Digital security incidents against the Armenian Civil Society in 2019 - 2020

MEDIA DIVERSITY INSTITUTE - ARMENIA www.mdi.am

Table of Contents

Introduction

This research aims to present the general trends in digital security and targeted cyberattacks against the Armenia civil society over the past two years, to take an in-depth look at some of the most prominent incidents and thus help the civil society better prepare for the future.

The data for this research was collected via the CyberHUB-AM digital support helpdesk, established by the Media Diversity Institute – Armenia in 2019.

CyberHUB-AM is an IT support hub and a Threat lab for the Armenian civil society — NGOs, Human Rights defenders, activists, journalists and independent media. It serves as a contact point and a help desk for the abovementioned groups in Armenia and collects, analyzes and, where appropriate, responsibly and anonymously shares incident data and threat indicators with the global threat intelligence community.

Media Diversity Institute – Armenia (MDIA) is a non-profit, non-governmental organization that seeks to leverage the power of the traditional media, social media and new technologies to safeguard human rights, help build a democratic, civil society, give voice to the voiceless and deepen the collective understanding of different types of social diversity. MDIA was established on April 18, 2006. Since 2018 MDIA has become more involved in Digital Security, technologies for exposing disinformation and misinformation and has provided IT audits, risk assessments, triage and security incident response to dozens of prominent Armenian Human Rights and media organizations, activists, journalists.

This research was implemented within the CSF Armenian National Platform Secretariat support to the ANP Working Groups' activities.

This research was produced with the financial support of the European Union. Its contents are the sole responsibility of the author and do not necessarily reflect the views of the European Union.

Definition of Terms

For the purposes of this research, we will define the **civil society** as non-governmental organizations [NGOs], community groups, civil initiatives, charitable organizations, faith-based organizations, professional associations, foundations as well as NGO-based media, freelance journalists and independent civil activists.

For the purpose of this research, we will define a **digital security incident** (or a **cyber incident**) as an attempt to breach (access without authorization) a computer, a computerized system, a network or an IT system preserved on mechanical data carrier, which has been done by violating the protective system and has affected the integrity or availability of the data, or the data has been copied, destroyed, isolated, or other substantial damage has been caused to the computer, a computerized system, a network or IT system[1].

For the purpose of this research, we will define a **cyber attack** as any attempt to damage, disrupt or gain unauthorized access to computer systems, networks or devices.

For the purpose of this research, we will define a **cyber threat** as information about malicious attempts to damage or disrupt devices, services and networks.

For the purpose of this research, we will define a **threat indicator**[2] as information about a behavior that is consistent with a threat.

For the purpose of this research, we will define a **threat actor** as a person or entity responsible for an event or incident that impacts, or has the potential to impact, the safety or security of civil society organizations and representatives.

[1] http://www.parliament.am/legislation.php?sel=show&ID=1349#9.24
[2] https://www.sans.org/reading-room/whitepapers/threatintelligence/triaging-alerts-threat-indicators-37945

General Context and the Threat Actors

The two-year period covered in this study was a period of great changes in Armenia, which went through a period of political turmoil following the 2018 velvet revolution, followed by the global pandemic of COVID-19 and above all, the 2020 Nagorno-Karabakh war and the post-war crisis.

Armenian Government

Starting from 2018, when the vocal opposition politician and former journalist Nikol Pashinyan swept to power as a result of the 'velvet revolution," the user data and content restriction requests from the Armenian authorities to Facebook increased significantly according to Facebook's Transparency report[3].

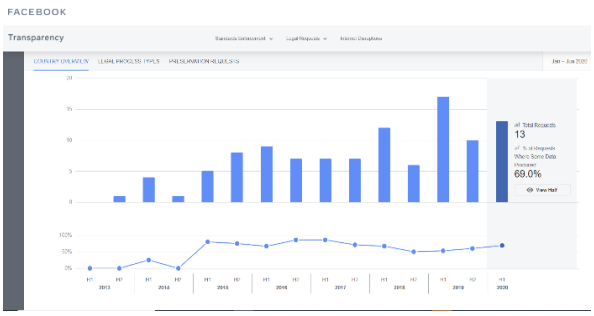


Figure 1

The incumbent authorities also demonstrated willingness to resort to threats and force to silence critics and descent.

In one such example, the Armenian Prime Minister Nikol Pashinyan directly instructed the National Security Service (NSS) to 'take action" against "fake Facebook users," who, according to him, deal in manipulations of public opinion.

One day after PM's call for action a Facebook user, writing under the pseudonym "Dukhov Hayastan" was detained for questioning[4]. Admittedly, the Facebook page was known for provocative publications, some of which could be seen as inciting hostility and hatred, as well as libel, defamation and fake news about PM Nikol Pashinyan, speaker of parliament Ararat Mirzoyan and other representatives of the ruling party[5].

On a related note, on January 5th, 2020 a Facebook user was detained for allegedly posting false information about Prime Minister Nikol Pashinyan's statements regarding the assassination of Iranian top military commander Qasem Soleimani under a fake Facebook account named "Դիանա Հարությունյան." The National Security Service said in a statement that the Facebook account 'threatened' national security[6].

On March 16, 2020 the Government declared a state of emergency, introducing a range of limitations for Armenian citizens[7]. The decision was approved at a special session of parliament dominated by members of Pashinyan's "My Step" alliance. Citing the need to prevent "panic-mongering", the government decided that media reports and posts in social media on some specific aspects of the COVID-19 related situation will have to reflect official reports, and that information reported "in violation of the provisions of this clause must be subject to immediate removal by persons who reported it."

[3] https://transparency.facebook.com/government-data-requests/country/AM
[4] https://www.azatutyun.am/a/29865315.html
[5] "Dukhov Hayastan" page admin affiliated with RPA - FIP.AM
[6] Host of "Diana Harutyunyan" Fake Facebook Page arrested: NSS (iravaban.net)
[7] "Armenia Declares State Of Emergency Over Coronavirus Outbreak," RFE/RL's Armenian service, March 2020, https://bit.ly/3peWrXx

The ban was implemented in a highly controversial manner, with police officers turning up at people's homes and demanding to delete social media posts and forcing media outlets to pull down articles. The whole process was qualified by local media watchdogs as disproportionate[8]. On March 24th the OSCE Representative on Freedom of the Media, Harlem Désir, expressed his concerns[9] about the situation in Armenia in the context of the fight against disinformation related to the COVID-19 pandemic.

Following the public outcry and the criticism of the international and local watchdogs, on March 25 the RA Government reviewed its March 16 decision and ended the disproportionate limitations of covering issues related to the coronavirus[10]. Issues, however, remained, as certain restrictions remained in place, for example it was required to publish official information without editing.

In a more startling move, the Armenian authorities launched[11] on March 24th a mobile app, which was supposed to allow a user to fill in a questionnaire "and receive a pretty accurate information about one's health." At close examination, however, it turned out that the app is built to track users' data[12]. Suren Krmoyan, Adviser to Deputy Prime Minister, has said[13] that the source code for the app was provided to the Armenian side by the Islamic Republic of Iran. It was translated and modified by Armenian specialists. The app was identified by several anti-virus engines as malware and was strongly criticized by privacy advocates. As a result, the Armenian government pulled it down and built a new app, which was made available on April 5th, 2020 and which was seen as a safer alternative.

Meanwhile, on March 31st the National Assembly adopted a bill, which gave the government the ability to track and process telecom data about all citizens, thus limiting the citizens' rights to the protection of personal data, privacy, freedom of communication. The decision to mass-track all the citizens was criticized by privacy advocates and human rights organizations, however, the authorities pressed on with its implementation. Starting from September 11, the State of Emergency on the territory of the Republic of Armenia was terminated, along with the legal provisions, which allowed mass-tracing citizens.

Representatives of the Former Administration

Armenian civil society also faces attacks from the representatives and supporters of the previous ruling elite, which have demonstrated that they are willing and capable of attacking the civil society organizations and human rights defenders, whom they blame for losing power following the 2018 Velvet revolution in Armenia.

In 2019 - 2020 there were targeted digital attacks against the civil society, while on November 10, after leaders of Armenia, Azerbaijan, and Russia signed an agreement to end fighting over Nagorno-Karabakh,

[8] The state of freedom of speech in Armenia, violations of the rights of journalists and the media 2020, 1st quarterly report, Committee to Protect Freedom of Expression, April 2020, https://bit.ly/3jP3faD

[9] "Coronavirus response should not impede the work of the media in Armenia, says OSCE Media Freedom Representative," OSCE, March, 2020 https://bit.ly/3khfWeq

[10] "Փոփոխություններ են կատարվել լրատվամիջոցների գործունեության առնչվող դրույթներում," Azatutyun.am, March, 2020, https://bit.ly/3pgtWbR

[11] https://www.aravot.am/2020/03/24/1102007/

[12] AC19.am հավելվածը վնասաբեր չէ, սակայն լրտեսական ծրագրերին բնորոշ հնարավորություններ ունի. վերլուծություն | CyberHUB-AM

[13] https://media.am/hy/verified/2020/03/25/20368/

an angry mob physically attacked[14] the Armenian branch of Open Society Foundations (OSF) as well as the Armenian service of Radio Free Europe / Radio Liberty (RFE/RL). In the case of the OSF attackers took away a DVR device, while in the case of the RFE/RL they tried to take away a server[15], but were forced to flee after RFE/RL journalists called the police.

The Threat from Russia

Russian hacker groups have shown interest in the Armenian civil society in the past as was the case of hacking prominent Armenian journalist Maria Titizian[16], who was among the 41 targets of the Fancy Bear cyber espionage group (aka APT28) in 2015, in the wake of the protests of "Electric Yerevan" over rising energy bills. APT28 was also active in Armenia on 2017, during a disinformation campaign spanning 39 countries and including Armenian civil society members, politicians, government and military targets[17].

In 2020 researchers from the security company ESET discovered[18] a watering hole (aka strategic web compromise) operation carried out by one of Russia's oldest cyberespionage groups – Turla[19] that was targeting several high-profile Armenian websites. Turla had compromised at least four Armenian websites, including one belonging to a civil society organization – the Armenian Institute of International and Security Studies. According to ESET telemetry, the following websites were compromised: aiisa[.]am: The Armenian Institute of International and Security Affairs, armconsul[.]ru: The consular Section of the Embassy of Armenia in Russia, mnp.nkr[.]am: Ministry of Nature Protection and Natural Resources of the Republic of Artsak, adgf[.]am: The Armenian Deposit Guarantee Fund. According to the researchers, the websites were compromised since at least the beginning of 2019.

Azerbaijani hackers

In 2020 the heaviest fighting in years between Armenian and Azerbaijani sides took place, which first started with the July 12 – 16 clashes in Tavush Province of Armenia, and continued through the September 27 - November 10 war in the disputed territory of Nagorno-Karabakh.

The war on the ground was accompanied by an intense cyberwar. In the months leading up to the war, as well as during the war itself, the Azerbaijani hacker forums and channels published breached data and documents from some of the most important Armenian government institutions and electronic systems, including the "Mulberry Groupware" electronic document management system, screenshots of hacked government websites, databases, footage from high-definition surveillance camera systems deployed in Yerevan and much more.

As a result of these successful Azerbaijani attacks, many government websites were defaced, breached or taken offline for extended periods of time.

[14] Երևանում Սորոսի հիմնադրամի գրասենյակի գործով ձերբակալվածներ դեռ չկան. գրասենյակը լուռ է (armeniasputnik.am)
[15] Demonstrators attack RFE/RL office in Armenia, assault 2 journalists - Committee to Protect Journalists (cpj.org)
[16] Russian hackers hunted journalists in years-long campaign (apnews.com)
[17] Tainted Leaks: Disinformation and Phishing With a Russian Nexus - The Citizen Lab
[18] Tracking Turla: New backdoor delivered via Armenian watering holes (eset.ee)
[19] Turla, Waterbug, WhiteBear, VENOMOUS BEAR, Snake, Krypton, Group G0010 | MITRE ATT&CK®

Occasionally NGOs and independent media websites also came under attack. And while those attacks were not specifically targeted at the civil society, but rather were attacks at everything Armenian, we have to consider the continuous threat from Azerbaijani hackers.

Other nation-state hackers

In April 2019 Cisco Talos, one of the largest commercial threat intelligence teams in the world, said they have found a highly advanced hacker group, likely backed by a nation-state, which they say has targeted 40 government and intelligence agencies, telecom firms and internet giants in 13 countries for more than two years.

The hacker group, which Talos calls "Sea Turtle" — an internal codename that ended up sticking —targets companies by hijacking their DNS. That allows the hackers to point a target's domain name to a malicious server of their choosing. The hackers gained access to the registrar that manages Armenia's top-level domains, allowing the group to potentially target any .am domain name. Talos wouldn't name the targets of the attacks nor name the registrars at risk, citing the risk of further or copycat attacks — and the researchers wouldn't name the state likely behind the group, instead deferring to the authorities to attribute[20]. But the researchers said Armenia, along with Egypt, Turkey, Sweden, Jordan and the United Arab Emirates were among the countries where it found victims.

So far no fresh research has been published about this attack and little is known about its possible targets, however, it is important for the Armenian civil society to be aware that yet another highly sophisticated state-backed hacker group has demonstrated interest in attacking the Armenian cyberspace.

[20] Cisco Talos Intelligence Group - Comprehensive Threat Intelligence: DNS Hijacking Abuses Trust In Core Internet Service

Analysis of Trends

In 2019 the Threat lab analyzed 32 digital security incidents, while in 2020 the number was 51. Looking at Figure 2 below, we can see that July 2020 and the period between September – November, 2020 were the months when most attacks were registered. This dynamic is clearly connected with the July 2020 clashes between Armenian and Azerbaijani forces in the Tavush region of Armenia and the September 27 – November 10, 2020 war in Nagorno-Karabakh.

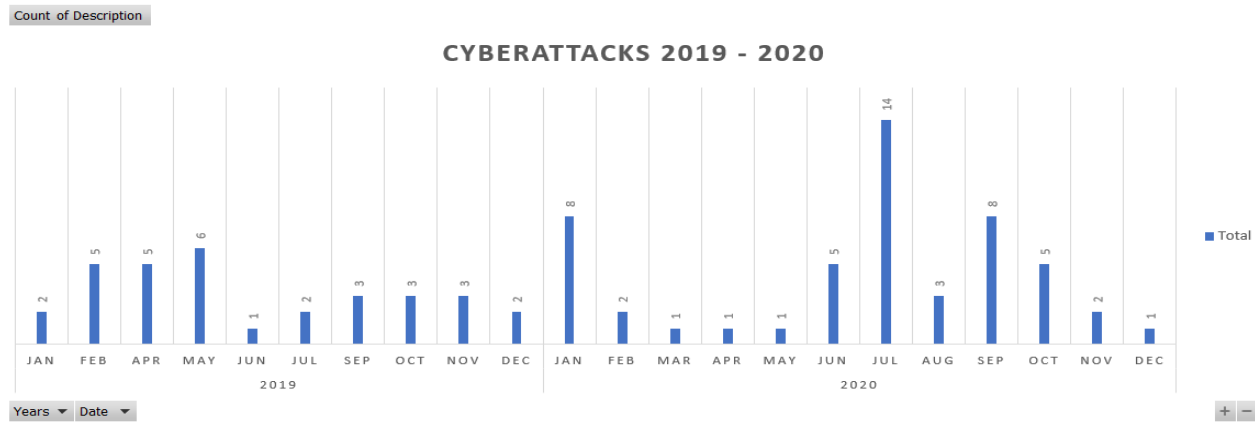


Figure 2

After the initial triage, we picked 16 cases for a more in-depth research in 2019, and 22 in 2020. The majority of the targeted attacks researched in 2019 were directed against NGOs, while in 2020 the media (independent media and NGO-based media) were the top target. (Figures 3, 4).

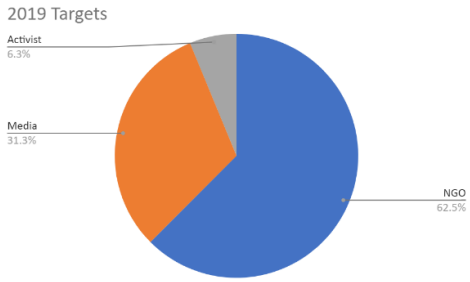


Figure 3

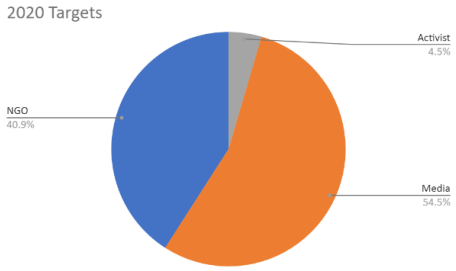


Figure 4

The following broad categories of attacks were observed in 2019 and 2020 against the civil society in Armenia:

- Website hacks (excluding DDoS) – we have included in this category hacks that involved penetrating web servers using exploits, vulnerabilities, misconfigurations, backdoors, etc.
- DDoS – included distributed denial-of-service (DDoS) attacks, in which hackers tried to overwhelm target servers or its network, infrastructure with a flood of Internet traffic, thus preventing legitimate users from getting to the attacked sites.
- Phishing – we encountered a number of attempts to obtain sensitive information or data, such as usernames, passwords or other sensitive details, by impersonating as a trustworthy entity in email spoofing, instant messaging.

- Email Hacks (excluding phishing) – we have grouped a variety of hacking techniques employed to break into target's email into this category, often involving brute forcing the passwords, using previously leaked passwords due to data breaches or trying password reset options.
- Physical attacks – attempts to break into an organization's offices and seize computers, servers, digital equipment.
- Malware – we encountered stalker-ware on an activist's android phone, as well as a case of trying to infect the target, an NGO leader with a malicious email attachment in the course of the research.
- Mass reporting, harassment – we have categorized the cases of cyberbullying, harassment, mass reporting social media profiles of NGO leaders, journalists, activists into this category.

Looking at the data, we can see that in 2019 the majority of the attacks were directed against civil society websites – 43%. If we include also DDoS attacks, which are essentially carried out with the same aim, the number is even more substantial and reaches 50.1% (Figure 5). We saw a big shift to phishing attacks and other types of attacks targeted at email in 2020 (Figure 6).

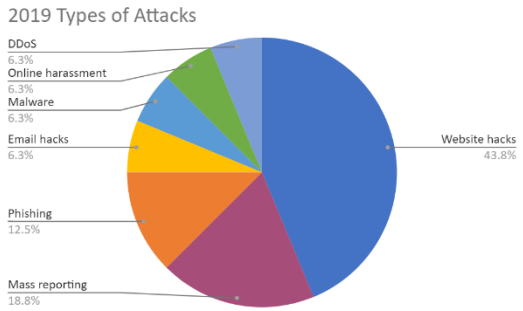


Figure 5

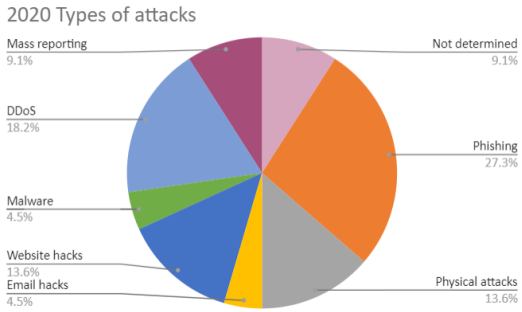


Figure 6

The phishing attacks in 2020 also grew more complex and included various messengers, Facebook and Instagram, social engineering.

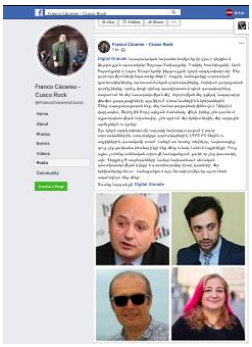
In case of the successful website hacks and email hacks (breaches) we found that human factor was often the blame: outdated CMSs and WordPress plugins, weak or reused passwords, lack of multifactor authentication, mixing work and personal accounts (email, social media). This in turn demonstrates a shortage of actionable policies and training, as well as insufficient level of IT capacity in the NGOs, independent media and activists.

NOTE: The year 2020 was characterized a by the emergency rule established since March 2020 to fight the COVID-19 pandemic, which was followed by Armenian – Azerbaijani clashes in July and September – November, which were accompanied by an intense cyberwarfare between Armenian and Azerbaijani sides. However, most of those attacks weren't specifically targeted at the NGOs, so we have not included those in this research.

Case Studies

Below we will try to present some of the cyber attacks that we have responded to throughout the research period. We will, of course, share only as much detail as we are authorized and are sure that will help other civil society actors, without further damaging the victims of those incidents.

HR Activists blocked on Facebook



From May 8th to May 14th the Facebook pages of the Programs Director at Union of Informed Citizens NGO Daniel Ioannisyan, Council Chairman of the Journalists' Club "Asparez" Levon Barseghyan and the director of the Women's Resource Centre in Yerevan Lara Aharonian were temporarily blocked on Facebook. In all the cases the profiles were mass reported as fake profiles and were recovered after contacting Facebook and submitting the required documents to prove that the profiles below were real persons.

May 17th a Facebook page, calling themselves "Digital Granate Civil Initiative" published a post[21], claiming that they are responsible for blocking 3 prominent Armenian civil activists and the political analyst Stepan Safaryan on Facebook. The post said its objective was "cleaning the internet from pro-Soros grant-suckers, foreign agents, corrupt politicians."

The activists' accounts were restored after submitting IDs to Facebook and going through the recovery process. The "Digital Granate Civil Initiative" page was taken down after a number of reports submitted by supporters and colleagues of the targeted activists.

As part of this research, we have contacted Facebook and asked for more data about the "Digital Granate Civil Initiative," but we haven't heard back.

Stalkerware on an environmental activists' phone

In November 2019 an Armenian environmental activist, who was actively involved in the protests against the gold mining project in Amulsar, on the border between the provinces (Marz) of Vayots Dzor and Sunnik, asked CyberHUB-AM to investigate a mobile phone, which the activist thought was compromised, because the threat actor had sent a screenshot from the phone and threatened the activist.

On December 15, 2019 CyberHUB-AM's Threat lab extracted three similar trojan Android packages (APK) from the victim's headset. These three samples were identified as members of the same malware family: MobileTool. This is a type of stalkerware[22], which is used to spy on the actions and data of the victim on their handset.

There are a number of versions of this malware observed in the wild. The entity which wrote the malware has a website and business presence and sells this trojan openly[23].

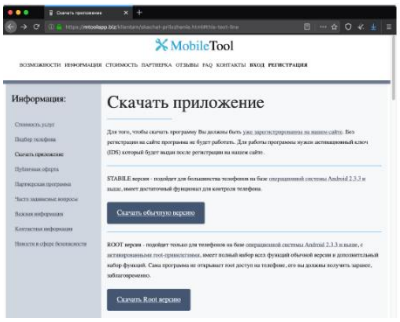
All three MobileTool samples are Android packages (APK). Each contains a DEX file with malicious code in the APK archive. The package names are made up of four random words, with each package name starting with the prefix "org.". These package names are listed in Table 1 below:

[21] "Digital Granate Civil Initiative" Facebook page, currently blocked, http://bit.ly/2XnDDZq
[22] https://stopstalkerware.org/about/what-is-stalkerware/
[23] hxxps://mtoolapp[.]biz/

Filename	Package Name
UTW022 Service_25.18.apk	org.dowser.freewill.rehinges.typp
UIAC Service_25.13.apk	org.westmost.poind.mispen.drolled
UCM46 Service_25.17.apk	org.baywood.wintles.unmatted.limp

Table 1: MobileTool Package Names

All three packages request a large set of permissions. The collection of permissions gives access to all user data, sms, logs, call logs, camera, microphone, and location. Dynamic analysis of the samples shows that they require a registration step after install. A dialog mentions registering on the developer's website for an "IDS". During this initialization process, the handset contacts two hostnames: ip.mobiletoolapp[.]com and apiru.mobiletoolapp[.]com. The second connection made during initialization is to port 2002 on hostname apiru.mobiletoolapp[.]com.



According to the open source, the website for the developer of MobileTool contains a number of clues as to the origin of malware. Additionally, a download link is provided for 6 the latest version of the malware (Figure 7).

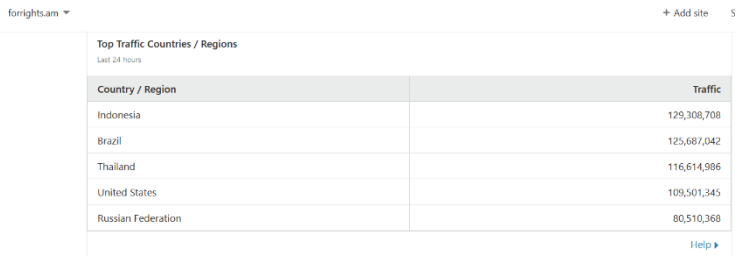
The page on the site with company information for "OEME-R Technology" mentions Minsk, which is located in Belarus. The official address of the company is shown to be located in Israel.

From the log of app activity on the phone we discovered that all three versions of the app had been downloaded and installed on the phone on September 13, 2019. This has been done bypassing the Google Play store. We were not able to find traces of remote control software on the phone, USB debugging was turned off, which indicates that perhaps the attacker had physical access to the device.

Also, from the log of internet consumption, it was clear that one of the versions of the app (UCM46 Service) had been consumed the most amount of traffic (1,33 GB), which explains how the attackers got hold of the screenshot from the phone we talked about earlier.

DDoS attack against Forrights.am

The website of Journalists for Human Rights NGO -- http://forrights.am, came under attack on December 12, 2019, which brought down the site for several days and forced the provider of its shared hosting to turn off the domain completely. The CyberHUB-AM team moved the site to a virtual private server (VPS) and put it behind the CloudFlare DDoS protection service on December 18, 2019, which allowed us to gain more visibility into the attack.



Already on December 19, 2019 it became clear that the attacker is using infrastructure in Indonesia, Brazil, Thailand, United States and Russia. The intensity of the attack was around 150k/RPS (150,000 requests per second) and continued till December 22, 2020 (for 10 days), until the DDoS mitigation and protective measures on the VPS rendered them mostly ineffective and the attacks stopped.

As is often the case with DDoS attacks, it is nearly impossible to attribute to a threat actor. However, the editor of Forrights.am has stated publicly that she has "substantiated suspicions" that the attack was ordered by one of Armenia's most prominent oligarchs. Incidentally, on the day of the attack Forrights.am published an article about a court case related to the Russian – Armenian tycoon Samvel Karapetyan.

Phishing Email Sent to Bloomberg Correspondent

Sara Khojoyan, a correspondent of Bloomberg News, received a phishing email containing malicious URL masquerading as a PDF attachment with a topical theme of information about cooperation between Armenia and China in November 2019.

The subject of the message was "Справка о перспектиквах сотрудничества РА с КНР.pdf" (Translation: Information on the prospects of cooperation between Armenia and China.pdf).

The email body had a phishing URL that was redirected via Google. This is almost certainly to prevent detection of the URL.

Redirector URL

hxxps://www[.]google[.]com/url?q=hxxps://files-shared[.]notification-node[.]online/viewer/view/?token=db01089dd48ee4a24b56c90e9c030f30&source=gmail&ust=1573718079186000&usg=AFQjCNEP_nOrw-wLoRBgdfkE2wyehQ-jgQ

URL

hxxps://files-shared[.]notification-node[.]online/viewer/view/?token=db01089dd48ee4a24b56c90e9c030f30

The file name in the email subject as well as in the body of the email were in Russian language. This email was sent from one Gmail account to the victim's account, also on Gmail. Opening the attachment was leading to a fake Google Drive login page.

Following passive DNS information from the phishing URL hostname, two IP addresses and four domains were revealed.

Hostname

files-shared.notification-node[.]online

IP Addresses

185.174.173[.]52	AS 21100 (ITL LLC)
185.174.173[.]36	AS 21100 (ITL LLC)

These four domains (notification-node[.]online, service-online[.]top, activity-service-online[.]site, activity-service[.]site) appear to be part of a single phishing campaign. Through a partner organization we learned

that the phishing campaign seems to have targeted several other journalists working in various CIS countries.

Hacking of Yahoo, Gmail and Facebook of the head of "Pahapan Foundation"

In January 2020 Inga Manukyan, the head of "Pahapan Foundation" asked to help recover her Facebook account and the Facebook page of “Pahapan Foundation”, which she lost access to because of a hack.

On close inspection it turned out that the attackers had first broken into Inga Manukyan’s Yahoo Mail by using an exposed password[24]. Since the Yahoo mail was used as a login option for Mrs. Manukyan’s Facebook account and as a password recovery option for her Gmail account, the attackers soon got hold of those accounts as well and changed passwords.

Tracing back the hacker using the data from account logs, notifications via email, an IP address and a location, as well as the attacker’s device were identified.

IP Address / Device / Location

103.255.4.86	Huawei P9 Lite Smart	Lahore, Pakistan

Thanks to the support of the CyberHUB-AM helpdesk team and our partners AccessNow, all the accounts were successfully recovered, although access to Facebook was restored only in May 2020.

[24] Every single Yahoo account was hacked - 3 billion in all (cnn.com)

Conclusions and Recommendations

- Armenian Civil Society faces diverse internal and external threats: political powers in Armenia – both governing and in opposition, Russian cyber espionage groups, Azerbaijani hackers, global cyber criminal gangs. Website hacks, DDoS, Phishing, Malware, cyber bullying, online harassment, misinformation, defamation, conspiracy are some of the most common types of attacks that the Armenian Civil Society faces.
- Armenian authorities and law-enforcement bodies have been demonstrating readiness to track and deanonymize critical voices, as well as resort to the use of malware and telecom data to trace internet users. The civil society needs to more vocally criticize the authorities to prevent its downward slide on the way of digital human rights and internet freedoms.
- In many cases, attacks succeeded due to the human factor: weak or reused passwords, lack of multifactor authentication, use of shadow IT at work, mixing work and personal accounts (email, social media). This in turn demonstrates that the civil society as a whole needs more digital security training.
- Recent cases of physical attacks on civil society organizations and media and the registered case of taking away a DVR device, as well as attempts to take a server, make it important for civil society organizations to include physical attacks in the list of their digital threats.
- Civil Society organizations should start developing their risk management systems and make sure that the top management is engaged in developing risk assessments, holding IT audits at their organizations

EASTERN PARTNERSHIP Civil Society Forum

Funded by the European Union

Media Diversity Institute Armenia

This research was implemented within the CSF Armenian National Platform Secretariat support to the ANP Working Groups' activities.

This research was produced with the financial support of the European Union. Its contents are the sole responsibility of the author and do not necessarily reflect the views of the European Union.