События безопасности, сопровождающие покушения на хищения финансовых средств клиентов в системах дистанционного банковского обслуживания

Е. В. Янауэр

Управление информационной безопасности

ОАО «Россельхозбанк»

Особенности ОАО «Россельхозбанк»

- Имеет разветвленную региональную структуру (более 1600 дополнительных офисов в 78 регионах страны)
- Имеет разветвленную IT-архитектуру
- Основной оборот денежных средств осуществляется в регионах

Дополнительные сложности

- Централизованный контроль ситуации
- Своевременное обнаружение атаки
- Оперативное реагирование
- Разбор инцидентов в регионах
- Разработка методик предотвращения атак для Банка в целом

Схема мошеннических действий

Этап атаки	Основные признаки	Способы обнаружения	Меры предотвращения развития атаки
Заражение рабочего места ДБО клиента вредоносной программой (ВП). Злоумышленник получает доступ к ключевым документам клиента	Зараженность вредоносным кодом рабочего места ДБО клиента	Обеспечение антивирусной защиты компьютерного средства и рабочих станций клиента и своевременная проверка клиентом рабочего места ДБО с использованием антивирусных программ с актуальными базами	По своевременному сообщению клиента об обнаружении ВП - приостановка Банком обработки электронных платежных поручений (ПП), смена скомпрометированных ключей
Подготовка к хищению: изучение состояния счета, активности клиента в пользовании системой ДБО	До 15 дней после вирусной активности – «мнимое» затишье и отсутствие активных действий злоумышленника		
Формирование фиктивного электронного ПП	В журнале ДБО IP-адрес отличается от обычно используемого клиентом. Чаще всего перевод на счет платежной карты физического лица в крупном розничном банке	Дополнительный контроль всех ПП на крупные суммы. Запрос дополнительного подтверждения клиентом по альтернативным каналам связи по всем «необычным» поручениям	В случае платежа, законность осуществления которого не подтверждена клиентом – приостановка обработки электронных ПП, смена скомпрометированных ключей
Блокировка доступа клиента к управлению компьютерным средством и рабочей станцией клиентского места системы ДБО. Маскировка совершенных действий	Атака на отказ оборудования ДБО клиента/банка. Активизация деструктивной ВП на рабочем месте ДБО клиента	Мониторинг доступности системы ДБО	По сообщению клиента о неработоспособности или нештатном функционировании рабочего места ДБО – приостановка обработки электронных ПП, выявление причин нештатной ситуации

Анализ попыток хищений

По каждому этапу атаки удалось определить:

- Основные признаки атаки, с учетом типичных проявлений
- Способы обнаружения атаки
- Меры предотвращения дальнейшего развития атаки
- Меры по сбору информации для последующего разбора инцидента

В целом были определены:

- Общие методы противодействия атаке и минимизации рисков ее удачного завершения
- Порядок сбора информации для последующего разбора инцидента

Предпринятые меры

- Своевременное информирование клиентов о требованиях безопасности, выполнение которых обязательно для предотвращения хищений денежных средств злоумышленниками
- Разработаны и направлены службам безопасности региональных филиалов типовые рекомендации по обеспечению информационной безопасности системы ДБО
- Разработан типовой порядок разбора инцидентов, который позволяет оперативно получить всю необходимую информацию для передачи в территориальные подразделения «К» органов внутренних дел
- Установлен типовой порядок взаимодействия с территориальными подразделениями «К» органов внутренних дел при разборе инцидентов

Спасибо за внимание!

Е. В. Янауэр,

Управление информационной безопасности

ОАО «Россельхозбанк»