THE STANDOFF

Современные угрозы: что изменилось и что делать бизнесу

Артём Синицын
Руководитель программ ИБ в странах Центральной и Восточной Европы
Microsoft

Microsoft

Digital Defense Report 2020

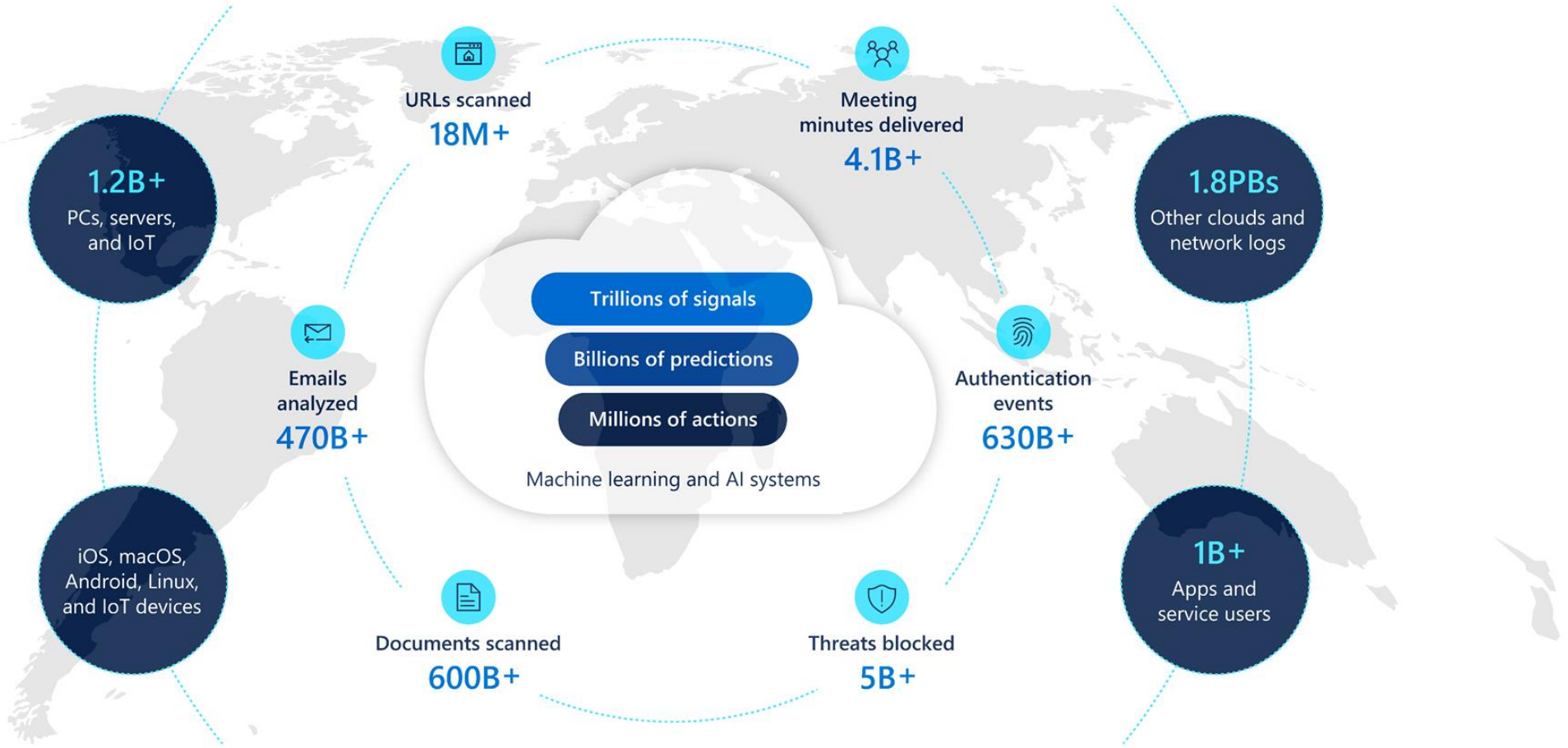
Microsoft

Сентябрь 2019 – Сентябрь 2020

На базе анализа:
8 триллионов сигналов в день
Интервью тысяч экспертов ИБ из 77 стран

Источники сигналов

Ежемесячный объем анализируемой службами ИБ Microsoft информации

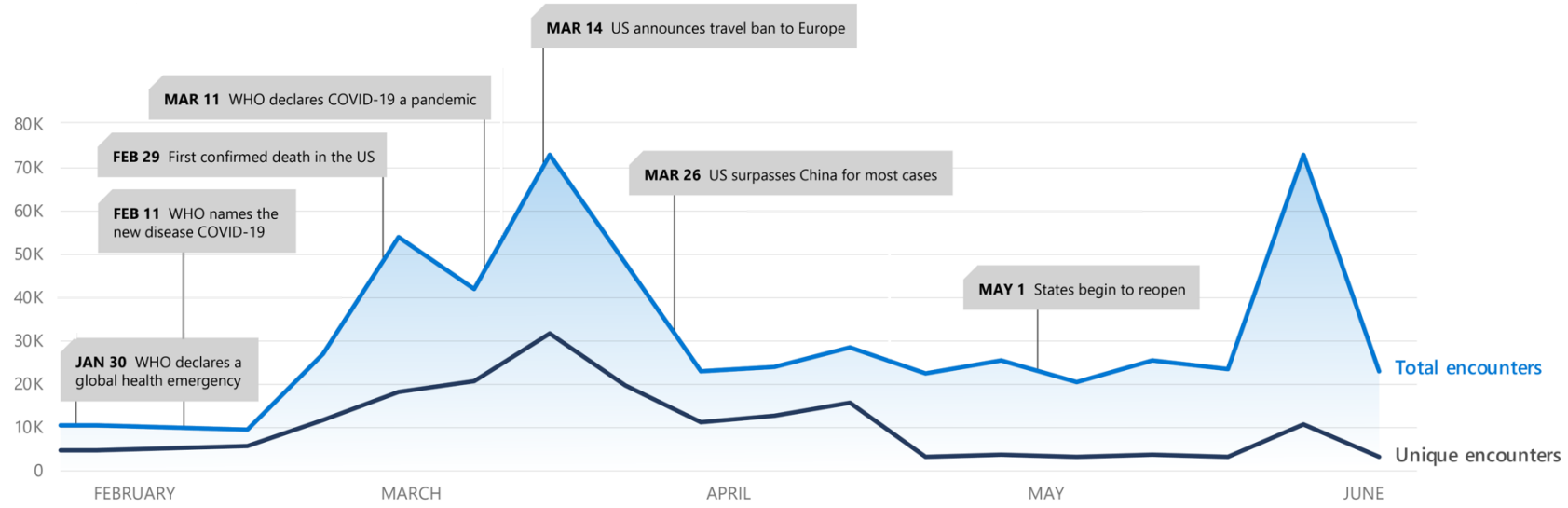


Microsoft

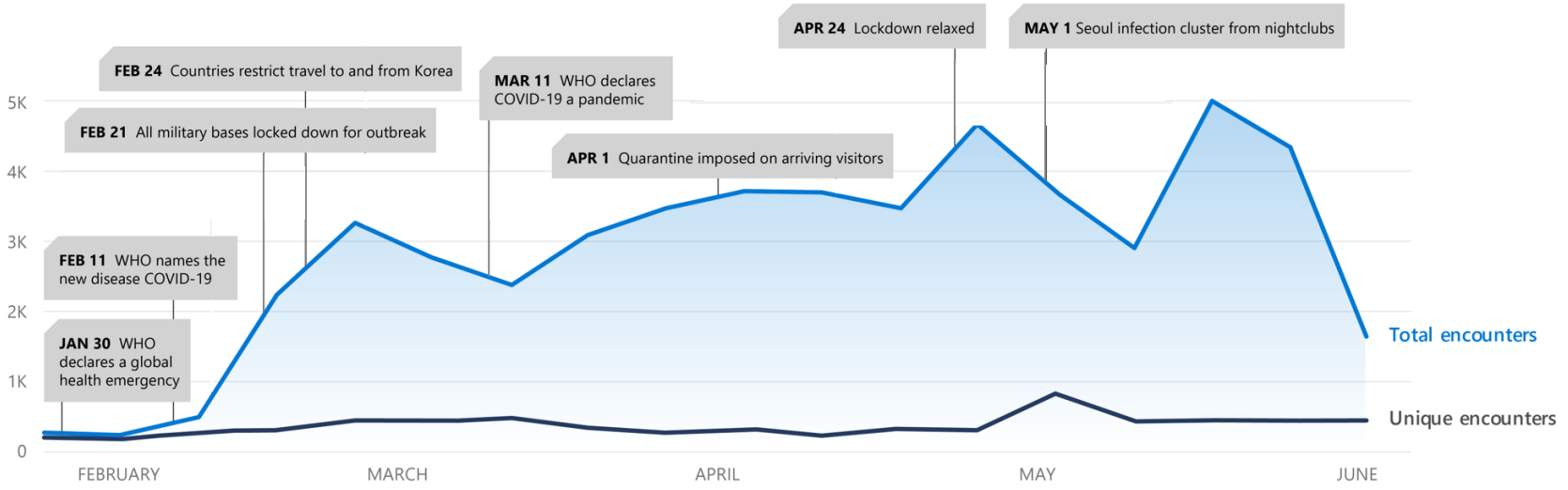
Фишинг: эксплуатация темы пандемии

Злоумышленники эксплуатируют новостную повестку

Атаки, замаскированные под новости: США



Атаки, замаскированные под новости: Южная Корея



Распределение атак, использующих тему COVID-19 по количеству вредоносных образцов (июль 2020)

Фишинг и компрометация бизнес-переписки

Microsoft

Выявлено за последний год:

6T
Messages scanned

~13B
Malicious emails blocked

~1.6B
URL-based email phishing threats blocked

~1.7-2B
URL payloads being created each month, orchestrated through thousands of phishing campaigns

Для получения учетных данных злоумышленники стали использовать фишинговые атаки

Любимые бренды для маскировки

Microsoft
zoom
amazon
ups

Наиболее пострадавшие индустрии

- Бухгалтерские услуги & Консалтинг
- Дистрибуция, продажи
- IT-сервисы
- Недвижимость
- Образование
- Здравоохранение
- Химическая промышленность
- Высокие технологии & Электроника
- Юридические услуги
- Аутсорсинг

Пример фишинг-атаки

Microsoft

1 Set up criminal Infrastructure

Set up fake domains or compromise legitimate ones

Gather information on potential victims

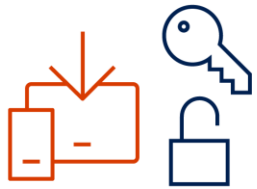
2 Send malicious messages

3 Entice victim to click

Click sends victim to fake domain (spoofed site)

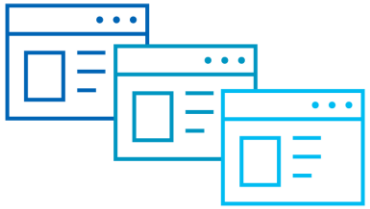
4 Victim's credentials are stolen

Victim inserts credentials into a fake web form



Or, malware is downloaded to victim's device to gather credentials

5 Victim's data is sent to "drop account"



Cybercriminals use victim's credentials on other legitimate sites

Or, use them to gain access to corporate networks and data

Пример компрометации бизнес-переписки

Microsoft

1

Cybercriminal poses as CEO using any of a variety of methods (such as spoofing, impersonation, or credential theft)

2

Cybercriminal gains access to mail account and may monitor the CEO's mail to gain additional information, to increase the sophistication of the attack and the likelihood of success

Monitors mail for information on:

- Relationships
- Common phrases
- Calendar, business activities, travel
- Wire transfers

Sets mailbox forwarding rules using keywords, keeping certain email traffic hidden from the CEO

- Sample keywords: "invoice," "accounts receivable," "funds," "overdue," "payroll," "IBAN"
- Mails with keywords are forwarded to a collection email account controlled and monitored by the cybercriminal

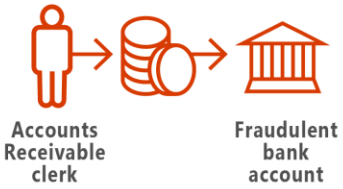
3

Cybercriminal masquerades as CEO

Cybercriminal sends email that is crafted to appear as though it's coming from a trusted or important position at work, such as the victim's manager, CEO, CFO, vendor/business partner, or someone the person would take notice of.

4

Victim wires business payment to fraudulent bank account

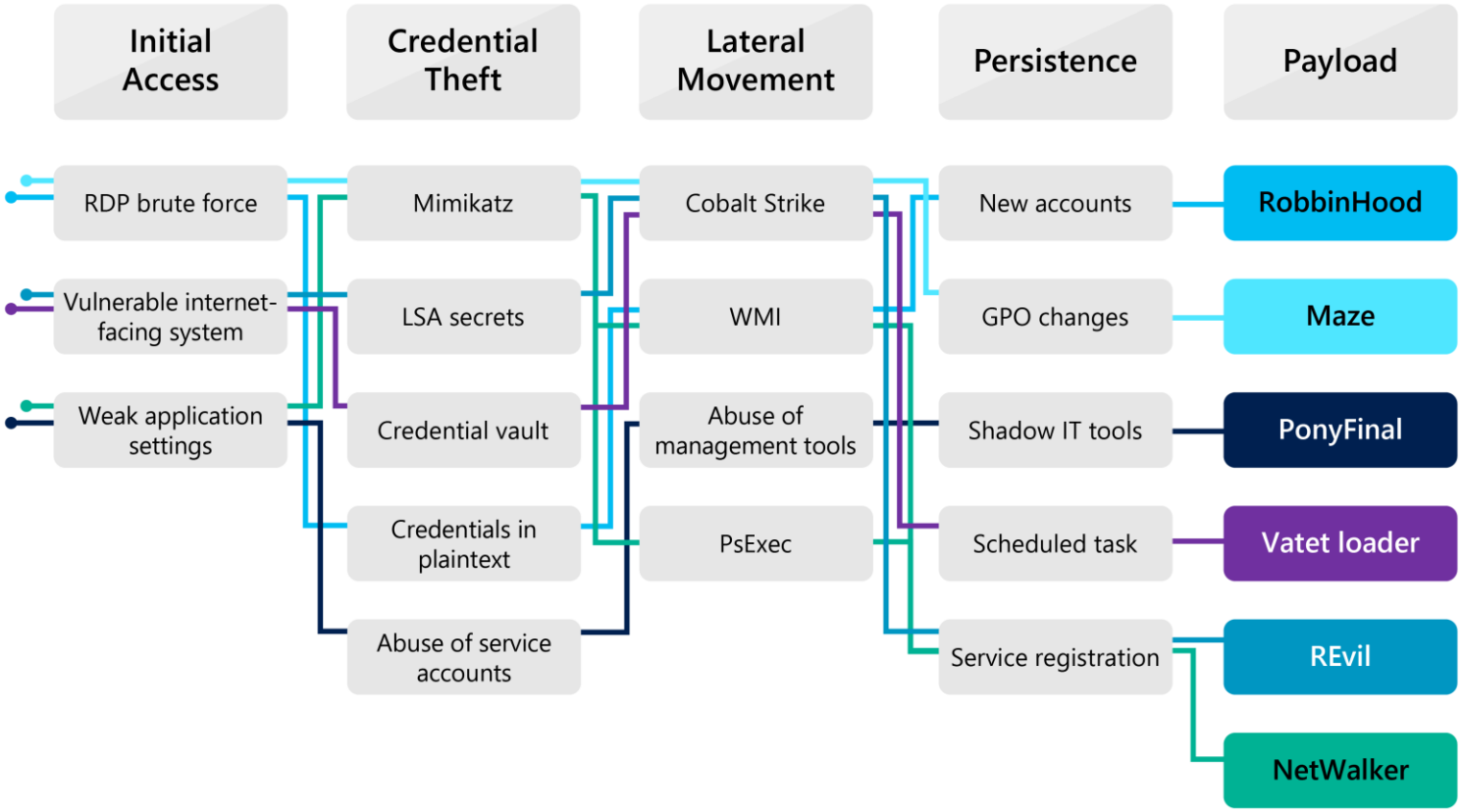


Victim (e.g. Accounts Receivable clerk) wires payment to a fraudulent bank account, as directed by the cybercriminal masquerading as the CEO, CFO, or business partner.

Microsoft

Программы-вымогатели

Вымогатели стали главной причиной реагирования на инциденты ИБ



Сократилось время пребывания в системе жертвы – в некоторых случаях менее 45 мин

Преступники тщательно выбирают наиболее выгодные дату и время атаки

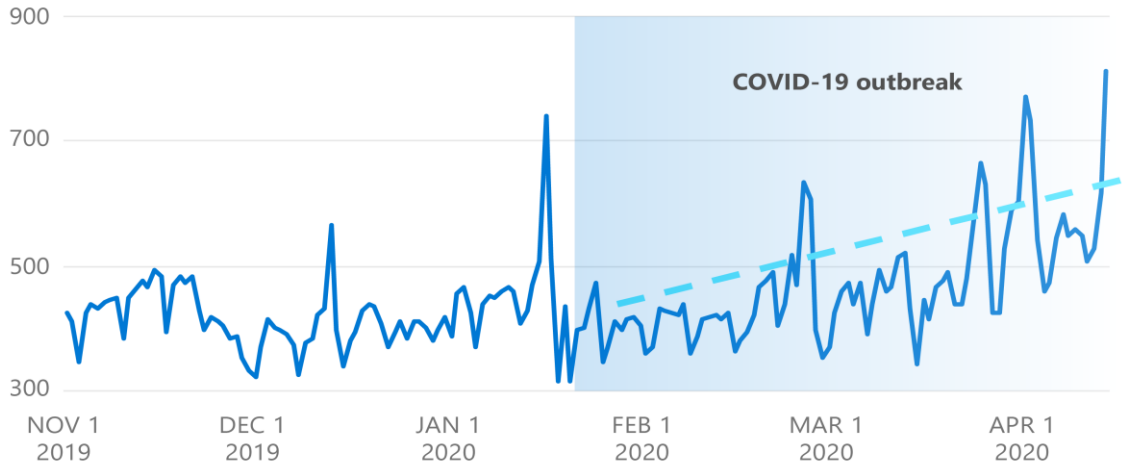
Октябрь 2019 – сентябрь 2020

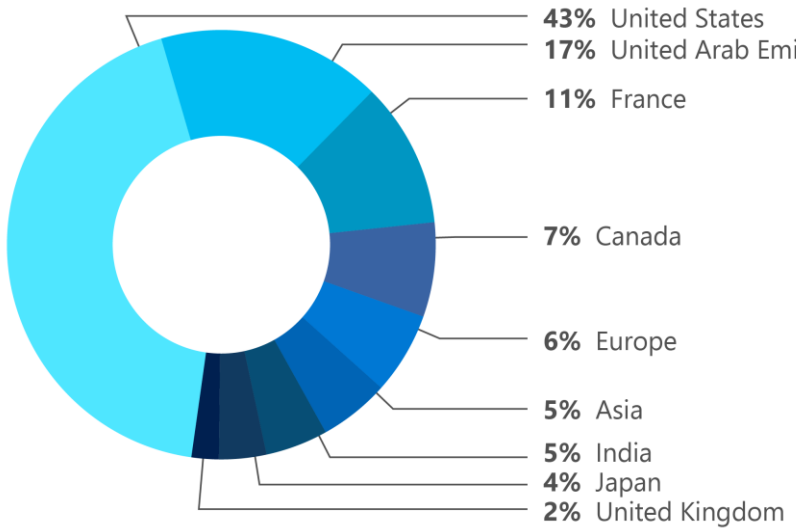
THE STANDOFF

Microsoft

Атаки на инфраструктуру

DDoS-атаки: рост с началом пандемии





Январь 2020 – июнь 2020

В марте 2020 Microsoft предотвратила от 600 до 1000 уникальных DDoS-атак в день

Это на 50% превышает число подобных атак до пандемии

THE STANDOFF

Microsoft

Компрометация учетных записей

Компрометация учетных записей

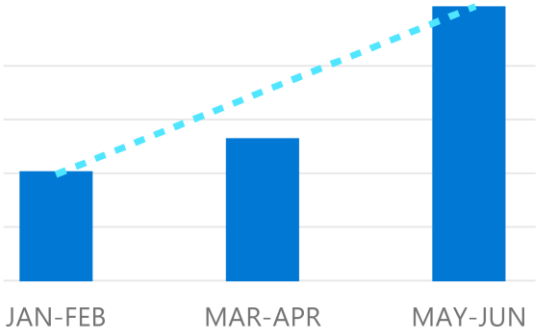
Microsoft

THE STANDOFF

Identity based attacks

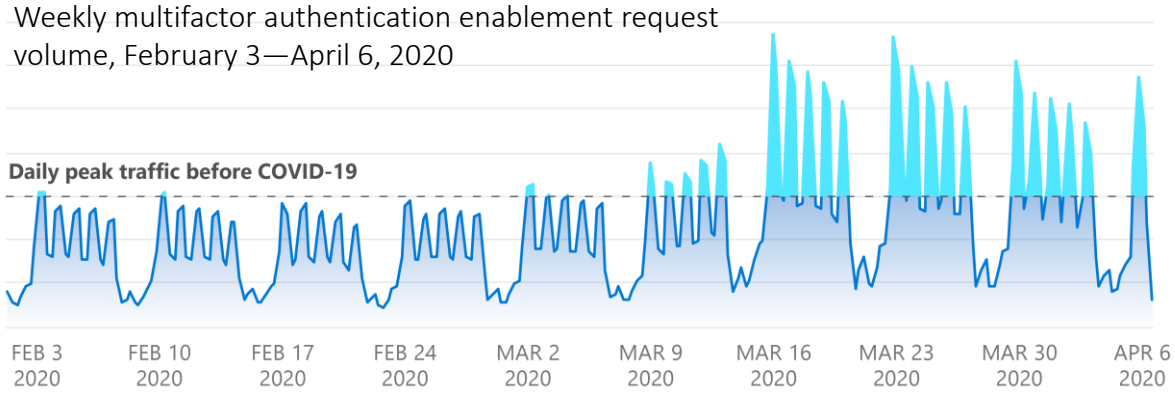
Password brute force attempts against Azure AD accounts

Azure Active Directory saw an increase in identity-based attacks using brute force on enterprise accounts during the first half of 2020.



Strong authentication methods are key to defending against these attacks

Weekly multifactor authentication enablement request volume, February 3—April 6, 2020



Approximate twofold increase in MFA-enablement requests after the onset of COVID-19, as work-from-home policies were enacted.

Microsoft

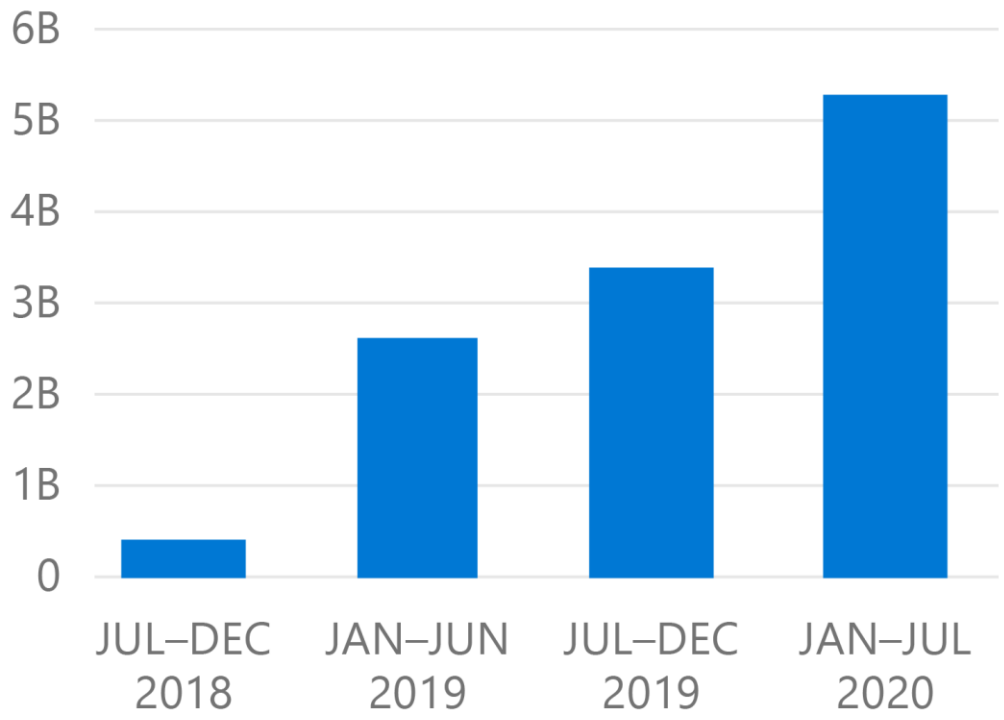
Интернет вещей

Рост числа угроз IoT составил 35%

Microsoft

THE STANDOFF

Общее число атак



В первой половине 2020 зафиксировано на 35% больше угроз IoT по сравнению с показателем второго полугодия 2019

CyberX Risk Report

Data from 1,800 Industrial Control System Networks

Microsoft

71%

Sites have old versions of Windows without regular patching

64%

Have unencrypted passwords facilitating compromise

66%

Sites that are not automatically updating with latest AV definitions

54%

Have devices able to be remotely accessed enabling attackers to pivot undetected

27%

ICS devices that have direct connections to the internet

CyberX: recently acquired by Microsoft

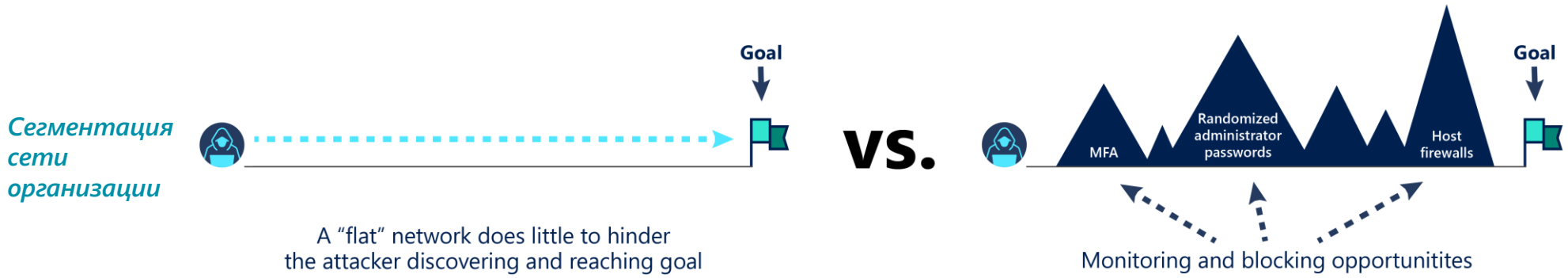
Microsoft

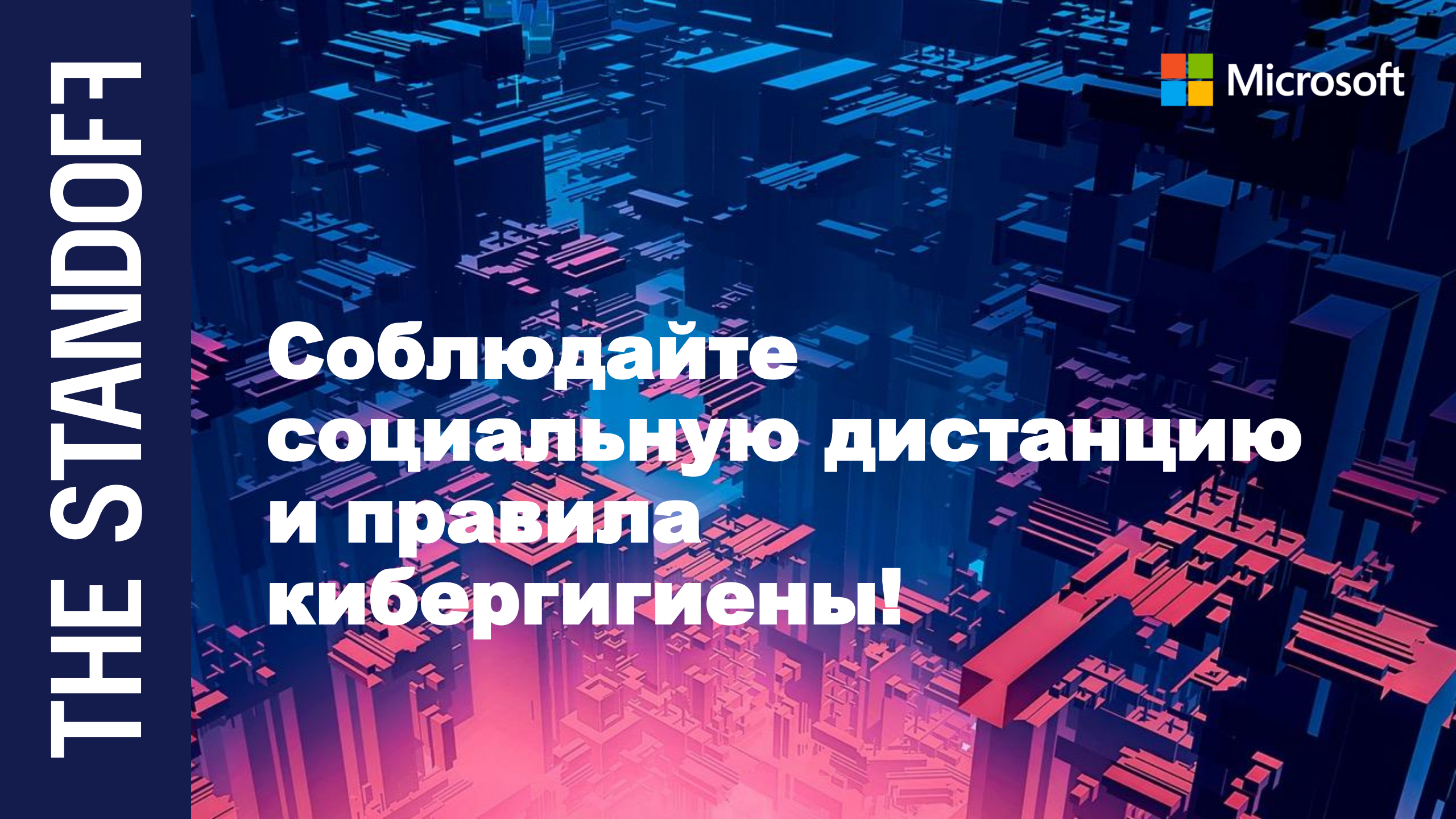
Что делать бизнесу?

Что можно сделать уже сегодня

Пять основных шагов для безопасности бизнеса

1. Внедрите многофакторную аутентификацию (MFA)
2. Разумная бизнес-переписка – соблюдайте правила кибергигиены
3. Своевременно обновляйте ваши приложения и системы
4. Следуйте принципу наименьшего уровня привилегий
5. Замедлите атаки с помощью сегментации вашей сети




THE STANDOFF
Microsoft
Соблюдайте социальную дистанцию и правила кибергигиены!