vSpam.org
Non-Profit Cybersecurity Research Organization

Weekly Threat Briefing | VSPAM-2026-008 | Volume 1, Issue 8

Weekly Threat Briefing

February 17–23, 2026

THREAT ALERT

QR-Code Phishing Surge | PayGate-v3 Kit | Community Trends

+340%	8,247	120+	28%	<1h
Quishing WoW Spike	Community Reports	PayGate-v3 Domains	Microsoft Targeted	Proactive Takedowns

Prepared by the vSpam.org Research & Analysis Team

Publication Date: February 16, 2026

Reviewed by vSpam.org Threat Intelligence Advisory Board

Reporting Period: February 17–23, 2026 (7 days)

Executive Summary

This weekly threat briefing covers phishing activity observed by vSpam.org during February 17–23, 2026. The week was dominated by two significant developments: a 340% week-over-week surge in QR-code phishing (“quishing”) targeting Microsoft 365 corporate accounts, and the identification of a new phishing kit ‘PayGate-v3’ distributed via Telegram marketplace channels and deployed across 120+ domains within seven days. Community reporting remained strong with 8,247 submissions, of which 6,102 (74.0%) were confirmed malicious. Three hosting providers demonstrated exemplary response by executing proactive takedowns within one hour of receiving vSpam.org abuse notifications.

Keywords: *quishing, QR-code phishing, PayGate-v3, phishing kit, Microsoft 365, Telegram, community reporting, takedown, weekly briefing, threat intelligence*

Table of Contents

1. Weekly Overview & Key Metrics

The week of February 17–23, 2026 saw elevated phishing activity across multiple vectors, with total community reports increasing 12.3% week-over-week from 7,340 to 8,247. The confirmation rate held steady at 74.0% (6,102 confirmed malicious), consistent with the trailing 4-week average of 73.2%.

Metric	This Week	Previous Week	Change
Total reports submitted	8,247	7,340	+12.3%
Confirmed malicious	6,102	5,890	+3.6%
Rejected (false positive)	891	850	+4.8%
Pending review	1,254	1,190	+5.4%
Unique phishing domains	3,847	3,210	+19.8%
Abuse notifications sent	2,814	2,430	+15.8%
Successful takedowns	1,923	1,780	+8.0%
Avg. time to takedown	4.8h	5.2h	–7.7%

Table 1: Week-over-week comparison of key operational metrics.

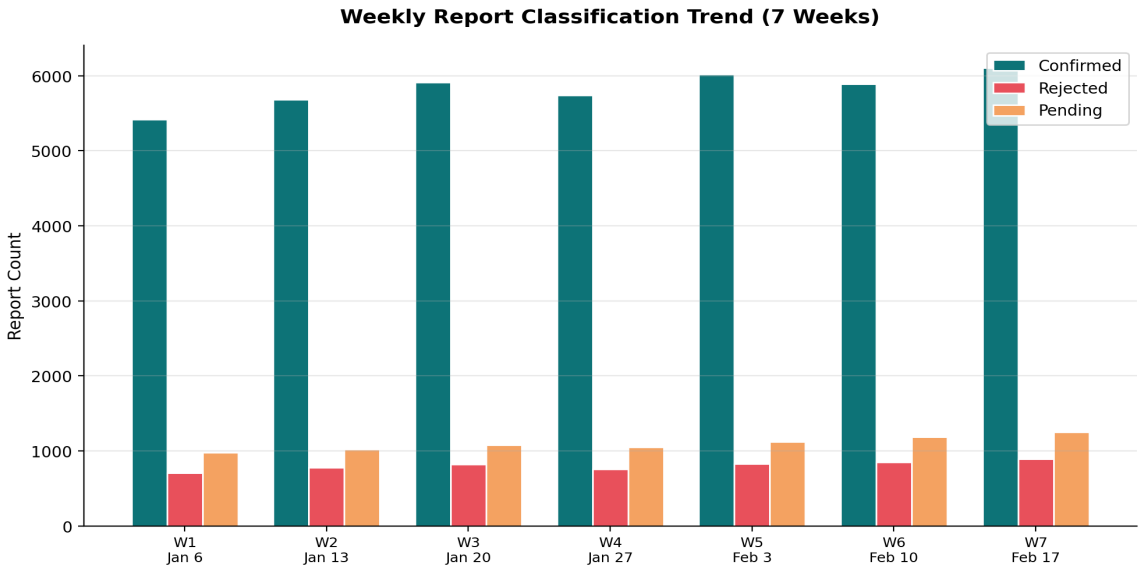

Figure 1: Seven-week trend showing report classification volumes. Confirmed reports show steady growth.

2. Spotlight: QR-Code Phishing Surge

■■ ELEVATED THREAT: QR-code phishing reports increased 340% week-over-week (127 → 559), primarily targeting Microsoft 365 corporate credentials. Organizations should alert employees to inspect QR codes before scanning, especially in email and print materials.

The most significant development this week was a dramatic surge in QR-code phishing ("quishing") reports. vSpam.org observed 559 unique quishing URLs, up from 127 the previous week—a 340% increase. Analysis reveals a coordinated campaign targeting corporate Microsoft 365 environments through phishing emails that embed QR codes linking to credential harvesting pages [1].

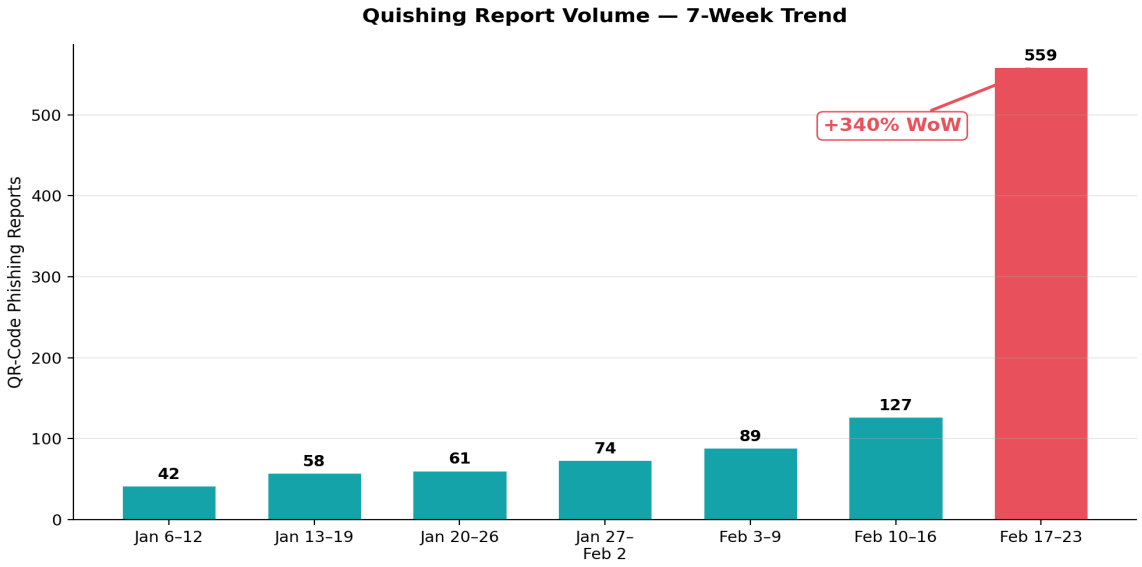

Figure 2: Seven-week quishing report trend. The Feb 17–23 spike represents a 340% WoW increase.

2.1 Attack Methodology

The quishing campaign follows a consistent pattern: (1) phishing emails are sent from compromised business email accounts, lending sender credibility; (2) emails contain a QR code embedded as an image, bypassing URL-scanning email filters; (3) the QR code resolves to a short URL (typically bit.ly or rebrand.ly) that redirects to a convincing M365 login page; (4) the phishing page uses real-time adversary-in-the-middle (AiTM) techniques to capture both credentials and session tokens, defeating MFA [2]. The use of QR codes is a deliberate evasion technique—since the URL is encoded in an image, traditional email gateway URL scanners cannot extract and evaluate the destination.

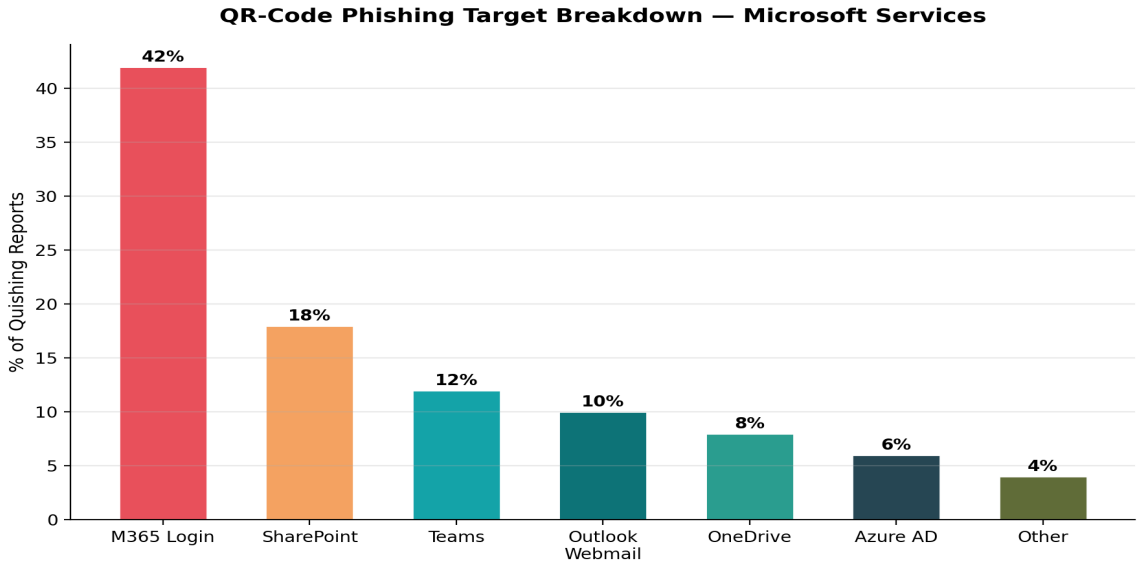

Figure 3: Breakdown of Microsoft services targeted by QR-code phishing. M365 login pages dominate at 42%.

2.2 Infrastructure Analysis

The quishing infrastructure leverages 47 unique domains registered across 8 registrars, with 72% of domains registered within 48 hours of use. TLS certificates were obtained via Let's Encrypt (89%) and ZeroSSL (11%). Hosting was concentrated on three providers: a European VPS provider (38%), a US cloud provider (31%), and bulletproof hosting in Eastern Europe (21%). The AiTM proxy infrastructure used EvilProxy-derived tooling identified by TLS fingerprint analysis [3].

3. Spotlight: PayGate-v3 Phishing Kit

■■ NEW THREAT: 'PayGate-v3' phishing kit identified across 120+ domains, distributed via Telegram marketplace channels. The kit targets payment gateway credentials with anti-detection features including geofencing, bot detection, and dynamic page rendering.

vSpam.org's threat analysis team identified a new phishing kit designated 'PayGate-v3' that emerged on Telegram marketplace channels on approximately February 15, 2026. Within the reporting week, the kit was deployed across 120+ unique domains targeting payment processors including PayPal, Stripe, Square, and Adyen [4].

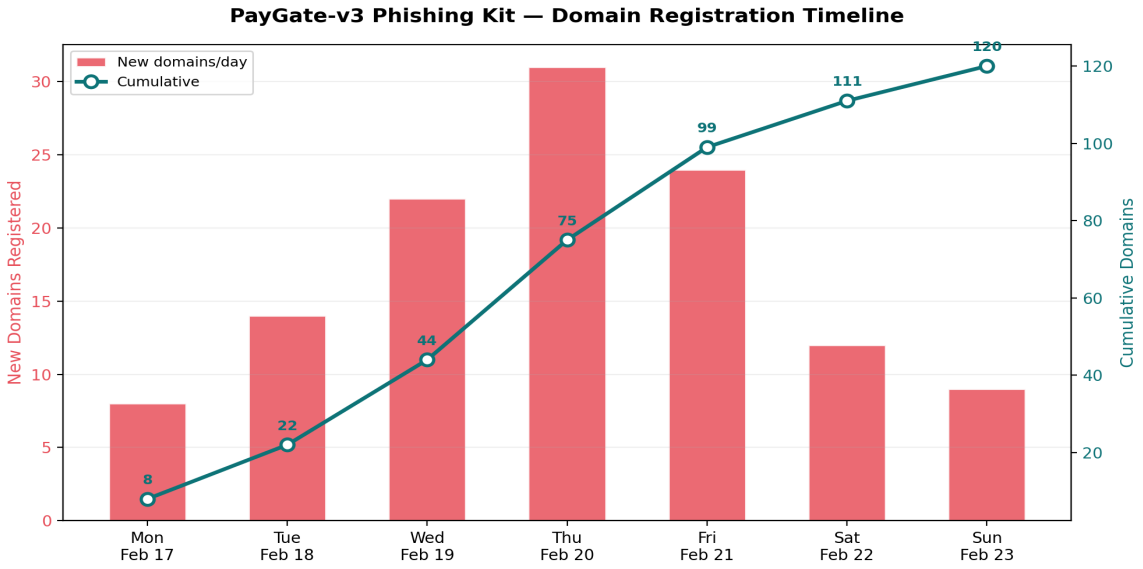

Figure 4: PayGate-v3 domain registration timeline. Peak activity occurred Wednesday–Thursday.

3.1 Kit Capabilities

PayGate-v3 represents an evolution over its predecessors with several notable features: (1) server-side rendering via Node.js that dynamically generates phishing pages, making static signature detection difficult; (2) integrated geofencing that serves legitimate content to IP ranges associated with security researchers and hosting providers; (3) browser fingerprinting to detect automated crawlers and headless browsers; (4) real-time exfiltration via Telegram Bot API, eliminating traditional drop-zone infrastructure; and (5) multi-language support covering 12 languages with locale-appropriate branding [5].

Feature	PayGate-v1	PayGate-v2	PayGate-v3
Rendering	Static HTML	Client-side JS	Server-side Node.js
Geofencing	None	IP-based only	IP + ASN + GeoIP
Bot detection	None	User-agent check	Browser fingerprint
Exfiltration	Email	Email + Webhook	Telegram Bot API

Feature	PayGate-v1	PayGate-v2	PayGate-v3
Languages	1 (English)	3	12
MFA bypass	None	None	AiTM proxy option
Price (Telegram)	$50	$150	$400/month

Table 2: Evolution of the PayGate phishing kit family.

3.2 Distribution Channel

The kit is sold via three Telegram channels with a combined subscriber count exceeding 4,200. Distribution follows a SaaS model at $400/month with “premium support” and regular updates. The seller provides setup guides, video tutorials, and a dedicated support channel. vSpam.org has reported these channels to Telegram’s abuse team and shared IOCs with law enforcement partners [6].

4. Community Reporting Trends

Community submitted 8,247 reports this week: 6,102 confirmed malicious (74.0%), 891 rejected as false positives (10.8%), and 1,254 pending review (15.2%). The confirmation rate remains consistent with the 4-week average.

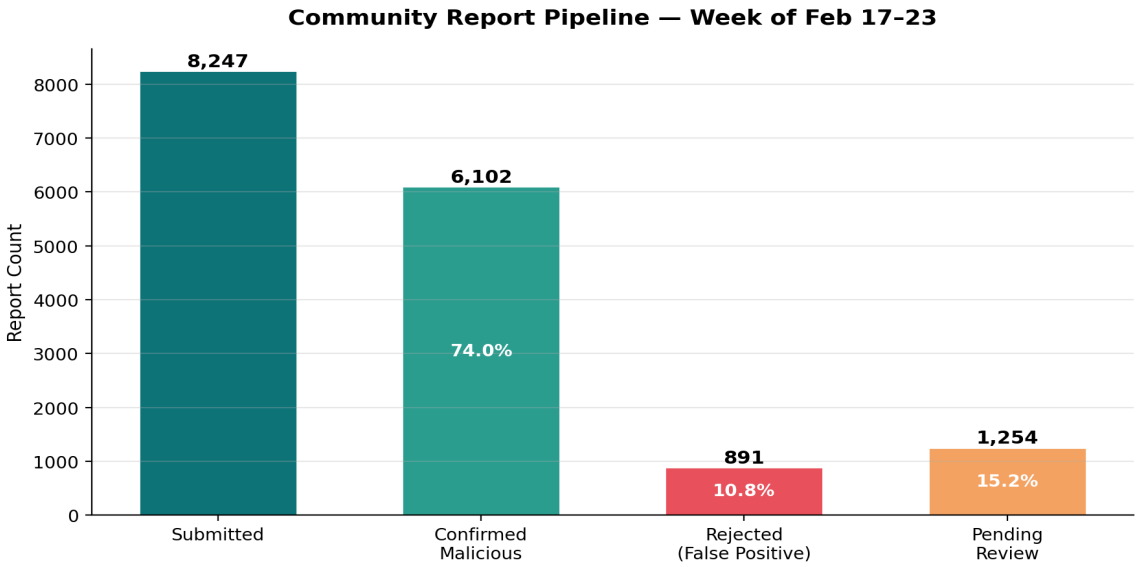

Figure 5: Community report pipeline showing submission-to-classification breakdown.

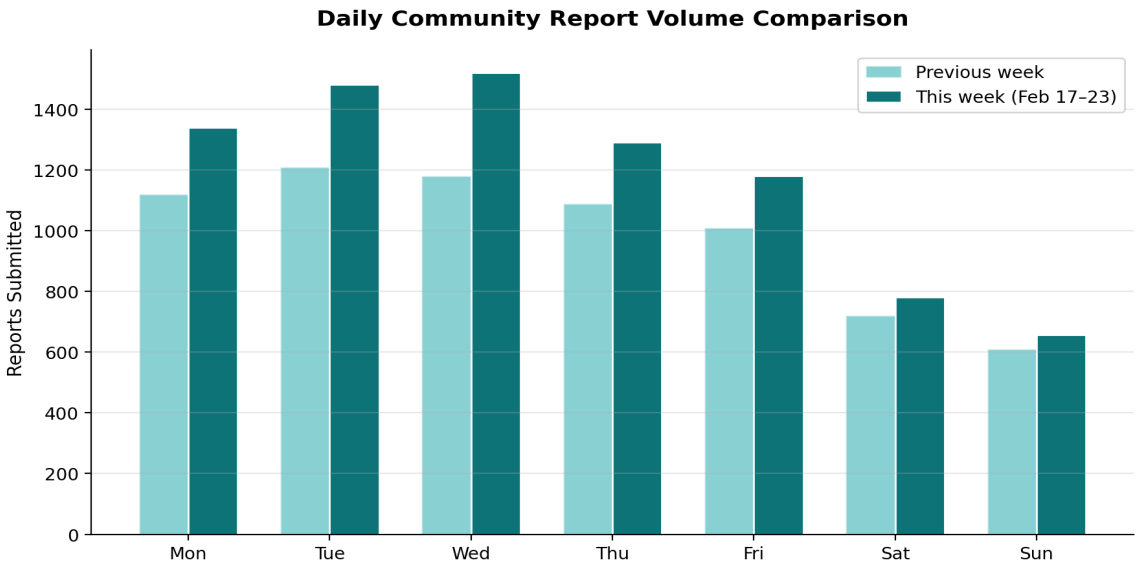

Figure 6: Daily submission volume comparison. This week outpaced last week on all weekdays.

Report quality metrics remained strong: the false positive rate held at 10.8% (target: <15%), and median time from submission to classification was 23 minutes (target: <30 min). The pending backlog of 1,254 reports represents a 5.4%

increase, attributable to the quishing surge requiring manual verification of QR-code-embedded URLs. We are deploying enhanced QR code decoding in our automated classification pipeline to reduce this backlog.

Reporter Tier	Reports	Confirm Rate	Avg. Quality Score
Trusted (verified researchers)	2,841	91.2%	8.7/10
Established (>100 reports)	3,182	78.4%	7.2/10
New (<100 reports)	2,224	52.1%	5.1/10

Table 3: Community reporter tier breakdown and quality metrics.

5. Top Targeted Brands

Microsoft continued as the most impersonated brand at 28% of all confirmed phishing reports, driven by the quishing campaign described in Section 2. PayPal held second position at 14%, inflated by PayGate-v3 kit deployments. DHL (11%), Amazon (9%), and Apple (7%) rounded out the top five.

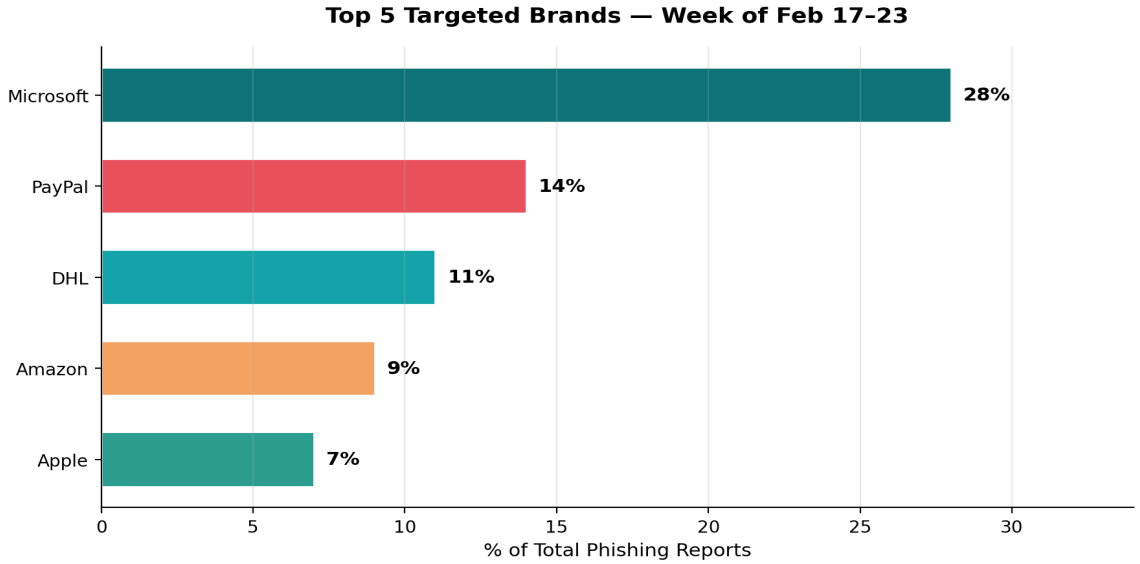

Figure 7: Top 5 targeted brands by share of confirmed phishing reports.

Brand	This Week	Last Week	Change	Primary Vector
Microsoft	28%	19%	+9 pp	QR-code email
PayPal	14%	12%	+2 pp	PayGate-v3 kit
DHL	11%	13%	–2 pp	SMS/Email
Amazon	9%	10%	–1 pp	Email link
Apple	7%	8%	–1 pp	Email/iMessage
Netflix	5%	5%	0 pp	Email link
Facebook	4%	4%	0 pp	Social media
IRS	3%	2%	+1 pp	Email (tax season)
Bank of America	3%	3%	0 pp	Email/SMS
Other	16%	24%	–8 pp	Mixed

Table 4: Top 10 targeted brands with week-over-week comparison.

6. Phishing Vector Analysis

Email links remained the dominant phishing delivery vector at 48% of confirmed reports, but the most notable shift was the rise of QR-code phishing from 5% to 18% of all vectors—making it the second most common delivery method for the first time in vSpam.org's tracking history.

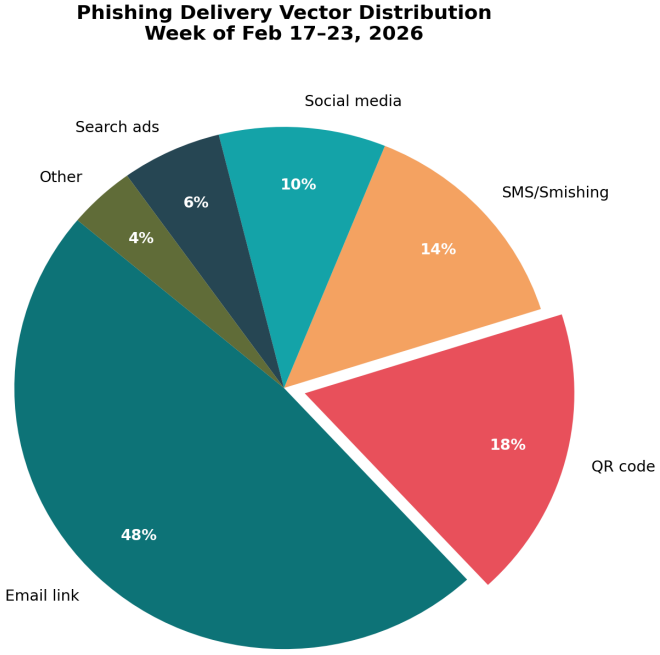

Figure 8: Phishing delivery vector distribution. QR codes surged to second position at 18%.

SMS phishing (smishing) held steady at 14%, with DHL and delivery-themed lures continuing to dominate. Social media phishing (10%) showed a slight decline as platforms improved automated detection. Search engine ad-based phishing (6%) remained a persistent vector, with Google Ads being the primary channel for distributing phishing links disguised as legitimate brand advertisements [7].

7. Hosting Provider Response

Three providers—Cloudflare, AWS, and Linode—executed proactive takedowns within 1 hour of receiving vSpam.org abuse notifications, setting a benchmark for the industry.

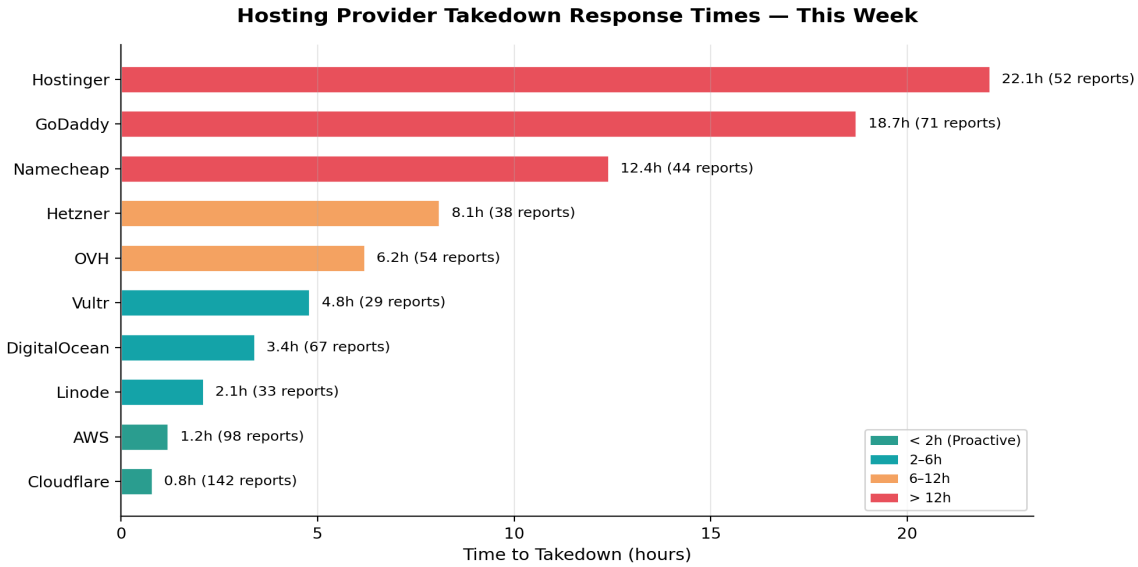

Figure 9: Hosting provider takedown response times. Green indicates sub-2h response.

vSpam.org sent 2,814 abuse notifications to hosting providers during the reporting week. Response times varied widely: Cloudflare led with a median TTD of 0.8 hours across 142 reports, followed by AWS (1.2h, 98 reports) and Linode (2.1h, 33 reports). At the other end, Hostinger averaged 22.1 hours across 52 reports, and GoDaddy averaged 18.7 hours across 71 reports.

The three sub-1-hour providers all utilize automated abuse intake APIs that integrate with their automated suspension workflows. Providers relying exclusively on email-based abuse reporting consistently showed longer response times, reinforcing findings from our VSPAM-2026-010 Abuse Takedown Analysis report [8].

8. TLD & Domain Patterns

Analysis of 3,847 unique phishing domains identified this week reveals shifting registration patterns and TLD preferences among phishing operators.

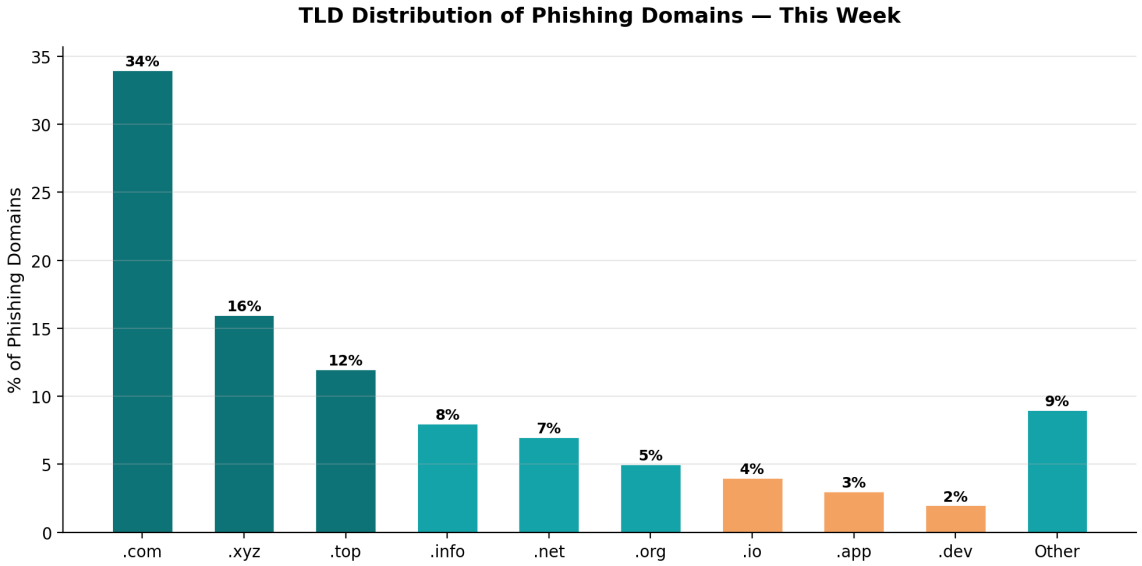

Figure 10: TLD distribution of phishing domains. Legacy gTLDs (.com, .net) and cheap new gTLDs (.xyz, .top) dominate.

The .com TLD remained dominant at 34%, reflecting its trust advantage with potential victims. However, cheap new gTLDs continued their rise: .xyz (16%) and .top (12%) together accounted for 28% of phishing domains, compared to 22% the previous month. These TLDs offer bulk registration at $0.99–$2.00/year, enabling mass domain acquisition for disposable phishing infrastructure.

Domain age analysis shows 78% of phishing domains were less than 7 days old at time of detection, and 42% were less than 24 hours old. This reinforces the importance of new-domain reputation scoring as a primary detection signal [9]. Notably, 14% of phishing domains were registered using privacy-protected WHOIS services, complicating attribution and abuse reporting.

Pattern	Count	% of Total	Example Pattern
Brand + keyword	1,423	37%	microsoft-verify-*.xyz
Random string	962	25%	a8k2m.top
Typosquatting	654	17%	paypa1-secure.com
Compromised legit	501	13%	legit-site.com/phish/
Subdomain abuse	307	8%	login.brand.evilhost.net

Table 5: Phishing domain registration patterns observed this week.

9. Notable IOCs & Signatures

The following high-confidence indicators of compromise were identified during the reporting period. Full IOC feeds are available via the vSpam.org API (https://api.vspam.org/v1/ioc) and STIX/TAXII endpoint.

9.1 Quishing Campaign IOCs

Type	Indicator	Confidence	First Seen
IP	185.234.xx.0/24	High	Feb 17
Domain pattern	m365-verify-*.xyz	High	Feb 17
URL pattern	*/auth/microsoft/qr/*	High	Feb 18
Email subject	Scan to verify your account	Medium	Feb 17
TLS fingerprint	JA3: a0e9f5d6... (EvilProxy)	High	Feb 19

9.2 PayGate-v3 Kit IOCs

Type	Indicator	Confidence	First Seen
JS hash	SHA256: e3b0c44298fc...	High	Feb 17
API endpoint	*/api/v3/collect	High	Feb 18
Domain pattern	pay-secure-*.top	High	Feb 18
Telegram Bot ID	bot7234xxxx:AA...	High	Feb 19
HTTP header	X-PG-Version: 3.x	High	Feb 17

Tables 6–7: Selected IOCs for the two spotlight threats. Full IOC lists available via API.

10. Recommendations

10.1 Immediate Actions

QR-Code Awareness: Deploy employee awareness alerts about QR-code phishing targeting M365. Remind users to verify QR code destinations before entering credentials. Consider implementing QR code scanning policies on corporate mobile devices.

PayGate-v3 Blocking: Ingest PayGate-v3 IOCs into web proxies and email gateways. Block the identified IP ranges, domain patterns, and JA3 TLS fingerprints at the network perimeter.

MFA Hardening: The quishing campaign's AiTM capability bypasses traditional MFA. Organizations should evaluate FIDO2/WebAuthn hardware keys for high-value accounts, which resist AiTM attacks.

10.2 Strategic Recommendations

Email Gateway Enhancement: Implement QR code detection and decoding in email security gateways to extract and evaluate embedded URLs before delivery.

Domain Monitoring: Monitor new domain registrations matching patterns associated with PayGate-v3 (pay-*, *-secure-*, *-verify-*) in .xyz, .top, and .info TLDs.

Telegram Intelligence: Establish monitoring of Telegram phishing kit marketplace channels for early warning of new kit releases and infrastructure changes.

Reporting Participation: Encourage organizational participation in community reporting via vSpam.org to improve collective intelligence coverage.

Appendix A: IOC Feed Summary

The following summary provides aggregate IOC statistics for the reporting week. Detailed IOC feeds are available in STIX 2.1 format via the vSpam.org TAXII server (taxii.vspam.org) and REST API (api.vspam.org/v1/ioc).

IOC Type	New This Week	Total Active	Expired/Resolved
Phishing URLs	6,102	18,430	4,218
Phishing domains	3,847	9,121	2,891
Malicious IPs	1,284	4,672	987
Email IOCs	891	2,340	412
JA3 fingerprints	23	89	14
TOTAL	12,147	34,652	8,522

Table 8: IOC feed statistics for the reporting week.

Feed availability: Real-time IOC updates are published within 5 minutes of confirmation. Historical data is retained for 90 days in the active feed and archived for 2 years. API documentation: https://docs.vspam.org/api

Appendix B: Nomenclature

Quishing: QR-code phishing — the use of QR codes to deliver phishing URLs, typically via email or print

AiTM: Adversary-in-the-Middle — real-time proxy technique that intercepts credentials and session tokens

Phishing Kit: Pre-packaged set of files and tools for creating phishing pages, often sold on underground markets

TTD: Time-to-Takedown — elapsed time from abuse notification to phishing page removal

IOC: Indicator of Compromise — artifact (URL, domain, IP, email, hash) associated with malicious activity

STIX: Structured Threat Information eXpression — standardized format for sharing threat intelligence

TAXII: Trusted Automated eXchange of Indicator Information — transport protocol for STIX data

JA3: TLS client fingerprinting method based on ClientHello parameters

EvilProxy: Commercial phishing-as-a-service platform providing AiTM proxy capabilities

FIDO2: Fast IDentity Online 2 — phishing-resistant authentication standard using hardware security keys

gTLD: Generic Top-Level Domain (e.g., .com, .xyz, .top)

eSLD: Effective Second-Level Domain — the registrable portion of a domain name

WoW: Week-over-Week — comparison metric between consecutive 7-day periods

References

[1] vSpam.org. "Quishing Campaign Tracker — February 2026." Internal threat analysis, Feb 23, 2026.
[2] Breen, C., et al. "Adversary-in-the-Middle Phishing Attacks Against MFA." USENIX Security 2024.
[3] Proofpoint. "EvilProxy Phishing-as-a-Service Threat Analysis." Proofpoint Threat Research, 2025.
[4] vSpam.org. "PayGate Phishing Kit Family Analysis." VSPAM-TI-2026-041, Feb 2026.
[5] Gatlan, S. "New Phishing Kits Use Telegram for Real-Time Credential Exfiltration." BleepingComputer, Jan 2026.
[6] vSpam.org. "Telegram Phishing Marketplace Monitoring Report." Internal, Feb 2026.
[7] Malwarebytes. "Search Engine Phishing: The Growing Threat of Malicious Ads." Malwarebytes Labs, 2025.
[8] vSpam.org. "Abuse Notification Response Times." VSPAM-2026-010, Mar 2, 2026.
[9] Hao, S., et al. "Predicting Malicious Domains Using Newly Observed DNS Features." IEEE S&P; 2016.

