CIRT и извлеченные уроки из пандемии COVID-19

Тренды промышленной безопасности 2020

Evgeny Goncharov

Head of Kaspersky ICS CERT

September 2020

kaspersky

Covid-19 в целевых атаках

- Covid-19 в APT на организации в Азербайджане
- Covid-19 в APT на промышленную организацию в России

Covid-19 в APT на организации в Азербайджане

Azərbaycan Respublikası Nazirlər Kabineti yanında operativ qərargahın

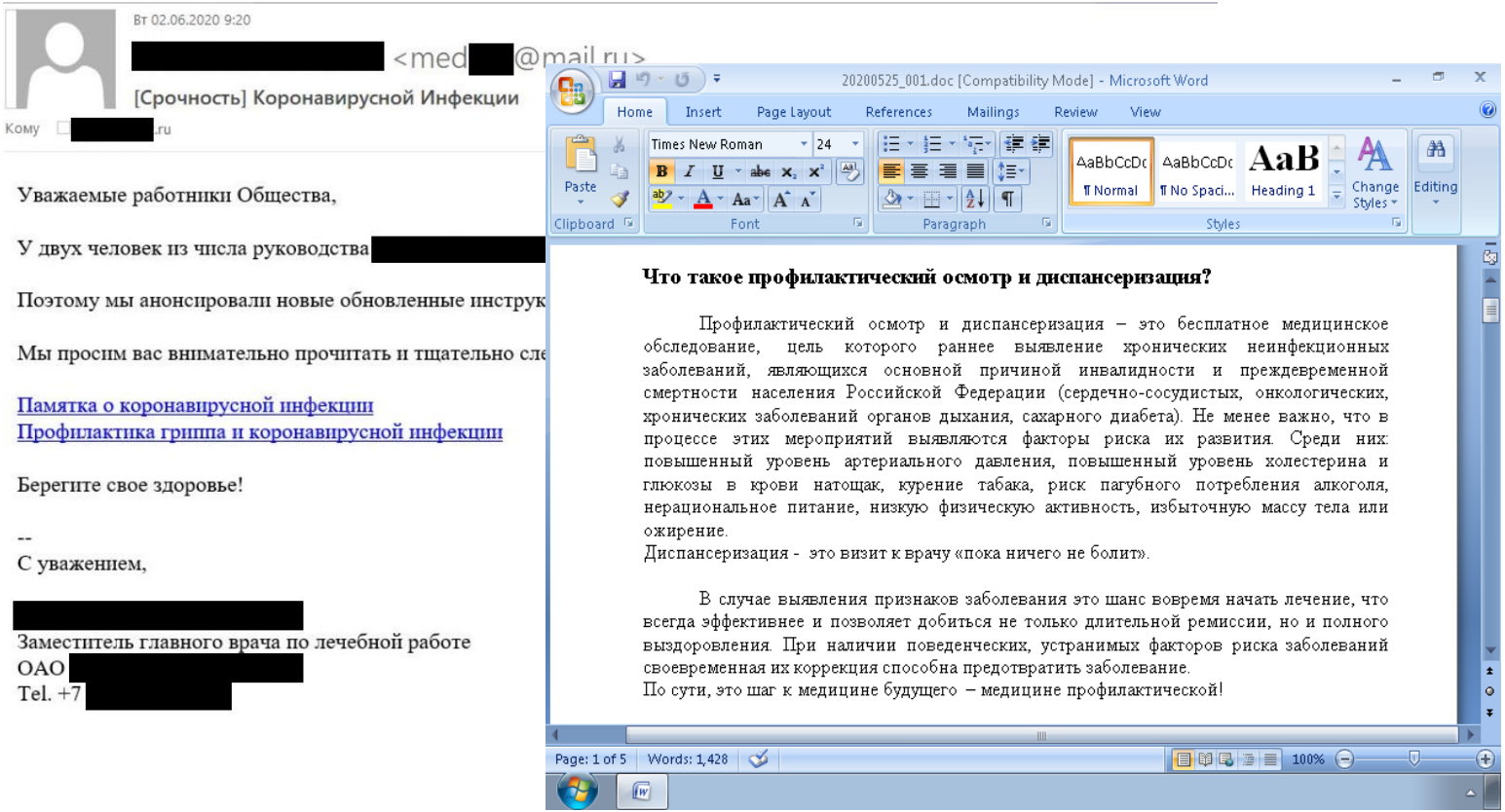
Koronavirus infeksiyası (COVID-19) dünya ölkələri arasında sürətlə yayılmaqda davam edir. Virusun uzun inkubasiya dövrünün olması, yayılma sürəti və vaksinin hələ də tapılmaması dövlətləri daha da cidditədbirlər görməyə sövq edir. Ümumdünya Səhiyyə Təşkilatı tərəfindən koronavirus infeksiyasının qlobal pandemiya elan olunduğunu nəzərə alaraq və virusun qarşısının alınması istiqamətindəUmumdünya Səhiyyə Təşkilatının tövsiyə və tələblərindən irəli gələrək ölkəərazisində bir sıra təxirəsalınmaz tədbirlərin həyata keçirilməsi zərurəti yaranmışdır. Bununla əlaqədar bir ay müddətində kütləvitədbirlərin təxirə salınması qərara alınmışdır. Həmçinin, dövlət vəözəl sektora aid qurumlardan, vətəndaşlardan xüsusi qaydalara ciddi riayət etmələri tələb olunur.

Azərbaycan Respublikası Nazirlər Kabineti yanında Operativ Qərargah 14 mart 2020-ci il saat 00:00-dan etibarən ölkəərazisində tətbiq olunacaq bəzi sosial izolyasiya tədbirlərini diqqətəçatdırır:

- ölkəüzrə bütün kütləvi tədbirlər, o cümlədən mədəni-idman tədbirləri təxirə salınır, artıq təyin olunmuş tədbirlərin tarixi dəyişdirilir;

13. Çindən gələn məktub və bağlamalar koronavirusa yoluxdura bilər. Xeyr, tədqiqatlar koronavirusların zərflər və bağlamalarda çox qalmadığını göstərib.
14. Ev heyvanları koronavirusa yoluxdura bilər. Bununla bağlı heç bir dəlil yoxdur.
15. Pnevmoniyaya qarşı peyvəndlər koronavirusdan qoruya bilər. Xeyr, bu virus köklü şəkildə fərqlənir və xüsusi bir peyvəndi yoxdur.
16. Burunun duzlu su (aptekdə satılan) ilə müntəzəm olaraq yuyulması infeksiyadan qoruyur. Xeyr, bu yalnız ümumi bir soyuqdəymədən qoruya bilər.
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 vasitədir. Antibiotiklər viruslara təsir etmir.
19. Dəniyə kunciut yağı sürtmək koronavirusdan qorunmağa kömək edir. Xeyr, yağ virusu öldürmür.
20. Həkimlər artıq infeksiyanın qarşısının alınması və ya müalicəsi üçün nəzərdə tutulmuş dərman vasitələri əldə edə biliblər. Xeyr, bu cür dərman hələ də yoxdur.

Covid-19 в APT на промышленную организацию в России



Вт 02.06.2020 9:20

[redacted] <med[redacted]@mail.ru>

[Срочность] Коронавирусной Инфекции

Кому [redacted].ru

Уважаемые работники Общества,

У двух человек из числа руководства[redacted]

Поэтому мы анонсировали новые обновленные инструк

Мы просим вас внимательно прочитать и тщательно сле

Памятка о коронавирусной инфекции
Профилактика гриппа и коронавирусной инфекции

Берегите свое здоровье!

--
С уважением,

[redacted]
Заместитель главного врача по лечебной работе
ОАО [redacted]
Tel. +7 [redacted]

20200525_001.doc [Compatibility Mode] - Microsoft Word

Home | Insert | Page Layout | References | Mailings | Review | View

Times New Roman 24

Paste | Clipboard | Font | Paragraph | Styles | Change Styles | Editing

¶ Normal | ¶ No Spaci... | Heading 1

Что такое профилактический осмотр и диспансеризация?

Профилактический осмотр и диспансеризация – это бесплатное медицинское обследование, цель которого раннее выявление хронических неинфекционных заболеваний, являющихся основной причиной инвалидности и преждевременной смертности населения Российской Федерации (сердечно-сосудистых, онкологических, хронических заболеваний органов дыхания, сахарного диабета). Не менее важно, что в процессе этих мероприятий выявляются факторы риска их развития. Среди них: повышенный уровень артериального давления, повышенный уровень холестерина и глюкозы в крови натощак, курение табака, риск пагубного потребления алкоголя, нерациональное питание, низкую физическую активность, избыточную массу тела или ожирение.
Диспансеризация - это визит к врачу «пока ничего не болит».

В случае выявления признаков заболевания это шанс вовремя начать лечение, что всегда эффективнее и позволяет добиться не только длительной ремиссии, но и полного выздоровления. При наличии поведенческих, устранимых факторов риска заболеваний своевременная их коррекция способна предотвратить заболевание.
По сути, это шаг к медицине будущего – медицине профилактической!

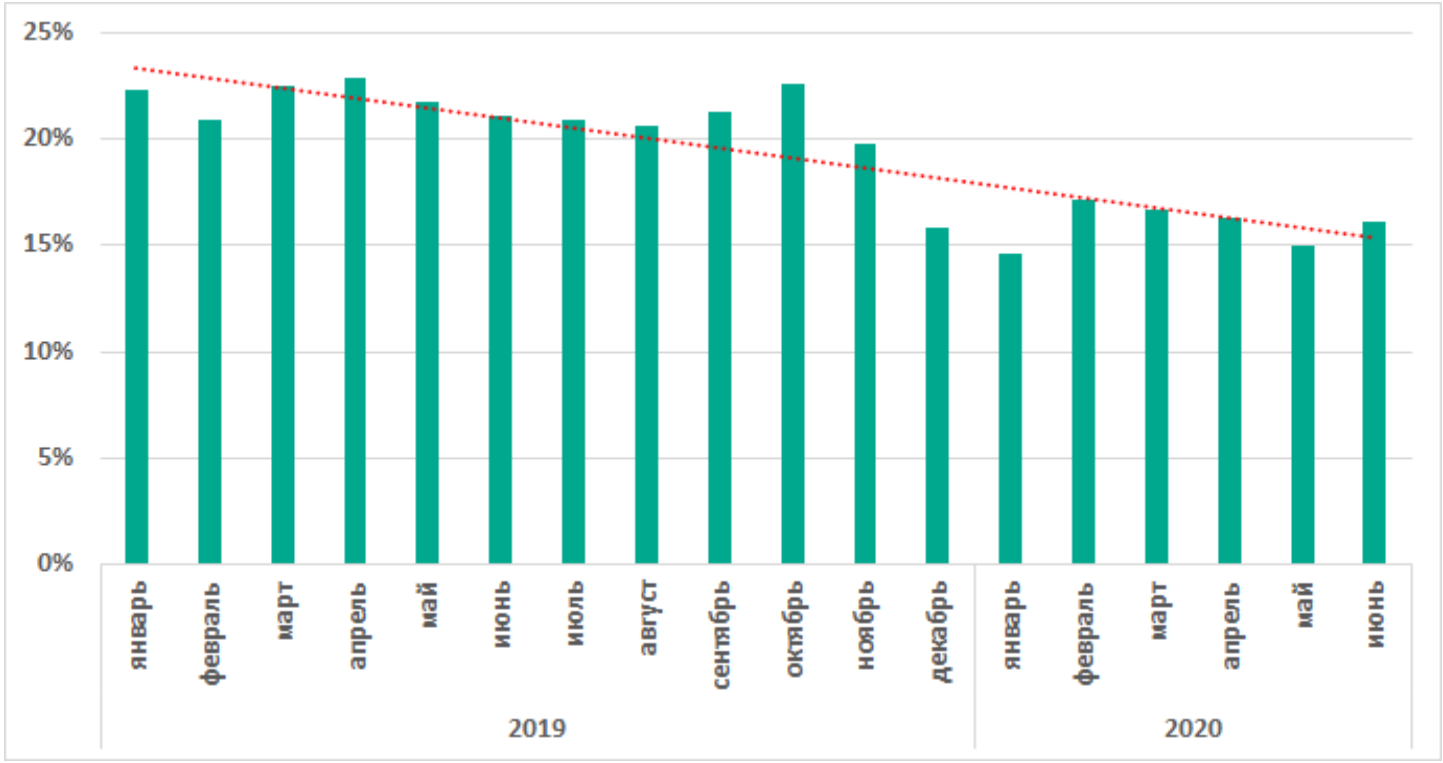
Page: 1 of 5 | Words: 1,428 | 100%

Изменения ландшафта угроз АСУТП

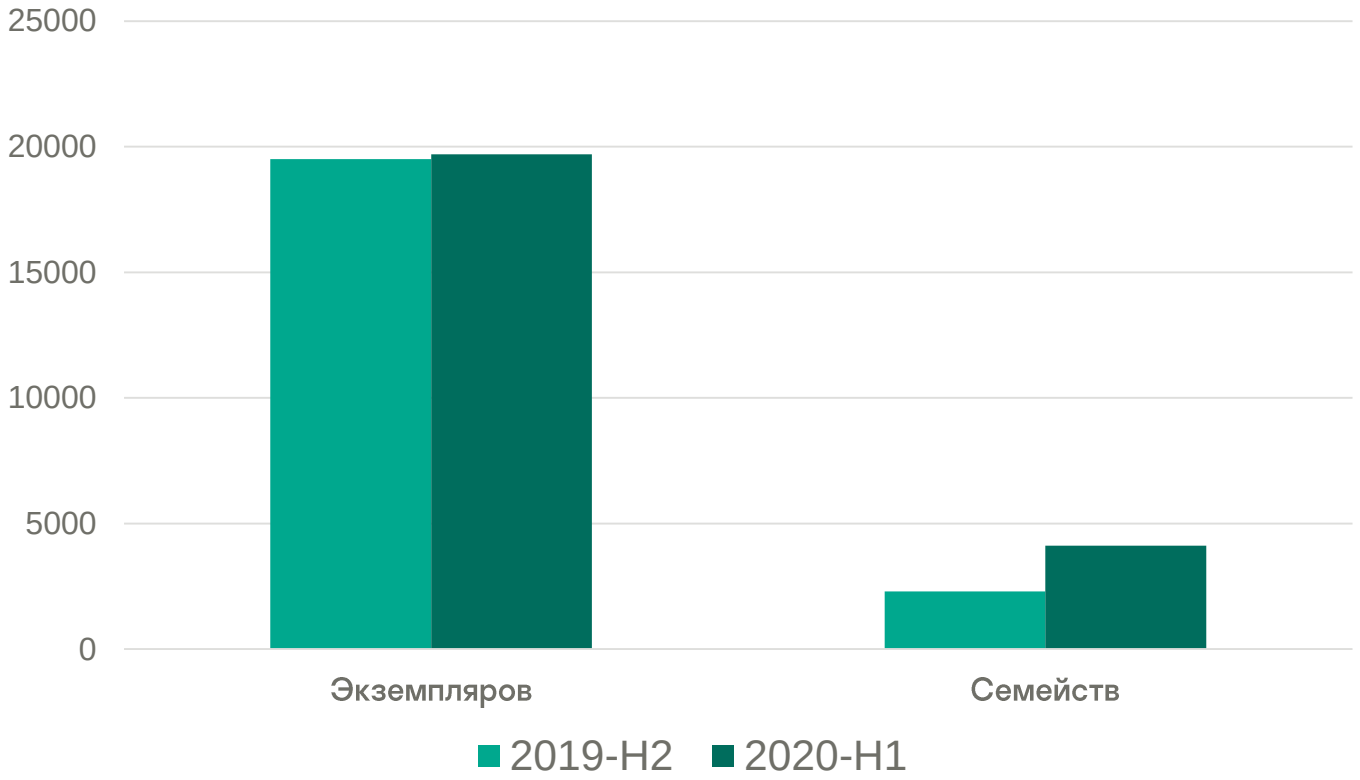
- Уменьшение % атакованных компьютеров
- Увеличение степени нацеленности атак и разнообразия ВПО
- Атака на промышленные предприятия в России

Уменьшение % атакованных компьютеров

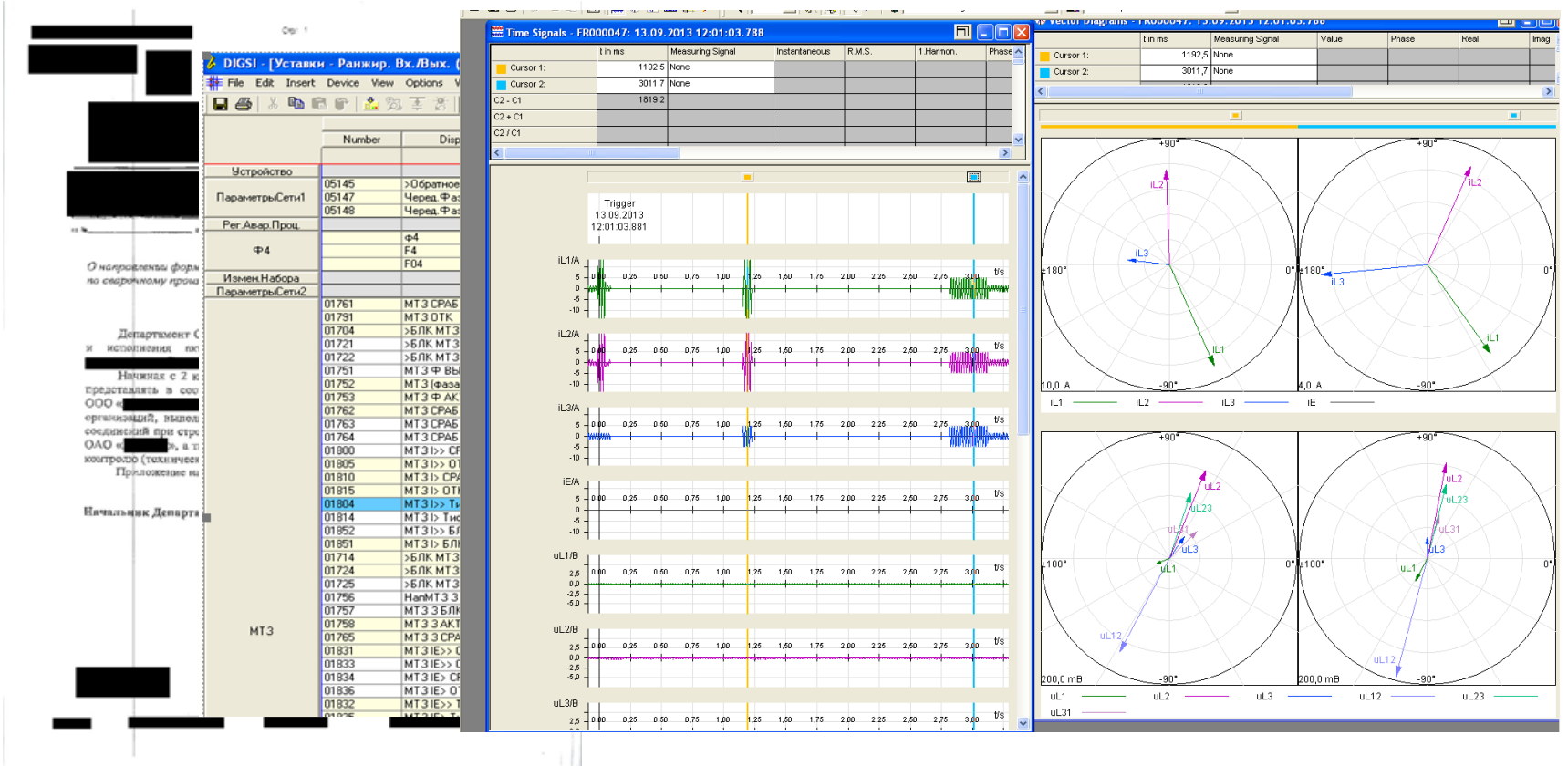
%АСУТП, на которых были заблокированы вредоносные объекты



Увеличение степени нацеленности атак: разнообразие ВПО



Пример: атака на промышленные предприятия в России

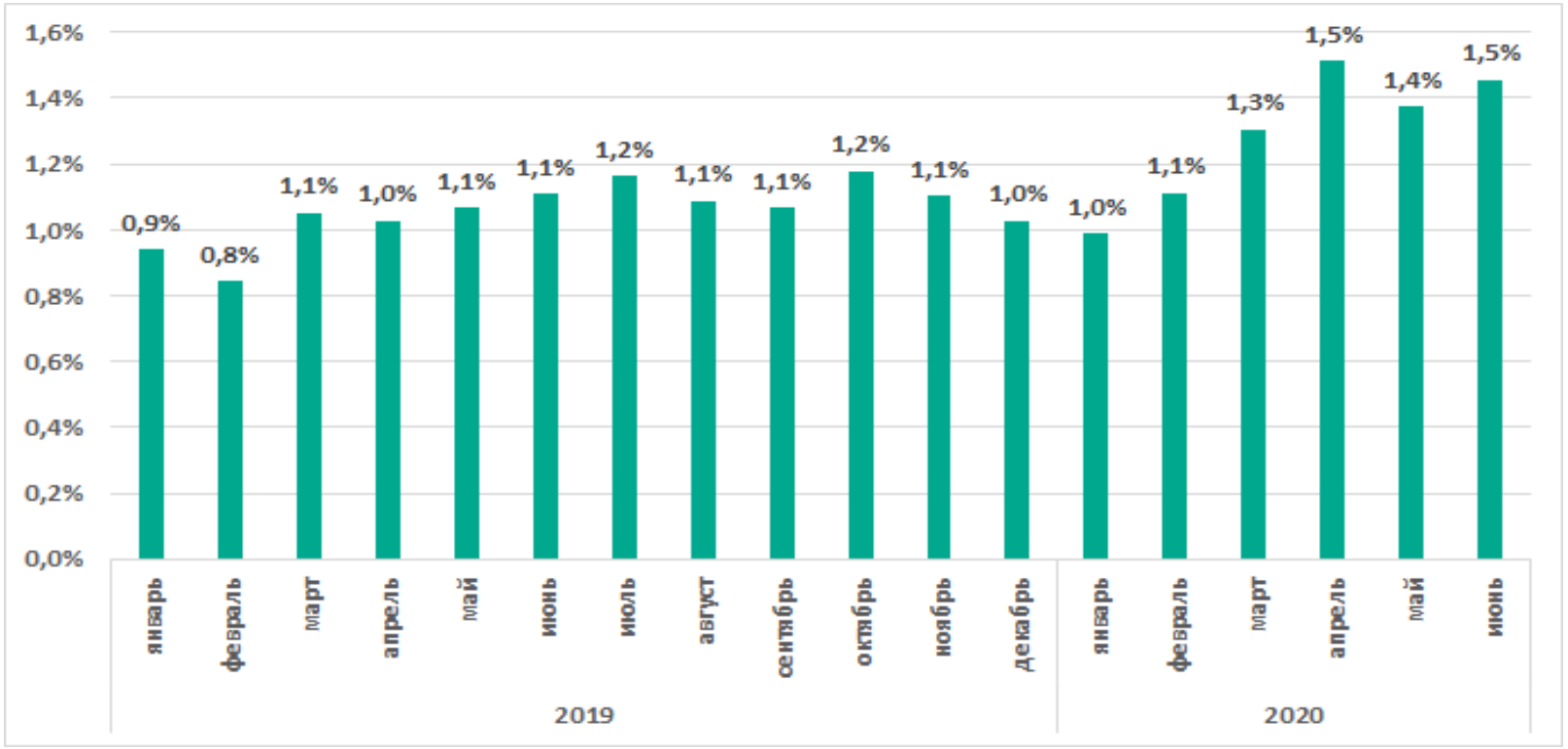


Изменения поверхности атаки АСУТП

- Оценка влияния удалённой работы
- Возможные последствия: атаки вымогателей
- Статистика атак по отраслям

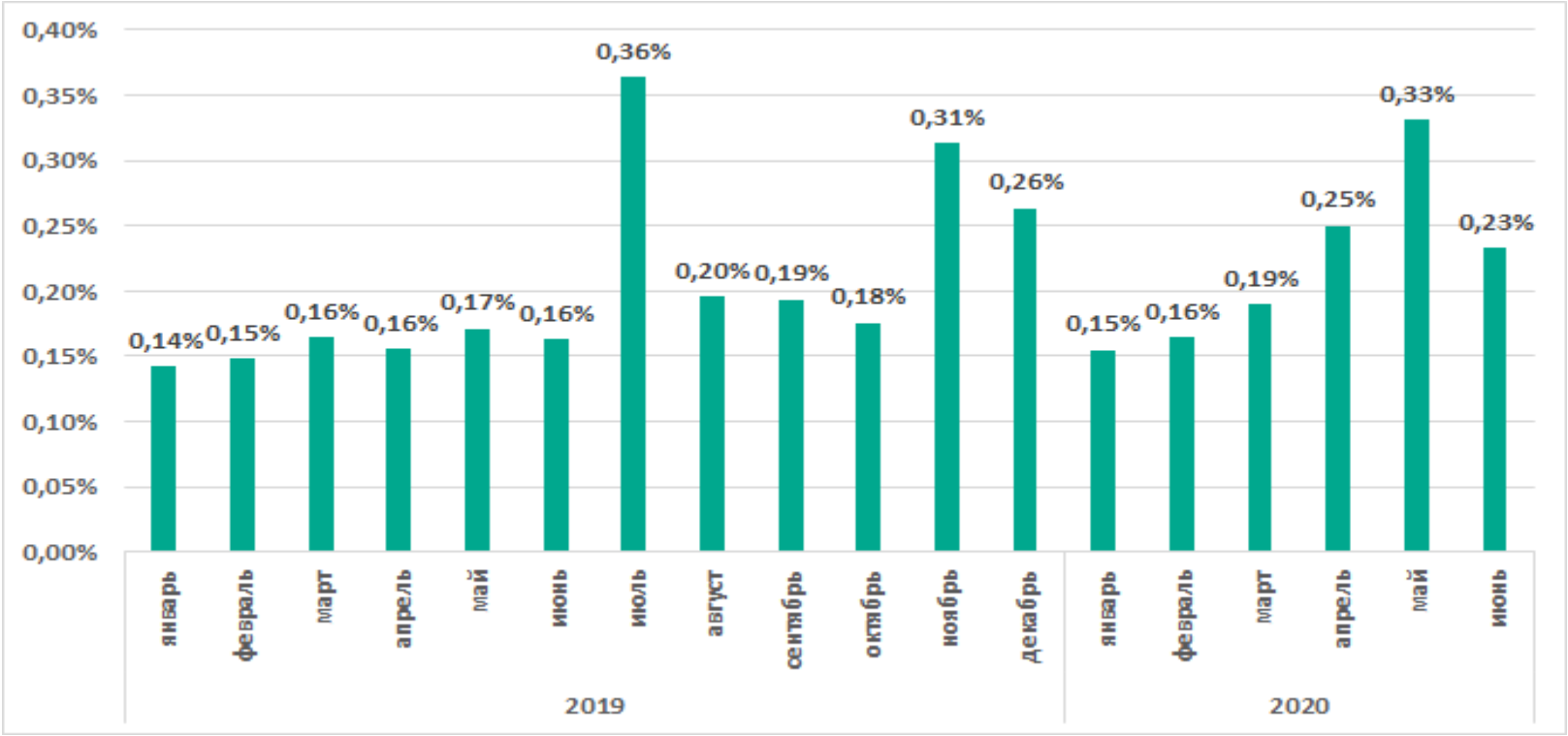
Изменения поверхности атаки АСУТП: влияние удалённой работы

% компьютеров АСУТП, доступных по RDP, январь 2019 – июнь 2020



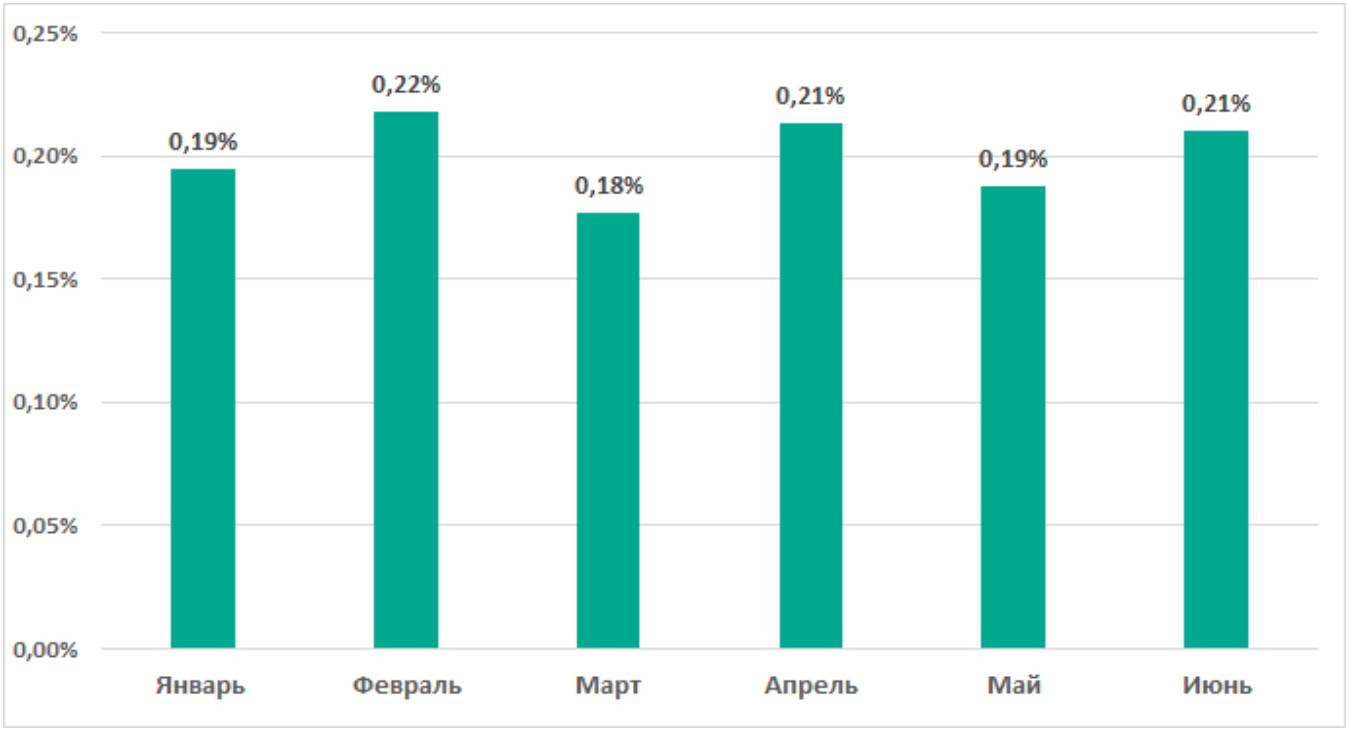
Изменения поверхности атаки АСУТП: влияние удалённой работы

% АСУТП, на которых фиксировались попытки подбора паролей к RDP



Возможные последствия: атаки вымогателей

%АСУТП, на которых были заблокированы вымогатели

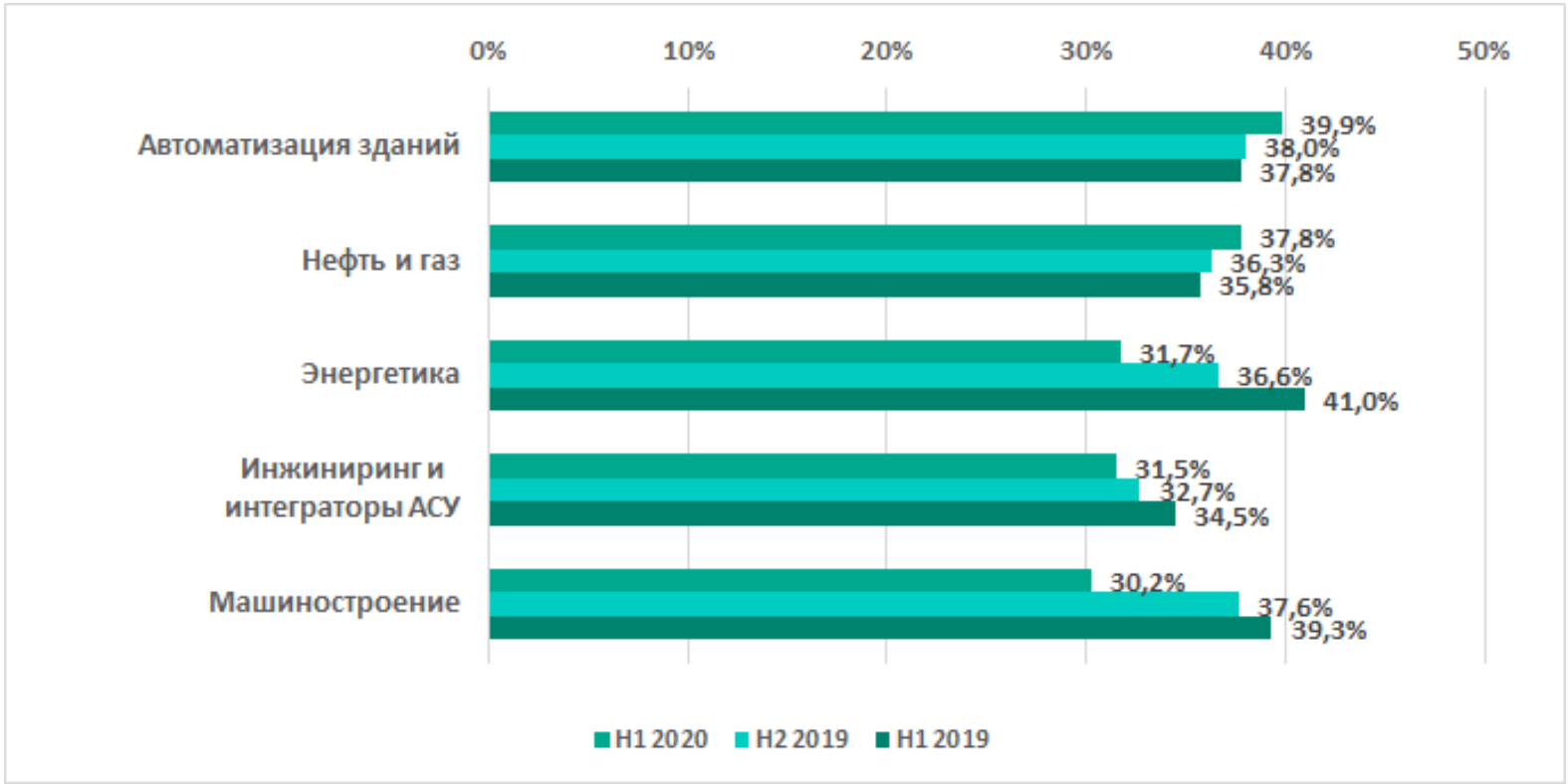


Атаки вымогателей: примеры громких инцидентов за первое полугодие 2020

- Атака вымогателя остановила производство компании Picanol в Бельгии, Румынии и Китае
- Атаки Ruyk на медицинские учреждения в США
- Атака вымогателя на датского производителя насосных решений DESMI Атака Ragnar Locker на португальскую энергетическую компанию EDP
- Атака на промышленные объекты швейцарского производителя поездов Stadler
- Атаки Mailto и Nefilim на австралийскую логистическую компанию Toll Group
- Атака шифровальщика Sodinokibi на электроэнергетические компании в Великобритании и Бразилии
- Атака на австралийского производителя напитков Lion
- Атаки с использованием шифровальщика Snake на автомобилестроительные и прочие промышленные компании в Китае, Японии и Европе

Тенденции 2020: статистика по отраслям

% компьютеров АСУТП, на которых было заблокировано ВПО



Спасибо!
Вопросы?

Для связи:
ics-cert@kaspersky .com
evgeny.goncharov@kaspersky.com

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

kaspersky