Kerrdown, Software S0585 | MITRE ATT&CK®

Archived: 2026-04-05 15:45:13 UTC

Domain	ID		Name	Use
Enterprise	T1059	.005	Command and Scripting Interpreter: Visual Basic	Kerrdown can use a VBS base64 decoder function published by Motobit.[2]
Enterprise	T1140		Deobfuscate/Decode Files or Information	Kerrdown can decode, decrypt, and decompress multiple layers of shellcode. [2]
Enterprise	T1574	.001	Hijack Execution Flow: DLL	Kerrdown can use DLL side-loading to load malicious DLLs.[2]
Enterprise	T1105		Ingress Tool Transfer	Kerrdown can download specific payloads to a compromised host based on OS architecture.[2]
Enterprise	T1027	.013	Obfuscated Files or Information: Encrypted/Encoded File	Kerrdown can encrypt, encode, and compress multiple layers of shellcode.[2]
		.015	Obfuscated Files or Information: Compression	Kerrdown can encrypt, encode, and compress multiple layers of shellcode.[2]
Enterprise	T1566	.001	Phishing: Spearphishing Attachment	Kerrdown has been distributed through malicious e-mail attachments.[1]
		.002	Phishing: Spearphishing Link	Kerrdown has been distributed via e-mails containing a malicious link.[1]

Domain	ID		Name	Use
Enterprise	T1082		System Information Discovery	Kerrdown has the ability to determine if the compromised host is running a 32 or 64 bit OS architecture.[2]
Enterprise	T1204	.001	User Execution: Malicious Link	Kerrdown has gained execution through victims opening malicious links.[1]
		.002	User Execution: Malicious File	Kerrdown has gained execution through victims opening malicious files.[1][2]

Source: https://attack.mitre.org/software/S0585