Gotta fly: Lazarus targets the UAV sector

By Peter KálnaiAlexis Rapin

Archived: 2026-04-05 15:11:43 UTC

ESET researchers have recently observed a new instance of Operation DreamJob – a campaign that we track under the umbrella of North Korea-aligned Lazarus – in which several European companies active in the defense industry were targeted. Some of these are heavily involved in the unmanned aerial vehicle (UAV) sector, suggesting that the operation may be linked to North Korea's current efforts to scale up its drone program. This blogpost discusses the broader geopolitical implications of the campaign, and provides a high-level overview of the toolset used by the attackers.

> **Key points of this blogpost:**
>
> - Lazarus attacks against companies developing UAV technology align with recently reported developments in the North Korean drone program.
> - The suspected primary goal of the attackers was likely the theft of proprietary information and manufacturing know-how.
> - Based on the social-engineering technique used for initial access, trojanizing open-source projects from GitHub, and the deployment of ScoringMathTea, we consider these attacks to be a new wave of the Operation DreamJob campaign.
> - The group's most significant evolution is the introduction of new libraries designed for DLL proxying and the selection of new open-source projects to trojanize for improved evasion.

Profile of Lazarus and its Operation DreamJob

The Lazarus group (also known as HIDDEN COBRA) is an APT group linked to North Korea that has been active since at least 2009. It is responsible for high-profile incidents such as both the Sony Pictures Entertainment hack and tens-of-millions-of-dollar cyberheists in 2016, the WannaCryptor (aka WannaCry) outbreak in 2017, and a long history of disruptive attacks against South Korean public and critical infrastructure since at least 2011. The diversity, number, and eccentricity in implementation of Lazarus campaigns define this group, as well as that it performs all three pillars of cybercriminal activities: cyberespionage, cybersabotage, and pursuit of financial gain.

Operation DreamJob is a codename for Lazarus campaigns that rely primarily on social engineering, specifically using fake job offers for prestigious or high-profile positions (the "dream job" lure). This name was coined in a 2020 blogpost by ClearSky, and overlaps with campaigns like DeathNote or Operation North Star. Targets are predominantly in the aerospace and defense sectors, followed by engineering and technology companies and the media and entertainment sector. In these campaigns, the attackers usually deploy trojanized open-source plugins for software like Notepad++ and WinMerge that serve as droppers and loaders, and payloads like ImprudentCook, ScoringMathTea, BlindingCan, miniBlindingCan, LightlessCan for Windows, and SimplexTea for Linux. The primary goal is cyberespionage, focusing on stealing sensitive data, intellectual property, and proprietary information, and the secondary goal is financial gain.

Overview

Starting in late March 2025, we observed in ESET telemetry cyberattacks reminiscent of Operation DreamJob campaigns. The in-the-wild attacks successively targeted three European companies active in the defense sector. Although their activities are somewhat diverse, these entities can be described as:

- a metal engineering company (Southeastern Europe),
- a manufacturer of aircraft components (Central Europe), and
- a defense company (Central Europe).

All cases involved droppers that have the interesting internal DLL name, DroneEXEHijackingLoader.dll, which led us down the drone segment rabbit hole. Also, initial access was likely achieved via social engineering – an Operation DreamJob specialty. The dominant theme is a lucrative but faux job offer with a side of malware: the target receives a decoy document with a job description and a trojanized PDF reader to open it.

The main payload deployed to the targets was ScoringMathTea, a RAT that offers the attackers full control over the compromised machine. Its first appearance dates to late 2022, when its dropper was uploaded to VirusTotal. Soon after, it

was seen in the wild, and since then in multiple attacks attributed to Lazarus' Operation DreamJob campaigns, which makes it the attacker's payload of choice for already three years. It uses compromised servers for C&C communication, with the server part usually stored under the WordPress folder containing design templates or plugins.

In summary, we attribute this activity with a high level of confidence to Lazarus, particularly to its campaigns related to Operation DreamJob, based on the following:

- Initial access was obtained by social engineering, convincing the target to execute malware disguised as a job description, in order to succeed in a hiring process.
- Trojanizing open-source projects and then crafting their exports to fit the DLL side-loading seems to be an approach specific to Operation DreamJob.
- The flagship payload for later stages, ScoringMathTea, was used in multiple similar attacks in the past.
- The targeted sectors, located in Europe, align with the targets of the previous instances of Operation DreamJob (aerospace, defense, engineering).

Geopolitical context

The three targeted organizations manufacture different types of military equipment (or parts thereof), many of which are currently deployed in Ukraine as a result of European countries' military assistance. At the time of Operation DreamJob's observed activity, North Korean soldiers were deployed in Russia, reportedly to help Moscow repel Ukraine's offensive in the Kursk oblast. It is thus possible that Operation DreamJob was interested in collecting sensitive information on some Western-made weapons systems currently employed in the Russia-Ukraine war.

More generally, these entities are involved in the production of types of materiel that North Korea also manufactures domestically, and for which it might be hoping to perfect its own designs and processes. In any case, there is no indication that the targeted companies supply military equipment to the South Korean armed forces – which could have been another element explaining Operation DreamJob's interest in these companies. Interestingly, however, at least two of these organizations are clearly involved in the development of UAV technology, with one manufacturing critical drone components and the other reportedly engaged in the design of UAV-related software.

The interest in UAV-related know-how is notable, as it echoes recent media reports indicating that Pyongyang is investing heavily in domestic drone manufacturing capabilities. Although this endeavor can be traced back to more than a decade ago, many observers posit that North Korea's recent experience of modern warfare in the Russia-Ukraine war has only reinforced Pyongyang's resolution with regard to its drone program. The North Korean regime is now reportedly receiving assistance from Russia to produce its own version of the Iranian-made Shahed suicide drone and is also apparently working on low-cost attack UAVs that could be exported to African or Middle Eastern countries.

Assessing the "drone connection"

If one thing is clear, it is that North Korea has relied heavily on reverse engineering and intellectual property theft to develop its domestic UAV capabilities. As recent open-source reports illustrate, North Korea's current flagship reconnaissance drone, the Saetbyol-4, looks like a carbon copy of the Northrop Grumman RQ-4 Global Hawk, while its multipurpose combat drone, the Saetbyol-9, bears a striking resemblance to General Atomics' MQ-9 Reaper. The fact that both designations replicate the number associated with their US equivalent might even be a not-so-subtle nod to that effect. Although these aircrafts' performance may well differ from those of their US counterparts, there is little doubt that the latter served as a strong inspiration for North Korea's designs.

This is probably where cybercapabilities enter the fray. While other intelligence resources were likely mobilized by Pyongyang to help copy Western UAVs, there are indications that cyberespionage may have played a role. In recent years, multiple campaigns affecting the aerospace sector (including UAV technology specifically) have been attributed to North Korea-aligned APT groups, with Operation North Star (a campaign presenting some overlap with Operation DreamJob) being one of them. In 2020, ESET researchers documented a similar campaign, which we then named Operation In(ter)ception and later attributed to Lazarus with high confidence. As several groups related to Lazarus have been formally linked to North Korean intelligence services by US authorities and others, these precedents strongly suggest that cyberespionage is likely one of the tools leveraged by the regime for reverse engineering Western UAVs – and that groups operating under the broad Lazarus umbrella are taking an active part in this effort.

In this context, we believe that it is likely that Operation DreamJob was – at least partially – aimed at stealing proprietary information, and manufacturing know-how, regarding UAVs. The Drone mention observed in one of the droppers significantly reinforces this hypothesis.

To be clear, we can only hypothesize as to the specific kind of information that Operation DreamJob was after. However, we have found evidence that one of the targeted entities is involved in the production of at least two UAV models that are currently employed in Ukraine, and which North Korea may have encountered on the frontline. This entity is also involved in the supply chain of advanced single-rotor drones (i.e., unmanned helicopters), a type of aircraft that Pyongyang is actively developing but has not proved able to militarize so far. These may be some of the potential motivations behind Operation DreamJob's observed activities. More generally, as North Korea is reportedly in the process of building a factory for mass-producing UAVs, it might also be looking for privileged knowledge regarding UAV-related industrial processes and manufacturing techniques.

Reports from Google's Mandiant in September 2024 and from Kaspersky in December 2024 describe tools used by Lazarus in its Operation DreamJob in 2024. In this section, we mention the tools to which the group shifted in Operation DreamJob in 2025. Based on their position in the execution chain, we distinguish two types of tools: early stages that consist of various droppers, loaders, and downloaders; and the main stages that represent payloads like RATs and complex downloaders that give the attackers sufficient control over the compromised machine.

Besides the in-the-wild cases seen in ESET telemetry, the activity of the attackers also manifested as VirusTotal submissions occurring at the same time. A trojanized MuPDF reader, QuanPinLoader, a loader disguised as a Microsoft DirectInput library (dinput.dll), and a variant of ScoringMathTea were submitted from Italy in April and June 2025; BinMergeLoader was submitted in August 2025 from Spain.

Droppers, loaders, and downloaders

Generally, Lazarus attackers are highly active and deploy their backdoors against multiple targets. This frequent use exposes these tools and allows them to become detected. As a countermeasure, the group's tools are preceded in the execution chain by a series of droppers, loaders, and simple downloaders. Typically, the loaders used look for the next stage on the file system or in the registry, decrypt it using AES-128 or ChaCha20, and manually load it in memory via the routines implemented in the MemoryModule library; a dropper is basically a loader but contains the next stage embedded in its body. The main payload, ScoringMathTea in all cases observed, is never present on the disk in unencrypted form. Example execution chains are seen in Figure 1. In some cases, the attackers also deployed a complex downloader that we call BinMergeLoader, which is similar to the MISTPEN malware reported by Google's Mandiant. BinMergeLoader leverages the Microsoft Graph API and uses Microsoft API tokens for authentication.

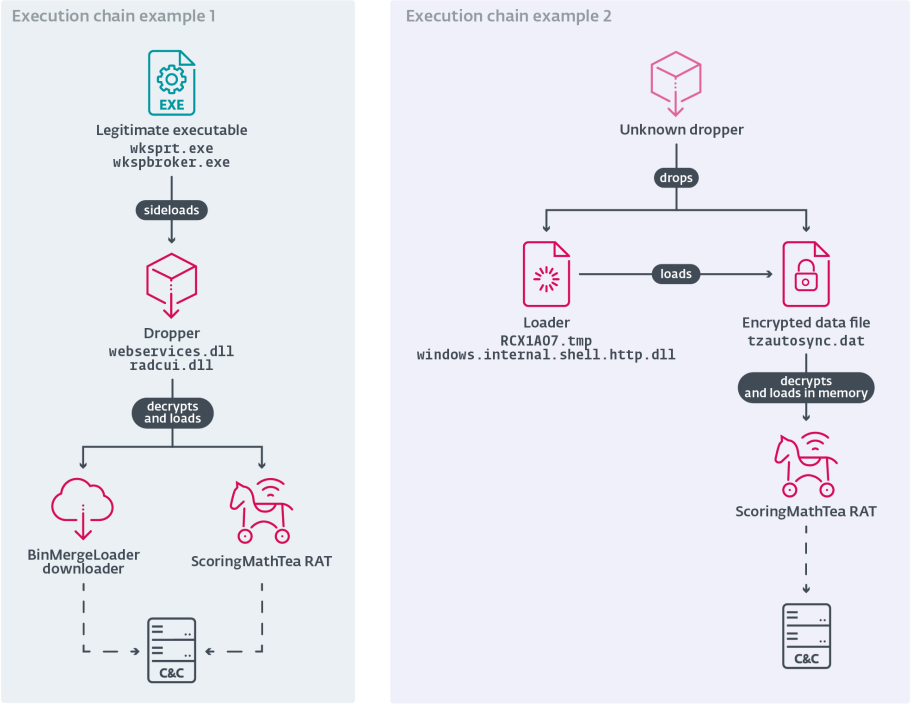

Figure 1. Examples of 2025 Operation DreamJob execution chains delivering BinMergeLoader and ScoringMathTea

The attackers decided to incorporate their malicious loading routines into open-source projects available on GitHub. The choice of project varies from one attack to another. In 2025, we observed the following malware:

- Trojanized TightVNC Viewer and MuPDF reader that serve as downloaders.
- A trojanized end-of-life libpcre v8.45 library for Windows, serving as a loader.
- A loader that has the Mandarin Chinese symbol 样 (yàng in the Pinyin transliteration) as an icon in the resources. It also contains the string SampleIMESimplifiedQuanPin.txt, which suggests that it is probably based on the open-source project Sample IME, a TSF-based input method editor demo. We call this QuanPinLoader.
- Loaders built from the open-source project DirectX Wrappers.
- Downloaders built from open-source plugins for WinMerge (DisplayBinaryFiles and HideFirstLetter). We call the two trojanized plugins BinMergeLoader.
- Trojanized open-source plugins for Notepad++, specifically a downloader very similar to BinMergeLoader (NPPHexEditor v10.0.0 by MacKenzie Cumings) and a dropper of an unknown payload (ComparePlus v1.1.0 by Pavel Nedev). The latter binary contains the PDB path E:\Work\Troy\안정화\wksprt\comparePlus-master\Notepad++\plugins\ComparePlus\ComparePlus.pdb, which suggests the origin of the project (comparePlus-master) and its intended legitimate parent process (wksprt). Also, 안정화 means stable in Korean, which indicates that the code was likely properly tested and reliable.

One of the droppers (SHA-1: 03D9B8F0FCF9173D2964CE7173D21E681DFA8DA4) has the internal DLL name DroneEXEHijackingLoader.dll and is disguised as a Windows Web Services Runtime library in order to be successfully side-loaded; see Figure 2. We believe that the substring drone is there to designate both a UAV device and the attacker's internal campaign name.

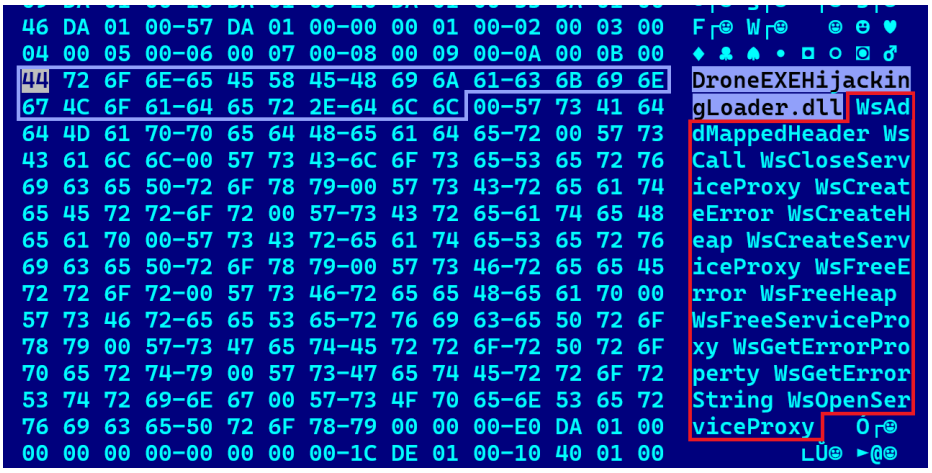

Figure 2. A dropper with a suspicious internal name and exports from a legitimate Microsoft library

Table 1 shows a typical combination of legitimate executable files (EXEs) and malicious dynamic link libraries (DLLs) delivered to the victim's system (this is analogous to Table 1 in our blogpost on an attack against a Spanish aerospace company in 2023). The DLLs in the third column are either trojanized open-source applications (see the fourth column for the underlying project) or a standalone malware binary without such benign context, with a legitimate EXE side-loading it. The location folder (the first column) is unusual for such legitimate applications. Malicious DLLs use the DLL proxying technique, in order not to break the execution. Therefore, when a DLL is also a trojanized project, it contains two heterogeneous types of exports: first the set of functions required for DLL proxying, and second the set of functions exported from the open-source project.

Table 1. Summary of binaries involved in the attack

Location folder	Legitimate parent process	Malicious side-loaded DLL	Trojanized project (payload)
N/A	wksprt.exe*	webservices.dll*	ComparePlus v1.1.0 (N/A)
%ALLUSERSPROFILE%\EMC\ %ALLUSERSPROFILE%\Adobe\	wksprt.exe	webservices.dll	Standalone (ScoringMathTea)

Location folder	Legitimate parent process	Malicious side-loaded DLL	Trojanized project (payload)
%ALLUSERSPROFILE%\	wkspbroker.exe	radcui.dll	DirectX wrappers d3d8.dll/ddraw.dll (ScoringMathTea)
%APPDATA%\Microsoft\RemoteApp\	wkspbroker.exe	radcui.dll	Standalone (BinMergeLoader)

* Denotes a VirusTotal submission and its likely parent process. The payload is unknown, since a long command-line argument is required for its decryption from the trojanized project.

ScoringMathTea

ScoringMathTea is a complex RAT that supports around 40 commands. Its name is a combination of the root ScoringMath, taken from a C&C domain used by an early variant (www.scoringmnmathleague[.]org), and the suffix -Tea, which is ESET Research's designation for a North Korea-aligned payload. It was first publicly documented by Kaspersky in April 2023 and later by Microsoft in October 2023 under the name ForestTiger, which follows the internal DLL name or the PDB information found in some samples.

Its first appearance can be traced back to VirusTotal submissions from Portugal and Germany in October 2022, where its dropper posed as an Airbus-themed job offer lure. The implemented functionality is the usual required by Lazarus: manipulation of files and processes, exchanging the configuration, collecting the victim's system info, opening a TCP connection, and executing local commands or new payloads downloaded from the C&C server. The current version does not show any dramatic changes in its feature set or its command parsing. So the payload is probably receiving continuous, rather minor improvements and bug fixes.

Regarding ESET telemetry, ScoringMathTea was seen in attacks against an Indian technology company in January 2023, a Polish defense company in March 2023, a British industrial automation company in October 2023, and an Italian aerospace company in September 2025. It seems that it is one of the flagship payloads for Operation DreamJob campaigns, even though Lazarus has more sophisticated payloads like LightlessCan at its disposal.

Conclusion

For nearly three years, Lazarus has maintained a consistent modus operandi, deploying its preferred main payload, ScoringMathTea, and using similar methods to trojanize open-source applications. This predictable, yet effective, strategy delivers sufficient polymorphism to evade security detection, even if it is insufficient to mask the group's identity and obscure the attribution process. Also, even with widespread media coverage of Operation DreamJob and its use of social engineering, the level of employee awareness in sensitive sectors – technology, engineering, and defense – is insufficient to handle the potential risks of a suspicious hiring process.

Although alternative hypotheses are conceivable, there are good reasons to think that this Operation DreamJob campaign was in no small part intended to collect sensitive information on UAV-related technology. Considering North Korea's current efforts at scaling up its drone industry and arsenal, it seems likely that other organizations active in this sector will whet the appetite of North Korea-aligned threat actors in the near future.

> *For any inquiries about our research published on WeLiveSecurity, please contact us at threatintel@eset.com.*
>
> *ESET Research offers private APT intelligence reports and data feeds. For any inquiries about this service, visit the ESET Threat Intelligence page.*

IoCs

A comprehensive list of indicators of compromise and samples can be found in our GitHub repository.

Files

SHA-1	Filename	Detection	Description
28978E987BC59E75CA22562924EAB93355CF679E	TSMSISrv.dll	Win64/NukeSped.TL	QuanPinLoader.
5E5BBA521F0034D342CC26DB8BCFECE57DBD4616	libmupdf.dll	Win64/NukeSped.TE	A loader disguised as a MuPDF rendering library v3.3.3.
B12EEB595FEEC2CFBF9A60E1CC21A14CE8873539	radcui.dll	Win64/NukeSped.TO	A dropper disguised as a RemoteApp and Desktop Connection UI Component library.
26AA2643B07C48CB6943150ADE541580279E8E0E	HideFirstLetter.DLL	Win64/NukeSped.TO	BinMergeLoader.
0CB73D70FD4132A4FF5493DAA84AAE839F6329D5	libpcre.dll	Win64/NukeSped.TP	A loader that is a trojanized libpcre library.
03D9B8F0FCF9173D2964CE7173D21E681DFA8DA4	webservices.dll	Win64/NukeSped.RN	A dropper disguised as a Microsoft Web Services Runtime library.
71D0DDB7C6CAC4BA2BDE679941FA92A31FBEC1FF	N/A	Win64/NukeSped.RN	ScoringMathTea.
87B2DF764455164C6982BA9700F27EA34D3565DF	webservices.dll	Win64/NukeSped.RW	A dropper disguised as a Microsoft Web Services Runtime library.
E670C4275EC24D403E0D4DE7135CBCF1D54FF09C	N/A	Win64/NukeSped.RW	ScoringMathTea.
B6D8D8F5E0864F5DA788F96BE085ABECF3581CCE	radcui.dll	Win64/NukeSped.TF	A loader disguised as a RemoteApp and Desktop Connection UI Component library.
5B85DD485FD516AA1F4412801897A40A9BE31837	RCX1A07.tmp	Win64/NukeSped.TH	A loader of an encrypted ScoringMathTea.
B68C49841DC48E3672031795D85ED24F9F619782	TSMSISrv.dll	Win64/NukeSped.TL	QuanPinLoader.
AC16B1BAEDE349E4824335E0993533BF5FC116B3	cache.dat	Win64/NukeSped.QK	A decrypted ScoringMathTea RAT.
2AA341B03FAC3054C57640122EA849BC0C2B6AF6	msadomr.dll	Win64/NukeSped.SP	A loader disguised as a Microsoft DirectInput library.
CB7834BE7DE07F89352080654F7FEB574B42A2B8	ComparePlus.dll	Win64/NukeSped.SJ	A trojanized Notepad++ plugin

SHA-1	Filename	Detection	Description
			disguised as a Microsoft Web Services Runtime library. A dropper from VirusTotal.
262B4ED6AC6A977135DECA5B0872B7D6D676083A	**tzautosync.dat**	**Win64/NukeSped.RW**	**A decrypted ScoringMathTea, stored encrypted on the disk.**
086816466D9D9C12FCADA1C872B8C0FF0A5FC611	**N/A**	**Win64/NukeSped.RN**	**ScoringMathTea.**
2A2B20FDDD65BA28E7C57AC97A158C9F15A61B05	**cache.dat**	**Win64/NukeSped.SN**	**A downloader similar to BinMergeLoader built as a trojanized NPPHexEditor plugin.**

Network

IP	Domain	Hosting provider	First seen	Details
23.111.133[.]162	coralsunmarine[.]com	HIVELOCITY, Inc.	2024-06-06	ScoringMathTea C&C server: https://coralsunmarine[.]com/wp-content/themes/flatsome/inc/functions/function-hand.ph
104.21.80[.]1	kazitradebd[.]com	Cloudflare, Inc.	2025-01-11	ScoringMathTea C&C server: https://kazitradebd[.]com/wp-content/themes/hello-elementor/includes/customizer/customizer-hand.php
70.32.24[.]131	oldlinewoodwork[.]com	A2 Hosting, Inc.	2024-06-14	ScoringMathTea C&C server: https://oldlinewoodwork[.]com/wp-content/themes/zubin/inc/index.php
185.148.129[.]24	www.mnmathleague[.]org	A2 Hosting, Inc.	2024-06-15	ScoringMathTea C&C server: https://www.mnmathleague[.]org/ckeditor/adapters/inde
66.29.144[.]75	pierregems[.]com	Namecheap, Inc.	2024-08-11	ScoringMathTea C&C server: https://pierregems[.]com/wp-content/themes/woodmart/inc/configs/js-hand.php
108.181.92[.]71	www.scgestor.com[.]br	Psychz Networks	2024-07-15	ScoringMathTea C&C server: https://www.scgestor.com[.]br/wp-content/themes/vantage/inc/template-headers.php
104.247.162[.]67	galaterrace[.]com	GNET Internet Telekomunikasyon A.S.	2024-06-27	ScoringMathTea C&C server: https://galaterrace[.]com/wp-content/themes/hello-elementor/includes/functions.php
193.39.187[.]165	ecudecode[.]mx	Heymman Servers Corporation	2025-05-14	ScoringMathTea C&C server: https://ecudecode[.]mx/redsocial/wp-content/themes/buddyx/inc/Customizer/usercomp.php
172.67.193[.]139	www.anvil.org[.]ph	Cloudflare, Inc.	2025-02-22	ScoringMathTea C&C server: https://www.anvil.org[.]ph/list/images/index.php
77.55.252[.]111	partnerls[.]pl	Nazwa.pl Sp.z.o.o.	2025-06-02	ScoringMathTea C&C server: https://partnerls.pl/wp-content/themes/public/index.php

IP	Domain	Hosting provider	First seen	Details
45.148.29[.]122	trainingpharmacist .co[.]uk	Webdock.io ApS	2024-06-13	ScoringMathTea C&C server: https://trainingpharmacist.co.uk/bootstrap/bootstrap.php
75.102.23[.]3	mediostresbarbas .com[.]ar	DEFT.COM	2024-06-05	ScoringMathTea C&C server: https://mediostresbarbas.com[.]ar/php_scrip/banahostin
152.42.239[.]211	www.bandarpowder [.]com	DigitalOcean, LLC	2024-09-19	ScoringMathTea C&C server: https://www.bandarpowder[.]com/public/assets/buttons/
95.217.119[.]214	spaincaramoon[.]com	Hetzner Online GmbH	2025-04-30	ScoringMathTea C&C server: https://spaincaramoon[.]com/realestate/wp-content/plugins/gravityforms/forward.php

MITRE ATT&CK techniques

This table was built using version 17 of the MITRE ATT&CK framework.

Tactic	ID	Name	Description
Resource Development	T1584.004	Compromise Infrastructure: Server	ScoringMathTea uses compromised servers for C&C.
	T1587.001	Develop Capabilities: Malware	All stages in the attack were likely developed by the attackers.
Execution	T1106	Native API	Windows APIs are essential for ScoringMathTea to function and are resolved dynamically at runtime.
	T1129	Shared Modules	ScoringMathTea is able to load a downloaded DLL with the exports fun00 or exportfun00.
	T1204.002	User Execution: Malicious File	Lazarus attackers relied on the execution of trojanized PDF readers.
Persistence	T1574.002	Hijack Execution Flow: DLL Side-Loading	Trojanized droppers (webservices.dll, radcui.dll) use legitimate programs (wksprt.exe, wkspbroker.exe) for their loading.
Defense Evasion	T1134.002	Access Token Manipulation: Create Process with Token	ScoringMathTea can create a new process in the security context of the user represented by a specified token.
	T1140	Deobfuscate/Decode Files or Information	The main payload, ScoringMathTea, is always encrypted on the file system.

	T1027.007	Obfuscated Files or Information: Dynamic API Resolution	ScoringMathTea resolves Windows APIs dynamically.
	T1027.009	Obfuscated Files or Information: Embedded Payloads	The droppers of all malicious chains contain an embedded data array with an additional stage.
	T1620	Reflective Code Loading	The droppers and loaders use reflective DLL injection.
	T1055	Process Injection	ScoringMathTea and BinMergeLoader can reflectively load a DLL in the process specified by the PID.
Discovery	T1083	File and Directory Discovery	ScoringMathTea can locate a file by its name.
	T1057	Process Discovery	ScoringMathTea can list all running processes.
	T1082	System Information Discovery	ScoringMathTea can mimic the ver command.
Command and Control	T1071.001	Application Layer Protocol: Web Protocols	ScoringMathTea and BinMergeLoader use HTTP and HTTPS for C&C.
	T1573.001	Encrypted Channel: Symmetric Cryptography	ScoringMathTea encrypts C&C traffic using the IDEA algorithm and BinMergeLoader using the AES algorithm.
	T1132.001	Data Encoding: Standard Encoding	ScoringMathTea adds a base64-encoding layer to its encrypted C&C traffic.
Exfiltration	T1041	Exfiltration Over C2 Channel	ScoringMathTea can exfiltrate data to its C&C server.

Source: https://www.welivesecurity.com/en/eset-research/gotta-fly-lazarus-targets-uav-sector/