

Ampire 360°



ПЕРСПЕКТИВНЫЙ
МОНИТОРИНГ

Ampire 360°

ПОЛИГОН КИБЕРБЕЗОПАСНОСТИ



Threat Intelligence

SOC & DFIR

Offensive Security

Киберучения

ИИ и киберзащита

Киберполигон Ampire

📅 14 октября





Киберландшафт 2026

Кристина Стрельцова

Ведущий специалист направления
исследований киберугроз

Перспективный мониторинг

Анна Хромова

Заместитель начальника отдела
исследований киберугроз

Перспективный мониторинг



Тренды 2026

1

- AI как усилитель атак

2

- Переход от «реактивной» защиты к необходимости проактивной безопасности

3

- Использование легитимного доступа

4

- Рост кибершпионажа и скрытого присутствия в инфраструктуре

5

- Рост DDoS-атак

6

- Атаки через подрядчика

Каналы атаки



Съёмные
носители/сетевые
папки



Почта и
фишинг



Мессенджеры



Подрядчики



VPN/RDP/RDWeb



Уязвимости

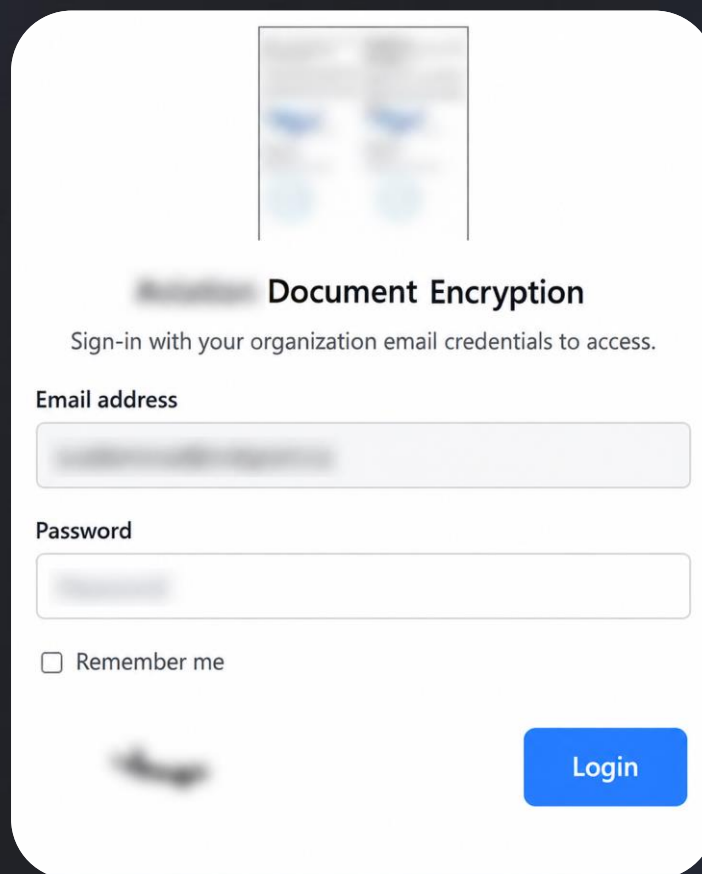
Немного статистики

- Рост DDoS-атак в России



Немного статистики

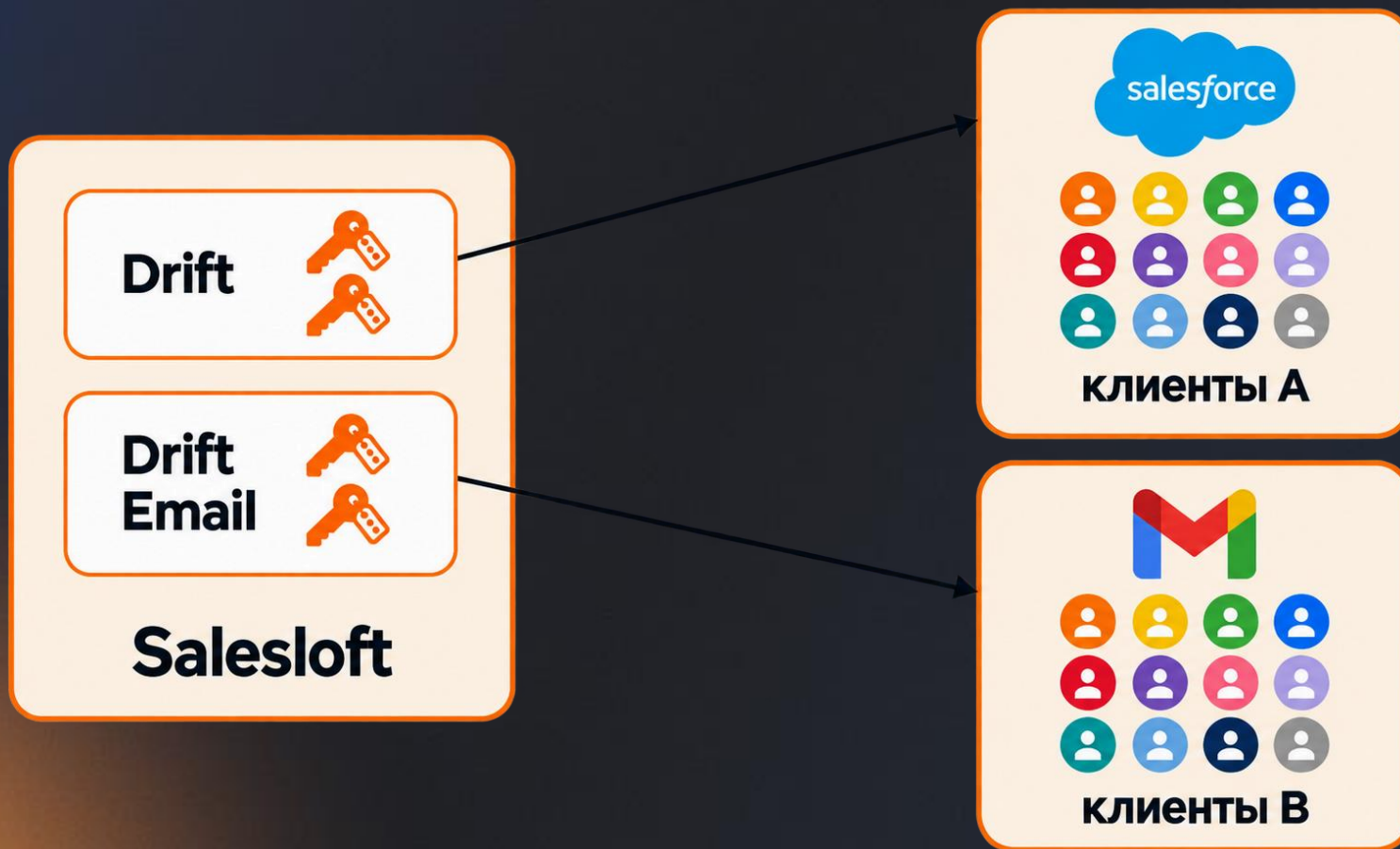
65%*



The screenshot shows a login interface for 'Document Encryption'. At the top is a blurred image of a document. Below it, the title 'Document Encryption' is followed by the instruction 'Sign-in with your organization email credentials to access.' There are two input fields: 'Email address' and 'Password'. Below the password field is a checkbox labeled 'Remember me'. A blue 'Login' button is positioned at the bottom right of the form. The entire interface is reflected below it.

- ▶ Использование учётных данных

Крупный кейс на международном рынке

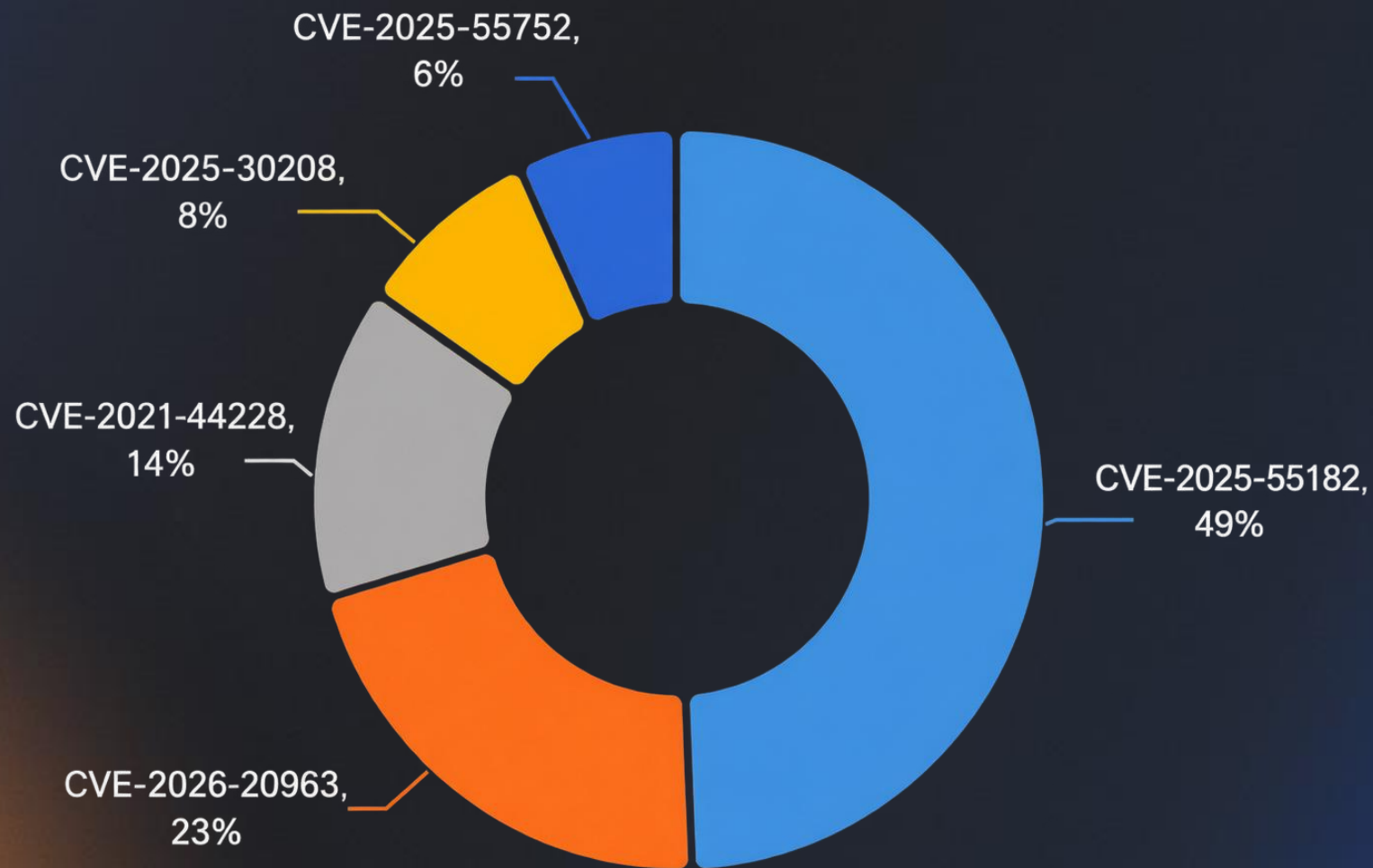


Уязвимости

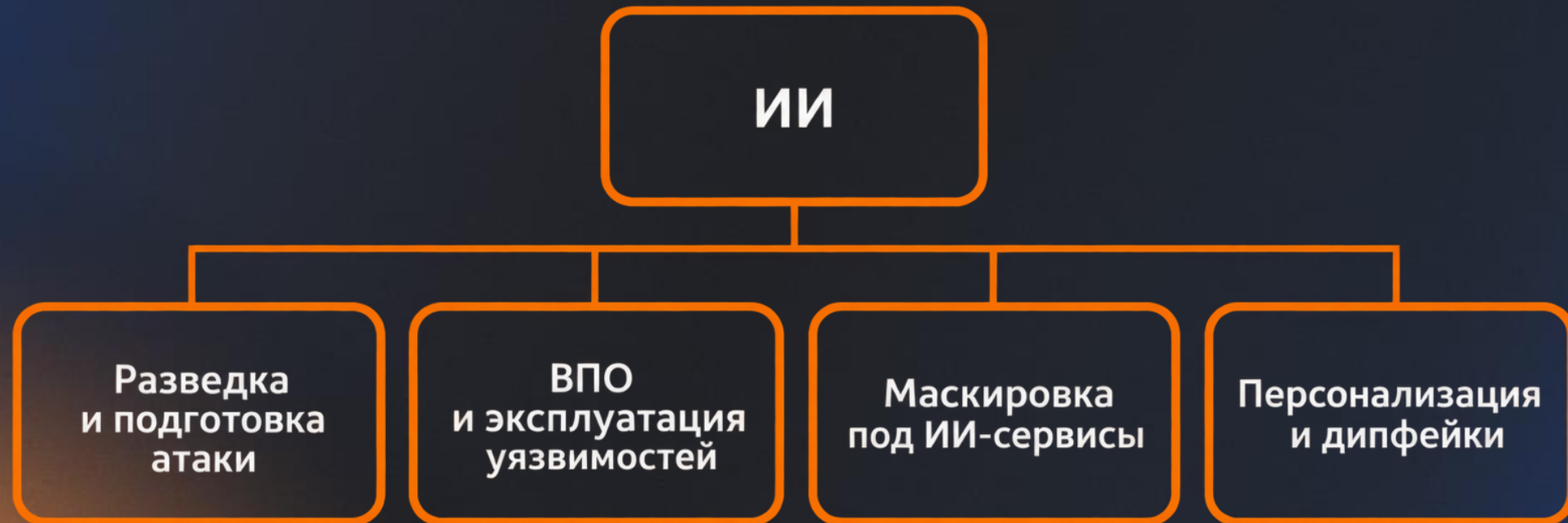


По данным cve.org

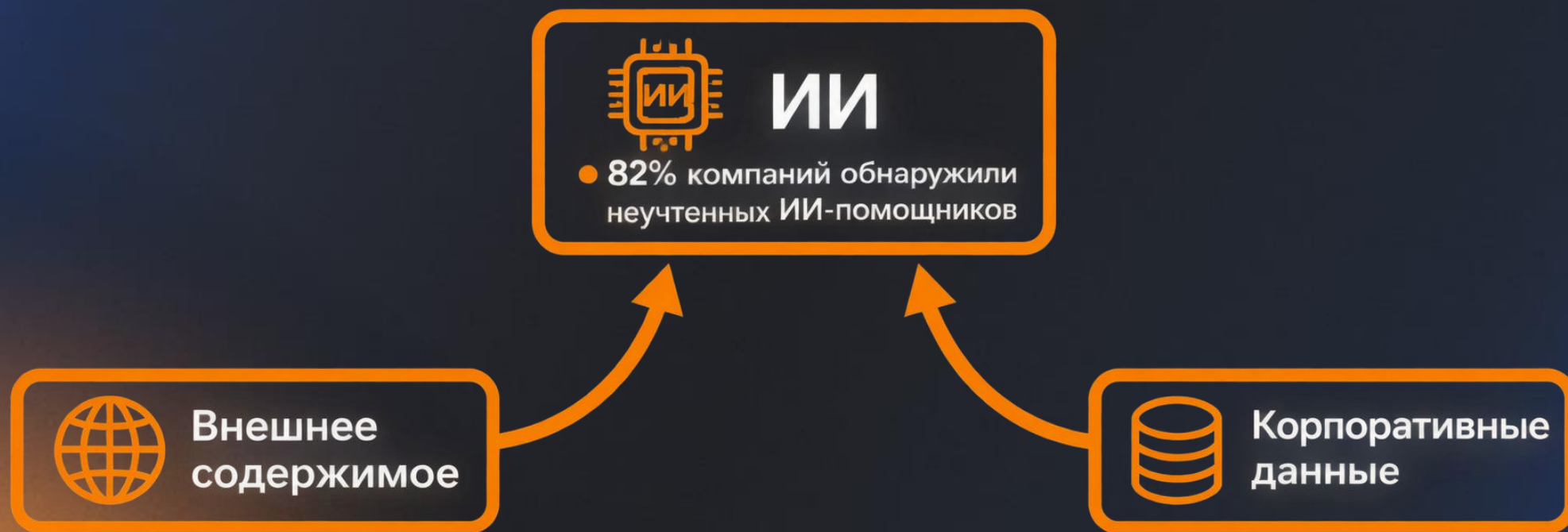
Наиболее эксплуатируемые



Фишинг и ИИ



ИИ-помощник в корпоративной среде



Атаки через
поддельные ИИ
сервисы

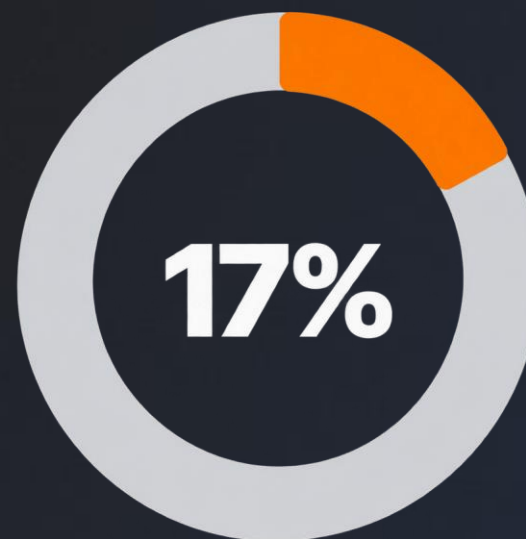
~50%

Подрядчики



1 из 4

успешных проникновений —
через подрядчика

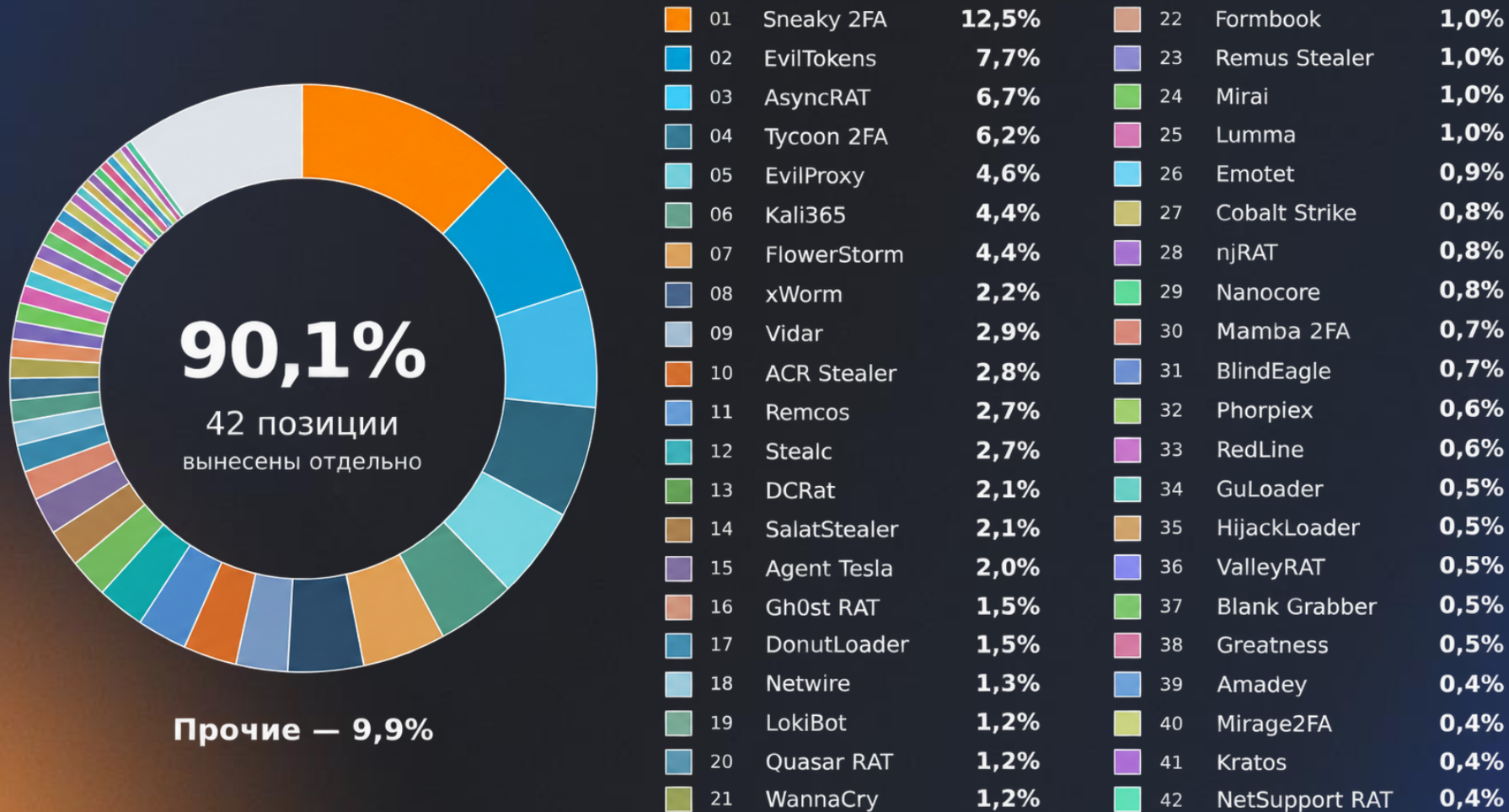


всех расследованных
инцидентов связаны
с подрядчиками

Вредоносное ПО для кражи данных и доступа

1	Vidar 2.0	MaaS, Lifetime
2	RedLine Stealer	MaaS
3	LummaC2 (Lumma)	Modular MaaS
4	Raccoon Stealer v2	IaaS (подписка)
5	StealC*	MaaS
6	BlackGuard	Infostealer
7	XWorm	RAT/Stealer/DDoS

Популярные ВПО



EvilTokens



IAB-as-a-Service — монетизация поверхности атаки



Предложения IAB



6 178

проанализированных
предложений

Telegram-каналы и теневые форумы



7-14 дней

среднее время продажи доступа

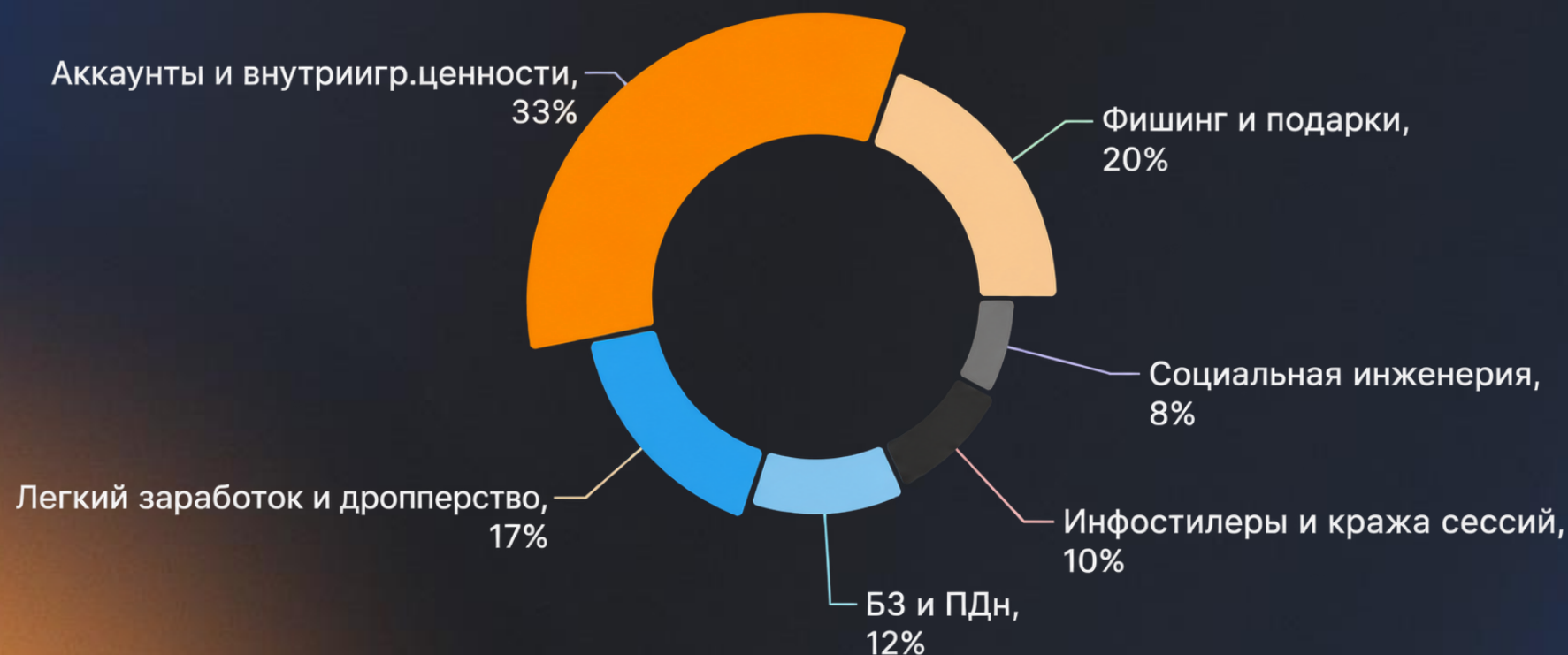
Востребованные предложения
могут быть проданы за 1-3 дня



RDP, VPN, RDWeb — 57%
наиболее распространённые
типы доступа

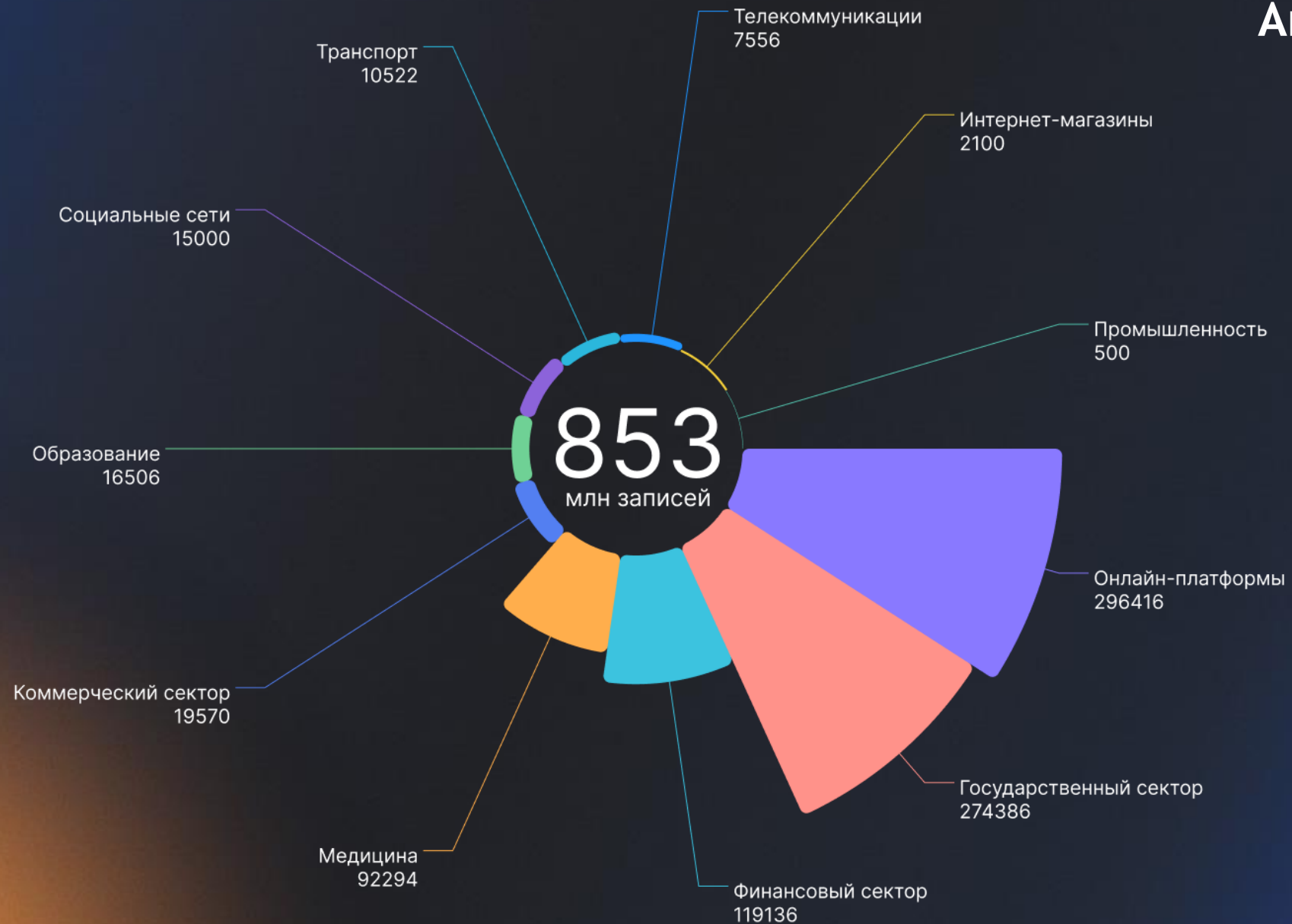
Остальное: веб-оболочки, учётные записи,
панели управления и др.

Детская безопасность. Что продают в даркнете?

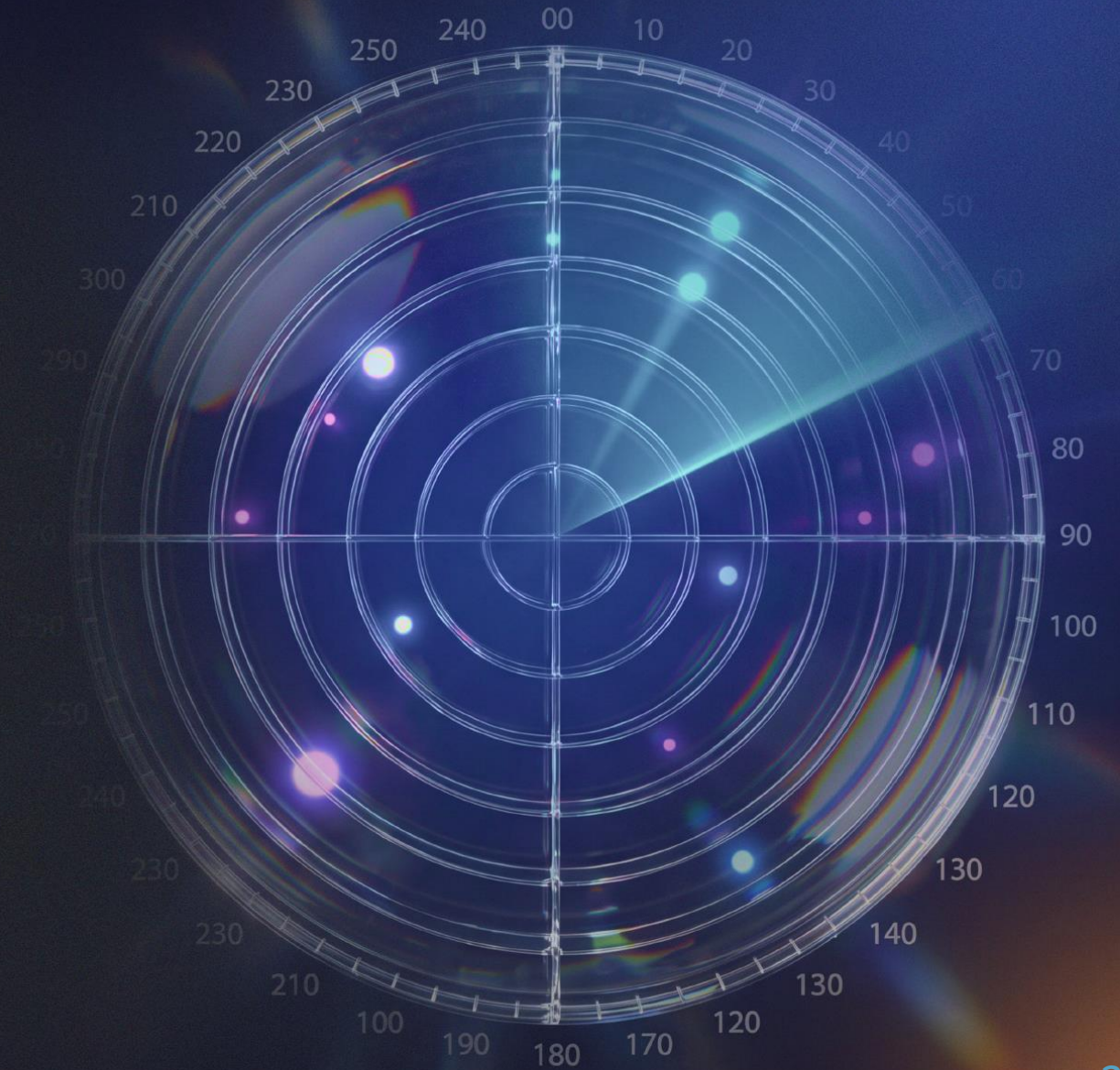


Подростки, которые
периодически или
очень часто
сталкиваются
с фейками





Актуализация ландшафта



Источники

Отчёты вендоров

Регуляторы

Внутренняя
экспертиза

Новостной фон

*Какие группировки могут добавиться

Источники

Отчёты вендоров

- А что делать, если группировка ранее не была известна?

Названия группировок (в том числе альтернативные)

Российские первоисточники

Зарубежные первоисточники

Рагнарёк: F6 исследовала атаки группировки вымогателей VantaCore

На данный момент известно как минимум о семи жертвах данной группировки. Атакующие имеют явно нескромные аппетиты: суммы запрашиваемых выкупов составляют миллионы долларов.

28 августа, 2026



Stan Ghouls targeting Russia and Uzbekistan with NetSupport RAT

05 FEB 2026

7 minute read



AUTHORS

website uses cookies

We use cookies to personalise content and ads, to provide social media features and to analyse our traffic. We also share information about your use of our site with our social media, advertising and analytics partners who may combine it with other information that you've provided to them.

Core Werewolf меняет клыки: троян CoreRAT в атаках на российские

Атакующие применили самописное вредоносное ПО



Ampire Kinomaps B.ZONE Threat Intelligence

© 12 минут 30 июня 2026 г.

Core Werewolf и выявили ранее неизвестный троян удаленного управления с помощью 7zSFX и Rust-дропперов. Злоумышленники используют троян в Telegram. Среди предполагаемых целей атакующих — инфраструктура промышленного комплекса. Ретроспективный анализ

Источники

Отчёты вендоров

Регуляторы

Внутренняя
экспертиза

Сбор, анализ, дополнение, **добавление**
новой информации

Источники

Отчёты вендоров

Регуляторы

Внутренняя
экспертиза

Новостной фон

*Какие группировки могут добавиться

А что меняется?

Core Werewolf меняет клыки: троян CoreRAT в атаках на российские организации

Вместо UltraVNC злоумышленники применили самописное вредоносное ПО



Введение

С июня по июль 2026 года мы зафиксировали активность кластера Core Werewolf и выявили ранее неизвестный троян удаленного доступа, который назвали CoreRAT. Вредоносная нагрузка распространялась с помощью 7zSFX и Rust-дропперов. Злоумышленники проникали в инфраструктуру через фишинговые письма, которые рассылали в Telegram. Среди предполагаемых целей атакующих были российские организации государственного управления и оборонно-промышленного комплекса. Ретроспективный анализ показал, что CoreRAT использовался как минимум с марта 2026 года.

Авторы
Komanga B.ZONE Threat Intelligence
12 минут 30 июня 2026 г.

Есть ли что-то новое?

TARGETING

Отрасли

Государственный сектор

Здравоохранение

Индустрия развлечений

Инженерия

Наука

Оборонный сектор

Производство

СМИ

Связь

Строительство

Технологический сектор

Транспорт

Финансовые услуги

Энергетика

АРСЕНАЛ

Инструменты

CoreRAT (TokenBuoy)

Goodbye

MeshCentral

RClose

Reverse SSH

TokenBuoySH

UltraVNC

MITRE ATTACK

Техники

T1021.002 Remote Services: SMB/Windows Admin Shares

T1021.004 Remote Services: SSH

T1021.005 Remote Services: VNC

T1027.002 Obfuscated Files or Information: Software Packing

T1027.010 Obfuscated Files or Information: Command Obfuscation

T1036 Masquerading

T1036.004 Masquerading: Masquerade Task or Service

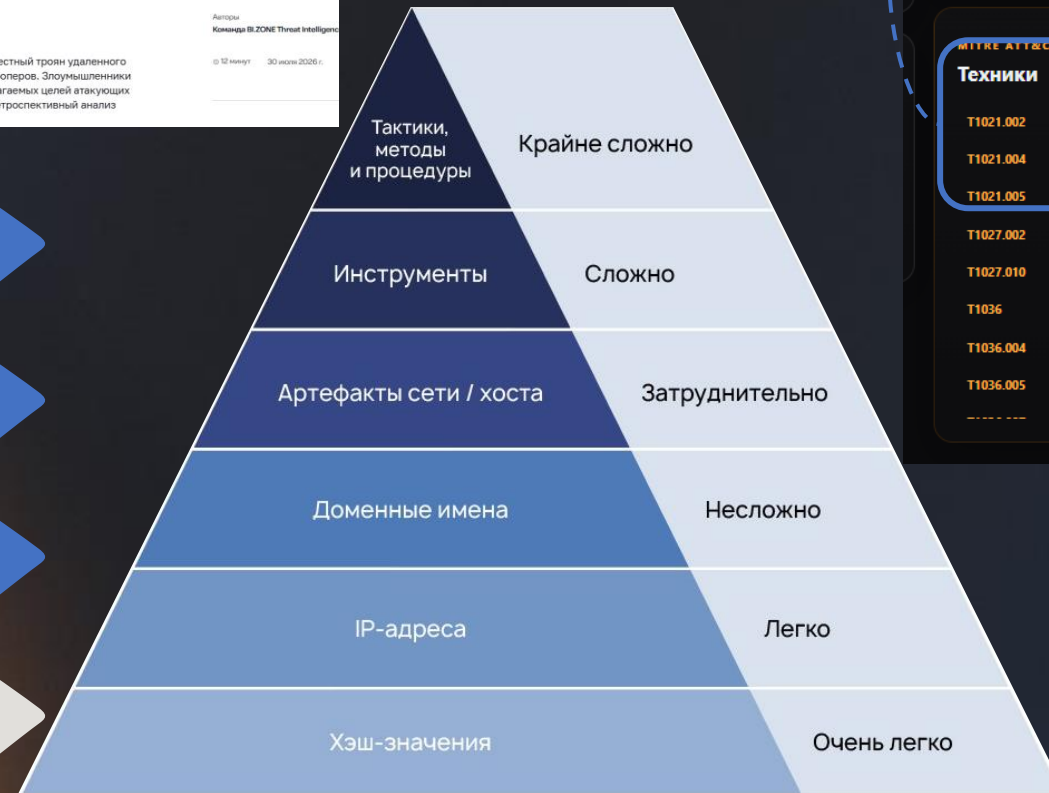
T1036.005 Masquerading: Match Legitimate Resource Name or Location

Артефакты

Инструменты

TTPs

Отрасль



С какими проблемами столкнулись?

01 Как определить корректность данных

CobaltStrike, BEACON, cobalt_strike
= одна экосистема

02 Как систематизировать данные

Габон	Габон
Гватемала	Гватемала
Германия	Германия
Голландия	Нидерланды
Гонконг	Китай
Греция	Греция
Грузия	Грузия
Дания	Дания
Доминиканская республика	Доминиканская Республика

Авиакосмическая отрасль	Авто- и авиакосмическая промышленность
Аэрокосмическая отрасль	Авто- и авиакосмическая промышленность
Ядерные исследования	Атомная энергетика
Государственное управление	Государственный сектор
Госучреждения	Государственный сектор
Добыча полезных ископаемых	Добывающая промышленность
Нефтегазовая отрасль	Добывающая промышленность
Отрасль добычи полезных ископаемых	Добывающая промышленность
Горное дело	Добывающая промышленность
Прочее	Другие
Индустрия досуга и развлечений	Индустрия развлечений
Организация досуга и развлечений	Индустрия развлечений
Развлечения	Индустрия развлечений
Компании, разрабатывающие технологии и инновации	Информационные технологии
Исламские активисты и теологи	Исламские активисты и теологи
Бизнес	Коммерческий сектор
Логистика	Логистика
Академическое сообщество	Наука
Нанотехнологии	Наука
Недвижимость	Недвижимость
Негосударственные организации	Некоммерческий сектор
Оборонная промышленность	Оборонная промышленность
Военные организации	Оборонный сектор
Оборонная отрасль	Оборонный сектор
Оборонный сектор	Оборонный сектор
Правительственные организации	Правительственные организации

Как было и как стало

Было: .xlsx-файл

1	Актор	Страны происхождения	Атакуемые страны
	Antler Werewolf		Россия, Китай
2			
3	APT-C-63		Сирия, Китай, Россия, Израиль
	APT35	Иран	Россия, США, Ближний Восток
4			
	Aquatic Werewolf		Россия

Другие названия	Атакуемые индустрии	Инструменты
Longhorn, Lamberts, APT-C-39, PLATINUM TERMINAL, Vault7, APT-Q-92	Технологический сектор, Авто- и авиакосмическая промышленность, Наука, Образование, Государственный сектор, Энергетика, Связь, Финансовые услуги, СМИ	Lambert, Athena, Fluxwire, Grasshopper, AfterMidnight, HIVE, ChimayRed, DePriMon
APT-Q-94, Triangulation, Sand Eagle	Государственный сектор, Информационные технологии	DcRAT, BPO Triangulation
Agent Serpens, COBALT MIRAGE, Charming Kitten, G0059, Magic Hound, Mint Sandstorm, Newscaster, Newscaster Team, Parastoo, Phosphorus, TunnelVision	СМИ, Энергетика, Оборонный сектор, Коммерческий сектор, Связь	
Dark River	Инженерия, Государственный сектор, Наука, Другие	MataDoor (MATAv5), CVE-2021-40444

Стало: единая платформа

A

Arcane Wolf

Mythic Likho, Arcane Werewolf

Главная особенность этой группы — использование собственных агентов для фреймворка Mythic, известных как Loki и Merlin. Эти инструменты, разработанные на базе популярных решений с открытым исходным кодом, были...

ЦЕЛЕВЫЕ СТРАНЫ

Россия

ПРОИСХОЖДЕНИЕ

Украина

15 индикаторов

1 отчетов

A

Asgard Wolf

THOR Ransomware, VantaCore

Описание группировки пока не добавлено.

ЦЕЛЕВЫЕ СТРАНЫ

Россия

ПРОИСХОЖДЕНИЕ

Не определено

23 индикаторов

1 отчетов

B

C

THREAT ACTOR - ID 6

C.A.S

Pandemonium Hydra, Cyber Anarchy Squad

Обновлено 2024-09-15

Редигировать

Описание

Общая информация

Индикаторы

Отчеты

Граф связей

профиль

Общая информация

Основное название

CAS

Другие названия

Pandemonium Hydra, Cyber Anarchy Squad

Страны происхождения

Украина

Атакуемые страны

Россия, Беларусь

Добавлено

2024-09-04

Последнее изменение

2024-09-15

ЦЕЛЕВЫЕ

Казахста

12 инди

аналитика

Особенности

Группа публикует информацию о некоторых своих атаках в Telegram-канале, где также размещает украденные данные. Во время этих атак группа крадет данные, к которым удалось получить доступ, и затем использует майнер либо шифровальщик. В качестве метода персонального доступа к инфраструктуре жертв использует компрометацию публично доступных сервисов. Было обнаружено использование CVE-2023-52447 для повышения привилегий в Linux-системах.

таргетинг

Отрасли

Государственный сектор

Индустрия развлечений

Информационные технологии

Образование

Производство

Розничная торговля

Сель

Транспорт

арсенал

Инструменты

3D

Adminer

ADRecon

Babuk

BloodHound

BOOFICE

BrowserNif

Chisel

CVE-2020-0688

CVE-2021-41773

CVE-2022-1388

CVE-2022-28113

CVE-2023-52447

Fscan

G00tM1k

LockBit

Metasploit

Meterpreter

Mimikatz

ngrok

Nmap

P0wny-shell

PBBac

RCrack

Reverse RAT

Spark RAT

TeamViewer

XenAppRansomware

MITRE ATT&CK

Техники

T1003

OS Credential Dumping

T1003.008

OS Credential Dumping / ntlmrelay and ntlmshadow

T1021.001

Remote Services: Remote Desktop Protocol

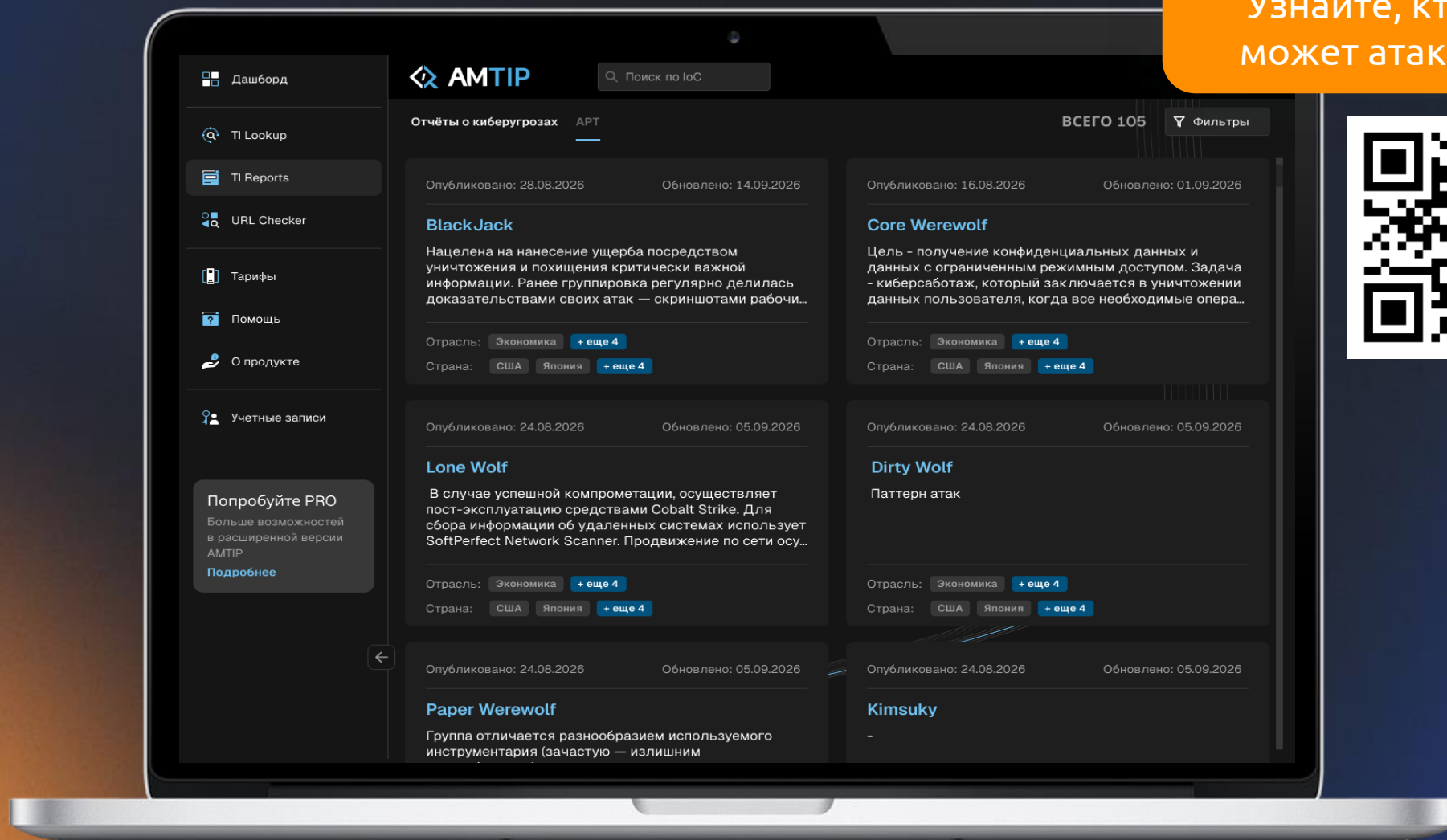
T1021.004

Remote Services: SSH

Делимся нашей экспертизой

Ampire 360°

Узнайте, кто вас
может атаковать



Благодарим за внимание

Кристина Стрельцова

Ведущий специалист направления
исследований киберугроз
Перспективный мониторинг

Анна Хромова

Заместитель начальника отдела
исследований киберугроз
Перспективный мониторинг



Ampire 360°