THREAT CURE
RE-ARCHITECT YOUR THREAT LANDSCAPE

ThreatCure

Cyber Threat Advisory

StegoLoader Campaign

(Remcos RAT and Agent Tesla)

Description

Remcos RAT and Agent Tesla
The primary malware payloads delivered.

CATEGORY

Malware

SEVERITY

High

Platforms

Windows

IMPACT

- Data Theft and Credential Compromise
- Remote System Control
- Financial and Operational Impact
- Widespread Distribution via Phishing

The researchers have identified a novel malware technique involving **bitmap steganography within 32-bit .NET applications** to deliver multi-stage payloads. Threat actors embed malicious code inside image resources bundled in otherwise legitimate-looking executables, leveraging multiple layers of obfuscation and dynamic assembly loading to evade detection.

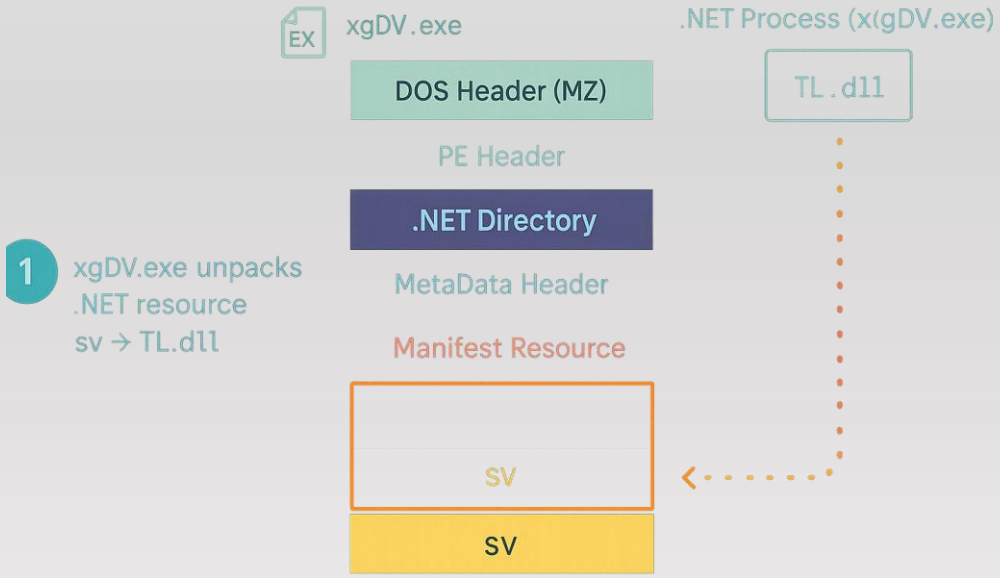
These attacks, primarily distributed via spam emails, have targeted critical industries in Türkiye and Asia. Through a series of in-memory decryption and unpacking stages, the final payload is deployed commonly variants of **Agent Tesla**, **Remcos RAT**, or **XLoader**. Understanding this layered delivery mechanism helps defenders proactively detect and mitigate similar threats in enterprise environments.

Attack Lifecycle: Technical Overview

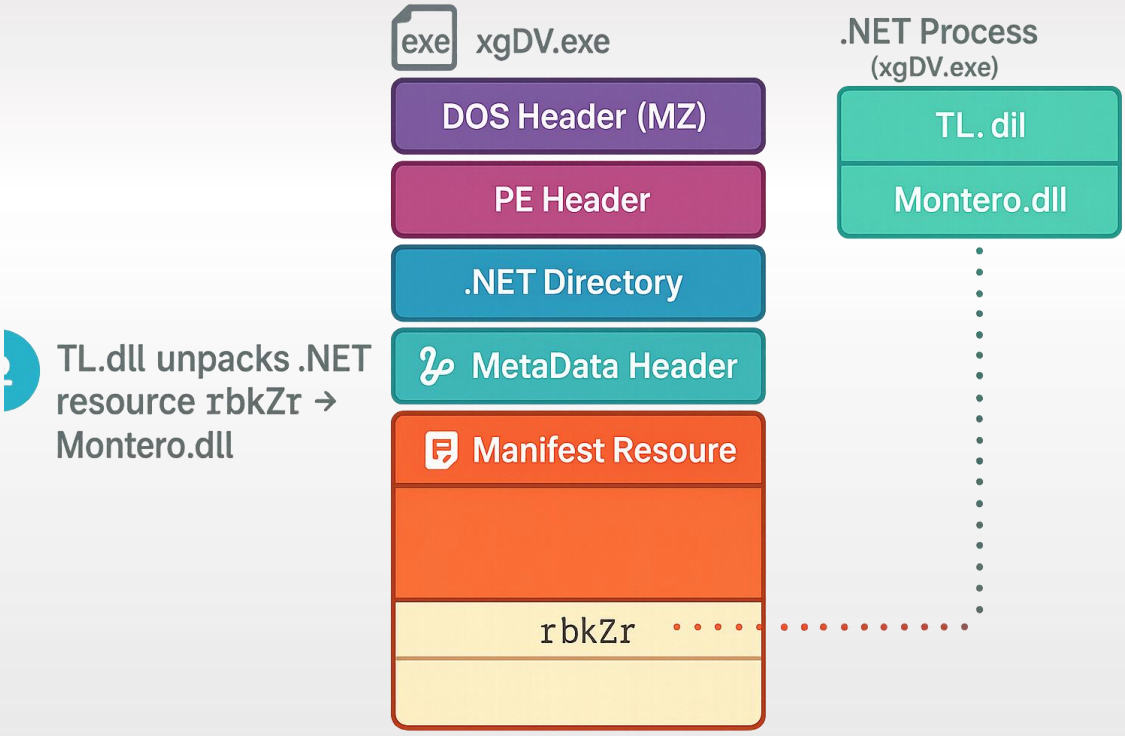
- **Stage 1: Dropper Loader (xgDV.exe)**
  - Delivered via malicious email attachment (ZIP containing .exe)
  - Mimics a legitimate Windows Forms application (e.g., "OCR Tool")
  - Contains bitmap resource (sv) disguised as an image
  - Loads and decrypts the resource into memory as a .NET assembly (TL.dll) using the Initialize Component () method
- **Stage 2: First Loader (TL.dll)**
  - Reflectively loaded in-memory
  - Extracts a second bitmap-encoded resource (rbzR) embedded in the original EXE
  - Decrypts the content into another .NET assembly (Montero.dll) using Late Binding calls
- **Stage 3: Second Loader (Montero.dll)**
  - Applies XOR and subtraction-based decryption to unpack an embedded byte array (uK5APqTdSG)
  - Generates and loads final payload executable: Remington.exe
  - Supports various flags controlling execution style (e.g., forked vs. in-process)
- **Stage 4: Final Payload Execution**
  - Final stage belongs to Agent Tesla family
  - Steals credentials, keystrokes, clipboard data, and browser information
  - Exfiltrates data via SMTP over TLS

Process Evaluation

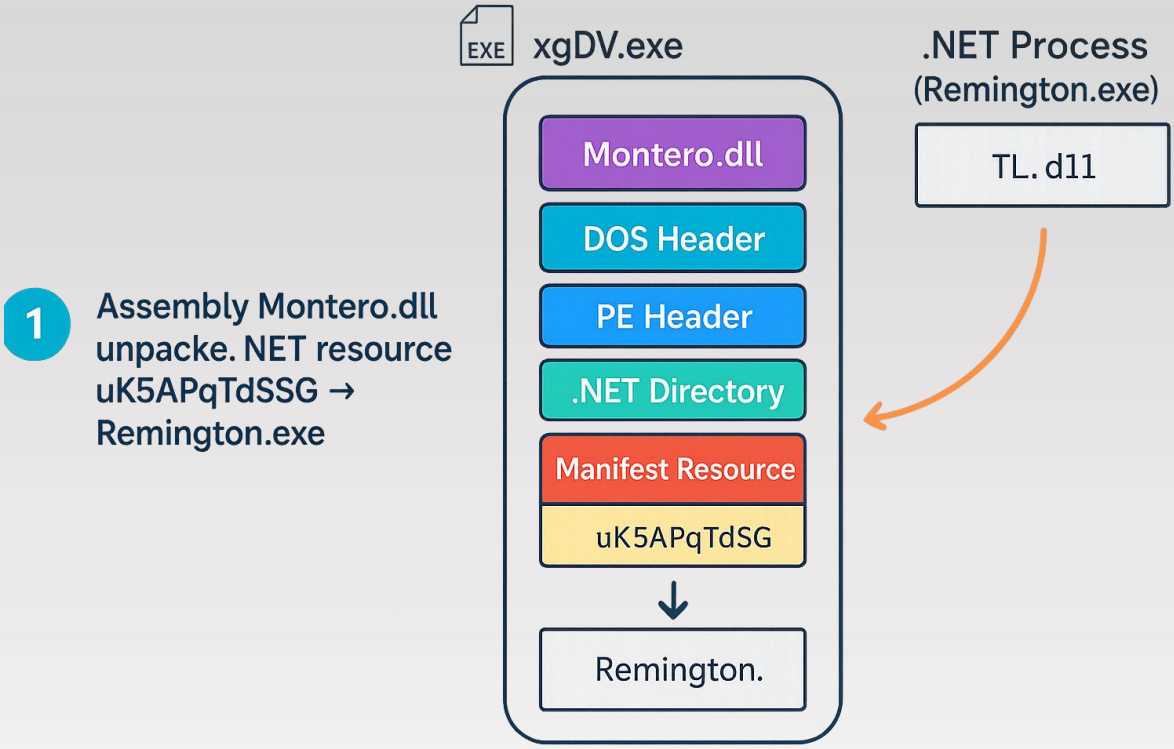
Stage 1: Initial Payload



Stage 2: TL.dll



Stage 3: Montero.dll



Stage 4: Final Payload

In the final phase of this multi-stage malware campaign, an Agent Tesla variant is executed directly in memory to evade detection. Agent Tesla is a .NET-based Remote Access Trojan (RAT) known for its capabilities to log keystrokes, capture screenshots, and extract credentials from applications such as web browsers and email clients.

In this instance, the malware is configured to exfiltrate stolen data via the Simple Mail Transfer Protocol (SMTP) using the following credentials:

SMTP Server: hosting2[.]ro.hostsailor[.]com:587
Sender Email: packagelog@gtpv[.]online
Recipient Email: package@gtpv[.]online
Password: 7213575aceACE@@

Indicator of Compromise

SHA-256

5adff9ae840c6c245c0a194088a785d78d91fe734ee46a7d51605c1f64f6dadd
30b7c09af884dfb7e34aa7401431cdabe6ff34983a59bec4c14915438d68d5b0
5487845b06180dfb329757254400cb8663bf92f1eca36c5474e9ce3370cadbde
ac5fc65ae9500c1107cdd72ae9c271ba9981d22c4d0c632d388b0d8a3acb68f4
5487845b06180dfb329757254400cb8663bf92f1eca36c5474e9ce3370cadbde
ac5fc65ae9500c1107cdd72ae9c271ba9981d22c4d0c632d388b0d8a3acb68f4
511af3c08bd8c093029bf2926b0a1e6c8263ceba3885e3fec9b59b28cd79075d
604cbcfa7ac46104a801a8efb7e8d50fa674964811ec7652f8d9dec123f8be1f
98195a4d27e46066b4bc5b9baea42e1e5ef04d05734c556d07e27f45cb324e80
a4a6364d2a8ade431974b85de44906fe8abfed77ab74cc72e05e788b15c7a0cf
3b83739da46e20faebecf01337ee9ff4d8f81d61ecbb7e8c9d9e792bb3922b76
8146be4a98f762dce23f83619f1951e374708d17573f024f895c8bf8c68c0a75
9ed929b60187ca4b514eb6ee8e60b4a0ac11c6d24c0b2945f70da7077b2e8c4b

MD5

8da84a9b6ec08f07a7c17e2036ee8600
546af1ef5db849e44a6a2dad582a1954
e7cb657dfaec55d61ab84188a1a7070c
2e1c86a62e206b7f0bfc72bed968f8f6
2e1c86a62e206b7f0bfc72bed968f8f6
ebfa1be35c0e8a0a1704d137a216f33b
21126c20ee531d38eefbe374b0b0b8f1
26c0f91863bb8694a3e2bb6843ec5da4
dfdaabf6991667c442c092621c433f8d

Indicator of Compromise

SHA-1

8293d0722efb8e70bc3a71df5d114dc9312a5133
e7aa5b71896ffdcfd73ecd79bffb72f60303cdc1
53ce251ffd8111a5fd17da0aa3d1469deb94cc2d
6feeca796d154a786a3f73ae0c1de3f4a36692c3
6feeca796d154a786a3f73ae0c1de3f4a36692c3
4785a2e7f483d58c7ac4d63b9e6f9026df346f86
ec4e33bce123e3365a295816d18001b11043e178
86d1a36f47750a0ce9f623f1025a8db26e5dab33
aaad4dfbd58b133fd9fc97fcb94c3fb7bfdece39

Remediation

- **Email & Web Gateway**
- Block ZIP or EXE attachments from unknown senders
- Enable content disarm and reconstruction (CDR) to sanitize file attachments
- Deploy AI-based detection to analyze LNK, HTA, or image-embedded executables
- **Endpoint Protection**
- Enable detection for PowerShell, reflection-based code execution, and image parsing anomalies
- Apply execution control policies (e.g., AppLocker, WDAC) to restrict untrusted EXEs
- Monitor %APPDATA%, %TEMP%, and %LOCALAPPDATA% for suspicious file drops
- **Behavioral Monitoring**
- Watch for dynamic Assembly. Load(byte[]), reflection API usage, or string decryption functions
- **Awareness & Training**
- Educate users to avoid opening ZIP attachments containing executables, even from familiar sources
- Emphasize caution on emails referencing urgent procurement, invoice, or shipping matters

ThreatCure

Cyber Threat Advisory

Secure your byte world

(Remcos RAT and Agent Tesla)

StegoLoader Campaign