Pandora, Software S0664 | MITRE ATT&CK®

Archived: 2026-04-05 18:00:14 UTC

Domain	ID		Name	Use
Enterprise	T1071	.001	Application Layer Protocol: Web Protocols	Pandora can communicate over HTTP.[1]
Enterprise	T1543	.003	Create or Modify System Process: Windows Service	Pandora has the ability to gain system privileges through Windows services.[1]
Enterprise	T1573	.001	Encrypted Channel: Symmetric Cryptography	Pandora has the ability to encrypt communications with D3DES.[1]
Enterprise	T1068		Exploitation for Privilege Escalation	Pandora can use CVE-2017-15303 to bypass Windows Driver Signature Enforcement (DSE) protection and load its driver.[1]
Enterprise	T1574	.001	Hijack Execution Flow: DLL	Pandora can use DLL side-loading to execute malicious payloads.[1]
Enterprise	T1105		Ingress Tool Transfer	Pandora can load additional drivers and files onto a victim machine.[1]
Enterprise	T1112		Modify Registry	Pandora can write an encrypted token to the Registry to enable processing of remote commands.[1]
Enterprise	T1027	.015	Obfuscated Files or Information: Compression	Pandora has the ability to compress stings with QuickLZ.[1]

Domain	ID		Name	Use
Enterprise	T1057		Process Discovery	Pandora can monitor processes on a compromised host.[1]
Enterprise	T1055		Process Injection	Pandora can start and inject code into a new `svchost` process.[1]
Enterprise	T1553	.006	Subvert Trust Controls: Code Signing Policy Modification	Pandora can use CVE-2017-15303 to disable Windows Driver Signature Enforcement (DSE) protection and load its driver.[1]
Enterprise	T1569	.002	System Services: Service Execution	Pandora has the ability to install itself as a Windows service.[1]
Enterprise	T1205		Traffic Signaling	Pandora can identify if incoming HTTP traffic contains a token and if so it will intercept the traffic and process the received command.[1]
