Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 23:46:55 UTC

Tool: Grandoreiro

Names	Grandoreiro
Category	Malware
Type	Banking trojan, Credential stealer
Description	(segurancainformatica) Grandoreiro is a Latin American banking trojan targeting Brazil, Mexico, Spain, Peru, and has now extended to Portugal. Cybercriminals attempt to compromise computers to generate revenue by exfiltrating information from victims' devices, typically banking-related information. During April and May 2020, a new Grandoreiro variant was identified. This piece of malware includes improvements in the way it is operating. The threat has been disseminating via malscam campaigns, as in the past, and the name of the victim is used as a part of the malicious attachment name, as shown below.
Information	<https://seguranca-informatica.pt/the-updated-grandoreiro-malware-equipped-with-latenbot-c2-features-in-q2-2020-now-extended-to-portuguese-banks/> <https://www.welivesecurity.com/2020/04/28/grandoreiro-how-engorged-can-exe-get/> <https://www.welivesecurity.com/wp-content/uploads/2020/07/ESET_Threat_Report_Q22020.pdf> <https://securelist.com/the-tetrade-brazilian-banking-malware/97779/> <https://www.zscaler.com/blogs/security-research/grandoreiro-banking-trojan-new-ttps-targeting-various-industry-verticals> <https://www.proofpoint.com/us/blog/threat-insight/copacabana-barcelona-cross-continental-threat-brazilian-banking-malware> <https://www.welivesecurity.com/en/eset-research/eset-takes-part-global-operation-disrupt-grandoreiro-banking-trojan/> <https://www.interpol.int/News-and-Events/News/2024/Disrupting-a-Grandoreiro-malware-operation> <https://www.trendmicro.com/en_us/research/24/d/trend-micro-collaborated-with-interpol-in-cracking-down-grandore.html> <https://securityintelligence.com/x-force/grandoreiro-banking-trojan-unleashed/> <https://flashpoint.io/blog/grandoreiro-malware-exploits/>

	<https://securelist.com/grandoreiro-banking-trojan/114257/> <https://www.forcepoint.com/blog/x-labs/grandoreiro-trojan-targets-mexico-argentina-spain> <https://hackread.com/grandoreiro-strikes-geofenced-phishing-attacks-latam/>
MITRE ATT&CK	<https://attack.mitre.org/software/S0531/>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.grandoreiro>
AlienVault OTX	<https://otx.alienvault.com/browse/pulses?q=tag:grandoreiro>

Last change to this tool card: 21 April 2025

Download this tool card in JSON format

All groups using tool Grandoreiro

Changed	Name	Country	Observed	
Unknown groups				
	[Interesting malware not linked to an actor yet]			

1 group listed (0 APT, 0 other, 1 unknown)
