New Ransomware “Diavol” Being Dropped by Trickbot

binarydefense.com/threat_watch/new-ransomware-diavol-being-dropped-by-trickbot/

Garrett Thompson

When handling an incident, FortiGuard Labs security researchers noticed that Trickbot had begun to deploy Conti and Diavol ransomware in the same attack. According to the researchers, Conti and Diavol had striking similarities including:

“The two ransomware families’… use of asynchronous I/O operations for file encryption queuing to using virtually identical command-line parameters for the same functionality (i.e., logging, drives and network shares encryption, network scanning).”

Despite the similarities, there is **no direct connection** that the Trickbot gang developed Diavol like Conti and Ryuk. Because Trickbot is used for access as a service for ransomware gangs it is affiliated with, the connection between Diavol and the Trickbot gang cannot be assumed, but from a practical defense perspective, organizations should continue to focus efforts on detecting Trickbot, Cobalt Strike, and domain profiling reconnaissance methods used prior to ransomware deployment.