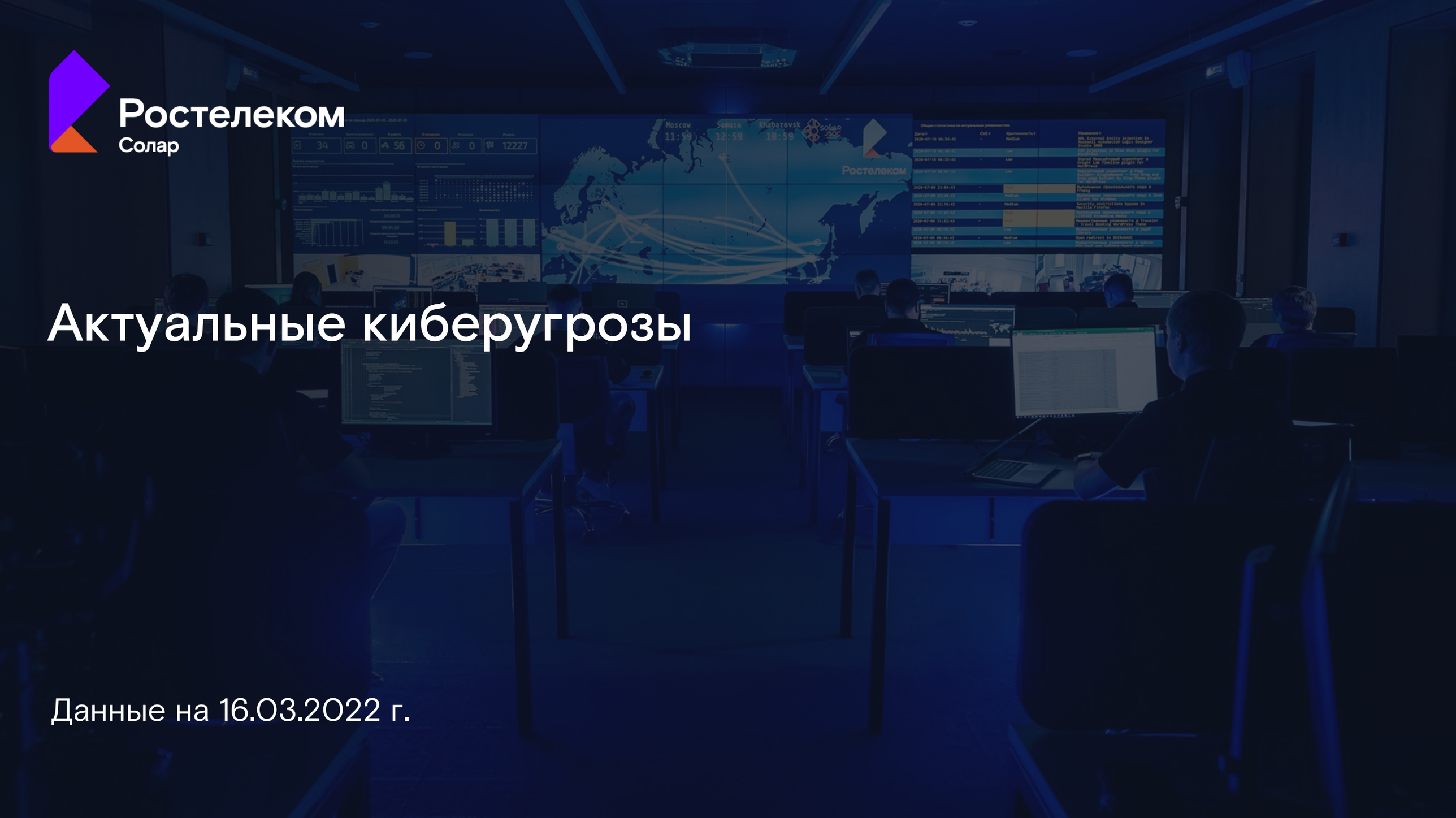
Ростелеком
Солар



Актуальные киберугрозы

Данные на 16.03.2022 г.

Ситуация сегодня

90% компаний, находящихся под защитой «Ростелеком-Солар», ежедневно подвергаются нападениям **широковещательным DDoS с использованием заграничных ботнетов.** Емкость некоторых фокусированных атак превышала 750 Гбит/с

Рост атак через подрядчиков (дефейс через взлом счетчиков и баннеров)

Необратимое **шифрование данных без возможности выкупа** при взломе уязвимых инфраструктур

Проправительственные группировки повысили активность в части **проникновения и закрепления в объектах КИИ и компаниях госсектора на территории РФ**

Массовые атаки на веб-ресурсы со стороны иностранных злоумышленников. Bug Bounty на уровне страны

Эксплуатация **новых критических уязвимостей**

Ростелеком Солар

Ситуация сегодня

В первые дни

Со стороны профессиональных группировок:

- ориентация на госсектор и компании, попавшие в санкционные списки

Со стороны группировок низкого и среднего уровней:

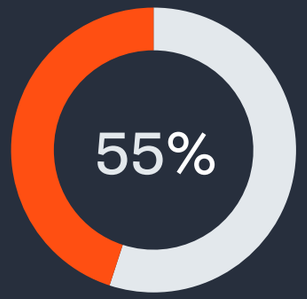
- использование наиболее доступных инструментов
- быстрые удары без тяжелых длительных последствий

Вероятное развитие событий:

- Точечные удары по КИИ
- Усложнение атак
- Разработка нового ВПО и совершенствование существующих инструментов для повышения эффективности
- Использование зараженных хостов инфраструктур в качестве точек входа
- Использование supply chain

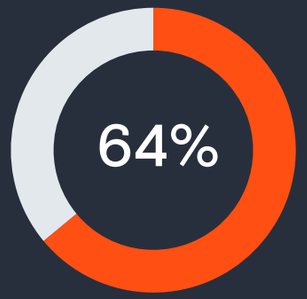
Ростелеком Солар

Многие компании уязвимы перед злоумышленниками



крупных компаний неспособны эффективно противодействовать кибератакам

Accenture, 2021 г.



уязвимостей, выявленных по результатам **внутренних пентестов**, характеризуются **высоким уровнем критичности**

уязвимостей, выявленных по результатам **внешних пентестов**, характеризуются **средним или высоким уровнем критичности**

проектов по внутреннему пентесту были завершены полной компрометацией инфраструктуры и захватом доменов

Solar JSOC, 2021 г.

Ростелеком Солар

14:22, 28 февраля 2022 Интернет и СМИ

Хакеры взломали сайты российских изданий

Группировка Anonymous взломала сайты ТАСС, «Ъ» и «Известий»

Фото: Valentyn Ogirenko / Reuters

Группировка Anonymous взломала сайты информационного агенства ТАСС, а также изданий «Коммерсантъ», «Известия», «Фонтанка», «Мел», Forbes. Сообщения об этом появляются при попытке зайти на страницы ресурсов.

Хакеры начали масштабную атаку на российские информационные ресурсы. На сайтах изданий группировка опубликовала сообщения с призывами остановить специальную военную операцию по защите Донбасса.

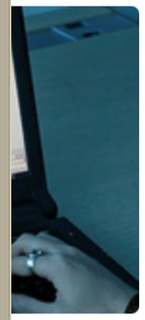
Позже редакция издания «Коммерсантъ» подтвердила РИА Новости информацию о том, что их сайт подвергся взлому.

Об атаке в Telegram-канале также сообщило Forbes. «Как и некоторые другие СМИ мы столкнулись с атакой на наш сайт. Мы делаем все возможное, чтобы устранить проблему как можно скорее», — говорится в сообщении.

Ростелеком Солар

14:22, 28 февраля 2022 Интернет и СМИ

Хакеры взломали сайты российских



nko / Reuters

нную

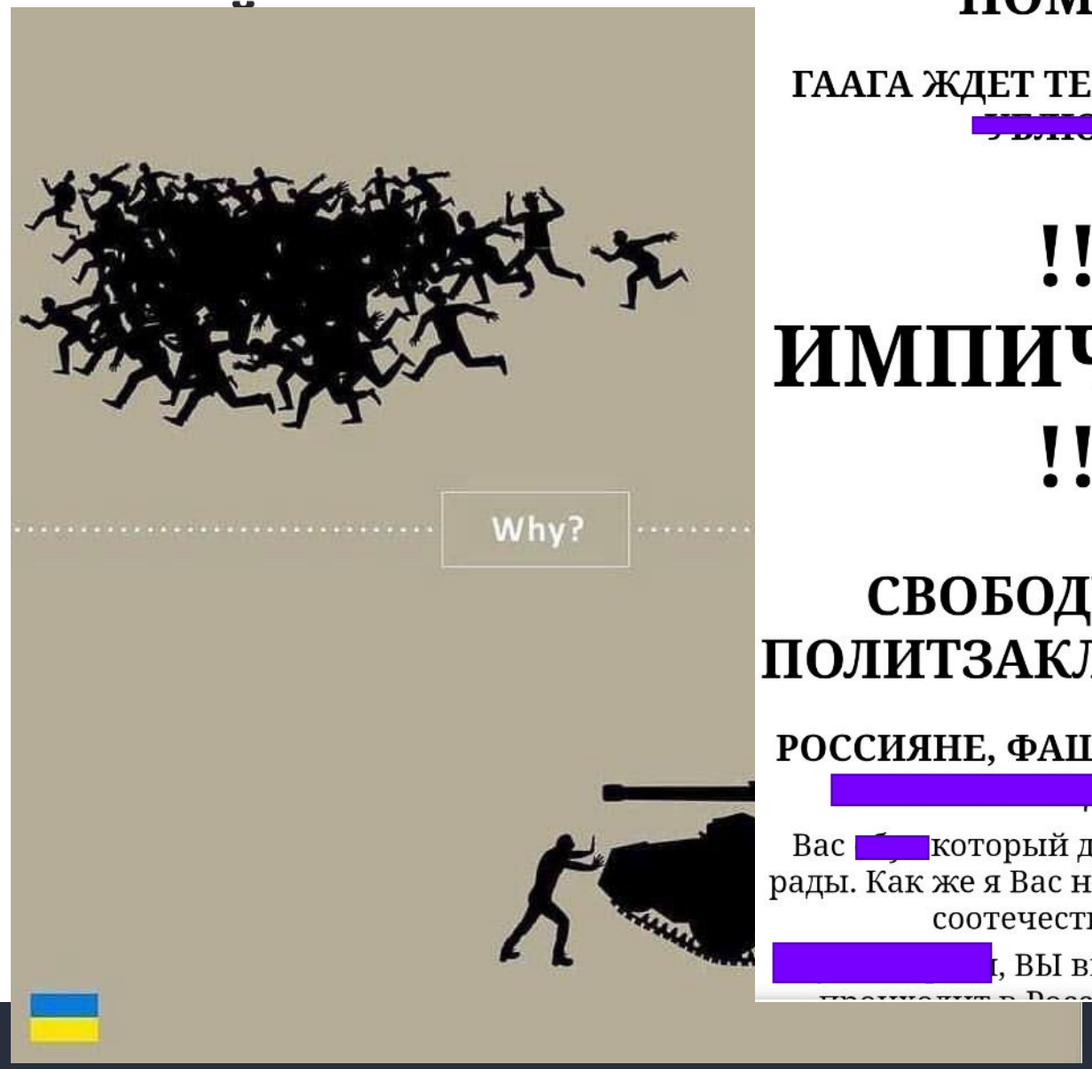
е

тся в

Ростелеком Солар

14:22, 28 февраля 2022 Интернет и СМИ

Хакеры взломали сайты р



sakhalin.arbitr.ru

ПУТИН ТЕРРОРИСТ НОМЕР 1

ГААГА ЖДЕТ ТЕБЯ И ВСЕХ ВАС [redacted]

!!!

ИМПИЧМЕНТ

!!!

СВОБОДУ ВСЕМ ПОЛИТЗАКЛЮЧЕННЫМ!

РОССИЯНЕ, ФАШИСТЫ ЭТО ВЫ!

[redacted]!

Вас [redacted]который десяток лет, а вы и рады. Как же я Вас ненавижу, "дорогие" соотечественники.

[redacted], ВЫ виноваты в том что

Ростелеком Солар

14:22, 28 февраля 2022 Интернет и СМИ

Хакеры взломали сай

sakhalin.arbitr.ru

рады. Как же я Вас ненавижу, "дорогие" соотечественники.

[redacted], ВЫ виноваты в том что

www.mchs.gov.ru

mchs.gov.ru

Не удается получить доступ к сайту

Превышено время ожидания ответа от сайта **www.mchs.gov.ru**.

Попробуйте сделать следующее:

- Проверьте подключение к Интернету.
- Проверьте настройки прокси-сервера и брандмауэра.

ERR_CONNECTION_TIMED_OUT

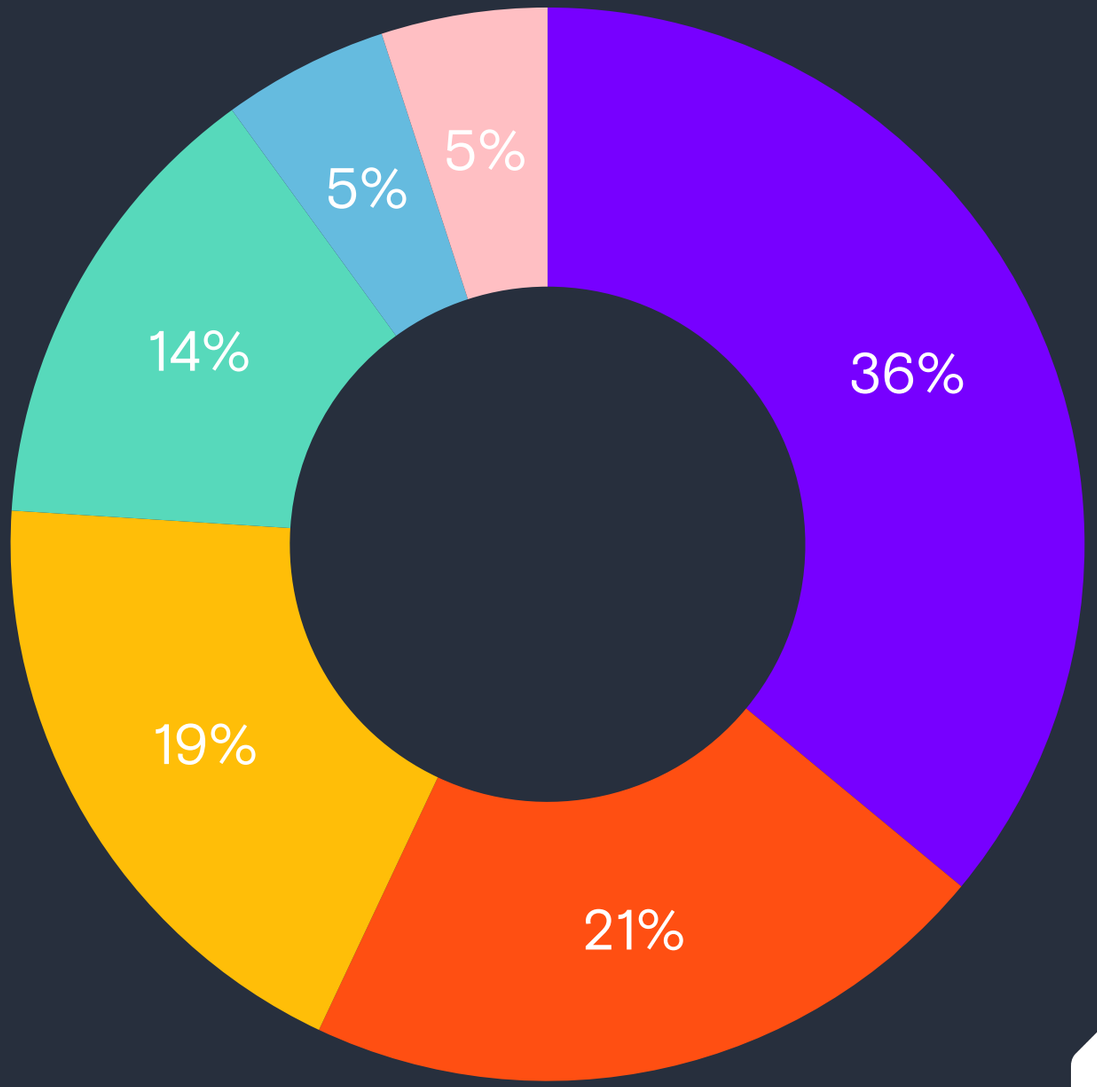
Сведения

Перезагрузить

Ростелеком Солар

Распределение массовых атак по отраслям

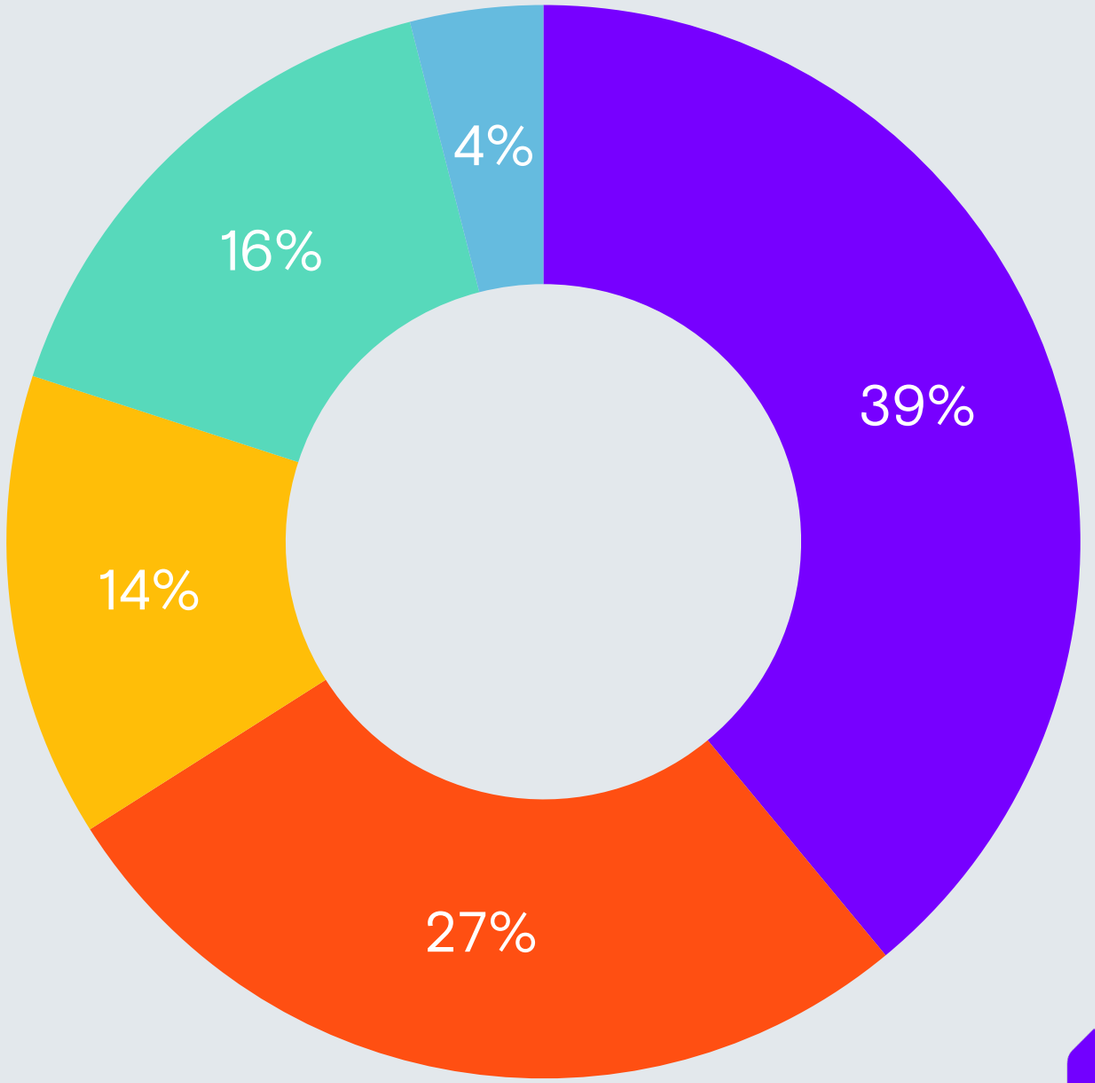
Образование	36%
Госсектор	21%
Здравоохранение	19%
Промышленность	14%
Финансы	5%
ТЭК	5%



Ростелеком Солар

Распределение APT-атак по отраслям

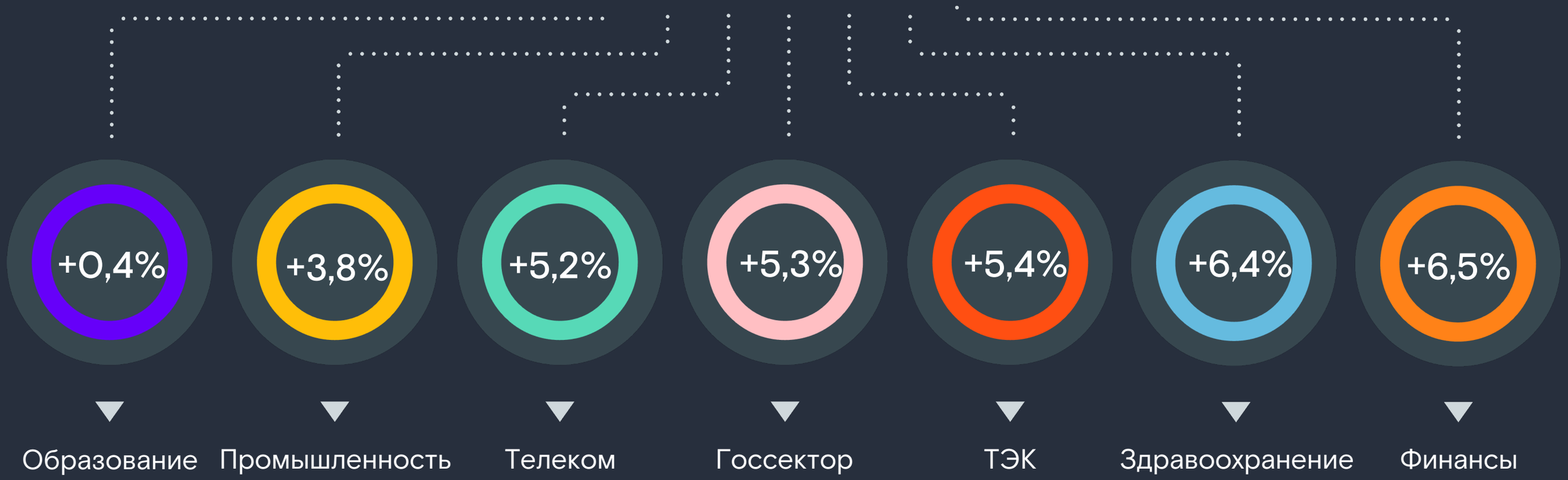
Госсектор	39%
ТЭК	27%
Финансы	14%
Промышленность	16%
Другое	4%



Ростелеком Солар

Динамика за последний месяц

Рост числа всех типов атак по отраслям (активные заражения инфраструктур)



Ростелеком Солар

Прогнозы

Повышенный уровень DDoS-атак в течение длительного времени

Рост числа атак со стороны проправительственных группировок

Увеличение числа массовых сканирований внешней инфраструктуры на предмет наличия уязвимостей и недостатков

Сохранение вектора атак для распространения паники среди населения и бизнеса

Использование скомпрометированных учетных записей для проникновения во внутреннюю сеть

Увеличение числа атак со стороны профессиональных группировок с целью монетизации. Вектор – фишинг

Ростелеком Солар

Рекомендации

Регулярное проведение инвентаризации внешнего периметра

Проведение работ по повышению осведомленности сотрудников в вопросах ИБ

Резервное копирование и инвентаризация иностранного ПО

Отключение неиспользуемых сервисов

Использование решений для мониторинга внутреннего и внешнего периметра и открытых источников

Настройка расширенного аудита

Аккуратный патч-менеджмент. Проверка обновлений в тестовой среде

Усиленный контроль подрядчиков

Оперативная организация выявления и реагирования на инциденты ИБ (например, по сервисной модели)

Ростелеком Солар

Ростелеком
Солар

Ким Наталья

+7 (924) 131-13-53

n.kim@rt-solar.ru