CYBER THREAT ANALYSIS

RUSSIA

Recorded Future®

By Insikt Group®

August 2, 2023

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

Executive Summary

Since at least March 2023, Insikt Group has tracked new infrastructure that we attribute as associated with the threat activity group BlueCharlie, a group that has overlaps with the Russia-nexus group publicly known as Callisto/Calisto, COLDRIVER, and Star Blizzard/SEABORGIUM. Insikt Group previously tracked this threat activity under the temporary designator TAG-53. We are now graduating this threat cluster to the cryptonym BlueCharlie due to overlapping tactics, techniques, and procedures (TTPs) and our increased confidence that the activities we have observed are conducted by a Russia-based threat actor.

Insikt Group has observed BlueCharlie build new infrastructure, which includes 94 new domains. Several of the TTPs currently 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 (1, 2, 3). 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. Some of the changes in TTPs were also likely precipitated by the threat group's increased awareness of operations security (OPSEC).

While Insikt Group was unable to determine victimology or targeting for this campaign at the time of this writing, BlueCharlie has in the past targeted entities in the government, higher education, defense, and political sectors, as well as non-governmental organizations (NGOs), activists, journalists, think tanks, and national laboratories. Potential victims in those sectors should improve their phishing defenses, implement FIDO2-compliant multi-factor authentication, use threat intelligence and attack surface intelligence for rapid and complete information, and educate third-party vendors on the risks involved. Failure to do so may result in the loss of credentials to business-critical resources, leaking of proprietary information related to business or national security, and damage to brand reputation for suffering a breach.

Key Findings

- BlueCharlie continues to build new infrastructure in the pursuit of phishing campaigns and credential harvesting, and it continues to favor certain elements such as the use of preferred registrars, ASNs, and a certificate authority.
- While the group uses relatively common techniques to conduct attacks (such as the use of phishing and a historical reliance on open-source offensive security tools), its likely continued use of these methods, determined posture, and progressive evolution of tactics suggests the group remains formidable and capable.
- Given the group's observed operational tempo and willingness to adapt to public reporting on its activity, we expect to see BlueCharlie continue operations for the foreseeable future. We similarly expect the group to continue to evolve its TTPs based on precedent.

Background

BlueCharlie is a Russia-linked threat activity group that has links to groups that have been active since at least 2017. BlueCharlie conducts operations focused on information gathering to enable further espionage, but also for use in hack-and-leak operations. BlueCharlie targets individuals and organizations in North Atlantic Treaty Organization (NATO) nations, entities in Ukraine, and institutions like government, higher education, defense, and political sectors, non-governmental organizations (NGOs), activists, journalists, think tanks, and national laboratories. Past incidents include a hack-and-leak operation that tried to build a narrative around high-level Brexit proponents planning a coup as well as a cyberespionage campaign targeting Brookhaven National Laboratory, Argonne National Laboratory, and Lawrence Livermore National Laboratory between August and September 2022. In January 2023, cybersecurity firm Nisos observed personally identifiable information related to technical details of COLDRIVER campaigns, and found ties to a Russian national, Andrey Korinets, as a potential member of the group. Insikt Group has not independently verified Korinets's affiliation with BlueCharlie activity at this time.

BlueCharlie has carried out persistent phishing and credential theft campaigns that further enable intrusions and data theft. The group likely uses open sources to conduct extensive reconnaissance in advance of intrusion operations in order to improve the likelihood that its spearphishing operations will succeed. In at least one case, Star Blizzard/SEABORGIUM created fraudulent profiles on various social media platforms, including LinkedIn, to conduct reconnaissance on targeted entities. Some of the messages included resources that spoofed pages from prominent organizations to build credibility. Campaigns between 2015 and 2020 relied on emails purporting to come from popular mail services and often contained malicious links or attachments.

Threat and Technical Analysis

Following public reporting (1, 2, 3, 4, 5, 6), including our own, we observed that BlueCharlie changed its TTPs as of at least mid-December 2022 — shortly after our report and other industry reporting exposed its credential harvesting infrastructure.

Domain Name Structure

Since the release of our initial report describing TAG-53 activity, the threat group has shifted its use of certain words in its domains to a new pattern.

In our previous report, all but 1 of the 38 domains discovered via BlueCharlie tracking used similarly structured domain names, primarily made up of 2 terms (depicted in **Figure 1** below) separated by a hyphen, such as "cloud-safety[.]online". The exception to the above rule was *proxycrioisolation[.]com*. While the structure has changed for the most recent activity, the new naming convention is consistent and highly similar across all 94 observed domains. Prior activity relied on a trailing URL structure for

phishing attacks, such as *http[:]//goo-ink[.]online/**adfs[.]llnl[.g]ov/ks/*** (1, 2), which emulates a Lawrence Livermore National Laboratory Microsoft Active Directory instance. This shift in tactics away from trailing URL structures to the new hyphenated, random-word naming convention has stymied the identification of victims and targeting by the group in this most recent campaign. The use of these trailing URLs can be configured[1] in the config.yaml file of Evilginx, an open-source offensive security tool previously used by BlueCharlie. While we have identified a number of new domains, we have not observed the use of these trailing URL paths at the time of this writing; however, this does not preclude their active use.

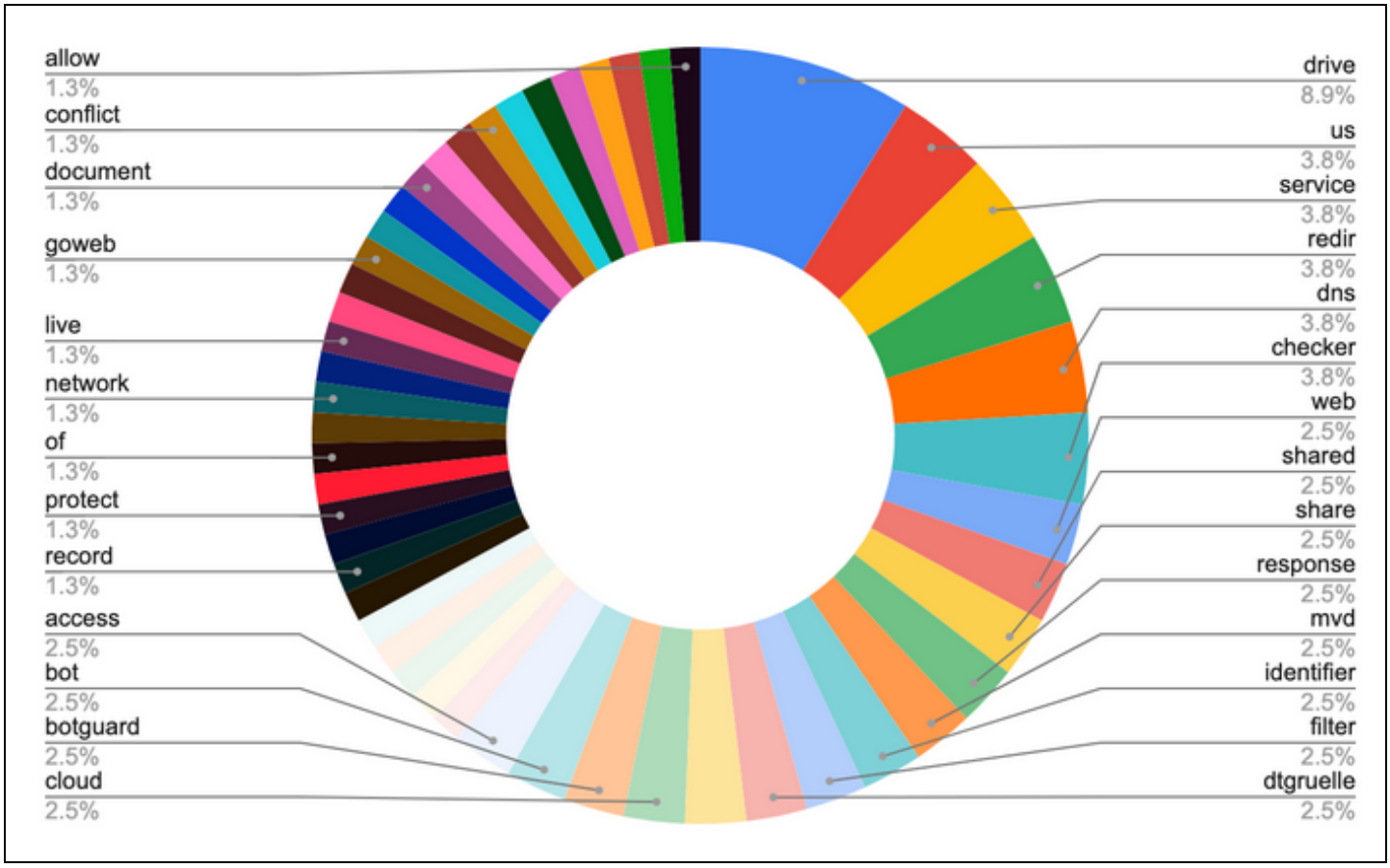


Figure 1: *Breakdown of terms used in BlueCharlie from January to November 2022 (Source: Recorded Future)*

Since at least December 17, 2022, BlueCharlie has chosen domain-naming themes centered around information technology and cryptocurrency, shown in **Figure 2**, with domain names such as *cloudrootstorage[.]com*, *directexpressgateway[.]com*, *storagecryptogate[.]com*, or *pdfsecxcloudroute[.]com*. **Appendix A** contains a complete list of the identified domains. Almost all of the domains we identified share this theme and are consistent, similar to prior BlueCharlie conventions.

[1] https[:]//github[.]com/kgretzky/evilginx2/blob/511860ca993b73e0d412c372c8aaa4b70ba5a7e1/core/config.go

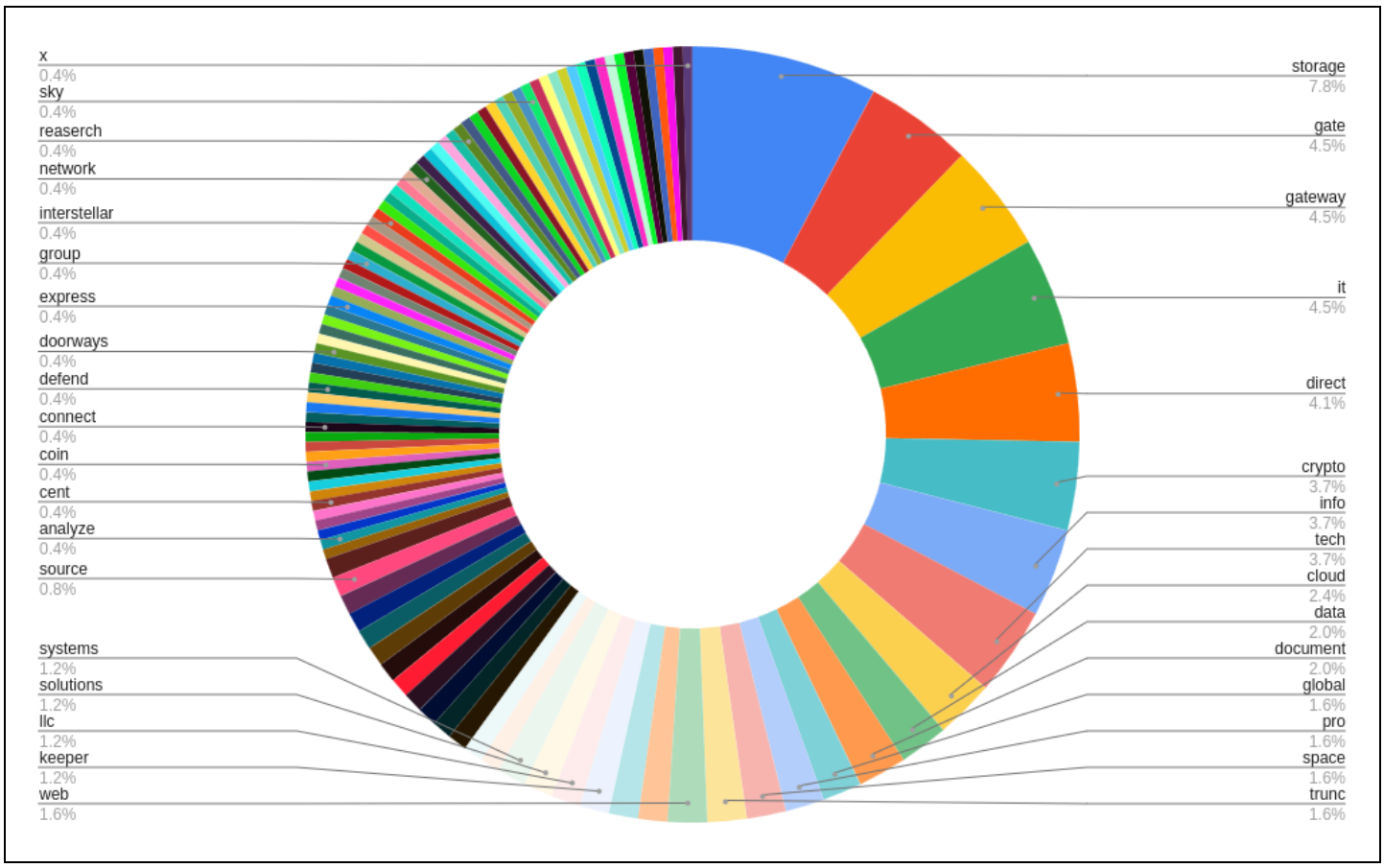


Figure 2: *Breakdown of terms used in BlueCharlie activity since November 2022 (Source: Recorded Future)*

We also identified commonly used words between the old and new activity:

- check/checker
- dns
- cloud
- control/controls
- docs
- document
- network
- of
- protect/protected/protector
- safety
- storage
- transfer
- web

We have not observed any direct impersonation of target domains at this time, such as the previously observed *dtgruelle-us[.]com* or *mvd-redir[.]ru*, which emulate a US logistics company and the Russian Ministry of Internal Affairs, respectively — a departure from past behavior.

Registrars

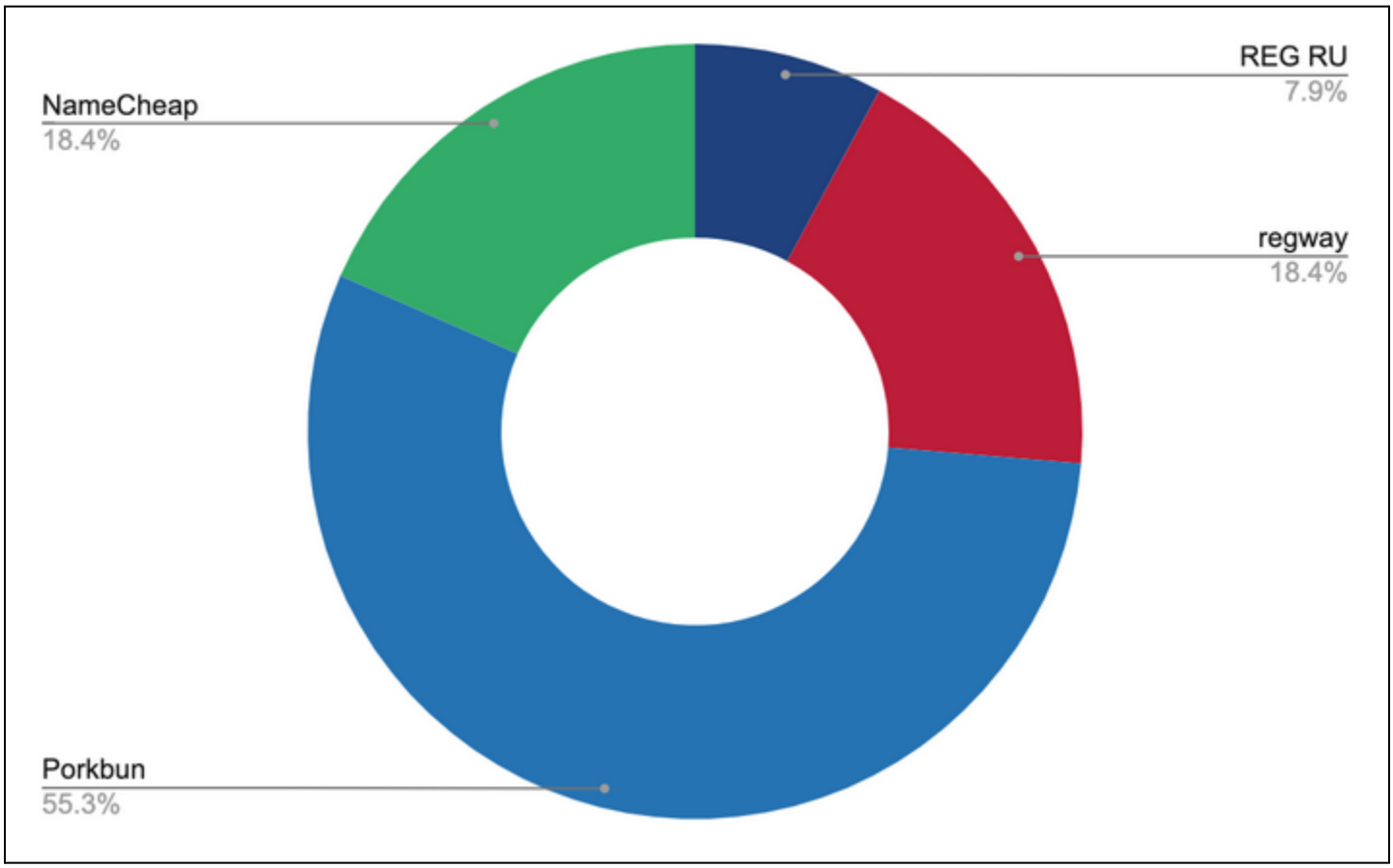


Figure 3: *Breakdown of domain registrars used by BlueCharlie in the previous campaign, January to November 2022 (Source: Recorded Future)*

In previous reporting, we identified that for the majority of their domain registrations, BlueCharlie preferred the Porkbun registrar, followed by NameCheap, Regway, and REG RU, depicted in the graph in **Figure 3** above.

In BlueCharlie's current activity, the group overwhelmingly preferred the registrar NameCheap, with 78 out of 94 identified domains being registered through this service, depicted in **Figure 4** below. Nevertheless, the group showed signs of its past preferences, such as the registration of the *webgateway[.]ru* and *deskactivitygm[.]com* domains through Regway, and *threatcenterofreaserch[.]com* registered via Porkbun, which was previously identified in open sources in Calisto's older campaign and also reappears under the aforementioned newly identified infrastructure.

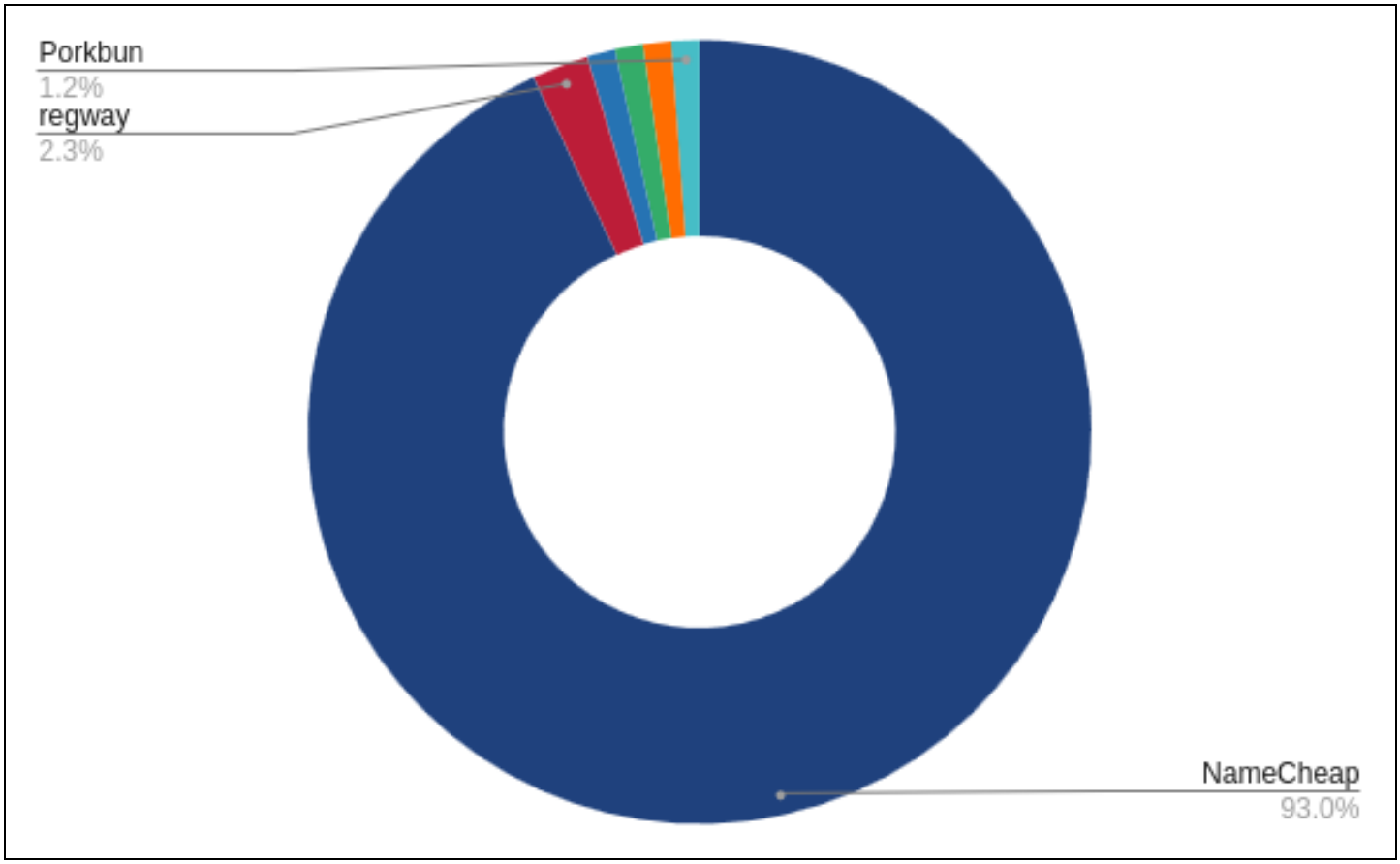


Figure 4: *Breakdown of domain registrars used by BlueCharlie in the current campaign, November 2022 to March 2023 (Source: Recorded Future)*

Autonomous Systems

In our previous reporting, we identified the Autonomous System Numbers (ASNs) where the BlueCharlie IP addresses were most commonly found, shown in **Table 1** below.

ASN	AS Name	BlueCharlie Domain Count
AS52000	MIRhosting	11
AS54290	Hostwinds	10
AS44094	WEBHOST1-AS	4
AS62240	Clouvider	4
AS62005	BV-EU-AS	3
AS44477	STARK-INDUSTRIES	2
AS16276	OVH	1
AS20278	NEXEON	1
AS206446	CLOUDLEASE	1
AS43624	STARK-INDUSTRIES-SOLUTIONS-AS	1

Table 1: *ASN detail breakdown for previous BlueCharlie-linked domains (Source: Recorded Future)*

In our current observations of BlueCharlie ASNs in use, we highlight the reuse of the following:

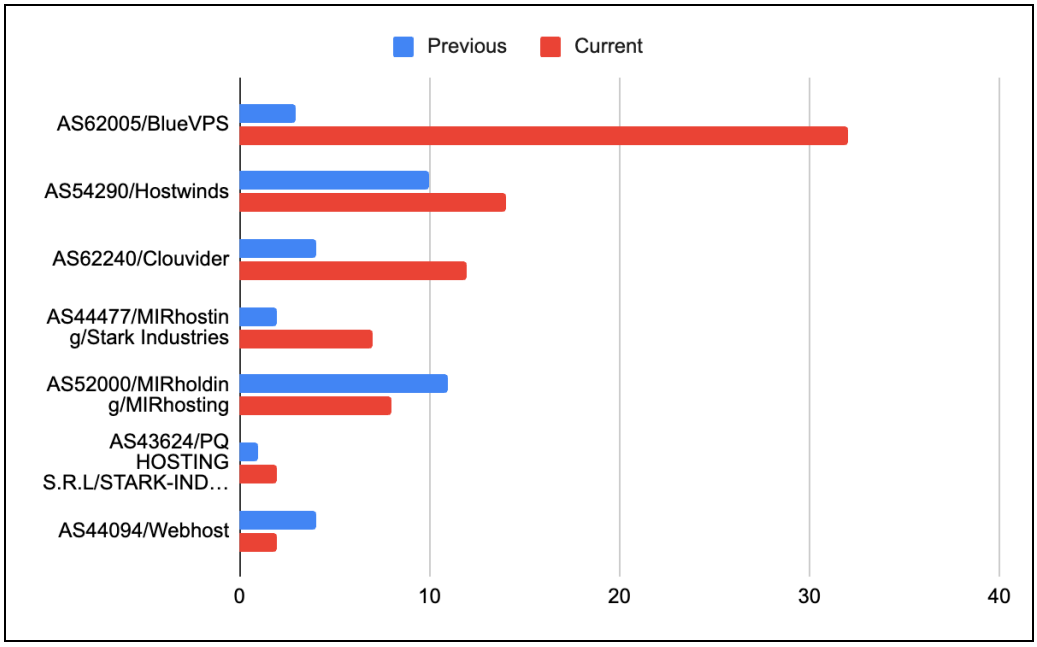


Figure 5: *Breakdown of Autonomous Systems (AS) used by BlueCharlie in the previous and current campaign (Source: Recorded Future)*

Table 2 contains a further breakdown of the most recently observed ASNs in use by BlueCharlie:

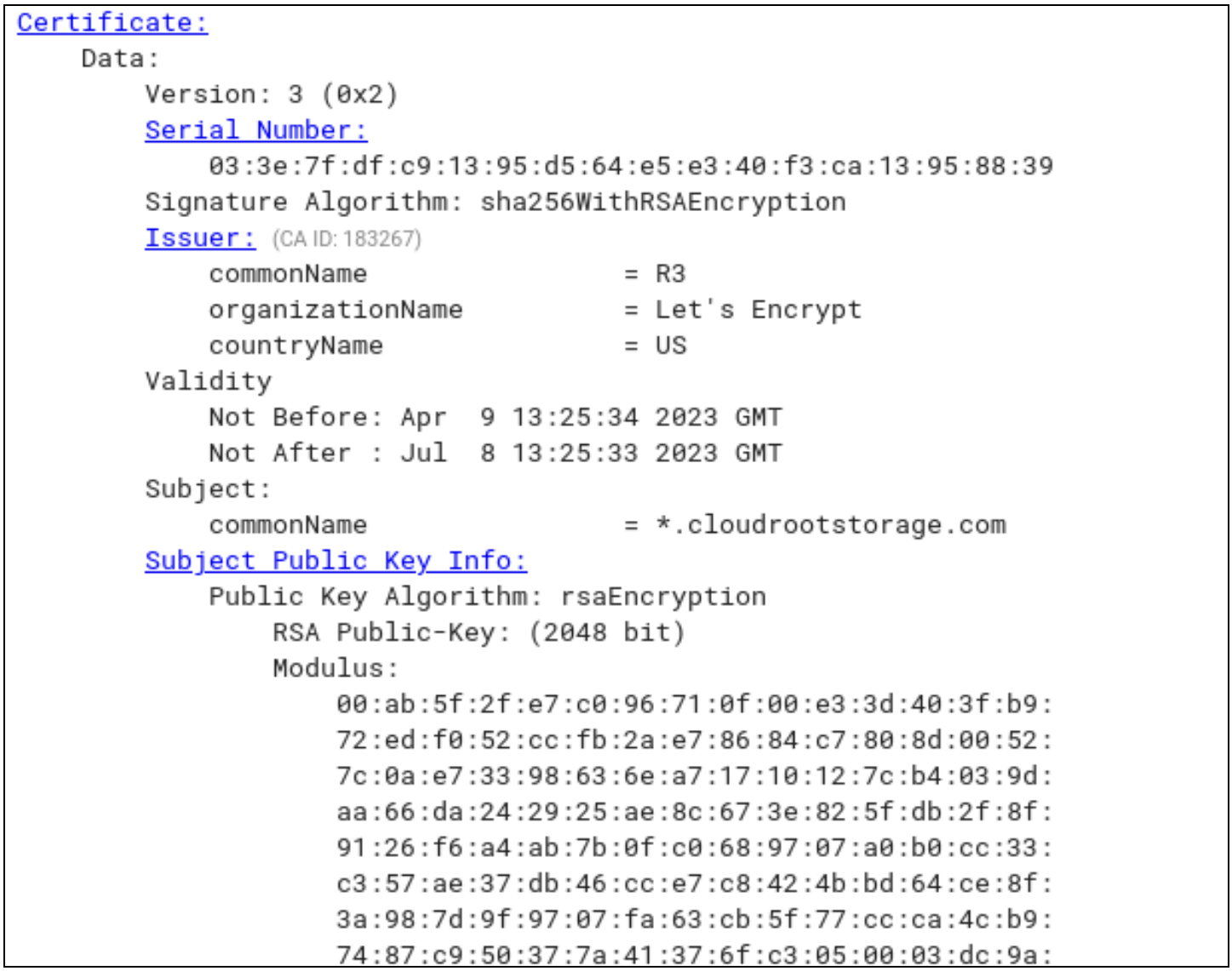
ASN	AS Name	BlueCharlie Domain Count
AS36352	ColoCrossing	35
AS62005	BlueVPS OU	32
AS54290	Hostwinds LLC	14
AS62240	Clouvider	12
AS44477	MIRhosting/Stark Industries	7
AS52000	MIRholding/MIRhosting	8
AS22612	Namecheap	8
AS43624	PQ HOSTING S.R.L.	2
AS44094	Webhost LLC	2
AS49392	LLC Baxet	2
AS62904	Eonix Corporation	2
AS3257	GTT Communications Inc.	1

Table 2: *ASN detail breakdown for current BlueCharlie-linked domains (Source: Recorded Future)*

Additionally, industry reporting suggests that Stark Industries, MIRhosting, and Perfect Quality (PQ) Hosting (all present in the current activity) are related to Ivan Neculiti, a Moldovan national. Cybersecurity firm Team Cymru stated that it frequently observes "all three hosting companies being used to host malicious content, or … used directly for attack infrastructure", specifying that "the website hucksters[.]net, which amongst other things seeks to expose individuals involved in fraud and spam, has previously profiled NECULITI".

X.509 TLS Certificates

Previously, all identified BlueCharlie domains were found to host corresponding X.509 TLS certificates provided by Let's Encrypt. The prevalent use of Let's Encrypt TLS certificates allows for further correlations between BlueCharlie domains and infrastructure, strengthening the clustering of this activity. The group continues to rely almost exclusively on Let's Encrypt security certificates. The only exception to this rule that we identified was the domain *bittechllc[.]net*, which used the ZeroSSL Certificate Authority. The remainder relied on Let's Encrypt certificates. See, for example, the *cloudrootstorage[.]com* domain's certificate as found at crt.sh and depicted in **Figure 6** below.



```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            03:3e:7f:df:c9:13:95:d5:64:e5:e3:40:f3:ca:13:95:88:39
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: (CA ID: 183267)
            commonName                = R3
            organizationName          = Let's Encrypt
            countryName               = US
        Validity
            Not Before: Apr  9 13:25:34 2023 GMT
            Not After : Jul  8 13:25:33 2023 GMT
        Subject:
            commonName                = *.cloudrootstorage.com
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                RSA Public-Key: (2048 bit)
                Modulus:
                    00:ab:5f:2f:e7:c0:96:71:0f:00:e3:3d:40:3f:b9:
                    72:ed:f0:52:cc:fb:2a:e7:86:84:c7:80:8d:00:52:
                    7c:0a:e7:33:98:63:6e:a7:17:10:12:7c:b4:03:9d:
                    aa:66:da:24:29:25:ae:8c:67:3e:82:5f:db:2f:8f:
                    91:26:f6:a4:ab:7b:0f:c0:68:97:07:a0:b0:cc:33:
                    c3:57:ae:37:db:46:cc:e7:c8:42:4b:bd:64:ce:8f:
                    3a:98:7d:9f:97:07:fa:63:cb:5f:77:cc:ca:4c:b9:
                    74:87:c9:50:37:7a:41:37:6f:c3:05:00:03:dc:9a:
```

Figure 6: *Security certificate for the* cloudrootstorage[.]com *domain (Source: crt.sh)*

Mitigations

Phishing and spearphishing from state-sponsored advanced persistent threat (APT) groups presents an imminent threat to organization networks and personal information. Phishing allows a threat actor access to privileged material or the ability to install their own exploit software, such as ransomware or command-and-control software.

- Implement multi-factor authentication (MFA) on all internet-facing web applications and appliances, especially webmail. MFA is something you know (a password) and something you have (a text message or code from a MFA application). This way, if a threat actor has your password, they are likely unable to authenticate as they lack the MFA code.

- Use a FIDO2-compliant MFA token.
- Train employees, contractors, and third-party vendors to protect against phishing, spearphishing, and social engineering. Refreshing employees, vendors, contractors and third-party entities with this phishing training often (at least annually) is critical to prevent credential harvesting and unwanted intrusions to your network.
- Disable all macros, particularly macros loading by default, in Microsoft Office products.
- Ensure that all attachments are scanned for malicious artifacts and behavior.
- Enforce a frequent password reset policy and strong password requirements for all internet-facing web applications and internal applications, especially webmail/email.
- Use a stand-alone password manager (such as BitWarden or 1Password) to generate strong passwords, and use unique passwords for each service. Passwords should not be reused across services/websites.
- Configure your intrusion detection systems (IDS), intrusion prevention systems (IPS), or any network defense mechanisms in place to alert on — and upon review, consider blocking connection attempts to and from — the external IP addresses and domains listed in the appendix.

Outlook

BlueCharlie has demonstrated the ability to adapt and evolve over time to public reporting, and will likely continue to change their TTPs based on past precedent. Given the group's historical use of phishing (which is likely occurring in the new activity), we recommend network defenders employ robust anti-phishing training and highly encourage the use of a FIDO2-compliant multi-factor authentication token, such as a Yubikey. Recorded Future Threat Intelligence (TI), Third-Party Intelligence, and SecOps Intelligence modules users can monitor real-time output from Network Intelligence analytics to identify suspected targeted intrusion activity involving your organization or key vendors and partners.

Appendix A — IOCs

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

About Insikt Group®

Recorded Future's Insikt Group, the company's threat research division, comprises analysts and security researchers with deep government, law enforcement, military, and intelligence agency experience. Their mission is to produce intelligence that reduces risk for clients, enables tangible outcomes, and prevents business disruption.

About Recorded Future®

Recorded Future is the world's largest intelligence company. Recorded Future's cloud-based Intelligence Platform provides the most complete coverage across adversaries, infrastructure, and targets. By combining persistent and pervasive automated data collection and analytics with human analysis, Recorded Future provides real-time visibility into the vast digital landscape and empowers clients to take proactive action to disrupt adversaries and keep their people, systems, and infrastructure safe. Headquartered in Boston with offices and employees around the world, Recorded Future works with more than 1,600 businesses and government organizations across more than 70 countries.