Protecting Democratic Institutions from Cyber Threats

By Steven Masada

Published: 2024-10-03 · Archived: 2026-04-05 16:27:21 UTC

Microsoft's Digital Crimes Unit (DCU) is disrupting the technical infrastructure used by a persistent Russian nation-state actor Microsoft Threat Intelligence tracks as Star Blizzard. Today, the United States District Court for the District of Columbia unsealed a civil action brought by Microsoft's DCU, including its order authorizing Microsoft to seize 66 unique domains used by Star Blizzard in cyberattacks targeting Microsoft customers globally, including throughout the United States. Between January 2023 and August 2024, Microsoft observed Star Blizzard target over 30 civil society organizations – journalists, think tanks, and non-governmental organizations (NGOs) core to ensuring democracy can thrive – by deploying spear-phishing campaigns to exfiltrate sensitive information and interfere in their activities.

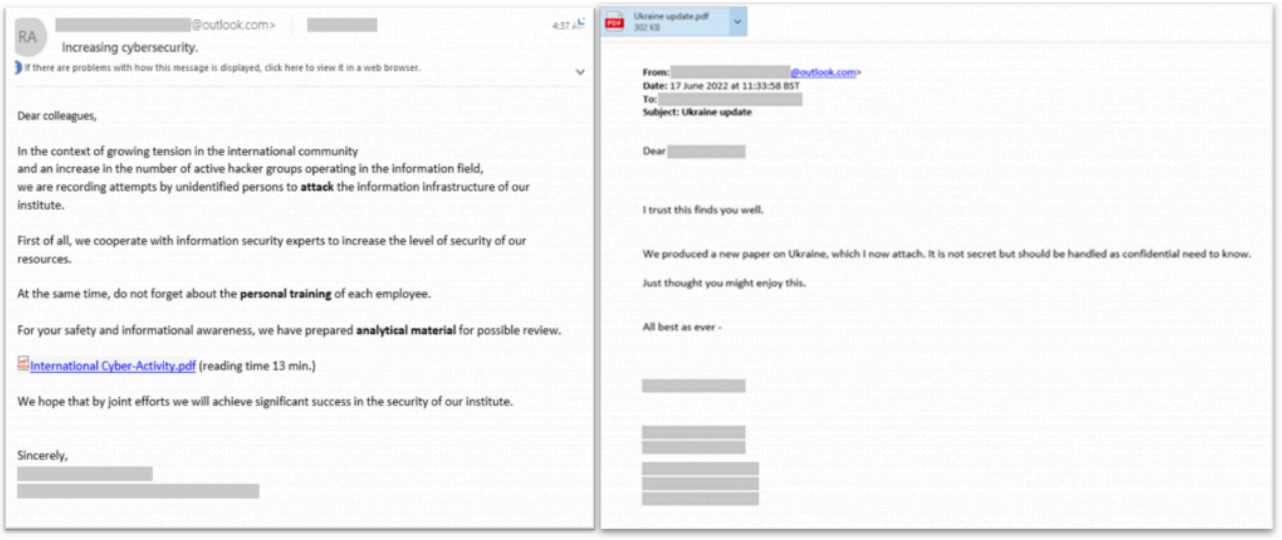
We are filing this lawsuit with the NGO Information Sharing and Analysis Center (NGO-ISAC) and have coordinated with the Department of Justice (DOJ), which simultaneously seized 41 additional domains attributed to the same actor. Together, we have seized more than 100 websites. Rebuilding infrastructure takes time, absorbs resources, and costs money. By collaborating with DOJ, we have been able to expand the scope of disruption and seize more infrastructure, enabling us to deliver greater impact against Star Blizzard.

While we expect Star Blizzard to always be establishing new infrastructure, today's action impacts their operations at a critical point in time when foreign interference in U.S. democratic processes is of utmost concern. It will also enable us to quickly disrupt any new infrastructure we identify through an existing court proceeding. Furthermore, through this civil action and discovery, Microsoft's DCU and Microsoft Threat Intelligence will gather additional valuable intelligence about this actor and the scope of its activities, which we can use to improve the security of our products, share with cross-sector partners to aid them in their own investigations and identify and assist victims with remediation efforts.

Star Blizzard's operations are relentless, exploiting the trust, privacy, and familiarity of everyday digital interactions.

Star Blizzard (also known as COLDRIVER and Callisto Group) has actively engaged in various forms of cyberattacks and activity since at least 2017. Since 2022, Star Blizzard has improved their detection evasion capabilities while remaining focused on email credential theft against the same targets. Our actions today will impact those capabilities. Most recently, Star Blizzard targets NGOs and think tanks that support government employees and military and intelligence officials, especially those providing support to Ukraine and in NATO countries such as the United States and the United Kingdom, as well as in the Baltics, Nordics, and Eastern Europe. They have been particularly aggressive in targeting former intelligence officials, Russian affairs experts, and Russian citizens residing in the U.S. In 2023, the British government and its allies attributed Star Blizzard to the Russian Federal Security Service (FSB) and exposed the actor's attempted interference in UK politics through the targeting of elected officials, think tanks, journalists and the public sector.

is persistent. They meticulously study their targets and pose as trusted contacts to achieve their goals. Since January 2023, Microsoft has identified 82 customers targeted by this group, at a rate of approximately one attack per week. This frequency underscores the group's diligence in identifying high-value targets, crafting personalized phishing emails, and developing the necessary infrastructure for credential theft. Their victims, often unaware of the malicious intent, unknowingly engage with these messages leading to the compromise of their credentials. These attacks strain resources, hamper operations and stoke fear in victims — all hindering democratic participation.



Examples of phishing emails from Star Blizzard.

Star Blizzard's ability to adapt and obfuscate its identity presents a continuing challenge for cybersecurity professionals. Once their active infrastructure is exposed, they swiftly transition to new domains to continue their operations. For example, on August 14, 2024, The Citizen Lab of the University of Toronto's Munk School and digital rights group Access Now, itself a non-profit member of NGO-ISAC, which filed a declaration in support of this civil action, published a comprehensive research paper highlighting the persistent threat posed by this actor. Since publishing this report, Access Now and The Citizen Lab have been investigating several additional cases and believe at least one of these cases is associated with Star Blizzard. This shows that Star Blizzard remains active and is not deterred despite governments, companies, and civil society exposing their malicious activities.

Star Blizzard's activities underscore the importance of upholding international norms to govern responsible state behavior online.

Today's action is an example of the impact we can have against cybercrime when we work together. We applaud DOJ for their collaboration in this and other significant matters and encourage governments globally to engage and embrace industry partners, such as Microsoft, in a shared mission of combatting increasingly sophisticated threats operating in cyberspace. Microsoft's DCU will continue our efforts to proactively disrupt cybercriminal infrastructure and collaborate with others across the private sector and with civil society, government agencies and law enforcement to fight back against those who seek to cause harm. DCU likewise will continue to innovate and develop new and creative ways to detect, disrupt, and deter the techniques and tactics of sophisticated cybercriminals to protect individuals online.

As a best practice, we encourage all civil society groups to harden their cybersecurity protections, use strong multi-factor authentication like passkeys on both personal and professional accounts, and enroll in Microsoft's AccountGuard program for an additional layer of monitoring and protection from nation-state cyber-attacks.

However, these efforts and commitments must be coupled with an application of international norms to limit cyberattacks associated with nation–states that purposely target the parts of society that enable democracy to thrive. Star Blizzard's observed activity violates the UN Framework for Responsible State Behavior Online, a clear set of norms agreed upon by all UN member states to prevent their territories from being used for malicious online activity. By taking action against Star Blizzard, Microsoft and its partners are reinforcing the importance of these internationally agreed norms and demonstrating a commitment to their enforcement, aiming to protect civil society and uphold the rule of law in cyberspace.

Tags: cyberattacks, cybercrime, cybersecurity, Microsoft AccountGuard, Microsoft Threat Intelligence Center, phishing, Russia, The Digital Crimes Unit

---