Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 20:46:29 UTC

Tool: TOITOIN

Names	TOITOIN
Category	Malware
Type	Banking trojan, Backdoor, Info stealer, Credential stealer
Description	(Zscaler) In the ever-evolving landscape of cyber threats, researchers from Zscaler ThreatLabz have recently uncovered a concerning development: a new targeted attack campaign striking businesses in the Latin American (LATAM) region. This sophisticated campaign employs a trojan that follows a multi-staged infection chain, utilizing specially crafted modules throughout each stage. These modules are custom designed to carry out malicious activities, such as injecting harmful code into remote processes, circumventing User Account Control via COM Elevation Moniker, and evading detection by Sandboxes through clever techniques like system reboots and parent process checks. The ultimate payload of this campaign is a new Latin American Trojan called TOITOIN, which incorporates a unique XOR decryption technique to decode its configuration file. Once decrypted, the trojan gathers crucial system information, as well as data pertaining to installed browsers and the Topaz OFD Protection Module, before sending it to the command and control server of the attackers in an encoded format.
Information	<https://www.zscaler.com/blogs/security-research/toitoin-trojan-analyzing-new-multi-stage-attack-targeting-latam-region>

Last change to this tool card: 05 September 2023

Download this tool card in JSON format

All groups using tool TOITOIN

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

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