Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 15:09:35 UTC

Tool: UpDocX

Names	UpDocX
Category	Malware
Type	Backdoor, Keylogger, Exfiltration
Description	UpDocX was written in VB.NET and compiled without any attempts at obfuscating the source code. There is also no attempt in obfuscating C2 network traffic. It has limited functionality and appears to be a simple backdoor used solely for keylogging and uploading documents to designated C2 servers. The attackers have, however, put some effort into avoiding detection and hindering investigations. UpDocX has a list of extensive clean-up functions responsible for eliminating evidence of compromise, which indicates a degree of caution often not observed in targeted attacks.
Information	<https://paper.seebug.org/papers/APT/APT_CyberCriminal_Campagin/2015/UnFIN4ished_Business_pwd.pdf
AlienVault OTX	<https://otx.alienvault.com/browse/pulses?q=tag:UpDocX>

Last change to this tool card: 20 April 2020

Download this tool card in JSON format

All groups using tool UpDocX

Changed	Name	Country	Observed	
APT groups				
	FIN4, Wolf Spider		2013	

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