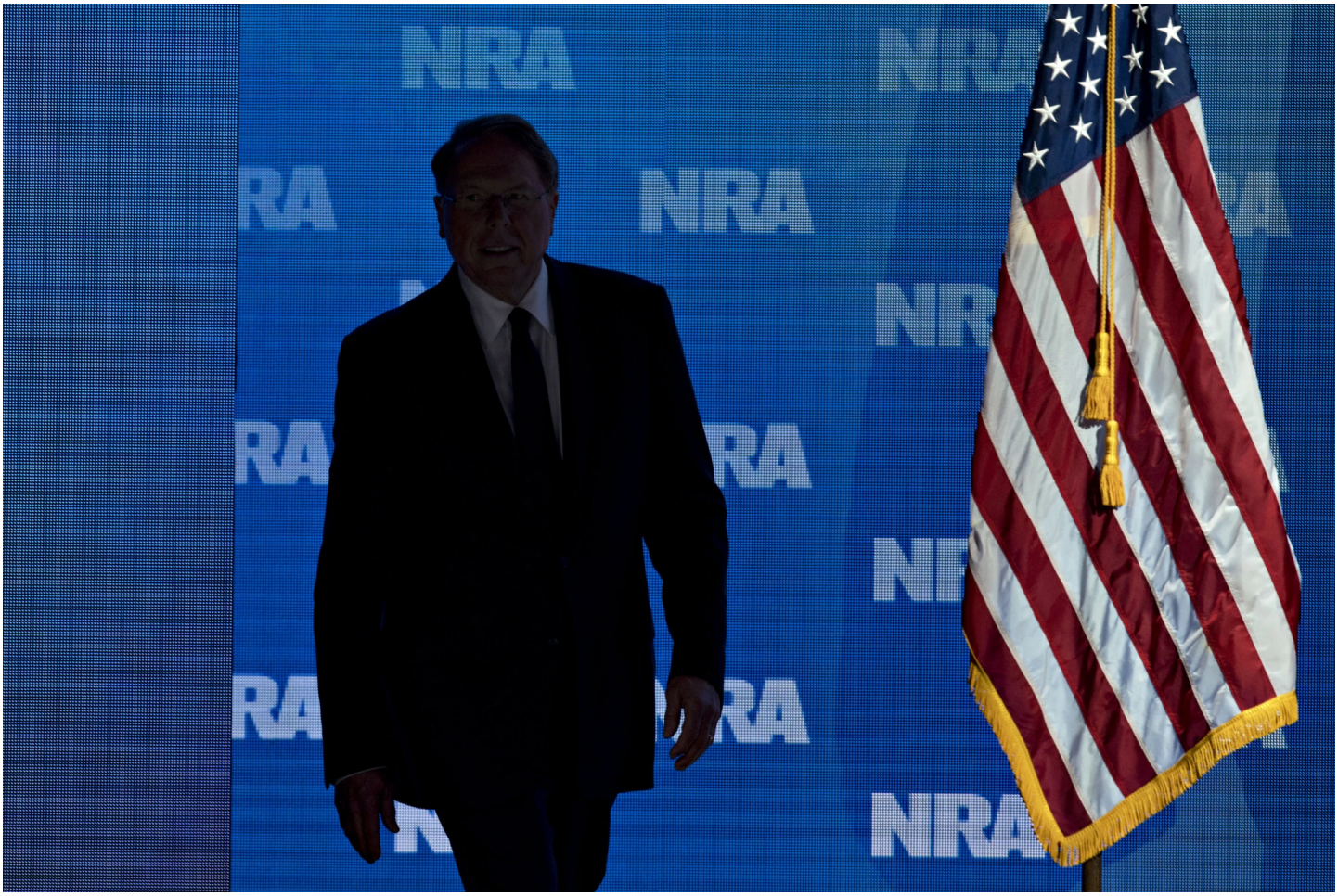
SECURITY

Cybercriminals claim to have hacked the NRA

A ransomware group that experts say is based in Russia has posted what it claims are 13 National Rifle Association files to the dark web.



Wayne LaPierre, chief executive officer of the National Rifle Association, arrives to speak during the NRA annual meeting in Dallas on May 4, 2018. Daniel Acker / Bloomberg via Getty Images file

Oct. 28, 2021, 2:12 AM CST / Updated Oct. 28, 2021, 4:34 AM CST

By Kevin Collier

A notorious Russian cybercriminal group has posted what appear to be National Rifle Association files to the dark web.

The group, known as Grief, posted 13 files to its website Wednesday and claimed to have hacked the NRA. It is threatening to release more of the files if not paid, though it did not publicly state how much.

Like many ransomware gangs, Grief often posts a handful files stolen from a victim in an efforts to spur a ransom payment.

While paying any ransomware hacker is a risk, Grief is particularly tricky. Cybersecurity experts widely believe Grief is a rebranded effort by a group of Russian cybercriminals who previously used the nickname Evil Corp, which is currently under sanctions by the U.S. Treasury Department.

"It's the same group," said Allan Liska, a ransomware analyst at the cybersecurity firm Recorded Future.

The NRA didn't respond when reached for comment. It did, however, post a tweet saying that "does not discuss matters relating to its physical or electronic security," and that the organization "takes extraordinary measures to protect information regarding its members, donors, and operations."

Grief, though a criminal group, isn't known for bluffing when it claims an organization was a victim, said Brett Callow, who tracks ransomware groups at the cybersecurity company Emsisoft.

Recommended

TECH NEWS

Emoji reactions were a cute addition to Facebook. They became a headache.

WORLD

Iran says sweeping cyberattack took down gas stations across country

"I'm not aware of any incidents in which Grief/Evil Corp has attempted to take credit for other operations' attacks," Callow said.

Most of the files viewed by NBC News relate to NRA grants. They include blank grant proposal forms, a list of recent grant recipients, an email to a recent grant winner earlier this month, as well as a W-9 form. The leak also includes the minutes from a Sept. 24 NRA teleconference meeting.

Cybercriminals, many of them based in and near Russia, have made ransomware a constant threat in recent years, regularly hacking businesses, schools, police departments and various other institutions. While the White House has taken several steps to improve U.S. defenses, ransomware is still a lucrative criminal enterprise. Last year, it cost nearly $75 billion in damages worldwide, Emsisoft found.

Jen Easterly, the director of the Cybersecurity and Infrastructure Security Agency, said earlier this month that Russian ransomware hackers have yet to make “any significant, material changes” to their frequent attacks against American businesses.

On Friday, after the FBI reportedly took down one major ransomware group, several others vowed retaliation and to punish the U.S.

Kevin Collier

Kevin Collier is a reporter covering cybersecurity, privacy and technology policy for NBC News.