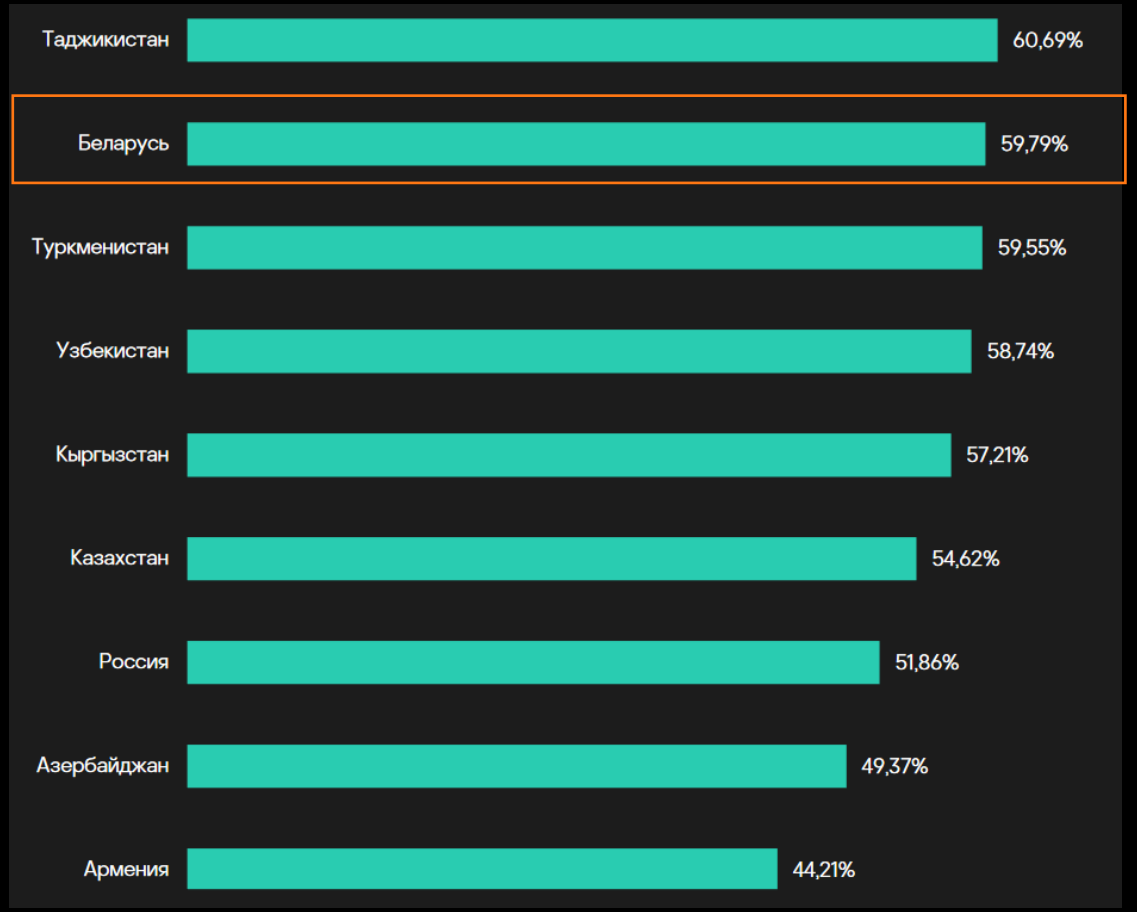
Защита от угроз 0-day в современных реалиях

Максим Автоненко
ООО “Безопасные технологии и системы”

Минск, 2024

Ландшафт киберугроз в Беларуси

С Q1-2023 по Q1-2024 зафиксировано в среднем 60 атак в квартал на компании из различных сфер деятельности.

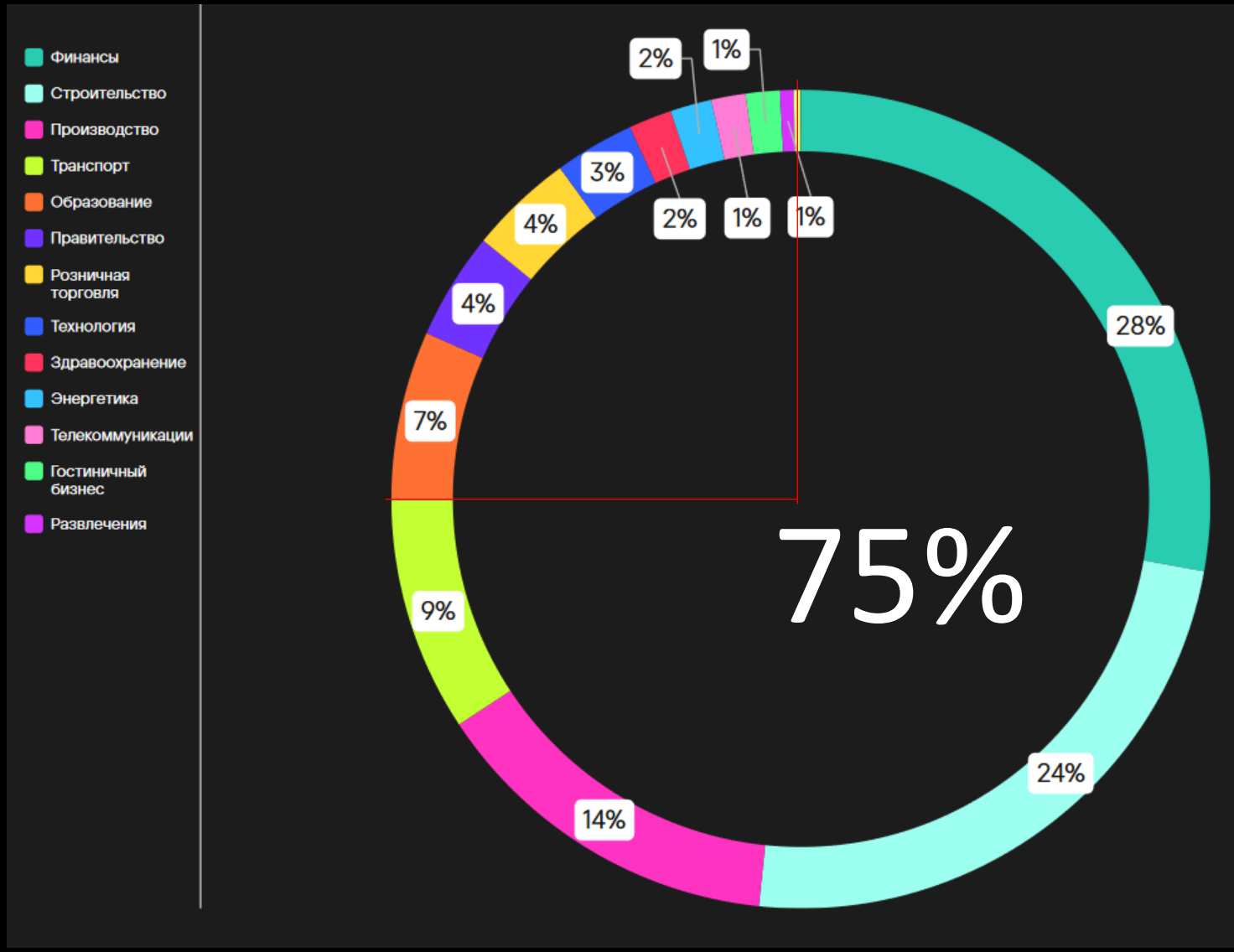


Согласно отчёту Касперского по странам СНГ Беларусь заняла 2-е место по количеству атак в 2024 году.

https://go.kaspersky.com/rs/802-IJN-240/images/Report_Threat_Landscape_RU.pdf

Ландшафт киберугроз в Беларуси

75% - атак приходилось:
финансы;
строительство;
производство;
транспорт.



Ландшафт киберугроз в Беларуси

По информации в открытых источниках видно, что результатом атак нередко становятся утечки персональных данных клиентов компаний.

крупный сервис бронирования пассажирских перевозок

https://auto.onliner.by/2024/02/21/atlas-vzlomali

крупный портал о недвижимости

https://t.me/s/cpd_by?q=realt

2-е место **по количеству атак в 2024 году.**

Ландшафт киберугроз в Беларуси

Всё чаще в СМИ нашей страны затрагивается тема персданных.

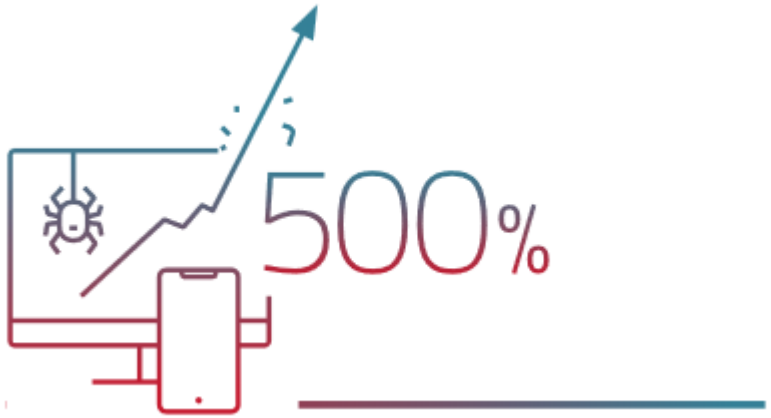
В 2024 г. Национальный центр защиты персональных данных получил 6 уведомлений о нарушениях системы защиты персональных данных, утечки коснулись около 2 млн записей с данными белорусских граждан.

Причина:
Нереализованные меры по обеспечению их защиты, а также незащищенность внешнего контура информационных систем.

2-е место **по количеству атак в 2024 году.**

Ситуация с угрозами продолжает ухудшаться

Атаки на мобильные приложения



по сравнению с 2023 число атак в 2024 на мобильные приложения выросло на 500%

Увеличение активности Хактивистов

Biggest worry for western countries supporting Ukraine

NoName057(16)

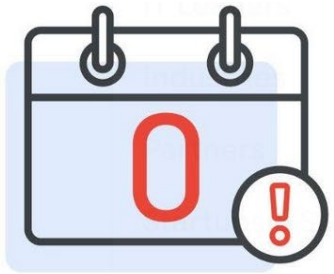
Anonymous Sudan found motivation in religion, politics and money

Killnet leader Killmilk became the most influential pro-Russian hacktivist

из отчета Radware

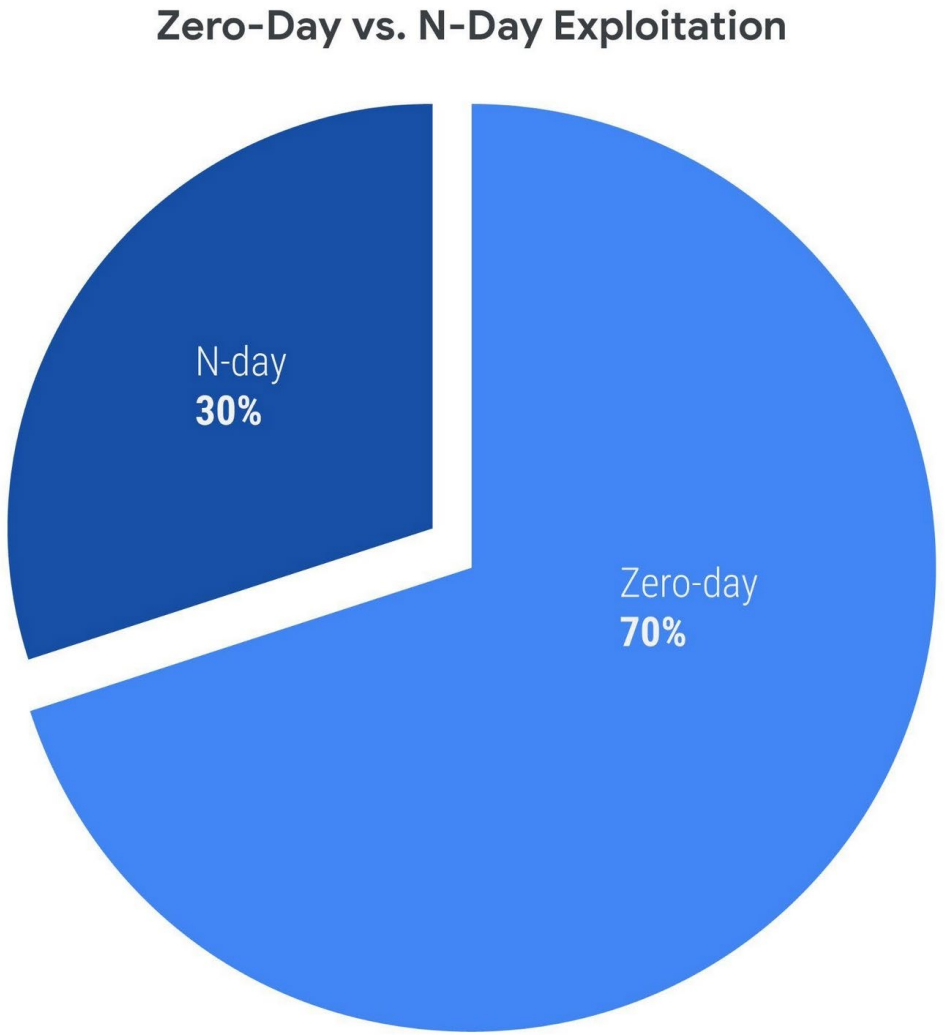
Outsource IT .BY

Ситуация с угрозами продолжает ухудшаться



70%
уязвимостей были эксплуатированы как 0-day

В 2023 году среднее время эксплуатации (Time-To-Exploit) составило пять дней, что значительно быстрее, наблюдавшегося среднего значения TTE в 32 дня в 2022 году.



https://cloud.google.com/blog/topics/threat-intelligence/time-to-exploit-trends-2023

Ситуация с угрозами продолжает ухудшаться

Разнообразие

Более 19,6 млн уникальных 0-day атак ежедневно в мире

Масштаб

Увеличение количества попыток эксплуатирования более чем на 400%.

Скорость

Автоматические атаки выполняются в разных регионах в течение 1 часа после первого удачного взлома.

из отчета paloaltonetworks

Ситуация с угрозами продолжает ухудшаться

Пример: CVE-2024-21762 (08-02-2024)

Уязвимость в **FortiOS**, которая позволяет провести атаку на межсетевой экран (МСЭ) снаружи защищаемого периметра и выполнить произвольный код.
Включена в каталог Known Exploited Vulnerabilities Catalog от CISA, содержащий уязвимости для, которых есть подтверждённые факты эксплуатации "in the wild“

IR Number	**FG-IR-24-015**
Date	**Feb 8, 2024**
Severity	**Critical**
CVSSv3 Score	**9.6**
Impact	**Execute unauthorized code or commands**
CVE ID	**CVE-2024-21762**

Информационный ресурс securitylab.ru "добродушно" упомянул о сотнях тысяч устройств, которые до сих пор не обновлены, подрывая безопасность систем

Требования регуляторов

ПЕРЕЧЕНЬ

требований к системе защиты информации, подлежащих включению в техническое задание

	Наименование требований	Условие об обязательности выполнения требований в соответствии с классом типовых информационных систем									
		4-ин	4-спец	4-бг	4-юл	4-дсп	3-ин	3-спец	3-бг	3-юл	3-дсп
4	Требования по защите системы защиты информации информационной системы										
4.1	Обеспечение изменения атрибутов безопасности сетевого оборудования, системного программного обеспечения и средств защиты информации, установленных по умолчанию	+	+	+	+	+	+	+	+	+	+
4.2	Обеспечение обновления объектов информационной системы	+	+	+	+	+	+	+	+	+	+

Обеспечить обновления = минимизировать риск

Но обеспечить **регулярные обновления ПО** ≠
защититься от 0-day угроз

Решение есть

1. Использование проверенных временем вендоров для защиты информации.
2. Использование ML для обнаружения 0-day.
3. Обновление сигнатур угроз не реже 1 раза в час.
4. Использование песочницы для динамического анализа неизвестных угроз.

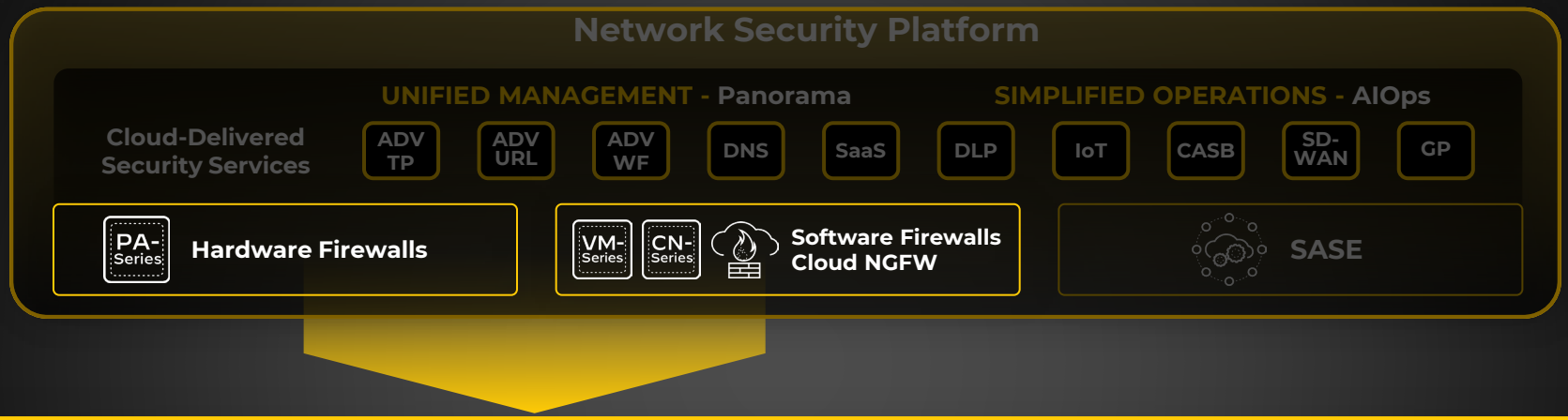
1.Использование проверенных временем вендоров для защиты информации.

Figure 1: Magic Quadrant for Network Firewalls

2. Использование ML для обнаружения 0-day.

Paloaltonetworks — Первый в Мире ML-Powered Next-Generation Firewall

Next Generation Firewalls



- **11 раз подряд лидер в Квадранте Gartner** для Сетевых Фаерволов
- **Встроенный ML 4го поколения :** лучшее в отрасли соотношение цены и качества

Быстрее

<10 seconds

от обнаружения угроз к их предотвращению. В 180 раз быстрее, чем конкурирующие продукты

Безопаснее

48%

благодаря встроенному машинному обучению в режиме реального времени предотвращено больше 0-day атак по сравнению с другими вендорами

3. Обновление сигнатур угроз не реже 1 раза в час

PARUS

PARUS SECURITY CLOUD

РОССИЙСКАЯ ФЕДЕРАЦИЯ

СВИДЕТЕЛЬСТВО

о государственной регистрации программы для ЭВМ

№ 2024612718

«Автоматизированная информационная система PARUS SECURITY CLOUD»

Правообладатель: ***Общество с ограниченной ответственностью «Стайл Телеком» (RU)***

Заявка № **2024610961**
Дата поступления **22 января 2024 г.**
Дата государственной регистрации
в Реестре программ для ЭВМ ***05 февраля 2024 г.***

Руководитель Федеральной службы по интеллектуальной собственности

ДОКУМЕНТ ПОДПИСАН ЭЛЕКТРОННОЙ ПОДПИСЬЮ
Сертификат 429b6a0fe3853164baf96f83b73b4aa7
Владелец Зубов Юрий Сергеевич
Действителен с 10.08.2023 по 02.08.2024

Ю.С. Зубов

Outsource IT .BY

PARUS SECURITY CLOUD возвращает стабильность в инфраструктуру на базе решений **Paloalto** и **Fortinet**:

- **Автоматическое** обновлений сигнатур безопасности
- **Минимальные** задержки получения обновлений
- **Усиленная** URL категоризация по кирилличному сегменту интернет
- **Белая** схема лицензирования

4. Использование песочницы для динамического анализа неизвестных угроз.


PARUS
PARUS BOX

PARUS BOX

Зачем нужна песочница для работы межсетевых экранов?

Свежие коллекции

Потоковый AV > 80%

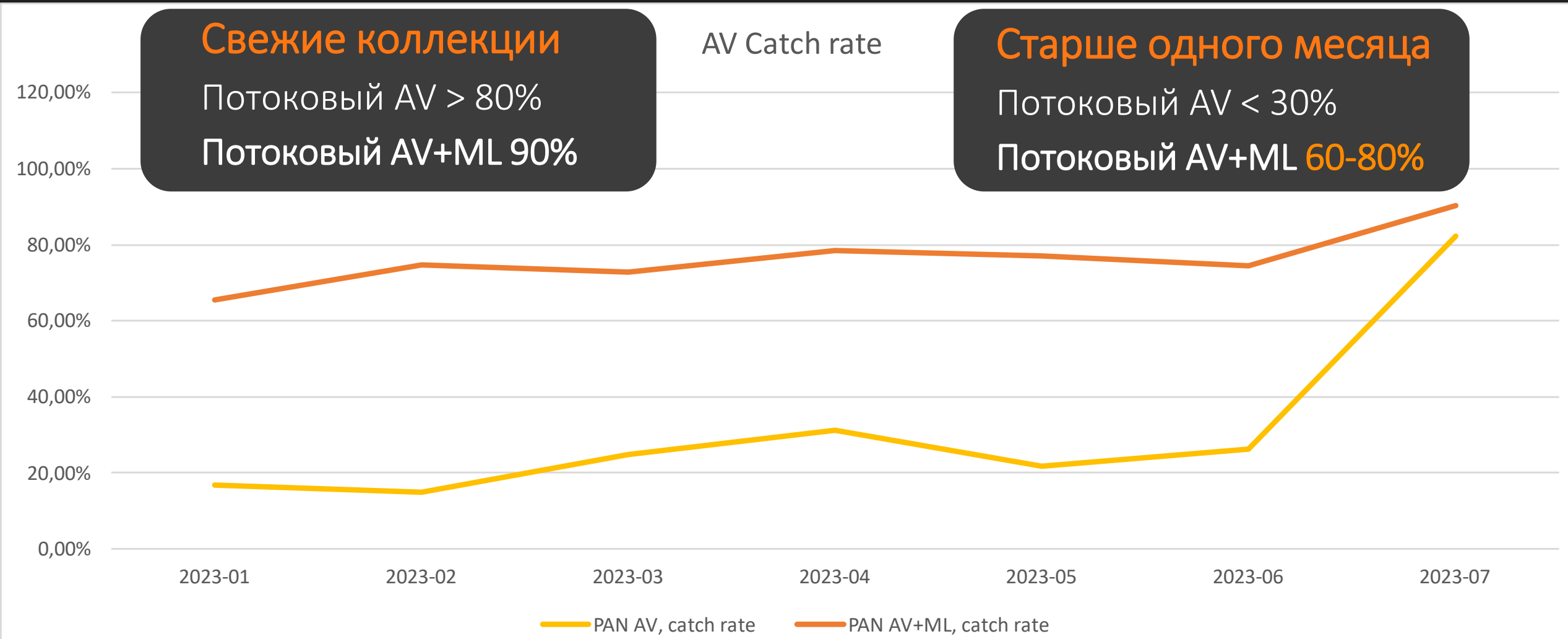
Потоковый AV+ML 90%

AV Catch rate

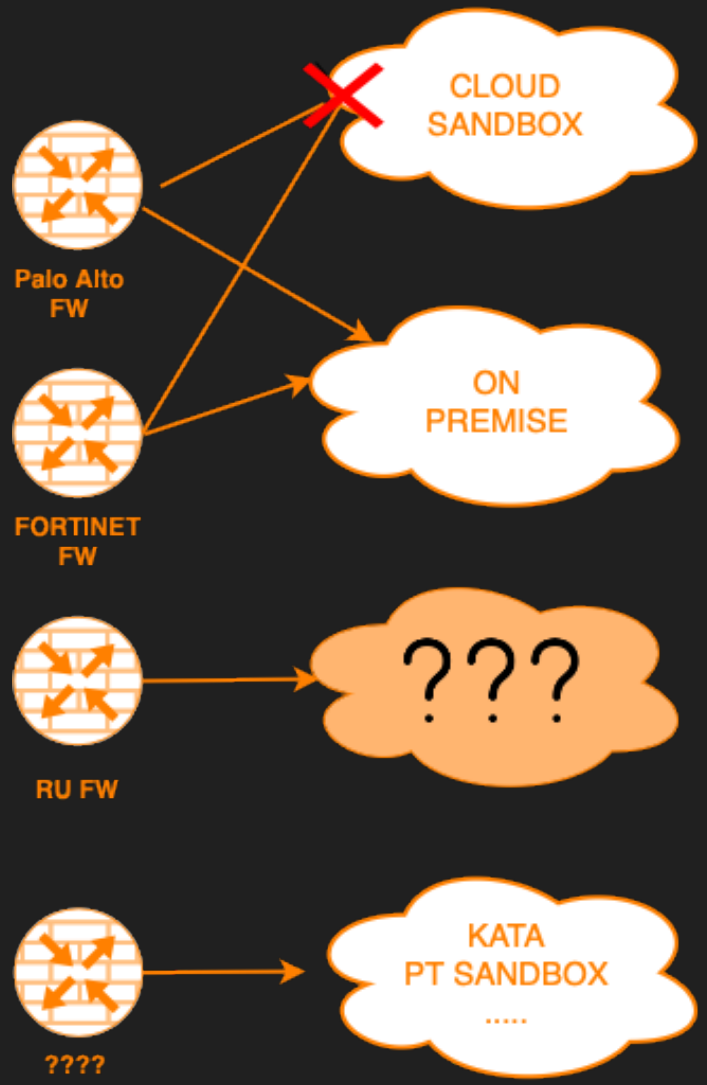
Старше одного месяца

Потоковый AV < 30%

Потоковый AV+ML 60-80%



PARUS BOX



Облачные сервисы производителей

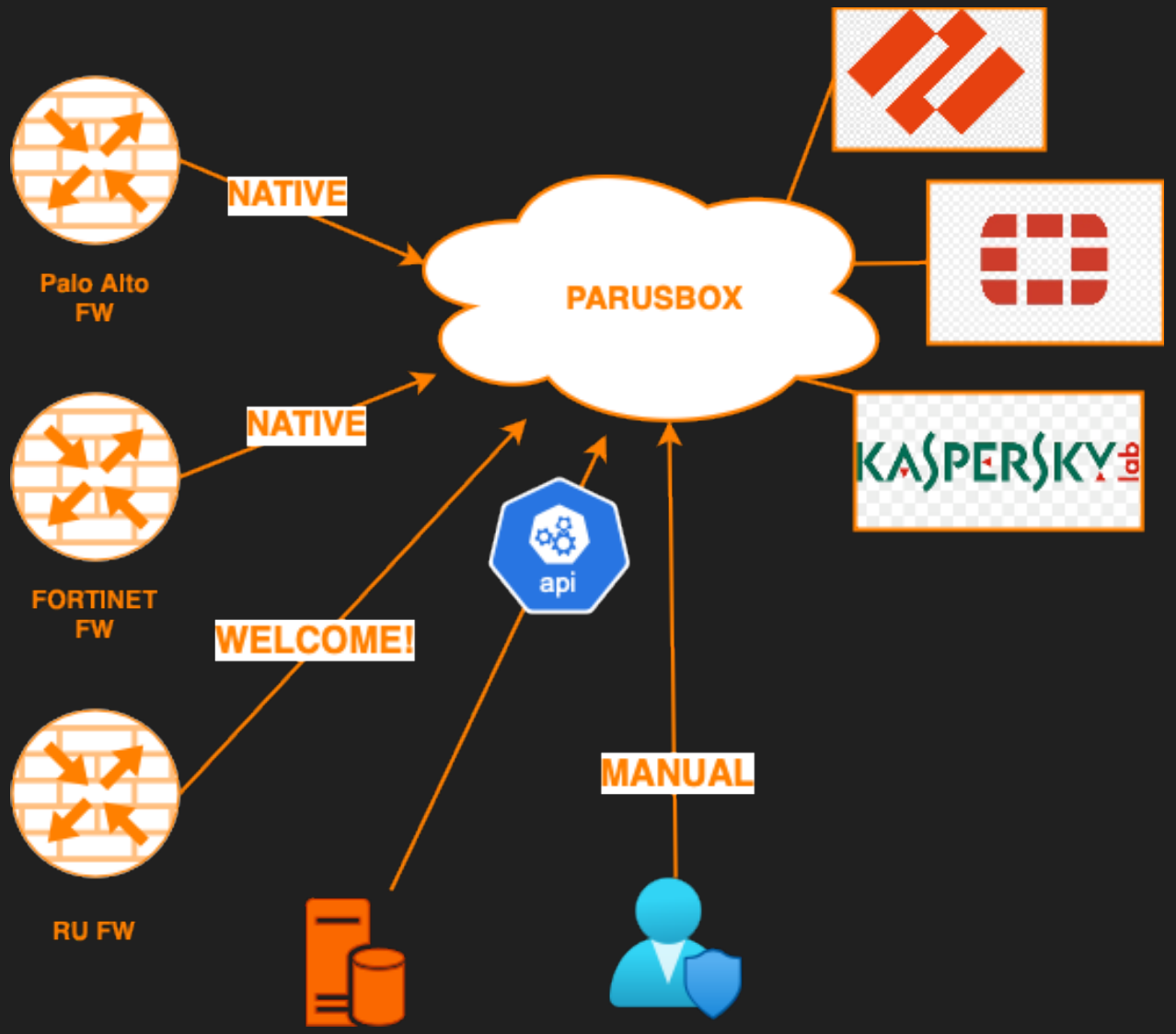
1. Зарубежные облака недоступны для РБ
2. Отправка файлов и мета-информации заграницу
3.Проверка только по базе/движку определенного производителя
4. Проприетарные протоколы взаимодействия

On-premise решения

1.Большой CAPEX, сложность ввоза, обслуживание и сервисная поддержка
2.Ограничения по производительности и масштабируемости
3.Ограничения по типам проверяемых файлов
4.Проприетарные протоколы.

Какие песочницы использовать для импортозаместительных межсетевых экранов?

PARUS BOX



CLOUD. REALTIME. MULTIVENDOR

00. Upload

Archive Detection (>20), extracting, calculation
File Type, Size Detection

01. PRE FILTER

PARUS DB
Palo Alto Threat Vault
Kaspersky Threat Lookup

02. STATIC SCAN

FORTINET

KASPERSKY

03. DYNAMIC SCAN

Palo Alto WF500 Farm
FortiSandbox Farm
Kaspersky Sandbox

04. CPORTAL

до 15 минут

PARUS BOX

PARUS

Проверка неизвестных файлов на предмет вредоносной активности

ПОДДЕРЖИВАЕМЫЕ ТИПЫ ФАЙЛОВ

- Adobe Flash
- Java Archives (JAR)
- MS Office
- Portable executables (PE)
- PDF
- Archives Password protected archives
- Scripts
- ELF
- APK

АНАЛИЗ ФАЙЛОВ

- Статический
- Поведенческий
  - Windows 7/10
  - Android ARM, x86
  - CentOS 7
  - Ubuntu 20

ВЕРДИКТЫ

- Benign
- Malware
- Grayware

PARUS BOX

Проверка неизвестных файлов на предмет вредоносной активности

ЛОКАЛИЗАЦИЯ

- Файлы не отправляются во внешние сервисы
- Сервис полностью локализован в РФ, на мощностях Yandex Cloud.
- В планах на следующий год развернуть локальное облако в аттестованном ЦОД РБ.

ИНТЕРФЕЙСЫ PARUSBOX

- Palo Alto NGFW (нативная интеграция)
- FortiGate (модуль FortiSandbox + DTL)
- API
- Portal Upload Form
- Готовность к интеграции с отечественными производителями межсетевых экранов

PARUS BOX

PARUS

ПОДДЕРЖИВАЕМЫЕ ТИПЫ ФАЙЛОВ

PE

.dll .exe .fon .ini .lnk .msi
.scr .upx

FLASH, JAR, PDF

.swf .jar .pdf

SCRIPT

.bat .cmd .js .jse .pl .ps1 .py .rc
.sh .vbs .wsf

ARCHIVE

.7z .ace .arj .bz2 .cab
.gz .iso .kgb
.lzh .rar .tar .tgz .xz .z
.zip

LINUX

.bin .conf .deb .elf
.img .rpm .so

MS-OFFICE

.csv .doc .docm .docx .dot .dotm
.dotx .iqy .one .pot
.potm .potx .ppam .pps .ppsm
.ppsx .ppt .pptm .pptx
.rtf .sldm .sldx .thmx .xlam .xls
.xlsb .xlsx .xlt .xltm .xltx

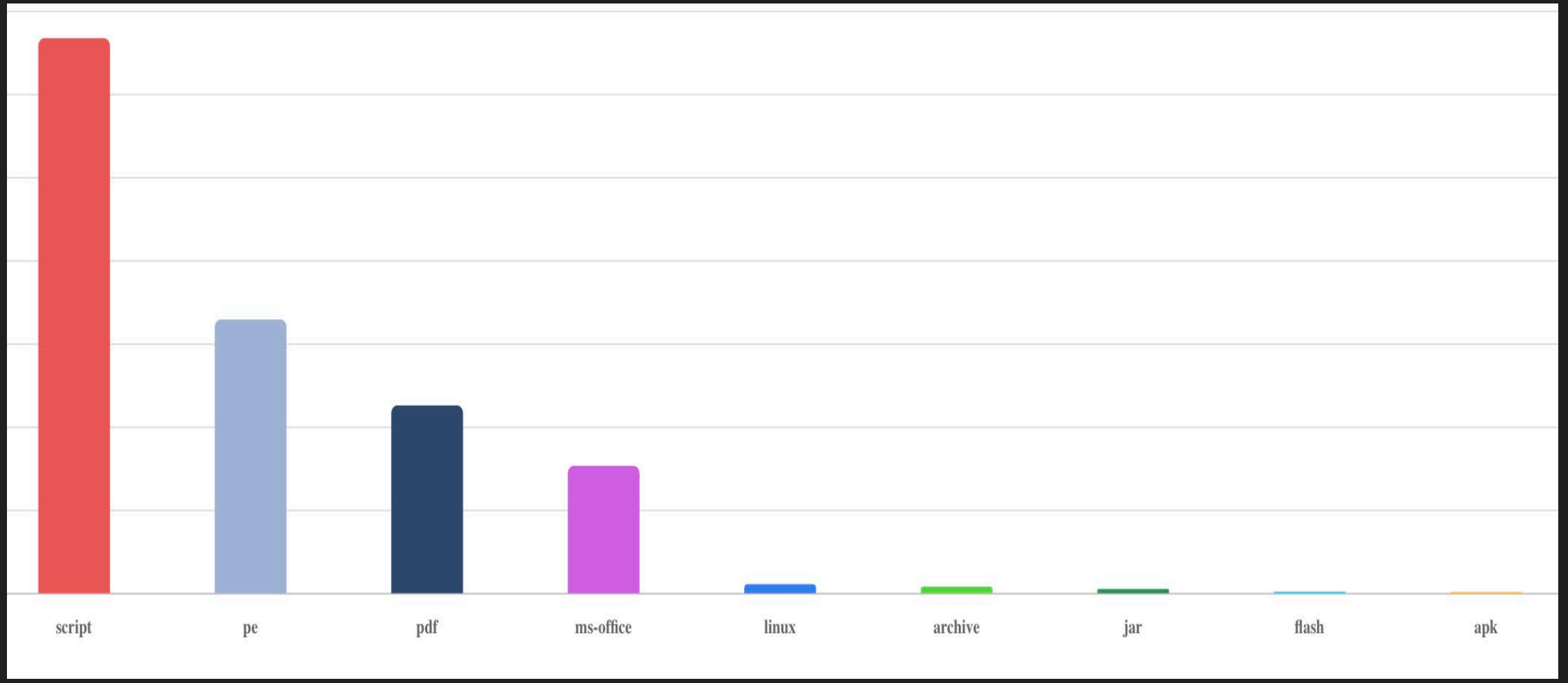
APK

.aab .apk .arsc .dex
.keystore .obb

PARUS BOX

PARUS

НАИБОЛЕЕ ЧАСТО ПРОВЕРЯЕМЫЕ ТИПЫ



PARUS BOX

PARUS

Verdict	MALWARE открыть VirusTotal
First seen (UTC)	10.10.2024 06:46:41
Last seen (UTC)	10.10.2024 06:46:41
Hits	1
File size	35511 байт
File type	archive
File name	GEFA-Order 739292638-002-UUE.UUE
Source URL	unknown
Source IP	64.188.23.211:51899
	UNKNOWN MEDIUM RISK

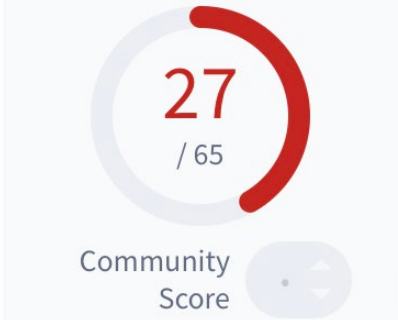
Таблица проверок

ИСТОЧНИК	ВЕРДИКТ	ДАТА (UTC)	ДЕТАЛИ
Palo Alto Networks	MALICIOUS	10.10.2024 06:47:09	Type: trojan Subtype: virus Family: WGeneric Name: Virus/Win32.WGeneric.ekpadt
Fortinet			-
Kaspersky			-

527e507dfe226e6e9aa4affea4979eed40deb83d06cbed8db6f5de087d272d72

Хронология (UTC)

10.10.2024 04:54 – PA Threat Vault create time
10.10.2024 06:46 – Palo Alto NGFW с актуальными установленными пакетами AV и WF пропускает этот файл как неизвестный на песочницу PARUSBOX
10.10.2024 06:49 - Устройство заказчика получает вердикт Malware по данному файлу



VirusTotal

10.10.2024 19.00

Kaspersky - VHO:Trojan PSW.MSIL.Stealer.gen
Fortinet – MSIL/Agent.RIJ!tr.dldr

PARUS BOX

PARUS

Verdict	MALWARE открыть VirusTotal
First seen (UTC)	17.10.2024 06:52:26
Last seen (UTC)	17.10.2024 06:52:26
Hits	1
File size	1837568 байт
File type	pe
File name	tun.dll
Source URL	objects.githubusercontent.com/github-production-release-asset-2e65be/590178204/94493c6b-4c34-436b-98fe-11cbc2d4fe06?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Credential=releaseassetproduction/20241017/us-east-1/s3/aws4_request&X-Amz-Date=20241017T065134Z&X-Amz-Expires=300&X-Amz-Signature=0d69035c744bdbb929284f7207e9708a522357fbd07471ba0a41f89ae9006c00&X-Amz-SignedHeaders=host&response-content-disposition=attachment;%20filename=InvisibleManXRay-x64.zip&response-content-type=application/octet-stream SHAREWARE AND FREEWARE LOW RISK
Source IP	185.199.108.133:443 UNKNOWN MEDIUM RISK

Таблица проверок

ИСТОЧНИК	ВЕРДИКТ	ДАТА (UTC)	ДЕТАЛИ	ОТЧЕТ
Palo Alto Networks	MALWARE	17.10.2024 07:00:30	-	
Fortinet	HIGH RISK	17.10.2024 06:56:00	Category: Trojan Name: N/A	

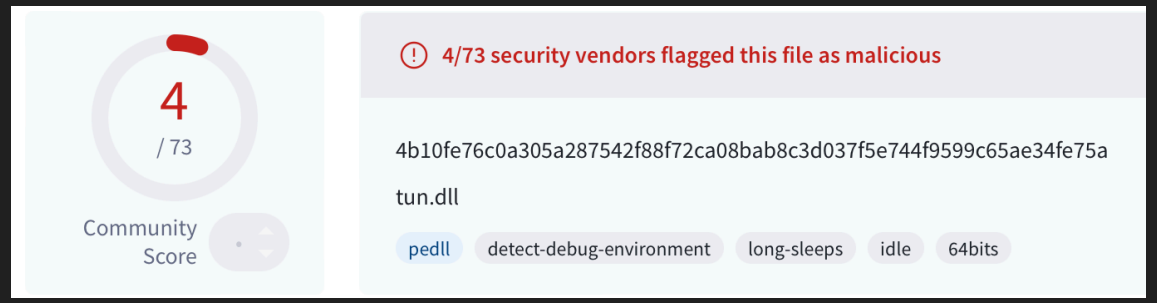
4b10fe76c0a305a287542f88f72ca08bab8c3d037f5e744f9599c65ae34fe75a

0-day (UTC)

17.10.2024 07:00 - Устройство заказчика получает вердикт Malware по данному файлу
17.10.2024 07:45 – PA Threat Vault NOT FOUND
17.10.2024 06:52 – KTIP NOT CATEGORIZED

VirusTotal

17.10.2024 07.45



PARUS BOX

PARUS

Чем больше источников, тем лучше

SHA256	Verdict Palo Alto	Verdict Fortinet	Kaspersky Lookup	Verdict Threat Vault	File type	File name
...ce4c0	Malware	Clean	Unknown	No data	pdf	reglament_rus.pdf

SHA256	Verdict Palo Alto	Verdict Fortinet	Kaspersky Lookup	Verdict Threat Vault	File type	File name
...0158e	Benign	Malicious	Unknown	Malicious	archive	DHL DOCS0001.arj

SHA256	Verdict Palo Alto	Verdict Fortinet	Kaspersky Lookup	Verdict Threat Vault	File type	File name
...b8a50	Malware	Clean	Malware	Malicious	ms-office	Quotation.xls

PARUS

ООО "Безопасные технологии и системы"
УНП 193303745

Напишите нам: info@outsourceit.by

Юр. адрес: 220053, Беларусь, г. Минск, ул. Нововиленская, д.38 каб.11

Почтовый адрес: 220026, Беларусь, г. Минск, ул. Жилуновича 26, а/я 96

Outsource IT .BY