

New Star Blizzard spear-phishing campaign targets WhatsApp accounts

microsoft.com/en-us/security/blog/2025/01/16/new-star-blizzard-spear-phishing-campaign-targets-whatsapp-accounts/

January 16, 2025



[Skip to main content](#)



By

In mid-November 2024, Microsoft Threat Intelligence observed the Russian threat actor we track as Star Blizzard sending their typical targets spear-phishing messages, this time offering the supposed opportunity to join a WhatsApp group. This is the first time we have identified a shift in Star Blizzard's longstanding tactics, techniques, and procedures (TTPs) to leverage a new access vector. Star Blizzard's targets are most commonly related to government or diplomacy (both incumbent and former position holders), defense policy or international relations researchers whose work touches on Russia, and sources of assistance to Ukraine related to the war with Russia.

In our last blog post about [Star Blizzard](#), we discussed how the threat actor targeted dozens of civil society organizations—journalists, think tanks, and non-governmental organizations (NGOs)—between January 2023 and August 2024 by deploying spear-phishing campaigns to exfiltrate sensitive information and interfere in their activities. Since October 3, 2024, Microsoft and the US Department of Justice have seized or taken down more than 180 websites related to that activity. While this coordinated action had a short-term impact on Star Blizzard's phishing operations, we noted at the time that after this threat actor's active infrastructure was exposed, they swiftly transitioned to new domains to continue their operations, indicating that the threat actor is highly resilient to operational disruptions.

We assess the threat actor's shift to compromising WhatsApp accounts is likely in response to the exposure of their TTPs by Microsoft Threat Intelligence and other organizations, including national cybersecurity agencies. While this campaign appears to have wound down at the end of November, we are highlighting the new shift as a sign that the threat actor could be seeking to change its TTPs in order to evade detection.

As part of our continuous monitoring, analysis, and reporting on the threat landscape, we are sharing our information on Star Blizzard's latest activity to raise awareness of this threat actor's shift in tradecraft and to educate organizations on how to harden their attack surfaces against this and similar activity. We also directly notify customers who have been targeted or compromised, providing them with the necessary information to help secure their environments.

Targeting WhatsApp account data

Star Blizzard's new spear-phishing campaign, while novel in that it uses and targets WhatsApp for the first time, exhibits familiar spear-phishing TTPs for Star Blizzard, with the threat actor initiating email contact with their targets, to engage them, before sending them a second message containing a malicious link. The sender address used by the threat actor in this campaign impersonates a US government official, continuing Star Blizzard's practice of impersonating known political/diplomatic figures, to further ensure target engagement. The

initial email sent to targets contains a quick response (QR) code purporting to direct users to join a WhatsApp group on “the latest non-governmental initiatives aimed at supporting Ukraine NGOs.” This code, however, is intentionally broken and will not direct the user towards any valid domain; this is an effort to coax the target recipient into responding.

Dear [REDACTED]

I hope this message finds you well.

We have established a private WhatsApp group to facilitate discussions regarding the latest non-governmental initiatives aimed at supporting Ukraine. This platform will also serve as a means to coordinate the distribution of government-allocated funds for this purpose.

You can join us using this QR code below:

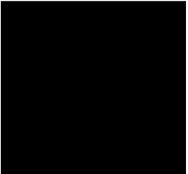


Figure 1. Star Blizzard initial spear-phishing email with broken QR code

When the recipient responds, Star Blizzard sends a second email containing a Safe Links-wrapped [t\[.\]ly](#) shortened link as the alternative link to join the WhatsApp group.

[REDACTED]

I apologize for the inconvenience with the QR code. Kindly try this alternative link:
[US-Ukraine NGOs Group](#)

It should work without any issues.

Figure 2. Star Blizzard follow-on spear-phishing email with URL link

When this link is followed, the target is redirected to a webpage asking them to scan a QR code to join the group. However, this QR code is actually used by WhatsApp to connect an account to a linked device and/or the WhatsApp Web portal. This means that if the target follows the instructions on this page, the threat actor can gain access to the messages in their WhatsApp account and have the capability to exfiltrate this data using existing browser plugins, which are designed for exporting WhatsApp messages from an account accessed via WhatsApp Web.

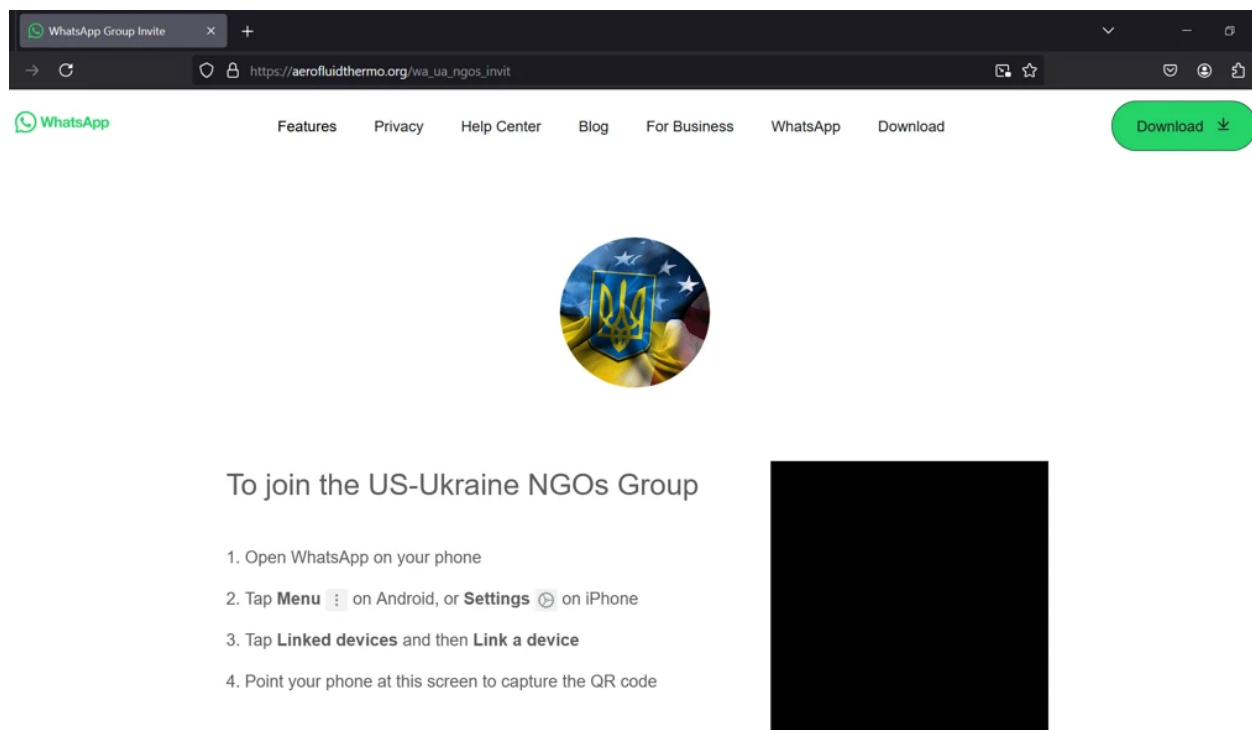


Figure 3. Malicious Star Blizzard phishing attempt using WhatsApp linking QR code

While this campaign was limited and appeared to have terminated at the end of November, it nevertheless marked a break in long-standing Star Blizzard TTPs and highlighted the threat actor's tenacity in continuing spear-phishing campaigns to gain access to sensitive information even in the face of repeated degradations of their operations.

Microsoft Threat Intelligence recommends that all email users belonging to sectors that Star Blizzard typically targets always remain vigilant when dealing with email, especially emails containing links to external resources. These targets are most commonly related to:

- Government or diplomacy (incumbent and former position holders)
- Research into defense policy or international relations when related to Russia
- Assistance to Ukraine related to the ongoing conflict with Russia

When in doubt, contact the person you think is sending the email using a known and previously used email address to verify that the email was indeed sent by them.

Mitigations

To harden networks against the Star Blizzard activity listed above, defenders can implement the following:

- Implement Microsoft Defender for Endpoint on Android and iOS, which includes anti-phishing capabilities that also apply to QR code phishing attacks, blocking phishing sites from being accessed.
- Enable network protection in Microsoft Defender for Endpoint

- Ensure that tamper protection is enabled in Microsoft Defender for Endpoint
- Run endpoint detection and response in block mode so that Microsoft Defender for Endpoint can block malicious artifacts, even when your non-Microsoft antivirus does not detect the threat or when Microsoft Defender Antivirus is running in passive mode.
- Configure investigation and remediation in full automated mode to let Microsoft Defender for Endpoint take immediate action on alerts to resolve breaches, significantly reducing alert volume.
- Turn on PUA protection in block mode in Microsoft Defender Antivirus
- Turn on cloud-delivered protection in Microsoft Defender Antivirus or the equivalent for your antivirus product to cover rapidly evolving attacker tools and techniques.
- Turn on Microsoft Defender Antivirus real-time protection.
- Encourage users to use Microsoft Edge and other web browsers that support SmartScreen, which identifies and blocks malicious websites, including phishing sites, scam sites, and sites that host malware.
- Turn on Safe Links and Safe Attachments for Office 365.
- Use the Attack Simulator in Microsoft Defender for Office 365 to run realistic, yet safe, simulated phishing and password attack campaigns. Utilize the QR code payload in attack simulation training scenarios to mirror Star Blizzard's and other threat actor's QR code spear-phishing techniques.

Microsoft Defender XDR detections

Microsoft Defender XDR customers can refer to the list of applicable detections below. Microsoft Defender XDR coordinates detection, prevention, investigation, and response across endpoints, identities, email, apps to provide integrated protection against attacks like the threat discussed in this blog.

Customers with provisioned access can also use Microsoft Security Copilot in Microsoft Defender to investigate and respond to incidents, hunt for threats, and protect their organization with relevant threat intelligence.

Microsoft Defender for Endpoint

The following alerts might indicate threat activity associated with this threat. These alerts, however, can be triggered by unrelated threat activity and are not monitored in the status cards provided with this report.

Star Blizzard activity group

Hunting queries

Microsoft Defender XDR

Surface events that may have communicated with the Star Blizzard C2s.

```

let domainList = dynamic(["civilstructgeo.org", "aerofluidthermo.org"]);
union
(
    DnsEvents
    | where QueryType has_any(domainList) or Name has_any(domainList)
    | project TimeGenerated, Domain = QueryType, SourceTable = "DnsEvents"
),
(
    IdentityQueryEvents
    | where QueryTarget has_any(domainList)
    | project Timestamp, Domain = QueryTarget, SourceTable = "IdentityQueryEvents"
),
(
    DeviceNetworkEvents
    | where RemoteUrl has_any(domainList)
    | project Timestamp, Domain = RemoteUrl, SourceTable = "DeviceNetworkEvents"
),
(
    DeviceNetworkInfo
    | extend DnsAddresses = parse_json(DnsAddresses), ConnectedNetworks =
parse_json(ConnectedNetworks)
    | mv-expand DnsAddresses, ConnectedNetworks
    | where DnsAddresses has_any(domainList) or ConnectedNetworks.Name
has_any(domainList)
    | project Timestamp, Domain = coalesce(DnsAddresses, ConnectedNetworks.Name),
SourceTable = "DeviceNetworkInfo"
),
(
    VMConnection
    | extend RemoteDnsQuestions = parse_json(RemoteDnsQuestions),
RemoteDnsCanonicalNames = parse_json(RemoteDnsCanonicalNames)
    | mv-expand RemoteDnsQuestions, RemoteDnsCanonicalNames
    | where RemoteDnsQuestions has_any(domainList) or RemoteDnsCanonicalNames
has_any(domainList)
    | project TimeGenerated, Domain = coalesce(RemoteDnsQuestions,
RemoteDnsCanonicalNames), SourceTable = "VMConnection"
),
(
    W3CIISLog
    | where csHost has_any(domainList) or csReferer has_any(domainList)
    | project TimeGenerated, Domain = coalesce(csHost, csReferer), SourceTable =
"W3CIISLog"
),
(
    EmailUrlInfo
    | where UrlDomain has_any(domainList)
    | project Timestamp, Domain = UrlDomain, SourceTable = "EmailUrlInfo"
),
(
    UrlClickEvents
    | where Url has_any(domainList)
    | project Timestamp, Domain = Url, SourceTable = "UrlClickEvents"
)

```

)
| order by TimeGenerated desc

Microsoft Sentinel

Microsoft Sentinel customers can use the TI Mapping analytics (a series of analytics all prefixed with 'TI map') to automatically match the malicious domain indicators mentioned in this blog post with data in their workspace. If the TI Map analytics are not currently deployed, customers can install the Threat Intelligence solution from the [Microsoft Sentinel Content Hub](#) to have the analytics rule deployed in their Sentinel workspace.

While the below queries are not linked to any specific threat actor, they are effective in detecting potential phishing attempts. Implementing these queries can help you stay vigilant and safeguard your organization from phishing attacks

- [Delivered Bad Emails from Top bad IPv4 addresses](#)
- [Phishing Link Execution Observed](#)
- [Successful Signin from Phishing Link](#)
- [Suspicious URL Clicked](#)
- [Email Delivered to Inbox](#)

Microsoft Security Copilot

Security Copilot customers can use the standalone experience to [create their own prompts](#) or run the following [pre-built promptbooks](#) to automate incident response or investigation tasks related to this threat:

- Incident investigation
- Microsoft User analysis
- Threat actor profile
- Threat Intelligence 360 report based on MDTI article

Note that some promptbooks require access to plugins for Microsoft products such as Microsoft Defender XDR or Microsoft Sentinel.

Threat intelligence reports

Microsoft customers can use the following reports in Microsoft products to get the most up-to-date information about the threat actor, malicious activity, and techniques discussed in this blog. These reports provide the intelligence, protection information, and recommended actions to prevent, mitigate, or respond to associated threats found in customer environments.

Microsoft Defender Threat Intelligence

Microsoft Security Copilot customers can also use the [Microsoft Security Copilot integration](#) in Microsoft Defender Threat Intelligence, either in the Security Copilot standalone portal or in the [embedded experience](#) in the Microsoft Defender portal to get more information about this threat actor.

Indicators of compromise

| Indicator | Type | Last seen |
|-----------------------|--------|--------------|
| civilstructgeo[.]org | Domain | October 2024 |
| aerofluidthermo[.]org | Domain | October 2024 |

References

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

Learn more

For further information on the threats detailed in this blog post, refer to these additional Microsoft blogs:

For the latest security research from the Microsoft Threat Intelligence community, check out the Microsoft Threat Intelligence Blog: <https://aka.ms/threatintelblog>.

To get notified about new publications and to join discussions on social media, follow us on LinkedIn at <https://www.linkedin.com/showcase/microsoft-threat-intelligence>, and on X (formerly Twitter) at <https://twitter.com/MsftSecIntel>.

To hear stories and insights from the Microsoft Threat Intelligence community about the ever-evolving threat landscape, listen to the Microsoft Threat Intelligence podcast: <https://thecyberwire.com/podcasts/microsoft-threat-intelligence>.

Related Posts



Dec 4, 202416 min read

Frequent freeloader part I: Secret Blizzard compromising Storm-0156 infrastructure for espionage

Microsoft has observed Secret Blizzard compromising the infrastructure and backdoors of the Pakistan-based threat actor we track as Storm-0156 for espionage against the Afghanistan government and Indian Army targets.



Oct 29, 202413 min read

Midnight Blizzard conducts large-scale spear-phishing campaign using RDP files

Since October 22, 2024, Microsoft Threat Intelligence has observed Russian threat actor Midnight Blizzard sending a series of highly targeted spear-phishing emails to individuals in government, academia, defense, non-governmental organizations, and other sectors. This activity is ongoing, and Microsoft will continue to investigate and provide updates as available. Based on our investigation of previous Midnight [...]



Research

Threat intelligence

Microsoft Defender

Threat actors

Dec 7, 2023 28 min read

Star Blizzard increases sophistication and evasion in ongoing attacks

Microsoft Threat Intelligence continues to track and disrupt malicious activity attributed to a Russian state-sponsored actor we track as Star Blizzard, who has continuously improved their detection evasion capabilities while remaining focused on email credential theft against targets.



Research

Threat intelligence

Threat actors

Aug 15, 202212 min read

Disrupting SEABORGIUM's ongoing phishing operations

The Microsoft Threat Intelligence Center (MSTIC) has observed and taken actions to disrupt campaigns launched by SEABORGIUM in campaigns involve persistent phishing and credential theft campaigns leading to intrusions and data theft.

Get started with Microsoft Security

Microsoft is a leader in cybersecurity, and we embrace our responsibility to make the world a safer place.

[Learn more](#)

A horizontal banner with a yellow background. On the left, there is a blue curved shape with a green circle inside. On the right, there is a grey curved shape with a blue circle inside. The text "Protect it all with Microsoft Security" is centered in the yellow area.

**Protect it all
with Microsoft Security**