SeaDuke, Software S0053 | MITRE ATT&CK®

Archived: 2026-04-05 18:02:55 UTC

Domain	ID		Name	Use
Enterprise	T1071	.001	Application Layer Protocol: Web Protocols	SeaDuke uses HTTP and HTTPS for C2.[1]
Enterprise	T1560	.002	Archive Collected Data: Archive via Library	SeaDuke compressed data with zlib prior to sending it over C2.[2]
Enterprise	T1547	.001	Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder	SeaDuke is capable of persisting via the Registry Run key or a .lnk file stored in the Startup directory.[3]
		.009	Boot or Logon Autostart Execution: Shortcut Modification	SeaDuke is capable of persisting via a .lnk file stored in the Startup directory.[3]
Enterprise	T1059	.001	Command and Scripting Interpreter: PowerShell	SeaDuke uses a module to execute Mimikatz with PowerShell to perform Pass the Ticket.[4]
		.003	Command and Scripting Interpreter: Windows Command Shell	SeaDuke is capable of executing commands.[3]
Enterprise	T1132	.001	Data Encoding: Standard Encoding	SeaDuke C2 traffic is base64-encoded.[3]
Enterprise	T1114	.002	Email Collection: Remote Email Collection	Some SeaDuke samples have a module to extract email from Microsoft Exchange servers using compromised credentials.[4]

Domain	ID		Name	Use
Enterprise	T1573	.001	Encrypted Channel: Symmetric Cryptography	SeaDuke C2 traffic has been encrypted with RC4 and AES.[2][3]
Enterprise	T1546	.003	Event Triggered Execution: Windows Management Instrumentation Event Subscription	SeaDuke uses an event filter in WMI code to execute a previously dropped executable shortly after system startup. [5]
Enterprise	T1070	.004	Indicator Removal: File Deletion	SeaDuke can securely delete files, including deleting itself from the victim. [4]
Enterprise	T1105		Ingress Tool Transfer	SeaDuke is capable of uploading and downloading files.[3]
Enterprise	T1027	.002	Obfuscated Files or Information: Software Packing	SeaDuke has been packed with the UPX packer.[3]
Enterprise	T1550	.003	Use Alternate Authentication Material: Pass the Ticket	Some SeaDuke samples have a module to use pass the ticket with Kerberos for authentication.[4]
Enterprise	T1078		Valid Accounts	Some SeaDuke samples have a module to extract email from Microsoft Exchange servers using compromised credentials.[4]

Source: https://attack.mitre.org/software/S0053