A Pain in the Mist

Published: 2025-11-20 · Archived: 2026-04-05 22:36:31 UTC

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.
