More_eggs, Software S0284 | MITRE ATT&CK®

Archived: 2026-04-05 18:13:43 UTC

Domain	ID		Name	Use
Enterprise	T1071	.001	Application Layer Protocol: Web Protocols	More_eggs uses HTTPS for C2.[1][2]
Enterprise	T1059	.003	Command and Scripting Interpreter: Windows Command Shell	More_eggs has used cmd.exe for execution.[2][5]
Enterprise	T1132	.001	Data Encoding: Standard Encoding	More_eggs has used basE91 encoding, along with encryption, for C2 communication.[2]
Enterprise	T1140		Deobfuscate/Decode Files or Information	More_eggs will decode malware components that are then dropped to the system.[2]
Enterprise	T1573	.001	Encrypted Channel: Symmetric Cryptography	More_eggs has used an RC4-based encryption method for its C2 communications.[2]
Enterprise	T1070	.004	Indicator Removal: File Deletion	More_eggs can remove itself from a system.[1][2]
Enterprise	T1105		Ingress Tool Transfer	More_eggs can download and launch additional payloads.[1][2]
Enterprise	T1027	.013	Obfuscated Files or Information: Encrypted/Encoded File	More_eggs's payload has been encrypted with a key that has the hostname and processor family information appended to the end.[5]

Domain	ID		Name	Use
Enterprise	T1518	.001	Software Discovery: Security Software Discovery	More_eggs can obtain information on installed anti-malware programs.[1]
Enterprise	T1553	.002	Subvert Trust Controls: Code Signing	More_eggs has used a signed binary shellcode loader and a signed Dynamic Link Library (DLL) to create a reverse shell.[2]
Enterprise	T1218	.010	System Binary Proxy Execution: Regsvr32	More_eggs has used regsvr32.exe to execute the malicious DLL.[2]
Enterprise	T1082		System Information Discovery	More_eggs has the capability to gather the OS version and computer name.[1][2]
Enterprise	T1016		System Network Configuration Discovery	More_eggs has the capability to gather the IP address from the victim's machine.[1]
		.001	Internet Connection Discovery	More_eggs has used HTTP GET requests to check internet connectivity.[2]
Enterprise	T1033		System Owner/User Discovery	More_eggs has the capability to gather the username from the victim's machine.[1][2]

Source: https://attack.mitre.org/software/S0284/