Living off the Land - Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 23:43:16 UTC

Tool: Living off the Land

Names	Living off the Land LOLBins LOLBAS
Category	Tools
Description	(Talos) Attackers' trends tend to come and go. But one popular technique we're seeing at this time is the use of living-off-the-land binaries — or 'LoLBins'. LoLBins are used by different actors combined with fileless malware and legitimate cloud services to improve chances of staying undetected within an organisation, usually during post-exploitation attack phases. Living-off-the-land tactics mean that attackers are using pre-installed tools to carry out their work. This makes it more difficult for defenders to detect attacks and researchers to identify the attackers behind the campaign. In the attacks we're seeing, there are binaries supplied by the victim's operating system that are normally used for legitimate purposes, but in these cases, are being abused by the attackers. (LOLBAS Project) The goal of the LOLBAS project is to document every binary, script, and library that can be used for Living Off The Land techniques. A LOLBin/Lib/Script must: • Be a Microsoft-signed file, either native to the OS or downloaded from Microsoft. • Have extra 'unexpected' functionality. It is not interesting to document intended use cases. o Exceptions are application whitelisting bypasses • Have functionality that would be useful to an APT or red team Interesting functionality can include: • Executing code o Arbitrary code execution o Pass-through execution of other programs (unsigned) or scripts (via a LOLBin)

	• Compiling code • File operations o Downloading o Upload o Copy • Persistence o Pass-through persistence utilizing existing LOLBin o Persistence (e.g. hide data in ADS, execute at logon) • UAC bypass • Credential theft • Dumping process memory • Surveillance (e.g. keylogger, network trace) • Log evasion/modification • DLL side-loading/hijacking without being relocated elsewhere in the filesystem.
Information	<https://github.com/LOLBAS-Project/LOLBAS> <https://lolbas-project.github.io/> <https://blog.talosintelligence.com/2019/11/hunting-for-lolbins.html> <https://www.microsoft.com/security/blog/2021/03/09/azure-lolbins-protecting-against-the-dual-use-of-virtual-machine-extensions/> <https://www.darkreading.com/edge-articles/is-an-attacker-living-off-your-land-> <https://www.cybereason.com/blog/threat-hunting-from-lolbins-to-your-crown-jewels> <https://pentera.io/blog/the-lol-isnt-so-funny-when-it-bites-you-in-the-bas/> <https://www.darkreading.com/vulnerabilities-threats/as-lotl-attacks-evolve-so-must-defenses> <https://blog.barracuda.com/2025/03/03/living-off-the-land--how-threat-actors-use-your-system-to-steal-> <https://www.helpnetsecurity.com/2025/07/01/bitdefender-lotl-security-incidents-phasr/>
AlienVault OTX	<https://otx.alienvault.com/browse/pulses?q=tag:lolbin>

Last change to this tool card: 16 August 2025

Download this tool card in JSON format

All groups using tool Living off the Land

Changed	Name	Country	Observed	
APT groups				
	↳ Subgroup: Scattered Spider	[Unknown]	2022-Aug 2025	

	Antlion		2011	
	APT 20, Violin Panda		2014-2017	
	APT 29, Cozy Bear, The Dukes		2008-Feb 2025	●
	APT 33, Elfin, Magnallium		2013-Apr 2024	
	APT 41		2012-Jul 2025	●
	↳ Subgroup: Earth Freybug		2012	
	AVIVORE		2015	
	Berserk Bear, Dragonfly 2.0		2015-May 2017	
	BlackTech, Circuit Panda, Radio Panda		2010-Oct 2020	
	Bronze Highland		2012-Jul 2024	
	Cadet Blizzard		2020-Jun 2024	●
	Calypso		2016-Aug 2021	
	Chafer, APT 39		2014-Sep 2020	●
	Comment Crew, APT 1		2006-May 2018	●
	Dark Pink	[Unknown]	2022-Feb 2023	
	El Machete	[Unknown]	2010-Mar 2022	
	Emissary Panda, APT 27, LuckyMouse, Bronze Union		2010-Aug 2023	
	FIN6, Skeleton Spider	[Unknown]	2015-Oct 2021	●
	Flax Typhoon		2021-Nov 2023	
	FunnyDream		2018	
	Gallmaker	[Unknown]	2017	
	Gangnam Industrial Style	[Unknown]	2019	
	Goblin Panda, Cycldek, Conimes		2013-Jun 2020	

	Gorgon Group		2017-Jul 2020	
	Honeybee	[Unknown]	2017	
	Hydrochasma	[Unknown]	2022	
	Ke3chang, Vixen Panda, APT 15, GREF, Playful Dragon		2010-Oct 2024	
	Kimsuky, Velvet Chollima		2012-Aug 2025	●
	Lazarus Group, Hidden Cobra, Labyrinth Chollima		2007-May 2025	●
	Leviathan, APT 40, TEMP.Periscope		2013-Jul 2021	●
	LightBasin		2016	
	Lotus Blossom, Spring Dragon, Thrip		2012-Aug 2024	
	↳ Subgroup: DEV-0270, Nemesis Kitten		2022-Nov 2023	
	MuddyWater, Seedworm, TEMP.Zagros, Static Kitten		2017-Jul 2025	●
	Naikon, Lotus Panda		2010-Apr 2022	
	OilRig, APT 34, Helix Kitten, Chrysene		2014-Sep 2024	●
	OPERA1ER	[Unknown]	2016-Jul 2023	●
	Operation Digital Eye		2024	
	Operation Silent Skimmer	[Unknown]	2022	
	Orangeworm	[Unknown]	2015-Jan 2020	
	Platinum		2009-Nov 2019	
	Sandworm Team, Iron Viking, Voodoo Bear		2009-Dec 2024	●
	Silence, Contract Crew	[Unknown]	2016-Aug 2022	
	Sofacy, APT 28, Fancy Bear, Sednit		2004-Apr 2025	●
	Stone Panda, APT 10, menuPass		2006-Mar 2025	●
	TA505, Graceful Spider, Gold Evergreen		2006-Nov 2022	●

	TeleBots		2015-Oct 2020	●
	Temper Panda, admin@338		2014	
	Tonto Team, HartBeat, Karma Panda		2009-Apr 2023	
	Turbine Panda, APT 26, Shell Crew, WebMasters, KungFu Kittens		2010-Oct 2018	●
	Turla, Waterbug, Venomous Bear		1996-2024	
	Volt Typhoon		2020-Aug 2025	●
	Whitefly, Mofang	[Unknown]	2012-Jul 2018	
	WIRTE Group	[Middle East]	2018-Feb 2024	

Other groups

	CoralRaider		2023-Feb 2024	
	Karakurt	[Unknown]	2021-Sep 2022	
	TA554	[Unknown]	2017	

58 groups listed (55 APT, 3 other, 0 unknown)

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=d54e09cf-97b7-40a4-b30e-4c0a2bf0ea40