Server Software Component: Web Shell, Sub-technique T1505.003 - Enterprise

Archived: 2026-04-05 16:19:01 UTC

C0034 2022 Ukraine Electric Power Attack

During the 2022 Ukraine Electric Power Attack, Sandworm Team deployed the Neo-REGEORG webshell on an internet-facing server.[3]

G1030 Agrius

Agrius typically deploys a variant of the ASPXSpy web shell following initial access via exploitation.[4]

G0007 APT28

APT28 has used a modified and obfuscated version of the reGeorg web shell to maintain persistence on a target's Outlook Web Access (OWA) server.[5]

G0016 APT29

APT29 has installed web shells on exploited Microsoft Exchange servers.[6][7]

G0050 APT32

APT32 has used Web shells to maintain access to victim websites.[8]

G0082 APT38

APT38 has used web shells for persistence or to ensure redundant access.[9]

G0087 APT39

APT39 has installed ANTAK and ASPXSPY web shells.[10]

C0040 APT41 DUST

APT41 DUST involved use of web shells such as ANTSWORD and BLUEBEAM for persistence.[11]

G1023 APT5

APT5 has installed multiple web shells on compromised servers including on Pulse Secure VPN appliances.[12][13]

S0073 ASPXSpy

ASPXSpy is a Web shell. The ASPXTool version used by Threat Group-3390 has been deployed to accessible servers running Internet Information Services (IIS).[14]

G0135 BackdoorDiplomacy

BackdoorDiplomacy has used web shells to establish an initial foothold and for lateral movement within a victim's system.[15]

G1043 BlackByte

BlackByte has used ASPX web shells following exploitation of vulnerabilities in services such as Microsoft Exchange.[16][17]

S1118 BUSHWALK

BUSHWALK is a web shell that has the ability to execute arbitrary commands or write files.[18]

C0017 C0017

During C0017, APT41 deployed JScript web shells through the creation of malicious ViewState objects.[19]

C0032 C0032

During the C0032 campaign, TEMP.Veles planted Web shells on Outlook Exchange servers.[20]

S0020 China Chopper

China Chopper's server component is a Web Shell payload.[2]

G1012 CURIUM

CURIUM has been linked to web shells following likely server compromise as an initial access vector into victim networks.[21]

C0029 Cutting Edge

During Cutting Edge, threat actors used multiple web shells to maintain presence on compromised Connect Secure appliances such as WIREFIRE, GLASSTOKEN, BUSHWALK, LIGHTWIRE, and FRAMESTING.[22][23]

G0009 Deep Panda

Deep Panda uses Web shells on publicly accessible Web servers to access victim networks.[24]

G0035 Dragonfly

Dragonfly has commonly created Web shells on victims' publicly accessible email and web servers, which they used to maintain access to a victim network and download additional malicious files.[25]

G1003 Ember Bear

Ember Bear deploys web shells following initial access for either follow-on command execution or protocol tunneling. Example web shells used by Ember Bear include P0wnyshell, reGeorg, P.A.S. Webshell, and custom variants of publicly-available web shell examples.[26][27]

G1016 FIN13

FIN13 has utilized obfuscated and open-source web shells such as JspSpy, reGeorg, MiniWebCmdShell, and Vonloesch Jsp File Browser 1.2 to enable remote code execution and to execute commands on compromised web server.[28]

G0117 Fox Kitten

Fox Kitten has installed web shells on compromised hosts to maintain access.[29][30]

S1120 FRAMESTING

FRAMESTING is a web shell capable of enabling arbitrary command execution on compromised Ivanti Connect Secure VPNs.[18]

C0041 FrostyGoop Incident

FrostyGoop Incident deployed a ReGeorg variant web shell to impacted systems following initial access for persistence.[31]

G0093 GALLIUM

GALLIUM used Web shells to persist in victim environments and assist in execution and exfiltration.[32][33]

S1117 GLASSTOKEN

GLASSTOKEN is a web shell capable of tunneling C2 connections and code execution on compromised Ivanti Secure Connect VPNs.[23]

G0125 HAFNIUM

HAFNIUM has deployed multiple web shells on compromised servers including SIMPLESEESHARP, SPORTSBALL, China Chopper, and ASPXSpy.[34][35][36][37][38][39]

C0038 HomeLand Justice

For HomeLand Justice, threat actors used .aspx webshells named pickers.aspx, error4.aspx, and ClientBin.aspx, to maintain persistence.[40][41]

G0094 Kimsuky

Kimsuky has used modified versions of open source PHP web shells to maintain access, often adding "Dinosaur" references within the code.[42]

G0065 Leviathan

Leviathan relies on web shells for an initial foothold as well as persistence into the victim's systems.[43][44][45]

C0049 Leviathan Australian Intrusions

Leviathan relied extensively on web shell use following initial access for persistence and command execution purposes in victim environments during Leviathan Australian Intrusions.[45]

S1119 LIGHTWIRE

LIGHTWIRE is a web shell capable of command execution and establishing persistence on compromised Ivanti Secure Connect VPNs.[18]

S1188 Line Runner

Line Runner is a persistent Lua-based web shell.[46]

G0059 Magic Hound

Magic Hound has used multiple web shells to gain execution.[47][48]

G1051 Medusa Group

Medusa Group has utilized webshells to an exploited Microsoft Exchange Server.[49]

G1009 Moses Staff

Moses Staff has dropped a web shell onto a compromised system.[50]

G0129 Mustang Panda

Mustang Panda has used China Chopper web shells to maintain access to victims' environments.[51]

S1189 Neo-reGeorg

Neo-reGeorg can be installed on compromised web servers to tunnel C2 connections.[52][3]

G0049 OilRig

OilRig has used web shells, often to maintain access to a victim network.[53][54][55][56]

C0012 Operation CuckooBees

During Operation CuckooBees, the threat actors generated a web shell within a vulnerable Enterprise Resource Planning Web Application Server as a persistence mechanism.[57]

C0014 Operation Wocao

During Operation Wocao, threat actors used their own web shells, as well as those previously placed on target systems by other threat actors, for reconnaissance and lateral movement.[58]

S0072 OwaAuth

OwaAuth is a Web shell that appears to be exclusively used by Threat Group-3390. It is installed as an ISAPI filter on Exchange servers and shares characteristics with the China Chopper Web shell.[14]

S0598 P.A.S. Webshell

P.A.S. Webshell can gain remote access and execution on target web servers.[59]

S1108 PULSECHECK

PULSECHECK is a web shell that can enable command execution on compromised servers.[12]

S1113 RAPIDPULSE

RAPIDPULSE is a web shell that is capable of arbitrary file read on targeted web servers to exfiltrate items of interest on the victim device.[13]

S1187 reGeorg

reGeorg is a web shell that has been installed on exposed web servers for access to victim environments.[7][26]

G0034 Sandworm Team

Sandworm Team has used webshells including P.A.S. Webshell to maintain access to victim networks.[59]

G1041 Sea Turtle

Sea Turtle deployed the SnappyTCP web shell during intrusion operations.[60][61]

S0185 SEASHARPEE

SEASHARPEE is a Web shell.[54]

C0058 SharePoint ToolShell Exploitation

During SharePoint ToolShell Exploitation, threat actors followed exploitation of SharePoint servers with installation of a malicious .aspx web shell (spinstall0.aspx) that was written to the `_layouts/15/` directory, granting persistent HTTP-based access.[62][63][64][65][66][67]

S1110 SLIGHTPULSE

SLIGHTPULSE is a web shell that can read, write, and execute files on compromised servers.[12]

S1163 SnappyTCP

SnappyTCP is a reverse TCP shell with command and control capabilities used for persistence purposes.[60]

S1112 STEADYPULSE

STEADYPULSE is a web shell that can enable the execution of arbitrary commands on compromised web servers.[12]

S0578 SUPERNOVA

SUPERNOVA is a Web shell.[68][69][70]

G0027 Threat Group-3390

Threat Group-3390 has used a variety of Web shells.[71]

G0131 Tonto Team

Tonto Team has used a first stage web shell after compromising a vulnerable Exchange server.[72]

G0081 Tropic Trooper

Tropic Trooper has started a web service in the target host and wait for the adversary to connect, acting as a web shell.[73]

C0039 Versa Director Zero Day Exploitation

Versa Director Zero Day Exploitation resulted in the deployment of the VersaMem web shell for follow-on activity.[74]

G0123 Volatile Cedar

Volatile Cedar can inject web shell code into a server.[75][76]

G1017 Volt Typhoon

Volt Typhoon has used webshells, including ones named AuditReport.jspx and iisstart.aspx, in compromised environments.[77]

S1115 WIREFIRE

WIREFIRE is a web shell that can download files to and execute arbitrary commands from compromised Ivanti Connect Secure VPNs.[22]
