Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 17:13:12 UTC

Tool: Gootkit

Names	Gootkit Gootloader Xswkit talalpek Waldek
Category	Malware
Type	Backdoor, Banking trojan, Credential stealer, Info stealer
Description	(Sentinel Labs) The Gootkit Banking Trojan was discovered back in 2014, and utilizes the Node.JS library to perform a range of malicious tasks, from website injections and password grabbing, all the way up to video recording and remote VNC capabilities. Since its discovery in 2014, the actors behind Gootkit have continued to update the codebase to slow down analysis and thwart automated sandboxes. This post will take a look into the first stage of Gootkit, which contains the unpacking phase and a malicious downloader that sets up the infected system, and its multiple anti-analysis mechanisms.
Information	<https://labs.sentinelone.com/gootkit-banking-trojan-deep-dive-anti-analysis-features/> <https://threatvector.cylance.com/en_us/home/threat-spotlight-gootkit-banking-trojan.html> <https://securityintelligence.com/news/new-gootkit-malware-sample-evades-detection-with-path-exclusion/> <https://www.lexsi.com/securityhub/homer-simpson-brian-krebs-rencontrent-zeus-gootkit/> <http://blog.cert.societegenerale.com/2015/04/analyzing-gootkits-persistence-mechanism.html> <https://securityintelligence.com/gootkit-developers-dress-it-up-with-web-traffic-proxy/> <https://forums.juniper.net/t5/Security-Now/New-Gootkit-Banking-Trojan-variant-pushes-the-limits-on-evasive/ba-p/319055> <https://www.f5.com/labs/articles/threat-intelligence/tackling-gootkit-s-traps> <https://securelist.com/blog/research/76433/inside-the-gootkit-cc-server/> <https://www.us-cert.gov/ncas/alerts/TA16-336A> <http://www.vkremez.com/2018/04/lets-learn-in-depth-dive-into-gootkit.html>

	<https://securityintelligence.com/gootkit-bobbing-and-weaving-to-avoid-prying-eyes/> <https://www.s21sec.com/en/blog/2016/05/reverse-engineering-gootkit/> <http://blog.trendmicro.com/trendlabs-security-intelligence/fake-judicial-spam-leads-to-backdoor-with-fake-certificate-authority/> <https://news.drweb.com/show/?i=4338&lng=en> <https://www.cyphort.com/angler-ek-leads-to-fileless-gootkit/> <https://news.sophos.com/en-us/2021/03/01/gootloader-expands-its-payload-delivery-options/> <https://securelist.com/gootkit-the-cautious-trojan/102731/> <https://www.trendmicro.com/en_us/research/22/g/gootkit-loaders-updated-tactics-and-fileless-delivery-of-cobalt-strike.html> <https://www.trendmicro.com/en_us/research/23/a/gootkit-loader-actively-targets-the-australian-healthcare-indust.html> <https://www.mandiant.com/resources/blog/tracking-evolution-gootloader-operations> <https://www.cybereason.com/blog/threat-alert-gootloader-seo-poisoning-and-large-payloads-leading-to-compromise> <https://securityintelligence.com/x-force/gootbot-gootloaders-new-approach-to-post-exploitation/> <https://www.cybereason.com/blog/i-am-goot-loader> <https://unit42.paloaltonetworks.com/javascript-malware-gootloader/>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.gootkit>
AlienVault OTX	<https://otx.alienvault.com/browse/pulses?q=tag:Gootkit>

Last change to this tool card: 26 August 2024

Download this tool card in JSON format

All groups using tool Gootkit

Changed	Name	Country	Observed	
Other groups				
	TA554	[Unknown]	2017	

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