Neoichor, Software S0691 | MITRE ATT&CK®

Archived: 2026-04-05 12:39:46 UTC

Domain	ID		Name	Use
Enterprise	T1071	.001	Application Layer Protocol: Web Protocols	Neoichor can use HTTP for C2 communications.[1]
Enterprise	T1005		Data from Local System	Neoichor can upload files from a victim's machine.[1]
Enterprise	T1070		Indicator Removal	Neoichor can clear the browser history on a compromised host by changing the `ClearBrowsingHistoryOnExit` value to 1 in the `HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Privacy` Registry key.[1]
Enterprise	T1105		Ingress Tool Transfer	Neoichor can download additional files onto a compromised host.[1]
Enterprise	T1559	.001	Inter-Process Communication: Component Object Model	Neoichor can use the Internet Explorer (IE) COM interface to connect and receive commands from C2.[1]
Enterprise	T1112		Modify Registry	Neoichor has the ability to configure browser settings by modifying Registry entries under `HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer`.[1]
Enterprise	T1082		System Information Discovery	Neoichor can collect the OS version and computer name from a compromised host.[1]

Domain	ID		Name	Use
Enterprise	T1614	.001	System Location Discovery: System Language Discovery	Neoichor can identify the system language on a compromised host.[1]
Enterprise	T1016		System Network Configuration Discovery	Neoichor can gather the IP address from an infected host.[1]
		.001	Internet Connection Discovery	Neoichor can check for Internet connectivity by contacting bing[.]com with the request format `bing[.]com?id=<GetTickCount>`.[1]
Enterprise	T1033		System Owner/User Discovery	Neoichor can collect the user name from a victim's machine.[1]

Source: https://attack.mitre.org/software/S0691