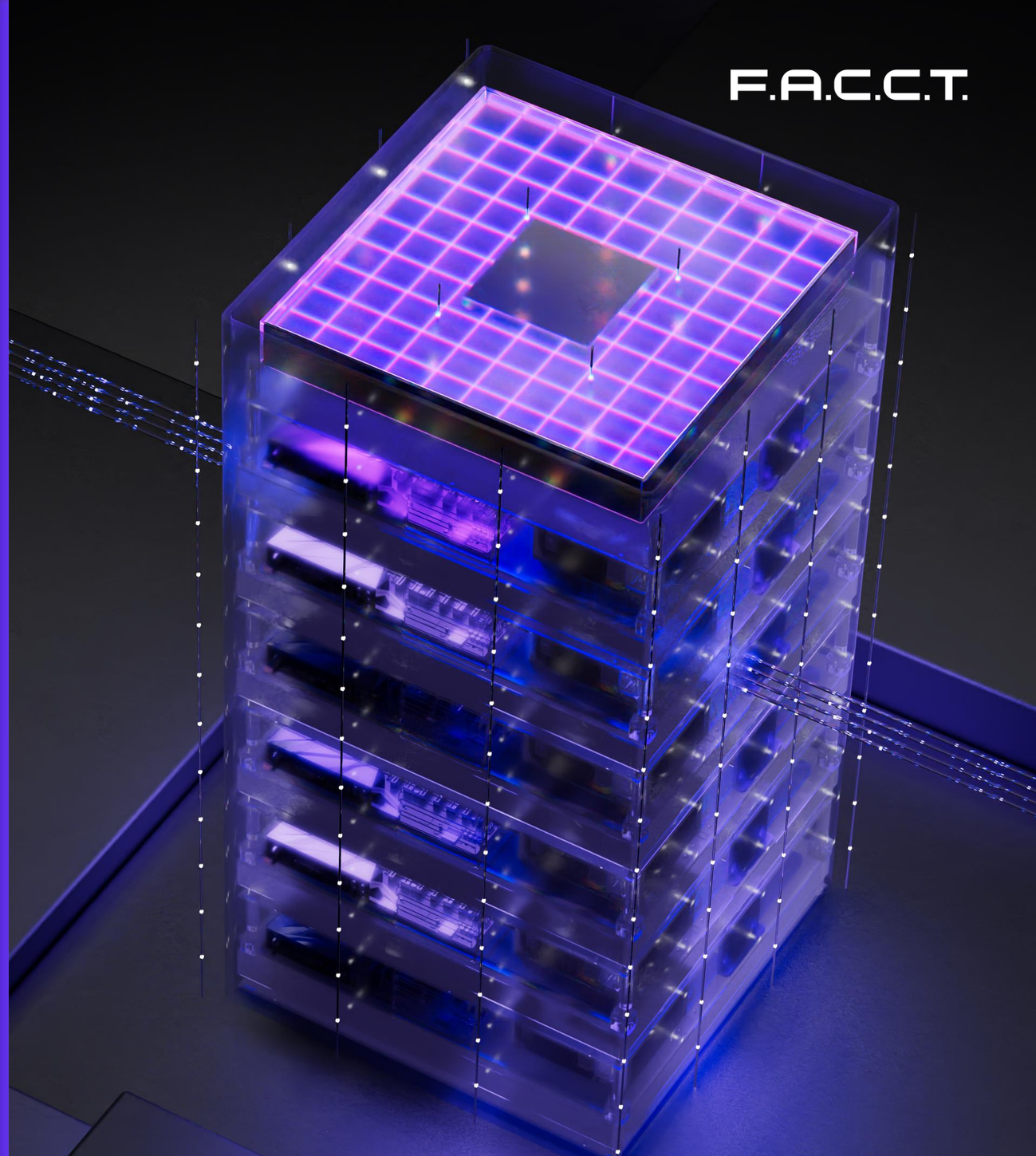
# КИБЕРПРЕСТУПНОСТЬ В РОССИИ И СНГ - 2024

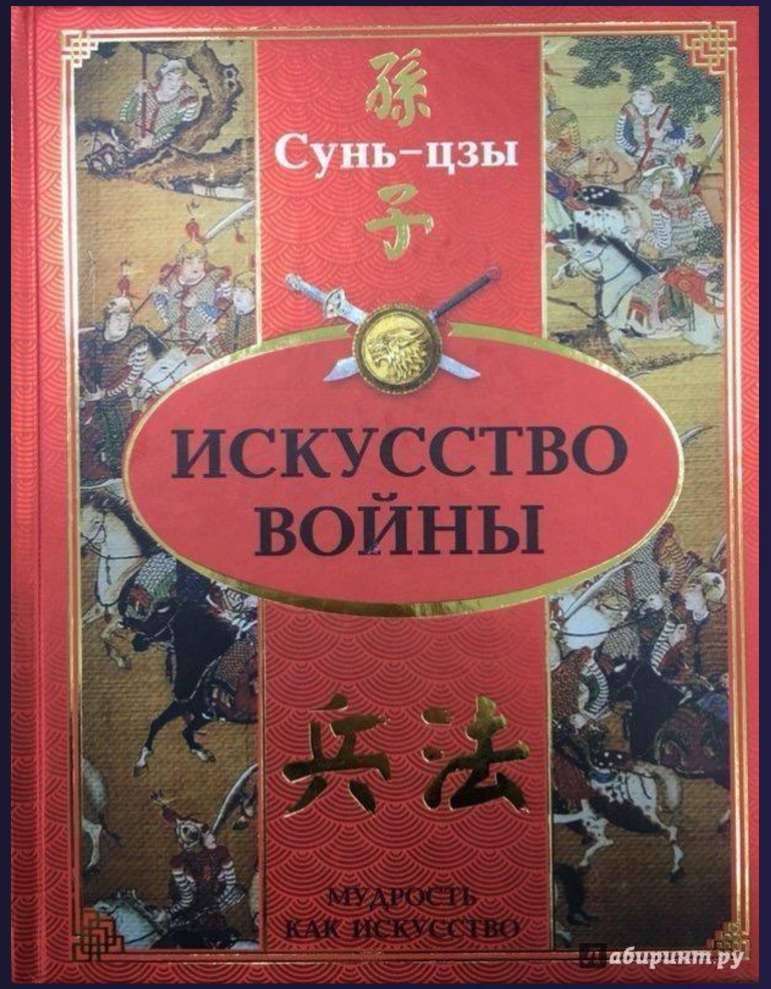
Тренды, аналитика и прогнозы
по данным региональной кибербразведки

СЕРГЕЙ ЗОЛОТУХИН
Консультант по кибербезопасности



F.A.C.C.T.

# Если не знаешь, с кем сражаешься, победить невозможно



# Прогосударственные  хакеры (APT)

F.A.C.C.T.

- **Шпионаж**
- **Диверсии**

Особые приметы:
- Не привлекают к себе внимания.
- Профессионально готовятся к атаке.
- Используют популярные инструменты, чтобы затруднить атрибуцию.

# Активность прогосударственных хакерских групп в РФ и СНГ в 2023 году

F.A.C.C.T.

**14** прогосударственных хакерских групп атаковали Россию и страны СНГ в 2023 году

Наиболее активные группы:

- XDSpy
- Cloud Atlas
- TridentCrow
- Tomiris
- Sand Eagle
- UAC-0063
- Mustang Panda
- Core Werewolf
- APT37
- Space Pirates
- Hellhounds
- Sticky Werewolf
- ToddyCat
- Mysterious Werewolf

# Активность прогосударственных хакерских групп в РФ и СНГ в 2023 году

F.A.C.C.T.

## Топ-5 атакованных стран


## Топ-5 атакованных отраслей

# Хактивисты

F.A.C.C.T.

- **Дефейсы**
- **DDoS**
- **Фейки**

Особые приметы:

- Максимально привлекают внимание к своим кампаниям
- Широко разрекламированная акция часто оказывается «пустышкой»
- Могут быть использованы спецслужбами в своих целях

# Хактивисты

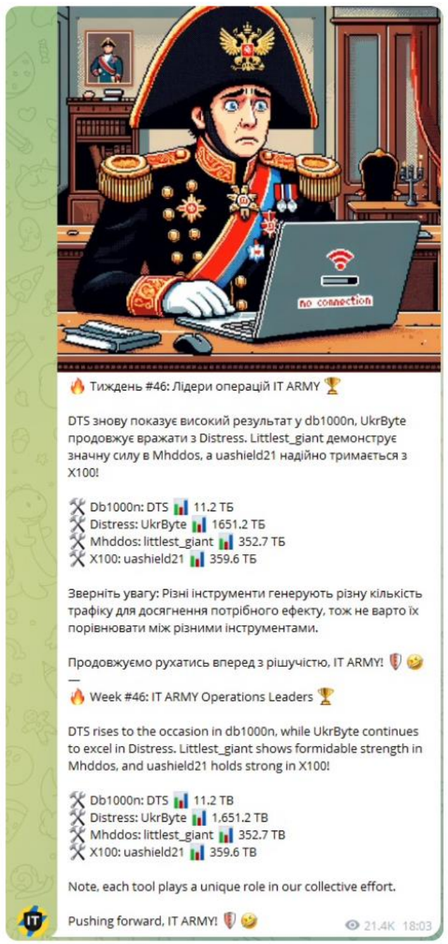
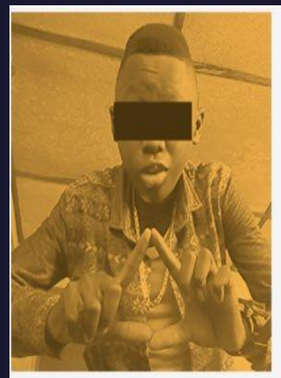



Рис. 16. Пример еженедельного сообщения в Telegram-канале IT Army of Ukraine



W3bh4x0r

Местонахождение: Нигерия
Участник таких групп, как: Nigeria Cyber Force, United Nigeria Cyber Force, Extreme Crew, Naija S3curity Kill3rs, Nigerian Gray Hat Hackers и Cyb3r Command0s.

**United Islamic Cyber Force (UICF)**
**- DDoS-атаки (отказ в обслуживании)**
**- дефейс (подмена\блокировка сайта)**

**Апрель 2013 #OpIsrael**
**(«Хакинтифада»)**

**Январь 2015 #OpFrance**

AnoaGhost

Местонахождение: Индонезия
Участник UICF, Indonesian Security, Secret Code Army и !nsp3ct0r Team.

# Киберкриминал

F.A.C.C.T.

- **Кража денег**
- **Кража данных**
- **Вымогательство**
- **Шантаж**

Особые приметы:

- Всегда следуют за деньгами
- Отрабатывают актуальную повестку
- Структурно и технически копируют IT-компании

# Шифровальщики

F.A.C.C.T.

Наиболее агрессивная группировка

C0met (ранее Shadow) / Twelve

Наиболее распространенные шифровальщики

LockBit

Conti

Babuk

Рекорд года:

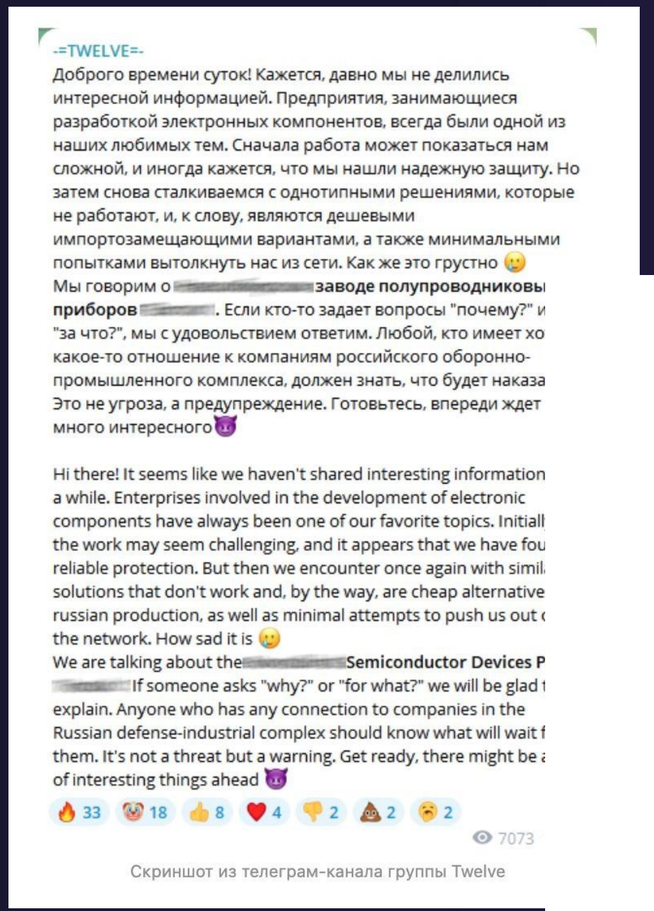
**200 млн рублей**

за расшифровку данных

Средняя сумма первоначального выкупа:

**37 млн рублей**

# Группа “двойного назначения” Comet(Shadow)/Twelve F.A.C.C.T.



-=TWELVE=-

Доброго времени суток! Кажется, давно мы не делились интересной информацией. Предприятия, занимающиеся разработкой электронных компонентов, всегда были одной из наших любимых тем. Сначала работа может показаться нам сложной, и иногда кажется, что мы нашли надежную защиту. Но затем снова сталкиваемся с однотипными решениями, которые не работают, и, к слову, являются дешевыми импортозамещающими вариантами, а также минимальными попытками вытолкнуть нас из сети. Как же это грустно 😢
Мы говорим о [redacted]**заводе полупроводниковы приборов** [redacted]. Если кто-то задает вопросы "почему?" и "за что?", мы с удовольствием ответим. Любой, кто имеет хо какое-то отношение к компаниям российского оборонно-промышленного комплекса, должен знать, что будет наказа Это не угроза, а предупреждение. Готовьтесь, впереди ждет много интересного😈

Hi there! It seems like we haven't shared interesting information a while. Enterprises involved in the development of electronic components have always been one of our favorite topics. Initiall the work may seem challenging, and it appears that we have fou reliable protection. But then we encounter once again with simil solutions that don't work and, by the way, are cheap alternative russian production, as well as minimal attempts to push us out the network. How sad it is 😢
We are talking about the [redacted]**Semiconductor Devices P** [redacted] If someone asks "why?" or "for what?" we will be glad t explain. Anyone who has any connection to companies in the Russian defense-industrial complex should know what will wait f them. It's not a threat but a warning. Get ready, there might be a of interesting things ahead 😈

🔥 33 🤡 18 👍 8 ❤️ 4 👎 2 💩 2 😘 2

7073

Скриншот из телеграм-канала группы Twelve

# Утечки данных в РФ и СНГ в 2023 году

F.A.C.C.T.

2022 г. **311** случаев публичных утечек

2023 г. **246** новых случаев публичных утечек

## 296 000 000 строк

**с данными пользователей суммарно содержали утечки 2023 года**

**142 448 695**

записей содержали электронные адреса

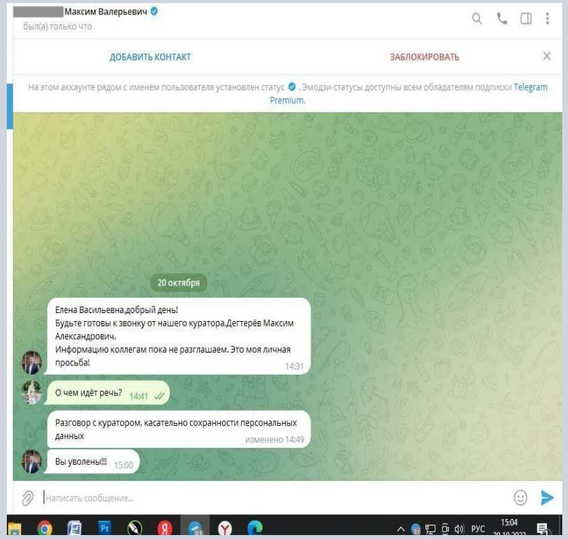
**81 663 922**

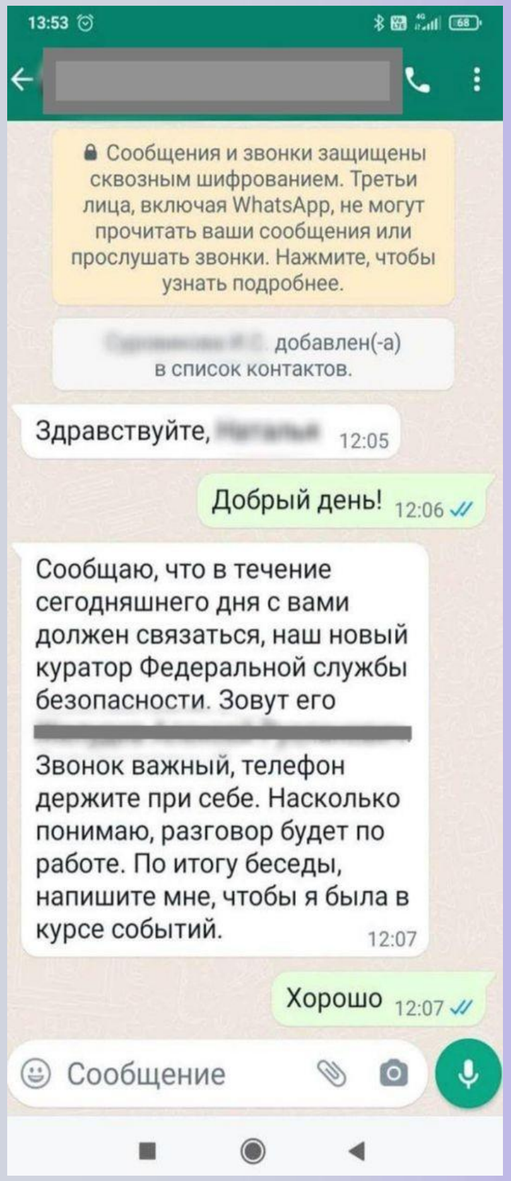
из них были уникальным

## Статистика утечек данных по странам

# Мошенничество FakeBoss


**14 млрд. руб похитили мошенники**



# Оперативная информация о новых группах и атаках

# ПИРАМИДА СКАМА

F.A.C.C.T.

Распределение ролей в типичной преступной группе, работающей по схеме «Мамонт» — фейковой курьерской доставке товаров с досок объявлений

**+1400** преступных групп появилось в 2019 — 2023 гг

Атакуют российских пользователей*:

**17 активных сообществ по схеме «Мамонт»** | **6 сообществ — по схеме Fake Date**

*по данным на октябрь 2023 года

**ВЛАДЕЛЕЦ БИЗНЕСА**
Инвестиции в запуск, масштабирование. Часто сам является админом или сдает админам телеграм-бота.

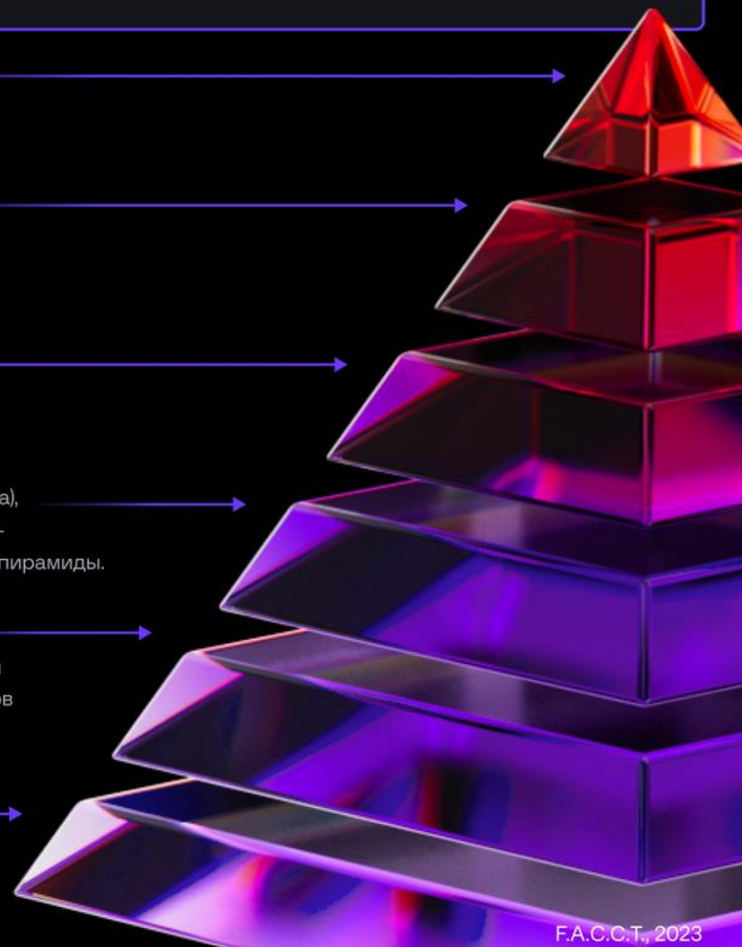
**«АДМИН» (TOPIC STARTER)**
Отвечает за рекрутинг, создание и функционирование групп в телеграмме, чат-ботов для генерации фишинговых страниц, регистрацию новых аккаунтов, техподдержку.

**РАЗРАБОТЧИКИ**
Отвечают за создание, улучшения скам-инструментов. Работают как в группе, так и под заказ.

**САППОРТЫ** (Техподдержка), **ДРОПЫ** (Вывод и обналичка), **ВБИВЕРЫ** (Списание денежных средств со счета жертвы) — круглосуточная поддержка технической и финансовой работы пирамиды.

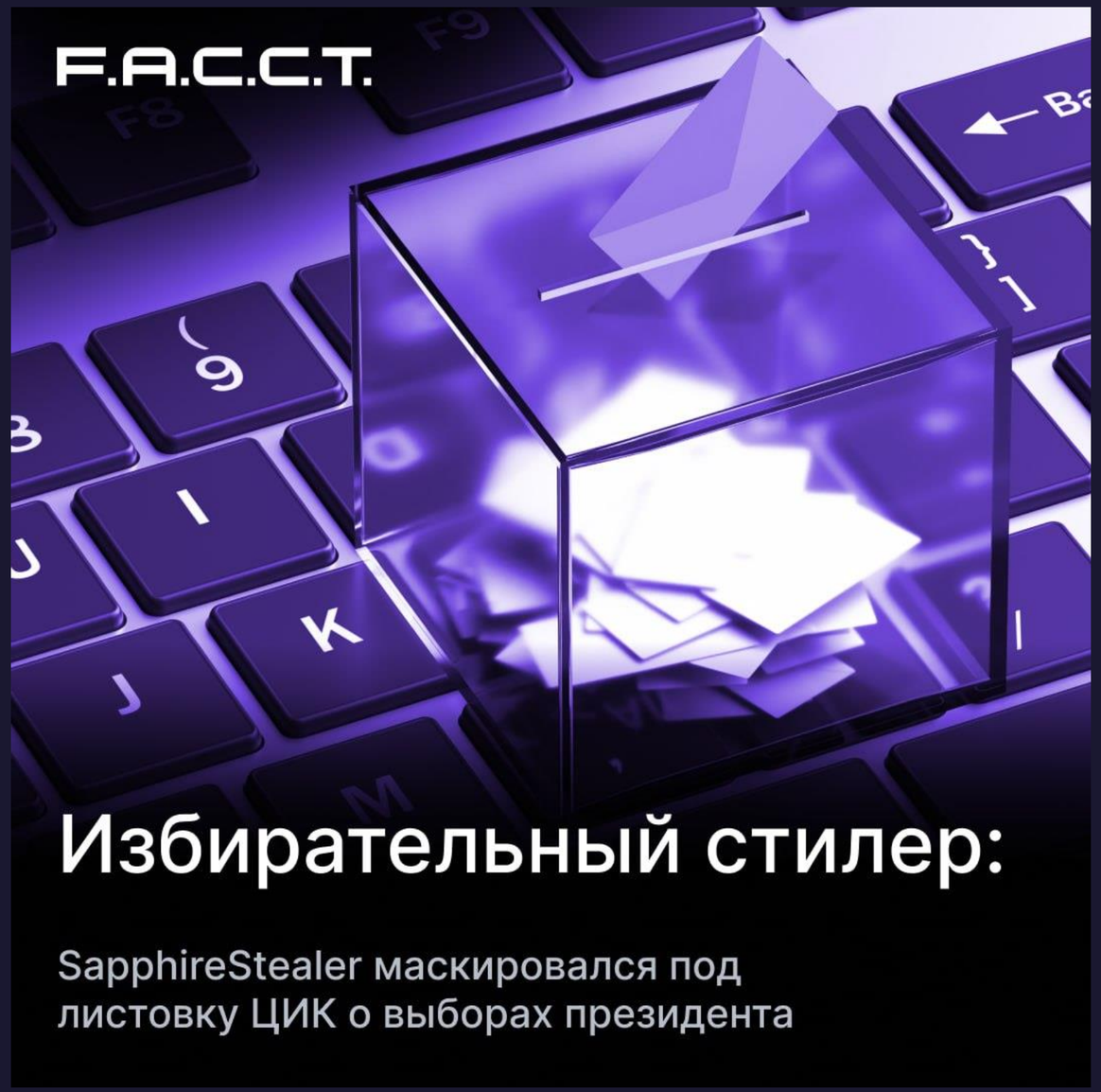
**ПРОЗВОНЩИКИ** (техподдержка по телефону), **ВОЗВРАТЕРЫ** (услуги по лже-возврату), их задача довести жертву до ввода данных карты/перевода денег на счет скамеров **БОМБЕРЫ** (организуют спам-атаку на жертв).

**ВОРКЕРЫ** («рабочие лошадки» —100-1000 человек в группе, привлекают трафик на мошеннические ресурсы), ведут коммуникации с жертвами и отправку фишинговых ссылок.



# SapphireStealer: новый стилер

F.A.C.C.T.




28.03.2024
Специалисты Threat Intelligence F.A.C.C.T. обнаружили в pdf-листовке к президентским выборам модифицированный стилер SapphireStealer, способный перехватывать данные браузеров и мессенджеров. Документ распространялся  с ресурса, замаскированного под домен Правительства РФ.

https://habr.com/ru/companies/f_a_c_c_t/articles/803339/

# PhantomCore: новая группа кибершпионов

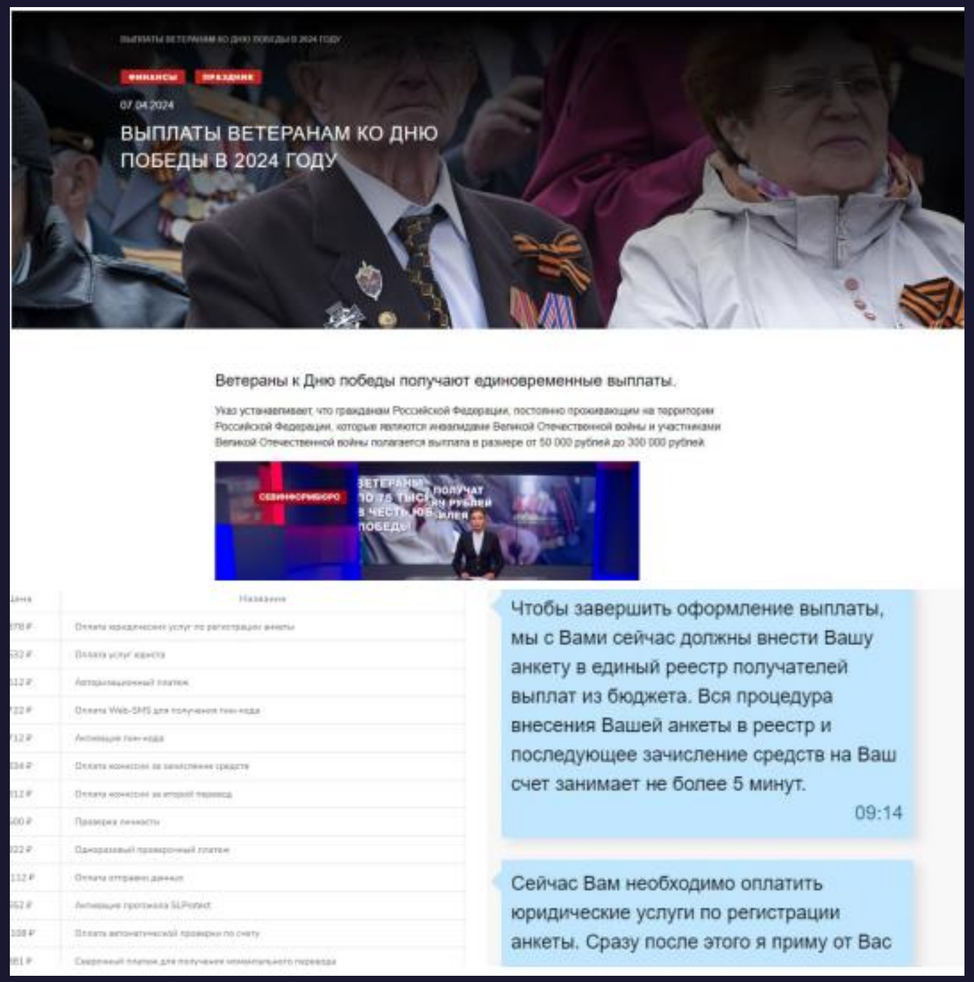
F.A.C.C.T.


09.04.2024

Новая преступная группа вымогателей Muliaka атакует российские компании с декабря 2023 года. Злоумышленники оставляют минимальное количество следов.

https://www.facct.ru/blog/ransomware-2023-2024/

# Новый сценарий к Дню Победы

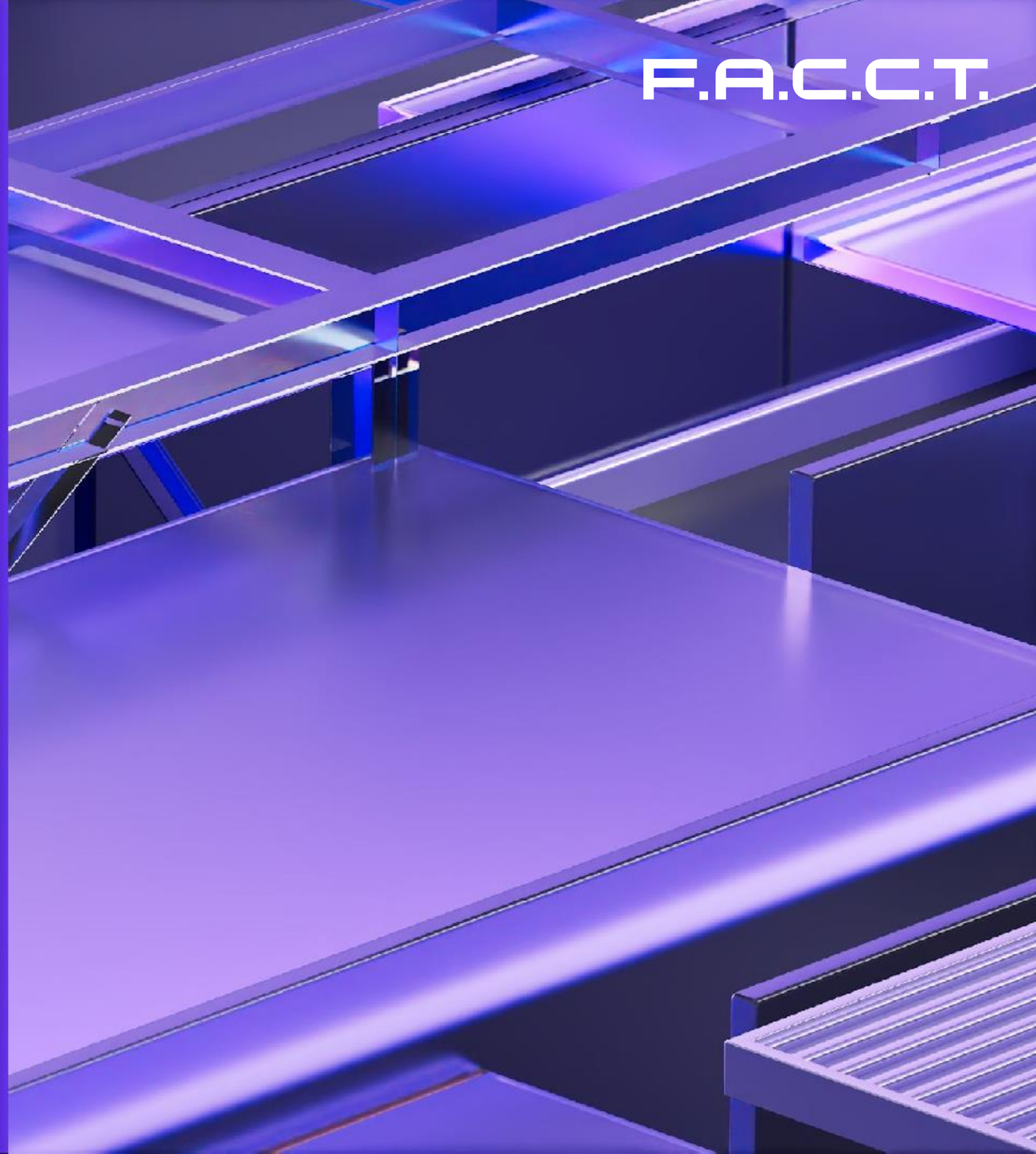



16.04.2024
Специалисты F.A.C.C.T. обнаружили новые партнерские программы, нацеленные на пожилых людей — в том числе ветеранов.

😢 Со слезами на глазах:
Мошеннический сценарий к Дню Победы

https://www.facct.ru/blog/scam-partner-programs/

# Расследуем и предотвращаем киберпреступления с 2003 года.



F.A.C.C.T.

facct.ru
info@facct.ru

facct.ru/blog
+7 495 984 33 64