Remcos RAT Detection: UAC-0050 Hackers Launch Phishing Attacks Impersonating the Security Service of Ukraine

socprime.com/blog/remcos-rat-detection-uac-0050-hackers-launch-phishing-attacks-impersonating-the-security-service-of-ukraine/

Veronika Telychko

CERT-UA researchers have recently published a novel heads-up that covers ongoing phishing attacks against Ukraine involving distribution of Remcos RAT. The group in charge of this offensive campaign, which involves massively distributing spoofing emails with a false sender identity masquerading as the Security Service of Ukraine, is tracked as UAC-0050.

UAC-0050 Attack Analysis Covered in the CERT-UA#8026 Alert

On November 13, 2023, CERT-UA released a security notice unveiling a novel phishing campaign distributing Remcos RAT and attributed to the UAC-0050 group. The latter is considered behind a couple of phishing attacks targeting Ukrainian organizations in February 2023. Both malicious operations involved spreading Remcos Trojan and relied on a false sender identity to lure victims into opening weaponized emails.

In the latest campaign, attackers take advantage of phishing emails impersonating the sender as the Security Service of Ukraine and involving lure RAR files. The last archive within the malicious email includes an EXE file that leads to deploying Remcos on the impacted instances. Adversaries maintain persistence by creating an entry in the Run key of the OS registry.

The malware configuration file contains 8 IP addresses of the C2 servers that are linked to the popular Malaysian web hosting provider known as Shinjiru. Notably, the domain names are registered via the russian company REG.RU.

Detect UAC-0050 Latest Phishing Attacks Using Remcos RAT

Throughout 2023, UAC-0050 has launched a series of attacks against Ukraine abusing the phishing attack vector and distributing Remcos Trojan, including the most recent adversary campaign addressed in the CERT-UA#8026 alert. SOC Prime Platform arms defenders with detection algorithms against existing and emerging threats, so organizations can continuously enhance their cyber resilience. Follow the link below to obtain relevant Sigma rules filtered by the custom tag “CERT-UA#8026” to proactively detect phishing attacks covered in the latest CERT-UA heads-up.

Sigma rules to detect attacks by UAC-0050 covered in the CERT-UA#8026 alert

To reach the comprehensive list of SOC content for other attacks against Ukraine linked to UAC-0050, press **Explore Detections.** The detection content is mapped to the MITRE ATT&CK framework, enriched with CTI and relevant metadata, and can be used across multiple security analytics platforms while bridging the gap between multiple language formats.

Explore Detections

Teams can also hunt for file, host, and network IOCs provided by CERT-UA using SOC Prime’s open-source IDE for Detection Engineering that now supports IOC packaging. Try Uncoder IO to automatically create performance-optimized search queries and immediately run them in your SIEM or EDR environment while shaving seconds off your threat investigation.


Use Uncoder IO to hunt for UAC-0050 adversary activity with custom search queries based on IOCs from the CERT-UA#8026 alert.

MITRE ATT&CK Context

Leveraging MITRE ATT&CK provides granular visibility into the context of offensive operations attributed to UAC-0050. Explore the table below to see the full list of dedicated Sigma rules addressing the corresponding ATT&CK tactics, techniques, and sub-techniques.

Tactics	Techniques	Sigma Rule
Execution	Command and Scripting Interpreter: Unix Shell (T1059.004)	FIFO Special File Creation (via cmdline)
Possible Python (GTFOBin) Activity by Use of Unusual Command Arguments (via cmdline)		
Privilege Escalation	Exploitation for Privilege Escalation (T1068)	Possible Python (GTFOBin) Activity by Use of Unusual Command Arguments (via cmdline)
Possible perl (GTFOBin) Privilege Escalation by Use of Unusual Command Arguments (via cmdline)		
Defense Evasion	Abuse Elevation Control Mechanism (T1548)	Possible Python (GTFOBin) Activity by Use of Unusual Command Arguments (via cmdline)
Abuse Elevation Control Mechanism: Sudo and Sudo Caching (T1548.003)	Running Shell (zsh/bash/sh) in Privileged Context (via cmdline)	
Hide Artifacts: Hidden Files and Directories (T1564.001)	Hidden File Was Created On Linux Host (via file_event)	
Credential Access	Exploitation for Credential Access (T1212)	Possible Python (GTFOBin) Activity by Use of Unusual Command Arguments (via cmdline)
Modify Authentication Process: Pluggable Authentication Modules (T1556.003)	Shared Object File Was Created (via file_event)	
Collection	Data from Local System (T1005)	Possible Python (GTFOBin) Activity by Use of Unusual Command Arguments (via cmdline)
Command and Control	Non-Application Layer Protocol (T1095)	FIFO Special File Creation (via cmdline)
Exfiltration	Exfiltration Over Web Service (T1567)	Possible Python (GTFOBin) Activity by Use of Unusual Command Arguments (via cmdline)