Threat Group Cards: A Threat Actor Encyclopedia

Tool: NineBlog

Names	NineBlog
Category	Malware
Type	Reconnaissance, Backdoor
Description	(FireEye) We noticed the decoded VBScript backdoors from recent activity were nearly identical (with some small changes) to the first NINEBLOG variants we observed in 2013. The minimal code changes may be due to the fact that the encoding provides enough obfuscation to prevent detection, allowing the core functionality of the backdoor to remain the same. Additionally, newer variants of the VBScript include some code enhancements.
Information	<https://www2.fireeye.com/rs/848-DID-242/images/rpt-southeast-asia-fall-2015.pdf> <https://www.fireeye.com/blog/threat-research/2013/08/the-curious-case-of-encoded-vb-scripts-apt-nineblog.html>

Last change to this tool card: 01 May 2020

Download this tool card in JSON format

All groups using tool NineBlog

Changed	Name	Country	Observed	
APT groups				
	NineBlog		2013	

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