DoppelPaymer FBI PIN on Dec 10, 2020

TLP: WHITE
10 December 2020
PIN Number
20201210-001
Please contact the FBI with
any questions related to this
Private Industry Notification.
Local Field Offices:
www.fbi.gov/contact-us/field-
offices
The following information is being provided by the FBI, with no guarantees or warranties, for potential use at the sole discretion of recipients to protect against cyber threats. This data is provided to help cyber security professionals and system administrators guard against the persistent malicious actions of cyber actors. This product was coordinated with DHS-CISA.
This PIN has been released TLP: WHITE: Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.
DoppelPaymer Ransomware Attacks on
Critical Infrastructure Impact Critical Services
Summary
Since late August 2019, unidentified actors have used DoppelPaymer ransomware to encrypt data from victims within critical industries worldwide such as healthcare, emergency services, and education, interrupting citizens' access to services. Since its emergence in June 2019, DoppelPaymer ransomware has infected a variety of industries and targets, with actors routinely demanding six- and seven-figure ransoms in Bitcoin (BTC). Prior to infecting systems with ransomware, the actors' exfiltrate data to use in extortion schemes and have made follow-on telephone calls to victims to further pressure them to make ransom payments.
Threat Details
DoppelPaymer ransomware attacks since June 2019 have negatively impacted the provision of healthcare, emergency, and education services to citizens worldwide.