10 YEARS JETSECURITY CONFERENCE 2019

Компьютерные угрозы. Будущее в опасности: кто виноват и что делать?

Сергей Новиков

Заместитель руководителя глобального центра исследований и анализа угроз
Sergey.Novikov@Kaspersky.com

kaspersky

ЗАЧЕМ НУЖЕН ОБЗОР?

kaspersky

Анализ предыдущей активности позволяет понять следующие шаги

Понимание эволюции сложных атак: методов и инструментов

Дает возможность взглянуть на ландшафт угроз в целом по миру

ПРИРОДА УГРОЗ

kaspersky

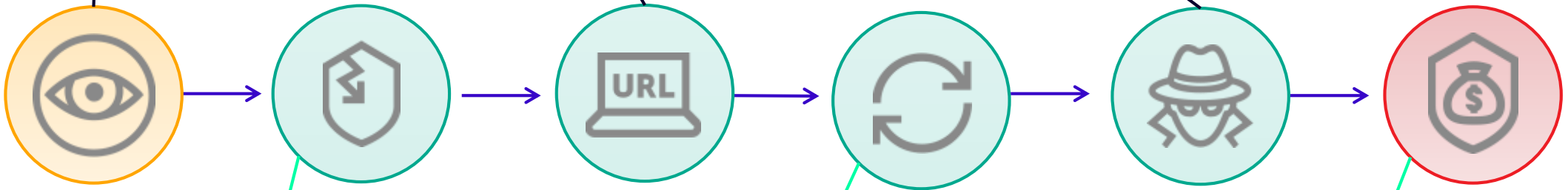
Кибероружие

Целевые атаки на организации

Традиционная киберпреступность

ЧТО СКРЫВАЕТСЯ ЗА ЦЕЛЕВОЙ АТАКОЙ?

kaspersky



- сбор данных
- подготовка стратегии

Подготовка к атаке

- новые «серые» домены
- доставка команд

Доставка

- «чистые» объекты
- зашифрованные

C&C

- имитация обычной активности
- кража аккаунтов
- ничего не нарушая

Побочные действия

- быстро
- тихо
- без ущерба

Исполнение

Нанесение ущерба и исчезновение

- замести все следы
- удалить все логи
- незаметно оставить бекдор

10 YEARS JETSECURITY CONFERENCE 2019

ЦЕЛЕВЫЕ АТАКИ

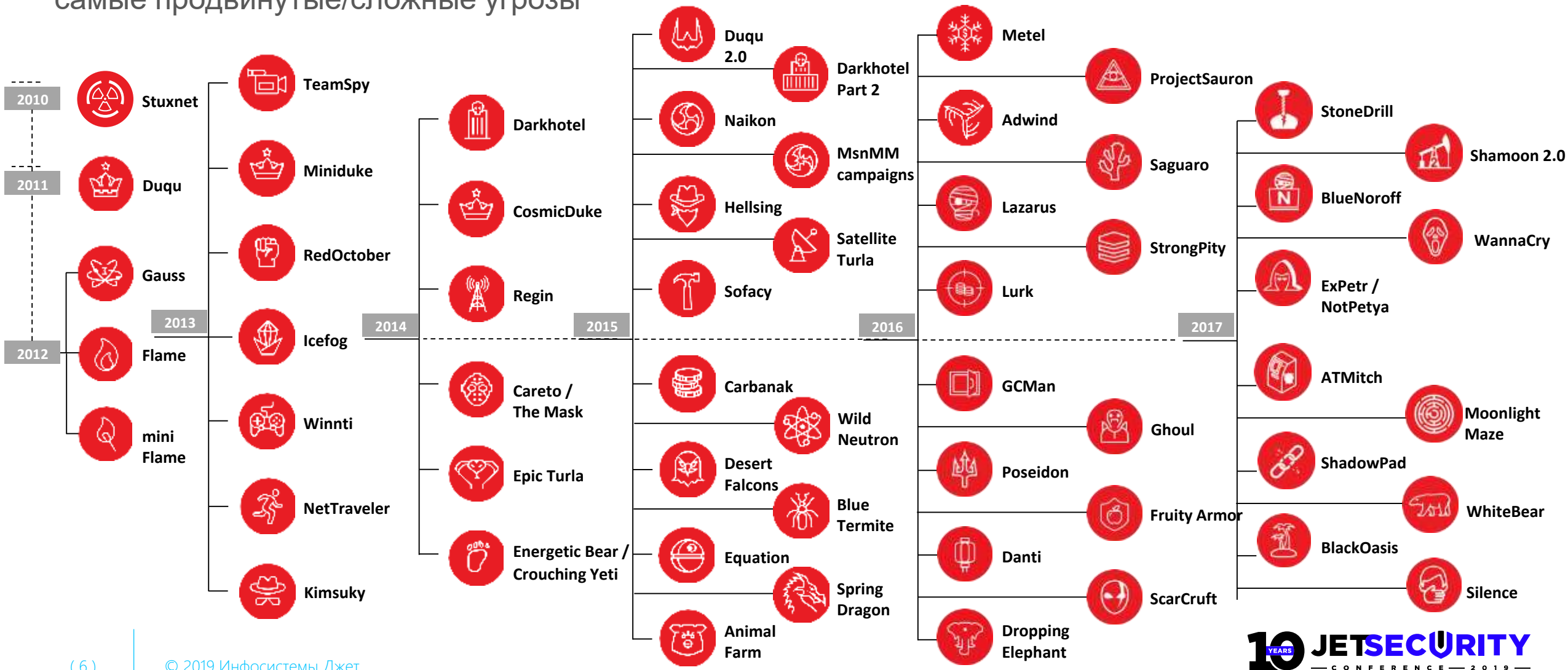
kaspersky

- Более 130 действующих APT-групп
  - ✓ Из них около 20 «коммерческих»
  - ✓ Около 25 атакуют цели в России
  - ✓ 20+ групп говорят на китайском языке
- Атаки на цепочки поставщиков (Supply chain)
- Большое количество новых игроков
- Использование открытых утилит

АНОНСИРОВАННЫЕ APT-КАМПАНИИ

kaspersky

Мы обнаруживаем и анализируем
самые продвинутые/сложные угрозы



10 YEARS JETSECURITY CONFERENCE 2019

КРИТИЧЕСКИЕ АППАРАТНЫЕ УЯЗВИМОСТИ

kaspersky

- Meltdown/Spectre/уязвимости в процессорах AMD
- Эти уязвимости открывают возможность создания новых методов эксплуатации
- Атаки на виртуальные среды, гипервизоры и единый расширяемый интерфейс прошивки (UEFI)

ФИНАНСОВЫЕ УГРОЗЫ

kaspersky

- Использование технологий APT-атак
- Атаки на SWIFT
- Взломы банкоматов, заражения PoS-терминалов
- Атаки на системы приема онлайн-платежей
- Диджитализация атак

ГОРЯЧАЯ ТЕМА - АТАКИ НА РОУТЕРЫ

kaspersky

- В течении последних лет мы обнаружили несколько групп, использующих атаки на роутеры
  - ✓ SynfulKnock and Regin
  - ✓ CloudAtlas APT
- Govcert advisory о нетипичных перезагрузках в девайсах известного производителя
- Уязвимости/zero day в Mikrotik (CVE-2018-7445) и Cisco smart install protocol misuse (CVE-2018-0171)
- LuckyMouse APT использует взломанные роутеры в качестве C&C

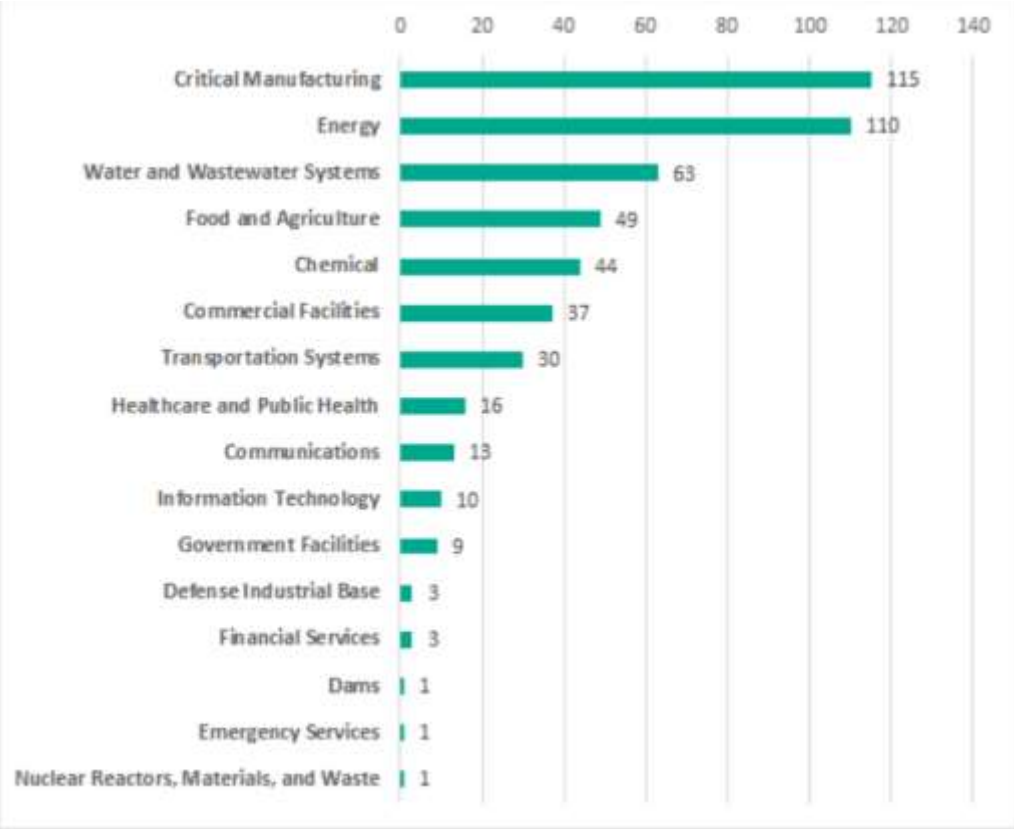
БАЛКАНИЗАЦИЯ, СОЦИАЛЬНЫЙ ХАОС И ПРОПАГАНДА

kaspersky

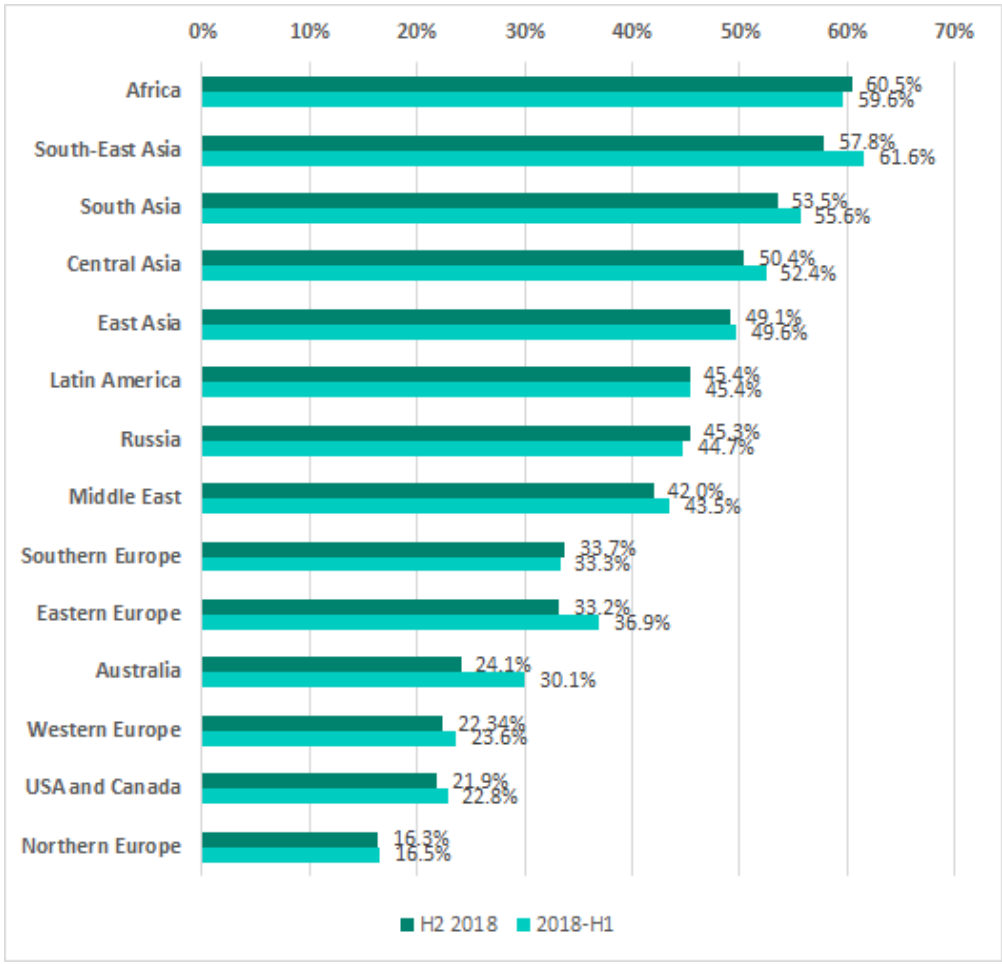
- Блокировки и закрытие различных сервисов в Интернете
- Громкие утечки пользовательских данных: Facebook, Equifax, Uber и т.д…
- Атаки на выборы
- Пропаганда и массовая дезинформация

ИНДУСТРИАЛЬНЫЕ СИСТЕМЫ (АСУ ТП)

kaspersky



Количество уязвимых решений, используемых в разных индустриях на объектах АСУ ТП в 2018 году



Распространение уязвимостей на объектах АСУ ТП в 2018 году

https://ics-cert.kaspersky.com/reports/2019/03/27/threat-landscape-for-industrial-automation-systems-h2-2018/

ПРОГНОЗЫ НА 2019-2020

kaspersky

- Больше атак на производителей софта
- Атрибуция станет почти невозможной
- Автоматизация атак на банкоматы
- Продвинутые атаки на UEFI
- Майнеры, мобильные угрозы
- Атаки на IoT, в т.ч. Промышленный IoT
- Увеличение риска целевых атак с применением программ-вымогателей
- Интернет пропаганда, манипулирование и взломы СМИ и социальных медиа

ЧТО ДЕЛАТЬ?

kaspersky

1. Обучение персонала
2. Внедрение процессов
3. Использование защитных технологий

ВЫВОД

Пришло время выбрать
цифрового телохранителя!

10 YEARS JETSECURITY
CONFERENCE 2019

СПАСИБО ЗА ВНИМАНИЕ!

Сергей Новиков

Заместитель руководителя глобального центра исследований и анализа угроз
Sergey.Novikov@Kaspersky.com

kaspersky