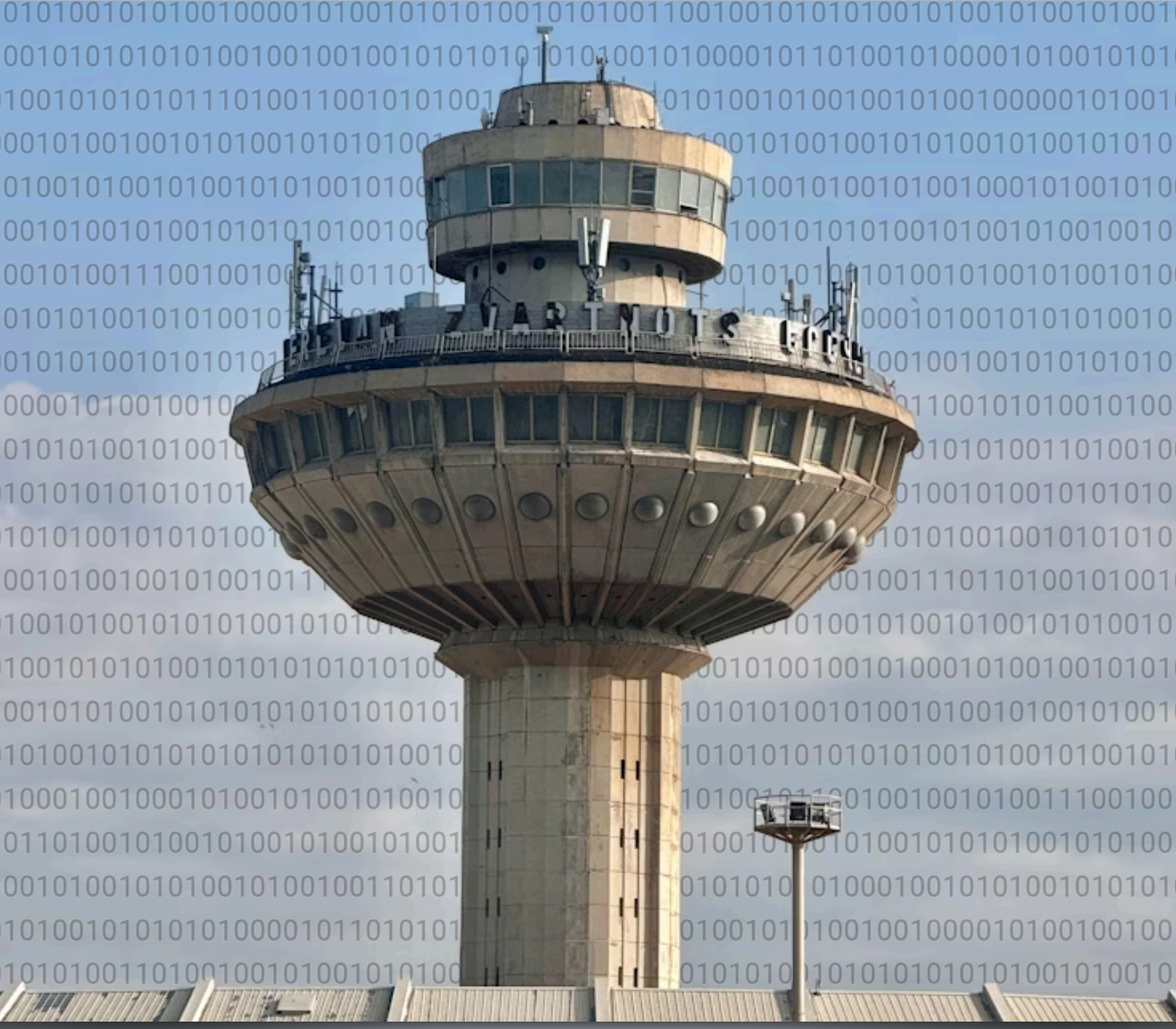


Photo by Mika Hovsepyan | Illustration by MDI | Zvartnots International Airport , Yerevan, Armenia

Armenia Cybersecurity Threat Landscape 2024

Media Diversity Institute

CyberHUB

Spyware Accountability Initiative

Table of Contents

Introduction

Armenia's digital security environment faced significant challenges in 2024, largely driven by geopolitical tensions and sophisticated cyber threats. The country's strategic pivot toward the European Union, United States and reduced dependence on Russia appears to have intensified these cybersecurity risks.

The threat landscape encompasses multiple sectors, with targeted attacks against government institutions, media organizations, and civil society groups. State-sponsored cyber espionage has become particularly concerning, with advanced spyware deployments observed during the Armenia-Azerbaijan conflict. These persistent attacks on Armenia's digital infrastructure have raised serious security concerns.

Major technology companies and cybersecurity organizations have documented these threats, emphasizing the urgent need for strengthened defensive measures to safeguard sensitive information and critical systems.

This report provides an updated overview of key cyber threats facing Armenia – including mercenary spyware, phishing, DDoS attacks, website hacks, remote access trojans (RATs), and insider threats – and examines significant incidents, trends in cybercrime and state-sponsored attacks, as well as the responses by Armenian authorities and cybersecurity organizations. The goal is to offer cybersecurity professionals, policymakers, and journalists a data-driven analysis of Armenia’s cyber resiliency and emerging risks in 2024.

Armenia Cybersecurity Threat Landscape 2024 serves as a sequential update to the previous annual publication, which detailed the state of cybersecurity in the Republic of Armenia.

Geopolitical Dynamics and Cybersecurity Challenges

Armenia's cybersecurity landscape cannot be separated from its geopolitical context. The longstanding conflict between Armenia and Azerbaijan has frequently extended into cyberspace. Azerbaijan's 2020-2023 military offensives against Nagorno-Karabakh and Armenia were preceded by heavy cyberattacks on Armenian government agencies, including malware phishing.

These events exemplify how military operations are often preceded or accompanied by coordinated cyber offensives. Armenian targets have also been in the crosshairs of regional and global cyber powers.

Notably, **NSO Group's Pegasus spyware** was used against Armenian officials and activists during intense phases of the conflict, marking the first confirmed use of Pegasus in an international war setting. Potential targets received threat notifications from Apple in 2024 as well, which usually is a good indicator that spyware attacks are continuing. The cyber capabilities of Azerbaijan have been enhanced through collaboration with its military partners, including the provision of Israeli technology, which has been identified as a component of Azerbaijan's cyber arsenal.

At the same time, ostensibly allied states have conducted espionage in Armenia: Russian state-backed hacking groups (including GRU associated **APT28 (Fancy Bear)** and FSB-associated **Turla**) have been active, targeting Armenian government institutions via spear-phishing and other tactics.

In January 2024, the hacking group Anonymous Russia launched distributed denial-of-service (DDoS) attacks against Armenian government websites, banks, and telecommunications companies,

allegedly in response to Armenia's growing ties with Western nations.

Subsequently, in March 2024, Anonymous Sudan, a group affiliated with Russia, claimed responsibility for a cyberattack on Team Telecom, a prominent Armenian mobile operator. These incidents highlight the increasing involvement of Russian-affiliated hacker groups in targeting Armenian digital infrastructure.

Additionally, in June 2024, the People's Cyber Army of Russia launched distributed denial-of-service (DDoS) attacks on Armenian government websites, coinciding with diplomatic strains between Yerevan and Moscow.

In parallel, Armenia pursued the advancement of its relationships with the European Union and the United States. In January 2025, Armenia and the United States signed a Charter of Strategic Partnership, aiming to enhance bilateral relations across various domains, including defense and cybersecurity. This partnership facilitates Armenia's access to U.S. technological expertise, particularly in modernizing its nuclear sector and developing artificial intelligence capabilities.

Domestically, Armenia's persistent political instability, exacerbated by the 2020 Nagorno-Karabakh conflict and subsequent border tensions, has created a fertile ground for cyberattacks targeting media outlets and opposition figures. This trend reflects a broader attempt by various actors to manipulate and control the information landscape, a tactic increasingly prevalent in hybrid warfare. Recent analyses highlight the growing use of disinformation and targeted cyber campaigns to influence public discourse and undermine public institutions.

Domestic Cybersecurity Initiatives

Against this backdrop, Armenia has been striving to improve its cybersecurity posture as part of a broader digital transformation. The government adopted a **Digitalization Strategy** that emphasizes innovative technologies, e-governance, and cybersecurity integration. Multiple Computer Emergency Response Teams (CERTs) have been established, and cybersecurity legislation is in development.

In March 2024, Armenia announced the establishment of a National Center for Information Security and Cryptography to bolster information protection and develop secure software solutions.

Furthermore, to enhance cyber resilience, Armenia hosted its first national cybersecurity exercise in December 2024, in collaboration with the International Telecommunication Union (ITU). The event engaged over 150 representatives from critical infrastructure sectors, focusing on strengthening defenses against cyber threats.

Concurrently, legislative efforts have been initiated to address the rising incidence of cybercrimes. A proposed law aims to protect digital infrastructures, including electronic trading platforms and communication services, by providing comprehensive legal mechanisms to combat cyber threats. This initiative responds to a significant increase in cybercrimes, which doubled between 2021 and 2023.

However, capacity and coordination challenges persist. In late 2023, Armenia's Audit Chamber reported that a planned National Cybersecurity Center had yet to be stood up and that **cyber defense preparedness in government agencies remains weak**, with no regular drills or real-time monitoring in place. The Audit Chamber's chairman

noted that Armenia ranks only **93rd out of 193 countries** in global cybersecurity indices – highlighting considerable room for improvement. This mix of high threat exposure and still-maturing defenses defines the cybersecurity landscape going into 2024.

Media Literacy and Countering Disinformation

Recognizing the role of information warfare in undermining national security, Armenia has implemented strategies to combat disinformation. In December 2023, the government introduced the Concept and Action Plan of the Struggle against Disinformation 2024-2026, aiming to bolster capacities in both the public and private sectors and promote media literacy among citizens. These measures are designed to empower the populace to critically assess information sources, thereby mitigating the impact of fake news and external propaganda.

Next

Mercenary Spyware

The use of mercenary spyware, or commercial spyware, in Armenia has become a significant concern, particularly in the context of national security and personal privacy. Mercenary spyware refers to software developed by private companies and sold to governments or other entities, often covertly, to monitor and extract data from targeted individuals' devices. This type of spyware is known for its sophisticated capabilities, including recording keystrokes, capturing screenshots, tracking locations, and even activating microphones and cameras without the user's knowledge.

In Armenia, mercenary spyware has reportedly been utilized in efforts to gather intelligence and monitor activities of interest. The deployment of such spyware can be seen as a double-edged sword; while it provides authorities with advanced tools to counter cyber threats and criminal activities, it simultaneously raises ethical and legal questions regarding surveillance and the right to privacy. Instances of misuse, where spyware is employed to target political opponents, journalists, or activists, have sparked public outcry and demands for greater transparency and oversight.

The rise of mercenary spyware in Armenia underscores the urgent need for robust regulatory frameworks and cybersecurity measures. The government must balance the benefits of these powerful tools against the potential for abuse, ensuring that the use of commercial spyware is conducted within legal boundaries and respects human rights. Additionally, public awareness and media literacy campaigns are essential to educate citizens about the risks associated with spyware and to promote vigilance in protecting personal data. As Armenia continues to navigate its digital transformation, addressing the challenges posed by mercenary spyware will be critical in safeguarding both national security and individual freedoms.

Phishing

In recent years, Armenia has witnessed a troubling rise in phishing attacks, which have become a prevalent threat to both individuals and organizations. Phishing, a method of cybercrime where attackers masquerade as trustworthy entities to deceive victims into revealing sensitive information, continues to evolve in sophistication and impact. These attacks often involve emails, social media messages, or fake websites designed to trick recipients into disclosing passwords, financial details, or personal information. The increase in phishing activities is particularly concerning given Armenia's ongoing digital transformation and the growing reliance on online services for communication, commerce, and governance.

The consequences of phishing attacks in Armenia are manifold, affecting various sectors and demographics. For businesses, a successful phishing attack can lead to financial loss, compromised proprietary information, and reputational damage. Government agencies are also vulnerable, with potential breaches threatening national security and public trust. On an individual level, victims may face identity theft, drained bank accounts, and psychological stress. Despite efforts to enhance cybersecurity, including legislative measures and technological advancements, the persistence of phishing underscores the necessity for continuous vigilance and education. Citizens and organizations must be equipped with the knowledge to recognize and respond to such threats effectively.

To mitigate the impact of phishing attacks, Armenia has embarked on several initiatives aimed at strengthening cyber resilience. Public awareness campaigns are crucial in educating citizens about the tactics of phishers and promoting safe online practices. Additionally, cybersecurity training programs for businesses and government

employees help build a proactive defense against phishing attempts. The implementation of robust security protocols, such as multi-factor authentication and regular system updates, further fortifies defenses against these deceptive attacks. As Armenia strives to bolster its cybersecurity landscape, a concerted effort involving technological, educational, and legislative strategies is essential to safeguard its digital domain from the relentless threat of phishing.

DDoS

Distributed Denial of Service (DDoS) attacks have emerged as a significant cybersecurity threat in Armenia, impacting various sectors and institutions. These attacks involve overwhelming a target's online services with a flood of internet traffic, rendering them inaccessible to legitimate users. The perpetrators of DDoS attacks often exploit networks of compromised computers, known as botnets, to generate the massive volume of traffic required to disrupt service. In Armenia, numerous companies, government agencies, and even critical infrastructure have fallen victim to these disruptive attacks, highlighting the urgent need for enhanced cybersecurity measures.

The consequences of DDoS attacks in Armenia are far-reaching, affecting both the public and private sectors. For businesses, a successful DDoS attack can result in significant financial losses due to downtime, decreased productivity, and potential reputational damage. Government services may also experience disruption, hindering public access to essential services and eroding trust in digital governance. Furthermore, the impact on critical infrastructure, such as energy and healthcare systems, can have severe implications for national security and public safety. The increasing frequency and sophistication of DDoS attacks underscore the necessity for a robust and coordinated response to safeguard Armenia's digital landscape.

To mitigate the effects of DDoS attacks, Armenia has undertaken various initiatives aimed at strengthening its cyber defenses. Investments in advanced cybersecurity technologies, such as intrusion detection systems and anti-DDoS solutions, are crucial in detecting and neutralizing these threats. Collaboration with international partners and cybersecurity organizations can provide valuable insights and resources to enhance Armenia's capabilities in countering DDoS attacks. Additionally, fostering a culture of cybersecurity awareness among citizens and organizations is essential in building a resilient digital ecosystem. As Armenia continues to advance its digital transformation, addressing the challenges posed by DDoS attacks will be critical in ensuring the stability and security of its online services.

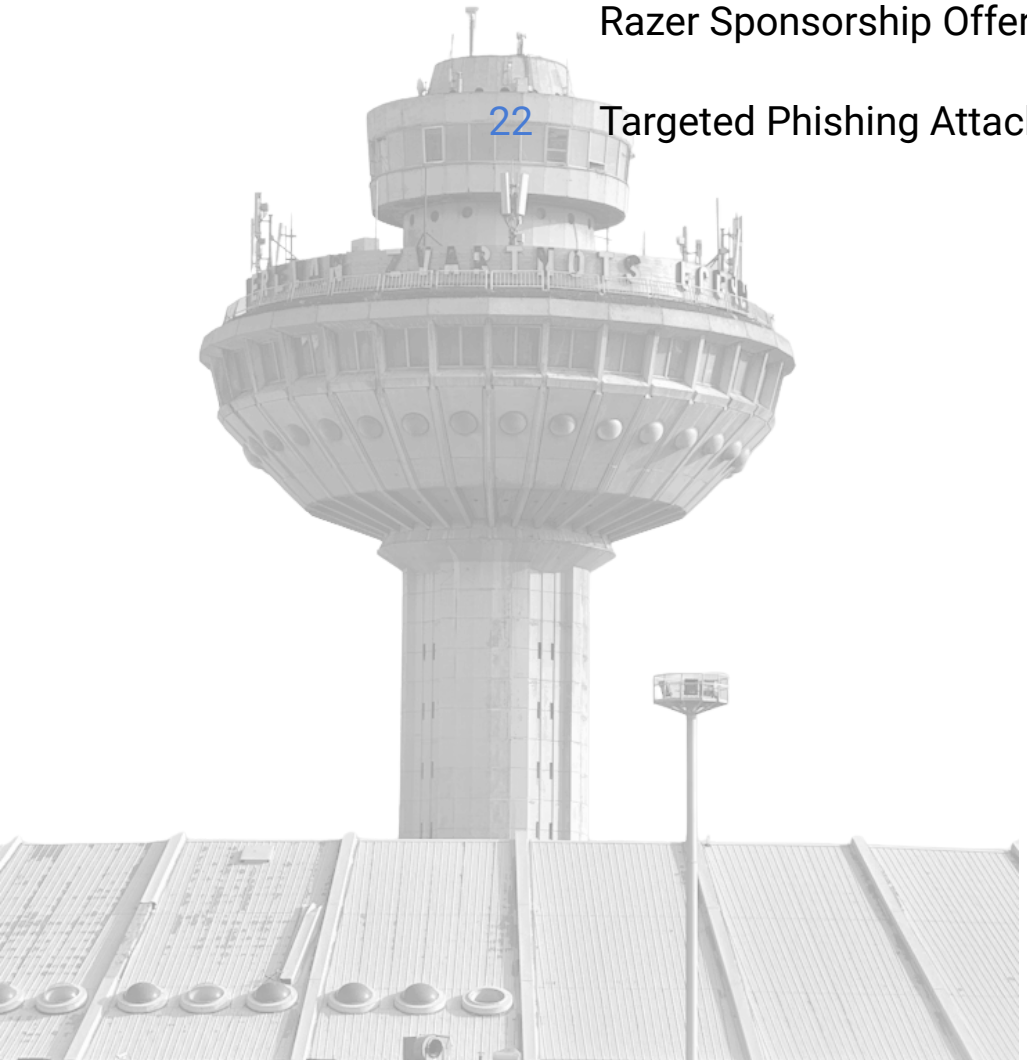
Website Hacks

Website hacks and defacements represent a significant and ongoing cybersecurity threat in Armenia, affecting various organizations, including civil society and media entities. These attacks often involve exploiting vulnerabilities in web applications, such as outdated plugins in content management systems like WordPress. Successful breaches can lead to attackers gaining administrative access, redirecting website visitors to malicious sites, or defacing the website content with propaganda or disruptive messages.

The impact of website hacks extends beyond immediate disruption, potentially causing financial losses, reputational damage, and a loss of public trust. Notable incidents include compromises of Armenian hosting providers running outdated software, leading to widespread website compromises, and regular targeting by foreign hacking groups, particularly from Azerbaijan and Turkey. The persistence of these threats underscores the critical need for continuous security measures, including regular software updates, robust vulnerability management,

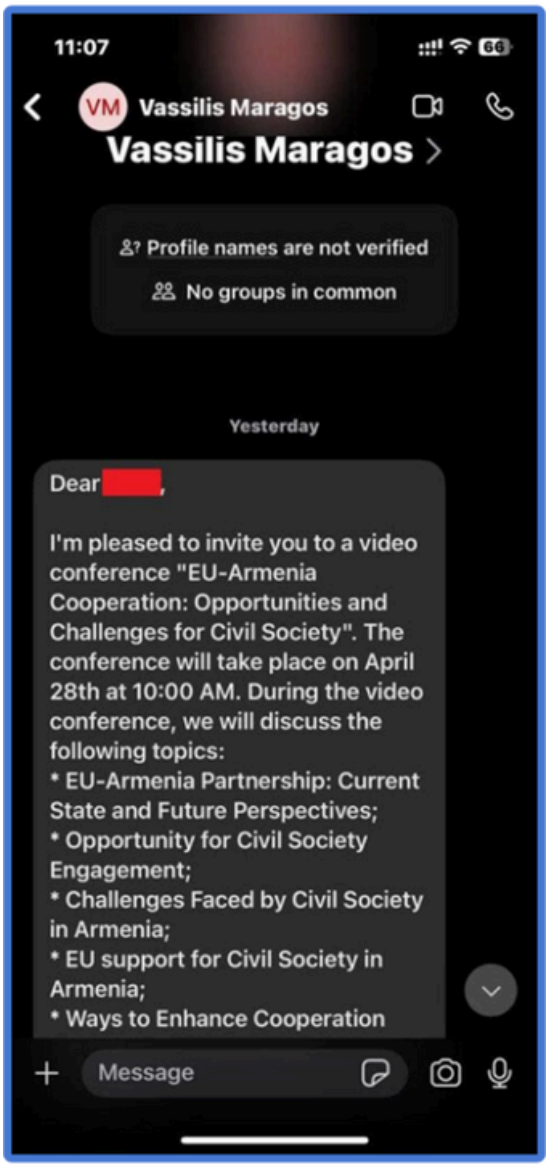
and employee training on secure online practices, to safeguard Armenia's digital presence from these prevalent cyberattacks.

Next



The case studies presented below highlight a sophisticated campaigns against Armenian civil society and HROs. We've observed increased activity of Russian APTs, as they used novel tactics to compromise and attack CSOs. By studying such cases, organizations and cybersecurity teams can learn to recognize evolving techniques, enhance their defense mechanisms, and foster global collaboration to combat cybercrime effectively.

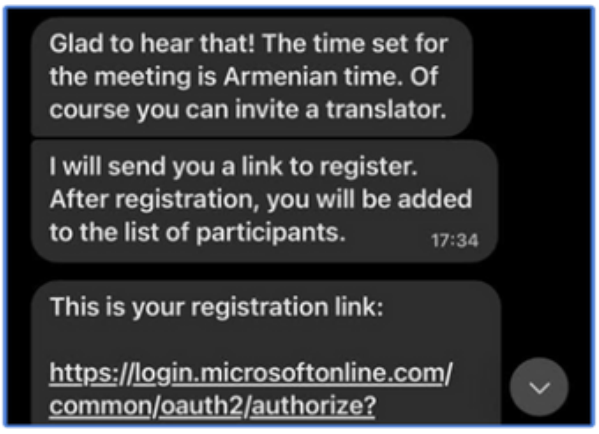
EU Delegation Impersonated in Targeted Attack Against Armenian NGOs



A sophisticated spearphishing campaign was identified targeting dozens of NGOs in Armenia on April 8th, 2025. The attackers impersonated Vassilis Maragos, the EU Ambassador and Head of Delegation in Armenia, initiating contact through **Signal messenger**. The phishing message, disguised as an invitation to a video conference titled "EU-Armenia Cooperation: Opportunities and Challenges for Civil Society," aimed to trick recipients into believing they were being invited to a legitimate event. The message specified that the video conference would take place on April 28th at 10:00 AM on the Microsoft Teams Video platform. Victims were instructed to agree to participate, upon which they would be registered.

The phishing attempt involved a malicious URL disguised as a Microsoft Teams meeting link. The message contained a link from a **legitimate Microsoft login page**. Once the targeted individual successfully logged in, the process would redirect to a separate browser window containing a **Microsoft authentication token**. The crucial step for the attackers was then to instruct the targeted individual to **copy and paste this new link (containing the authentication token) and send it back to the attacker** via Signal. This action would then trigger a **Microsoft Entra ID device joining process** on the victim's account.

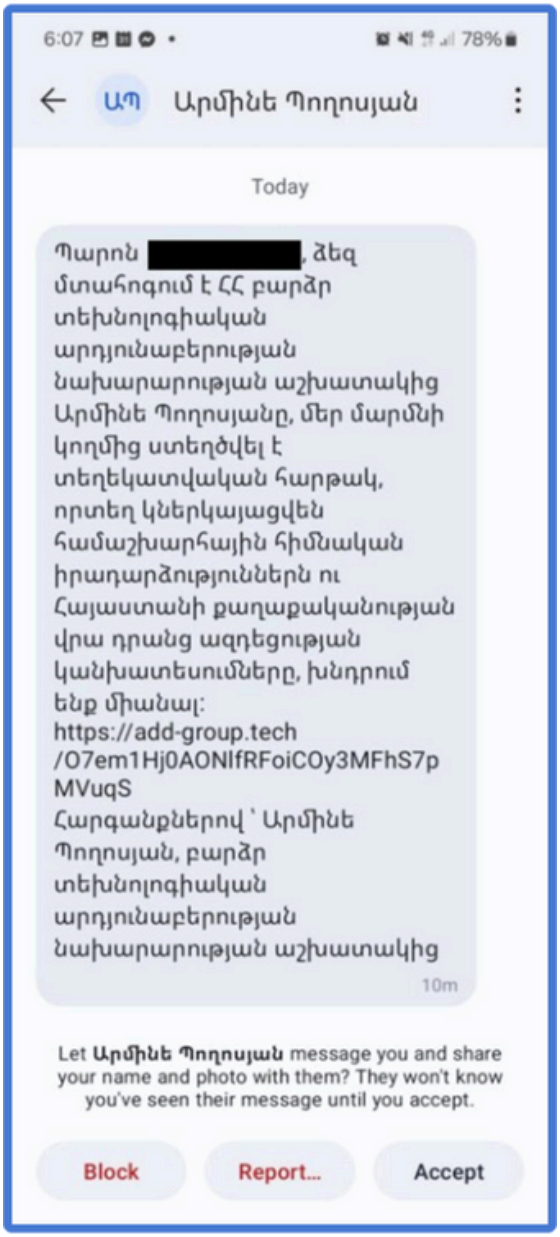
The attackers were able to successfully compromise at least one account belonging to a key Civil Society Organization (CSO) leader. The CyberHUB-AM team, working with the CSO's IT manager, provided incident response. During this process, they observed how the attackers successfully enrolled into the CSO leader's Microsoft Entra ID and tried to access it via **Microsoft Azure CLI**. The connections originated from the IP addresses: **95.182.124.124, 46.8.213.90, 188.130.142.95** all of which were identified as belonging to the cloud server provider **Biterika Group LLC, based in Russia**.



When the initial attack was thwarted by the incident response team, the attackers demonstrated significant persistence. They re-established contact via Signal, providing another link and instructing the victim to go through the procedure again. The attacker claimed, "I clarified, you did everything right, but for some reason it didn't work. You'll have to do the same thing again and IT will fix it," attempting to re-engage the victim and regain access.

Relation to Veloxity Reports: This incident strongly correlates with the advanced persistent threat (APT) activities and techniques detailed in recent Veloxity reports, particularly "Phishing for Codes: Russian Threat Actors Target Microsoft 365 OAuth Workflows" (April 22, 2025) and "Multiple Russian Threat Actors Targeting Microsoft Device Code Authentication" (February 13, 2025).

Spear Phishing in Armenia: Inside a Persistent Campaign by UNC5792



In early March 2025, CyberHUB-AM identified a targeted spear phishing campaign focused on individuals and organizations within Armenia's civil society and public sector. The campaign exhibited IOCs consistent with advanced persistent threat (APT) operations and has been attributed to **UNC5792**, a group previously identified by Mandiant.

The attackers impersonated an imaginary "Armine Poghosyan", who is supposedly "an employee" of Armenia's High-Tech Industry Ministry, using Signal to send messages inviting recipients to a purported "information platform" on global and Armenian political events. The core of the attack involves highly malicious, temporary URLs (initially on add-group.tech, then shifting to group-add.com), which are designed

to compromise the targets; notably, the attackers demonstrated real-time adaptability by providing a new, active malicious link on a different domain immediately after being informed that the initial URL had expired.

The phishing attempt was delivered via the **Signal** messaging platform, deviating from traditional email-based vectors and reflecting a shift toward secure, encrypted platforms for social engineering operations.

Three domains were observed as part of the infrastructure: add-group.tech, group-add.com, signal-groups-add.com. All 3 domains were assessed as malicious with high severity by VirusTotal and supported by intelligence from Mandiant and Google Threat Intelligence. All 3 were attributed by Mandiant to UNC5792.

Notably, these URLs were temporary in nature. Attempts to analyze the links in a controlled environment by CyberHUB-AM revealed that the original URL had already expired, indicating that the threat actor employed infrastructure designed for short-lived accessibility, reducing the window of opportunity for defenders to respond.

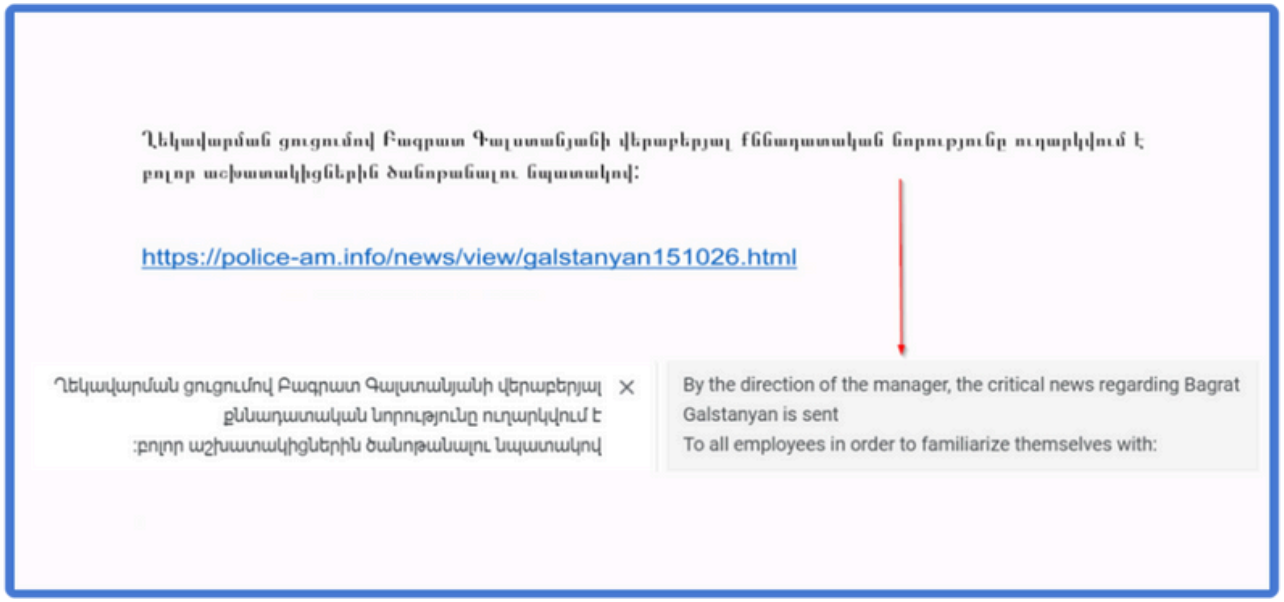
The incident also demonstrated **real-time adaptability**. When a targeted user—under the observation of investigators—informed the attacker that the original link had expired, a **new, functioning URL** was immediately provided. This behavior confirms that the attacker was actively monitoring communication and managing the phishing infrastructure in an agile manner.

Pastejacking Attacks in Armenia: A Growing Cybersecurity Threat

October 30, 2024 | Security researcher Simon Kenin has documented a specific type of cyberattack known as “Pastejacking,” targeting Armenia.

The attack is using the context of the recent political protests in the country and the name of the leader of the opposition protests Bagrat Galstanyan, a cleric of the Armenian Apostolic Church.

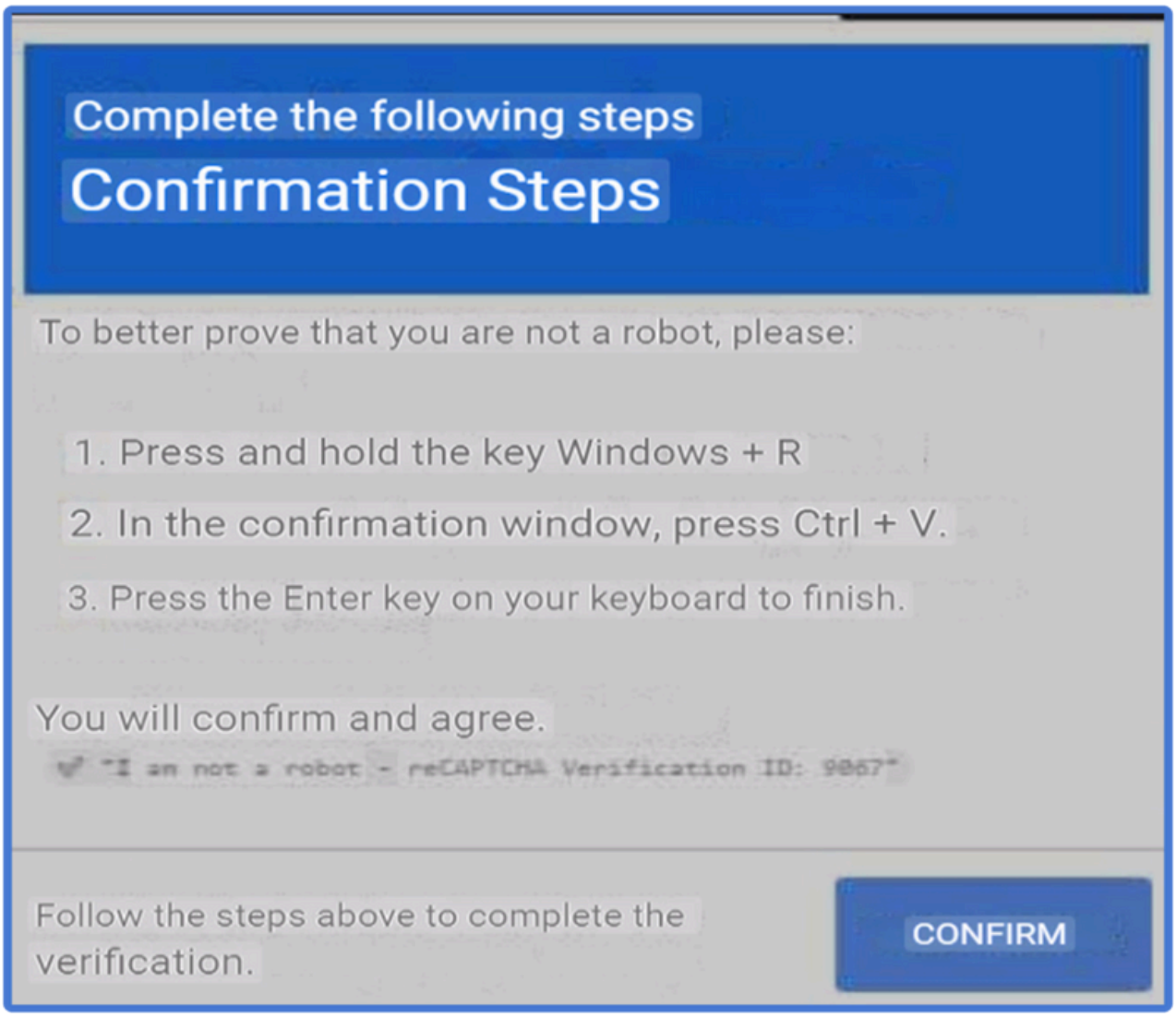
The researcher has found a word document written in Armenian which contains a link at the bottom:



Armenia — Screenshot from the blog-post of security researcher Simon Kenin, Yerevan, 30-Oct-2024

The link leads to a domain registered to look like the legitimate domain of the Armenian police. The domain has been registered this month — on 7th October, 2024, and is currently on-hold, apparently for being flagged as a phishing site. VirusTotal has some details, including some text scraped from the site, while it was still up and clearly showing keywords related to the Armenian Police.

Simon's blog-post is more helpful here as well. According to the researcher, opening the link used to lead to a captcha message in Armenian, which itself leads to the pastejacking attack itself.



Armenia — Screenshot from the blog-post of security researcher Simon Kenin, Yerevan, 30-Oct-2024

For the further details of the attack check out this link: https://k3yp0d.blogspot.com/2024/10/something-phishy-is-happening-in-armenia.html?lr=1730206198313.

What is Pastejacking?

Pastejacking is a cyberattack technique where attackers manipulate the content copied to a user's clipboard. When a user copies text from a malicious website, the clipboard content is replaced with something different, often harmful. This can lead to unintended actions when the user pastes the content elsewhere, such as in a terminal or a document.

For example, a user might copy a seemingly harmless URL or command from a website, but when they paste it, the content has been altered to execute a malicious command or redirect to a phishing site. This can result in unauthorized access, data breaches, or the installation of malware.

How Pastejacking Works

1. **Clipboard Manipulation**: Attackers use JavaScript to alter the clipboard content when a user copies text from a webpage. This script can replace the copied text with malicious commands or links.
2. **Execution of Malicious Commands**: When the user pastes the altered content into a terminal or command prompt, the malicious command is executed, potentially compromising the system.
3. **Phishing and Redirection**: The altered clipboard content can also redirect users to phishing sites, where attackers can steal sensitive information like login credentials.

Recommendations to Protect Against Pastejacking

4. **Be Cautious with Copying**: Avoid copying text from untrusted websites. If you must copy text, verify the content before pasting it.
5. **Verify Pasted Content**: Always double-check the content you paste, especially in sensitive environments like terminals or command prompts.
6. **Educate and Train**: Raise awareness about Pastejacking among employees and provide training on safe browsing practices.

By staying vigilant and adopting these protective measures, you can significantly reduce the risk of falling victim to Pastejacking attacks.

Phishing & Malware Distribution via Fake Razer Sponsorship Offer

Date: December 18, 2024
Target: Narek Kirakosyan, Armenian journalist
Threat Level: High (Level 1)
Reported by: CyberHUB-AM

Summary:
On December 18, 2024, a sophisticated phishing attack targeted Narek Kirakosyan, a well-known Armenian journalist. The attackers impersonated Razer Inc., a reputable gaming hardware company, to distribute malware through a fake sponsorship offer.

Attack Details:

- **Phishing Email**: The attackers sent an email from contact@razer-us.com, a domain impersonating the legitimate razer.com domain. The email body contained a detailed sponsorship offer, including links to supposed collaboration examples and a media kit.
- **Malicious Links**: The email included a shortened URL (https://bit.ly/RazerPromoKit) leading to a Dropbox-hosted malicious archive.
- **Malware**: The archive contained two malicious files:
  - msimg32.dll (SHA256: 693cc086089277f083b680ed822d988c2ea80483bd40caff202adccaa736bce4)
  - Razer – Contract and payment terms for partners on YouTube URL version.exe (SHA256: 08c7fb6067acc8ac207d28ab616c9ea5bc0d394956455d6a3eecb73f8010f7a2)

Indicators of Compromise (IOCs):

- **Email Source**: contact@razer-us.com
- **Email Destination**: narek.journalist@gmail.com
- **Fake Domain**: razer-us.com (Registered on December 12, 2024)
- **Mail Server IP**: 198.54.127.77
- **Hosting Server IP**: 198.54.118.220
- **Malicious File Names**:
  - msimg32.dll
  - Razer – Contract and payment terms for partners on YouTube URL version.exe
- **File Hashes**:
  - msimg32.dll (MD5: 0d61f3fe33123d0fdc20a7db2c969c4f)
  - Razer – Contract and payment terms for partners on YouTube URL version.exe (MD5: 4864a55cff27f686023456a22371e790)
- **VirusTotal Analysis Links**:
  - msimg32.dll
  - Razer – Contract and payment terms for partners on YouTube URL version.exe

Analysis:

The attackers leveraged social engineering techniques to craft a convincing phishing email, exploiting the journalist's interest in potential sponsorship deals. The use of a fake domain closely resembling the legitimate Razer domain added credibility to the attack. The inclusion of malicious files disguised as legitimate documents aimed to compromise the target's system upon download and execution.

Recommendations:

- **Email Security**: Implement advanced email filtering and phishing detection mechanisms.

- **User Awareness**: Conduct regular training sessions on recognizing phishing attempts and verifying the authenticity of emails.
- **Network Security**: Monitor network traffic for suspicious activity and block access to known malicious domains and IP addresses.
- **Endpoint Protection**: Ensure robust antivirus and anti-malware solutions are in place to detect and mitigate threats.

Targeted Phishing Attack on Armenian NGO

On May 28, 2025, CyberHUB-AM identified a sophisticated phishing attack targeting one of its NGO partners.

Dear Sir

Please find your formal invitation from the Republic of Armenia's Office of the Prime Minister attached.

VAHAGNKHACHATRYAN0-INVITATION-SCANDOC.PDF

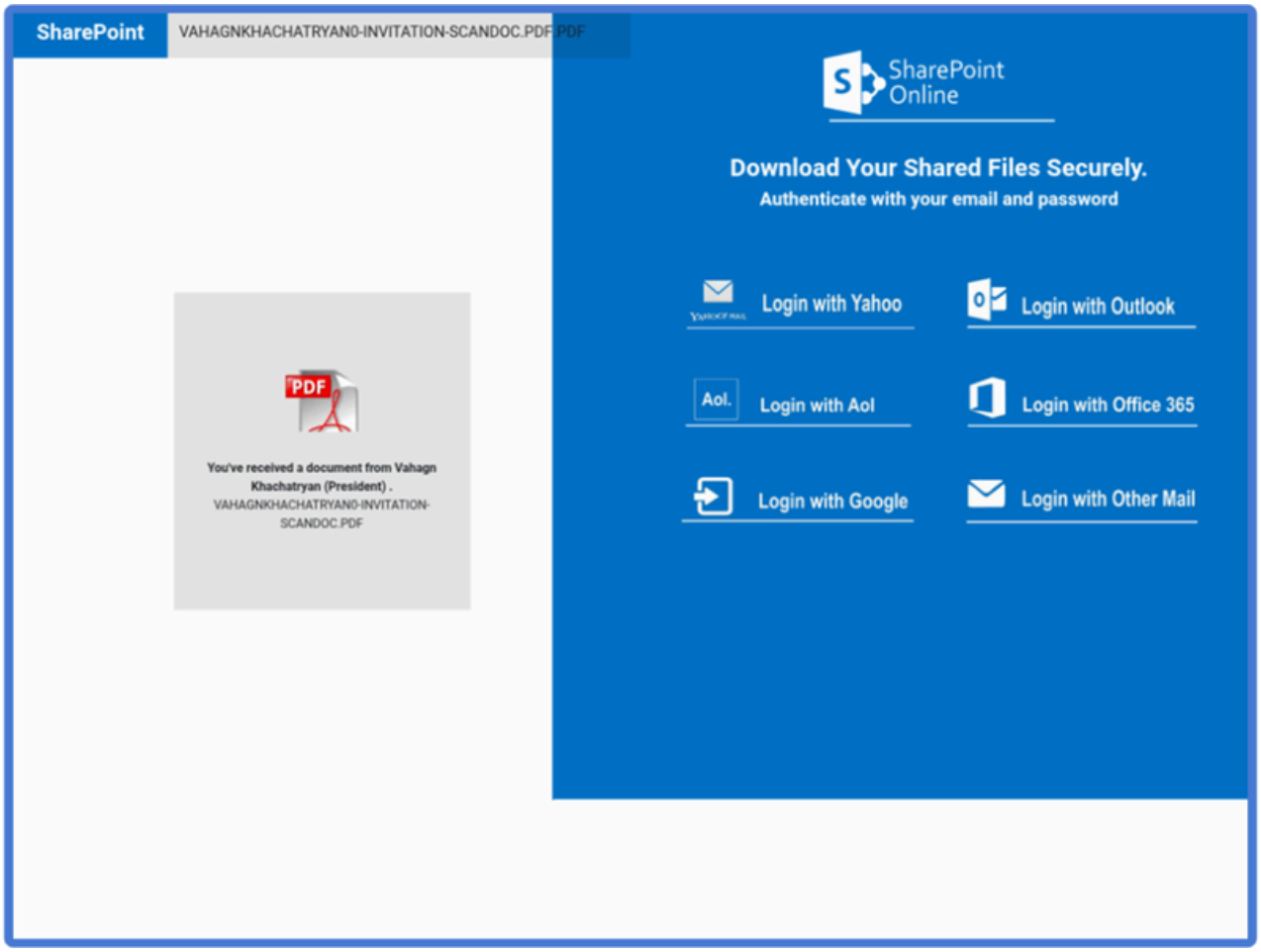
Regards

Arayik Harutyunyan

Chief of Staff (Armenia)
Address: Republic Square, Government House 1, 0010 Yerevan, Republic of Armenia
chief0fstaff@gov.am
Tel:(+374 60) 372109
Mobile:(+374 96) 030000

The attacker sent a phishing email with a PDF attachment link disguised as an official document—VAHAGNKHACHATRYAN0-INVITATION-SCANDOC.PDF.

The URL hxxps[://]snip[.]ly/l9xqzf redirected to a malicious GitHub Pages site (hxxps[://]asw910[.]github[.]io/ar[.]mernia[.]github[.]io/index[.]html) crafted to mimic legitimate content. Embedded JavaScript within the page (jquery.min.js) initiated a credential harvesting routine, forwarding credentials to a compromised endpoint: hxxps[://]wbbuffetchurrascobh[.]com[.]br/wp-admin/email[.]php.



Target

The attack was explicitly aimed at civil society—specifically an Armenian NGO—demonstrating the threat actors' strategic interest in advocacy organizations and regional politics.

Tactics, Techniques, and Procedures (TTPs)

Reconnaissance

- **Target Profiling**: The phishing lure was customized with Armenian president Vahagn Khachaturyan's name (VAHAGN KHACHATRYAN), it came on behalf of Prime Minister's Cheif of Staff, indicating prior knowledge or research.

Resource Development

- **Infrastructure Use**:
  - GitHub user asw910 (newly created) hosted the payload on GitHub Pages.
  - Redirect chain employed Snip.ly to mask the final malicious domain.

Delivery

- **Phishing Email**: Delivered via standard email channels, containing a socially engineered link to trigger curiosity and urgency—hallmarks of spear phishing.

Credential Access

- **Credential Harvesting**: Malicious JavaScript on the GitHub page captured submitted credentials and exfiltrated them using a POST request to a hijacked WordPress backend.

Obfuscation

- **Code Masquerading**: The phishing payload masqueraded as a common JavaScript library (jquery.min.js) to evade detection.

MITRE ATT&CK Mapping

- T1566.001 – Phishing: Spearphishing Attachment
- T1584 – Compromise Infrastructure
- T1204.002 – User Execution: Malicious File
- T1056.001 – Input Capture: Keylogging (via credential form capture)
- T1071.001 – Application Layer Protocol: Web Protocols

Lessons Learned

1. **Malicious Use of Reputable Infrastructure:** Hosting malicious content on GitHub and using a known link shortener (Snip.ly) demonstrates how attackers exploit trusted services to improve click-through rates and bypass filters.
2. **Targeted Civil Society Attacks**: The attack was not random. It reflects growing trends where politically motivated actors focus on NGOs, journalists, and activists, aligning with patterns described in various regional threat reports.
3. **Credential Capture via POST**: This common but effective technique underlines the importance of inspecting outbound POST traffic for anomalies, especially to foreign domains or unrecognized endpoints.
4. **Defensive Gaps**: Absence of URL filtering or user training enabled the victim to follow the malicious link. Organizations must prioritize layered security, including endpoint protection and DNS-based filtering.

Recommendations

- **Implement Domain-based Message Authentication (SPF, DKIM, DMARC):** To detect spoofed emails more effectively.
- **Block Access to URL Shorteners**: Unless whitelisted, to reduce click-through on potentially obfuscated URLs.
- **Monitor GitHub and similar repositories for lookalike domains:** As attackers increasingly abuse developer platforms to serve payloads.
- **Conduct Regular Phishing Simulations and Awareness Training:** Tailor campaigns to mimic current threat actor techniques.

Conclusion

This report underscores the evolving methods attackers use to exploit reputable infrastructures and highlights the growing threat to civil society. The discussed incidents and patterns emphasize the urgent need for improved defenses, user education, and proactive threat monitoring. By implementing the outlined recommendations, organizations can significantly bolster their security posture against targeted attacks.