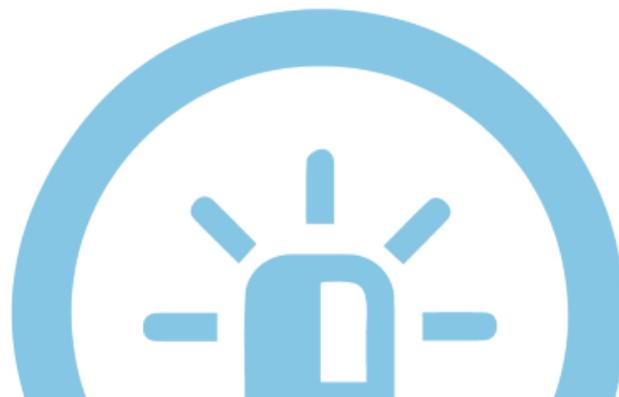




105082, Россия, г. Москва
ул. Большая Почтовая, 55/59с
Телефон: +7 (495) 972-98-26
E-mail: info@it-task.ru



Инциденты из жизни компаний



КОД
ИНФОРМАЦИОННОЙ
БЕЗОПАСНОСТИ

#CODEIB



105082, Россия, г. Москва
 ул. Большая Почтовая, 55/59с
 Телефон: +7 (495) 972-98-26
 E-mail: info@it-task.ru



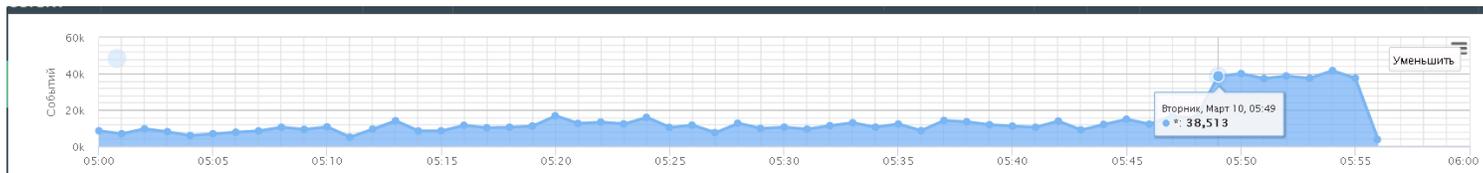
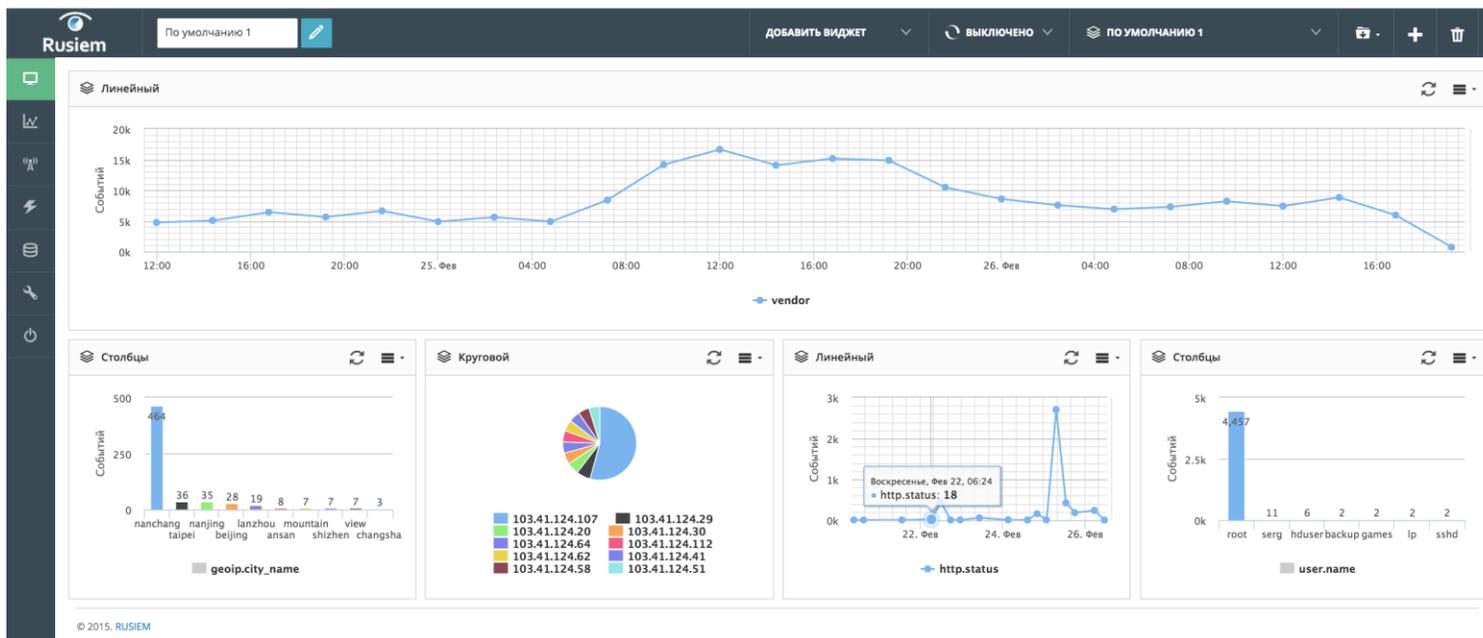
Rusiem

ВСЁ ПОД КОНТРОЛЕМ



КОД
ИНФОРМАЦИОННОЙ
БЕЗОПАСНОСТИ

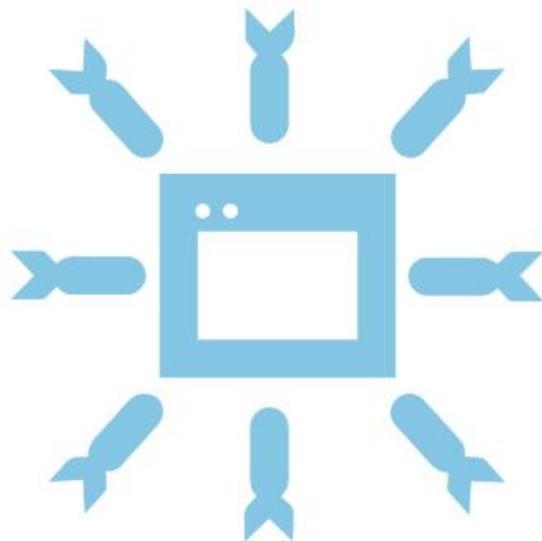
Почему мы много видели?



#CODEIB

(APT) Целевые атаки

Цель: Получить доступ к ценным данным и сохранить его как можно дольше

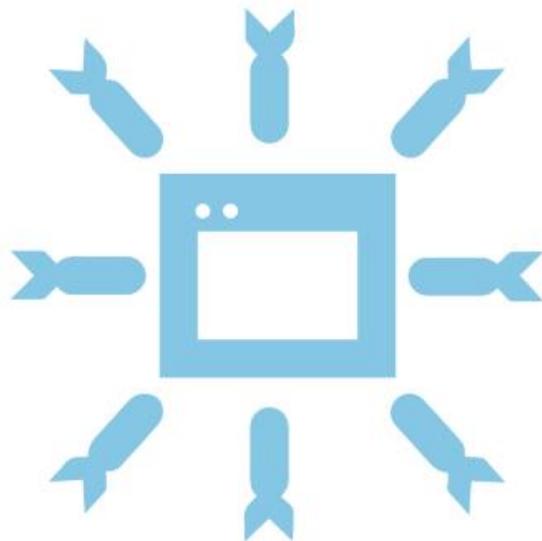


Характеристики APT:

- атакует группа;
- атаки направлены на конкретные компании или производственные сектора;
- атакующие стремятся к полному контролю над жертвой;
- атакующие вернутся;
- атакующие тщательно маскируют свое присутствие;
- сигнатуры для обнаружения APT - будут недоступны долгое время после начала атаки, поскольку индивидуальный подход и скрытность
- лишают антивирусных вендоров какой бы то ни было информации о методах злоумышленников;
- используются эксплойты нулевого дня;
- мощная продуманная социальная атака;
- атакующие наблюдают за жертвой в режиме реального времени.



105082, Россия, г. Москва
ул. Большая Почтовая, 55/59с
Телефон: +7 (495) 972-98-26
E-mail: info@it-task.ru



КОД
ИНФОРМАЦИОННОЙ
БЕЗОПАСНОСТИ

Примеры реализации



#CODEIB

Как это выглядит?





105082, Россия, г. Москва
ул. Большая Почтовая, 55/59с
Телефон: +7 (495) 972-98-26
E-mail: info@it-task.ru



КОД
ИНФОРМАЦИОННОЙ
БЕЗОПАСНОСТИ

Что делать?

- Использование классических решений
 - Защита от таргетированных атак
 - Обучение пользователей
 - SIEM
 - Антифрод
-
- *Информация на компьютерах?*
 - VDI
 - DLP
 - VPN
 - Proxy
-
- *Как вывести данные из ЦОДа?*

#CODEIB



105082, Россия, г. Москва
ул. Большая Почтовая, 55/59с
Телефон: +7 (495) 972-98-26
E-mail: info@it-task.ru

Вопросы



Степченков Максим

Генеральный директор АйТи Таск

Сот.: +7 (903) 164-31-31

E-mail: m.stepchenkov@it-task.ru

www.it-task.ru

Спасибо за внимание!



КОД
ИНФОРМАЦИОННОЙ
БЕЗОПАСНОСТИ

#CODEIB