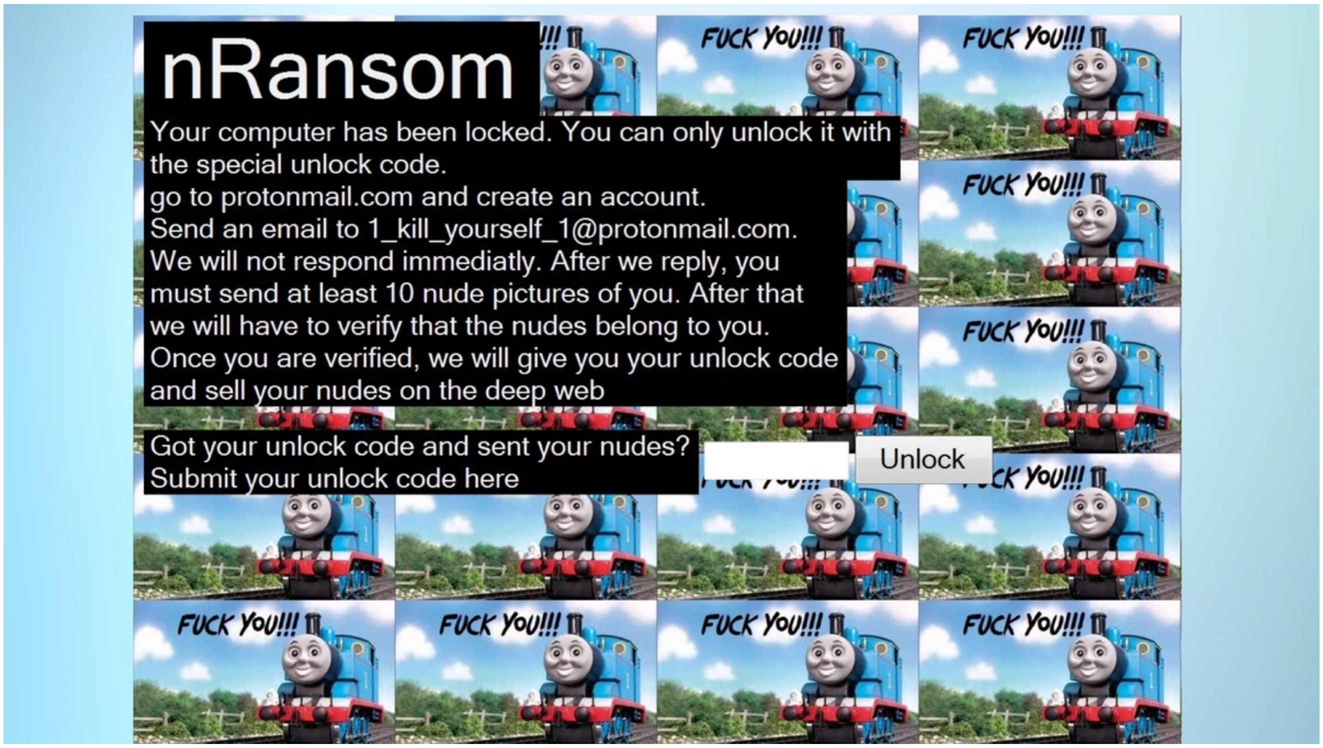
This Ransomware Demands Nudes Instead of Bitcoin

motherboard.vice.com/en_us/article/yw3w47/this-ransomware-demands-nudes-instead-of-bitcoin



nRansom

Your computer has been locked. You can only unlock it with the special unlock code.
go to protonmail.com and create an account.
Send an email to 1_kill_yourself_1@protonmail.com.
We will not respond immediatly. After we reply, you must send at least 10 nude pictures of you. After that we will have to verify that the nudes belong to you.
Once you are verified, we will give you your unlock code and sell your nudes on the deep web

Got your unlock code and sent your nudes?
Submit your unlock code here

For years, cybercriminals have been extorting victims by locking their computers with malware. The hackers promise to give the victim their files back as long as they fork over the cryptocurrency—typically Bitcoin—within the stipulated time limit. Now, someone has added a new, perverse twist to this tried and tested scheme: demanding naked photographs instead of Bitcoin.

Researchers at MalwareHunterTeam, a research group focused on ransomware, spotted the software, called nRansomware on Thursday. The group posted a screenshot of the message that's displayed when a victim gets infected:

"Your computer has been locked," reads the message, which then asks the victim to email the hackers. "After we reply, you must send at least 10 nude pictures of you. After that we will have to verify that the nudes belong to you."

The message is displayed on top of an haphazard background made of several images of the fictional children's character Thomas the Tank Engine and a smiley face with the writing "FUCK YOU!!!" in bold. It's not clear how many people have been hit with this ransomware, or how serious the hackers behind it really are.

> **Read more: This Is What It Looks Like When You Get Hit with the NotPetya Ransomware**

To some extent, the malware does appear to be legitimate. The file, nRansom.exe, is classified as malicious by several antivirus engines, including VirusTotal and Hybrid Analysis, which are both public malware repositories. Other users on Twitter also reported spotting more samples of this particular ransomware.

Malware can end up on these repositories if someone manually submits an entry and details what and does and how, or if malware is submitted and is then automatically analyzed. Motherboard attempted to infect a virtual machine with the malware but was unable to do so.

This could very well be a prank, given that it doesn't actually encrypt files, according to MalwareHunterTeam and another researcher who looked at the malware.

"It is a screenlocker, so files aren't encrypted," MalwareHunterTeam told Motherboard in a Twitter direct message. "We have no information about anyone getting infected with this."

The malware also appears to play looped music—from a file called your-mom-gay.mp3 that is actually the Curb Your Enthusiasm theme song—in the background, according to the MalwareHunterTeam.

We contacted the hackers via the email address included in their ransom message. They didn't immediately respond to our questions.

In any case, while this ransomware is clearly gross, sadly, it's not unexpected. Hackers have for years used malware to spy on women and steal their nudes or access their webcams.

This story has been updated to note that this ransomware doesn't actually encrypt files.

> ***Got a tip? You can contact this reporter securely on Signal at +1 917 257 1382, OTR chat at lorenzo@jabber.ccc.de, or email lorenzo@motherboard.tv***