

Operation SignSight - Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 13:25:45 UTC

[Home](#) > [List all groups](#) > Operation SignSight

APT group: Operation SignSight

Names	Operation SignSight (<i>ESET</i>)
Country	[Unknown]
Motivation	Information theft and espionage
First seen	2020
Description	<p>(ESET) Just a few weeks after the supply-chain attack on the Able Desktop software, another similar attack occurred on the website of the Vietnam Government Certification Authority (VGCA): ca.gov.vn. The attackers modified two of the software installers available for download on this website and added a backdoor in order to compromise users of the legitimate application.</p> <p>ESET researchers uncovered this new supply-chain attack in early December 2020 and notified the compromised organization and the VNCERT. We believe that the website has not been delivering compromised software installers as of the end of August 2020 and ESET telemetry data does not indicate the compromised installers being distributed anywhere else. The Vietnam Government Certification Authority confirmed that they were aware of the attack before our notification and that they notified the users who downloaded the trojanized software.</p>
Observed	Countries: Vietnam .
Tools used	Mimikatz , PhantomNet .
Information	< https://www.welivesecurity.com/2020/12/17/operation-signsight-supply-chain-attack-southeast-asia/ >

Last change to this card: 07 January 2021

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

Source: <https://apt.eta.org.th/cgi-bin/showcard.cgi?u=e8cfaf96-906e-42f6-a677-da2aee6b662d>