Command and Scripting Interpreter: JavaScript, Sub-technique T1059.007 - Enterprise

Archived: 2026-04-05 12:47:39 UTC

S0622 AppleSeed

AppleSeed has the ability to use JavaScript to execute PowerShell.[10]

G0050 APT32

APT32 has used JavaScript for drive-by downloads and C2 communications.[11][12]

S0373 Astaroth

Astaroth uses JavaScript to perform its core functionalities. [13][14]

S0640 Avaddon

Avaddon has been executed through a malicious JScript downloader.[15][16]

S1246 BeaverTail

BeaverTail has executed malicious JavaScript code.[17][18][19][20][21] BeaverTail has also been compiled with the Qt framework to execute in both Windows and macOS.[22]

S1180 BlackByte Ransomware

BlackByte Ransomware is distributed as a JavaScript launcher file.[23]

S0482 Bundlore

Bundlore can execute JavaScript by injecting it into the victim's browser.[24]

C0015 C0015

During C0015, the threat actors used a malicious HTA file that contained a mix of encoded HTML and JavaScript/VBScript code.[25]

C0017 C0017

During C0017, APT41 deployed JScript web shells on compromised systems.[26]

S0631 Chaes

Chaes has used JavaScript and Node.Js information stealer script that exfiltrates data using the node process.[27]

G0080 Cobalt Group

Cobalt Group has executed JavaScript scriptlets on the victim's machine.[28][29][30][31][32][33]

S0154 Cobalt Strike

The Cobalt Strike System Profiler can use JavaScript to perform reconnaissance actions.[34]

G1052 Contagious Interview

Contagious Interview has leveraged JavaScript in the execution of their downloader malware targeting Windows devices using a NodeJS script titled nvidia.js.[35]

S0673 DarkWatchman

DarkWatchman uses JavaScript to perform its core functionalities.[36]

S0695 Donut

Donut can generate shellcode outputs that execute via JavaScript or JScript.[37]

G1006 Earth Lusca

Earth Lusca has manipulated legitimate websites to inject malicious JavaScript code as part of their watering hole operations.[38]

S0634 EnvyScout

EnvyScout can write files to disk with JavaScript using a modified version of the open-source tool FileSaver.[39]

G0120 Evilnum

Evilnum has used malicious JavaScript files on the victim's machine.[40]

G0037 FIN6

FIN6 has used malicious JavaScript to steal payment card data from e-commerce sites.[41]

G0046 FIN7

FIN7 used JavaScript scripts to help perform tasks on the victim's machine.[42][43]

S1144 FRP

FRP can support the use of a JSON configuration file.[44]

S1138 Gootloader

Gootloader can execute a Javascript file for initial infection.[45][46]

S0417 GRIFFON

GRIFFON is written in and executed as JavaScript.[47]

S1249 HexEval Loader

HexEval Loader has executed malicious JavaScript code.[48][49]

G0126 Higaisa

Higaisa used JavaScript to execute additional files.[50][51][52]

G0119 Indrik Spider

Indrik Spider has used malicious JavaScript files for several components of their attack.[53]

S0260 InvisiMole

InvisiMole can use a JavaScript file as part of its execution chain.[54]

S0283 jRAT

jRAT has been distributed as HTA files with JScript.[55]

S0648 JSS Loader

JSS Loader can download and execute JavaScript files.[56]

G0094 Kimsuky

Kimsuky has used JScript for logging and downloading additional tools.[57][58] Kimsuky has used TRANSLATEXT, which contained four Javascript files for bypassing defenses, collecting sensitive information and screenshots, and exfiltrating data.[59]

S0356 KONNI

KONNI has executed malicious JavaScript code.[60]

S1075 KOPILUWAK

KOPILUWAK had used Javascript to perform its core functions.[61]

S1160 Latrodectus

Latrodectus has used JavaScript files as part its infection chain during malicious spam email campaigns.[62][63][64]

G0140 LazyScripter

LazyScripter has used JavaScript in its attacks.[65]

G0077 Leafminer

Leafminer infected victims using JavaScript code.[66]

S0455 Metamorfo

Metamorfo includes payloads written in JavaScript.[67]

G0021 Molerats

Molerats used various implants, including those built with JS, on target machines.[68]

G1019 MoustachedBouncer

MoustachedBouncer has used JavaScript to deliver malware hosted on HTML pages.[69]

G0069 MuddyWater

MuddyWater has used JavaScript files to execute its POWERSTATS payload.[70][71][72]

G0129 Mustang Panda

Mustang Panda has executed a JavaScript payload utilizing wscript.exe on the endpoint.[73]

S0228 NanHaiShu

NanHaiShu executes additional Jscript code on the victim's machine.[74]

C0016 Operation Dust Storm

During Operation Dust Storm, the threat actors used JavaScript code.[75]

C0036 Pikabot Distribution February 2024

Pikabot Distribution February 2024 utilized obfuscated JavaScript files for initial Pikabot payload download.[76]

S0223 POWERSTATS

POWERSTATS can use JavaScript code for execution.[70]

S0650 QakBot

The QakBot web inject module can inject Java Script into web banking pages visited by the victim.[77][78]

G1031 Saint Bear

Saint Bear has delivered malicious Microsoft Office files containing an embedded JavaScript object that would, on execution, download and execute OutSteel and Saint Bot.[79]

G0121 Sidewinder

Sidewinder has used JavaScript to drop and execute malware loaders.[80][81]

G0091 Silence

Silence has used JS scripts.[82]

S1124 SocGholish

The SocGholish payload is executed as JavaScript.[83][84][85][86]

S0646 SpicyOmelette

SpicyOmelette has the ability to execute arbitrary JavaScript code on a compromised host.[87]

G1033 Star Blizzard

Star Blizzard has used JavaScript to redirect victim traffic from an adversary controlled server to a server hosting the Evilginx phishing framework.[88]

S1183 StrelaStealer

StrelaStealer has been distributed as a malicious JavaScript object.[89][90][91]

G0092 TA505

TA505 has used JavaScript for code execution.[92][93]

G1037 TA577

TA577 has used JavaScript to execute additional malicious payloads.[94]

G1038 TA578

TA578 has used JavaScript files in malware execution chains.[94]

G0010 Turla

Turla has used various JavaScript-based backdoors.[95]

S0476 Valak

Valak can execute JavaScript containing configuration data for establishing persistence.[96]

S1116 WARPWIRE

WARPWIRE is a credential harvester written in JavaScript.[97]

C0037 Water Curupira Pikabot Distribution

Water Curupira Pikabot Distribution initial delivery included obfuscated JavaScript objects stored in password-protected ZIP archives.[98]

G1035 Winter Vivern

Winter Vivern delivered malicious JavaScript to exploit targets when exploiting Roundcube Webmail servers.[99]

S0341 Xbash

Xbash can execute malicious JavaScript payloads on the victim's machine.[100]

S1248 XORIndex Loader

XORIndex Loader has executed malicious JavaScript code.[101]
