Threat Actor Infrastructure

Each extension's configuration server is a unique domain or subdomain, distinct from other infrastructure in the extension's main application code. For example, for the malicious KProxy extension, the main application code uses `kproxy[.]com` and the config server is at `kproxy[.]site`. We also note that the hardcoded integer IDs used in the heartbeat requests are in a loose incremental range and may suggest a much greater scope of operations by this threat actor.

Extension ID	Name	Last Updated	Config Server	ID
mdaboflcmhejfihjcbmdiebgfchigjcf	Blipshot: one click full page screenshots	July 4, 2024	blipshotextension[.]com	164
gaoflciahikhligngeccdecgfjngejlh	Emojis - Emoji Keyboard	July 4, 2024	emojikeyboardextension[.]com	166
fedimamkpgiemhacbdhkkaihgofncola	WAToolkit	July 4, 2024	watoolkit[.]com	9997
jlhgcomgldfapimdboelilfcipigkgik	Color Changer for YouTube	July 5, 2024	colorchanger[.]net	148
jdjldbengpgdcfkljfdmakdgmfpneldd	Video Effects for YouTube And Audio Enhancer	July 5, 2024	ytvideoeffectsextension[.]com	160
deljjimclpnhngmikaiiodgggdniaooh	Themes for Chrome and YouTube™ Picture in Picture	July 17, 2024	themesforytextension[.]com	155
giaoehhefkmchjbbdnahgeppblbdejmj	Mike Adblock für Chrome | Chrome-Werbeblocker	July 18, 2024	adblockforytextension[.]com	158
hmooaemjmediafeacjplpbpenjnpcneg	Page Refresh	July 25, 2024	pagerefresh-extension[.]com	112
acbiaofoeebeinacmcknopaikmecdehl	Wistia Video Downloader	August 8, 2024	wistiaextension[.]com	156
nlgphodeccebbcnkgmokeegopgpnjfkc	Super dark mode	August 11, 2024	sdmextension[.]com	167
fbcgkphadgmbalmlklhbdagcicajenei	Emoji keyboard emojis for chrome	August 11, 2024	emojikeyboardforchrome[.]com	170
alplpnakfeabeiebipdmaenpmbgknjce	Adblocker for Chrome - NoAds	August 22, 2024	noadsadblocker[.]com	94
ogcaehilgakehloljjmajoempaflmdci	Adblock for You	September 10, 2024	abu-xt[.]com	147
onomjaelhagjjojbkcafidnepbfkpnee	Adblock for Chrome	September 10, 2024	abfc-extension[.]com	199
bpconcjcammlapcogcnnelfmaeghhagj	Nimble capture	September 27, 2024	api.nimblecapture[.]com	172
gdocgbfmddcfnlnpmnghmjicjognhonm	KProxy	October 8, 2024	kproxyservers[.]site	151