Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 17:02:25 UTC

Tool: Citadel

Names	Citadel
Category	Malware
Type	Banking trojan, POS malware, Info stealer, Credential stealer
Description	(Malwarebytes) Citadel is an offspring of the (too) popular Zeus crimekit whose main goal is to steal banking credentials by capturing keystrokes and taking screenshots/videos of victims' computers. Citadel came out circa January 2012 in the online forums and quickly became a popular choice for criminals. A version of Citadel (1.3.4.5) was leaked in late October and although it is not the latest (1.3.5.1), it gives us a good insight into what tools the bad guys are using to make money.
Information	<https://blog.malwarebytes.com/threat-analysis/2012/11/citadel-a-cyber-criminals-ultimate-weapon/> <https://www.arbornetworks.com/blog/asert/the-citadel-and-gameover-campaigns-of-5cb682c10440b2ebaf9f28c1fe438468/> <http://blog.jpcert.or.jp/2016/02/banking-trojan--27d6.html> <http://www.xylibox.com/2016/02/citadel-0011-atmos.html> <https://www.secureworks.com/research/point-of-sale-malware-threats> <https://en.wikipedia.org/wiki/Citadel_(malware)>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.citadel>
AlienVault OTX	<https://otx.alienvault.com/browse/pulses?q=tag:citadel>

Last change to this tool card: 25 May 2020

Download this tool card in JSON format

All groups using tool Citadel

Changed	Name	Country	Observed

APT groups				
	MoneyTaker		2016	
Other groups				
	Retefe Gang, Operation Emmental		2013	

2 groups listed (1 APT, 1 other, 0 unknown)

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=7e9130ea-d66e-4ea8-b950-2a7dae68f51b