

OwaAuth, Software S0072 | MITRE ATT&CK®

Archived: 2026-04-05 16:07:44 UTC

Domain	ID	Name	Use
Enterprise	T1071 .001	Application Layer Protocol: Web Protocols	OwaAuth uses incoming HTTP requests with a username keyword and commands and handles them as instructions to perform actions. ^[1]
Enterprise	T1560 .003	Archive Collected Data: Archive via Custom Method	OwaAuth DES-encrypts captured credentials using the key 12345678 before writing the credentials to a log file. ^[1]
Enterprise	T1083	File and Directory Discovery	OwaAuth has a command to list its directory and logical drives. ^[1]
Enterprise	T1070 .006	Indicator Removal: Timestamp	OwaAuth has a command to timestop a file or directory. ^[1]
Enterprise	T1056 .001	Input Capture: Keylogging	OwaAuth captures and DES-encrypts credentials before writing the username and password to a log file, <code>C:\log.txt</code> . ^[1]
Enterprise	T1036 .005	Masquerading: Match Legitimate Resource Name or Location	OwaAuth uses the filename owaauth.dll, which is a legitimate file that normally resides in <code>%ProgramFiles%\Microsoft\Exchange Server\ClientAccess\Owa\Auth\</code> ; the malicious file by the same name is saved in <code>%ProgramFiles%\Microsoft\Exchange Server\ClientAccess\Owa\bin\</code> . ^[1]
Enterprise	T1505 .003	Server Software Component: Web Shell	OwaAuth is a Web shell that appears to be exclusively used by Threat Group-3390 . It is installed as an ISAPI

Domain	ID	Name	Use
			filter on Exchange servers and shares characteristics with the China Chopper Web shell. ^[1]
	.004	Server Software Component: IIS Components	OwaAuth has been loaded onto Exchange servers and disguised as an ISAPI filter (owaaauth.dll). The IIS w3wp.exe process then loads the malicious DLL. ^[1]

Source: <https://attack.mitre.org/software/S0072/>