Оксиджен софтвер

Полный цикл расследования инцидента одним инструментом. Это реально!

Полина Мельникова

Маркетолог,
«Оксиджен Софтвер»

APT-атака (Advanced Persistent Threat)

имеет конкретные цели, направленные против определенной организации.

Чаще всего APT-атакам подвергаются:

1. Государственные предприятия
2. Медицинские учреждения
3. Промышленные предприятия
4. Сфера науки и образования
5. Финансовые компании
6. IT-компании

Средняя сумма ущерба: **239 миллионов долларов США**

На восстановление системы уходит: **около 512-ти часов**

Страны, подвергшиеся атакам RTM

1. Россия
2. Белоруссия
3. Казахстан, Украина и др. страны

Оксиджен софтвер

ТОР 10 семейств банковского вредоносного ПО

	Название	Вердикты
1	Emotet	Backdoor.Win32.Emotet
2	Zbot	Trojan.Win32.Zbot
3	CliptoShuffler	Trojan-Banker.Win32.CliptoShuffler
4	RTM	Trojan-Banker.Win32.RTM
5	Nimnul	Virus.Win32.Nimnul
6	Trickster	Trojan.Win32.Trickster
7	Neurevt	Trojan.Win32.Neurevt
8	SpyEye	Trojan-Spy.Win32.SpyEye
9	Danabot	Trojan-Banker.Win32.Danabot
10	Nymaim	Trojan.Win32.Nymaim

Топ-10 семейств банковского ВПО (1 квартал 2020 г.)

2019 г . – 21,6% - жертвы RTM

Группировка RTM (Read the Manual – «читай инструкцию»)

Факты об RTM:

1. Начала проявлять себя с 2015 г.
2. За несколько месяцев могут рассылать более 11 000 вредоносных писем.
3. Сосредоточена на коммерческих компаниях.
4. В 2020 г. увеличила свою активность в два раза.

4 способа получения RTM IP-адреса серверов управления:

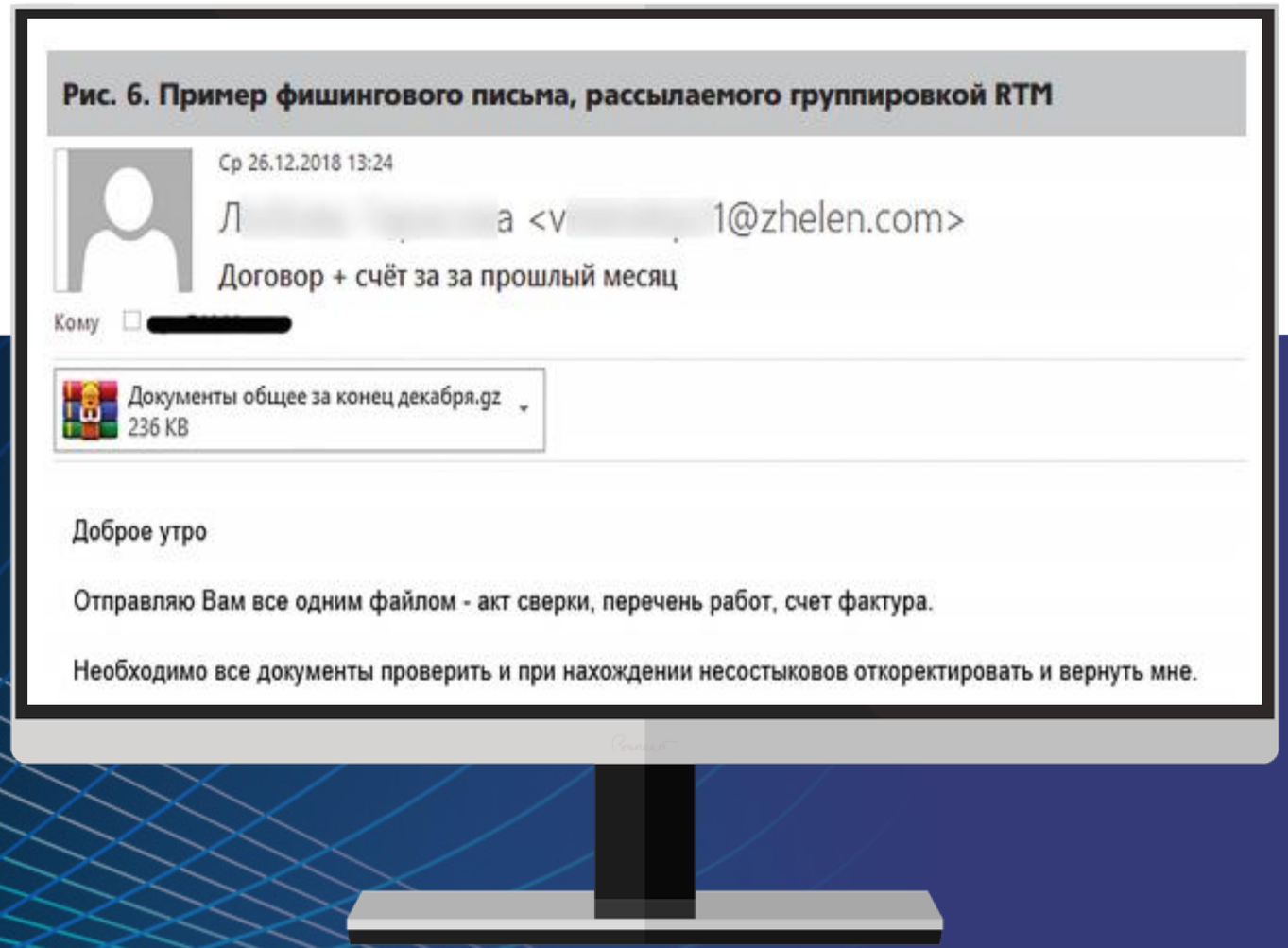
1. RSS (2015 – 2016 гг.)
2. .bit (2016 – 2019 гг.)
3. Tor (2019 г.)
4. Биткоин (с 2019 г.)

Продукты бренда «Мобильный Криминалист»

«МК Эксперт Плюс»: совершенный многофункциональный инструмент для высокоскоростной и эффективной работы с данными из мобильных устройств, дронов, облачных сервисов и ПК

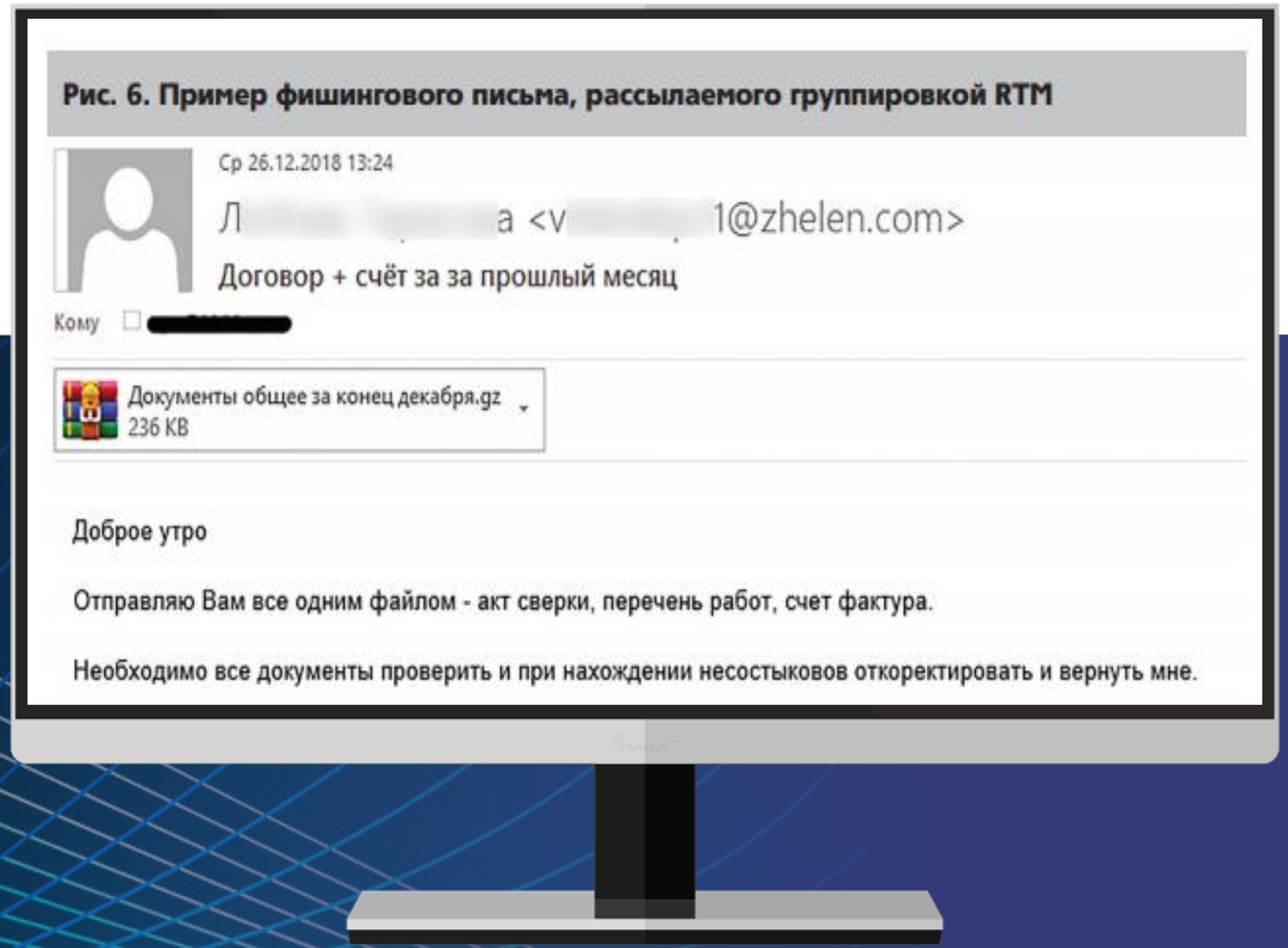
«МК Десктоп»: многофункциональный инструмент, позволяющий извлекать, расшифровывать и анализировать ключевые данные из персональных компьютеров, ноутбуков и серверов на операционных системах Windows, macOS, GNU/Linux или образов жестких дисков в формате .e01 с файловой системой NTFS.

Оксиджен софтвер



Кейс

1. Получение письма
2. Открытие вложения
3. Заражение системы



Что делать?

1 **Применение классического метода**

2 **Использование одного инструмента от «Оксиджен Софтвер»**

Оксиджен
софтвер

ВОПРОСЫ?

Оксиджен
софтвер

БЛАГОДАРЮ
ЗА ВНИМАНИЕ!