С нами надежно.

РоссельхозБанк

Опыт взаимодействия с ГосСОПКА
Реагирование на компьютерные атаки на объектах КИИ

Д.А. Машков
АО «Россельхозбанк»

Безопасность объектов критической информационной инфраструктуры

РоссельхозБанк

Государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации (Система «ГосСОПКА»)

Национальный координационный центр по компьютерным инцидентам (НКЦКИ)

Заключение Соглашения о взаимодействии с Федеральной службой безопасности Российской Федерации при решении задач, касающихся обнаружения, предупреждения и ликвидации последствий компьютерных атак

Создание подразделения – Корпоративный центр взаимодействия с Системой «ГосСОПКА»

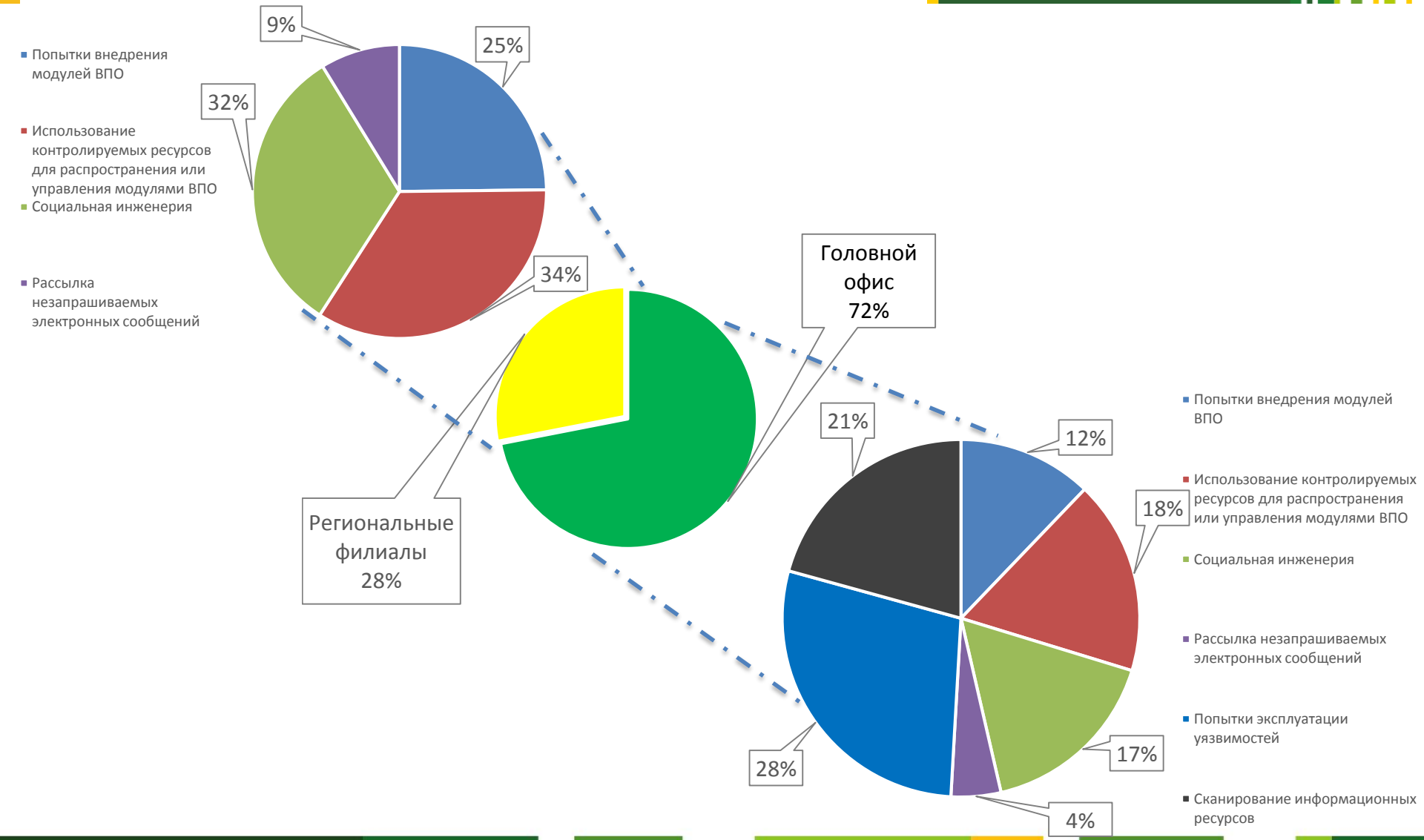
Подключение к Системе «ГосСОПКА»

Взаимодействие с НКЦКИ

РоссельхозБанк

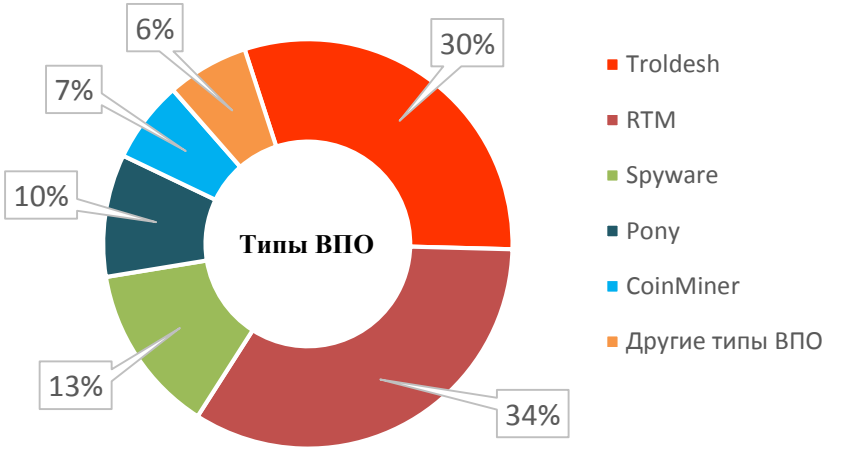
- Приказ ФСБ России от 19.06.2019 № 282
- Приказ ФСБ России от 24.07.2018 № 367
- Приказ ФСБ России от 24.07.2018 № 368
- Регламент взаимодействия с Системой «ГосСОПКА»
- Федеральный закон от 26.07.2017 № 187-ФЗ

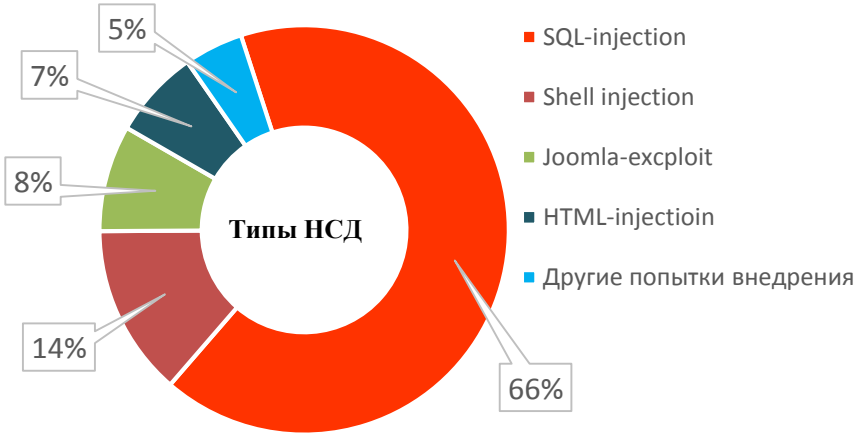
Типы компьютерных атак

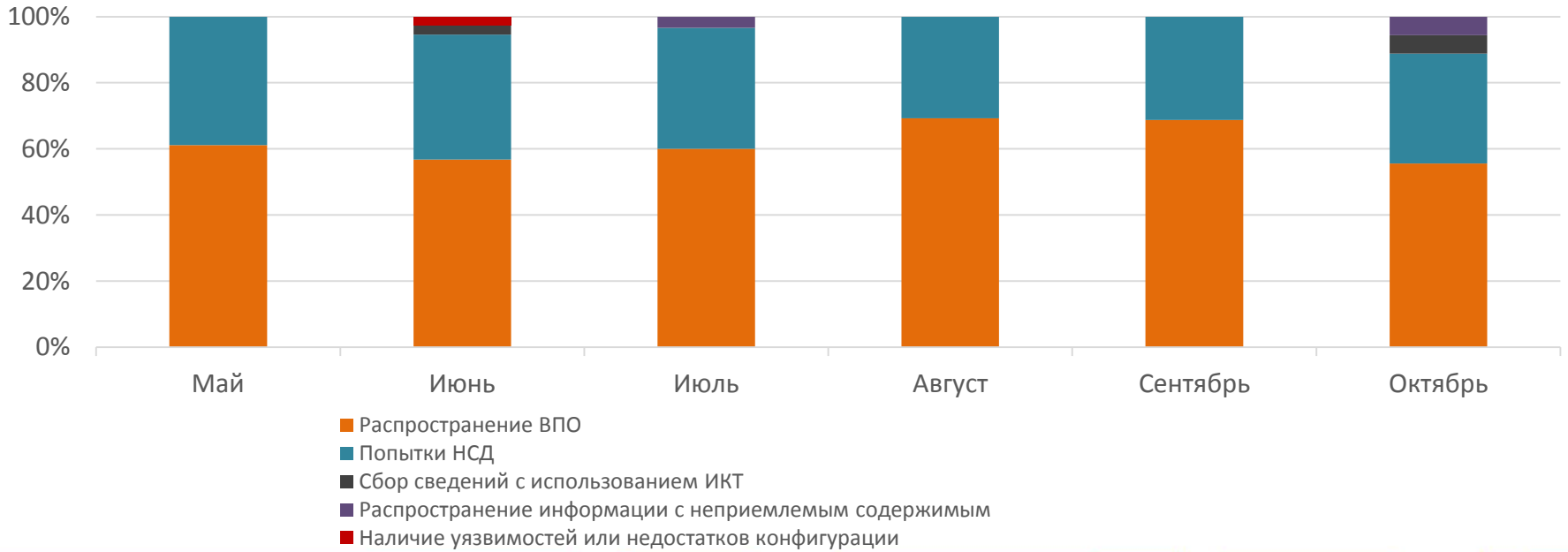


Распространенные киберугрозы (статистика за 6 месяцев 2019)

РоссельхозБанк



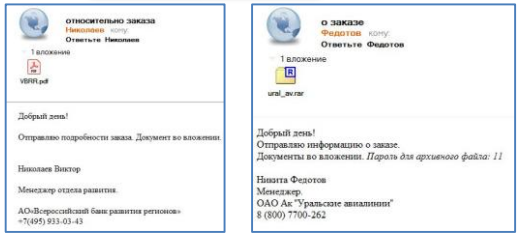




Кейс 1: Распространение ВПО/внедрение ВПО Troldesh

РоссельхозБанк

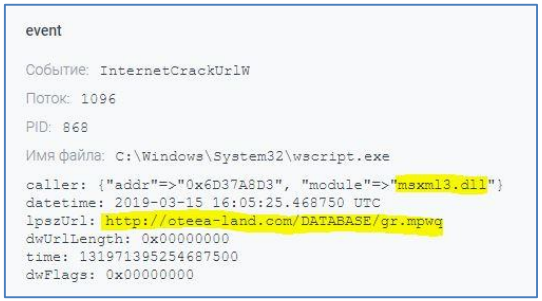
Входящие письмо



Открытие вложения .pdf, .rar, .zip и т.д.

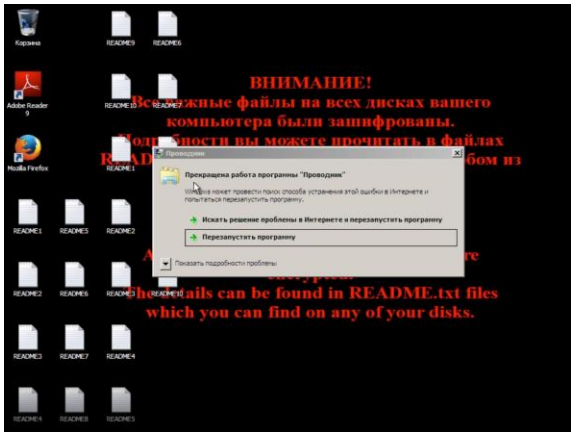
Запуск wscript.exe

Загрузка модулей ВПО из легальных репозиториев



ВПО изменяет реестр Windows, устанавливая себя в автозапуск, подменяя файл csrss.exe

ВПО уведомляет жертву о заражении



Зашифрование файлов на АРМ

C:\Sython27\Lib\lib2to3\tests\data\fixers\myfixes\0B8A7478971D8652BA12.crypted000007

Кейс 2: SQL-injection

РоссельхозБанк

Методов SQL-injection

- HTTP_POST_SQL_UnionSelect
- HTTP_POST_SQL_Select_Count
- HTTP_POST_SQL_WaitForDelay
- HTTP_POST_GroupBy
- HTTP_SQL_Sleep

Злоумышленник в одном из российских регионов

Анализ действий атакующего

Официальный сайт Банка

Корпоративный центр взаимодействия с Системой «ГосСОПКА»

ГОССОПКА
Обнаружение. Предупреждение. Ликвидация.
НКЦКИ

Управление «К» МВД России

По результатам анализа действий злоумышленника собраны и переданы в уполномоченные органы сведения о нескольких тысячах компьютеров предположительно объединенных единой бот сетью (IP-адрес, MAC-адрес, версия операционной системы, логин пользователя и др.)

Кейс 3: Madspot Digital Security Team

РоссельхозБанк

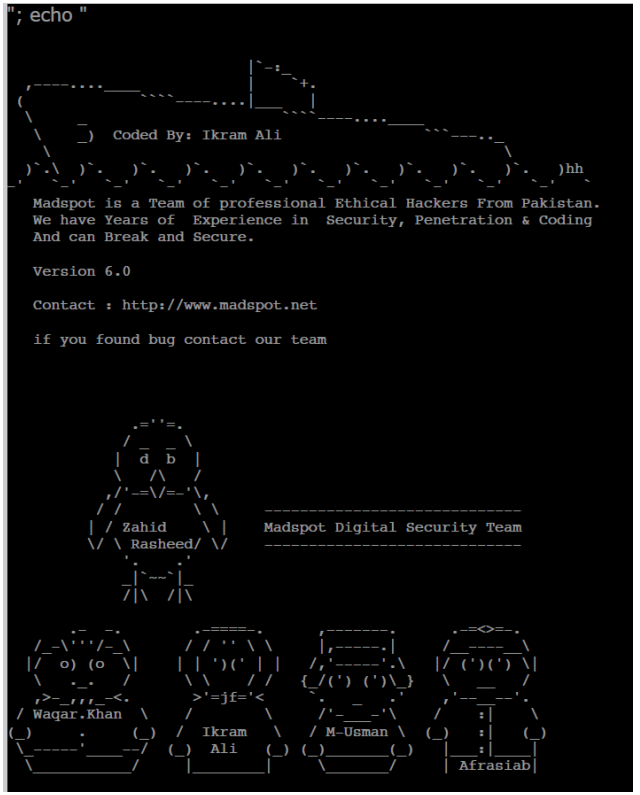
Корпоративный центр взаимодействия с Системой «ГосСОПКА»

www.m****iry.com/style/factory_big_img/**1.jpg**

Сайт контрагента www.m**iry.com**

ГОССОПКА
Обнаружение. Предупреждение. Ликвидация.
НКЦКИ

PHP Shell



Повышение уровня реагирования на киберугрозы

Спасибо за внимание

Д.А. Машков
Начальник Корпоративного центра взаимодействия с Системой «ГосСОПКА» управления информационной безопасности Департамента безопасности АО «Россельхозбанк», mashkov@rshb.ru