# Russian Star Blizzard New Evasion Techniques To Hijack Email Accounts

By **Guru Baran**


Hackers target email accounts because they contain valuable personal and financial information. Successful email breaches enable threat actors to:-

- Identity theft
- Financial fraud
- Unauthorized access to sensitive data

Cybersecurity researchers at Microsoft Threat Intelligence team recently unveiled that the Russian state-sponsored actor, Star Blizzard (aka SEABORGIUM, COLDRIVER, Callisto Group), has increased its sophistication and developed new evasion techniques to utilize in ongoing attacks.

Star Blizzard enhanced evasion techniques since 2022, focusing on email credential theft, and they target the following entities aligning with Russian interests:-

- International affairs
- Defense
- Logistics for Ukraine
- Academia

Microsoft improves defenses against spear-phishing and is grateful for the collaboration with the following global cybersecurity partners:-

- UK NCSC
- US NSA CCC
- FBI

**New TTPs**

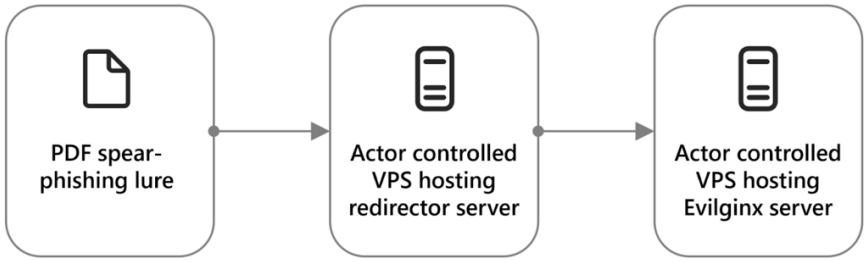
Here below, we have mentioned all the new TTPs identified by the cybersecurity analysts at the Microsoft Threat Intelligence team:-

- Use of server-side scripts to prevent automated scanning
- Use of email marketing platform services
- Use of a DNS provider to resolve actor-controlled domain infrastructure
- Password-protected PDF lures or links to cloud-based file-sharing platforms
- Randomizing DGA for actor-registered domains

**Russian Star Blizzard Attack Chain**

Star Blizzard focuses on email credential theft, favoring cloud-based providers. They persist with the Evilginx framework, relying on spear-phishing via email and custom PDF lures.

Redirection to actor-controlled infrastructure involves dedicated VPS pairs and, for target email providers, consistent use of Evilginx with "phishlet."



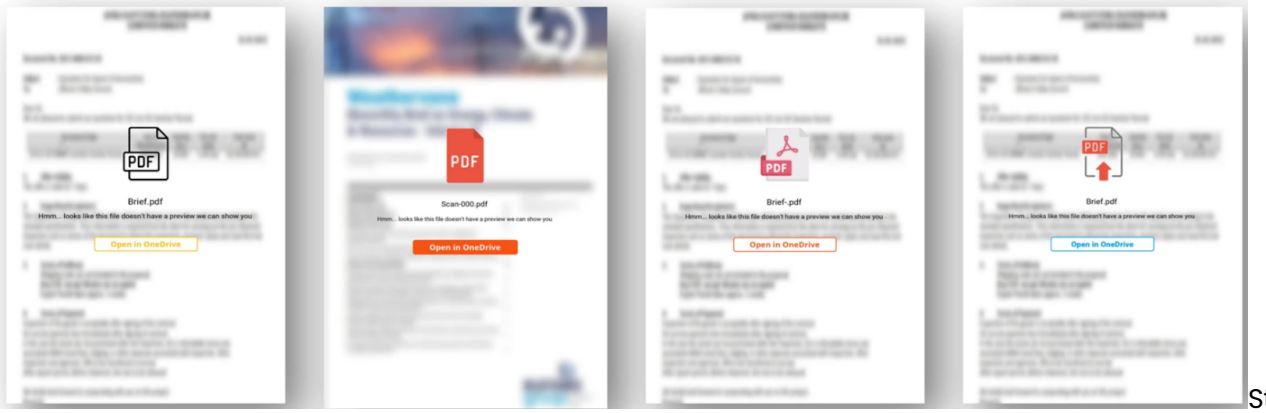

Star Blizzard redirection chain (Source – Microsoft)

Connected users and organizations in these areas are potential Star Blizzard targets:-

- Government or diplomacy
- Research into defense policy or international relations when related to Russia.
- Assistance to Ukraine related to the ongoing conflict with Russia.

Emails mimic known contacts via Proton email accounts (@proton.me, @protonmail.com), and the initial message requests a document review, but it does not provide any attachment or link to the document.

After the response, a follow-up includes a PDF file or link to a cloud-hosted PDF that will be unreadable with a misleading content-enable button.



Star Blizzard PDF lures (Source – Microsoft)

Pressing the PDF button opens a link, starting a redirection chain. The “Docs” page appears, followed by a CAPTCHA, and then the Sign-in screen displays the targeted email in the username field.

The host domain is actor-controlled, not the expected server domain. Password entry triggers an authentication request.

If approved, the account is compromised, and then the threat actor gains full access with successfully compromised credentials.

**Recommendations**

Here below, we have mentioned all the recommendations provided by the cybersecurity researchers:-

- Make sure to use advanced anti-phishing solutions.
- Always run EDR in block mode.
- In full automated mode, always configure investigation and remediation.
- On Microsoft Defender Antivirus, make sure to turn on cloud-delivered protection and automatic sample submission.
- As a baseline set of policies, always use security defaults.
- Continuous access evaluation is a must.
- All suspicious or anomalous activities must be monitored continuously.
- To recheck links on click, ensure proper configuration of Microsoft Defender for Office 365.
- In Microsoft Defender for Office 365, make sure to use the Attack Simulator.
- Always encourage users to use web browsers that support Microsoft Defender SmartScreen.
- Block executable files from running unless.
- Block execution of potentially obfuscated scripts.