Drive-by Compromise, Technique T1189 - Enterprise

Archived: 2026-04-05 16:01:15 UTC

C0057 3CX Supply Chain Attack

During the 3CX Supply Chain Attack, AppleJeus compromised the `www.tradingtechnologies[.]com` website hosting a hidden IFRAME to exploit visitors, two months before the site was known to deliver a compromised version of the X_TRADER software package.[5]

G0138 Andariel

Andariel has used watering hole attacks, often with zero-day exploits, to gain initial access to victims within a specific IP range.[6][7]

G0073 APT19

APT19 performed a watering hole attack on forbes.com in 2014 to compromise targets.[8]

G0007 APT28

APT28 has compromised targets via strategic web compromise utilizing custom exploit kits.[9] APT28 used reflected cross-site scripting (XSS) against government websites to redirect users to phishing webpages.[10]

G0050 APT32

APT32 has infected victims by tricking them into visiting compromised watering hole websites.[11][12]

G0067 APT37

APT37 has used strategic web compromises, particularly of South Korean websites, to distribute malware. The group has also used torrent file-sharing sites to more indiscriminately disseminate malware to victims. As part of their compromises, the group has used a Javascript based profiler called RICECURRY to profile a victim's web browser and deliver malicious code accordingly.[13][14][15]

G0082 APT38

APT38 has conducted watering holes schemes to gain initial access to victims.[16][17]

G0001 Axiom

Axiom has used watering hole attacks to gain access.[18]

S0606 Bad Rabbit

Bad Rabbit spread through watering holes on popular sites by injecting JavaScript into the HTML body or a `.js` file.[19][20]

G0060 BRONZE BUTLER

BRONZE BUTLER compromised three Japanese websites using a Flash exploit to perform watering hole attacks.[21]

S0482 Bundlore

Bundlore has been spread through malicious advertisements on websites.[22]

C0010 C0010

During C0010, UNC3890 actors likely established a watering hole that was hosted on a login page of a legitimate Israeli shipping company that was active until at least November 2021.[23]

G1012 CURIUM

CURIUM has used strategic website compromise to infect victims with malware such as IMAPLoader.[24]

G1034 Daggerfly

Daggerfly has used strategic website compromise for initial access against victims.[25]

G0070 Dark Caracal

Dark Caracal leveraged a watering hole to serve up malicious code.[26]

G0012 Darkhotel

Darkhotel used embedded iframes on hotel login portals to redirect selected victims to download malware.[27]

G0035 Dragonfly

Dragonfly has compromised targets via strategic web compromise (SWC) utilizing a custom exploit kit.[28][29][30]

G1006 Earth Lusca

Earth Lusca has performed watering hole attacks.[31]

G0066 Elderwood

Elderwood has delivered zero-day exploits and malware to victims by injecting malicious code into specific public Web pages visited by targets within a particular sector.[32][33][34]

S0531 Grandoreiro

Grandoreiro has used compromised websites and Google Ads to bait victims into downloading its installer.[35][36]

S0483 IcedID

IcedID has cloned legitimate websites/applications to distribute the malware.[37]

S0215 KARAE

KARAE was distributed through torrent file-sharing websites to South Korean victims, using a YouTube video downloader application as a lure.[14]

G0032 Lazarus Group

Lazarus Group delivered RATANKBA and other malicious code to victims via a compromised legitimate website.[38][39]

G0077 Leafminer

Leafminer has infected victims using watering holes.[40]

G0065 Leviathan

Leviathan has infected victims using watering holes.[41]

S0451 LoudMiner

LoudMiner is typically bundled with pirated copies of Virtual Studio Technology (VST) for Windows and macOS.[42]

G0095 Machete

Machete has distributed Machete through a fake blog website.[43]

G0059 Magic Hound

Magic Hound has conducted watering-hole attacks through media and magazine websites.[44]

G1020 Mustard Tempest

Mustard Tempest has used drive-by downloads for initial infection, often using fake browser updates as a lure.[45][46][47][48]

C0016 Operation Dust Storm

During Operation Dust Storm, the threat actors used a watering hole attack on a popular software reseller to exploit the then-zero-day Internet Explorer vulnerability CVE-2014-0322.[49]

G0040 Patchwork

Patchwork has used watering holes to deliver files with exploits to initial victims.[50][51]

G0068 PLATINUM

PLATINUM has sometimes used drive-by attacks against vulnerable browser plugins.[52]

S0216 POORAIM

POORAIM has been delivered through compromised sites acting as watering holes.[14]

G0056 PROMETHIUM

PROMETHIUM has used watering hole attacks to deliver malicious versions of legitimate installers.[53]

S0496 REvil

REvil has infected victim machines through compromised websites and exploit kits.[54][55][56][57]

G0048 RTM

RTM has distributed its malware via the RIG and SUNDOWN exploit kits, as well as online advertising network `Yandex.Direct`.[58][59]

S1086 Snip3

Snip3 has been delivered to targets via downloads from malicious domains.[60]

S1124 SocGholish

SocGholish has been distributed through compromised websites with malicious content often masquerading as browser updates.[45]

G0027 Threat Group-3390

Threat Group-3390 has extensively used strategic web compromises to target victims.[61][62]

G0134 Transparent Tribe

Transparent Tribe has used websites with malicious hyperlinks and iframes to infect targeted victims with Crimson, njRAT, and other malicious tools.[63][64][65]

G0010 Turla

Turla has infected victims using watering holes.[66][67]

G0124 Windigo

Windigo has distributed Windows malware via drive-by downloads.[68]

G0112 Windshift

Windshift has used compromised websites to register custom URL schemes on a remote system.[69]

G1035 Winter Vivern

Winter Vivern created dedicated web pages mimicking legitimate government websites to deliver malicious fake anti-virus software.[70]
