Severity

Medium

Analysis Summary

Grandoreiro is a globally widespread malware and uses modular installers to evade detection. The malware makes use of the victim's privileges and access to perform fraudulent banking transactions. This helps them evade the security measures used by banking institutions. A specific DGA (Domain Generation Algorithm) is used by the malware to hide the CnC addresses used during an attack. Grandoreiro follows a Malware-as-a-Service (MaaS) business model and is operated by many cybercrime groups. The malware is mainly used to target Brazillian and European Banks. "The cluster targeting Brazil used hacked websites and Google Ads to drive users to download the malicious installer. The campaign targeting other countries used spear-phishing as the delivery method."

Impact

- Credential Theft
- Information Theft
- Financial Loss

Indicators of Compromise

MD5

- f72e8569ac0b2773739201cfe981ad37
- 707fea47360c6b3e29ef14e59d21901f
- 9d9231f90d34d0296963f50aa9d901d7
- b39ab852c2471dd73776ea76631f17e8
- 22ccdaee217eb353545b2119bd72b85b
- 75987fa33df9d166ff1f0d84d953f2f7

SHA-256

- b6e4164dd365203dc5a2ea1f22b2416da6854c523fb5de0308cbf00054579c27
- 994cae8bc8fce62a930294846d11731616581179ef28e06ff1d8541f28a4e020
- 690c48016ee1d44a8e143c20685dd59c03e281c6d2601b41834bbee028e442f1
- c86df2f76fe86c65a0a1a956bd6043090e04d9c144e4203ed8cd14ceac1df2d5
- a2a81630770bd92e65b664c6a9eeadaacdafef6c471ae810ef26b9a809de34ec
- e6f5c8be7349d6bfc6de23c0b967d13ca64b076c1d1d52a899476c8ea7f9dce6

SHA-1

- f933369ede2edc19ab38603848497bb92c9fd661
- 10d824febd09e42a9329c5f83c4a24b21caa7c4e
- 2da5319d4fc63b4e96596b89a2eb86a836817440
- 6e15573ecf5cd057e89353d80e413140451e977d
- 9800d7bccf26d32f5b7718d9f9e086c76a1bcd00
- 7974a02f36463af2e38c7e249d613e6e26cbfebd

Remediation

- Block all threat indicators at your respective controls.
- Search for IOCs in your environment.