A DECADE OF EFFORTS TO KEEP INDEPENDENT AZERI MEDIA ONLINE

Qurium has been hosting Azeri media since December 2010, when online newspaper Azadliq (Azadlıq Qəzeti Azərbaycanın) was migrated to our hosting platform after being targeted by DDoS attacks. Since then a dozen media outlets and human rights organizations have migrated to our secure hosting infrastructure to seek protection against targeted digital attacks. For more than a decade, Qurium has monitored and mitigated a wide range of cyber attacks against the websites and since 2016, no less than twenty forensics reports have been released to document our findings.

Denial of service

When the Azeri media organizations reached out to Qurium in the early 2010s, they mostly suffered from website stability issues. Most of the newspapers were running old Content Management Systems (CMS) poorly maintained and with signs of targeted and non targeted intrusions. During those first years, the challenge was to deal with the frequent **denial of service attacks,** some of them lasting several days. The websites were frequently flooded during key events in the country by means of "**stress testing services**", third party **pay-as-you-go** services that provided means to overload the websites. The Denial of Service attacks were in the 100- 2000 Mbps range and very effective to take down any website that was hosted without technical means to scrub the traffic using specialized mitigation hardware worth tens of thousands of Euros. During five years (2010-2015), Qurium mitigated dozens of denial of service attacks against Azeri media, and was forced to invest in mitigation hardware and to increase its Internet capacity. Commercial mitigation of denial of service was not possible for Azeri media organizations as average cost for such services was close to 1,000 Euro/month for a small website.

Apart from investing in specialized hardware and capacity to fight Denial of Service attacks, a great part of our effort in those years was to trace the "stress testing services", report network Abuse to hosting providers and bring the services offline. During 2014-2016, several corporate efforts made Denial of Service more difficult for the attackers, both Cloudflare (2014) and later Google (2016) started to offer free protection to journalists and human rights groups and many stress testing services (aka "booters") since then were dismantled by FBI, such as the infamous VDOS Booter and the Mirai botnet.

After three years of research and development (2014-2017), Qurium built its own mitigation hardware and upgraded its Internet capacity by a factor of 200. Although the Denial of service attacks slowly had decreased since 2017, new challenges emerged. Internet Network Interference.

Internet Network Interference

Having denial of service attacks under control, forced the attackers to implement new strategies against the targeted sites. In late 2013, a new type of challenge emerged when we discovered that websites

artificially were slowed down. Instead of blocking the websites that clearly would expose the motivations and those responsible for the disruptions, the websites were slowed down by limiting the amount of bandwidth available to reach them. Qurium was forced to develop a method to detect "Internet Congestion" and to keep moving affected websites to other IP addresses to keep them online. Other large providers, such as Akamai, hosting other Azeri media was also slowed down and was unable to respond effectively to the challenge.

Exposing a coordinated cyberwar strategy

Not until 2017, Qurium could fully understand that there was a "cyberwar strategy" against the Azeri media sites we hosted. During that year, we received customized denial of service, pen testing and vulnerability scans and the first reports of targeted malware.

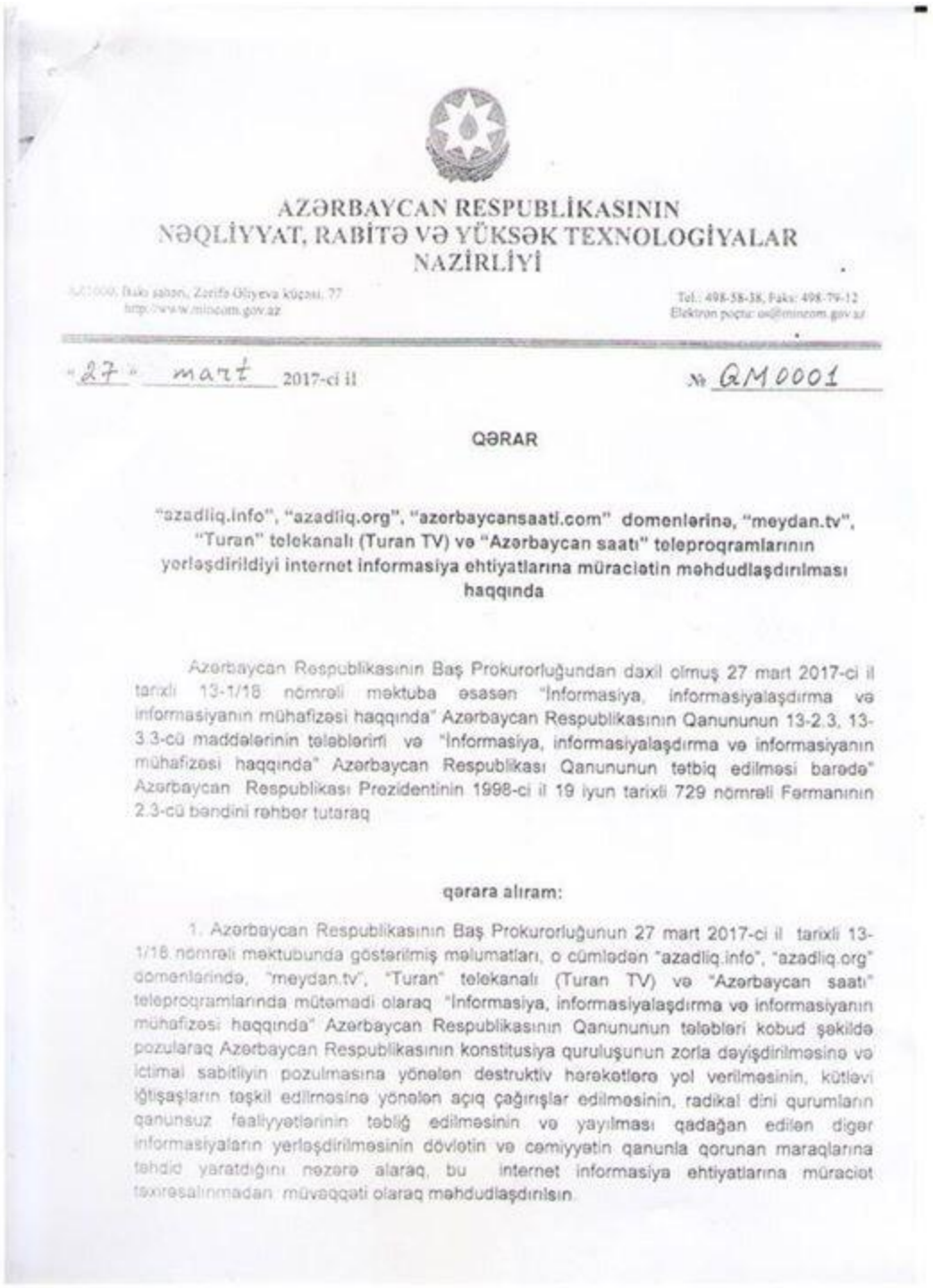
A series of diverse attacks and forensics analysis including tracing back the source of a malware sent to journalists helped us to confirm that the new **Ministry of Transport, Communications and High Technologies** and the "hacker community" built around the government, sponsored cybersecurity events were actively targeting our hosted media.

After hosting and protecting Azeri media for almost seven years, we had no doubt about the actors behind the attacks, and could publicly document that a "State Actor" was orchestrating diverse forms of cyber attacks.

Deep Packet Inspection

Despite all the efforts to bring down the media sites hosted with Qurium, the websites were steadily increasing in visitors and visibility in the country so new measures against them were needed. In April 2017, we identified that new technical means were implemented in several operators to block some of the websites. The Azeri authorities had invested in Deep Packet Inspection equipment to block the media outlets once and for all.

By the end of April 2017 Qurium learned that there was a court order against some of our hosted media organizations. To our surprise, the websites under Deep Packet Inspection were many more than the ones mentioned in the court order. The court order stated that the listed websites (Azadliq.info, Azadliq.org, Azerbaycansaati.com, Meydan.tv and Turan TV) were **"creating threats to the legitimate interests of the state and society"** and must therefore be blocked.



AZƏRBAYCAN RESPUBLİKASININ
NƏQLİYYAT, RABİTƏ VƏ YÜKSƏK TEXNOLOGİYALAR
NAZİRLİYİ

AZ1000, Bakı şəhəri, Zərifə Əliyeva küçəsi, 77
http://www.mincom.gov.az

Tel.: 498-58-38, Faks: 498-79-12
Elektron poçtu: ...@mincom.gov.az

"27" mart 2017-ci il № QM0001

QƏRAR

"azadliq.info", "azadliq.org", "azerbaycansaati.com" domenlərinə, "meydan.tv", "Turan" telekanalı (Turan TV) və "Azərbaycan saatı" teleproqramlarının yerləşdirildiyi internet informasiya ehtiyatlarına müraciətin məhdudlaşdırılması haqqında

Azərbaycan Respublikasının Baş Prokurorluğundan daxil olmuş 27 mart 2017-ci il tarixli 13-1/18 nömrəli məktuba əsasən "İnformasiya, informasiyalaşdırma və informasiyanın mühafizəsi haqqında" Azərbaycan Respublikasının Qanununun 13-2.3, 13-3.3-cü maddələrinin tələblərini və "İnformasiya, informasiyalaşdırma və informasiyanın mühafizəsi haqqında" Azərbaycan Respublikası Qanununun tətbiq edilməsi barədə" Azərbaycan Respublikası Prezidentinin 1998-ci il 19 iyun tarixli 729 nömrəli Fərmanının 2.3-cü bəndini rəhbər tutaraq

qərara alıram:

1. Azərbaycan Respublikasının Baş Prokurorluğunun 27 mart 2017-ci il tarixli 13-1/18 nömrəli məktubunda göstərilmiş məlumatları, o cümlədən "azadliq.info", "azadliq.org" domenlərində, "meydan.tv", "Turan" telekanalı (Turan TV) və "Azərbaycan saatı" teleproqramlarında mütəmadi olaraq "İnformasiya, informasiyalaşdırma və informasiyanın mühafizəsi haqqında" Azərbaycan Respublikasının Qanununun tələbləri kobud şəkildə pozularaq Azərbaycan Respublikasının konstitusiya quruluşunun zorla dəyişdirilməsinə və ictimai sabitliyin pozulmasına yönələn destruktiv hərəkətlərə yol verilməsinin, kütləvi iğtişaşların təşkil edilməsinə yönələn açıq çağırışlar edilməsinin, radikal dini qurumların qanunsuz fəaliyyətlərinin təbliğ edilməsinin və yayılması qadağan edilən digər informasiyaların yerləşdirilməsinin dövlətin və cəmiyyətin qanunla qorunan maraqlarına təhdid yaratdığını nəzərə alaraq, bu internet informasiya ehtiyatlarına müraciət təxirəsalınmadan müvəqqəti olaraq məhdudlaşdırılsın.

As a result of this new twist in the Azeri cyberwar strategy, that included enforcing blocking by legal means to all the operators, Qurium reacted by analyzing the traffic signatures of each Deep Packet Inspection (DPI) hardware enabled in the country so as to find means to circumvent the blocking.

The two year long research (2017-2019) resulted in the identification of DPI hardware from Allot Communications and Sandvine inside several operators in Azerbaijan.

As a countermeasure against the DPI hardware, Qurium built a new network architecture capable of making the blocking ineffective, forcing the providers and the government of Azerbaijan to contact the hardware suppliers for the necessary upgrades to handle our commitment to keep media online.

Qurium also developed "Bifrost" an anti-blocking service that mirrors blocked websites in Cloud storage services like Amazon S3 or Google Cloud Storage. The first version of Bifrost was developed as a result of the March 2017 blocking in Azerbaijan. Within no less than 11 days after Azadliq was blocked by DPI, a live mirror of the website was available to the Azeri readers. The mirror remains reachable today, more than four years after the initial blocking took place.

While improved Internet blocking became the trend of 2018 and was rolled out in all Internet service providers, Denial of service attacks never stopped. Our hosted partners were targeted by several attacks after publishing articles concerning the tensions between SOCAR and Palmani in 2018 or the real estate properties of the Aliyev family in early 2019.

Website floods continue

By 2018, many of the "stress testing services" often used to launch the Denial of Service attacks had been dismantled world wide. The attackers were forced to find new alternatives to conduct their traffic floods aiming to take the websites offline. During another forensic investigation we traced back this new source of denial of service to Russian Fineproxy (Region40). By identifying the service provider used to conduct the attacks, we could not only expose their business practices but also their management that kindly disabled the account of the attacker.

In late 2018, Denial of Service became a second priority in the strategy to harass Azeri media and once again other means were needed.

Hacking Team and Internal Affairs

During early 2020, phishing emails targeting journalists intensified, aiming to gain control of their social media accounts and to closely monitor their online communications. Thanks to the leaked files by Wikileaks in 2015, in which the Azeri Ministry of Internal Affairs showed interest to buy surveillance technology from "Hacking Team" and a leaked database of hacking forum "Nulled" we managed to trace back the phishing attacks to the online user **man474019** (sandman) and the the IP address **85{.}132.24.77** of the Ministry of Internal Affairs of Azerbaijan.

By April 2020, Qurium could finally link the denial of service attacks launched using Fineproxy service with the very same threat actor from the Ministry of Internal Affairs: sandman. Access to the sandman github account provided us with a good insight of the toolset that was being used against online media and journalists in Azerbaijan.

A final report of our findings showed even more advanced capabilities, like the ability to create fake SMS or hijack SMS sent to the journalists giving the attackers the ability to take control over their social media accounts.

Phishing remains a major attack vector against journalists and human right activists, the latest phishing campaign in early July 2021 impersonated human rights watch so as to implant a malware capable of recording the desktop and webcam or exfiltrate all important documents of the victims.

A decade dedicated to stop alternative voices in Azerbaijan

What started in 2010 and went on for years with Denial of service attacks using third party stress testing services was extended with more sophisticated attacks in 2017 including targeted phishing and the introduction of dedicated hardware to block the websites using technologies such as DART from Allot and PCEF from Sandvine.

The national blocking of many websites, not always supported by legal court orders, has been weaponized to limit visibility of the media in the country. Despite our multiple efforts to provide alternatives to make the content available, the blocking has had a huge impact in the revenue creation of the alternative media and the growth of readership.

After the introduction of Internet blocking by means of more sophisticated deep packet inspection against alternative websites in 2018, many of the blocked media opted to increase their presence in Facebook but that has proven to be an advantageous situation for the Azeri government and their secret cyber operations as Facebook has showed a bad track record in dealing with “coordinated inauthentic behavior” in the country.