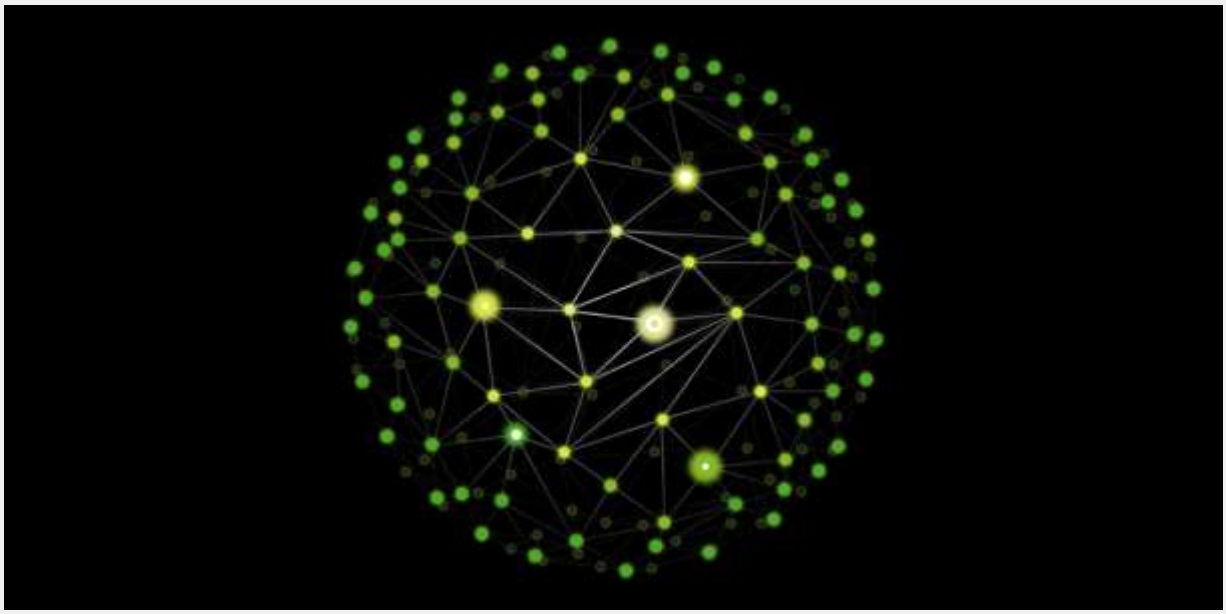
Deloitte.

MAKING AN IMPACT THAT MATTERS since 1845

Baku, Azerbaijan | Risk Advisory | 16 November 2020



Deloitte Cyber & Technology News digest

Issue #7

Azerbaijan

The official telegram channel of the Ministry of Defence has been launched

On October the official telegram channel of the Ministry of Defence of the Republic of Azerbaijan was launched.

Source: xeberler.az, October 1, 2020

Hacker attacks on government websites have been prevented

Attempts by hacker groups to attack 83 state websites are wrong. The statement was announced by the Centre for Combating Computer Incidents of the State Service for Special Communications and Information Security. Although DDoS attempts were made to attack these sites at 1-2 AM, each of these attacks was successfully prevented.

Source: xeberler.az, October 2, 2020

Hackers hacked the IT systems of Azerbaijan’s government

Security researchers from Cisco's Talos division have reported a vicious campaign in which hackers secretly hacked into the IT networks of the Azerbaijani government and gained an access to the diplomatic passports of some representatives.

Source: securitylab.ru, October 7, 2020

Azerbaijani users of Mail.ru are being "phishing" attacked

The Electronic Security Service under the Ministry of Transport, Communications and High Technologies has registered mass phishing campaigns against Azerbaijani users of Mail.ru e-mail service misleading users to download a file containing malicious software.

Source: xeberler.az, October 9, 2020

The number of e-signature users rose by 15 percent

In January-September of this year, 30,784 e-signature (e-İmza) certificates were issued by the National Certification Services Centre, which is 15% more in comparison to the beginning of the year.

Source: xeberler.az, October 12, 2020

Fake messages are sent on behalf of Azerbaijani banks

The Electronic Security Service under the Ministry of Transport, Communications and High Technologies has stated that the fake emails were sent on behalf of Azerbaijani banks. That emails were sent through proxy servers due to the attack of main servers by hackers. The appeal also notes that the Ministry of Finance of the Republic of Azerbaijan as well as the Central Bank call on citizens to withdraw funds from bank accounts in connection with alleged cyber-attacks.

Source: mincom.gov.az, October 12, 2020

"AzScienceNet"'s users have been victims of phishing attacks

Mass "phishing" attacks were registered against the users of the e-mail service of the "AzScienceNet" science computer network of the Institute of Information Technologies of ANAS (Azerbaijan National Academy of Sciences). According to the Institute of ANAS, the purpose of "phishing" attacks is to create fear and anxiety among the population by spreading disinformation as well as to use users' devices for malicious purposes by spreading their devices with malware viruses.

Source: xeberler.az, October 13, 2020

The Ministry of Transport, Communications and High Technologies warns citizens

The Electronic Security Service under the Ministry of Transport, Communications and High Technologies has stated that fake messages were sent on behalf of the Association of Banks of Azerbaijan via Telegram, WhatsApp and other channels. Adversaries were stating that Azerbaijani

banks have been subjected to cyber-attacks and until the Electronic Security Service under the Ministry of Transport, Communications and High Technologies investigates this issue, accounts are temporarily going to be frozen.

Source: mincom.gov.az, October 13, 2020

Fake messages are sent on behalf of the processing centre of Azerbaijan

On behalf of the Azericard processing centre, specious messages are sent to bank account holders regarding "transfer / deletion" under the fake name "Azericard". According to Azericard, these items are not related to Azericard and contain disinformation.

Source: xeberler.az, October 14, 2020

The ministry recommended the sites to reinforce the security measures

Attempts are being made by hackers to spread misinformation through cyber-attacks carried out using the security vulnerabilities of a number of news sites in our country. In this regard, the Ministry of Transport, Communications and High Technologies of the Republic of Azerbaijan recommends that the owners of all private Internet resources, especially news sites, strengthen appropriate security measures to prevent the insidious actions of the adversary.

Source: xeberler.az, October 15, 2020

Warning: threat of "phishing" attack

The "phishing" e-mail sent to users states that the Information Center of the State Agency for Citizen Services and Social Innovations under the President of the Republic of Azerbaijan has prepared a special training program for Foreign Ministry employees in order to protect against the growing cyber attacks. At the same time, in order to participate in the training, you will be asked to enter your corporate email and password. When a user logs in and provides information, that information falls into the hands of cybercriminals.

Source: mincom.gov.az, October 20, 2020

Fake emails are sent on behalf of the Deposit Insurance Fund

The fake letters sent to citizens by e-mail allegedly state that the Deposit Insurance Fund will be suspended from November 1, 2020 and the funds will be directed to the military needs of the state. The Electronic Security Service under the Ministry of Transport, Communications and High Technologies informs citizens that this information does not reflect the truth.

Source: mincom.gov.az, October 26, 2020

E-government developed hybrid classification method to detect articles related to terrorism

Methods of multi-purpose intellectual analysis of information belonging to citizens in the e-government environment have been developed. The main scientific-theoretical and practical issues are the analysis of the current state of e-government analysis technologies and problem

identification, the development of methods for classifying and filtering texts promoting terrorism, the development of methods for detecting and analyzing hidden social networks.

Source: xeberler.az, October 27, 2020

Fake emails are sent on behalf of the Ministry of Transport, Communications and High Technologies

The adversary sends "phishing" e-mails on behalf of the Ministry of Transport, Communications and High Technologies. Fake emails ask users to register and confirm their e-mails within 48 hours by accessing the link provided in the letter. Otherwise, those users will not be able to use their emails. In order to increase the reliability of the false letter, the text shall include the flag and coat of arms of the Republic of Azerbaijan, the logo of the ministry, the address and the name of the official. The purpose is to capture relevant information by distracting users, forcing them to access malicious links, and thus finding access to the equipment and network used by those individuals.

Source: mincom.gov.az, October 29, 2020

CIS

Russia

Russian SMB doubles spending on cybersecurity

Analysts of the antivirus company Kaspersky Lab conducted another survey, during which it was found that Russian small and medium-sized businesses have significantly increased their security spending.

Source: anti-malware.ru, October 1, 2020

IT companies offered the Ministry of Digital Affairs to install the Russian operating system on all computers

IT companies offered the Ministry of Digital Affairs to install the Russian operating system on all computers that will be sold in the country. This should not affect the stability of the devices, but will increase their price, experts said.

Source: securitylab.ru, October 6, 2020

Russian Union of Industrialists and Entrepreneurs: A bill banning modern encryption protocols for sites in the Russian Federation

Russia was concerned with bill that prohibits modern encryption protocols. Business believes it is tantamount to disconnecting from the global internet.

Source: securitylab.ru, October 6, 2020

Requirements of the Federal Security Service and the Ministry of Digital Affairs prevent the development of 5G networks in the Russian Federation

Federal Security Service and the Ministry of Digital Affairs require the installation of domestic crypto protection on 5G network equipment for certification of base stations and smartphones. However, the manufacturers of this equipment do not intend to modify the devices for local requirements..

Source: securitylab.ru, October 8, 2020

The largest Russian IT-associations complained about the collection of data from Muscovites

According to the decree of the mayor of the capital, the Moscow authorities obliged employers to provide the numbers of mobile phones, cars and transport cards "Troika" of employees who switched to remote working. IT associations consider it illegal to collect and transfer personal information to third parties without the consent of employees.

Source: securitylab.ru, October 13, 2020

In 2020, theft from the accounts of Russians doubled

As the Prosecutor General's Office calculated, every fifth case of theft in Russia falls on the theft of funds from a citizen's account. In comparison with 2019, for eight months of 2020, there were twice as many similar incidents.

Source: anti-malware.ru, October 13, 2020

Norway accused Russia of cyberattack on the country's parliament

Norway blames Russia for the hacker attack on the Storting (national assembly) email system, the country's government website says. The message of the Ministry of Foreign Affairs does not specify whether the accusation is linked to Russian government agencies or to hackers - Russian citizens.

Source: securitylab.ru, October 14, 2020

Insiders account for 60% of data leaks in Russia

This year, 91% of Russian companies have already faced a leak of a client base, financial documents or personnel data. In the overwhelming majority of cases, the information was leaked through the fault of the employees themselves, moreover, 60% of incidents were the result of intentional actions, the rest - inattention or non-observance of basic safety rules.

Source: anti-malware.ru, October 16, 2020

Sberbank warned Russians about fraudulent calls from "prosecutors"

Sberbank warns Russians about new tricks of fraudsters who are now hiding behind the prosecutor's office. By talking to the victim on the phone, he is persuaded to transfer money to a special account.

Source: anti-malware.ru, October 16, 2020

66% of Russians allow collection of personal data to fight COVID-19

Most Russians agree to provide their personal data to the authorities if it helps to fight the spread of the coronavirus infection COVID-19.

Source: anti-malware.ru, October 19, 2020

Russian government agencies were told how to switch to domestic crypto communication

The government of the Russian Federation has published recommendations for the transition of state services to the use of domestic methods and means of encryption.

Source: anti-malware.ru, October 19, 2020

Moscow authorities will spend 155 million rubles on mass surveillance of citizens

Within six months, 220 hardware and software complexes will be placed at public transport stops to collect MAC addresses of user devices and track pedestrian movement along them.

Source: securitylab.ru, October 20, 2020

Sberbank creates a system to track transactions and movement of Russians

Sberbank is developing a geo-analytics service for businesses and regional authorities that will analyze banking transactions of Russians and compare them with information about the physical location of retail outlets.

Source: securitylab.ru, October 20, 2020

Yandex for the first time published a report on government requests for user data

The Russian multinational company Yandex for the first time published a report on transparency, in which it spoke about the number of requests from government agencies for user data.

Source: securitylab.ru, October 26, 2020

Russian phone scammers switch to auto-dialing

Telephone fraud with the use of robotic programs for initial calls is gaining popularity in Russia.

Source: anti-malware.ru, October 27, 2020

Sverdlovsk scammers stole 1 million rubles from the bank using a unique scheme

The group was allegedly engaged in theft of funds from one of the Yekaterinburg banks by unauthorized debiting of funds to pay for gasoline at gas stations in Yekaterinburg and the Sverdlovsk region.

Source: securitylab.ru, October 28, 2020

Phishers sharply increase the number of attacks on Russian banks

Russian credit institutions are sounding the alarm: the number of phishing attacks on employees' mailboxes has recently grown significantly.

Source: anti-malware.ru, October 28, 2020

Kazakhstan

Hackers look to amass browser passwords

The integrated e-mail gateway has linked multiple mailings containing malicious software to government agencies. They were blocked by software and not delivered to final recipients.

Source: profit.kz, October 5, 2020

Kazakhstanis lose an average of 12 thousand tenge due to cyber fraudsters

Kazakhstan has seen an increase in fraudster activity through e-mail, SMS, social networks, instant messengers and especially telephones. Bank card holders careless sending bank details by messenger or bank card photos in chats are also suffering.

Source: profit.kz, October 5, 2020

Cyber incident response services to appear in Kazakhstan banks

The Kazakhstan Agency for Financial Market Regulation and Development has introduced a requirement from 1 January 2021 that Kazakhstan banks launch a special service for responding to cyber incidents.

Source: profit.kz, October 6, 2020

Dangerous AVEMARIA family virus attacks Kazakhstan

During the monitoring of the Kazakhstan segment of the Internet, the Computer Incident Service of the State Technical Service (KZ-CERT) registered the document with a suspicious attachment. KZ-CERT experts have identified this document as malware. KZ-CERT experts have determined that the

malware software file belongs to the AVEMARIA family and is designed to track information and record user keystrokes. The software collects information on email and social media credentials, as well as data from online banking applications, etc.

Source: profit.kz, October 14, 2020

Kazakhstan cybersecurity appreciated in the international arena

The Cybersecurity Alliance for Mutual Progress held its fifth annual conference from 14-20 September 2020 to discuss information security issues and analyse the most significant information security incidents in 2019-2020.

Source: profit.kz, October 19, 2020

List of sites safe for children to be developed in Kazakhstan

Deputy Chair of the Kazakhstan Committee for the Protection of Children's Rights Yulia Ovechkina says Kazakhstan will have developed a list of safe sites for children by the end of the year.

Source: profit.kz, October 19, 2020

Internet fraud in Kazakhstan: thousands of cases remain unsolved

Cases of Internet fraud have been growing recently. Most remain unsolved due to the complexity of investigations.

Source: profit.kz, October 21, 2020

Kazakhstani wallets targeted by scammers

This October saw the number of requests to check suspicious Internet resources increase. Earlier, KZ-CERT had already warned about the risk of data leakage in the field of e-commerce. Experts have developed recommendations to protect the bank card information of Kazakhstanis.

Source: profit.kz, October 26, 2020

UAPF warns Kazakhstanis about fraudsters

The Unified Accumulative Pension Fund has warned contributors and recipients of fraudulent offers to provide individual pension account statements for a fee have become more frequent in social networks and messengers.

Source: profit.kz, October 27, 2020

UAPF website interruptions: Kazakhstanis check pension savings

The number of Unified Pension Savings Fund statement requests on the eGov website has increased fivefold, leading to pension fund portal overloads.

Source: profit.kz, October 27, 2020

Low detection rate of Internet fraudsters in Kazakhstan explained

The Deputy Head of the Criminal Police Department Yerlan Omarbekov announced at a department briefing that the internal affairs bodies had solved 1.7 out of 8.3 thousand cases of Internet fraud in 2020, detaining about 400 people. The number of Internet crimes increases with the development of cyberspace.

Source: profit.kz, October 27, 2020

Kaspi experiences "technical issues"

On 28 October, the Kaspi.kz payment system suffered a serious failure leaving customers without access to financial transactions and card payments, unable to withdraw or pay in cash at ATMs, or make payments and transfers. No official reasons for the system failure have been given, but bank representatives are promising to restore normal service as soon as possible.

Source: profit.kz, October 28, 2020

Kyrgyzstan

Parliament website hacked in Kyrgyzstan

The Kyrgyzstan parliament announced that its official website had been hacked, with the perpetrators demanding $ 10,000 in ransom.

Source: securitylab.ru, October 19, 2020

Uzbekistan

CCTV cameras to identify anyone violating mask regimes in Uzbekistan

According to the Regional Department of Internal Affairs' press service, the Fergana region has launched a pilot photo and video programme to identify people not wearing masks.

Source: profit.kz, Octoer 19, 2020

Uzbekistan plans to join PayPal

Uzbekistan Minister for the Development of Information Technology and Communications Shukhrat Sodikov, has announced that Uzbekistan, the only Central Asian country not yet connected to the PayPal money transfer system, will soon be joining the system.

Source: profit.kz, October 28, 2020

Mongolia

Use of electronic signatures discussed in Mongolia

Mongolia's Standing Committee for Innovation and Electronic Policy discussed the use of electronic signatures and official correspondence between government agencies.

Source: profit.kz, October 7, 2020

Turkmenistan

Access to Yandex and Google blocked in Turkmenistan

The search, mail and news services Google and Yandex opened on 5 and 6 October with varying success. Yandex was down come evening time, while mobile communication VPNs and Wi-Fi, including paid options, had been blocked.

Source: profit.kz, October 8, 2020

MAKING AN IMPACT THAT MATTERS since 1845

deloitte.az

25E Nobel Avenue,
Baku, AZ1025, Azerbaijan