

#sandworm #uac0125 #apt44 #russia #military #russianukrainianwar #apt... | Idan Tarab

[in linkedin.com/posts/idan-tarab-7a9057200_sandworm-uac0125-apt44-activity-727555552368209921-lg7p](https://www.linkedin.com/posts/idan-tarab-7a9057200_sandworm-uac0125-apt44-activity-727555552368209921-lg7p)



[View profile for Idan Tarab](#)

[Idan Tarab](#)

Security analyst, MDR @ At-Bay

3mo Edited

!!- - - Awareness - - -!! __ Cyber Threat Alert __ 🇷🇺 "Under Siege: Sandworm's Fake Army+ App Threatens Ukraine's Military Operations" 🇺🇦 --- #Sandworm #UAC0125 #APT44 #Russia #military #RussianUkrainianWar #APT #TTPS #Ukraine #Threat #Malware #Cybersecurity #Cyberattacks --- ► Flow: #Phishing > #HTML(#Fake App) > #processInjection > launch #powershell > #Persistence > #DirectoryCreated > #Collection [#infoStealer] > #Exfiltration via #TOR / #C2 💡 - - #Summary- - - 💡 Sandworm is a notorious advanced persistent threat (APT) group linked to the Russian military intelligence agency GRU, specifically Unit 74455. Active since at least 2009, it is known for cyber-espionage and cyber-warfare operations aimed at critical infrastructure, geopolitical adversaries, and organizations in Ukraine, often serving Russian state interests. Sandworm's attacks are characterized by their disruptive and destructive nature. 🔑 - - #Motivation- - - 🔑 - Geopolitical & Military Aims: Aligning with Russian interests, destabilizing adversaries (e.g., Ukraine) and weakening NATO/EU unity. - Disruption & Espionage: Targeting critical infrastructure (e.g., NotPetya), stealing sensitive data, and creating economic chaos. - Political Leverage & Norms: Using cyber-attacks for coercion, influencing foreign policy, and challenging global cyber laws. 🎯---#Geopolitical Drive and #Attribution---🎯 1. Ukraine Focus: Sandworm targets Ukrainian government, critical systems, and energy grids due to the ongoing Russia-Ukraine conflict. 2. NATO & EU

Targets: The group aims to undermine Western stability by attacking NATO and EU members. 3. Election Interference: Linked to broader Russian efforts to influence elections, including the 2016 U.S. Presidential Election --- ✂ - - #c2 / #Network - - ✂
 wvtmsouaa2gt6jmcuxj5hkfrqdss5lhcoqijt5dl7gfrueu3i5mkad[.]onion 🗑 Ref:
<https://lnkd.in/dqPD8i6H> <https://lnkd.in/dUTbq7Nc> <https://lnkd.in/dZMMa2XK> ♦ - -TTP's &
 More informative details via comments- -♦ - - - #IOC #TA #RE #Cyberthreat - - -
 #phishingattack #security #hacking #intelligence #innovation #Informationsecurity
 #technology #threat hunting #threat detection #threat intel #cyberwarfare #threat intelligence
 #idapro #ip #detection #infosec #decoy #NetworkSecurity #encryption #espionage #threats
 #virustotal #network #emailsecurity #dfir #APTs #research #cert #ethicalhacking #csirt
 #intelligence #redteam #threatprevention #ir #x32dbg #hunting #security #ttp #cti
 #threatanalysis #reverseengineering #cyber #osint #informationsecurity #threatactors #soc
 #edr #cybersecuritynews #geopolitics #cyberintelligence #CloudSecurity #cybercriminals
 #security #securityresearch #CyberDefense #cth #secops #cybernews #incidentresponse
 #thehackernews #manipulation #malwareanalysis #cyberchef #obfuscation #powershell
 #threatactor BleepingComputer The Hacker News Cyber Security News® Dark Reading
 Threat Intelligence Lab SecurityWeek The Cyber Security Hub™ Cyber Threat Intelligence®

-  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

 37 10 Comments

 Idan Tarab, graphic

Idan Tarab

Security analyst, MDR @ At-Bay

3mo

🌟 TTPS: Exploitation of Public-Facing Applications (T1190): Spearphishing Link -> (T1566.002) Exfiltration Over C2 Channel (T1041) Command-Line Interface (T1059) PowerShell (T1059.001) Registry Run Keys / Startup Folder (T1547.00) Encrypted Channel: Asymmetric Cryptography (T1573.002) SSH (T1021.004) Web Protocols (T1071.001) Remote File Copy (T1105) File and Directory Discovery (T1083) Application Layer Protocol: Remote Access Software (T1071.003) Indicator Removal on Host: File Deletion (T1070.004) Application Layer Protocol: Remote File Copy (FTP, SFTP, etc.) - T1071.004 -

Like

Reply

1 Reaction

 [Idan Tarab](#), _graphic

 [Idan Tarab](#), _graphic

[Idan Tarab](#)

Security analyst, MDR @ At-Bay

3mo

🌟 - - - Key Highlights in Context- - - 🌟 - Tor-based Hidden Services: Establishing a hidden service using Tor, which is often a key tactic for maintaining anonymity and avoiding detection in cybercrime operations. - SSH Setup and Security: Generating SSH keys and configuring the SSH service to open a backdoor (on a custom port) for remote access. - Data Exfiltration: Using curl to send system information over a Tor network to a secure, hidden address. - Persistence and Evasion: The script ensures persistence by starting essential services and hides activities by using encrypted tunnels and remote data exfiltration. - File Deletion for Evasion: The rm commands are used to remove sensitive files and trace evidence (such as SSH keys, system info, and the Tor package) after execution, ensuring that the attacker leaves no forensic footprint and minimizes the risk of detection or recovery of critical data.

[Like](#)

[Reply](#)

[1 Reaction](#) 2 Reactions

 [Eyal Haiman](#), _graphic

[Eyal Haiman](#)

CTI Analyst at Clearsky Cyber Security | Information Science Student at Bar Ilan University

3mo

Nice findings, This Attack appears in a blog published by the CERT of Ukraine and linked to TA named UAC-0125 which is probably associated with APT44 aka Sandworm
<https://cert.gov.ua/article/6281701>

[Like](#)

[Reply](#)

1 Reaction

 [Gal Jacobson](#) _graphic

[Gal Jacobson](#) 

Full-Stack Engineer @ Houzz 

3mo

Nice findings! Best researcher here! 🙌

[Like](#)

[Reply](#)

1 Reaction

 [Emil Pinus, graphic](#)

[Emil Pinus](#)

Security administrator | Penetration testing | Incident Response

3mo

If you need Ukrainian translation let me know 😁

[Like](#)

[Reply](#)

1 Reaction

 [Ariel Davidpur 🇮🇱, graphic](#)

[Like](#)

[Reply](#)

[1 Reaction](#) 2 Reactions

 [Elad damari, graphic](#)

[Like](#)

[Reply](#)

[1 Reaction](#) 2 Reactions

 [Din Serussi, graphic](#)

[Like](#)

[Reply](#)

[1 Reaction](#) 2 Reactions

[See more comments](#)

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