TREND MICRO™ | research

Аналитическое исследование Trend Micro по киберугрозам за первое полугодие 2022 г.

Бахтияр Баймагамбет

Региональный представитель Тренд Майкро

в Центральной Азии

Trend Micro Казахстан

Представительство в Астане и Алматы

Свыше 120 государственных учреждений,

50 коммерческих клиентов и более 10 нац.компаний.

Гос.программа «Киберщит»

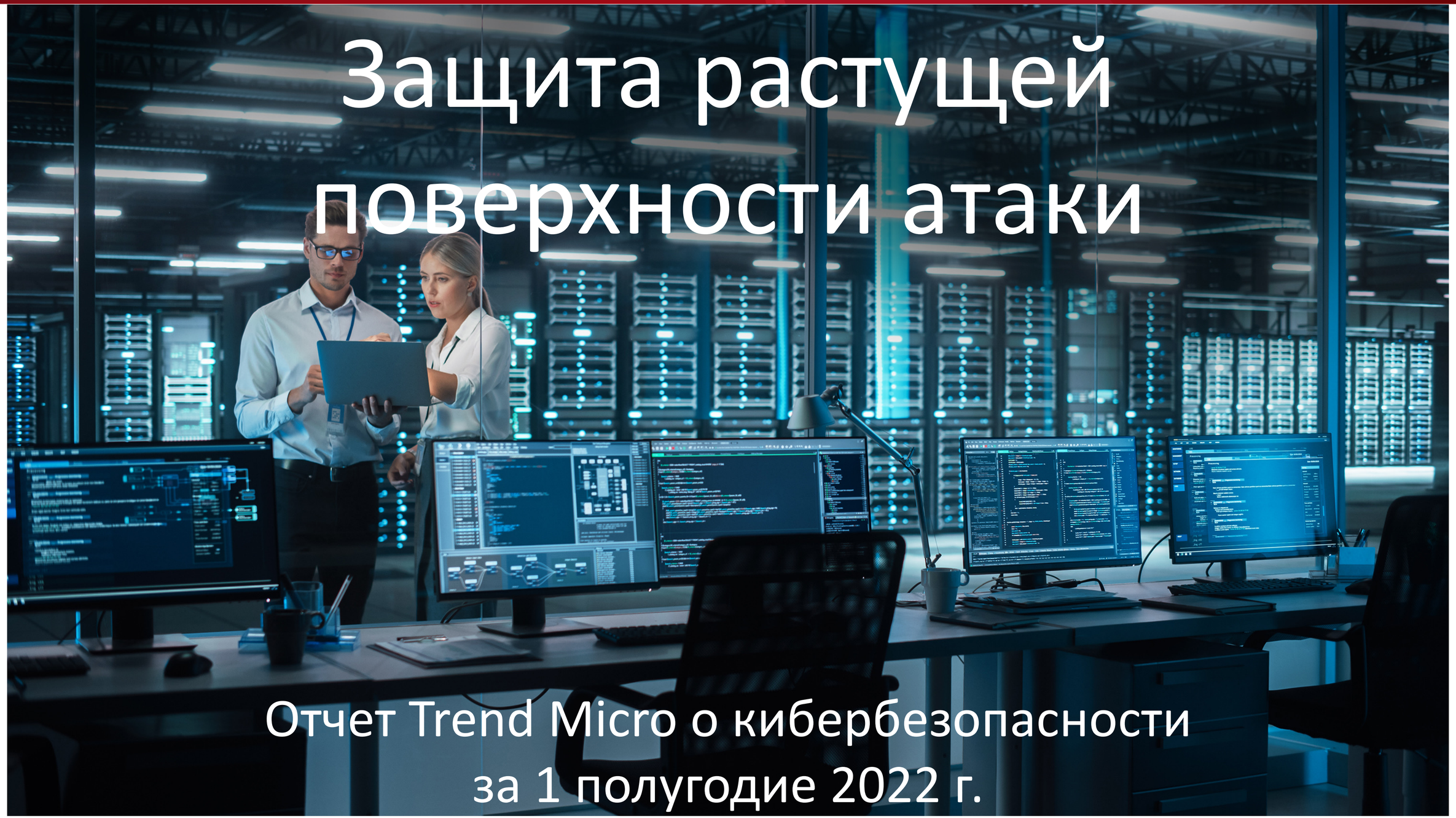
Наличие опыта построения ОЦИБ

Инженерный ресурс в Астане и Алматы

Локальная техническая поддержка 24*7*365

Результаты за 5 лет в Казахстане

Защита растущей поверхности атаки



Отчет Trend Micro о кибербезопасности за 1 полугодие 2022 г.

Сбор аналитической информации о поверхности атаки

400 000 коммерческих и 20 млн частных клиентов

TREND MICRO | research

Поверхность атаки тревожит специалистов

73% of IT security decision makers are concerned about the digital attack surface.

43% argue that the attack surface is spiraling out of control.

37% describe the attack surface as constantly evolving and messy.

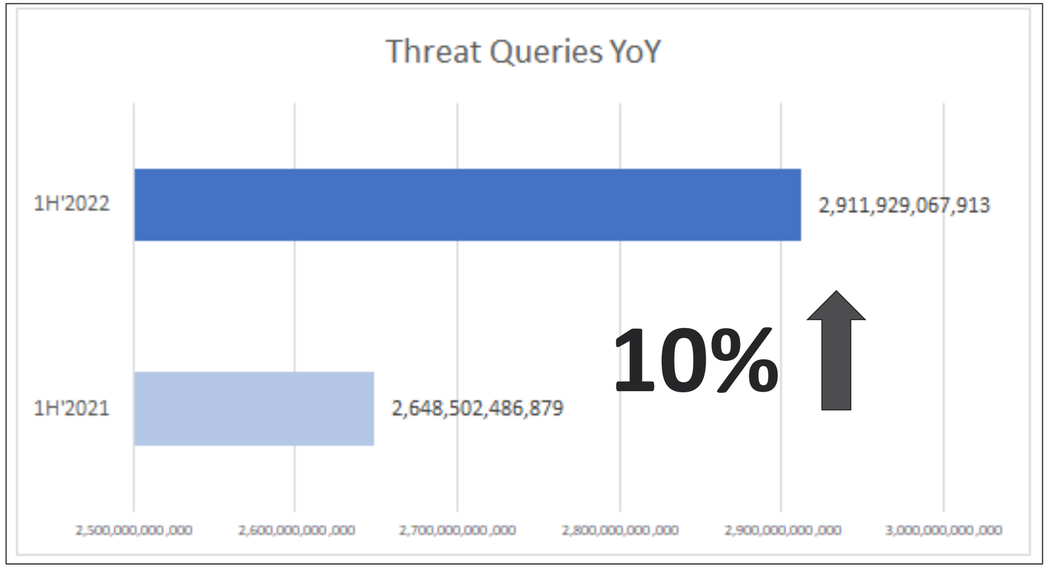
Areas where organizations have the least security insight into

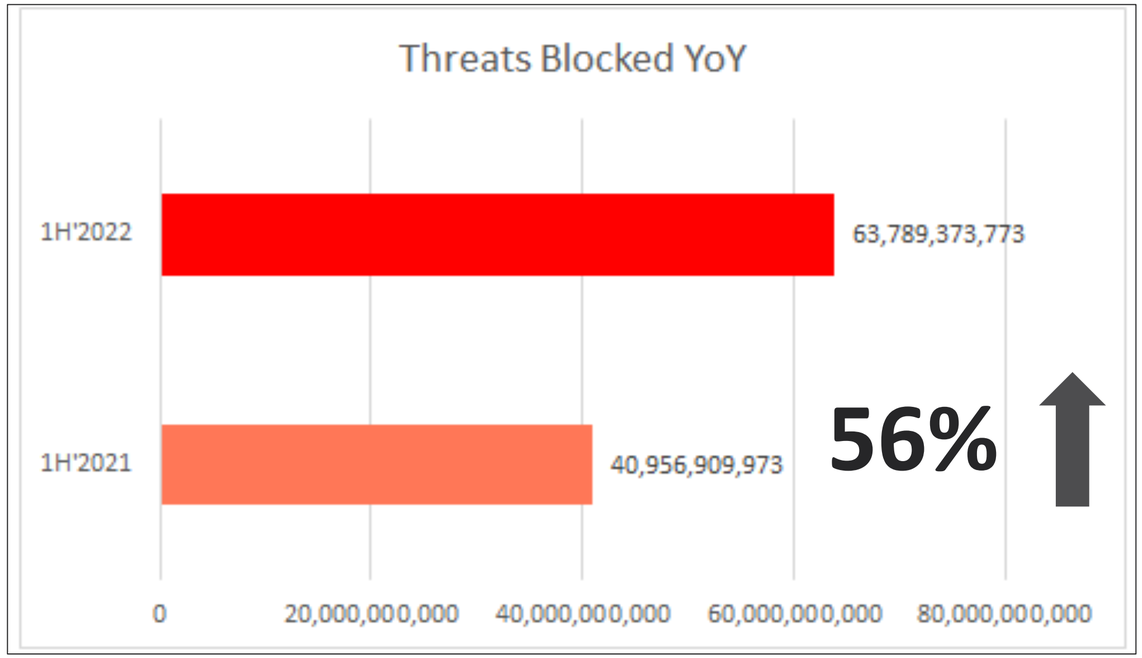
37% Cloud assets

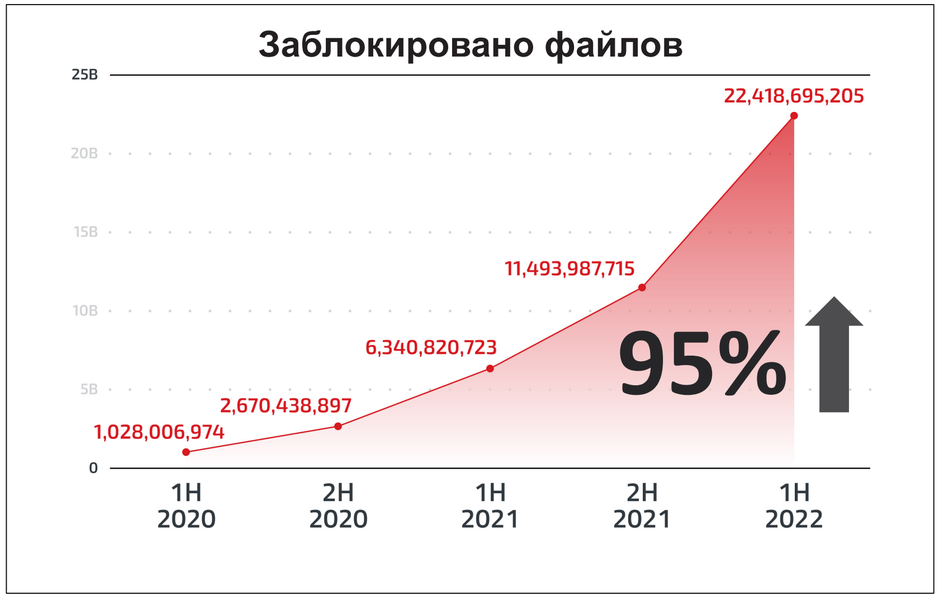
34% Networks

32% End-user assets

Данные об угрозах по годам







TREND MICRO | research

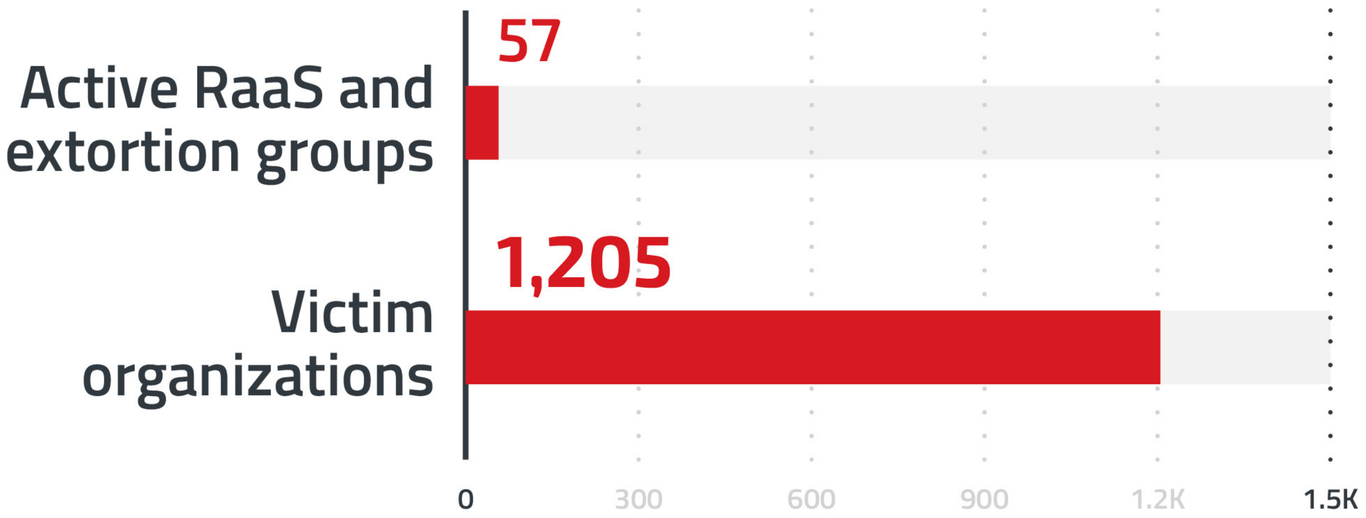
TREND MICRO | research

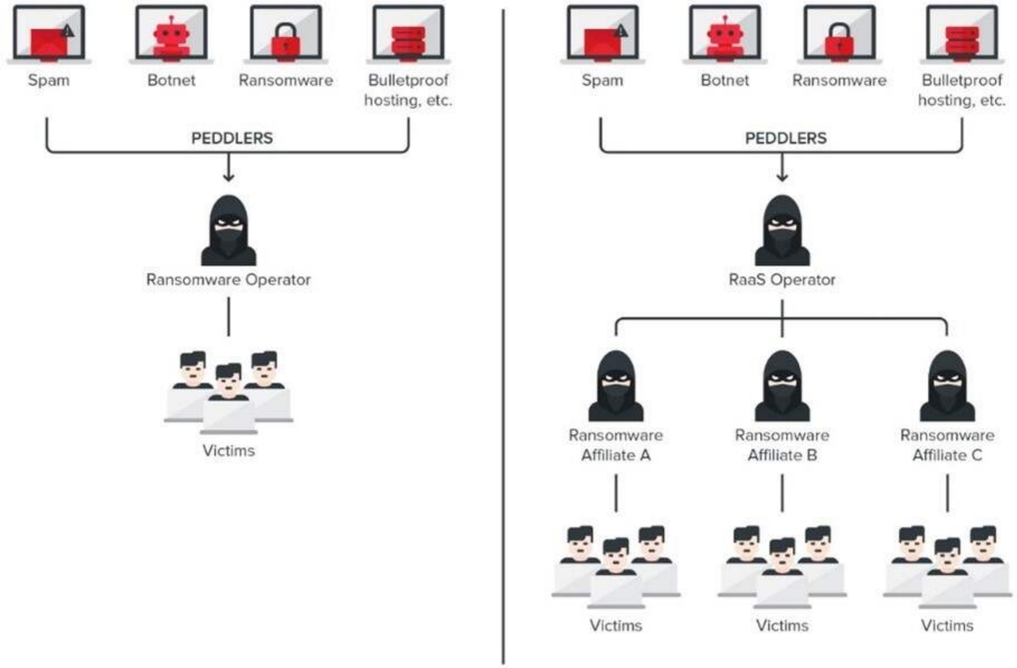
RANSOMWARE

Ландшафт угроз, связанных с программами-вымогателями, продолжает развиваться: появляются новые игроки и прибыльные методы монетизации

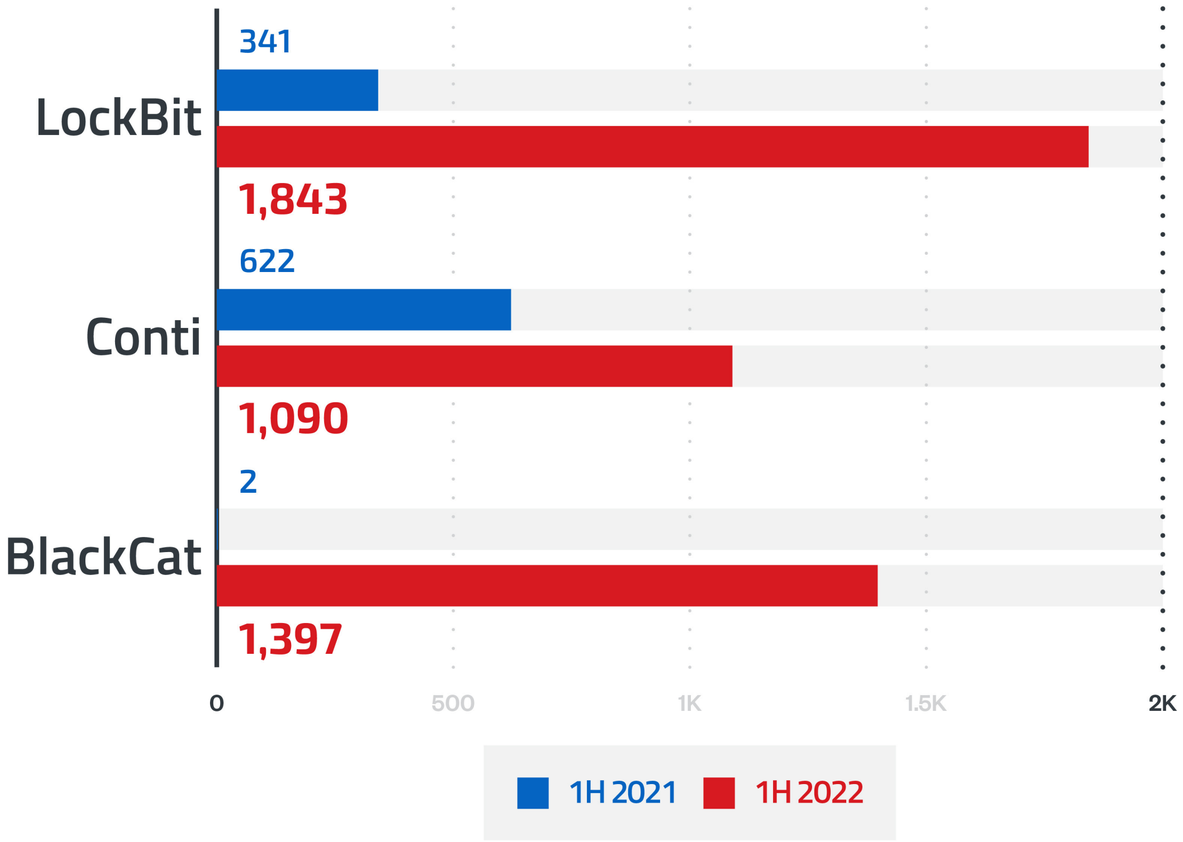
Отчет Trend Micro о кибербезопасности за 1 полугодие 2022 г.

Программы-вымогатели: изменения



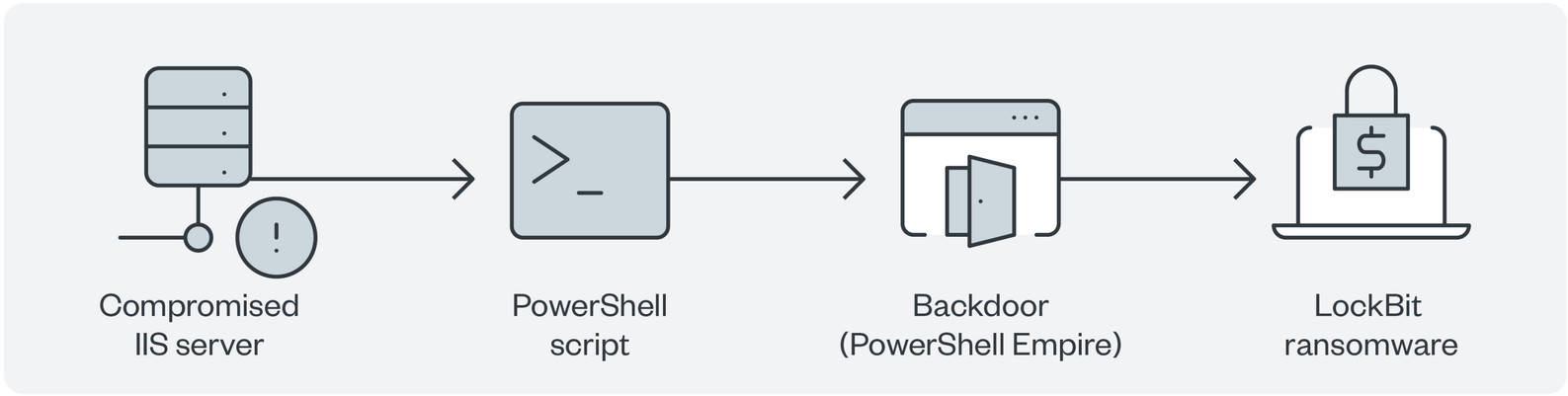


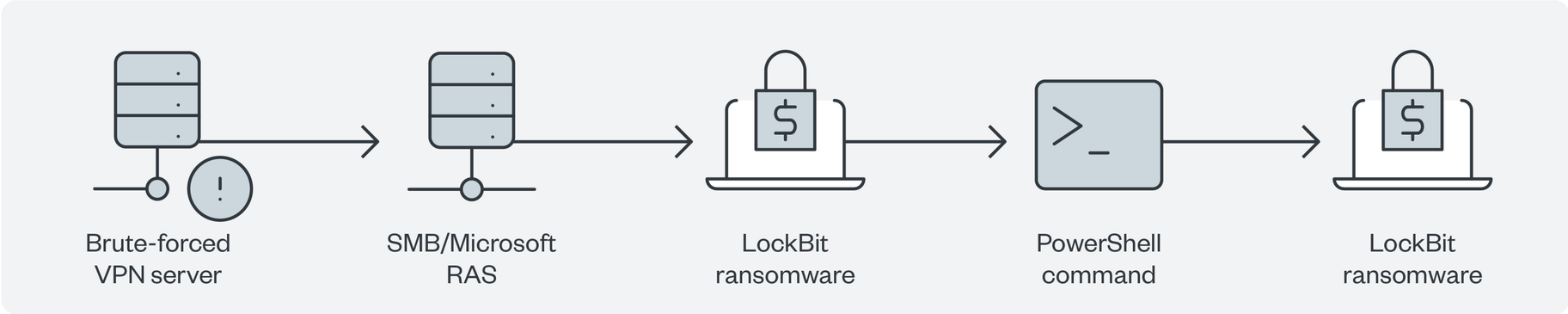
Группы программ-вымогателей



В первой половине 2022 г. основными игроками на рынке RaaS были LockBit, Conti и BlackCat.

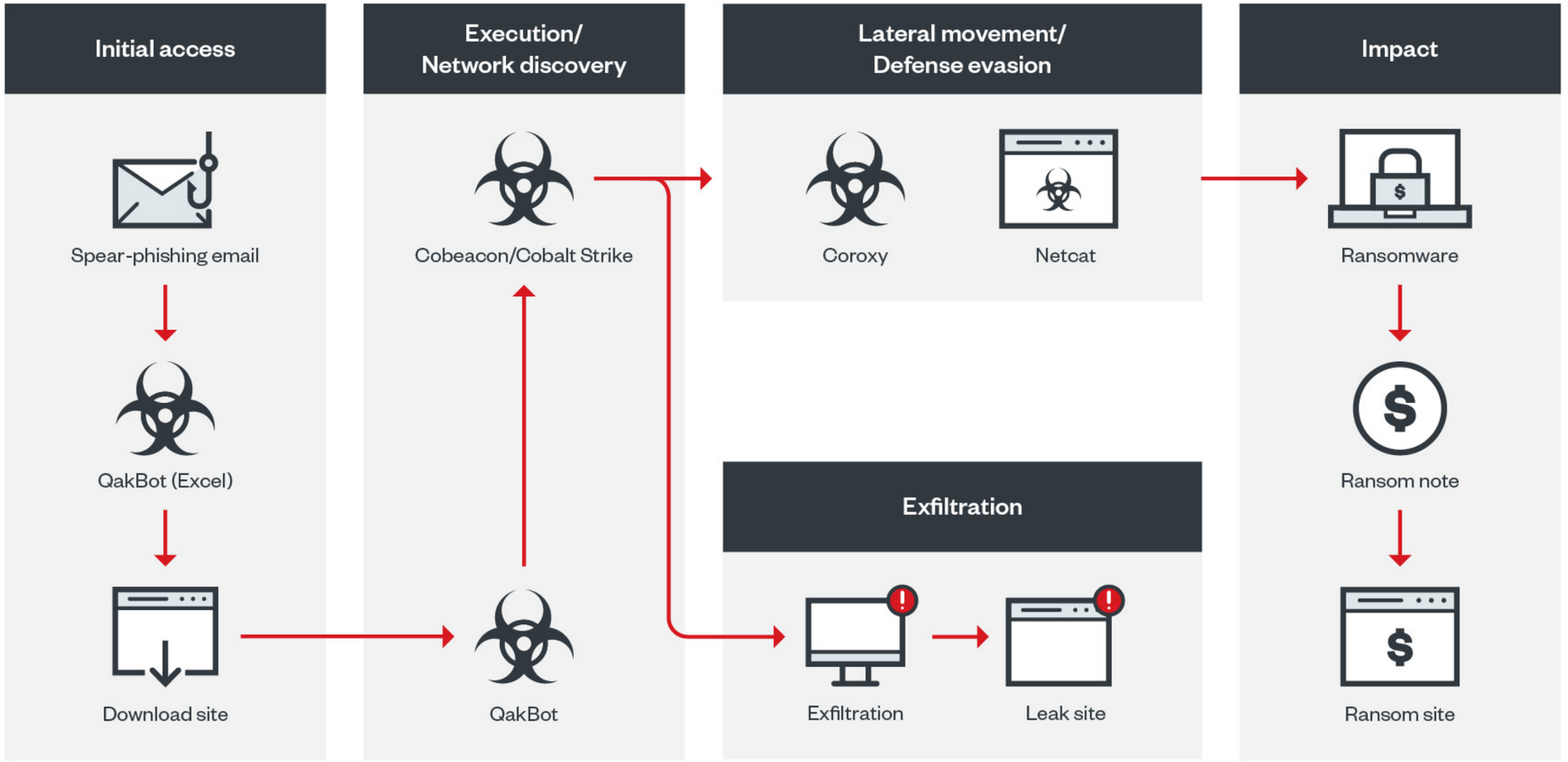
Жизненный цикл атаки LockBit



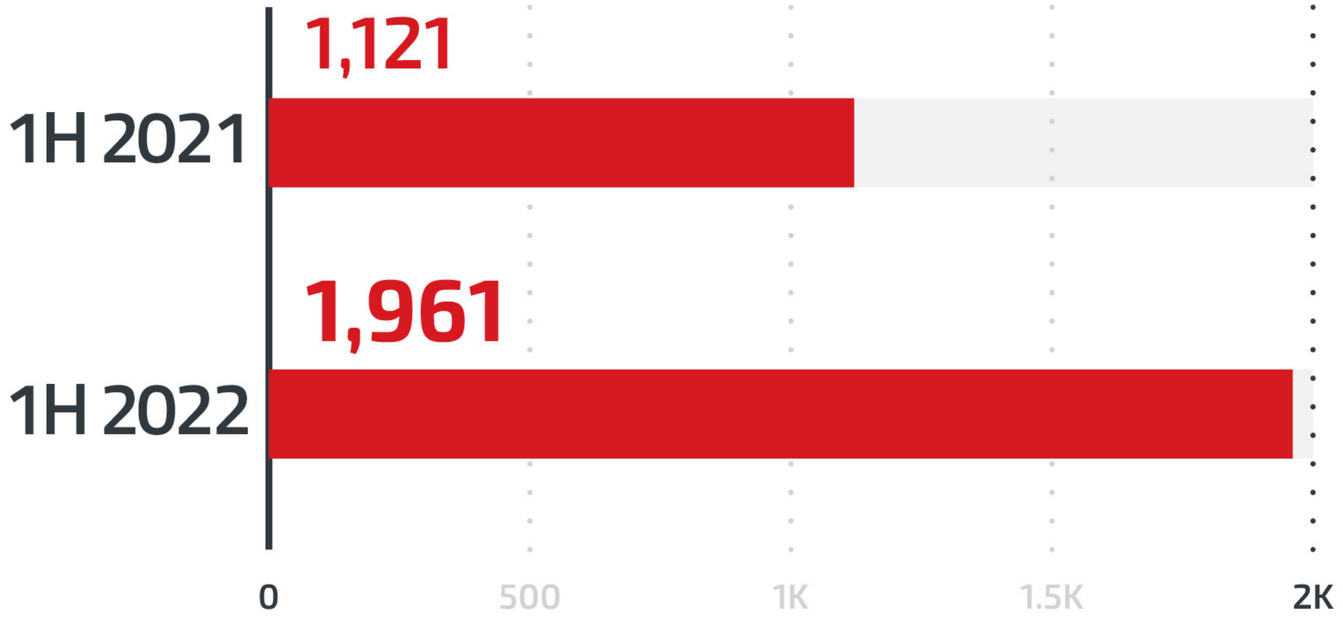


Жизненный цикл атаки Conti

Black Basta



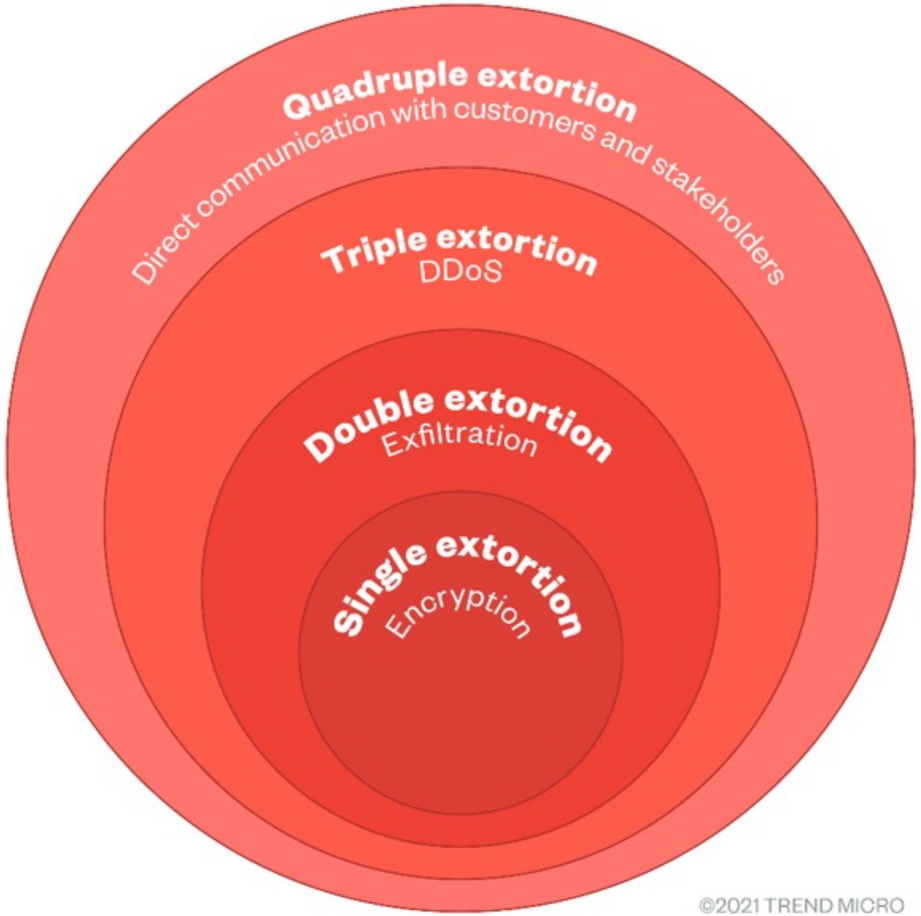
Программы-вымогатели для Linux



- В первой половине 2022 года гипервизор VMware ESXi усиленно атаковали.
- В конце 2021 года операторы LockBit на подпольном форуме объявили о LockBit Linux-ESXi Locker версии 1.0, предназначенном для атак на Linux.
- В мае 2022 года был обнаружен новый вариант программы-вымогателя под названием Cheerscrypt, который атаковал устройства, использующие ESXi.

Тактики применения программ-вымогателей

- Злоумышленники стали использовать **больше этапов вымогательства**.
- Усиливается давление на организации с целью получения выкупа.



Прогнозы

- Продолжаются атаки с различными техниками вымогательства
- Злоумышленники все чаще выбирают целью для атак крупные организации из критически важных отраслей (подход Big game hunting, «Охота на крупную дичь»)
- Усиливается сотрудничество между киберпреступниками (AaaS и RaaS)
- Самые распространенные угрозы:
  - кража учетных данных;
  - эксплуатация общедоступных устройств и систем;
  - применение для атак легитимных инструментов.

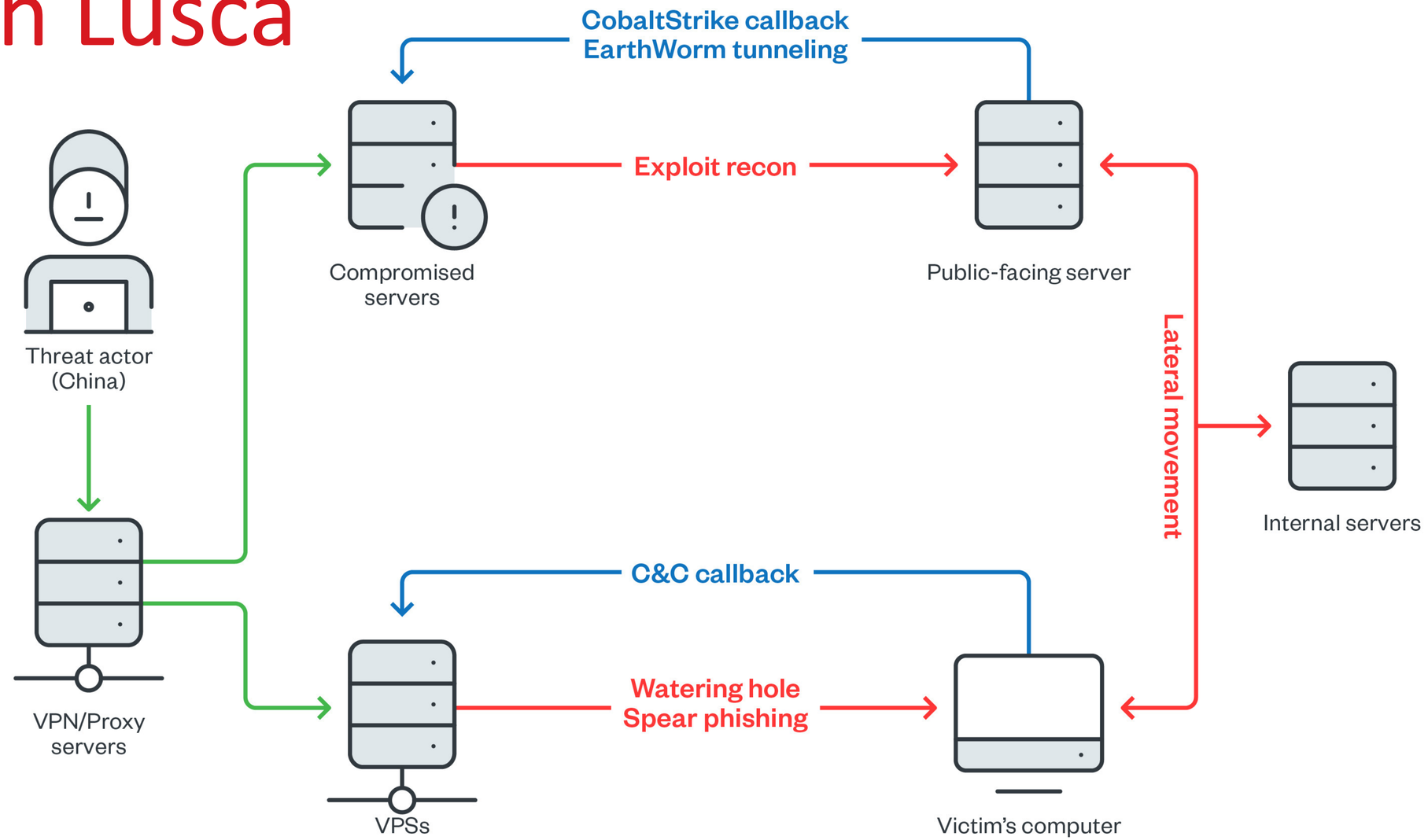
TREND MICRO | research

TARGETED ATTACKS

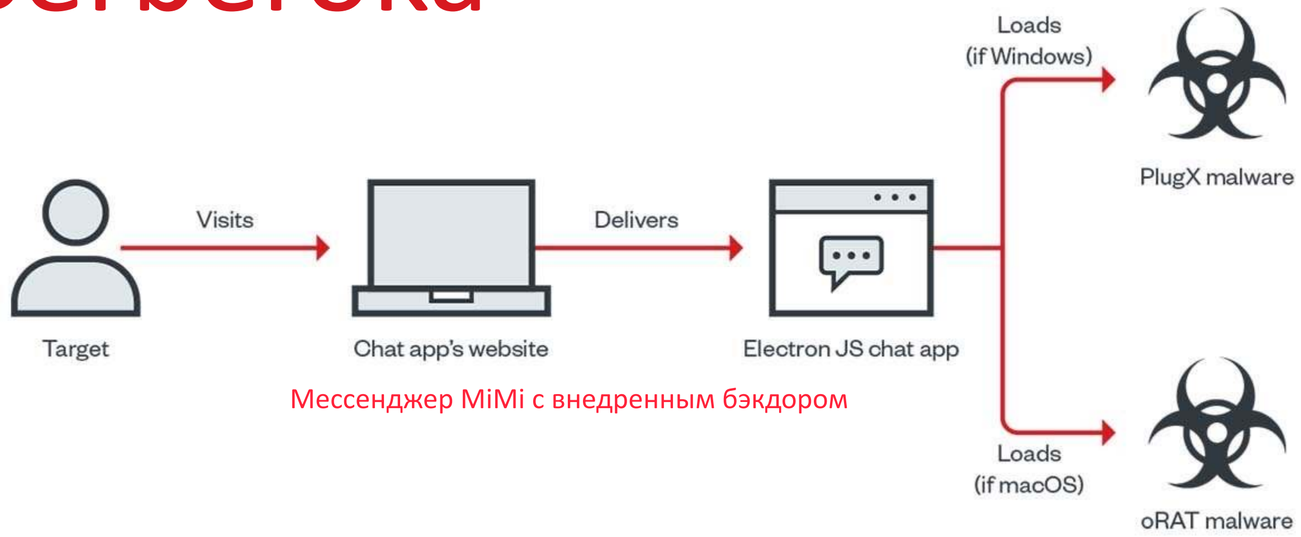
Такие группировки киберпреступников, как Earth Lusca и Earth Berberoka, используют для своих атак комплекс инструментов и обширную инфраструктуру

Отчет Trend Micro о кибербезопасности за 1 полугодие 2022 г.

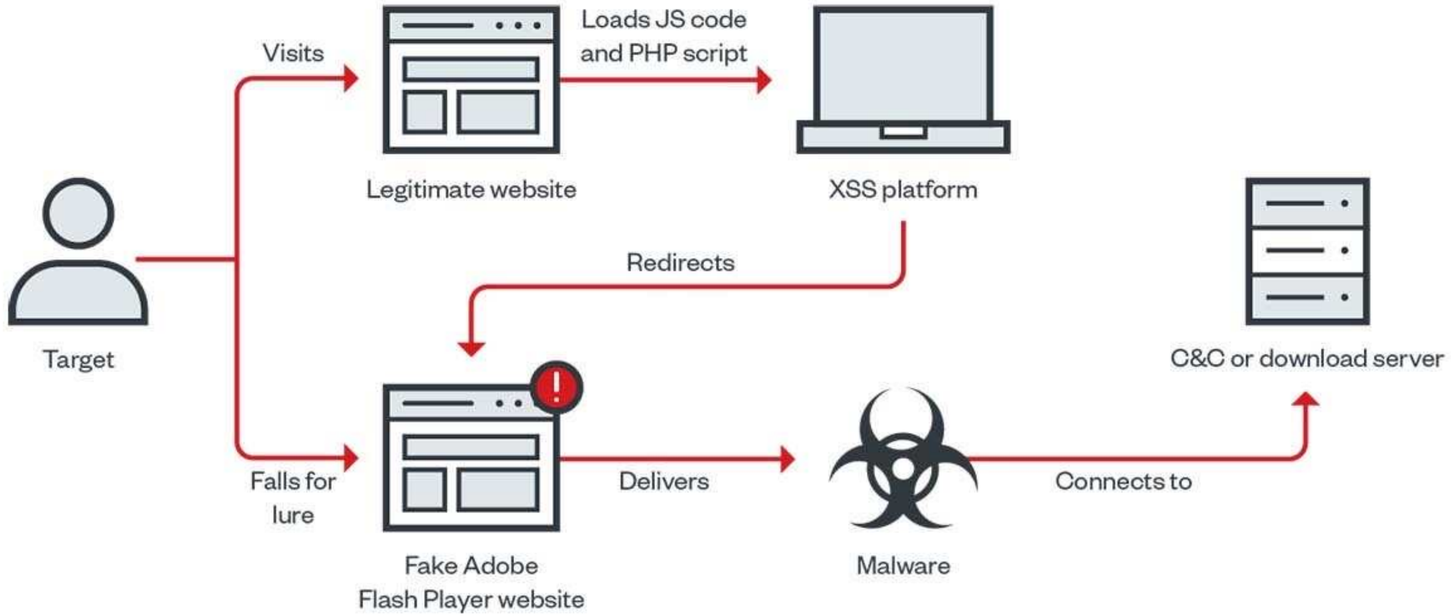
Earth Lusca



Earth Berberoka



Мессенджер MiMi с внедренным бэкдором



Тактики злоумышленников

- Масштабная разведка перед атакой
- Рост числа атак на активы, работающие не на Windows, а на других платформах
- Активное применение анти-форензики
- Атаки, охватывающие различные части сети
- Атаки из взломанной сети партнера / атаки на цепочки поставок

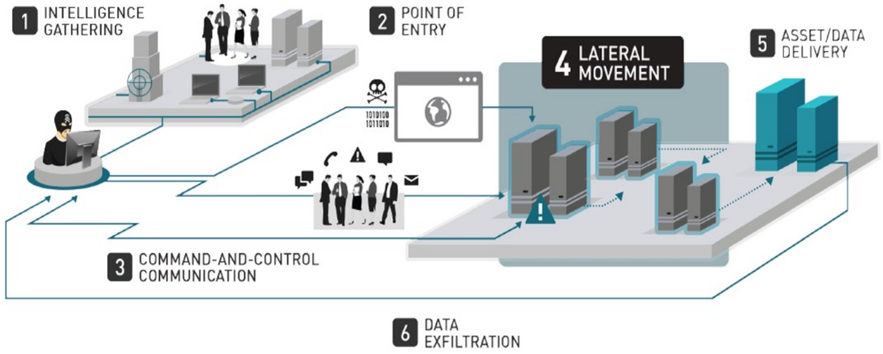


Figure 1. Six Stages of an APT attack

Прогнозы

Злоумышленники продолжают использовать в своих интересах:

- ✓ ошибки сотрудников;
- ✓ беззаботное отношение к ИБ;
- ✓ технические сбои;
- ✓ облачную инфраструктуру;
- ✓ OT-сети (недостаток грамотных специалистов).

Злоумышленники непрерывно совершенствуют инструменты, тактики и процедуры (TTP)

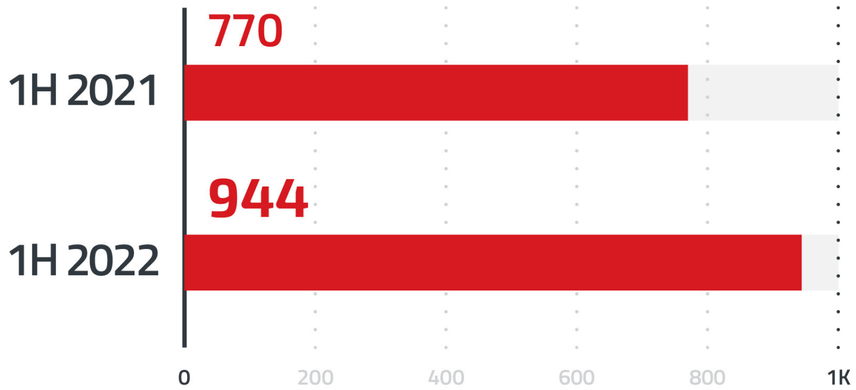
TREND MICRO | research

VULNERABILITIES

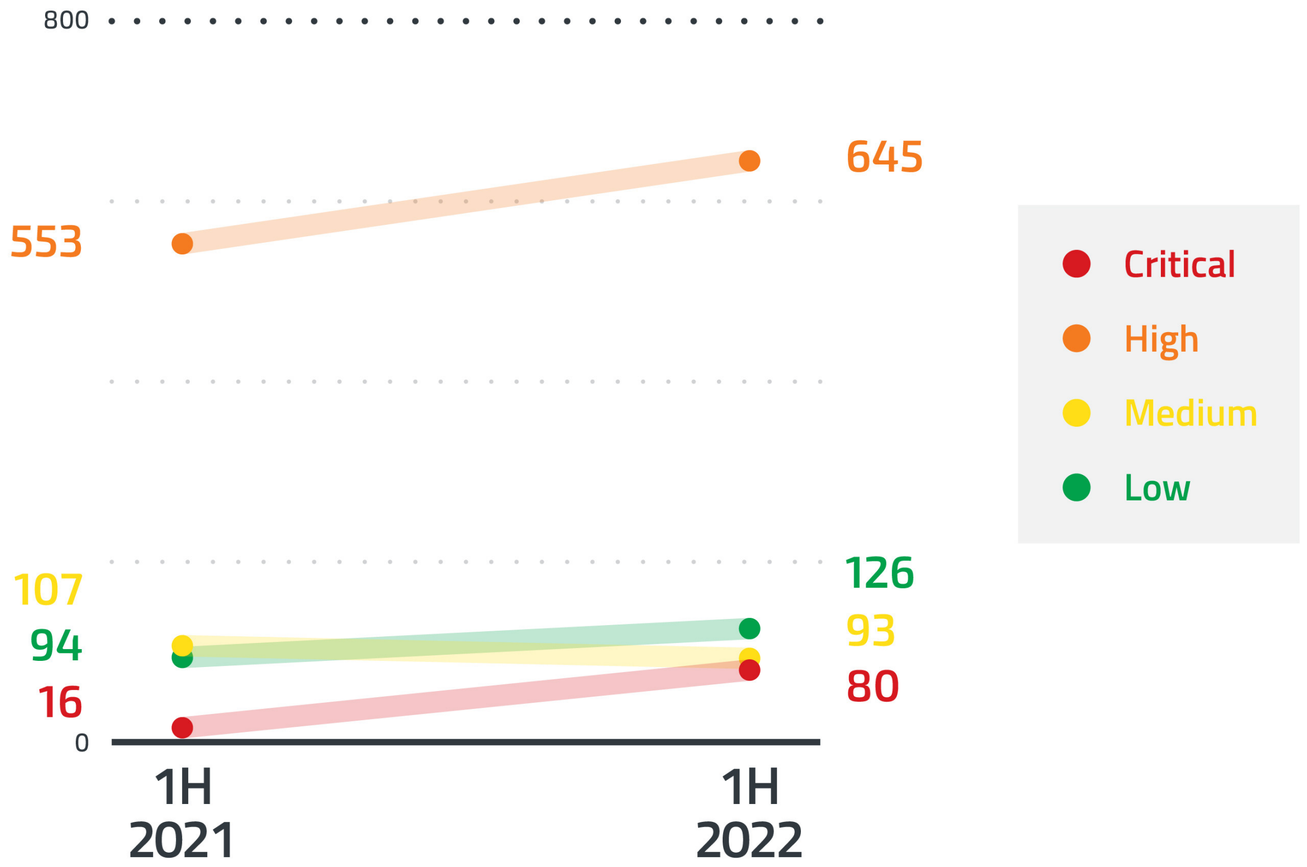
В первой половине 2022 года выросло количество критических и чрезвычайно серьезных уязвимостей

Отчет Trend Micro о кибербезопасности за 1 полугодие 2022 г.

Уязвимости, раскрытые ZDI



на **23%** ↑ раскрытых уязвимостей



Первое полугодие 2021 г. и 2022 г. Сравнение числа уязвимостей, раскрытых с помощью программы Trend Micro «Инициатива нулевого дня» (ZDI), с учетом степени их серьезности.

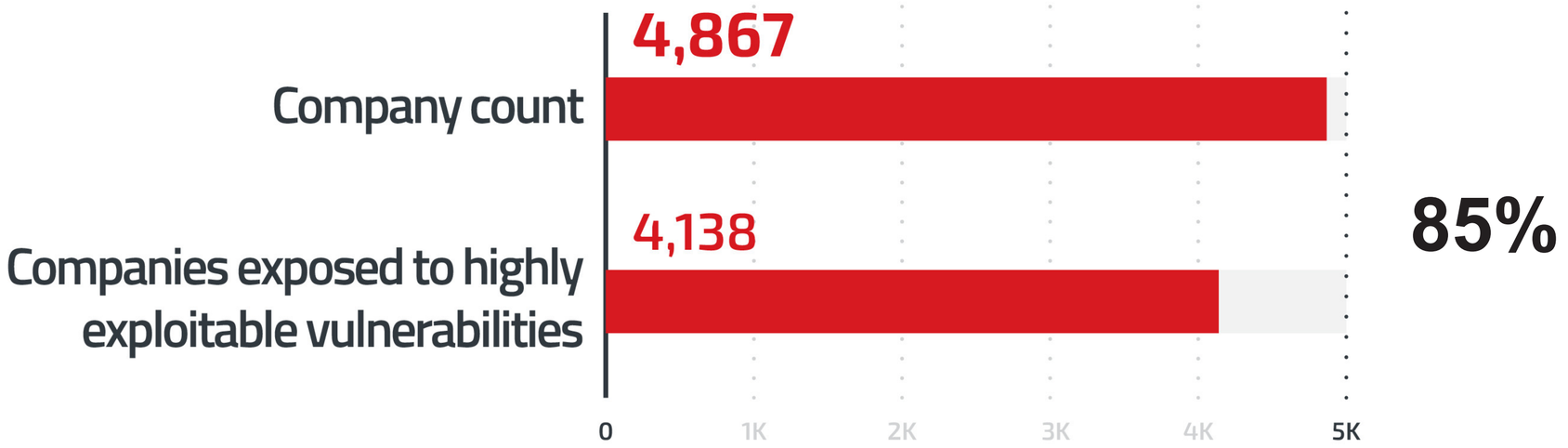
TREND MICRO™ research

Уязвимости, которые эксплуатируют больше всего

Rule ID	CVE ID number	Hits	Affected products
29739	CVE-2017-14100	15,200,809	Asterisk 11.x before 11.25.2, 13.x before 13.17.1, and 14.x before 14.6.1 and Certified Asterisk 11.x before 11.6-cert17, and 13.x before 13.13-cert5
17056	CVE-2014-3567	9,107,139	OpenSSL before 0.9.8zc, 1.0.0 before 1.0.0o, and 1.0.1 before 1.0.1j
1095	CVE-2000-0884	4,447,190	IIS 4.0 and 5.0
3886	CVE-2010-0817	2,597,362	Microsoft SharePoint Server 2007 12.0.0.6421 and possibly earlier and SharePoint Services 3.0 SP1 and SP2.
	CVE-2011-1264		Microsoft Windows Server 2003 SP2 and Server 2008 Gold, SP2, R2, and R2 SP1
40693	CVE-2021-35394	1,166,969	Realtek Jungle SDK version v2.x up to v3.4.14B
2023	CVE-2005-1380	711,159	BEA Admin Console 8.1
	CVE-2010-0817		Microsoft SharePoint Server 2007 12.0.0.6421 and possibly earlier and SharePoint Services 3.0 SP1 and SP2
	CVE-2010-3936		Microsoft Forefront Unified Access Gateway (UAG) 2010 Gold, 2010 Update 1, and 2010 Update 2
	CVE-2017-0068		Microsoft Edge
10146	CVE-2010-2861	648,690	Adobe ColdFusion 9.0.1 and earlier
	CVE-2013-3336		Adobe ColdFusion 9.0, 9.0.1, 9.0.2, and 10
31852	CVE-2014-0224	597,386	OpenSSL before 0.9.8za, 1.0.0 before 1.0.0m, and 1.0.1 before 1.0.1h
6161	CVE-2008-1451	580,030	Microsoft Windows 2000 SP4 and Server 2003 SP1 and SP2
31936	CVE-2018-10562	518,502	Dasan GPON home routers

Filter ID	Solution	Related CVEs	Detected event counts
1009667	Deep Security	CVE-2017-14495	114,995,958,044
1000853	Deep Security	CVE-2006-4154	5,665,473,527
1011242	Deep Security	CVE-2021-44228	4,794,466,414
1003766	Apex One	CVE-2009-2524	995,700,958
1004398	Deep Security	CVE-2010-2730	967,669,441
1010971	Deep Security	CVE-2021-29441	846,824,548
1006027	Deep Security	CVE-2014-0098	417,996,287
1011456	Deep Security	CVE-2022-26134	381,361,877
1008445	Apex One	CVE-2017-8543	266,267,487
1008713	Apex One	CVE-2017-11815	188,900,588

Уязвимые организации



Прогнозы

- ✓ Большинство атак будет эксплуатировать известные уязвимости
- ✓ Будут больше эксплуатироваться уязвимости нулевого дня
- ✓ IoT-устройства будут иметь известные, но не исправленные уязвимости
- ✓ Будут эксплуатироваться уязвимости любых ОС, не только Windows
- ✓ Будет больше атак на критичные для бизнеса приложения

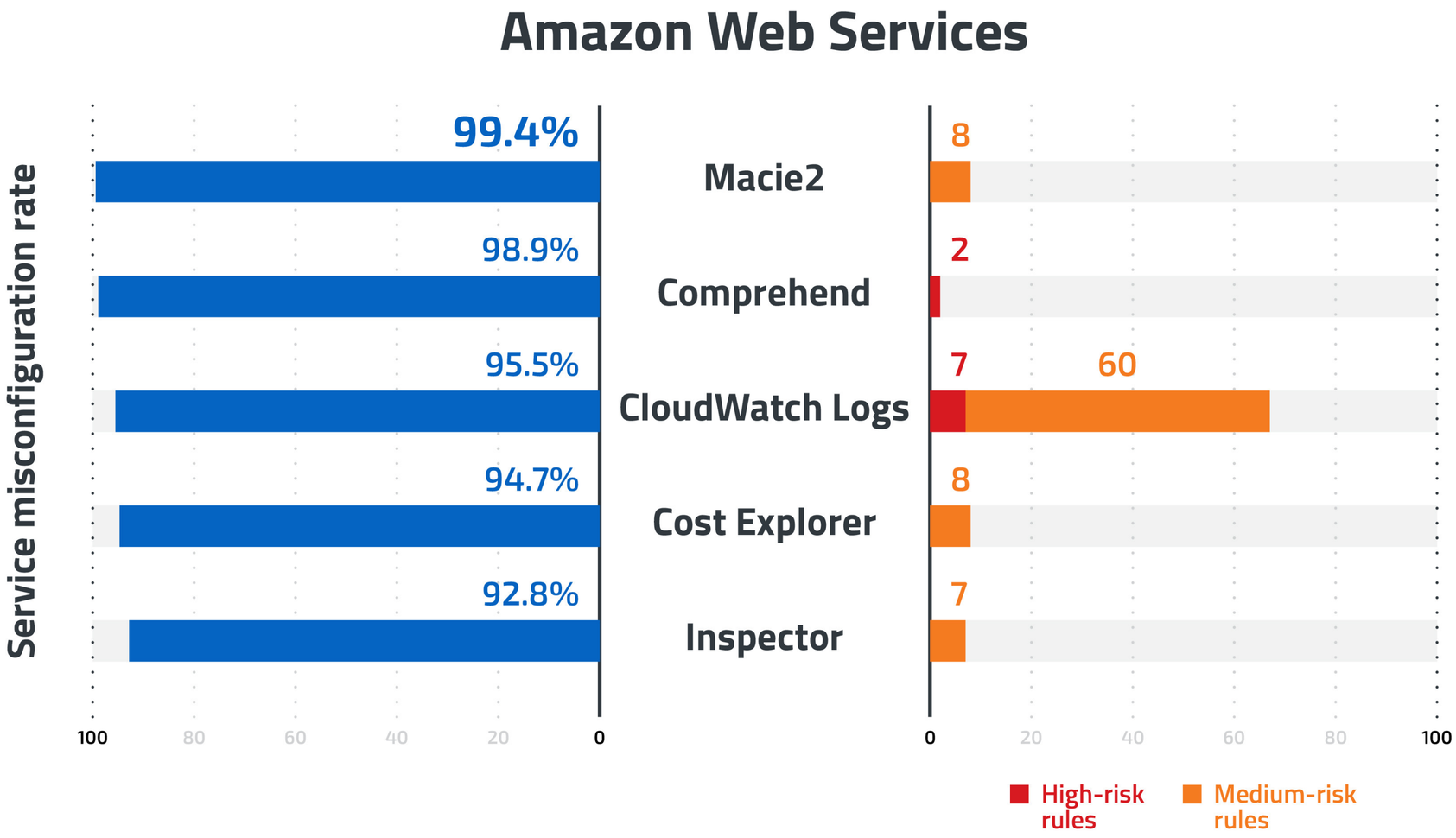
TREND MICRO | research

CLOUD THREATS

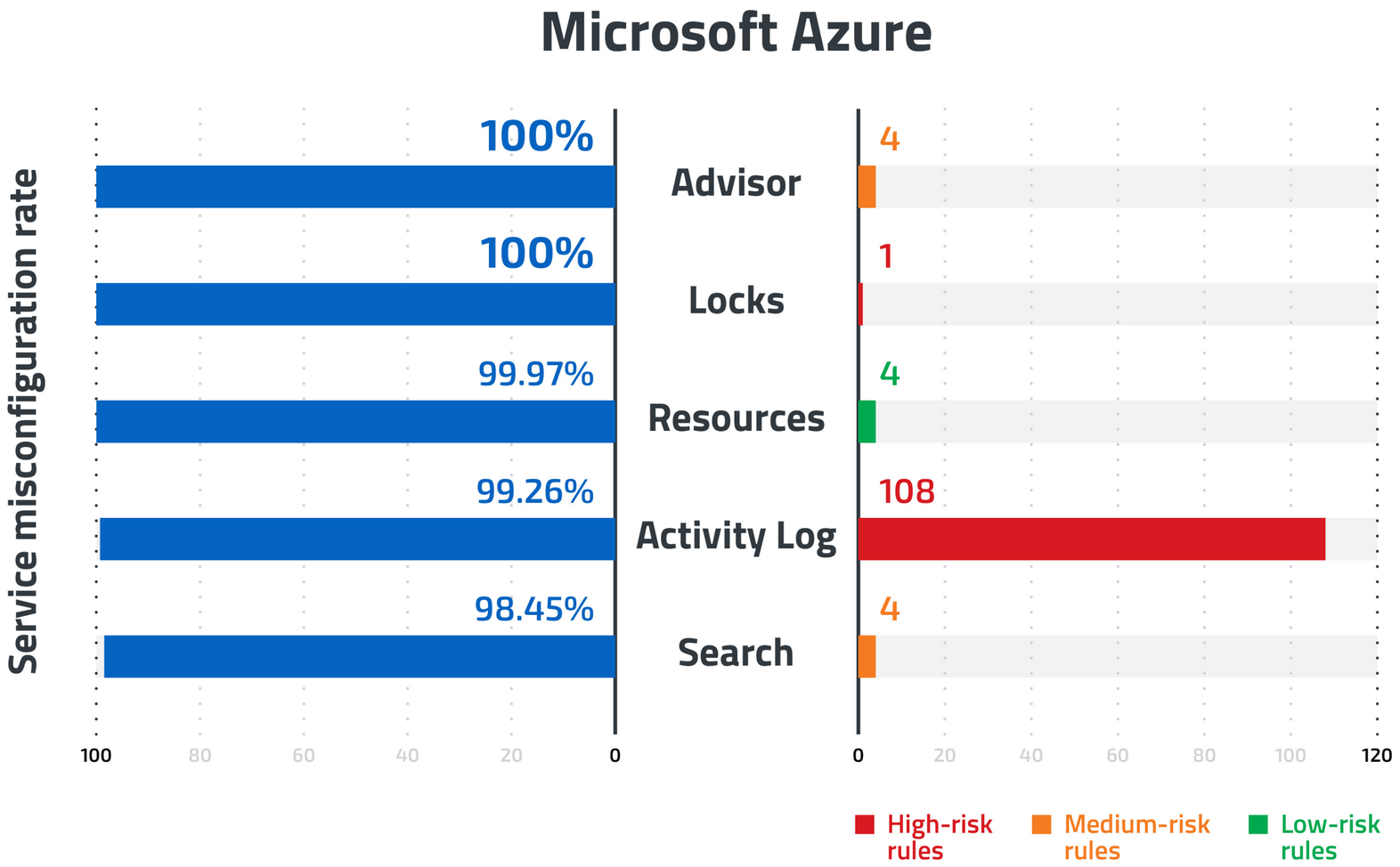
Ошибки облачной конфигурции — серьезная проблема для большинства организаций

Отчет Trend Micro о кибербезопасности за 1 полугодие 2022 г.

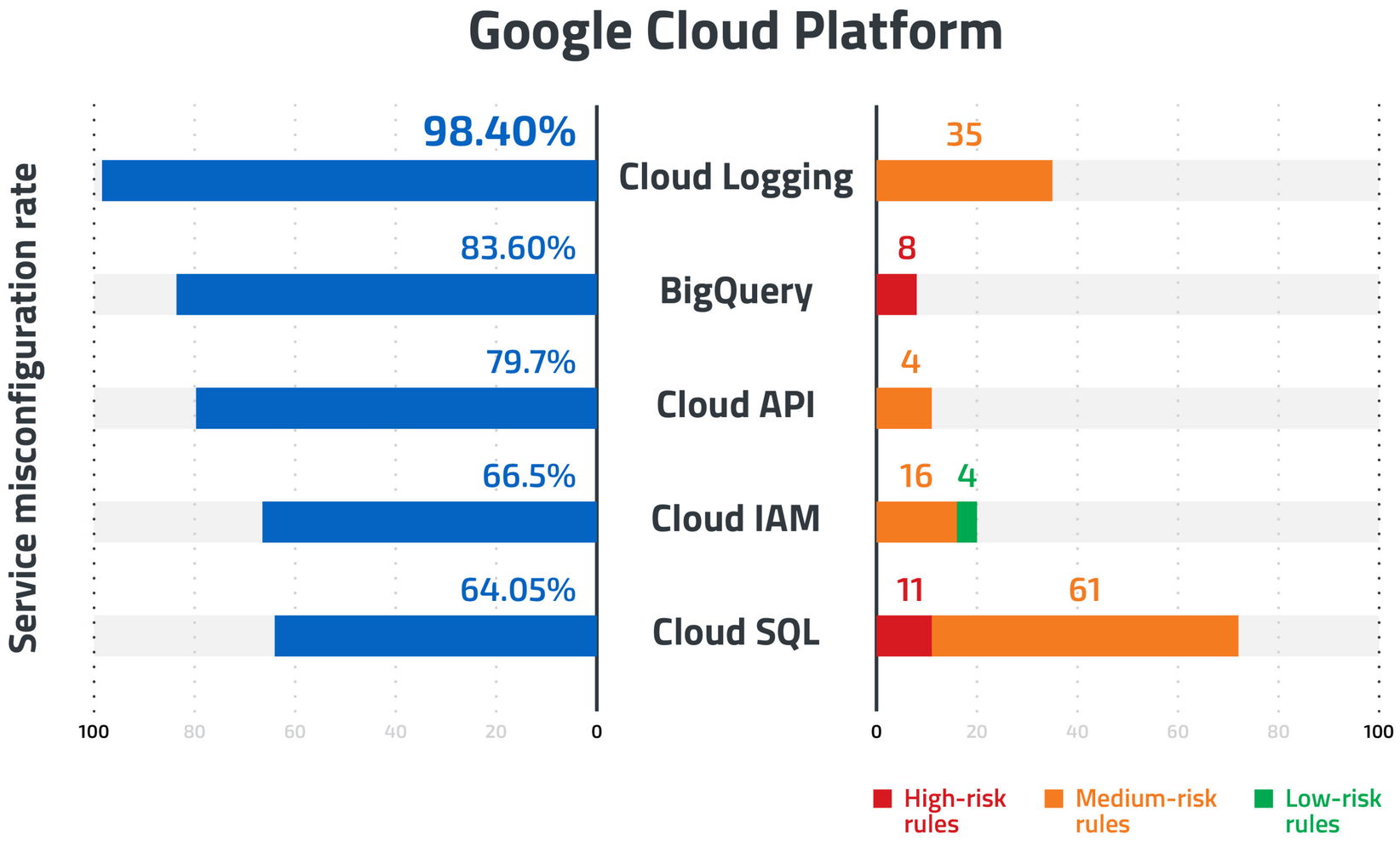
Ошибки облачной конфигурации



Ошибки облачной конфигурации

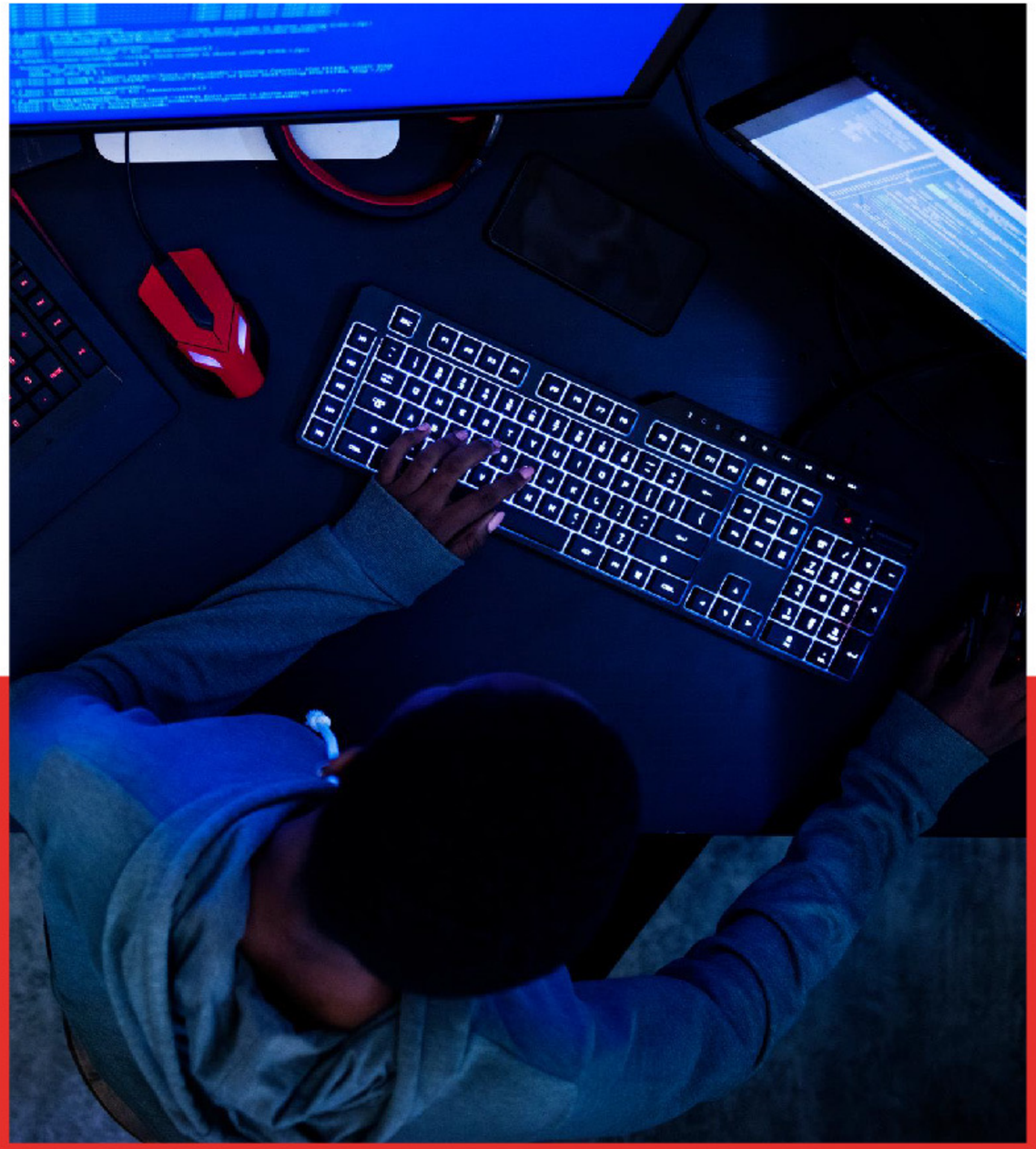


Ошибки облачной конфигурации



Прогнозы

- ✓ **Ошибки конфигурации.** Ошибки облачной конфигурации и в будущем останутся одной из основных проблем.
- ✓ **Угрозы на уровне приложений / API.** Общедоступные конечные точки в облаке предоставляют пользователям доступ к приложению, но в то же время подвергают его опасности со стороны злоумышленников.
- ✓ **Цепочки поставок.** Большинство современных приложений построены на основе большого количества программных компонентов с открытым исходным кодом.
- ✓ **Майнинг криптовалют.** Гибкость и адаптивность облака отлично подходят для разработчиков, но эти же качества позволяют злоумышленникам путем незаконного доступа получать деньги.



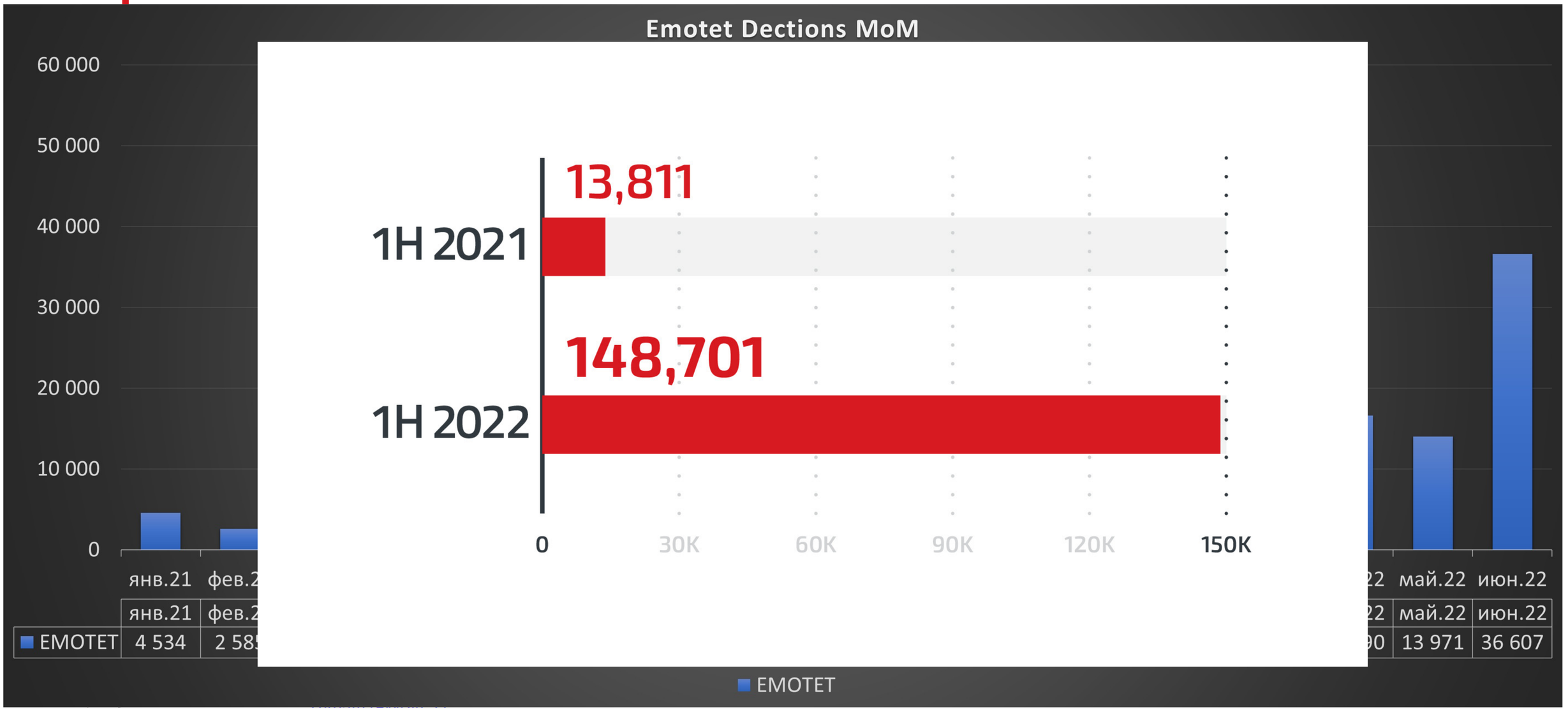
TREND MICRO | research

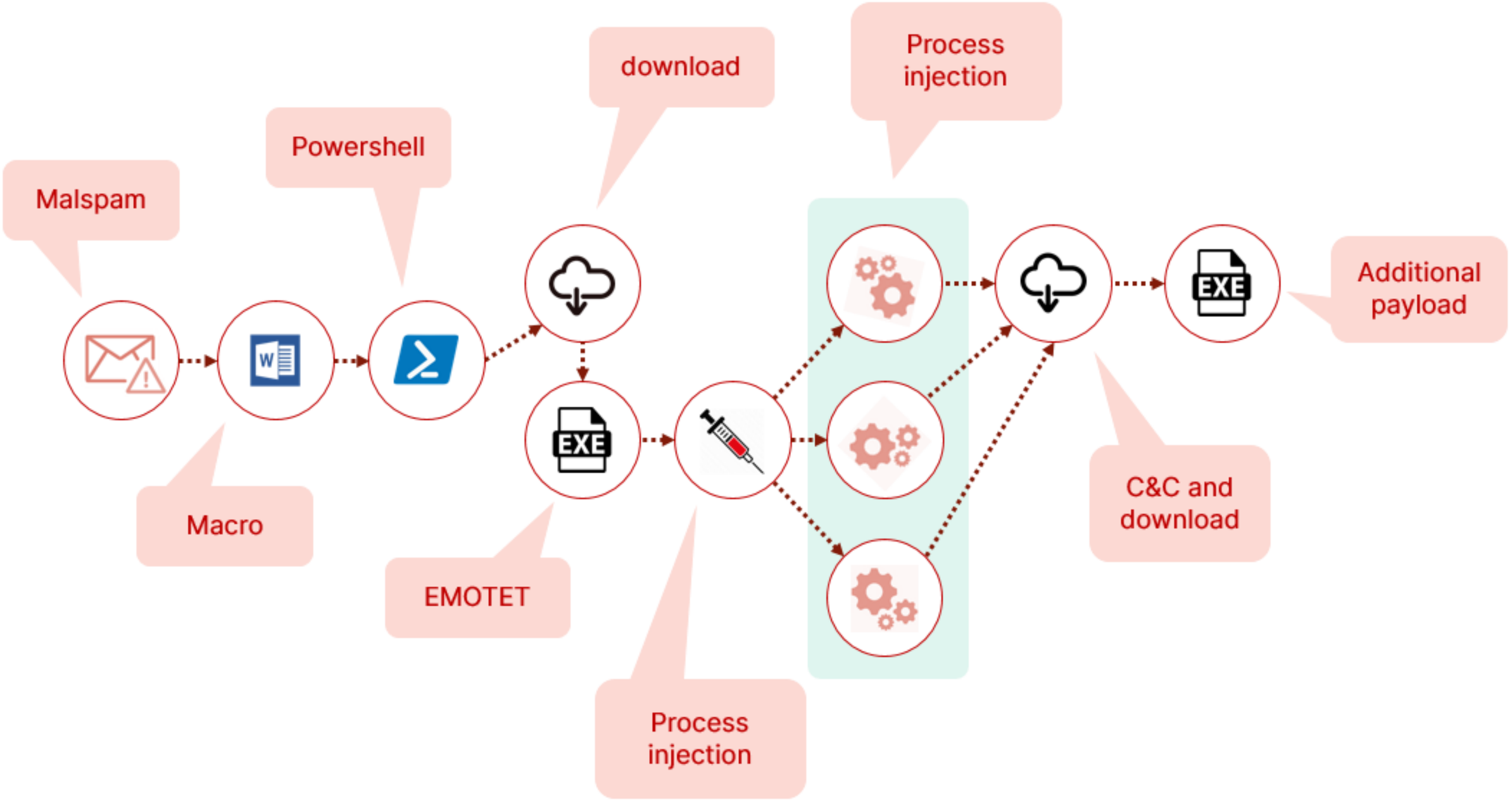
THREATS

Часто как специалисты по безопасности, так и широкая общественность уделяет львиную долю внимания новым семействам вредоносных программ, но «старые» эффективные вредоносные программы по-прежнему представляют угрозу для организаций.

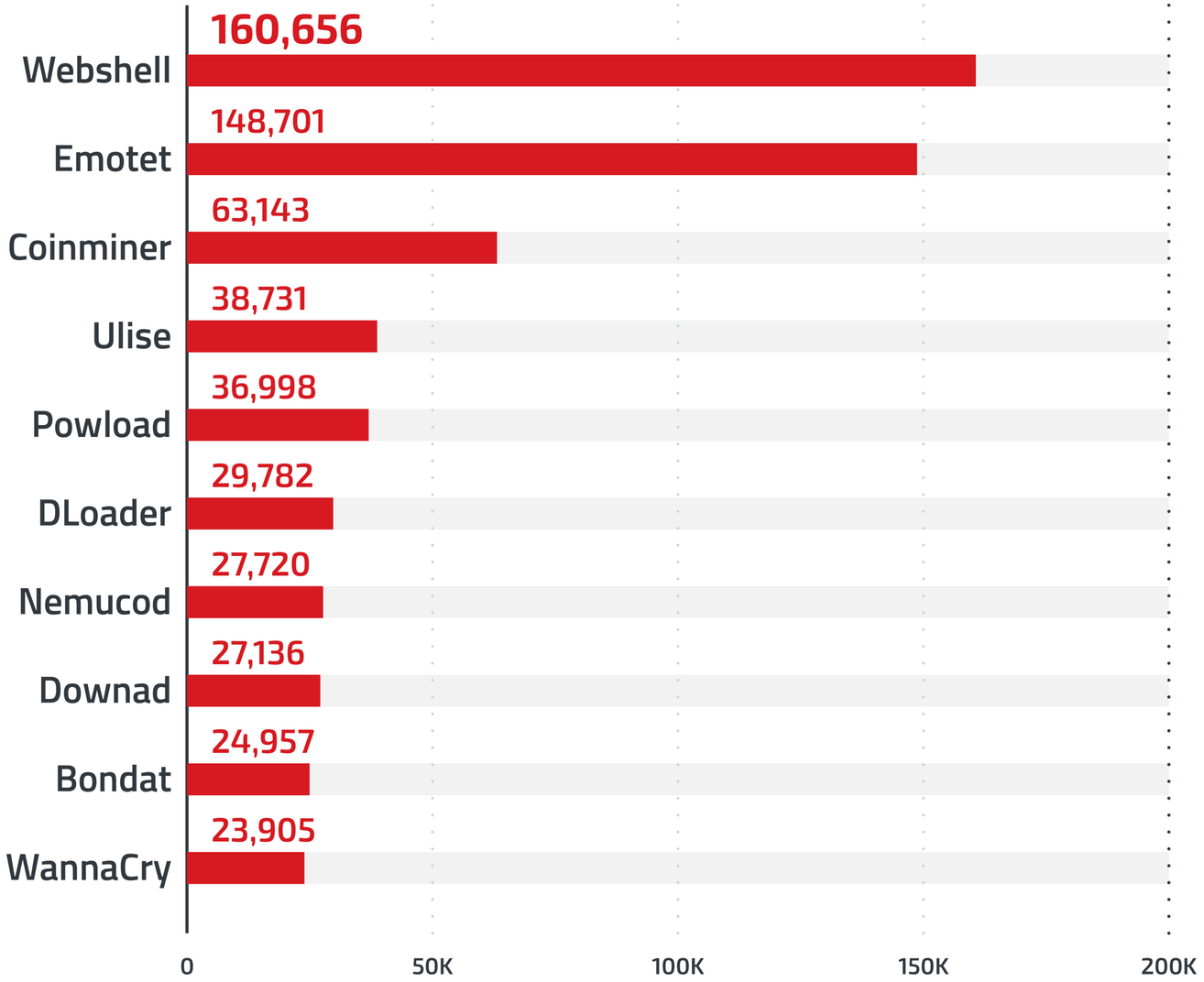
Отчет Trend Micro о кибербезопасности за 1 полугодие 2022 г.

Угрозы: Emotet



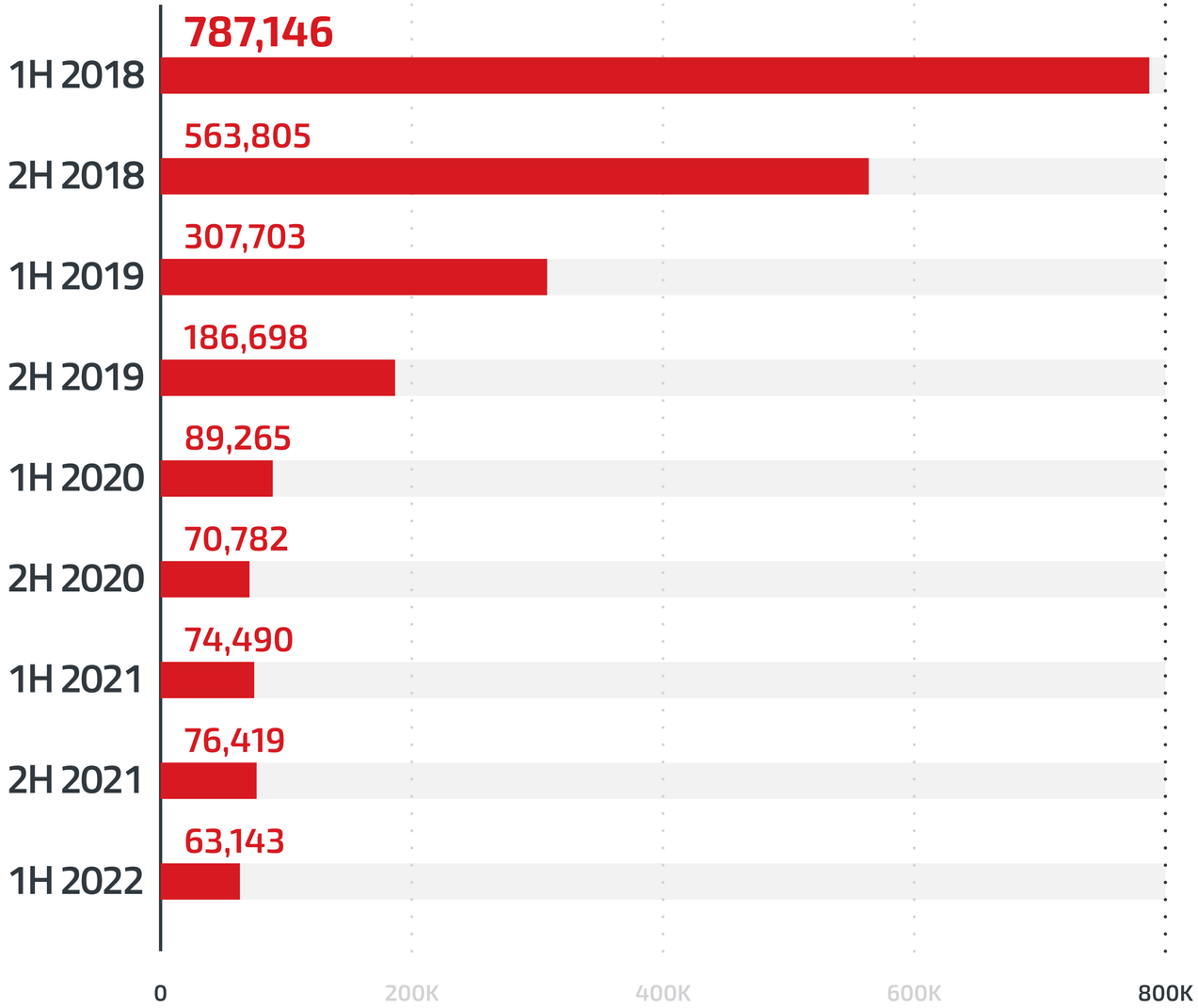


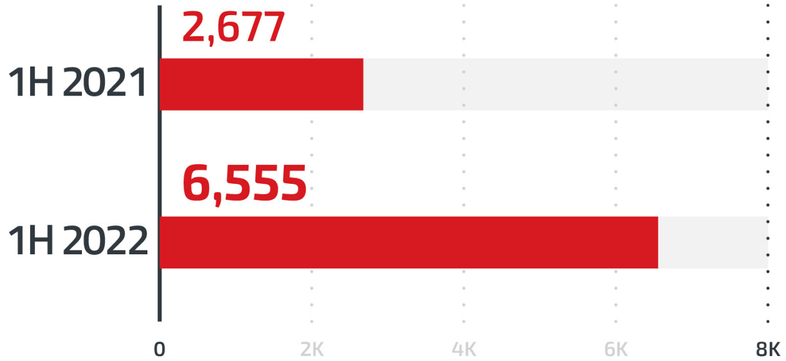
Самые распространенные вредоносные программы



TREND MICRO | research

Уровень криптомайнинга снижается





TREND MICRO™ | research

Криптомайнинговые группировки

Kek Security

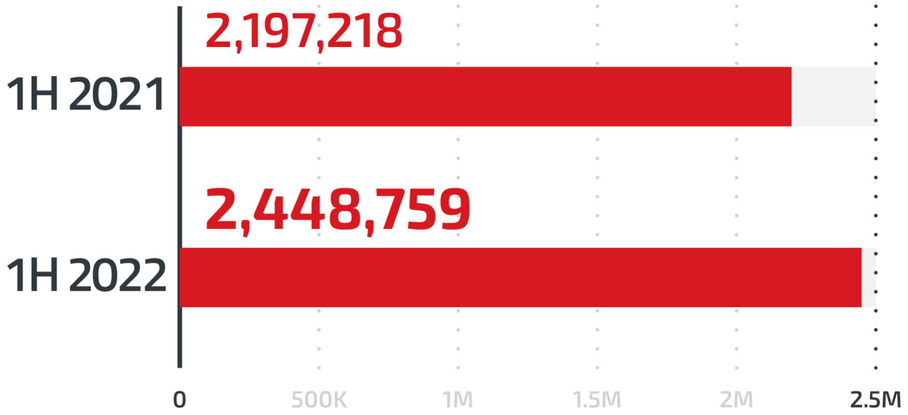
Kinsing

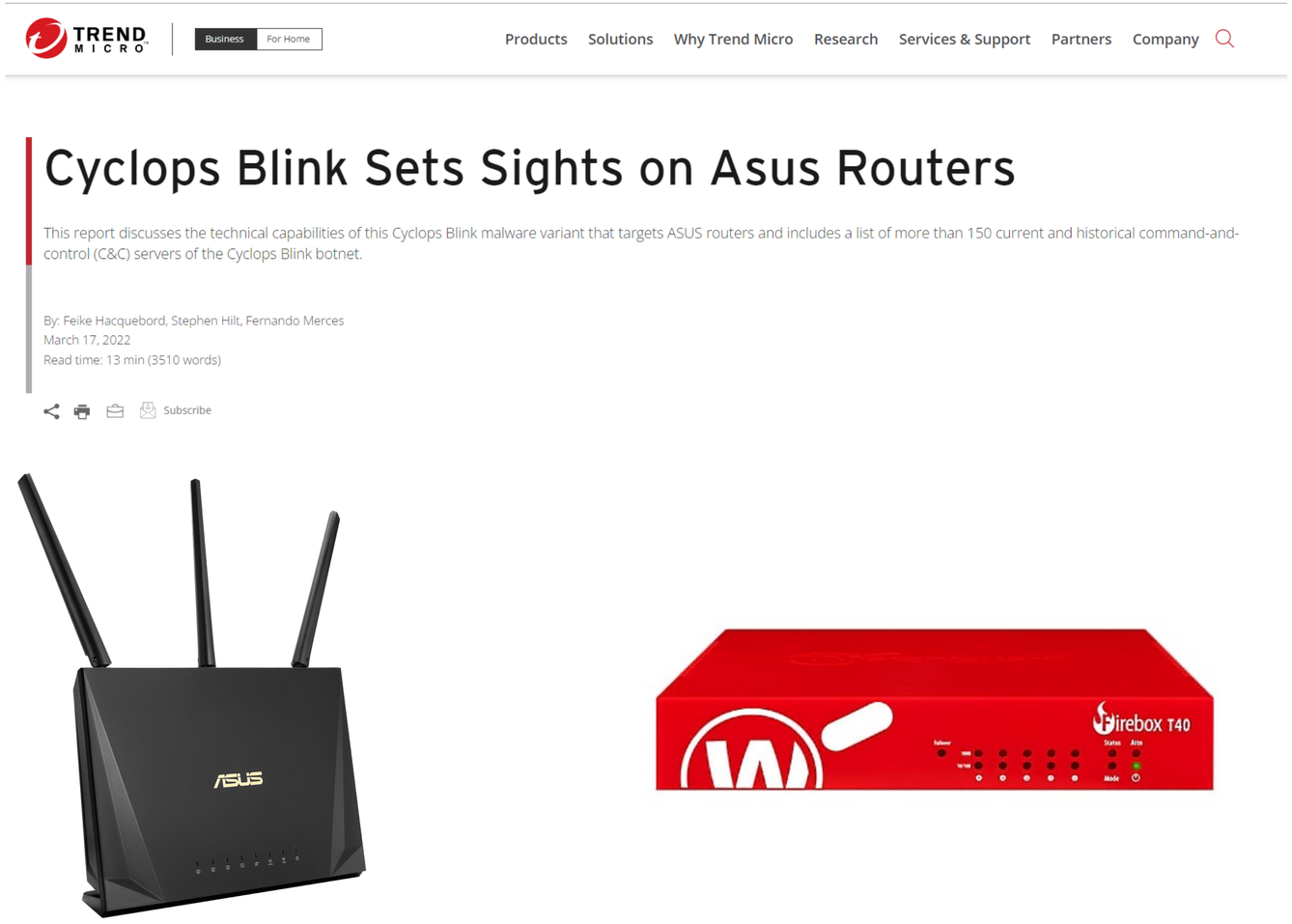
8220

Outlaw

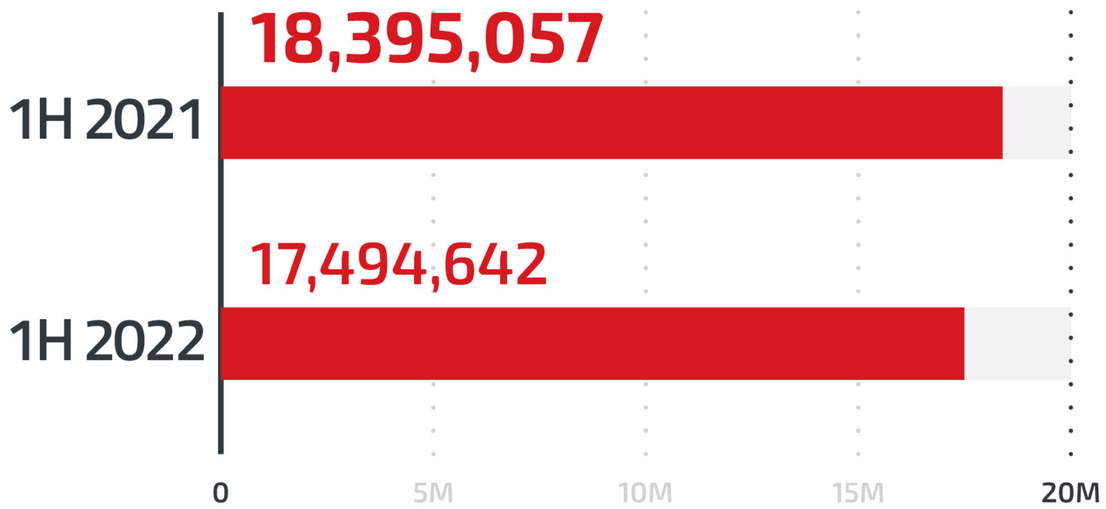
TeamTNT

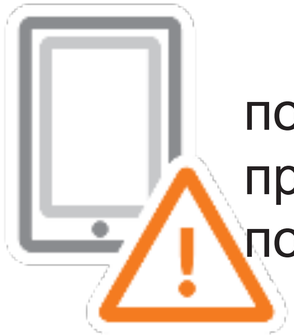
Угрозы Интернету вещей





Угрозы для мобильных устройств





поддельные мобильные приложения, замаскированные под ПО для криптомайнинга

Общие тенденции развития угроз

- Продолжение сотрудничества злоумышленников
- Расширение возможностей для вымогательства
- Больше атак, в том числе направленных
- Исследование поверхности атаки
- Нацеленность на организации с плохой кибергигиеной

TREND MICRO | research

MULTILAYERED DEFENSES

AGAINST THREATS FROM ALL ANGLES

Развивающаяся поверхность атаки требует применения действенной многоуровневой защиты и эффективных технологий безопасности

Отчет Trend Micro о кибербезопасности за 1 полугодие 2022 г.

Жизненный цикл управления рисками поверхности атаки

ОПРЕДЕЛЕНИЕ ПОВЕРХНОСТИ АТАКИ

Непрерывный мониторинг кибер-ресурсов, формирующих поверхность атаки организации с учетом динамики во времени, в сравнении с отраслевыми показателями

ОЦЕНКА РИСКОВ

Оценка векторов риска, статуса уязвимостей, конфигурации защитных средств и типов атак.

СНИЖЕНИЕ РИСКОВ

Применяйте надлежащие упреждающие защитные средства или принимайте соответствующие меры для снижения и устранения рисков в масштабах всего предприятия

Лучшие практики

- ✓ Разработайте и регулярно тестируйте план реагирования на инциденты.
- ✓ Защитите административные учетные записи (особенно в системах, доступных через интернет), в том числе для доступа к ним используйте многофакторную аутентификацию.
- ✓ Отслеживайте и идентифицируйте использования легитимных инструментов (например, Mimikatz, Cobalt Strike, PSexec и т.д.), чтобы определить, не является ли их использование злонамеренным.
- ✓ Проанализируйте свои решения по кибербезопасности вместе с вендором, чтобы гарантированно использовать последние версии и все доступные передовые технологии обнаружения.
- ✓ Разработайте на основе рисков подход к управлению исправлением уязвимостей, чтобы определять, какие пакеты исправлений являются критически важными и требуют немедленной установки. Также обратите внимание на предотвращения вторжений (IPS) с функцией виртуального исправления, как на дополнение к выпускам официальных пакетов исправлений.
- ✓ Разработайте и внедрите для своих сотрудников программу обучения по вопросам ИБ, которая включает симуляцию фишинговых атак, чтобы научить распознавать угрозы. Также необходимо провести обучение ваших облачных архитекторов.
- ✓ Приобретите современную платформу кибербезопасности, которая обеспечивает лучшую видимость, информирует обо всех этапах кибератаки и может обнаружить атаку на раннем этапе, чтобы предотвратить ее развитие.

Платформа кибербезопасности Trend Micro

Trend Micro vision one

Центр обеспечения безопасности

Мониторинг и анализ рисков

XDR
Расширенное обнаружение и реагирование

Управление агентами и политиками

Trend Micro apex one

Защита пользователей

Рабочие станции

Моб. устройства

Эл. почта

Web

Приложения

Trend Micro cloud one

Защита гибридного облака

Серверы

Виртуальные машины

Облачные рабочие нагрузки

Контейнеры

Приложения

Сканирование ПО с открытым кодом

Облачная сеть

Защита облака Соответствие требованиям

Хранилище файлов

Trend Micro network one

Защита сетей

Предотвращение

Обнаружение

Защита IoT

Песочницы

Глобальная информация об угрозах

TREND MICRO research

Угрозы

Уязвимости

Киберпреступники

Прогнозы

Типовые компоненты платформы

Управление аккаунтами и лицензиями

Основные технологии и модули безопасности

Архитектура данных и аналитика

Инфраструктура SaaS

Интеграция с экосистемой

Microsoft 365, Google, box, aws, Microsoft Azure, Google Cloud, kubernetes, vmware, docker, QUALYS, RAPID7, TAXII, STIX, paloalto, Check Point, splunk>, ArcSight, FORTINET, IBM Radar

Безопасный обмен цифровой информацией во всем мире

Более 30 лет на страже кибербезопасности

1,7 млрд долл. США ежеквартально от продаж и иных источников дохода, с момента выхода на биржу в 1998 году

Свыше 500 000 коммерческих клиентов, в числе которых 9 из 10 крупнейших компаний мира из рейтинга Fortune Global 500

7000 сотрудников в 65 странах мира, посвятивших себя обеспечению безопасности

Ева Чен (Eva Chen), генеральный директор и соучредитель Trend Micro

Как связаться с представителями Trend Micro

Вы можете пообщаться с представителем Trend Micro уже сегодня, чтобы понять, смогут ли ваши стратегии безопасности противостоять современным угрозам.

- Торговый представитель
  - Телефон: +7 701 527 73 77
  - Email: bakhtiyar_baymagambet@trendmicro.com

Trend Micro Казахстан

Представительство в Астане и Алматы

Свыше 120 государственных учреждений,

50 коммерческих клиентов и более 10 нац.компаний.

Гос.программа «Киберщит»

Наличие опыта построения ОЦИБ

Инженерный ресурс в Астане и Алматы

Локальная техническая поддержка 24*7*365

Поддержка отечественных производителей

Результаты за 5 лет в Казахстане

Благодарим за внимание