Ransomware gang wants to short the stock price of their victims

therecord.media/ransomware-gang-wants-to-short-the-stock-price-of-their-victims/

April 22, 2021

The operators of the Darkside ransomware are expanding their extortion tactics with a new technique aimed at companies that are listed on NASDAQ or other stock markets.

In a message posted on their dark web portal, the Darkside crew said it is willing to notify crooked market traders in advance so they can short a company's stock price before they list its name on their website as a victim.

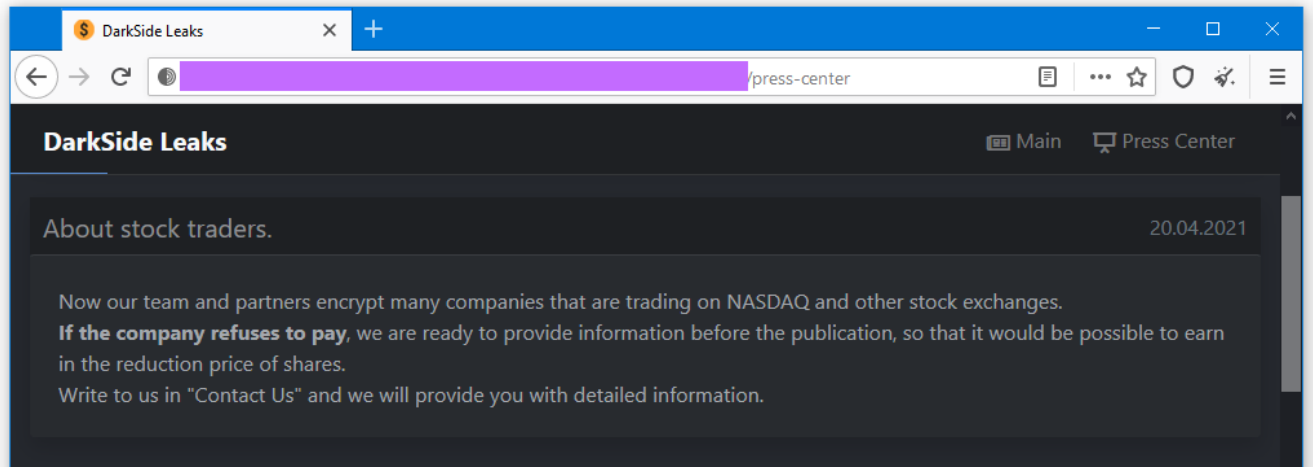

Image: The Record

The Darkside crew believes that the negative impact of having a traded company's name listed on its website would be enough to cause its stock price to fall and for a crooked trader to make a profit.

"While other ransomware families previously discussed how to leverage the effect of a publicly disclosed cyber attack on the stock market, they have never made it their official attack vector," Dmitry Smilyanets, threat intel analyst at Recorded Future, told *The Record* today.

"DarkSide becomes the first ransomware variant to make it formal."

However, the announcement also serves as an indirect method to threaten hacked companies that not paying the ransom demand could result in negative press large enough to impact their market listings and enough to push some victims into paying the asked ransom.

This approach is just the latest in a long list of techniques that ransomware gangs have been adding to their extortion arsenals.

Other gangs have previously used:

- cold-calls to threaten victims that were preparing to restore data from backups
- tried making personal threats against the executives responsible for approving the ransom payment
- threatened to notify business partners
- threatened companies with DDoS attacks
- threatened companies that they'd notify journalists about their security breaches
- threatened to notify privacy watchdog agencies about a breach so the company can get fined
- and even sent emails to a victim's clients, asking the customers to put pressure on the company to pay its ransom demand and avoid having the customers' data leaked online

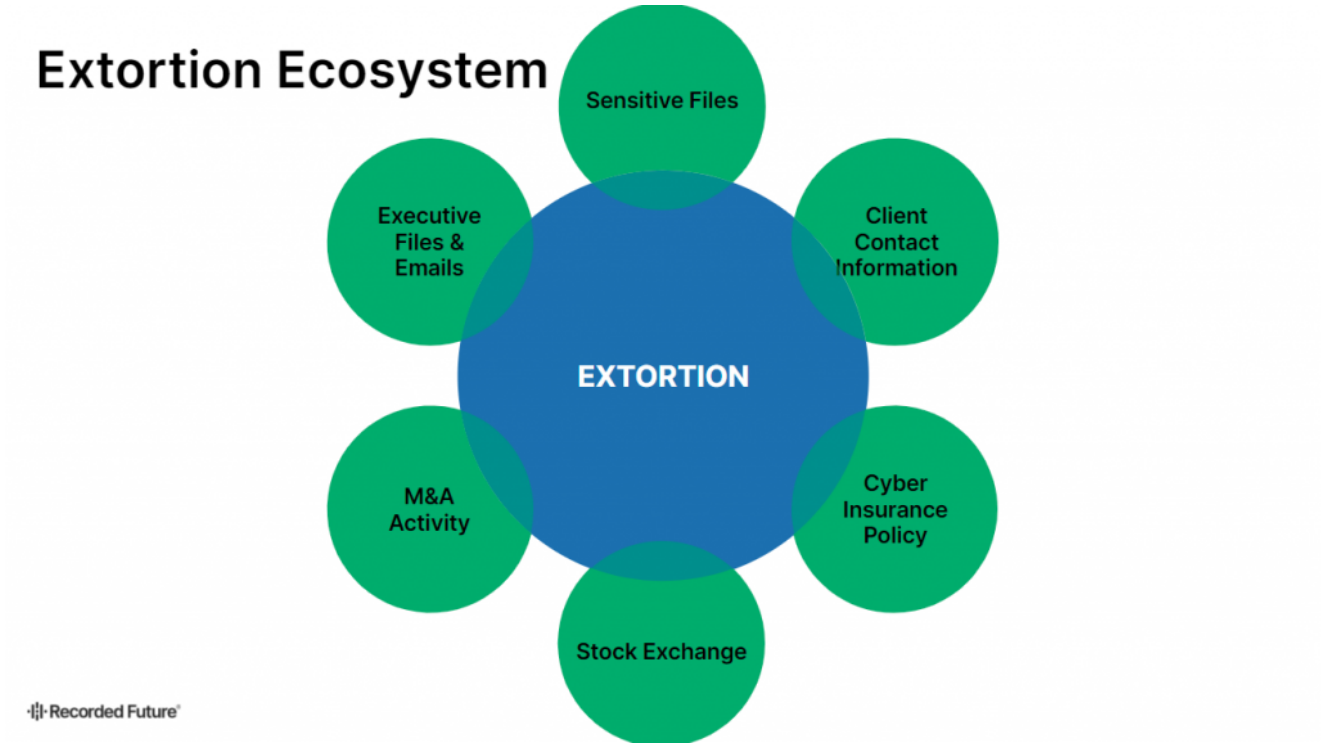

Image: Recorded Future

All of these tactics are usually deployed once ransomware gangs learn that a company whose data they stole and/or encrypted does not plan to pay the demanded ransom fee.

Once the original ransom demand is declined, ransomware groups start putting additional pressure on victims with the tactics listed above.

“We have anecdotal evidence that fewer people are paying ransom, which means ransomware actors have to find new ways to extort money from victims,” Allan Liska, a security researcher at Recorded Future specialized in the ransomware landscape, told *The Record* in an interview today.

“We saw that with threats of DDoS attacks last year but those didn’t really seem to work so they are looking for other ways,” Liska added.

However, the chances of this new extortion technique working are slim. In a tweet today, Liska said that none of the previous ransomware attacks were severe enough to cause long-term damage to a company’s market listing, with the price taking only small hits for very short periods.

> Shorting ransomware victim stock is something that @thegumshoo and I have been speculating about for a while. BUT, most companies don’t take a noticeable hit in their stock price after a ransomware attack – at least not long term. https://t.co/CIBGN13Sl6
>
> — Allan “Ransomware Sommelier 🍷” Liska (@uuallan) April 22, 2021

Furthermore, any large short bets are most likely to be picked up and investigated by the Securities and Exchange Commission or other regulatory bodies, and not many traders are likely to take up Darkside's offer for such minimal gains and maximum regulatory risks.

Tags

- cybercrime
- Darkside
- extortion
- NASDAQ
- Ransomware
- SEC
- stock market

Catalin Cimpanu is a cybersecurity reporter for The Record. He previously worked at ZDNet and Bleeping Computer, where he became a well-known name in the industry for his constant scoops on new vulnerabilities, cyberattacks, and law enforcement actions against hackers.