Кибербезопасность IoT и систем видеонаблюдения: подход «Лаборатории Касперского»

Марат Нуриев
Менеджер по развитию бизнеса
KasperskyOS в направлении IoT

kaspersky

Вызовы для кибербезопасности: рост количества угроз

1998	50 угроз в день
2008	15 000 угроз в день
2020	> 400 000 угроз в день

kaspersky

Вызовы для кибербезопасности: рост количества угроз

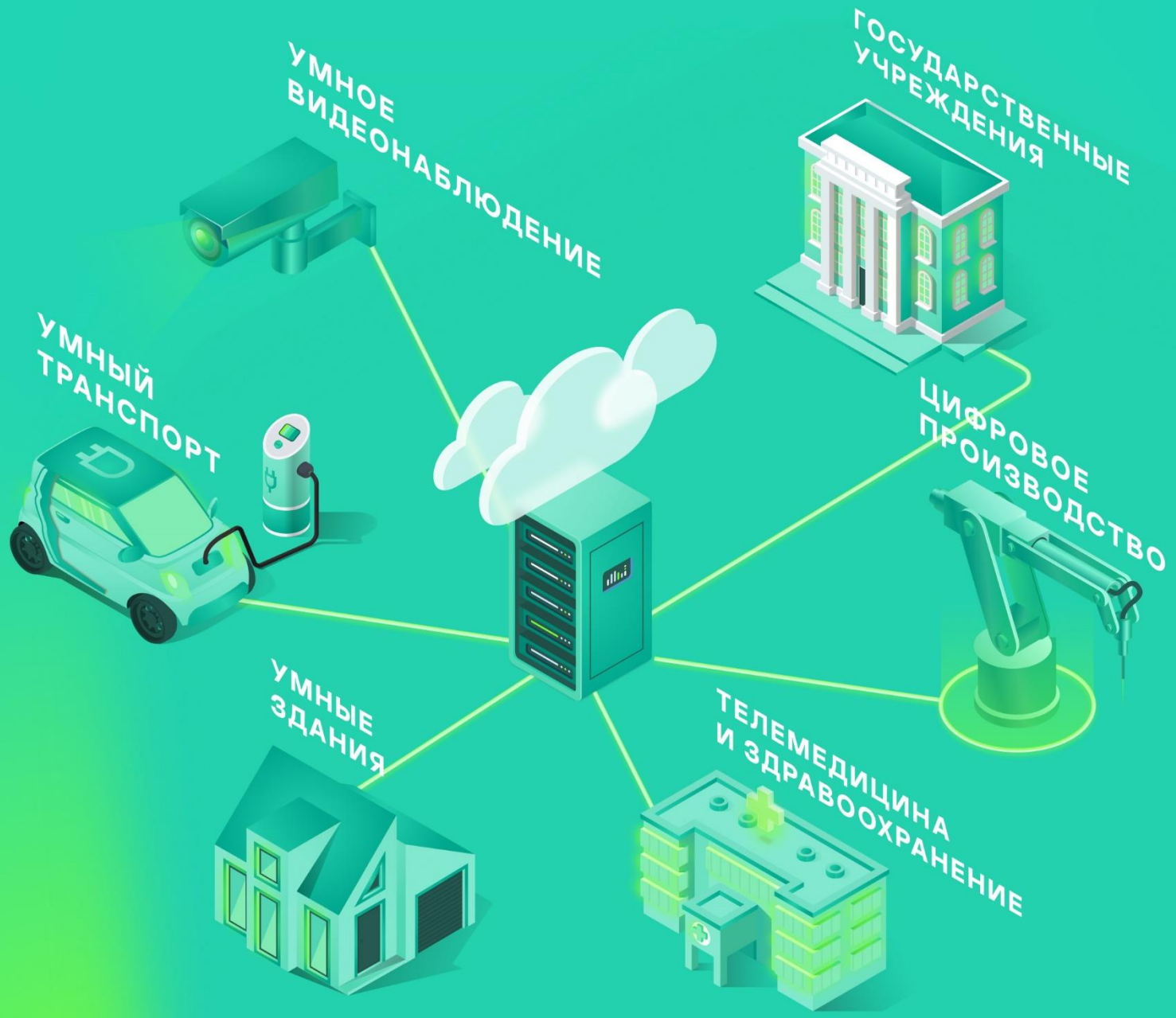
1998	50 угроз в день
2008	15 000 угроз в день
2020	> 400 000 угроз в день

Количество защитных технологий постоянно растет		
- AntiVirus / signatures / SRC checker / … - application behavior blocker - system behavior blocker - whitelisting - …	- anonymizer - device control - script checker - URL filtering - statistic analyzer - IM antivirus - secure payment - Web antivirus - …	- anti-DDOS - anti-spam - anti-phishing - parental control - update control - firewall - sandboxing - …

Несмотря на все усилия, индустрия не справляется с возрастающим потоком угроз

kaspersky

IoT — одна из основ цифровой трансформации



Уязвимости в библиотеках для встраиваемых устройств

Обнаружена компанией JSOF в июне 2020 года

- Затрагивает по всему миру миллионы устройств, использующих сетевую библиотеку **Trek** для стека TCP/IP
- Trek TCP/IP была разработана в 1990-х гг.
- Большинство устройств нет возможности обновить: либо они устарели, либо на них не выходят обновления

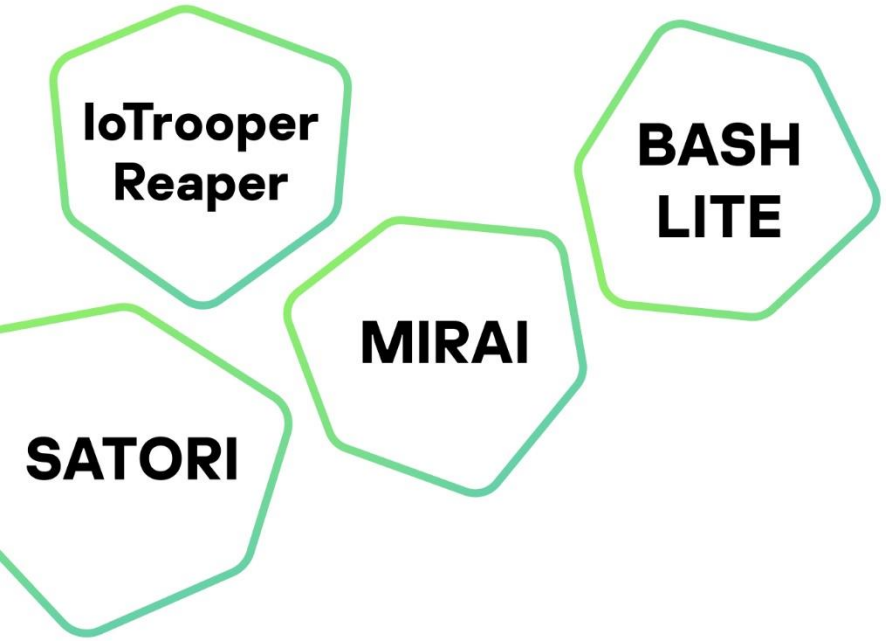
Источник: https://www.jsof-tech.com/ripple20/

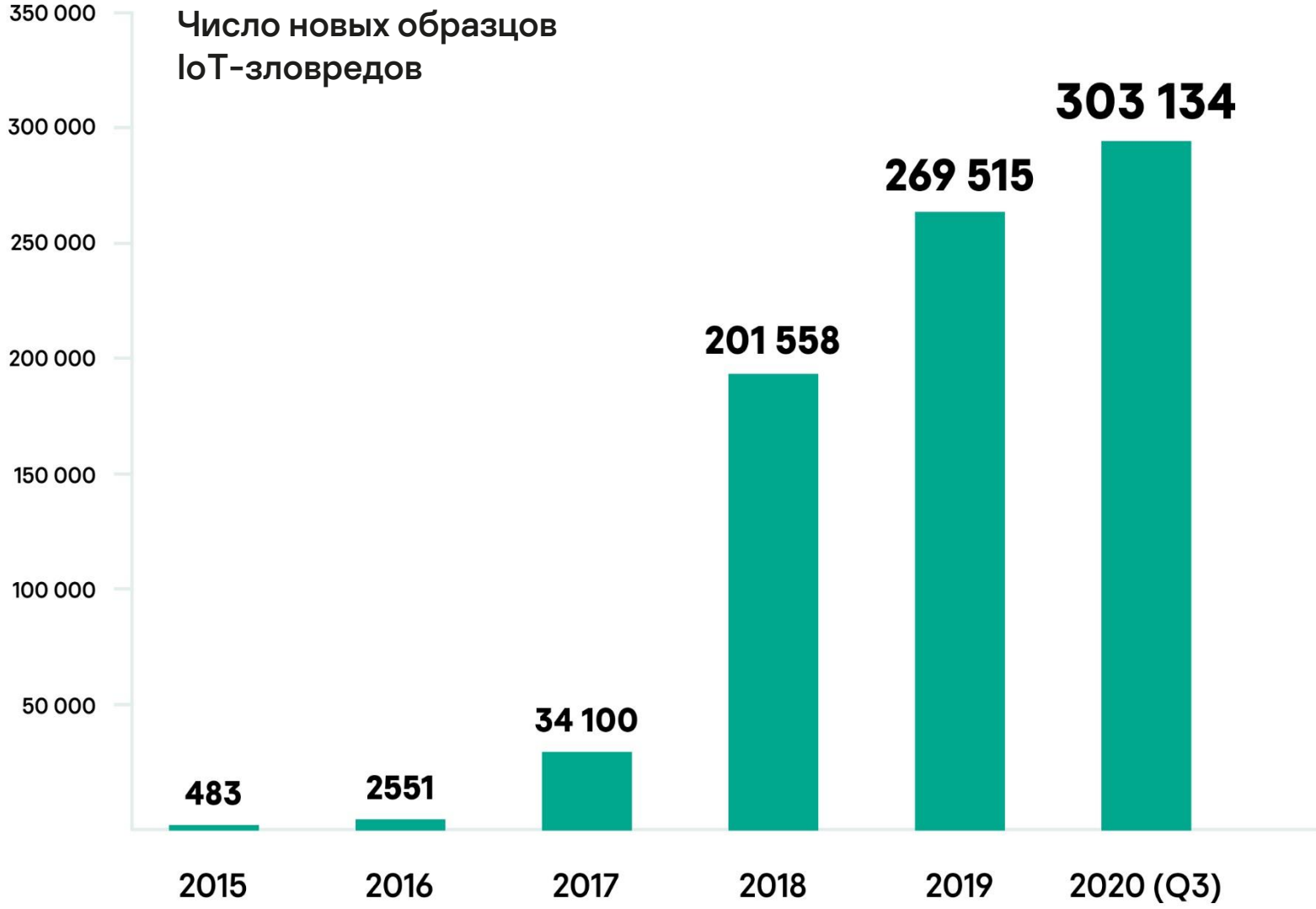
Обнаружена компанией Forescout в декабре 2020 года

- Описаны 33 новых уязвимости в четырех open source-реализациях стека TCP/IP — uIP, FNET, picoTCP и Nut/Net
- Выявленные уязвимости могут привести к удаленному выполнению кода, отказу в обслуживании, раскрытию информации
- Стеки протоколов используются в продукции 158 вендоров-производителей коммуникационных модулей, офисной оргтехники, IoT

Источник: https://www.forescout.com/research-labs/amnesia33/

Статистика по угрозам

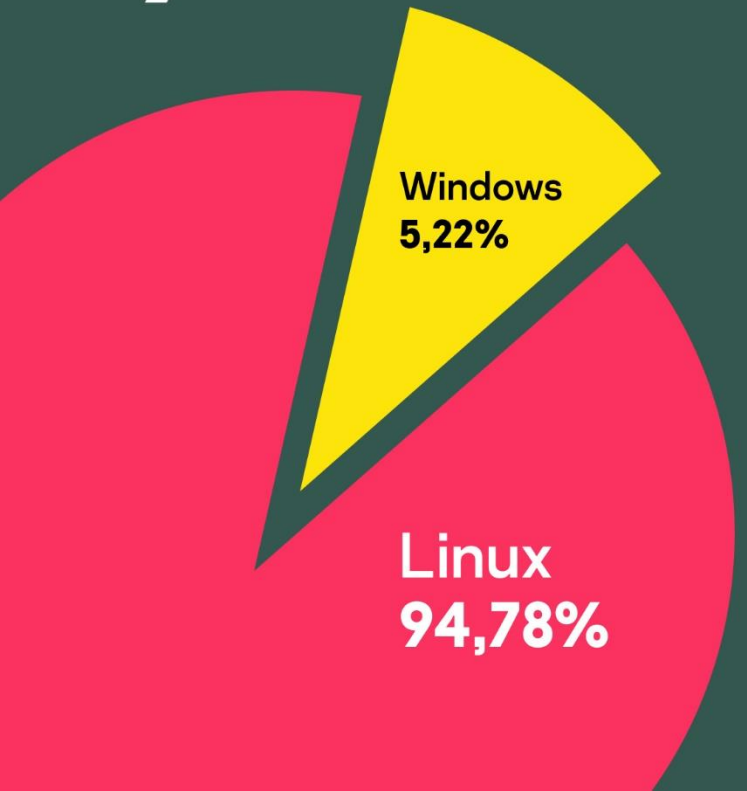




Источник: «Лаборатория Касперского»

kaspersky

9 из 10 атак на устройства IoT эксплуатируют уязвимости в Linux



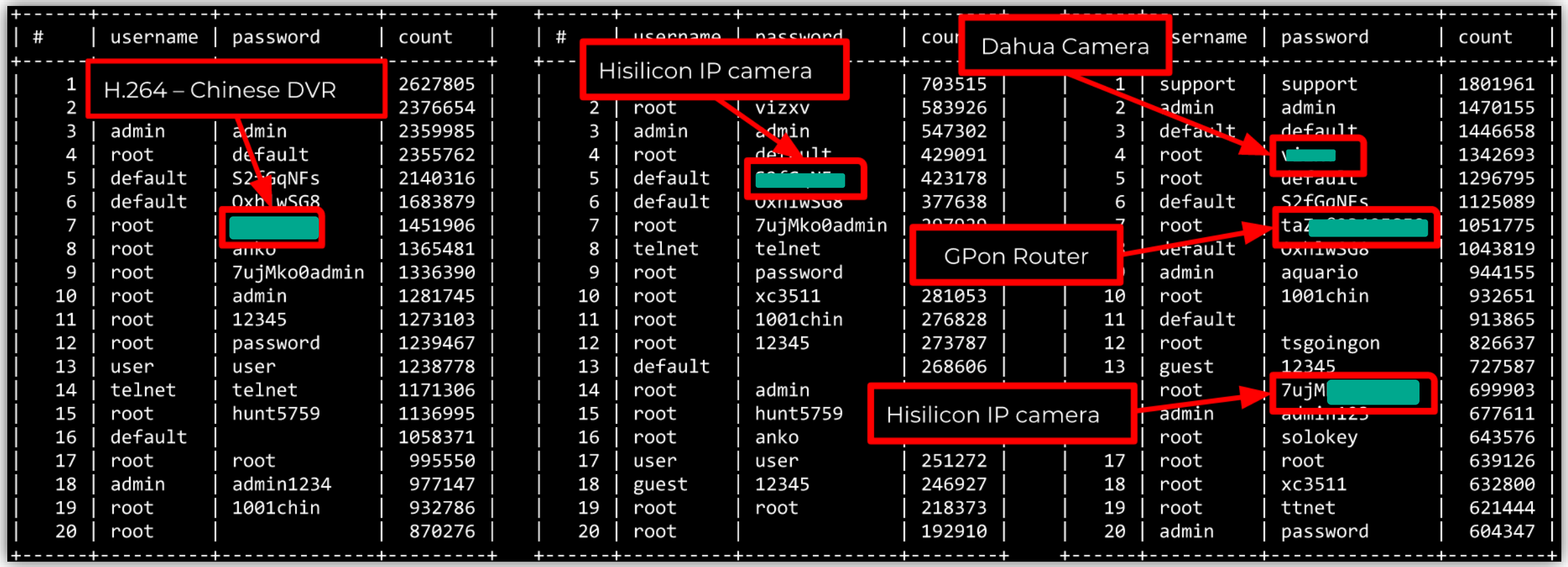
Соотношение атак устройств (ботнетов)

Топ-10 зловредов, загружаемых на зараженное IoT-устройство в результате успешной атаки

2020 (Q2)

	%	
1	**37.78**	Trojan-Downloader.Linux.NyaDrop.b
2	**17,47**	Backdoor.Linux.Mirai.b
3	**12,72**	HEUR:Backdoor.Linux.Mirai.b
4	**9,76**	HEUR:Backdoor.Linux.Gafgyt.a
5	**7,99**	Backdoor.Linux.Mirai.ba
6	**4,49**	HEUR:Backdoor.Linux.Mirai.ba
7	**2,23**	Backdoor.Linux.Gafgyt.bj
8	**1,66**	HEUR:Trojan-Downloader.Shell.Agent.p
9	**1,26**	Backdoor.Linux.Mirai.cn
10	**0,73**	HEUR:Backdoor.Linux.Mirai.c

Исследование «Лаборатории Касперского»: ТОП-20 паролей для атаки на IoT-устройства



#	username	password	count
1			2627805
2			2376654
3	admin	admin	2359985
4	root	default	2355762
5	default	S2fGqNFs	2140316
6	default	Oxhlw[redacted]	1683879
7	root	[redacted]	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

2018 – Q3

#	username	password	count
1			703515
2	root	vizxv	583926
3	admin	admin	547302
4	root	default	429091
5	default	[redacted]	423178
6	default	OxhlwSG8	377638
7	root	7ujMko0admin	[redacted]
8	telnet	telnet	[redacted]
9	root	password	[redacted]
10	root	xc3511	281053
11	root	1001chin	276828
12	root	12345	273787
13	default		268606
14	root	admin	[redacted]
15	root	hunt5759	[redacted]
16	root	anko	[redacted]
17	user	user	251272
18	guest	12345	246927
19	root	root	218373
20	root		192910

2018 – Q4

#	username	password	count
1	support	support	1801961
2	admin	admin	1470155
3	default	default	1446658
4	root	[redacted]	1342693
5	root	default	1296795
6	default	S2fGqNFs	1125089
7	root	taZ[redacted]	1051775
8	[redacted]	OxhlwSG8	1043819
9	admin	aquario	944155
10	root	1001chin	932651
11	default		913865
12	root	tsgoingon	826637
13	guest	12345	727587
14	root	7ujM[redacted]	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

2019 – Q1

Источник: https://securelist.com/iot-a-malware-story/94451/

kaspersky

Взлом систем видеонаблюдения — в ТОПе новостей

Хакеры взломали камеры видеонаблюдения в тюрьме и транслировали видео на YouTube

07:51 / 26 Декабря, 2019

государственные учреждения | хакинг | видеонаблюдение | IoT

ИСТОРИИ

Хакер случайно взломал внутреннюю сеть РЖД и получил доступ к камерам наблюдения на перронах и вокзалах

НОВОСТИ

Злоумышленники могут взломать камеры наблюдения через 0-day уязвимость Peekaboo

Мария Нефёдова , 18.09.2018 1 комментарий 7394

Взломанные частные камеры видеонаблюдения позволили хакерам создать в Москве собственную систему слежки

30.10.2020 [12:56], Геннадий Детинич

Согласно инсайду из среды хакеров, к которому получили доступ «Известия», примерно каждая одиннадцатая установленная в Москве частная камера видеонаблюдения доступна для взлома. В сумме это даёт примерно 15 000 уязвимых камер, и все они размещены либо в жилищах москвичей, либо в частных магазинах/учреждениях. Камеры в муниципальном владении защищены и недоступны для взлома. Но даже частные камеры позволяют в масштабах города легко следить за гражданами и их передвижением, уверяет источник.

kaspersky

Основные проблемы киберзащиты встраиваемых систем

Интернет вещей

kaspersky

Интернет угроз

Основные проблемы IoT/IIoT

Уязвимости в
программном обеспечении

Не проработана
архитектура безопасности

Уязвимости в
ОС общего назначения

Как решить проблему?

Создать такое окружение, которое не позволит программам исполнить недекларируемые возможности (код) и предотвратит эксплуатацию уязвимостей

Основа для создания кибериммунных IT-систем будущего

KasperskyOS

- Встроенная безопасность
- Микроядерная архитектура
- Разделение на домены безопасности
- Доверенное поведение

KasperskyOS с нуля разработана в «Лаборатории Касперского»

kaspersky

KasperskyOS: направления развития и применение

ПРИМЕНЕНИЕ:

- Интернет вещей (IoT) и умный город
- Транспорт и транспортная инфраструктура
- Промышленная инфраструктура
- Телекоммуникационное оборудование
- Инфраструктура виртуальных рабочих столов (VDI)
- Корпоративные экранные устройства для сотрудников

KasperskyOS

- Умные города, IoT, энергетика, дорожное движение
- Автомобили, автобусы, поезда
- IoT-гейтвеи, IIoT, SCADA, PLC
- Коммутаторы, маршрутизаторы, Wi-Fi, МЭ
- Тонкие клиенты
- Мобильные телефоны, планшеты
- OEM

kaspersky

Подход «Лаборатории Касперского» к защите систем видеонаблюдения

Киберриски для систем видеонаблюдения: подключение непосредственно на объекте

Для видеосервера актуальны те же угрозы, что и для любого другого устройства на Windows или Linux

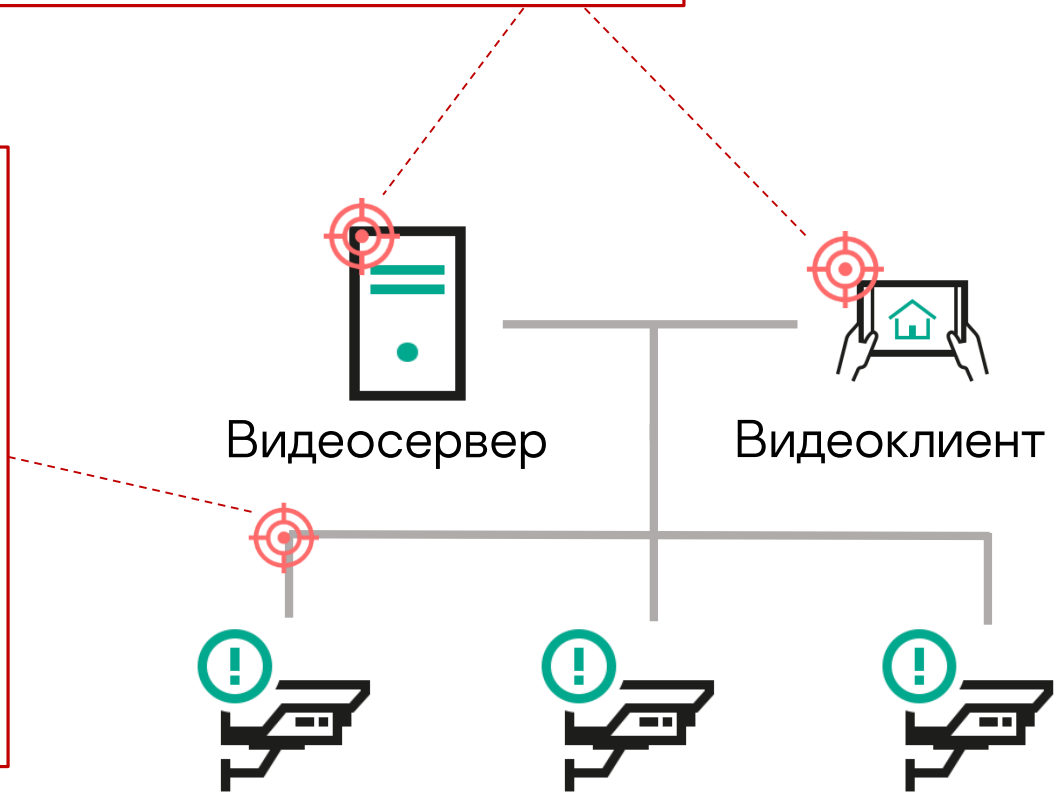
kaspersky

Киберриски для систем видеонаблюдения: подключение непосредственно на объекте

Для видеосервера актуальны те же угрозы, что и для любого другого устройства на Windows или Linux

Если получить физический доступ к камере, можно:

- Выполнить перепрошивку
- Изменить конфигурацию
- Сменить пароль
- Подделать сертификат SSL
- Установить вредоносное ПО
- Заменить SIM-карту



kaspersky


kaspersky
ADVANTECH
Kaspersky
IoT Secure
Gateway

Как решить проблемы?

Сниффинг пользовательских данных

Эксплуатация уязвимостей ПО

Доставка вредоносного ПО через съемные носители

Kaspersky IoT Secure Gateway β

Неавторизованные устройства

DDoS-атаки

Вредоносное обновление прошивок

Сканирование и вторжение в систему

Защита системы видеонаблюдения с Kaspersky IoT Secure Gateway

Обнаружение зловредной активности:

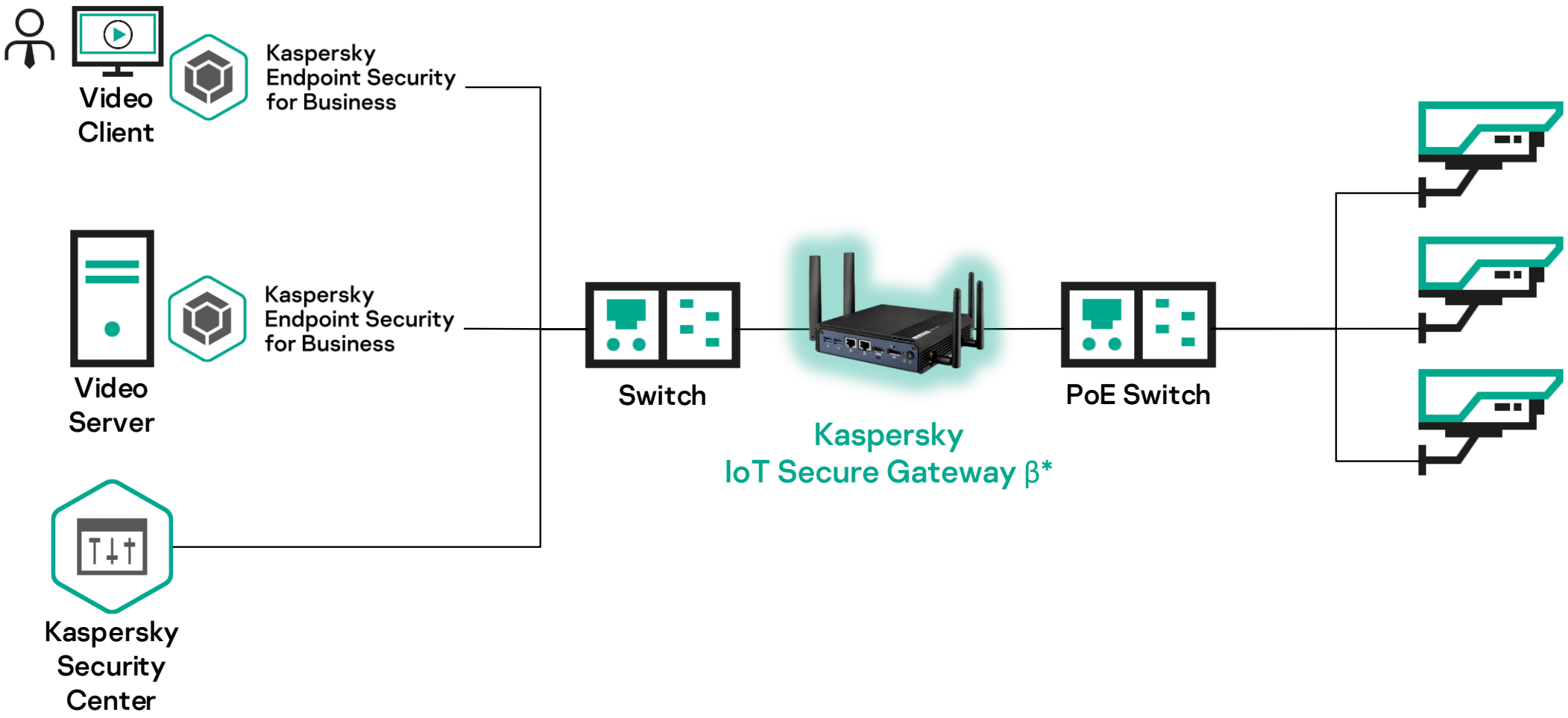
- Подключение новых устройств
- Вывод из строя камер
- Атаки на камеры со стороны видеосервера и видеоклиента
- IDS/IPS/Firewall

Разграничение доступа между видеосервером, видеоклиентом и камерами

* Данная версия продукта предназначена для некоммерческого пилотирования

kaspersky

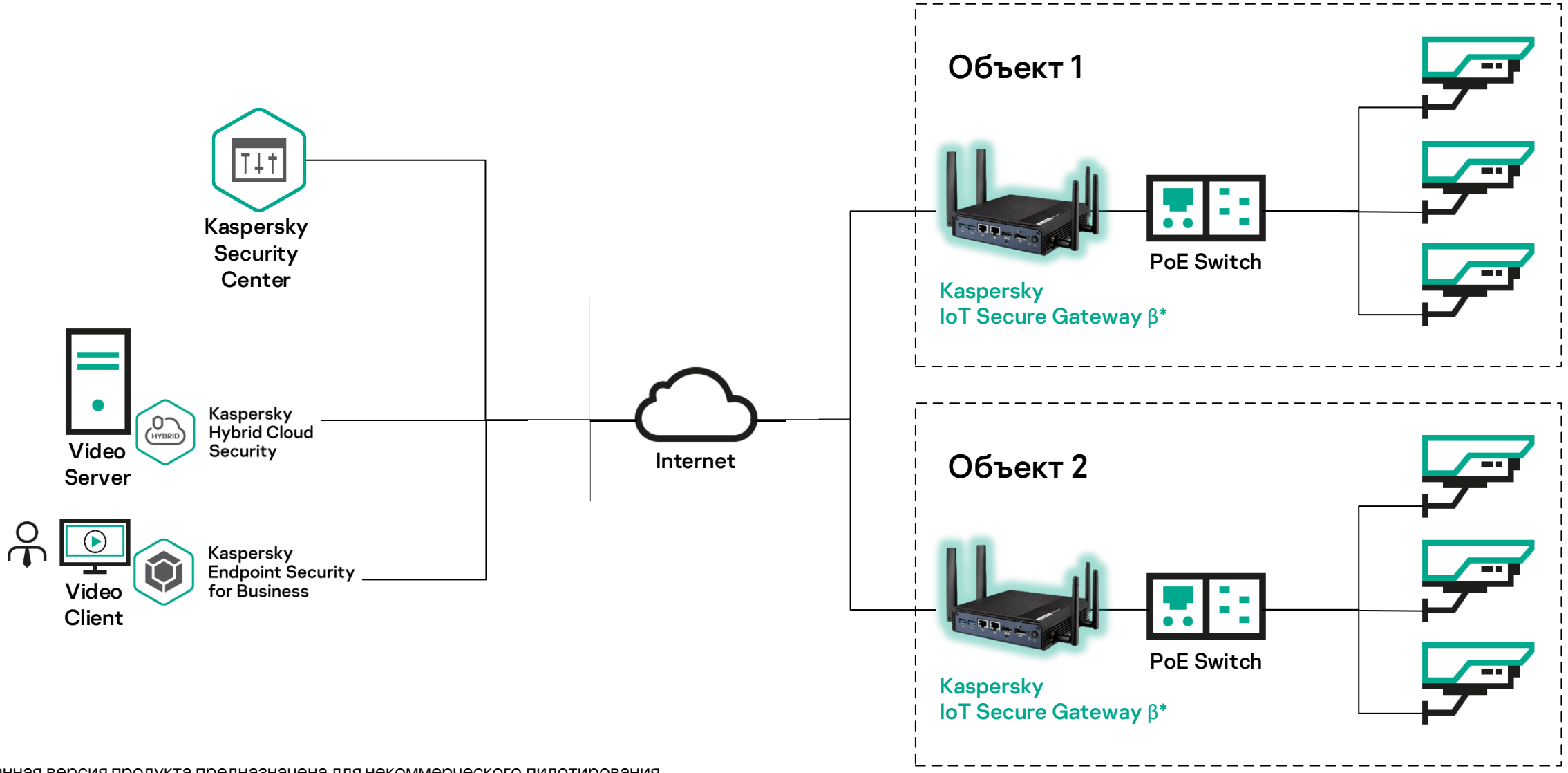
Решения «Лаборатории Касперского» для защиты систем видеонаблюдения



* Данная версия продукта предназначена для некоммерческого пилотирования

kaspersky

Решения «Лаборатории Касперского» для защиты облачных систем видеонаблюдения



* Данная версия продукта предназначена для некоммерческого пилотирования

Kaspersky IoT Secure Gateway в действии

г. Оренбург

Умный город

AXIS COMMUNICATIONS

Видеонаблюдение

НИИАС

АДАПТИВНЫЕ ПРОМЫШЛЕННЫЕ ТЕХНОЛОГИИ

Промышленный IoT

Спасибо за внимание!

https://os.kaspersky.ru/

Sales-KasperskyOS@kaspersky.com

kaspersky