Результаты мониторинга систем промышленной автоматизации

Второе полугодие 2022 года



Kaspersky

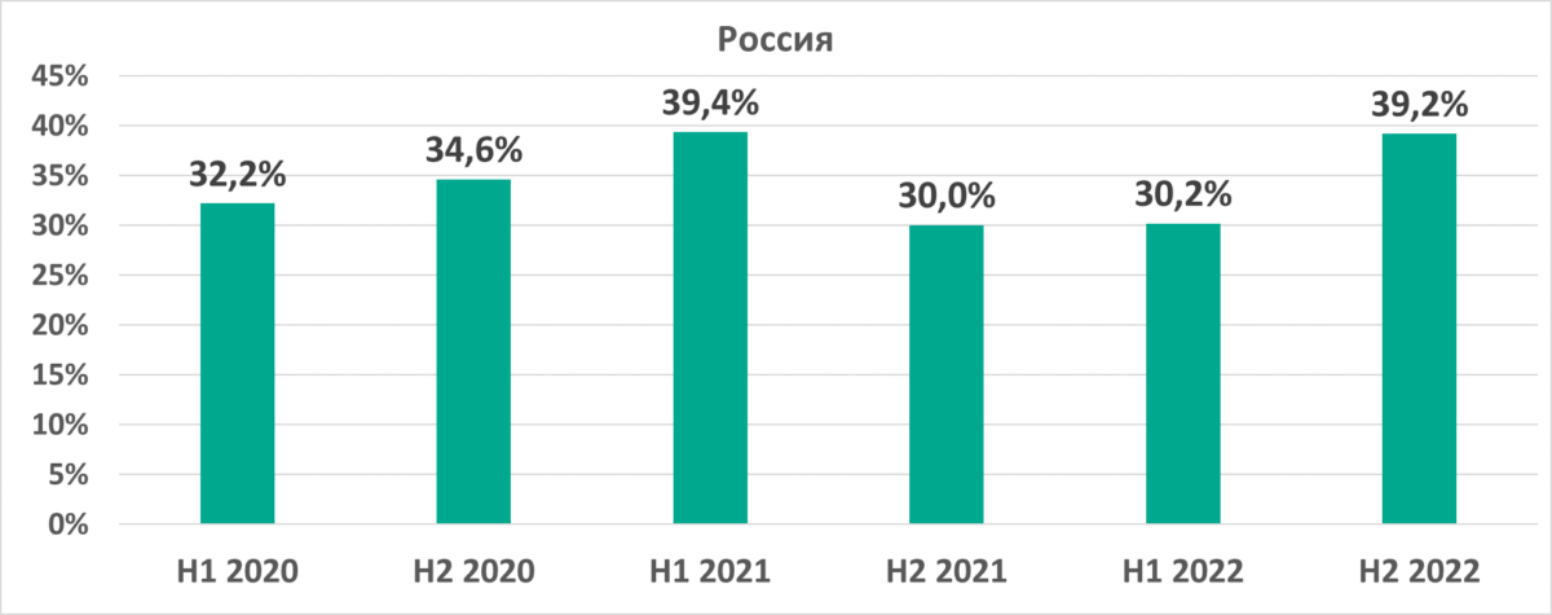
360 000+

Новых угроз обнаруживает «Лаборатория Касперского» **ежедневно**

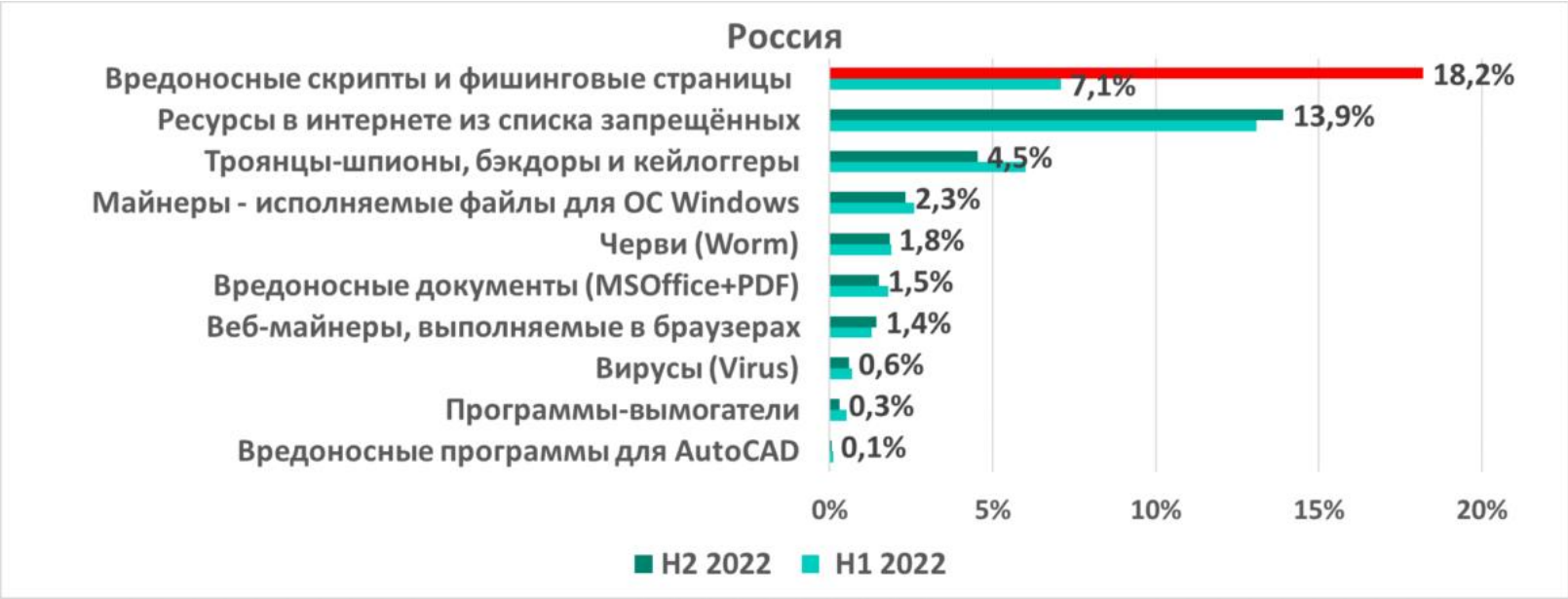
Источники информации мониторинга (они же – объекты атак):

- серверы управления и сбора данных (SCADA)
- серверы хранения данных (Historian)
- шлюзы данных (OPC)
- стационарные рабочие станции инженеров и операторов
- мобильные рабочие станции инженеров и операторов
- Human Machine Interface (HMI)
- компьютеры, используемые для администрирования технологических сетей
- компьютеры, используемые для разработки ПО для систем промышленной автоматизации

Процент компьютеров АСУ, на которых были заблокированы вредоносные объекты



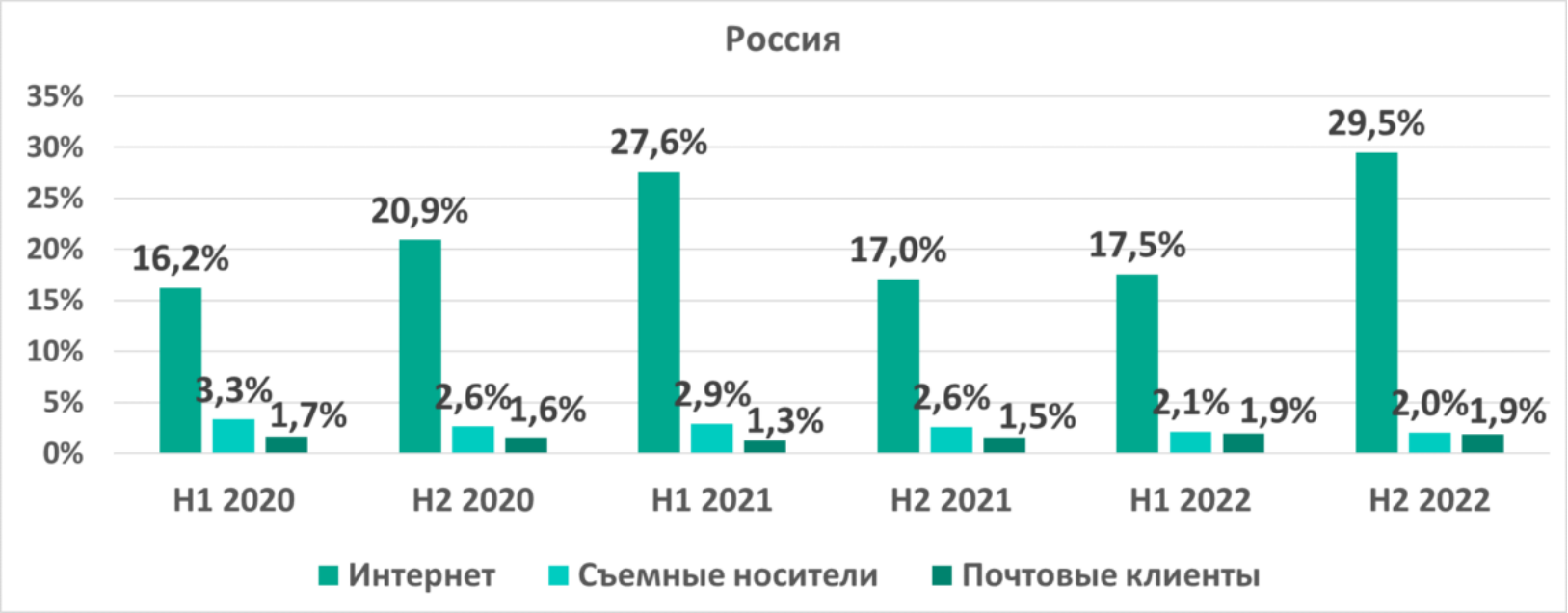
КТО (и ЧТО)???!


Россия
Вредоносные скрипты и фишинговые страницы
18,2%
7,1%
Ресурсы в интернете из списка запрещённых
13,9%
Троянцы-шпионы, бэкдоры и кейлоггеры
4,5%
Майнеры - исполняемые файлы для ОС Windows
2,3%
Черви (Worm)
1,8%
Вредоносные документы (MSOffice+PDF)
1,5%
Веб-майнеры, выполняемые в браузерах
1,4%
Вирусы (Virus)
0,6%
Программы-вымогатели
0,3%
Вредоносные программы для AutoCAD
0,1%
0%
5%
10%
15%
20%
H2 2022
H1 2022

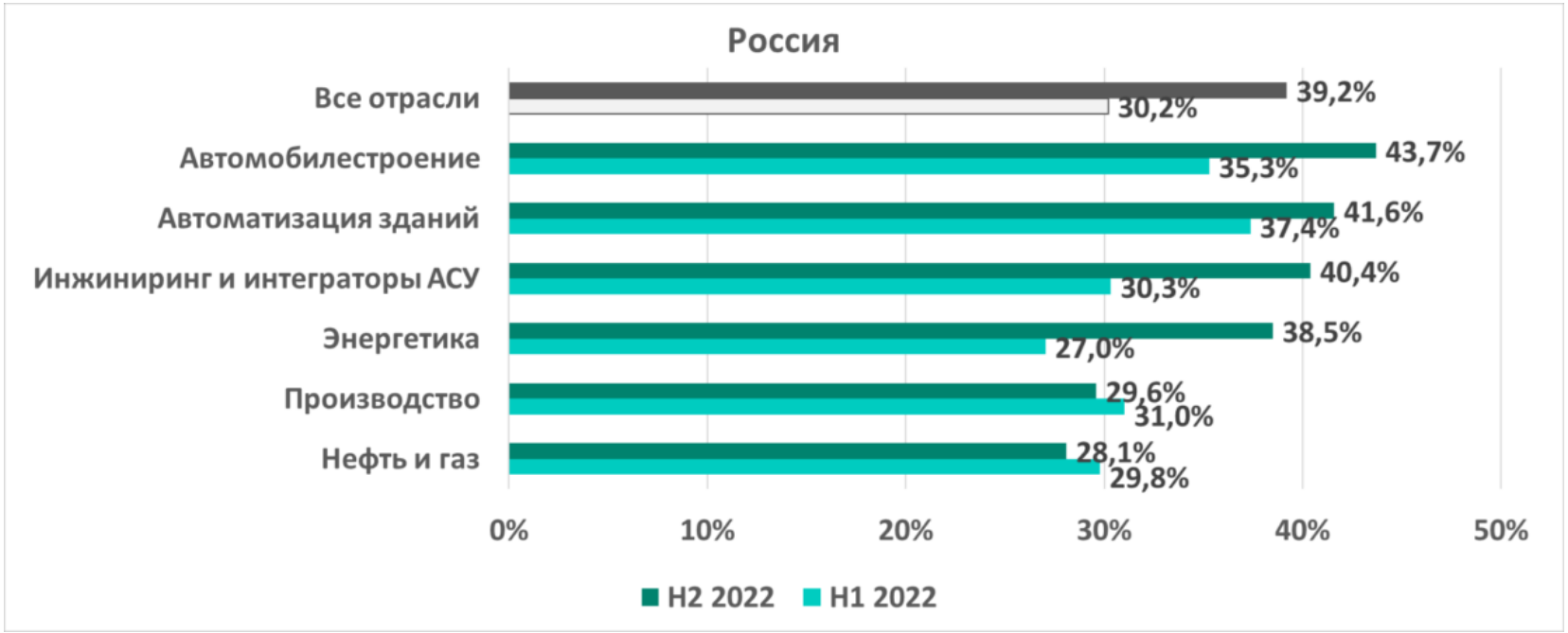
КТО (и ЧТО)?!!! (а конкретней)

- Уязвимость CVE-2022-27228 в модуле «Опросы, голосования» «движка» Bitrix CMS
- Позволяет атакующему выполнить произвольный код на стороне веб-сервера
- Массово заражались используемые на атакованных сайтах JavaScript файлы с целью перенаправления на сторонние вредоносные веб-ресурсы и фишинговые страницы
- **Обнаружена в марте 2022 (!!!)**

Через ЧТО?!!! (векторы атак)



А кто – цель (а жертвы кто)???



Тактики&техники и другие факторы ([не]успеха):

- Фишинг (в том числе фишинговые письма «на злобу дня», украденные ранее документы и почтовые ящики, в т.ч. у «смежных» организаций и партнёров)
- Использование протрояненных («поломанных») дистрибутивов, а также «патчей» и генераторов ключей общеупотребимого и специализированного ПО
- 0- и N-day уязвимости (которые теперь закрываются медленнее ввиду ухудшения доступности обновлений безопасности некоторых решений)
- Ошибки в конфигурации (типа оставленных паролей «по умолчанию»), в т.ч. СЗИ
- Использование популярных «облачных» сервисов в качестве CnC
- **И флЭшки (!!!)**

kaspersky

СПАСИБО за ВНИМАНИЕ!

Вопросы?

- **АО "Лаборатория Касперского"**
- **Москва, 125212**
- **Ленинградское шоссе, д.39А, стр.3**
- **+7 (495) 797-87-00**
- **www.kaspersky.ru**