Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 14:31:52 UTC

Tool: Sneepy

Names	Sneepy ByeByeShell
Category	Malware
Type	Reconnaissance, Backdoor
Description	(Rapid7) The main backdoor installed and executed on the victims' systems appears to be a custom reverse shell with just a handful of features. Due to a lack of public literature about this case, I decided to dub this family as ByeByeShell. When disassembling the binary you can quickly understand the mechanics of the backdoor. After some quick initialization, the backdoor XORs an embedded string with 0x9D to extract the IP address of the C&C server. Subsequently it establishes a connection to it (generally on port 80) and checks in with some basic information about the system. After the check-in message is sent, the malware enters a continuous loop in which it will keep silently waiting for commands from the open socket connection. From now on, it expects some manual interaction from the attacker. The supported commands are: • shell • comd • sleep • quit • kill
Information	<https://blog.rapid7.com/2013/08/19/byebye-and-the-targeting-of-pakistan/> <https://researchcenter.paloaltonetworks.com/2016/09/unit42-confucius-says-malware-families-get-further-by-abusing-legitimate-websites/>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.sneepy>
AlienVault OTX	<https://otx.alienvault.com/browse/pulses?q=tag:sneepy>

Last change to this tool card: 14 May 2020

Download this tool card in JSON format

All groups using tool Sneepy

Changed	Name	Country	Observed	
APT groups				
	Confucius		2013-Aug 2021	

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

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=a14d2307-9669-4ae7-afd3-f2af09e498b2