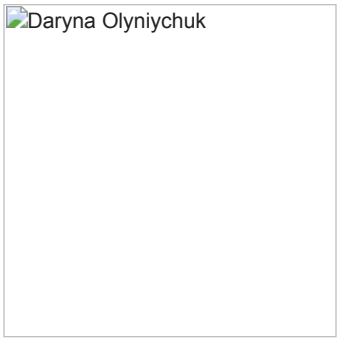
New Phishing Attack Detection Attributed to the UAC-0050 and UAC-0096 Groups Spreading Remcos Spyware

socprime.com/blog/new-phishing-attack-detection-attributed-to-the-uac-0050-and-uac-0096-groups-spreading-remcos-spyware/

Daryna Olyniychuk



February 2023 can be marked as a month of ongoing adversary campaigns against Ukraine, exploiting the phishing attack vector and leveraging remote access software. Close on the heels of phishing attacks spreading Remcos RAT and abusing Remote Utilities software, another mass email distribution targeting Ukrainian organizations garners attention from cyber defenders. The latest CERT-UA#6011 alert details this targeted phishing campaign impersonating the Pechersk District Court of Kyiv and aimed to drop Remcos spyware on the compromised systems.

Phishing Attacks Leveraging Remcos Malware Covered in the CERT-UA#6011 Alert

With the one-year anniversary of the full-scale war in Ukraine approaching, offensive forces are increasing their malicious activity, mainly via the phishing attack vector. In February 2023, at least three ongoing adversary campaigns against Ukraine were in the spotlight in the cyber threat arena, all of which took advantage of the remote access tools highly likely for cyber espionage activities.

On February 21, 2023, CERT-UA researchers issued a new alert warning cyber defenders of another phishing attack spreading Remcos spyware. The ongoing fraudulent email campaign follows familiar behavioral patterns observed in earlier February's attacks. Threat actors masquerade the sender as the Pechersk District Court of Kyiv and apply a lure RAR file striving to trick targeted users into opening it. The infection chain is triggered by extracting the archive, which contains a TXT file and another password-protected RAR file. The latter, in turn, contains the malicious executable lure file with a fraudulent digital signature disguised as a legitimate one. Launching the latter EXE file will end up dropping Remcos spyware on the compromised system.

After gaining access to the targeted system and successfully spreading infection, threat actors proceed with data exfiltration and can exploit the compromised computer for network reconnaissance and further attacks on the organization's infrastructure.

CERT-UA investigation has linked the adversary behavior patterns observed in the ongoing phishing campaign with the similar ones displayed by threat actors in another February cyber attack exploiting Remote Utilities software. Researchers have discovered identical IP addresses used for one of the emails in the latest campaign and the previous one. Based on observed behavioral similarities, CERT-UA researchers suggest tracking two hacking collectives behind both campaigns (UAC-0050 and UAC-0096) under a single identifier UAC-0050.

Detect the Latest Remcos Spyware Campaign Targeting Ukrainian Entities

Ukraine keeps fighting on the frontline of the first-ever full-scale cyber war in human history, constantly withstanding the avalanche of cyber attacks against government bodies and business assets. To help Ukraine and its allies proactively defend against russia-affiliated intrusions of any scale and detect adversary TTPs, SOC Prime Platform for collective cyber defense provides access to a comprehensive list of Sigma rules detecting the malicious activity and associated with Remcos spyware and Remote Utilities software abuse. All the detections are compatible with 25+ SIEM, EDR, and XDR solutions to ensure security practitioners can leverage those matching their security environment.

Hit the **Explore Detections** button below to reach the dedicated set of curated alerts and hunting queries enriched with extensive metadata, including MITRE ATT&CK® references and cyber threat intelligence links. To streamline the search for relevant Sigma rules, SOC Prime Platform supports filtering by custom tags "UAC-0050", "UAC-0096", and "CERT-UA#6011" based on a dedicated CERT-UA alert and the corresponding identifiers of the hacking collectives.

Explore Detections

Security performers can also streamline their threat hunting activities by searching for relevant indicators of compromise by leveraging the novel version of Uncoder.IO tool that helps to covert IoCs into curated hunting queries ready to run in a chosen SIEM & XDR environment. Just find relevant IoCs by using the search bar or paste the text with file, host, or network IoCs provided by CERT-UA to instantly get a performance-optimized query. Uncoder.IO is a free project developed with privacy in mind — no authentication, no log collection, and all data is kept session-based for your peace of mind.


IOCs from the CERT-UA#6011 alert to search for Remcos-related threats via Uncoder.IO

MITRE ATT&CK Context

To delve into the in-depth context behind the Remcos malicious campaign reported in the CERT-UA#6011 alert, all above-referenced Sigma rules are tagged with ATT&CK v12 addressing the relevant tactics and techniques:

Tactics	Techniques	Sigma Rule
Initial Access	Phishing (T1566)	Execution from RAR Archive (via process_creation)
Suspicious Extracted Files from an Archive (via file_event)		
Archive Extraction Directly from Mail Client (via process_creation)		
Execution from Zip (via process_creation)		
Persistence	Boot or Logon Autostart Execution (T1547)	Possible Persistence Points [ASEPs - Software/NTUSER Hive] (via registry_event)

Join SOC Prime's Detection as Code platform to improve visibility into threats most relevant to your business. To help you get started and drive immediate value, book a meeting now with SOC Prime experts.

Join for Free Book a Meeting