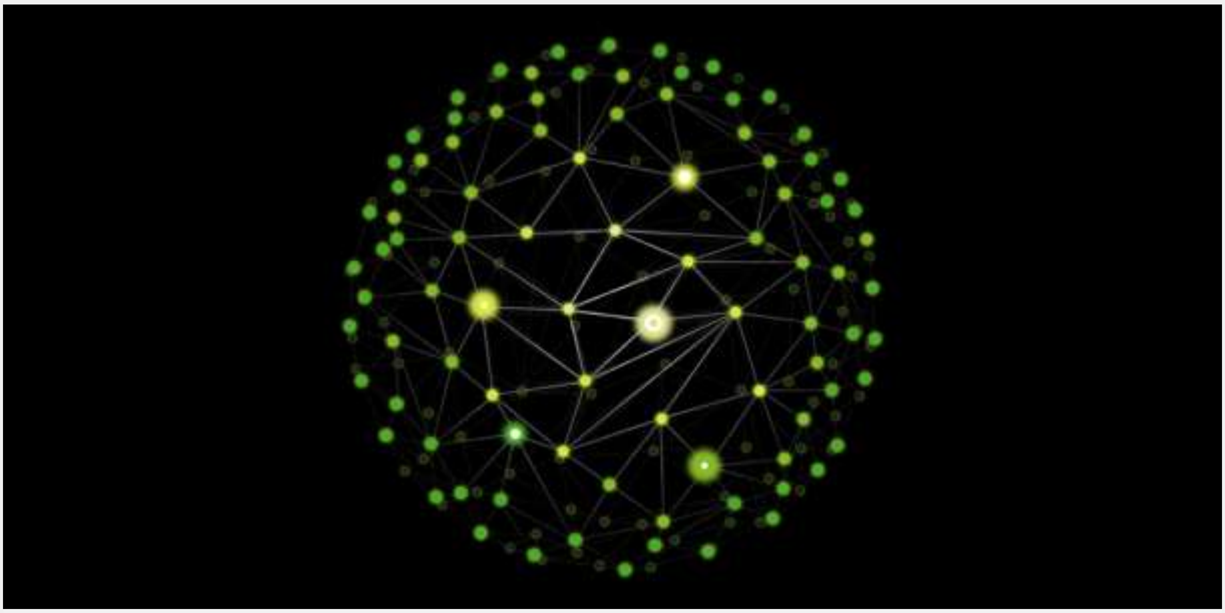
Deloitte.

MAKING AN IMPACT THAT MATTERS since 1845

Azerbaijan | Risk Advisory | 17 June 2021



Deloitte Cyber & Technology News digest

#13

Azerbaijan

A number of Azerbaijani government agencies do not have data system development policies

According to a report on audit chamber activities for 2020, many government agencies in Azerbaijan do not have medium-term strategic documents or policies outlining investment directions associated with data system development. The report also notes that data system management covers operational levels and is more technical support focused.

Source: xeberler.az, April 5, 2021

Biometric signatures will be used in Azerbaijan

Work is underway in Azerbaijan to introduce biometric signatures, which is a new recognition technology that will replace e-signature cards and tokens in the future. It will allow users to authorise documents using individual biometric data such as fingerprints, eyes and so forth. The

SHA-1 cryptographic algorithm, which currently provides digital signature security, is being replaced by the more secure SHA-2.

Source: xeberler.az, April 19, 2021

The Electronic Security Service once again warns of "phishing" attacks

The Electronic Security Service is warning the public about “phishing” attacks targeting banks in recent days. Cybercriminals are attempting to seize bank and other personal details by abusing technical support services in Azerbaijani banks. The scheme involves mobile numbers being called on behalf of bank employees, and any transfer is made in their name, requiring a card account number, password, confirmation code and other personal details.

Source: cert.az, April 20, 2021

Another Azerbaijani bank due to activate an e-signature service

Rabitabank is expected to activate an e-signatures service for its customers. The bank has made a request to the State Tax Service and hopes to be able to “offer about 10 digital solutions and products this year, which are currently being actively worked on”.

Source: xeberler.az, April 21, 2021

More electronic fraud revealed in Azerbaijan

“Attention! The next page, which was used by fraudsters to seize contact information, deceive them and seize card information, has been exposed”, the State Service for Special Communications and Information Security - Centre for Combating Computer Incidents reports. According to the information, scammers are trying to deceive the public by creating the following type of website: https://azerdostavka.shop/. The website is not currently active.

Source: xeberler.az, April 23, 2021

State Service: The new version of WhatsApp steals your personal data

A new version of WhatsApp called WhatsApp Pink has appeared and is gaining popularity according to the Centre for Combating Computer Incidents of the State Service for Special Communications and Information Security. The report also says that WhatsApp Pink is a completely malicious application: "This malicious APK is spreading through WhatsApp groups in the form of links." WhatsApp Pink first asks for your registration information and then steals your personal data.

Source: xeberler.az, April 28, 2021

Cybercriminals create fake pages similar to Azerpocht's official website

The Electronic Security Service is warning the public about fake websites opened in the name of Azerpocht, claiming a group of cyber-fraudsters has been creating fake websites similar to the official Azerpocht website to obtain funds illegally. Their target is anyone selling items online. The cyber-fraudsters, acting as buyers, write to the sellers from fake WhatsApp numbers and ask them to enter their card details on a fake site made to look like Azerpocht to make payment. Once the seller logs on and provides his or her card detail, the funds on the account balance fall into the hands of cyber-fraudsters.

Source: xeberler.az, April 28, 2021

Azerbaijan's first antivirus software presented

A first "beta" test version of a pest analysis application is ready after a long period of development. The statement came from the State Service's Centre for Combating Computer Incidents.

Source: xeberler.az, April 30, 2021

An "Electronic prosecutor's office" information system to be created in Azerbaijan

An "electronic prosecutor's office" information system will be created to ensure the application of modern information and communication technologies in the activities of the Azerbaijani prosecutor's office.

Source: xeberler.az, May 8, 2021

Azerbaijan has developed a five-year cyber security strategy

Azerbaijan is expected to approve a national strategy for information and cyber security covering 2021-2025. The statement came from the Ministry of Transport, Communications and High Technologies. According to the report, the action plan for the implementation of this strategy also includes provisions for improving the legislation in this area.

Source: xeberler.az, May 14, 2021

42% of computers in Azerbaijan still use Windows 7

According to Kaspersky statistics, 42% of computers in Azerbaijan still have Windows 7 installed, which ended in January 2020. An outdated version of the operating system may work well, but it is easier to attack if it is no longer supported. At the end of the system's life, vulnerabilities remain, and patches are not released for them, making it easier for attackers to gain access to information. The share of Windows 7 users among home users is 48%, among small and medium entrepreneurs - 14%, and among micro-businesses - 30%. It is especially important for small businesses to keep their operating systems up-to-date, as they do not have separate resources to combat cybersecurity.

Source: xeberler.az, May 17, 2021

The fight against online fraud and cyber threats is intensifying

A new, improved and more functional version of the Blacklist.gov.az project, created by the State Service for Special Communications and Information Security, has been launched. According to the Center for Combating Computer Incidents, the project aims to strengthen the fight against online fraud and cyber threats in the country, to expose the collection of domain names used in cyber-fraud and cyberattacks, as well as protective extensions for web browsers, API integration to protect internet users.

Source: xeberler.az, May 24, 2021

CIS

Russia

Fraudsters using “Yandex.Money” to deceive Russians

The classic mechanism for getting hold of bank card details in Russia through malicious emails is experiencing a rebirth. Scammers, posing as Yandex.Money e-wallet operators, demand funds be transferred to a bitcoin wallet under the threat of publishing compromising videos, RIA News reports.

Source: banki.ru, April 5, 2021

Experts have counted over 1.5 thousand pseudo-banks in Runet since the start of the year

In Russia, the number of pseudo-banks grew 20% in Q1 2021 to 1,529, according to the cybersecurity company BI.ZONE. The number of phishing sites is growing, as it proves to be the cheapest and most effective to reach as many members of the public as possible, explained Evgeny Voloshin, director of the company's expert services block. The average time needed to block fraudulent resources is between 10 and 70 hours, but in extreme cases, the time required to limit access can be up to several weeks, he stressed.

Source: banki.ru, April 6, 2021

Experts: scammers use Telegram bots and Google forms to automate phishing

User data stolen as a result of phishing attacks is increasingly being uploaded not only via e-mail, but also in legitimate services as Google forms and the Telegram messenger, according to a study by Group-IB. Automated phishing makes use of Telegram bots on ready-made platforms as they are able to control the entire phishing attack process and keep a record of any funds stolen.

Source: banki.ru, April 7, 2021

Central Bank: social engineering remains the main threat to financial cybersecurity

Social engineering remains the main threat to financial cybersecurity, but its share in total theft is falling, according to the Russian Central Bank's "2020 review of operations performed without the consent of financial institution clients" report.

The share of social engineering in all unauthorised operations decreased at the end of 2020 to 61.8% (from 68.6% in 2019) thanks to the joint efforts of the Bank of Russia, financial organisations and law enforcement agencies to increase the public cyber literacy, the regulator said in a statement.

Source: banki.ru, April 12, 2021

Mass use of biometrics could lead to an increase in cybercrime numbers

The widespread use of biometric identification may lead to an increase in fraud using the technology. The opinion was expressed at a TASS press conference by the president of the InfoWatch group of companies, chairperson of the board of the association of software developers "techestvenny soft" Natalya Kasperskaya.

Source: banki.ru, April 14, 2021

Moody's: small banks in Russia are more exposed to cyber fraud risks

TASS reports that small banks in Russia are more exposed to cyber fraud according to Moody's.

Source: banki.ru, April 20, 2021

The data of hundreds of Russian companies appears in the public domain

Kommersant reports that the corporate data of hundreds of large and thousands of small Russian companies has appeared in the public domain, referring to information from the softline company Infosecurity. The organisations posted information on the boards of the free online project manager Trello. Almost a million public Trello boards are currently indexed by search engines, with thousands of them containing confidential information, analysts have said. In Russia, Trello boards are mainly used by small and medium-sized businesses; representatives of large organisations, including banks, according to Infosecurity.

Source: banki.ru, April 20, 2021

Bank fraudsters have started using robots to call customers

Russian scammers have learned to use robots similar to those used by financial organisations, calling customers with individual offers, referring to banking sector experts. According to Alexey Konyaev, head of analytical solutions for countering fraud and financial crime at SAS Russia / CIS, robots are becoming popular in the early stages of fraud conversations, saving time when eliminating anyone not taken in by the scam. The scammers' main tool is psychological pressure. If the potential victim does not drop the call and shows interest, then the call is transferred to a "bank employee", who will continue the conversation. Mr Konayev added that if we remember this mechanism, it should be easy to distinguish between an attacker and a real financial organisation.

Source: iz.ru, May 6, 2021

"Collecting data from social networks is easier than from bank leaks"

Data from social networks is a more effective way of finding information on a potential victim for a fraudster than from bank leaks, said Artem Sychev, Central Bank Information Security Department Deputy Head, who oversees the Centre for Monitoring and Responding to Financial Sector Cyber Attacks.

Source: iz.ru, May 12, 2021

A series of cyber attacks on Russian government agencies has identified

Rostelecom-Solar, a Rostelecom subsidiary and provider of cybersecurity technology, together with the National Coordination Centre for Computer Incidents, has identified a series of cyber group attacks on Russian authorities. According to the provider, the hackers' main goal is to compromise IT infrastructure and steal confidential information, including documentation from isolated segments and key employee email correspondence.

Source: banki.ru, May 12, 2021

Kazakhstan

Data of over 3 million people in Kazakhstan leaked to the Internet

During an investigation into a data security incident, the KZ-CERT Computer Incident Response Service established that the data of over 3 million Facebook users in Kazakhstan had been compromised - one hacker forum user published a database of over 533 million Facebook users from 106 countries.

Source: profit.kz, April 5, 2021

Amendments to laws protecting personal data developed in Kazakhstan

Draft changes have been proposed to legislative acts protecting personal data in Kazakhstan, Zakon.kz reports. The amendments focus on article 145 "Image Rights", with the proposed new version stating that another person's image (including photographs, video recordings or works of art in which the person is depicted) can only be used or distributed with their consent or that of their legal representatives, or heirs after their death.

Source: profit.kz, April 14, 2021

Illegal distribution of personal data already being punished

The Ministry of Digital Development’s Information Security Committee was set up as the personal data protection authority in Kazakhstan last summer and is currently carrying out unscheduled inspections based on complaints from individuals and materials received from other government agencies. Committee members are also initiating administrative cases around the legality of the collection and processing of personal data, as well as compliance with protection measures. Ruslan Abdikalikov, Information Security Committee Chairman, spoke about the results of the analysis during a CCS briefing.

Source: profit.kz, April 15, 2021

The State Technical service deters a cyberattack on state agencies

The GTS KZ-CERT computer incident response service has reported malicious mailing on behalf of First Heartland Jýsan Bank, noting that it was not an isolated case, and popular brands were common targets for fake mailing lists. In this specific case, the mail was received from a fictitious bank employee requesting bids for services and, allegedly attaching a technical specification.

Source: profit.kz, May 6, 2021

Kyrgyzstan

Kyrgyzstan not satisfied with digitalisation

Taalay Baiterekov, Head of the Kyrgyz Republic Digital Transformation Department, has said that the digitalisation process in Kyrgyzstan is very slow, but confirmed that every effort will be used to develop it, involving representatives from the business community. He was speaking at a briefing discussing “government IT plans after the dismissal of the heads of five enterprises”, Sputnik reports.

Source: profit.kz, April 28, 2021

Kyrgyzstan wants to reorganise IT state-owned enterprises

The plan, according to the head of the government’s digital transformation department Taalay Baiterekov, is to streamline state IT-enterprises by combining them into one centralised organisation within the framework of "government IT plans after the dismissal of the heads of five enterprises." The measure should help reduce the number of administrative staff and attract more programmers, helping generate quality products that will find a practical use in the market. The corresponding government resolution is currently undergoing approval, but it is not yet known what form of ownership the new organisation will take, Sputnik reports.

Source: profit.kz, April 30, 2021

MAKING AN
IMPACT THAT
MATTERS
since 1845

deloitte.az

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited (“DTTL”), its global network of member firms, and their related entities. DTTL (also referred to as “Deloitte Global”) and each of its member firms are legally separate and independent entities. DTTL does not provide services to clients. Please see www.deloitte.com/about to learn more.

Deloitte is a leading global provider of audit and assurance, consulting, financial advisory, risk advisory, tax and related services. Our network of member firms in more than 150 countries and territories serves four out of five Fortune Global 500® companies. Learn how Deloitte’s approximately 330,000 people make an impact that matters at www.deloitte.com.

This communication contains general information only, and none of Deloitte Touche Tohmatsu Limited, its member firms or their related entities (collectively, the “Deloitte network”) is, by means of this communication, rendering professional advice or services. Before making any decision or taking any action that may affect your finances or your business, you should consult a qualified professional adviser. No entity in the Deloitte network shall be responsible for any loss whatsoever sustained by any person who relies on this communication.

25E Nobel Avenue,
Baku, AZ1025, Azerbaijan