Dropping Elephant APT Group Targets Turkish Defense Industry With New Campaign and Capabilities: LOLBAS, VLC Player, and Encrypted Shellcode - Arctic Wolf

By Arctic Wolf

Published: 2025-07-23 · Archived: 2026-04-05 19:13:30 UTC

Executive Summary

The Arctic Wolf® Labs team has identified a new campaign by cyber-espionage group Dropping Elephant targeting Turkish defense contractors, specifically a manufacturer of precision-guided missile systems. The campaign employs a five-stage execution chain delivered via malicious LNK files disguised as conference invitations sent to targets interested in learning more about unmanned vehicle systems.

The attack leverages legitimate binaries (VLC Media Player and Microsoft Task Scheduler) for defense evasion through DLL side-loading techniques. This represents a significant evolution of this threat actor's capabilities, transitioning from the x64 DLL variants observed in November 2024, to the current x86 PE executables with enhanced command structures.

The campaign's timing appears to coincide with heightened Türkiye*-Pakistan defense cooperation and recent India-Pakistan military tensions, suggesting the targeting may be geopolitically motivated. Infrastructure analysis reveals deliberate operational security measures, including the impersonation of legitimate websites for command-and-control (C2) infrastructure.

The campaign demonstrates how threat actors combine social engineering with precisely crafted lures to gather strategic intelligence from their targets. In this blog, we'll break down the attack step-by-step to show how this is achieved, as well as discussing proactive steps organizations can take to defend themselves against this type of attack.

** The Republic of Turkey changed its official name to The Republic of Türkiye on 26 May 2022.*

Key Intelligence Findings:

Threat Attribution and Evolution

- **Threat Actor**: Dropping Elephant (aka Patchwork or Quilted Tiger).
- **Technical Evolution**: Diversification from x64 DLL to x86 PE architecture, with reduced library dependencies.
- **Campaign Scope**: Multi-country targeting in prior campaigns, with Türkiye-specific operational focus in this specific campaign.

Attack Methodology

- **Initial Access**: Spear-phishing, with conference-themed LNK files.
- **Execution**: Five-component PowerShell-based download chain from malicious domain expouav[.]org.
- **Defense Evasion**: VLC DLL side-loading, file extension manipulation, scheduled task persistence.
- **Command Structure**: Enhanced C2 protocol, using C-standard library's strtok() for parsing and CreateThread execution.

Target Profile

- **Primary Target**: A Turkish precision-guided systems manufacturer.
- **Sector**: Defense industrial base, specifically missile and rocket systems.
- **Geopolitical Context**: Türkiye's military cooperation with Pakistan amid regional tensions.

Infrastructure Assessment

- **Delivery**: expouav[.]org (created 2025-06-25). This malicious domain mimics the legitimate conference website waset.org.
- **C2**: roseserve[.]org (registered 2025-06-23). This malicious site impersonates the Pardus project, a Linux distribution project developed with support from the government of Türkiye.
- **Hosting**: DEDIPATH-LLC/STARK-INDUSTRIES (U.S./GB hosting for Türkiye-focused operations).
- **PTR records** points to tk99671283030[.]avanetco[.]com (Created on 2025-06-27 over 2.56.127[.]187). Avanetco is a virtual private server (VPS) reseller headquartered in Iran.
- **Operational timeline**: Infrastructure preparation began in June 2025 and has been in active operation since July 2025.

Introducing Dropping Elephant

Dropping Elephant (also known as Patchwork or Quilted Tiger) is a relatively new advanced persistent threat (APT) group suspected to be of Indian origin. First identified in December 2015, the group has been observed using social engineering techniques, including spear-phishing and watering hole attacks, which involve compromising or impersonating legitimate websites known to be frequented by the groups' targets.

It has also been known to exploit malware distribution vulnerabilities, and has used fake downloadable apps to drop malware such as VajraSpy, an Android-targeted remote access trojan (RAT), and BADNEWS RAT.

Based on campaign analysis, Dropping Elephant's primary motivation is most likely espionage. Initially targeting South and Southeast Asia, the group has since expanded its sights to include victims worldwide, including Europe and the United States. It uses a range of custom tooling and techniques for intelligence-gathering, particularly focusing on individuals, organizations and sectors with diplomatic and economic ties to China.

The industry sectors most highly targeted by this APT group to date include Defense, Energy, Financial, Government, IT, Aviation, NGOs, Think Tanks, and Pharmaceutical.

Attack Chain Breakdown

1. The Conference Invitation

The threat actor kicks off the attack by delivering a malicious LNK file to the intended targets:

```
Unmanned_Vehicle_Systems_Conference_2025_In_Istanbul.lnk
```

– an opportunity for defense industry professionals working on drone and missile technologies to attend a conference. The technical details of this file are shown in the table below.

Field	Value
Name	Unmanned_Vehicle_Systems_Conference_2025_In_Istanbul.lnk
SHA-256	341f27419becc456b52d6fbe2d223e8598065ac596fa8dec23cc722726a28f62
File Type/ Signature	.lnk file
Size	5.11KB

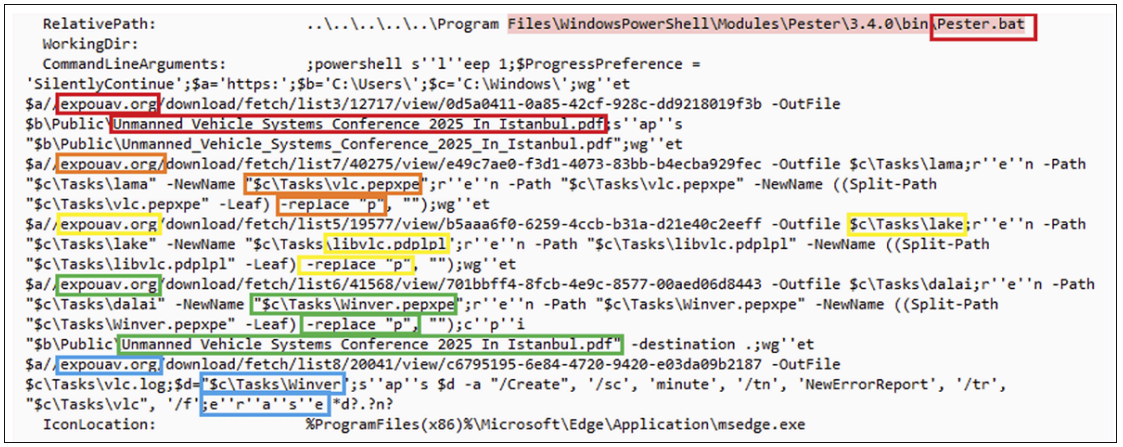


Figure 1: Unmanned_Vehicle_Systems_Conference_2025_In_Istanbul.lnk structure.

Upon execution, the lnk file invokes PowerShell, which in turn reaches out via Wget to a Cloudflare-protected hosting site – expouav[.]org – and retrieves several files.

Pester.bat is a Windows batch file that is part of the PowerShell Pester testing framework. It's classified as a Living Off the Land Binary and Script (LOLBAS) due to its potential for abuse by threat actors. In this campaign, extra quotation marks are inserted into the commands by the threat actor to evade common string-matching detections for potentially suspicious commands.

As part of the process of establishing persistence, a scheduled task is created which abuses VLC, the popular legitimate media player software, to side-load malicious DLL files. VLC Media Player's popularity springs a trap on the unwitting targets, playing on the user's trust in familiar software to help advance the threat actor's attack chain.

2. Silent Execution

The PowerShell code is executed in a manner which enables it to bypass restrictions (should they be enabled) as well as hide any progress indicators of its functionality from the user, to remain stealthy during execution.

```
"sleep 1;$ProgressPreference = 'SilentlyContinue'"
```

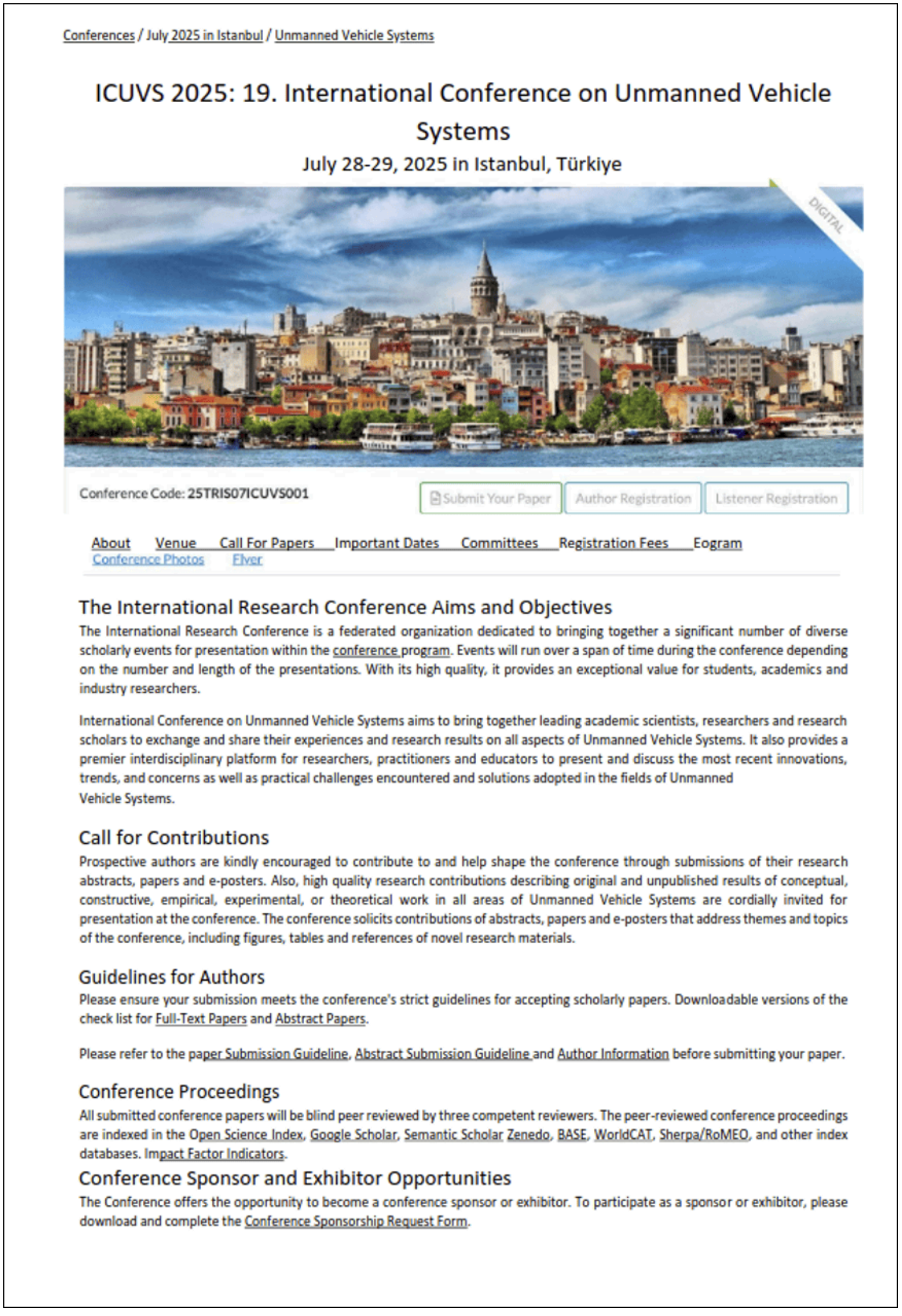
3. Downloads Multiple Files from expouav[.]org

The expouav[.]org domain referenced within the LNK file was registered on 06/25/2025. It hosts a PDF lure mimicking https://waset.org/unmanned-vehicle-systems-conference-in-july-2025-in-istanbul (a legitimate website). The real conference name is "*ICUVS 2025: 19. International Conference on Unmanned Vehicle Systems*", and it takes place on July 28th and 29th, 2025 in Istanbul, Türkiye.

Figure 2: Legitimate waset.org website with the same conference information used by the fake PDF-based replica.

Assets used in the PDF lure were copied from the official website. The copy is nearly identical and even includes the original conference code.

The PDF document serves as a visual decoy, designed to distract the user while the rest of the execution chain runs silently in the background.



Conferences / July 2025 in Istanbul / Unmanned Vehicle Systems

ICUVS 2025: 19. International Conference on Unmanned Vehicle Systems

July 28-29, 2025 in Istanbul, Türkiye

DIGITAL

Conference Code: 25TRIS07ICUVS001

Submit Your Paper | Author Registration | Listener Registration

About Venue Call For Papers Important Dates Committees Registration Fees Eogram
Conference Photos Flyer

The International Research Conference Aims and Objectives

The International Research Conference is a federated organization dedicated to bringing together a significant number of diverse scholarly events for presentation within the conference program. Events will run over a span of time during the conference depending on the number and length of the presentations. With its high quality, it provides an exceptional value for students, academics and industry researchers.

International Conference on Unmanned Vehicle Systems aims to bring together leading academic scientists, researchers and research scholars to exchange and share their experiences and research results on all aspects of Unmanned Vehicle Systems. It also provides a premier interdisciplinary platform for researchers, practitioners and educators to present and discuss the most recent innovations, trends, and concerns as well as practical challenges encountered and solutions adopted in the fields of Unmanned Vehicle Systems.

Call for Contributions

Prospective authors are kindly encouraged to contribute to and help shape the conference through submissions of their research abstracts, papers and e-posters. Also, high quality research contributions describing original and unpublished results of conceptual, constructive, empirical, experimental, or theoretical work in all areas of Unmanned Vehicle Systems are cordially invited for presentation at the conference. The conference solicits contributions of abstracts, papers and e-posters that address themes and topics of the conference, including figures, tables and references of novel research materials.

Guidelines for Authors

Please ensure your submission meets the conference's strict guidelines for accepting scholarly papers. Downloadable versions of the check list for Full-Text Papers and Abstract Papers.

Please refer to the paper Submission Guideline, Abstract Submission Guideline and Author Information before submitting your paper.

Conference Proceedings

All submitted conference papers will be blind peer reviewed by three competent reviewers. The peer-reviewed conference proceedings are indexed in the Open Science Index, Google Scholar, Semantic Scholar Zenedo, BASE, WorldCAT, Sherpa/RoMEO, and other index databases. Impact Factor Indicators.

Conference Sponsor and Exhibitor Opportunities

The Conference offers the opportunity to become a conference sponsor or exhibitor. To participate as a sponsor or exhibitor, please download and complete the Conference Sponsorship Request Form.

Figure 3: Unmanned_Vehicle_Systems_Conference_2025_In_Istanbul.pdf PDF lure content.

This targeting occurs as Türkiye commands 65% of the global UAV export market and develops critical hypersonic missile capabilities, while simultaneously strengthening defense ties with Pakistan during a period of heightened India-Pakistan tensions.

It specifically reflects the strategic value of technologies and intelligence services to understand Türkiye and possibly NATO capabilities. Access to NATO-standard defense technologies and interoperability protocols provides insights into Western military capabilities and strategic planning.

4. File Evasion Technique

The simultaneous download of five distinct files represents a carefully orchestrated operation. Each component serves a specific purpose.

Files are dropped to the user's Tasks folder, with additional characters in the extension to bypass detection by security systems. Once the file is saved to disk, the command automatically removes the extra characters, leaving the file with an executable extension, ready to run.

Detailed Technical Analysis

The first stage of the execution of Dropping Elephant's attack chain is a .LNK file that contains PowerShell code. This script loads five files sequentially:

1. Visual Lure for Distraction

```
File: Unmanned_Vehicle_Systems_Conference_2025_In_Istanbul.pdf
SHA-256: 588021b5553838fae5498de40172d045b5168c8e608b8929a7309fd08abfaa93
```

2. Legitimate VLC Video Player File

VLC Video Player is a free and open-source cross-platform multimedia player from VideoLAN, a non-profit organization. The player itself is legitimate, but (as with many digital tools) can be abused by cybercriminals.

Original downloaded name: "lama" → renamed to C:\Windows\Tasks\vlc.exe

```
SHA-256: 4cc729b554326ccc62205d46b95353dcb34cadf095b904e941814e902e0925b2
```

```
Compile date:           1996-06-10 14:30:50
VersionInfo:
  CompanyName:          VideoLAN
  ProductName:          VLC media player
  ProductVersion:       3,0,21,0
  InternalName:         vlc
  OriginalFilename:     vlc.exe
  FileVersion:          3.0.21
  FileDescription:      VLC media player
  LegalCopyright:       Copyright © 1996-2024 VideoLAN and VLC Authors
  LegalTrademarks:      VLC media player, VideoLAN and x264 are registered trademarks from VideoLAN
Certificate:
  Issuer:               DigiCert Trusted G4 Code Signing RSA4096 SHA384 2021 CA1 (DigiCert, Inc. / ??? / US)
  Subject:              VideoLAN (VideoLAN / ??? / FR)
  Validity:             from 2024-06-07 to 2027-06-08
  SerialNumber:         09d08ebda06be07c815ea7af25ef6875
  HashAlgorithm:        SHA1
  CryptAlgorithm:       RSA
Exports:
  Module name:          vlc.exe
  Exports date:         2024-06-08 21:21:15
```

Figure 4: Legitimate VLC.exe file information.

3. Malicious DLL Library

Original file name: "lake" → renamed to libvlc.dll
Purpose: This library is responsible for running and decoding the shellcode.

```
SHA-256: 2cd2a4f1fc7e4b621b29d41e42789c1365e5689b4e3e8686b80f80268e2c0d8d
```

Project file name: newdll.dll
Compilation date: 2025-06-26 08:54:47

4. Legitimate Microsoft Task Scheduler

Original downloaded name: “dalai” → renamed to C:\Windows\Tasks\Winver.exe
Description: Legitimate Microsoft Task Scheduler file

```
SHA-256: 013c013e0efd13c9380fad58418b7aca8356e591a5cceffdb910f7d8b0ad28ef
```

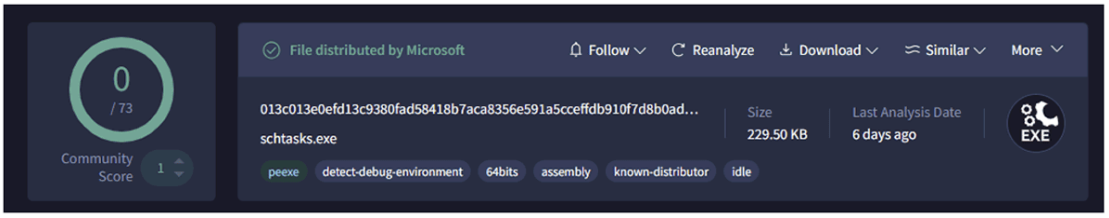


Figure 5: Legitimate schtask.exe (Microsoft Task Scheduler).

5. Encrypted Shellcode

File: vlc.log
Location: C:\Windows\Tasks\vlc.log

```
SHA-256: 89ec9f19958a442e9e3dd5c96562c61229132f3acb539a6b919c15830f403553
```

```
000000000:  d71094ca3e6b45c0fed07e69a6c524bd8a5c7764613f4ac9128dc5e87834ed42d7f5d4ae332e53f0ce936d9342c3005ad9779ff31f8e24c7
000000070:  7f6503b561c54aaa05bf78ebad186ff194a24c9244cbb0990b9c88ef46a92e3841b53d5559ac8b4d512abc278523f777743768bf96ad9512
0000000e0:  8bee74c0959cf133a793fc266b1d1c659b4e9ac1f4cfffdaf1e3be920bcb11f08e4d674793b1b1c1fe424afd8e1b5c6ce861d39121e1a28e
000000150:  004416d1fae4881ae048ba9c39cf56e6af092f8aaf844b98fb3456f7f1076f9e46b088581ce99dd5893778049168d6efd7fd83ccaf4d3454
0000001c0:  a561771c24717cbced05510a8c6f271dd9a1b6bcd2d9fc61a0437d18dc027ba7648d193d5c98931da113253f97acfb7b07267d2a162195c1
000000230:  792dc2c8549db0e6001d434019c41caeaac37745e959959f98c4045931b691d7af0a23d504f2540d56930d99c1cd854ee2027e324bddb8d7
0000002a0:  173e4dc9ad1cccd05d537f0f42d9a84eb714afb6e1594a872d39c037abb47c96b2aa2954b9c8b6c536ae0eb9f80a229b8dc042403e62e5d6
000000310:  b86048156ae54102288c70e976f246f58fb1a1beda65098e3d38d6a601a778cc4a5f256ac65bb5272ac7ed8a55ae2b5e6c11191196279a4c
000000380:  1ae68339df64ce60b71a9c7eae79871cf39033b801639fe56afb2bbd3d216947d095e402723e2f0ce8d14d4d53db5191cfe6256951710308
0000003f0:  505e34537a5a2899307cfc0be367b785ba5ddfd9dd9e5b04f0a2616e9c73517e01e98e91bf422fe5df9ab8d12389f1568d1d3703757f1383
000000460:  083e1df12efa750f8bbb3b31ac7505584724773417cd34c442c9387bd25698d3355349cbe4f435560baea0611981c2fd8b58e49493ae42b7
0000004d0:  20f1097735733dce19ca777d69d62d40b0d08cd0f0ed71cb085c51c5e7d0bc49d45285ba58690998f0cf89aaac7080ee26612ae7d4350eef
000000540:  0d8c5c152a5065d05c0fa05970f5b406fa4562c6348d16dd2616d6c4ef21d7aeb2568bd71173622436e496e9114b9cd8c1ecf2cef3121ace
0000005b0:  c5a666cffd49f74f1f8108cefae392f8fb09138282d7b5e5fac6b63f9be2b452fc5a37ec808e8495363a37ae5374e3991639579ce789d730
000000620:  bd6ae673027f25afc9f43601ae47156d41293c34dd1bd14748ac771e2444670fee840963e4f380806b8f433a5410aa449756ee1f2d564de8
000000690:  040f0a32d9d0fa2d93fccf020dfe72031f3a35c01facf4f49c5ded8adcbe248dd22cd121d80761c4838bbe35aaefeee0a224390469425fd9
000000700:  1ce3b93b79a989c29feecf11cd3deefbdb76c03eb27ecbc3466d757ed07b6bdc3d6268a44816ce922d021a13a860d425221c408b1bfd8125
000000770:  3cc3164413f2bf6250bf87dbeda51d09d4ba96b3158939441aed34ff024e6db83832a6debefcbb74702e945682c8ec80073630223f62b097
0000007e0:  bbb60c9fd307569c91b641635205d0ab0fcd273b4d4ec2b29aa4b4cfbdf8029e978483eebac8c2b97973c25e3b1f7007105ae52dec8835a7
000000850:  2dbda05b3e912c7185b3b120a6bd58e48785b7377df6bb77e4ec3372fdc835eecacf7acd9032ef591d8be4cc739d29907f0ff9ce018b3220
```

Figure 6: Encrypted shellcode.

Execution Process

The following command creates a scheduled task using PowerShell and a pre-loaded legitimate Schtasks.exe Microsoft file:

PowerShell scheduled task:

```
saps "C:\Windows\Tasks\Winver" -a "/Create", '/sc', 'minute', '/tn', 'NewErrorReport', '/tr', "C:\Windows\Tasl
```

This scheduled task executes a legitimate VLC Player file which runs a DLL. The DLL acts as a shellcode loader that decrypts the ciphertext shellcode stored in vlc.log. The payload is launched in the VLC Player memory address space.

Shellcode Decryption

Decryption key: “76bhu93FGRjZX5hj876bhu93FGRjX5”

```
v15 = 0;
v16 = 26128;
v17 = 32;
qmemcpy(v18, "76bhu93FGRjZX5hjg76bhue93FGRjZX5", sizeof(v18));
phKey = 0;
if ( CryptImportKey(hProv, pbData, 0x2Cu, 0, 0, &phKey) )
{
  if ( CryptSetKeyParam(phKey, 1u, v20, 0) )
  {
    v29 = (BYTE *)malloc(Size);
    if ( v29 )
    {
      memcpy(v29, Src, Size);
      pdwDataLen = Size;
      if ( CryptDecrypt(phKey, 0, 1, 0, v29, &pdwDataLen) )
      {
        v11 = 0;
        v10 = pdwDataLen;
        hModule = GetModuleHandleW(L"ntdll.dll");
        if ( hModule )
        {
          NtAllocateVirtualMemory = GetProcAddress(hModule, "NtAllocateVirtualMemory");
          NtProtectVirtualMemory = GetProcAddress(hModule, "NtProtectVirtualMemory");
          NtCreateThreadEx = GetProcAddress(hModule, "NtCreateThreadEx");
          if ( NtAllocateVirtualMemory && NtProtectVirtualMemory && NtCreateThreadEx )
          {
            v5 = (int (__stdcall *)(_DWORD, _DWORD, _DWORD, _DWORD, _DWORD, _DWORD))NtAllocateVirtualMemory;
            CurrentProcess = GetCurrentProcess();
            if ( v5(CurrentProcess, &v11, 0, &v10, 12288, 4) )
            {
              return -3;
```

Figure 7: Shellcode decryption code.

Once decrypted, the shellcode becomes the final payload:

Field	Value
Name	N/A
SHA-256	8b6acc087e403b913254dd7d99f09136dc54fa45cf3029a8566151120d34d1c2
File Type/ Signature	x86 PE
Size	139.37 KB (142,712 bytes)
Declared Timestamp	Fri Jul 26 09:12:19 2024

```
[x]
Count of sections              5 | Machine                 Intel386
Symbol table  00000000[00000000] |       Fri Jul 26 11:12:19 2024
Size of optional header     00E0 | Magic optional header      010B
Linker version             14.38 | OS version                 6.00
Image version               0.00 | Subsystem version          6.00
Entry point            00018E36 | Size of code           00019A00
Size of init data      00008800 | Size of uninit data    00000000
Size of image          00026000 | Size of header         00000400
Base of code           00001000 | Base of data           0001B000
Image base             00400000 | Subsystem                Console
Section alignment      00001000 | File alignment         00000200
Stack          00100000/00001000 | Heap           00100000/00001000
Checksum               00000000 | Number of dirs                16
Overlay        00022000[00000D78/3448/3,367 Kb]
```

Figure 8: Decrypted shellcode header.

Digital Reconnaissance

Once executed in the system, the malware performs a series of actions that facilitate profiling of the infected device:

- Creates mutex ghjghkj to prevent multiple instances from running at once.
- Gathers victim's computer name via GetComputerNameW.
- Collects username via GetUserNameW.
- Retrieves system firmware information.
- Checks processor features and capabilities for sandboxing evasion.
- Performs system time and performance counter queries.
- Takes screenshots of the screen and saves them as JPGs for C2 upload. This technique can be particularly useful when the targeted users work in a remote environment, where the sought-after data is stored not on the infected endpoint, but on a remote server. Screen-capturing is therefore vital to capture sensitive data, such as diagrams or classified projects stored on a clean remote server.

```
if (CreateStreamOnHGlobal(nullptr, 1, &var_88) >= 0)
{
    HDC eax_7 = GetDC(nullptr);
    int32_t cy = GetSystemMetrics(SM_CYSCREEN);
    int32_t cx = GetSystemMetrics(SM_CXSCREEN);
    HDC eax_8 = CreateCompatibleDC(eax_7);
    HBITMAP eax_9 = CreateCompatibleBitmap(eax_7, cx, cy);
    SelectObject(eax_8, eax_9);
    BitBlt(eax_8, 0, 0, cx, cy, eax_7, 0, 0, 0x40cc0020);
    GpBitmap* var_80 = nullptr;
    int96_t var_44_1 = (int96_t){0};
    var_44_1 = &Gdiplus::Bitmap::`vftable'{for `Gdiplus::Image'};
    *(uint32_t*)((char*)var_44_1)[8] =
        GdipCreateBitmapFromHBITMAP(eax_9, nullptr, &var_80);
    *(uint32_t*)((char*)var_44_1)[4] = var_80;
    var_8_1 = 1;
    uint32_t numEncoders = 0;
    uint32_t size = 0;
    GdipGetImageEncodersSize(&numEncoders, &size);
    uint32_t _Size = size;
```

Figure 9: Screenshot-capture command.

Network Communication

To assess outside network connectivity, several external sites are queried.

External Services Contact:

- **com/raw** is used to determine external IP address
- **iplocation.net/?cmd=ip-country** is used for geolocation
- **co** is used for additional IP information
- **Mozilla/5.0** user-agent is used to blend with legitimate traffic

Command and Control:

C2 Server: roseserve[.]org

Figure 10: The threat actor's C2 server.

Reporting to C2 is based on the /post action, with structured parameters.

Figure 11: /post action via YcKOjLMxiwCZfSS//comrCVPEffFiPvF.php to C2.

Dropping Elephants' RAT: Version Comparison Analysis

When comparing code between older versions of Dropping Elephants' RAT from November 2024 and newer versions, we observed several key differences:

Architecture Change

- **New version**: x86 EXE executable
- **Old versions**: x64 DLL

Referential Samples:

```
November 2024 version: 01a635a11a140aef906efe9db22fb66b0d6510e1e702870c4c728099fd5ab455
```

```
Version targeting Türkiye: 8b6acc087e403b913254dd7d99f09136dc54fa45cf3029a8566151120d34d1c2
```

Code Optimization

Another interesting difference is that the threat group has begun using fewer library functions. For example, C2 command parsing in the new version is done with raw code, while the old version used the "C function" – memcmp, a function in C and C++ used to compare the contents of two memory blocks.

Command Processing

After receiving C2 commands, the code next compares them with a command list. Then, using CreateThread, it transfers execution to the appropriate code thread. Any string received by the server is split into tokens using the strtok function with

'$' delimiters.

```
415  p_String = (char *)&String;
416  if ( a8 > 0xF )
417    p_String = String;
418  v90 = strtok(p_String, "$");
419  if ( !v90 )
420  {
421    v171 = &a45;
422    if ( a50 > 0xF )
423      v171 = (_DWORD **)a45;
```

Figure 12: Splitting into tokens with '$' delimiter.

Network Infrastructure Analysis

roseserve[.]org serves as the malicious C2 for the attack we observed on Türkiye.

Infrastructure Details:

- **PTR DNS record**: tk99671283030.avanetco.com (avanetco.com is a legitimate commercial web hosting provider headquartered in Iran).
- **Title response**: "Pardus – TÜBİTAK"
- **Redirect**: Clicking "Turkish language" takes you to https://pardus.org.tr/en/ (a legitimate website with a very similar design). This choice demonstrates cultural and technical knowledge of the technology landscape in Türkiye, and the country's technological independence.

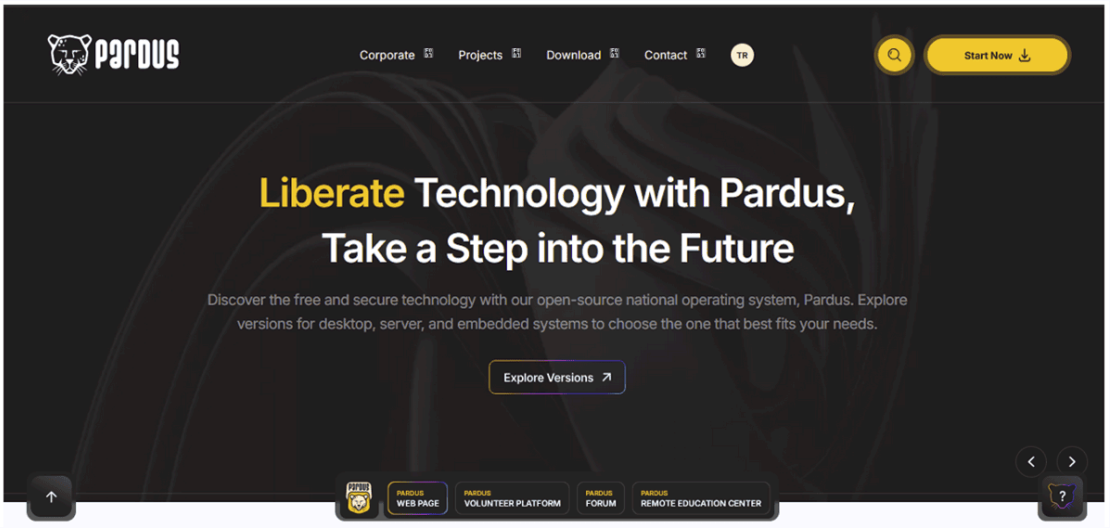


Figure 13: Fake website hosted on rosereserve[.]org, mimicking the legitimate Pardus website.

Timeline:

- **June 12-18, 2025**: Threat actor prepares and configures 2.56.127[.]187.
- **June 23, 2025**: roseserve[.]org domain is purchased.
- **June 29, 2025**: Historical snapshot shows an impersonation of the Anadolu Agency (a news agency headquartered in Türkiye) website – see Figure 14, below.

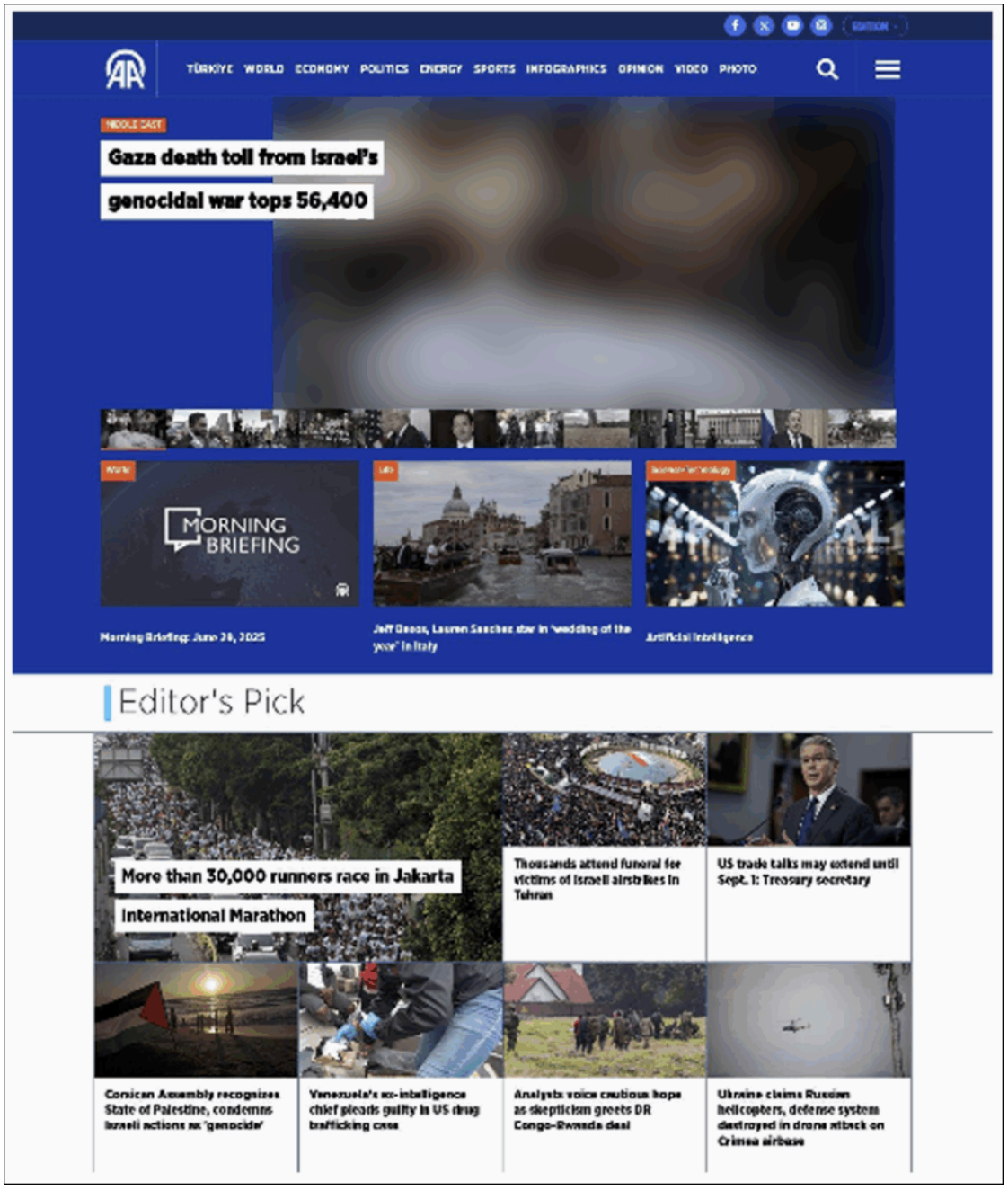


Figure 14: An early attempt at impersonating a real news agency's website on rosereserve[.]org.

Hosting Information:

The C2 server roseserve[.]org runs on **2.56.127[.]187.**

- **Owner**: DEDIPATH-LLC
- **ASN**: AS 35913
- **Country**: U.S.
- **CIDRs**: 2[.]56.127.0/24

Secondary owner: STARK-INDUSTRIES

- **ASN**: AS 44477
- **Country**: GB
- **CIDRs**: 2[.]56.127.0/24

Website Comparison:

Hunting pivot for fake Pardus banner: \n\t\tPardus – TÜBİTAK\t

Original header: “Home – Pardus – TÜBİTAK” (TÜBİTAK is the Scientific and Technological Research Council of Türkiye, the developer of the Pardus operating system).

Original/legitimate pardus.org.tr: Points to real domain on IP address 193.140.63.90 (Türkiye).

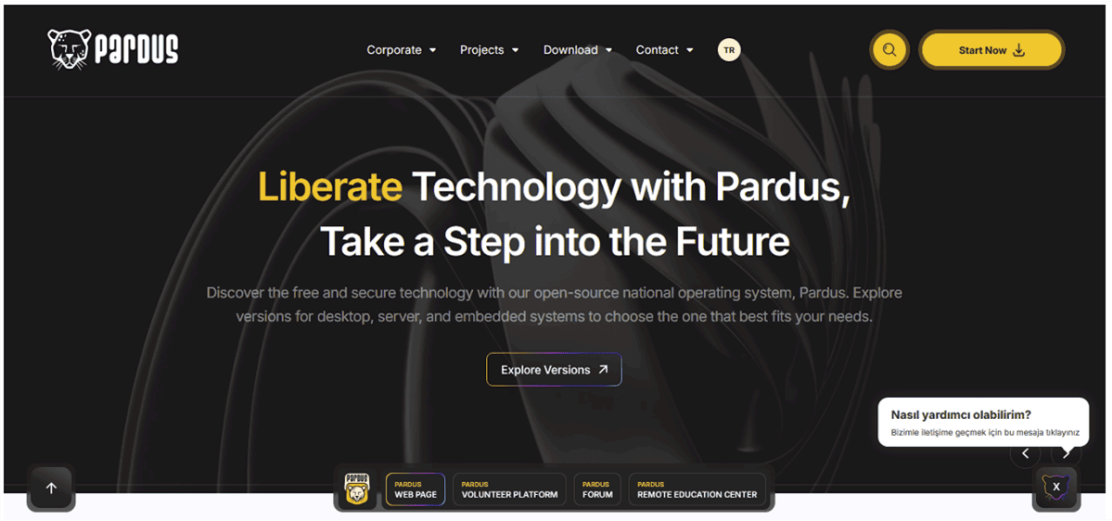


Figure 15: Legitimate Pardus website.

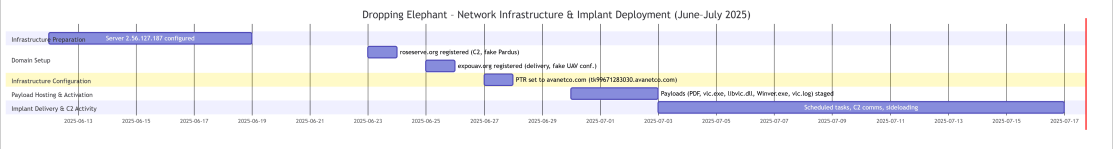


Figure 16: Network infrastructure and implant deployment timeline (Click to enlarge).

Remote Control Arsenal:

The code receives data in this order: C2 command + arguments.

Available Commands:

- **3Up3** – Downloads a file from a remote server, adds the .exe extension to it, and runs it. The URL is passed to this function as a parameter. This command transforms victim workstations into staging platforms for additional malware deployment, enabling the threat actor to adapt their tools based on discovered network data and security measures.
- **3gnfm9** – Unknown function.
- **3gjdfghj6** – Executes threat actor commands via cmd.exe and reports results to C2. It provides direct system access, enabling the threat actor to operate with the same privileges as a legitimate employee.
- **3ngjfng5** – Uploads stolen data to C2.
- **3CRT3** – Unknown function.
- **3APC3** – Shellcode loader command: Receives filename and process startup string. The process is launched via cmd, with the code injecting data from the file into the running process. Essentially, this is a shellcode loader command. The process can be any process, and the file can be any file, but it must already exist in the system. They most likely deploy it to the victim using other commands. In this context, the C2 code launches QueueUserAPC for asynchronous thread execution.
- **3SC3** – Screenshot command: Takes a screenshot and sends it to the server. (“**SC**” in this command is likely an abbreviation for **Sc**reenshot)

Victimology

The target of the campaign analyzed in this report is Türkiye, which Dropping Elephant most likely seeks to undermine via their cyber-espionage campaign against a major Turkish defense contractor and weapons manufacturer headquartered in the country. The company specializes in space systems, air defense systems, land systems, Naval systems, missile systems, ballistic systems, and subsystems.

How Arctic Wolf Protects Its Customers

Arctic Wolf is committed to ending cyber risk, and when active campaigns are identified, we move quickly to protect our customers.

Arctic Wolf Labs has leveraged threat intelligence around Dropping Elephants' activity to implement new detections in the Arctic Wolf® Aurora™ Platform to protect customers. As we discover new information, we will enhance our detections to account for additional IOCs and techniques leveraged by this threat group.

Conclusion

The campaign analyzed in this blog exhibits highly strategic victim selection focused on Türkiye's defense industrial base, specifically precision-guided weapons manufacturing capabilities. The timing of this targeted campaign aligns with Turkish military cooperation agreements with Pakistan, indicating the threat actor's awareness of geopolitical developments and the opportunity to strategically exploit them through social engineering techniques.

Dropping Elephant demonstrates continued operational investment and development through architectural diversification from x64 DLL to x86 PE formats, and enhanced C2 protocol implementation through impersonation of legitimate websites.

The reduction in library dependencies and adoption of strtok-based command parsing indicates deliberate operational security improvements and codebase optimization by the group. The five-stage execution chain employs established living-off-the-land binaries and scripts (LOLBAS) techniques, with VLC DLL side-loading representing the primary evasion mechanism.

The two-month preparation timeline from domain registration (June 2025) to active operations (July 2025) suggests careful campaign execution planned well in advance of the July 28 – 29 Unmanned Aerial Vehicle conference in Istanbul, Türkiye, rather than ad-hoc or indiscriminate targeting.

Recommendations

As with many historical Dropping Elephant campaigns, the group leverages social engineering and spear phishing emails to obtain initial access into victim environments. The group relies heavily on user interaction in their campaigns. Significant effort is put into creating convincing lures and enticing emails that victims are more likely to interact with; in this case, centered around the upcoming conference about UAVs in Istanbul, Türkiye.

Social engineering and phishing emails are not completely remediated with security controls. However, educating users about the risks of interacting with unsolicited emails, particularly if the emails originate from outside their organization or call for urgent action, is a good start. Adding a "report phishing" button to your organization's email solution can empower users to report suspected phishing emails to your Security Operations Center (SOC) or IT security team.

User education, such as general security awareness training, is one of the important elements in preventing Dropping Elephant and other groups from obtaining access to your organization. Ensure all employees are aware of good security hygiene practices. Fostering a culture where employees feel safe reporting suspected phishing attempts or potential security breaches can greatly increase your organization's chances of preventing a successful compromise.

For those without the time to devote to creating security training resources from scratch, the Arctic Wolf Managed Security Awareness® training solution delivers easily digestible security lessons for employees, including regular phishing simulations and a "Report Phish" button, along with many other features.

Dropping Elephant's primary motivation is espionage, focusing on obtaining long-term access to sensitive business and military information. Recognizing this, network segmentation, or isolating sensitive information, can help reduce your attack

surface. Network segmentation limits where a threat actor can move through your environment and confines them to patient zero.

Also ensure your organization enforces the Principle of Least Privilege, both at the user level as well as the network level, to prevent threat groups from obtaining additional access if compromised.

Some additional methods you might consider include:

- **Patch Often, Update Always:** The entire attack surface of an organization is fair game for a sophisticated threat actor, from the gateways and endpoints to the networks and servers. Organizations should make sure to keep applications and operating systems regularly updated, and consider employing virtual patching for legacy systems.
- **Put Proactive Defenses in Place:** Intrusion prevention and detection systems have their place among firewalls and sandboxes to prevent attackers from exploiting security gaps. Endpoint Detection and Response (EDR) platforms can uncover hidden red flags before it's too late, so consider implementing enterprise solutions such as Arctic Wolf® Aurora™ Endpoint Defense.
- **Enforce "Least Privilege" Principles:** Lock down tools or block the use of tools normally reserved for system administrators. Behavior monitoring and application control can block unusual or suspicious routines executed by suspicious files.
- **Consider the use of Secure Email Gateway** solutions, to help proactively filter out malicious emails.
- By leveraging the Windows Defender Application Control in Microsoft Windows, organizations can assess which tools, software and applications are used within their digital environments. Locking down or continually reassessing such lists may reduce the likelihood of threat actors leveraging Living-off-the-Land (LOTL) binaries within their environment.
- Staffing a Security Operations Center to protect your company is a costly endeavor, and may not be feasible for many organizations. Arctic Wolf® Managed Detection and Response (MDR) provides 24×7 monitoring of your networks, endpoints, and cloud environments to detect, respond to, and remediate modern cyberattacks.
- Finally, consider leveraging contextual cyber threat intelligence (CTI) to build an organizational risk profile and maintain updated threat models based on the geolocation, business profile and vertical your organization operates in. Such an intelligence program can help organizations to anticipate attacks and prioritize defenses based on the knowledge of the adversary and their tradecraft.

Appendix

YARA Hunting and Detection Rule

```
rule Dropping_Elephant_RAT {
    meta:
        description = "Rule for detecting Dropping Elephant RAT"
        last_modified = "2025-07-16"
        author = "The Arctic Wolf Labs team"
        version = "1.0"
        sha256 = "8b6acc087e403b913254dd7d99f09136dc54fa45cf3029a8566151120d34d1c2"
    strings:
        $a1 = "%s=33up$!!$%s$!!$%s" ascii wide
        $a2 = "%s=uep$@$%s$@$%s" ascii wide
        $a3 = "%s=%s$!!$%s" ascii wide
        $a4 = "%s=%s$!!$%s$!!$%s" ascii wide
        $a5 = "%s=%s!$$$!%s" ascii wide
        $a6 = "%s=%s!@!%s!@!%lu" ascii wide
        $a7 = "%s=%s!$$$!%s!$$$!%s" ascii wide
        $a8 = "%s=error@$$@%s@$$@%s" ascii wide
        $a9 = "%s=%s$!!$%s$!!$%s$!!$%s$!!$%s$!!$%s$!!$" ascii wide
    condition:
        (uint16(0) == 0x5A4D) and (filesize < 1MB) and (all of ($a*))
}
```

Indicators of Compromise (IOCs)

File Indicators

Name	SHA-256
Unmanned_Vehicle_Systems_Conference_2025_In_Istanbul.lnk	341f27419becc456b52d6fbe2d223e8598065ac596fa8dec23cc72272(
Unmanned_Vehicle_Systems_Conference_2025_In_Istanbul.pdf	588021b5553838fae5498de40172d045b5168c8e608b8929a7309fd08
lake (libvlc.dll)	2cd2a4f1fc7e4b621b29d41e42789c1365e5689b4e3e8686b80f80268
vlc.log	89ec9f19958a442e9e3dd5c96562c61229132f3acb539a6b919c15830
Decrypted Shellcode	8b6acc087e403b913254dd7d99f09136dc54fa45cf3029a8566151120

Scheduled Task

```
saps "C:\Windows\Tasks\Winver" -a "/Create", '/sc', 'minute', '/tn', 'NewErrorReport', '/tr', "C:\Windows\Tasl
```

Network Indicators

- **expouav[.]org** – Dropping website
- **roseserve[.]org** – C2 server

Mutant Object

Sessions\1\BaseNamedObjects\ghjghkj

Detailed MITRE ATT&CK® Mapping

MITRE ID	Technique	Confirmed Procedure	Evidence
T1566.001	Spear-phishing Attachment	LNK file distributed as conference invitation	File: Unmanned_Vehicle_Systems_Conference_2025_In_Istanbul.lnk (SHA-256: 341f27419becc…etc.)
T1059.001	PowerShell	LNK file executes PowerShell with bypass and stealth parameters	Command: -ep 1;$ProgressPreference = ‘SilentlyContinue’
T1105	Ingress Tool Transfer	PowerShell downloads five files from delivery infrastructure	Source: expouav[.]org via Wget
T1036.005	Match Legitimate Name or Location	Files renamed to legitimate Windows binary names	lama → vlc.exe, dalai → Winver.exe, lake → libvlc.dll

T1027	Obfuscated Files or Information	Shellcode encrypted and stored as log file	File: vlc.log with decryption key: 76bhu93FGRjZX5hj876bhu93FGRjX5
T1574.002	DLL Side-Loading	VLC Media Player loads malicious libvlc.dll	Host: vlc.exe, Malicious: libvlc.dll (SHA-256: 2cd2a4f1fc…etc.)
T1055	Process Injection	Shellcode injected into VLC player memory space	Target: VLC process, Payload: Decrypted x86 PE (SHA-256: 8b6acc087e…etc.)
T1053.005	Scheduled Task	PowerShell creates persistent scheduled task	Command: saps “C:\Windows\\Tasks\Winver” -a “/Create”, ‘/sc’, ‘minute’, ‘/tn’, ‘NewErrorReport’
T1140	Deobfuscate/Decode Files or Information	Runtime shellcode decryption within libvlc.dll	Input: vlc.log, Output: x86 PE (139.37 KB)
T1070.006	Timestomp	Compilation timestamp manipulation for anti-forensics	Backdated to: Fri Jul 26 09:12:19 2024 vs. actual campaign timeline (2025)
T1562.001	Disable or Modify Tools	PowerShell execution policy bypass	Parameter: -ep 1 (Execution policy bypass)
T1082	System Information Discovery	System profiling via Windows APIs	APIs: GetComputerNameW, GetUserNameW, Firmware information collection
T1124	System Time Discovery	System time and performance counter queries	Purpose: Sandboxing evasion and timing analysis
T1497	Virtualization/Sandbox Evasion	Processor feature detection for environment analysis	Checks: CPU capabilities, virtualization features
T1113	Screen Capture	Screenshot collection and processing	APIs: CreateStreamOnHGlobal, GetSystemMetrics(SM_CYSCREEN/SM_CXSCREEN)
T1071.001	Web Protocols	HTTPS communication with C2 server	C2: roseserve[.]org, Method: HTTP POST to /post endpoint

T1573.001	Symmetric Cryptography	Encrypted C2 communications	User-Agent: Mozilla/5.0 for traffic blending
T1132.001	Standard Encoding	Structured command parsing with delimiters	Parser: strtok function with $ delimiter
T1102.002	Bidirectional Communication	Command execution and data exfiltration	Commands: 3Up3, 3gnfm9, 3gjdfghj6, 3ngjfng5, 3CRT3, 3APC3, 3SC3
T1041	Exfiltration Over C2 Channel	System data and screenshots transmitted to C2	Channel: HTTPS to roseserve[.]org
T1583.001	Acquire Infrastructure	Custom domains with legitimate site impersonation	Domains: expouav[.]org (mimics waset.org), roseserve[.]org (mimics pardus.org.tr)

About Arctic Wolf Labs

Arctic Wolf Labs is a group of elite security researchers, data scientists, and security development engineers who explore security topics to deliver cutting-edge threat research on new and emerging adversaries, develop and refine advanced threat detection models with artificial intelligence and machine learning, and drive continuous improvement in the speed, scale, and detection efficacy of Arctic Wolf's solution offerings.

Arctic Wolf Labs brings world-class security innovations to not only Arctic Wolf's customer base, but the security community at large.
