Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 18:44:14 UTC

Tool: Valak

Names	Valak Valek
Category	Malware
Type	Backdoor, Info stealer, Loader
Description	(Cybereason) The Valak Malware: The Valak Malware is a sophisticated malware previously classified as a malware loader. Though it was first observed in late 2019, the Cybereason Nocturnus team has investigated a series of dramatic changes, an evolution of over 30 different versions in less than six months. This research shows that Valak is more than just a loader for other malware, and can also be used independently as an information stealer to target individuals and enterprises. Targeting Enterprises: More recent versions of Valak target Microsoft Exchange servers to steal enterprise mailing information and passwords along with the enterprise certificate. This has the potential to access critical enterprise accounts, causing damage to organizations, brand degradation, and ultimately a loss of consumer trust. Targets US and Germany: This campaign is specifically targeting enterprises in the US and Germany. With a Rich Modular Architecture: Valak's basic capabilities are extended with a number of plugin components for reconnaissance and information stealing. Using Fast Development Cycles: Valak has evolved from a loader to a sophisticated, multi-stage modular malware that collects plugins from its C2 server to expand its capabilities. The Cybereason Nocturnus team has observed over 30 different versions in about 6 months. Designed for Stealth: Valak is a stealthy malware that uses advanced evasive techniques like ADS and hiding components in the registry. In addition, over time the developers of Valak chose to abandon using PowerShell, which can be detected and prevented by modern security products.
Information	<https://www.cybereason.com/blog/valak-more-than-meets-the-eye> <https://labs.sentinelone.com/valak-malware-and-the-connection-to-gozi-loader-confcrew/> <https://unit42.paloaltonetworks.com/valak-evolution/>

	<https://medium.com/@prsecurity_/casual-analysis-of-valak-c2-3497fdb79bf7> <https://security-soup.net/analysis-of-valak-maldoc/> <https://blog.talosintelligence.com/2020/07/valak-emerges.html>
MITRE ATT&CK	<https://attack.mitre.org/software/S0476/>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/js.valak>

Last change to this tool card: 30 December 2022

Download this tool card in JSON format

All groups using tool Valak

Changed	Name	Country	Observed	
Other groups				
	TA551, Shathak		2016-Jan 2021	

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