Five signs ransomware is becoming an industry

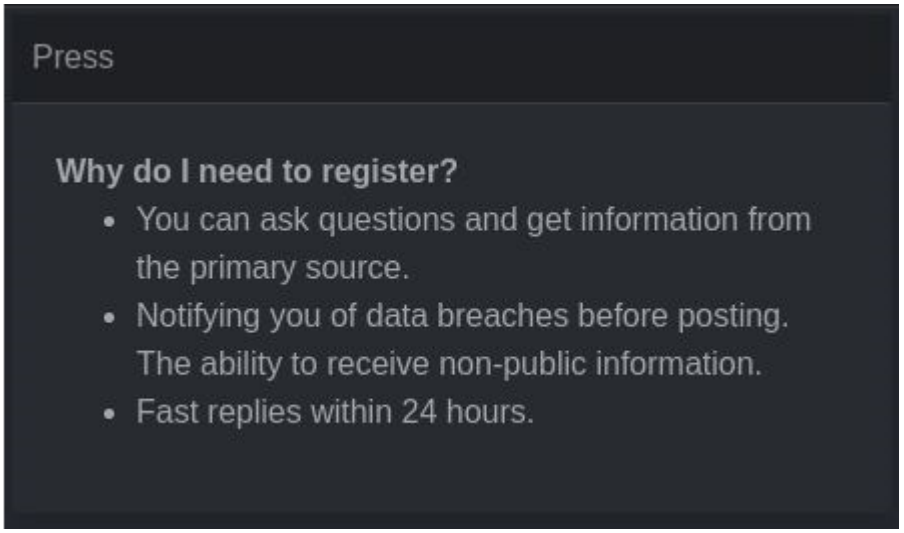
By Roman Dedenok

Published: 2021-04-16 · Archived: 2026-04-05 21:04:04 UTC

Not content with its innovative victim-pressuring tactics, the DarkSide ransomware gang has forged ahead with DarkSide Leaks, a professional-looking website that could well be that of an online service provider, and is using traditional marketing techniques. What follows are the five most illustrative examples of one gang's transformation from an underground criminal group to an enterprise.

1. Media contacts

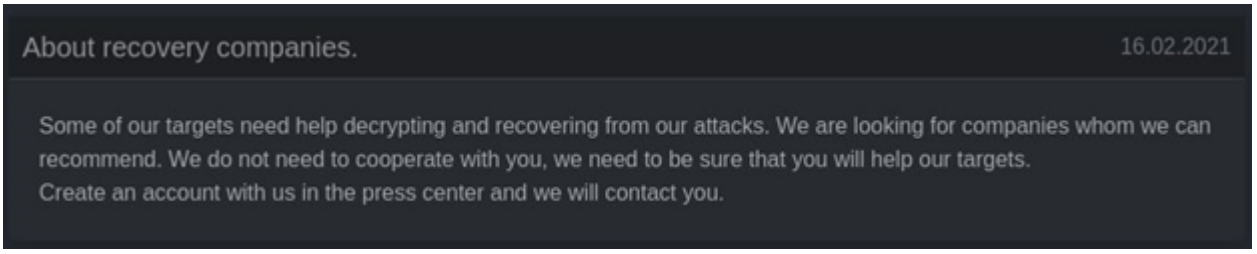
Legitimate companies always provide some sort of press center or media zone. The DarkSide cybercriminals have followed suit, publishing news about upcoming leaks and letting journalists ask questions in their press center.



At least, that's what they say. In reality, DarkSide's aim is to generate as much online buzz as possible. More media attention could lead to more widespread fear of DarkSide, potentially meaning a greater chance the next victim will decide just to pay instead of causing trouble.

2. Decryption company partnerships

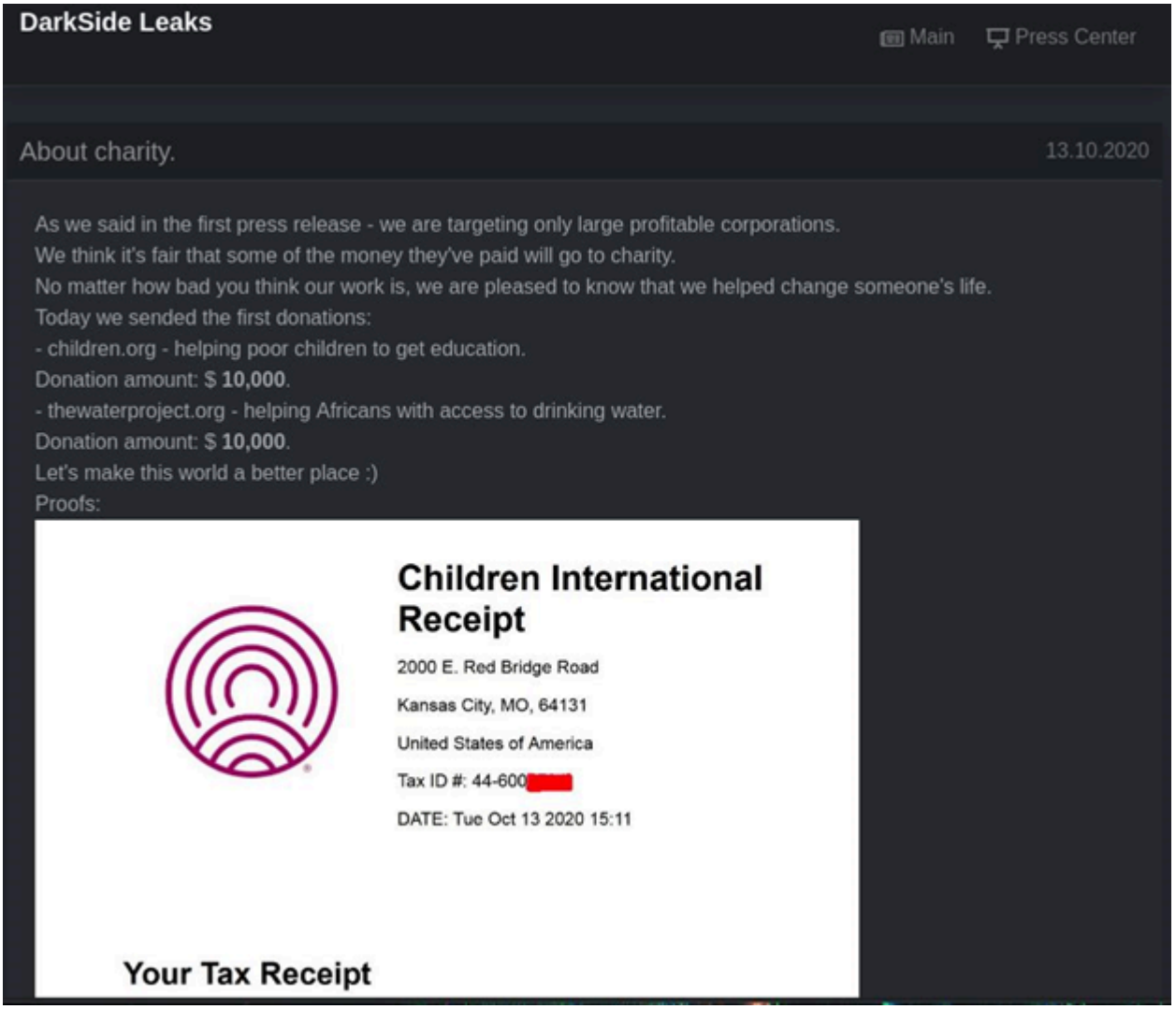
DarkSide's extortionists are seeking partners among companies that provide legitimate data decryption services. The ostensible reason is that some victims do not have their own infosec departments and have to rely on outside experts to decrypt their data. DarkSide offers such experts technical support and discounts linked to the amount of work they do.



The subterfuge should be obvious, here. The crooks aren't looking out for victims who can't decrypt the data; they're looking for big money. State-owned companies may be prohibited from negotiating with extortionists, but they're free to work with companies that provide decryption services. The latter act as a kind of intermediary in this case, pretending to restore data but in fact simply paying the crooks and pocketing the change. That may be legal, but it smacks strongly of criminal collusion.

3. Charitable donations

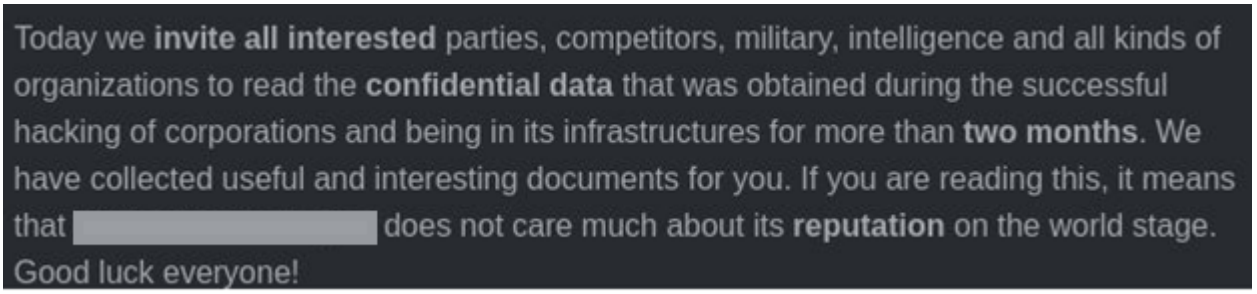
The extortionists have been donating to charity, and they post about their donations on DarkSide Leaks. Why bother? Apparently, to persuade those reluctant to pay ransom that some of the money will go to a good cause.



Here, we actually have another catch, in that some countries, including the US, prohibit charitable organizations from taking money obtained illegally. In other words, such payments would never actually reach them.

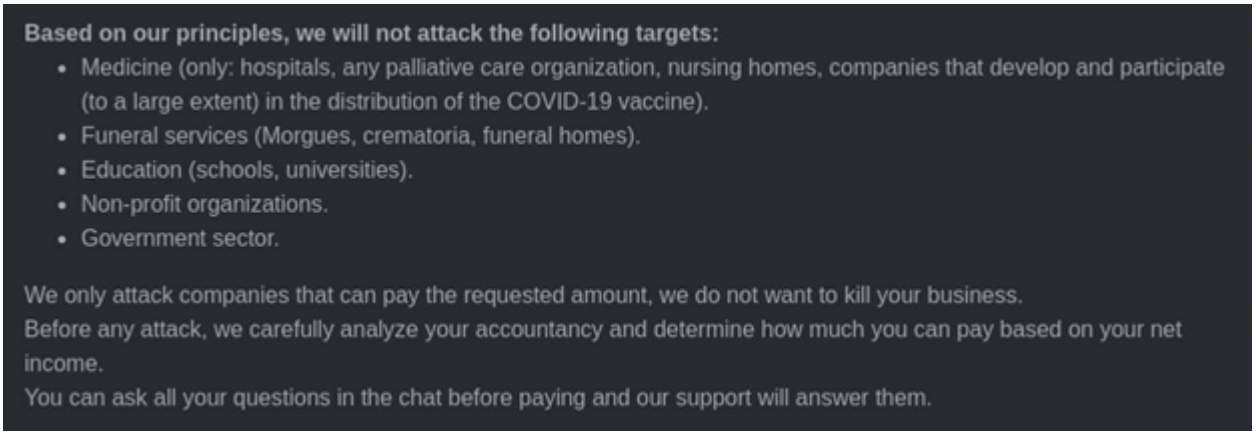
4. Business analytics

Originally, nobody but criminals and some infosec experts tended to see the stolen information ransomware operators posted, typically on hacker forums. Now, some cybercriminals have added data and market analysis, and they look for leverage in company contacts, clients, partners, and competitors before leaking stolen information. They can then send links to stolen files directly to interested parties. The main goal, again, is to inflict maximum damage on the target so as to encourage payment and intimidate future victims.



5. Declaration of moral principles

DarkSide Leaks contains an ethical principles declaration — just like the ones real corporations post on their websites. Here, cybercriminals make claims, for example saying they'd never attack medical companies, funeral parlors, educational institutions, or nonprofit or government organizations. In this case, we are not sure what the goal of this declaration might be. Is the victim supposed to think, "These people care, so I'll definitely pay them"?



A recent incident involving schoolkids' data reveals the lie. Technically, that target wasn't an educational institution, but it was the school's data that the crooks threatened to publish.

What to do

Cybercriminals clearly have the resources to invest in market analysis, professional collaborations, and charity. The way to defeat them is to cut off their sources of income. That means:

- Don’t pay ransom. It’s a bold move that may have consequences, but not paying is the right option. See Eugene Kaspersky’s recent post about why you should never give in;
- Install a reliable security solution on all connected devices to cut off any ransomware schemes before they begin.
