CYBER THREAT ANALYSIS

RUSSIA

Recorded Future®

Insikt Group®

August 27, 2026

BlueDelta Targets Defense and Diplomacy with HOOKEDGE

Insikt Group identified Russian state-sponsored group BlueDelta (APT28) targeting government, diplomatic, and defense organizations in Romania, Spain, and Türkiye between September 2025 and April 2026.

BlueDelta delivered HOOKEDGE, a lightweight batch-script successor to HEADLACE, via macro-enabled Word documents that abuse webhook[.]site for C2, payload staging, and data exfiltration.

BlueDelta continued its longstanding use of legitimate internet services for C2, payload staging, and data exfiltration, blending malicious traffic with normal web activity to evade network defenses.

Analysis cut-off date: July 20, 2026

Executive Summary

Insikt Group has identified a series of BlueDelta initial access campaigns conducted between late September 2025 and early April 2026, targeting government and diplomatic organizations in Romania, Spain, and Türkiye. The campaigns delivered a lightweight Windows batch-script backdoor, dubbed "HOOKEDGE," via macro-enabled Microsoft Word documents using diplomatic-themed lures, including material impersonating Spain's Ministry of the Presidency, Justice and Relations with the Cortes, created shortly after a September 2025 meeting between Spanish and Moldovan officials.

Insikt Group assesses with moderate confidence that this activity was conducted by BlueDelta (which overlaps with APT28, Fancy Bear, and Forest Blizzard), a Russian state-sponsored threat group attributed to the Main Directorate of the General Staff of the Armed Forces of the Russian Federation (GRU). This assessment is based on significant code and tradecraft overlap between HOOKEDGE and the HEADLACE backdoor used in prior BlueDelta campaigns, consistent infrastructure patterns, and targeting consistent with known Russian intelligence collection priorities.

HOOKEDGE shares HEADLACE's core architecture, abusing legitimate webhook services for command-and-control (C2), payload staging, and data exfiltration, enabling malicious activity to blend with legitimate network traffic while reducing the operational overhead of dedicated infrastructure. The implant has undergone continuous refinement between September 2025 and April 2026, likely to evade automated sandbox environments and adapt to reduced free-tier API limits on *webhook[.]site*.

BlueDelta continues to invest in lightweight, easily adaptable initial-access tooling to support intelligence collection against European government and diplomatic targets. Rather than introducing new capabilities, the group has steadily refined its existing tradecraft, emphasizing operational resilience by adapting established tooling to evolving defensive measures and infrastructure constraints.

Organizations should prioritize blocking macro execution from internet-originated documents and implementing detection coverage for scheduled task abuse, headless Microsoft Edge execution, and outbound connections to webhook services.

Key Findings

- Between late September 2025 and early April 2026, BlueDelta conducted a series of initial access campaigns against defense manufacturing and diplomatic organizations in Romania, Spain, and Türkiye. BlueDelta used macro-enabled Word documents to deploy HOOKEDGE, a lightweight batch-script backdoor that shares significant code and tradecraft overlap with BlueDelta's earlier implant, HEADLACE.
- The campaigns employed both diplomatic-themed and generic lures. Early activity impersonated Spanish government material, while later campaigns adopted generic macro-enablement lures. One diplomatic lure was created shortly after a meeting between Spanish and Moldovan officials, potentially reflecting an effort to collect intelligence relevant to Russia ahead of Moldova's September 2025 parliamentary elections.
- BlueDelta continued to refine HOOKEDGE between September 2025 and April 2026, introducing changes to lure documents, execution methods, and beaconing intervals while maintaining the malware's core functionality and infrastructure model.
- For targets assessed as having higher intelligence value, BlueDelta deployed a second-stage HOOKEDGE payload with a much shorter beaconing interval. This gave operators more responsive tasking and follow-on activity, while keeping the webhook endpoints used for initial access from being exhausted.
- BlueDelta has historically demonstrated a preference for legitimate internet services (LIS) to facilitate C2, payload staging, and data exfiltration, with *webhook[.]site*'s free tier serving as the group's exclusive choice across these campaigns.

Background

BlueDelta is a Russian state-sponsored threat group attributed to the Main Directorate of the General Staff of the Armed Forces of the Russian Federation (GRU), and overlaps with activity publicly tracked as APT28, Fancy Bear, and Forest Blizzard. The group has conducted espionage-focused cyber operations for more than a decade, consistently targeting government, diplomatic, defense, and policy-related organizations in support of Russian intelligence requirements.

BlueDelta has a well-documented history of obtaining initial access through spearphishing, credential theft, and lightweight custom tooling. Previous campaigns have employed malicious documents, Windows batch scripts, and living-off-the-land techniques (LotL), frequently abusing LIS and free web infrastructure for C2, payload staging, and data exfiltration. Insikt Group documented BlueDelta's 2023 use of the HEADLACE malware family, a lightweight, batch-based backdoor used during the early stages of intrusions to execute follow-on payloads and commands in initial access campaigns targeting organizations across Europe.

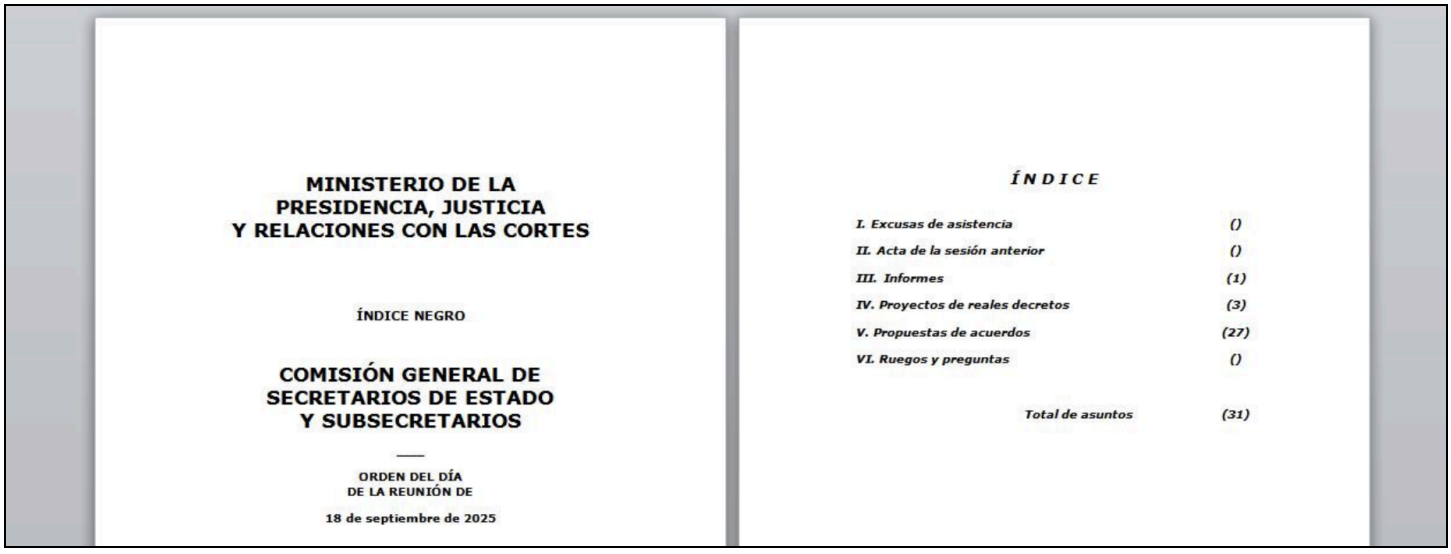
The activity detailed in this report represents a direct continuation of those operations. The HOOKEDGE backdoor shares significant code and tradecraft overlap with HEADLACE, demonstrating BlueDelta's continued preference for lightweight, easily modified malware that can be rapidly adapted to operational requirements. Similar activity has also been reported publicly by Lab52 under the name Operation MacroMaze.

Threat Analysis

Lure Documents and Targeting

BlueDelta's choice of lure documents across these campaigns reflects deliberate targeting of European diplomatic audiences and reveals collection priorities consistent with known Russian intelligence requirements. Between late September 2025 and early April 2026, Insikt Group identified several malicious macro-enabled Word documents likely used by BlueDelta in initial access campaigns targeting government or diplomatic personnel in multiple European countries.

The earliest identified lure, first seen on September 26, 2025, purported to be a September 15, 2025, meeting agenda from Spain's Ministry of the Presidency, Justice and Relations with the Cortes, as shown in **Figures 1** and **2**. Although the document's authenticity could not be verified, BlueDelta has historically used authentic government documents, including publicly available material, as phishing lures.



MINISTERIO DE LA
PRESIDENCIA, JUSTICIA
Y RELACIONES CON LAS CORTES

ÍNDICE NEGRO

COMISIÓN GENERAL DE
SECRETARIOS DE ESTADO
Y SUBSECRETARIOS

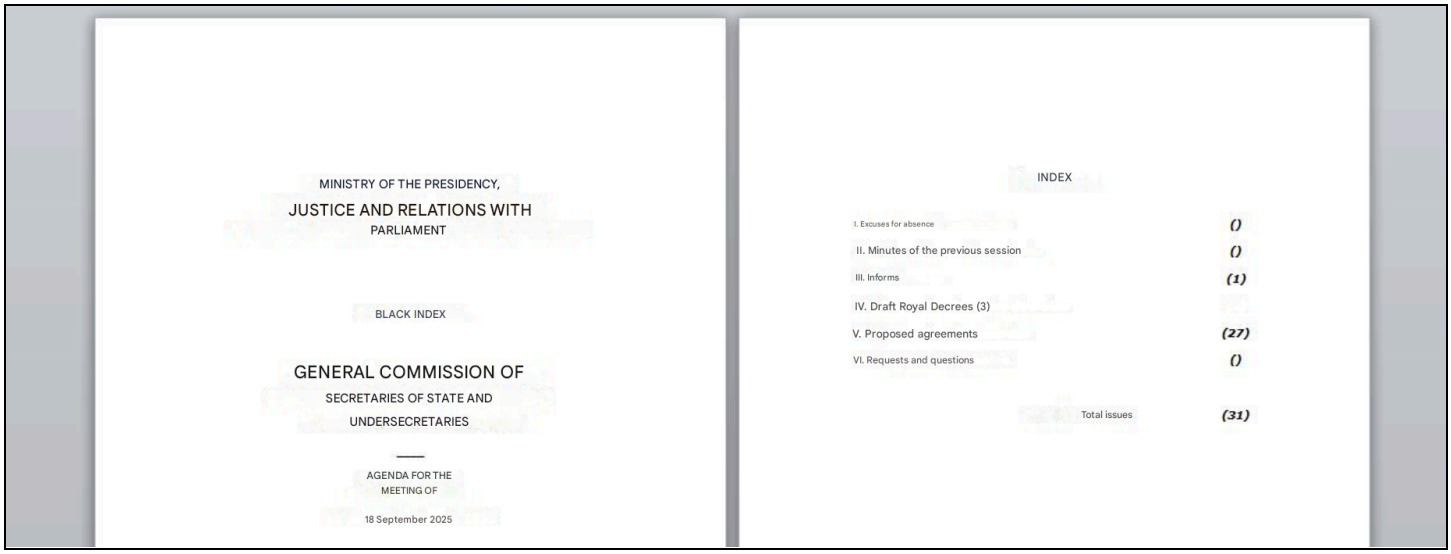
ORDEN DEL DÍA
DE LA REUNIÓN DE

18 de septiembre de 2025

ÍNDICE

I. Excusas de asistencia	()
II. Acta de la sesión anterior	()
III. Informes	(1)
IV. Proyectos de reales decretos	(3)
V. Propuestas de acuerdos	(27)
VI. Ruegos y preguntas	()
Total de asuntos	(31)

Figure 1: *Screenshot of Spain's Ministry of the Presidency, Justice, and Relations with the Cortes document (Source: Recorded Future)*



MINISTRY OF THE PRESIDENCY,
JUSTICE AND RELATIONS WITH
PARLIAMENT

BLACK INDEX

GENERAL COMMISSION OF
SECRETARIES OF STATE AND
UNDERSECRETARIES

AGENDA FOR THE
MEETING OF

18 September 2025

INDEX

I. Excuses for absence	()
II. Minutes of the previous session	()
III. Informs	(1)
IV. Draft Royal Decrees (3)	
V. Proposed agreements	(27)
VI. Requests and questions	()
Total issues	(31)

Figure 2: *Machine translation of Spain's Ministry of the Presidency, Justice, and Relations with the Cortes document (Source: Recorded Future)*

The document was created shortly after the ministry's September 8, 2025, meeting with Moldovan officials. The timing of this lure document may indicate an attempt to exploit legitimate diplomatic activity, likely of intelligence interest to Russia, ahead of Moldova's September 2025 parliamentary elections.

Between October and December 2025, BlueDelta moved away from using diplomatic lures and instead used a more generic social engineering approach, presenting recipients with either junk data or a prompt instructing them to click to "Enable Content" to display the document, as shown in **Figures 3** and **4**.

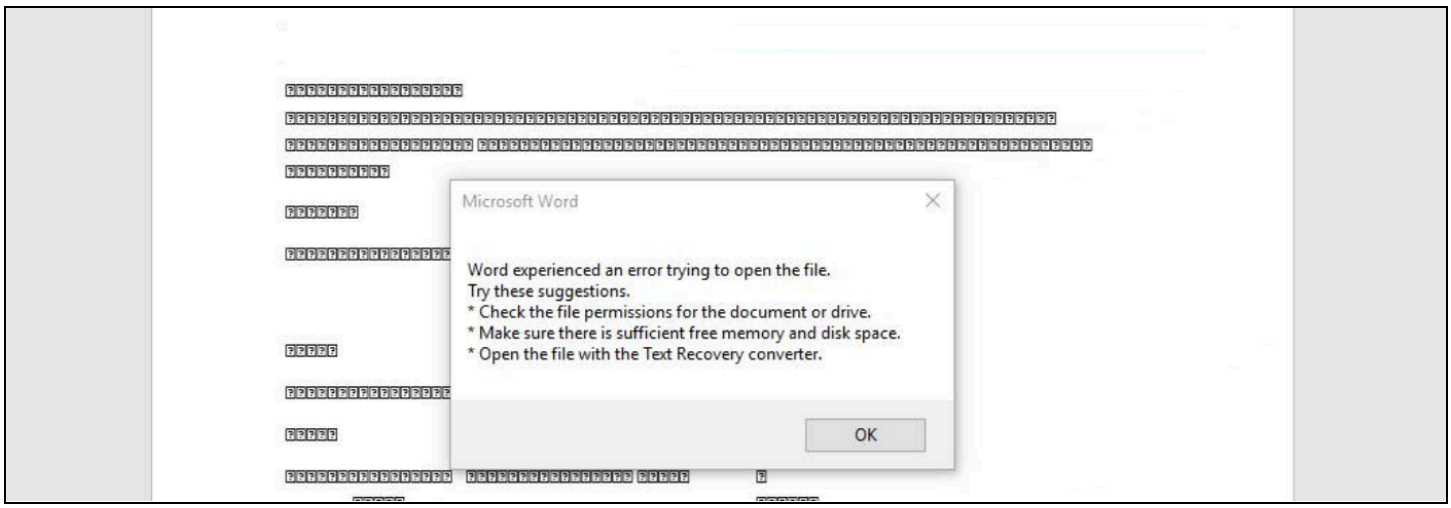


Figure 3: *Screenshot of HOOKEDGE lure document (Source: Recorded Future)*

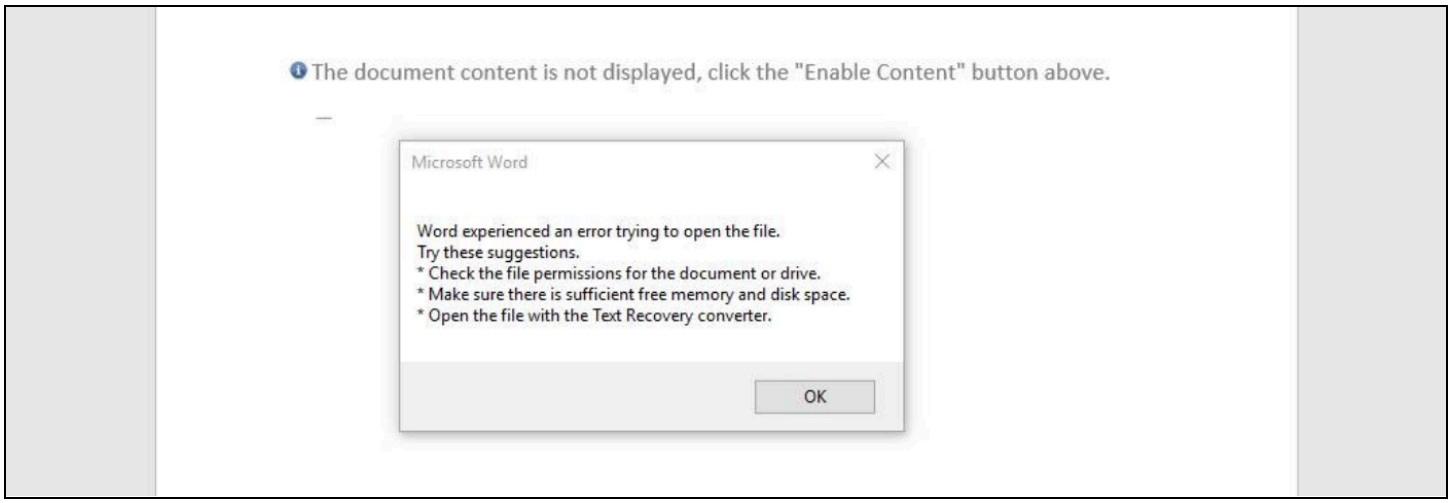


Figure 4: *Screenshot of HOOKEDGE lure document (Source: Recorded Future)*

After enabling macros, a fake Microsoft Word error message was displayed to the user, a technique designed to discourage further scrutiny of the document. This shift away from targeted lure content could suggest that BlueDelta broadened its targeting during this period. These campaigns likely were targeting institutions in Romania.

In early April 2026, Insikt Group identified additional HOOKEDGE variants that, based on network telemetry, targeted organizations in Türkiye.

Insikt Group assesses with medium confidence that the targeting pattern across these campaigns reflects active Russian intelligence collection against European diplomatic targets, particularly those involved in or adjacent to Moldovan political affairs and broader NATO-adjacent European governance.

HOOKEDGE Delivery and Execution

BlueDelta used macro-enabled Microsoft Word documents, likely delivered via spearphishing attachments, as the primary delivery mechanism for HOOKEDGE, relying on victim interaction to trigger execution and using a multi-stage installer chain designed to establish persistence while minimizing forensic artifacts. The high-level execution flow is illustrated in **Figure 5**.

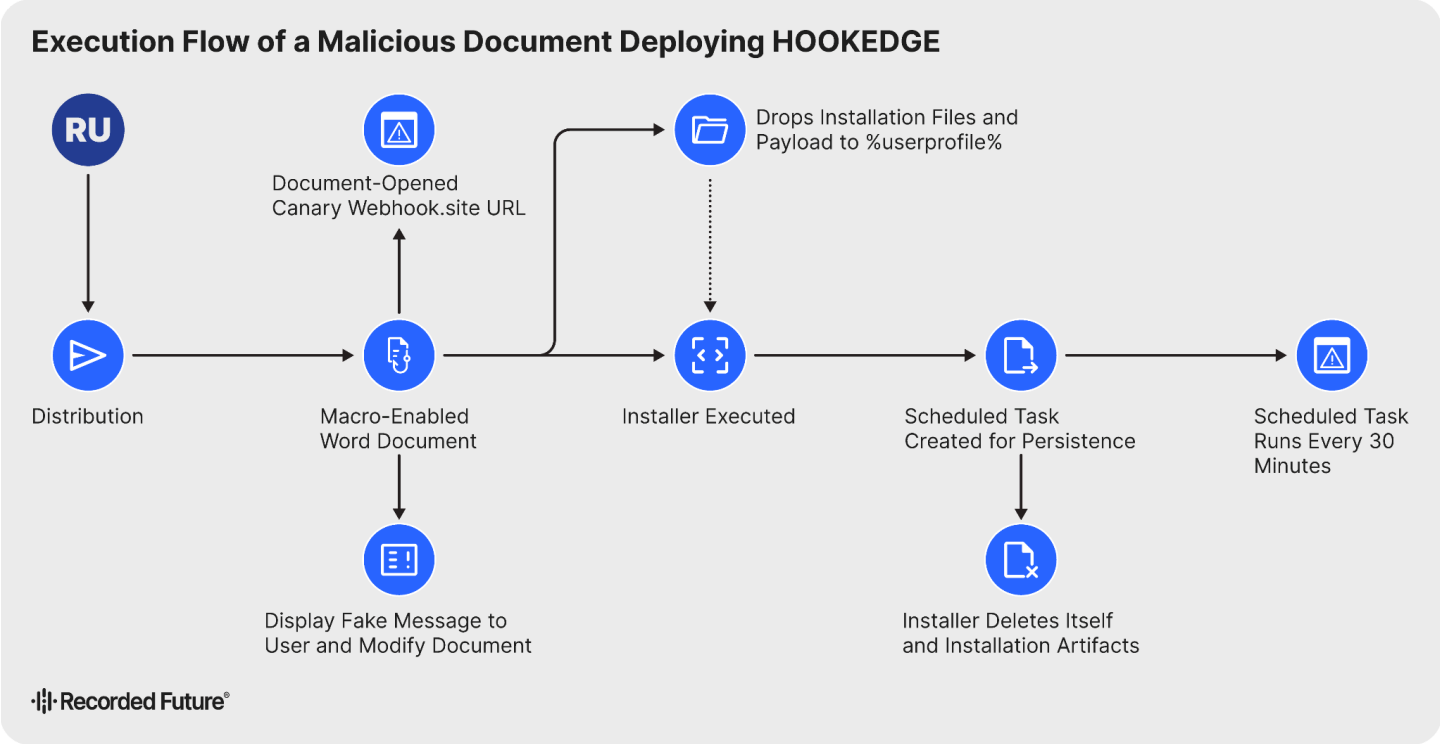


Figure 5: *Execution flow of a malicious Word document deploying HOOKEDGE (Source: Recorded Future)*

When a recipient opens a lure document and enables macros, the document's `AutoOpen()` subroutine executes immediately, writing six files to the `%userprofile%` directory and launching the HOOKEDGE installer chain, as shown in **Table 1**. The files dropped to disk serve distinct roles across delivery, execution, persistence, and exfiltration staging.

Filename	Role
cf25f91c-0a20-4339-834f-02f73e8bc75e.bat	HOOKEDGE
cf25f91c-0a20-4339-834f-02f73e8bc75e.vbs	HOOKEDGE Launcher
cf25f91c-0a20-4339-834f-02f73e8bc75e.cmd	Installer
5744c020-a8d9-4755-abfb-cde6ccd450af.vbs	Installer Launcher
cf25f91c-0a20-4339-834f-02f73e8bc75e.htm	Exfiltration Staging (Header)
cf25f91c-0a20-4339-834f-02f73e8bc75e.xhtml	Exfiltration Staging (Footer)

Table 1: *Files dropped by the malicious Word document and their roles in the HOOKEDGE infection chain (Source: Recorded Future)*

Once the installer launcher executes, it creates a scheduled task that runs every 30 minutes, launching the HOOKEDGE launcher with the HOOKEDGE payload as its argument. The installer then deletes itself, the installer launcher, and the task definition file, removing the primary installation artifacts from the `%userprofile%` directory. All dropped files except the installer launcher are named using the globally unique identifier (GUID) associated with the staging/tasking webhook, whereas the installer launcher uses the GUID associated with the exfiltration webhook.

The malicious document also contains a hidden image referencing a remote webhook URL: *hxxp://webhook[.]site/62114596-33f5-47fb-9012-0223529e5a13/docopened[.]jpg*. This serves as a document-open "canary," alerting BlueDelta operators when a victim opens the lure. Later variants used the filename `doc.jpg` in place of `docopened.jpg`. Insikt Group also identified webhooks using the filename `mailopened.jpg`, indicating that BlueDelta likely used a similar canary mechanism to monitor when recipients opened phishing emails, providing operators with visibility into campaign delivery success before any payload execution.

Insikt Group assesses that the installer chain's self-deletion behavior reflects a deliberate effort to reduce the forensic footprint of the initial compromise and complicate post-incident investigation.

HOOKEDGE Backdoor Analysis

HOOKEDGE is a lightweight Windows batch backdoor that enables remote command execution by retrieving arbitrary `.cmd` payloads from a staging webhook, executing them on the infected host, and exfiltrating the resulting output. The simplified execution flow is illustrated in **Figure 6**.

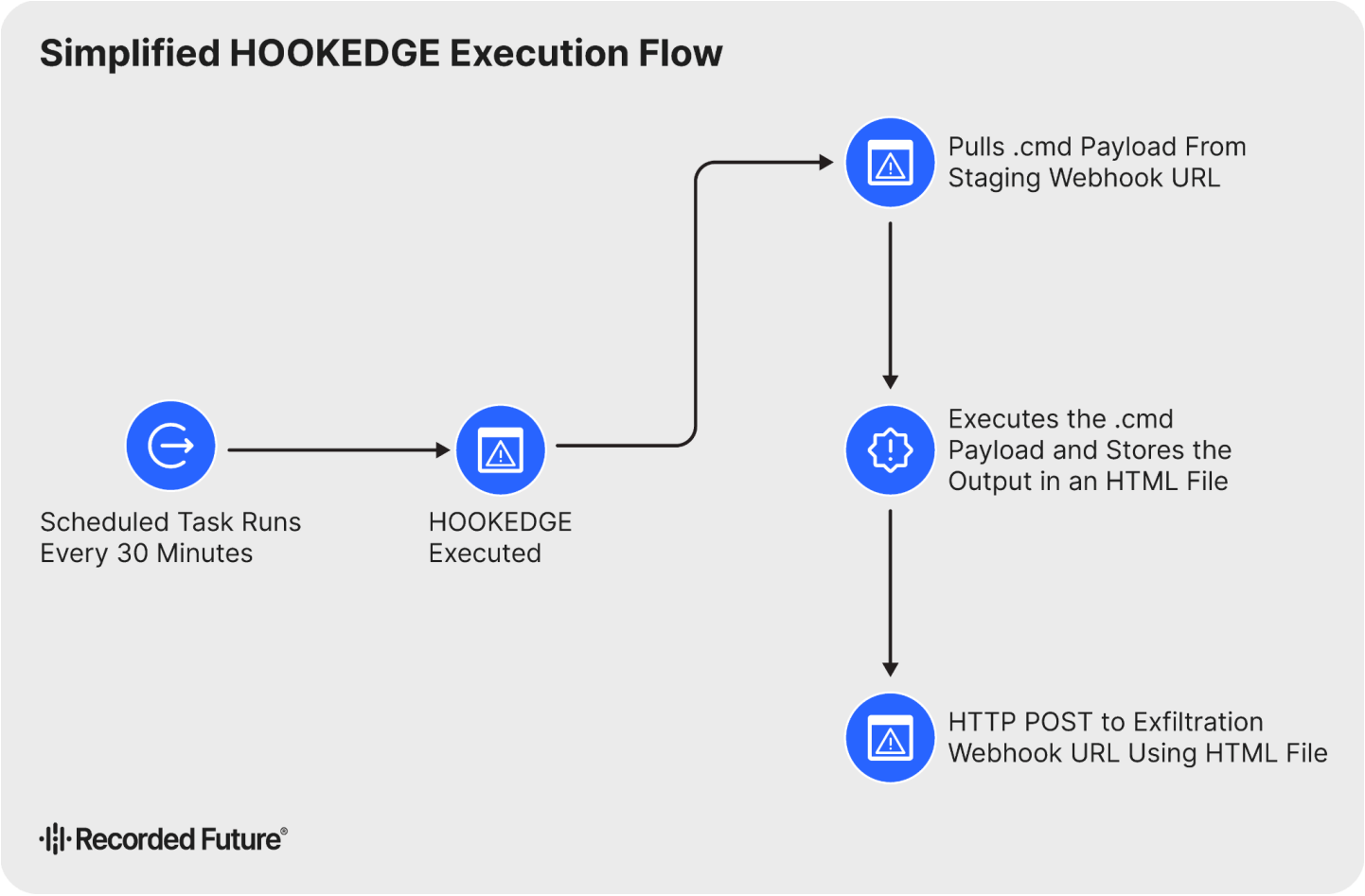


Figure 6: *Simplified HOOKEDGE execution flow (Source: Recorded Future)*

At its core, HOOKEDGE operates as a polling loop: each time the scheduled task fires, the backdoor retrieves a command payload from a staging webhook, executes it, and exfiltrates the output to a separate exfiltration webhook. This two-webhook architecture separates tasking from exfiltration. Each execution cycle performs the following sequence:

1. Deletes residual files from the `%userprofile%\Downloads\` directory, including `.75e`, `.tmp`, and `.crdownload` files; the `.75e` extension is derived from the final three characters of the GUID used in the staging webhook URL
2. Issues a Microsoft Edge request to the staging webhook URL, which returns HTML containing JavaScript that automatically downloads one or more `.75e` files to the `%userprofile%\Downloads\` directory

3. Concatenates all retrieved `.75e` files into a `.cmd` file, executes it, and stores the output to a temporary file in `%userprofile%\`
4. Assembles an HTML exfiltration file by wrapping the command output between the pre-staged `.htm` header and `.xhtml` footer files dropped during installation
5. Launches a second Edge instance to open the assembled HTML file, which auto-submits a form on load and makes an HTTP POST request of the command output to the exfiltration webhook
6. Deletes all temporary files generated during the cycle and terminates any processes whose window titles match the HOOKEDGE task identifier

A notable aspect of HOOKEDGE is its use of `msedge.exe` for both tasking and exfiltration. By generating network traffic through a legitimate web browser rather than a commonly abused LotL binary (LOLBin) or a custom binary, the malware blends its communications with normal enterprise browsing activity.

HOOKEDGE's code and structural design have significant overlap with HEADLACE, a backdoor used by BlueDelta in previous campaigns. Both HOOKEDGE and HEADLACE use Windows batch as the primary scripting language, abuse LIS for C2 and exfiltration, and employ hidden browser instances for C2 communication. Additionally, the second-stage payloads retrieved by HOOKEDGE share JavaScript code with the payloads previously observed in HEADLACE campaigns, using identical variable names, properties, structure, and base64 encoding schemes for automated file downloads. Insikt Group assesses, with moderate confidence, that HOOKEDGE is a direct evolutionary successor to HEADLACE, developed and maintained by the same operators.

Second-Stage Deployment and Tiered Tasking

BlueDelta used HOOKEDGE not only as a stand-alone initial access tool but as a delivery mechanism for additional HOOKEDGE payloads configured for more intensive, responsive tasking, indicating a tiered operational model in which initial access infrastructure is used to triage victims and escalate collection against those deemed to be of higher intelligence value.

The second-stage installer is very similar to the initial installer dropped by the lure document. It drops a new HOOKEDGE payload and launcher, and establishes persistence via a new scheduled task. The main differences are the beaconing interval and the C2 URLs. The first-stage scheduled task runs every 30 minutes, whereas the second-stage scheduled task runs as frequently as every five minutes. This shorter time interval allows the operators to issue commands and receive output far more rapidly, supporting interactive post-compromise activity rather than the slower polling cadence of the initial implant.

The two-stage architecture also helps to mitigate one of BlueDelta's infrastructure constraints. *webhook[.]site*'s free tier imposes a maximum of 100 requests per unique endpoint, meaning a 30-minute beaconing interval would exhaust a given endpoint's request allocation within approximately two to three days. By moving high-priority victims to dedicated second-stage webhook endpoints, BlueDelta effectively separates initial-access infrastructure from active collection infrastructure,

ensuring that ongoing operator tasking and collection do not prematurely exhaust the limited request quotas of the initial-access webhook endpoints.

Insikt Group assesses with moderate confidence that deploying a second HOOKEDGE payload to the same victim constitutes a deliberate triage mechanism. The first-stage implant establishes broad initial access; operators likely use network telemetry, such as document-open canary requests and successful communications with staging or exfiltration webhook endpoints, to identify victims that warrant more intensive tasking. This operational pattern is consistent with BlueDelta's long-established preference for lightweight, low-noise initial access tooling that supports selective, intelligence-driven follow-on activity.

HOOKEDGE Refinement over Time

BlueDelta iteratively refined HOOKEDGE and its delivery throughout the reporting period, modifying lure documents, execution methods, phishing telemetry, and beaconing intervals while preserving the malware's core architecture. Across observed variants, the group transitioned from diplomatic-themed to generic macro-enablement lures, changed Microsoft Edge execution from headless to a hidden window, and introduced email-open canaries. A summary of all key changes is provided in **Table 2** below.

First Seen	Key Changes
2025-09-26	Diplomatic lure (Spanish Ministry)
2025-10-07	Generic Lure; 20-minute beaconing interval
2025-12-04	Minor changes to the generic lure; Edge hidden window rather than headless
2026-01-19	Minor changes to the generic lure
2026-01-20	`mailopened.jpg` canary detected in network telemetry
2026-04-08	Minor changes to the generic lure; Canary filename changed to `doc.jpg`
2026-06-29	Minor changes to VBA obfuscation, document-open canary removed

Table 2: *HOOKEDGE campaign refinement over time (Source: Recorded Future)*

One of the most significant operational changes was increasing the first-stage beacon interval from 30 to 61 minutes. Insikt Group assesses that this adjustment likely reduced the effectiveness of automated sandbox environments that typically monitor execution for up to 60 minutes while also slowing consumption of the finite request quotas imposed by *webhook[.]site*, extending the operational lifespan of the group's infrastructure.

The introduction of `/mailopened.jpg` canaries in January 2026 campaigns expanded BlueDelta's visibility into the phishing lifecycle, allowing operators to distinguish between email opens, document opens, and successful macro execution. This level of phishing delivery tracking is highly useful as a feedback mechanism, allowing BlueDelta to assess the success of each stage of its campaigns.

In July 2026 campaigns, BlueDelta removed the document-open canary — previously, a consistent feature used to capture victim IP addresses at the moment of document opening — from observed HOOKEDGE samples. While the operational motivation behind this change is unclear, it may reflect an intent to reduce network-based indicators of compromise.

Malicious Infrastructure

BlueDelta has continued to rely on *webhook[.]site* for all C2, payload staging, and data exfiltration across the campaigns documented in this report. This represents a deliberate infrastructure choice that focuses on detection evasion and operational simplicity over the control and flexibility offered by dedicated infrastructure. This has proven consistently effective against network-based defensive controls.

webhook[.]site is a legitimate, publicly accessible service that allows users to create unique HTTPS endpoints to receive and inspect HTTP requests. In HOOKEDGE operations, BlueDelta uses individual webhook endpoints for distinct functions: document-open and email-open canaries, command and payload staging, and exfiltration capture. Each function is assigned a separate endpoint, and endpoint universally unique identifiers (UUIDs) are reused as filenames for files dropped during installation, a design that ties the infrastructure directly to the implant's file-naming scheme and simplifies operator management of campaign components.

HOOKEDGE's network communications are designed to blend with legitimate web activity. Outbound connections from infected hosts are directed to a legitimate HTTPS service, with a web browser serving as the HTTP client. This leaves defenders with relatively few anomalous characteristics beyond the specific webhook URLs and execution context. Traffic of this type is resistant to detection approaches that rely on domain or IP reputation, static blocklists, or TLS inspection policies that exempt trusted services.

Across the observed campaigns, BlueDelta administered its *webhook[.]site* endpoints from NordVPN IP addresses. This use of a commercial virtual private network (VPN) service for infrastructure administration further complicates attribution by removing direct operator IP visibility, and is consistent with BlueDelta's broader operational security practices observed in prior campaigns. The combination of a legitimate web service for C2 and a commercial VPN for administration means that neither the traffic nor its origin provides a reliable attribution signal through conventional network monitoring alone.

The request limits imposed by *webhook[.]site*'s free tier, which allowed a maximum of 100 requests per unique endpoint, likely influenced BlueDelta's operational tempo. Insikt Group assesses that these constraints drove both the extension of HOOKEDGE's beaconing interval and the use of dedicated

second-stage webhook endpoints for higher-priority targets. Despite these limitations, BlueDelta continued to rely on *webhook[.]site*, suggesting that the operational benefits of using a legitimate web service outweighed the finite request quotas. The ability to rapidly provision new endpoints at no cost further reduced the impact of these limitations.

Mitigations

- **Use Recorded Future Threat Intelligence:** Recorded Future customers should monitor Intelligence Cards, Risk Lists, and associated indicators related to BlueDelta infrastructure, including *webhook[.]site* URLs, malware samples, and phishing lures. Organizations can use the Recorded Future Intelligence Operations Platform to identify newly observed BlueDelta-related infrastructure and prioritize investigations involving related activity.
- **Harden Microsoft Office Macro Security:** Disable macros from internet-originated documents where operationally feasible and enforce Microsoft's recommended macro-blocking policies. Organizations should restrict the execution of unsigned VBA macros.
- **Implement Phishing-Resistant Authentication:** Deploy phishing-resistant multi-factor authentication (MFA), such as FIDO2 security keys or certificate-based authentication, for email, VPN, and other externally accessible services. While HOOKEDGE provides initial access and post-compromise capabilities, BlueDelta has historically relied on credential theft to expand access within targeted environments.
- **Monitor for Scheduled Task Abuse:** Detect and investigate the creation of scheduled tasks that execute scripts, batch files, or interpreters such as `wscript.exe`, `cscript.exe`, `cmd.exe`, and `powershell.exe` from user-writable directories. HOOKEDGE relies on scheduled tasks for persistence across all observed variants.
- **Monitor for Suspicious Browser Automation:** Investigate unusual execution of Microsoft Edge in headless mode, particularly instances launched with command-line arguments such as `--headless=new`, local HTML files, or data URLs. These behaviors are uncommon in most enterprise environments and were used by HOOKEDGE for tasking and data exfiltration.
- **Inspect Outbound Traffic to Legitimate File-Sharing and Webhook Services:** Organizations should review outbound connections to services such as *webhook[.]site* and other webhook, file-hosting, and content-delivery platforms. If any are not being used by the company, they should be blocked completely. While these services are legitimate, they are increasingly abused by threat actors for command-and-control, payload staging, and data exfiltration.
- **Develop and Exercise Incident Response Procedures:** Establish procedures for investigating phishing incidents, credential compromise, and suspicious scheduled-task creation. Organizations should ensure security teams can rapidly identify compromised hosts, collect forensic evidence, and contain infections before follow-on malware is deployed.

Outlook

BlueDelta is likely to continue conducting initial access campaigns against European government and diplomatic organizations in support of Russian intelligence collection. Given the enduring strategic importance of European governance, NATO-related affairs, and diplomatic engagement with former Soviet republics, the intelligence requirements driving this activity are unlikely to diminish in the near term.

Since it was first detected in September 2025, HOOKEDGE has been continuously improved by BlueDelta. The threat group has changed HOOKEDGE's delivery mechanisms, beaconing intervals, and infrastructure management practices in response to shifts in the defensive landscape and the operational constraints of *webhook[.]site*. Further improvements and refinements are likely, and Insikt Group assesses that future changes will probably remain operationally motivated and oriented toward detection evasion and infrastructure resilience.

Given BlueDelta's history of periodically retiring initial-access tooling once it attracts sufficient detection coverage, HOOKEDGE will eventually be superseded. HOOKEDGE's replacement will probably retain proven tradecraft elements: use of LOLBins, abuse of legitimate web services for C2, and LotL execution. JavaScript-based payload delivery and GUID-formatted file-naming conventions have appeared consistently across both HEADLACE and HOOKEDGE, and these patterns are worth monitoring for continuity into future tooling.

Across all campaigns documented in this report, BlueDelta relied exclusively on *webhook[.]site*'s free tier for command-and-control, payload staging, and data exfiltration. Insikt Group assesses that increased disruption of *webhook[.]site*, whether through abuse mitigation or defensive detection, would more likely drive a migration to another legitimate web service than to dedicated attacker-controlled infrastructure. This assessment is supported by the group's previous migration from *mocky[.]io* to *webhook[.]site* during HEADLACE campaigns, demonstrating a preference for adapting legitimate infrastructure rather than operating its own.

Appendix A: Indicators of Compromise

URLs:

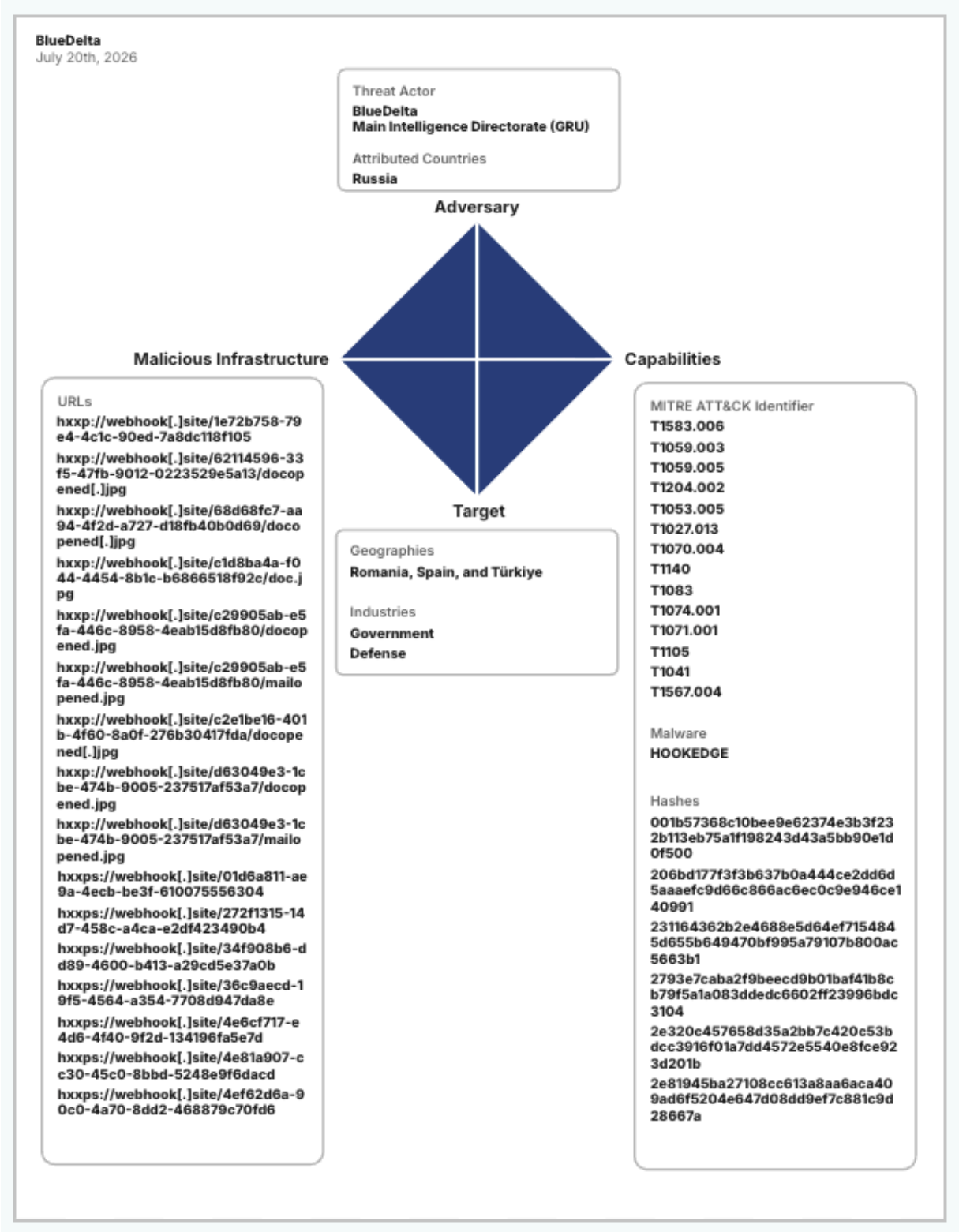
hxxp://webhook[.]site/1e72b758-79e4-4c1c-90ed-7a8dc118f105
hxxp://webhook[.]site/62114596-33f5-47fb-9012-0223529e5a13/docopened[.]jpg
hxxp://webhook[.]site/68d68fc7-aa94-4f2d-a727-d18fb40b0d69/docopened[.]jpg
hxxp://webhook[.]site/c1d8ba4a-f044-4454-8b1c-b6866518f92c/doc[.]jpg
hxxp://webhook[.]site/c29905ab-e5fa-446c-8958-4eab15d8fb80/docopened[.]jpg
hxxp://webhook[.]site/c29905ab-e5fa-446c-8958-4eab15d8fb80/mailopened[.]jpg
hxxp://webhook[.]site/c2e1be16-401b-4f60-8a0f-276b30417fda/docopened[.]jpg
hxxp://webhook[.]site/d63049e3-1cbe-474b-9005-237517af53a7/docopened.jpg
hxxp://webhook[.]site/d63049e3-1cbe-474b-9005-237517af53a7/mailopened[.]jpg
hxxps://webhook[.]site/01d6a811-ae9a-4ecb-be3f-610075556304
hxxps://webhook[.]site/272f1315-14d7-458c-a4ca-e2df423490b4
hxxps://webhook[.]site/34f908b6-dd89-4600-b413-a29cd5e37a0b
hxxps://webhook[.]site/36c9aecd-19f5-4564-a354-7708d947da8e
hxxps://webhook[.]site/4e6cf717-e4d6-4f40-9f2d-134196fa5e7d
hxxps://webhook[.]site/4e81a907-cc30-45c0-8bbd-5248e9f6dacd
hxxps://webhook[.]site/4ef62d6a-90c0-4a70-8dd2-468879c70fd6
hxxps://webhook[.]site/5744c020-a8d9-4755-abfb-cde6ccd450af
hxxps://webhook[.]site/5dbed3be-f1c9-41e5-b5d5-e961d08b5fba
hxxps://webhook[.]site/655a413e-4a66-4987-8f5b-f5cbfe34cdd6
hxxps://webhook[.]site/68ff1679-974b-4d15-9ce0-799892c63f04
hxxps://webhook[.]site/752c57b9-20d1-4990-a909-fd212ab71dcd
hxxps://webhook[.]site/81f3d140-eb6e-4d72-a6ca-e6e952c3d9c2
hxxps://webhook[.]site/82911ae6-ea27-4996-a664-2322e89da9ae
hxxps://webhook[.]site/9f2837e2-8321-46a5-aee5-ccdda349f864
hxxps://webhook[.]site/a3f4e990-0b2a-4f6a-a02e-c573005de3ee
hxxps://webhook[.]site/a72d8905-b15f-4e95-9a8f-5e4bb7dc9b3d
hxxps://webhook[.]site/bbdbf60c-8593-4660-9620-d3c0de24a8ab
hxxps://webhook[.]site/c24a31e4-691e-4a7b-96af-037ae735d358
hxxps://webhook[.]site/cf25f91c-0a20-4339-834f-02f73e8bc75e
hxxps://webhook[.]site/d993e113-a672-48aa-a382-64c5aaac56eb

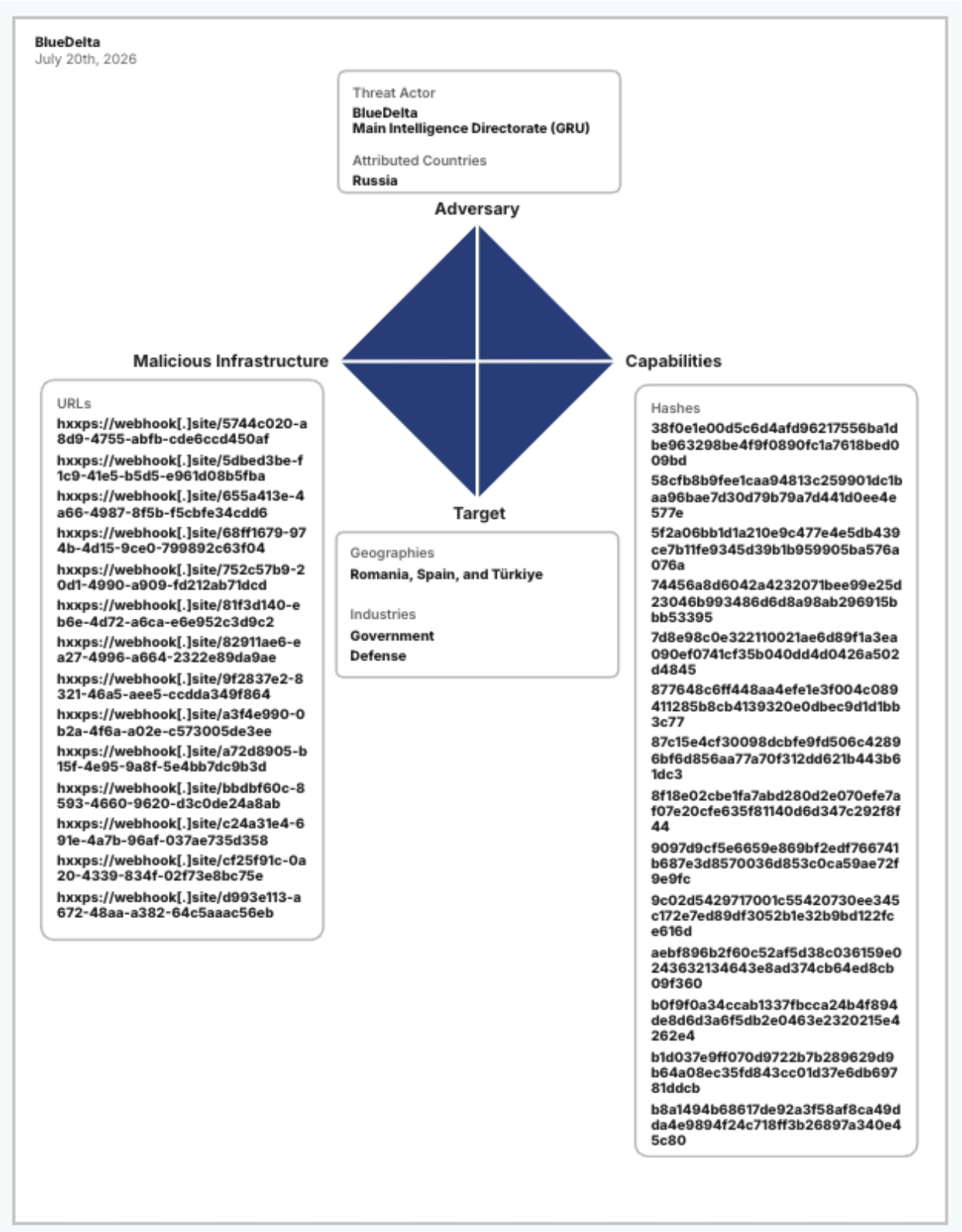
Hashes:

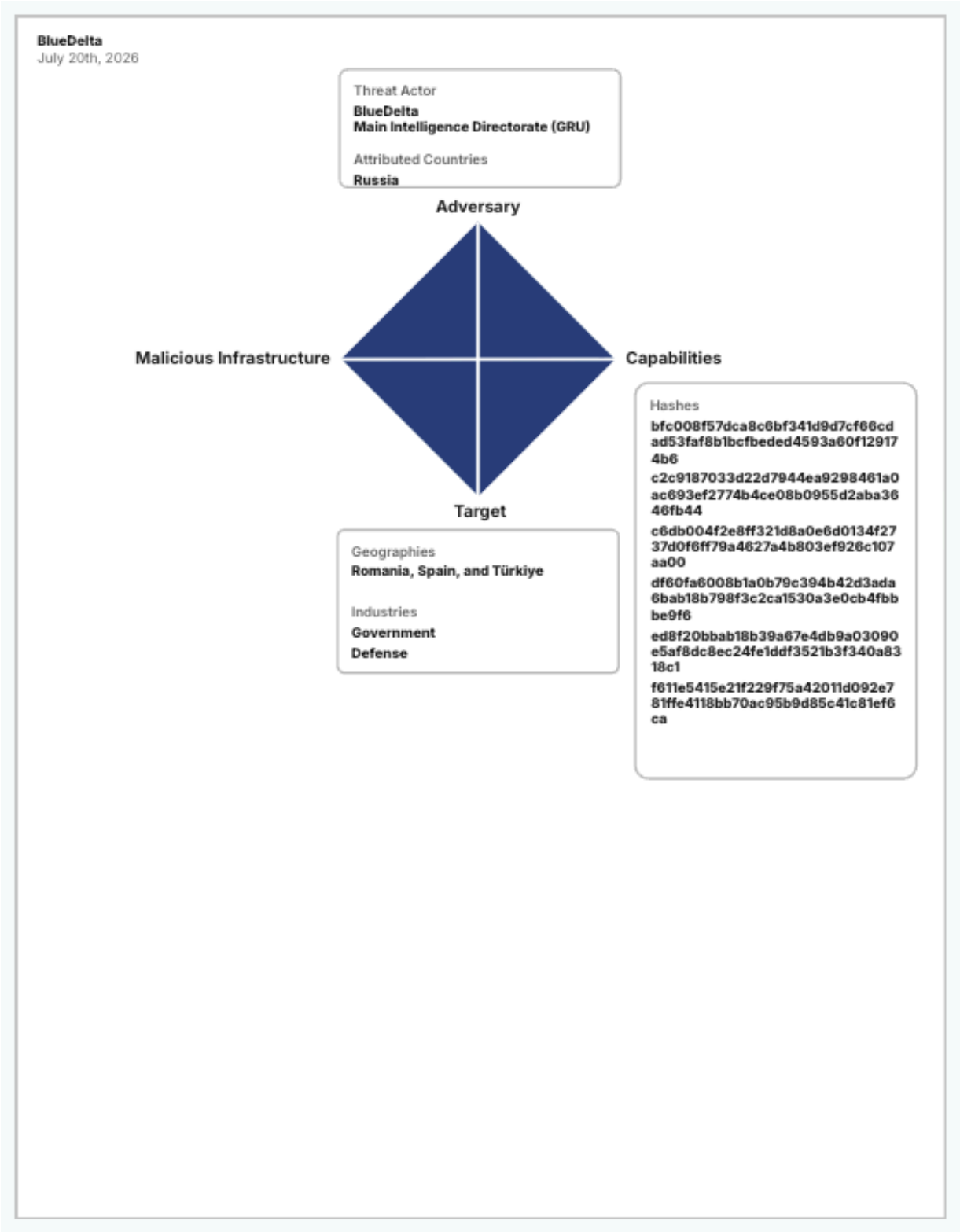
001b57368c10bee9e62374e3b3f232b113eb75a1f198243d43a5bb90e1d0f500
206bd177f3f3b637b0a444ce2dd6d5aaaefc9d66c866ac6ec0c9e946ce140991
231164362b2e4688e5d64ef7154845d655b649470bf995a79107b800ac5663b1
2793e7caba2f9beecd9b01baf41b8cb79f5a1a083ddedc6602ff23996bdc3104
2e320c457658d35a2bb7c420c53bdcc3916f01a7dd4572e5540e8fce923d201b
2e81945ba27108cc613a8aa6aca409ad6f5204e647d08dd9ef7c881c9d28667a
38f0e1e00d5c6d4afd96217556ba1dbe963298be4f9f0890fc1a7618bed009bd
58cfb8b9fee1caa94813c259901dc1baa96bae7d30d79b79a7d441d0ee4e577e
5f2a06bb1d1a210e9c477e4e5db439ce7b11fe9345d39b1b959905ba576a076a
74456a8d6042a4232071bee99e25d23046b993486d6d8a98ab296915bbb53395
7d8e98c0e322110021ae6d89f1a3ea090ef0741cf35b040dd4d0426a502d4845
877648c6ff448aa4efe1e3f004c089411285b8cb4139320e0dbec9d1d1bb3c77
87c15e4cf30098dcbfe9fd506c42896bf6d856aa77a70f312dd621b443b61dc3
8f18e02cbe1fa7abd280d2e070efe7af07e20cfe635f81140d6d347c292f8f44
9097d9cf5e6659e869bf2edf766741b687e3d8570036d853c0ca59ae72f9e9fc
9c02d5429717001c55420730ee345c172e7ed89df3052b1e32b9bd122fce616d

```
aebf896b2f60c52af5d38c036159e0243632134643e8ad374cb64ed8cb09f360
b0f9f0a34ccab1337fbcca24b4f894de8d6d3a6f5db2e0463e2320215e4262e4
b1d037e9ff070d9722b7b289629d9b64a08ec35fd843cc01d37e6db69781ddcb
b8a1494b68617de92a3f58af8ca49dda4e9894f24c718ff3b26897a340e45c80
bfc008f57dca8c6bf341d9d7cf66cdad53faf8b1bcfbeded4593a60f129174b6
c2c9187033d22d7944ea9298461a0ac693ef2774b4ce08b0955d2aba3646fb44
c6db004f2e8ff321d8a0e6d0134f2737d0f6ff79a4627a4b803ef926c107aa00
df60fa6008b1a0b79c394b42d3ada6bab18b798f3c2ca1530a3e0cb4fbbbe9f6
ed8f20bbab18b39a67e4db9a03090e5af8dc8ec24fe1ddf3521b3f340a8318c1
f611e5415e21f229f75a42011d092e781ffe4118bb70ac95b9d85c41c81ef6ca
```

Appendix B: Diamond Model of Intrusion Analysis




BlueDelta
July 20th, 2026
Threat Actor
BlueDelta
Main Intelligence Directorate (GRU)
Attributed Countries
Russia
Adversary
Malicious Infrastructure
Capabilities
Target
URLs
hxxps://webhook[.]site/5744c020-a8d9-4755-abfb-cde6ccd450af
hxxps://webhook[.]site/5dbed3be-f1c9-41e5-b5d5-e961d08b5fba
hxxps://webhook[.]site/655a413e-4a66-4987-8f5b-f5cbfe34cdd6
hxxps://webhook[.]site/68ff1679-974b-4d15-9ce0-799892c63f04
hxxps://webhook[.]site/752c57b9-20d1-4990-a909-fd212ab71dcd
hxxps://webhook[.]site/81f3d140-eb6e-4d72-a6ca-e6e952c3d9c2
hxxps://webhook[.]site/82911ae6-ea27-4996-a664-2322e89da9ae
hxxps://webhook[.]site/9f2837e2-8321-46a5-aee5-ccdda349f864
hxxps://webhook[.]site/a3f4e990-0b2a-4f6a-a02e-c573005de3ee
hxxps://webhook[.]site/a72d8905-b15f-4e95-9a8f-5e4bb7dc9b3d
hxxps://webhook[.]site/bbdbf60c-8593-4660-9620-d3c0de24a8ab
hxxps://webhook[.]site/c24a31e4-691e-4a7b-96af-037ae735d358
hxxps://webhook[.]site/cf25f91c-0a20-4339-834f-02f73e8bc75e
hxxps://webhook[.]site/d993e113-a672-48aa-a382-64c5aaac56eb
Geographies
Romania, Spain, and Türkiye
Industries
Government
Defense
Hashes
38f0e1e00d5c6d4afd96217556ba1dbe963298be4f9f0890fc1a7618bed009bd
58cfb8b9fee1caa94813c259901dc1baa96bae7d30d79b79a7d441d0ee4e577e
5f2a06bb1d1a210e9c477e4e5db439ce7b11fe9345d39b1b959905ba576a076a
74456a8d6042a4232071bee99e25d23046b993486d6d8a98ab296915bbb53395
7d8e98c0e322110021ae6d89f1a3ea090ef0741cf35b040dd4d0426a502d4845
877648c6ff448aa4efe1e3f004c089411285b8cb4139320e0dbec9d1d1bb3c77
87c15e4cf30098dcbfe9fd506c42896bf6d856aa77a70f312dd621b443b61dc3
8f18e02cbe1fa7abd280d2e070efe7af07e20cfe635f81140d6d347c292f8f44
9097d9cf5e6659e869bf2edf766741b687e3d8570036d853c0ca59ae72f9e9fc
9c02d5429717001c55420730ee345c172e7ed89df3052b1e32b9bd122fce616d
aebf896b2f60c52af5d38c036159e0243632134643e8ad374cb64ed8cb09f360
b0f9f0a34ccab1337fbcca24b4f894de8d6d3a6f5db2e0463e2320215e4262e4
b1d037e9ff070d9722b7b289629d9b64a08ec35fd843cc01d37e6db69781ddcb
b8a1494b68617de92a3f58af8ca49dda4e9894f24c718ff3b26897a340e45c80


BlueDelta
July 20th, 2026
Threat Actor
BlueDelta
Main Intelligence Directorate (GRU)
Attributed Countries
Russia
Adversary
Malicious Infrastructure
Capabilities
Target
Geographies
Romania, Spain, and Türkiye
Industries
Government
Defense
Hashes
bfc008f57dca8c6bf341d9d7cf66cdad53faf8b1bcfbeded4593a60f129174b6
c2c9187033d22d7944ea9298461a0ac693ef2774b4ce08b0955d2aba3646fb44
c6db004f2e8ff321d8a0e6d0134f2737d0f6ff79a4627a4b803ef926c107aa00
df60fa6008b1a0b79c394b42d3ada6bab18b798f3c2ca1530a3e0cb4fbbbe9f6
ed8f20bbab18b39a67e4db9a03090e5af8dc8ec24fe1ddf3521b3f340a8318c1
f611e5415e21f229f75a42011d092e781ffe4118bb70ac95b9d85c41c81ef6ca

Appendix C: MITRE ATT&CK Techniques

Tactic: Technique	ATT&CK Code
Resource Development: Web Services	T1583.006
Execution: Windows Command Shell	T1059.003
Execution: Visual Basic	T1059.005
Execution: Malicious File	T1204.002
Persistence: Scheduled Task	T1053.005
Defense Evasion: Encrypt/Encode File	T1027.013
Defense Evasion: File Deletion	T1070.004
Defense Evasion: Deobfuscate/Decode Files or Information	T1140
Discovery: File and Directory Discovery	T1083
Collection: Local Data Staging	T1074.001
Command and Control: Web Protocols	T1071.001
Command and Control: Ingress Tool Transfer	T1105
Exfiltration: Exfiltration Over C2 Channel	T1041
Exfiltration: Exfiltration Over Webhook	T1567.004

Recorded Future reporting contains expressions of likelihood or probability consistent with US Intelligence Community Directive (ICD) 203: Analytic Standards (published January 2, 2015). Recorded Future reporting also uses confidence level standards employed by the US Intelligence Community to assess the quality and quantity of the source information supporting our analytic judgments.

About Insikt Group®

Recorded Future's Insikt Group, the company's threat research division, comprises analysts and security researchers with deep government, law enforcement, military, and intelligence agency experience. Their mission is to produce intelligence that reduces risk for customers, enables tangible outcomes, and prevents business disruption.

About Recorded Future®

Recorded Future is the world's largest intelligence company. The Recorded Future Intelligence Operations Platform provides the most complete coverage across adversaries, infrastructure, and targets. By combining precise, AI-driven analytics with the Intelligence Graph® populated by specialized threat data, Recorded Future enables cyber teams to see the complete picture, act with confidence, and get ahead of threats that matter before they impact your business. Headquartered in Boston with offices around the world, Recorded Future works with more than 1,900 businesses and government organizations across 80 countries.

Learn more at recordedfuture.com