More_eggs

attack.mitre.org/software/S0284/

More_eggs is a JScript backdoor used by Cobalt Group and FIN6. Its name was given based on the variable "More_eggs" being present in its code. There are at least two different versions of the backdoor being used, version 2.0 and version 4.4. [1][2]

ID: S0284

ⓘ

Associated Software: SKID, Terra Loader, SpicyOmelette

ⓘ

Type: MALWARE

ⓘ

Platforms: Windows

Contributors: Drew Church, Splunk

Version: 3.0

Created: 17 October 2018

Last Modified: 23 April 2021

Version Permalink
Live Version

Associated Software Descriptions

Name	Description
SKID	[3]
Terra Loader	[2][4]
SpicyOmelette	[2]

Techniques Used

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]

Domain	ID	Name	Use	
Enterprise	T1070	.004	Indicator Removal on Host: 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	Obfuscated Files or Information	More_eggs's payload has been encrypted with a key that has the hostname and processor family information appended to the end.[5]	
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]	

Domain	ID	Name	Use	
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]	

Groups That Use This Software

ID	Name	References
G0120	Evilnum	[5]
G0080	Cobalt Group	[1][3]
G0037	FIN6	[2][4]

References

Svajcer, V. (2018, July 31). Multiple Cobalt Personality Disorder. Retrieved September 5, 2018. Villadsen, O.. (2019, August 29). More_eggs, Anyone? Threat Actor ITG08 Strikes Again. Retrieved September 16, 2019. Crowdstrike. (2020, March 2). 2020 Global Threat Report. Retrieved December 11, 2020. Visa Public. (2019, February). FIN6 Cybercrime Group Expands Threat to eCommerce Merchants. Retrieved September 16, 2019. Porolli, M. (2020, July 9). More evil: A deep look at Evilnum and its toolset. Retrieved January 22, 2021.