Secrets of ransomware gang spilled after it announced support for Russia

March 9 2022, by Jeff Stone and Jack Gillum, Bloomberg News

Credit: CC0 Public Domain

On Feb. 25, a notorious ransomware group known as Conti expressed support for Russia as the country invaded Ukraine. It turned out to be a bad idea: days later, a massive trove of the gang's secrets was leaked.

The data contains details on specific hacking campaigns, Bitcoin wallets used by the gang and ruminations on the future of cryptocurrency as a tool for money laundering. In one chat message, a member of Conti expressed fury that someone associated with their group had targeted a website inside Russia ("Such d—-heads," this person called colleagues). Another detailed an attempted hack on a contributor to an investigative journalism outlet probing the suspected poisoning of a prominent Kremlin critic ("Bro don't forget about Navalny").

The files also divulged the organized-crime equivalent of proprietary secrets: particulars on the gang's use of specific malware tools and insights on their negotiation techniques. Taken together, experts told Bloomberg News, the Conti leak may have done more to expose its members and undermine its methods than investigations by law enforcement and security firms. The files expose the group's organizational structure and clues about the techniques used to stay ahead of police, which represents valuable intelligence.

While conversations and negotiations with hackers have leaked before, few have matched the Conti trove's scale and detail. It offers an unprecedented, behind-the-scenes look into a group that used phony email attachments, stolen passwords and phone calls to bilk more than $200 million from its victims last year, the cryptocurrency-tracking firm Chainalysis Inc. told Bloomberg News.

Multiple security experts confirmed the trove was legitimate. They offered different theories on how Conti's files were made public, with some suggesting a leak by a Ukrainian member of the gang or perhaps a researcher with inside access. Conti is both a type of ransomware and the name of the group behind it. It was first observed in 2020 and uses the "ransomware-as-a-service" model in which new groups of hackers lease malicious software to "affiliates" in exchange for a cut of the proceeds. It is known for ruthlessness, targeting hospitals during the

COVID-19 epidemic and crippling Ireland's healthcare system last year.

The hacking group used front companies to contact sales representatives from legitimate security vendors Sophos and Carbon Black to obtain samples of antivirus software offerings, documents show. By testing malware against widely used security tools, Conti could find weak spots in the technology to circumvent popular cyber products, said Dave Kennedy, co-founder of the security firm TrustedSec, who has been tracking Conti for years.

"We've spent countless hours researching this group and where they're from," he said. "This leak provides a lot of data on how they run operations, so we can improve our own defenses and figure out how they would operate. It's pretty awesome." Targets were frequently small- and medium-sized firms, or organizations in the developing world, he said.In response to a request for comment, a Sophos representative said in an email that the company had flagged the Conti account as suspicious when hackers tried purchasing Sophos software, and the group abandoned the transaction. Carbon Black didn't respond to a request for comment.

The logs also show how Conti and its affiliates would infiltrate multiple companies each week—trading ideas on the best ruses to get victims to pay. In one leaked conversation, hackers debated whether to send a ransomware victim a sample of stolen data in order to prove they breached the company. At other times, they discussed the likelihood that a victim would be able to download encrypted data from the cloud, eliminating the incentive to pay a ransom.

One hacker, called Professor, told associates he didn't want to leak the data of a small California company specializing in agricultural labor contracts because it would have been unrealistic to gather and publish the company's information due to problems with the victim's network.

The company didn't ultimately pay the ransom, opting instead to restore its data from a recent backup. "We just didn't want to pay criminals," said Luis Romero, an office manager at Hall Ag Enterprises, which shuttered for a day in October 2020 after Conti demanded $700,000, a fee he said the company couldn't afford.

Within two days, Conti moved on, setting its sights on Angelica Corp., an Illinois-based healthcare products company. The hackers gathered contract information, company projections and personal data and used them to try intimidating the victim into paying, according to the documents. Angelica didn't respond to a request for comment.

Other American firms like Shook Construction, logistics broker Western Overseas Corp. and a manufacturer called Varroc Lighting Systems Inc. were all in the crosshairs, according to the chat logs. The three companies didn't respond to requests seeking comment.

Bloomberg News found several dozen cryptocurrency wallets among the chat logs, which totaled more than $12 million as of Wednesday, a figure that has varied with Bitcoin value. Gang members used the wallets included in the chat logs to reinvest in their technical infrastructure, pay affiliate customers and send Bitcoin to other malware operators, like developers of the TrickBot financial crime tool, said Jackie Koven, cyber threat intelligence lead at Chainalysis.

"We can see from this leak that Conti is comprised of various gangs and groups, but they are also operating somewhat autonomously," she said.

They had political targets, too, reportedly going after a contributor to the investigative journalism group Bellingcat for looking into the alleged poisoning of Kremlin critic Alexey Navalny.

Bellingcat Executive Director Christo Grozev confirmed on Twitter that

a contributor had been targeted at the time.

Like some other ransomware gangs, Conti appears to avoid Russian targets. The chats indicate that a middle manager named Troy put a stop to one such attempted attack. "Not this one. Removing it," Troy wrote. "They should be beaten up for such a thing. What if I did not notice that? Then we would have been f——ed."

Cybersecurity researchers said the pullback was further evidence of the tacit approval that Russia gives to certain cybercriminals—so long as they don't attack entities inside its borders.

Suspected ties between Russian intelligence and cybercriminals have been made public before. The U.S. Treasury Department in 2019 accused the alleged leader of the hacking group Evil Corp., Maksim Yakubets, of providing "direct assistance" to Kremlin-sponsored cyber efforts. Prosecutors also have charged a number of alleged Russian hackers with cooperating with the Federal Security Service, or FSB, dating back to 2012.

A spokesperson for the Russian embassy in Washington didn't respond to an inquiry seeking comment. Russia has previously denied engaging in malicious cyberattacks.

"With this particular group, it seems like they had a relationship to a Russian government group," said John Fokker, head of cyber investigations at the security firm Trellix and a former member of a Dutch police unit that investigates advanced hackers. "When you see conversations like, 'We shouldn't hit this organization because we're going to get screwed,' that's not the kind of thing you see often in chats like this."

Content Agency, LLC.