Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 13:28:51 UTC

Tool: Comnie

Names	Comnie
Category	Malware
Type	Backdoor
Description	(Palo Alto) Unit 42 has been tracking a series of attacks using a remote backdoor malware family named Comnie, which have been observed targeting organizations in the East Asia region. Comnie, first named by Sophos seemingly after the Windows LNK file name it created, is a custom malware family that is used in targeted attacks, and has been observed in the wild since at least April 2013. The Comnie malware family is notable in that it leverages online blogs and third-party services to obtain command and control (C2) information. Recent instances of the malware have been observed leveraging github.com, tumbler.com, and blogspot.com. Attackers using Comnie are leveraging malicious macros that initially hide decoy documents and shows them when the victim enables macros. These decoys documents pertain to various subject matters that the targets would be likely to be interested in.
Information	<https://unit42.paloaltonetworks.com/unit42-comnie-continues-target-organizations-east-asia/>
MITRE ATT&CK	<https://attack.mitre.org/software/S0244/>
AlienVault OTX	<https://otx.alienvault.com/browse/pulses?q=tag:comnie>

Last change to this tool card: 22 April 2020

Download this tool card in JSON format

All groups using tool Comnie

Changed	Name	Country	Observed
APT groups			

	Blackgear		2018-Jul 2018	

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

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=3b94ba59-fbb3-4852-8442-4b5483208a67