CAPS In Focus 12 October 2017 www.capsindia.org

Centre for Air Power Studies (CAPS)

Forum for National Security Studies (FNSS)

80/17

nRansom: Ransomware that demands beyond monetary gains

E.Dilipraj

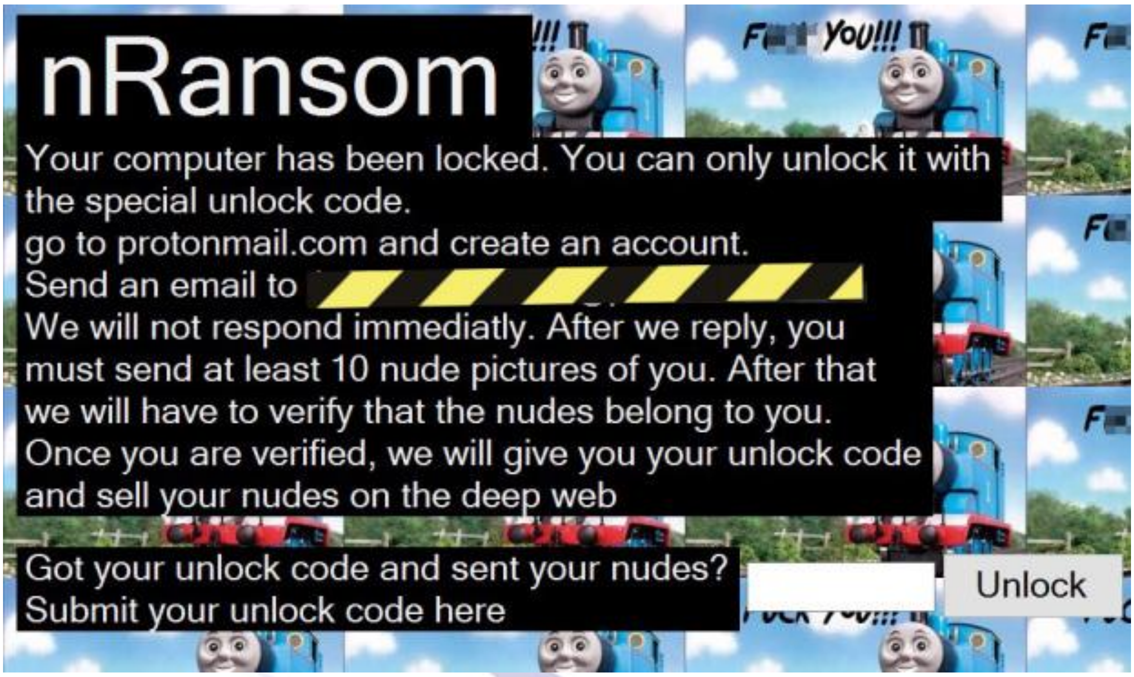
Associate Fellow, CAPS

Keywords: Ransomware, cyber security, nRansom, Wannacry, No more ransom, Europol

Not long ago the term 'Ransomware' was making buzz across the world, as it was only in May 2017 WannaCry ransomware spread so fast infecting more than 230,000 computers in over 150 countries creating havoc in some critical institutions including UK's National Health Service, Spain's Telefónica, FedEx, Deutsche Bahn and many more.[1] Although the global cyber community has been seriously observing and tracking the ransomware phenomenon since 2012, when it started to emerge as a critical threat to computer security, it can be stated that Wannacry popularized the phenomenon among the masses. Even before the havoc of Wannacry, there were many other ransomwares such as Cryptowall, Locky, Teslacrypt, TorrentLocker, Cerber, Zcryptor, etc that had their role in disrupting the computer security around the world. Adding on to this list, 'nRansom' is the recent ransomware that has attracted the attention of the cyber community across the world mainly due to the demands that it makes to its victims.

There have been two variants of this ransomware discovered so far: first by MalwareHunterTeam on September 22, 2017 and second by Karsten Hanh on the following days.[2] This ransomware stealthily infiltrates computers and blocks access to the system and also shows a message from the attacker which contains the demands. The demands made by this ransomware are the most absurd part as well as unusual from the previous instances which would usually demand for monetary transfers mainly through Bitcoins. While, the first variant of nRansom demanded 10 nude pictures of the victim to be mailed to the attacker through a special mail id (Refer Fig. 1), the second variant went several steps ahead and demanded in addition 20 nudes and instructed the victims to kill 10 people whilst recording the murder and that proof be sent to them through mail.[3]

Fig 1: Screenshot of demand for nRansom first variant.



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 [redacted]
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

By the nature of the absurd demands, nRansom differs from its predecessors and it can be stated that it has in fact opened the Pandora's Box for demands and has also widened the business of ransomware. Also considering the first variant's demand, if a victim falls prey to the attackers and accepts the demands then the victim is at the mercy of the attackers forever. Also this form of demands are made in order to discourage the victims to approach the law enforcing agencies, as such an effort would only end up in putting them in a more embarrassing situation.

This ransomware attack is a direct breach on individual's privacy and it should be considered highly criminal in nature. Also given the nature of the demands, it can be concluded that the perpetrators of nRansom only target individuals and not organizations contrary to the previous cases of ransomware attacks. In that case, it only makes one wonder if the targets would be gender biased leaning towards the feminine gender.

nRansom is only a beginning in terms of the future ransomware menace with regards to the demands that would be more creatively evil and destructive. No one country or cyber security company can tackle this global menace. It has to be a global effort with cooperation and collaboration between countries around the world, security companies, law enforcement agencies and other stakeholders. There has already been a positive step taken in this regard from Europol. On July 25, 2016 the Dutch National Police, Europol, Intel Security and Kaspersky Labs joined forces and launched an initiative called No More Ransom (an online portal), a new step in the cooperation between law enforcement and the private sector to fight ransomware together.[4] With an aim to provide a helpful online resource for victims of ransomware, this online portal www.nomoreransom.org assists users to find information on what ransomware is, how it works and also guides the users as to how to protect themselves. More importantly, the portal also provides decryption tools for more than 85 ransomwares and the database is updated as and when new decryption tool is developed for a new ransomware. More such collaborative efforts are needed from countries, private security companies and law enforcement agencies across the globe and the scope of such collaborations must be widened beyond ransomwares and address other aspects of cyber security too.

Although it is easy to say that the menace of ransomware has to be tackled on a global collaboration model, the responsibility is equal for individuals too. The fact that ransomware is gaining more popularity is only stressing on the importance of data security. Clearly Data is becoming the Oil of the future and Data Security is going to be the business of the future. As data generators it is the responsibility of every individual to be aware of its security and best practices. Awareness related to data security is the need of the hour in this highly interconnected, lighting speed communication environment from global to national to individual level.

Ransomwares like nRansom and more such threats are here to stay at least for some time in the future. It is the collective responsibility of the global community to curb this menace from becoming a global business. Finally it can be stated that, it is time for the global cyber community to quickly shift focus towards building awareness, safety and security to the existing technologies rather than to rush towards inventing half-cooked new technologies driven by profits and immediate gains.

(Disclaimer: The views and opinions expressed in this article are those of the author and do not necessarily reflect the position of the Centre for Air Power Studies [CAPS])

Notes

[1] "Cyber-attack: Europol says it was unprecedented in scale" *BBC News*, 14 May 2017, in http://www.bbc.com/news/world-europe-39907965, Accessed on 10 October 2017.

[2] "nRansom Ransomware", September 25, 2017, https://www.pcrisk.com/removal-guides/11712-nransom-ransomware, accessed on October 10, 2017.

[3] Ibid.

[4] "No More Ransom: Law Enforcement and IT Security Companies Join Forces to Fight Ransomware", Press Release, Europol, 25 July 2016, https://www.europol.europa.eu/newsroom/news/no-more-ransom-law-enforcement-and-it-security-companies-join-forces-to-fight-ransomware, accessed on 11 October 2017.