

Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-02 11:18:28 UTC

Tool: SysUpdate

Names	SysUpdate FOCUSEJORD HyperSSL Soldier
Category	Malware
Type	Backdoor , Loader , Downloader
Description	(SecureWorks) SysUpdate is a multi-stage malware used exclusively by BRONZE UNION. It has been delivered by multiple methods.
Information	< https://www.secureworks.com/research/a-peek-into-bronze-unions-toolbox > < https://research.nccgroup.com/2018/05/18/emissary-panda-a-potential-new-malicious-tool/ > < https://www.trendmicro.com/en_us/research/21/d/iron-tiger-apt-updates-toolkit-with-evolved-sysupdate-malware-va.html > < https://www.fireeye.com/blog/threat-research/2021/08/unc215-chinese-espionage-campaign-in-israel.html >
MITRE ATT&CK	< https://attack.mitre.org/software/S0663/ >
Malpedia	< https://malpedia.caad.fkie.fraunhofer.de/details/win.hyperssl >

Last change to this tool card: 30 December 2022

Download this tool card in [JSON](#) format

All groups using tool SysUpdate

Changed	Name	Country	Observed
APT groups			
	Emissary Panda , APT 27 , LuckyMouse , Bronze Union		2010-Aug 2023

	UNC215		2019	
--	------------------------	---	------	--

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

[1](#)

Source: <https://apt.eta.or.th/cgi-bin/listgroups.cgi?u=7ee199cb-0299-4e33-9082-efc768f5096c>