REPORT ON DATA BREACHES INVOLVING UZBEK CITIZENS

DATA LEAK REPORT

O’zbekiston fuqarolariga tegishli ma’lumotlarning sizib chiqishi holatlari haqida hisobot.

CYBER BRO

Umumiy Ma’lumotlar

CYBERO

Cyber Threat Intelligence (CTI)
Darkweb Investigation
Data Leak Monitoring

CTI (Cyber Threat Intelligence) – bu kiberxavfsizlik tahdidlarini tahlil qilish, xakerlik guruhlari faoliyatini kuzatish va oldindan xabardor bo‘lish uchun mo‘ljallangan razvedka usuli hisoblanadi. Uning asosiy maqsadi – kiberhujumlarni oldindan aniqlash va ularni bartaraf etish.

CTI jarayoni quyidagi bosqichlarni o‘z ichiga oladi :

1. Ma’lumot to‘plash – DarkNet, DeepWeb, ijtimoiy tarmoqlar, xakerlar forumlari va boshqa noqonuniy ma’lumot almashish manbalaridan ma’lumotlarni yig’ish va tahlil qilish.
2. Tahlil qilish va xakerlik guruhlarini kuzatish – noma’lum tahdid vektorlarini aniqlash va ularning xatti-harakatlarini oldindan bashorat qilish.
3. Xavf darajasini baholash – tahdid manbalarini, potensial nishonlarni va zararlanish darajasini aniqlash.
4. Hujum oldini olish va himoya choralarini ishlab chiqish – zararli faoliyatni bloklash, tizimlar xavfsizligini kuchaytirish va foydalanuvchilarni xabardor qilish.

DarkNet – bu shifrlangan va maxsus brauzerlar (masalan, Tor, I2P) orqali kirish mumkin bo‘lgan internet qismi bo‘lib, u noqonuniy faoliyat uchun keng qo‘llaniladi. Ko‘pincha, DarkNet’da quyidagi turdagi ma’lumotlar almashinadi:

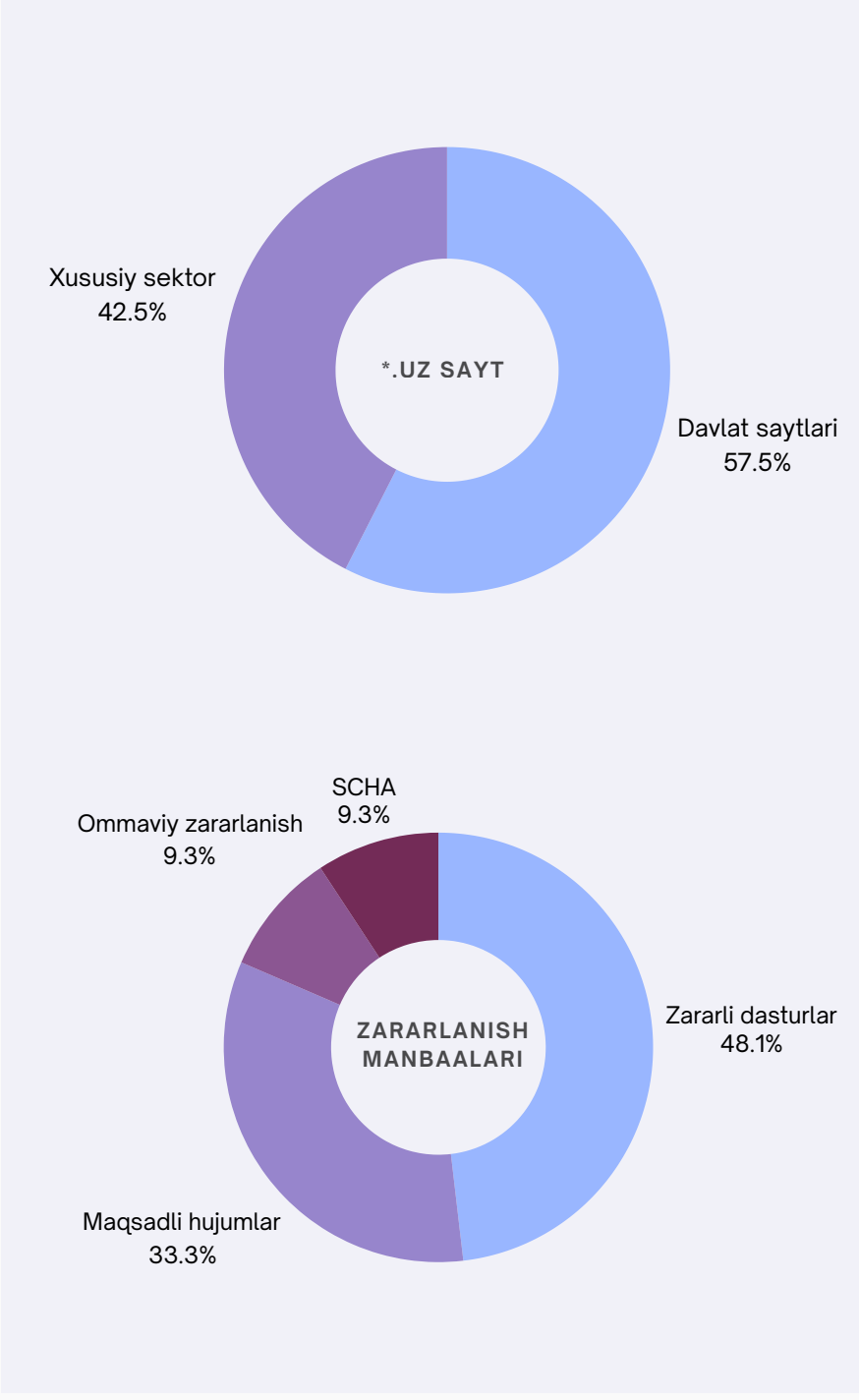
- O‘g‘irlangan shaxsiy ma’lumotlar (shaxsiy guvohnomalar, bank hisoblari, parollar).
- Kredit karta va to‘lov ma’lumotlari.
- Xakerlik vositalari va ekspluatatsiyalari (exploit).
- Ransomware va boshqa zararli dasturlar orqali qo’lga kiritilgan va sotuvga qo’yilgan ma’lumotlar.

*.UZ domen hududi bo’yicha sizib chiqqan ma’lumotlar statistikasi

“CITIZENSEC” Kiber razvedka natijalariga ko’ra, internetda O’zbekiston fuqarolariga tegishli bo’lgan 10 milliondan ortiq shaxsiy ma’lumotlar mavjud.

Data Leak (ma’lumotlarning sizib chiqishi) – bu shaxsiy, korporativ yoki davlatga tegishli maxfiy ma’lumotlarning noqonuniy ravishda DarkNet yoki boshqa ochiq manbalarda tarqalishi. Bunday sizib chiqishlar quyidagi yo‘llar bilan sodir bo‘lishi mumkin:

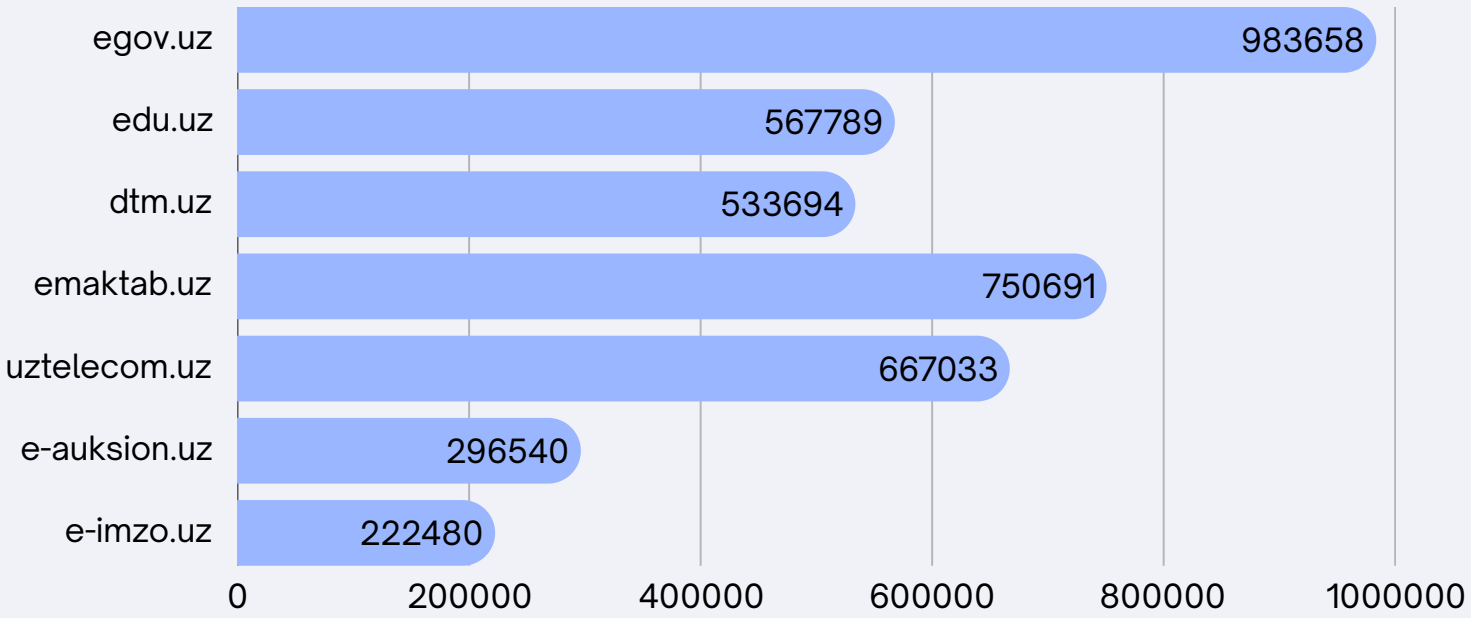
- Xaker hujumlari – fishing, ransomware, SQL Injection va boshqa hujumlar orqali.
- Ichki xodimlarning noqonuniy harakatlari, tashkilot ichidagi xodimlar ma’lumotlarni sotib yuborishi.
- Zaxira ma’lumotlarining ochiq qolishi, noto‘g‘ri konfiguratsiya qilingan serverlar yoki bulutli xostinglardagi ochiq bazalar.
- Brute Force Attacks – login va parollarni taxmin qilish orqali buzib kirish, bunga asosan oddiy va oson parol ishlatish sabab bo’ladi.
- Malware & Ransomware – zararli dasturlar orqali tizimga noqonuniy kirish va ma’lumotlarni shifrlash yoki o‘g‘irlash.
- Xodimlarning qasddan ma’lumot tarqatishi – norozi yoki ishdan ketgan xodimlarda tizimdan foydalanish huquqi saqlab qolinganda sodir bo’lishi mumkin.



SCHA - tashqi xizmat ko‘rsatuvchi kompaniya yoki yetkazib beruvchi orqali tizimning zararlanishi.

TOP Sohalar

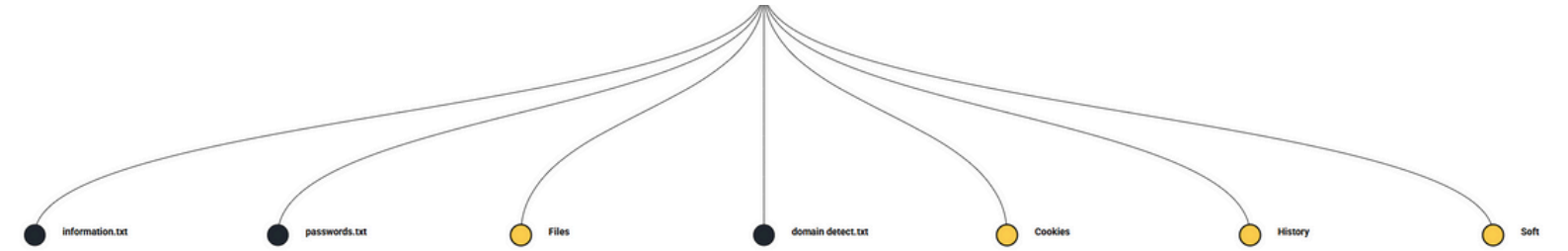
2024-yilning olti oyi davomida quyidagi domen nomlaridan eng ko’p ma’lumotlar sizib chiqqanligi aniqlandi.



Ko’rib turganingizdek hukumat va ta’lim soxalari, qolaversa sog’liqni saqlash hamda xususiy sektor eng ko’p zarar ko’rgan sohalar sifatida ko’riladi. Hukumat va ta'lim tashkilotlarida ko'pincha zaif xavfsizlik protokollari qo’llaniladi, Masalan, shifrlashning yo'qligi, kuchli parollarni talab qilmaslik va ikki bosqichli autentifikatsiyani o'rnatmaslik ma'lumotlar sizib chiqishining asosiy sabablari bo'lishi mumkin. Bundan tashqari foydalanuvchilarning turli qatlamda va turlicha kiber savodxonlikga ega ekanligi, osongina zararli ma’lumot o’g’irlovchi “infostealer” lar orqali zararlanishga sabab bo’lmoqda.

*GOV.uz

O'zbekiston Respublikasi Hukumatining rasmiy portali bo'lib, u davlat xizmatlarini taqdim etish, ma'lumotlarni yetkazish va boshqa ko'plab davlat tizimlariga kirish imkoniyatlarini yaratadi. Ushbu portal orqali aholiga va yuridik shaxslarga ko'plab xizmatlar taqdim etiladi. Hukumat va ta'lim sohalaridagi foydalanuvchi ma'lumotlarini himoya qilish juda muhimdir. Foydalanuvchilar, o'z navbatida, kuchli parollarni ishlatish, ikki bosqichli autentifikatsiya va xavfsiz bog'lanish protokollaridan foydalangan holda o'zlarini himoya qilishlari kerak. Shuningdek, fishing va zararli dasturlardan saqlanish uchun ehtiyotkorlik va xavfsizlikka alohida e'tibor qaratishi zarur. Quyida maxfiy ma’lumotlari sizib chiqqan 983 mingdan ortiq foydalanuvchilardan namunalar keltiriladi, namunalarda xavfsizlik yuzasidan foydalanuvchilarning parollari keltirilmaydi.



URL	Login
my.gov.uz	916xxxx03
elections.gov.uz	bux_usk_179
id.egov.uz	asror_3497
id.egov.uz	MDI_1711
id.egov.uz	zaychikobidova
id.egov.uz	husanxxxxdbekov
elections.gov.uz	bux_usk190
id.egov.uz	avazjon6363
id.egov.uz	Dilshoddek01
id.egov.uz	vicond
id.egov.uz	solijxxxxmov@gmail.com
id.egov.uz	1bk12256
id-cloud.egov.uz	gulhayo19071989
id-cloud.egov.uz	creative.boy
id.egov.uz	fH7GHcUVPJ

Umumiy ma’lumot

Infostealerlardan ximoyalanish uchun bir nechta texnik choralar va ishlarni amalga oshirish zarur. Birinchi navbatda, tizimni muntazam yangilab turish, barcha xavfsizlik yangilanishlarini o'rnatish lozim. Shuningdek, antivirus va anti-malware dasturlarini o'rnatib, ularni muntazam ravishda yangilab borish ham muhim. Foydalanuvchi tomonidan foydalaniladigan barcha parollarni kuchli va murakkab qilish, shuningdek, ikki faktorli autentifikatsiyani (2FA) yoqish xavfsizlikni sezilarli darajada oshiradi. Internetda ishlashda faqat ishonchli va xavfsiz veb-saytlar va ilovalardan foydalanish kerak. Shubhali va noma'lum manbalardan yuklab olingan fayllardan saqlanish lozim. Tizimda administrator huquqlari faqat zarur bo'lganda berilishi kerak, shuningdek, "rootkit" yoki boshqa zararli dasturlarning tizimga kirishiga yo'l qo'ymaslik uchun tarmoq monitoringi va xavfsizlik devorlari (firewall) o'rnatish lozim. Xodimlar va foydalanuvchilarni xavfsizlikka oid treninglardan o'tkazish ham muhimdir, chunki inson faktori ko'pincha zaif nuqta bo’lib xizmat qiladi. Dasturlarning ishlashini monitoring qilish, tarmoqda nojo'ya faoliyatlarni aniqlash va oldini olish uchun tarmoq traffigini tahlil qilish, shuningdek, zarur hollarda tizimga kirish uchun shifrlash texnologiyalarini qo'llash xavfsizlikni mustahkamlashga yordam beradi.

Infostealerlar turlari	MITRE ATT&CK TTP
Raccoon Stealer	Credential Dumping (T1003), Data Staged (T1074), Input Capture (T1056)
RedLine Stealer	Credential Dumping (T1003), Data Collection (T1119), Remote File Copy (T1105)
Vidar Stealer	Data Staged (T1074), Credential Dumping (T1003), Exploitation for Privilege Escalation (T1068)
Formbook	Credential Dumping (T1003), Data Encrypted (T1022), System Information Discovery (T1082)
LokiBot	Data Staged (T1074), Credential Dumping (T1003), Input Capture (T1056)
Lumma Stealer	Data Collection (T1119), Credential Dumping (T1003), Input Capture (T1056)

Har bir stealer malware o'ziga xos tarzda MITRE ATT&CK texnikalarini qo'llaydi. Ular tizimga kirish, parollarni yig'ish, ma'lumotlarni shifrlash va boshqalarni amalga oshiradilar. Ushbu ma'lumotlar tizimlarning qanday qilib himoyalanishi kerakligini aniqlashda yordam beradi.

Stealer hujum davomida MITRE ATT&CK (Advanced Persistent Threat) tizimida mavjud bo'lgan turli xil TTPs (Tactics, Techniques, and Procedures) usullaridan foydalanadi. Bu usullar, hujumchilarni tizimga kirishi, ma'lumotlarni o‘g‘irlashi va ularni boshqarish uchun qanday usullarni qo‘llashlarini tasvirlaydi.

Ma’lumot o’g’irlovchi eng keng tarqalgan dasturlar oilasi

1. Emotet:
   - Emotet dastlab elektron pochta orqali spam xabar ko’rinishida tarqatilgan va o‘g‘irlangan ma'lumotlarni to‘plashda ishlatilgan. Ushbu stealer foydalanuvchining brauzer parollarini va boshqa ma'lumotlarini o‘g‘irlaydi.
2. Lumma Stealer:
   - Lumma stealer kriptovalyuta hamyonlari, 2FA ma'lumotlarini, brauzer parollarini va foydalanuvchi ma'lumotlarini o‘g‘irlaydi. Dastur o‘zining modulli tuzilmasi bilan ajralib turadi, ya'ni foydalanuvchilar qo‘shimcha funksiyalarni o‘zgartirishi yoki qo‘shishi mumkin.
3. RedLine Stealer:
   - RedLine Stealer o‘zining yengil va samarali ishlash tartibi bilan mashhur. U foydalanuvchi ma'lumotlarini, brauzerlarda saqlagan parollarni, kredit kartalari haqida ma'lumotlarni va kriptovalyuta hamyonlari o‘g‘irlaydi.
4. Raccoon Stealer:
   - Raccoon Stealer barcha yirik brauzerlarni, kriptovalyuta hamyonlarini va ijtimoiy tarmoqlardagi hisoblarni o‘g‘irlaydi.
5. AZORult:
   - AZORult — bu ko‘plab ma'lumotni o‘g‘irlaydigan stealer bo‘lib, foydalanuvchining brauzer parollarini, cookie'larini, chat ma'lumotlarini va boshqa sezgir fayllarni o‘g‘irlaydi. AZORult, shuningdek, tarmoqdan boshqa zararli dasturlarni yuklab olish imkonini ham beradi.
6. Formbook:
   - Formbook — bu parollar, brauzer cookie’lari, email ma'lumotlari va boshqa foydalanuvchi ma'lumotlarini yig‘adigan stealer. Dastur shuningdek, foydalanuvchining tizimiga zararli kodni kiritish va boshqa malware yuklash imkonini ham beradi.
7. Vidar Stealer:
   - Vidar Stealer — shaxsiy va moliyaviy ma'lumotlarni o‘g‘irlashga qaratilgan dastur bo‘lib, u kriptovalyuta hamyonlari, brauzer parollarini va ijtimoiy media hisoblarini o‘g‘irlaydi.
8. QuasarRAT (Remote Access Trojan):
   - QuasarRAT — bu keng tarqalgan stealer va remote access trojan (RAT) bo‘lib, foydalanuvchining kompyuteriga to‘liq kirish imkoniyatini beradi. U shuningdek, parollar va boshqa sezgir ma'lumotlarni o‘g‘irlaydi.

Stealerlar taktikalari va hujum usullari:

- **Fishing hujumlari:** Zararli havolalar va soxta e-mail xabarlari orqali foydalanuvchini zararli dasturlarni yuklashga undash.
- **Ijtimoiy muhandislik:** Foydalanuvchilarni soxta saytlarga olib borish va ularning login ma'lumotlarini o‘g‘irlash.
- **Zararli dasturlarni tarqatish:** Stealerlar ko‘pincha zararli ilovalar yoki cracklangan dasturlar orqali tarqatiladi.

O'zbekiston domeni ma'muriyati statistikasiga ko‘ra, mamlakatimizda **136 mingdan** ortiq domen nomlari mavjud. Bizning kiber razvedka tahlillarimizga ko‘ra, **10 milliondan** ortiq foydalanuvchilarning maxfiy ma'lumotlari, jumladan login parollar va shaxsiy ma'lumotlari dark web’da tarqalganligi aniqlandi. Xakerlar o‘g‘irlagan bu ma'lumotlar millionlab foydalanuvchilar hamda, **10 mingga** yaqin vebsaytlarni tahdid ostida qoldirmoqda.

Xavfsizlikni ta'minlash uchun ushbu vebsayt ma'murlarini ogohlantirish hamda, doimiy monitoring qilib borish zarur. Shu maqsadda **CYBER-BRO kiberxavfsizlik kompaniyasi** tomonidan **CitizenSec threat intelligence tizimi** ishlab chiqildi. Ushbu tizim **"Citizen" (fuqarolar) va "Security" (xavfsizlik)** so'zlarining birlashmasi sifatida, kiberxavfsizlikni ta'minlaydigan, foydalanuvchilarni himoya qilishga va tezkor xabardor qilishga qaratilgan tizim vazifasini bajaradi. Sizib chiqqan ushbu maxfiy malumotlar foydalanuvchilarning shaxsiy hisoblariga kirish, boshqarish hamda o'zgartirish kiritish uchun ishlatilishi mumkin. Bundan tashqari ushbu malumotlar xakerlar tomonidan kiberhujumlarda samarali foydalanilishi mumkin. Tizimning bir qancha foydali hususiyatlari mavjud, bular:

- Tezkor xabardor qilish
- Shaxsiy ma'lumotlar ximoyasi ta’minlash
- Kiberhujumlarning oldini olish
- Jiddiy moliyaviy zararlarning oldini olish
- Ma'lumotlarni kuzatishdan iborat

Shunday qilib, **CitizenSec** tizimi har qanday tashkilot yoki shaxs uchun ma'lumotlarni himoya qilishda samarali yordamchi bo'la oladi.

Ma’lumotlar har kuni to’ldirilib boriladi va sun’iy intellekt orqali qayta ishlanadi, ma’lumotlar manbaalari sifatida :

1. OSINT (Open-Source Intelligence) – ochiq manbalar: forumlar, bloglar, ijtimoiy tarmoqlar, xabarlar tahlil qilinadi.
2. Dark Web va Deep Web – maxfiy forumlar, ma’lumotlar bozorlari.
3. Honeypotlar – maxsus tuzilgan tuzoq tizimlari orqali hujumchilar faoliyatini kuzatish.
4. Malware – zararli dasturlar bazalari (VirusTotal, Hybrid Analysis va boshqa).
5. CTI Feeds va Sharing Platformalar – STIX/TAXII, MISP, AlienVault OTX kabi tizimlardan tahdid ma’lumotlari almashinuvi orqali UZ segmenti uchun ma’lumotlar olinadi.
6. Tahliliy vositalar – SIEM va boshqa cloud tizimlari orqali log-fayllar va hodisalar tahlili orqali ma’lumotlar almashiniladi.

#	Sohalar	Namuna domenlar	Zarar ko‘rganlarning tahminiy soni
1	Hukumat & E-hizmatlar	egov.uz, gov.uz, e-imzo.uz	4,485,223
2	Ta’lim	dtm.uz, edu.uz, emaktab.uz, maktab.uz	2,165,981
3	Telekommunikatsiya & ISP	uztelecom.uz	667,033
4	E-tijorat & Moliyaviy xizmatlar	olx.uz, payme.uz	719,638
5	Auksion & Savdo	e-auksion.uz	296,540
6	Texnologiya & IT	uzbekcoders.uz, plcforum.uz.ua	799,295
7	Transport & Logistika	uzbmb.uz	426,037
8	Ommaviy axborot vositalari & Ko‘ngilochar	mediabay.uz	138,914
9	Ta’limga oid resurslar	uz.kundalik.mobile	131,075

Ushbu jadvalda siz asosan 2023-2024 yillar orasida o’tkazilgan tekshiruvlar va kiber razvedka ma’lumotlari tahlilining tahminiy natijalarini ko’rishingiz mumkin. Ma’lumotlar deyarli har kuni qo’shilib, yangilanib boriladi, shu sabab ko’rsatgichlar va statistika doimiy o’zgaruvchan. Siz hozirda maxsus telegram bot orqali o’z ma’lumotlaringizni tekshirishingiz mumkin. Keyinchalik har bir fuqaro o’zining unikal ma’lumotlari (telefon raqami, ism familiyasi, email, passport) orqali xavfsizligi holatini tekshirishi mumkin bo’ladi.

O‘zbekistonda oxirgi 6oylik ma’lumotlar tahliliga ko’ra, 10,023 ta kompyuter infostealer viruslari bilan zararlangan. Eng so‘nggi infostealer ma’lumotlari 2025-yil 22-mart kuni yuklangan.

Ko‘pchilik parollarini yangilash orqali kiberxavfsizlik tahdidi bartaraf etildi deb o‘ylaydi. Ammo **Cyber Threat Intelligence** natijalari shuni ko‘rsatadiki, parollar yangilangan taqdirda ham quyidagi xavflar saqlanib qolishi mumkin:

1. **Credential Stuffing va eski parollardan foydalanish**
   - Hujumchilar avvalgi sizib chiqqan parollarni boshqa xizmatlarga nisbatan sinab ko‘radi
   - Agar foydalanuvchi eski parolni boshqa joyda ishlatgan bo‘lsa, bu hisoblar hali ham xavf ostida bo‘lishi mumkin.
2. **PII** (Shaxsiy identifikatsiya ma’lumotlari) orqali ijtimoiy muhandislik hujumlari
   - Shaxsiy ma’lumotlaringiz (ISM, email, telefon, IP-manzil) yordamida spear-phishing va social engineering hujumlari amalga oshirilishi mumkin.
   - Hujumchilar SIM swap yoki Account Takeover (ATO) usullari orqali 2FA (ikki bosqichli autentifikatsiya) himoyasini aylanib o‘tishi ham mumkin.
3. **Qayta takror ishlatiladigan parollar va boshqa tizimlarga tahdid**
   - Foydalanuvchilar ko‘pincha bir xil yoki o‘xshash parollardan foydalanadi.
   - Yangi parol ham avvalgi parol ko’rinishida bo‘lsa (masalan, Meningparolim2024 → Meningparolim2025), uni **Password Spraying, brute-force** hujumlari orqali topish osonlashadi.
4. **Hujumchilar allaqachon tizimga kirib olgan bo‘lishi mumkin**
   - Agar hujumchilar **Access Token, Session Hijacking**, yoki **Backdoor** orqali tizimga kirgan bo‘lsa, parolni yangilash yetarli emas. Ular uzoq muddat tizimda qolish uchun barcha zamonaviy texnikalarni qo’llashadi.
   - **Persistent Threat** (uzoq muddatli tahdid) mavjud bo‘lishi mumkin, masalan, **APT** hujumlari orqali tizim ichida yashirin qolish mumkin. Bu esa uzoq muddat kiberjosuslik amaliyotlarini bajarish imkonini beradi.

Yuqoridagilar sabab siz o’z ma’lumotlaringiz, tashkilot va xodimlar ma’lumotlarini doimiy monitoring qilib borishingiz zarur. Bu sizga:

- Kim va qachon zararlanganligi
- Qanday kiber xujum natijasida zararlanganligi
- Zarar ko’lamini baholash
- Bundan tashqari zararlanish nuqtasini aniqlash orqali tizimda tarqalib ketishning oldini olishingiz mumkin bo’ladi.
- Xodimlarning ma’lumotlari sizib chiqishi haqida tezkor xabardor bo’lishingiz, tezkor choralar ko’rish imkoniyatini yaratadi. Kritikal darajadagi muhim axborot infratuzilmalarida (MAI) bu juda muhim, aks holda zarar ko’lami kiberdiversiya va kiberterrorizm holatigacha borishi mumkin.

Ushbu jadvalda siz asosan 2024-yilning 4-choragi uchun IT provayderlarga tegishli bo'lgan foydalanuvchilarning sizib chiqqan ma'lumotlari haqida qisqacha statistikani ko'rishingiz mumkin.

Provayder	Infostealer turlari	Domenlar
Eskiz IT	RedLine (160), Lumma (120), Vidar (22), Raccoon (20)	my.eskiz.uz host1.eskiz.uz
Uztelecom	RedLine (2446), Lumma (968), Vidar (376), Raccoon (134)	cabinet.uztelecom.uz msms.uztelecom.uz
AIRNET	RedLine (60), Lumma (44), Vidar (8), Raccoon (4)	billing.airnet.uz cpanel.airnet.uz
Ahost	RedLine (562), Lumma (332), Vidar (80), Raccoon (26), Azorult (22)	clients.ahost.uz server1.ahost.uz

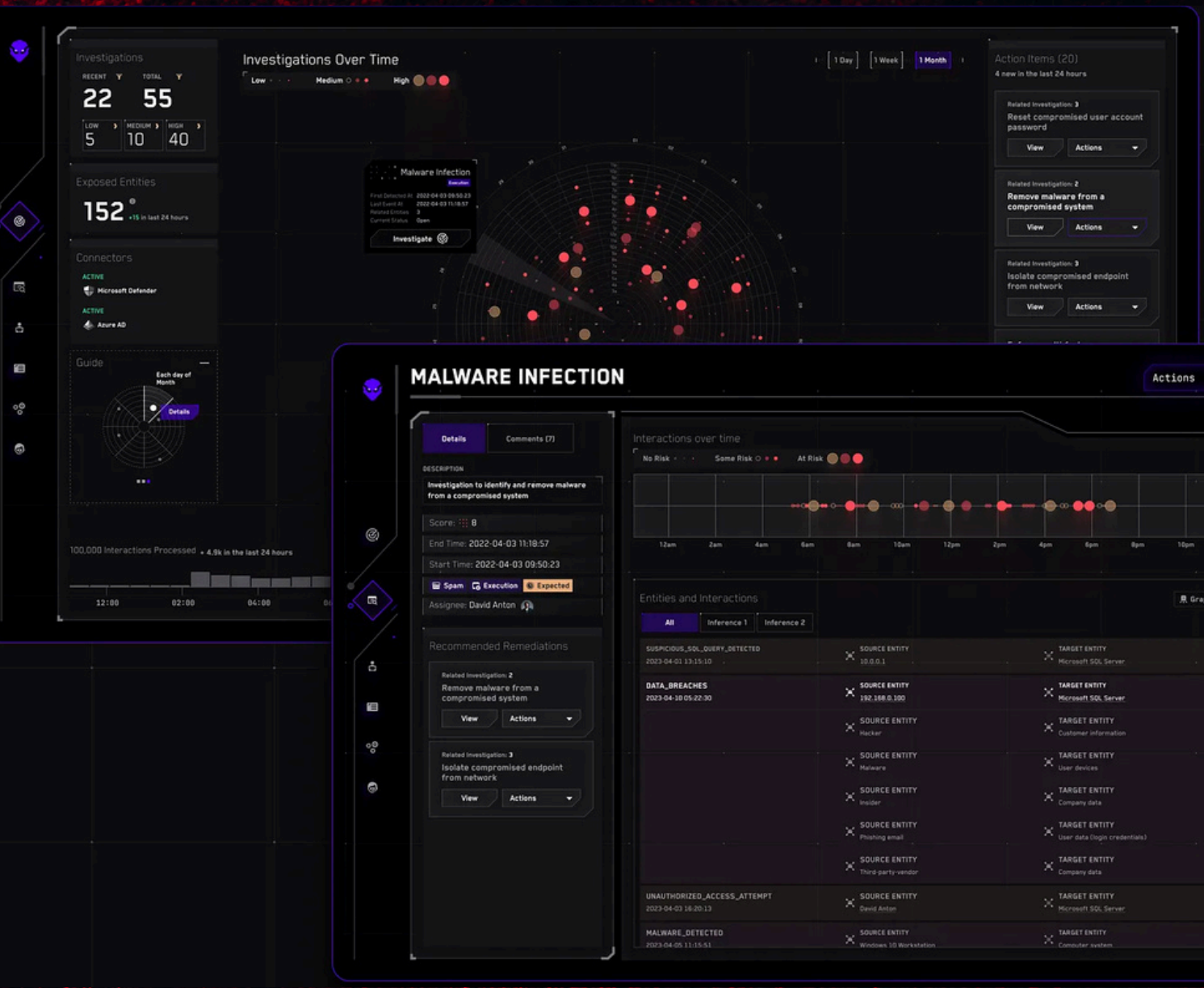
Xosting va provayderlar uchun xavflar

Brend obro'siga putur yetishi. Hosting kompaniyasining mijozlar oldidagi ishonchi pasayadi. Ma'lumotlari buzilgan mijozlar boshqa xizmat ko'rsatuvchilarga o'tib ketishi mumkin. Bu esa daromadning kamayishiga va bozor ulushining yo'qotilishiga olib keladi.
Regulyatorlar va qonuniy muammolar. O'zbekiston fuqarolari shaxsiga doir ma'lumotlarni himoya qilish to'g'risidagi qonunlari buzilgan bo'lsa, provayderlar jarimalar yoki litsenziya cheklovlariga duch kelishi mumkin. Xalqaro mijozlar uchun esa GDPR kabi qonunlarga zid kelish katta moliyaviy yo'qotishlarga sabab bo'lishi mumkin.
Ichki tizimlarning buzilishi va maxfiy ma'lumotlarning ochilishi. Hosting provayderlariga oid ma'lumotlar buzilgan bo'lsa, admin panellar, billing tizimlari va texnik xizmat platformalari xavf ostida qoladi. Xakerlar root-level (administrator darajasidagi) kirish huquqlarini olish orqali provayder infratuzilmasini butunlay egallashi mumkin. Provayderlar 2fa xizmatini faqat xohishga ko'ra emas, balki majburiy yoqishi hamda foydalanuvchilar xavfsizligi monitoringini ham olib borishi zarur.

Mijozlar uchun xavflar

Shaxsiy va biznes ma'lumotlarining o'g'irlanishi. Hosting foydalanuvchilarining login va parollari buzilgan bo'lsa, xakerlar ularning veb-saytlariga yoki email tizimlariga kira oladi. Natijada mijozning biznesi yoki shaxsiy ma'lumotlari xavf ostida qoladi. Fishing va firibgarlik hujumlari. orqali ma'lumotlari o'g'irlangan mijozlar kiberjinoyatchilar nishoniga aylanadi. Hujumchilar hosting provayderlarining nomidan fishing xabarlar yuborib, mijozlardan to'lov ma'lumotlari yoki shaxsiy ma'lumotlarni olishga harakat qilishi mumkin.

CYBERBRO



Davlat va xususiy sektor vakillari so’rov asosida o’zlariga tegishli bo’lgan IT tizimlari va ularga oid sizib chiqqan ma’lumotlarni batafsil hisobot ko’rinishida olishlari mumkin. Ushbu hisobotda foydalanuvchilar, zararlangan resurslar, faol parollar va zararlovchi virus haqida ma’lumot mavjud bo’ladi.

Jami 60 dan ortiq davlat tashkilotlari, vazirliklar hamda 15 ta bankga oid ma’lumotlarning sizib chiqishi holatlari aniqlangan. Quyida boshqa sohalarda ma’lumotlarning sizib chiqishi holatlari haqida qisqacha :

Nomi	Infostealer turlari	Domenlar
O‘zbekiston Respublikasi Markaziy banki	20 (Lumma, Generic Stealer, RedLine, Vidar)	cbu.uz
Ipoteka bank	452 (RedLine, Lumma, Vidar, Mystic, Raccoon)	ipotekabank.uz
Asaka Bank	202 (RedLine, Lumma, Vidar, Raccoon, Mystic)	asakabank.uz
Kapital Bank	80 (RedLine, Lumma, Vidar, Raccoon)	kapitalbank.uz
Hamkorbank	436 (RedLine, Lumma, Vidar, Raccoon, Azorult, Mystic)	hamkorbank.uz
Energetika vazirligi	115 (RedLine, Lumma)	minenergy.uz
Davlat soliq qo‘mitasi	210+ (RedLine, Lumma, Raccoon, Mystic)	soliq.uz
Davlat bojxona qo‘mitasi	140 (RedLine, Vidar)	customs.uz

Muayyan tashkilot bo‘yicha batafsil hisobot olmoqchi bo’lsangiz, biz bilan bog’laning.

Agar ushbu tashkilotlarning IT xavfsizlik bo‘limlari bu ma’lumotlarning to’liq shakliga qiziqsa, CYBER-BRO kompaniyasi kiber razvedka tahlili natijalarini va barcha foydalanuvchilarga tegishli ma’lumotlarni taqdim etishi mumkin.

Terminlarning ma’nolari

- Threat Intelligence (TI) – kiber tahdidlarni aniqlash, tahlil qilish va oldini olish uchun ma’lumotlar to‘plami.
- Threat Actor – kiberjinoyatchilar yoki zararli faoliyat yurituvchi shaxslar/guruhlar.
- APT (Advanced Persistent Threat) – uzoq muddatli, murakkab kiberhujumlar amalga oshiruvchi va davlatlar tomonidan moliyalashtiriluvchi xakerlik guruhlari.
- Insider Threat – tashkilot ichidagi xodimlar tomonidan insident sodir etilishi.
- Cyber Kill Chain – hujum jarayoni bosqichlarini ifodalovchi model (Reconnaissance, Weaponization, Delivery, Exploitation, Installation, Command & Control, Actions on Objectives).
- TTP (Tactics, Techniques, and Procedures) – hujumchilarning ishlatadigan usullari va strategiyalari.
- MITRE ATT&CK – kiber tahdid aktorlarining TTP’larini tavsiflovchi ochiq ma’lumotlar bazasi.

Ko‘rsatkichlar va kuzatuv terminlari:

- IOC (Indicators of Compromise) – zarar izlari va namunalari (IP-manzillar, domenlar, hash-summalar).
- IOA (Indicators of Attack) – hujumlarning oldindan aniqlashga yordam beruvchi belgilari.
- Threat Hunting – faol kiber tahdidlarni qidirish jarayoni.
- Threat Intelligence Feeds – real vaqt rejimida tahdid ma’lumotlarini taqdim etuvchi manbaalar.
- Risk Score – tahdidning xavflilik darajasini ifodalovchi baholash tizimi.

Analitika va monitoring vositalari:

- SIEM (Security Information and Event Management) – xavfsizlik hodisalarini to‘plash va tahlil qilish tizimi.
- SOC (Security Operations Center) – xavfsizlik hodisalarini monitoring va tahlil qiluvchi markaz.
- Honeypot – hujumchilarni jalb qilish uchun ishlatiladigan tuzoq tizimi.
- Sandboxing – zararli kodni xavfsiz muhitda tekshirish usuli.
- DGA (Domain Generation Algorithm) – zararli dasturlar tomonidan avtomatik ravishda domen yaratish usuli.
- C2 (Command and Control) – zararli dasturlarni boshqarish uchun ishlatiladigan serverlar.

Standart va almashuv formatlari:

- STIX (Structured Threat Information eXpression) – kiber tahdidlarni tavsiflash uchun standart format.
- TAXII (Trusted Automated Exchange of Indicator Information) – tahdid ma’lumotlarini almashish protokoli.
- MISP (Malware Information Sharing Platform) – kiber tahdidlar bo‘yicha ma’lumot almashish platformasi.

Bu terminlarni siz **Cyber Threat Intelligence** platformamizdagi tahdidlarni kuzatish, bashorat qilish va oldini olish uchun mavjud imkoniyatlarda uchratishingiz mumkin.

E’tiboringiz uchun rahmat!

Kiberxavfsizlik sohasidagi zamonaviy yechimlarimiz hamda kiber akademiyamiz sizning ushbu sohadagi barcha ehtiyojlaringizga javob bera oladi. Biz bilan bog’laning.

Toshkent shahri, Yunusobod tumani, 12-mavze, 20A-uy

+998 91 791 77 00

info@cyber-bro.uz

CYBER-BRO.uz