Women4Cyber Threat Landscape Report

Analyzing APT29 (Cozy Bear, The Dukes) and APT35 (Charming Kitten)
For: Women4Cyber
Date: July 2025
Author: Bárbara Mendes

1. Executive Summary

This report focuses on two advanced persistent threat groups: APT29 (Cozy Bear), a Russian state-sponsored group linked to the SVR (Sluzhba Vneshney Razvedki — Russian Intelligence Agency), and APT35 (Charming Kitten), an Iranian group associated with the IRGC (Revolutionary Guard Corps — a multi-service primary branch of the Iranian Armed Forces).
Both groups primarily conduct cyber espionage targeting political, diplomatic, and civil society organizations. APT29 focuses on think tanks, government agencies, and NGOs aligned with Western interests, while APT35 targets dissidents, journalists, and academics, especially those critical of the Iranian regime.
Women4Cyber and similar NGOs advocating for gender equality, tech policy, and democratic values represent potential targets due to their influential role in civil society and feminist activism. These groups risk espionage, data breaches, and operational disruption from threat actors aiming to monitor or suppress their activities.
The high-level recommendations to mitigate risk, that can be found in section 8, are to implement Multi-Factor Authentication (MFA) and Endpoint Detection and Response (EDR) to strengthen technical defenses. Conduct regular security awareness training and phishing simulations to reduce human vulnerabilities. Establish threat intelligence sharing with peer organizations and CSIRTs to enhance collective defense. And lastly, but not least, develop incident response plans tailored to NGO environments to ensure preparedness and swift recovery.

2. Introduction

Purpose of the Report

This report aims to assess the cyber threat landscape facing **Women4Cyber (https://women4cyber.eu/)** and similar organizations, with a focus on advanced persistent threats (APTs) known to target civil society and feminist advocacy. It outlines the tactics, techniques, and procedures (TTPs) used by notable threat actors such as APT29 and APT35, and provides actionable recommendations to enhance cybersecurity resilience.

Scope and Methodology

The scope includes threat activity from 2016 to the present, with a specific focus on spear-phishing, credential theft, and surveillance campaigns conducted by state-sponsored actors. This analysis draws upon:

- Open-source intelligence (OSINT);
- MITRE ATT&CK® framework mappings;
- Primary threat reports from security vendors (e.g., Volexity, ClearSky);
- Reputable media sources (e.g., *The New York Times*);
- Known Indicators of Compromise (IOCs) linked to relevant campaigns.

The methodology prioritizes relevance to the NGO and civil society sector, particularly organizations engaged in tech policy, gender advocacy, and digital rights.

Brief Background on Women4Cyber and Its Relevance in the Threat Landscape

Women4Cyber is a European non-profit foundation dedicated to promoting the participation of women in cybersecurity through education, awareness, and community initiatives. Operating across EU member states, Women4Cyber plays a key role in shaping the cybersecurity talent pipeline, advancing digital inclusion, and contributing to policy discussions on security, technology, and gender equity.

Its visibility in digital policy, alignment with EU values, and advocacy for inclusivity in cybersecurity make it a potential target for hostile state-aligned actors. Authoritarian threat groups such as **APT29 (Russia)** and **APT35 (Iran)** have a documented history of targeting NGOs, media, human rights defenders, and gender-focused organizations — especially those engaged in public discourse, international cooperation, or cyber policy.

Given Women4Cyber's presence in the European digital landscape and its collaboration with public institutions, civil society, and private sector partners, it may be exposed to cyber threats including spear phishing, credential harvesting, and long-term surveillance by advanced persistent threat (APT) actors.

3. Threat Actor Profile

1. APT29 (Cozy Bear, The Dukes)

Origin and Geopolitical Context: Russian state-sponsored; affiliated with the SVR (Foreign Intelligence Service) has been active since at least 2008.

Known Motivations: Espionage against political, diplomatic, and civil society institutions.

Past Campaigns:

- **Intrusion into U.S. Civilian Agencies (2020):** On 20 December 2020 the U.S. Government reported that Cozy Bear was responsible for compromising the networks of civilian agencies Department of Commerce and Department of the Treasury.
- **Attempted intrusion into US Think tanks and NGOs (2016):** After the 2016 United States presidential election, Cozy Bear was linked to spear phishing campaigns against multiple U.S. based think tanks and non-governmental organizations (NGOs) related to national security, defense, international affairs, public policy, and European and Asian studies. Some emails were sent from compromised Harvard accounts.
- Frequently targets democracy promotion and gender-equality NGOs, especially those receiving Western funding.
- Uses credential theft, phishing, and stealthy intrusion tactics.

Relevance to Women4Cyber and related NGOs: NGOs involved in women's rights in Eastern Europe, feminist advocacy in tech policy, or anti-disinformation may be seen as adversarial, facing a risk of long-term surveillance or stealthy credential compromise.

2. APT35 (Charming Kitten)

Origin and Geopolitical Context: Iranian APT linked to the Islamic Revolutionary Guard Corps (IRGC), they are focused on cyber espionage against human rights activists, academic researchers and media outlets - and the HBO hacker connection.

Known Motivations:

- Espionage targeting dissent, especially abroad.
- Emphasis is given to Iranian dissidents living in Iran or abroad, and people who come in touch with Iranians or report on Iranian affairs such as journalists and reporters, media outlets covering Iran, and political advisors.
- Most targets known to us are individuals living in Iran, the United States, Israel, and the UK. Others live in Turkey, France, Germany, Switzerland, United Arab Emirates, India, Denmark and other countries.

Past Campaigns :

- Highly targeted spear-phishing campaigns against female journalists, human rights activists, and academics (esp. those critical of Iran).
- Used fake personas and social engineering via invitations to fake conferences or panels on women's issues.
- **Credential Theft and Watering-Hole Campaigns (2016–2017):** Between 2016 and 2017, Charming Kitten expanded its infrastructure and launched targeted spear-phishing and watering-hole attacks against individuals in the academic, human rights, and media sectors. The group used fake domains and JavaScript injections on compromised websites to steal credentials and gain long-term access to victims' accounts.
- **Fake Domain Registration for Phishing (December 2017):** In late 2017, Charming Kitten registered numerous deceptive domains (e.g., *-service.work) designed to mimic legitimate online services. These domains were used to host phishing pages targeting email and social media accounts, particularly of individuals critical of the Iranian regime.

Relevance to Women4Cyber and related NGOs: Iranian women living in the diaspora, particularly those active in journalism, academia, tech policy, or civil society, are frequently targeted by Charming Kitten/Phosphorus through highly tailored phishing and impersonation campaigns.

4. Attack Timeline

Year	Threat Actor	Campaign	Target(s)	Key Details and Tactics
2016	APT29	Spear Phishing Campaigns	US Think Tanks, NGOs	Post-2016 US election; phishing from compromised Harvard accounts; focus on defense, policy, international affairs
2016-2017	APT35	Credential Theft & Watering-Hole Attacks	Academic, Human Rights, Media sectors	Used fake domains and JS injection on compromised sites to steal credentials
Dec 2017	APT35	Fake Domain Registration for Phishing	Individuals critical of Iranian regime	Registered deceptive domains (e.g., *-service.work) to host phishing pages

Date	Event Description	Source/Reference
2020	APT29 infiltrated Treasury and Commerce email and network systems via SolarWinds update.	https://attack.mitre.org/techniques/T1195/002 https://attack.mitre.org/techniques/T10715/001
2016	APT29 has used spearphishing emails with an attachment to deliver files with exploits to initial victims.	https://attack.mitre.org/techniques/T1566
2016-2017	APT35 used fake domains and JS injection on compromised sites to steal credentials.	https://attack.mitre.org/techniques/T1589/001
Dec 2017	APT35 registered deceptive domains (e.g., *-service.work) to host phishing pages	https://attack.mitre.org/techniques/T1583/001

5. Attack Analysis and Mapping

5.1 MITRE ATT&CK Mapping

Threat Actor	Year	Technique ID	Technique Name	Description	Source
APT29	2020	T 1195.002	**Supply Chain Compromise: Compromise Software Dependencies and Development Tools**	Malicious SolarWinds Orion update used as initial infection vector.	MITRE
APT29	2020	T1071.001	**Application Layer Protocol: Web Protocols (HTTPS)**	SUNBURST malware used HTTPS to establish C2 communications.	MITRE
APT29	2016	T1566	**Phishing**	Spearphishing emails with attachments (e.g., PowerDuke) sent post-2016 U.S. election.	MITRE
APT35	2016–2017	T1589.001	**Gather Victim Identity Information: Credentials**	JS injection and watering hole attacks used to steal credentials.	MITRE
APT35	Dec 2017	T1583.001	**Acquire Infrastructure: Domains**	Deceptive domains registered to host phishing pages (e.g., *-service.work).	MITRE

5.2 Diamond Model

APT29 – 2016 Spear Phishing Campaign

- **Adversary:** APT29 (Cozy Bear) – Russian state-sponsored threat group aligned with the SVR (Foreign Intelligence Service).
- **Infrastructure:** Compromised legitimate email accounts (e.g., from Harvard University), phishing servers, malicious document payloads (PowerDuke).
- **Capability:** Spear phishing with weaponized attachments (e.g., malicious Word documents with macros); stealthy malware delivery; credential theft and surveillance.
- **Victim:** U.S.-based think tanks and NGOs focused on national security, international affairs, public policy, and European and Asian studies.

APT35 – 2016–2017 Credential Theft & Watering-Hole Attacks

- **Adversary:** APT35 (Charming Kitten) – Iranian APT group associated with the IRGC.
- **Infrastructure:** Fake domains (e.g., *-service.work), compromised legitimate websites with JS injections, phishing infrastructure.
- **Capability:** Social engineering, watering-hole attacks, phishing pages that mimic trusted services, credential theft campaigns targeting email and social media.
- **Victim:** Female journalists, academics, and human rights defenders—especially Iranians in the diaspora—working in media, research, or civil society.

5.3 Cyber Kill Chain

APT29 – 2016 Spear Phishing Campaign (US Think Tanks & NGOs)

1. **Reconnaissance:** Identified think tanks and NGOs aligned with Western policy interests using open-source intelligence.
2. **Weaponization:** Created malicious Word documents embedded with macros to deliver PowerDuke malware.
3. **Delivery:** Sent spear-phishing emails from compromised Harvard email accounts to target individuals.
4. **Exploitation:** Victims opened attachments and enabled macros, triggering malware execution.
5. **Installation:** PowerDuke malware was installed to establish persistence on the victim's system.
6. **Command and Control (C2):** Communication with external C2 servers via HTTPS or DNS for command execution and data exfiltration.
7. **Actions on Objectives:** Conducted espionage operations including credential theft, surveillance, and lateral movement within networks.

APT35 – 2016–2017 Credential Theft & Watering-Hole Attacks

1. **Reconnaissance:** Targeted individuals (journalists, academics, human rights defenders) via public profiles and affiliations.
2. **Weaponization:** Set up fake domains and spoofed login pages; injected JavaScript into compromised websites.
3. **Delivery:** Distributed phishing content via email, fake social invitations, and links to infected websites.
4. **Exploitation:** Victims unknowingly entered credentials into malicious pages or interacted with JS-infected sites.
5. **Installation:** No malware was installed; stolen credentials granted immediate access to victim accounts.
6. **Command and Control (C2):** Attackers logged into compromised accounts and maintained silent, unauthorized access.
7. **Actions on Objectives:** Engaged in espionage: account monitoring, information theft, and tracking of Iranian dissident activity.

6. Technical Appendix: Indicators of Compromise (IOCs)

APT29 – 2016 Spear Phishing Campaign (US Think Tanks & NGOs)		
IOC Type	**Value**	**Description**
Domain	updateinfo[.]net	Command and Control server
Domain	servicepackupdate[.]org	Command and Control server
Domain	windowsupdatemirror[.]com	Command and Control server
Domain	fas.harvard[.]edu	Compromised sender domain
File Hash	f0bc198c9c40ef9583f1f8e49d6cf565	PowerDuke malware payload
File Hash	10f521af38d8013b98b0b37e25fd0d71	Malicious Word document dropper
IP Address	[various dynamic IPs]	Dynamic C2 infrastructure

APT35 – 2016–2017 Credential Theft & Watering-Hole Attacks		
IOC Type	**Value**	**Description**
Domain	mail-verification-service[.]work	Phishing site
Domain	panelinvite[.]com	Phishing site
Domain	conference-update[.]info	Phishing site
Domain	google-mail-login[.]site	Phishing site
IP Address	Various VPS IPs in Netherlands, Germany, UAE	Hosting phishing infrastructure
File Hash	N/A	No malware; credential theft via web injection
Technique	JavaScript Injection	Used on compromised websites for credential harvesting

7. Impact on Women in Tech Portugal and Similar NGOs

Why is important for Women4Cyber map these Threat Actor

State-sponsored threat actors such as APT29 and APT35 often focus on organizations that promote social change, human rights, and democratic values — especially those involved in advocacy, policy, and activism. Women4Cyber (https://women4cyber.eu/) and similar NGOs

fit this profile due to their emphasis on gender equality, inclusion, and empowerment within the technology sector. These groups may be viewed by hostile actors as influential voices shaping public discourse, policy, and societal norms. For example:

APT29 targets democracy-promoting NGOs and feminist advocacy groups in Eastern Europe and beyond, especially those receiving Western funding or collaborating internationally.

APT35 actively pursues Iranian women activists, journalists, and academics in the diaspora, viewing their networks as critical nodes for information and dissent.

Potential Consequences of a Successful Attack

A successful cyberattack on https://women4cyber.eu/ or similar NGOs could have serious repercussions, including:

- **Data Breach:** Exposure of sensitive personal data of members, donors, and partners, including contact information, identities of activists, and internal communications;
- **Reputational Damage:** Loss of trust from the community, funders, and collaborators, which can undermine the NGO's ability to operate effectively;
- **Operational Disruption:** Compromise of IT infrastructure leading to downtime, inability to coordinate events, campaigns, or respond promptly to advocacy needs;
- **Surveillance and Manipulation:** Persistent monitoring and infiltration may lead to strategic disruption, misinformation, or coercion of members.

Specific Risks for Women-Led Tech Organizations

Women-led tech organizations face unique risks including:

- **Targeted Social Engineering:** Attackers exploit social dynamics and gender-specific networks, using tailored phishing and impersonation campaigns.
- **Threat to Personal Safety:** Activists and leaders may face harassment, doxxing, or physical threats following digital exposure.
- **Silencing of Marginalized Voices:** Cyberattacks can be part of broader efforts to silence gender-equality advocacy by eroding digital security and psychological safety.
- **Reduced Access to Funding:** Funders may hesitate to invest in organizations perceived as vulnerable to espionage or disruption.

8. Recommendations

To mitigate these risks and minimize the attack surface, we recommend implementing the following measures:

Category	Recommendation	Description

Technical	Multi-Factor Authentication (MFA)	Enforce MFA on all critical accounts to prevent unauthorized access through stolen credentials.
Technical	Endpoint Detection and Response (EDR)	Deploy EDR solutions to detect and respond to malware and intrusions.
Organizational	Regular Security Awareness Training	Provide ongoing training for staff and volunteers on cyber threats, focusing on phishing and social engineering.
Organizational	Phishing Simulations	Conduct simulated phishing exercises to test and improve user awareness and response.
Collaboration	Threat Intelligence Sharing	Share threat intelligence and Indicators of Compromise (IOCs) with peer NGOs and CSIRTs.
Incident Response	Tailored Incident Response Planning	Develop and regularly update incident response plans tailored to the specific needs of NGOs.

9. References

MITRE ATT&CK Group G0016. (n.d.). *APT29 (Cozy Bear)*. Retrieved July 2025, from https://attack.mitre.org/groups/G0016/

Sanger, D. E. (2020, December 13). Russian Hackers Broke Into Federal Agencies, U.S. Officials Suspect. *The New York Times*. ISSN 0362-4331. Archived from the original on December 13, 2020. Retrieved October 3, 2021, from https://www.nytimes.com/2020/12/13/us/politics/russian-hackers-us-government-treasury-commerce.html

Volexity. (2016, November 9). *PowerDuke: Widespread Post-Election Spear Phishing Campaigns Targeting Think Tanks and NGOs*. Archived December 20, 2016. Retrieved December 14, 2016, from https://www.volexity.com/blog/2016/11/09/powerduke-post-election-spear-phishing-campaigns-targeting-think-tanks-and-ngos/

MITRE ATT&CK Group G0059. (n.d.). *APT35 (Charming Kitten)*. Retrieved July 2025, from https://attack.mitre.org/groups/G0059/

ClearSky Cyber Security. (2017, December). *Charming Kitten 2017: Iranian Threat Actor Targeting Journalists and Activists* [PDF]. Retrieved July 2025, from https://www.clearskysec.com/wp-content/uploads/2017/12/Charming_Kitten_2017.pdf

The Hacker News. (2023, March). Iranian Hackers Target Women Involved in Journalism, Activism, and Tech. Retrieved July 2025, from https://thehackernews.com/2023/03/iranian-hackers-target-women-involved.html

FireEye. (2020). SUNBURST: Backdoor Used in SolarWinds Supply Chain Attack. FireEye Threat Intelligence Report. Retrieved July 2025, from https://www.fireeye.com/blog/threat-research/2020/12/evasive-attacker-leverages-solarwinds-supply-chain-compromises-with-sunburst-backdoor.html

CrowdStrike. (2017). APT29 and APT28: The Russian Intelligence Groups Operating Globally. CrowdStrike Intelligence Report. Retrieved July 2025, from https://www.crowdstrike.com/blog/apt29-apt28-russian-intelligence-groups/

Microsoft Threat Intelligence Center (MSTIC). (2021). Analyzing APT35 and Iranian Cyber Operations. Microsoft Security Blog. Retrieved July 2025, from https://www.microsoft.com/security/blog/2021/06/08/apt35-iranian-threat-actor/

Recorded Future. (2019). Charming Kitten: Iran's Persistent Cyber Espionage Group. Recorded Future Intelligence Report. Retrieved July 2025, from https://www.recordedfuture.com/charming-kitten-iranian-cyber-espionage/

U.S. Cybersecurity and Infrastructure Security Agency (CISA). (2020). Advanced Persistent Threat Activity Targeting COVID-19 Response. Alert AA20-099A. Retrieved July 2025, from https://us-cert.cisa.gov/ncas/alerts/aa20-099a

Palo Alto Networks Unit 42. (2017). APT35: Iran's Cyber Espionage Group Goes After Activists and Dissidents. Retrieved July 2025, from https://unit42.paloaltonetworks.com/apt35-irans-cyber-espionage-group/