Threat Group Cards: A Threat Actor Encyclopedia

Tool: RatSnif

Names	RatSnif
Category	Malware
Type	Backdoor, Info stealer, Poisoning
Description	(Cylance) Blackberry Cylance threat researchers have analyzed the Ratsnif trojans, which offer a veritable swiss-army knife of network attack techniques. The trojans, under active development since 2016, combine capabilities like packet sniffing, gateway/device ARP poisoning, DNS poisoning, HTTP injection, and MAC spoofing.
Information	<https://threatvector.cylance.com/en_us/home/threat-spotlight-ratsnif-new-network-vermin-from-oceanlotus.html>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.ratsnif>
AlienVault OTX	<https://otx.alienvault.com/browse/pulses?q=tag:Ratsnif>

Last change to this tool card: 24 April 2021

Download this tool card in JSON format

All groups using tool RatSnif

Changed	Name	Country	Observed	
APT groups				
	APT 32, OceanLotus, SeaLotus		2013-Aug 2024	

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