

Kali365: Anatomy of a Microsoft 365 Phishing-as-a-Service Kit – From Telegram Hype to FBI Takedown Theater

By Trevor Hilligoss

Published: 2026-06-11 · Archived: 2026-08-06 02:02:01 UTC

The operators of Kali365 maintain an active marketing Telegram channel which has actively posted about the kit and advertised its features, including in this post first seen on **12 March 2026**:

Recaptured conversation

Telegram · direct message

▶ RECAPTURED

FROM Deleted Account · unknown · ID 0	TO Kali365 (@kali365_Link) · user · ID 5232348929
SOURCE Telegram · channel advertisement	SENT · SCRAPED (UTC) 2026-03-17T18:25:35Z 2026-03-18T00:26:52Z

U

User 0

🔥 Kali365 — Device Code Phishing Panel

👤 Why It's Dangerous

🎯 Victim logs in on [microsoft.com](#) itself — real domain, real SSL, zero suspicion 🔒
Bypasses MFA automatically — the user completes MFA for you on Microsoft's real page 🤪 No cookies that expire — you get OAuth refresh tokens that last months 🛡️
Undetectable landing pages — 12 pixel-perfect designs (OneDrive, Teams, SharePoint, DocuSign, Adobe, Voicemail...) ⚡ 5 attack flows in one lure — device code, cookies, device→cookies, cookies→device,

🧠 Post-Capture Superpowers

Full inbox access — read, search, reply, forward, delete — all from the browser 📧

🦾 Stealth Mode 🚫

Suppress security alerts — auto-deletes MFA notifications, password change emails, sign-in warnings before the victim sees them

🔗 Contact harvester — extracts every email from contacts

B2B sender

Cookies link

Device code link

Extractor

Sorter

All in one

Dm [@kali365_Link](#)

18:25

🔒 This conversation was recaptured — read only

➤

Notably, Kali365 advertised two phishing methods that are [purpose-built to defeat MFA](#): Adversary-in-The-Middle (AiTM) and Device Code phishing:

The earliest branded capture (February 15, 2026) shows the cookie-theft side plainly (victim redacted):

SESSION CAPTURED - Kali365

 Email: <redacted>
 Password: <redacted>
 Cookies: 9 captured

 Domain: test.ginxp11.uk

SpyCloud's continuous recapture of dark web and criminal ecosystem data reveals a highly active affiliate base, with thousands of successfully phished victims identified during the kit's three-plus months of operation, intelligence that would otherwise remain invisible to defenders.

In the graph below you can see an immediate adoption of AiTM capabilities after the February release, followed by a shift in favor of device code phishing beginning in March and reaching its zenith at the end of the month.

Targeting and demographics. Captured victims skew toward **small/mid businesses** (construction, scaffolding, fuel, manufacturing, professional services), replicating the classic invoice/BEC target profile. Some very large businesses were also found within the victim data; however, exposure to large companies is mostly due to communication with compromised mailboxes, especially those of [suppliers or partners](#).

Geography (victim login country, from the kit's geo-IP):

Verticals (domain-name heuristic + top victims); clearest concentrations in:

01

The vertical mix (construction, manufacturing, professional services, energy) is exactly the invoice/payment-heavy economy, and it lines up with the kit's built-in keyword-monitoring (invoice, payment, proposal, wire).

02

Nonprofits, faith-based orgs, school districts, and small local governments (tend to have weaker MFA/security, real payment flows) show up across the entire lifespan of the kit.

03

Many domains show multiple distinct compromised mailboxes (3+ per org for several; double-digits for the top nonprofits), consistent with the kit's contact-harvester and intra-org expansion.

04

Compromised mailboxes are reused to attack the victim's own contacts/customers (reply-chain hijacking, the bank-detail-change BEC emails we observed) so that each org victim is also a launch point against its partners (secondary victims).

05

Compromised mailboxes enable persistent monitoring of email communications from suppliers, partners, and customers. Even organizations that weren't compromised can still be exposed by way of communicating with a compromised mailbox.

06

Because Kali365 captures session cookies and OAuth refresh tokens, not passwords, standard MFA provided no protection for these victims. These are session/refresh-token captures; the victims had logins that "worked," so notification + token/session revocation (not just password resets) is the [required remediation](#).

Timelining major milestones

Timelining the major milestones in Kali365's short existence (so far) shows an aggressive iteration process that has been remarkably reactive to defensive shifts by Microsoft and others.

The major changes:

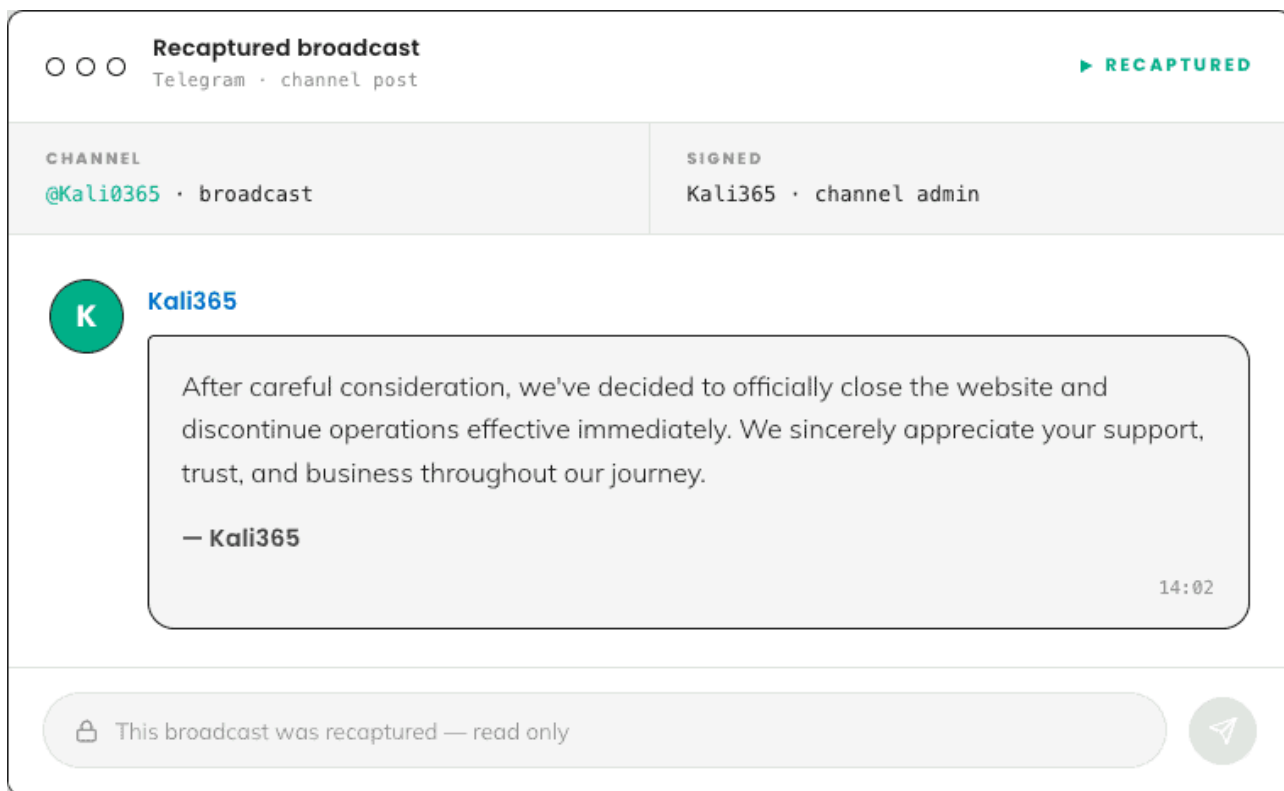
For a kit that wouldn't even be eating solid foods if it were a human baby, it's had quite a few big events since its February birthdate.

The migration (May 7-8)

At ~18:00 UTC on May 7, 2026, Kali365 notified all customers that the PhaaS kit was moving operations to blackoctopusking.live, providing the excuse of seeking "more anonymous infrastructure" as the reason for the shift, and apparent rebrand (foreshadowing). This action effectively retired their previously-used domains octopi365.com / kali365.xyz and related infrastructure.

The FBI bulletin and the "shutdown" (May 21)

The FBI issued a public service announcement via the Internet Crime Complaint Center ("IC3") on May 21, which named Kali365 as a PhaaS targeting Microsoft 365 Access Tokens. The operators **reposted the PSA into their own channel** and, **13 seconds later**, seemingly announced their retirement:



So, you may be asking: *why are we taking the time to share this research, if the devs are retired and the kit is effectively dead?*

The rebrand

SpyCloud’s analysis of messages between customers revealed that the “Octopus” brand was actually in use for some time *prior* to the attempted rebrand. On May 12, one customer publicly referred to the Electron-based Outlook app as “greenoctopus,” and on May 14, the source code for the panel was quietly updated from Kali365 Live to Green Octopus 3.1.0.

Notably, beyond a few cosmetic changes, the infrastructure largely remained the same. Existing customers were advised to log in with their existing usernames and passwords, and were informed that their tokens and captures had been seamlessly migrated. The operators even claimed that linked Cloudflare workers (lures) would still work post-migration.

While AiTM phishes **dropped by about 34%** post rebrand, device code phishes climbed again, peaking around mid-May at roughly half their late-March high. Taken together, the left and right sides of the graph above are effectively indistinguishable (given the inherently spiky nature of successful phishes), and Pam from The Office would be excused for thinking they were the same picture (*may be a deep-cut for some*).

Given all this, we assess this “rebrand” was less a stealthy move to escape scrutiny than the cyber equivalent of a fugitive dyeing their hair and changing clothes while leaving a face tattoo in plain sight: the panel got a new domain and an octopus paint job, but the kali365-live user-agent, the “Kali365 Team” sign-off, and the same operators, accounts, lures, and wallets never changed, and the octopus theme (octopi365) predated the “new” brand anyway.

Based on SpyCloud's observability into the operators and operations of the Kali365 kit, we can paint a rough picture of the likely user base and targeting methodologies of the kit.

During the first full month of operation, the customer base soared from zero to approximately **300 by the end of March**, with that number increased to **at least 500 distinct affiliate operators** with active Kali365 subscriptions by the beginning of May.

Considering Kali365's observed subscription price (\$250/30 days) and an operating window of roughly February-June 2026, we estimate the operator(s) earned on the order of \$200K–\$350K USD in subscription revenue since launch. Blockchain tracing of the payment wallets they advertised to customers corroborates that range and, if anything, pushes it toward the top end.

The advertised BTC and USDT addresses resolve to a single, interconnected cluster (the wallets transact with one another and consolidate into shared cash-out points), and they were funded by hundreds of distinct paying counterparties. Inbound payments were overwhelmingly USDT on Tron, concentrated in March–May 2026 and peaking in May, precisely matching the kit's growth curve and a monthly-renewal model.

On the outflow side, the cluster consolidated and cashed out through mainstream centralized exchanges – a single primary USDT consolidation wallet alone routed roughly \$128K off-chain – and a meaningful share of inflows traced to a flagged money-laundering service, situating Kali365's proceeds within a known illicit-finance network. Notably, the operator's longest-lived Bitcoin cash-out address shows ~1.3 BTC (comfortably six figures) moving through it since 2024, predating Kali365 itself, a marker of the broader, longer-running fraud income that sits on top of the subscription business.

None of these figures include deposit addresses presumably shared in private customer DMs, nor the proceeds of the actor's own hands-on phishing and Business Email Compromise (BEC), so all of the above should be read as a floor.

Most importantly, Kali365's affiliates are not loyal to any single kit. The same actors run Kali365 side-by-side with rival PhaaS panels – [Tycoon 2FA](#), Kratos, Nova, and generic AiTM/"Microsoft" kits – often in parallel. In practice, an affiliate treats these kits as interchangeable tools in one workflow: whichever panel best fits the target, be it AiTM cookie theft, OAuth device-code, or straight [credential capture](#), feeds the same operator's pipeline and the same downstream fraud (BEC, mailbox monetization).

This ecosystem behaves less like a set of isolated buyers and more like a loose collective: reseller sub-tiers (a single subscriber reselling access to a dozen-plus of their own sub-clients), shared, kit-provided lure infrastructure (e.g., Cloudflare Workers), referral programs, and pooled results pipelines; structurally similar to the way "traffer" teams band together to share infrastructure, access, and proceeds.

The Kali365 shutdown announcement bought the operators a news cycle and cost them nothing. Captures kept landing, the panel kept its user-agent, the wallets kept consolidating, and the only thing that really changed was the paint job.

What persists following this faux retirement is the capability and the people running it. The same affiliates rotate between Kali365, Tycoon, and whatever launches next, feeding the same BEC pipeline regardless of the logo on the panel or username of the person selling it.

Because Kali365 steals session tokens that persist independently of credentials, password resets are ineffective for remediation. Effective response requires explicit session revocation, token invalidation, and MFA re-enrollment. Teams that prioritize visibility into exposed device code grants and anomalous token activity over simple password resets have a better chance of preventing and mitigating these threats.

SpyCloud helps enterprises worldwide protect billions of accounts and stop identity-driven attacks before they start. To see insights on your organization's exposed data, check your exposure now.

Source: <https://spycloud.com/blog/kali365-anatomy-of-a-microsoft365-phishing-as-a-service-kit/>