Предупреждение! Зафиксирована рассылка ВПО!

1. Краткое описание угрозы

Зафиксированы факты распространения вредоносного программного обеспечения от имени КБ «Юнистрим».

2. Основные индикаторы компрометации

1	URL-адреса и IP-адреса, к которым производятся обращения	23.227.201[.]13 dovecotd[.]com
2	Отправитель письма	m.tsutskin@unistream[.]com 94.127.156[.]7. **Обращаем ваше внимание, что адрес отправителя относится к легальному почтовому адресу КБ «Юнистрим»! Необходимо удалить письма с указанной ниже темой!**

Ниже приведены данные по известным файлам из рассылки.

Информацию об обнаружении файлов антивирусными средствами различных производителей вы можете получить, например, по данным сайта virustotal.com, введя в поле поиска соответствующие файлам хэш-суммы, либо обратившись в техническую поддержку вендора использующегося в вашей организации антивирусного средства.

Обращаем внимание на то, что использование авторами рассылки ВПО иных имён файлов, кроме указанных в настоящем бюллетене, **не исключено**.

1) "Fraud.scr".

MD5	3003a8bb4b1c9d971af971af0a561ab0
SHA1	e4fc11fbab0bf45ffa4201e5fc884bed54112529
SHA256	621c7910549a9a752167c147d068461b4120c7cd4e6e67ea633680fd0adfb16a
Размер файла (байт)	415232

3. Примеры текста писем

1	Заголовок (тема) письма	Попытки хищений

4. **Рекомендуемые меры противодействия**
   - Провести обновление антивирусных баз;
   - Контролировать соединения с IP-адресами, указанными в п.2;
   - На критичных АРМ и серверах инфраструктуры проверить создание системных служб с аргументом запуска base64 (код события 7045 в журнале «Система»), в случае обнаружения отключить зараженное устройство от локальной сети и, по возможности, выполнить переустановку ОС. В случае невозможности переустановки, свяжитесь со специалистами ФинЦЕРТ;
   - В случае технической возможности, убедиться, что на IDS-системах включено обнаружение Mimikatz.

Обращаем ваше внимание на то, что ФинЦЕРТ не отправляет неподписанные письма с вложениями! Открытие вложений писем из неподтверждённых источников может привести к компрометации ваших информационных систем и сетей!

В случаях выявления подобных инцидентов, просьба незамедлительно направлять информацию на электронный адрес fincert@cbr.ru. Информацию по возможному вредоносному программному обеспечению следует направлять в архиве (например, *.rar) с паролем virus или infected с указанием предполагаемого способа заражения.