Hive Pro®

Threat Level

Red

✓ CISA:AA23-341A

HiveForce Labs

# THREAT ADVISORY

ACTOR REPORT

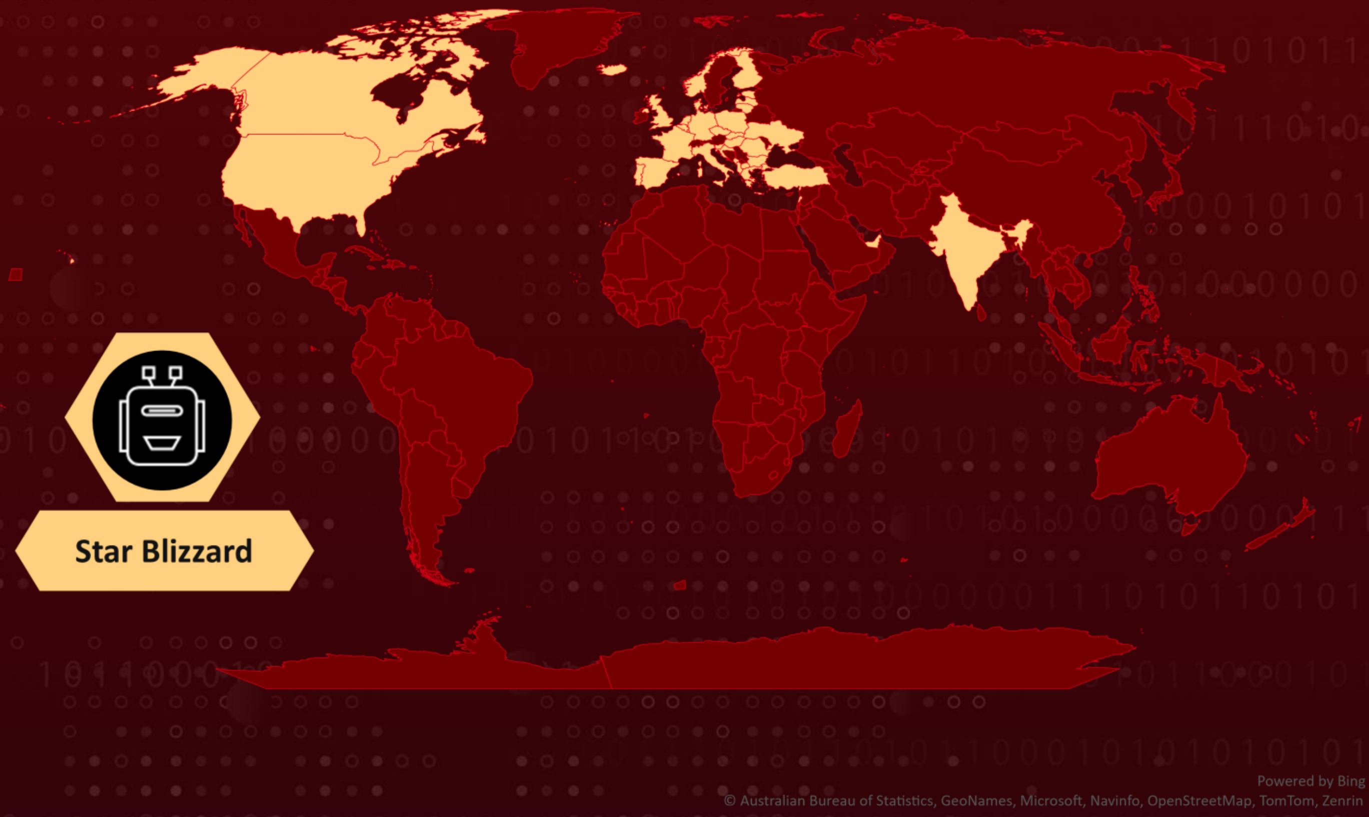
## Star Blizzard Continues to Refine Their Tradecraft for Evasion and Stealth

| Date of Publication | Admiralty code | TA Number |
|---|---|---|
| December 08, 2023 | A1 | TA2023494 |

# Summary

**First Appearance:** 2019
**Actor Name:** Star Blizzard (aka Cold River, Nahr el bared, Nahr Elbard, Cobalt Edgewater, TA446, Seaborgium, TAG-53, BlueCharlie, Blue Callisto,  Calisto)
**Target Industries:**  Academia, Defense, Governmental Organizations, NGOs, Think Tanks and Politicians
**Target Region:** Canada, India, Lebanon, UAE, Ukraine, USA, NATO, UK

## Actor Map


Star Blizzard
Powered by Bing
© Australian Bureau of Statistics, GeoNames, Microsoft, Navinfo, OpenStreetMap, TomTom, Zenrin

# Actor Details

#1 The Russia-based threat actor Star Blizzard persists in employing spear-phishing attacks to successfully target organizations and individuals across different geographical regions, primarily for information-gathering activities. Notably, Star Blizzard has enhanced its capabilities to evade detection since 2022, all while maintaining a focus on email credential theft against the same set of targets.

#2 Star Blizzard uses spear-phishing tactics to target individuals or groups by creating email accounts impersonating known contacts, create fake social media profiles, often impersonating respected experts, and include invitations to conferences or events, adding another layer of deceptive techniques.

#3 Star Blizzard employs various email providers to conduct phishing attacks, disseminating links to websites or documents. After building trust, the target is directed to a server controlled by the actor, where they are prompted to input their account credentials. The malicious link may be embedded in emails or shared through file-sharing platforms. Star Blizzard utilizes EvilGinx to extract credentials and session cookies, allowing them to bypass two-factor authentication.

#4 Star Blizzard has adopted new evasive techniques, include the implementation of server-side scripts to thwart automated scanning of actor-controlled infrastructure, leveraging email marketing platform services to conceal the actual email sender addresses, using DNS providers to obscure the IP addresses of actor-controlled VPS infrastructure, employing password-protected PDF lures or links to cloud-based file-sharing platforms, and transitioning to a more randomized domain generation algorithm for actor-registered domains.

#5 These implemented measures are crafted to improve evasion capabilities and fortify defenses against actor-controlled domains. Spear-phishing, a well-established technique employed by numerous threat actors, remains a potent tool, with Star Blizzard demonstrating ongoing success by evolving and adapting this technique.

## Actor Group

| NAME | ORIGIN | TARGET REGIONS | TARGET INDUSTRIES |
|---|---|---|---|
| Star Blizzard (aka Cold River, Nahr el bared, Nahr Elbard, Cobalt Edgewater, TA446, Seaborgium, TAG-53, BlueCharlie, Blue Callisto, Calisto) | Russia | Canada, India, Lebanon, UAE, Ukraine, USA, NATO, UK | Academia, Defense, Governmental Organizations, NGOs, Think Tanks and Politicians |
| | MOTIVE | | |
| | Information theft and espionage | | |

# Recommendations

**Remain vigilant:** Be wary of clicking on suspicious links or visiting untrusted websites, as they may contain malicious content. Exercise caution when opening emails or messages from unknown sources, as they could be part of phishing attempts.

**Exercise caution when dealing with email attachments:** Avoid downloading attachments from unsolicited or suspicious emails. Be cautious when opening archive files from unknown sources, as they could contain malware.

**Email Security Measures**: Employ robust email security solutions to detect and block malicious attachments and links. Consider using advanced threat protection (ATP) and email filtering technologies to sandbox suspicious or untrusted URLs.

## Potential MITRE ATT&CK TTPs

| | | | |
|---|---|---|---|
| TA0043<br>Reconnaissance | TA0042<br>Resource Development | TA0001<br>Initial Access | TA0005<br>Defense Evasion |
| TA0006<br>Credential Access | TA0009<br>Collection | T1593<br>Search Open Websites/Domains | T1078<br>Valid Accounts |
| T1585<br>Establish Accounts | T1585.001<br>Social Media Accounts | T1585.002<br>Email Accounts | T1583<br>Acquire Infrastructure |
| T1583.001<br>Domains | T1586<br>Compromise Accounts | T1586.002<br>Email Accounts | T1566<br>Phishing |
| T1566.001<br>Spearphishing Attachment | T1566.002<br>Spearphishing Link | T1550<br>Use Alternate Authentication Material | T1550.004<br>Web Session Cookie |
| T1539<br>Steal Web Session Cookie | T1114<br>Email Collection | T1114.002<br>Remote Email Collection | T1114.003<br>Email Forwarding Rule |

## Indicator of Compromise (IOCs)

| TYPE | VALUE |
|---|---|
| Domains | centralitdef[.]com,<br>rootgatewayshome[.]com,<br>directstoragepro[.]com,<br>infocryptoweb[.]com,<br>cloudwebstorage[.]com,<br>cryptdatahub[.]com, |

| TYPE | VALUE |
|---|---|
| Domains | datainfosecure[.]com,<br>servershieldme[.]com,<br>scandefinform[.]com,<br>guardittech[.]com,<br>storageinfohub[.]com,<br>docsinfohub[.]com,<br>dbasechecker[.]com,<br>dbasecheck[.]com,<br>gaterecord[.]com,<br>directsgate[.]com,<br>storageinformationsolutions[.]com,<br>storagedatadirect[.]com,<br>informationdoorwaycertificate[.]com,<br>datagatewaydoc[.]com,<br>panelittechweb[.]com,<br>panelitsolution[.]com,<br>keeperdocument[.]com,<br>keeperdocumentgatewayhub[.]com,<br>docview[.]cloud,<br>protectitbase[.]com,<br>webcatalogpro[.]com,<br>infoformdata[.]com,<br>keydatastorageunit[.]com,<br>docanalizergate[.]com,<br>docanalizerhub[.]com,<br>hubdatapage[.]com,<br>skyinformdata[.]com,<br>docsaccessdata[.]com,<br>datacryptosafe[.]com,<br>cloudsetupprofi[.]com,<br>setupprofi[.]com,<br>analyzedatainfo[.]com,<br>infocryptodata[.]com,<br>datadocsview[.]com,<br>gatedocsview[.]com,<br>hubinfodocs[.]com,<br>proffsolution[.]com,<br>proffitsolution[.]com,<br>defproresults[.]com,<br>greatnotifyinfo[.]com,<br>topnotifydata[.]com,<br>topinformdata[.]com,<br>defoffresult[.]com,<br>cloudinfodata[.]com,<br>webpartdata[.]com,<br>infostoragegate[.]com, |

| TYPE | VALUE |
|---|---|
| Domains | wardenstoragedoorway[.]com,<br>myposcheck[.]com,<br>poscheckdatacenter[.]com,<br>checkdatapos[.]com,<br>docdatares[.]com,<br>datawebhub[.]com,<br>cloudithub[.]com,<br>secitweb[.]com,<br>documentitsolution[.]com,<br>keeperinformation[.]com,<br>webprodata[.]com,<br>clouditprofi[.]com,<br>cryptoinfostorage[.]com,<br>rootinformationgateway[.]com,<br>gatewaydocumentdata[.]com,<br>gatewayitservices[.]com,<br>infoviewerdata[.]com,<br>infoviewergate[.]com,<br>webitresourse[.]com,<br>homedocsdata[.]com,<br>homedocsview[.]com,<br>webdataproceed[.]com,<br>directkeeperstorage[.]com,<br>gatewaykeeperinformation[.]com,<br>rootgatestorage[.]com,<br>documentinformationsolution[.]com,<br>getclouddoc[.]com,<br>statusfiles[.]com,<br>webstaticdata[.]com,<br>cloudwebfile[.]com,<br>statuswebcert[.]com,<br>nextgenexp[.]com,<br>informationkeeper[.]com,<br>documentgatekeeper[.]com,<br>cryptogatesolution[.]com,<br>rootgatewaystorage[.]com,<br>infoviewstorage[.]com,<br>infoconnectstorage[.]com,<br>infolookstorage[.]com,<br>judicialliquidators[.]com,<br>safetyagencyservice[.]com,<br>dynamiclnk[.]com,<br>temphoster[.]com,<br>documententranceintelligence[.]com,<br>documentgateprotector[.]com,<br>readinfodata[.]com, |

| TYPE | VALUE |
|---|---|
| Domains | readdatainform[.]com,<br>webcryptoinfo[.]com,<br>storageinfodata[.]com,<br>keeperdatastorage[.]com,<br>keepinformationroot[.]com,<br>keyservicebar[.]com,<br>bitespacedev[.]com,<br>cryptodocumentinformation[.]com,<br>directdocumentinfo[.]com,<br>techpenopen[.]com,<br>loginformationbreakthrough[.]com,<br>alldocssolution[.]com,<br>documentkeepersolutionsystems[.]com,<br>docholdersolution[.]com,<br>infodocitsolution[.]com,<br>securebrowssolution[.]com,<br>secbrowsingate[.]com,<br>secbrowsingsystems[.]com,<br>docguardmaterial[.]com,<br>dockeeperweb[.]com,<br>docsecgate[.]com,<br>documentsecsolution[.]com,<br>cryptogatehomes[.]com,<br>topcryptoprotect[.]com,<br>safedocumentgatesolution[.]com,<br>safedocitsolution[.]com,<br>docscontentview[.]com,<br>docscontentgate[.]com,<br>openprojectgate[.]com,<br>infowardendoc[.]com,<br>wardensecbreakthrough[.]com,<br>lawsystemjudgement[.]com,<br>explorewebdata[.]com,<br>doorwayseclaw[.]com,<br>entryloginpoint[.]com,<br>wardenlawsec[.]com,<br>entrygatebreak[.]com,<br>digitalworkdata[.]com,<br>digitalhubdata[.]com,<br>craftfilelink[.]com,<br>createtempdoc[.]com,<br>provideexplorer[.]com,<br>reviewopenfile[.]com,<br>govsafebreakthrough[.]com,<br>govlawentrance[.]com,<br>storagekeepdirect[.]com, |

| TYPE | VALUE |
|---|---|
| Domains | storageguarddirect[.]com,<br>storagekeeperexpress[.]com,<br>onestorageprotectordirect[.]com,<br>lawwardensafety[.]com,<br>entrancequick[.]com,<br>seclawdoorway[.]com,<br>wardengovermentlaw[.]com,<br>getvaluepast[.]com,<br>transferlinkdata[.]com,<br>remcemson[.]com,<br>osixmals[.]com,<br>entranceto[.]com,<br>govermentsecintro[.]com,<br>itbugreportbeta[.]com,<br>theitbugreportbeta[.]com,<br>sockintrodoorway[.]com,<br>maxintrosec[.]com,<br>doorgovcommunity[.]com,<br>tarentrycommunity[.]com,<br>webfigmadesignershop[.]com,<br>webfigmadesigner[.]com,<br>logincontrolway[.]com,<br>vertransmitcontrol[.]com,<br>everyinit[.]com,<br>aliceplants[.]com,<br>countingtall[.]com,<br>silenceprotocol[.]com,<br>mintwithapples[.]com,<br>winterholds[.]com,<br>ziplinetransfer[.]com,<br>translatesplit[.]com,<br>getfigmacreator[.]com,<br>postrequestin[.]com,<br>tarifjane[.]com,<br>configlayers[.]com,<br>winterhascometo[.]com,<br>inyourheadexp[.]com,<br>glorybuses[.]com,<br>janeairintroduction[.]com,<br>vikingonairplane[.]com,<br>marungame[.]com,<br>victorinwounder[.]com,<br>paneindestination[.]com,<br>trastamarafamily[.]com,<br>territoryedit[.]com,<br>vectorto[.]com, |

| TYPE | VALUE |
|---|---|
| Domains | johnysadventure[.]com,<br>paternenabler[.]com,<br>fastnamegenerator[.]com,<br>literallyandme[.]com,<br>andysalesproject[.]com,<br>pandawithrainbow[.]com,<br>natalyincity[.]com,<br>machinerelise[.]com,<br>industrialcorptruncate[.]com,<br>constructionholdingnewlife[.]com,<br>adventuresrebornpanda[.]com,<br>cryingpand[.]com,<br>industrialwatership[.]com,<br>olohaisland[.]com,<br>voodoomagician[.]com,<br>newestchairs[.]com,<br>cpuisocutter[.]com,<br>incorpcpu[.]com,<br>gulperfish[.]com,<br>leviathanfish[.]com,<br>truncationcorp[.]com,<br>gzipinteraction[.]com,<br>ghostshowing[.]com,<br>hallowenwitch[.]com,<br>certificatentrance[.]com,<br>apiwebdata[.]com,<br>apidatahook[.]com,<br>apireflection[.]com,<br>protectionoffice[.]tech,<br>lazyprotype[.]com,<br>angelicfish[.]com,<br>globalyfish[.]com,<br>medicprognosis[.]com,<br>medicoutpatient[.]com,<br>krakfish[.]com,<br>stingrayfish[.]com,<br>incorpreview[.]com,<br>truncatetrim[.]com,<br>corporatesinvitation[.]com,<br>triminget[.]com,<br>firewitches[.]com,<br>solartemplar[.]com,<br>encryptionrenewal[.]com,<br>sslkeycert[.]com,<br>barbarictruths[.]com,<br>castlefranks[.]com,<br>comintroduction[.]com,<br>corpviewer[.]com |

# References

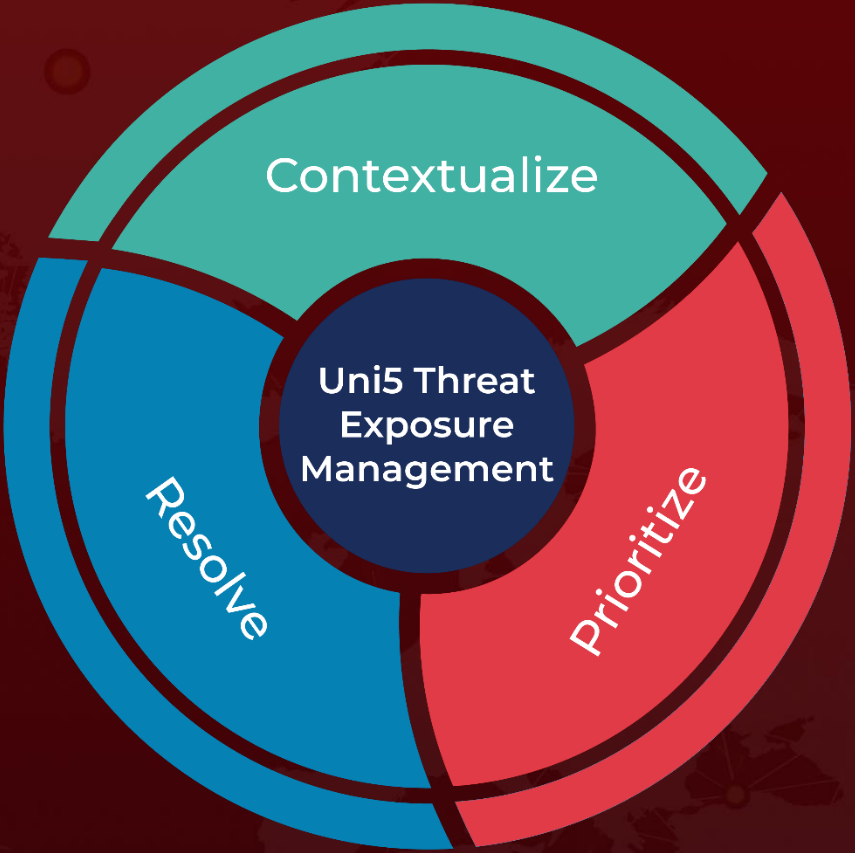
https://www.microsoft.com/en-us/security/blog/2023/12/07/star-blizzard-increases-sophistication-and-evasion-in-ongoing-attacks/

https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-341a

# What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with **HivePro Uni5**: Threat Exposure Management Platform.



REPORT GENERATED ON

**December 08, 2023 • 4:10 AM**

More at www.hivepro.com