Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 16:20:51 UTC

Tool: BazarBackdoor

Names	BazarBackdoor BazarLoader BEERBOT BazarCall KEGTAP Team9Backdoor bazaloader
Category	Malware
Type	Backdoor, Downloader
Description	(BleepingComputer) After a victim launches the downloaded file, the loader will sleep for a short period of time and then connect to command and control servers to check-in and download the backdoor payload. To get the address of the command and control servers, BazarLoader will use the Emercoin decentralized DNS resolution service to resolve various hostnames that use the 'bazar' domain. The 'bazar' domain can only be utilized on Emercoin's DNS servers, and as it is decentralized, it makes it difficult, if not impossible, for law enforcement to seize the hostname. After the payload is downloaded, it will be filelessly injected into the C:\Windows\system32\svchost.exe process. Security researcher Vitali Kremez told BleepingComputer that this is done using the Process Hollowing and Process Doppelgänging techniques. After a period of time, both Kremez and James have told BleepingComputer that the backdoor will download and execute the Cobalt Strike penetration testing and post-exploitation toolkit on the victim's machine.
Information	<https://www.bleepingcomputer.com/news/security/bazarbackdoor-trickbot-gang-s-new-stealthy-network-hacking-malware/> <https://www.cybereason.com/blog/a-bazar-of-tricks-following-team9s-development-cycles> <https://cofense.com/the-ryuk-threat-why-bazarbackdoor-matters-most/> <https://www.advanced-intel.com/post/anatomy-of-attack-inside-bazarbackdoor-to-ryuk-ransomware-one-group-via-cobalt-strike>

	<https://cofense.com/blog/bazarbackdoor-stealthy-infiltration> <https://www.bleepingcomputer.com/news/security/trickbots-bazarbackdoor-malware-is-now-coded-in-nim-to-evade-antivirus/> <https://www.fortinet.com/blog/threat-research/new-bazar-trojan-variant-is-being-spread-in-recent-phishing-campaign-part-I> <https://www.fortinet.com/blog/threat-research/new-bazar-trojan-variant-is-being-spread-in-recent-phishing-campaign-part-II> <https://www.cert.ssi.gouv.fr/uploads/CERTFR-2021-CTI-006.pdf> <https://thedfirreport.com/2021/03/08/bazar-drops-the-anchor/> <https://news.sophos.com/en-us/2021/04/15/bazarloader/> <https://unit42.paloaltonetworks.com/bazarloader-malware/> <http://www.intel471.com/blog/cobalt-strike-cybercriminals-trickbot-qbot-hancitor> <https://www.intezer.com/blog/malware-analysis/wrapping-up-a-year-of-infamous-bazar-campaigns/> <https://beta.darkreading.com/attacks-breaches/microsoft-tracks-new-bazacall-malware-campaign> <https://cofense.com/blog/nested-files-evade-segs/> <https://cyware.com/news/bazarbackdoor-uses-new-obfuscation-tricks-to-challenge-security-369b4c0b> <https://www.bleepingcomputer.com/news/security/fake-dmca-and-ddos-complaints-lead-to-bazaloader-malware/> <https://unit42.paloaltonetworks.com/bazarloader-network-reconnaissance/> <https://news.sophos.com/en-us/2021/11/11/bazarloader-call-me-back-attack-abuses-windows-10-apps-mechanism/> <https://www.trendmicro.com/en_us/research/21/k/bazarloader-adds-compromised-installers-iso-to-arrival-delivery-vectors.html> <https://thedfirreport.com/2021/11/29/continuing-the-bazar-ransomware-story/> <https://www.bleepingcomputer.com/news/security/malicious-csv-text-files-used-to-install-bazarbackdoor-malware/> <https://abnormalsecurity.com/blog/bazarloader-contact-form> <https://unit42.paloaltonetworks.com/bazarloader-anti-analysis-techniques/> <https://www.advintel.io/post/bazarcall-advisory-the-essential-guide-to-call-back-phishing-attacks-that-revolutionized-the-data> <https://www.trellix.com/en-us/about/newsroom/stories/research/evolution-of-bazarcall-social-engineering-tactics.html>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.bazarbackdoor>

Last change to this tool card: 18 November 2022

Download this tool card in JSON format

All groups using tool BazarBackdoor

Changed	Name	Country	Observed	
APT groups				
	FIN12	[Unknown]	2018	
	Wizard Spider, Gold Blackburn		2014-May 2025	
Other groups				
	UNC1878	[Unknown]	2020	

3 groups listed (2 APT, 1 other, 0 unknown)

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=45260893-fa7b-4738-aecd-7d6ad6cc1577