NRA: No comment on Russian ransomware gang attack claims

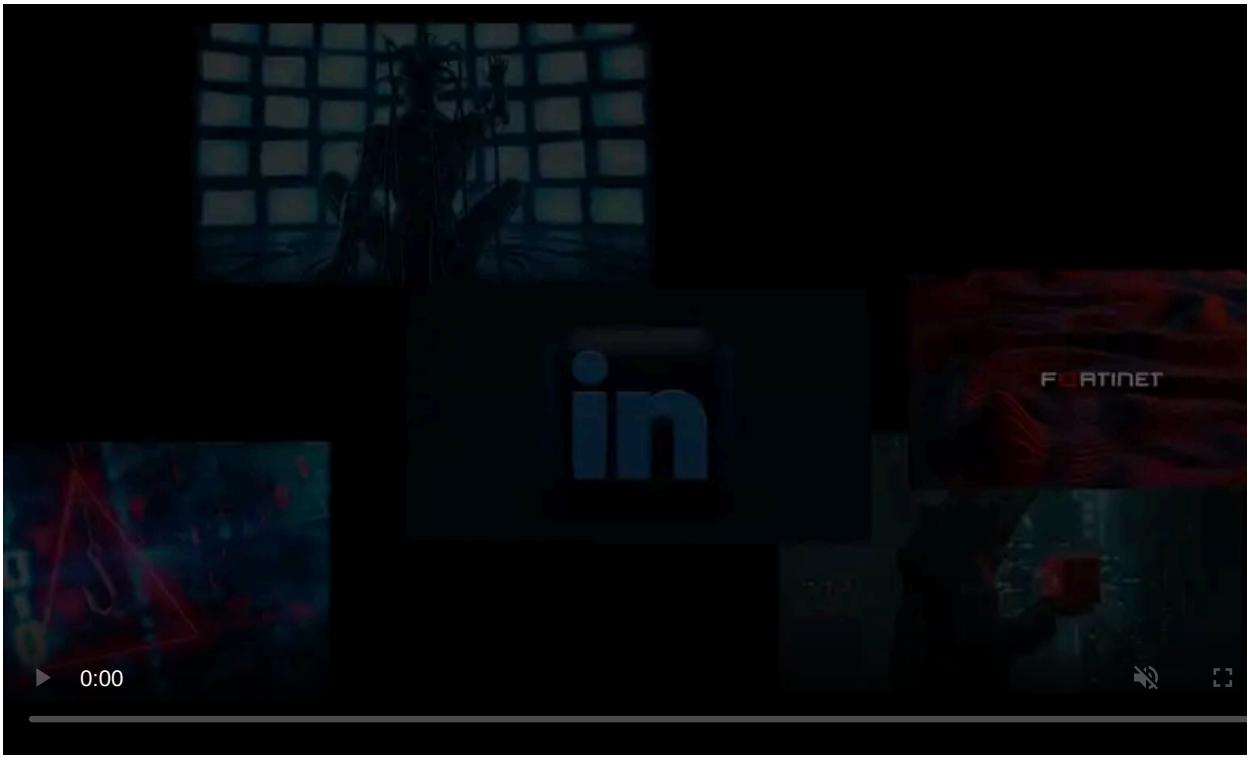
By Lawrence Abrams

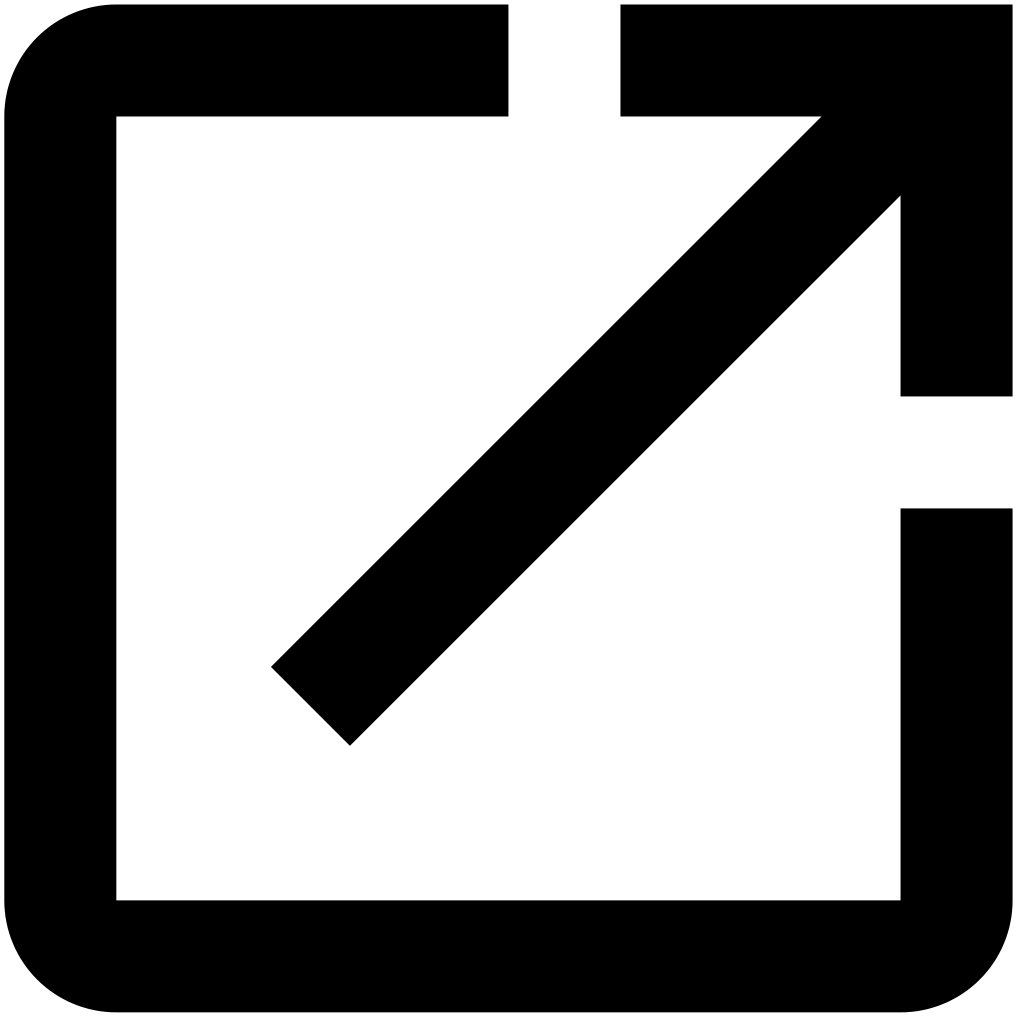
Published: 2021-10-27 · Archived: 2026-04-05 19:26:46 UTC

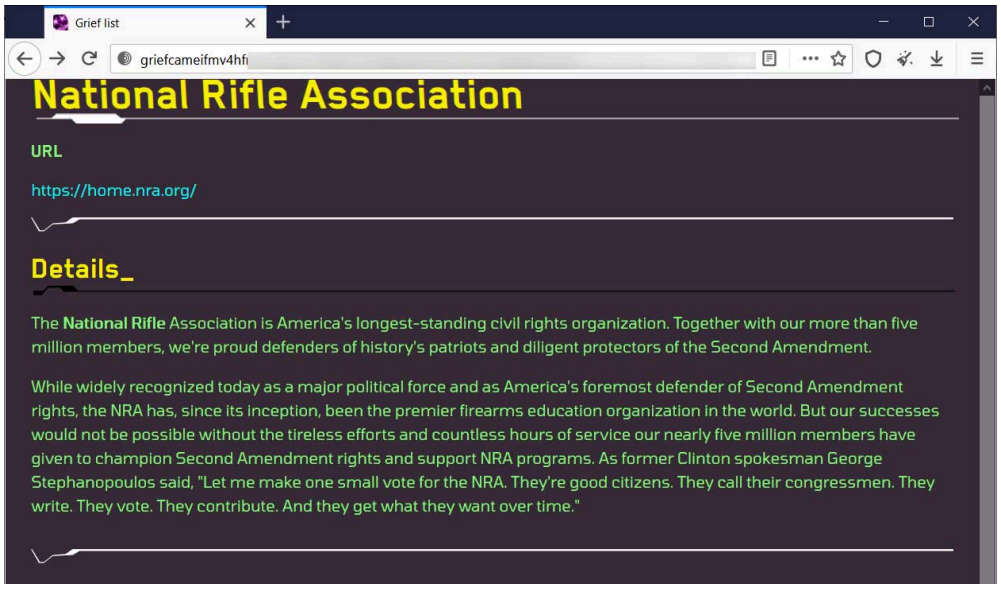
The Grief ransomware gang claims to have attacked the National Rifle Association (NRA) and released stolen data as proof of the attack.

Today, the ransomware gang added the NRA as a new victim on their data leak site while displaying screenshots of Excel spreadsheets containing US tax information and investments amounts.

The threat actors also leaked a 2.7 MB archive titled 'National Grants.zip,' that we have been told contains alleged NRA grant applications


0:00





NRA entry on the Grief ransomware data leak site

Earlier this morning, BleepingComputer contacted the NRA multiple times, including speaking to the NRA's Director of Communications Amy Hunter but did not receive any answers regarding the alleged attack.

The NRA later published a statement saying they do not comment on physical or electronic security of their organization.

> "NRA does not discuss matters relating to its physical or electronic security. However, the NRA takes extraordinary measures to protect information regarding its members, donors, and operations – and is vigilant in doing so." - Andrew Arulanandam, managing dir., NRA Public Affairs.

Grief tied to Russian hacking group

The Grief ransomware gang is believed to be tied to a Russian hacking group known as Evil Corp.

Evil Corp has been active since 2009 and has been involved in numerous malicious cyber activities, including the distribution of the Dridex trojan to steal online banking credentials and steal money.

The hacking group turned to ransomware in 2017, when they released ransomware known as BitPaymer. BitPaymer later morphed into the DoppelPaymer ransomware operation in 2019.

After years of attacking US interests, the US Department of Justice charged members of the Evil Corp for stealing over $100 million and added the hacking group to the Office of Foreign Assets Control (OFAC) sanction list.

Soon after, the US Treasury later warned that ransomware negotiators might face civil penalties for facilitating ransom payments to gangs on the sanction list.

Since then, Evil Corp has been routinely releasing new ransomware strains under different names to evade US sanctions. These ransomware families include WastedLocker, Hades, Phoenix CryptoLocker, PayLoadBin, and, more recently, the Macaw Locker.

However, their original ransomware, DoppelPaymer, ran for years under the same name until May 2021, when they stopped listing new victims on their data leak site.

One month later, the Grief ransomware gang emerged, with security researchers believing to be a rebrand of DoppelPaymer based on code similarities.

As Grief is linked to Evil Corp, it is likely that ransomware negotiators will not facilitate ransom payments without the victim first getting approval from the OFAC.
