Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 12:45:03 UTC

Tool: Carbanak

Names	Carbanak Anunak Sekur Sekur RAT
Category	Malware
Type	Reconnaissance, Backdoor
Description	(Kaspersky) Carbanak is a backdoor used by the attackers to compromise the victim's machine once the exploit, either in the spear phishing email or exploit kit, successfully executes its payload. This section provides a functional analysis of Carbanak's capabilities. Carbanak copies itself into "%system32%\com" with the name "svchost.exe" with the file attributes: system, hidden and read-only. The original file created by the exploit payload is then deleted. To ensure that Carbanak has autorun privileges the malware creates a new service. The naming syntax is " Sys" where ServiceName is any existing service randomly chosen, with the first character deleted. For example, if the existing service´s name is "aspnet" and the visible name is "Asp.net state service", the service created by the malware would be "aspnetSys" with a visible name of "Sp.net state service". Before creating the malicious service, Carbanak determines if either the avp.exe or avpui.exe processes (components of Kaspersky Internet Security) is running. If found on the target system, Carbanak will try to exploit a known vulnerability in Windows XP, Windows Server 2003, Windows Vista, Windows Server 2008, Windows 7, Windows 8, and Windows Server 2012, CVE-2013-3660, for local privilege escalation. We believe this is not relevant and that the attackers adapt their tools to the victim´s defenses.
Information	<https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2018/03/08064518/Carbanak_APT_eng.pdf>

	<https://www.fireeye.com/blog/threat-research/2017/06/behind-the-carbanak-backdoor.html> <https://www.fireeye.com/blog/threat-research/2019/04/carbanak-week-part-one-a-rare-occurrence.html> <https://www.fox-it.com/en/wp-content/uploads/sites/11/Anunak_APT-against-financial-institutions2.pdf> <https://documents.trendmicro.com/assets/white_papers/wp-cashing-in-on-atm-malware.pdf> <https://thehackernews.com/2023/12/carbanak-banking-malware-resurfaces.html>
MITRE ATT&CK	<https://attack.mitre.org/software/S0030/>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.carbanak>

Last change to this tool card: 16 January 2024

Download this tool card in JSON format

All groups using tool Carbanak

Changed	Name	Country	Observed	
APT groups				
	Carbanak, Anunak		2013-Apr 2023	
	FIN7		2013-Jul 2024	

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

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=d4ee0ad6-9ba5-48cb-a289-f29476852d0e