Russian FSB cyber actor Star Blizzard continues worldwide spear-phishing campaigns

The Russia-based actor is targeting organisations and individuals in the UK and other geographical areas of interest.

Overview

The Russia-based actor Star Blizzard (formerly known as SEABORGIUM, also known as Callisto Group/TA446/COLDRIVER/TAG-53/BlueCharlie) continues to successfully use spear-phishing attacks against targeted organisations and individuals in the UK, and other geographical areas of interest, for information-gathering activity.

The UK National Cyber Security Centre (NCSC), the US Cybersecurity and Infrastructure Security Agency (CISA), the US Federal Bureau of Investigation (FBI), the US National Security Agency (NSA), the US Cyber National Mission Force (CNMF), the Australian Signals Directorate's Australian Cyber Security Centre (ASD's ACSC), the Canadian Centre for Cyber Security (CCCS), and the New Zealand National Cyber Security Centre (NCSC-NZ) assess that Star Blizzard is almost certainly subordinate to the Russian Federal Security Service (FSB) Centre 18.

Industry has previously published details of Star Blizzard. This advisory draws on that body of information.

This advisory raises awareness of the spear-phishing techniques Star Blizzard uses to target individuals and organisations. This activity is continuing through 2023.

Targeting profile

Since 2019, Star Blizzard has targeted sectors including academia, defence, governmental organisations, NGOs, think tanks and politicians.

Targets in the UK and US appear to have been most affected by Star Blizzard activity, however activity has also been observed against targets in other NATO countries, and countries neighbouring Russia.

During 2022, Star Blizzard activity appeared to expand further, to include defence-industrial targets, as well as US Department of Energy facilities.

Outline of the attacks

The activity is typical of spear-phishing campaigns, where an actor targets a specific individual or group, using information known to be of interest to the targets. In a spear-phishing campaign, an actor perceives their target to have direct access to information of interest, be an access vector to another target, or both.

Research and preparation

Using open-source resources to conduct reconnaissance, including social media and professional networking platforms, Star Blizzard identifies hooks to engage their target. They take the time to research their interests and identify their real-world social or professional contacts. [T1589; T1593]

Star Blizzard creates email accounts impersonating known contacts of their targets to help appear legitimate. They also create fake social media or networking profiles that impersonate respected experts [T1585.001] and have used supposed conference or event invitations as lures.

Star Blizzard uses webmail addresses from different providers, including Outlook, Gmail, Yahoo and Proton mail in their initial approach [T1585.002], impersonating known contacts of the target or well-known names in the target's field of interest or sector.

To appear authentic, the actor also creates malicious domains resembling legitimate organisations [T1583.001].

Microsoft Threat Intelligence Center (MSTIC) provides a list of observed Indicators of Compromise (IOCs) in their SEABORGIUM blog, but this is not exhaustive.

Preference for personal email addresses

Star Blizzard has predominantly sent spear-phishing emails to targets' personal email addresses, although they have also used targets' corporate or business email addresses. The actors may intentionally use personal emails to circumvent security controls in place on corporate networks.

Building a rapport

Having taken the time to research their targets' interests and contacts to create a believable approach, Star Blizzard now starts to build trust. They often begin by establishing benign contact on a topic they hope will engage their targets. There is often some correspondence between attacker and target, sometimes over an extended period, as the attacker builds rapport.

Delivery of malicious link

Once trust is established, the attacker uses typical phishing tradecraft and shares a link [T1566.002], apparently to a document or website of interest. This leads the target to an actor-controlled server, prompting the target to enter account credentials.

The malicious link may be a URL in an email message, or the actor may embed a link in a document [T1566.001] on OneDrive, Google Drive, or other file-sharing platforms.

Star Blizzard uses the open-source framework EvilGinx in their spear-phishing activity, which allows them to harvest credentials and session cookies to successfully bypass the use of two-factor authentication [T1539; T1550.004].

Exploitation and further activity

Whichever delivery method is used, once the target clicks on the malicious URL, they are directed to an actor-controlled server that mirrors the sign-in page for a

legitimate service. Any credentials entered at this point are now compromised.

Star Blizzard then uses the stolen credentials to log in to a target's email account [T1078], where they are known to access and steal emails and attachments from the victim's inbox [T1114.002]. They have also set up mail-forwarding rules, giving them ongoing visibility of victim correspondence [T1114.003].

The actor has also used their access to a victim email account to access mailing-list data and a victim's contacts list, which they then use for follow-on targeting. They have also used compromised email accounts for further phishing activity [T1586.002].

Conclusion

Spear-phishing is an established technique used by many actors, and Star Blizzard uses it successfully, evolving the technique to maintain their success.

Individuals and organisations from previously targeted sectors should be vigilant of the techniques described in this advisory.

In the UK you can report related suspicious activity to the NCSC.

Information on effective defence against spear-phishing is included in the 'Mitigation' section below.

MITRE ATT&CK ®

Tactic	Technique	ID	Procedure
Reconnaissance	Search Open Websites/Domains	T1593	Star Blizzard uses open-source research and social media to identify information about victims to use in targeting.
Reconnaissance	Gather Victim Identity Information	T1589	Star Blizzard uses online data sets and open-source resources to gather information about their targets.
Resource Development	Establish Accounts: Social Media Accounts	T1585.001	Star Blizzard has been observed establishing fraudulent profiles on professional networking sites to conduct reconnaissance.
Resource Development	Establish Accounts: Email Accounts	T1585.002	Star Blizzard registers consumer email accounts matching the names of individuals they are impersonating to conduct spear-phishing activity.
Resource Development	Acquire Infrastructure: Domains	T1583.001	Star Blizzard registers domains to host their phishing framework.
Resource Development	Compromise Accounts: Email Accounts	T1586.002	Star Blizzard has been observed using compromised victim email accounts to conduct spear-phishing activity against contacts of the original victim.
Initial Access	Valid Accounts	T1078	Star Blizzard uses compromised credentials, captured from fake log-in pages, to log in to valid victim user accounts.
Initial Access	Phishing: Spear-phishing Attachment	T1566.001	Star Blizzard uses malicious links embedded inemail attachments to direct victims to their credential-stealing sites.
Initial Access	Phishing: Spear-phishing Link	T1566.002	Star Blizzard sends spear-phishing emails with malicious links directly to credential-stealing sites, or to documents hosted on a file- sharing site, which then direct victims to credential-stealing sites.

Defence Evasion	Use Alternate Authentication Material: Web Session Cookie	T1550.004	Star Blizzard bypasses multi-factor authentication on victim email accounts by using session cookies stolen using EvilGinx.
Credential Access	Steal Web Session Cookie	T1539	Star Blizzard uses EvilGinx to steal the session cookies of victims directed to their fake log-in domains.
Collection	Email Collection: Remote Email Collection	T1114.002	Star Blizzard interacts directly with externally facing Exchange services, Office 365 and Google Workspace to access email and steal information using compromised credentials or access tokens.
Collection	Email Collection: Email Forwarding Rule	T1114.003	Star Blizzard abuse email-forwarding rules to monitor the activities of a victim, steal information, and maintain persistent access to victim's emails, even after compromised credentials are reset.

Mitigation

A number of mitigations will be useful in defending against the activity described in this advisory.

- **Use strong passwords**
  Use a separate password for email accounts and avoid password re-use across multiple services.
  See NCSC guidance: Top tips for staying secure online: Use a strong and separate password for your email
- **Use multi-factor authentication (MFA) to reduce the impact of password compromises**
  Also known as 2-factor authentication (2FA), 2 step verification (2SV) or two-step authentication

See NCSC guidance: Multi-factor authentication for online services and Setting up 2-Step Verification (2SV)

- **Protect your devices and networks by keeping them up to date**
  Use the latest supported versions, apply security updates promptly, use antivirus and scan regularly to guard against known malware threats
  See NCSC guidance: Device Security Guidance: Antivirus and other security software

- **Exercise vigilance. Spear-phishing emails are tailored to avoid suspicion**
  You may recognise the sender's name, but has the email come from an address that you recognise? Would you expect contact from this person's webmail address rather than their corporate email address? Has the suspicious email come to your personal/webmail address, rather than your corporate one? Can you verify that the email is legitimate via another means?
  See NCSC guidance: Phishing attacks: defending your organisation and the FBI Internet Crime Complaint Center (IC3): Current Industry Alerts

- **Enable your email providers' automated email scanning features**
  These are turned on by default for consumer mail providers.
  See NCSC blog post: Telling users to 'avoid clicking bad links' still isn't working

- **Disable mail-forwarding**
  Attackers have been observed to set up mail-forwarding rules to maintain visibility of target emails. If you cannot disable mail-forwarding, then monitor settings regularly to ensure that a forwarding rule has not been set up by an external malicious actor.

PUBLISHED

7 December 2023

WRITTEN FOR

Large organisations

Cyber security professionals

Public sector

NEWS TYPE

Alert