New Automated Phishing Platform Targeting U.S. Microsoft 365 Accounts

TL;DR

A highly automated phishing platform called Quantum Route Redirect is driving large-scale credential theft against Microsoft 365 accounts.

The tool filters out security scanners and directs real users to credential-harvesting sites, allowing low-skill attackers to run advanced campaigns. Activity is active across 90 countries, with the U.S. making up 76% of the victims.

Overview

Researchers at KnowBe4 have identified a new phishing-as-a-service (PhaaS) platform called Quantum Route Redirect (QRR), which allows attackers to launch Microsoft 365 credential theft campaigns. The kit has been active since early August 2025 and is built to automate every step of a phishing operation.

QRR has the ability to automatically distinguish between security scanners and real users. Security tools get redirected to safe, legitimate pages, while human victims are silently funneled to fraudulent Microsoft 365 login pages. This kind of evasion reduces the effectiveness of traditional email filtering and URL scanning.

Affected Platforms

- Microsoft 365 email and identity accounts
- Any environment relying on URL-scanning defenses, SEGs, or cloud-based email security layers

The platform has already been tied to activity across roughly 1,000 domains, with 76% of victims being in the U.S. QRR is designed to run phishing campaigns with minimal technical skill required from the attacker.

Key elements observed in current Quantum Route Redirect activity include:

- Ready-made templates such as DocuSign, payroll, payment alerts, voicemail messages, and QR-code phishing, all leading to fake Microsoft 365 login pages.

- Security scanners are redirected to safe sites, while real users are sent to credential-harvesting pages.

- Automated behavioral checks, fingerprinting, and proxy detection classify traffic without attacker involvement.
- Attackers can track impressions, browser details, and bot-to-human ratios through an interface.
- Campaigns rely on parked or compromised domains with recurring URL patterns to increase legitimacy and reduce detection.

Quantum Route Redirect slips past the tools most companies lean on (URL checks, email filters, and link scanning) and shows the real phishing page only to the user. That's why it's driving so many credential theft attempts right now. As long as attackers keep getting results from kits like this, we should expect more of it. To cut down on the chances of a successful attack, take a look at Aspire's recommendations below.

Aspire Protects

- Use layered email security and make sure your tools inspect message content, sender behavior, and URLs both before delivery and at time-of-click.
- Keep MFA enforced everywhere.
- Look for impossible travel, unusual devices, and sudden session changes tied to Microsoft 365 accounts.
- Limit sign-ins by location, device type, and session risk inside Microsoft Entra.
- Have a credential-compromise plan ready. Be able to isolate the user, revoke tokens, reset credentials, and review activity quickly.
- DocuSign requests, payroll changes, payment alerts, voicemail messages, and QR codes should be treated with caution. Train your staff on how to spot lures associated with this campaign.

TTPs to Watch

Initial Access

- Phishing [T1566] – The attacker may have sent a lure using DocuSign, payroll, payment alerts, voicemail emails, or QR codes to push the user toward a Quantum Route Redirect link.

Credential Access

- Web Credential Harvesting [T1056.003] – The attacker may direct the user to a fake Microsoft 365 sign-in page to capture credentials.

Defense Evasion

- Traffic Filtering [T1020] – The attacker may use Quantum Route Redirect's routing engine to send scanners to legitimate sites while real users were sent to the phishing page (only when necessary for evasion).

Targeted Industries

This phishing activity targets any organization using Microsoft 365 for email and identity.

- Finance
- Government
- Education
- Energy
- Healthcare
- Retail
- Technology
- Manufacturing

Aspire's Service Offerings

- **Aspire Managed XDR (MXDR)**
  - Aspire Managed XDR (MXDR) combines next-generation eXtended Detection and Response (XDR) technology, a 24x7 security operations center (SOC), and the expertise of a US-based team of security professionals to identify and respond to threats across a broader attack surface.

  - Building on the existing capabilities of Managed Detection and Response (MDR), Aspire Managed XDR integrates and correlates telemetry from endpoints, network, cloud, email, identity, and more. This advanced platform creates valuable context enabling end-to-end visibility across all threat vectors.

- Experienced security analysts and incident responders deliver 24x7 threat detection, analysis, and investigations – with both automated and human-led response actions to quickly mitigate cyber attacks.

- **Aspire Incident Response**
  - The ability to respond effectively to data breaches is critical to every organization. When attacks occur, IT leaders need a process that will ultimately maintain business continuity, protect the company reputation, and avoid fines, legal fees, and remediation costs.

  - Aspire offers incident response services to help you prepare for, manage, and recover from data breaches and network attacks. An experienced team uses industry-leading threat intelligence and the most current security technology to quickly respond to attacks, reduce damage, and minimize exposure.

Supporting Documentation

Quantum Route Redirect: Anonymous Tool Streamlining Global Phishing Attack