ПРОТИВОДЕЙСТВИЕ КИБЕРПРЕСТУПНОСТИ

COUNTERING CYBERCRIME

Daniar Kachkimbaev

kachkimbaev.da@cert.gov.kg

24 SEPTEMBER 2020

ПОДРАЗДЕЛЕНИЕ РЕАГИРОВАНИЯ НА КОМПЬЮТЕРНЫЕ ИНЦИДЕНТЫ CERT-KG

- В 2015 году создано подразделение реагирования на компьютерные инциденты.
- В 2018 году зарегистрировано наименование CERT-KG у правообладателя университета Карнеги-Меллона.
- По условиям соглашения подразделение CERT-KG включено в список национальных уполномоченных организаций по реагированию на компьютерные инциденты, имеющих право на использование знака «CERT», на официальном сайте данной организации www.cert.org, www.sei.cmu.edu.

LICENSE AGREEMENT

THIS AGREEMENT is effective as of the 15 day of August, 2018, by and between:

CARNEGIE MELLON UNIVERSITY

(hereinafter "CARNEGIE MELLON"), a non-profit organization organized and existing under the laws of the Commonwealth of Pennsylvania, United States of America, located at 5000 Forbes Avenue, Pittsburgh, PA 15213, and

Authorized to Use CERT™
CERT is a mark owned by
Carnegie Mellon University

СТАТИСТИКА КИБЕРУГРОЗ В КЫРГЫЗСТАНЕ

В целях противодействия киберугрозам подразделением кибербезопасности CERT-KG регулярно проводиться техническая проверка и аудит информационных систем государственных органов Кыргызской Республики.

ЗА 2019 ГОД В ИНФОРМАЦИОННЫХ СИСТЕМАХ ГОСУДАРСТВЕННЫХ ОРГАНОВ БЫЛО:

- **Зафиксировано образцов вредоносного программного обеспечения – 67 тыс.**

из них более **300** образцов являются угрозами нулевого дня 0-DAY

- **Выявлено соединений с вредоносными и потенциально опасными ресурсами - 672 355 соединений**
- **Выявлено попытки перенаправление на вредоносные домены - 8534**

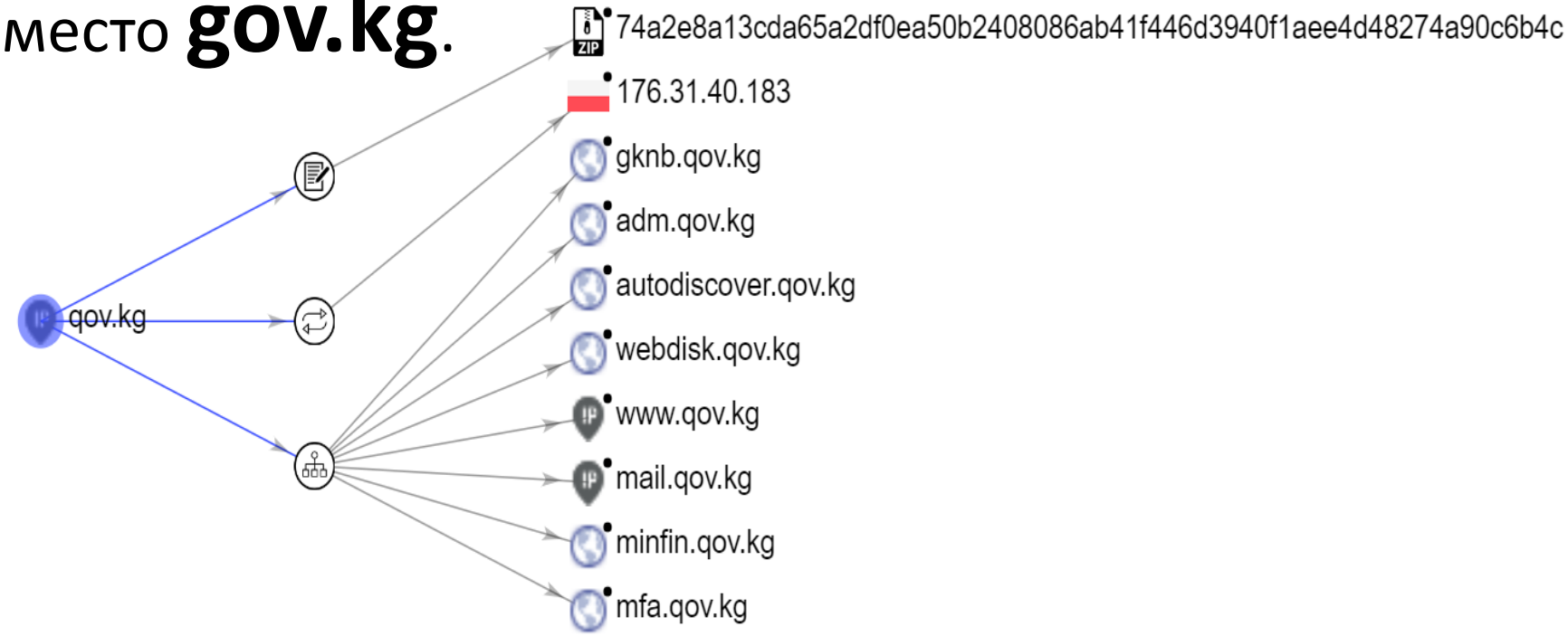
ВЫЯВЛЕНЫ ОБРАЩЕНИЕ И ЗАПРОСЫ К СЕРВЕРАМ, ИМЕЮЩИМ ОТНОШЕНИЕ:

APT 28 | APT Enfal | APT SixLittleMonkeys | APT PlugX | APT Octopus

APT Pitty Tiger | APT Zebrocy | APT RedOctober | APT IndigoZebra | APT NetTraveler

КИБЕРУГРОЗЫ В КЫРГЫЗСТАНЕ ВО ВРЕМЯ ПАНДЕМИИ 2020 ГОД

Во время пандемии участились фишинговые рассылки направленные на государственный сектор. При чём применялось хитрое словосочетание **qov.kg** вместо **gov.kg**.



В ходе анализа прикрепленного вредоносного вложения обнаружено, что файл крадет аутентификационных данных от различных сервисов с компьютера.

КИБЕРУГРОЗЫ В КЫРГЫЗСТАНЕ ВО ВРЕМЯ ПАНДЕМИИ 2020 ГОД

В первой половине 2020 года были обнаружены атаки направленные на государственный сектор со стороны зарубежных APT групп. Так, в ходе анализа вредоносной программы выявлено, что использовались такие вредоносные программы как **BackDoor.PlugX** для удаленного управления зараженными компьютерами и **BackDoor.WhiteBird.1** для шифрованного соединения с сервером управления.

Поскольку несанкционированное присутствие в инфраструктурах продолжалось не менее трех лет, а журналы событий с серверов выявляли совершенно разные семейства троянов, вероятно за этими атаками, стоит не одна, а несколько групп хакеров.

ВЗАИМОДЕЙСТВИЕ С МЕЖДУНАРОДНЫМИ И ЧАСТНЫМИ ОРГАНИЗАЦИЯМИ.

Курсы повышения квалификации

СПАСИБО ЗА ВНИМАНИЕ!