Тяжелый бой за светлое будущее.

Проблемы устранения уязвимостей в системах промышленной автоматизации

Владимир Дащенко

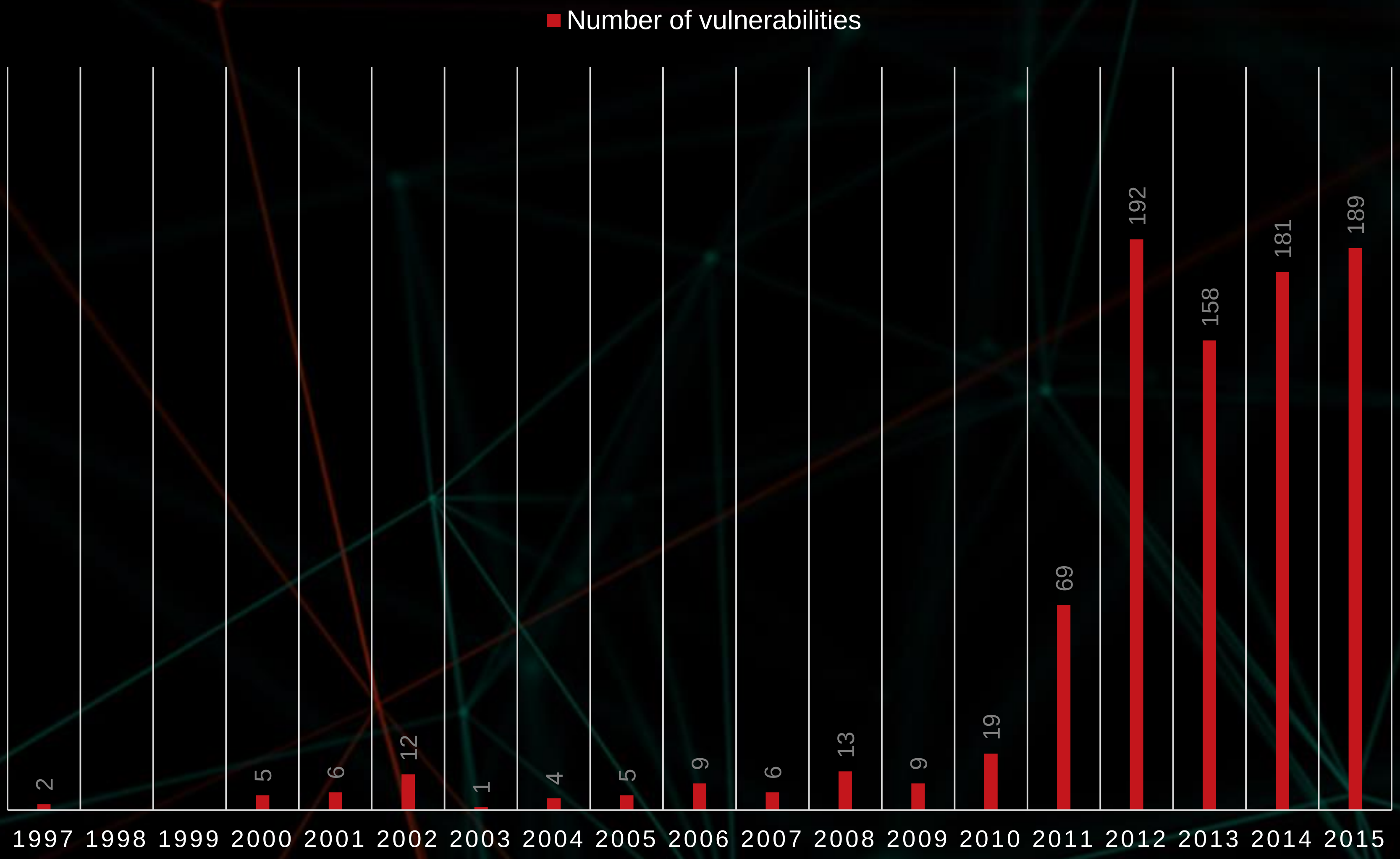
Старший исследователь безопасности

Группа защиты критических инфраструктур и Kaspersky Lab ICS CERT

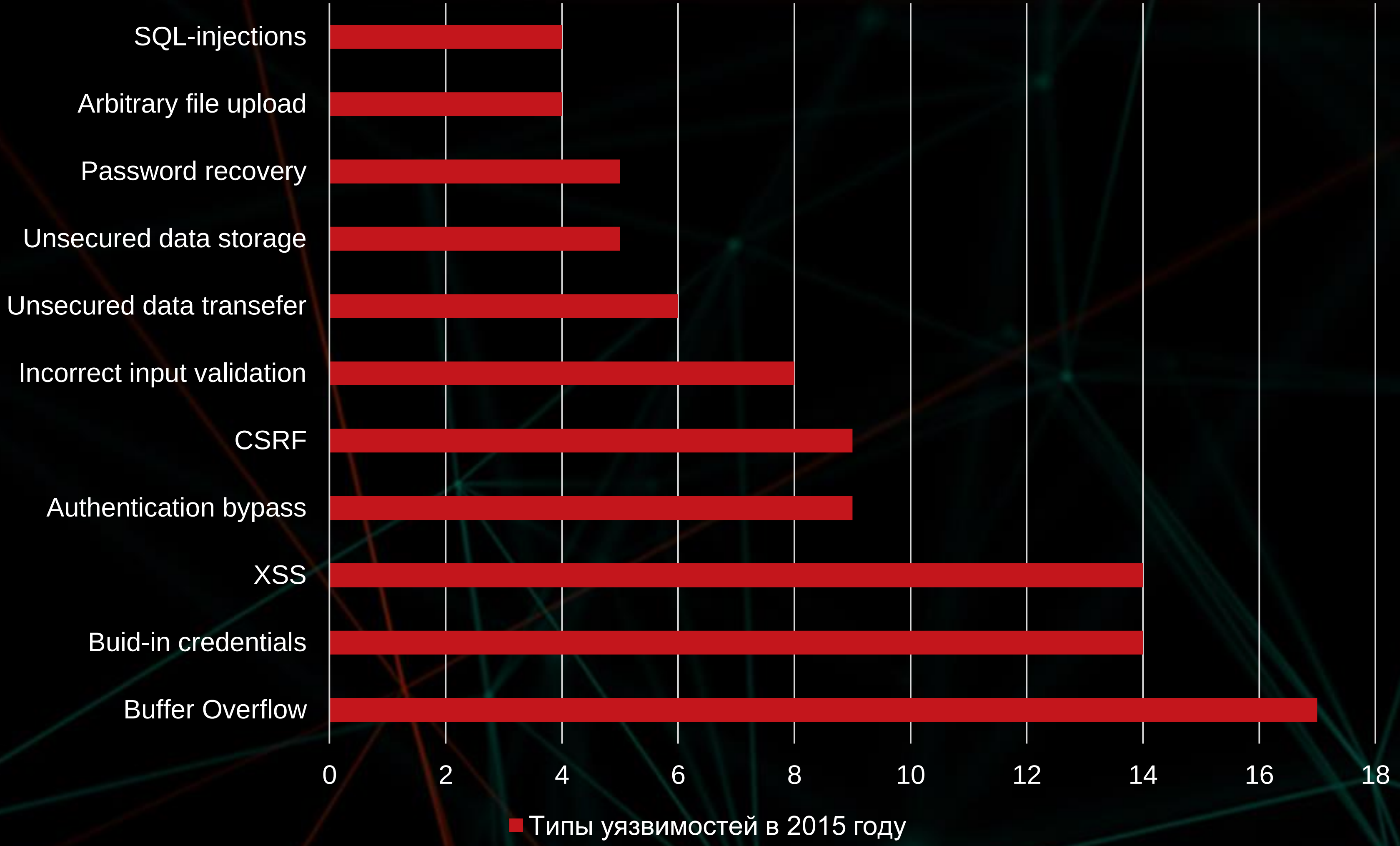
«Лаборатория Касперского»

Past

IDENTIFIED VULNERABILITIES

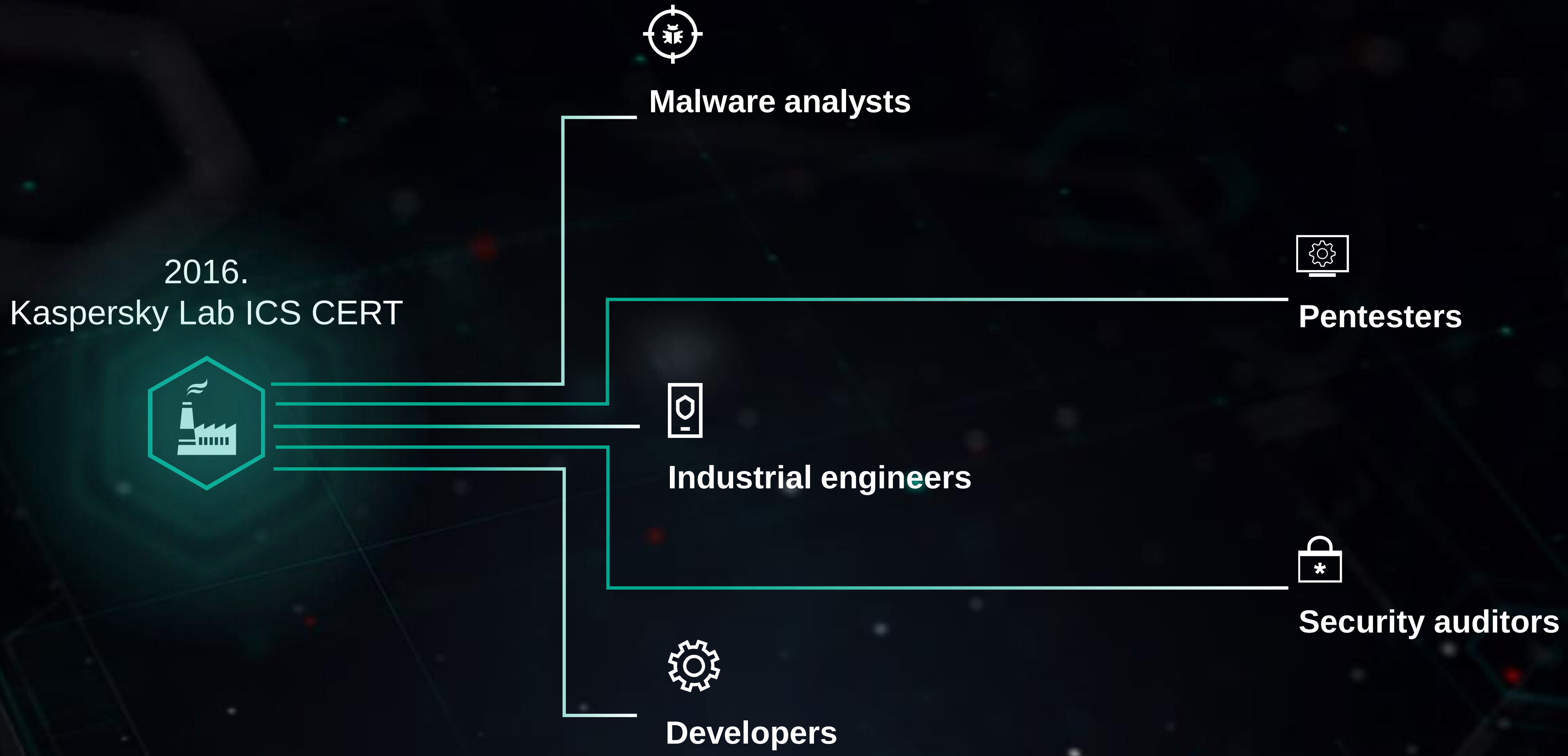


Vulnerability classes



Present

KL ICS CERT structure



2016.
Kaspersky Lab ICS CERT

Malware analysts

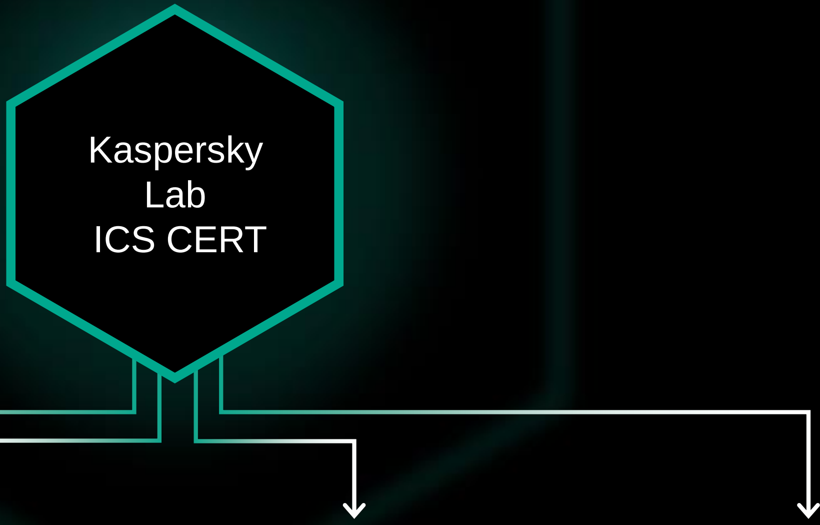
Pentesters

Industrial engineers

Security auditors

Developers

Activities



Kaspersky Lab ICS CERT

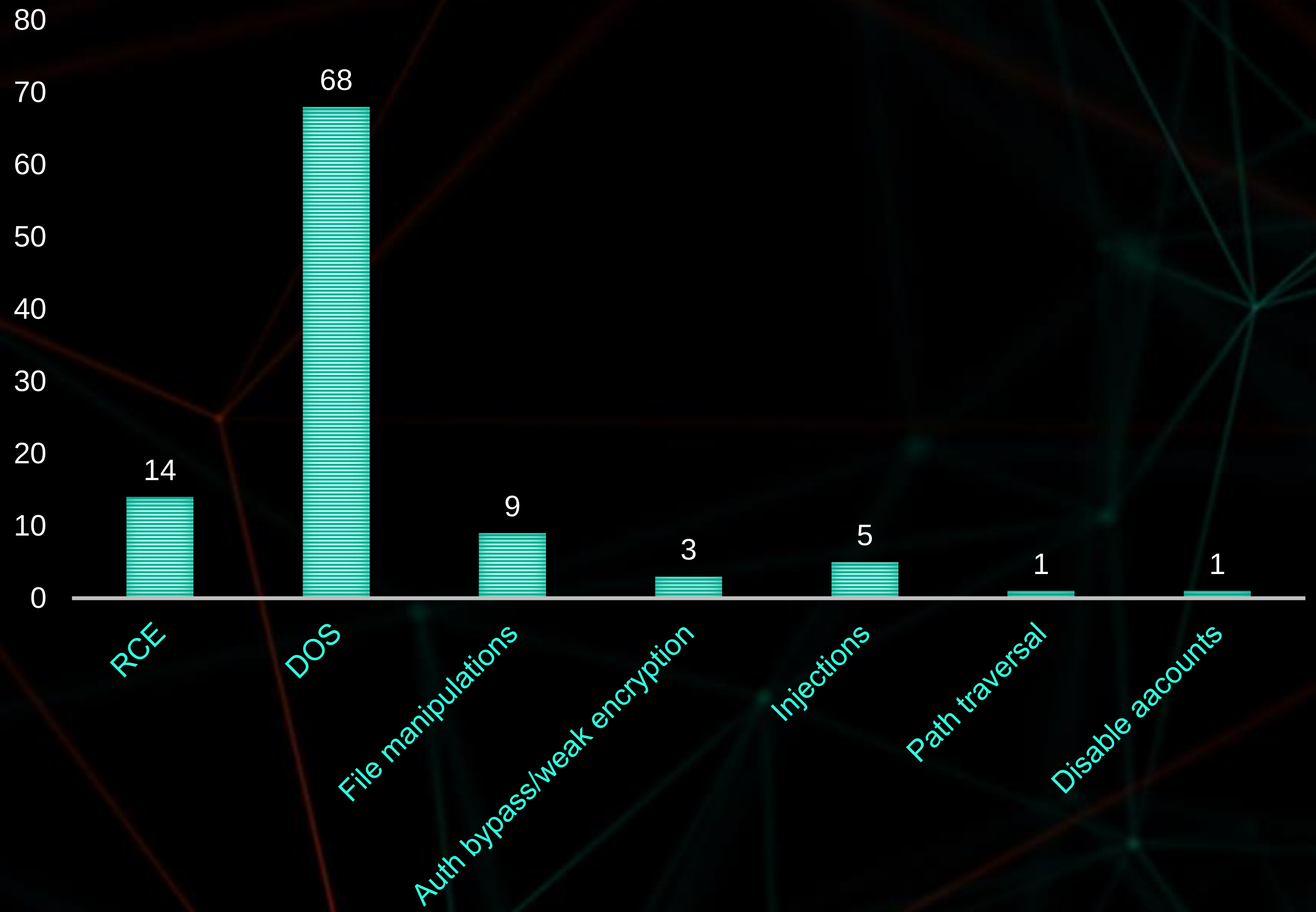
Поиск и анализ уязвимостей

Расследования и анализ сложных атак

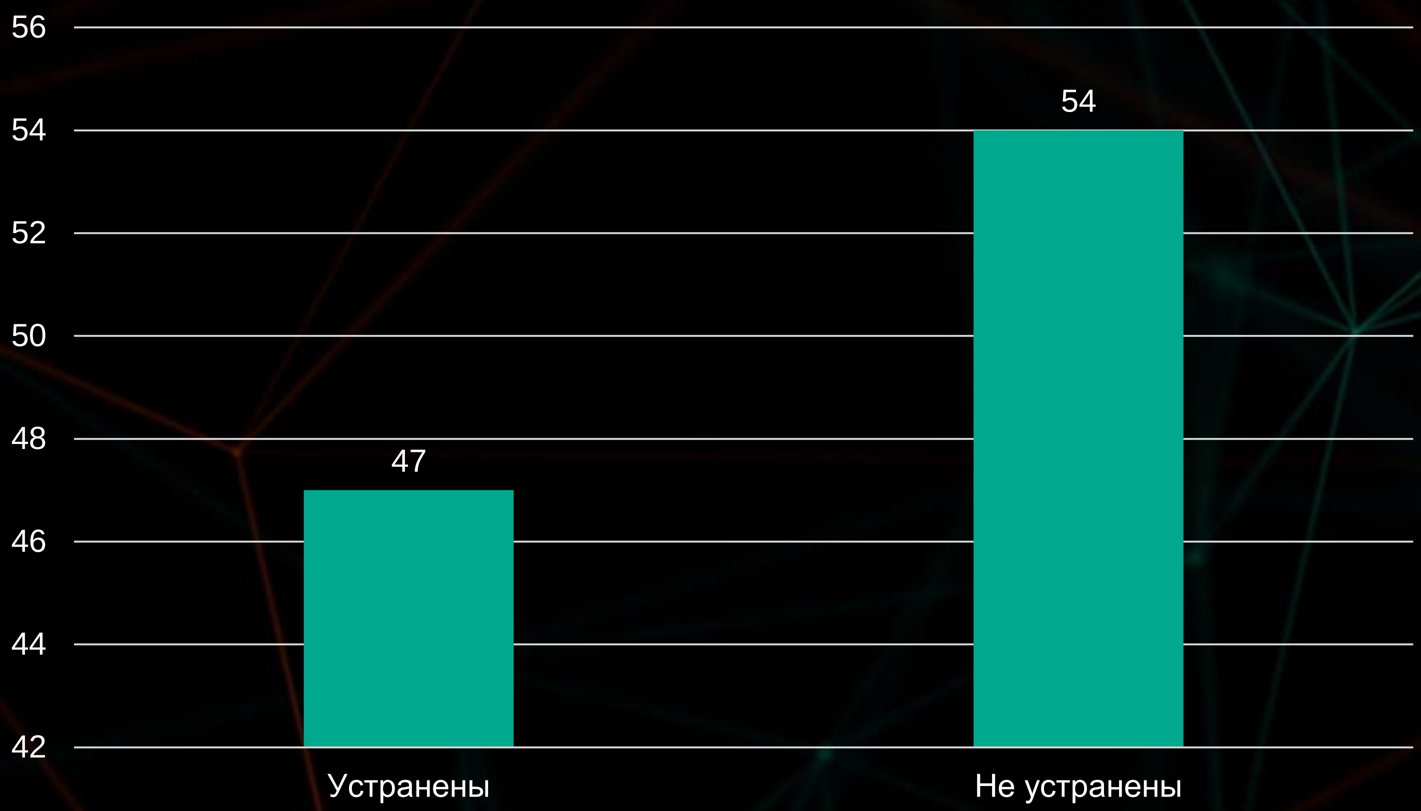
Анализ специализированного вредоносного ПО

Проведение тестирований на проникновение

Vulnerability Research Statistics

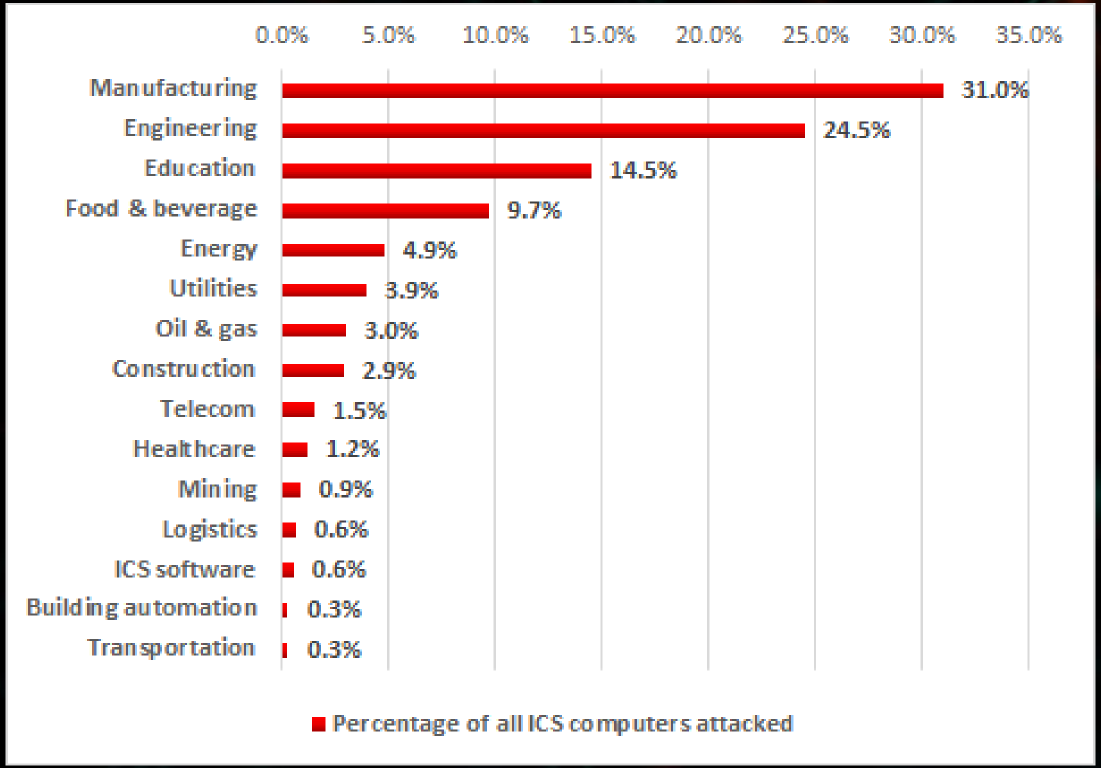


Patched?

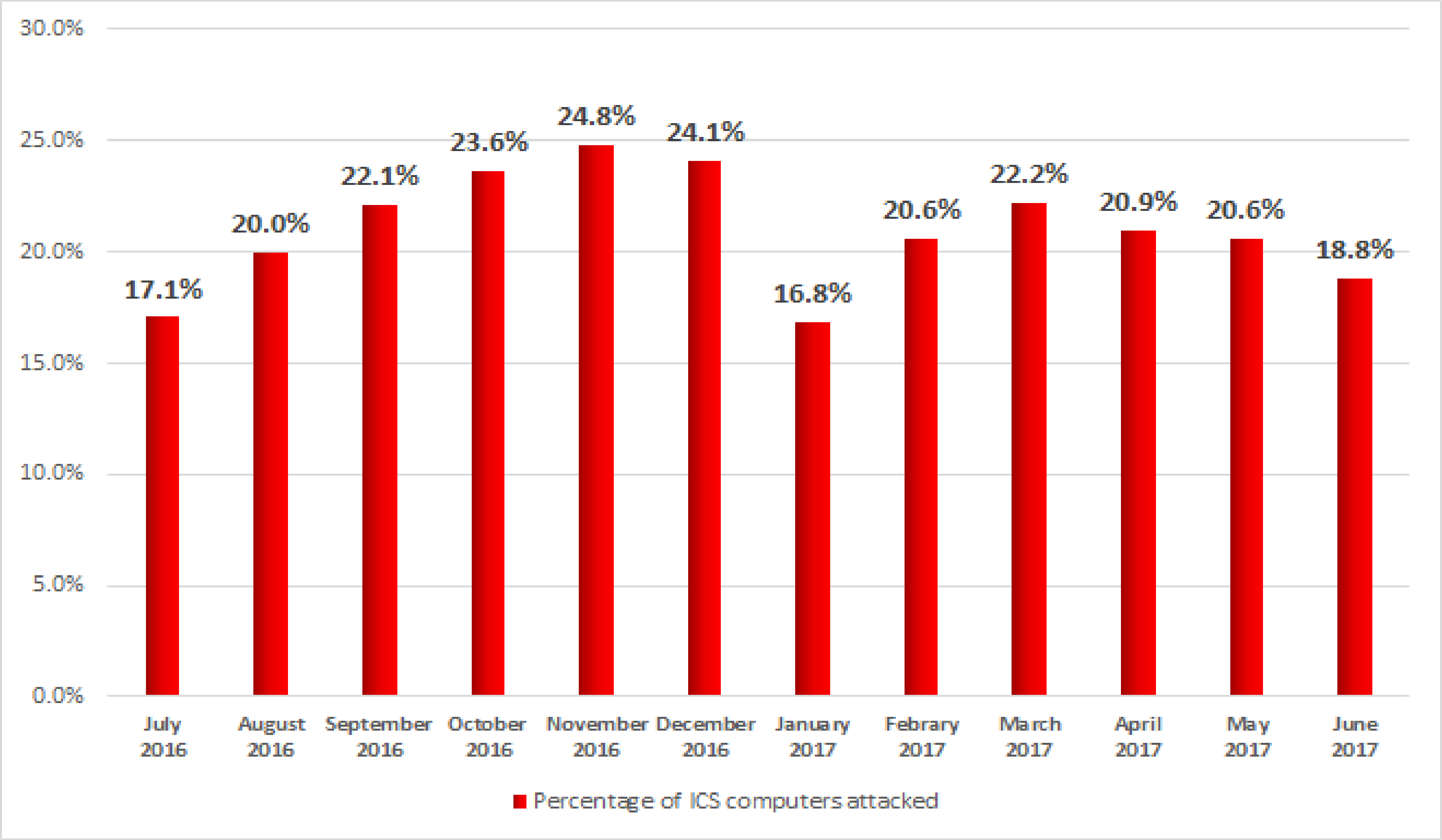


Industry statistics

- **Every 3rd ICS computer under attack was in manufacturing companies**
  ICS computers in manufacturing companies that produce various materials, equipment and goods accounted for about one third of all attacks

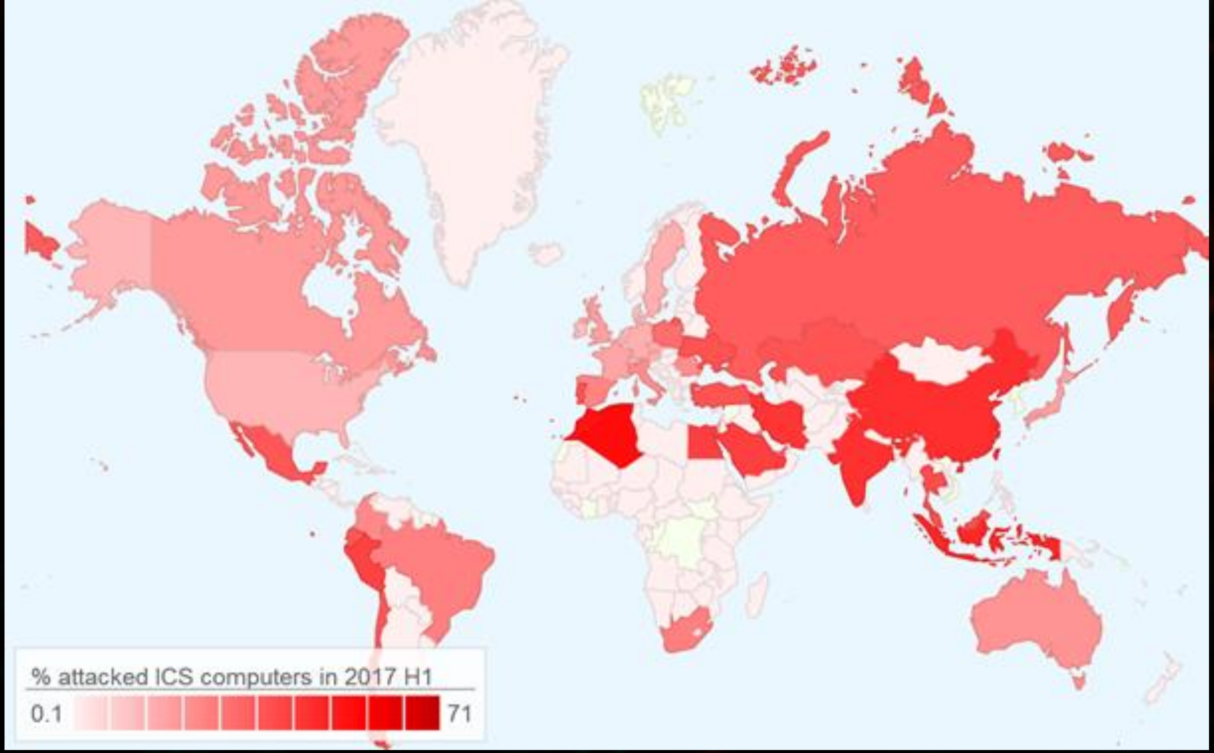


Monthly Statistics



Geographical Distribution of Attacks on Industrial Automation Systems

- **TOP 5 countries**
  Vietnam (71.0%)
  Algeria (67.1%)
  Morocco (65.4%)
  Indonesia (58.7%)
  China (57.1)



Ransomware nightmare

- **0.5% of computers** in the industrial infrastructure of organizations were attacked by encryption ransomware at least once.
- ICS computers in **63 countries** across the globe were under numerous encryption ransomware attacks
- **33 different families** of encryption ransomware were blocked on ICS computers

WANNACRY

13.4% of all computers in industrial infrastructure attacked

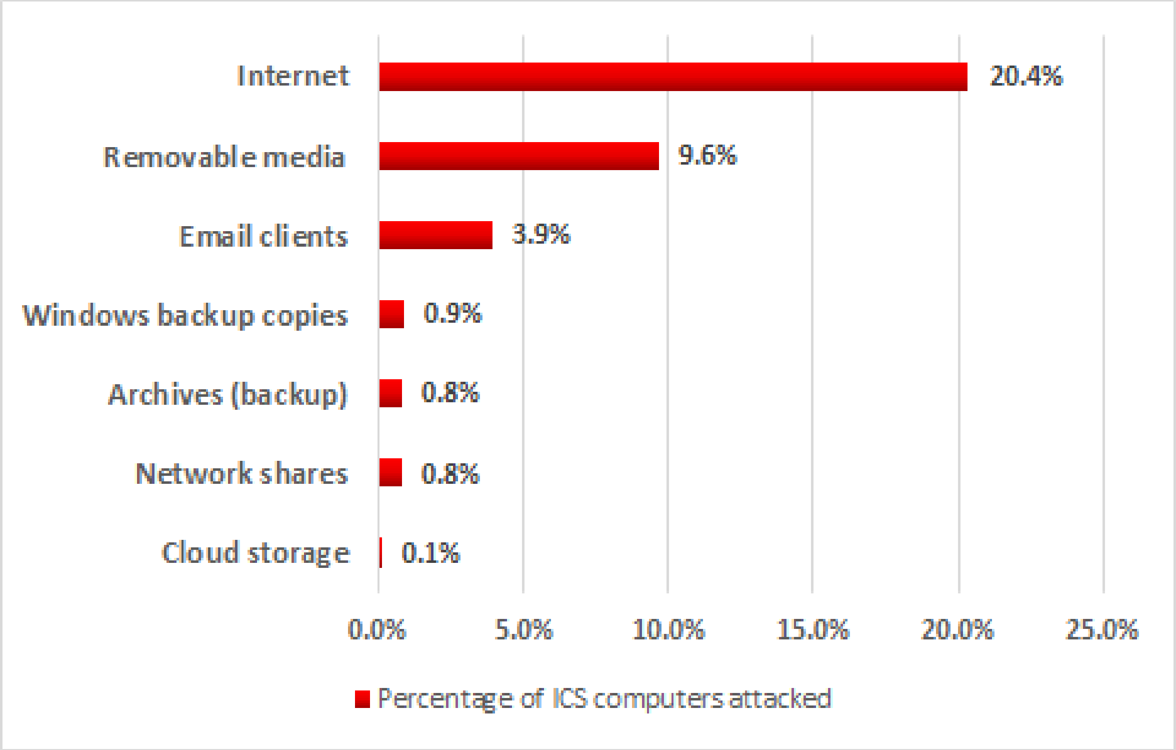
The most affected organizations included healthcare institutions and government sector

EXPETR

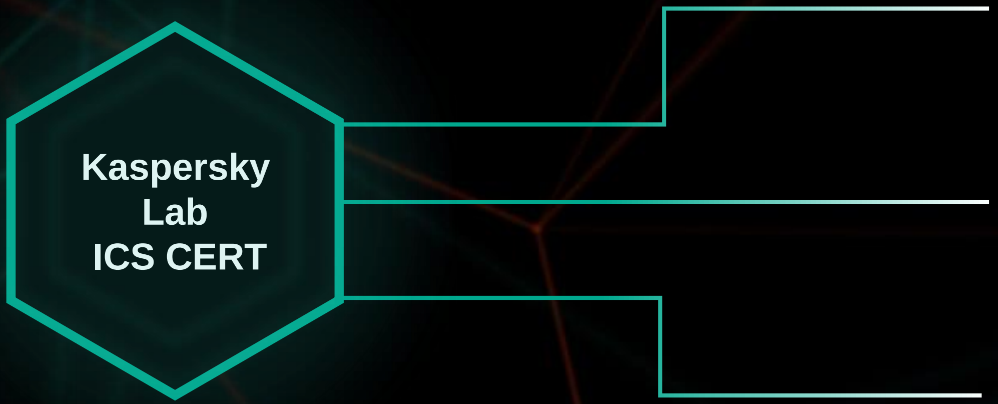
at least 50% of the companies from manufacturing, and Oil&Gas industries attacked

Source of infection

- **Internet – the main source of threats**
- Field statistics: 3rd party contractors can cause a damage
- 18,000 different modifications of malware belonging to more than 2,500 different families



Future



Kaspersky Lab ICS CERT

Vulnerability research in common solutions and platforms

IoT, IIoT, Connected Devices, Medical Devices

Backdoor research

Let’s talk!

Vladimir Dashchenko
Vladimir.Dashchenko@Kaspersky.com

ics-cert.kaspersky.ru
www.kaspersky.com

KASPERSKY lab