Industrial Cybersecurity Challenge

or

a Window of Opportunity?

Evgeny Goncharov

Head of Kaspersky ICS CERT

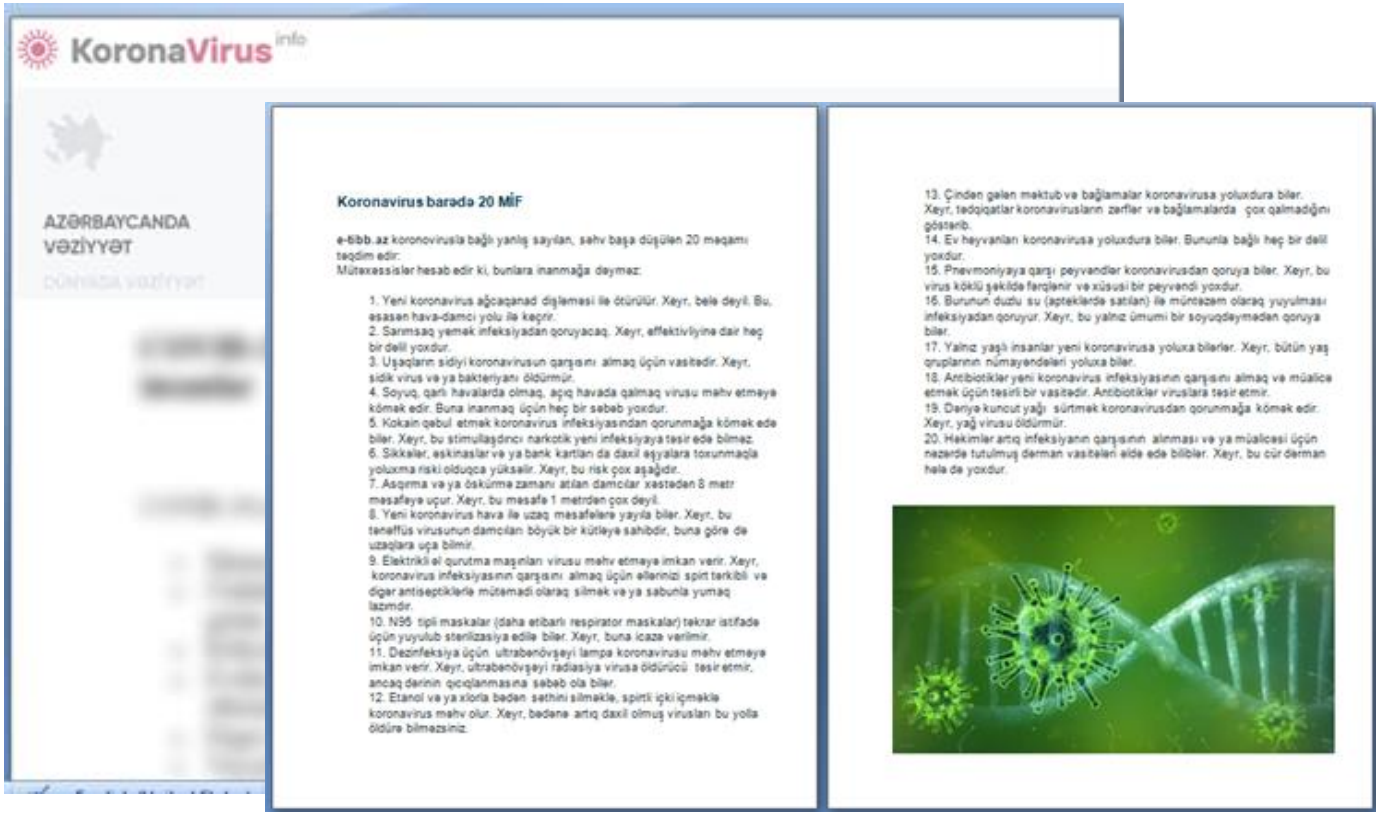
kaspersky

July 2020

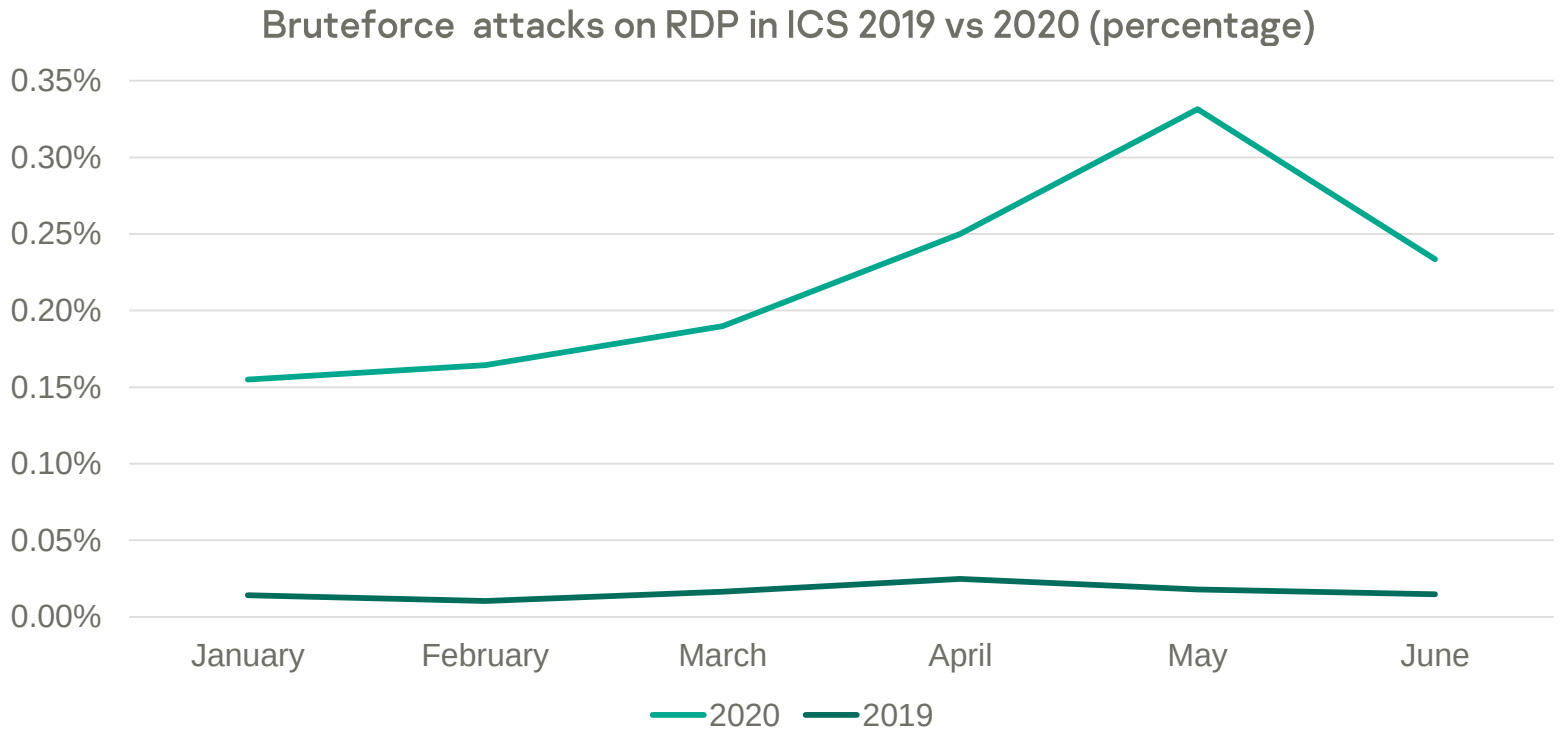
ICS Threat Landscape Changes

- Covid-19 in targeted and mass-spread attacks
- Global ICS attack surface changes

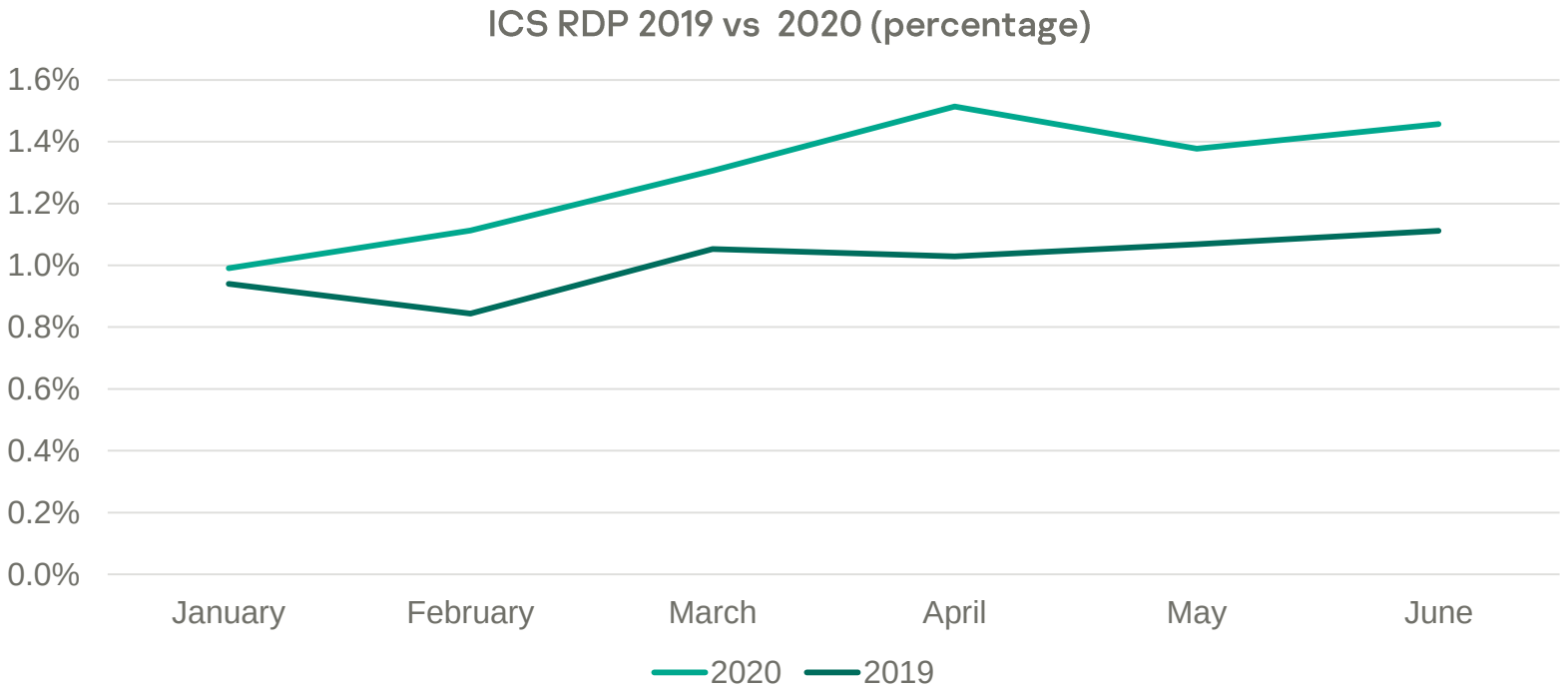
Covid-19 in targeted and mass-spread attacks



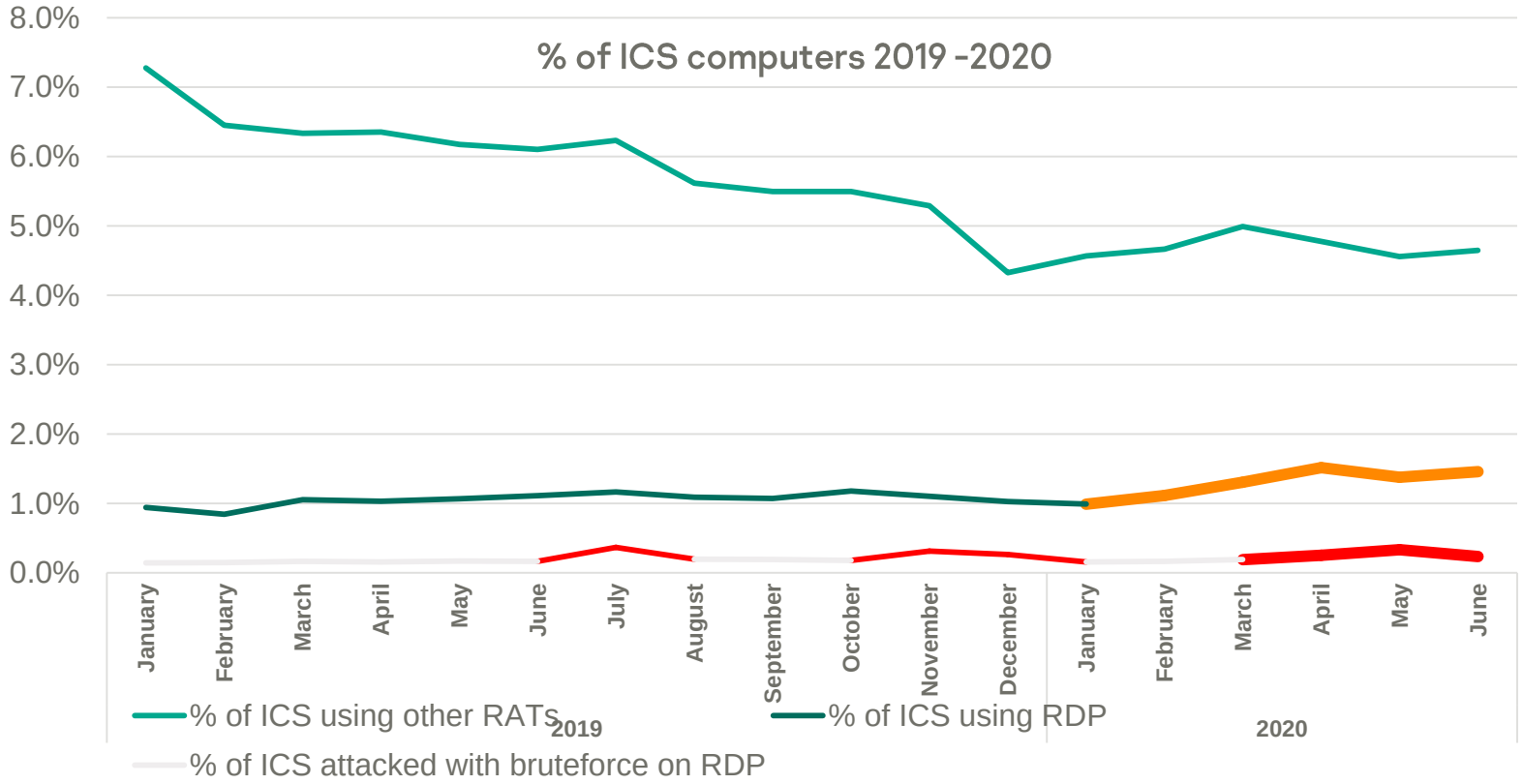
Global ICS threat landscape changes



Global ICS attack surface changes



Global ICS attack surface changes



Window of Opportunity

Security challenges to try and solve

Reverse engineering is "permitted":

USA (DMCA)→

(only) to achieve program-to program interoperability

Exemptions: consumer devices (including cars and medical devices)

EU (2016/94)→

...for lawfully acquired products

But except for when otherwise contractually agreed

And limited by copyright law (2009/24/EC) for interoperability purposes

Germany (TSA) →

since after the product is freely available on the market

But still... can be contractually restricted

As a result… the vendors…
still have their legitimate conventional

…and to make them think of a dark side

Coordinated Vulnerability Disclosure is

IT / Telecom →
…A day-to day practice,
most vendors have a CVD policy a bounty program

ICS / OT→
…Becoming a day-to day practice
But except for some multiple other cases

Transportation / Automotive →
…A hot topic
But still… vendors tend to not disclose anything

Coordinated Vulnerability Disclosure @

State level →

Some few countries have a CVD guideline:

https://english.ncsc.nl/publications/publications/2019/juni/01/coordinated-vulnerability-disclosure-the-guideline

But still… no laws or any other legislation

And majority do not regulate it at all

Regional / International levels →

ENISA published a good practice guide:

https://www.enisa.europa.eu/publications/vulnerability-disclosure

FIRST has its guidelines:

https://www.first.org/global/sigs/vulnerability-coordination/multiparty/guidelines-v1.0

But still… no any regulation, just good practice recommendations

As a result… the vendors…
still have their legitimate conventional

…and to make them think of a dark side

Thank you
and
let’s talk.

kaspersky