


Roaming Tiger - Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 18:07:20 UTC

[Home](#) > [List all groups](#) > Roaming Tiger

APT group: Roaming Tiger

Names	Roaming Tiger (<i>ESET</i>) Rotten Tomato (<i>Sophos</i>) CTG-7273 (<i>SecureWorks</i>) Bronze Woodland (<i>SecureWorks</i>)	
Country	 China	
Motivation	Information theft and espionage	
First seen	2014	
Description	(Palo Alto) In late 2014, ESET presented an attack campaign that had been observed over a period of time targeting Russia and other Russian speaking nations, dubbed “Roaming Tiger”. The attack was found to heavily rely on RTF exploits and at the time, thought to make use of the PlugX malware family.	
Observed	Countries: Belarus , Kazakhstan , Kyrgyzstan , Russia , Tajikistan , Ukraine , Uzbekistan .	
Tools used	BBSRAT , Gh0st RAT , PlugX .	
Operations performed	Aug 2015	< https://unit42.paloaltonetworks.com/bbsrat-attacks-targeting-russian-organizations-linked-to-roaming-tiger/ >
Information	< http://2014.zeronights.org/assets/files/slides/roaming_tiger_zeronights_2014.pdf >	

Last change to this card: 10 August 2021

Download this actor card in [PDF](#) or [JSON](#) format

Source: <https://apt.etda.or.th/cgi-bin/showcard.cgi?u=ee5e9d82-26c3-4f35-bee4-457ab5e20119>