On Wednesday, the Russian ransomware group Grief posted a sample of data that it claimed was stolen from the National Rifle Association. Dealing with ransomware is a pain under any circumstances. But Grief presents even more complications, because the group is connected to the notorious Evil Corp gang, which has been subject to US Treasury sanctions since December 2019. Even if you decide to pay Grief off, you could face serious penalties.

The US government has been increasingly aggressive about imposing sanctions on cybercriminal groups, and in recent months the White House has hinted that other ransomware actors may soon be blacklisted. And as these efforts ramp up, they're shaping the approaches of ransomware actors and victims alike.

The NRA has not confirmed the attack nor the validity of the purported stolen documents, which researcher say include materials related to grant applications, letters of political endorsement, and apparent minutes from a recent NRA meeting. It appears, they add, that the NRA was hit with ransomware late last week or over the weekend, which lines up with reports that the organization's email systems were down.

On Friday, Grief removed the NRA posting from its dark web site. Brett Callow, a threat analyst at antivirus company Emsisoft, cautions against reading too much into that development. Delistings can indicate that a payment took place, but can also simply mean that the group has entered negotiations with the victims, who in turn may be buying time to investigate the situation and formulate a response plan. Attackers will also occasionally abandon an extortion attempt if the incident is drawing too much attention from law enforcement.

More interesting, perhaps, is Grief itself, which most researchers agree is just one of many fronts for Evil Corp. Given the murky web of ransomware actors and their malware, some researchers believe that Grief is a spinoff group rather than Evil Corp itself. Analysts look at attackers' methods and infrastructure, including indicators like encryption file format and distribution mechanisms, to uncover links. In the case of Grief, the group has technical similarities to other Evil Corp–linked entities like DoppelPaymer, and uses the Dridex botnet—historically Evil Corp's signature product.

"Grief has been operating slowly and steadily for some time," Callow says. "What we've seen is Evil Corp cycling through various brands in order to either trick companies into paying, not realizing that they're dealing with a sanctioned entity, or perhaps to provide them with plausible deniability."

Ransomware experts note that sanctions have not stopped Evil Corp from attacking targets and getting paid. But they do seem to have impacted the group's operations, forcing the hackers to factor sanctions into how they present themselves and what they communicate to victims.

“It’s interesting. We don’t often see ransomware actors pretending to be other groups, because you want to make sure you get paid,” says Allan Liska, an analyst for the security firm Recorded Future. “If you’ve been hit by Conti or Lockbit, you know you’ve been hit by Conti or Lockbit. So I think that indicates a change in behavior because of the sanctions. DoppelPaymer, Grief, and several other ransomware strains and groups are tied to Evil Corp.”

Source: **An Apparent Ransomware Hack Puts the NRA in a Bind**