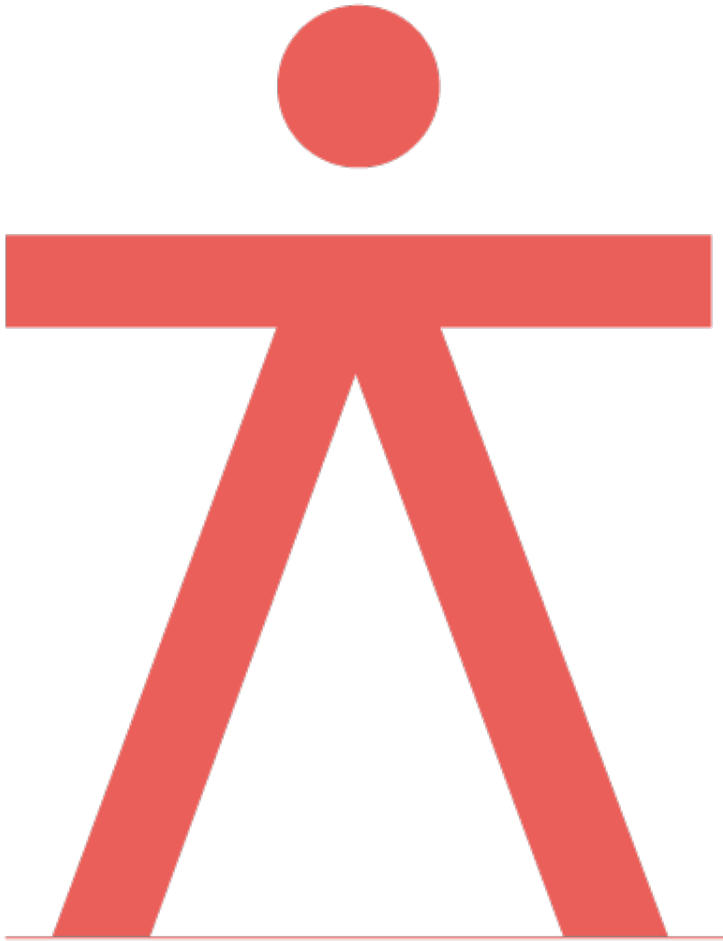
ГРУППА ЧТПЗ

КИБЕРБЕЗОПАСНОСТЬ, ЦИФРОВЫЕ РИСКИ И УГРОЗЫ.

Гусляев Георгий Александрович

КЛЮЧЕВЫЕ НАПРАВЛЕНИЯ РАЗВИТИЯ КИБЕРБЕЗОПАСНОСТИ

ГРУППА ЧТПЗ



- ✓ защищенность (защита от кибератак, включая политики, процедуры, технические средства и контрольные процедуры);
- ✓ бдительность (от распознавания угроз до их реализации);
- ✓ устойчивость (способность быстрого реагирования на атаки и восстановление после них).

АКТУАЛЬНЫЕ УГРОЗЫ КИБЕРБЕЗОПАСНОСТИ БЕЗОПАСНОСТИ

ГРУППА ЧТПЗ

- Нарушение конфиденциальности информации ограниченного доступа (коммерческая тайна, персональные данные и пр.);
- Запуск вредоносного программного обеспечения;
- Нарушение доступности инфраструктуры.

УВЕЛИЧЕНИЕ КОЛИЧЕСТВА ИНЦИДЕНТОВ ИБ В 2020

ГРУППА ЧТПЗ

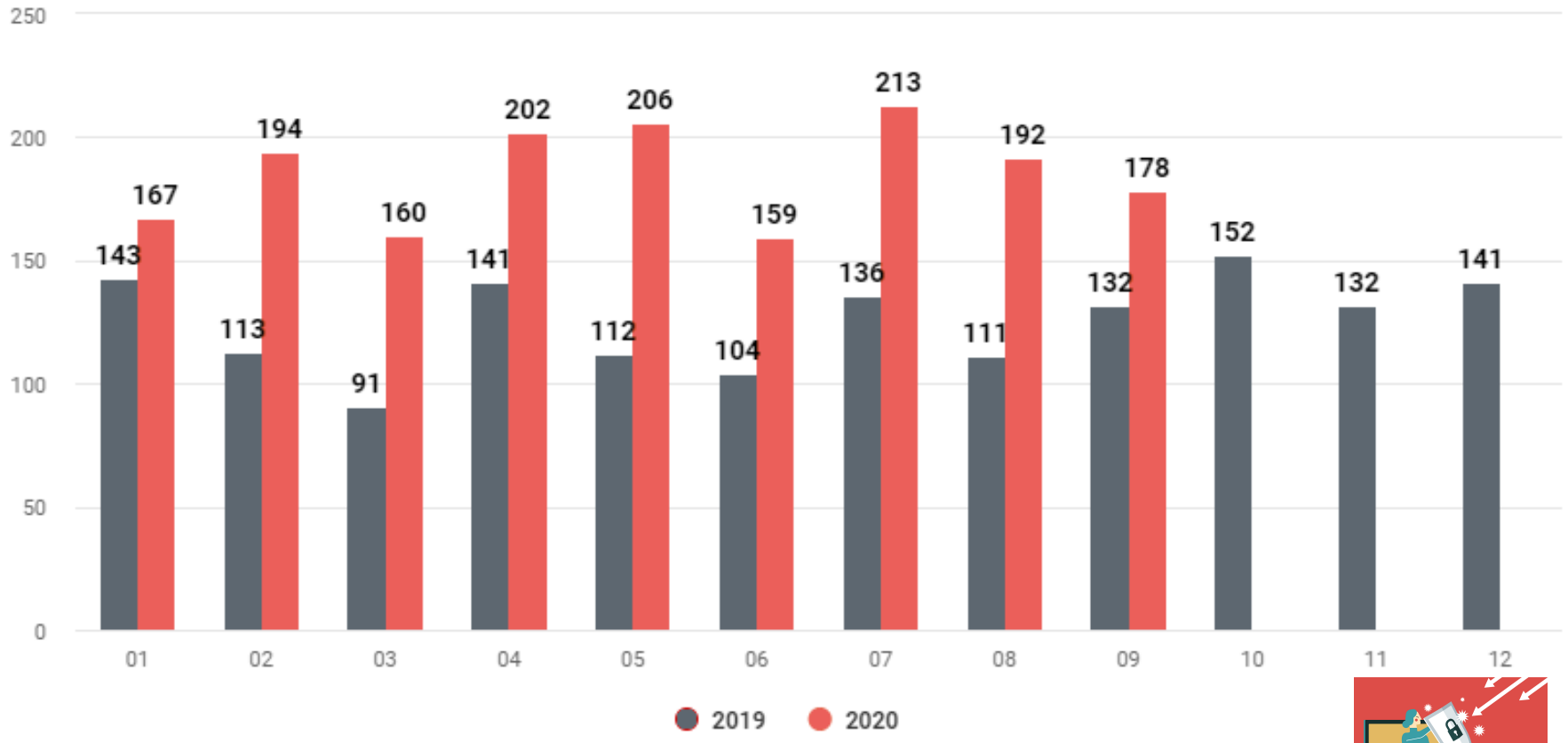


Рисунок 1. Количество инцидентов в 2019 и 2020 годах (по месяцам)

ЧТО ИЗМЕНИЛОСЬ В РАБОТЕ КОМПАНИЙ В 2020 ГОДУ?

ГРУППА ЧТПЗ

НАРУШЕНИЕ КОНФИДЕНЦИАЛЬНОСТИ ИНФОРМАЦИИ ОГРАНИЧЕННОГО ДОСТУПА. РИСИКИ

ГРУППА ЧТПЗ

- Более широкие возможности работника на «удаленке» для несанкционированного копирования информации;
- Трудности при организации контроля за большим потоком информации;
- Возможность несанкционированного/непреднамеренного доступа третьих лиц к устройствам, на которых обрабатывается информация;
- Возможность использования личных устройств, не соответствующих корпоративным политикам в области информационной безопасности, для обработки информации;
- Трудности с полноценным контролем обработки информации на личных устройствах.

ЗАПУСК ВРЕДОНОСНОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ. РИСКИ

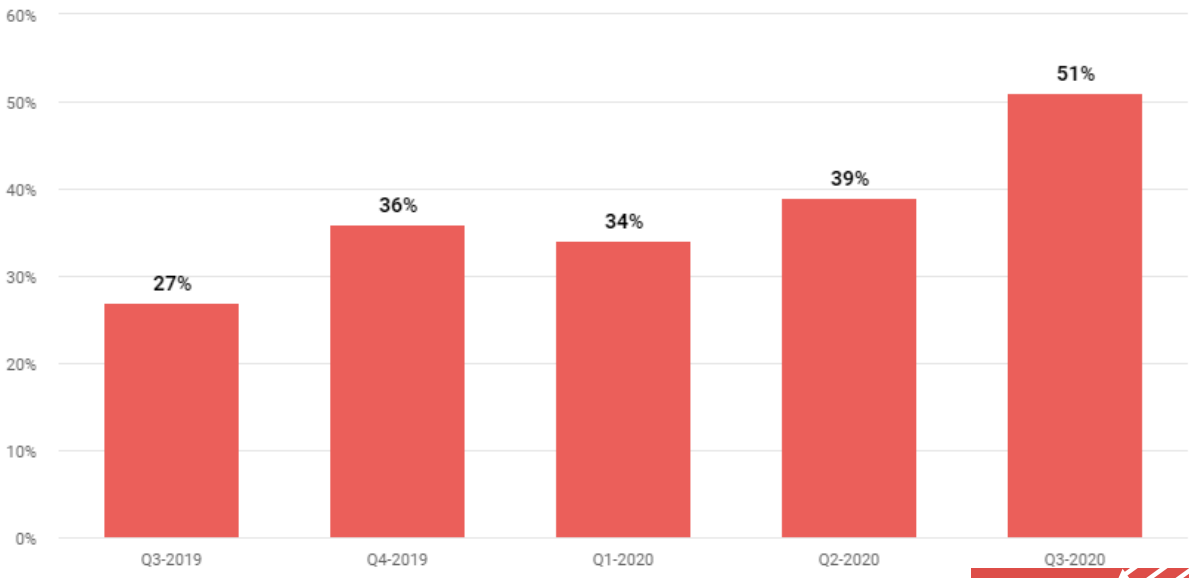
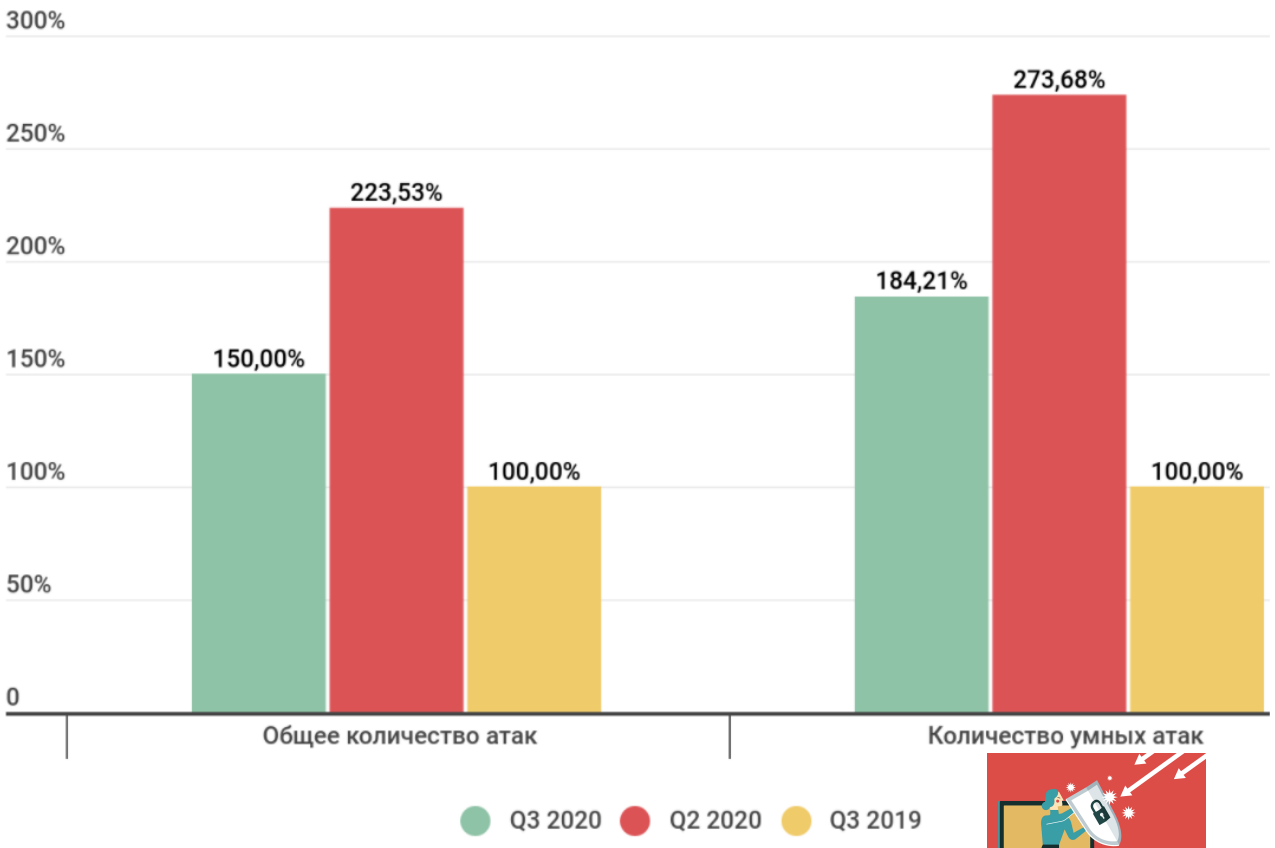


Рисунок 13. Атаки шифровальщиков (доля атак с использованием ВПО)

- Повышенная вероятность использования работниками неучтенных съемных носителей информации в удаленном режиме работы;
- Возможность отвлечения работника в удаленном режиме работы (посещение сторонних сайтов; загрузка, использование стороннего ПО);
- Невозможность полного контроля за наличием средств антивирусной защиты и обновлений безопасности на личных устройствах работников.

НАРУШЕНИЕ ДОСТУПНОСТИ ИНФРАСТРУКТУРЫ ДЛЯ ОБЕСПЕЧЕНИЯ УДАЛЕННОЙ РАБОТЫ

ГРУППА ЧТПЗ



- Увеличение значимости для бизнеса инфраструктуры, обеспечивающей удаленную работу;
- Возросшая нагрузка на сетевое оборудование и серверы;
- Общемировая тенденция увеличения числа DDoS-атак в 2020 г. (в сравнении с 2019 г.)

МЕТОДЫ АТАК НА ИНФРАСТРУКТУРУ ПРОМЫШЛЕННЫХ ПРЕДПРИЯТИЙ В 2020

ГРУППА ЧТПЗ

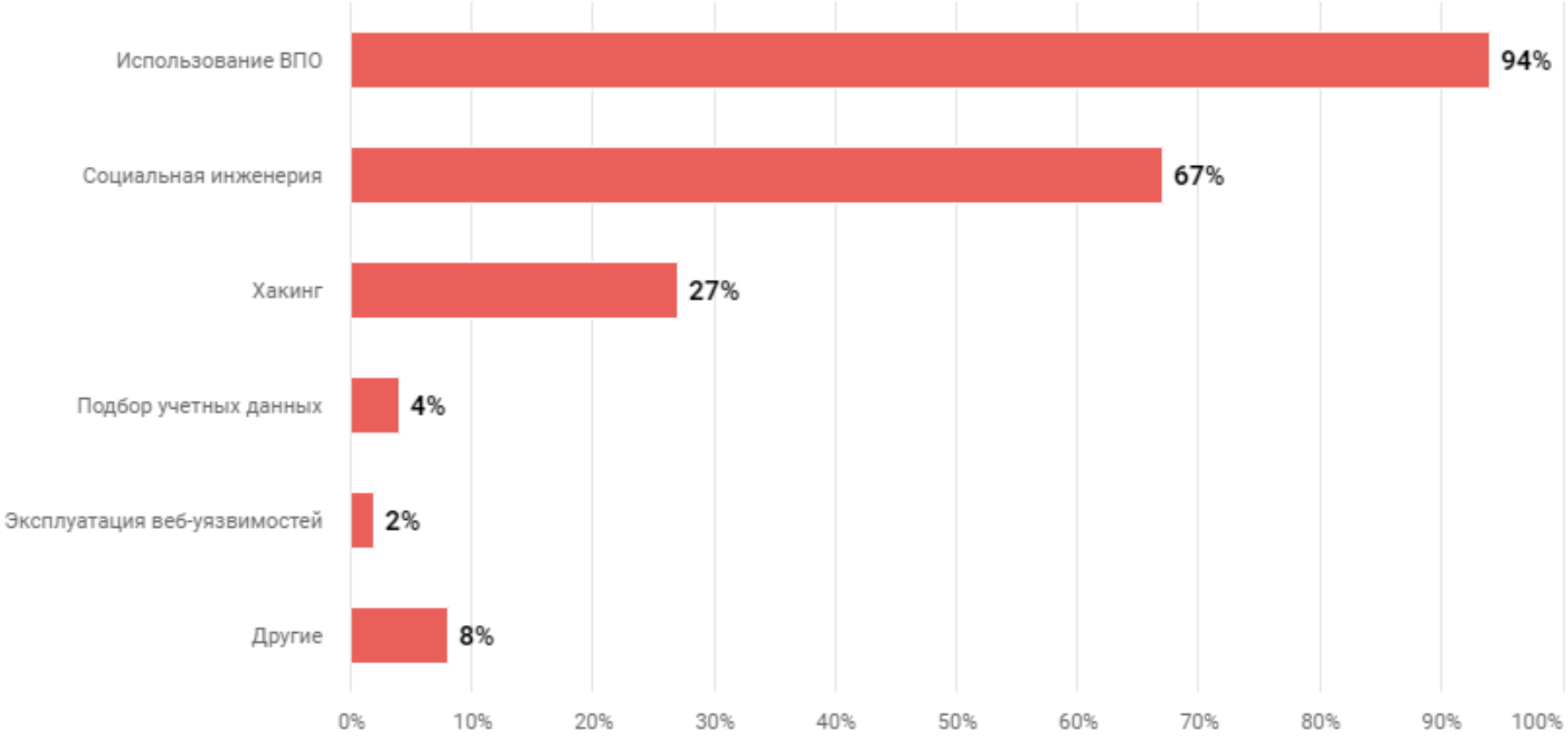


Рисунок 17. Методы атак (доля атак на промышленность)

ПРОБЛЕМЫ

ГРУППА ЧТПЗ

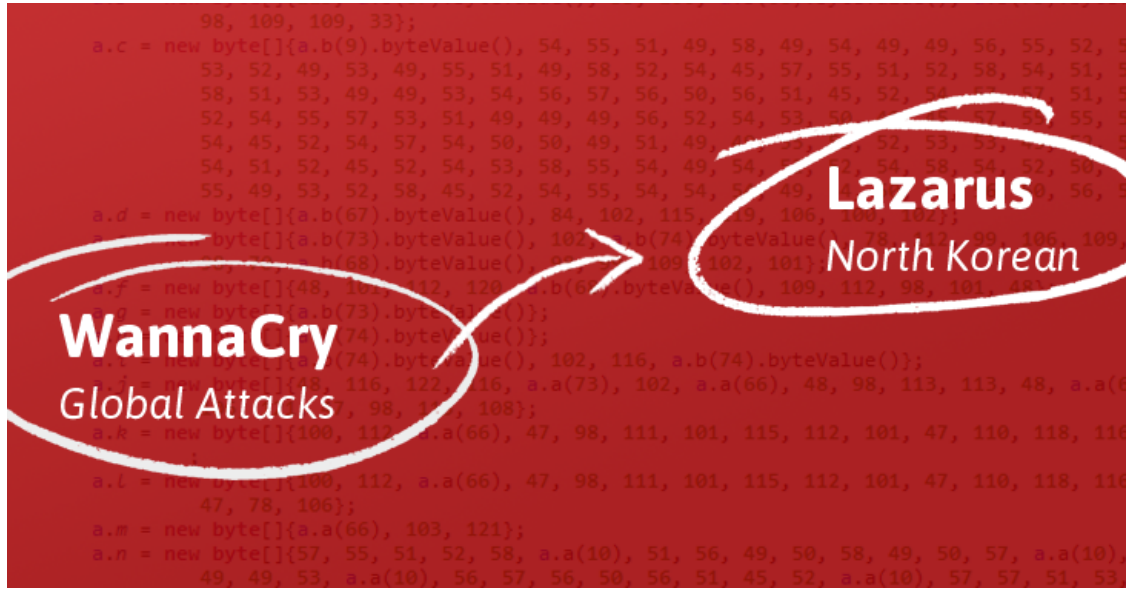
- Увеличение количества фишинговых атак в 2020 г., в том числе таргетированных, использующих повестку COVID-19*;
- Недостаточная осведомленность работников в вопросах информационной безопасности;
- Сниженная бдительность работников в удаленном режиме работы**.

* В апреле Google заблокировала 18 миллионов ежедневных вредоносных и фишинговых писем, связанных с коронавирусом (Google)

** 47% сотрудников назвали отвлечение внимания причиной того, что они попались на фишинговую аферу во время работы из дома (Tessian)

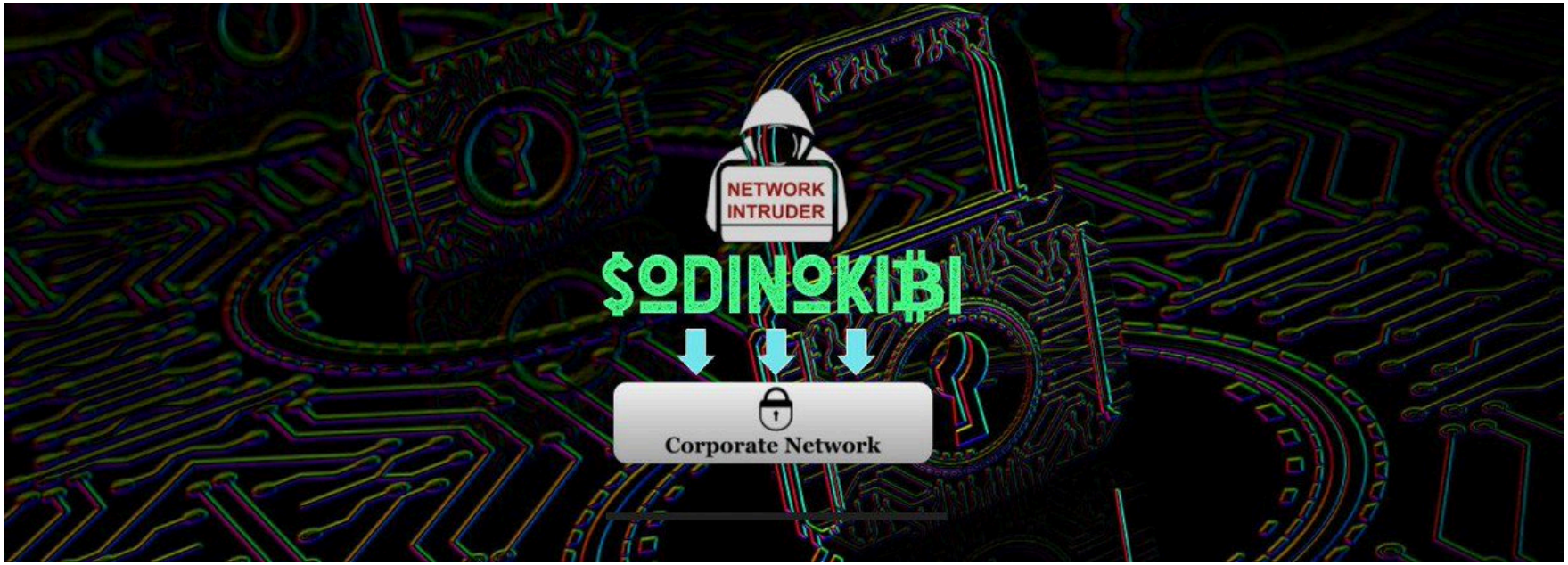
RANSOMEWARE AS A SERVICE

ГРУППА ЧТПЗ



RANSOMEWARE AS A SERVICE

ГРУППА ЧТПЗ



RANSOMEWARE AS A SERVICE

РЕЗЮМЕ. БДИТЕЛЬНОСТЬ

ГРУППА ЧТПЗ

- Это не только способность и возможность распознавать угрозы заранее, специальными программными, программно-аппаратными системами, каким то узким кругом «понимающих» работников, ИБ и ИТ специалистов.
- В современных условиях «бдительность» - некая тотальную величину.

Реалии нашего времени требуют, чтобы это была бдительность «всех и вся». Начиная от оператора принимающего осознанное решение открывать или нет сообщение от неизвестного адресата, до руководителей предприятия, четко понимающих и поддерживающих действия ответственных за кибербезопасность.

СПАСИБО
ЗА ВНИМАНИЕ!

ГРУППА
ЧТПЗ