Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 18:01:57 UTC

Tool: Konni

Names	Konni
Category	Malware
Type	Backdoor, Info stealer
Description	Konni is a remote administration tool, observed in the wild since early 2014. The Konni malware family is potentially linked to APT37, a North-Korean cyber espionage group active since 2012. The group primary victims are South-Korean political organizations, as well as Japan, Vietnam, Russia, Nepal, China, India, Romania, Kuwait, and other parts of the Middle East.
Information	<https://blog.talosintelligence.com/2017/05/konni-malware-under-radar-for-years.html> <https://blog.fortinet.com/2017/08/15/a-quick-look-at-a-new-konni-rat-variant> <https://vallejo.cc/2017/07/08/analysis-of-new-variant-of-konni-rat/> <http://blog.talosintelligence.com/2017/07/konni-references-north-korean-missile-capabilities.html> <https://us-cert.cisa.gov/ncas/alerts/aa20-227a> <https://blog.malwarebytes.com/threat-intelligence/2022/01/konni-evolves-into-stealthier-rat/> <https://medium.com/@DCSO_CyTec/to-russia-with-love-assessing-a-konni-backdoored-suspected-russian-consular-software-installer-ce618ea4b8f3>
MITRE ATT&CK	<https://attack.mitre.org/software/S0356/>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.konni>
AlienVault OTX	<https://otx.alienvault.com/browse/pulses?q=tag:konni>

Last change to this tool card: 07 March 2024

Download this tool card in JSON format

All groups using tool Konni

Changed	Name	Country	Observed

APT groups

	Reaper, APT 37, Ricochet Chollima, ScarCruft		2012-Mar 2025	

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

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=d238a221-2a1d-4558-9dbf-7a3a6bbb0d22