

Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 18:45:29 UTC

APT group: AtlasCross

Names	AtlasCross (<i>NSFOCUS</i>)
Country	[Unknown]
Motivation	Information theft and espionage
First seen	2023
Description	<p>(NSFOCUS) After an in-depth study of the attack process, NSFOCUS Security Labs found that this APT attacker is quite different from known attacker characteristics in terms of execution flow, attack technology stack, attack tools, implementation details, attack objectives, behavior tendency and other main attribution indicators. The technical level and cautious attitude shown by this attacker during this activity are also worthy of attention.</p> <p>Therefore, NSFOCUS Security Labs identified the orchestrator of this event as a new attacker and named it AtlasCross.</p> <p>NSFOCUS Security Labs validated the high-level threat attributes of AtlasCross in terms of development technology and attack strategy through an in-depth analysis of its attack metrics. At this current stage, AtlasCross has a relatively limited scope of activity, primarily focusing on targeted attacks against specific hosts within a network domain. However, the attack processes they employ are highly robust and mature. NSFOCUS Security Labs deduce that this attacker is highly likely to deploy this attack process into larger-scale network attack operations.</p> <p>The organizational origin of the AtlasCross attacker cannot be determined.</p>
Observed	
Tools used	AtlasAgent , DangerAds .
Information	< http://nsfocusglobal.com/warning-newly-discovered-apt-attacker-atlascross-exploits-red-cross-blood-drive-phishing-for-cyberattack/ >

Last change to this card: 12 October 2023

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

Source: <https://apt.eta.or.th/cgi-bin/showcard.cgi?u=44cf4c8d-c5b1-467a-a474-ed16373f0881>