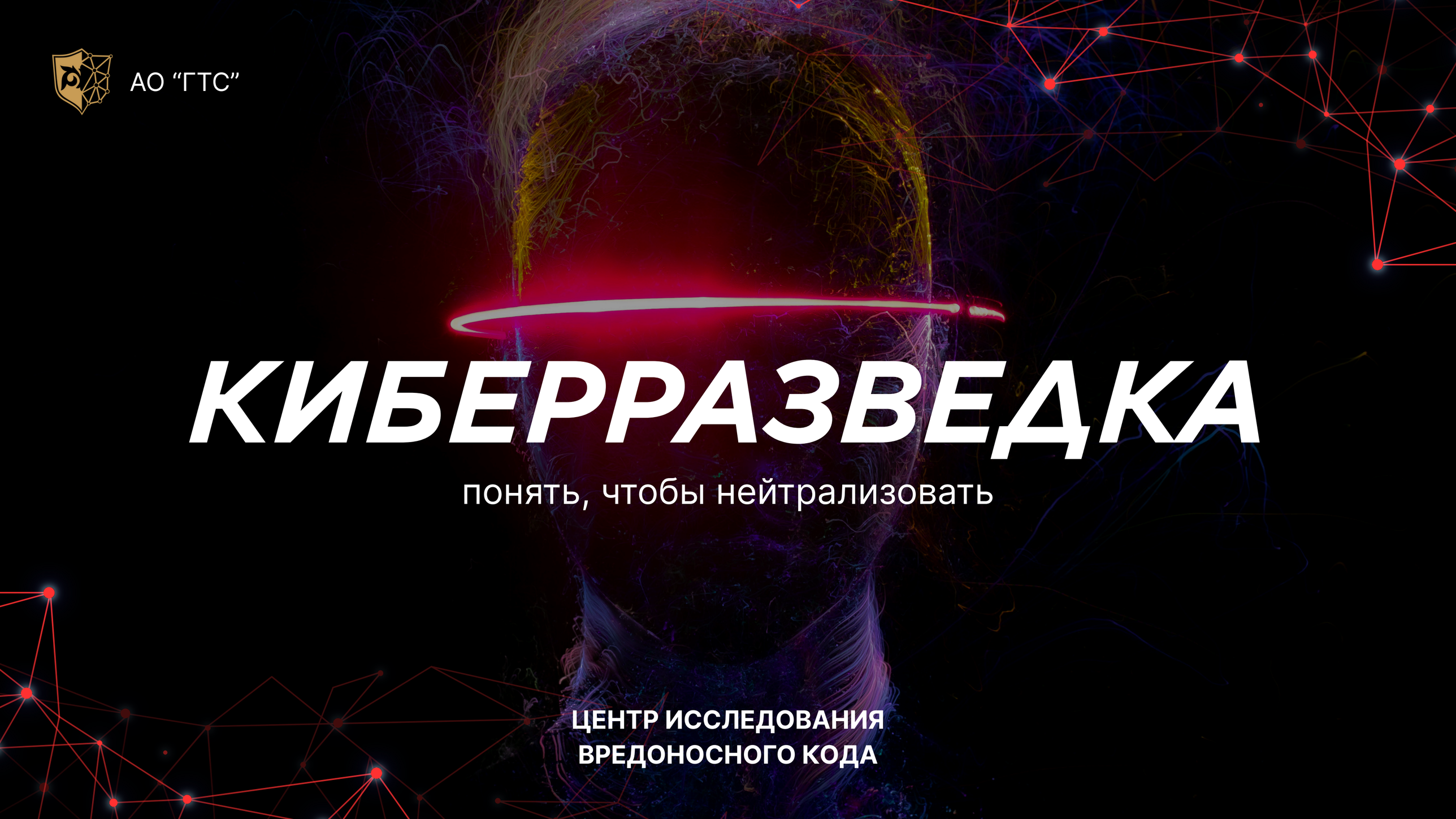


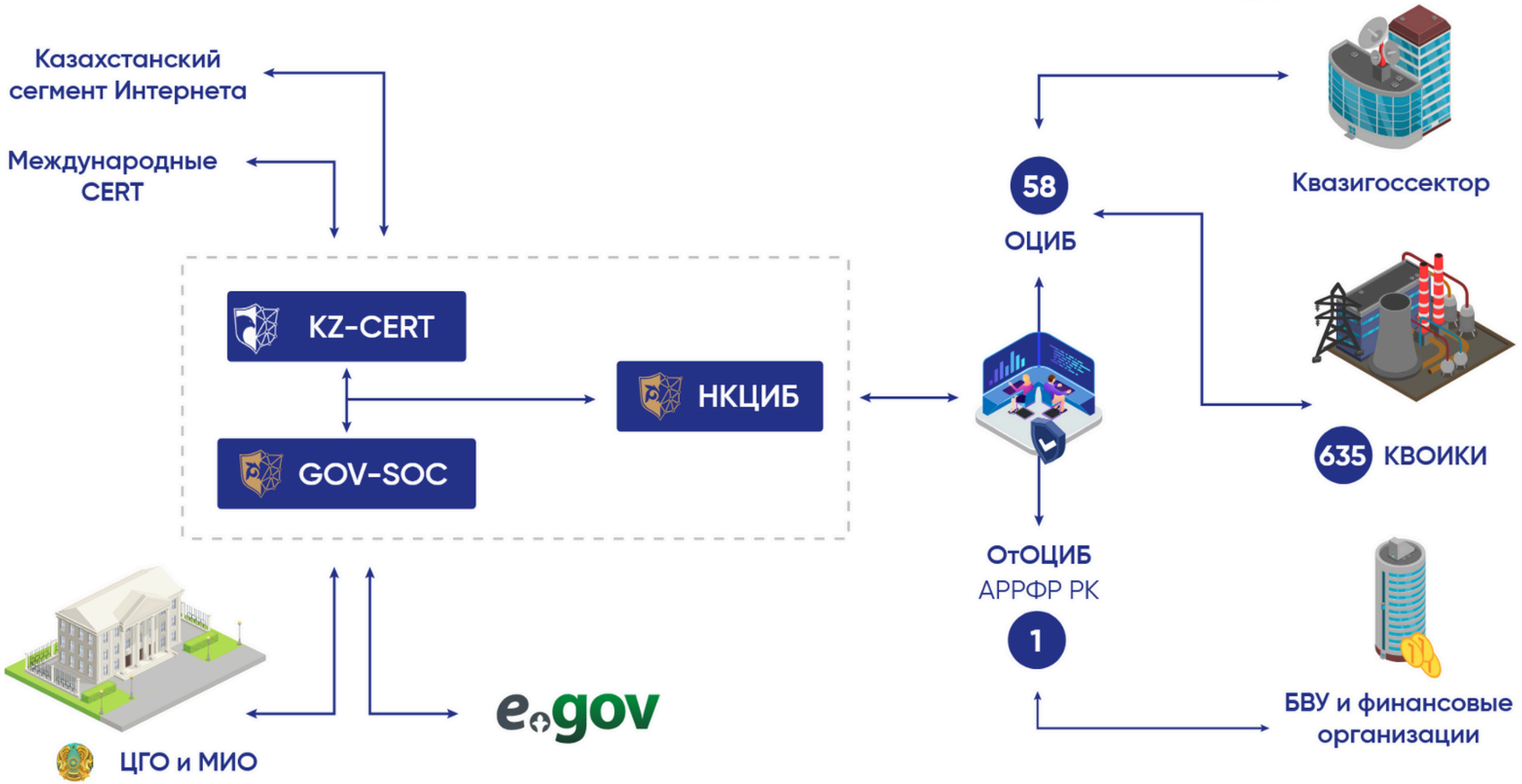
АО “ГТС”

КИБЕРРАЗВЕДКА

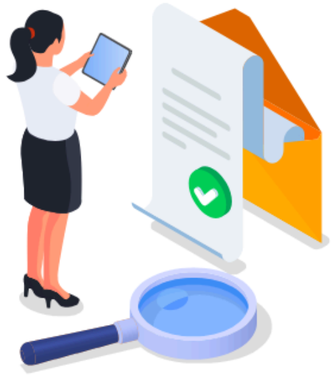
понять, чтобы нейтрализовать

ЦЕНТР ИССЛЕДОВАНИЯ ВРЕДОНОСНОГО КОДА

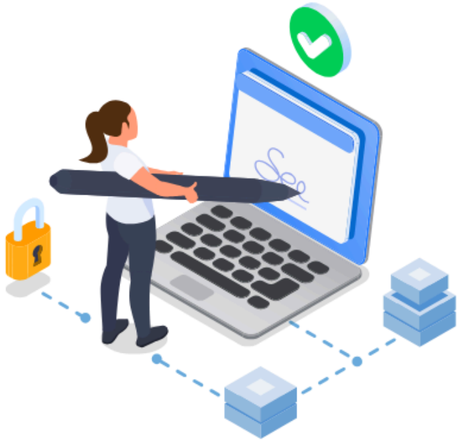
ФУНКЦИОНАЛЬНАЯ СХЕМА



ЦИКЛ



Экспертиза технической документации



Проверка информационных систем на соответствие их требованиям ИБ

Интернет-портал SYNAQ

Мониторинг обеспечения ИБ объекта

Национальный координационный центр информационной безопасности

АО “ГТС”

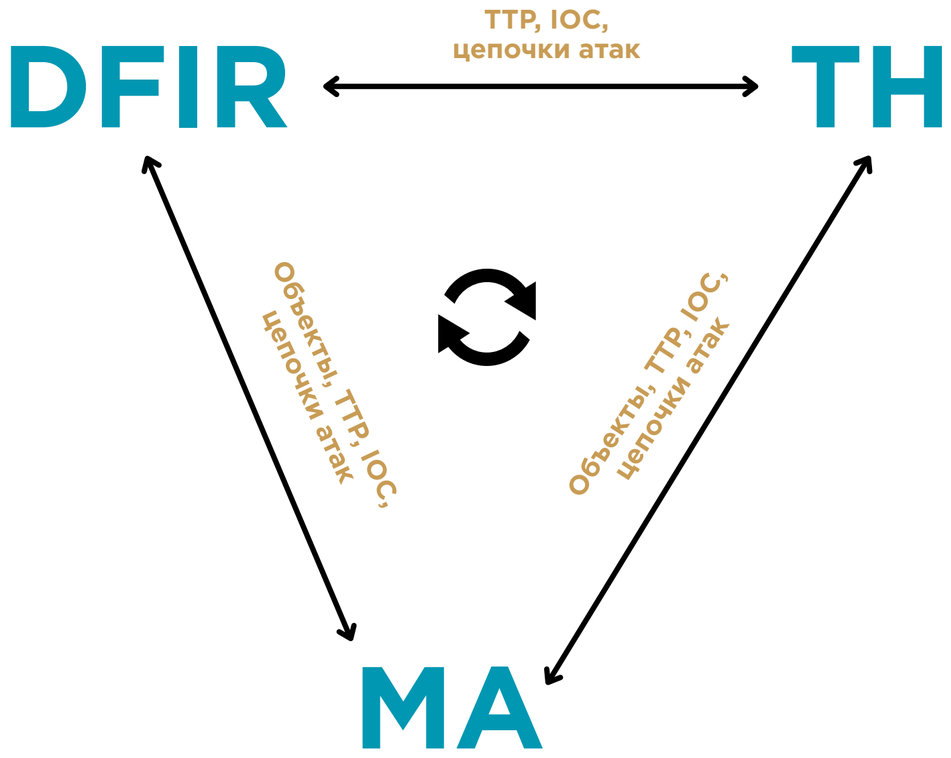
МЕЖДУНАРОДНОЕ СОТРУДНИЧЕСТВО

МЕМОРАНДУМЫ С CERT/CSIRT

- **JPCERT/CC** (Япония)
- **CNCERT/CC** (Китай)
- **TR-CERT** (Турция)
- **CERT.UA** (Украина)
- **aeCERT** (ОАЭ)
- **CERT.GOV.MD** (Молдова)
- **CERT.GOV.AZ** (Азербайджан)
- **CERT. AZ** (Азербайджан)
- **APCERT** (Малайзия)
- **CERT.BG** (Болгария)
- **INCD** (Израиль)
- **CERT.LV** (Латвия)
- **UZCERT** (Узбекистан)
- **ID-CERT** (Индонезия)
- **CERT.GOV.GE** (Грузия)
- **Türkmenaragatnaşyk** (Туркменистан)

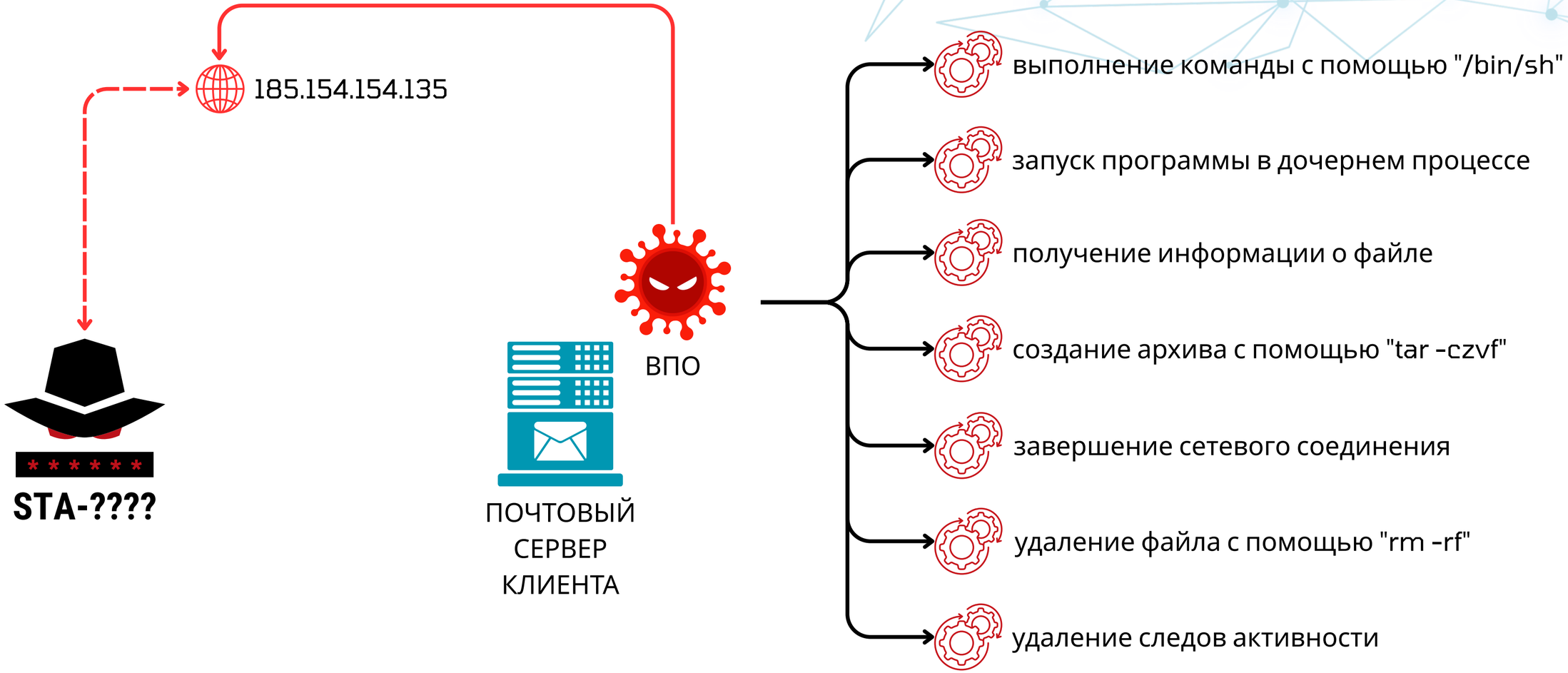
ОСОБЕННОСТИ ВЗАИМОДЕЙСТВИЯ ЦИВК

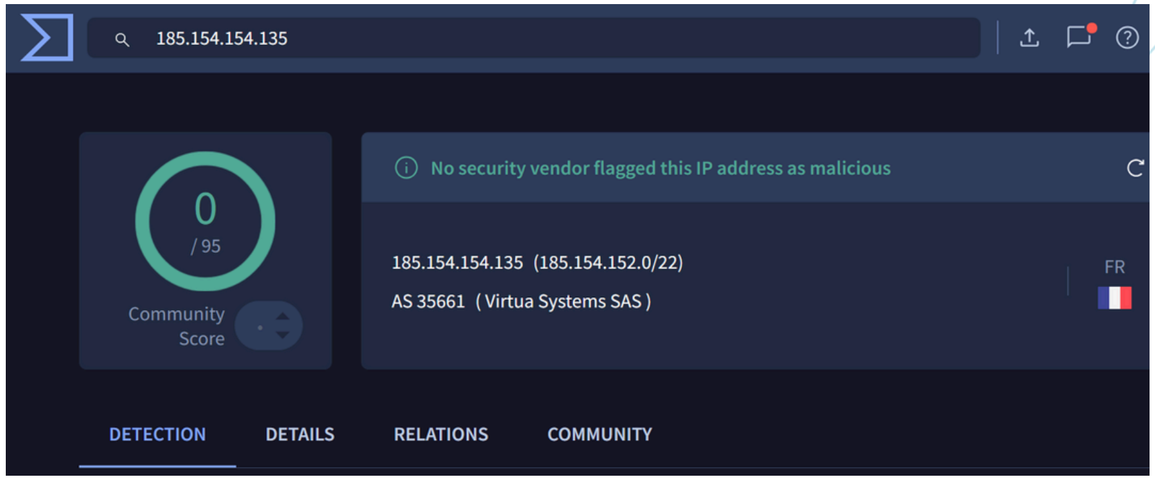
ВНЕШНИЕ



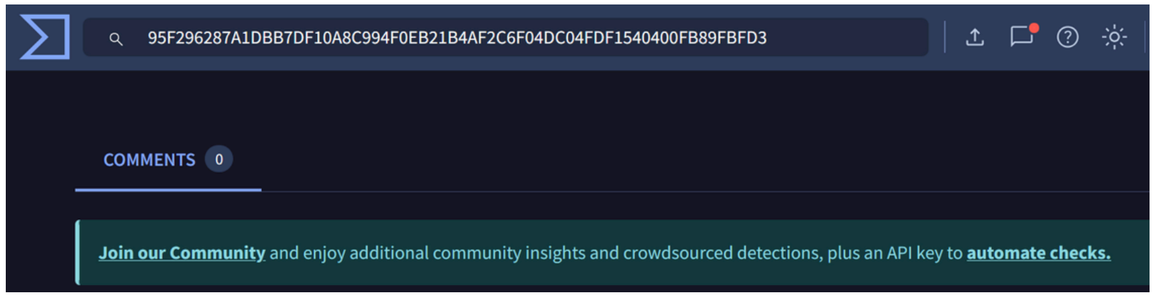
ВНУТРЕННИЕ

Мартовская Активность 2025

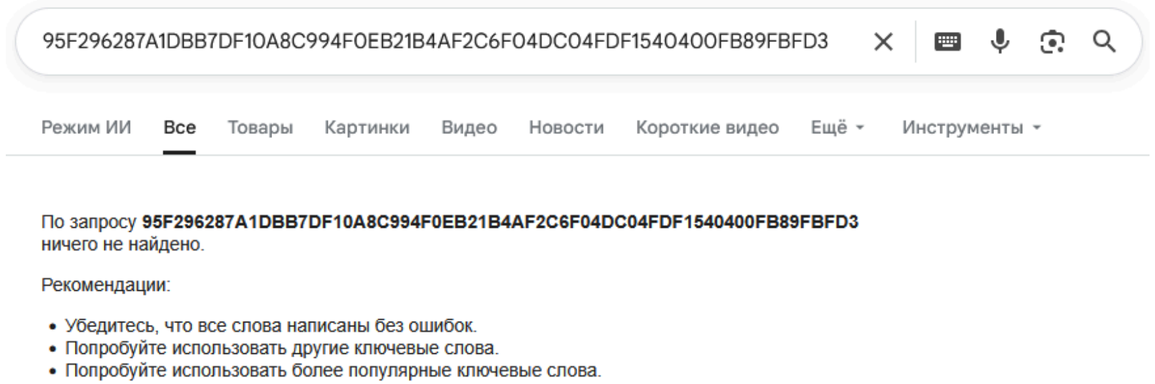

185.154.154.135
STA-????
ВПО
ПОЧТОВЫЙ СЕРВЕР КЛИЕНТА
выполнение команды с помощью "/bin/sh"
запуск программы в дочернем процессе
получение информации о файле
создание архива с помощью "tar -czvf"
завершение сетевого соединения
удаление файла с помощью "rm -rf"
удаление следов активности



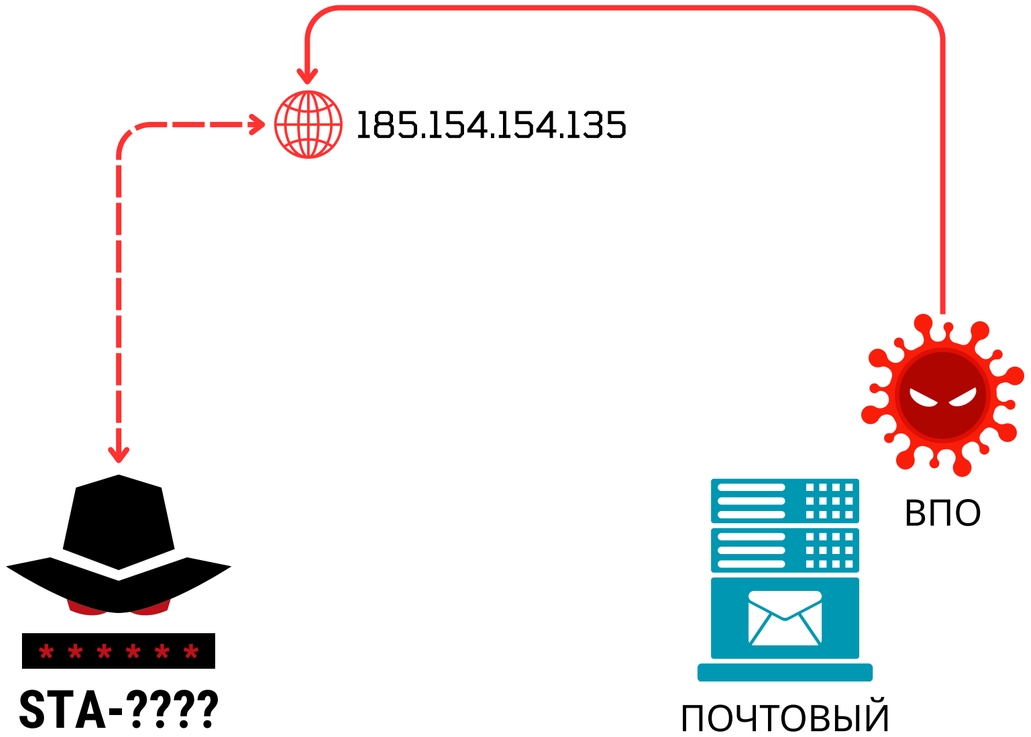
НЕТ УПОМИНАНИЙ :(



НЕТ УПОМИНАНИЙ :(



НЕТ УПОМИНАНИЙ :(



- включение шифрования сетевого трафика [7]
- отправка POST-запроса на указанный URI (/news/data_form.php)
- изменение канала управления

With the support of active C2 probing services, we successfully identified three C2 servers that are still active in the wild. These servers responded to the online packets and sent a command 7 to the bots, requesting them to enable traffic encryption. They have been active since 2024, demonstrating the continued presence of the MystRodX threat.

```
00000000  10 00 00 00 01 00 00 00  01 00 00 00 01 00 00 00   ........ ........
    00000000  10 04 00 00 01 00 00 00  07 00 00 00 00 00 00 00   ........ ........
    00000010  2d cc 0a 85 62 f0 42 44  1f 2a 85 16 5c fc 39 a3   -...b.BD .*..\.9.
    00000020  da 69 00 a6 35 1a 48 ab  2e 8f db 86 12 18 76 24   .i..5.H. ......v$
```

MystRodX configurations include RSA public keys for decrypting command 7. Attackers typically use distinct keys for different campaigns, with two known keys

включение шифрования сетевого трафика [7]

изменение канала управления

Upon receiving the ICMP packet, MystRodX establishes a communication connection with `192.168.96.1:443` and sends an HTTP-formatted check-in message. This behavior aligns perfectly with our expectations, confirming the accuracy of our analysis.

	Source	Destination	Protocol
1	192.168.96.1	192.168.96.129	ICMP
2	192.168.96.129	192.168.96.1	TCP
3	192.168.96.1	192.168.96.129	TCP
4	192.168.96.129	192.168.96.1	TCP
5	192.168.96.129	192.168.96.1	HTTP

```
00000000  50 4f 53 54 20 2f 6e 65  77 73 2f 64 61 74 61 5f   POST /ne ws/data_
00000010  66 6f 72 6d 2e 70 68 70  20 48 54 54 50 2f 31 2e   form.php  HTTP/1.
00000020  31 0d 0a 43 6f 6e 74 65  6e 74 2d 54 79 70 65 3a   1..Conte nt-Type:
```

отправка POST-запроса на указанный URI (/news/data_form.php)

Home About EN 奇安信 X 实验室

APT

MystRodX: The Covert Dual-Mode Backdoor Threat

Alex.Turing, WangZhiCheng, Acey9

2025年8月27日 • 13 min read

27 августа 2025 года
новый вредонос - MystRodX
неизвестная APT-группировка

Background

On June 6, 2025, **XLab's Cyber Threat Insight and Analysis System(CTIA)** picked up activity from IP 139.84.156.79 distributing a suspicious ELF file—dst86.bin—with a low VirusTotal hit rate of only 4/65. While conventional scanners labeled it as **Mirai**, our AI module remained silent. That mismatch caught our attention.

6 июня 2025 года
сервер распространения:
139.84.156.79

MystRodX is a typical backdoor implemented in C++, supporting features like file management, port forwarding, reverse shell, and socket management.

Compared to typical backdoors, MystRodX stands out in terms of **stealth** and **flexibility**.

обычный бэкдор
с красивым названием?

QAX 奇安信 | АО “ГТС”

IOC

Downloader

```
http://139.84.156[.]79/dst-x86.bin
```

НЕТ СОВПАДЕНИЙ :(

C2 & Campaign

```
airtel.vpndns.net:443    neybquno
149.28.130.195:443       zoufkcfr

149.28.137.254:8010      neybquno
149.28.137.254:8443      zoufkcfr


156.244.6.68:443         unknown
185.22.153.228:443       unknown
```

НЕТ СОВПАДЕНИЙ :(

Sample MD5

```
Dropper
5e3a2a0461c7888d0361dd75617051c6 *dst
72d377fa8ccf23998dd7c22c9647fc2a *chargen
5bf67ce1b245934965557de6d37f286f *daytime


fa3b4d5fd1f6c995395244f36c18ffec *dst
a46f2c771fb580e2135ab898731be9a7 *chargen
e8fcb7f3f0edfc7d1a99918dc14527d1 *daytime
1f003437e3d10e07f5ee5f51c61c548f *networkd
```

НЕТ СОВПАДЕНИЙ :(

With the support of active C2 probing services, we successfully identified three C2 servers that are still active in the wild. These servers responded to the online packets and sent a command 7 to the bots, requesting them to enable traffic encryption. They have been active since 2024, demonstrating the continued presence of the MystRodX threat.

```
00000000  10 00 00 00 01 00 00 00  01 00 00 00 01 00 00 00   ........ ........
    00000000  10 04 00 00 01 00 00 00  07 00 00 00 00 00 00 00   ........ ........
    00000010  2d cc 0a 85 62 f0 42 44  1f 2a 85 16 5c fc 39 a3   -...b.BD .*..\.9.
    00000020  da 69 00 a6 35 1a 48 ab  2e 8f db 86 12 18 76 24   .i..5.H. ......v$
```

MystRodX configurations include RSA public keys for decrypting command 7. Attackers typically use distinct keys for different campaigns, with two known keys

включение шифрования сетевого трафика [7]

изменение канала управления

Upon receiving the ICMP packet, MystRodX establishes a communication connection with 192.168.96.1:443 and sends an HTTP-formatted check-in message. This behavior aligns perfectly with our expectations, confirming the accuracy of our analysis.

	Source	Destination	Protocol
1	192.168.96.1	192.168.96.129	ICMP
2	192.168.96.129	192.168.96.1	TCP
3	192.168.96.1	192.168.96.129	TCP
4	192.168.96.129	192.168.96.1	TCP
5	192.168.96.129	192.168.96.1	HTTP

```
00000000  50 4f 53 54 20 2f 6e 65  77 73 2f 64 61 74 61 5f   POST /ne ws/data_
00000010  66 6f 72 6d 2e 70 68 70  20 48 54 54 50 2f 31 2e   form.php  HTTP/1.
00000020  31 0d 0a 43 6f 6e 74 65  6e 74 2d 54 79 70 65 3a   1..Conte nt-Type:
```

отправка POST-запроса на указанный URI (/news/data_form.php)

C2 & Campaign

```
airtel.vpndns.net:443    neybquno
149.28.130.195:443       zoufkcfr

149.28.137.254:8010      neybquno
149.28.137.254:8443      zoufkcfr


156.244.6.68:443         unknown
185.22.153.228:443       unknown
```

185.154.154.135 ?

QAX 奇安信 | АО "ГТС"

Октябрьская Активность 2025

```
00000000  74 63 62 69 70 6b 72 6e 00 00 00 00 bb 01 00 00  |tcbipkrn....»...|
00000010  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  |................|
00000020  01 00 00 00 01 00 00 00 00 00 00 00 31 39 39 30  |............1990|
00000030  2d 30 32 2d 32 38 20 31 37 3a 30 36 3a 30 31 00  |-02-28 17:06:01.|
00000040  74 65 73 74 00 00 00 00 00 00 00 00 00 00 00 00  |test............|
00000050  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  |................|
00000060  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  |................|
00000070  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  |................|
00000080  31 38 35 2e 31 35 34 2e 31 35 34 2e 31 33 35 00  |185.154.154.135.|
00000090  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  |................|
000000a0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  |................|
000000b0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  |................|
```

ВПО - TrustFall (МАРТ 2025)

```
└─# strings /media/sf_Steppe/t.config
tcbipkrn
1990-02-28 17:06:01
test
185.154.154.135
-----BEGIN PUBLIC KEY-----
MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA3CQDfpxsBgO5gjqykkaZ
D5UvIK4AVuJIVEry3yqBWypetR8/vjXODQhLmviTnT/zeo0rcoiYUK95UKWmRzRp
C3YTmugUi1QgfPHt9kRrgstRNOBVIyrcXyl93rhjIpYmRWTcz+524OAD5NeAOmaK
KUW61QtNWpjZ5n2QCt0DlNx3+hYBKLcIX/+7CbYAQRlngwDuzkKOZe59pvPCB//A
uPoVJJVXYimlku8PcV8WCsHnqMlMWmbvRRgbAxoghYYn8ng/NRm9Q7OyU+V0TW4I
IGw0xOEafrs9liph5BeA7YmazkSgQlxznOuiINettNxFSi97j7O5zICSSZMPygDy
bwIDAQAB
-----END PUBLIC KEY-----
```

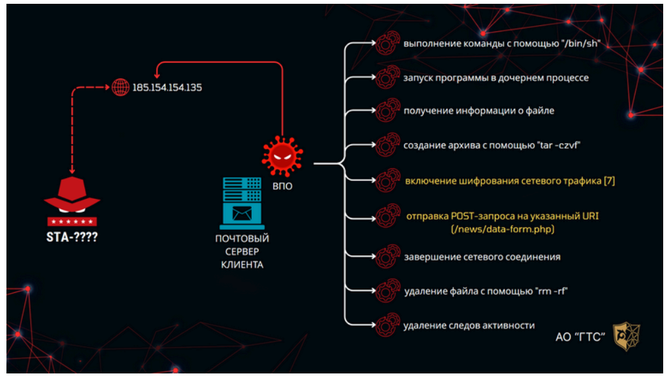
```
00000000  62 61 65 65 61 6a 7a 62 00 00 00 00 bb 01 00 00  |baeeajzb....»...|
00000010  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  |................|
00000020  01 00 00 00 01 00 00 00 00 00 00 00 31 39 39 30  |............1990|
00000030  2d 30 32 2d 32 38 20 31 37 3a 30 36 3a 30 31 00  |-02-28 17:06:01.|
00000040  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  |................|
00000050  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  |................|
00000060  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  |................|
00000070  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  |................|
00000080  32 31 33 2e 31 35 39 2e 36 34 2e 36 00 00 00 00  |213.159.64.6....|
00000090  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  |................|
000000a0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  |................|
000000b0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  |................|
```

ВПО - TrustFall (ОКТЯБРЬ 2025)

```
└─# strings /media/sf_Steppe/b.config
baeeajzb
1990-02-28 17:06:01
213.159.64.6
-----BEGIN PUBLIC KEY-----
MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAzTbQEOol/YRsNymd3vXZ
j4GVeo1KNuRtpMejQJRrpGsIbjTR1Y9lxgGzxMM2IEQI/LA2gjQ9l9qZzhAGWUwq
AnQbqGNbqwny5piWqX7JxzQ6GNJpAI1XMh+A6yhD4q+bXWbHB+nyOEEHICd0P9Km
SSwUHndfT3Znv1FENCO3CGpI+eoZdj1E4acilDuJy/DKQlDxcUIx1yepM7F9Vtmm
qaZeFNbiGfpzqGFSA2gycyI15sOqivuUipkp9w/AxcPDau99tgXg0Chf9E8ddoun
0u1Bsb3BaT//d48lLiOdtT8qaz/PgFX2hKLkGPG319uDPX7V4YGg+z6aKa1UoAwe
OwIDAQAB
-----END PUBLIC KEY-----
```

АО “ГТС”

первое исследование ВПО - TrustFall



отчет об исследовании ВПО - MystRodX

эмуляция агента (клиента), зондирование сетей для идентификации инфраструктуры ВПО - TrustFall

07.03.2025

06.06.2025

27.08.2025

03.10.2025

07.10.2025

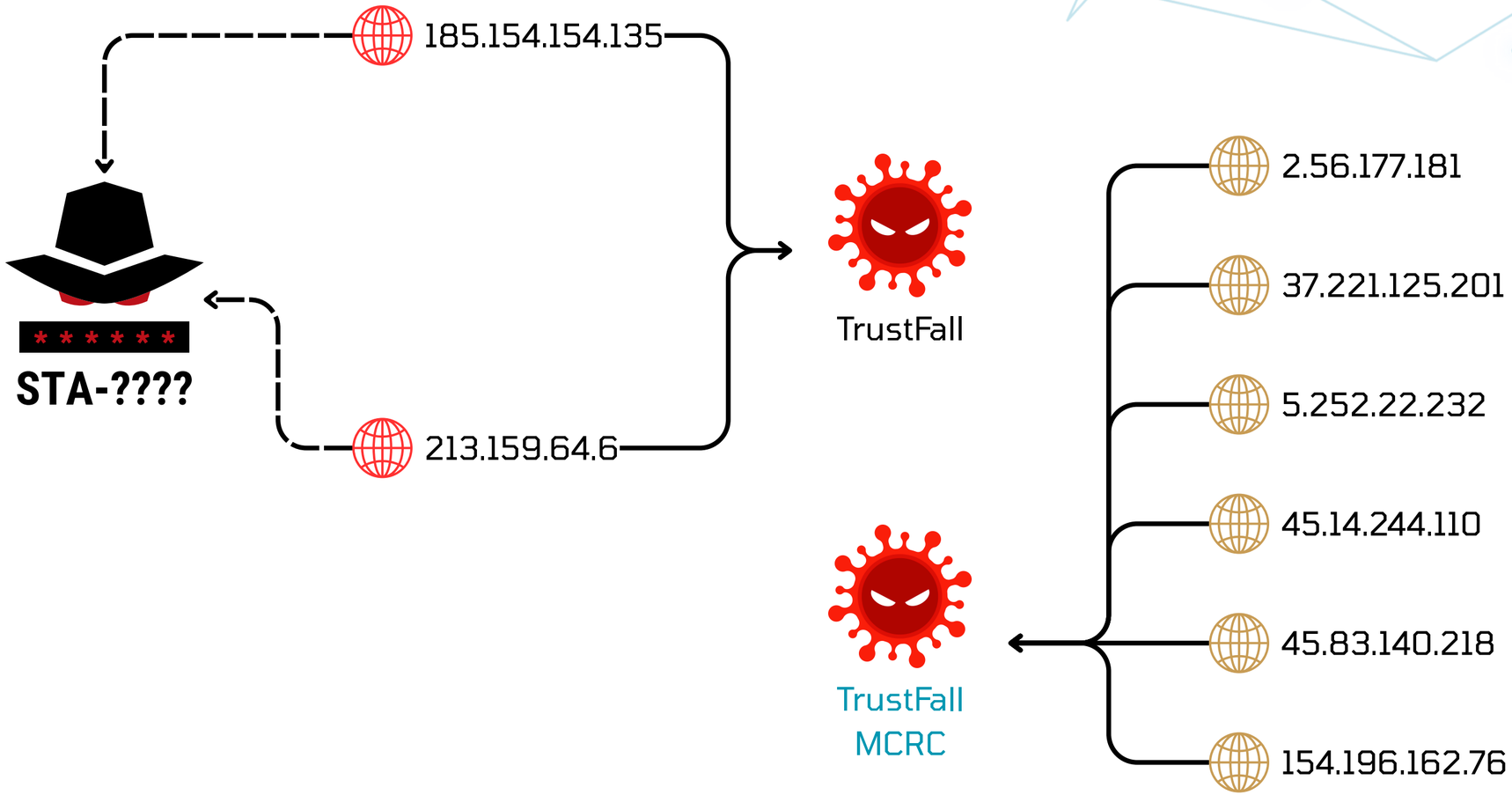
Background

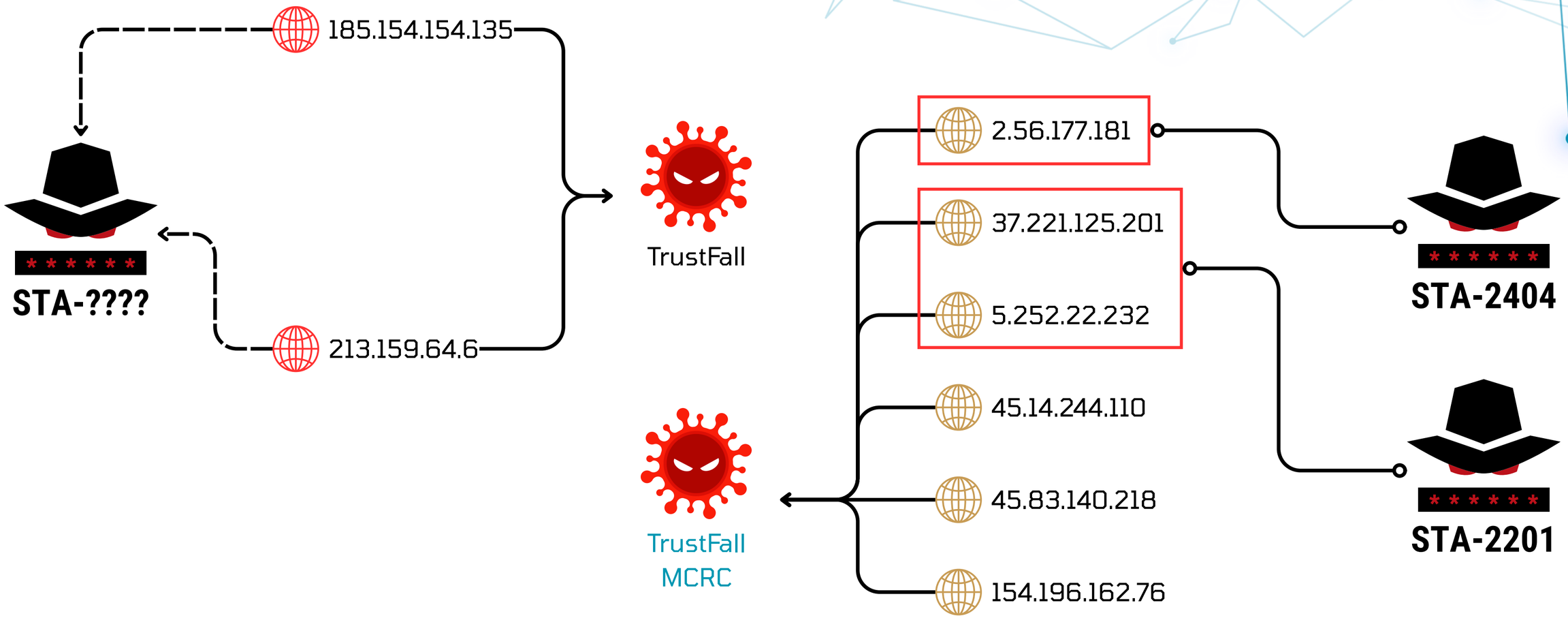
On June 6, 2025, **XLab's Cyber Threat Insight and Analysis System(CTIA)** picked up activity from IP 139.84.156.79 distributing a suspicious ELF file—dst86.bin—with a low VirusTotal hit rate of only 4/65. While conventional scanners labeled it as **Mirai**, our AI module remained silent. That mismatch caught our attention.

первое обнаружение ВПО - MystRodX

извлечение конфигов:

- tcbipkrn.config:
  - 185.154.154.135
- baeeajzb.config:
  - 213.159.64.6


185.154.154.135
******
STA-????
213.159.64.6
TrustFall
TrustFall
MCRC
2.56.177.181
37.221.125.201
5.252.22.232
45.14.244.110
45.83.140.218
154.196.162.76


185.154.154.135
213.159.64.6
STA-????
TrustFall
TrustFall
MCRC
2.56.177.181
37.221.125.201
5.252.22.232
45.14.244.110
45.83.140.218
154.196.162.76
STA-2404
STA-2201

STA-2201

КРАТКАЯ ИНФОРМАЦИЯ

Кодовое наименование: STA-2201

Описание: Хакерская группировка, замеченная первой в 2019 году. Она отмечается разнообразным профилем – начиная от получения первичного доступа (т.е. действует как Initial Access Broker) заканчивая хищением и эксфильтрацией данных (т.е. функционирует как классическая хакерская группировка). Активность группировки существенно изменилась после [redacted] скрытно [redacted]

Отрасль: Государственное управление, Операторы связи

STA-2404

КРАТКАЯ ИНФОРМАЦИЯ

Кодовое наименование: STA-2404

Описание: Передовая хакерская группировка, сформированная в результате [redacted] с [redacted] года [redacted] Активность данной группы отслеживается с марта 2024 года (первая волна) и мая 2024 года (вторая волна) [redacted]

Отрасль: Государственное управление, Энергетика, Здравоохранение, Наука, Транспорт, Финансы

STIR - STS TI-REPORTS
РЕКОНСТРУКЦИЯ АТАК STA

Информация об отчёте	
Наименование:	Microsoft Exchange как орудие злоумышленников
Идентификатор:	STIR-2301
Дата отчёта:	11.09.2023 версия 1.0
TLP:	AMBER+STRICT

Информация об отчёте	
Наименование:	Оператор связи на прицеле у STA-2201
Идентификатор:	STIR-2302
Дата отчёта:	10.11.2023 версия 1.0
TLP:	AMBER+STRICT

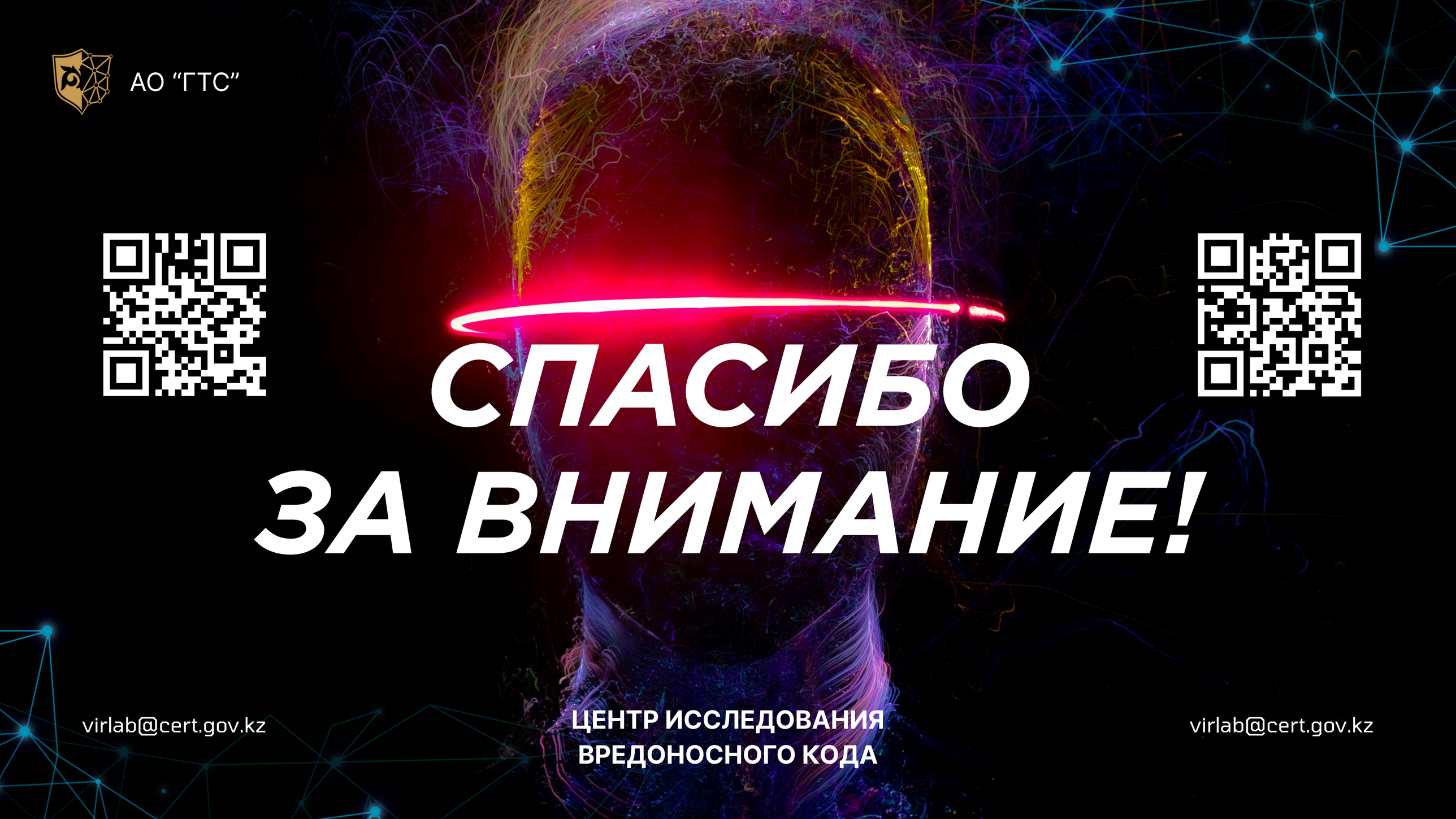
Информация об отчёте	
Наименование:	STA-2303 – еще один брокер первичного доступа.
Идентификатор:	STIR-2404
Дата отчёта:	17.10.2024
TLP:	AMBER+STRICT

MITRE AT&&CK:	
Tactic	**Technique**

TLP: AMBER+STRICT

INITIAL ACCESS	T1190 – Exploit Public-Facing Application T1078.002 – Valid Accounts: Domain Accounts
EXECUTION	T1059.001 – Command and Scripting Interpreter: PowerShell T1059.003 – Command and Scripting Interpreter: Windows Command Shell T1059.004 – Command and Scripting Interpreter: Unix Shell
PERSISTENCE	T1505.003 – Server Software Component: Web Shell T1505.004 – Server Software Component: IIS Components T1543.003 – Create or Modify System Process: Windows Service T1053.005 – Scheduled Task/Job: Scheduled Task T1078.002 – Valid Accounts: Domain Accounts
DEFENSE EVASION	T1036.005 – Masquerading: Match Legitimate Name or Location T1036.008 – Masquerading: Masquerade File Type T1550.002 – Use Alternate Authentication Material: Pass the Hash
CREDENTIAL ACCESS	T1003 – OS Credential Dumping
COMMAND AND CONTROL	T1105 – Ingress Tool Transfer T1572 – Protocol Tunneling

АО “ГТС”



СПАСИБО ЗА ВНИМАНИЕ!

virlab@cert.gov.kz

ЦЕНТР ИССЛЕДОВАНИЯ ВРЕДОНОСНОГО КОДА

virlab@cert.gov.kz