Sodinokibi/REvil Ransomware Attacks

Overview

Since January 2020, the Arete IR practice has responded to forty-one (41) Sodinokibi engagements. The industry has seen two big changes with Sodinokibi/REvil from their shift to exfiltrating data as of January 2020, and more, recently with their move to only accepting payments in Monero cryptocurrency (XMR). Recently our IR practice responded to a Sodinokibi/REvil engagement where we dug into the ransomware itself and this article is meant to provide information on the ransomware behavior observed during the engagement. Our intention is to summarize some of the high-level information on Sodinokibi/REvil for general awareness, as well as provide a technical overview with behavioral indicators back to the community to help network defenders become more familiar with this threat.

Statistical Data from Arete's Metrics

The information listed below is based on forty-one (41) Sodinokibi cases since Jan 2020. Our IR and Data Analytics practices work hand-in-hand to track key data points for every ransomware engagement. The IR practice tracks data points on the ransomware variant and collects statistics based on handled engagements:

- Arete has responded to 64 Sodinokibi/REvil cases since Sep 2019 with 41 of those since Jan 2020 Finance-4 | Healthcare-14 |Manufacturing-8 | Professional Services-17 | Public Service-11 | Tech/Engineering-6 | Critical Infrastructure-4
- 25 out of the 64 Sodinokibi/REvil engagements involved an MSP that was the initial point of entry
- Ransom paid for 40 of the 64 matters
- The average ransom demand is 31.93 BTC
- The average ransom demand paid in US dollars has been $145,235.31
- The maximum ransom demand paid in US dollars has been $759,835.29
- The minimum ransom demand paid in US dollars has been $4,550.98
- Threat actors have provided the decryption key 100% of the time
- Data exfiltration has only occurred in 7.14% of the engagements
- The major infection vector has been Remote Access (RDP) at 54.72% of the time
- The average business downtime is approximately 8.27 days