Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 13:12:45 UTC

APT group: NineBlog

Names	NineBlog *(FireEye)*
Country	China
Motivation	Information theft and espionage
First seen	2013
Description	(FireEye) FireEye has been tracking ongoing activity associated with a unique and relatively stealthy group we first identified in 2013 using the name “APT.NineBlog.“ The name NINEBLOG refers to a specific backdoor used by the threat group; some versions of the backdoor use the string ‘nineblog’ in their command and control (CnC) URI path. We have observed this group targeting organizations primarily in South Asia and the Middle East. The threat group is notable because it employs Visual Basic Scripts (VBScripts) as a backdoor, a tactic we do not often observe. The group can maintain a low profile probably because the VBScripts are small and stealthy in their execution. The NINEBLOG malware is difficult to detect because the VBScripts are encoded and the actors employ SSL network communications. We have observed intermittent activity from this group since we first identified it in 2013, and we saw a spike in activity during mid-2015. We assess that one of the probable targets of the group’s 2015 campaign is a Southeast Asian government, based on the specificity of some of the decoy documents. In addition to the anti-analysis techniques, the group has used SSL communications since we first identified this activity in 2013. The use of encrypted SSL traffic makes it extremely difficult to develop network-based signatures to detect the malware’s communications.
Observed	Sectors: Government. Countries: South Asia, Southeast Asia and Middle East.
Tools used	NineBlog.
Information	<https://www.fireeye.com/blog/threat-research/2013/08/the-curious-case-of-encoded-vb-scripts-apt-nineblog.html> <https://www2.fireeye.com/rs/848-DID-242/images/rpt-southeast-asia-fall-2015.pdf>

Last change to this card: 01 May 2020

Download this actor card in PDF or JSON format
