FlawedAmmyy

attack.mitre.org/software/S0381/

FlawedAmmyy is a remote access tool (RAT) that was first seen in early 2016. The code for FlawedAmmyy was based on leaked source code for a version of Ammyy Admin, a remote access software.[1]

ID: S0381

ⓘ

Type: MALWARE

ⓘ

Platforms: Windows

Version: 1.1

Created: 28 May 2019

Last Modified: 20 March 2020

Version Permalink
Live Version

Enterprise Layer

download view

Techniques Used

Domain	ID	Name	Use

Domain	ID	Name	Use	
Enterprise	T1071	.001	Application Layer Protocol: Web Protocols	FlawedAmmyy has used HTTP for C2.[1]
Enterprise	T1001	Data Obfuscation	FlawedAmmyy may obfuscate portions of the initial C2 handshake.[1]	
Enterprise	T1573	.001	Encrypted Channel: Symmetric Cryptography	FlawedAmmyy has used SEAL encryption during the initial C2 handshake.[1]
Enterprise	T1120	Peripheral Device Discovery	FlawedAmmyy will attempt to detect if a usable smart card is current inserted into a card reader.[1]	
Enterprise	T1069	.001	Permission Groups Discovery: Local Groups	FlawedAmmyy enumerates the privilege level of the victim during the initial infection.[1]
Enterprise	T1518	.001	Software Discovery: Security Software Discovery	FlawedAmmyy will attempt to detect anti-virus products during the initial infection.[1]
Enterprise	T1082	System Information Discovery	FlawedAmmyy beacons out the victim operating system and computer name during the initial infection.[1]	
Enterprise	T1033	System Owner/User Discovery	FlawedAmmyy enumerates the current user during the initial infection.[1]	

Domain	ID	Name	Use
Enterprise	T1047	Windows Management Instrumentation	FlawedAmmyy leverages WMI to enumerate anti-virus on the victim.[1]

Groups That Use This Software

ID	Name	References
G0092	TA505	[1][2][3]
G0037	FIN6	[4]

References

Proofpoint Staff. (2018, March 7). Leaked Ammyy Admin Source Code Turned into Malware. Retrieved May 28, 2019. Hiroaki, H. and Lu, L. (2019, June 12). Shifting Tactics: Breaking Down TA505 Group's Use of HTML, RATs and Other Techniques in Latest Campaigns. Retrieved May 29, 2020. Schwarz, D. et al. (2019, October 16). TA505 Distributes New SDBbot Remote Access Trojan with Get2 Downloader. Retrieved May 29, 2020. Visa Public. (2019, February). FIN6 Cybercrime Group Expands Threat to eCommerce Merchants. Retrieved September 16, 2019.