ТБ-Форум 2023

2023.
Проблемы безопасности пром. предприятий

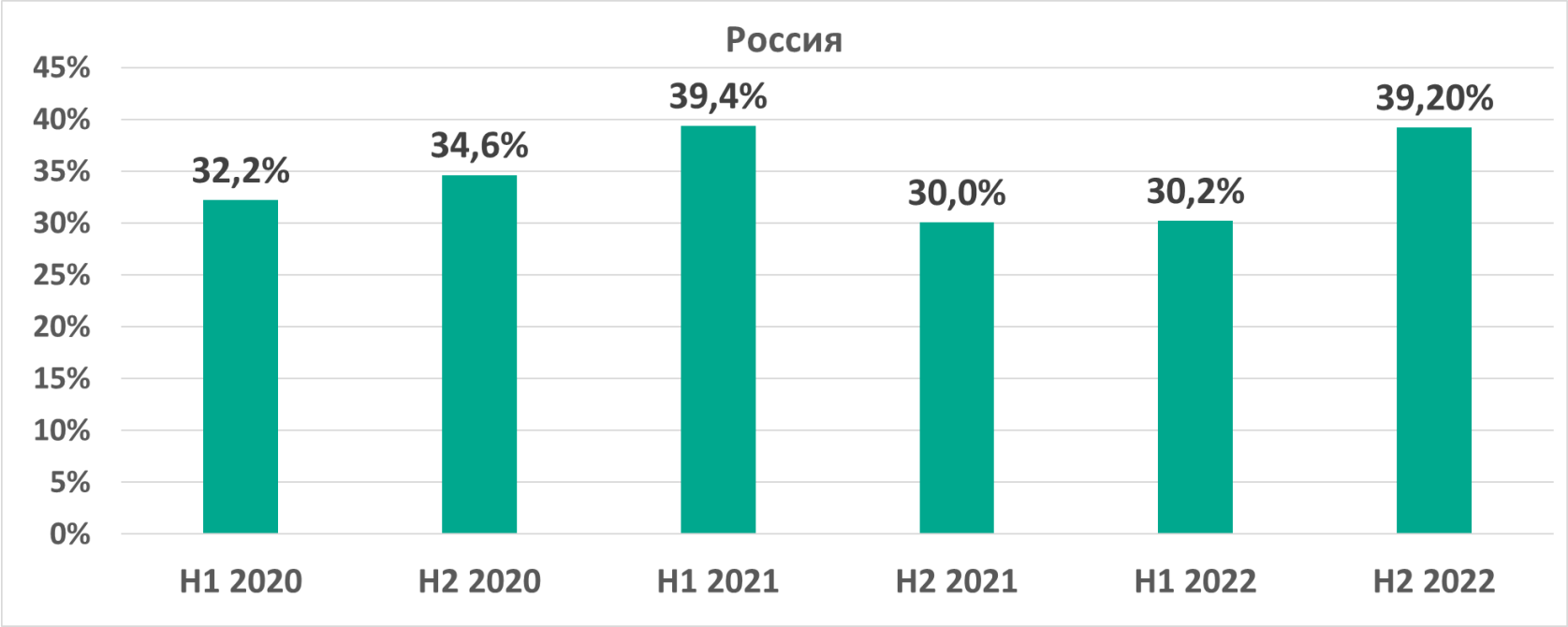
Evgeny Goncharov

Kaspersky ICS CERT

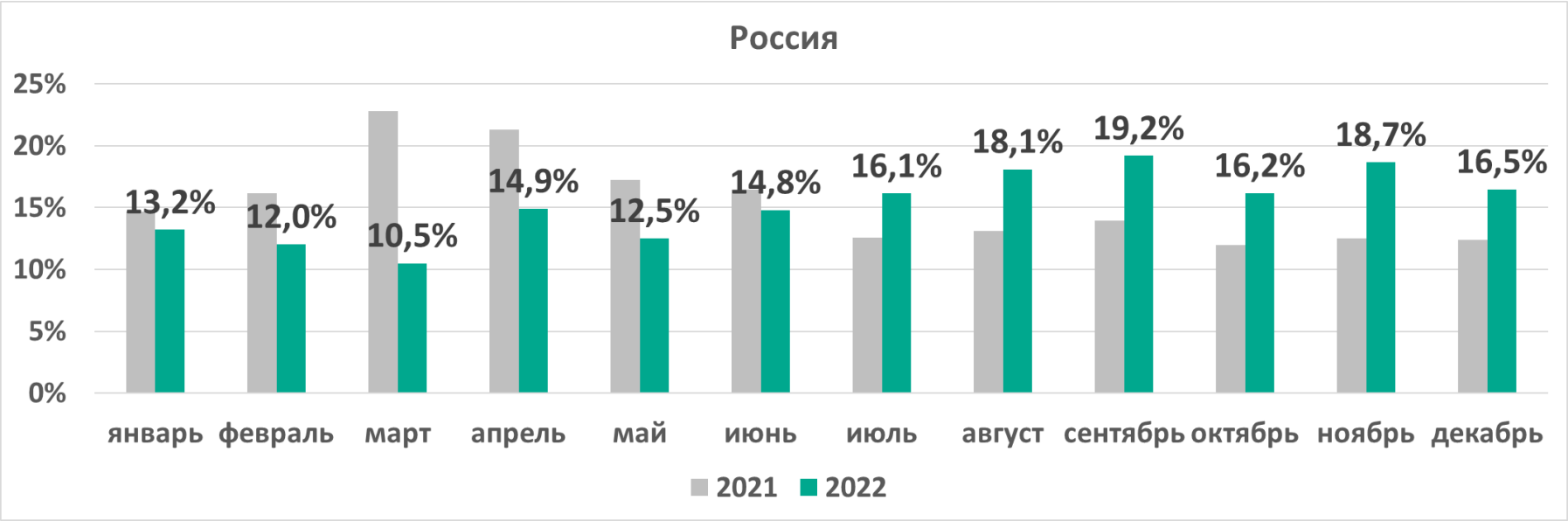
Февраль 2023

kaspersky

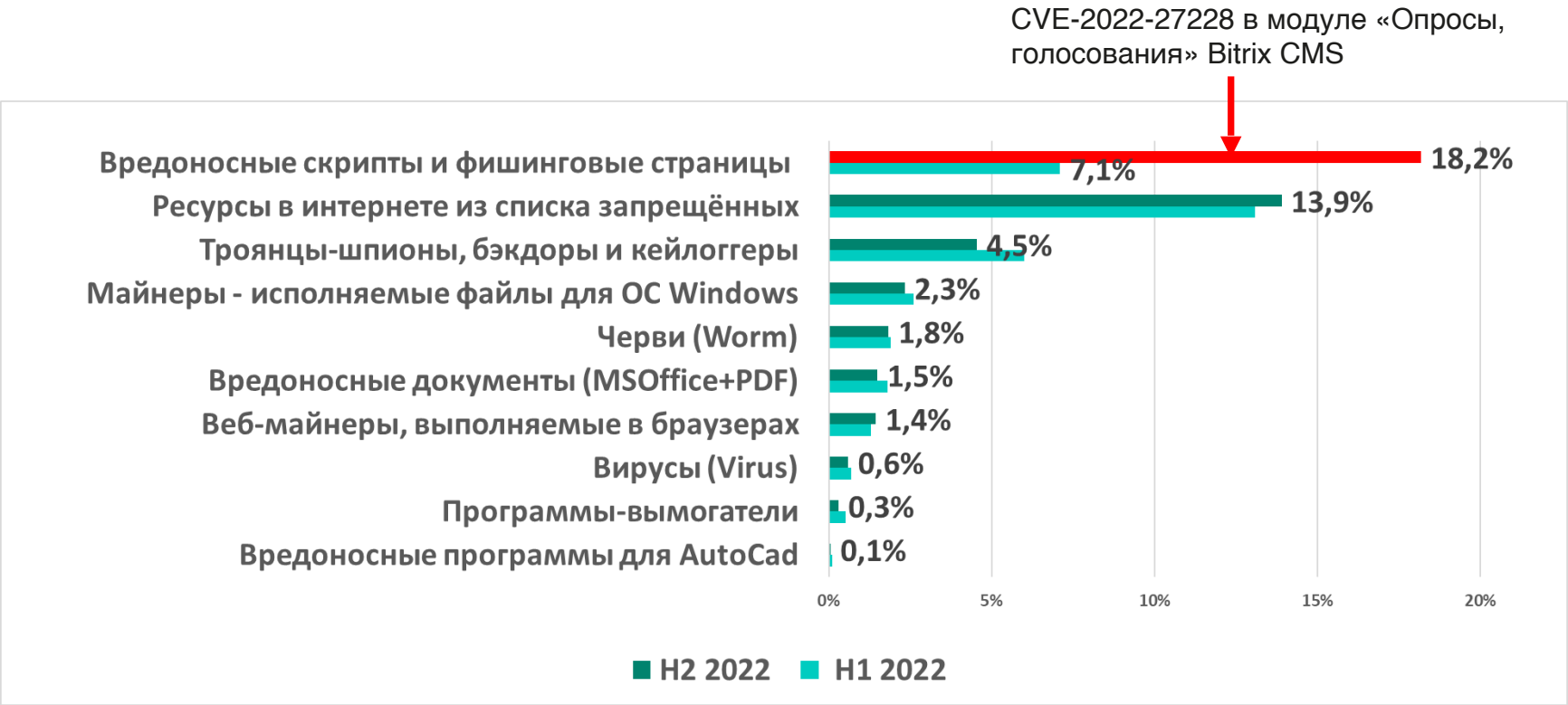
% атакованных АСУ, 2020-2022



% атакованных АСУ, 2021 - 2022



% атакованных АСУ в России, 2021 - 2022



«Импортозамещение» и уязвимости Шрёдингера. Пример №1

Регистрационный номер	Наименование программного обеспечения	Код класса	Класс программного обеспечения	Дата регистрации	Адрес сайта
[redacted]	[redacted]	05.15	Информационные системы для решения специфических отраслевых задач	25.06.2021	Ссылка
		04.04	Среды разработки, тестирования и отладки		

«Импортозамещение» и уязвимости Шрёдингера

Регистрационный номер	Наименование программного обеспечения	Код класса	Класс обесп
[redacted]	[redacted]	05.15	Инфо специ
		04.04	Средь

МИНИСТЕРСТВО ЦИФРОВОГО РАЗВИТИЯ, СВЯЗИ И МАССОВЫХ КОММУНИКАЦИЙ РОССИЙСКОЙ ФЕДЕРАЦИИ

ПРИКАЗ

_____ № [redacted]

Москва

О формировании и ведении единого реестра российских программ для электронных вычислительных машин и баз данных и единого реестра программ для электронных вычислительных машин и баз данных из государств – членов Евразийского экономического союза, за исключением Российской Федерации

В соответствии с пунктами 25, 26 Правил формирования и ведения единого реестра российских программ для электронных вычислительных машин и баз данных и единого реестра программ для электронных вычислительных машин и баз данных из государств – членов Евразийского экономического союза, за исключением Российской Федерации, утвержденных постановлением Правительства Российской Федерации от 16 ноября 2015 г. № 1236 «Об установлении запрета на допуск программного обеспечения, происходящего из иностранных государств, для целей осуществления закупок для обеспечения государственных и муниципальных нужд» (далее – Правила), и на основании решения Экспертного совета по программному обеспечению при Министерстве цифрового развития, связи и массовых коммуникаций Российской Федерации (далее – Экспертный совет) от 31 мая 2021 г.

ПРИКАЗЫВАЮ:

1. Включить сведения о программном обеспечении в единый реестр российских программ для электронных вычислительных машин и баз данных с присвоением класса (классов) в соответствии с документами заявителя согласно приложению № 1 к настоящему приказу.

2. Включить сведения о программном обеспечении в единый реестр российских программ для электронных вычислительных машин и баз данных

«Импортозамещение» и уязвимости Шрёдингера

Регистрационный номер	Наименование программного обеспечения	Код класса	Класс обесп
[redacted]	[redacted]	05.15	Инфо специ
		04.04	Средь

МИНИСТЕРСТВО ЦИФРОВОГО РАЗВИТИЯ, СВЯЗИ И МАССОВЫХ КОММУНИКАЦИЙ РОССИЙСКОЙ ФЕДЕРАЦИИ

ПРИКАЗ

_____ № [redacted]

Москва

О формировании и ведении единого реестра российских программ для электронных вычислительных машин и баз данных и единого реестра программ для электронных вычислительных машин и баз данных из государств – членов Евразийского экономического союза, за исключением Российской Федерации

В соответствии с пунктами 25, 26 Правил формирования и ведения единого реестра российских программ для электронных вычислительных машин и баз данных и единого реестра программ для электронных вычислительных машин и баз данных из государств – членов Евразийского экономического союза, за исключением Российской Федерации, утвержденных постановлением Правительства Российской Федерации от 16 ноября 2015 г. № 1236 «Об установлении запрета на допуск программного обеспечения, происходящего из иностранных государств, для целей осуществления закупок для обеспечения государственных и муниципальных нужд» (далее – Правила), и на основании решения Экспертного совета по программному обеспечению при Министерстве цифрового развития, связи и массовых коммуникаций Российской Федерации (далее – Экспертный совет) от 31 мая 2021 г.

ПРИКАЗЫВАЮ:

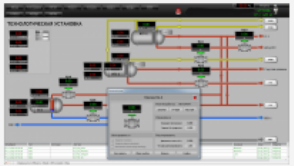
1. Включить сведения о программном обеспечении в единый реестр российских программ для электронных вычислительных машин и баз данных с присвоением класса (классов) в соответствии с документами заявителя согласно приложению № 1 к настоящему приказу.

2. Включить сведения о программном обеспечении в единый реестр российских программ для электронных вычислительных машин и баз данных

МИНИСТЕРСТВО ЦИФРОВОГО РАЗВИТИЯ, СВЯЗИ И МАССОВЫХ КОММУНИКАЦИЙ РОССИЙСКОЙ ФЕДЕРАЦИИ

Регистр
номер

[redacted]

Заказчик/Объект	Название	Фото
[redacted] БКНС-2 Казанского нефтегазоконденсатного месторождения	Автоматизированная система управления технологическими процессами подготовки технологической воды и ее последующей перекачки далее по ходу технологического процесса повышения пластового давления	
[redacted] ГКС Северо-Останинского месторождения	Система мониторинга и обработки информации о ходе технологического процесса контроля состояния объектов пожарной охраны а так же объектов с потенциальной возможностью появления опасной концентрацией горючих газов. А так же с возможностью управления запуском газового и пенного пожаротушения подконтрольных объектов.	
[redacted] ГКС Северо-Останинского месторождения	Автоматизированная система управления технологическими процессами объектов газокомпрессорной станции	
[redacted] ДНС Западно-Крапивинского месторождения	Система мониторинга и обработки информации о ходе технологического процесса подготовки нефти	

```
$ head -n10 ./[redacted]-3.18.6-Base-debian.x86_64/opt[redacted]AR/3.18/ReadmeP006.txt
=====================================================================
Patch P006 "DECEMBER-2021" for WinCC OA Version 3.18      December 2021
=====================================================================


Summary:
========


 Enhancements and bugfixes for WinCC OA.
```

Siemens WinCC OA

“ CVE-2022-33139, CVSSv3: 9.8

The following versions of SIMATIC WinCC OA, a SCADA HMI system, are affected:

- SIMATIC WinCC OA v3.16: All versions
- SIMATIC WinCC OA v3.17: All versions
- SIMATIC WinCC OA v3.18: All versions

Siemens (https://cert-portal.siemens.com/productcert/pdf/ssa-111512.pdf)

Главная / Список уязвимостей

ФИЛЬТРАЦИЯ

Контекстный поиск по названию уязвимости

Введите слово или словосочетание

Производитель ПО

Siemens AG

Тип ПО

Выберите тип ПО

Программное обеспечение

SIMATIC WinCC OA

По Вашему запросу найдено **9** записей

Выводить по: 10, 20, 50, 100 Сортировка:

BDU:2022-03715	Уязвимость SCADA-системы SIMATIC WinCC, связанная с во аутентификации на стороне клиента, позволяющая нарушите
BDU:2021-02031	Уязвимость сетевого программного обеспечения Siemens, свя написании элементов или путей поиска, позволяющая наруш код с повышенными привилегиями

Программное обеспечение

Выберите программное обеспечение

[redacted]

Совпадений не найдено

Управлять уязвимостями

Уведомление пользователей

Канал приёма информации о новых уязвимостях

Поиск новых уязвимостей в продукте

Уязвимости в используемых компонентах

Чем Kaspersky может помочь?

Анализ безопасности продукта

Анализ процессов разработки и поддержки

Threat Intelligence

Тренинги по поиску уязвимостей

Ближний Восток. Цементный завод

Периодическое зависание PLC в OT сети

(~150 PLC)

Какой-либо привязки ко времени

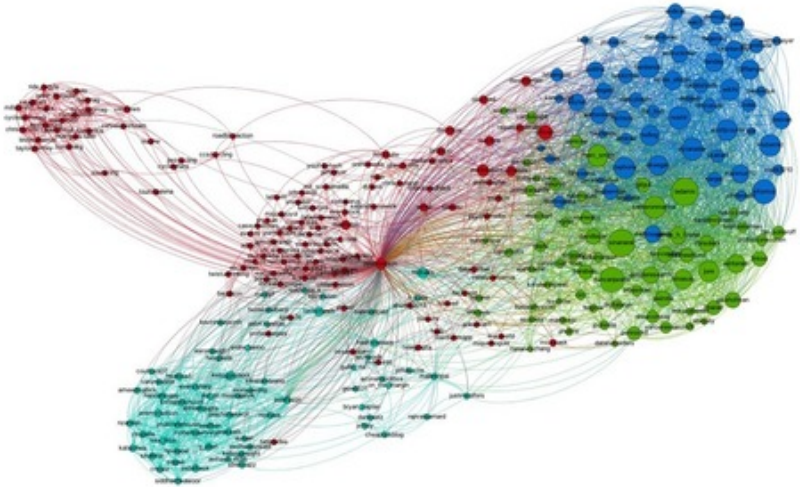
/ периодичности нет

Оборудование исправно, проверено

вендором

Предположение клиента: Целевая атака?

- В анализе записи сетевого трафика мы обнаружили большое количество DNS запросов к серверу управления старой вредоносной программы (Trojan-DDOS)
- Сам сервер был заблокирован ещё в 2012 году, однако вредоносная программа продолжает попытки к нему подключиться



- Оказалось, что в технологическая сеть построена на PLC (вместо промышленных маршрутизаторов)
- Большое количество DNS запросов вызывало отказ в обслуживании (DoS) контроллеров

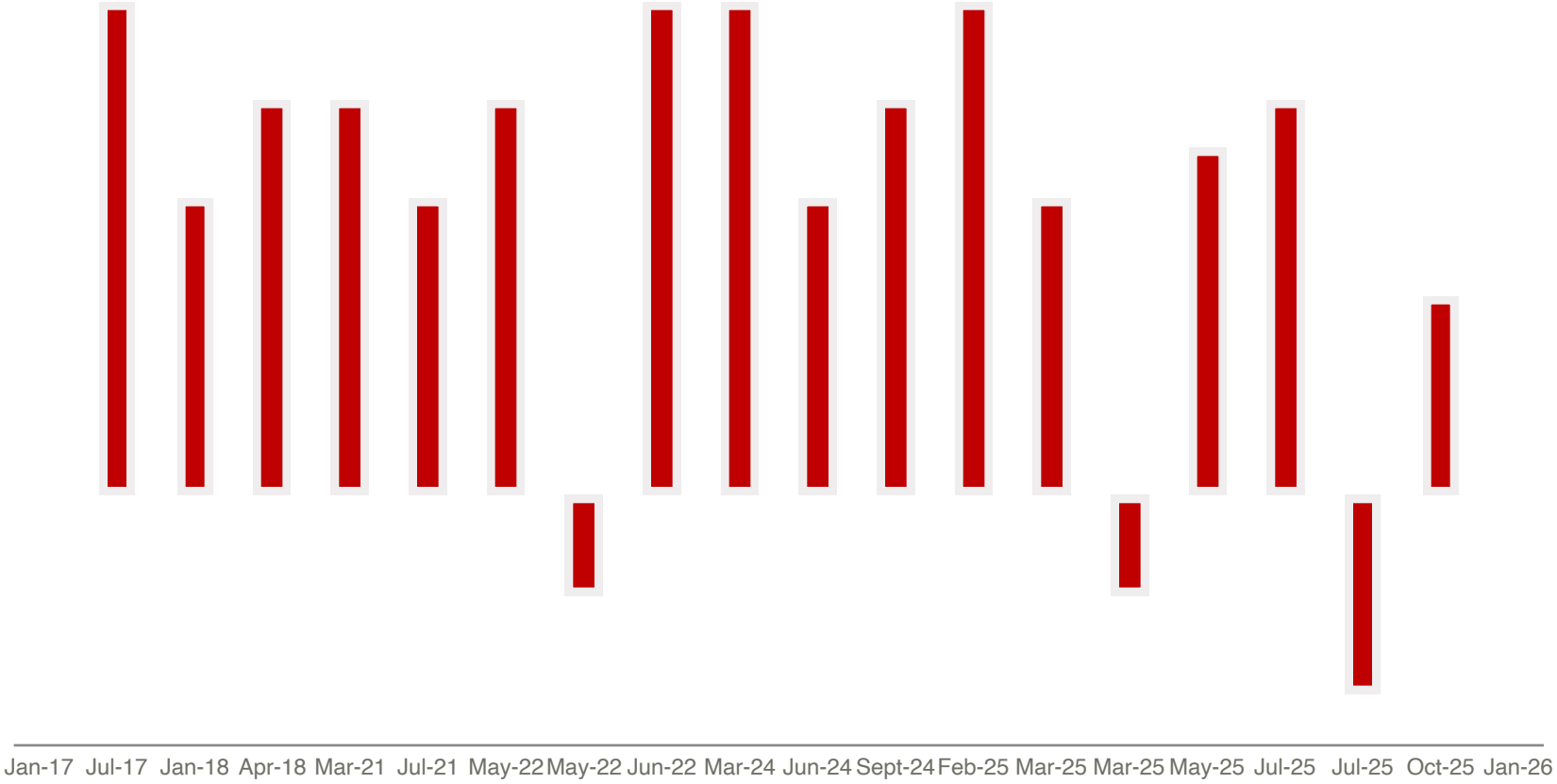
- множество различных отраслей
- TOP IT- и IT-Sec-вендоры
- предприятия ВПК и гос. контракторы, с доступом к национальным и внутриблоковым (NATO) ресурсам

https://news.brp.com/news-releases/news-release-details/brp-reports-cyberattack
https://www.desfa.gr/en/press-center/press-releases/anakoinwsh
https://www.south-staffs-water.co.uk/news/important-statement
https://blog.talosintelligence.com/2022/08/recent-cyber-attack.html
https://investors.hensoldt.net/websites/hensoldt/English/3080/news-detail.html?newsID=2325049
https://www.mbda-systems.com/2022/08/01/hacking-allegations-against-mbda-italy/

Тысячи промышленных организаций скомпрометированы в 2021-2022:

- десятки промышленных организаций подтвердили факто компрометации
- сотни - на сайтах группировок вымогателей
- тысячи скомпрометированы, но пока ’не тронуты’

Хорошо известные истории



Цепочка поставки: основные вектора

- Скомпрометированный провайдер IT-услуг
- Скомпрометированный телеком
- Скомпрометированный регистратор доменов
- Скомпрометированный certification authority
- Сайт вендора ПО / инфраструктура обновления
- Внедрение вредоносного кода на этапе сборки продукта

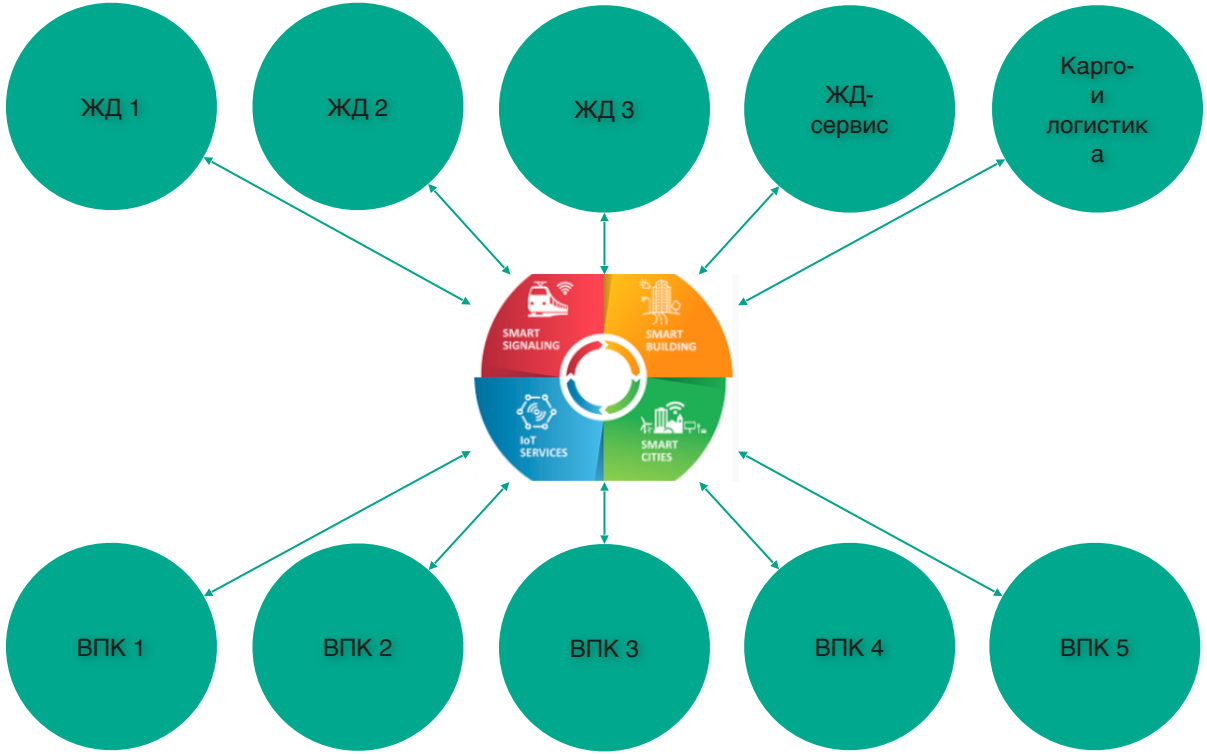
Пример атаки: RedEcho

https://www.recordedfuture.com/redecho-targeting-indian-power-sector/

Пример атаки: RedEcho

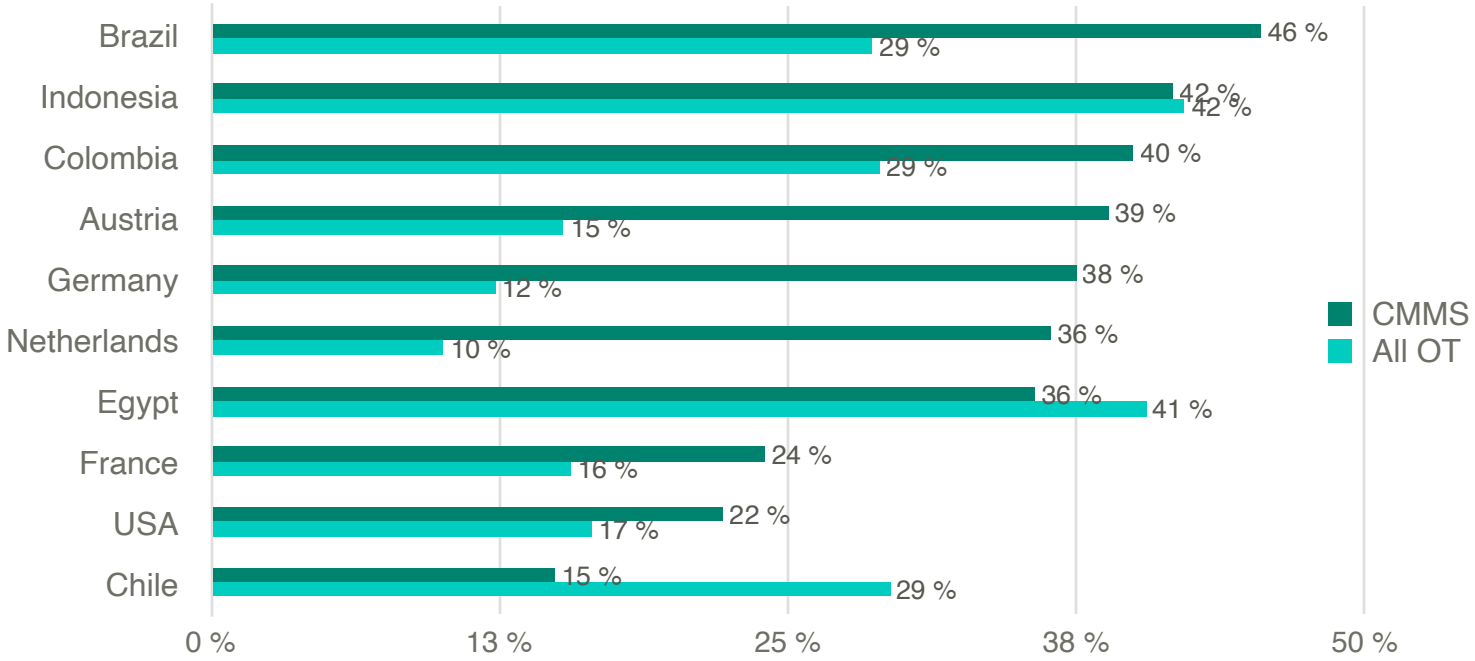
- ShadowPad в атаках на промышленные предприятия в Индии, Канаде, Афганистане и Украине
- Предположение о последствиях для энергетики в Индии (отключение потребителей)

Supply chain attack example: smart things connecting victims

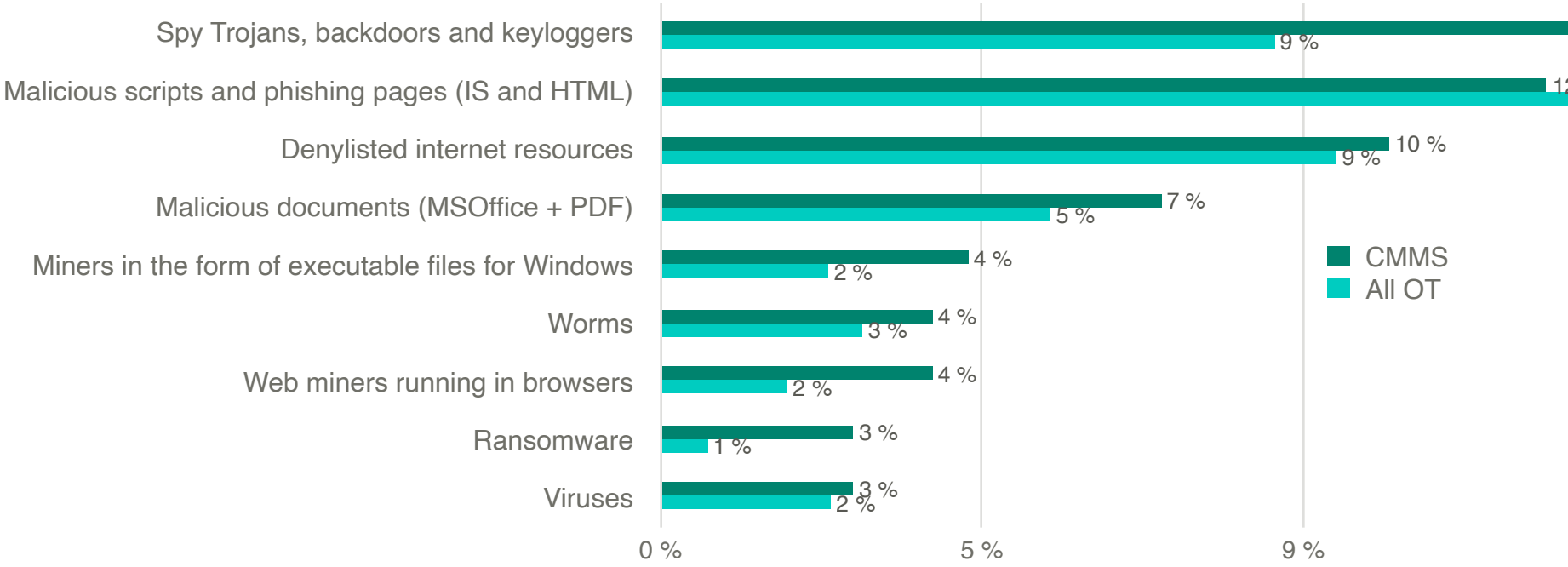


https://securelist.com/apt-trends-report-q3-2021/104708/

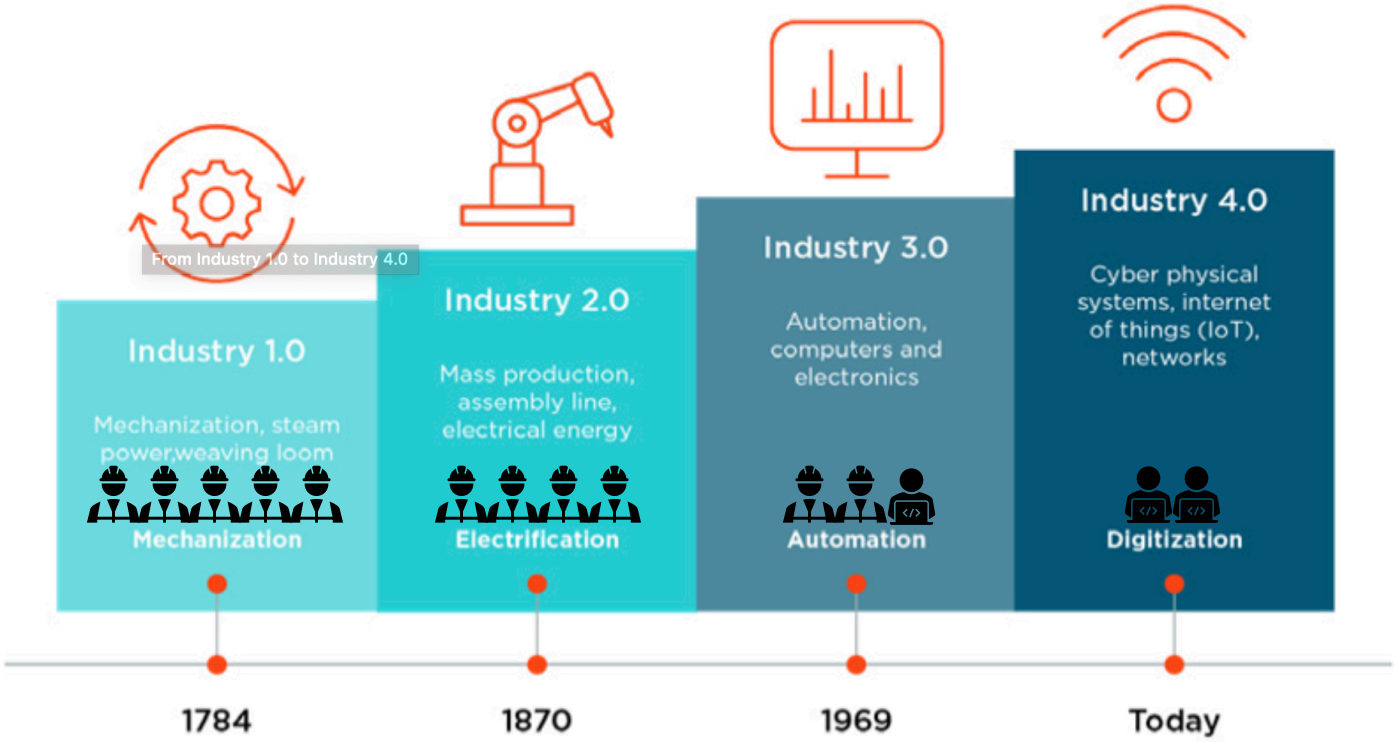
% атакованных CMMS (Computerized Maintenance Management System), 1H 2022



% атакованных CMMS, 1H 2022

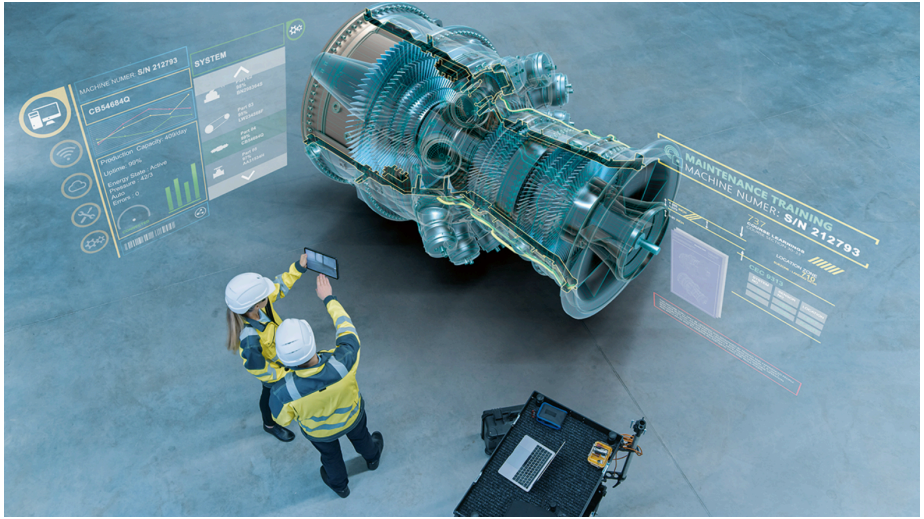


What does make things different?



https://www.wsimulation.eu/smart-manufacturing-technologies-benefits/

- Формула Stuxnet 2.0?
  - Нет нужды в инсайдере
  - Не нужно захватывать корабли и воссоздавать копии целевых объектов
  - Используй цифровые двойники



Спасибо!
Вопросы?

Contacts:
ics-cert@kaspersky .com
evgeny.goncharov@kaspersky.com

Details:
https://ics-cert.kaspersky.ru

kaspersky