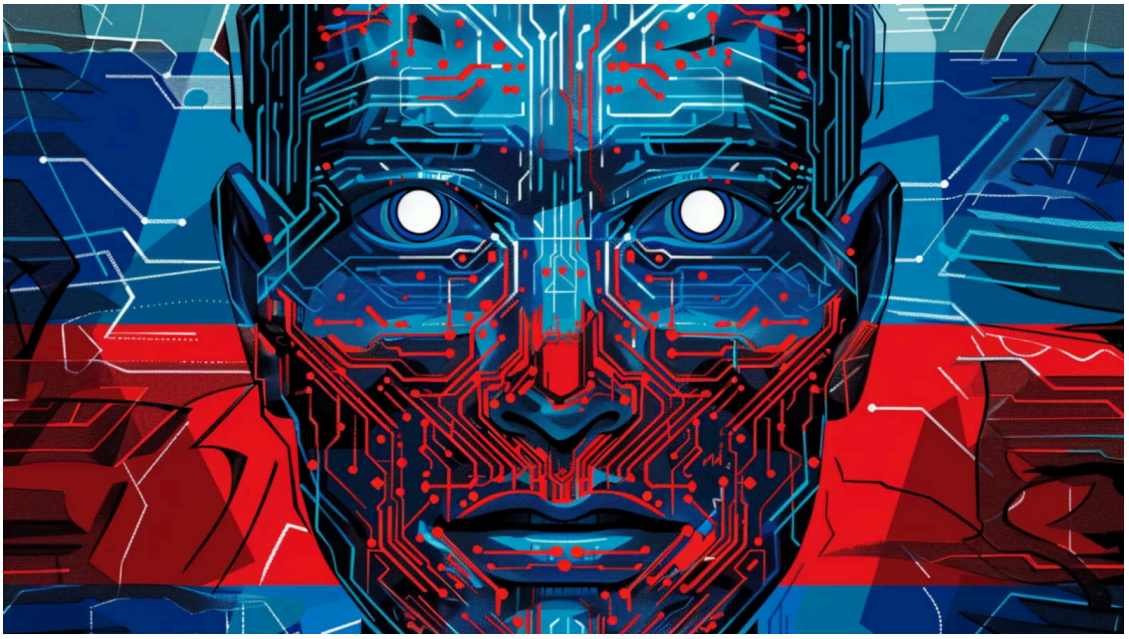
Russian Sandworm hackers targeted 20 critical orgs in Ukraine

By Bill Toulas

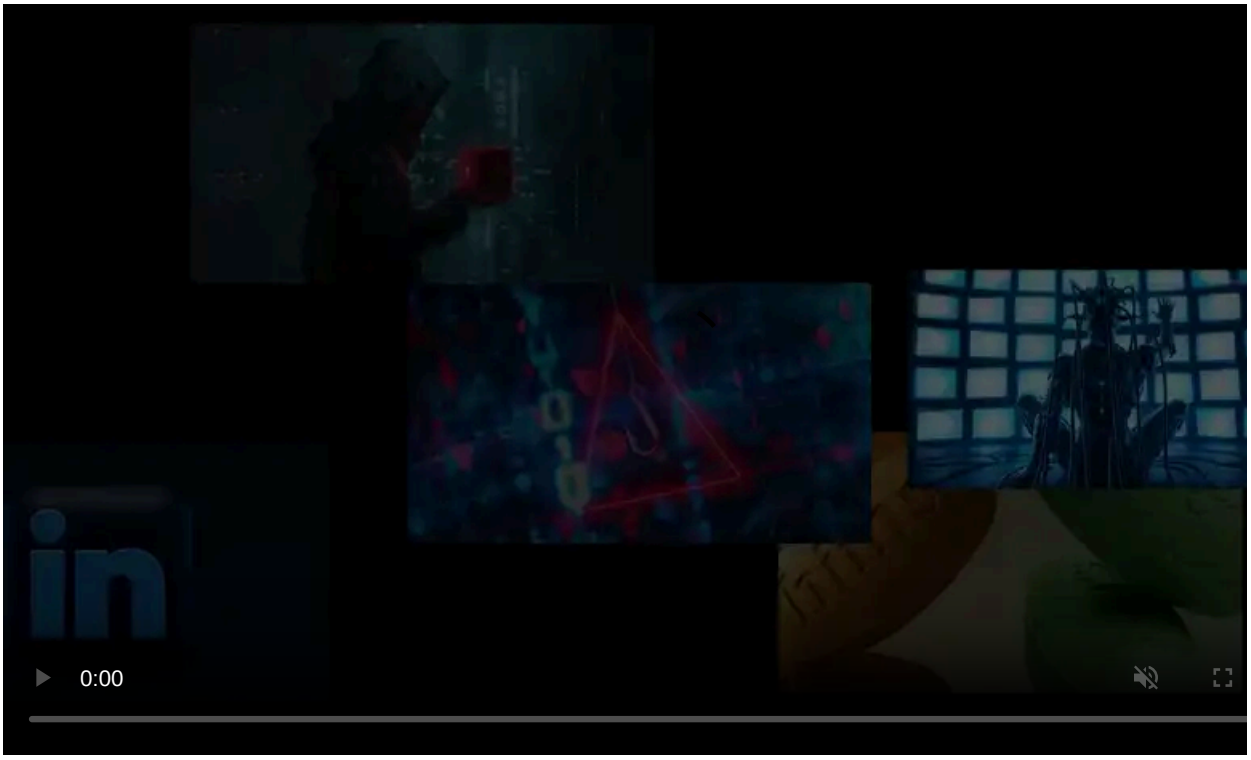
Published: 2024-04-22 · Archived: 2026-04-05 18:06:42 UTC

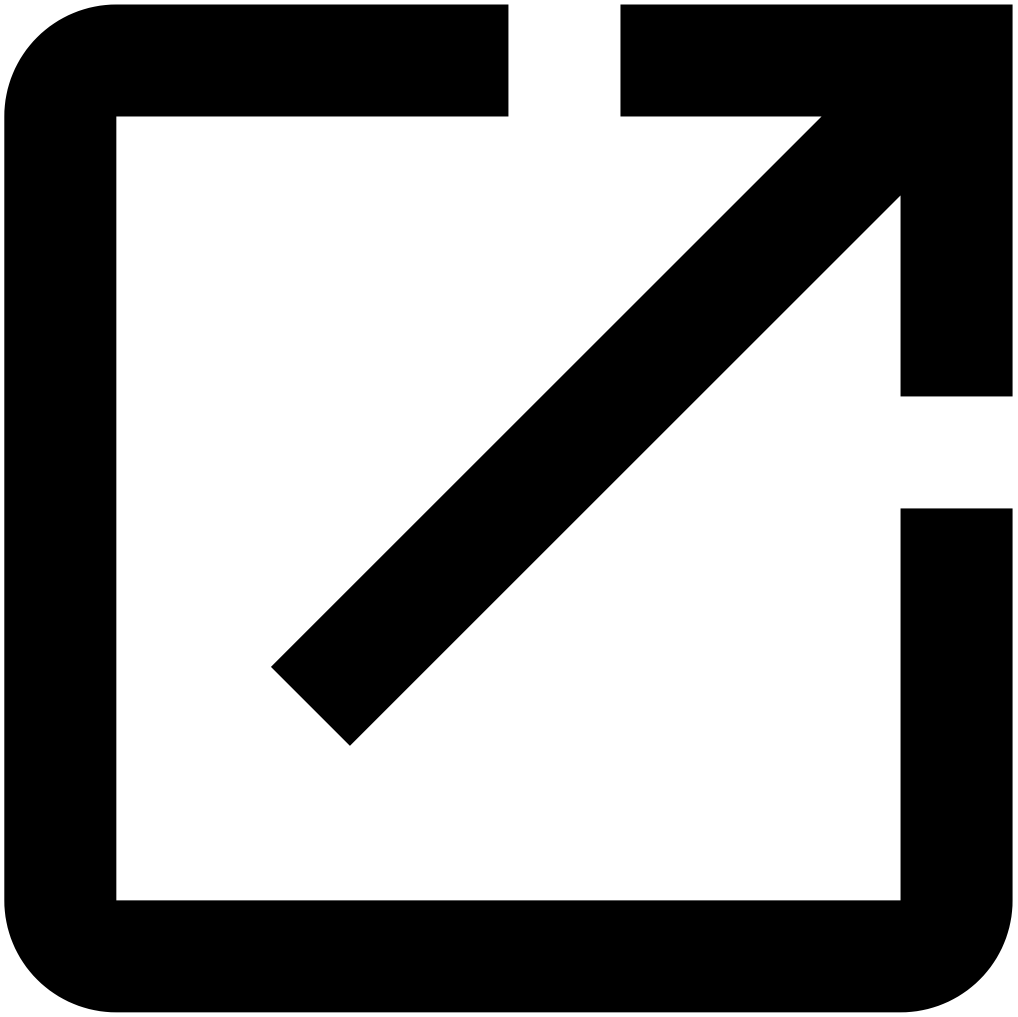


Russian hacker group Sandworm aimed to disrupt operations at around 20 critical infrastructure facilities in Ukraine, according to a report from the Ukrainian Computer Emergency Response Team (CERT-UA).

Also known as BlackEnergy, Seashell Blizzard, Voodoo Bear, and APT44, the hackers are believed to be associated with Russia's Main Directorate of the General Staff of the Armed Forces (the GRU), carrying out cyberespionage and destructive attacks on various targets.

CERT-UA reports that in March 2024, APT44 conducted operations to disrupt information and communication systems at energy, water, and heating suppliers in 10 regions of Ukraine.


0:00



The attacks occurred in March and in some cases the hackers were able to infiltrate the targeted network by poisoning the supply chain to deliver compromised or vulnerable software, or through the software provider's ability to access organization's systems for maintenance and technical support.

Sandworm also combined previously documented malware with new malicious tools (BIASBOAT and LOADGRIP for Linux) to obtain access and move laterally on the network.

CERT-UA experts have confirmed the compromise of at least three "supply chains," as a result of which the circumstances of the initial unauthorized access either correlate with the installation of software containing backdoors and vulnerabilities or are caused by the regular technical ability of the supplier employees to access the organizations' ICS for maintenance and technical support. – CERT-UA (machine translated).

The Ukrainian agency notes that Sandworm's breaches were made easier by the targets' poor cybersecurity practices (e.g. lack of network segmentation and insufficient defenses at the software supplier level).

From March 7 to March 15, 2024, CERT-UA engaged in extensive counter-cyberattack operations, which included informing affected enterprises, removing malware, and enhancing security measures.

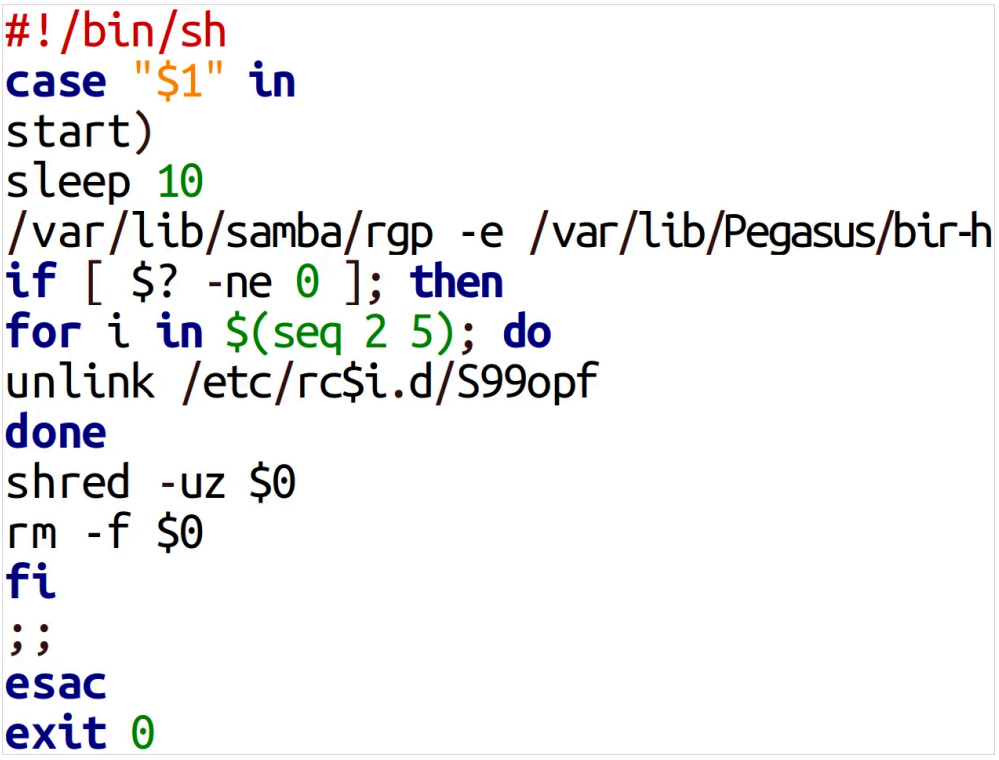
Based on the findings from investigating the logs retrieved from the compromised entities, Sandworm relied on the following malware for its attacks on Ukraine's utility suppliers:

- **QUEUESEED/IcyWell/Kapeka**: C++ backdoor for Windows that collects basic system information and executes commands from a remote server. It handles file operations, command execution, and configuration updates and can delete itself. Communications are secured via HTTPS, and data is encrypted using RSA and AES. It stores its data and maintains persistence on infected systems by encrypting its configuration in the Windows registry and setting up tasks or registry entries for automatic execution.

```
<?xml version="1.0" encoding="UTF-16"?>
<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">
  <RegistrationInfo>
    <Date>XXXX-XX-09T13:23:44</Date>
    <Author>SERVER\Администратор</Author>
    <URI>\Microsoft\Windows\OneDrive</URI>
  </RegistrationInfo>
  <Triggers>
    <BootTrigger>
      <StartBoundary>XXXX-XX-09T13:23:00</StartBoundary>
      <Enabled>true</Enabled>
    </BootTrigger>
  </Triggers>
  <Settings>
    <MultipleInstancesPolicy>IgnoreNew</MultipleInstancesPolicy>
    <DisallowStartIfOnBatteries>true</DisallowStartIfOnBatteries>
    <StopIfGoingOnBatteries>true</StopIfGoingOnBatteries>
    <AllowHardTerminate>true</AllowHardTerminate>
    <StartWhenAvailable>false</StartWhenAvailable>
    <RunOnlyIfNetworkAvailable>false</RunOnlyIfNetworkAvailable>
    <IdleSettings>
      <Duration>PT10M</Duration>
      <WaitTimeout>PT1H</WaitTimeout>
      <StopOnIdleEnd>true</StopOnIdleEnd>
      <RestartOnIdle>false</RestartOnIdle>
    </IdleSettings>
    <AllowStartOnDemand>true</AllowStartOnDemand>
    <Enabled>true</Enabled>
    <Hidden>false</Hidden>
    <RunOnlyIfIdle>false</RunOnlyIfIdle>
    <WakeToRun>false</WakeToRun>
    <ExecutionTimeLimit>PT72H</ExecutionTimeLimit>
    <Priority>7</Priority>
  </Settings>
  <Actions Context="Author">
    <Exec>
      <Command>cmd</Command>
      <Arguments>/c start "" C:\Windows\system32\rundll32.exe "C:\ProgramData\Microsoft\hasuti.wll",#1</Arguments>
    </Exec>
  </Actions>
  <Principals>
    <Principal id="Author">
      <UserId>S-1-5-18</UserId>
      <RunLevel>LeastPrivilege</RunLevel>
    </Principal>
  </Principals>
</Task>
```

QUEUESEED scheduled execution *(CERT-UA)*

- **BIASBOAT (new)**: a Linux variant of QUEUESEED that emerged recently. It is disguised as an encrypted file server and operates alongside LOADGRIP.
- **LOADGRIP (new)**: also a Linux variant of QUEUESEED developed in C, used to inject a payload into processes using the ptrace API. The payload is usually encrypted, and the decryption key is derived from a constant and a machine-specific ID.



```
#!/bin/sh
case "$1" in
start)
sleep 10
/var/lib/samba/rgp -e /var/lib/Pegasus/bir-h
if [ $? -ne 0 ]; then
for i in $(seq 2 5); do
unlink /etc/rc$i.d/S99opf
done
shred -uz $0
rm -f $0
fi
;;
esac
exit 0
```

Bash script that loads BIASBOAT and LOADGRIP *(CERT-UA)*

- **GOSSIPFLOW**: Go-based malware use on Windows to set up tunneling using the Yamux multiplexer library; it provides SOCKS5 proxy functionality to help exfiltrate data and secure communication with the command and control server.

Additional malicious tools CERT-UA discovered during the investigation are from the open source space and include the Weevly webshell, the Regeorg.Neo, Pitvotnacci, and Chisel tunnelers, LibProcessHider, JuicyPotatoNG, and RottenPotatoNG.

The threat actors used these tools to maintain persistence, hide malicious processes, and elevate their privileges on compromised systems.

The Ukrainian agency belives that the purpose of these attacks was to increase the effect of Russian missile strikes on the targeted infrastructure facilities.

Last week, Mandiant exposed Sandworm's connection to three hacktivist-branded Telegram groups that have previously claimed attacks on critical infrastructure in Europe and the U.S.

CERT-UA's report provides a long list of indicators of compromise that includes files, hosts, and network details.
