Detecting two unusual versions of ransomware, shows that the world of ransomware has become diversified

International cybersecurity researchers recently found two completely new types of ransomware that are quite strange. They carry very different and rarely recorded features, which are the alarm bells, showing that the world of ransomware has become diverse.

Especially in the context of the number of ransomware gangs as well as ransomware attacks recorded more and more frequently today.

Both new ransomware strains appeared around February, and were spotted by cybersecurity researchers at Trend Micro - AlumniLocker and Humble. It is worth mentioning that these two versions of ransomware are both trying to 'tap' data from victims in different ways, even though they are targeting bitcoin.

After analyzing in depth, the researchers discovered that AlumniLocker is a variant of the Thanos ransomware. As soon as the target's data is encrypted, it will immediately request payment of 10 Bitcoin ransom in exchange for the decryption key - about 450,000 USD currently.

This ransomware is usually transmitted through a malicious PDF attachment disguised as a valid invoice, distributed and included in phishing emails. This PDF file contains a link that will extract the ZIP file running the PowerShell script to trigger the payload and execute the ransomware.

Like the growing number of ransomware campaigns, the attackers behind AlumniLocker threatened to release stolen data from victims if they didn't pay the ransom within 48 hours. In practice, though, this ransom is too large and may be beyond the victim's ability to pay.

AlumniLocker's 'ambitious' ransom demands and other contradictions in the hacking technique - including how the website disclosing stolen data doesn't actually work - may indicate that the people behind it The malicious code is most likely just the 'novice' to move to work in this ransomware array.

'It seems that this could be a new group of hackers, not experienced in optimizing the effectiveness of attacks because the ransom is much higher than usual. In addition, the website's inactive leak is another example that this is a new hacker group, " said Jon Clay, senior security engineer at Trend Micro.

A second new ransomware strain, Humble, made its debut in February as well, as it works in a completely different way. First, Humble requires a much smaller data ransom than AlumniLocker, at just 0.0002 Bitcoin - less than $ 10 at current rates. This suggests that Humble may be targeting individual individuals instead of organizations as a common trend in the ransomware world.

It is not known exactly how Humble was distributed, but researchers note that the malware is more likely to be transmitted via phishing attacks.

In an attempt to push the victim to pay the ransom, Humble threatened by saying that if they rebooted their system, the Master Boot Record (MBR) would be rewritten, making the computer unusable.

Humble is an unusual ransomware strain because it is compiled with an executable shell (Bat2Exe) in a batch file. What's more odd is that it uses Discord - a voice, text, and video communication service popular among gamers - to send reports back to the operators behind it.

Both of these new types of ransomware are unusual, but they both point to the caveat that ransomware continues to be the 'promised land' for cybercriminals, where it's easier to pocket large amounts of illegal money. ever.