Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 22:04:43 UTC

Tool: RedLeaves

Names	RedLeaves BUGJUICE
Category	Malware
Type	Reconnaissance, Backdoor
Description	(US-CERT) The REDLEAVES implant consists of three parts: an executable, a loader, and the implant shellcode. The REDLEAVES implant is a remote administration Trojan (RAT) that is built in Visual C++ and makes heavy use of thread generation during its execution. The implant contains a number of functions typical of RATs, including system enumeration and creating a remote shell back to the C2.
Information	<https://www.us-cert.gov/ncas/alerts/TA17-117A> <http://blog.macnica.net/blog/2017/12/post-8c22.html> <https://www.accenture.com/t20180423T055005Z__w__/se-en/_acnmedia/PDF-76/Accenture-Hogfish-Threat-Analysis.pdf> <http://blog.jpcert.or.jp/.s/2017/04/redleaves---malware-based-on-open-source-rat.html> <https://www.jpcert.or.jp/magazine/acreport-redleaves.html> <https://www.pwc.co.uk/cyber-security/pdf/cloud-hopper-annex-b-final.pdf> <http://go.recordedfuture.com/hubfs/reports/cta-2019-0206.pdf> <https://github.com/nccgroup/Cyber-Defence/tree/master/Technical%20Notes/Red%20Leaves>
MITRE ATT&CK	<https://attack.mitre.org/software/S0153/>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.redleaves>
AlienVault OTX	<https://otx.alienvault.com/browse/pulses?q=tag:redleaves>

Last change to this tool card: 14 May 2020

Download this tool card in JSON format

All groups using tool RedLeaves

Changed	Name	Country	Observed	
APT groups				
	Stone Panda, APT 10, menuPass		2006-Mar 2025	

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

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=30de5fb0-f7b6-4795-9732-e90515d91451