NetWire RC - Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 17:06:40 UTC

Tool: NetWire RC

Names	NetWire RC NetWire RAT NetWired RC NetWire NetWeird Recam
Category	Malware
Type	POS malware, Backdoor, Keylogger, Credential stealer
Description	Netwire is a RAT, its functionality seems focused on password stealing and keylogging, but includes remote control capabilities as well. Keylog files are stored on the infected machine in an obfuscated form. The algorithm is: for i in range(0,num_read): buffer[i] = ((buffer[i]-0x24)^0x9D)&0xFF
Information	<http://researchcenter.paloaltonetworks.com/2014/08/new-release-decrypting-netwire-c2-traffic/> <https://www.circl.lu/pub/tr-23/> <https://www.fireeye.com/blog/threat-research/2017/09/apt33-insights-into-iranian-cyber-espionage.html> <http://blog.talosintelligence.com/2017/12/recam-redux-deconfusing-confuserex.html> <https://www.secureworks.com/blog/netwire-rat-steals-payment-card-data> <https://maskop9.wordpress.com/2019/01/30/analysis-of-netwiredrc-trojan/> <https://yoroi.company/research/new-cyber-operation-targets-italy-digging-into-the-netwire-attack-chain/> <https://blog.talosintelligence.com/2022/01/nanocore-netwire-and-asyncrat-spreading.html>
MITRE ATT&CK	<https://attack.mitre.org/software/S0198/>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.netwire>

AlienVault OTX	<https://otx.alienvault.com/browse/pulses?q=tag:Netwire>

Last change to this tool card: 28 December 2022

Download this tool card in JSON format

All groups using tool NetWire RC

Changed	Name	Country	Observed	
APT groups				
	APT 33, Elfin, Magnallium		2013-Apr 2024	
	Gorgon Group		2017-Jul 2020	
	OPERA1ER	[Unknown]	2016-Jul 2023	
	Operation Armor Piercer		2020	
	PassCV		2016	
	RATicate	[Unknown]	2019	
	TA2541	[Unknown]	2017	

7 groups listed (7 APT, 0 other, 0 unknown)

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=0ddad3ec-e810-4333-827b-2d03a3627403