

UAC-0057 Attack Detection: A Surge in Adversary Activity Distributing PICASSOLOADER and Cobalt Strike Beacon

By Veronika Zahorulko

Published: 2024-07-25 · Archived: 2026-04-05 15:25:25 UTC

Defenders have observed a sudden surge in the adversary activity of the [UAC-0057](#) hacking group targeting Ukrainian local government agencies. Attackers distribute malicious files containing macros aimed at launching [PICASSOLOADER](#) on the targeted computers, which leads to the delivery of [Cobalt Strike Beacon](#).

Detect UAC-0057 Activity Covered in the CERT-UA#10340 Alert

[Since the full-scale war outbreak](#), the UAC-0057 hacking collective has repeatedly targeted Ukrainian organizations. To detect the latest UAC-0057 campaign and analyze the group's activity retrospectively, cyber defenders might rely on SOC Prime's Platform for collective cyber defense, which offers a complete product suite for AI-powered Detection Engineering, Automated Threat Hunting, and Detection Stack Validation.

By following the link below, security professionals can access the comprehensive detection stack addressing the latest UAC-0057 activity. Alternatively, experts can browse Threat Detection Marketplace filtering detections by the "CERT-UA#10340" tag based on the alert ID.

[Sigma rules for UAC-0057 attack detection based on the CERT-UA#10340 alert](#)

All detection algorithms are mapped to the [MITRE ATT&CK® framework](#), enriched with actionable CTI and metadata, and are ready to deploy into dozens of cloud-native and on-premises security analytics platforms.

To obtain the broader detection stack addressing UAC-0057 tactics, techniques, and procedures, security engineers can access the relevant Sigma rules collection by clicking the **Explore Detections** button below.

[Explore Detections](#)

The [dedicated CERT-UA alert](#) also provides a collection of IOCs to identify attacks related to the most recent UAC-0057 campaign. By relying on SOC Prime's [Uncoder AI](#), defenders can simplify IOC matching by instantly converting relevant threat intelligence into custom performance-optimized queries tailored for the language format of the chosen SIEM or EDR and ready to hunt in the selected environment.

UAC-0057 Attack Analysis

The UAC-0057 group, also known under the moniker of GhostWriter, has been launching multiple offensive operations primarily targeting Ukrainian state bodies throughout 2023. For instance, in September 2023, [UAC-0057 launched a malicious campaign](#) against the Ukrainian government and educational institutions, abusing a WinRAR zero-day (CVE-2023-38831) to deliver PICASSOLOADER. In the summer of 2023, the group leveraged the same loader to infect targeted networks with njRAT.

In July 2024, CERT-UA observed a sudden spike in the group’s activity. Adversaries weaponized files containing malicious macros to spread [PICASSOLOADER](#) and [Cobalt Strike Beacon](#) on the impacted systems.

According to the [latest CERT-UA alert](#) on the UAC-0057 activity, the contents of the uncovered files with macros (“oborona.rar,” “66_oborona_PURGED.xls,” “trix.xls,” “equipment_survey_regions_.xls,” “accounts.xls,” “spreadsheet.xls,” “attachment.xls,” “Podatok_2024.xls”) are linked to local government reform, taxation, and financial-economic indicators.

Based on the CERT-UA research, UAC-0057 may have targeted both project office specialists and their counterparts among employees of relevant local government authorities in Ukraine.

MITRE ATT&CK Context

Leveraging MITRE ATT&CK provides extensive visibility into the behavior patterns related to the latest UAC-0057 malicious activity targeting Ukrainian local government agencies. Explore the table below to see the full list of dedicated Sigma rules addressing the corresponding ATT&CK tactics, techniques, and sub-techniques.

Source: <https://socprime.com/blog/uac-0057-attack-detection-a-surge-in-adversary-activity-distributing-picassoloader-and-cobalt-strike-beacon/>