Newly Found Sugar Ransomware is Now Being Offered as RaaS

cyware.com/news/newly-found-sugar-ransomware-is-now-being-offered-as-raas-641cfa69

While the ransomware landscape is ever filled with a variety of sophisticated ransomware, a new ransomware family, dubbed Sugar, has surfaced lately to wreak havoc.

What do we know so far?

- The cyber threat team at retail giant Walmart has uncovered the new ransomware family Sugar, which is now being made available to cybercriminals as a Ransomware-as-a-Service (RaaS).
- Written in Delphi, the ransomware was initially spotted in November 2021.
- Although not many details about the ransomware are available, researchers claim that the Sugar ransomware primarily targets individuals rather than enterprise networks.
- Based on the telemetry by Fortiguard, the ransomware has infected users in Canada, Thailand, the U.S., Israel, and Lithuania.
- However, it is still unclear how the ransomware is being distributed to the targets.

Other characteristics

- Once executed, the ransomware encrypts files on the compromised machines and appends the ‘encoded01’ extension to them.
- The malware then displays a ransom note on the victim’s machines, asking for a ransom of around $4.01 in Bitcoin.
- The ransom note strikes similarities with that employed by the REvil ransomware - except for some differences and misspellings.
- Moreover, the Tor site used by the ransomware resembles that of the Cl0p ransomware.

Conclusion

While it is still early to predict the impact, the RaaS operations of the Sugar ransomware group are believed to expand the attack scope for its affiliates. This can provide the group with more opportunities to achieve its malicious objectives. Therefore, organizations must take steps to bolster their defense systems to thwart such threats.

Sugar ransomware | Ransomware-as-a-service (RaaS)

Publisher

Cyware