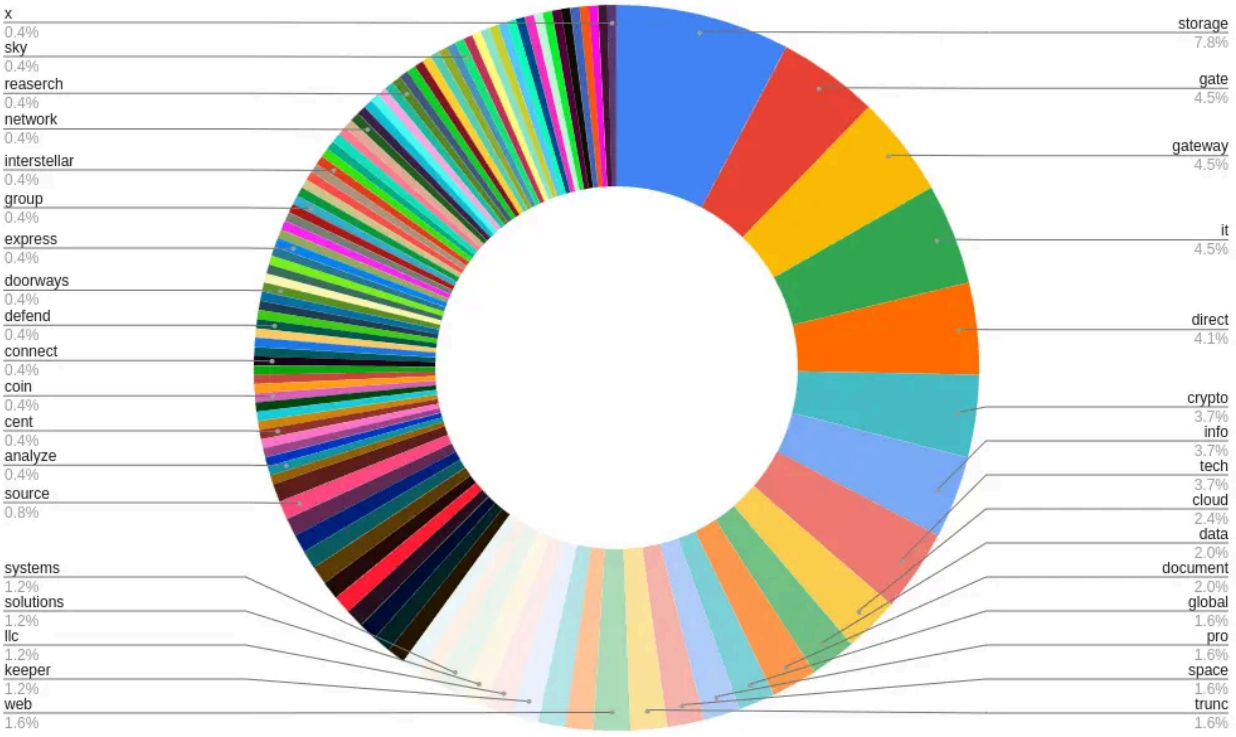
BlueCharlie, Previously Tracked as TAG-53, Continues to Deploy New Infrastructure in 2023 | Recorded Future

By Insikt Group

Archived: 2026-04-05 13:08:18 UTC

Insikt Group has been tracking the threat activity group BlueCharlie, associated with the Russia-nexus group Callisto/Calisto, COLDRIVER, and Star Blizzard/SEABORGIUM. BlueCharlie, a Russia-linked threat group active since 2017, focuses on information gathering for espionage and hack-and-leak operations. BlueCharlie has evolved its tactics, techniques, and procedures (TTPs) and built new infrastructure, indicating sophistication in adapting to public disclosures and improving operations security. While specific victims are unknown, past targets include government, defense, education, political sectors, NGOs, journalists, and think tanks.



Breakdown of terms used in BlueCharlie activity since November 2022

Recently, Insikt Group observed BlueCharlie build new infrastructure for likely use in phishing campaigns and/or credential harvesting, which consists of 94 new domains. Several of the TTPs seen in the recent operation depart from past activity, suggesting that BlueCharlie is evolving its operations, potentially in response to public disclosures of its operations in industry reporting. Since Insikt Group's initial tracking of the group in September

2022, we have observed BlueCharlie engage in several TTP shifts. These shifts demonstrate that these threat actors are aware of industry reporting and show a certain level of sophistication in their efforts to obfuscate or modify their activity, aiming to stymie security researchers.

To counter BlueCharlie's threat, network defenders should enhance phishing defenses, implement FIDO2-compliant multi-factor authentication, use threat intelligence, and educate third-party vendors. BlueCharlie's continued use of phishing and its historical adaptation to public reporting suggest it will remain active and evolve further in its operations.

To read the entire analysis with endnotes, click here to download the report as a PDF.

Appendix A — Indicators of Compromise

BlueCharlie Domains:
bittechllc[.]net
centeritdefcity[.]com
checkscreenit[.]com
cloudcpanelhost[.]com
clouddefsystems[.]com
cloudrootstorage[.]com
commandentrance[.]com
computertechdirectsystems[.]com
computingtechstudio[.]com
configuregatewayglobal[.]com
controlgatestorage[.]com
controlsstoragedirect[.]com
controlstoragesolutions[.]com
cryptdatagate[.]com
cryptoanalyzetech[.]com
cryptotechdirect[.]com
cryptothistech[.]com
datagatellc[.]com
datagatewayglobal[.]com
datastoragecrypto[.]com
definform[.]com
deskactivitygm[.]com
directdocumentgate[.]com
directdocumentgateway[.]com
directexpressgateway[.]com
directstoragegate[.]com
docsinfogate[.]com
documentdirectllc[.]com
documentdirectto[.]com
entrywaycenter[.]com
gateblurbrepository[.]com
gatecryptospace[.]com
gateinfosecure[.]com
gatestoragetech[.]com
gatewaydocsint[.]com
gatewayitsol[.]com
gatewayrecord[.]com
gawecryptoinfosolutions[.]com
getinfostarter[.]com
incappcloud[.]com

infocryptogate[.]com
infogatestorage[.]com
informationcoindata[.]com
informationswitchsystems[.]com
infostorageroute[.]com
intelligencerepository[.]com
itgatestorage[.]com
itinfogate[.]com
keepitlabgroup[.]com
managercodepro[.]com
meshgoin[.]com
myitappnext[.]com
myittechnext[.]com
networkgoin[.]com
oneinformationcrypto[.]com
pdfdirectglobal[.]com
pdfsecxcloudroute[.]com
po.vatangate[.]com
prodefendme[.]com
prokeeperit[.]com
protectedviews[.]com
protectordocumentcenter[.]com
realeasyconfiguregateway[.]com
realitsolutionprimary[.]com
safetydocsgateway[.]com
secureglobaltele[.]com
serverguarditweb[.]com
shielditlabel[.]com
shortinfoonline[.]com
skycithereforeit[.]com
solutionsseccloud[.]com
sourcedoorway[.]com
sourcedoorways[.]com
stateinfospace[.]com
storagecryptogate[.]com
storagecryptoweb[.]com
storageinfogate[.]com
storagekeeperinfopro[.]com
storagekeeperinfotech[.]com
storagerootconnect[.]com
storagetruncservices[.]com
storagetruncservices[.]com

storagewarden[.]com
suppdatacent[.]com
threatcenterofreaserch[.]com
transfer-dns[.]com
truncstorage[.]com
truncstorage[.]com
webgateway[.]ru
webgatewayenter[.]com
webinterstellar[.]com
yourdirectinfospace[.]com
yourspaceprotector[.]com

BlueCharlie IP Addresses:
104.140.180[.]125
104.140.180[.]126
104.168.32[.]133
104.168.46[.]21
107.174.45[.]104
107.174.45[.]106
107.175.21[.]29
138.124.183[.]150
138.124.183[.]150
142.11.194[.]133
142.11.195[.]232
142.11.196[.]83
142.11.199[.]18
146.19.170[.]161
146.19.170[.]162
162.19.175[.]92
172.245.191[.]18
172.245.220[.]195
172.245.220[.]206
172.245.254[.]219
172.245.33[.]142
172.245.33[.]188
185.138.164[.]123
185.138.164[.]229
185.250.151[.]11
185.250.151[.]11
192.210.214[.]114
192.210.214[.]150
192.210.215[.]125
192.227.162[.]32

192.236.146[.]12
192.236.195[.]192
192.236.195[.]192
192.3.111[.]149
192.3.111[.]200
192.3.118[.]108
192.3.223[.]33
192.3.228[.]170
192.3.228[.]182
192.3.73[.]140
192.3.73[.]143
194.213.18[.]35
194.213.18[.]96
198.46.174[.]172
198.46.174[.]188
23.254.253[.]127
23.94.152[.]50
23.94.231[.]161
23.94.236[.]80
23.94.96[.]12
23.94.99[.]19
23.94.99[.]22
23.94.99[.]26
23.94.99[.]30
45.137.155[.]33
45.144.30[.]160
45.144.31[.]92
45.66.249[.]101
45.66.249[.]101
45.66.249[.]83
45.8.146[.]119
45.8.146[.]213
45.8.146[.]227
45.86.230[.]104
45.86.230[.]171
45.86.230[.]61
5.61.63[.]19
77.91.126[.]29
77.91.126[.]29
85.239.52[.]228
85.239.52[.]44
85.239.53[.]154

85.239.53[.]19
85.239.53[.]54
85.239.53[.]73
85.239.54[.]200
85.239.54[.]205
85.239.54[.]242
85.239.54[.]244
85.239.54[.]54
85.239.54[.]84
85.239.54[.]84
85.239.60[.]103
85.239.60[.]105
85.239.60[.]105
85.239.60[.]71
85.239.61[.]52
91.210.164[.]40
91.228.10[.]45
91.231.186[.]105
91.231.186[.]33
94.131.8[.]189
95.164.18[.]80

Appendix B — MITRE ATT&CK Techniques

Tactic: Technique	**ATT&CK Code**
Reconnaissance: Phishing for Information	T1598
Resource Development: Stage Capabilities	T1608
