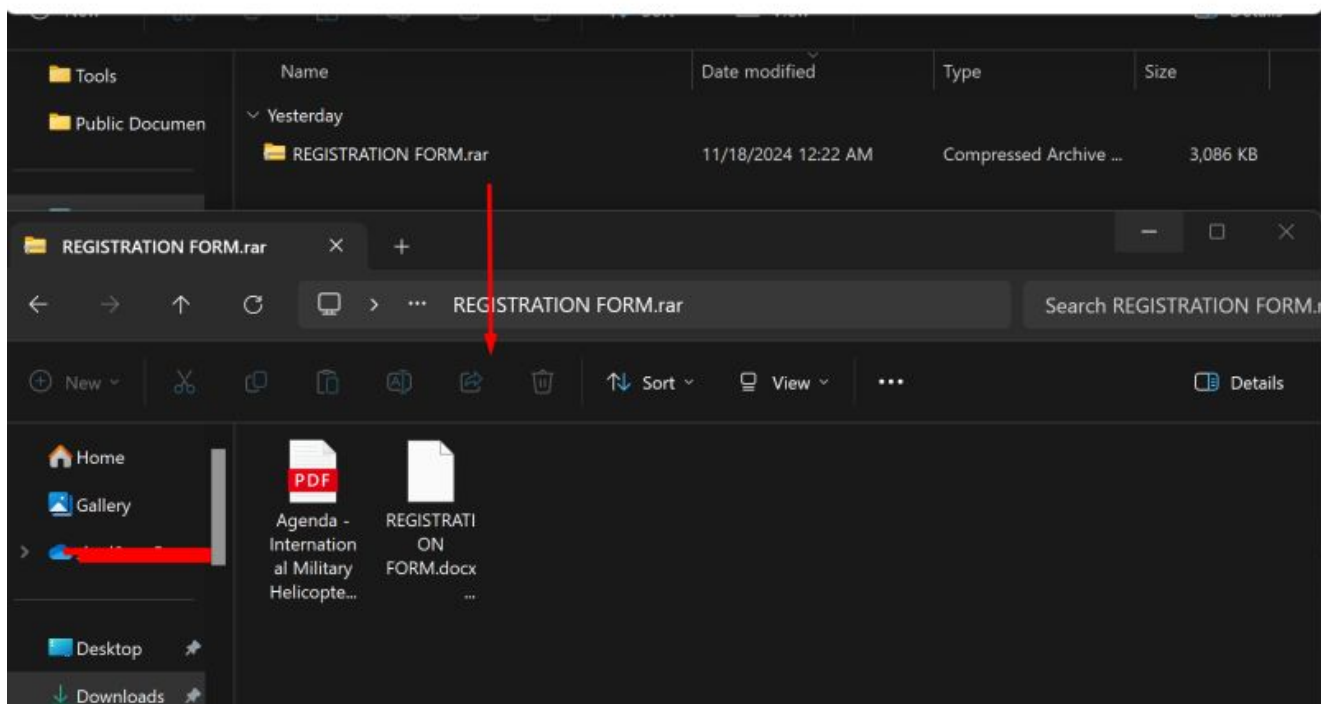
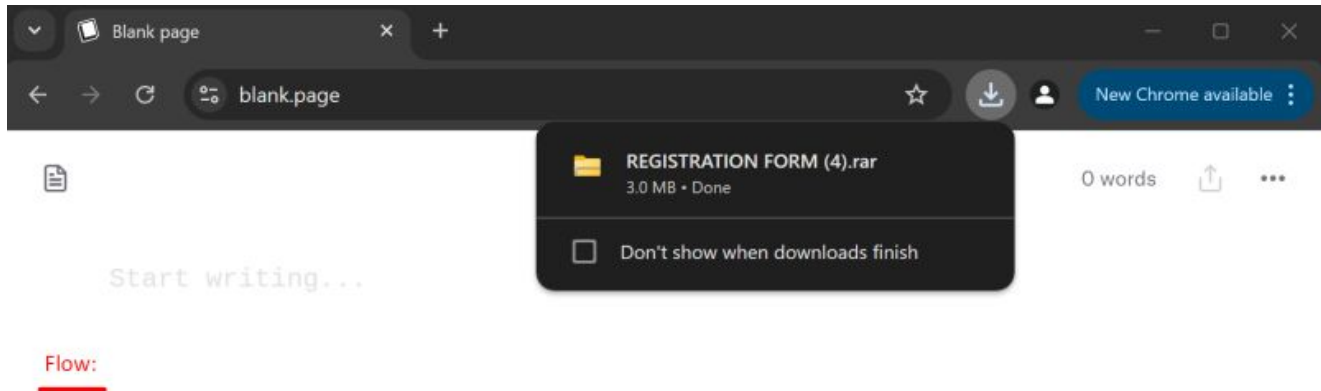


#uac0099 #apt #russianukrainianwar #ttps #threat #ukrainerussiawar...

[in linkedin.com/posts/idan-tarab-7a9057200_uac0099-apt-russianukrainianwar-activity-7264650176080855040-Zuud/](https://www.linkedin.com/posts/idan-tarab-7a9057200_uac0099-apt-russianukrainianwar-activity-7264650176080855040-Zuud/)



[View profile for Idan Tarab, graphic](#)

[Idan Tarab](#)

Security analyst, MDR @ At-Bay

1mo Edited

--- 🚨 Threat alert 🚨 --- 🇺🇦 "The IT Army of Ukraine: Cyber Resistance in the Digital Battlefield" 🇷🇺 #UAC0099 #APT #RussianUkrainianWar #TTPS #threat #Ukrainerussiawar #malware #Cybersecurity #CERTUA --- ► Flow: #Phishing Link -> .Rar_drops ->

Contains_decoyPDF +.#LNK[docx] -> .LNK_execution -> c2_remote_Server_Connecting [newyorktimes[.]life] -> Decoy_Docx_Established [Temp] -> Schtask_created -> .#VBS +firefox[.]exe created -> execution -> c2_recieverData [Post_req] --- 💡 Who Are They? #UAC-0099 is a cyber threat actor group, tracked by security agencies, known for carrying out advanced and persistent cyberattacks. While their specific origin is not definitively confirmed, UAC-0099 is often associated with nation-state interests and geopolitical motives. Known for espionage, data theft, and network manipulation. --- 🎯 #Agenda: 1. Government Agencies: Targeting military and intelligence for sensitive political and strategic data. 2. Private Corporations: Focused on sectors like tech, defense, finance, and energy for intellectual property and financial data. 3. Critical Infrastructure: Aiming to sabotage or control systems like energy grids and transportation to disrupt security or economic stability. - -- 📖 #Motivation: 1. State-Sponsored Espionage: Driven by national security goals, such as gathering sensitive data on government, military, or critical infrastructure targets. 2. Intellectual Property Theft: Aimed at stealing trade secrets or technology to gain an economic edge for a nation-state or corporation. 3. Cyber Warfare and Sabotage: Involved in attacks on critical infrastructure to destabilize adversaries and disrupt operations in hybrid warfare. 4. Influence and Espionage: Targeting foreign governments to manipulate diplomacy and gain political leverage. --- ⚙️ #c2: newyorktimes[.]life 🔑 #!p: 188[.]114[.]96[.]3 172[.]67[.]204[.]39 🗄️ Dropbox: cutt[.]ly/zeJ914md 💧 #SchTask: ExplorerCoreUpdateTaskMachine 🟡 Ref: t.ly/7RWx3 t.ly/A_fgU ♦--TTP's & More information via comments--♦ - - - #IOC #TA #RE #Phishing #Cyberthreat - - - #phishingattack #hacking #threat hunting #threat detection #threat intel #cyberwarfare #threat intelligence #phishing emails #ukraine #russia #detection #infosec #NetworkSecurity #threats #virustotal #network #email security #dfir #email protection #APTs #research #cert #ethical hacking #csirt #intelligence #redteam #threat prevention #ir #hunting #security #ttp #cti #threat analysis #reverse engineering #cyber #osint #information security #threat actors #soc #edr #cybersecurity news #cyber intelligence #CloudSecurity #cybercriminals #security #security research #CyberDefense #cth #secops #cybernews #incident response #persistence #malware analysis #bleeping computer #the hacker news #cyberchef #base64 #obfuscation #powershell #infostealer #threat actor BleepingComputer The Hacker News The Cyber Security Hub™ CERT-UA Dark Reading The Record from Recorded Future News BBC News Reuters HackRead Media

-  No alternative text description for this image
-  No alternative text description for this image
-  No alternative text description for this image
-  No alternative text description for this image
-  No alternative text description for this image

   47 7 Comments

 Idan Tarab

Idan Tarab

Security analyst, MDR @ At-Bay

1mo

🔗 Conclusion: UAC-0099 is a sophisticated and stealthy threat actor, likely tied to nation-state interests and focused on long-term cyber espionage campaigns. The group's agenda is driven by geopolitical objectives, including espionage, economic advantage, and potential sabotage. Whether stealing intellectual property, exfiltrating government secrets, or attacking critical infrastructure, their ultimate goal is to gather intelligence and disrupt their adversaries without raising immediate alarm.

Like

Reply

1 Reaction

 Idan Tarab

Idan Tarab

Security analyst, MDR @ At-Bay

1mo

🚩 Interesting Usages: 1. Copy Ps[.]exe from the System32 directory to the Public folder. 2. Generates dynamic URLs using random digits (between 5 and 15 characters) to form unique strings. 3. Exfiltrates data: hxxps://newyorktlimes[.]life/api/values/refresh[.] 4. Transmits information such as the system's IP, username, and other details. 5. The using of "whoami" command

Like

Reply

1 Reaction

 Idan Tarab

Idan Tarab

Security analyst, MDR @ At-Bay

1mo

🌟 TTPS: Exploitation of Public-Facing Applications (T1190): Spearphishing Link -> (T1566.002) Defacement (T1071) Exfiltration Over C2 Channel (T1041) Command-Line Interface (T1059) PowerShell (T1059.001) Visual Basic (T1059.005) Registry Run Keys / Startup Folder (T1547.00)

[Like](#)

[Reply](#)

1 Reaction

 [Idan Tarab](#)

[Idan Tarab](#)

Security analyst, MDR @ At-Bay

1mo

sha256: 0f05990ef107e49b59bc8d736cdd9535e514efb18e5246fb2b7dc2b7d3305784 [vbs]
a09ff4aad90ba69c97bd3266111206817e0fde7c2870d2d8c0507264d37b837d [lnk]
1a802982b11acb5cd8428d7b18b1882c68d3124c203179dd2ccd047768bafb8e [rar]

[Like](#)

[Reply](#)

1 Reaction

 [Din Serussi](#)

The king is back Great info

[Like](#)

[Reply](#)

[1 Reaction](#) 2 Reactions

 [Shai Gabay](#)



[Like](#)

[Reply](#)

[1 Reaction](#) 2 Reactions

[See more comments](#)

To view or add a comment, [sign in](#)