Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-06 03:21:08 UTC

Tool: Outlook Backdoor

Names	Outlook Backdoor FACADE
Category	Malware
Type	Backdoor, Info stealer, Exfiltration
Description	(ESET) The Turla Outlook backdoor has two interesting functionalities. First, it steals emails by forwarding all outgoing emails to the attackers. It mainly targets Microsoft Outlook, a widely used mail client, but also targets The Bat!, a mail client very popular in Eastern Europe. Second, it uses email messages as a transport layer for its Command & Control (C&C) protocol. Data, such as files requested via a command of the backdoor, is exfiltrated in specially-crafted PDF documents attached to emails, and commands are also received in PDF attachments. Thus, its behavior is particularly stealthy. It is important to note that no vulnerabilities were used either in PDF readers nor in Outlook. What actually happens is that the malware is able to decode data from the PDF documents and interpret it as commands for the backdoor.
Information	<https://www.welivesecurity.com/wp-content/uploads/2018/08/Eset-Turla-Outlook-Backdoor.pdf>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.outlook_backdoor>

Last change to this tool card: 23 April 2020

Download this tool card in JSON format

All groups using tool Outlook Backdoor

Changed	Name	Country	Observed
APT groups			

	Turla, Waterbug, Venomous Bear		1996-2024	

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