NRansom: Ransomware that demands your nudes

By John Snow

Published: 2017-09-22 · Archived: 2026-04-05 18:22:55 UTC

- Ransomware

A new blocker called nRansom locks users out of their computers and demands not money, but nude pictures.

- September 22, 2017

Ransomware has been called the scourge of the Internet for quite a while. It's really one of the twenty-first century's main cyberthreats, and recently it has taken … quite a turn. Researchers from MalwareHunterTeam have discovered a new strain of ransomware, called nRansom, that blocks victims' computers, but instead of requiring money to unlock the computer, it demands nude photos.

This ransomware seems to be not a cryptor, but rather a blocker, which means that in case of infection it doesn't encrypt your files, but simply blocks access to your computer. The ransom note that appears on the screen informs victims that the only way to get back access to their computers is to send the aforementioned pictures: ten of them, nude, and demonstrably of the victims.

They state that they will somehow verify those nudes really belong to the victim before sending the code that unlocks the computer.

https://twitter.com/malwrhunterteam/status/910952333084971008

At this point, nRansom has been seen only as a file called nRansom.exe, which means it affects only Windows users.

We can only speculate on what the criminals are planning to do with any photos they manage to get. They'll probably use the pictures to shame the victims and extort either more nudes or money.

As always, we advise you not to pay the ransom if your computer gets infected. The word "pay" in this case is as legitimate as in any other; private information is no less payment than money.

Kaspersky Internet Security detects nRansom as Trojan-Ransom.MSIL.Agent.zz and neutralizes it right away. In case the blocker has somehow sneaked onto your PC, you can unblock the computer by pressing Ctrl + Alt + Shift + F4 simultaneously. It's necessary to run a full scan of your system after that. You can read more about that here.

That technique is available in all of our flagship security solutions, and it works against all blockers, in case they somehow get onto your computer. However, if you always keep protection running, that scenario is highly unlikely; Kaspersky Internet Security neutralizes almost all ransomware species before they can do anything at all, and any that manage to sneak in under the radar are detected by System Watcher when they attempt to do anything malicious.

Tips
