

Industrial Cybersecurity Challenge or a Window of Opportunity?

Evgeny Goncharov

Head of Kaspersky ICS CERT

ICS Threat Landscape Changes

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

KoronaVirus info

**AZƏRBAYCANDA
VƏZİYYƏT**

DÜNYADA VƏZİYYƏT

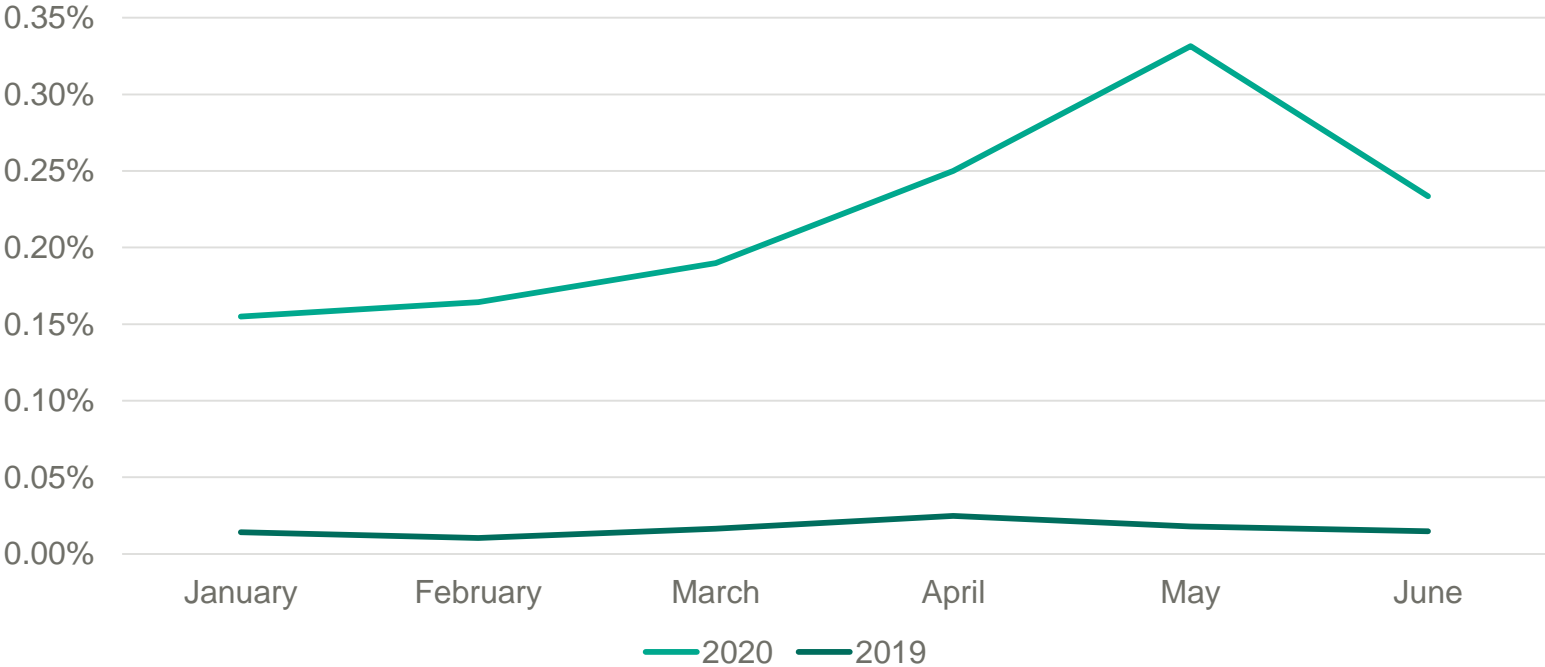
Koronavirus barədə 20 MİF

e-fbb.az koronavirusla bağlı yanlış sayılan, səhv başa düşülən 20 məqamı təqdim edir:
Mütəxəssislər hesab edir ki, bunlara inanmağa dəyməz:

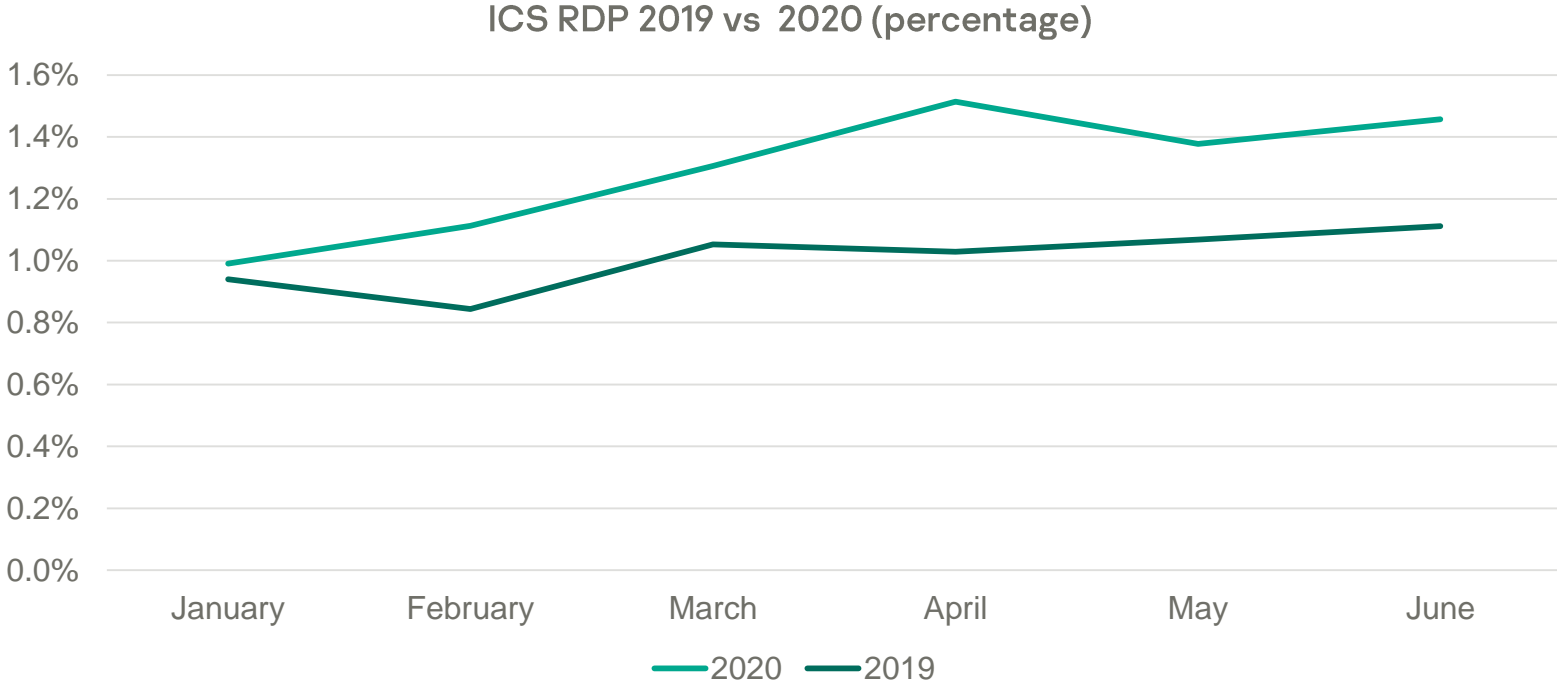
1. Yeni koronavirus açığa qədər digərləsi ilə ötürülür. Xeyr, belə deyil. Bu, əsasən hava-damcı yolu ilə keçir.
2. Sarmsaq yemək infeksiyadan qoruyacaq. Xeyr, effektivliyinə dair heç bir dəlili yoxdur.
3. Uşaqların sidiyi koronavirusun qarşısını almaq üçün vəstədir. Xeyr, sidiq virus və ya bakteriyaları öldürmür.
4. Soyuq, qarlı havalarda olmaq, açıq havada qalmaq virusu məhv etməyə kömək edir. Buna inanmaq üçün heç bir səbəb yoxdur.
5. Kokain qəbul etmək koronavirus infeksiyasından qorunmağa kömək edə bilər. Xeyr, bu stimullaşdırıcı narkotik yeni infeksiyaya təsir edə bilməz.
6. Sikkələr, eskinaslar və ya bank kartları da daxil əşyalara toxunmaqla yoluxma riski olduqca yüksəkdir. Xeyr, bu risk çox aşağıdır.
7. Açıqma və ya öskürmə zamanı astan damcıları xəstədən 8 metr məsafəyə uçur. Xeyr, bu məsafə 1 metrdən çox deyil.
8. Yeni koronavirus hava ilə uzaq məsafələrə yayıla bilər. Xeyr, bu tənəffüs virusunun damcıları böyük bir kütləyə sahibdir, buna görə də uzaqlara uça bilmir.
9. Elektrikli el qurutma maşınları virusu məhv etməyə imkan verir. Xeyr, koronavirus infeksiyasının qarşısını almaq üçün əlinizi spirt tərkibli və digər antiseptiklərlə mütəmadi olaraq silmək və ya sabunla yumaq lazımdır.
10. N95 tipli maskalar (daha etibarlı respirator maskalar) təkrar istifadə üçün yuyulub sterilizasiya edilə bilər. Xeyr, buna icazə verilmir.
11. Dezinfeksiya üçün ultrabənövşəyi lampa koronavirusu məhv etməyə imkan verir. Xeyr, ultrabənövşəyi radiasiya virusu öldürücü təsir etmir, ancaq dərinin qıçqanmasına səbəb ola bilər.
12. Etanol və ya xlorid bədən səthinə silməklə, spirtli içki içməklə koronavirus məhv olur. Xeyr, bədənə artıq daxil olmuş virusları bu yolla öldürə bilməzsiniz.
13. Çindən gələn məktub və bağımlar koronavirusa yoluxdura bilər. Xeyr, tədqiqatlar koronavirusların zərflər və bağımlalarda qorunmadığını göstərib.
14. Ev heyvanları koronavirusa yoluxdura bilər. Bununla bağlı heç bir dəlili yoxdur.
15. Pnevmoniyaya qarşı peyvəndlər koronavirusdan qoruyur. Xeyr, bu virus köklü şəkildə fərqlənir və xüsusi bir peyvəndi yoxdur.
16. Burunun duzlu su (apteklərdə satılan) ilə müntəzəm olaraq yuyulması infeksiyadan qoruyur. Xeyr, bu yalnız ümumi bir soyuqdaymadan qoruyur.
17. Yalnız yaşlı insanlar yeni koronavirusa yoluxa bilərlər. Xeyr, bütün yaş qruplarının nümayəndələri yoluxa bilər.
18. Antibiotiklər yeni koronavirus infeksiyasının qarşısını almaq və müalicə etmək üçün təsirli bir vəstədir. Antibiotiklər viruslara təsir etmir.
19. Dəriyə kuncut yağı sürmək koronavirusdan qorunmağa kömək edir. Xeyr, yağ virusu öldürmür.
20. Həkimlər artıq infeksiyanın qarşısını alması və ya müalicəsi üçün nəzərdə tutulmuş dərman vəstələri əldə edə bilərlər. Xeyr, bu cür dərman hələ də yoxdur.

Global ICS threat landscape changes

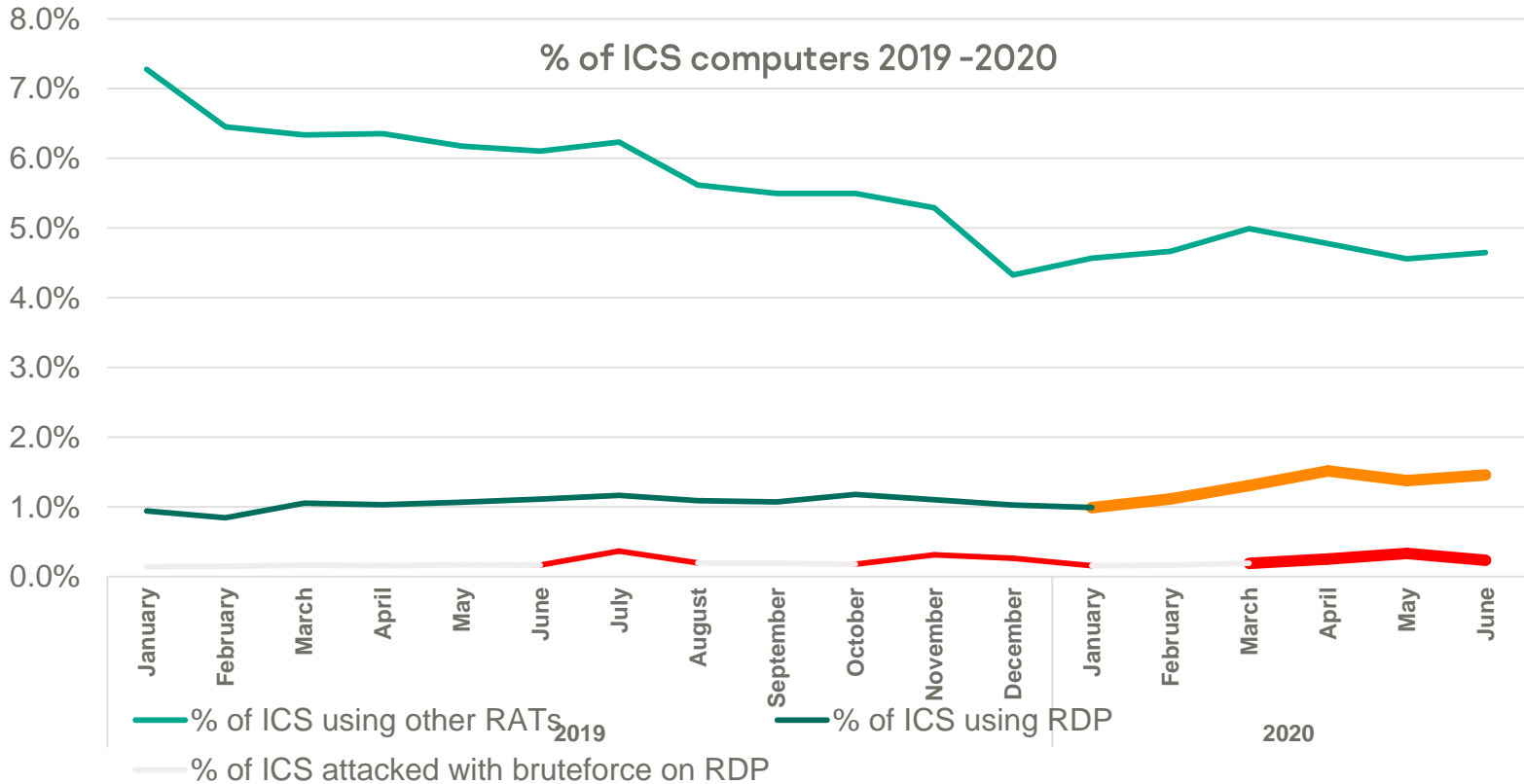
Bruteforce attacks on RDP in ICS 2019 vs 2020 (percentage)



Global ICS attack surface changes



Global ICS attack surface changes



Window of Opportunity

Security challenges to try and solve

The 90'es legacy

8



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**

The 90'es legacy

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

The 90'es legacy

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