

*Восстановление репутации
после инцидента*

Сергей Сторчак

- специалист по информационной безопасности
- 11 лет в ИБ



ser-storchak.blogspot.com



ser-storchak@mail.ru



[@ser_storchak](https://twitter.com/ser_storchak)

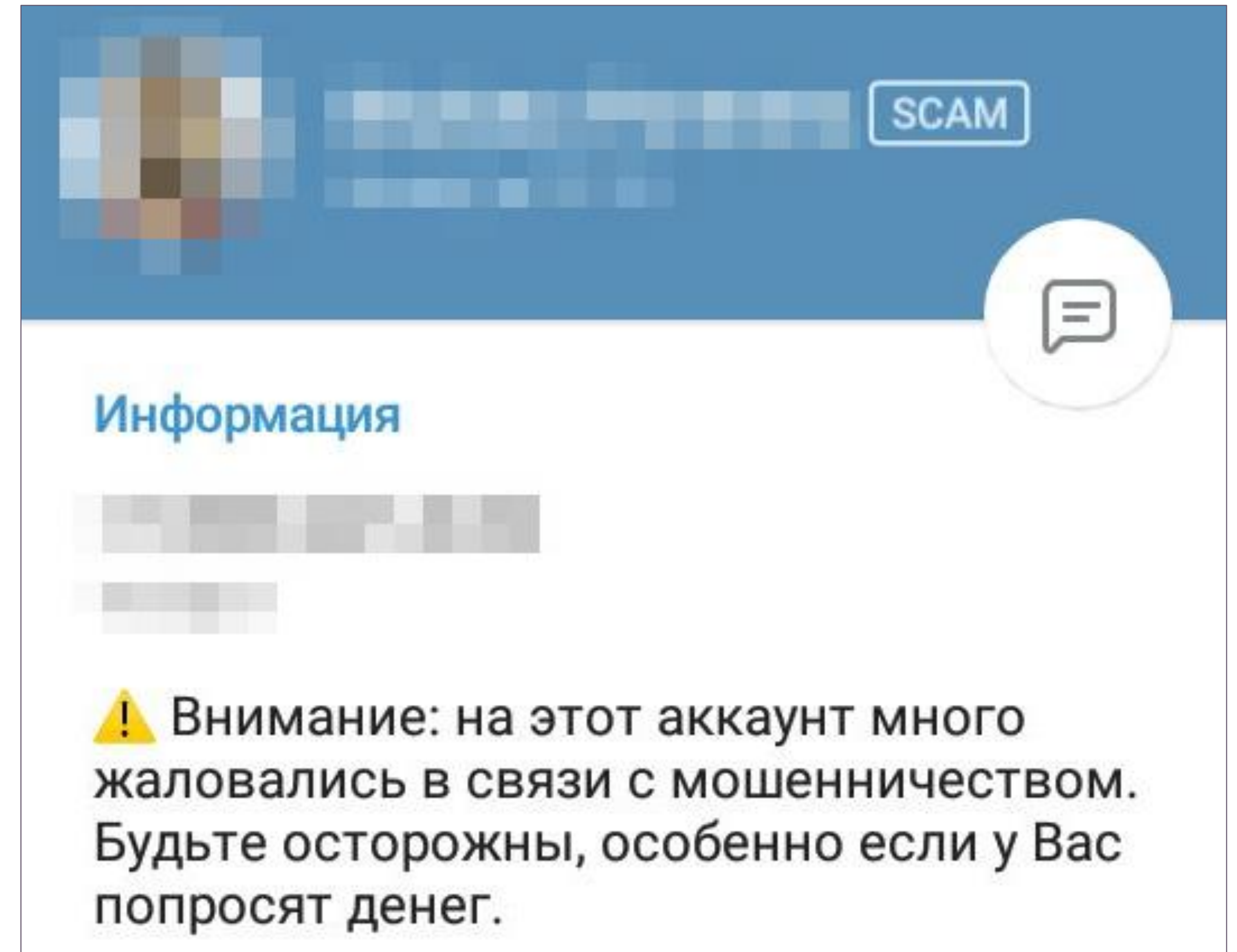
Презентация отражает личную точку зрения автора,
а не его работодателя.

Сайт криптобиржи блокируется
антивирусами из-за чего бизнес теряет
клиентов

Задачи:

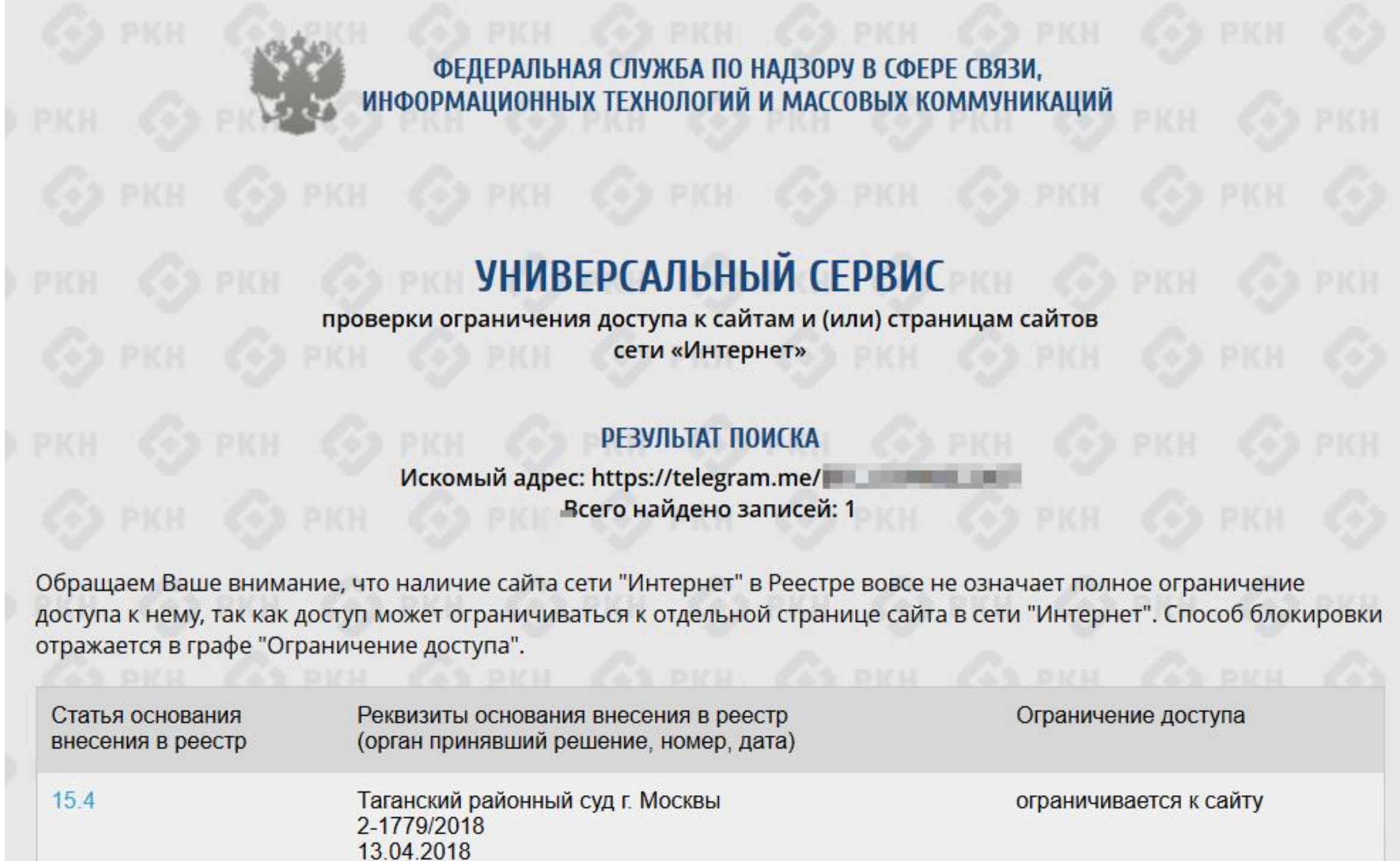
- установить причину блокировки
- связаться с антивирусными
производителями для удаления сайта
из черных списков

Срок исполнения: 4 месяца



Причины блокировки

- Сайт и Telegram-аккаунты считаются мошенническими – многочисленные жалобы пользователей в чатах и на форумах
- Telegram-бот в черном списке РКН – криптовалюта официально в России не разрешена



ФЕДЕРАЛЬНАЯ СЛУЖБА ПО НАДЗОРУ В СФЕРЕ СВЯЗИ,
ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ И МАССОВЫХ КОММУНИКАЦИЙ

УНИВЕРСАЛЬНЫЙ СЕРВИС
проверки ограничения доступа к сайтам и (или) страницам сайтов
сети «Интернет»

РЕЗУЛЬТАТ ПОИСКА
Искомый адрес: <https://telegram.me/>
Всего найдено записей: 1

Обращаем Ваше внимание, что наличие сайта сети "Интернет" в Реестре вовсе не означает полное ограничение доступа к нему, так как доступ может ограничиваться к отдельной странице сайта в сети "Интернет". Способ блокировки отражается в графе "Ограничение доступа".



Статья основания внесения в реестр	Реквизиты основания внесения в реестр (орган принявший решение, номер, дата)	Ограничение доступа
15.4	Таганский районный суд г. Москвы 2-1779/2018 13.04.2018	ограничивается к сайту

ОТЗЫВЫ ПОЛЬЗОВАТЕЛЕЙ

Google Play Игры **Приложения** Фильмы Книги Детям

TeamViewer QuickSupport

TeamViewer

	2,5★ 103 тыс. отзывов	50 млн+ Количество скачиваний	 Для всех ⓘ
--	--------------------------	----------------------------------	---

Критерии включения в ЧС

1. Связан с потенциально нежелательным, шпионским или вредоносным ПО.
2. Предлагает партнерскую программу, которая платит комиссию за распространение потенциально нежелательного ПО.
3. Связан с вредоносными или сомнительными порталами, поисковыми системами или хакерскими сайтами.
4. Отсутствует политика конфиденциальности или используется сторонняя политика конфиденциальности, в которой отсутствует информация о сборе данных и других методах, используемых сайтом.
5. Отсутствует или не включает приемлемое исполнение лицензионного соглашения/условия использования.
6. Отслеживает поведение при просмотре веб-страниц и передает эту информацию на удаленный сервер.
7. Собирает личную информацию без явного согласия в условиях использования, лицензионном соглашении или политике конфиденциальности.

Критерии включения в ЧС

8. Сайт оказывает услуги пользователям ЕС, но явно не соблюдает требования GDPR.
9. Сайт, включая любые другие веб-сайты или домены, принадлежащие, поддерживаемые или аффилированные с ними, которые обнаруживаются любым антивирусом или упоминаются в их базе данных.
10. Сайт, заблокированный регистратором домена.
11. Рекламодатели или другие сторонние поставщики, которые размещают свой контент на сайтах, которые, устанавливают/распространяют потенциально нежелательное и вредоносное ПО.
12. Сайты причастные к фишингу или другому нежелательному поведению.
13. Сайт, маскирующийся под другой бренд и продающий товары незаконным способом.

*<https://threatcenter.crdf.fr/criteria.html>

VirusTotal

Files Referring			
Scanned	Detections	Type	Name
2020-05-15	18 / 60	JavaScript	071d5c44d21c365c13
2020-05-10	12 / 58	JavaScript	334755
2020-05-08	9 / 60	JavaScript	output.158974021.txt
2020-05-06	11 / 60	JavaScript	02fb0e5db977b02c3.
2020-05-06	10 / 59	JavaScript	4f241a13194abb0474c
2020-04-30	8 / 59	JavaScript	output.157799511.txt
2020-04-26	8 / 60	JavaScript	6af54c2a366d9d7cdc
2020-05-03	11 / 71	Win32 EXE	GruadEnige.exe
2020-04-26	8 / 60	JavaScript	output.157378271.txt
2020-04-15	34 / 59	JavaScript	071d5c44d21c365c13


URLs ⓘ		
Scanned	Detections	URL
2020-03-01	2 / 72	http://[redacted]/en/terms
2020-02-25	3 / 72	http://[redacted]/p2p
2020-02-25	4 / 73	http://[redacted]/ru/p2p
2020-03-01	2 / 72	http://[redacted]/ru/blog/kak_obeder
2020-02-25	3 / 72	http://[redacted]/en/market
2020-03-10	3 / 71	http://[redacted]/
2019-08-16	0 / 71	http://[redacted]/p2p
2020-02-25	3 / 72	http://[redacted]/htt
2020-02-24	2 / 72	http://[redacted]/ru/
2020-03-06	2 / 71	http://[redacted]/

*<https://www.shodan.io/>

*<https://github.com/gregzem/aibolit>

*<https://www.virustotal.com/>

VirusTotal



3
/ 59

Community Score

⚠️ 3 security vendors and no sandboxes flagged this file as malicious

963b3db7e0e2906fc031148767342988a78506f8991c1c3aa4fd38c05250f2d7
4R1LKX3G.js
javascript

18.12 KB
Size

2020-07-04 01:32:46 UTC
2 years ago

DETECTION DETAILS COMMUNITY

Security Vendors' Analysis ⓘ

AegisLab	⚠️ Trojan.Script.Epcl.4!c	Ikarus	⚠️ Trojan.JS.Cryxos
Qihoo-360	⚠️ Virus.js.qexvmc.1	Ad-Aware	✅ Undetected

F-Secure

Trojan:JS/Cryxos

CLASSIFICATION

Category:

Malware

Type:

Trojan

Platform:

JS

Aliases:

Trojan.Cryxos.[variant], JS:Trojan.Cryxos.[variant], Trojan:JS/Kotka.A, Trojan:JS/Kotka.B

SUMMARY

Cryxos trojans display an alarming notification message saying that the user's computer or web browser has been 'blocked' due to a virus infection, and that their personal details are 'being stolen'. The user is then directed to call a phone number for assistance in the 'removal process'. This is a version of a 'call support' scam.

Hybrid-Analysis

The screenshot displays the Hybrid Analysis web interface. At the top, there is a navigation bar with the Hybrid Analysis logo and several menu items: Sandbox, Quick Scans, File Collections, Resources, and Request Info. A search bar on the right contains the text "IP, Domain, Hash...".

The main content area features a report for the file "4R1LKX3G.js". The report includes the following information:

- Threat Status:** malicious (indicated by a red box)
- Threat Score:** 50/100
- AV Detection:** 4%
- Labeled as:** Trojan.JS #phishing (indicated by a blue box)

Below the threat information, there are several buttons for actions: Overview, Sample unavailable, Downloads, External Reports, Re-analyze, Hash Not Seen Before, and No similar samples. A "Request Report Deletion" button is also present.

The "Incident Response" section is highlighted, showing "MITRE ATT&CK™ Techniques Detection". A summary states: "This report has 2 indicators that were mapped to 4 attack techniques and 4 tactics." A "View all details" button is provided for further information.

On the right side, a vertical navigation menu lists various report sections: Incident Response, Indicators, File Details, Screenshots (2), Hybrid Analysis (1), Network Analysis, Extracted Strings, Extracted Files (0), Notifications, and Community (0). A "Back to top" link is located at the bottom of this menu.

Взаимодействие с вендорами

Здравствуйте!

<домен> является законным сайтом. Злоумышленники использовали его в своих программах для перевода криптовалют. Счета киберпреступников на данный момент заблокированы. В связи с этим просим вас удалить следующие URL-адреса из базы фишинговых сайтов:

<URL-адреса>...

Есть подозрение, что некоторые антивирусные движки ссылаются на ваши результаты, что затрудняет удаление с других фишинговых баз.

Мы готовы предоставить дополнительную информацию, если это необходимо. Наши контакты: <email>

СЛОЖНОСТИ ВЗАИМОДЕЙСТВИЯ

- Поиск контактов для обратной связи
- Время выполнения заявки:
 - в теории 12-24 часа
 - на практике 3-14 дней
- Рекурсия



*<https://blog.virustotal.com/2016/05/maintaining-healthy-community.html>

*<https://www.amtso.org/news/recommendations-when-including-detection-technologies-in-multi-scanner-services/>

Санкции

Error 1009

Ray ID: 746ca0c79ab716ec • 2022-09-07 04:16:16 UTC

Access denied

What happened?

The owner of this website (www.hybrid-analysis.com) has banned the country or region your IP address is in (RU) from accessing this website.

Рекомендации

- Ежеквартальная полная антивирусная проверка веб-серверов
- Мониторинг открытых портов
- Патчинг ПО

- Рекомендуемые сервисы
 - BlacklistMaster, <https://www.blacklistmaster.com/>
 - VirusTotal, <https://www.virustotal.com/>



Спасибо!

Вопросы

Сергей Сторчак



ser-storchak.blogspot.com



ser-storchak@mail.ru



sergey.storchak@distillery.com



[@ser_storchak](https://twitter.com/ser_storchak)