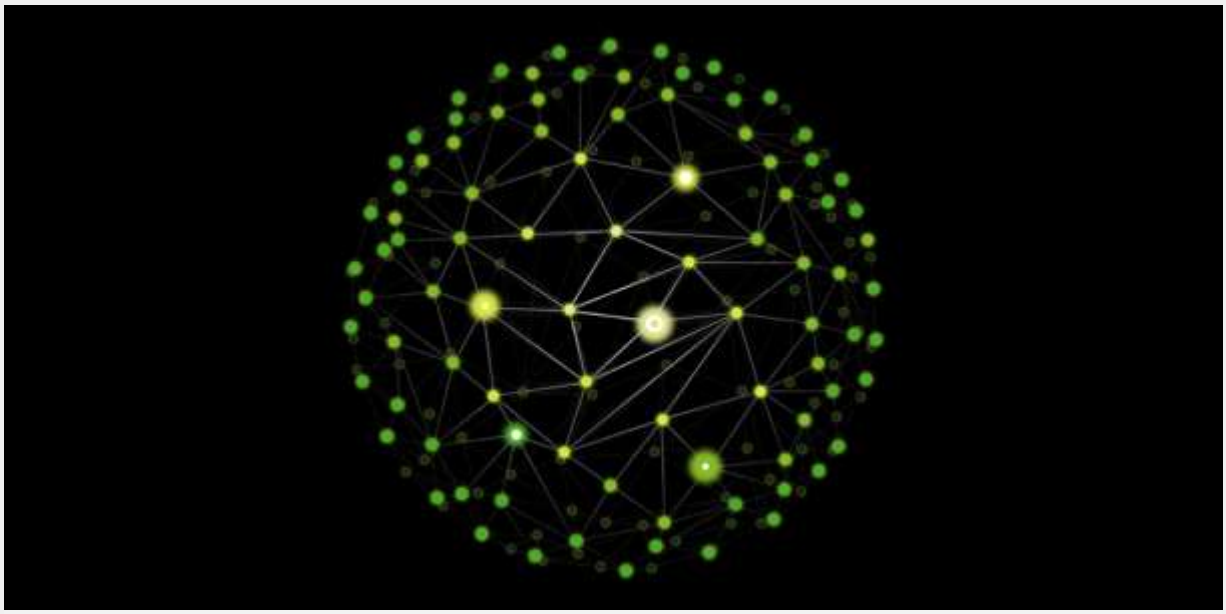
Deloitte.

MAKING AN IMPACT THAT MATTERS since 1845

Azərbaycan | Risk Məsləhətləri | 17 İyun 2021



Deloitte Kiber Təhlükəsizlik və Texnologiya Xəbərlərinin icmalı
13-cü buraxılış

English version below

Azərbaycan

Azərbaycanın bir sıra dövlət qurumlarında informasiya sistemlərinin inkişafı ilə bağlı siyasət mövcud deyil

Azərbaycanın bir sıra dövlət qurumlarında əksər hallarda informasiya sistemlərinin inkişafı ilə əlaqəli sərmayə istiqamətlərini müəyyənləşdirən və onlara əsaslandırma bazası ola biləcək ortamüddətli strateji sənədlər və ya siyasətlər mövcud deyil. Bu barədə "Hesablama Palatasının 2020-ci ildə fəaliyyəti haqqında" hesabatda bildirilir. Qeyd olunur ki, qurumlarda yaradılan informasiya sistemlərinin idarə olunması yalnız operativ səviyyədə təşkil edilib və daha çox texniki dəstək funksiyasını yerinə yetirir.

Mənbə: xeberler.az, 5 aprel 2021

Azərbaycanda biometrik imzalar tətbiq olunacaq

Azərbaycanda biometrik imzaların tətbiqi istiqamətində işlər aparılır. Söhbət gələcəkdə e-imza kartlarını və tokenləri əvəz edəcək yeni tanınma texnologiyasından gedir. Onun vasitəsilə istifadəçilər zəruri olan sənədləri fərdi biometrik göstəricilərlə (barmaq izi, üz, göz və s.) təsdiqləyə biləcəklər. Hazırda rəqəmli imzanın təhlükəsizliyini təmin edən SHA-1 kriptoqrafik alqoritmi daha təhlükəsiz hesab olunan SHA-2 ilə əvəz edilir.

Mənbə: xeberler.az, 19 aprel 2021

Elektron Təhlükəsizlik Xidməti növbəti dəfə “fişinq” hücumları barədə xəbərdarlıq edib

Nəqliyyat, Rabitə və Yüksək Texnologiyalar Nazirliyi yanında Elektron Təhlükəsizlik Xidməti vətəndaşları son günlərdə bankları hədəf alan “fişinq” hücumları barədə xəbərdar edir. Kiberdələduzlar Azərbaycan banklarının texniki dəstək xidmətinin adından sui-istifadə edərək vətəndaşların bank məlumatlarını və digər fərdi məlumatlarını ələ keçirməyə çalışırlar. Belə ki, həyata keçirilən kiberhücumlarda bank əməkdaşlarının adından vətəndaşların mobil nömrələrinə zənglər edilərək, onların adına hər hansı köçürmənin həyata keçirildiyi bildirilir və təsdiqləmə üçün kart hesab nömrəsi, şifri, təsdiqləmə kodu və sair fərdi məlumatların təqdim edilməsi tələb olunur.

Mənbə: cert.az, 20 aprel 2021

Azərbaycanın daha bir bankı e-imza xidmətini aktivləşdirəcək

Yaxın gələcəkdə "Rabitəbank" tərəfindən müştərilərə elektron imzanın (e-imza) əldə edilməsi xidmətini aktivləşdirəcəyi gözlənilir. Bununla bağlı bank tərəfindən Dövlət Vergi Xidmətinə müraciət olunub: "Ümumilikdə, cari il ərzində bank tərəfindən 10-a yaxın rəqəmsal həll və məhsul təklif olunacağı gözlənilir ki, onların üzərində hazırda aktiv işlər aparılır".

Mənbə: xeberler.az, 21 aprel 2021

Daha bir elektron dələduzluq faktı ifşa edildi

“Diqqət! Dələduzların alış-veriş səhifələrindən vətəndaşların əlaqə vasitələrini ələ keçirərək onları aldadan və kart məlumatlarını ələ keçirmək üçün istifadə etdikləri növbəti səhifə ifşa olundu”. Bu barədə Xüsusi Rabitə və İnformasiya Təhlükəsizliyi Dövlət Xidməti - Kompüter İnsidentlərinə Qarşı Mübarizə Mərkəzindən məlumat verilib. Məlumata görə, dələduzlar aşağıdakı tipli veb sayt yaradaraq vətəndaşları aldatmağa çalışır: https://azerdostavka.shop/. Veb sayt hazırda aktiv deyil.

Mənbə: xeberler.az, 23 aprel 2021

Dövlət Xidməti: “WhatsApp”ın yeni versiyası şəxsi məlumatlarınızı oğurlayır

Bu günlərdə “WhatsApp Pink” adlı “WhatsApp”ın yeni bir versiyası ortaya çıxıb və populyarlıq qazanmağa başlayıb. Bu barədə Xüsusi Rabitə və İnformasiya Təhlükəsizliyi Dövlət Xidmətinin Kompüter İnsidentlərinə Qarşı Mübarizə Mərkəzinin açıqlamasında bildirilir. Məlumatda həmçinin

deyilir ki, “WhatsApp Pink” tam zərərli bir tətbiqdir: “Bu zərərverici APK link şəklində “Whatsapp” qruplar vasitəsilə yayılmaqdadır. “WhatsApp Pink” əvvəlcə qeydiyyat məlumatlarınızı soruşur və bundan sonra şəxsi məlumatlarınızı oğurlayır”.

Mənbə: xeberler.az, 28 aprel 2021

Kiberdələduzlar “Azərpoçt”un rəsmi saytına oxşar saxta səhifələr yaradır

Nəqliyyat, Rabitə və Yüksək Texnologiyalar Nazirliyi yanında Elektron Təhlükəsizlik Xidməti vətəndaşları “Azərpoçt” MMC adına açılan saxta saytlar barədə xəbərdar edir. MMC-dən bildirilib ki, bir qrup kiberdələduz qeyri-qanuni yolla maddi vəsait əldə etmək məqsədilə “Azərpoçt”un rəsmi saytına oxşar saxta saytlar yaradır. Onların hədəfi onlayn alqı-satqı səhifələrində müxtəlif məhsulların satışını həyata keçirən vətəndaşlardır. Kiberdələduzlar alıcı qismində saxta “WhatsApp” nömrələrindən bu vətəndaşlara yazaraq məhsulu almaq istədiyini bildirir və ödənişin həyata keçirilməsi üçün satıcıdan “Azərpoçt” MMC-nin adına açılan saxta sayta daxil olaraq kart hesabı məlumatlarını daxil etməsini istəyirlər. Vətəndaş bu keçidə daxil olaraq kart hesabının məlumatlarını təqdim etdikdə hesabın balansında olan vəsait kiberdələduzların əlinə keçir.

Mənbə: xeberler.az, 28 aprel 2021

Azərbaycanın ilk antivirus proqramı təqdim edilib

Uzun zamandır üzərində işlədiyimiz zərərvericilərin analizi üçün hazırlanmış olan tətbiqin ilkin “beta” test versiyası artıq hazırdır. Bu barədə Xüsusi Rabitə və İnformasiya Təhlükəsizliyi Dövlət Xidmətinin Kompüter İnsidentlərinə Qarşı Mübarizə Mərkəzinin açıqlamasında bildirilir.

Mənbə: xeberler.az, 30 aprel 2021

“Elektron prokurorluq” informasiya sistemi yaradılacaq

Azərbaycan prokurorluq orqanlarının fəaliyyətində müasir informasiya-kommunikasiya texnologiyalarının tətbiqini təmin edən “Elektron prokurorluq” informasiya sistemi yaradılacaq.

Mənbə: xeberler.az, 8 may 2021

Azərbaycanda kibertəhlükəsizlik üzrə beşillik strategiya hazırlanıb

Azərbaycanda 2021-2025-ci illəri əhatə edən informasiya və kibertəhlükəsizlik üzrə milli strategiyanın təsdiq edilməsi gözlənilir. Bu barədə Nəqliyyat, Rabitə və Yüksək Texnologiyalar Nazirliyindən bildirilib. Məlumata görə, qeyd olunan strategiyanın həyata keçirilməsi üzrə tədbirlər planında sahə üzrə qanunvericiliyin təkmilləşdirilməsi ilə bağlı müddəalar da öz əksini tapıb.

Mənbə: xeberler.az, 14 may 2021

Azərbaycandakı kompyuterlərin 42 faizində hələ də Windows 7 istifadə olunur

Kaspersky-nin statistik məlumatına görə, Azərbaycanda kompüterlərin 42%-də hələ də baza dəstəyi 2020-ci ilin yanvarında başa çatmış Windows 7 əməliyyat sisteminə quraşdırılıb. Əməliyyat sisteminin köhnəlmiş bir versiyası yaxşı işləyə bilər, lakin əgər o, artıq dəstəklənmirsə, ona hücum etmək daha asandır. Sistemin ömrü bitdikdə, zəifliklər olduğu kimi qalır, onlar üçün yamaqlar (patch) buraxılmır, bu da təcavüzkarların məlumat əldə etməsini asanlaşdırır. Ev istifadəçiləri arasında Windows 7 istifadə edənlərin payı 48%, kiçik və orta sahibkarlar arasında - 14%, mikrobiznes nümayəndələrində isə 30%-dir. Kiçik müəssisələrin əməliyyat sistemini müasir səviyyədə saxlaması xüsusilə vacibdir, çünki onlar kiber təhlükəsizliklə mübarizə üçün ayrıca resurslara sahib deyillər.

Mənbə: xeberler.az, 17 may 2021

Onlayn dələduzluq və kibertəhdidlərə qarşı mübarizə gücləndirilir

Xüsusi Rabitə və İnformasiya Təhlükəsizliyi Dövlət Xidməti tərəfindən yaradılan "Blacklist.gov.az" layihəsinin yeni təkmilləşdirilmiş və daha funksional versiyası istifadəyə verilib. Kompüter İnsidentlərinə qarşı Mübarizə Mərkəzindən verilən məlumata görə, layihənin məqsədi ölkədə son zamanlar artan onlayn dələduzluq və kibertəhdidlərə qarşı mübarizəni gücləndirmək, kiberdələduzluq və kibertəhücumlarda istifadə olunan domen adlarını toplamaqla ifşa etmək, eləcə də sistemə inteqrasiya edilmiş veb-bələdçilər üçün qoruyucu genişlənmə ("extension"), API inteqrasiya imkanları vasitəsi ilə internet istifadəçilərini qorumaqdır.

Mənbə: xeberler.az, 24 may 2021

MDB

Rusiya

Fırıldaqçılar rusiyalıları aldatmaq üçün “Yandex.Money”-dən istifadə edir

Rusiyada zərərli e-poçtlar vasitəsilə bank kartı detallarına sahib olmağın klassik mexanizmi yenidən gündəmdədir. RİA News xəbər verir ki, özünü Yandex.Money e-cüzdan operatoru kimi təqdim edən fırıldaqçılar, kompromat videoların yayımlanması təhdidi altında vəsaitlərin bitcoin cüzdanına köçürülməsini tələb edirlər.

Mənbə: banki.ru, 5 aprel 2021

Mütəxəssislər, ilin əvvəlindən bəri Runetdə 1,5 mindən çox yalançı bank saydılar

BI.ZONE kiber təhlükəsizlik şirkətinə görə Rusiyada yalan bankların sayı 2021-ci ilin I rübündə% 20 artaraq 1.529-a çatıb. Firmanın ekspert xidmətləri blokunun direktoru Evgeniy Voloşin izah etdi ki, fişinq saytlarının sayı artmaqdadır, çünki cəmiyyətin mümkün qədər çox üzvünə çatmağın ən ucuz və ən təsirli yoludur. Saxta mənbələrin qarşısını almaq üçün lazım olan orta müddət 10 ilə 70 saat

arasındadır, lakin həddindən artıq hallarda girişi məhdudlaşdırmaq üçün lazım olan vaxt bir neçə həftəyə qədər ola bilər.

Mənbə: banki.ru, 6 aprel 2021

Mütəxəssislər: fırıldaqçılar fişinqi avtomatlaşdırmaq üçün Telegram botlarından və Google formalarından istifadə edirlər

Fişinq hücumları nəticəsində oğurlanan istifadəçi məlumatları getdikcə e-poçt vasitəsilə deyil, həm də Google formaları və Telegram messenceri kimi qanuni xidmətlərə yüklənir, Group-IB-in apardığı araşdırmaya görə. Avtomatlaşdırılmış fişinq, hazırlanan platformalarda Telegram botlarından istifadə edir, çünki fişinq hücumu prosesini tam idarə edə və oğurlanmış hər hansı bir vəsaitin qeydini apara bilir.

Mənbə: banki.ru, 7 aprel 2021

Mərkəzi Bank: sosial mühəndislik maliyyə kiber təhlükəsizlik üçün əsas təhlükə olaraq qalır

Sosial mühəndislik maliyyə kiber təhlükəsizlik üçün əsas təhlükə olaraq qalır, lakin Rusiya Mərkəzi Bankının “Maliyyə təşkilatı müştərilərinin razılığı olmadan həyata keçirilən əməliyyatların 2020-ci il icmalı” hesabatına əsasən, ümumilikdə oğurluqdakı payı azalmaqdadır.

Sosial mühəndisliyin bütün icazəsiz əməliyyatlardakı payı, Rusiya Bankı, maliyyə təşkilatları və hüquq mühafizə orqanlarının ictimai kiber savadlılığı artırmaq üçün birgə səyləri sayəsində 2020-ci ilin sonunda 61.8% -ə (2019-cu ildə 68.6% -dən) düşdü.

Mənbə: banki.ru, 12 aprel 2021

Biometriyadan kütləvi istifadə kiber cinayətlərin sayının artmasına səbəb ola bilər

Biometrik identifikasiyadan geniş istifadə saxtakarlığın artmasına səbəb ola bilər. Fikri TASS mətbuat konfransında InfoWatch şirkətlər qrupunun prezidenti, “Otechestvenny soft” proqram təminatı istehsalçıları assosiasiyasının idarə heyətinin sədri Natalya Kasperskaya söylədi.

Mənbə: banki.ru,14 aprel 2021

Moody's: Rusiyadakı kiçik banklar daha çox kiber fırıldaqçılıq risklərinə məruz qalır

TASS xəbər verir ki, Rusiyadakı kiçik banklar daha çox Moody's agentliyinə görə kiber fırıldaqçılığa məruz qalırlar.

Mənbə: banki.ru, 20 aprel 2021

Yüzlərlə Rusiya şirkətinin məlumatları ictimaiyyətə sızmışdır

Kommersant, yüzlərlə iri və minlərlə kiçik rus şirkətinin korporativ məlumatlarının, İnfosecurity softline şirkətinin məlumatlarına istinad edərək ictimai məkanda ortaya çıxdığını bildirir. Təşkilatlar

pulsuz onlayn layihə meneceri Trello-nun lövhələrində məlumat yerləşdirdilər. Analitiklər, hazırda axtarış sistemləri tərəfindən bir milyona yaxın ictimai Trello lövhəsinin indekslənməsinin aparıldığını, bunların daxilində məxfi məlumatların olduğunu söylədilər. Rusiyada Trello lövhələri əsasən kiçik və orta sahibkarlar, banklar da daxil olmaqla böyük təşkilatların nümayəndələri tərəfindən istifadə olunur.

Mənbə: banki.ru, 20 aprel 2021

Bank fırıldaqçıları müştərilərə zəng etmək üçün robotlar istifadə etməyə başladılar

Rus fırıldaqçılar, bank sektoru mütəxəssislərinə istinad edərək, fərdi təkliflərlə müştərilərə zəng edərək maliyyə təşkilatlarının istifadə etdiyi robotlara bənzər robotlardan istifadə etməyi öyrəndilər. SAS Rusiya / MDB-də fırıldaqçılığa və maliyyə cinayətlərinə qarşı analitik həllərin rəhbəri Aleksey Konyaevə görə, robotlar saxtakarlıq söhbətlərinin ilkin mərhələlərində populyarlaşaraq fırıldaqçı tərəfindən qəbul edilməyən hər kəsi ləğv edərkən zaman qazanır. Dolandırıcıların əsas vasitəsi psixoloji təzyiqdir. Potensial qurban zəngdən imtina etmirsə və maraq göstərirsə, zəng söhbəti davam etdirəcək bir "bank işçisinə" köçürülür. Cənab Konayev əlavə etdi ki, bu mexanizmi xatırlasaq, təcavüzkarla həqiqi maliyyə təşkilatı arasında fərq qoyulması asan olmalıdır.

Mənbə: iz.ru, 6 may, 2021

"Sosial şəbəkələrdən məlumat toplamaq bank məlumatlarının sızmasından daha asandır"

Mərkəzi Bankın İnformasiya Təhlükəsizliyi Departamentinin rəis müavini Artem Sychev, sosial şəbəkələrdən alınan məlumatlar, bir fırıldaqçı üçün potensial bir qurban haqqında məlumatları bank sızmalarından əldə etməkdən daha asan olduğunu bildirdi.

Mənbə: iz.ru, 12 may, 2021

Rusiya dövlət qurumlarına edilən bir sıra kiber hücumlar təsbit edildi

Rostelecom-un törəmə şirkəti və kiber təhlükəsizlik texnologiyasının təminatçısı olan Rostelecom-Solar, Kompüter İnsidentləri üzrə Milli Koordinasiya Mərkəzi ilə birlikdə Rusiya hakimiyyət orqanlarına qarşı bir sıra kiber qrup hücumlarını müəyyənləşdirdi. Təchizatçıya görə, hakerlərin əsas məqsədi daxili İT infrastrukturuna giriş əldə etmək və təcrid olunmuş seqmentlərdən sənədlər və işçilərin elektron poçt yazışmaları daxil olmaqla məxfi məlumatları oğurlamaqdır.

Mənbə: banki.ru, 12 may, 2021

Qazaxıstan

Qazaxıstanda 3 milyondan çox vətəndaşın məlumatları internetə sızdı

Məlumat təhlükəsizliyi hadisəsi ilə bağlı aparılan araşdırma zamanı, KZ-CERT Kompüter İnsidentlərinə Müdaxilə Xidməti Qazaxıstandakı 3 milyondan çox Facebook istifadəçisinin

məlumatlarının pozulduğunu təsbit etdi - bir haker forum istifadəçisi 106 ölkədən 533 milyondan çox Facebook istifadəçisinin məlumat bazasını yayımladı.

Mənbə: profit.kz, 5 aprel 2021

Qazaxıstanda fərdi məlumatları qoruyan qanunlara dəyişikliklər hazırlandı

Zakon.kz xəbər verir ki, Qazaxıstanda fərdi məlumatları qoruyan qanunvericilik aktlarına dəyişiklik layihəsi təklif edildi. Dəyişikliklər 145 saylı "Təsvir hüquqları" maddəsinə yönəldilib, təklif olunan yeni versiyada başqa bir şəxsin şəklinin (şəxsin təsvir olunduğu fotoşəkillər, video qeydlər və ya sənət əsərləri daxil olmaqla) yalnız onların və ya onların razılığı ilə istifadə edilə və ya paylana biləcəyi bildirilir.

Mənbə: profit.kz, 14 aprel 2021

Fərdi məlumatların qanunsuz yayılması artıq cəzalandırılır

Rəqəmsal İnkişaf Nazirliyinin Məlumat Təhlükəsizliyi Komitəsi keçən yay Qazaxıstanda fərdi məlumatların qorunması orqanı kimi yaradıldı və hal-hazırda ayrı-ayrı şəxslərin şikayətləri və digər dövlət qurumlarından alınan materiallar əsasında planlaşdırılmamış yoxlamalar aparır. Komitə üzvləri ayrıca fərdi məlumatların toplanılması və işlənməsinin qanuniliyi, habelə qoruma tədbirlərinə riayət olunması barədə inzibati işlər qaldırırlar. İnformasiya Təhlükəsizliyi Komitəsinin sədri Ruslan Abdikalikov CCS brifinqi zamanı təhlilin nəticələrindən danışdı.

Mənbə: profit.kz, 15 aprel 2021

Dövlət Texniki xidməti dövlət qurumlarına edilən kiberhücumun qarşısını alır

GTS KZ-CERT Kompüter insidentlərinə cavab xidməti "First Heartland Jısan" Bankının adından zərərli fişinq məktublar barədə məlumat verib, bunun yeganə hal olmadığını qeyd edib və populyar brendlərin tez-tez saxta e-poçt siyahılarının obyektinə çevrildiklərini qeyd ediblər. Bu halda məktub Bankın uydurma əməkdaşından göndərilmişdir, hansı ki, xidmətlər üçün təkliflər istəyib və texniki spesifikasiyanı qoşmalara əlavə etmişdir.

Mənbə: profit.kz, 6 may 2021

Qırğızıstan

Qırğızıstan rəqəmsallaşmadan razı deyil

Qırğızıstan Respublikası Rəqəmsal Çevrilmə Departamentinin rəhbəri Taalay Baiterekov Qırğızıstanda rəqəmsallaşdırma prosesinin çox yavaş olduğunu söylədi, lakin iş dünyasının nümayəndələrini əhatə edən bu səylərin inkişaf etdirilməsi üçün hər cür səy göstəriləcəyini təsdiqlədi. Sputnik xəbər verir ki, o, "beş müəssisə rəhbərinin işdən çıxarılmasından sonra dövlətin İT planları" nı müzakirə edən brifinqdə danışdı.

Mənbə: profit.kz, 28 aprel 2021

Qırğızıstan İT dövlət müəssisələrini yenidən təşkil etmək istəyir

Hökümətin rəqəmsal çevrilmə şöbəsinin müdiri Taalay Baiterekovun sözlərinə görə, plan, "beş müəssisə rəhbərinin işdən çıxarılmasından sonra dövlətin İT planları" çərçivəsində dövlət İT müəssisələrini bir mərkəzləşdirilmiş təşkilata birləşdirərək düzəltməkdir. Tədbir, inzibati heyət sayını azaltmağa və daha çox proqramçı cəlb etməyə kömək etməli və bazarda praktiki istifadə tapa biləcək keyfiyyətli məhsullar yaratmağa kömək etməlidir. Sputnik xəbər verir ki, müvafiq hökumət qərarı hazırda təsdiqlənməkdədir, lakin yeni təşkilatın hansı mülkiyyət formasını alacağı hələ məlum deyil.

Mənbə: profit.kz, 30 aprel 2021

Deloitte Cyber & Technology News digest

Issue #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

Nobel pr. 25E, Bakı Ağ Şəhər Ofis Binası
Bakı, AZ1025, Azərbaycan Respublikası