Cybercrime, RFQ dalla Turchia veicola AgentTesla e zgRAT

difesaesicurezza.com/cyber/cybercrime-rfq-dalla-turchia-veicola-agenttesla-e-zgrat/

Francesco Bussoletti

RFQ dalla Turchia veicola AgentTesla e zgRAT. L'allegato zip del messaggio, arrivato anche in Italia, contiene un file exe: il primo malware, che scarica il secondo. I dati rubati sono poi esfiltrati via SMTP

Una RFQ di prodotti dalla Turchia è l'esca per una nuova campagna AgentTesla e zgRAT, arrivata anche in Italia.

L’allegato zip contiene un file exe: il primo malware che, tramite Powershell, scarica il secondo. I dati rubati sono poi esfiltrati via SMTP.

AgentTesla, tramite la funzione keylogger, è in grado di acquisire tutto ciò che l’utente digita. Inoltre, può rubare email e credenziali del browser e acquisire schermate. Infine, ha la possibilità di impartire comandi da remoto sul PC infetto, come scaricare payload aggiuntivi o aggiornare quelli presenti.