Azərbaycan Respublikası Xüsusi Rabitə və İnformasiya Təhlükəsizliyi Dövlət Xidməti
Kompüter İnsidentlərinə Qarşı Mübarizə Mərkəzi

MALWARE RESEARCH LAB REPORT

2023-2024 yekunları dair hesabat

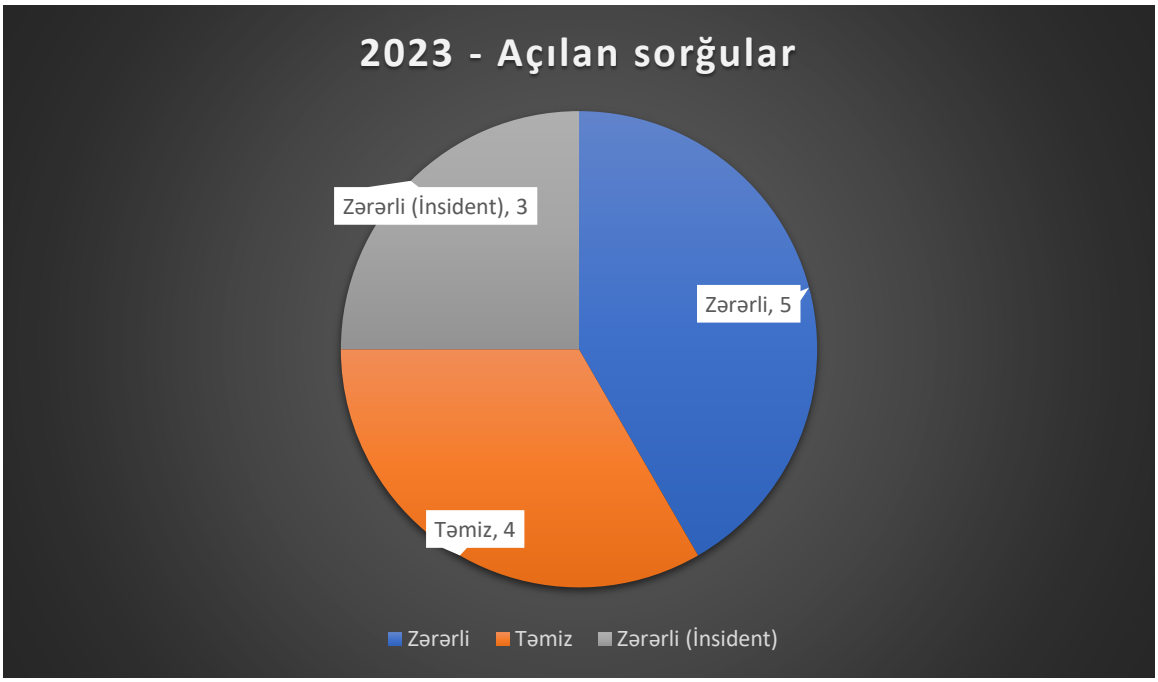
Analyst(s): Click or tap here to enter text.
E-Mail: mrl.report@cert.gov.az
SHA-1: Click or tap here to enter text.
Timestamp: 12/25/2024

MÜNDƏRİCAT

2023-cü il

Virus laboratoriya

2023-cü il ərzində laboratoriyamızda (idarəetmə sistemi) ümumilikdə 12 sorğu açılmışdır. Açılan sorğulardan 3-ü dövlət qurumlarında baş verən insidentlər ilə bağlı olmuşdur. Aparılmış analizlər nəticəsində sorğuların 4-ü təmiz, geriyə qalan 8-i isə zərərli olaraq təyin edilmişdir.



Məqalələr

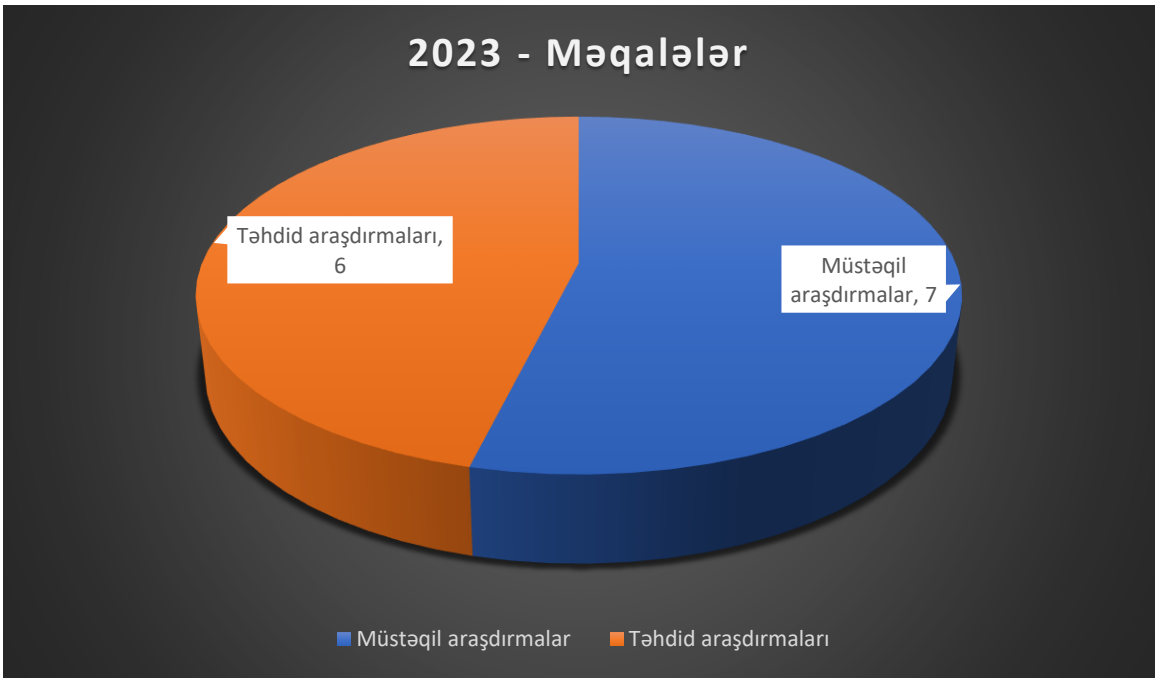
2023-cü ildə rəsmi saytımızda 13 məqalə yayımlanmışdır. Bunlardan 7-i müstəqil araşdırmalar, 6 məqalə isə təhdid araşdırmaları kateqoriyasına daxil edilmişdir.

Təhdid araşdırmaları:

- https://mrl.cert.gov.az/az/articles/view/95
- https://mrl.cert.gov.az/az/articles/view/108
- https://mrl.cert.gov.az/az/articles/view/114
- https://mrl.cert.gov.az/az/articles/view/94
- https://mrl.cert.gov.az/az/articles/view/93
- https://mrl.cert.gov.az/az/articles/view/92

Müstəqil araşdırmalar:

- https://mrl.cert.gov.az/az/articles/view/115
- https://mrl.cert.gov.az/az/articles/view/111
- https://mrl.cert.gov.az/az/articles/view/107
- https://mrl.cert.gov.az/az/articles/view/104
- https://mrl.cert.gov.az/az/articles/view/103
- https://mrl.cert.gov.az/az/articles/view/100
- https://mrl.cert.gov.az/az/articles/view/98



Proyektlər

Tusi Paleon

2023-cü il sentyabr ayında laboratoriya olaraq zərərverici forensikası üçün nəzərdə tutulan "**Tusi Paleon**" alətinin 1.0b beta versiyasını istifadəyə verdik. Sözü gedən alətin yeni versiyasıları ilə birlikdə yeni təlimatlardırma sisteminə keçid edildi.

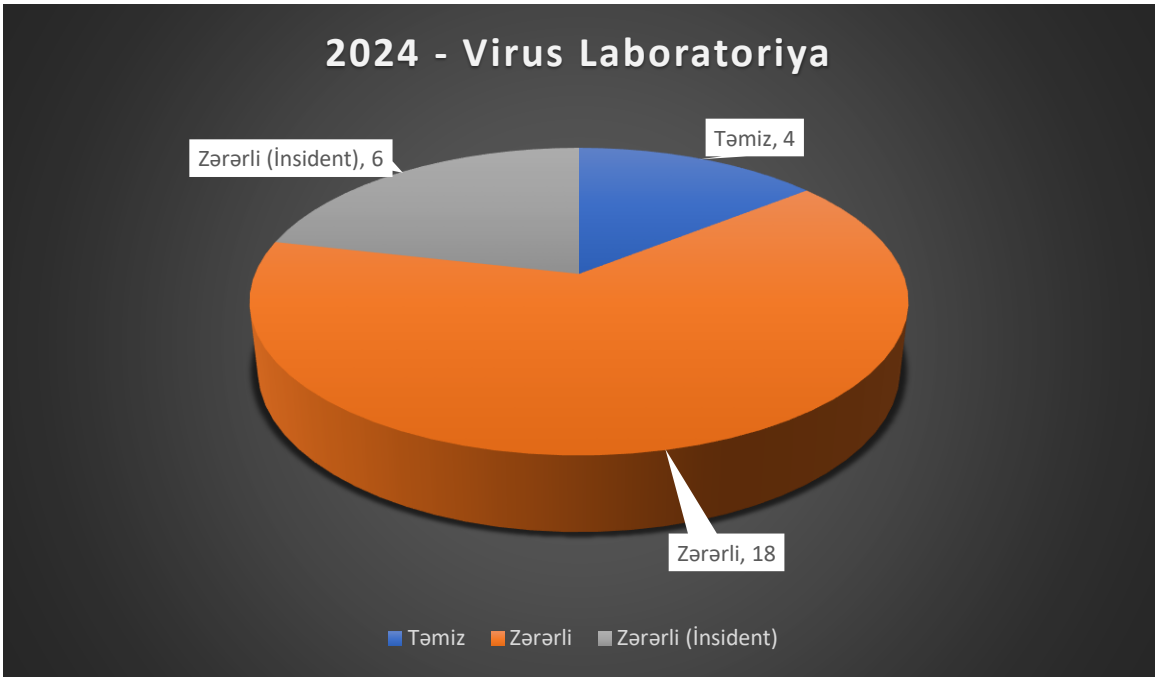
Tusi Paleon UI

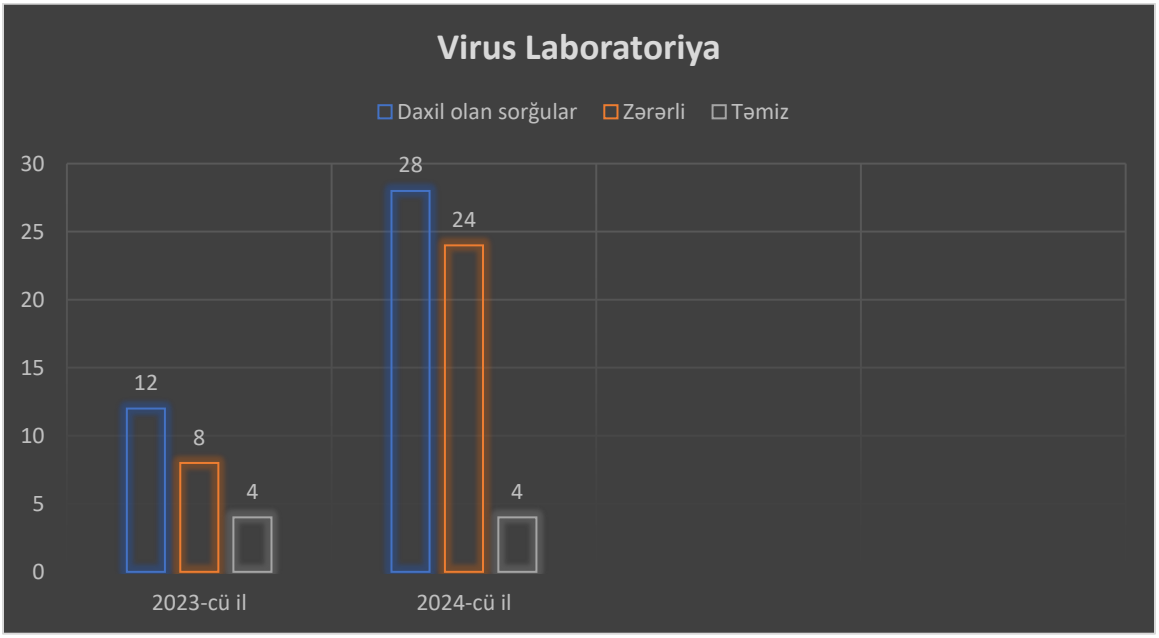
Tusi Paleon alətinin ixrac etdiyi məlumatları emal etmək üçün "**Tusi Paleon UI**" aləti də 2023-cü ildə ictimaiyyətə təqdim edildi.

2024-cü il

Virus Laboratoriya

2024-cü il laboratoriyamızda ümumilikdə 28 sorğu açılmışdır. Açılan sorğulardan 6-sı dovlət qurumlarında baş verən insidentlər ilə bağlı olub. Aparılmış analizlər nəticəsində sorğulardan 4-ü təmiz, 24-ü zərərli olaraq təyin edilmişdir.





Şəkil 1 Aşağıdakı diaqram öncəki il ilə virus laboratoriyasına daxil olan sorğuların müqayisəsini göstərir.

Məqalələr

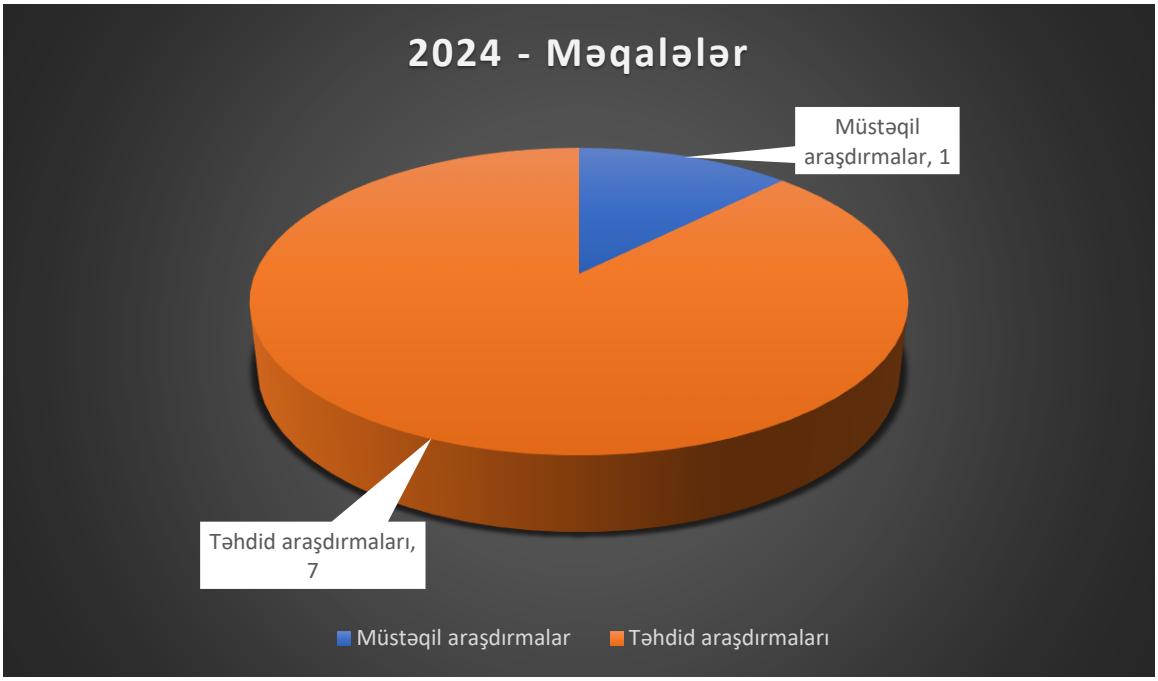
2024-cü ildə rəsmi saytımızda 8 məqalə paylaşılmışdır. Bunlardan 7-si təhdid araşdırmaları, 1-i isə müstəqil araşdırmalar kateqoriyasına daxil edilmişdir.

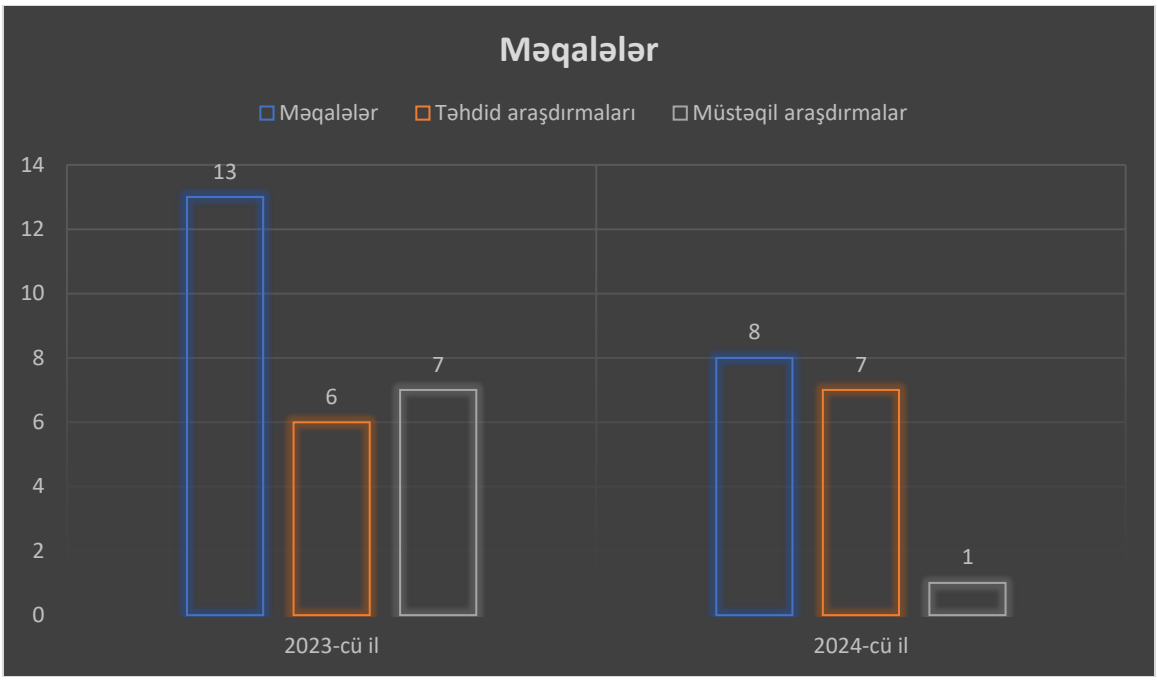
Təhdid araşdırmaları

- https://mrl.cert.gov.az/az/articles/view/125
- https://mrl.cert.gov.az/az/articles/view/124
- https://mrl.cert.gov.az/az/articles/view/118
- https://mrl.cert.gov.az/az/articles/view/121
- https://mrl.cert.gov.az/az/articles/view/117
- https://mrl.cert.gov.az/az/articles/view/119
- https://mrl.cert.gov.az/az/articles/view/120

Müstəqil araşdırmalar

https://mrl.cert.gov.az/az/articles/view/126





Şəkil 2 Aşağıdakı diaqram öncəki il ilə paylaşılan məqalələrin müqayisəsini göstərir.

Proyektlər

10CHunter

2023-cü ildə hazırlanmasına qərar verilən “10CHunter” alətinin ilk prototipi bu il etibarı ilə tamamlanaraq sınaq çalışmalarına başlanılmışdır. 2025-ci ilin ilk rübündə ictimaiyyət ilə paylaşılması planlaşdırılır.

Tusi Paleon & Paleon UI

2024-cü il dekabr ayında Tusi Paleon alətinin 1.4.0 və paralel olaraq Paleon UI alətinin 1.1.0b versiyası istifadə verilmişdir.