Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 13:24:21 UTC

Tool: PlugX

Names	PlugX Destroy RAT DestroyRAT Korplug Sogu Kaba Xamtrav Agent.dhwf RedDelta TIGERPLUG Thoper TVT
Category	Malware
Type	Reconnaissance, Backdoor, Keylogger, Info stealer, Exfiltration
Description	(US-CERT) PLUGX is a sophisticated Remote Access Tool (RAT) operating since approximately 2012. Although there are now many variants of this RAT in existence today, there are still characteristics common to most variants.
Information	<https://www.us-cert.gov/ncas/alerts/TA17-117A> <https://threatrecon.nshc.net/2019/03/19/sectorm04-targeting-singapore-custom-malware-analysis/> <http://blog.jpcert.or.jp/2015/01/analysis-of-a-r-ff05.html> <http://blog.jpcert.or.jp/2017/02/plugx-poison-iv-919a.html> <http://blog.jpcert.or.jp/.s/2017/04/redleaves---malware-based-on-open-source-rat.html> <https://countuponsecurity.com/2018/02/04/malware-analysis-plugx/> <https://circl.lu/assets/files/tr-12/tr-12-circl-plugx-analysis-v1.pdf> <https://www.rsa.com/content/dam/pdfs/2-2017/kingslayer-a-supply-chain-attack.pdf> <https://www.pwc.co.uk/cyber-security/pdf/cloud-hopper-annex-b-final.pdf> <http://blog.airbuscybersecurity.com/post/2014/01/plugx-some-uncovered-points.html> <https://community.rsa.com/thread/185439> <https://researchcenter.paloaltonetworks.com/2017/06/unit42-paranoid-plugx/>

	<https://www.lac.co.jp/lacwatch/people/20171218_001445.html> <https://countuponsecurity.com/2018/05/09/malware-analysis-plugx-part-2/> <https://securelist.com/time-of-death-connected-medicine/84315/> <https://www.arbornetworks.com/blog/asert/wp-content/uploads/2016/01/ASERT-Threat-Intelligence-Brief-2015-08-Uncovering-the-Seven-Point-Dagger.pdf> <https://blog.malwarebytes.com/threat-analysis/2016/08/unpacking-the-spyware-disguised-as-antivirus/> <https://www.sophos.com/en-us/medialibrary/pdfs/technical%20papers/plugx-thenextgeneration.pdf> <https://www.cybereason.com/blog/threat-analysis-report-plugx-rat-loader-evolution> <https://unit42.paloaltonetworks.com/plugx-variants-in-usbs/> <https://asec.ahnlab.com/en/49097/> <https://blog.sekoia.io/unplugging-plugx-sinkholing-the-plugx-usb-worm-botnet/> <https://www.bleepingcomputer.com/news/security/french-police-push-plugx-malware-self-destruct-payload-to-clean-pcs/> <https://www.bleepingcomputer.com/news/security/fbi-deletes-chinese-plugx-malware-from-thousands-of-us-computers/>
MITRE ATT&CK	<https://attack.mitre.org/software/S0013/>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.plugx>
AlienVault OTX	<https://otx.alienvault.com/browse/pulses?q=tag:plugx>
Playbook	<https://pan-unit42.github.io/playbook_viewer/?pb=plugx-malware>

Last change to this tool card: 22 February 2025

Download this tool card in JSON format

All groups using tool PlugX

Changed	Name	Country	Observed	
APT groups				
	APT 3, Gothic Panda, Buckeye		2007-Nov 2017	
	APT 17, Deputy Dog, Elderwood, Sneaky Panda		2009-Jun 2024	
	APT 20, Violin Panda		2014-2017	
	APT 31, Judgment Panda, Zirconium		2016-Mar 2024	

	APT 41		2012-Jul 2025	●
	AVIVORE		2015	
	Axiom, Group 72		2008-2008/2014	
	Barium		2016-Nov 2017	●
	Bookworm		2015	
	Bronze Starlight		2021-Mar 2023	
	Calypso		2016-Aug 2021	
	Carderbee		2023	
	CardinalLizard		2014	
	DragonOK		2015-Jan 2017	
	Earth Berberoka		2022	
	Earth Krahang		2022	
	Emissary Panda, APT 27, LuckyMouse, Bronze Union		2010-Aug 2023	
	Goblin Panda, Cycldek, Conimes		2013-Jun 2020	
	IronHusky		2017-Aug 2021	
	Leviathan, APT 40, TEMP.Periscope		2013-Jul 2021	●
	Mustang Panda, Bronze President		2012-Jun 2025	
	Naikon, Lotus Panda		2010-Apr 2022	
	NetTraveler, APT 21, Hammer Panda		2004-Dec 2015	
	Nightshade Panda, APT 9, Group 27		2013-Sep 2016	
	Operation Diplomatic Specter		2022	
	Operation Harvest		2016	

	Operation Jacana		2023	
	RedDelta		2020-Jul 2023	
	RedFoxtrot		2014-Aug 2021	
	RedGolf		2014	
	Roaming Tiger		2014-Aug 2015	
	Samurai Panda		2009	
	Space Pirates		2017-Nov 2024	
	Stone Panda, APT 10, menuPass		2006-Mar 2025	●
	TA428		2013-Jan 2022	
	TA459		2017-Apr 2022	
	Turbine Panda, APT 26, Shell Crew, WebMasters, KungFu Kittens		2010-Oct 2018	●
	Velvet Ant		2023-Jul 2024	
	Wicked Spider, APT 22		2018	

39 groups listed (39 APT, 0 other, 0 unknown)

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=20865c5a-3bb0-413b-b59b-9a994303a9c9