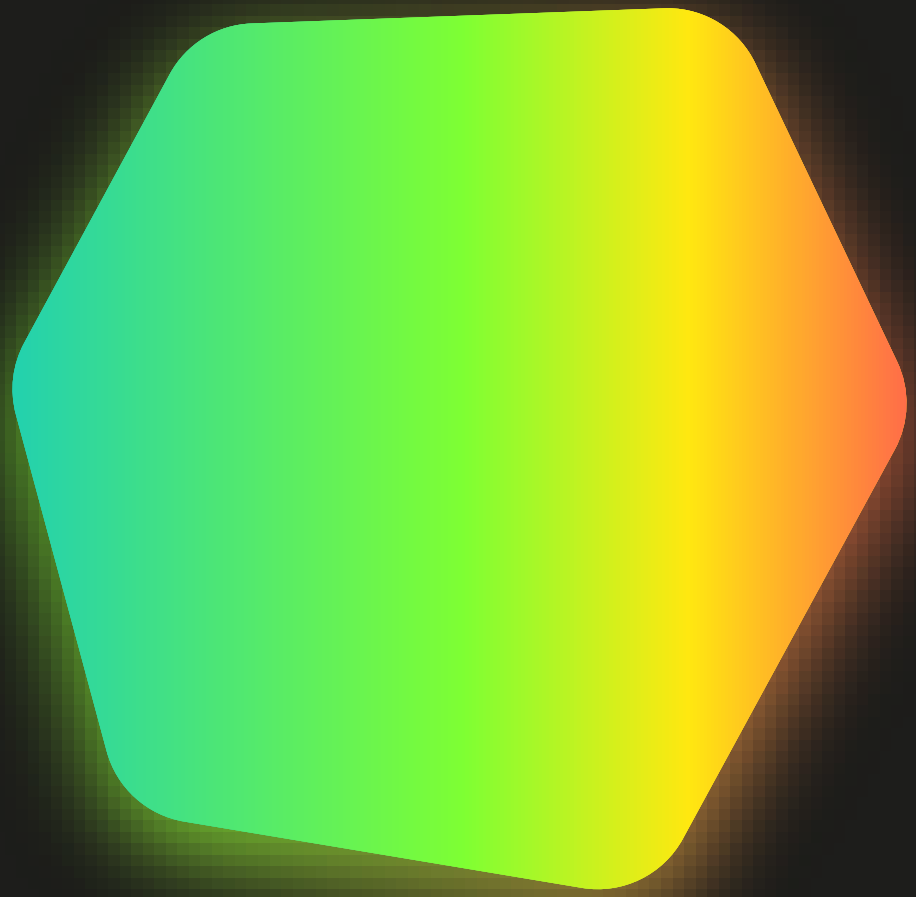
Ландшафт киберугроз и современные тренды ИБ



Татьяна Шишкова

Ведущий исследователь угроз информационной безопасности,
Глобальный центр исследований (GReAT)

Kaspersky

GREAT GLOBAL RESEARCH & ANALYSIS TEAM

Vitaly Kamluk
Head of GReAT APAC
GReAT APAC

Noushin Shabab
Senior Security Researcher
GReAT APAC

Saurabh Sharma
Senior Security Researcher
GReAT APAC

Jin Ye
Senior Security Researcher
GReAT APAC

Mohamad Amin Hasbini
Head of GReAT META
GReAT META

Sergey Lozhkin
Principal Security Researcher
GReAT META

Maher Yamout
Lead Security Researcher
GReAT META

Sherif Magdy
Senior Security Researcher
GReAT META

Abdessabour Arous
Security Researcher
GReAT META

Mert Degirmenci
Security Researcher
GReAT META

Marco Preuss
Deputy Director, GReAT
GReAT Europe

David Emm
Principal Security Researcher
GReAT Europe

Christian Funk
Lead Security Researcher
GReAT Europe

Marc Rivero
Lead Security Researcher
GReAT Europe

Giampaolo Dedola
Lead Security Researcher
GReAT Europe

Vasily Berdnikov
Lead Security Researcher
GReAT Europe

Jornt van der Wiel
Senior Security Researcher
GReAT Europe

Dan Demeter
Senior Security Researcher
GReAT Europe

Joao Godinho
Senior Security Researcher
GReAT Europe

Robin Kwiatkowski
Security Researcher
GReAT Europe

Igor Kuznetsov
Director GReAT
GReAT

APAC

Europe

Middle East & Africa

North America

Russia

LatAm

Kurt Baumgartner
Principal Security Researcher
GReAT US

Fabio Assolini
Head of GReAT LatAm
GReAT LatAm

Fabio Marenghi
Senior Security Researcher
GReAT LatAm

Anderson Leite
Security Researcher
GReAT LatAm

Lisandro Ubiedo
Security Researcher
GReAT LatAm

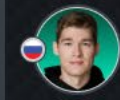
Leandro Cuozzo
Security Researcher
GReAT LatAm

Maria Isabel Manjarrez
Security Researcher
GReAT LatAm

Dmitry Galov
Head of GReAT Russia and CIS
GReAT Russia

Sergey Mineev
Principal Security Researcher
GReAT Russia

Sergey Belov
Principal Security Researcher
GReAT Russia



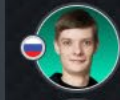
Boris Larin
Principal Security Researcher
GReAT Russia

Tatyana Shishkova
Lead Security Researcher
GReAT Russia

Konstantin Zykov
Senior Research Developer
GReAT Russia

Ilya Saveliev
Security Researcher
GReAT Russia

Leonid Bezvershenko
Security Researcher
GReAT Russia



Georgy Kucherin
Security Researcher
GReAT Russia

Dmitry Pikush
Junior Security Researcher
GReAT Russia

Polina Tretyak
Intern
GReAT Russia

kaspersky

Источники аналитических данных об угрозах

Масштаб современных угроз в сфере ИБ: 2023

220K+

компаний по всему миру мы оберегаем от киберугроз

6,1 млрд

кибератак было остановлено нашими решениями

437 млн

вредоносных атак, которые проводились с интернет-ресурсов, размещенных в различных странах мира, было отражено

325K

уникальных пользователей были защищены от вредоносного ПО для кражи денежных средств через онлайн-доступ к банковским счетам на устройствах

Про какие угрозы мы говорим, и что с ними делать?

411 000

Уникальных вредоносных объектов мы детектируем ежедневно (403 000 в 2023)

> 99%

Детектируются автоматизированными системами

106 млн

Уникальных вредоносных URL было обнаружено в 2023 году

> 200

Активных групп, связанных с Advanced Persistent Threat

Кибератаки на пользователей в Армении: 2024

26%

рядовых пользователей столкнулись с локальными угрозами

25%

корпоративных пользователей подверглись локальным угрозам

27%

корпоративных пользователей столкнулись с веб-угрозами

265K

попыток перехода пользователей на фишинговые страницы

25K

атак на мобильные устройства

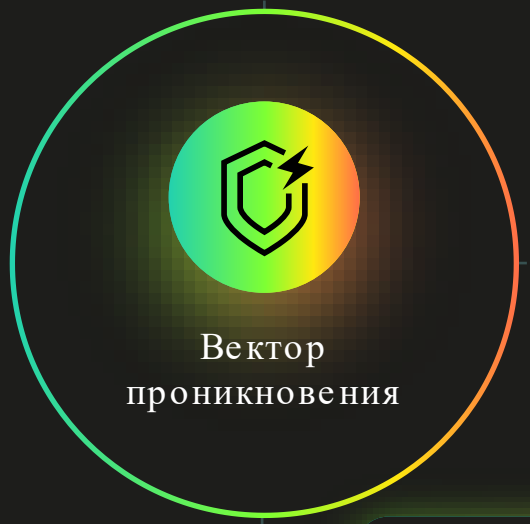
5,38%

доля почтового спама

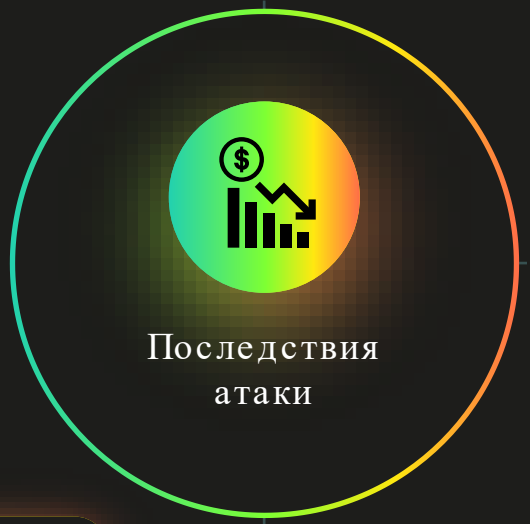
Источники: данные срабатывания решений Kaspersky за январь — май 2024

Общая информация по инцидентам в 2023 году

~75% попыток эксплуатации уязвимостей в 2023 году имели отношение к Microsoft Office



- 42,3% — Эксплуатация публично доступных приложений
- 20,3% — Скомпрометированные учетные данные
- 8,5% — Подбор паролей



- 33,3% — Зашифрованные данные
- 21,1% — Утечка данных
- 12,2% — Компрометация Active Directory

Важно также помнить про:
- Атаки на цепочки поставок (6,8%) – сейчас является трендом
- Таргетированный фишинг (5,1%) – вечная угроза для компаний

Индустрии

27,9%	12,2%	17,0%	8,8%
Государственный сектор	Финансовые организации	Промышленность	ИТ-компании

Регионы

47,3%	21,8%	10,9%	9,1%
Россия и СНГ	Америки	Ближний Восток	Европа

Источник: Incident Response Analyst Report 2023, Kaspersky (https://content.kaspersky-labs.com/se/media/ru/business-security/ir-analytical-report-2023.pdf)

Кибератаки в России и СНГ в 2022–2023 годах

Всплеск активности

- Собственная активность «хактивистов»
- Атаки, спонсируемые иными странами
- Атаки спецслужб иных стран

Приоритеты атакующих

- Нарушение критических процессов, с максимальным уроном
- Кибершпионаж
- Пропагандистские акции и дезинформация

Мишени атакующих

- Критические инфраструктуры и важные коммерческие поставщики
- Информационные порталы и ресурсы госслужб
- Расширенный спектр компаний-целей, участвующих в важных цепочках поставок

Наиболее атакуемые сектора экономики

20%

Промышленные предприятия

17%

Финансовые учреждения

14%

СМИ

8%

Информационные технологии

Источник: Данные по России Managed Detection and Response 2023, Kaspersky (https://content.kaspersky-labs.com/se/media/ru/business-security/mdr-analytical-report-2023.pdf)

1

Атаки на службу удалённого рабочего стола (RDP)

злоумышленники используют подобранные или украденные ранее учётные данные

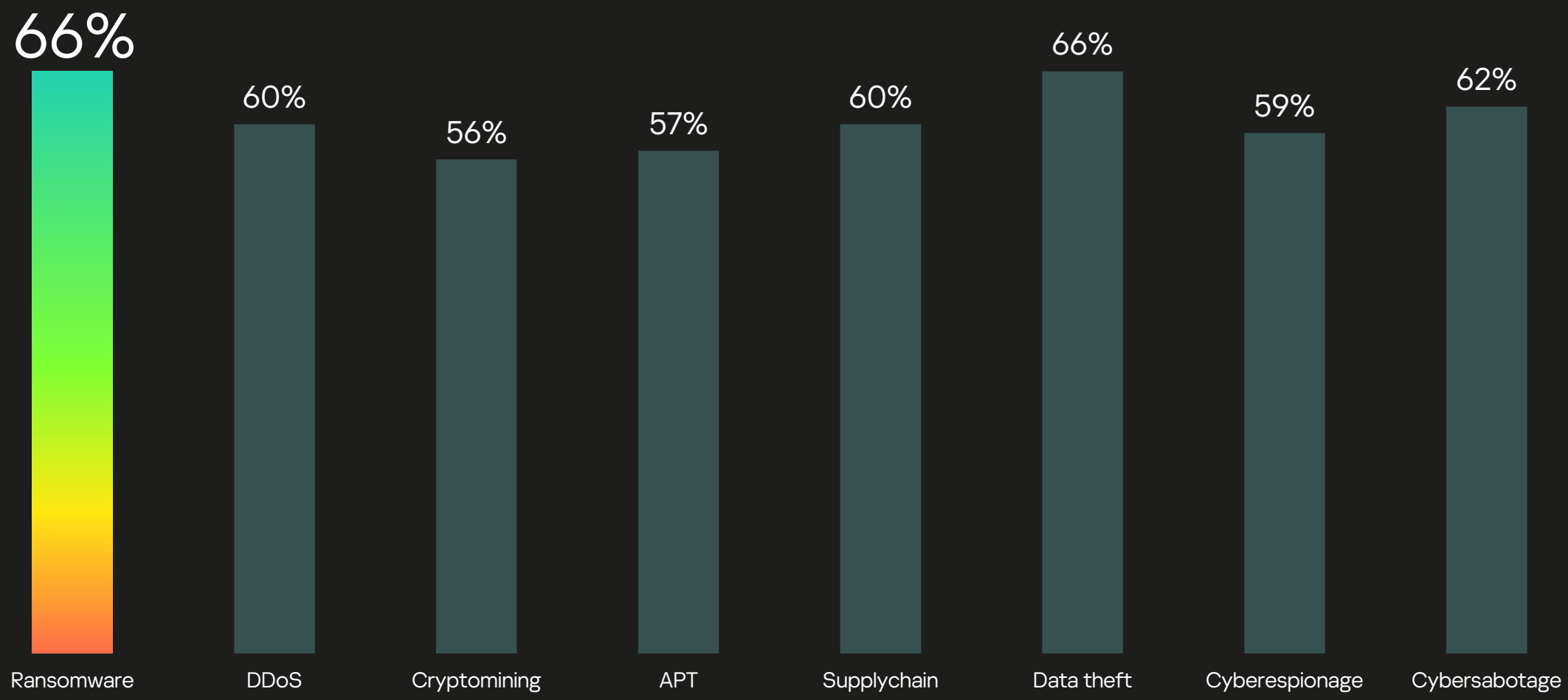
2

Фишинговые письма с вредоносными вложениями или ссылками

3

Вредоносные файлы на общедоступных ресурсах под видом образцов документов

Опрос: Вероятность различных типов угроз



Источник: Kaspersky Survey, 2022

Масштаб современных киберугроз для бизнеса

1

Отношение руководителей

68% руководителей считают, что ИБ-риски растут

2

Мотивация кибератак

71% атак финансово мотивированы

3

Рост атак шифровальщиков

В 2021-2022 доля пользователей, которые подверглись целевым атакам выросла почти в два раза

4

Инциденты

Уже три года шифрование данных остается для пользователей проблемой №1

5

Это плохо?

Количество попыток заражений упало на 36% в I квартале 2023 по сравнению с аналогичным периодом прошлого года

Да, но ситуация становится ещё более непростой!

* Kaspersky, Accenture, Verizon

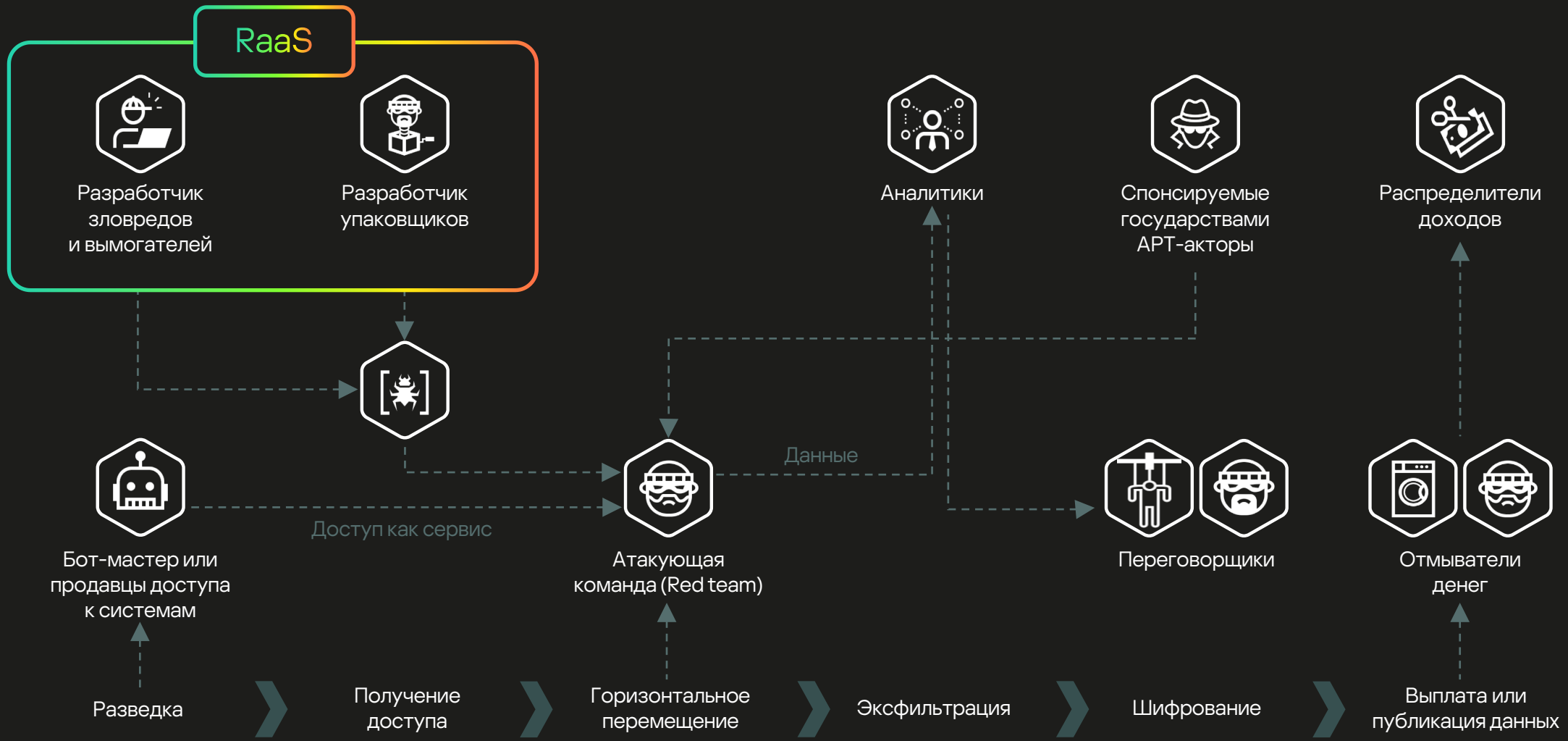
3 мифа о шифровальщиках

Киберпреступники — это компьютеризированные уголовники

Цели вымогательских атак определяются заранее

Банды кибервымогателей — это автономные группировки

Экосистема вымогательского «бизнеса»



Новые технические возможности

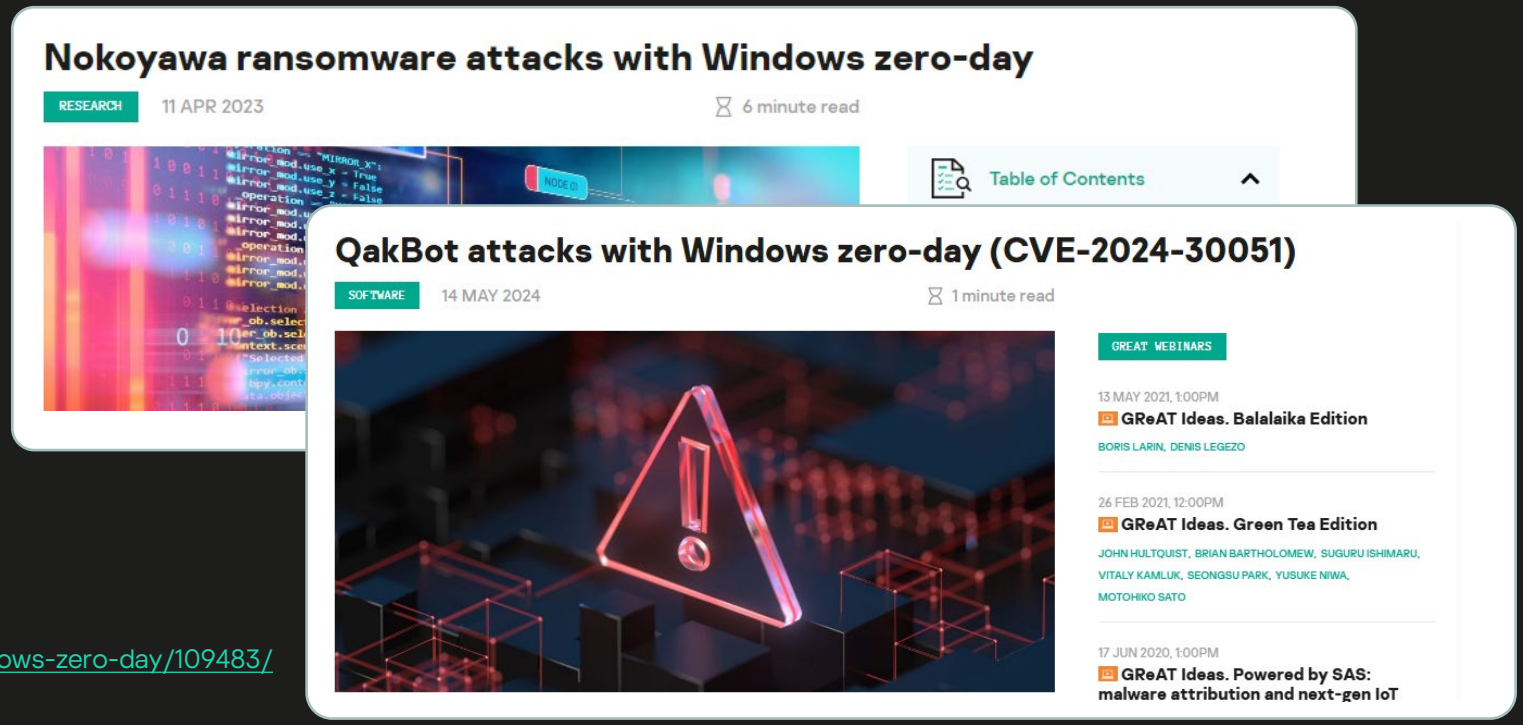
Мульти-платформенные шифровальщики становятся максимально адаптивными, новые техники самозащиты

0 days

Киберпреступники могут позволить покупку уязвимостей нулевого дня. Ранее они использовались только в APT атаках

Различные «бизнес-планы»

Для привлечения большего числа аффилированных лиц. Например, Lockbit поддерживает 3 различные версии одновременно



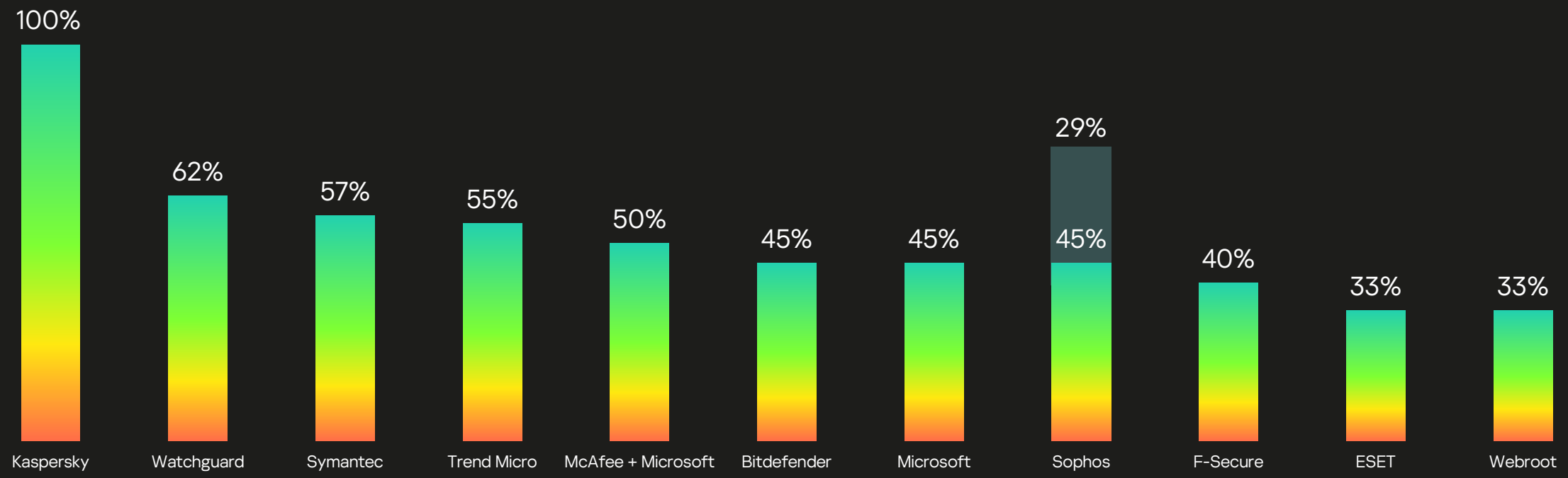
https://securelist.com/nokoyawa-ransomware-attacks-with-windows-zero-day/109483/
https://securelist.com/cve-2024-30051/112618/

Лучшая защита от шифровальщиков

Комплексная защита от Ransomware

Атака полностью заблокирована

Атака частично заблокирована



Лучшая защита от шифровальщиков

HOME USER WINDOWS

Advanced Threat Protection test

Protection against ransomware under Windows 10

AV-TEST The independent IT-Security Institute Magdeburg Germany

Manufacturer	Product
Avast	One Essential
AVG	Internet Security
Bitdefender	Internet Security
Kaspersky	Internet Security
Microsoft	Defender Antivirus
Microworld	Internet Security Suite
PC Matic	Application Whitelisting
F-Secure	SAFE
G DATA	Total Security
VIPRE Security	AdvancedSecurity
Norton	Norton 360
Malwarebytes	Premium
Avast	Free Antivirus

BUSINESS WINDOWS

Advanced Threat Protection test

Corporate protection vs. Ransomware

AV-TEST The independent IT-Security Institute Magdeburg Germany

APPROVED ENDPOINT PROTECTION WINDOWS ADVANCED

Manufacturer	Product	AV-TEST Certificate	Detected attacks (max. 10)	Protection score (max. 30 pts)
Avast	Business Antivirus Pro Plus		10	30.0
Bitdefender	Endpoint Security		10	30.0
Bitdefender	Endpoint Security (Ultra)		10	30.0
Check Point	Endpoint Security		10	30.0
Xcitium	Client Security		10	30.0
Kaspersky	Endpoint Security		10	30.0
Kaspersky	Small Office Security		10	30.0
Microsoft	Defender Antivirus		10	30.0
VMware	Carbon Black Cloud		10	30.0
WithSecure	Elements Endpoint Protection		10	30.0
G DATA	Endpoint Protection Business		10	29.0
Trellix	Endpoint Security		10	29.0

AV-TEST October 2022

www.av-test.org

No More Ransom! Не плати!

Иногда зараженному пользователю можно помочь получить доступ к зашифрованным файлам или заблокированной системе без необходимости платить выкуп

Мы создали хранилище ключей и утилит, позволяющих расшифровать данные, заблокированные троянцами-вымогателями разных типов

С 2018 года более 1,5 миллиона пользователей по всему миру смогли восстановить свои данные

Операция Триангуляция

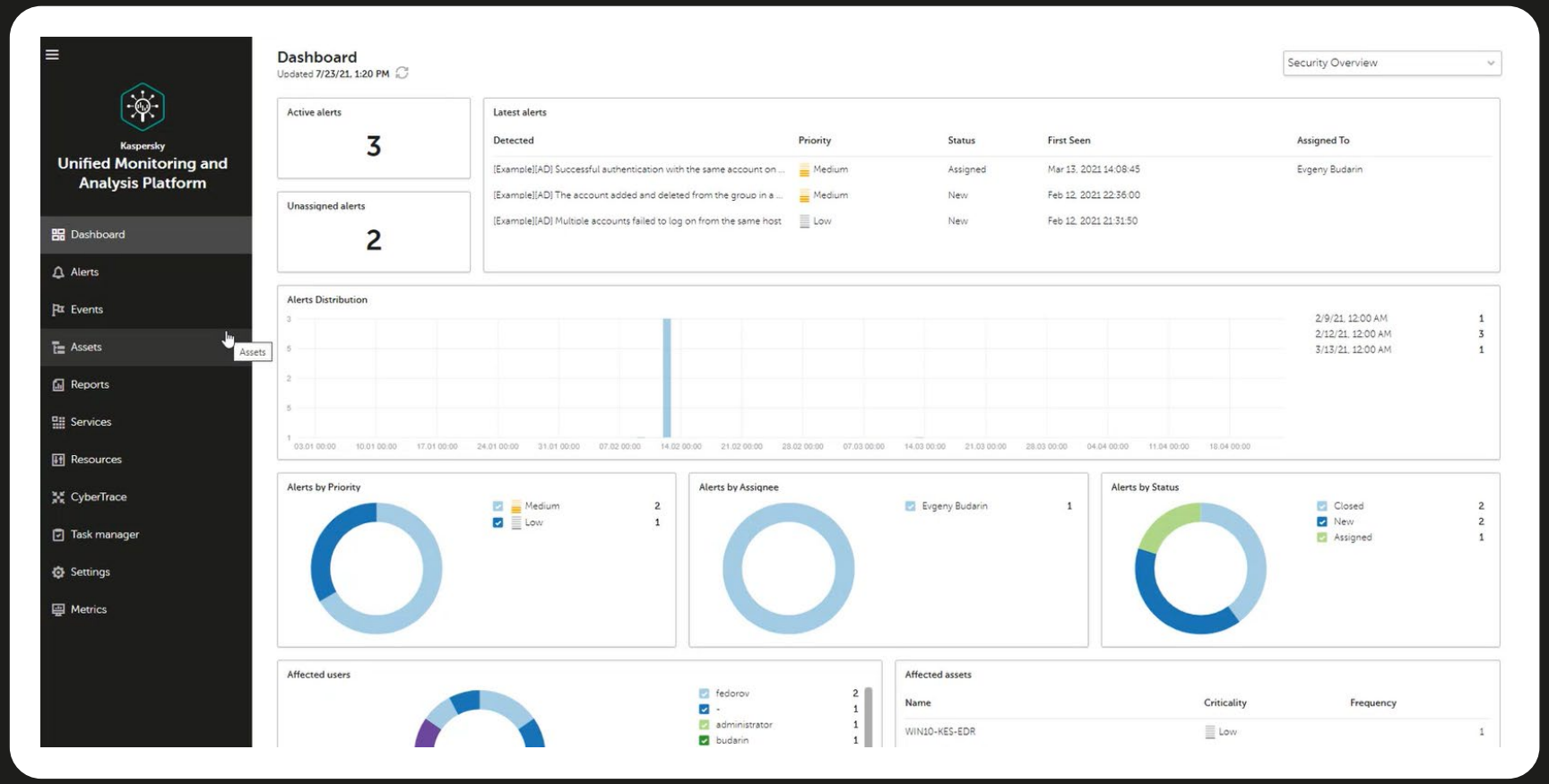
Операция Триангуляция: ранее неизвестная целевая атака на iOS-устройства

ОТЧЕТЫ О ЦЕЛЕВЫХ АТАКАХ (APT) 01 ИЮН 2023

5 мин. на чтение

Содержание

Обнаружение: SIEM-система Kaspersky Unified Monitoring and Analysis Platform



Заражение «Триангуляцией»

1

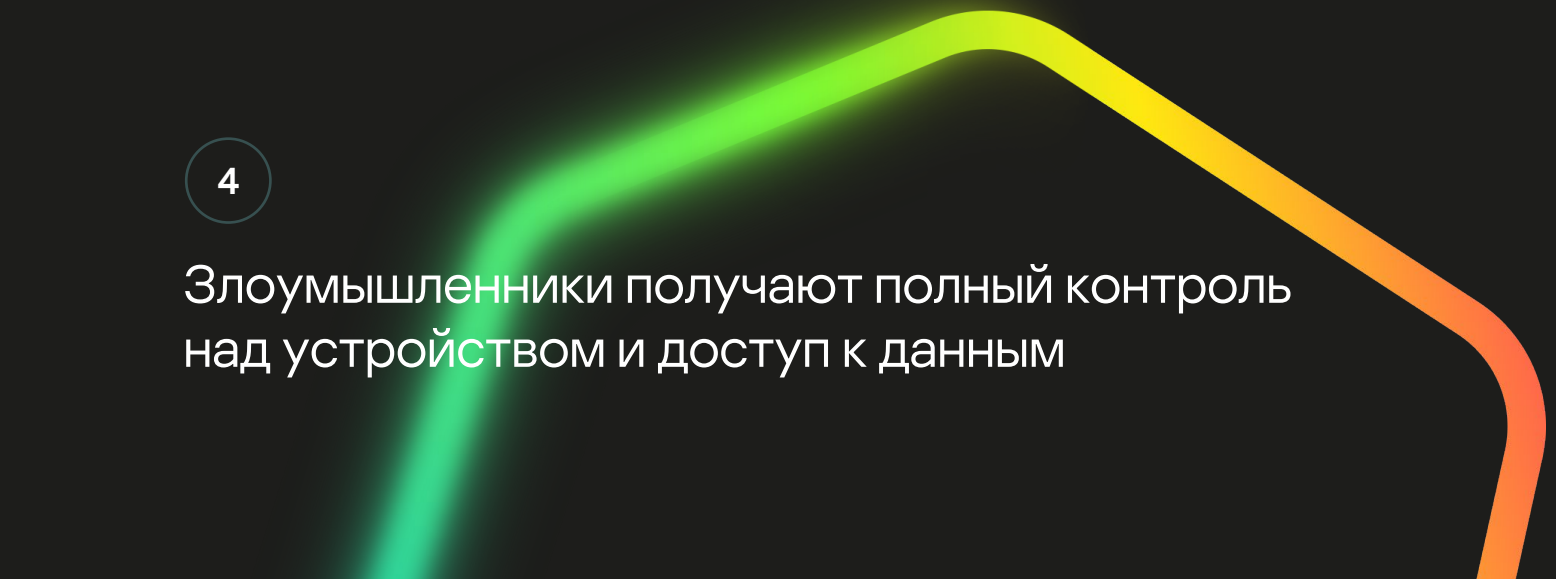
Устройство получает невидимое сообщение iMessage с вредоносным вложением

2

Без взаимодействия с пользователем, эксплойт из сообщения вызывает выполнение вредоносного кода

3

Код соединяется с сервером управления и приводит к последовательной загрузке нескольких «ступеней» вредоносной программы



4

Злоумышленники получают полный контроль над устройством и доступ к данным

5

Все следы удаляются в процессе заражения

Уникальные технические возможности атакующих

4

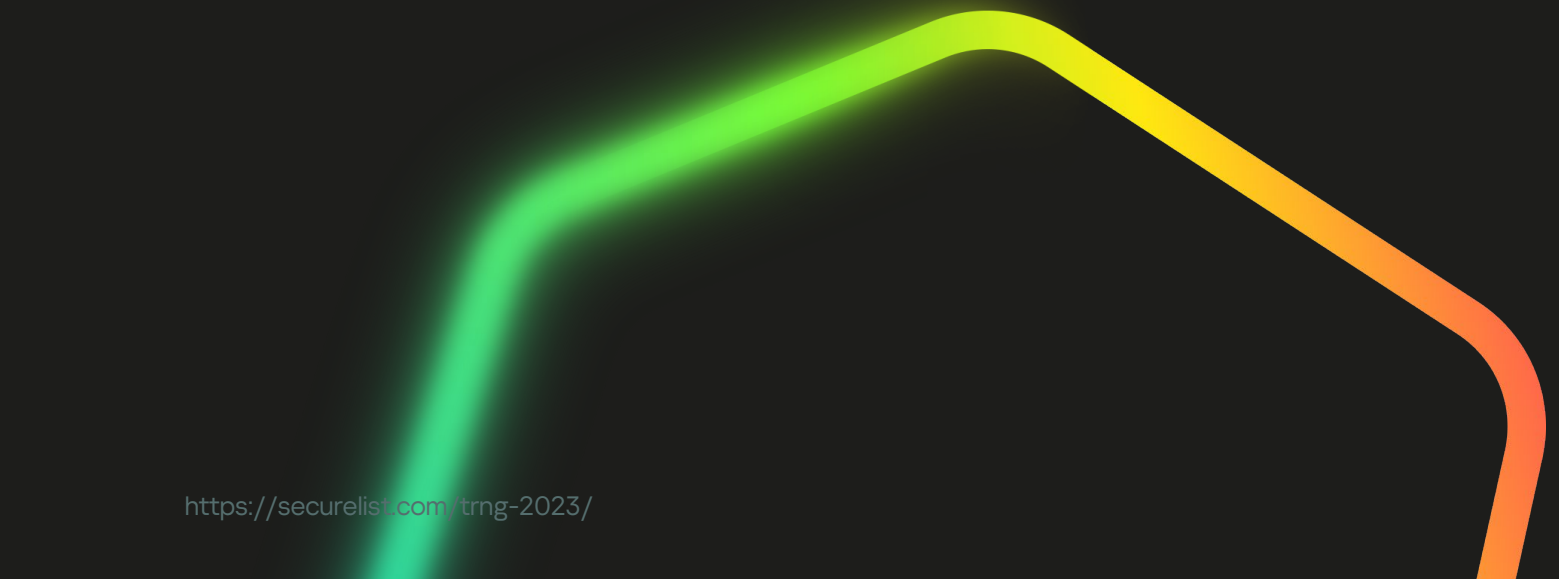
уязвимости нулевого дня использовались для заражений устройств

1

аппаратная уязвимость в процессорах Apple

>$1 млн

рыночная стоимость использованных эксплойтов



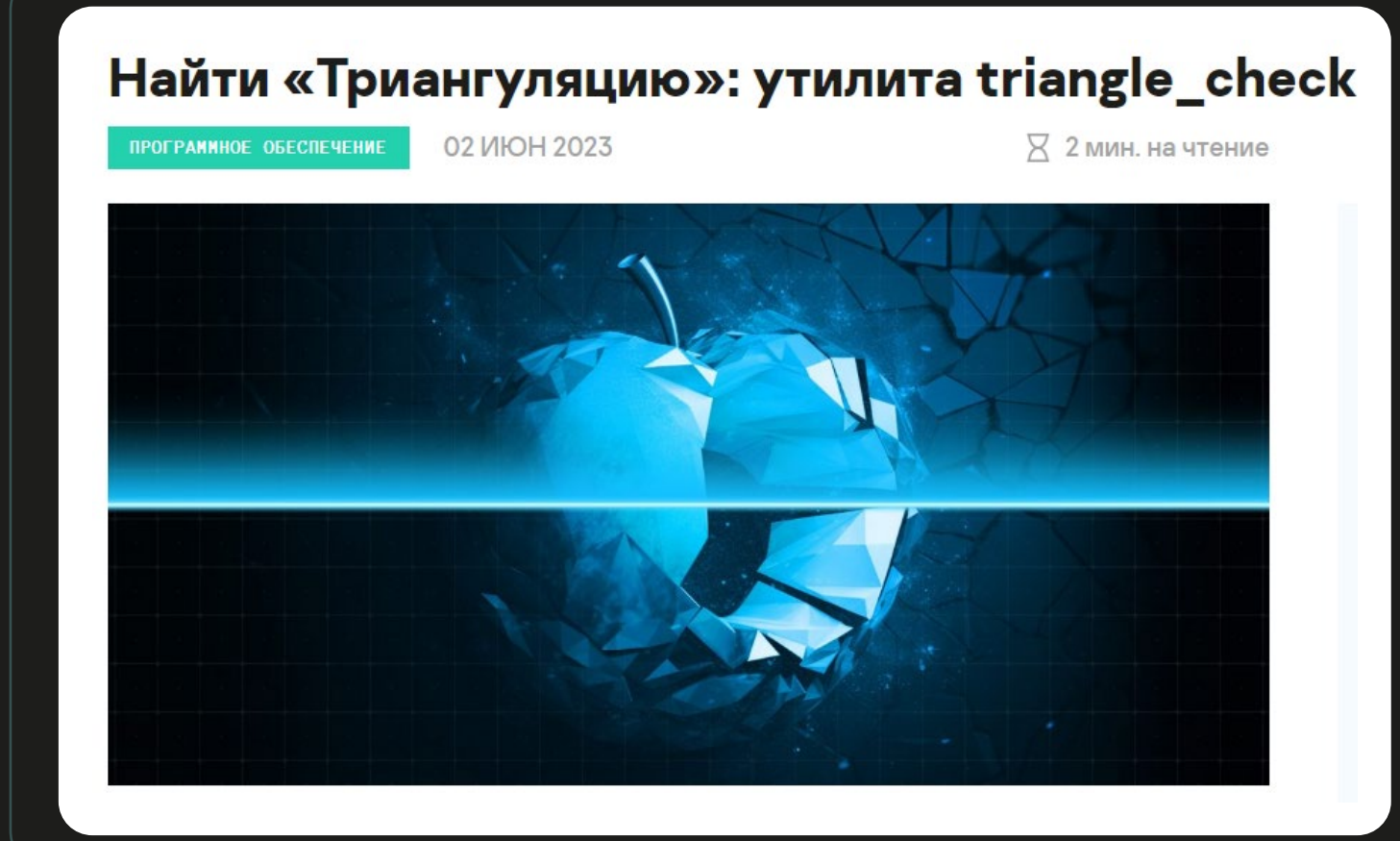
https://securelist.com/trng-2023/

Защита от «Триангуляции»

Оперативное
обновление iOS

Регулярная
перезагрузка

Отключение
iMessage



Атаки на цепочку поставок

241 npm and PyPI packages caught dropping Linux cryptominers

NPM supply-chain attack impacts hundreds of websites and apps

Python library 'ctx' uploads secrets to a Heroku endpoint

Heavily downloaded PyPI package 'ctx' has been compromised sometime this month with n
published versions exfiltrating your environment variables to an external server.

'ctx' is a minimal Python module that lets developers manipulate their dictionary ('dict') obj
variety of ways. The package, although popular, had not been touched since 2014 by its dev

Two more malicious Python packages in the PyPI

INCIDENTS 16 AUG 2022 4 minute read

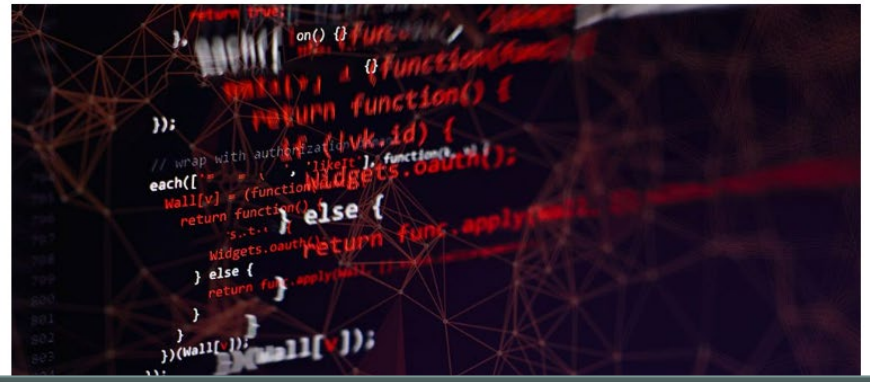
XZ backdoor story – Initial analysis

INCIDENTS 12 APR 2024 12 minute read

the Openwall OSS-security mailing list marked an
security, open source and Linux communities: the
XZ is a compression utility integrated into many popular

Not just an infostealer: Gopuram backdoor deployed through 3CX supply chain attack

APT REPORTS 03 APR 2023 4 minute read



GREAT WEBINARS

13 MAY 2021, 1:00PM
GReAT Ideas. Bala
BORIS LARIN, DENIS LEGEZO

26 FEB 2021, 12:00PM
GReAT Ideas. Gree
JOHN HULTQUIST, BRIAN BARTH
SUGURU ISHIMARU, VITALY KAML
YUSUKE NIWA, MOTOHIKO SATO

SECURELIST

INCIDENTS

LofyLife: malicious npm packages steal Discord tokens and bank card data

28 JUL 2022 1 minute read

Немного статистики по Opensource

Сотни миллионов

Opensource пакетов пакетов доступны разработчикам

100M+

Разработчиков используют GitHub

670

Вредоносных opensource пакетов обнаруживается в месяц в среднем

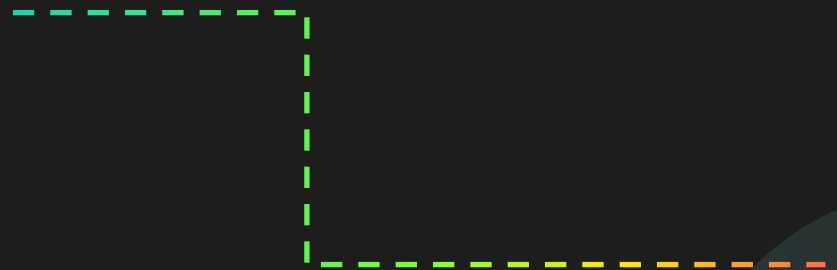
12 000

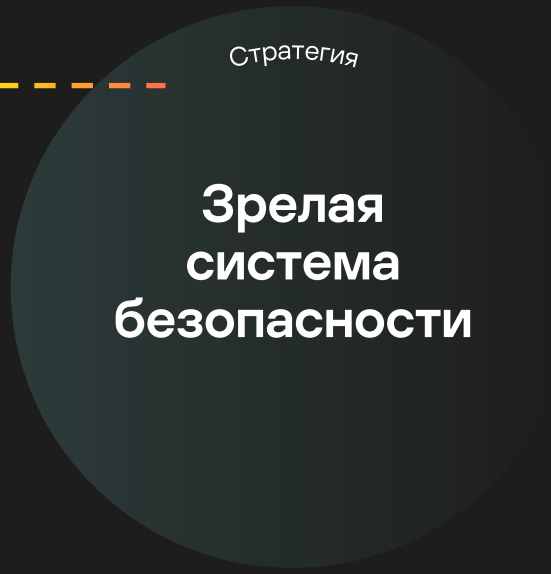
Уязвимых opensource пакетов известно к настоящему времени

Статистика взята из публичных источников, а также на основе внутренних данных Лаборатории Касперского по обнаружению вредоносных и уязвимых opensource пакетов.

Что необходимо компаниям в 2024 году?

Стратегия



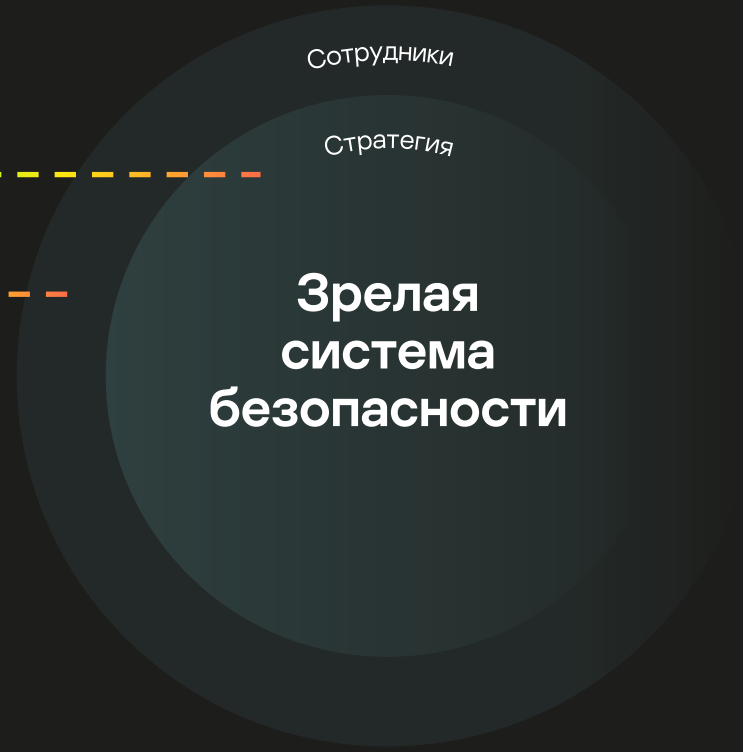


encyclopedia.kaspersky.ru/knowledge/strategies-for-mitigating-advanced-persistent-threats-apts

Что необходимо компаниям в 2024 году?

Стратегия

Сотрудники



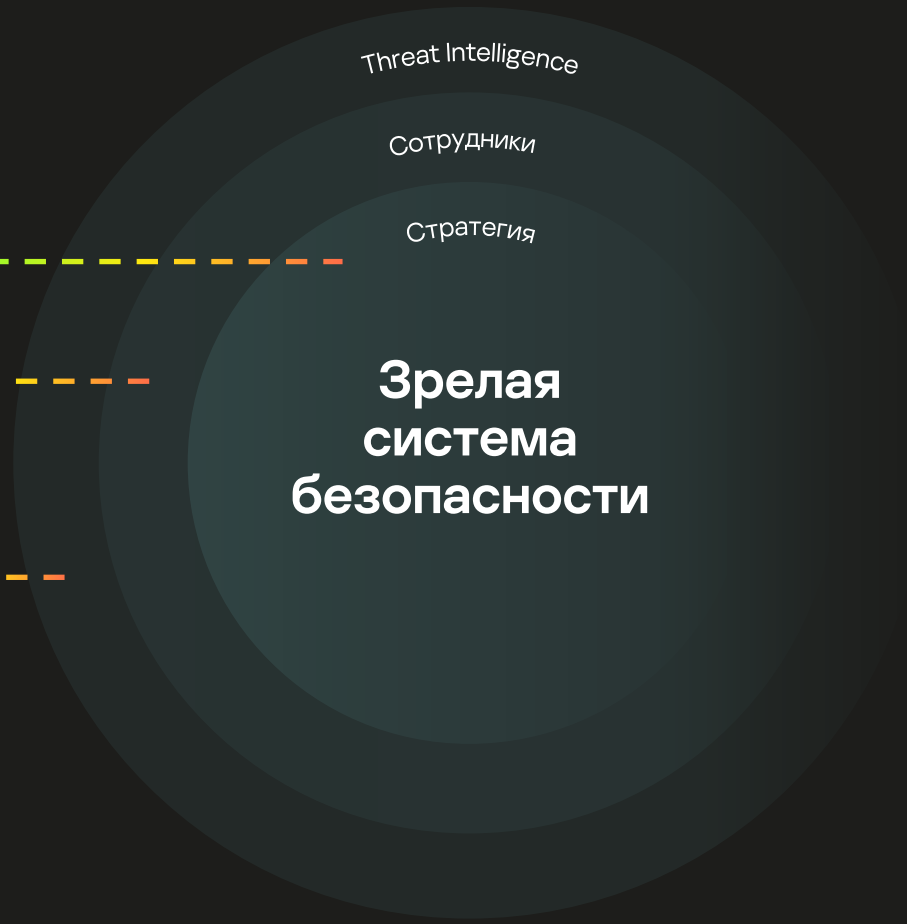
encyclopedia.kaspersky.ru/knowledge/strategies-for-mitigating-advanced-persistent-threats-apts

Что необходимо компаниям в 2024 году?

Стратегия

Сотрудники

Threat Intelligence



encyclopedia.kaspersky.ru/knowledge/strategies-for-mitigating-advanced-persistent-threats-apts

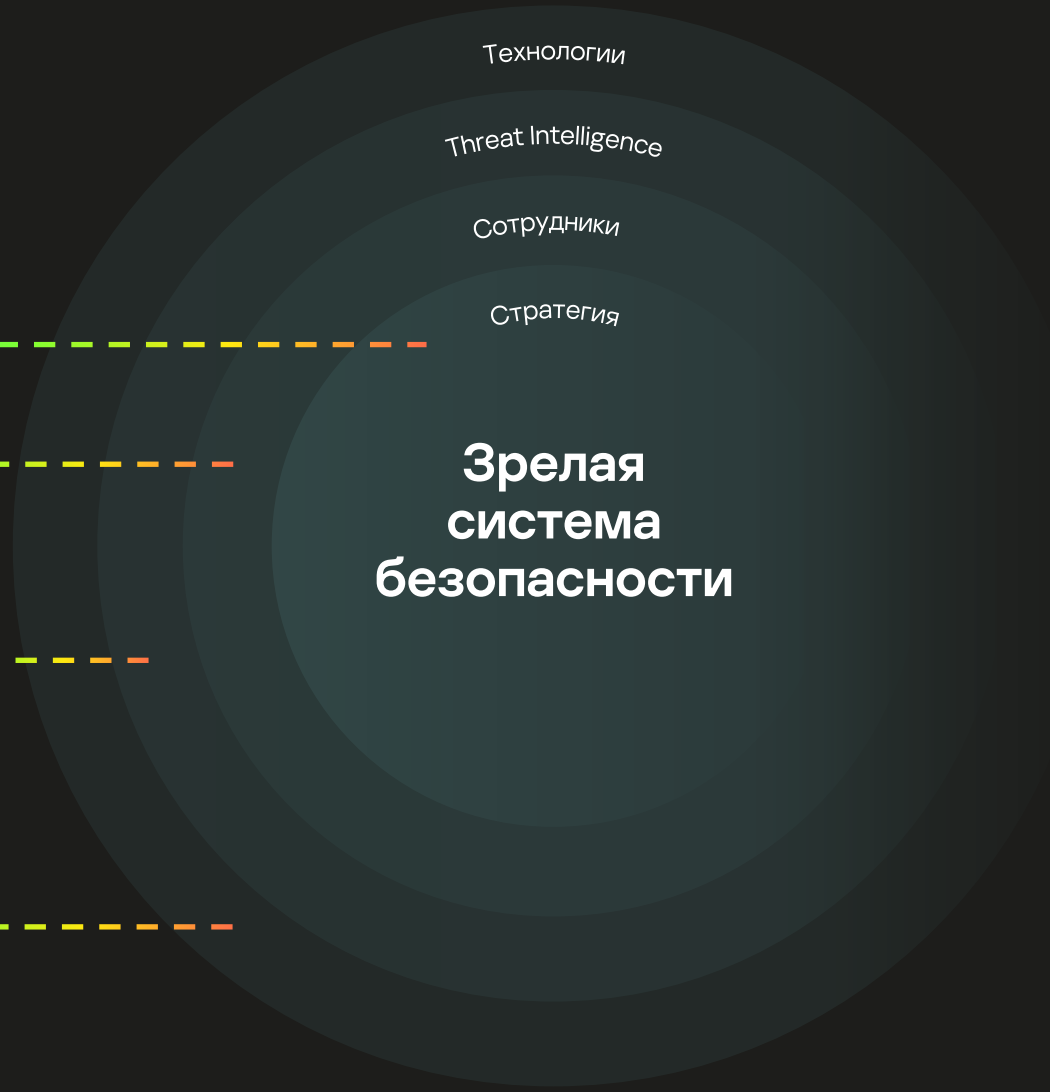
Что необходимо компаниям в 2024 году?

Стратегия

Сотрудники

Threat Intelligence

Технологии



encyclopedia.kaspersky.ru/knowledge/strategies-for-mitigating-advanced-persistent-threats-apts

Спасибо!

kaspersky