

A Pain in the Mist: Navigating Operation DreamJob's arsenal

 orangecyberdefense.com/global/blog/cert-news/a-pain-in-the-mist-navigating-operation-dreamjobs-arsenal

November 20, 2025



Authors:

Marine Pichon, Alexis Bonnefoi

Acknowledgments:

Special thanks to P. Kálnai (ESET) and E. Kee (BAE Systems) for their insights on the North Korean malware arsenal.

Special thanks to Alexandre Matousek, Friedl Holzner, Gordon Brebner, James O'Neill, and Nadine Scheid (Orange Cyberdefense).

[Download the full report](#)

Executive summary

- In August 2025, Orange Cyberdefense's CyberSOC and CSIRT investigated an intrusion targeting an **Asian subsidiary of a large European manufacturing organization**.
- The infection chain was initiated by a targeted WhatsApp Web message containing a **job-related** lure sent to a project engineer.

- The intrusion leveraged variants of the **BURNBOOK** loader and the **MISTPEN** backdoor as well as compromised **SharePoint** and **WordPress** resources for C2 infrastructure.
- The full PDF report aims to describe the infection chain we observed, and to provide a comparative analysis of the BURNBOOK and MISTPEN variants encountered. Recommendations and hunting guidance are also provided in the concluding section.
- We assess that this attack coincides with the longstanding **Operation DreamJob**. We also attribute the attacks artifacts with medium confidence to **UNC2970**.

Note: The analysis cut-off date for this report was November 17, 2025.

Infection chain

The infection chain was initiated by social engineering and a targeted WhatsApp message containing a job-related lure sent to a project engineer. This known social engineering tactic lured the victim to download and open a ZIP archive on its desktop, through the browser-based version of the WhatsApp mobile application (**WhatsApp Web**).

The archive contained:

- A malicious PDF file
- A legitimate open-source document viewing application **SumatraPDF.exe**
- A malicious DLL named **libmupdf.dll**

Once the PDF was opened, the legitimate executable sideloaded the malicious DLL, eventually executing a backdoor. We assess with high confidence **libmupdf.dll** is a recent **BURNBOOK** variant.

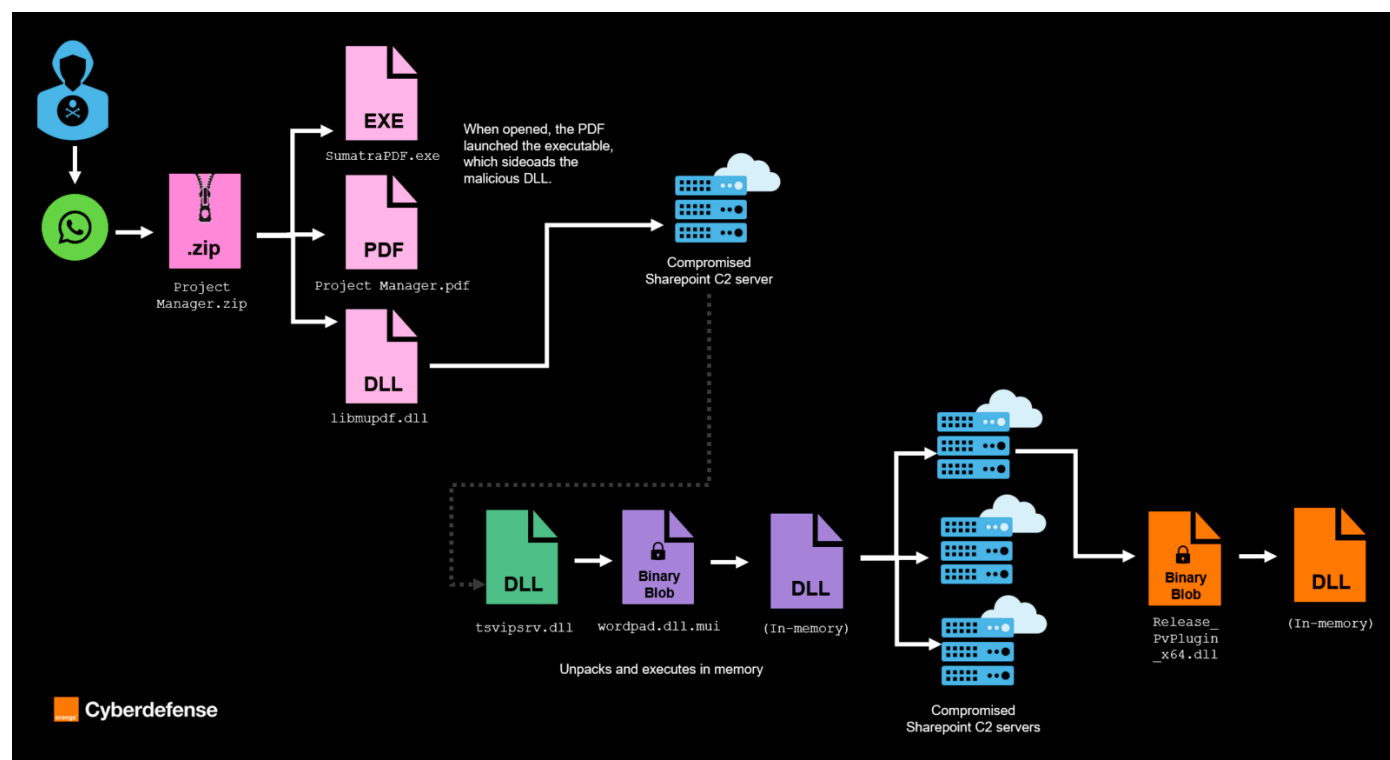


Figure 1: Partial description of the infection chain

Our CSIRT then observed the threat actors carry out **hands-on-keyboard activities** for at least six consecutive hours, using compromised WordPress sites with vulnerable plugins as part of their attack infrastructure. At this point, the 'low' volume of data exchanged suggests the network traffic primarily related to command and control, as opposed to data exfiltration activities. The threat actors notably made multiple LDAP queries to the Active Directory to extract lists of users and computers in the domain. Our CSIRT subsequently identified the compromise of both a backup account and an administrative account. The attacker used the 'pass-the-hash' technique, leveraging the accounts' password hashes to gain access without ever needing the plaintext passwords. This then allowed **lateral movement** to several servers in the domain.

Following successful network discovery and lateral movement, the threat actors were observed attempting to install another malicious payload on several devices. This payload, **TSVIPsrv.dll**, decrypted and executed in memory **wordpad.dll.mui**, which then initiated network connections to compromised SharePoint servers for C2 communications. We assess with high confidence TSVIPsrv.dll is a recent **MISTPEN** variant.

Upon many requests to SharePoint-based C2s, the payload received and decrypted another final payload, **Release_PvPlugin_x64.dll**. This one acts as a short information-stealing module.

[Download the full report](#)

Conclusion

Our technical report aimed to detail the characteristics of two key malware families - **BURNBOOK** and **MISTPEN** - leveraged by the North Korean **UNC2970** cluster, through DFIR insights and reverse engineering.

Despite its age, Operation DreamJob remains active and regularly upgraded. Attacks can be hard to detect due to their combination and chaining of a large number of constantly modified droppers, loaders, and simple downloaders designed to decrypt and execute in memory even more versatile malware.

Through the combined work of analysts across multiple Orange Cyberdefense teams, and by expanding on previously published CTI research, we aim to offer a clearer view of the current North Korean malware arsenal.

Recommendations

This campaign relies heavily on **social engineering** to compromise targets. It is therefore essential to ensure that personnel most likely to be approached - particularly roles in IT (developers, system administrators, helpdesk teams) and Human Resources - are fully **aware** of

the common tactics used, emphasizing on how threat actors frequently tailor job-themed lures and impersonate recruiters.

One of the campaign's notable initial access techniques involves using **WhatsApp Desktop** to deliver malicious content and initiate further social engineering exchanges. Restricting the use of WhatsApp Desktop as well as other similar instant messaging applications within the corporate environment or implementing monitoring controls to detect suspicious activity related to this application, can help disrupt this initial access vector.

It is also possible to identify and block potentially malicious software executed through DLL sideloading by using application control solutions capable of blocking suspicious DLL loads by legitimate software.

For organizations with an elevated risk profile, security operations teams should proactively **search for known indicators** associated with DPRK activity clusters. Regular threat hunting using relevant IOCs, behavioral patterns, and TTPs improves **early detection** and limits dwell time in the event of attempted compromise.

As a relevant hunting approach, you can for instance search for legitimate executables like SumatraPDF or TightVNC being created and executed inside the user's personal directory (ie. Downloads, %TEMP%, ...). You can also hunt for unexpected DLL loaded from non-standard directories.

Orange Cyberdefense's [Datalake](#) platform provides access to Indicators of Compromise (IoCs) related to this threat, which are automatically fed into our [Managed Threat Detection services](#). This enables proactive hunting for IoCs if you subscribe to our Managed Threat Detection service that includes Threat Hunting.

Orange Cyberdefense's [Managed Threat Intelligence](#) service offers the ability to automatically feed network-related IoCs into your security solutions. To learn more about this service and to find out which firewall, proxy, and other vendor solutions are supported, please get in touch with your Orange Cyberdefense Trusted Solutions representative.

The Orange Cyberdefense **Computer Security Incident Response team (CSIRT)** provides emergency consulting, incident management, and technical advice to help customers handle a security incident from initial detection to closure and full recovery. If you suspect being attacked, do not hesitate to call our [hotline](#).

IOCs

The Indicators of Compromise related to this investigation are also available on our [GitHub](#).

File IOCS

BURNBOOK variants

7b4cb382b364389c3bd1f4736411de17ceb213a7792733ae5dd90c8b01b4191f
ec5d14ca011ba8c12f4d51b0d463cf51051feaf1655c7f709dce3ffa625dfcf6
083d4a4ef6267c9a0ab57f1e5a2ed45ff67a0b4db83bbd43563458a223781120

MISTPEN variants

e3e0a87e18de05c4abb95fc21f22d6c9c367eb207dbbf2dd092673656caf7661
f5873ecd60390e7b86db5ddaf158ed201b386be26ad80af8a7da3576446520b8
aefc12b500b58fbc09ebbf34fe64b34cb32a27513478f4769447280ad23af4d2
0fdd97a597380498f6b2d491f8f50da8f903def4ea6e624b89757456c287f92d

wordpad.dll.mui

4eeec453e42c2898e2e9870bbec273834aeb8cdde8c826c036f9a7d0b568a25d

Network IOCs

cseabrahamlincoln-my[.]sharepoint[.]com

aerm-my.sharepoint[.]com

alex2moe-my[.]sharepoint[.]com/

diakoffice-my[.]sharepoint[.]com

isiswauitmedu-my.sharepoint[.]com

[https://tours-albatros\[.\]es/wp-content/plugins/soliloquy-lite/includes/global/skin\[.\]php](https://tours-albatros[.]es/wp-content/plugins/soliloquy-lite/includes/global/skin[.]php)

[https://kutahyasmmmo\[.\]org/wp-content/mu-plugins/natro/external_plugins/easy-wp-smtp/easy-wp-smtp-menu\[.\]php](https://kutahyasmmmo[.]org/wp-content/mu-plugins/natro/external_plugins/easy-wp-smtp/easy-wp-smtp-menu[.]php)

[https://coralsunmarine\[.\]com/wp-content/themes/flatsome/inc/functions/function-hand\[.\]php](https://coralsunmarine[.]com/wp-content/themes/flatsome/inc/functions/function-hand[.]php)