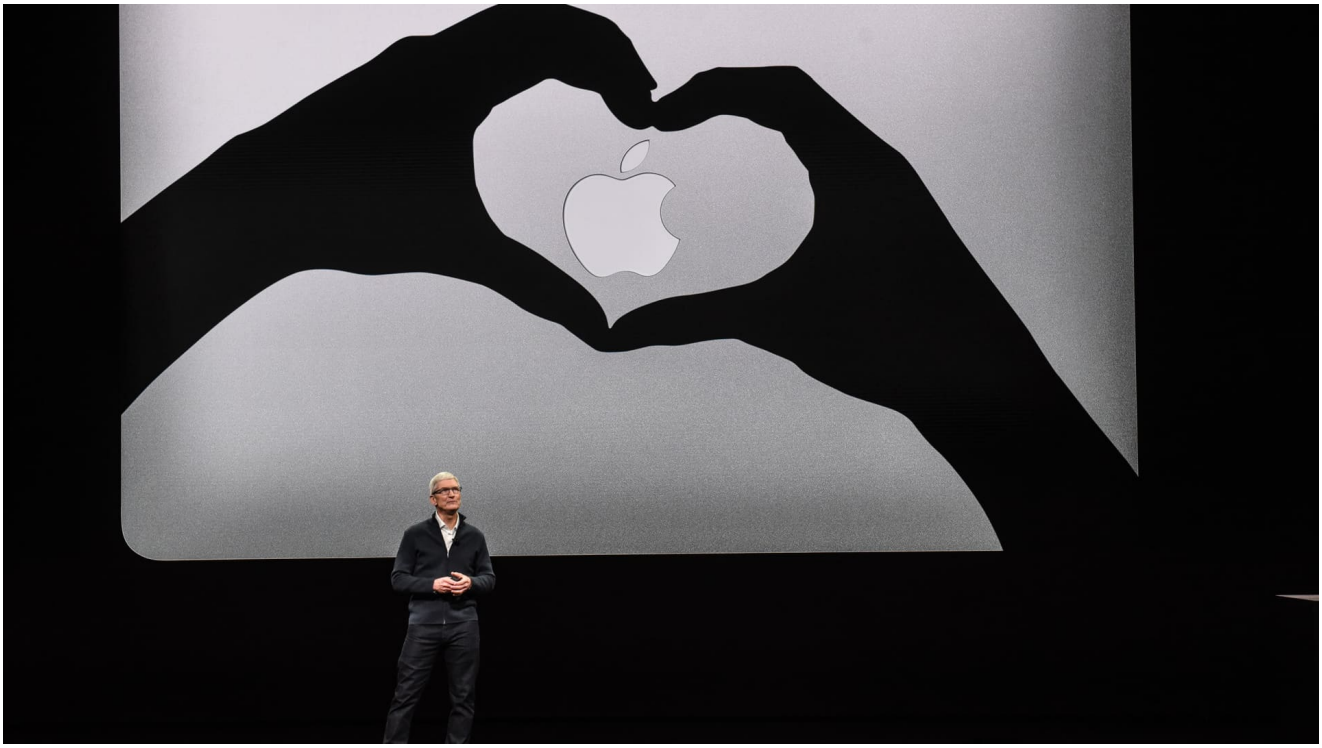
Axis of REvil: What we know about the hacker collective taunting Apple

cnbc.com/2021/04/23/axis-of-revil-inside-the-hacker-collective-taunting-apple.html

Eamon Javers April 23, 2021



Key Points

- A hacker group called REvil posted on the dark web it hacked an Apple supplier called Quanta Computer.
- In the note, it demanded that Apple pay $50 million in ransom or else it would release sensitive internal documents.
- Experts say it may presage a new era of emboldened ransomware attackers who are protected by Russian leader Vladimir Putin and empowered to take on the biggest companies in the world.

VIDEO4:4204:42

REvil: What we know about the hacker group that's holding Apple's data hostage

Squawk Box

The ransom note was both taunting and ominous: "Today we, the REvil Group, will provide data on the upcoming releases of the company beloved by many," the criminal hackers wrote.

In the note posted on the dark web the group told the world it hacked an Apple supplier called Quanta Computer and wanted $50 million in ransom or else it would release sensitive internal documents. "Tim Cook can say thank you Quanta," wrote REvil.

The extortion attempt, which came early this week, represented a significant escalation for a well-known hacker collective. And experts tell CNBC it may presage a new era of emboldened ransomware attackers who are protected by Russian leader Vladimir Putin and empowered to take on the biggest companies in the world.

Cybersecurity experts in the U.S. say the group has a long rap sheet of criminal activity against Western companies. Their analysis suggests REvil — pronounced like the letter "R" followed by the word "evil" — is largely made up of native Russian speakers and is likely located in a former Soviet state. Whoever they are, they have a taste for dark humor: REvil posts its stolen documents on a site on the dark web that it calls "Happy Blog."

"We know that they are protected most likely by Russian intelligence or the Russian government, as are most ransomware groups, which has allowed them to flourish over the last 18 months," said Marc Bleicher of Arete Incident Response, a cybersecurity firm that specializes in negotiations with criminal hackers. Bleicher says his firm has dealt with REvil 32 times in just the past 90 days.

"I think, you know, based on what we've seen so far, this may be just the tip of the iceberg over the last few months, and what you're going to start to see is organizations that are of the same size and stature as Apple," Bleicher said.

That means more CEOs need to brace for ransomware impact and for REvil's shockingly direct intimidation tactics. Bleicher said one signature of the group is stealing a CEO's personal cellphone number from company computers and then repeatedly calling that CEO to taunt him or her personally about the loss of data and to demand huge payouts.

Bleicher's firm has analyzed 173 previous REvil attacks and says it can see some patterns in how the gang operates. One thing becomes clear: Attacking Apple by name — and demanding $50 million — is on a much different scale from what REvil has operated on in the past. Thirty-one percent of the companies attacked by the group have been in professional services, not technology, Arete found. Nineteen percent have been in health care, and 16% in manufacturing.

The average ransom demand has also been much lower in the past, Arete found, at just under $728,000. After negotiations over the price, the average ransom actually paid is even lower than that: Just over $129,000.

It's a remarkably business-like operation, complete with customer service desks, software support teams and even a Craigslist-style marketplace to recruit new hackers to the enterprise.

Bleicher provided CNBC with one jobs posting for REvil that he found on the dark web. Written in Russian, it says:"We have 1 position for a person that gains accesses to networks, that already have active accesses. Monday we'll announce one of our largest attacks. We work 24x7. We are stable. We make money — a lot of money. We are waiting for you in our direct message."

Charles Carmakal, a senior vice president at the cybersecurity firm FireEye, said his rough estimate is the gang has collected a total of $100 million so far. That means a $50 million ransom would be an enormous step up for the group.

But everything in this criminal underworld is negotiable.

"I have seen other organizations being asked for $50 million," Carmakal said. "Nobody really realistically pays that much money. They'll try to negotiate it down to a number that is a little bit more reasonable and doable if they do decide to pay."

Carmakal said the huge ransom demand and high-profile target in this case may be more about getting attention — and scaring future victims — than it is about this one case. One possibility is the high-profile taunting and ransom note were only made public after a private negotiation that didn't end well from the hacker's point of view. So now they're leveraging that for publicity and intimidation.

"These groups tend to amplify their messages and try to coerce victims, usually after they don't feel like the victim is willing to pay," Carmakal said.

But why are companies sending these huge payments to criminal gangs at all? Carmakal said firms look at the scale of the potential damage and often conclude they have no choice.

"A lot of organizations feel compelled to pay because they don't want that data to get out there," he said. "They feel that they've got an obligation to their shareholders or partners or to the customer to prevent that data from making its way out onto the open market."

The latest REvil attack is still in play. The gang demanded payment from Apple by May 1 and said it would release more data every day. So far, though, no further Apple data has been dumped on the dark web.

That could be one indication, experts say, that ransom payment negotiations are already underway.