Web Service, Technique T1102 - Enterprise

Archived: 2026-04-05 17:12:38 UTC

G0050 APT32

APT32 has used Dropbox, Amazon S3, and Google Drive to host malicious downloads.[2]

C0040 APT41 DUST

APT41 DUST used compromised Google Workspace accounts for command and control.[3]

G1044 APT42

APT42 has used various links, such as links with typo-squatted domains, links to Dropbox files and links to fake Google sites, in spearphishing operations.[4][5][6]

S1081 BADHATCH

BADHATCH can be utilized to abuse `sslip.io`, a free IP to domain mapping service, as part of actor-controlled C2 channels.[7]

S0534 Bazar

Bazar downloads have been hosted on Google Docs.[8][9]

S0635 BoomBox

BoomBox can download files from Dropbox using a hardcoded access token.[10]

S1063 Brute Ratel C4

Brute Ratel C4 can use legitimate websites for external C2 channels including Slack, Discord, and MS Teams.[11]

S1039 Bumblebee

Bumblebee has been downloaded to victim's machines from OneDrive.[12]

C0017 C0017

During C0017, APT41 used the Cloudflare services for C2 communications.[13]

C0027 C0027

During C0027, Scattered Spider downloaded tools from sites including file.io, GitHub, and paste.ee.[14]

S0335 Carbon

Carbon can use Pastebin to receive C2 commands.[15]

S0674 CharmPower

CharmPower can download additional modules from actor-controlled Amazon S3 buckets.[16]

S1149 CHIMNEYSWEEP

CHIMNEYSWEEP has the ability to use use Telegram channels to return a list of commands to be executed, to download additional payloads, or to create a reverse shell.[17]

S1066 DarkTortilla

DarkTortilla can retrieve its primary payload from public sites such as Pastebin and Textbin.[18]

S0600 Doki

Doki has used the dogechain.info API to generate a C2 address.[19]

S0547 DropBook

DropBook can communicate with its operators by exploiting the Simplenote, DropBox, and the social media platform, Facebook, where it can create fake accounts to control the backdoor and receive instructions.[20][21]

G1011 EXOTIC LILY

EXOTIC LILY has used file-sharing services including WeTransfer, TransferNow, and OneDrive to deliver payloads.[22]

G0037 FIN6

FIN6 has used Pastebin and Google Storage to host content for their operations.[23]

G0061 FIN8

FIN8 has used `sslip.io`, a free IP to domain mapping service that also makes SSL certificate generation easier for traffic encryption, as part of their command and control.[24]

G0117 Fox Kitten

Fox Kitten has used Amazon Web Services to host C2.[25]

G0047 Gamaredon Group

Gamaredon Group has used GitHub repositories for downloaders which will be obtained by the group's .NET executable on the compromised system.[26]

S0561 GuLoader

GuLoader has the ability to download malware from Google Drive.[27]

S0601 Hildegard

Hildegard has downloaded scripts from GitHub.[28]

G0100 Inception

Inception has incorporated at least five different cloud service providers into their C2 infrastructure including CloudMe.[29][30]

S1160 Latrodectus

Latrodectus has used Google Firebase to download malicious installation scripts.[31]

G0140 LazyScripter

LazyScripter has used GitHub to host its payloads to operate spam campaigns.[32]

S1221 MOPSLED

MOPSLED can use third-party web services such as GitHub and Google Drive for C2.[33]

G0129 Mustang Panda

Mustang Panda has used DropBox URLs to deliver variants of PlugX.[34] Mustang Panda has also used Google Drive to host malicious downloads.[35]

S0198 NETWIRE

NETWIRE has used web services including Paste.ee to host payloads.[36]

S0508 ngrok

ngrok has been used by threat actors to proxy C2 connections to ngrok service subdomains.[37]

S1147 Nightdoor

Nightdoor can utilize Microsoft OneDrive or Google Drive for command and control purposes.[38][39]

C0005 Operation Spalax

During Operation Spalax, the threat actors used OneDrive and MediaFire to host payloads.[40]

S1130 Raspberry Robin

Raspberry Robin second stage payloads can be hosted as RAR files, containing a malicious EXE and DLL, on Discord servers.[41]

G1039 RedCurl

RedCurl has used web services to download malicious files.[42][43]

S1240 RedLine Stealer

RedLine Stealer has leveraged legitimate file sharing web services to host malicious payloads.[44][45]

G0106 Rocke

Rocke has used Pastebin, Gitee, and GitLab for Command and Control.[46][47]

S0546 SharpStage

SharpStage has used a legitimate web service for evading detection.[20]

S1178 ShrinkLocker

ShrinkLocker uses a subdomain on the legitimate Cloudflare resource "trycloudflare[.]com" to obfuscate the threat actor's actual address and to tunnel information sent from victim systems.[48]

S0589 Sibot

Sibot has used a legitimate compromised website to download DLLs to the victim's machine.[49]

S0649 SMOKEDHAM

SMOKEDHAM has used Google Drive and Dropbox to host files downloaded by victims via malicious links.[50]

S1086 Snip3

Snip3 can download additional payloads from web services including Pastebin and top4top.[51]

S1124 SocGholish

SocGholish has used Amazon Web Services to host second-stage servers.[52]

G0139 TeamTNT

TeamTNT has leveraged iplogger.org to send collected data back to C2.[53][54]

G0010 Turla

Turla has used legitimate web services including Pastebin, Dropbox, and GitHub for C2 communications.[15][55]

S0689 WhisperGate

WhisperGate can download additional payloads hosted on a Discord channel.[56][57][58][59][60]
