CONEWS FORUM 2023
ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ ЗАВТРА

Насколько безопасен интернет вещей ?

Андрей Ярных
член правления РОЦИТ
независимый эксперт по информационной безопасности

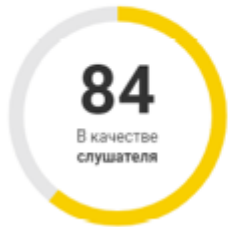
RUNET ID: https://runet-id.com/372/

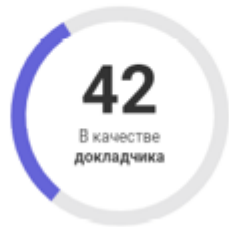
АНДРЕЙ ЯРНЫХ

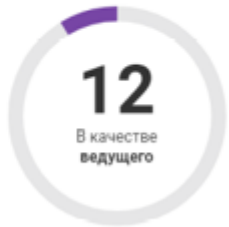
Член правления РОЦИТ, эксперт по GR и Информационной безопасности

Представлял позицию и интересы "Лаборатории Касперского" в следующих государственных органах:

- ГД ФС РФ
- СФ ФС РФ
- Общественная палата РФ
- Министерство связи РФ
- МИД РФ
- ОБСЕ
- БРИКС
- Парламентское собрание Союза Беларуси и России по теме "Единое информационное пространство Союзного государства"







Достижения

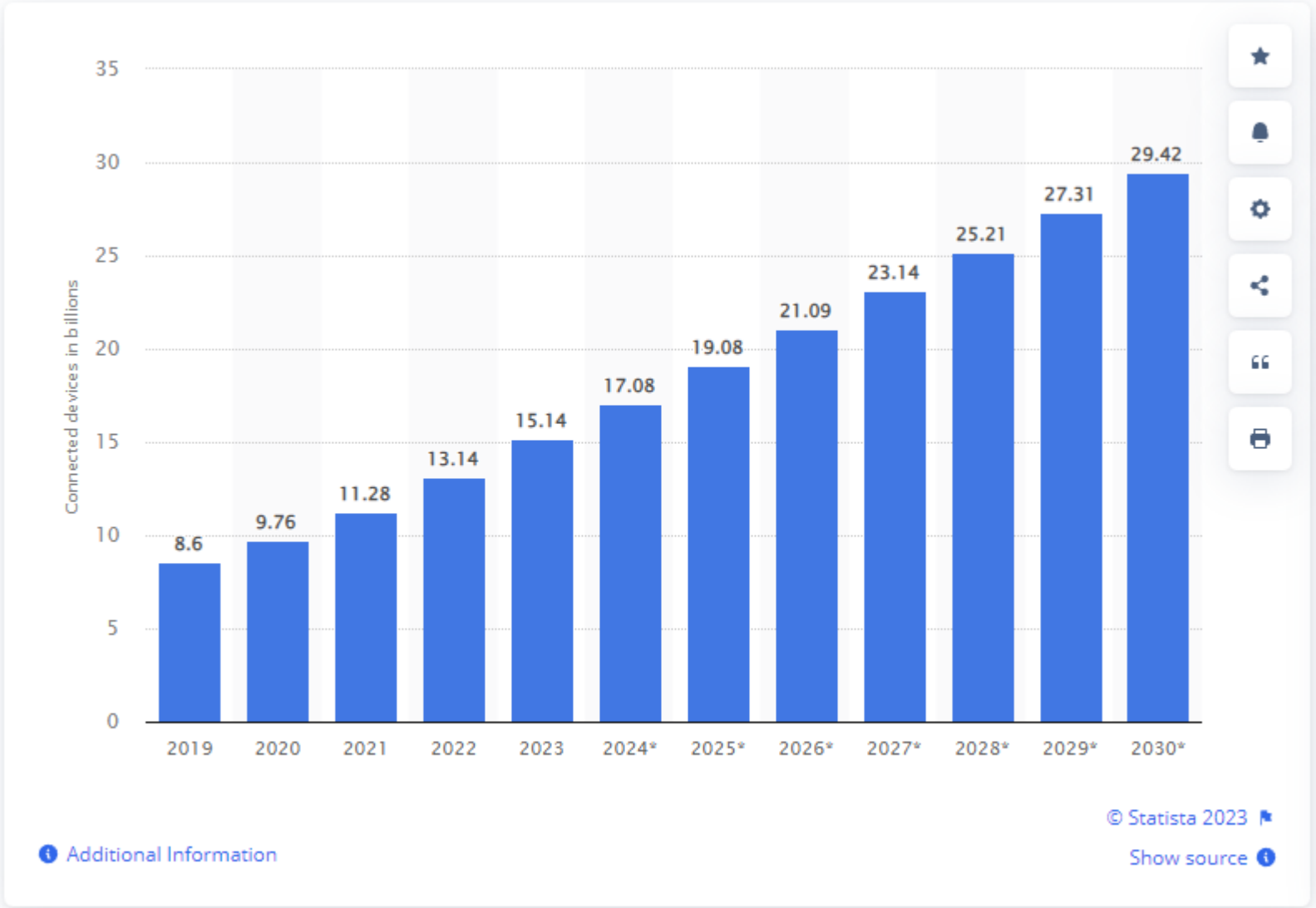
1. с 2001 года работал над созданием и развитием электронных продаж "Лаборатории Касперского" (от 0 до 25 миллионов долларов / год)
2. с 2003 года отвечал за сотрудничество с ведущими российскими интернет-проектами: совместные проекты с Rambler, Mail.ru, Яндекс, Ростелеком
3. с 2010 года работаю в государственных экспертных группах по представлению интересов компании
4. один из ветеранов Российского Интернета, https://runet-id.com/372/
5. член официальных и неофициальных групп в области электронной коммерции, поставщиков услуг, разработки программного обеспечения
6. эксперт рабочих групп Минцифры и Минпромторга (109 ПП РФ), РФРИТ.
7. эксперт в мероприятиях МИД РФ, ПИР Центр, ДК «Валдай», ТПП РФ.

Награды

- ✓ Почетная грамота Министерства связи и массовых коммуникаций Российской Федерации.
- ✓ Диплом компании «За вклад в развитие Лаборатории Касперского»
- ✓ Премия Рунета 2012 за проект Антивирус Касперского для Яндекса

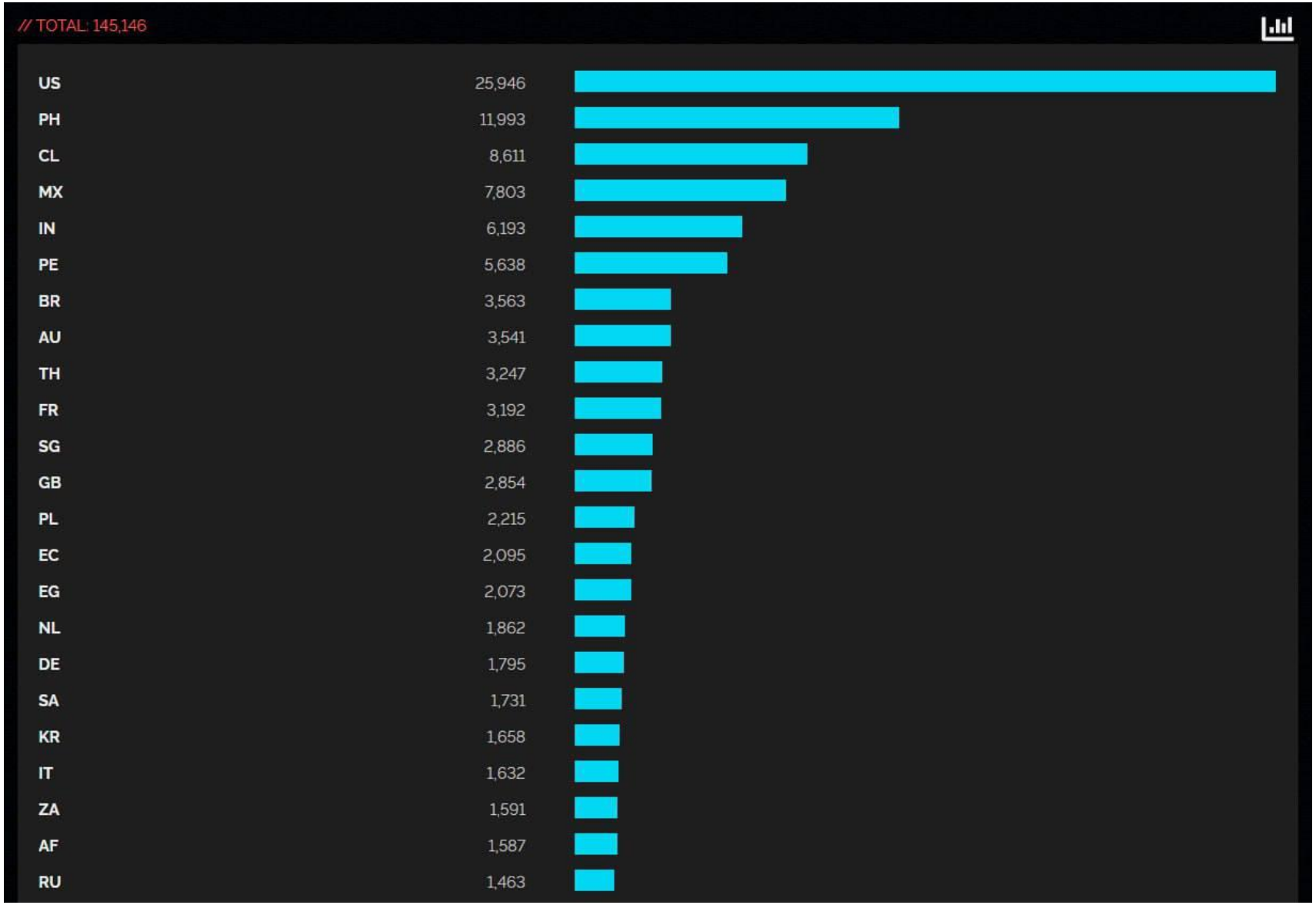
Number of Internet of Things (IoT) connected devices worldwide from 2019 to 2023, with forecasts from 2022 to 2030

(in billions)



Наиболее важным вариантом использования устройств Интернета вещей в потребительском сегменте являются потребительские интернет-устройства и мультимедийные устройства, такие как смартфоны, где, по прогнозам, к 2030 году число устройств интернета вещей вырастет более чем до 17 миллиардов. Другими вариантами использования более миллиарда устройств Интернета вещей к 2030 году являются подключенные (автономные) транспортные средства, ИТ-инфраструктура, отслеживание и мониторинг активов и интеллектуальная сеть.

statista



🚨 Идёт активная эксплуатация CVE-2023-20198 в Cisco IOS XE. Несмотря на предупреждения специалистов и отсутствие патчей, прямо сейчас в Интернет «торчат» почти 150 тысяч хостов

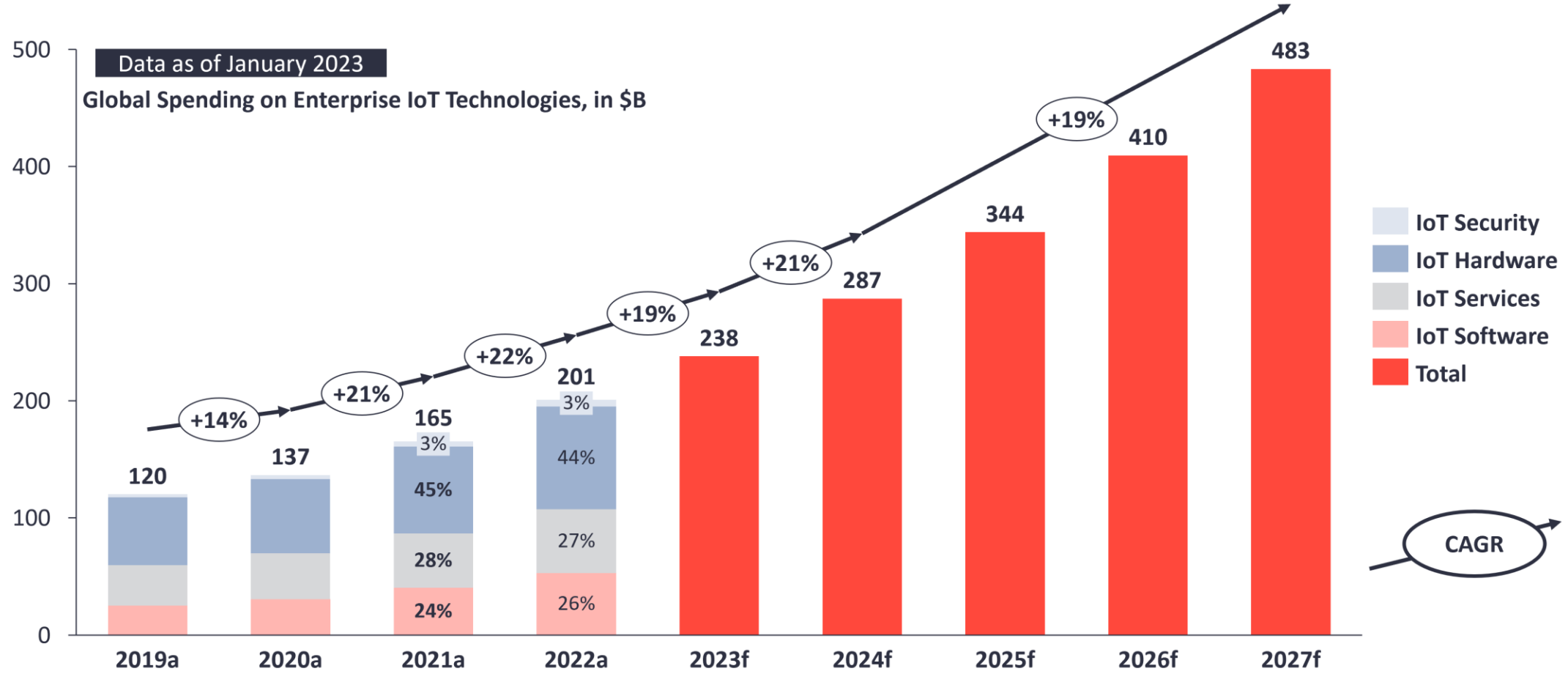
Из них полторы тысячи хостов — в России.

Значительная часть этих устройств уже скомпрометирована.

https://censys.com/cve-2023-20198-cisco-ios-xe-zeroday/

На момент публикации исследователи переписи наблюдали за 34 140 устройствами, на которых, по-видимому, был установлен бэкдор

Enterprise IoT market 2019–2027



Note: IoT Analytics defines IoT as a network of internet-enabled physical objects. Objects that become internet-enabled (IoT devices) typically interact via embedded systems, some form of network communication, or a combination of edge and cloud computing. The data from IoT-connected devices is often used to create novel end-user applications. Connected personal computers, tablets, and smartphones are not considered IoT, although these may be part of the solution setup. Devices connected via extremely simple connectivity methods, such as radio frequency identification or quick response codes, are not considered IoT devices. a: Actuals, f: Forecast

Таблица 1. Топ-10 наиболее перспективных технологий Интернета вещей в 2023 г.

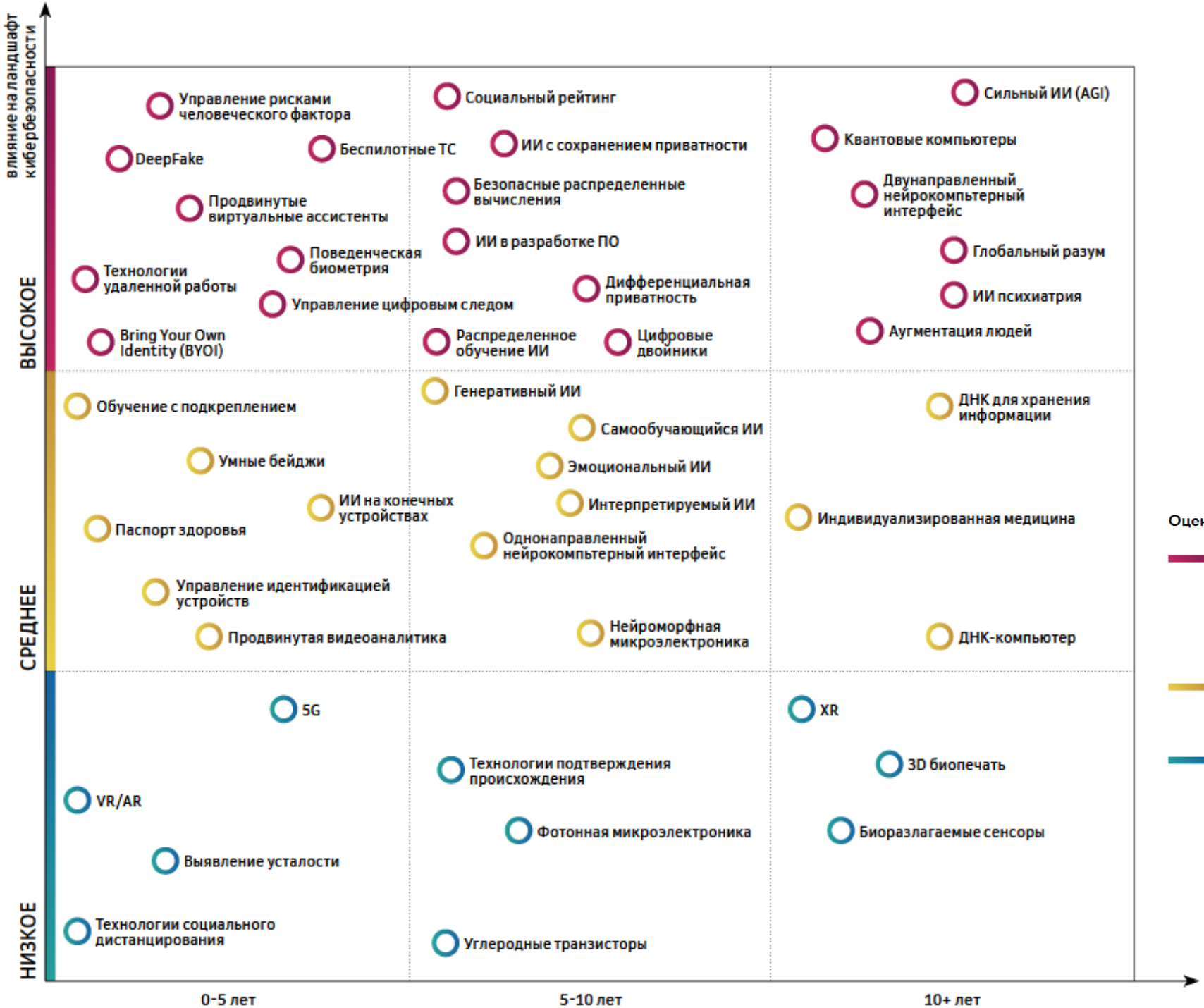
Ранг	Технологии	Индекс значимости	Уровень динамичности	Сроки массового внедрения
1	Интернет медицинских вещей (IoMT)	1.00		3-5 лет
2	Туманные вычисления и облачный Интернет вещей	0.97		1-2 года
3	Мобильный Интернет вещей	0.81		1-2 года
4	Искусственный интеллект вещей (AIoT)	0.70		3-5 лет
5	Интернет вещей для умного города / дома	0.58		1-2 года
6	Интернет робототехнических вещей (IoRT)	0.23		3-5 лет
7	Спутниковый Интернет вещей	0.21		4-6 лет
8	Носимый Интернет вещей	0.16		3-5 лет
9	Интеграция Интернета вещей и периферийных устройств	0.12		1-2 года
10	Интернет вещей на транспорте	0.09		1-2 года

Легенда:

Стабильные Растущие Быстрорастущие

Институт статистических исследований и экономики знаний (ИСИЭЗ) НИУ ВШЭ

Hypervector – график влияния перспективных технологий на ландшафт угроз кибербезопасности



Оценка влияния на ландшафт угроз имеет 3 градации:

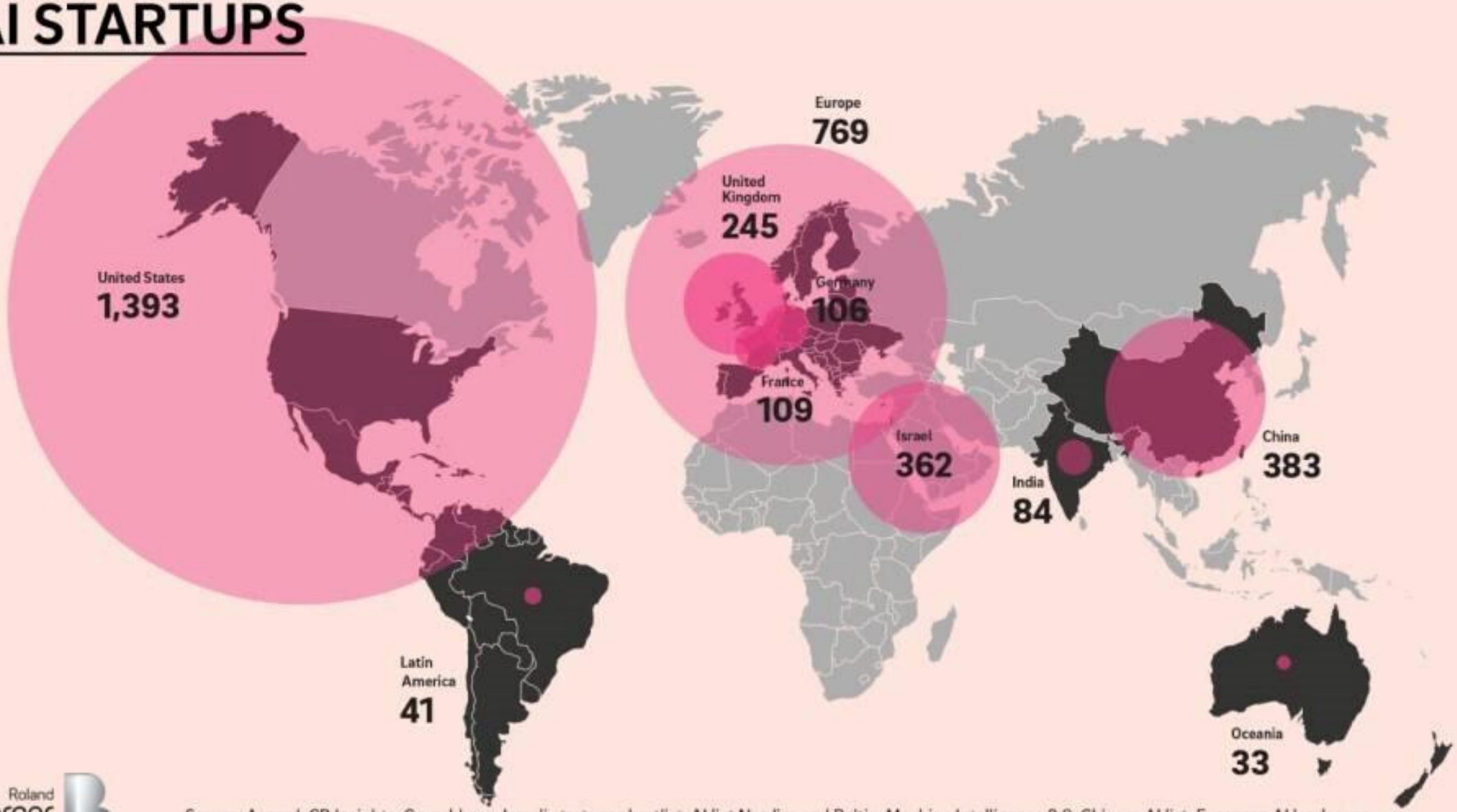
1 **Высокое** – технология существенно влияет на ландшафт угроз, создает возможности для реализации принципиально новых атак, создает новые поверхности атаки или существенно изменяет существующие. Также влияние оценивается, как высокое, если технология может быть использована для защиты от киберугроз и имеет существенное преимущество по сравнению с уже используемыми методами защиты.

2 **Среднее** – технология влияет на ландшафт угроз, не создает возможностей для принципиально новых атак или методов защиты, но при этом позволяет значимо повысить эффективность существующих методов атаки или защиты.

3 **Низкое** – технология практически не влияет на ландшафт угроз, не порождает новых угроз или методов защиты. Обеспечивает лишь небольшой рост эффективности атак или методов защиты от них.

источник: Sber Cybersecurity Lab.

THE RACE FOR LEADERSHIP: GLOBAL DISTRIBUTION OF AI STARTUPS

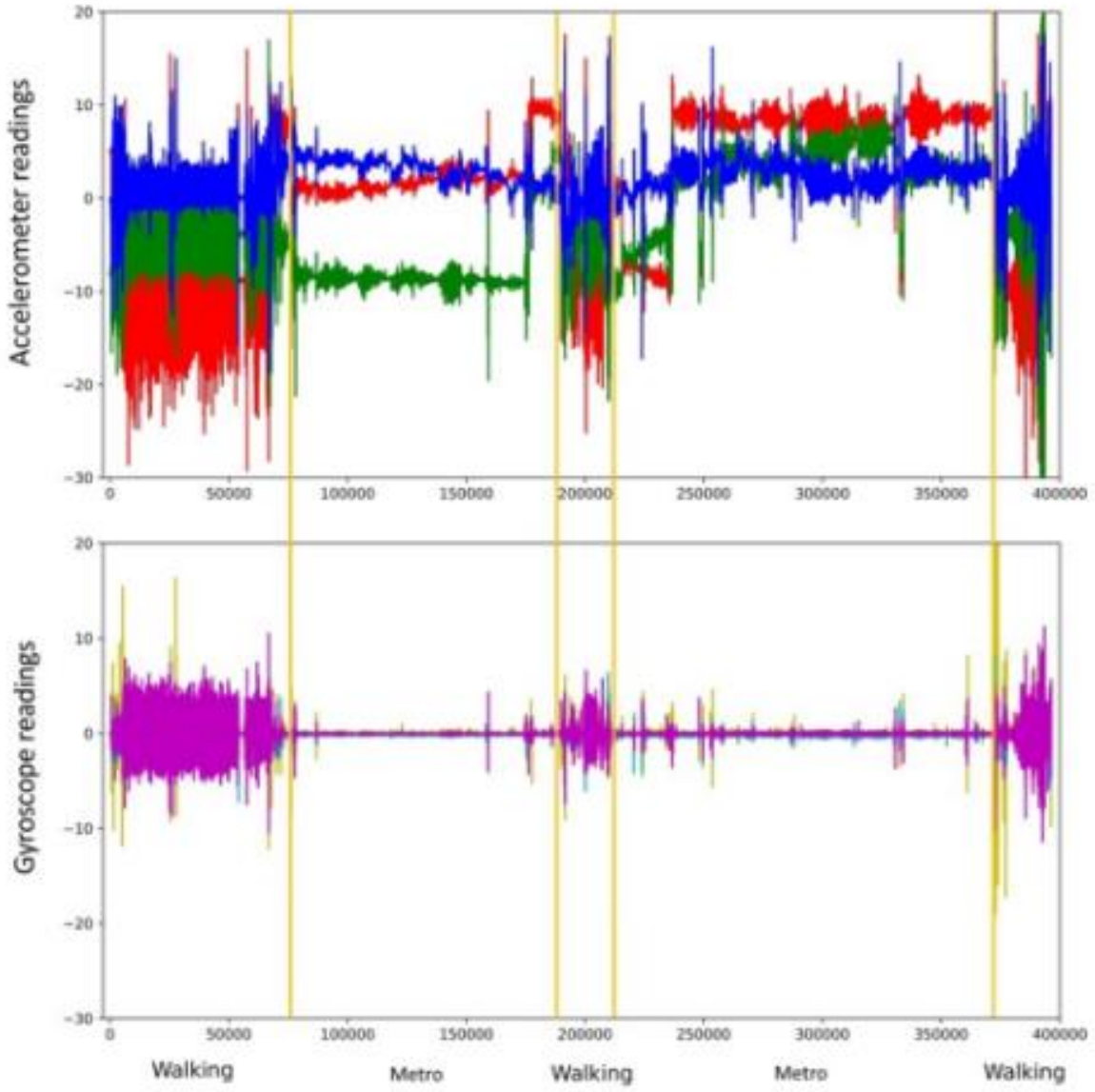


Roland Berger

Source: Asgard, CB Insights, Crunchbase, Israeli startups shortlist, AI list Nordics and Baltic, Machine Intelligence 2.0, Chinese AI list, European AI landscape, German AI landscape, Israeli AI startup map, Japanese AI list, UK AI list, French AI ecosystem, Korean AI list, own research.

Для целей нашего исследования мы написали довольно простое приложение на основе кода Google и провели несколько экспериментов с умными часами Huawei Watch (первое поколение), Kingwear KW88 и PYiALCY X200 на основе Android Wear 2.5 и Android 5.1 для Операционные системы SmartWatch.

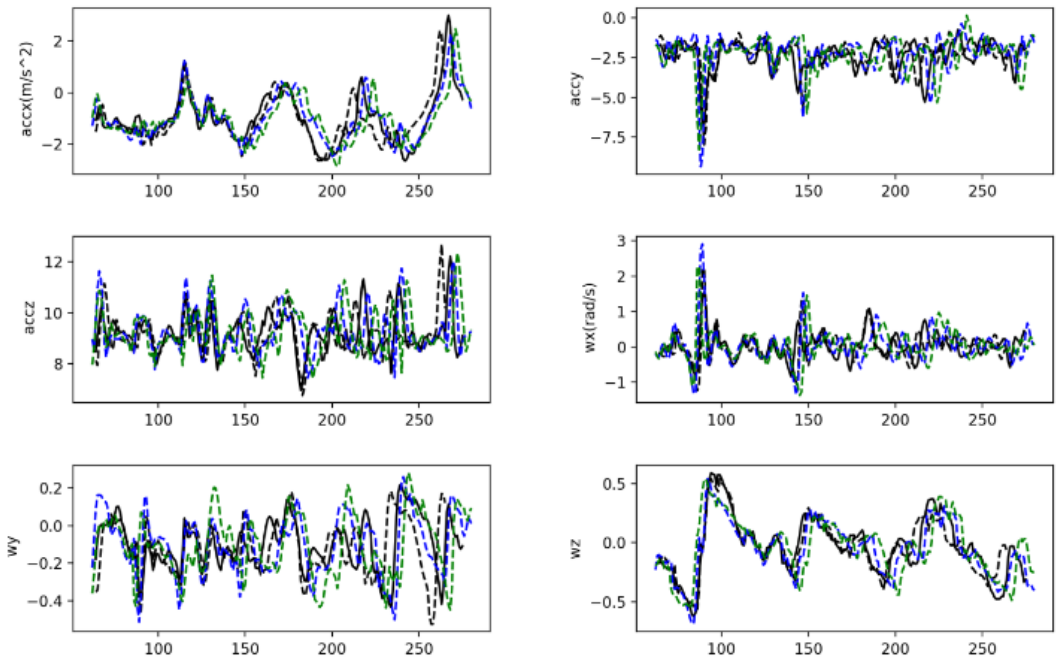
Эти часы были выбраны из-за их доступности и простоты написания приложений для них (мы предполагаем, что использование встроенного гироскопа и акселерометра в iOS пойдет по тому же пути).



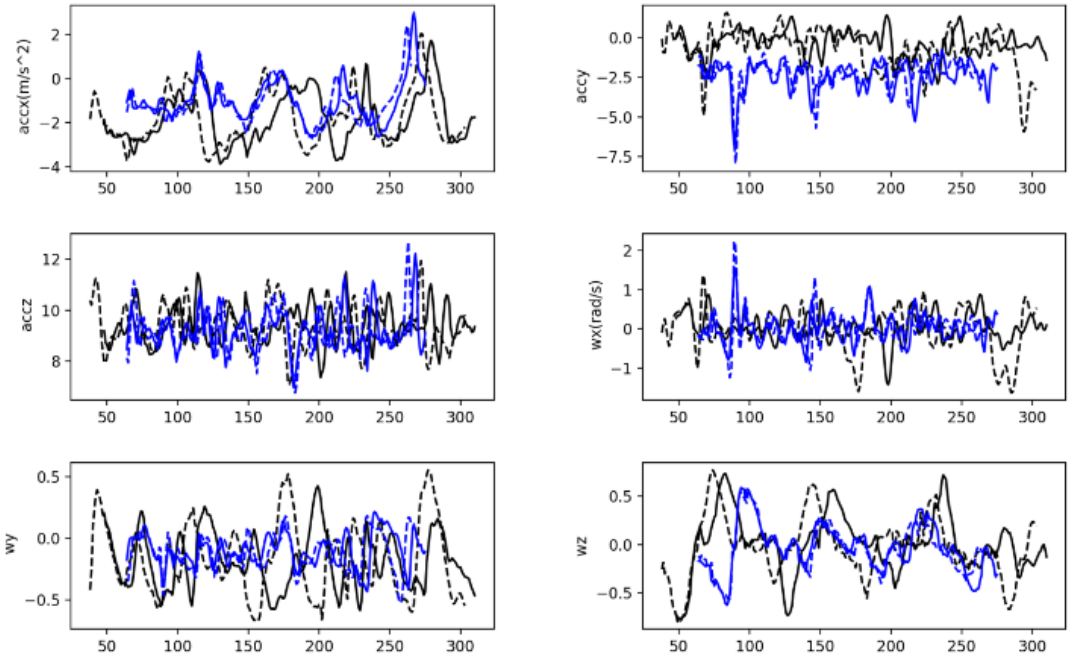
Accelerometer and gyroscope readings with decoding of areas

Это три периода ходьбы (12, 3 и 5 минут), чередующиеся с поездками на метро (20 и 24 минуты). Короткий интервал ходьбы имеет некоторые особые характеристики, поскольку он связан с переходом от одной линии метро к другой

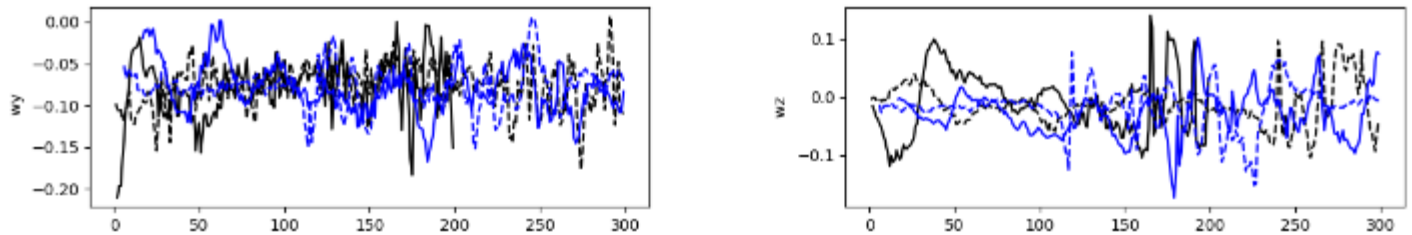
https://securelist.com/trojan-watch/85376/



Signal along the accelerometer and gyroscope axes for four attempts by one person to enter one password on a desktop computer

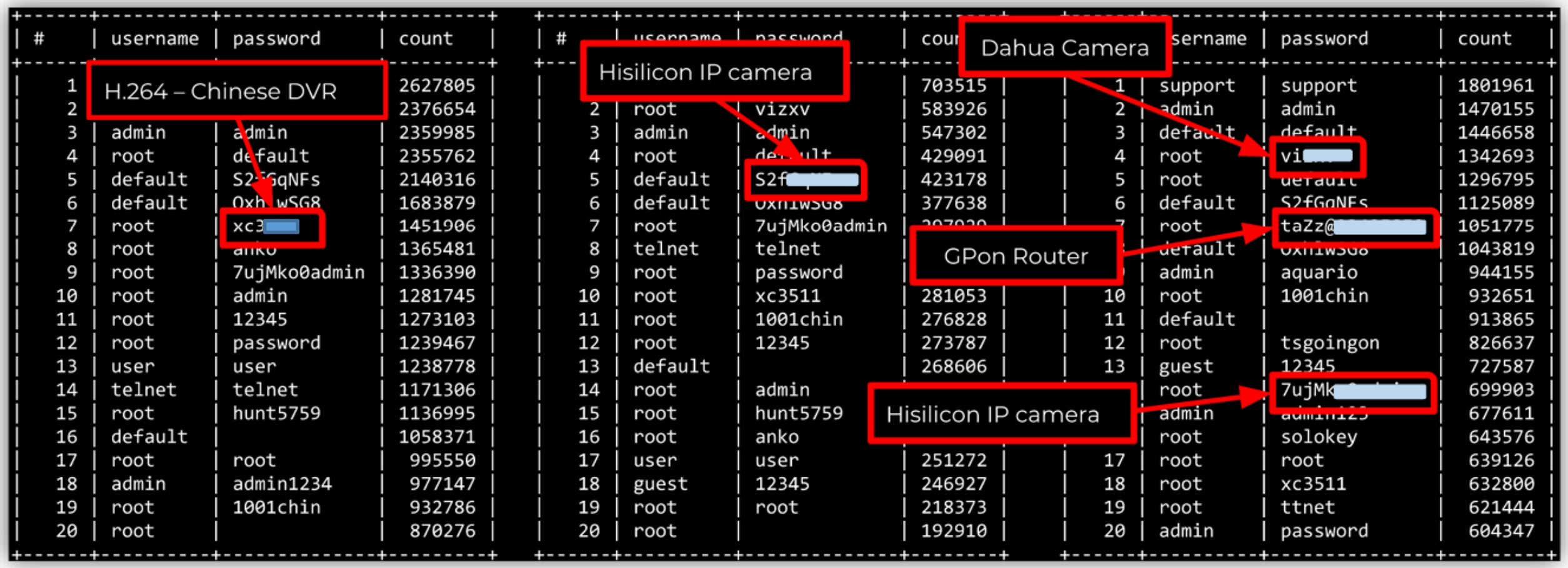


Signals along the accelerometer and gyroscope axes for attempts to enter the same password by different people on a desktop computer



Attempts to enter a smartphone unlock code by two different people

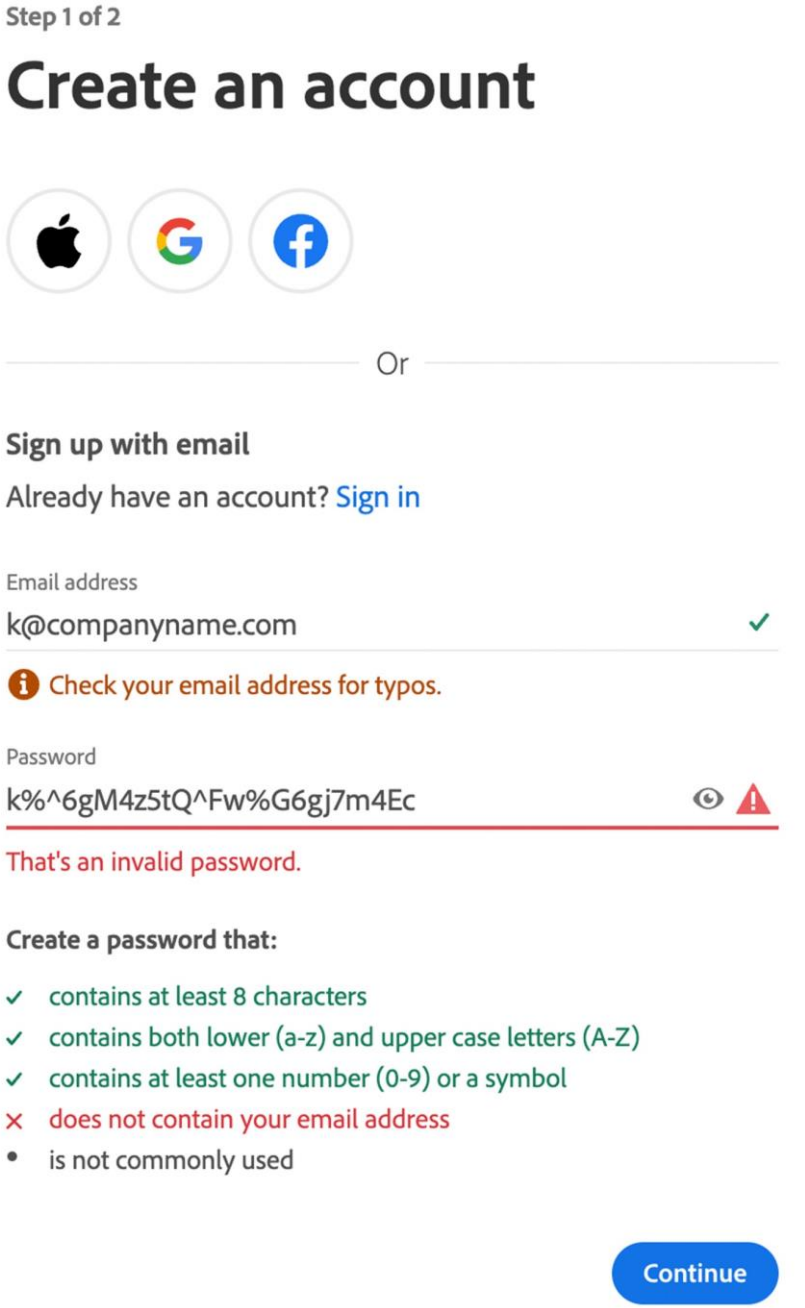
Top 20 passwords used for attacking IoT devices



#	username	password	count
1			2627805
2			2376654
3	admin	admin	2359985
4	root	default	2355762
5	default	S2fGqNFs	2140316
6	default	OxhlwSG8	1683879
7	root	xc3	1451906
8	root	anko	1365481
9	root	7ujMko0admin	1336390
10	root	admin	1281745
11	root	12345	1273103
12	root	password	1239467
13	user	user	1238778
14	telnet	telnet	1171306
15	root	hunt5759	1136995
16	default		1058371
17	root	root	995550
18	admin	admin1234	977147
19	root	1001chin	932786
20	root		870276

#	username	password	count
			703515
2	root	vizxv	583926
3	admin	admin	547302
4	root	default	429091
5	default	S2f	423178
6	default	OxhlwSG8	377638
7	root	7ujMko0admin	
8	telnet	telnet	
9	root	password	
10	root	xc3511	281053
11	root	1001chin	276828
12	root	12345	273787
13	default		268606
14	root	admin	
15	root	hunt5759	
16	root	anko	
17	user	user	251272
18	guest	12345	246927
19	root	root	218373
20	root		192910

#	username	password	count
1	support	support	1801961
2	admin	admin	1470155
3	default	default	1446658
4	root	vi	1342693
5	root	default	1296795
6	default	S2fGqNFs	1125089
7	root	taZz@	1051775
8	default	OxhlwSG8	1043819
9	admin	aquario	944155
10	root	1001chin	932651
11	default		913865
12	root	tsgoingon	826637
13	guest	12345	727587
14	root	7ujMk	699903
15	admin	admin123	677611
16	root	solokey	643576
17	root	root	639126
18	root	xc3511	632800
19	root	ttnet	621444
20	admin	password	604347

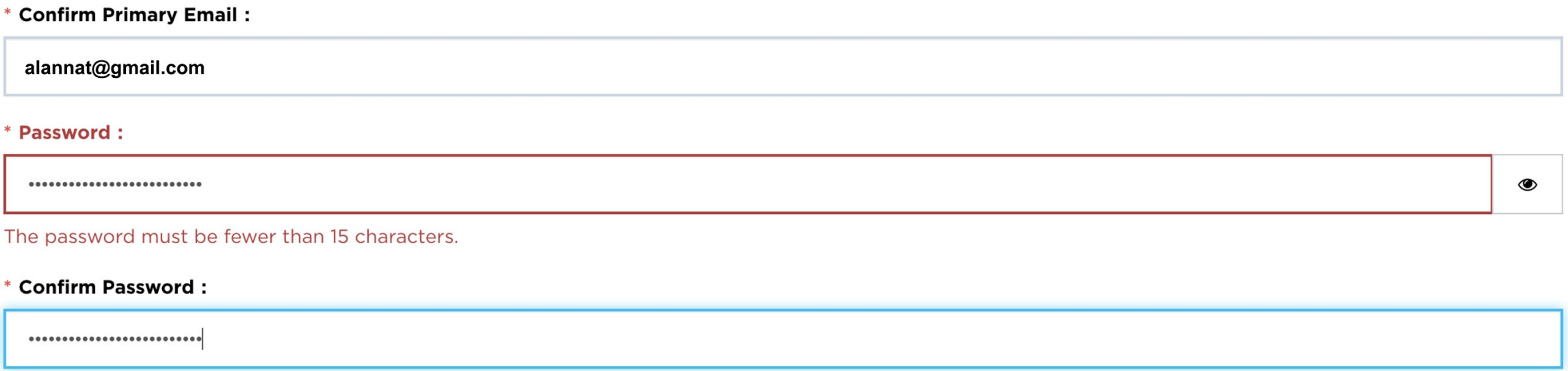


От регулярной смены паролей мало пользы

К паролям есть два требования, которые могут показаться не очень-то совместимыми. С одной стороны, чтобы надежно защитить учетную запись, нужно придумать пароль, который будет трудно подобрать. С другой стороны, этот пароль должно быть легко запомнить, иначе им невозможно будет пользоваться. Регулярная смена паролей действительно *отчасти* помогает с первым требованием, но второе делает трудновыполнимым.

Нам трудно постоянно заучивать длинные и сложные комбинации символов — мы же люди, а не роботы. Человек пытается «обмануть систему», так уж он устроен. Когда нас заставляют сменить пароль, мы не придумываем новый — мы просто немного меняем старый.

Для примера возьмем пароль *batman2018*. Если нужно будет его сменить, многие, скорее всего, просто сделают так: *batman2019*. Система воспримет этот пароль как новый, но по сути он остался тем же самым. И если старый пароль каким-то образом попадет в руки злоумышленникам, им несложно будет угадать новый.



Одна из самых вредных парольных политик — ограничение максимальной длины пароля. Не надо так!

На самом деле запоминать сложные и уникальные пароли проще, чем кажется на первый взгляд. Нужно просто знать правильный подход. Сложный на вид (и для запоминания) и сложный для взлома — это совсем не одно и то же.

К примеру, легко запоминаемый пароль *12345-vyshel-zaychik-naprimer* и страшная комбинация символов *?Y]G9gWJ48zYkFBc@{nKw!'q* обладают близкой надежностью — а на вид и не скажешь, верно? Фокус в том, что «зайчик» компенсирует все свои недостатки большей длиной.

Есть много других способов сочинить супернадежный пароль, но я хочу остановиться на том, который позволяет сочинять нужную комбинацию, используя ассоциации.

1. Вспомните фразу, строку из песни, цитату из фильма или же детскую колыбельную — то, что для вас много значит.
2. Запишите первые буквы из первых пяти слов.
3. Добавьте по одному специальному символу между каждой буквой.

На этом этапе у вас готова базовая комбинация, дополнив которую вы сможете сочинять бесконечное количество уникальных паролей. Осталось только понять, как использовать ассоциации, чтобы запомнить по одному паролю для каждого сайта.

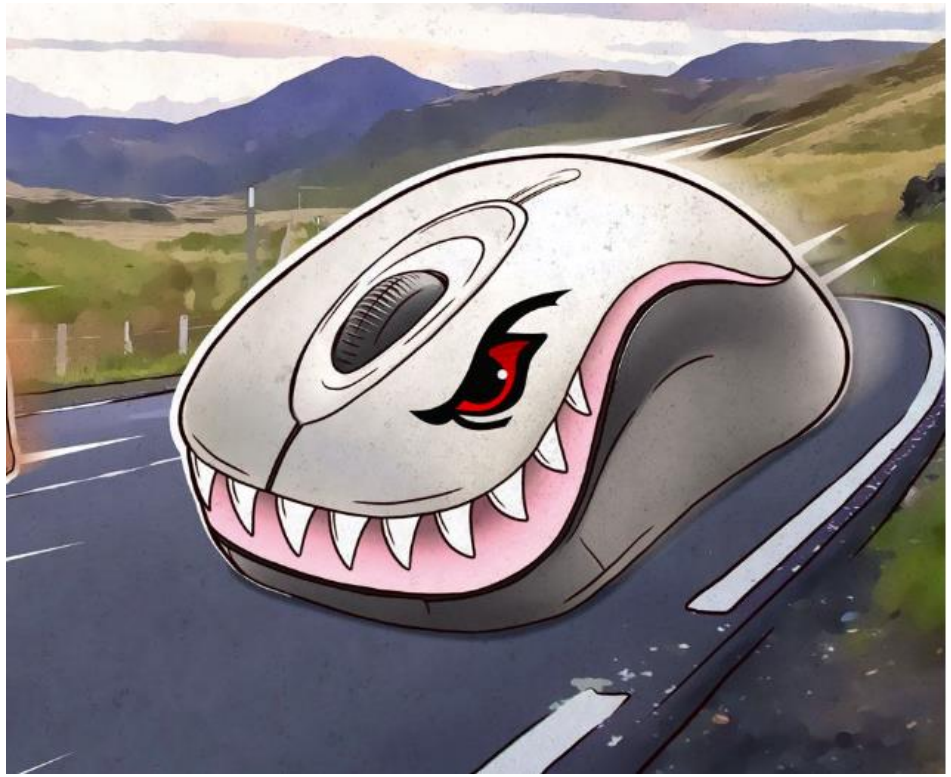
Таким образом, если в качестве ассоциативной фразы взять забавную строку «Twinkle Twinkle Little Star How I Wonder What You Are», а в качестве специального символа выбрать любимый знак всех любителей Твиттера и Инстаграма — «#», то пароль к Facebook будет «T#T#L#S#Hblue». Сочетание символов кажется бессмысленным любому постороннему человеку, но поскольку вы знаете систему и связанные с сайтом ваши личные ассоциации, то вам этот пароль покажется легким и понятным.

HOW LONG WILL IT TAKE TO CRACK YOUR PASSWORD

number of Characters	Numbers only	Upper or lower case letters	upper or lower case letters mixed	numbers, upper and lower case letters	numbers, upper and lower case letters, symbols
3	Instantly	Instantly	Instantly	Instantly	Instantly
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	3 secs	10 secs
6	Instantly	Instantly	8 secs	3 mins	13 mins
7	Instantly	Instantly	5 mins	3 hours	17 hours
8	Instantly	13 mins	3 hours	10 days	57 days
9	4 secs	6 hours	4 days	1 year	12 years
10	40 secs	6 days	169 days	106 years	928 years
11	6 mins	169 days	16 years	6k years	71k years
12	1 hour	12 years	600 years	108k years	5m years
13	11 hours	314 years	21k years	25m years	423m years
14	4 days	8k years	778k years	1bn years	5bn years
15	46 days	212k years	28m years	97bn years	2tn years
16	1 year	512m years	1bn years	6tn years	193tn years
17	12 years	143m years	36bn years	374tn years	14qd years
18	126 years	3bn years	1tn years	23qd years	1qt years

TIME IT TAKES A HACKER TO BRUTE FORCE YOUR PASSWORD IN 2023

Number of Characters	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	Instantly	Instantly
6	Instantly	Instantly	Instantly	Instantly	Instantly
7	Instantly	Instantly	2 secs	7 secs	31 secs
8	Instantly	Instantly	2 mins	7 mins	39 mins
9	Instantly	10 secs	1 hour	7 hours	2 days
10	Instantly	4 mins	3 days	3 weeks	5 months
11	Instantly	2 hours	5 months	3 years	34 years
12	2 secs	2 days	24 years	200 years	3k years
13	19 secs	2 months	1k years	12k years	202k years
14	3 mins	4 years	64k years	750k years	16m years
15	32 mins	100 years	3m years	46m years	1bn years
16	5 hours	3k years	173m years	3bn years	92bn years
17	2 days	69k years	9bn years	179bn years	7tn years
18	3 weeks	2m years	467bn years	11tn years	438tn years

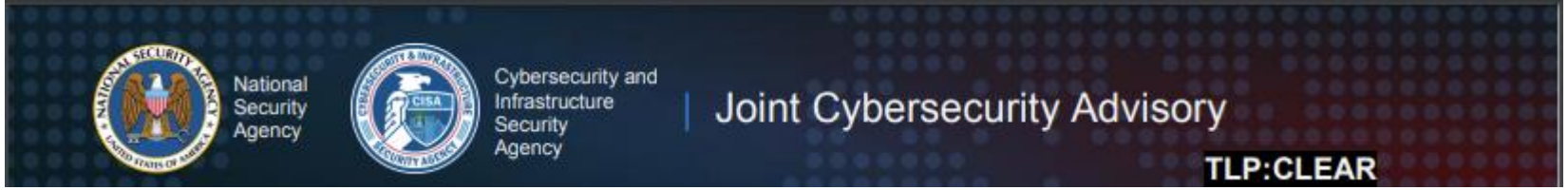


Но недавно произошел реальный случай. Сотрудник промышленного предприятия скачал фильм «Ла-Ла Ленд» на флешку. В итоге в изолированную сеть атомной электростанции попало вредоносное ПО.

Третье поколение USB-устройств, тестирующих системы на проникновение, — это уже совершенно другой уровень. Один из таких инструментов — WHID Injector. По сути, это Rubberducky с возможностью удаленного подключения. Благодаря поддержке Wi-Fi его уже не надо заранее программировать на определенный род деятельности: преступник может управлять устройством дистанционно, что дает ему возможность действовать по ситуации и работать в разных операционных системах.

Для защиты критически важной инфраструктуры следует использовать многоуровневый подход.

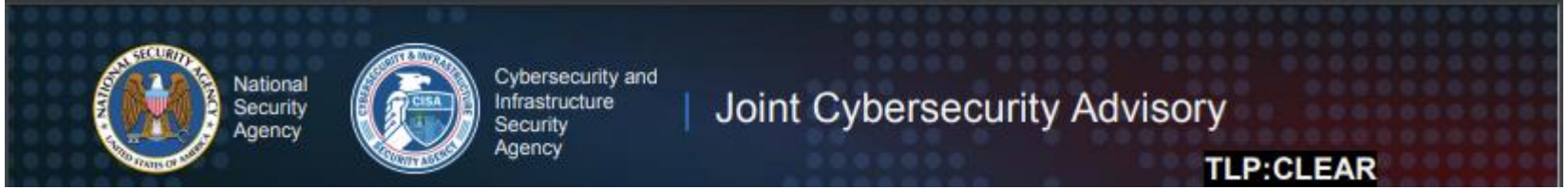
- Во-первых, обеспечьте безопасность на физическом уровне, чтобы посторонний не смог подключить USB-устройство к системе управления. Заблокируйте неиспользуемые USB-порты физически, также желательно исключить возможность извлечения уже подключенных HID-устройств.
- Проинструктируйте сотрудников, чтобы они были в курсе возможных угроз, в том числе со стороны вредоносных USB-устройств (как, например, в инциденте с «Ла-Ла Ленд»).
- Сегментируйте сеть и сконфигурируйте права доступа таким образом, чтобы злоумышленники не смогли добраться до систем управления критически важной инфраструктурой.



Самые типичные ошибки, которые встречали специалисты CISA и АНБ, разгребая инциденты и проводя аудиты в крупных американских организациях. Список применим к неамериканским или некрупным организациям на 100%.

1 Конфигурация приложений по умолчанию

Любое устройство или приложение, будь то файлообменник, принтер, почтовый сервер, система конференц-связи, часто содержит стандартные реквизиты доступа, которые забывают отключать и избыточно мягкие настройки, которые никто не меняет. Типичными примерами могут быть принтер, имеющий привилегированный сетевой доступ для удобства печати и веб-админку, или корпоративный сервер, где не отключили старые версии SMB. Весьма опасны стандартные настройки Active Directory Certificate Services, позволяющие выдать непривилегированному юзеру серверный сертификат или авторизоваться, получив TGT.



2 Неверное управление привилегиями пользователей и админов

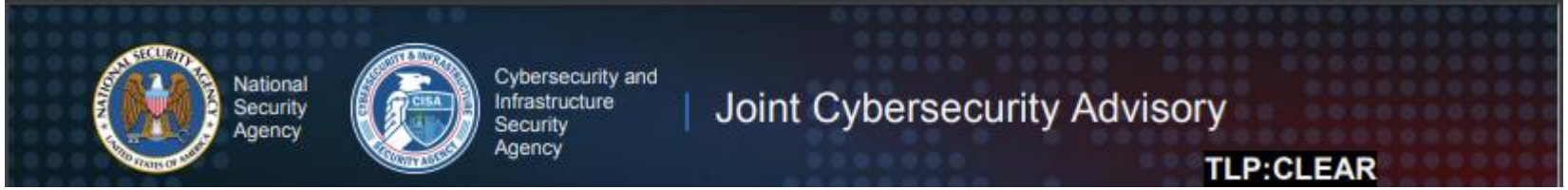
Наиболее типичные проблемы — избыточные права у обычных пользователей (постепенно полученные для каких-то временных нужд, но потом не отозванные), расширенные привилегии сервисных аккаунтов, а также высокие привилегии у админов, с которыми они работают постоянно. Атакующие целенаправленно выискивают такие привилегированные аккаунты, это сильно ускоряет им захват сети.

3 Недостаточный мониторинг внутренней сети

Во многих организациях отслеживается трафик только со внешних хостов и на избранных серверах, а во внутренней сети всё ограничивается мониторингом событий на конечных точках. Это затрудняет своевременное обнаружение атак и расследование инцидентов.

4 Отсутствие сетевой сегментации

Сети с различным назначением и уровнем важности зачастую не отделены друг от друга. Типичными проблемами являются полная взаимосвязь сетей с секретной и несекретной информацией, а также ИТ-сети и сети АСУ ТП. Иногда сегментация изначально существовала, но потом была случайно или «временно» нарушена — в организациях регулярно обнаруживается доступ к промышленной сети, которая по мнению ИТ и ИБ полностью изолирована от внешнего воздействия.

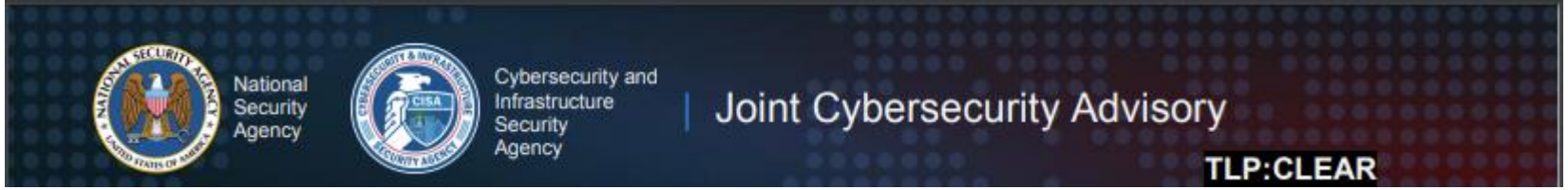


5 Низкая культура патч-менеджмента

Систематической проблемой является медленное и неполное применение патчей и обновлений. Рекомендовано в приоритетном порядке закрывать критические уязвимости и уязвимости, активно эксплуатируемые атакующими. Вторая, даже не проблема, а беда — в строю остаются многочисленные системы с глубоко устаревшими версиями ОС и приложений.

6 Возможность обойти контроль доступа

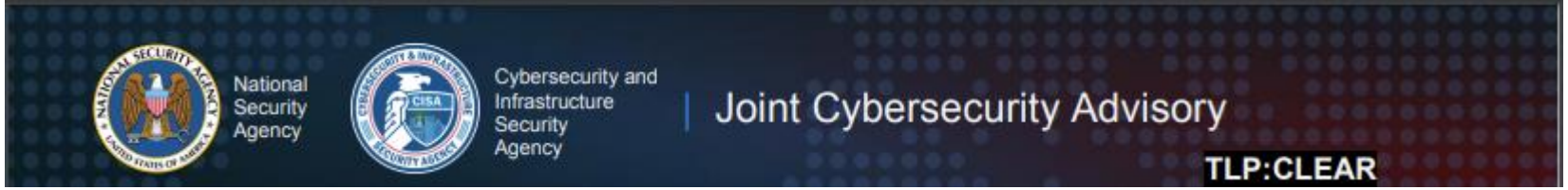
Настройки среды и приложений часто позволяют использовать такие атаки, как pass-the-hash и kerberoasting для доступа к нужным ресурсам без знания пароля.



7 Слабые или неверно настроенные методы MFA

Типовой ошибкой является такая настройка доступа, что аутентификация осуществляется только по смарт-карте, однако хэши для давно неиспользуемых паролей всё ещё считаются верными. Если не настроена политика устаревания хэшей, атакующие могут работать от имени данного аккаунта при помощи техник из п.6.

Другая распространенная проблема — методы MFA, недостаточно устойчивые к фишингу, например SMS-коды. Получать коды злоумышленники могут разными способами — от социальной инженерии и MFA-бомбардировки до атаки телеком-сети SS7 или нелегитимного дублирования SIM-карт.



Недостаточное ограничение доступа к сетевым папкам и сервисам

В корпоративных сетях регулярно обнаруживаются сетевые папки, к которым можно получить доступ без аутентификации или же административные хранилища, доступные обычным пользователям. На них нередко находятся в открытом виде файлы с паролями админов или другая важная информация.

Полный документ https://media.defense.gov/2023/Oct/05/2003314578/-1/-1/0/JOINT_CSA_TOP_TEN_MISCONFIGURATIONS_TLP-CLEAR.PDF

44 страницы включает TTP злоумышленников и мапинги MITRE ATT&CK

СПАСИБО!

Андрей Ярных

Yarnikh@gmail.com