Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 18:41:47 UTC

Tool: FlawedAmmyy

Names	FlawedAmmyy AmmyyRAT
Category	Malware
Type	Backdoor, Info stealer, Credential stealer, Exfiltration
Description	(Proofpoint) Ammyy Admin is a popular remote access tool used by businesses and consumers to handle remote control and diagnostics on Microsoft Windows machines. However, leaked source code for Version 3 of Ammyy Admin has emerged as a Remote Access Trojan called FlawedAmmyy appearing in a variety of malicious campaigns. For infected individuals, this means that attackers potentially have complete access to their PCs, giving threat actors the ability to access a variety of services, steal files and credentials, and much more. We have seen FlawedAmmyy in both massive campaigns, potentially creating a large base of compromised computers, as well as targeted campaigns that create opportunities for actors to steal customer data, proprietary information, and more.
Information	<https://www.proofpoint.com/us/threat-insight/post/leaked-ammyy-admin-source-code-turned-malware> <https://www.sans.org/reading-room/whitepapers/reverseengineeringmalware/unpacking-decrypting-flawedammyy-38930> <https://secrary.com/ReversingMalware/AMMY_RAT_Downloader/> <https://www.proofpoint.com/us/threat-insight/post/ta505-abusing-settingcontent-ms-within-pdf-files-distribute-flawedammyy-rat> <https://github.com/Coldzer0/Ammyy-v3>
MITRE ATT&CK	<https://attack.mitre.org/software/S0381/>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.flawedammyy>
AlienVault OTX	<https://otx.alienvault.com/browse/pulses?q=tag:flawedammyy>

Last change to this tool card: 13 May 2020

Download this tool card in JSON format

All groups using tool FlawedAmmyy

Changed	Name	Country	Observed	
APT groups				
	Buhtrap, Ratopak Spider		2015-Jun 2019	
	Carbanak, Anunak		2013-Apr 2023	
	Cobalt Group		2016-Oct 2019	
	FIN6, Skeleton Spider	[Unknown]	2015-Oct 2021	
	FIN11	[Unknown]	2016-Mar 2025	
	TA505, Graceful Spider, Gold Evergreen		2006-Nov 2022	

6 groups listed (6 APT, 0 other, 0 unknown)

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=12a4f267-6f13-4033-a9c9-f797fb2ebd45