ETDA สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์
Electronic Transactions Development Agency

Threat Group Cards: A Threat Actor Encyclopedia

Tool: RemcosRAT

Names	RemcosRAT Remcos Remvio Socmer
Category	Tools
Type	Backdoor, Info stealer, Exfiltration
Description	Remcos is a closed-source tool that is marketed as a remote control and surveillance software by a company called Breaking Security. Remcos has been observed being used in malware campaigns.
Information	<https://blog.trendmicro.com/trendlabs-security-intelligence/analysis-new-remcos-rat-arrives-via-phishing-email/> <https://www.riskiq.com/blog/labs/spear-phishing-turkish-defense-contractors/> <https://researchcenter.paloaltonetworks.com/2018/08/unit42-gorgon-group-slithering-nation-state-cybercrime/> <http://malware-traffic-analysis.net/2017/12/22/index.html> <https://blog.fortinet.com/2017/02/14/remcos-a-new-rat-in-the-wild-2> <https://krabsonsecurity.com/2018/03/02/analysing-remcos-rats-executable/> <https://myonlinesecurity.co.uk/fake-order-spoofed-from-finchers-ltd-sankyo-rubber-delivers-remcos-rat-via-ace-attachments/> <https://blog.talosintelligence.com/2018/08/picking-apart-remcos.html> <https://secrary.com/ReversingMalware/RemcosRAT/> <https://blog.malwarebytes.com/threat-analysis/2021/07/remcos-rat-delivered-via-visual-basic/> <https://blog.morphisec.com/remcos-trojan-analyzing-attack-chain> <https://www.fortinet.com/blog/threat-research/latest-remcos-rat-phishing> <https://therecord.media/remcos-spyware-ukraine-government-agencies-uac0050/> <https://www.mcafee.com/blogs/other-blogs/mcafee-labs/peeling-back-the-layers-of-remcosrat-malware/> <https://therecord.media/remcos-phishing-ukraine-government-agencies> <https://asec.ahnlab.com/en/58195/> <https://asec.ahnlab.com/en/60270/> <https://asec.ahnlab.com/en/65111/> <https://blog.sonicwall.com/en-us/2024/05/remcos-is-pairing-with-privateloader-to-extend-its-capabilities/> <https://asec.ahnlab.com/en/66463/> <https://www.fortinet.com/blog/threat-research/new-campaign-uses-remcos-rat-to-exploit-victims> <https://www.mcafee.com/blogs/other-blogs/mcafee-labs/the-stealthy-stalker-remcos-rat/>
MITRE ATT&CK	<https://attack.mitre.org/software/S0332/>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.remcos>
AlienVault OTX	<https://otx.alienvault.com/browse/pulses?q=tag:RemcosRAT>

Last change to this tool card: 27 December 2024

Download this tool card in JSON format

All groups using tool RemcosRAT

Changed	Name	Country	Observed

APT groups

APT 33, Elfin, Magnallium		2013-Apr 2024	
Blind Eagle		2018-Nov 2024	
Gamaredon Group		2013-Feb 2025	
Gorgon Group		2017-Jul 2020	
LazyScripter	[Unknown]	2018	
OPERA1ER	[Unknown]	2016-Jul 2023	
Operation Comando	[Unknown]	2018	
Operation Spalax	[Unknown]	2020	
RATicate	[Unknown]	2019	
TA2722	[Unknown]	2020	
TA558	[Unknown]	2018-Jun 2023	
Vendetta, TA2719		2020	

12 groups listed (12 APT, 0 other, 0 unknown)

↑

Infrastructure and Security Department
Electronic Transactions Development Agency

Follow us on

Report incidents

+66 (0)2-123-1227

helpdesk@etda.or.th