Threat Group Cards: A Threat Actor Encyclopedia

Tool: OwaAuth

Names	OwaAuth luckyowa
Category	Malware
Type	Backdoor, Credential stealer
Description	(SecureWorks) A web shell and credential stealer deployed to Microsoft Exchange servers. It is installed as an ISAPI filter. Captured credentials are DES-encrypted using the password '12345678' and are written to the log.txt file in the root directory. Like the China Chopper web shell, the OwaAuth web shell requires a password. However, the OwaAuth web shell password contains the victim organization's name.
Information	<https://www.secureworks.com/research/threat-group-3390-targets-organizations-for-cyberespionage> <https://threatpost.com/targeted-attack-exposes-owa-weakness/114925/>
MITRE ATT&CK	<https://attack.mitre.org/software/S0072/>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.owaauth>

Last change to this tool card: 14 May 2020

Download this tool card in JSON format

All groups using tool OwaAuth

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

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