|  |  |
| --- | --- |
|  |  |

***Софтуерът за изнудване (ransomware) е зловреден софтуер (malware), който превръща компютъра в заложник и посяга на намиращите се в него лични данни.*** Обикновено той прониква в компютъра през електронната поща чрез т.нар. фишинг съобщения, използвайки уязвимост на системата и др. Софтуерът за изнудване криптира данните в компютъра и киберпрестъпниците искат от жертвите си значителен откуп за възстановяването на криптираните данни в първоначалния им вид.  Дори ако потребителят заплати исканата сума, това не означава непременно, че данните ще бъдат възстановени.  Разгледайте графиката, която показва какво действително се случва при такава атака.



**Какво могат да направят потребителите в този случай?**

Съществуват някои прости мерки, които могат да ви предпазят от софтуера за изнудване:

1. Създавайте резервни копия (архив) на данните си #BackUp
2. Избягвайте да отваряте хипервръзки от неизвестни източници #Phishing
3. Актуализирайте редовно софтуера на вашите устройства #Patch
4. Ако устройствата ви са заразени, не плащайте поискания откуп! Виж на www.nomoreransom.org #Check

**Cyber Security is a Shared Responsibility**

ECSM е ежегодната кампания за осведомяване на ЕС, която се провежда всеки октомври в цяла Европа. Целта е да се повиши осведомеността относно киберзаплахите, да се спомага за кибернетичната сигурност сред гражданите и организациите и да се осигуряват ресурси за персонална защита в интернет чрез образоване и обмен на добри практики.

#CyberSecMonth #CyberAware #eSkills #Cybersecurity