

A Multi-Stage Steganographic Loader Campaign Deploying Diverse Payloads Globally

 labs.k7computing.com/index.php/a-multi-stage-steganographic-loader-campaign-deploying-diverse-payloads-globally

Harihara Sudhan

June 22, 2026

During the routine telemetry monitoring, we identified a detection on a suspicious file named **“GST Debit Note Apr_26.com”**, based on the telemetry data observed. This prompted us to investigate the sample further.

Our analysis revealed that the payload was a variant of the Remcos RAT malware family, distributed via a phishing campaign as an archive attachment. One notable characteristic of this infection chain was its reliance on in-memory execution techniques / fileless malware & Steganography. By avoiding disk-based artifacts, the threat reduces forensic evidence and increases its ability to evade traditional security tools and signature-based detection methods.

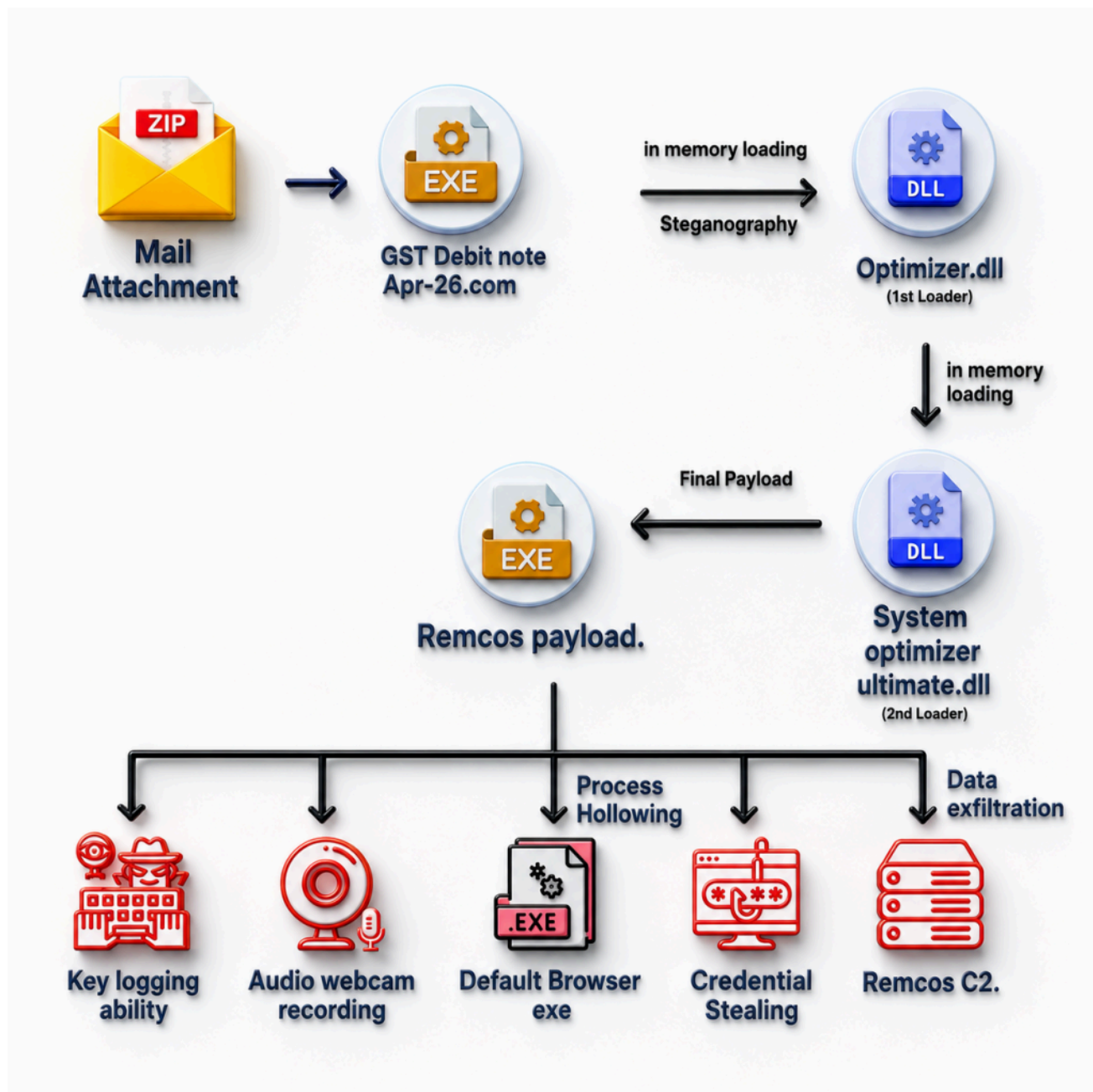


Figure -1: Kill chain of Remcos RAT

Upon downloading and extracting the archive, it drops a file named “**GST Debit Note Apr_26.com**”. Initial triage revealed that the file is a **32-bit .NET executable**. Further inspection using Detect It Easy indicated that the binary was **packed**. Additionally, the sample was found to be **unsigned**.

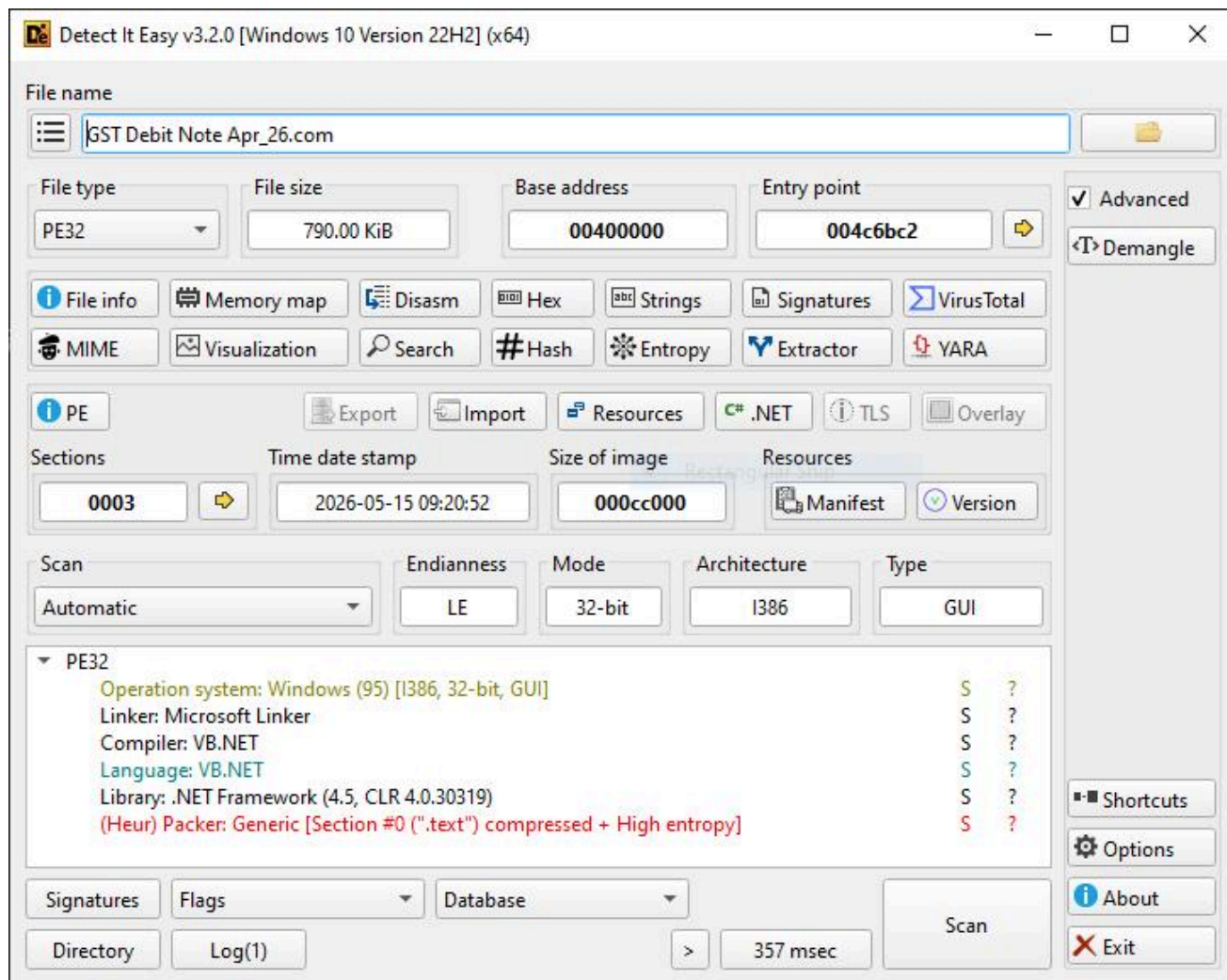


Figure -2: Viewing the attached executable came through phishing

Interestingly, the sample contains embedded Turkish-language artifacts, and the executable masquerades as a legitimate **brick-building game**. The decoy application is intended to run in the background after launch, likely to reduce user suspicion.

GST Debit Note Apr_26.com	
Property	Value
File Name	C:\Users\ \Desktop\GST Debit Note Apr_26.com
File Type	Portable Executable 32 .NET Assembly
File Info	No match found.
File Size	790.00 KB (808960 bytes)
PE Size	790.00 KB (808960 bytes)
Created	Monday 08 June 2026, 17.07.03
Modified	Friday 15 May 2026, 09.20.52
Accessed	Monday 08 June 2026, 17.07.17
MD5	897ABF678EDAD72998554EC18675092F
SHA-1	BE36EF651EED6808760153200A3A2A2B7060CCE5
Property	Value
Comments	Brick Builder Game
CompanyName	
FileDescription	Tuglalnsaatci
FileVersion	1.0.0.0
InternalName	oacY.exe
LegalCopyright	Copyright © 2026
LegalTrademarks	
OriginalFilename	oacY.exe
ProductName	Tuglalnsaatci
ProductVersion	1.0.0.0

Figure -3: Viewing the executable in CFF Explorer

Upon reversing the binary, we observed that it leverages **embedded resource content** for payload delivery. The malware hides and retrieves its next-stage components from resource sections, effectively using a **steganographic-style delivery technique** to obscure malicious content and complicate static analysis.

Upon extracting the embedded resource identified as SR1, we found that it contains a **serialized .NET Bitmap object**. The malware abuses this object as a container for hidden payload data, reinforcing the use of steganographic techniques for payload concealment and staged delivery.

```

Add-Type -AssemblyName System.Drawing

$asm = [System.Reflection.Assembly]::LoadFile(
    (Resolve-Path ".\sample.exe")
)
$resType = $asm.GetType(
    "TuglaInsaatci.Properties.Resources"
)
$prop = $resType.GetProperty(
    "SR1",
    [System.Reflection.BindingFlags] "Static,Public,NonPublic"
)
$bmp = $prop.GetValue($null)
$max = 71168
$list = New-Object System.Collections.Generic.List[byte]
for ($x = 0; $x -lt $bmp.Width; $x++)
{
    for ($y = 0; $y -lt $bmp.Height; $y++)|
    {
        if ($list.Count -ge $max) { break }
        $p = $bmp.GetPixel($x, $y)
        $list.Add($p.R)
        if ($list.Count -ge $max) { break }
        $list.Add($p.G)
        if ($list.Count -ge $max) { break }
        $list.Add($p.B)
    }
}
[IO.File]::WriteAllBytes(
    ".\payload.bin",
    $list.ToArray()
)
Write-Host "payload extracted"

```

Figure -4: Script used to extract the next loader from the resources (steganography)

The above script extracts the next-stage loader, **Optimax.dll**, and loads it directly into memory during execution without writing it to disk.

Property	Value
File Name	C:\Users\ \payload_extracted.exe
File Type	Portable Executable 32 .NET Assembly
File Info	Microsoft Visual Studio .NET
File Size	69.50 KB (71168 bytes)
PE Size	69.50 KB (71168 bytes)
Created	Monday 08 June 2026, 17.25.49
Modified	Tuesday 19 May 2026, 17.08.49
Accessed	Monday 08 June 2026, 17.26.04
MD5	AFE085B7324D72673EEF749FF5F21A49
SHA-1	A86F1039A8877804B1B2C99AED91312846CD40E5

Property	Value
Comments	AI-driven autonomous system optimization and self-healing platform
CompanyName	Quantum Performance Labs
FileDescription	OptiMax Quantum Suite
FileVersion	18.9.6.9847
InternalName	OptiMax.dll
LegalCopyright	
LegalTrademarks	OptiMax™
OriginalFilename	OptiMax.dll
ProductName	OptiMax Quantum
ProductVersion	18.9.6.9847

Figure -5: Viewing the 1st extracted loader

After extracting the next-stage loader – Optimax.dll, which is a **32-bit .NET DLL**. On reversing using dnspy, the 1st load – The code dynamically loads a .NET assembly directly from an in-memory byte array using reflection and late binding. Instead of loading a DLL from disk, the payload is reconstructed in memory (**this.pf.ToArray<byte>()**) and executed through AppDomain.Load, a technique commonly seen in packers, loaders, and fileless malware.

Name	Optimized	Dynamic	InMemory	Order	Version	Timestamp	Address	Process	AppDomain
System.Xml.dll	No	No	No	7	4.8.9221.0 built by: NET481REL1LAST_25H2	6/19/2025 1:58:41 AM	07070000-072F4000	[0x3130] GST Debit Note Apr_26 - Copy...	[1] GST Debit Note Apr_26
Accessibility.dll	No	No	No	8	4.8.9221.0 built by: NET481REL1LAST_25H2	6/19/2025 1:49:20 AM	06400000-0640A000	[0x3130] GST Debit Note Apr_26 - Copy...	[1] GST Debit Note Apr_26
System.Core.dll	No	No	No	9	4.8.9319.0 built by: NET481REL1LAST_25H2_B	8/22/2025 9:30:16 AM	06590000-0670C000	[0x3130] GST Debit Note Apr_26 - Copy...	[1] GST Debit Note Apr_26
Microsoft.VisualBasic.dll	No	No	No	10	14.8.9221.0 built by: NET481REL1LAST_25H2	6/19/2025 2:42:24 AM	064E0000-0657C000	[0x3130] GST Debit Note Apr_26 - Copy...	[1] GST Debit Note Apr_26
OptiMax	No	No	Yes	11	18.9.6.9847	5/13/2026 4:04:13 AM	086C0000-086D1600	[0x3130] GST Debit Note Apr_26 - Copy...	[1] GST Debit Note Apr_26
System Optimizer Ultimate	No	No	Yes	12	2025.1.0.0	5/15/2026 9:20:43 AM	08E80000-08F2B401	[0x3130] GST Debit Note Apr_26 - Copy...	[1] GST Debit Note Apr_26

Figure -6: Loaded modules at runtime

This DLL invokes another DLL in memory, which is named “[System Optimizer Ultimate.dll](#),” which is a second-stage loader that drops a final payload, which is also in memory. The final payload – Remcos, uses the process hollowing technique to run as a default browser process name, whichever the user has set.

Further behavioral analysis showed that, upon execution, the malware creates a copy of itself inside the **AppData\Roaming** directory under a randomized name, which is superhidden. It also has the capability of a complete cleanup to erase all its footprints.

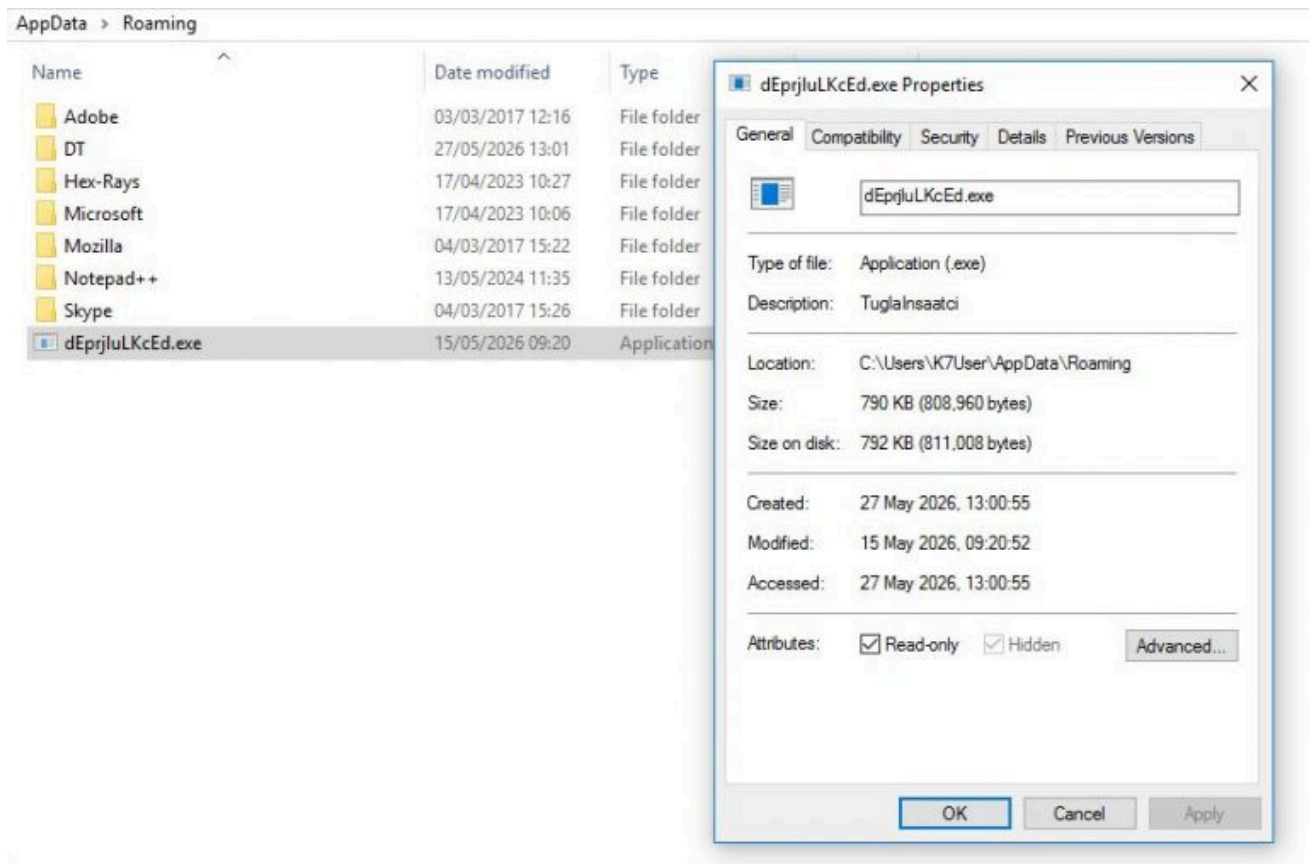


Figure-7: Self-copy with a hidden attribute

During execution, the malware drops an obfuscated **PowerShell script (.ps1)** along with an executable into the temporary directory.

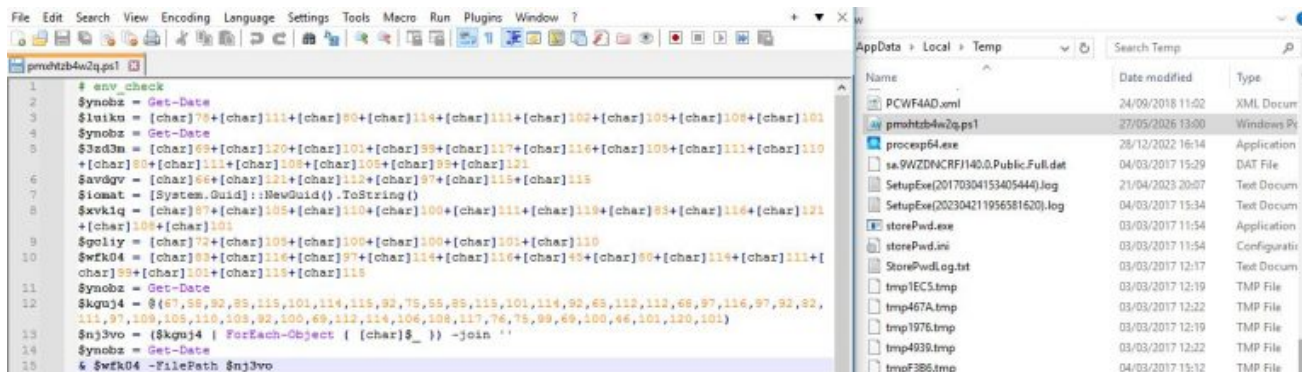


Figure -8: Dropped obfuscated PowerShell script

The dropped executable is then configured for persistence through a **Run registry key**, ensuring that it is automatically launched whenever the victim logs into the system.



Figure -9: Created Run Entry

Once persistence is established, the malware begins collecting victim data, and it also creates a mutex named “**Remcos_Mutex_Inj**”, thus confirming that the payload is **Remcos RAT**.

It checks for Sandbox & VM presence and proceeds: sandbox through “sbiedll.dll” and VM presence via this registry “hardware/acpi/dsdt/vbox_”. It also bypasses UAC by using eventviewer.exe. User activity monitoring – The code is continuously:

1. Monitors the active (foreground) window
2. Detects window title changes
3. Logs the new window title
4. Tracks user idle time
5. Reports when the user becomes active again

Also has the capability of audio and webcam recording.

The final payload achieves its persistence through the Run entry, winlogon.exe, & userinit. Also, it has browser credential theft, process hollowing, command execution, and self-management capabilities.

The sample contains dedicated functionality for handling browser artifacts, including Chrome stored logins, Chrome cookies, and Firefox stored credentials, indicating credential theft. It also has a full cleanup routine.

It stores the captured information in a file named **logs.dat**, which is subsequently exfiltrated to its command-and-control (C2) server at **62.102.148.212**.

AppData > Roaming > DT

Name	Date modified	Type	Size
 logs.dat	04/03/2017 15:34	DAT File	2 KB

Figure -10: location where the log entries are stored

Unknown | Last Update: 2026-05-01

 **62.102.148.212**

Inbound: Unknown | Outbound: Unknown | Nondirected Attack

Sweden, Stockholm's lan, Akersberga | AS 51815

VirusTotal: Add your API key
Greynoise: Unknown
URLhaus: -

SUMMARY | ACTIVITIES | **DNS** | RELATED FILES | INTERNET ASSETS | WHOIS | CERTIFICATES

PDNS (1)

Resolution Domain	Verdict	Intels	Resolution Time
acceic.ddns.net	 Malicious	C2 nRAT DDNS	2026-02-06 2 related IPs

Figure -11: detailed info on C2 IP

Further pivoting through VirusTotal revealed that similar samples associated with this campaign were also observed delivering additional malware families, including Agent Tesla, commodity stealers, MassLogger variants, Phantom Stealer, Dark Cloud, and Red Line Stealer, and Snake keyloggers, Formbook, xworm, strongly suggesting that it's a loader-as-a-service functionality; only the payload differs. This suggests that the infrastructure is likely being used as part of a broader malware distribution ecosystem rather than being exclusive to a single payload family.

Malware configuration file

remcos

Implant info

Family/toolkit: remcos

Network info

Extracted URLs

Scanned	Detections	Status	Categories	URL
2026-05-27	5 / 92	200	C2	http://62.102.148.212:37393
2026-05-27	5 / 92	-	C2	tcp://62.102.148.212:37393

Extracted IP addresses

IP address	Detections	Protocols	Port	Autonomous System	Country	Categories
62.102.148.212	12 / 91	HTTP	37393	51815	SE	C2
62.102.148.212	12 / 91	-	37393	51815	SE	C2
62.102.148.212	12 / 91	-	37393	51815	SE	C2

Figure -12: VT info

While browsing the metadata “Tuglainsaatci”, we found several samples that use MassLogger & Remcos as their final payloads.

signature:Tuglainsaatci

Save search Build your Search

IOCS -17 COMMENTS 0

Collapse filters

Sort by Export

Filters

IoC type: Files -17

Examples:

- ☐ Have 5 or more detections
- ☐ Have distribution vectors
- ☐ Have threat network infrastructure
- ☐ Have sandbox detonation report
- ☐ Have community comments
- ☐ Seen in the last month

Matches - 17/-17 Files

	Detections	First seen	Last seen
a4903ba8d565b62bfbc98c98c45a1b8c46d11064bc0c06f1215b2ff9f5ff30c TXKJ.exe peexe spreader assembly	45 / 71	2026-06-08 05:38:28	2026-06-08 05:38:28
1c0470d1ca409c9389dc469d92274e9131956e0db026e09caff4021e3d092152 uPRD.exe peexe assembly spreader	53 / 72	2026-05-21 05:06:15	2026-05-21 05:06:15
a58fc2d03abc7b89b5e45935ea0b790e37be88e1c67f2dfb25ba03e7d7ce91de AyqE.exe peexe spreader assembly persistence	53 / 68	2026-05-14 20:45:05	2026-05-20 11:21:39
bf69f267d59823eddabbfe3ca489c9b6ffa2595db9e92affe9bb141306521079 hbbF.exe peexe spreader assembly	57 / 71	2026-05-14 20:39:17	2026-05-18 13:46:25

Figure -13: On searching through the strings available in metadata

Payload filenames containing “NEFT”, “RTGS”, “IMPS”, and “GST” tie this campaign to India, where the Remcos RAT was deployed as the final payload.

2025-08-02	55 / 73	Win32 EXE	Neft payment receipt_602202511.scr
2025-03-08	59 / 73	Win32 EXE	HGSDS.exe
2025-12-07	43 / 66	RAR	neft%20payment%20receipt_602202511.rar

Figure -14: Filenames used in the campaign based in India-1

2026-05-01	40 / 71	Win32 EXE	IDBI_Payment receipt May_2026.com
2026-05-06	40 / 70	Win32 EXE	iLmN.exe
2026-05-02	49 / 71	Win32 EXE	8c90b962787baacf430c76047c984bc0e74b3221a38bf7f20aed0a8460b4ff8.exe
2026-05-07	69 / 72	Win32 EXE	a6af2a6cafe8e88983908997c45d4e1c25ee8aaa6b6ed91ceb184ba742bf2769.exe
2026-05-02	42 / 71	Win32 EXE	RTGS_IMPS payment receipt Ref no NCB2712080809712.com

Figure -15: Filenames used in the campaign based in India-2

Scanned	Detections	Type	Name
2025-03-08	69 / 73	Win32 EXE	544-75-0x0000000000400000-0x0000000000417000-memory.dmp
2025-03-10	60 / 73	Win32 EXE	eSKL.exe
2025-06-13	38 / 66	RAR	3fc6de0969438f83b059608b2a8e9e52cc3733306b4331c90367ef8a2cd192c7
2025-08-01	57 / 72	Win32 EXE	JLhC.exe
2025-08-05	57 / 73	Win32 EXE	SaNr.exe
2024-03-14	66 / 73	Win32 EXE	/home/petik/ptktriage/6bc7d010d6ffaba5f297001611e07f354f5a7aae664dea31c0810d23a68c7721
2026-03-19	55 / 72	Win32 EXE	/raid/kostada2/RawMal/family_based_dataset/final_dataset/Noon/Bazaar.2023.07__HEUR-Trojan-Spy.MSIL.Noon.gen-7092f70a3da40f994f74a966d0c31c42edd8ea933b6b853c5fe9618f8e166024
2025-03-08	60 / 73	Win32 EXE	68r0H.exe
2025-02-12	55 / 72	Win32 EXE	K2U1wzl.exe
2025-03-08	55 / 73	Win32 EXE	Tax Challan.exe
2025-06-11	37 / 66	RAR	a0ce34cf08f2448a970f423824e4195215f5ff7b6c58bd5a1a4a4ad4b5774be3
2026-03-24	67 / 73	Win32 EXE	C:\Windows\9q1wsy.exe
2025-07-31	55 / 72	Win32 EXE	kcER.exe
2026-03-14	50 / 73	Win32 EXE	C:\Windows\floc7.exe
2026-03-21	0 / 66	Office Open XML Spreadsheet	C:\Windows\tr6wc.exe
2025-06-16	36 / 73	Win32 EXE	C:\Users\user\AppData\Roaming\GKJVRf.exe
2025-07-31	55 / 72	Win32 EXE	kUEz.exe
2025-03-17	61 / 74	Win32 EXE	YFGjV.exe
2025-08-02	55 / 73	Win32 EXE	Neft payment receipt_602202511.scr
2025-03-08	59 / 73	Win32 EXE	HGSDS.exe
2025-12-07	43 / 66	RAR	neft%20payment%20receipt_602202511.rar

Figure -16: Filenames used in the campaign based in India-3

With the increasing risk of malware attacks, it's important to take steps to protect your data. Using a reliable security product like K7 Total Security and keeping it updated is crucial to defending against these threats.

IOCs

Names	Hash
Archive file	C2E25ABA8E2AD4CAFDD6C633B8CA0906
Gst debit bill Apr 2026.com	897ABF678EDAD72998554EC18675092F
Optimax.dll	AFE085B7324D72673EEF749FF5F21A49
System Optimizer Ultimate.dll	F3626A38FCF488C9EED54BEB8C7C116F
Remcos payload	4924369C0BDAF73B21EB992EB9DB4DEA
62.102.148.212:37393	Remcos C2
217.138.252.123:42830	
146.70.244.90:37393	