers Sue McDonald's for \$900 Million

Kytch alleges that the Golden Arches crushed its business—and left soft serve customers out in the cold.

ANDY GREENBERG

Putin and Biden Must Choose: How Does Russia Want to Lose?

As Russia's failures mount in its war against Ukraine, can Biden prevent an isolated Putin from doing the unthinkable?

GARRETT M. GRAFF

Netflix's US Password-Sharing Crackdown Isn't Happening—Yet

Accidental revisions to a US Help Center page sparked confusion about the streamer's next moves. But restrictions on account sharing are still coming soon.

LILY HAY NEWMAN

Enter the Hunter Satellites Preparing for Space War

True Anomaly, a startup backed by US senator JD Vance's VC firm, plans to launch prototype pursuit satellites on a SpaceX flight later this year.

MARK HARRIS