Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 19:25:20 UTC

Tool: vSkimmer

Names	vSkimmer
Category	Malware
Type	POS malware, Reconnaissance, Backdoor, Credential stealer, Botnet
Description	(XyliBox) Functions: - Track 2 grabber - HTTP Loader (Download & Execute) - Update bot itself Working Modes: - Online: If internet is reachable it will try to bypass firewalls and communicate to a the control panel. - Offline: If internet is not reachable it wait for a specific pendrive/flashdrive plugged in and copy logs to it. Server coded in PHP (can be modified on request to send logs to remote server, via smtp, etc..) Client coded in C++ no dependencies, 66kb, cryptable. (can be customized)
Information	<https://www.xylibox.com/2013/01/vskimmer.html> <http://vkremez.weebly.com/cyber-security/-backdoor-win32hesetoxa-vskimmer-pos-malware-analysis> <https://www.trendmicro.de/cloud-content/us/pdfs/security-intelligence/white-papers/wp-pos-ram-scraper-malware.pdf> <https://www.secureworks.com/research/point-of-sale-malware-threats>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.vskimmer>

Last change to this tool card: 25 May 2020

Download this tool card in JSON format

All groups using tool vSkimmer

Changed	Name	Country	Observed	
Unknown groups				
	[Interesting malware not linked to an actor yet]			

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