Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 16:14:23 UTC

Tool: SLUB

Names	SLUB
Category	Malware
Type	Reconnaissance, Backdoor, Info stealer, Downloader, Exfiltration
Description	(Trend Micro) We recently came across a previously unknown malware that piqued our interest in multiple ways. For starters, we discovered it being spread via watering hole attacks, a technique that involves an attacker compromising a website before adding code to it so visitors are redirected to the infecting code. In this case, each visitor is redirected only once. The infection was done by exploiting CVE-2018-8174, a VBScript engine vulnerability that was patched by Microsoft back in May 2018. Second, it uses a multi-stage infection scheme. After it exploits the vulnerability, it downloads a DLL and runs it in PowerShell (PS). This file, which is a downloader, then downloads and runs the second executable file containing a backdoor. The first stage downloader also checks for the existence of different kinds of antivirus software processes, and then proceeds to exit if any is found. At the time of discovery, the backdoor was seemingly unknown to AV products.
Information	<https://www.trendmicro.com/en_us/research/19/c/new-slub-backdoor-uses-github-communicates-via-slack.html> <https://blog.trendmicro.com/trendlabs-security-intelligence/SLUB-gets-rid-of-github-intensifies-slack-use/> <https://documents.trendmicro.com/assets/white_papers/wp-operation-earth-kitsune.pdf> <https://www.virusbulletin.com/uploads/pdf/conference_slides/2019/VB2019-LunghiHorejsi.pdf>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.slub>
AlienVault OTX	<https://otx.alienvault.com/browse/pulses?q=tag:slub>

Last change to this tool card: 24 April 2021

Download this tool card in JSON format

All groups using tool SLUB

Changed	Name	Country	Observed	
APT groups				
	Operation Earth Kitsune		2019-Late 2022	

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

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=576647b7-c4ec-4642-baa2-0d9b53d9ae3c