Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 14:25:12 UTC

Tool: Odinaff

Names	Odinaff
Category	Malware
Type	Backdoor, Info stealer
Description	(ZDNet) Odinaff is a sophisticated Trojan which is capable of taking screenshots of infected systems between every five and 30 seconds which it sends back to a remote command-and-control server. The Trojan also downloads and executes RC4 cipher keys and can issue shell commands. Once the Odinaff Trojan has performed the initial compromise of the infected machine, a second piece of malware known as Backdoor Batel is installed. This second malware infection is capable of running payloads solely in the memory, effectively enabling it to stealthily run in the background.
Information	<https://www.zdnet.com/article/odinaff-trojan-attacks-banks-and-more-monitoring-networks-and-stealing-credentials/>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.odinaff>
AlienVault OTX	<https://otx.alienvault.com/browse/pulses?q=tag:Odinaff>

Last change to this tool card: 23 April 2020

Download this tool card in JSON format

All groups using tool Odinaff

Changed	Name	Country	Observed	
APT groups				
	Carbanak, Anunak		2013-Apr 2023	

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