UAC-0102 Phishing Attack Detection: Hackers Steal Authentication Data Impersonating the UKR.NET Web Service

WRITTEN BY

Veronika Telychko

Technical Writer

[post-views]

July 26, 2024 · 4 min read

Leveraging public email services along with corporate email accounts is a common practice among government employees, military personnel, and the staff of other Ukrainian enterprises and organizations. However, adversaries might abuse these services to launch phishing attacks. Defenders have recently uncovered a new offensive activity aimed at stealing user authentication data by luring victims into using a fake web resource disguised as the popular UKR.NET service.

UAC-0102 Phishing Attack Analysis

On July 24, 2024, CERT-UA researchers issued a novel heads-up, CERT-UA#10381, notifying defenders of an ongoing phishing attack targeting UKR.NET users. Throughout July 2024, the UAC-0102 group has been distributing emails with archive attachments containing HTML files. Opening these files redirects the compromised user to a fraudulent website impersonating the UKR.NET service, further potentially leading to authentication data theft.

If targeted users enter their credentials leveraging the fraudulent web service, the authentication data will be sent to attackers, while victims will see a lure file downloaded onto the impacted computer.

To minimize the risks of the ongoing UAC-0102 phishing attack and help organizations reduce the attack surface, CERT-UA recommends enabling two-factor authentication, avoiding the use of public email services on official computers, setting up a filter to forward copies of incoming emails to a corporate email address, and enabling retrospective analysis of the email using existing security tools.

Detect UAC-0102 Phishing Attack Impersonating UKR.NET to Target Ukrainian Businesses

In the third year of the full-scale war in Ukraine, offensive forces are constantly increasing their malicious activity, frequently relying on the phishing attack vector to proceed with the intrusion. For instance, on July 17, 2024, CERT-UA reported a malicious campaign by UAC-0180, relying on phishing emails to drop GLUEEGG, DROPCLUE, and ATERA onto the networks of the Ukrainian defense contractors. The most recent CERT-UA alert warns of a UAC-0102 attack also utilizing phishing to steal sensitive data from enterprises in Ukraine.

To help cyber defenders proactively identify and secure their infrastructure from UAC-0102 attacks, SOC Prime's Platform for collective cyber defense provides access to a set of Sigma rules detecting the latest phishing campaign by adversaries.

Archive Extraction Directly from Mail Client (via process_creation)

This rule by the SOC Prime Team helps detect archive extraction via mail client (where the archive is an attachment) while being compatible with 27 SIEM, EDR, and Data Lake technologies. The detection is mapped to MITRE ATT&CK®, which addresses the Initial Access tactics, with Spearphishing Attachment (T1566.001) as a key sub-technique.

Suspicious File Download Direct IP (via proxy)

Another rule by the SOC Prime Team helps to identify suspicious executables, scripts, binary, or other file types downloaded directly from an IPv4 address, which is not usual. The detection algorithm is compatible with 22 SIEM, EDR, and Data Lake solutions and mapped to MITRE ATT&CK addressing the Command and Control tactics, with Ingress Tool Transfer (T1105) Web Protocols (T1071.001) as corresponding techniques and sub-techniques.

Security teams can also search for the relevant detection content using the tag "UAC-0102" based on the adversary identifier. Click the **Explore Detections** button to drill down to Sigma rules associated with the UAC-0102 attacks and dive into the comprehensive threat context behind the malicious activity, including CTI, ATT&CK references, and other relevant metadata.

Explore Detections

In addition, defenders can leverage IOCs linked to the latest UAC-0102 phishing attack provided in the CERT-UA#10381 alert. Rely on Uncoder AI to instantly convert threat intel into custom IOC queries and hunt for UAC-0102 activity in the selected SIEM or EDR environment.


Use Uncoder AI to hunt for IOCs related to the UAC-0102 activity based on the CERT-UA#10381 research

Stay ahead of emerging threats and cyber attacks of any scale and complexity with SOC Prime's Platform for collective cyber defense based on global threat intelligence, crowdsourcing, zero-trust, and AI.

Table of Contents