VALIDATION REPORT

CASE STUDY #003

Entity Category:

Online Learning Platform — Confirmed Impersonation

Submission Type:

Fake Sponsorship Offer with Malware Contract Link

This session was initiated upon receiving an unsolicited sponsorship email claiming to be from a globally recognized online learning platform. The email offered a $1,000 brand integration deal and directed the recipient to sign a contract through an unverified link — with the instruction that signing is only available on Windows. VASD flagged this in Layer 1. Layer 3 confirmed it. Entity names are withheld from public distribution.

DATE	ANALYST	SYSTEM	VERDICT
MAY 2026	VELURYN AGNECY	VASD v1.0	HIGH RISK — MALWARE

velurynandoc@gmail.com

SECTION 00

OPENING STATEMENT

The most dangerous emails are the ones that look the most real. Not because the deception is perfect — but because the brand being used is. A globally trusted name lowers every defence. That is the point. The scammer does not build credibility. They borrow it.

This email used the name, tone, and offer structure of a real, internationally recognized online learning platform. The integration brief was accurate. The pricing was realistic. The payment terms were standard. Everything was designed to pass a casual read. One line was not.

The signing process is only available on Windows.

No legitimate contract platform restricts signing to a single operating system. DocuSign works on any device. HelloSign works on any device. Adobe Sign works on any device. A Windows-only restriction is not a technical limitation. It is a delivery condition for a file that requires a Windows environment to execute.

> *"The danger is not in what they ask you to sign. It is in what the signing process installs on your machine."*

— Core finding, Layer 1.

SECTION 01

LAYER 1 — INITIAL SCREENING

Layer 1 failed this email on the first substantive signal examined. Everything after that is documentation of how far the deception was built.

SIGNAL	FINDING	STATUS
Windows-Only Contract Signing	The email states the contract signing process is only available on Windows. No legitimate legal signing platform — DocuSign, HelloSign, Adobe Sign, PandaDoc — restricts access by operating system. This is a malware delivery condition. The 'contract' is almost certainly an executable file designed to run on Windows.	✕ HIGH RISK
Recipient Name	The email is addressed to 'Andy.' If this was sent to someone whose name is not Andy, it is a mass-send with variable injection that failed — confirming automated bulk distribution, not a genuine individual outreach.	✕ HIGH RISK
Contract Link Hidden	The contract URL is not shown in the email body — replaced with asterisks. A legitimate sponsorship contract is sent via a named, trusted platform with a visible link. Concealing the destination is standard phishing practice.	✕ HIGH RISK
Sender Domain Unknown	No sender email address domain was provided for verification in the submitted email. Legitimate brand deal emails come from a verified corporate domain. Absence of this information is itself a flag at Layer 1.	■ FLAGGED
Tone Consistency	The email reads as professionally structured and warm. Tone and content are consistent with real sponsor outreach. This level of polish is deliberate — designed to delay scrutiny.	■ FLAGGED

LAYER 01 VERDICT	INITIAL SCREENING
HIGH RISK — Windows-only contract signing is a confirmed malware delivery pattern. Session escalated immediately.	

When a single signal is severe enough, VASD does not wait for Layer 2. The Windows-only signing instruction ended the surface review. The remaining layers exist to document the full scope of the threat.

SECTION 02

LAYER 2 — REAL-WORLD PRESENCE

Layer 2 examined the brand being impersonated. The platform is real. The email is not from them.

SIGNAL	FINDING	STATUS
Platform — Verified Real	The online learning platform referenced in this email is a legitimate, internationally operating company with millions of users, verified social presence, and a long-standing domain history.	✓ CLEAR
Official Domain Verified	The platform operates from a registered, long-standing corporate domain. All legitimate outreach from this company originates from that domain exclusively.	✓ CLEAR
Official Scam Alert — Published	The platform has published an official help center article specifically warning creators about fake sponsorship emails using their brand name. The article describes the exact pattern used in this email: friendly outreach, a deal offer, and a link or file designed to steal information or compromise accounts.	✕ HIGH RISK
Sender Domain — Not Verified as Official	The email submitted for this session did not include a visible sender domain from the platform's official corporate address. The impersonation uses the brand name without using the brand's verified infrastructure.	✕ HIGH RISK

LAYER 02 VERDICT	REAL-WORLD PRESENCE
HIGH RISK — Brand confirmed real. Email confirmed not from them. Official scam warning found.	

OFFICIAL CONFIRMATION

Scam confirmed by the impersonated brand itself.

The real organization has published an official help center article specifically warning creators about this email pattern. The scam is documented, named, and actively reported. This is not an inference. This is a confirmed impersonation campaign.

SECTION 03

LAYER 3 — DEEP VERIFICATION

Layer 3 examines the mechanism. Not just what the email claims — but what following its instructions would actually do to the recipient.

SIGNAL	FINDING	STATUS
Malware Delivery Mechanism	Windows-only contract links in creator outreach emails are a documented attack vector. The recipient is directed to download and open a file — typically disguised as a PDF or .docx — that executes a payload on Windows. Common outcomes: keylogger installation, credential harvesting, remote access trojan (RAT) deployment, or ransomware staging.	✕ HIGH RISK
Financial Data at Risk	A creator who proceeds and enters banking details for the 50% prepayment on the fraudulent platform submits financial information directly to the attacker. No prepayment will arrive. The data will be used or sold.	✕ HIGH RISK
Credential Harvesting Risk	If the contract link routes through a login page mimicking the real platform, the creator's account credentials are captured. Account takeover enables further attacks on the creator's audience.	✕ HIGH RISK
Scale of This Scam	The impersonated platform has escalated its public warning to a dedicated help center article, indicating the volume of reports received is significant. This is not a targeted attack. It is a widespread automated campaign against creators.	✕ HIGH RISK
50% Prepayment Promise	Promising payment after signing is a standard trust-building device in creator scams. It removes the financial suspicion. No money ever arrives — only the consequences of what was signed or downloaded.	■ FLAGGED

LAYER 03 VERDICT	DEEP VERIFICATION
HIGH RISK — Confirmed malware delivery architecture. Financial, credential, and device risk to recipient.	

SECTION 04

FINAL JUDGMENT

VERDICT: HIGH RISK — MALWARE

This email is not from the platform it claims to represent.

It is a confirmed impersonation campaign — documented by the real platform in an official public warning. The email uses accurate brand details, a realistic offer, and professional language to lower the recipient's guard before directing them to a Windows-only contract signing process.

That instruction is not a platform limitation. It is a delivery condition for malicious software.

A creator who follows the instructions in this email risks: device compromise through malware execution, financial data theft through a fraudulent payment portal, credential harvesting through a spoofed login, and account takeover with downstream impact on their audience.

None of these outcomes require the creator to do anything unusual. They only require the creator to trust the brand name in the email. That trust is the weapon.

RECOMMENDATION: Do not click any link in this email. Do not download any file. Do not reply. If you wish to verify whether a sponsorship offer is real, contact the brand directly through their official website — not through any contact information provided in the email. Report the email to the platform's official support. If any file from this email was already opened on a Windows machine, disconnect from the internet and run a full malware scan immediately.

LAYER SUMMARY

LAYER	NAME	FLAGS	RESULT
01	Initial Screening	5	HIGH RISK
02	Real-World Presence	2	HIGH RISK

03	Deep Verification	5	HIGH RISK
FINAL	**Combined Judgment**	12	HIGH RISK — MALWARE

SERIES COMPARISON

CASE	CATEGORY	TYPE	VERDICT
#001	Leadership & Coaching Platform	Credibility inflation	SUSPICIOUS
#002	Creator Affiliate Network	Labor extraction	HIGH RISK
#003	Online Learning Platform	Malware via contract link	HIGH RISK — MALWARE

This report was produced by VELURYN AGNECY — VASD Division. For inquiries: velurynandoc@gmail.com