

Vercel-hosted RMM abuse campaign evolves with Telegram C2 for victim filtering

 cloudflare.com/zh-cn/cloudforce-one/research/report/vercel-hosted-rmm-abuse-campaign-evolves-with-telegram-c2-for-victim-filtering

**Vercel-hosted RMM
abuse campaign
evolves with Telegram
C2 for victim filtering**



Campaign snapshot - Jan 20, 2026

Overview

In this snapshot, we will outline a novel phishing campaign observed from November 2025 to January 2026 which leverages the Vercel hosting platform to deliver a remote access tool. The campaign was first documented by CyberArmor in June 2025, although our latest intelligence confirms that this threat has not only persisted but evolved in its technical execution.

The core tactic remains the same: exploiting the "inherited trust" of *.vercel.app domains to bypass email filters and deceive users with financially themed lures, such as overdue invoices and shipping documents. However, the campaign has moved beyond simple file-dropping. We have now observed a sophisticated Telegram-gated delivery mechanism designed to filter out security researchers and automated sandboxes.

By transitioning from basic public file links to this "conditional delivery" model, the threat actors have demonstrated a concerted effort to evade the detection signatures generated by earlier reporting. This snapshot outlines the updated attack chain, the shift to GoTo Resolve (formerly LogMeIn) as a "Living off the Land" (LotL) tool, and critical mitigation strategies for security teams.

The lure: financial urgency and impersonation

This campaign's effectiveness hinges on exploiting the "abuse of trust" in legitimate services. Attackers craft phishing emails with financial or business themes, such as "unpaid invoices," "payment statements," or "document reviews."

These emails are not the primary lure; the Vercel-hosted link is. The attacker relies on:

1. Trusted domain: The vercel.app domain is legitimate and reputable, bypassing many email filters and lulling users into a false sense of security.
2. Plausible themes: The Vercel pages themselves are cleverly disguised, often impersonating a "secure" Adobe PDF viewer, a financial document portal, or a software download page.
3. Social engineering: In some cases, attackers masquerade as technical support, using the link to guide a victim to install the "fix."

This blended approach, using a trusted domain to host a thematically appropriate lure, manipulates the target into believing the interaction is safe and taking the desired action.

Attack chain breakdown

Stage 1: Initial delivery The target receives a phishing email containing a link. The email body is often minimal, using urgent language ("due payment," "invoice attached") to pressure the user into clicking the embedded vercel.app link.

In the example below, the large PDF icon is not a real attachment but a hyperlinked image. Clicking it redirects the user to the malicious Vercel URL.

"Invoice Details" phishing example.

The email below, for example, claims an invoice is "43 days past due," pressuring the victim to click the "Download as Pdf" link, which initiates the RMM infection chain:

An example of the financial urgency lure.

The below email targets Spanish-speaking users with a "security update" lure, threatening service suspension to force a click.

An example of multilingual targeting.

Some emails, like the one pictured below, use a "Potential Lawsuit Notice" theme to panic the user into downloading the malicious payload.

A phishing email impersonating a secure document signing portal.

The email page below, for example, mimics a Meta "Community Standards" warning, using the threat of page removal to trick social media managers into installing the backdoor.

A specialized lure targeting business account owners.

Stage 2: Evasion and redirection

Upon clicking the link, the target is *not* immediately served the payload. This is a key evasion step.

1. Fingerprinting: The malicious page first performs browser fingerprinting, collecting the victim's IP address, location, device type, and browser.
2. Data exfiltration: This data is exfiltrated to a threat-actor-controlled Telegram channel.
3. Conditional delivery: The server uses this data to decide whether to deliver the payload, filtering out security researchers, sandboxes, and non-target geolocations.

If the victim is deemed "valid," they are presented with the fake document viewer or invoice page and prompted to download the file.

Stage 3: Payload deployment and execution

This leads the user to download a file disguised as a document or statement (e.g., Statements05122025.exe, Invoice06092025.exe.bin).

- Payload: The executable is not custom malware but a "Potentially Unwanted Program" (PUP) — a legitimate, signed version of GoTo Resolve (formerly LogMeIn) remote access software.
- Execution: By abusing this "Living Off the Land" (LotL) tool, the attacker bypasses most signature-based antivirus detections.

Impact: Upon execution, the tool installs and establishes a connection to its remote servers, providing the attacker with a full backdoor and remote control over the victim's host.

Detection & mitigation

This campaign was identified through its use of Vercel as a file dropper and the specific detection fingerprints built to catch this behavior. To protect against similar attacks, organizations should:

- Enhance email security: Deploy security solutions that can analyze links at time-of-click and detect service abuse and brand impersonation.
- Monitor TLDs: Due to the high rate of abuse, organizations should consider enhanced monitoring of links from vercel.app and surge.sh subdomains, pending user verification.
- Application control: Enforce application whitelisting or strict policies governing the installation of new remote desktop and support tools.
- User training: Conduct phishing simulations that specifically educate users on the "abuse of trust" tactic, showing that a valid SSL certificate (padlock) and a known domain name do not always equal safety.

The following detections were written by Cloudflare Email Security to protect against phishing campaigns leveraging the techniques in this attack:

- SentimentCM.Banking.Invoice.Service_Abuse.Vercel.Link - 50K hits in last 30 days
- Brand_Impersonation.Facebook.Service_Abuse.Vercel.Link - 600 hits last 30 days
- Sentiment_CM.Shared_Document.Service_Abuse.Vercel.Link -
- Brand_Impersonation.Financial_Institutions.Service_Abuse.Vercel.Link

Service_Abuse.Vercel.URL_Shortener.Link - 500 hits last 30 days

IOCs

List all known technical indicators associated with the campaign in a structured format. Domains / IPs

Indicator	Description
duepaymentinvoiceattached[.]vercel[.]app	Primary dropper URL
paymentrequestoninvoicedueattached[.]vercel[.]app	Confirmed dropper
invoice-110493[.]vercel[.]app	Confirmed dropper
olierinvoiceunpaidmmpaid[.]vercel[.]app	Confirmed dropper

Indicator	Description
paidrepotstatementinvoice[.]vercel[.]app	Confirmed dropper
unpaidbillrequestedservicedetails[.]vercel[.]app	Likely malicious (matching TTPs)
requestpaymentdueattachedts[.]vercel[.]app	Likely malicious (matching TTPs)
outstandingstatementdetailsattachedrb[.]vercel[.]app	Likely malicious (matching TTPs)
salesrepacctstatementdetails[.]vercel[.]app	Likely malicious (matching TTPs)
remityourpendingpaymentdts[.]vercel[.]app	Likely malicious (matching TTPs)
unpaidinvoiceremitaath.vercel[.]app	OSINT confirmed
waybill-deliveryticket.vercel[.]app	OSINT confirmed
invstatement2025[.]vercel[.]app	OSINT confirmed
invstatement[.]vercel[.]app	OSINT confirmed
windowscopy[.]vercel[.]app	OSINT confirmed
invoices-attachedpdf[.]vercel[.]app	OSINT confirmed
dhl-delivery-report[.]vercel[.]app	OSINT confirmed
dhl-shipment-detail[.]vercel[.]app	OSINT confirmed
express-delivery-note[.]vercel[.]app	OSINT confirmed
docsignstatements[.]vercel[.]app	OSINT confirmed
shipment-docspdf[.]surge[.]sh	OSINT confirmed (Surge abuse)
mail[.]blta[.]ro	OSINT associated domain
findhome[.]cl	OSINT associated domain

Email Detection Fingerprint (EDF)

EDFs

c5cb396ae54b603d258e5f13406a6c3f2634:5f41ed9eb791e93b2a9fc0f9fa9a

9325095ca2363db05cf13b52eaeabc7318d8:3740be59ab1956808312a383dfe7

a3ac5cfb0300f69b81064009b59a747d610f:ccf6f6ec7cd7f5d9644b35126a52

0ea78867f46393d77935ff537bd7a6baa8d0:d0d4bbcaa1ef70d0c181b352995b

9c40e43e7949b169529d7b762776058053fc:bb3e648f443dc53af057b410a8da

ca98540ce07a126667b62138c1dc7962331f:0ac419138b1192bb7123bbe31e29

b0474a0717318bb722267ff4dd74dc860666:d0d4bbcaa1ef70d0c181b352995b

5d58506db4ca986ce4a5f9159cb1ecf8fdf1:d960688cf10bcb3912d5308b5cd8

89ff0771b0eb8800eda9476aa2d44c85a30d:1a941ab3b2b55db87951e63b1c1c

59884eccc1f25cfb24fdc7e3720e5ea179f5:8f40f3db487fb2831e3f0e210be6

d52e046054a1095fffbaaa0c2c6011642e29:ccf6f6ec7cd7f5d9644b35126a52

227b5b5bec01727e8f054e769fa37cdf5292:2e9def4e0848688eb35a7f21d2b8

ce054b668379a41f9dab9784c811ce777043:ccf6f6ec7cd7f5d9644b35126a52

5f4a2eb6ceea10d943e409ca0ce6885db2c9:2c871442c1d82cf23e6b75628695

bf44de26036d702a8d70fc6001361f580486:5dba91e93ca441a2ca03f1891927

a2994c362e1c429d5aaa89a3c380a4b25da2:21f0c8bb023db0044cbd7aed31bd

5d818afe83569bcd1ec9155a6d6dd4c2763e:d0d4bbcaa1ef70d0c181b352995b

e1e049a40e8fd300d71fd1c81a43cedc62db:28f5bb2aa7a48caa8aa0f19b92a6

EDFs

f06233562310e888bd86466c7ff9622654f3:ccf6f6ec7cd7f5d9644b35126a52

7eb18abf5a359a0a9af470b99ff86567494f:70f52637f8f8b97d5f7d3b37034e

71f6d009270d39fcda87ceb3bd55b626650a:fe149351d2dedcde0140ed4e353c

ef6a64505bfc132f3bbfe1d9b5de7bda5d28:ecf5ee72aae6b2cd65b105abfacb

4522ee2fc5c23d56f2a60290000dd6588552:98724cf65912b6c1974538624e58

7eb18abf5a359a0a9af470b99ff86567494f:8a053e1df14b0194232d240a4ea4

67c70b2f6d46d6e6d4410d343209d974c3d6:72cda4bee62a07fab89a32f78180

c3ad9d6fb34cf858b11987a29f4254716e0a:3a34ebc93162cb85645d65e3ba26

fb3a037baa97b36dbf4d312c50d1e1570a1

File Hashes

File Name	Hash / Description
Statements05122025.exe	SHA256: c1adb081862b983b67412fd91f389818106fde23e09fd203642de1bfc4cebad1
[Unknown]	SHA256: 23dc523bb403bac58750fec94c6ab8e18e6fe768a8235a790f1dbd90a321e7a3
[Unknown]	SHA256: de066fe772bc64886dc0487efa6de729f128bacbfcb351cfedec2d0a549173c1
[Unknown]	MD5: e230bf859e582fe95df0b203892048df
Monitor	[Unknown]
[Unknown]	MD5: f782c936249b9786cc7fac580da3ae0f
[Unknown]	MD5: 322a92b443faefe48fce629e8947e4e2

Get updates from Cloudforce One

[Subscribe](#)