Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 15:31:40 UTC

Tool: KOMPROGO

Names	KOMPROGO Splinter RAT
Category	Malware
Type	Reconnaissance, Backdoor, Info stealer, Downloader
Description	(Cylance) Splinter arrives as an MSBuild project file containing a Base64 encoded PowerShell script generated using the MSFvenom psh-reflection module. As in the case of Remy, it utilizes on-the-fly C# compilation and strips off several PowerShell wrappers before the shellcode that calls the final payload is invoked. The backdoor itself is a Win32 PE EXE file and has the capability to collect information, download and execute payloads, run WMI queries, and manipulate files, processes, and registry entries. The overall functionality of Splinter appears pretty much in line with the “KOMPROGO” malware (as described in the FireEye APT32 report).
Information	<https://www.cylance.com/content/dam/cylance-web/en-us/resources/knowledge-center/resource-library/reports/SpyRATsofOceanLotusMalwareWhitePaper.pdf> <https://www.fireeye.com/blog/threat-research/2017/05/cyber-espionage-apt32.html>
MITRE ATT&CK	<https://attack.mitre.org/software/S0156/>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.komprogo>
AlienVault OTX	<https://otx.alienvault.com/browse/pulses?q=tag:KOMPROGO>

Last change to this tool card: 14 May 2020

Download this tool card in JSON format

All groups using tool KOMPROGO

Changed	Name	Country	Observed
APT groups			

	APT 32, OceanLotus, SeaLotus		2013-Aug 2024	
	FIN10	[Unknown]	2016	

2 groups listed (2 APT, 0 other, 0 unknown)

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=27f94f7d-9871-458b-aac3-7d48efce7047