Pillowmint, Software S0517 | MITRE ATT&CK®

Archived: 2026-04-02 11:57:52 UTC

Domain	ID		Name	Use
Enterprise	T1560		Archive Collected Data	Pillowmint has encrypted stolen credit card information with AES and further enc with Base64.[1]
Enterprise	T1059	.001	Command and Scripting Interpreter: PowerShell	Pillowmint has used a PowerShell script to install a shim database.[1]
Enterprise	T1005		Data from Local System	Pillowmint has collected credit card data using native API functions.[1]
Enterprise	T1140		Deobfuscate/Decode Files or Information	Pillowmint has been decompressed by included shellcode prior to being launched.
Enterprise	T1546	.011	Event Triggered Execution: Application Shimming	Pillowmint has used a malicious shim database to maintain persistence.[1]
Enterprise	T1070	.004	Indicator Removal: File Deletion	Pillowmint has deleted the filepath `%APPDATA%\Intel\devmonsrv.exe`.[1]
		.009	Indicator Removal: Clear Persistence	Pillowmint can uninstall the malicious service from an infected machine.[1]
Enterprise	T1112		Modify Registry	Pillowmint has modified the Registry key `HKLM\SOFTWARE\Microsoft\DRM` to stor malicious payload.[1]
Enterprise	T1106		Native API	Pillowmint has used multiple native Windows APIs to execute and conduct proces injections.[1]
Enterprise	T1027		Obfuscated Files or Information	Pillowmint has obfuscated the AES key used for encryption.[1]
		.011	Fileless Storage	Pillowmint has stored a compressed payload in the Registry key `HKLM\SOFTWARE\Microsoft\DRM`.[1]
		.015	Compression	Pillowmint has been compressed and stored within a registry key.[1]
Enterprise	T1057		Process Discovery	Pillowmint can iterate through running processes every six seconds collecting a lis processes to capture from later.[1]

Domain	ID		Name	Use
Enterprise	T1055	.004	Process Injection: Asynchronous Procedure Call	Pillowmint has used the NtQueueApcThread syscall to inject code into svchost.ex
Enterprise	T1012		Query Registry	Pillowmint has used shellcode which reads code stored in the registry keys `\REGISTRY\SOFTWARE\Microsoft\DRM` using the native Windows API as well as re `HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters\In` as part of its C2.[1]

Source: https://attack.mitre.org/software/S0517