THREAT CURE

RE-ARCHITECT YOUR THREAT LANDSCAPE

ThreatCure

Cyber Threat Advisory

Grandoreiro Malware

Threat Actor Malware

Description

Grandoreiro Malware

CATEGORY

Malware

SEVERITY

Medium

Platforms

Windows & Linux

IMPACT

- Data Breach
- Financial losses
- Reputation Damage
- Credential Theft
- Business Disruption
- Increased Costs

Grandoreiro is a sophisticated banking Trojan primarily targeting Spanish and Latin American regions. Originating from Brazil, this malware is known for its advanced evasion techniques, including the use of legitimate software to avoid detection and its ability to block access to antivirus websites. It often spreads through phishing emails containing malicious attachments or links. Once installed, Grandoreiro monitors user activity, captures credentials, and facilitates unauthorized transactions by exploiting banking sessions. Its modular architecture allows it to update its capabilities, making it a persistent threat to financial institutions and their customers.

Indicator of compromise

SHA-256

f11e0cd1f8fcf1d24efe1067799e02536ca443521160bb28d8fcb12ec606bc15

314ef1e398e8d67500eca9992ae87c3cce9df2df19d3087cc4275d4439a8e30a

a9772d905693ffc6af1d11da43947e7fa5089a282ded865364582ade7a0f84c0

e53d2b092faa25adf2e2d4eff1a9c0bb05dd4631738fa2cb88c62eccda40dce9

SHA-1

f5080b7cf80a78aabb957c2e1d932f4a86dfa150

170e6bbbd9ad6216fb843f5562c47194b6f3c795

080cfe8a4e7dcd388cf5459fcce96b2b1a7090ba

57990711382ddc7fd99f6757ce7ad5f0fac969e3

MD-5

9e9a515259fedfcca8e96e9fac66a3d7

0307828ec37194201bf7a07bcf234f1b

93ecc955ee53033c6e6fe56b3914ed82

7492695ed01d88dbab5eaf8088a58545

Remedation

1. Segregate critical systems from less secure parts of the network to limit the spread of malware.
2. Deploy comprehensive endpoint security solutions that can detect and block malicious activities in real-time.
3. Regularly conduct cybersecurity awareness training focused on phishing threats and safe email handling procedures.
4. Implement network segmentation to isolate critical systems, reducing the risk of malware spreading across the organization.
5. Block all IOCs on your XDR, EDR and other security tools.

THREAT CURE
RE-ARCHITECT YOUR THREAT LANDSCAPE

ThreatCure

Cyber Threat Advisory

Secure your byte world

https://threatcure.net/ info@threatcure.net +1 (832) 271 2738