Threat intelligence analysis based on investigations conducted by PhishReaper and presented by LogIQ Curve

Threat intelligence analysis based on investigations conducted by PhishReaper and presented by LogIQ Curve

Contents:

Sections	Description	Page
About LogIQ Curve Cyber Threat Intelligence Services		- 3
Section 1 –	Executive Summary	- 4
Section 2 –	About LogIQ Curve & PhishReaper	- 7
Section 3 –	The Evolution of Phishing Attacks	- 10
Section 4 –	Methodology: How Threat Intelligence Was Collected	- 15
Section 5 –	Global Phishing Trends Observed	- 20
Section 6 –	Case Study Analysis: Real-World Phishing Campaign Investigations	- 25
Section 7 –	Key Technical Insights from the Investigations	- 35
Section 8 –	Industry Impact Analysis	- 39
Section 9 –	Defensive Recommendations	- 44
Section 10 –	Future Outlook: The Next Phase of Phishing Threats	- 48
Section 11 –	About the Authors & Research Attribution	- 52
Section 12 –	Contact & Engagement	- 55
Appendix A –	Indicators of Compromise (IOC Summary)	- 58
Appendix B –	Glossary of Cybersecurity Terms	- 61

About LogIQ Curve Cyber Threat Intelligence Services

LogIQ Curve provides advanced cybersecurity advisory and threat intelligence capabilities designed to help organizations identify and mitigate emerging digital threats.

In an increasingly complex cyber threat landscape, enterprises require proactive security strategies capable of detecting malicious infrastructure before attacks reach customers or internal systems. LogIQ Curve works with organizations across financial services, telecommunications, fintech, and enterprise sectors to strengthen cybersecurity resilience through intelligence-driven security frameworks.

As the **Exclusive OEM Partner of PhishReaper in Pakistan**, LogIQ Curve introduces advanced phishing detection technologies that enable organizations to identify phishing infrastructure during the earliest stages of deployment.

These capabilities allow organizations to detect malicious domains, brand impersonation infrastructure, and phishing ecosystems before they become operational.

LogIQ Curve supports organizations through a range of cybersecurity services, including:

- Phishing infrastructure monitoring
- Brand impersonation detection
- Threat intelligence analysis
- Cybersecurity advisory for enterprises and regulators
- SOC enablement and threat detection enhancement

By integrating proactive threat intelligence with enterprise security strategies, LogIQ Curve helps organizations transition from reactive security models toward intelligence-driven cyber defence.

Organizations interested in strengthening their cybersecurity posture and gaining early visibility into phishing threats are encouraged to engage with LogIQ Curve's cybersecurity team.

Contact: security@logiqcurve.com

Section 1

Executive Summary

LogIQ Curve Global Phishing Threat Intelligence Report 2026

Phishing continues to represent one of the most persistent and financially damaging cyber threats facing organizations worldwide. However, the nature of phishing campaigns has evolved significantly over the past decade. What once consisted primarily of deceptive emails has transformed into a complex ecosystem of infrastructure-driven cybercrime operations designed to evade detection and harvest sensitive information at scale.

The **LogIQ Curve Global Phishing Threat Intelligence Report 2026** presents a detailed analysis of modern phishing infrastructure based on threat-intelligence investigations conducted using the capabilities of the PhishReaper platform. These investigations reveal how attackers increasingly rely on carefully staged digital infrastructure, brand impersonation, and automation to conduct large-scale phishing operations.

As the **Exclusive OEM Partner of PhishReaper in Pakistan**, LogIQ Curve is committed to helping organizations detect malicious infrastructure before phishing campaigns reach their intended victims. Through this collaboration, LogIQ Curve brings advanced phishing-detection capabilities to enterprises, financial institutions, telecom operators, and government organizations seeking to strengthen their cybersecurity posture.

This report analyses **ten real-world phishing investigations**, each highlighting different aspects of modern phishing operations. The case studies reveal that contemporary phishing campaigns are no longer isolated incidents but are instead part of organized cybercrime ecosystems supported by persistent infrastructure, automated tooling, and deliberate evasion techniques.

One of the most striking findings from these investigations is the **growing gap between the emergence of phishing infrastructure and its detection by traditional security systems**. In several cases analysed in this report, malicious domains remained active for extended periods, sometimes weeks or months, before appearing in global threat-intelligence feeds.

For example, one banking phishing campaign targeting a major financial institution remained operational for **eighteen days before global detection systems recognized the threat**, while another campaign impersonating a financial platform continued operating for **over two weeks without triggering widespread alerts**. In a separate case involving a Middle Eastern banking brand, phishing infrastructure remained active for **eighty-two days**, demonstrating how attackers can sustain campaigns when detection mechanisms rely primarily on reactive intelligence.

These detection delays highlight a fundamental challenge in modern cybersecurity: many traditional security tools rely heavily on **historical indicators of compromise**. Such systems typically identify threats only after malicious activity has already been reported or observed in the wild. As attackers become increasingly aware of these limitations, they are designing phishing infrastructure specifically to evade early detection.

The investigations documented in this report reveal several common strategies used by attackers to bypass conventional security controls. These include the staging of dormant infrastructure months before use, the acquisition of expired domains with existing reputational trust, the use of cloud platforms to host malicious content, and techniques such as redirect laundering to deceive automated scanning systems.

In one particularly revealing case, attackers leveraged previously legitimate infrastructure associated with a creative media project. After the domain expired and changed ownership, it was repurposed into potential phishing infrastructure while still retaining a clean reputation profile. This type of domain repurposing highlights how the lifecycle of internet assets can become an overlooked component of the attack surface.

Another investigation documented how attackers exploited weaknesses within automated security pipelines themselves. By designing infrastructure that behaves differently during automated inspection than during actual attacks, threat actors were able to manipulate detection systems and extend the lifespan of phishing campaigns. This phenomenon represents a growing trend in which **the security stack itself becomes part of the attack surface**.

Financial services platforms emerged as one of the most frequently targeted sectors in the investigations analysed in this report. Payment gateways, mobile wallets, and online banking platforms were repeatedly impersonated by phishing campaigns designed to harvest financial credentials and payment information. These platforms present attractive targets for cybercriminals because they combine high trust among users with direct financial value.

Telecommunications platforms and cloud services also appeared as recurring targets. In several cases, attackers abused trusted cloud infrastructure to host phishing applications or deliver malware disguised as legitimate software downloads. Because such infrastructure originates from reputable service providers, many security tools hesitate to flag these environments as malicious.

To counter these evolving threats, organizations must move beyond purely reactive detection models and adopt **proactive threat-hunting strategies**. Proactive threat hunting focuses on identifying malicious infrastructure based on intent and behavioural signals rather than waiting for evidence of abuse.
The PhishReaper platform applies this philosophy through infrastructure-level analysis, examining domain patterns, hosting signals, behavioural indicators, and brand impersonation markers to identify phishing infrastructure during its earliest stages. By focusing on attacker intent rather than relying solely on reputation signals, such technologies enable security teams to detect malicious infrastructure before phishing campaigns reach widespread distribution.

The findings presented in this report reinforce the importance of adopting an infrastructure-centric view of cybersecurity. Rather than focusing solely on malicious emails or individual phishing pages, defenders must understand the broader ecosystem supporting phishing operations. This includes monitoring domain registrations, infrastructure transitions, hosting relationships, and reputation manipulation tactics used by attackers.

Organizations that adopt proactive threat-hunting technologies gain significant advantages in detecting emerging threats early. Early detection allows security teams to disrupt phishing infrastructure before it becomes operational, protecting users, financial assets, and organizational reputation.

As phishing campaigns continue to evolve in complexity and scale, proactive cybersecurity strategies will become essential for defending against modern cybercrime operations. The investigations presented in this report demonstrate that identifying phishing infrastructure early is not only possible but increasingly necessary for organizations seeking to stay ahead of emerging threats.

Through its partnership with PhishReaper, LogIQ Curve remains committed to helping organizations strengthen their cybersecurity defences and detect phishing campaigns before they escalate into major cyber incidents.

Threat Intelligence Key Findings

The investigations presented in this report reveal several critical insights into the evolving nature of phishing infrastructure and cybercrime operations.

Across ten real-world phishing campaigns targeting organizations in sectors including banking, fintech, telecommunications, and cloud services, several consistent patterns emerged.

First, modern phishing campaigns increasingly rely on **infrastructure staging techniques**. Attackers frequently register domains weeks or months before launching phishing campaigns, allowing malicious infrastructure to accumulate reputation signals before becoming operational.

Second, phishing campaigns now operate within **multi-domain infrastructure ecosystems** rather than relying on single malicious websites. These ecosystems often include redirect infrastructure, credential collection servers, and distributed hosting environments designed to evade automated detection systems.

Third, attackers are increasingly exploiting weaknesses in **reputation-based detection models**. Techniques such as redirect laundering and delayed activation allow phishing domains to appear benign during automated security scans.

Fourth, financial platforms remain the most frequently targeted sector. Payment gateways, banking portals, and digital wallet services present attractive targets because compromised credentials can be directly monetized.

Finally, the investigations demonstrate that many phishing campaigns remain undetected for extended periods when security systems rely primarily on reactive intelligence feeds.

These findings reinforce the importance of adopting **proactive threat-hunting strategies capable of identifying phishing infrastructure early in its lifecycle**.

Organizations that implement infrastructure-level monitoring and intelligence-driven security practices can significantly reduce the risk posed by modern phishing campaigns.

Section 2

About LogIQ Curve & PhishReaper

2.1 About LogIQ Curve

LogIQ Curve is a technology and cybersecurity solutions provider focused on helping organizations navigate an increasingly complex digital threat landscape. The company delivers services and platforms designed to support enterprises, financial institutions, telecom operators, and government organizations in strengthening their cybersecurity posture and protecting critical digital infrastructure.

Operating at the intersection of **software engineering, cybersecurity, and digital innovation**, LogIQ Curve works with organizations that require reliable, forward-looking solutions to address emerging cyber risks. These risks include phishing campaigns, digital brand abuse, credential harvesting attacks, and malicious infrastructure designed to evade traditional detection systems.

One of LogIQ Curve's key focus areas is **proactive cybersecurity intelligence**, enabling organizations to detect malicious activity before attacks impact users, systems, or financial assets. In modern cyber defence strategies, the ability to identify infrastructure supporting cybercrime operations, such as phishing domains, fraudulent websites, and malicious staging environments, has become increasingly critical.

To support this mission, LogIQ Curve collaborates with advanced cybersecurity platforms capable of identifying threats during the earliest stages of their lifecycle. Through these partnerships, the company provides organizations with access to technologies that go beyond conventional reactive security tools.

LogIQ Curve works with organizations across multiple sectors, including:

- Banking and financial services
- Telecommunications providers
- Fintech platforms
- Government agencies
- Enterprise technology organizations

By integrating advanced detection technologies with enterprise cybersecurity strategies, LogIQ Curve aims to help organizations **transition from reactive security models to proactive cyber defence frameworks**.

2.2 Strategic Partnership with PhishReaper

LogIQ Curve serves as the **Exclusive OEM Partner of PhishReaper in Pakistan**, bringing the platform's advanced phishing detection capabilities to organizations across the region.

PhishReaper is a cybersecurity platform focused on identifying phishing infrastructure and brand-impersonation campaigns before they reach their intended victims. Rather than relying solely on blocklists or previously reported malicious indicators, the platform7analysis infrastructure signals that reveal the intent behind suspicious domains and digital assets.

Through this partnership, LogIQ Curve enables organizations in Pakistan and beyond to benefit from **early-stage phishing detection technology** capable of identifying malicious infrastructure before phishing campaigns begin harvesting data or distributing malicious links.

The collaboration between LogIQ Curve and PhishReaper reflects a shared objective: improving visibility into the infrastructure supporting cybercrime operations and enabling organizations to detect threats earlier in their lifecycle.

Within this report, the phishing investigations analysed are based on threat-intelligence findings generated through the capabilities of the PhishReaper platform and presented to the global audience through LogIQ Curve.

2.3 The PhishReaper Platform

PhishReaper is designed to detect phishing infrastructure using **intent-driven analysis rather than traditional reputation-based detection models**.

Most conventional phishing detection systems rely on known indicators of compromise such as malicious URLs, blocklisted domains, or user reports. While these systems can eventually detect threats, they often do so only after phishing campaigns have already caused harm.

PhishReaper takes a fundamentally different approach by identifying signals that indicate a domain or digital asset was created for phishing activity.

This detection model focuses on analysing infrastructure characteristics such as:

- Suspicious domain naming patterns
- Brand impersonation signals
- Hosting and infrastructure relationships
- Behavioural indicators associated with phishing campaigns
- Attacker staging and deployment patterns

By analysing these signals, the platform can identify phishing infrastructure **during the early stages of its lifecycle**, often before the infrastructure is actively used in phishing campaigns.

2.4 Infrastructure-Level Threat Intelligence

One of the defining capabilities of the PhishReaper platform is its focus on **infrastructure-level threat intelligence**.

Rather than analysing phishing emails or individual malicious webpages in isolation, the platform examines the broader infrastructure ecosystem supporting phishing operations.

This approach enables investigators to identify patterns such as:

- Coordinated domain registration campaigns
- Clusters of infrastructure supporting phishing kits
- Malicious staging environments preparing for phishing attacks
- Brand impersonation infrastructure targeting financial services, payment platforms, and telecom services

By mapping these infrastructure relationships, PhishReaper provides a deeper understanding of how phishing campaigns are organized and deployed.

This type of intelligence is particularly valuable for organizations seeking to protect their brands, customers, and digital services from large-scale phishing operations.

2.5 Supporting Proactive Cyber Defense

The investigations presented throughout this report illustrate a clear trend: phishing operations are increasingly supported by persistent infrastructure designed to evade detection.

In many cases, malicious domains remain active for extended periods before traditional detection systems identify them. These delays create opportunities for attackers to harvest credentials, steal financial data, or distribute malware.

Technologies capable of identifying malicious infrastructure during its early stages provide organizations with a strategic advantage.

By detecting phishing infrastructure before campaigns become operational, security teams can:

- Protect customers from fraudulent websites
- Prevent credential harvesting attacks
- Safeguard payment platforms and financial services
- Preserve brand reputation and customer trust

Through its collaboration with PhishReaper, LogIQ Curve provides organizations with access to these proactive threat-intelligence capabilities.

Together, the two organizations aim to help enterprises transition from reactive cybersecurity approaches toward **proactive, intelligence-driven cyber defence strategies**.

2.6 The Role of Threat Intelligence in Modern Cybersecurity

Modern cyber threats are increasingly organized, automated, and scalable. As phishing campaigns evolve into infrastructure-driven operations, organizations must develop visibility into the digital environments where these campaigns originate.

Threat intelligence plays a critical role in enabling this visibility. By analysing infrastructure signals, behavioural patterns, and attacker tactics, threat-intelligence platforms can detect emerging threats before they reach users or corporate systems.

The findings presented in this report demonstrate how infrastructure-level intelligence can reveal phishing ecosystems that might otherwise remain hidden within the broader internet landscape.

As the cybersecurity environment continues to evolve, organizations that adopt proactive threat-intelligence strategies will be better positioned to identify emerging threats and defend against the next generation of phishing attacks.

Section 3

The Evolution of Phishing Attacks

3.1 From Simple Email Scams to Global Cybercrime Operations

Phishing has existed for more than two decades, evolving from simple email scams into one of the most sophisticated forms of cybercrime. While the core objective has remained the same, deceiving victims into revealing sensitive information, the methods used by attackers have become significantly more advanced.

Early phishing attacks were relatively unsophisticated. Attackers would send mass emails impersonating banks or online services, encouraging recipients to click on malicious links and enter their login credentials on fraudulent websites. These campaigns relied heavily on social engineering rather than technical sophistication.

Over time, however, attackers began developing more complex infrastructure to support phishing operations. Instead of launching isolated attacks, they built systems capable of supporting large-scale campaigns targeting thousands or even millions of users.

Today, phishing has evolved into an organized cybercrime industry supported by infrastructure networks, phishing kits, automation tools, and underground marketplaces.

3.2 Phase One: Email-Based Phishing

The earliest phishing campaigns primarily relied on deceptive emails designed to impersonate legitimate institutions such as banks, e-commerce platforms, and social media services.

Typical characteristics of early phishing campaigns included:

- Generic phishing emails sent to large mailing lists
- Simple fraudulent websites hosted on compromised servers
- Limited use of automation or infrastructure staging
- Easily detectable domain names and poor design quality

Although these campaigns were often technically simple, they proved highly effective due to the lack of cybersecurity awareness among many internet users during the early stages of online commerce.

Security tools at the time were primarily designed to detect malware rather than social engineering attacks, allowing phishing campaigns to grow rapidly.

3.3 Phase Two: Brand Impersonation and Targeted Campaigns

As cybersecurity awareness increased and email filters improved, attackers began refining their tactics.

Phishing campaigns evolved into **brand impersonation attacks**, where malicious websites closely replicated the appearance of legitimate organizations. Attackers copied logos, user interfaces, and login workflows from trusted brands to create convincing phishing environments.

This phase introduced several important developments:

- Domain names designed to resemble legitimate brand domains
- Professional-looking phishing websites mimicking official portals
- Targeted campaigns aimed at specific organizations or regions
- Phishing emails crafted to bypass spam filters

Financial institutions, payment platforms, and telecommunications companies became frequent targets because of the financial value associated with compromised accounts.

During this phase, attackers began using **phishing kits**, pre-built software packages that enabled cybercriminals to deploy phishing websites quickly and easily.

3.4 Phase Three: Infrastructure-Driven Phishing Ecosystems

The modern era of phishing is defined by the rise of **infrastructure-driven cybercrime ecosystems**. Instead of launching isolated phishing pages, attackers now deploy complex infrastructure designed to support large-scale operations.

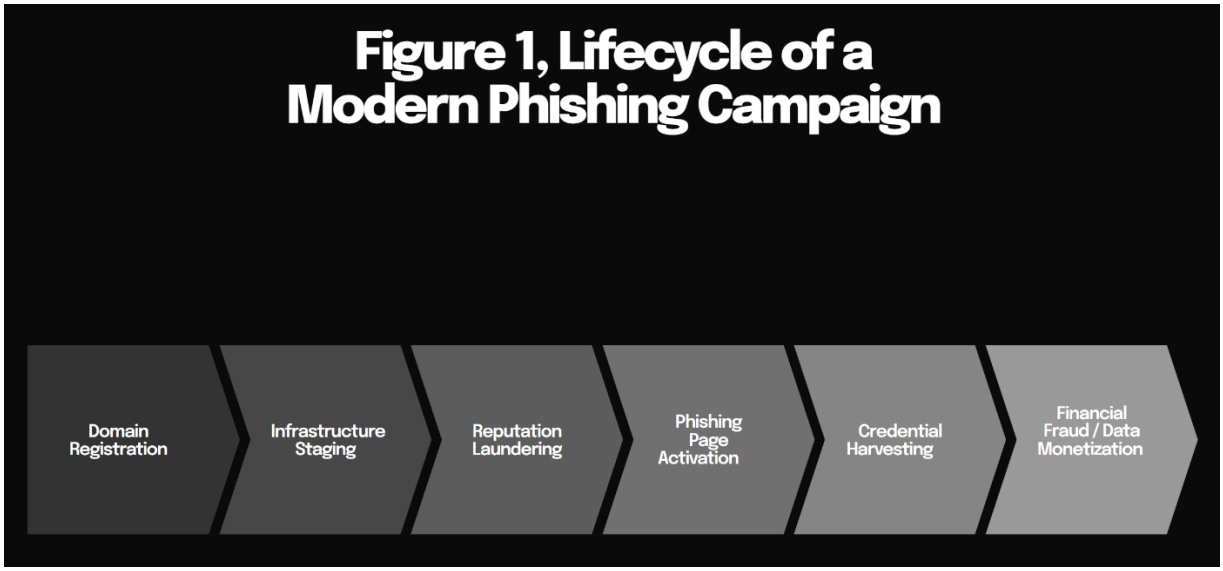
Modern phishing campaigns may involve:

- Clusters of coordinated phishing domains
- Staging infrastructure prepared months before use
- Automated domain registration campaigns
- Redirect networks used to evade security scanners
- Malware payload delivery disguised as legitimate downloads

This infrastructure allows attackers to rapidly launch and scale phishing operations while maintaining resilience against takedown efforts.

Investigations conducted using the capabilities of the PhishReaper platform have revealed that many phishing campaigns operate within **long-lived infrastructure ecosystems** rather than short-term attacks.

In several cases analysed in this report, phishing infrastructure remained active for weeks or even months before being detected by traditional security tools.



3.5 Automation and the Industrialization of Phishing

One of the most significant developments in modern phishing operations is the increasing use of automation.

Cybercriminals now employ automated tools capable of:

- Generating large numbers of phishing domains

- Deploying phishing websites at scale
- Collecting and managing stolen credentials
- Distributing phishing links through automated messaging systems

These tools have contributed to the **industrialization of phishing**, transforming it into a structured cybercrime business model.

Underground marketplaces now sell phishing kits, domain lists, stolen credentials, and infrastructure services that enable attackers to launch campaigns with minimal technical expertise.

This ecosystem allows cybercriminal groups to operate phishing campaigns as continuous operations rather than isolated attacks.

3.6 The Emergence of AI-Assisted Phishing

Recent developments in artificial intelligence have introduced new capabilities into the phishing landscape.

Attackers are increasingly experimenting with AI technologies to improve the effectiveness of phishing campaigns.

Examples include:

- AI-generated phishing emails with natural language quality
- Automated generation of phishing websites
- AI-assisted translation for multilingual phishing campaigns
- Intelligent targeting of victims based on publicly available data

These technologies enable attackers to produce more convincing phishing content and scale campaigns across multiple regions simultaneously.

As AI technologies continue to evolve, phishing campaigns are expected to become even more sophisticated and difficult to detect.

3.7 The Expanding Attack Surface

The attack surface for phishing operations has also expanded significantly.

While early phishing attacks targeted email users, modern campaigns may involve multiple channels, including:

- Email phishing campaigns
- SMS phishing (smishing)
- Messaging platform scams
- Malicious advertisements
- Fraudulent mobile applications

Attackers may combine these channels with infrastructure-level deception techniques such as redirect chains and domain reputation manipulation.

These multi-channel strategies allow phishing campaigns to reach larger audiences while complicating detection efforts.

3.8 Why Traditional Detection Approaches Are Struggling

The evolution of phishing infrastructure presents significant challenges for traditional cybersecurity tools.

Many security systems rely on **reactive detection models**, which identify threats only after malicious activity has been reported or observed.

However, modern phishing infrastructure is often designed to evade these systems by:

- Staging dormant domains that appear harmless during scanning
- Using redirects to legitimate websites during automated inspection
- Activating phishing content only after detection checks have passed

These tactics allow phishing infrastructure to remain undetected during the early stages of a campaign.

This detection gap highlights the need for **proactive threat-hunting technologies** capable of identifying malicious infrastructure based on intent rather than historical indicators.

3.9 The Need for Infrastructure-Level Threat Intelligence

As phishing campaigns continue to evolve, organizations must adopt security strategies capable of identifying threats earlier in their lifecycle.

Infrastructure-level threat intelligence focuses on detecting malicious infrastructure before phishing campaigns become operational.

This approach analyses signals such as:

- Suspicious domain registration patterns
- Brand impersonation indicators
- Hosting relationships between phishing assets
- Attacker infrastructure deployment patterns

Platforms capable of identifying these signals provide security teams with the ability to detect phishing campaigns during their earliest stages.

The investigations documented in this report demonstrate how proactive infrastructure analysis can reveal phishing ecosystems that would otherwise remain hidden within the broader internet environment.

3.10 The Future of Phishing Threats

The continued evolution of phishing suggests that attackers will increasingly adopt automation, artificial intelligence, and infrastructure-level deception techniques.

Future phishing campaigns may involve:

- AI-generated phishing content at scale
- Automated infrastructure generation
- Advanced evasion techniques targeting security tools
- Multi-channel phishing campaigns across digital platforms

Organizations that rely solely on reactive detection methods may find it increasingly difficult to defend against these threats.

Proactive threat-hunting technologies and infrastructure-level intelligence will play a critical role in identifying and disrupting phishing campaigns before they reach their intended victims.

Through its partnership with PhishReaper, LogIQ Curve aims to help organizations adopt these proactive cybersecurity strategies and strengthen their defences against the next generation of phishing threats.

Bibliography

- Verizon. 2024 Data Breach Investigations Report. Verizon Enterprise, 2024.
- Anti-Phishing Working Group. Phishing Activity Trends Report. APWG, 2024.
- ENISA. ENISA Threat Landscape Report. European Union Agency for Cybersecurity, 2023.
- Google Threat Analysis Group. Phishing Trends and Threat Insights. Google Security Blog, 2023.
- PhishReaper Threat Intelligence Team. Phishing Infrastructure Investigations. PhishReaper Blog Series, 2025–2026.

Section 4

Methodology: How Threat Intelligence Was Collected

4.1 Introduction

Understanding modern phishing campaigns requires more than simply identifying malicious emails or fraudulent websites. Contemporary phishing operations are supported by complex infrastructure ecosystems that include domain registrations, hosting environments, staging infrastructure, and automated deployment mechanisms.

To uncover these ecosystems, investigators must analyse signals that reveal attacker intent before phishing campaigns become visible through traditional detection systems.

The threat-intelligence findings presented in this report are based on investigations conducted using the infrastructure-analysis capabilities of the PhishReaper platform. These investigations focused on identifying early indicators of phishing infrastructure and mapping relationships between malicious digital assets.

The methodology combines **infrastructure analysis, behavioural pattern recognition, and automated threat hunting** to detect phishing operations during the early stages of their lifecycle.

4.2 Infrastructure-First Investigation Model

Traditional phishing investigations typically begin after an incident occurs, for example, when a phishing email is reported or when a malicious webpage is discovered.

In contrast, the methodology used in this report follows an **infrastructure-first approach**.

Instead of waiting for evidence of abuse, investigators analyse newly registered domains, hosting environments, and infrastructure patterns to determine whether they were created with malicious intent.

This approach focuses on identifying signals that indicate a domain or digital asset may be part of a phishing campaign even before the campaign becomes operational.

Infrastructure-first investigation allows security teams to identify phishing campaigns earlier and disrupt malicious infrastructure before it reaches victims.

4.3 Data Sources and Signals

The threat-intelligence investigations described in this report rely on multiple data sources that provide visibility into domain activity and infrastructure relationships.

Key signals analysed during investigations include:

Domain Registration Intelligence

Newly registered domains are often used in phishing campaigns because attackers require fresh infrastructure to launch operations.

Investigators analyse:

- Domain naming patterns that mimic legitimate brands
- Domain registration timelines
- Registrar information
- Domain age and lifecycle patterns

Brand tokens embedded within domain names, such as financial service brands, payment platforms, or telecommunications providers, often serve as early indicators of phishing infrastructure.

DNS and Hosting Signals
DNS records and hosting configurations provide valuable insights into the infrastructure supporting suspicious domains.

Investigators examine signals such as:

- DNS configuration changes
- Hosting provider relationships
- Shared infrastructure across multiple domains
- Historical hosting transitions

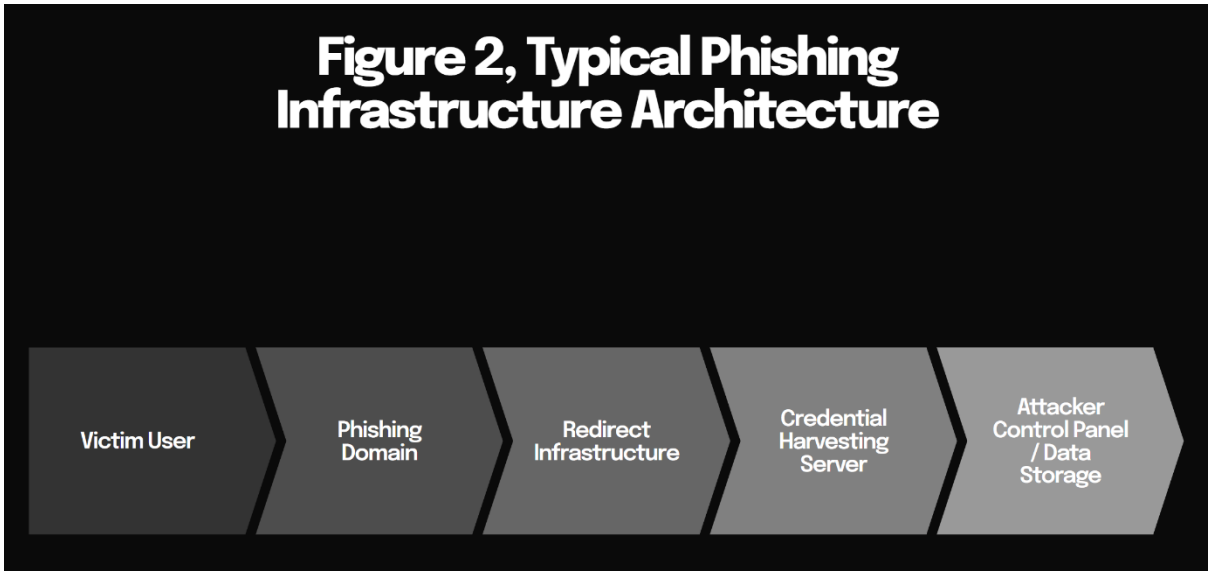
Clusters of domains sharing similar hosting characteristics may indicate coordinated phishing infrastructure.

Infrastructure Relationships
Modern phishing campaigns often involve multiple domains working together.

These domains may serve different functions within a phishing ecosystem, including:

- Staging environments for phishing pages
- Redirect infrastructure designed to evade detection
- Domains used to host phishing kits
- Domains used to collect stolen credentials

By mapping relationships between these assets, investigators can identify entire phishing ecosystems rather than isolated malicious webpages.



4.4 Behavioural Analysis

In addition to infrastructure signals, behavioural indicators play an important role in phishing detection.
Behavioural analysis examines how suspicious domains behave when accessed or scanned.

Investigators analyse behaviours such as:

- Redirect chains that lead to legitimate websites during automated scans
- Delayed activation of phishing pages
- Dynamic content rendering designed to evade detection
- Conditional payload delivery depending on visitor type

These behaviours are commonly used by attackers to manipulate automated scanning tools.

By identifying such patterns, investigators can determine whether infrastructure is likely intended for phishing activity.

4.5 Brand Impersonation Detection

A key component of phishing infrastructure analysis involves detecting **brand impersonation signals**. Attackers frequently embed recognizable brand names within domain names to increase the credibility of phishing websites.

Examples include domains impersonating:

- Banking institutions
- Payment platforms
- Telecommunications providers
- Cloud service providers
- Technology companies

The investigations presented in this report identified multiple phishing campaigns targeting brands within the financial services and fintech sectors.

Brand impersonation signals often serve as early indicators that a domain may be part of a phishing operation.

4.6 AI-Assisted Threat Hunting

The PhishReaper platform incorporates artificial intelligence to analyse infrastructure signals and identify suspicious patterns across large volumes of domain data.

AI-assisted threat hunting enables investigators to detect phishing infrastructure that might otherwise remain hidden within the broader internet ecosystem.

Key capabilities include:

- Automated analysis of domain naming patterns
- Detection of infrastructure clusters
- Behavioural anomaly detection
- Identification of staging infrastructure used in phishing campaigns

These capabilities allow investigators to identify suspicious infrastructure quickly and prioritize domains that require deeper analysis.

4.7 Case Study Investigation Workflow

Each phishing investigation described in this report followed a structured workflow designed to identify and analyse malicious infrastructure.

The investigation process typically included the following stages:

1. **Initial Detection**
   Identification of suspicious domains through infrastructure analysis.

2. **Signal Correlation**
   Analysis of domain registration patterns, hosting signals, and brand impersonation indicators.
3. **Behavioural Testing**
   Examination of domain behaviour to identify phishing content, redirect logic, or payload delivery mechanisms.
4. **Infrastructure Mapping**
   Identification of related domains and infrastructure components supporting the phishing ecosystem.
5. **Threat Assessment**

   Evaluation of potential risks associated with the infrastructure and documentation of findings.

This workflow allows investigators to move beyond isolated indicators and identify the broader infrastructure supporting phishing campaigns.

4.8 Limitations of Traditional Detection Approaches

One of the key observations from the investigations in this report is that many phishing campaigns remain undetected for extended periods when traditional security tools rely primarily on reactive detection models.

Common limitations include:

- Dependence on blocklists populated after incidents occur
- Reliance on user-reported phishing pages
- Limited visibility into infrastructure staging activity
- Lack of analysis of domain lifecycle transitions

Attackers often exploit these limitations by staging infrastructure months in advance or by using domains that initially appear benign during automated scanning.

These tactics allow phishing infrastructure to remain active until malicious activity becomes visible through traditional indicators.

4.9 Advantages of Proactive Threat Hunting

The infrastructure-analysis methodology used in this report provides several advantages for organizations seeking to defend against phishing campaigns.

These advantages include:

- Early detection of malicious infrastructure
- Identification of coordinated phishing ecosystems
- Visibility into attacker tactics and deployment strategies
- Improved protection for brands and digital services

By identifying suspicious infrastructure early, organizations can respond before phishing campaigns begin harvesting credentials or distributing malicious links.

This proactive approach represents a critical shift in modern cybersecurity defence strategies.

4.10 Supporting Intelligence-Driven Security

The methodology described in this section demonstrates how infrastructure-level threat intelligence can reveal phishing ecosystems that may otherwise remain hidden.

Organizations that adopt intelligence-driven cybersecurity strategies gain the ability to detect emerging threats earlier and respond more effectively.

Through its collaboration with PhishReaper, LogIQ Curve enables organizations to leverage these capabilities and strengthen their defences against infrastructure-driven phishing campaigns.

The case studies presented in the following sections illustrate how this methodology was applied to identify real-world phishing operations targeting financial institutions, payment platforms, telecommunications providers, and global technology brands.

Bibliography

- Mandiant. M-Trends 2024: Global Incident Response Insights. Google Cloud, 2024.
- CrowdStrike Intelligence. Global Threat Report. CrowdStrike, 2024.
- ENISA. Threat Landscape Report. European Union Agency for Cybersecurity, 2023.
- National Institute of Standards and Technology. Guide to Cyber Threat Information Sharing. NIST Special Publication 800-150.
- MITRE Corporation. MITRE ATT&CK Framework for Enterprise Threat Detection. MITRE, 2023.
- PhishReaper Threat Intelligence Team. Phishing Infrastructure Investigations. PhishReaper Blog Series, 2025–2026.

Section 5

Global Phishing Trends Observed

5.1 Introduction

The ten phishing investigations analysed in this report provide valuable insight into how modern phishing campaigns are designed, deployed, and sustained. While each campaign targeted different brands and industries, several consistent patterns emerged across the cases.

These patterns illustrate how phishing operations are evolving into structured cybercrime ecosystems supported by sophisticated infrastructure, automation, and deception techniques.

The findings also reveal a widening gap between the **deployment of phishing infrastructure and its detection by traditional security systems**, reinforcing the need for proactive threat-hunting strategies.

This section summarizes the key trends identified across the case studies.

5.2 Brand Impersonation Remains the Primary Attack Vector

One of the most consistent findings across the investigations is the continued dominance of **brand impersonation** as the central tactic in phishing campaigns.

Attackers exploit the trust associated with recognizable brands to increase the credibility of phishing websites and encourage victims to disclose sensitive information.

Brands targeted in the case studies include organizations operating in sectors such as:

- Global airlines
- Financial institutions
- Payment gateways
- Fintech platforms
- Telecommunications services
- Cloud and technology providers

By embedding brand names directly within domain names, attackers create domains that appear legitimate at first glance.

Examples of typical brand impersonation patterns include domains that incorporate words such as:

- “support”
- “verification”
- “account recovery”
- “payment confirmation”

These naming strategies increase the likelihood that users will trust phishing links and interact with fraudulent websites.

5.3 Financial Platforms Are the Most Attractive Targets

The investigations revealed a strong concentration of phishing campaigns targeting financial services platforms.

These platforms include:

- Online banking portals
- Payment processors

- Mobile wallet services
- Fintech platforms

Financial platforms are attractive targets for attackers because compromised credentials can be directly monetized.

Successful attacks may result in:
- Unauthorized financial transactions
- Stolen credit card information
- Fraudulent account access
- Identity theft

Several case studies, including campaigns targeting Stripe, Mastercard, and regional banking institutions, demonstrate how attackers design phishing environments specifically to capture financial credentials.

The targeting of payment platforms suggests that attackers prioritize infrastructure capable of delivering **direct financial returns**.

5.4 Dormant Infrastructure Staging

Another major trend observed across the case studies is the use of **dormant infrastructure staging**.

Attackers frequently register phishing domains months before they are used in active campaigns. During this staging period, domains may appear inactive or harmless.

However, these domains often contain underlying infrastructure that indicates preparation for phishing operations.

Common characteristics of staged phishing domains include:
- Valid DNS configuration
- Active hosting infrastructure
- TLS certificates issued shortly after registration
- Placeholder pages designed to avoid detection

Once these domains accumulate reputation and age within the internet ecosystem, attackers can activate phishing campaigns with minimal risk of early detection.

Dormant infrastructure staging represents a major challenge for traditional detection models that rely on observing malicious activity before taking action.

5.5 Reputation Manipulation Techniques

The investigations revealed that attackers increasingly attempt to manipulate reputation-based security systems.

Reputation scoring is commonly used by cybersecurity platforms to determine whether a domain is likely to be malicious.
However, attackers have developed techniques designed to influence these reputation systems.

Examples observed in the case studies include:
- Redirecting visitors to legitimate websites during automated scans
- Serving benign content until a phishing campaign begins

- Staging infrastructure that initially appears inactive

These techniques allow malicious domains to accumulate positive reputation signals before they are used for phishing attacks.

By the time malicious activity begins, security systems may already classify the domain as trustworthy.

5.6 Abuse of Cloud Infrastructure

Several phishing campaigns analysed in this report leveraged **trusted cloud platforms** to host malicious infrastructure.

Cloud hosting services provide attackers with several advantages:

- Scalable infrastructure
- Globally distributed hosting environments
- Trusted network reputation

Because cloud service providers host legitimate applications used by millions of organizations, security tools often treat such infrastructure with greater trust.

Attackers exploit this trust by deploying phishing environments within cloud-hosted applications or content delivery networks.

This tactic makes it more difficult for security tools to distinguish malicious activity from legitimate cloud-hosted services.

5.7 Expired Domain Repurposing

The investigations also revealed instances in which previously legitimate domains were repurposed for phishing activity after changing ownership.

Expired domains often retain positive reputation signals from their previous use. These signals may include:

- Backlinks from reputable websites
- Search engine indexing history
- Trusted hosting infrastructure

When attackers acquire such domains, they inherit these trust signals.

This allows phishing infrastructure to operate with reduced scrutiny from automated detection systems.

The repurposing of expired domains represents a subtle but increasingly common technique used to stage phishing operations.

5.8 The Rise of Infrastructure-Level Deception

Modern phishing campaigns increasingly rely on **infrastructure-level deception techniques** designed to evade automated scanning tools.

These techniques include:

- Redirect chains that conceal phishing pages
- Delayed activation of malicious content
- Conditional payload delivery based on visitor type

For example, a phishing domain may behave differently depending on whether the visitor is a security scanner or a real user.

Automated scanners may be redirected to legitimate websites, while real users encounter phishing pages. This type of deception significantly complicates the task of detecting phishing infrastructure.

5.9 Security Tools as an Emerging Attack Surface

One of the most concerning trends identified in the investigations is the growing tendency for attackers to exploit weaknesses in security tools themselves.

Attackers increasingly design phishing infrastructure to manipulate automated detection systems.

This may involve:

- Staging infrastructure specifically designed to pass security scans
- Triggering different behaviours during automated inspection
- Exploiting predictable scanning patterns used by security tools

As attackers study how security systems operate, they can design campaigns that intentionally evade detection mechanisms.

This phenomenon effectively turns the **security stack into an unintended attack surface**.

5.10 Phishing as an Organized Business Model

The case studies analysed in this report demonstrate that phishing operations are no longer limited to opportunistic cybercrime.

Instead, they increasingly resemble organized business operations supported by structured infrastructure and automated tooling.

Many phishing campaigns now exhibit characteristics such as:

- Persistent infrastructure designed for long-term use
- Automation tools for generating domains and phishing pages
- Coordinated campaigns targeting multiple brands simultaneously

These characteristics suggest that phishing operations are becoming **industrialized cybercrime ecosystems** capable of sustaining long-running campaigns.

5.11 Key Takeaways

The trends identified across the ten case studies highlight several important conclusions about the current state of phishing threats:

1. **Brand impersonation remains the dominant phishing tactic.**
2. **Financial services platforms are the most frequently targeted sector.**
3. **Attackers increasingly stage infrastructure months before launching campaigns.**
4. **Reputation manipulation is widely used to evade detection systems.**
5. **Cloud platforms are frequently abused to host phishing infrastructure.**
6. **Expired domains are being repurposed for malicious campaigns.**
7. **Security tools themselves are becoming part of the attack surface.**

These trends demonstrate that modern phishing campaigns rely heavily on infrastructure-level deception techniques designed to evade traditional security systems.

Organizations seeking to defend against these threats must adopt cybersecurity strategies capable of identifying phishing infrastructure early in its lifecycle.

Proactive threat-hunting platforms such as PhishReaper enable security teams to detect these signals and disrupt phishing campaigns before they reach victims.

Bibliography

- Mandiant. *M-Trends 2024: Global Incident Response Insights*. Google Cloud, 2024.
- CrowdStrike. *Global Threat Report*. CrowdStrike Intelligence, 2024.
- APWG. *Phishing Activity Trends Report*. Anti-Phishing Working Group, 2024.
- PhishReaper Threat Intelligence Team. *Threat Investigations*. PhishReaper Blog Series, 2025–2026.

Section 6

Case Study Analysis: Real-World Phishing Campaign Investigations

6.1 Introduction

The following case studies present detailed investigations into phishing campaigns uncovered through infrastructure-level threat hunting.

Each case study illustrates a different dimension of modern phishing operations, including:

- Brand impersonation campaigns targeting global organizations
- Infrastructure designed to evade automated detection systems
- Phishing ecosystems supported by coordinated domain networks
- Long-running campaigns operating undetected within the global internet infrastructure

These investigations demonstrate how phishing has evolved from isolated attacks into **structured cybercrime ecosystems supported by persistent infrastructure**.

The cases also highlight a recurring pattern observed across multiple investigations: **a significant delay between the deployment of phishing infrastructure and its detection by traditional security systems**.

By analysing infrastructure signals rather than relying solely on historical indicators of compromise, the PhishReaper platform was able to detect these phishing operations during early stages of their lifecycle.

The following ten case studies illustrate how this infrastructure-first approach can uncover phishing campaigns targeting organizations across sectors including aviation, banking, fintech, payment platforms, telecommunications, and cloud services.

Case Study 1

Qatar Airways Phishing Infrastructure

Overview

One of the investigations analysed in this report involved a phishing campaign impersonating a major international airline brand. The campaign targeted users through infrastructure designed to replicate legitimate airline services and capture sensitive information from victims.

Phishing campaigns targeting airline brands often attempt to exploit the high level of trust associated with well-known travel companies. Victims may encounter phishing pages designed to mimic airline booking portals, loyalty program interfaces, or account verification systems.

The infrastructure uncovered during this investigation revealed a coordinated ecosystem of phishing assets designed to support brand impersonation activity.

Infrastructure Characteristics

The phishing campaign relied on multiple domains designed to imitate the airline brand's digital presence.

Common characteristics observed in the infrastructure included:

- Domain names incorporating the airline's brand name
- Phishing pages replicating the appearance of legitimate airline interfaces
- Hosting infrastructure configured to support multiple phishing environments

These elements allowed attackers to create a convincing phishing environment capable of deceiving users who believed they were interacting with a legitimate airline service.

Detection Timeline

The investigation revealed that the phishing infrastructure had been active within the internet ecosystem before appearing in traditional threat-intelligence feeds.

The early detection of the campaign demonstrates the importance of identifying suspicious infrastructure signals before phishing campaigns begin harvesting victim data.

Traditional detection systems may not flag such infrastructure until phishing pages are actively reported or discovered by users.

Threat Implications

Phishing campaigns targeting airline brands can have several potential consequences:

- Theft of customer login credentials
- Fraudulent loyalty program activity
- Identity theft involving passenger data
- Reputational damage to the targeted brand

Airline companies and travel platforms often maintain large user bases, making them attractive targets for phishing campaigns.

The investigation highlights how attackers exploit brand trust to increase the effectiveness of phishing operations.

Figure 3, Detection Gap in Phishing Infrastructure

Day 0	Domain Registered
Day 5	Infrastructure Prepared
Day 10	Phishing Page Activated
Day 18	Detected by Traditional Security Tools

Case Study 2

HBL Phishing Campaign and the 18-Day Detection Gap

Overview

Another investigation analysed a phishing campaign targeting a major banking institution. The campaign impersonated the bank's online services and attempted to harvest sensitive financial credentials from victims.

Financial institutions remain among the most frequently targeted organizations in phishing campaigns due to the direct monetary value associated with compromised accounts.

The campaign uncovered during this investigation demonstrated a critical weakness in traditional phishing detection models.

Infrastructure Deployment

The phishing campaign involved infrastructure designed to mimic the bank's official online banking interface.

The phishing environment included:

- Domains resembling legitimate banking portals
- Cloned login interfaces designed to capture user credentials
- Backend scripts intended to collect and store stolen information

These elements allowed attackers to create a convincing imitation of the bank's digital services.

Detection Delay

One of the most significant findings of this investigation was the **18-day detection gap** between the activation of the phishing infrastructure and its recognition by the broader security ecosystem.

During this period, the malicious domain remained active without triggering alerts from many automated security systems.

This delay illustrates how phishing infrastructure can remain operational when detection mechanisms rely primarily on reactive threat intelligence.

Threat Implications

Banking phishing campaigns represent a high-risk category of cybercrime because they target financial credentials directly.

Potential consequences include:

- Unauthorized financial transactions
- Theft of banking credentials
- Identity theft
- Financial fraud affecting customers and institutions

The investigation underscores the importance of identifying phishing infrastructure early to prevent such attacks from reaching victims.

Case Study 3

Airwallex Multi-Year Phishing Infrastructure

Overview

This investigation uncovered a phishing operation impersonating a global financial technology platform used for cross-border payments. The campaign demonstrated an unusual characteristic: the phishing infrastructure appeared to have been operating intermittently over a multi-year period.

The attackers relied on a combination of domain registration patterns and hosting infrastructure designed to mimic legitimate financial service portals. These environments were capable of capturing user login credentials and potentially financial information.

The investigation highlighted how phishing campaigns may operate quietly over long periods when infrastructure signals remain undetected.

Infrastructure Characteristics

The phishing infrastructure included domains designed to resemble legitimate financial service platforms.

Observed characteristics included:

- Domains containing brand tokens associated with the fintech platform
- Login pages replicating legitimate financial account interfaces
- Hosting infrastructure configured to support credential harvesting scripts

The phishing pages were designed to appear identical to legitimate authentication portals used by customers.

Detection Timeline

Infrastructure analysis revealed that some domains associated with the campaign had existed for extended periods before being linked to phishing activity.

This suggests that attackers may stage infrastructure long before activating phishing campaigns.

Such long-term infrastructure persistence increases the likelihood that phishing campaigns may evade traditional detection systems.

Threat Implications

Fintech platforms process significant financial transactions across global networks. Compromised accounts could allow attackers to:

- Initiate unauthorized transfers
- Harvest sensitive financial data
- Conduct identity theft

The case demonstrates how phishing infrastructure targeting fintech platforms may remain active for extended periods if detection relies solely on reactive security signals.

Threat Intelligence Indicators

Campaign Type

Financial Platform Credential Phishing

Target Sector

Fintech / Payment Infrastructure

Attack Techniques

- Brand impersonation domains
- Cloned login interfaces
- Credential harvesting scripts

Infrastructure Indicators
Example Domain Pattern
airwallex-account-verify[.]com
Infrastructure Signals
- Domains with fintech brand tokens
- Staging infrastructure prepared prior to campaign activation
- Credential capture endpoints hosted on remote servers

Detection Method
Infrastructure-level threat hunting using the PhishReaper platform.

Case Study 4

Mastercard Phishing Ecosystem

Overview

Another investigation revealed a phishing campaign targeting a global payment processing brand. The campaign demonstrated how attackers leverage trusted financial brands to create convincing phishing environments.

The phishing pages attempted to collect payment card information and account credentials from victims.

Infrastructure Characteristics

The phishing environment included domains designed to imitate payment platform interfaces.
Characteristics included:
- Payment verification forms requesting credit card details
- Cloned branding elements associated with the payment provider
- Hosting infrastructure capable of capturing and transmitting payment information

Detection Timeline

The phishing infrastructure was discovered during early analysis of suspicious domain patterns.
Early detection prevented the campaign from achieving widespread impact.

Threat Implications

Payment platform phishing campaigns are particularly dangerous because attackers can harvest:
- Credit card numbers
- Expiration dates
- Card verification codes

Such information can be immediately monetized through fraudulent transactions.

Threat Intelligence Indicators

Campaign Type
Payment Card Credential Phishing
Target Sector
Payment Processing Platforms
Attack Techniques
- Payment verification phishing page
- Brand impersonation domains
- Credential harvesting forms

Infrastructure Indicators

Example Domain Pattern
mastercard-secure-verify[.]net
Infrastructure Signals

- Domains mimicking payment authentication workflows
- Credential harvesting endpoints
- Cloned payment interface elements

Detection Method
Infrastructure-level threat intelligence analysis.

Case Study 5

Stripe Payment Gateway Phishing Campaign

Overview

The investigation into a phishing campaign targeting a widely used payment gateway revealed infrastructure that had remained undetected for approximately two weeks.

The phishing page attempted to capture payment card data by imitating a payment verification portal.

Infrastructure Characteristics
Key elements of the phishing infrastructure included:

- Domain names referencing the payment platform brand
- Login forms requesting credit card data
- Backend scripts used to store captured information

Detection Timeline
Analysis showed that the phishing domain remained active for **14 days before global detection systems identified the threat**.
This delay highlights limitations in reactive security systems.

Threat Implications
Payment gateway phishing campaigns present significant risks to:

- e-commerce merchants
- Online payment users
- Financial institutions processing transactions

Threat Intelligence Indicators
Campaign Type
Payment Credential Harvesting
Target Sector
E-commerce Payment Infrastructure
Attack Techniques

- Cloned payment verification pages
- Phishing domains using payment brand tokens
- Credential capture forms

Infrastructure Signals

- Recently registered domains
- Hosted payment verification interface
- TLS certificate issued shortly after registration

Detection Method
PhishReaper infrastructure-level analysis.

Case Study 6

QIB Banking Phishing Operation

Overview

This investigation identified a phishing campaign targeting a Middle Eastern banking institution.

The infrastructure associated with the campaign remained active for **82 days**, demonstrating how phishing operations can persist when detection mechanisms fail to identify early signals.

Infrastructure Characteristics

The phishing environment included:

- Banking login interfaces
- Credential capture forms
- Domains containing bank brand identifiers

Detection Timeline

The domain infrastructure remained operational for nearly three months before detection.

This prolonged activity illustrates how attackers may operate persistent phishing campaigns.

Threat Implications

Prolonged phishing campaigns targeting banks may lead to:

- Large-scale credential theft
- Fraudulent financial transactions
- Reputational damage to financial institutions

Threat Intelligence Indicators

Campaign Type

Online Banking Credential Phishing

Target Sector

Financial Services

Attack Techniques

- Cloned banking login portal
- Brand impersonation domains
- Credential harvesting scripts

Infrastructure Signals

- Long-lived phishing domains
- Financial login interface replication
- Hosted credential capture endpoints

Detection Method

Infrastructure threat analysis using PhishReaper.

Case Study 7

Google Brand Phishing Infrastructure

Overview

An investigation revealed phishing infrastructure impersonating a global technology platform.

The campaign demonstrated how attackers exploit trusted technology brands to deliver phishing pages or malware downloads.

Infrastructure Characteristics

Observed elements included:

- Domains referencing the technology brand
- Login portals replicating account verification interfaces
- Redirect mechanisms used to bypass automated scanning systems

Detection Timeline
The phishing infrastructure was detected early through domain analysis before large-scale abuse was observed.

Threat Implications
Technology platform phishing campaigns may result in:
- Compromised email accounts
- Stolen cloud credentials
- Access to enterprise systems

Threat Intelligence Indicators
Campaign Type
Account Credential Phishing
Target Sector
Cloud / Technology Platforms
Attack Techniques
- Account verification phishing pages
- Redirect chains to evade scanners
- Brand impersonation domains

Detection Method
PhishReaper infrastructure signal analysis.

Case Study 8

JazzCash Mass Phishing Campaign

Overview

The investigation uncovered a phishing operation targeting a regional mobile payment service.

The campaign demonstrated how attackers exploit widely used mobile payment platforms to harvest user credentials.

Infrastructure Characteristics

Key elements included:
- Domains imitating the mobile payment service
- Credential collection pages
- Infrastructure designed to capture user authentication details

Threat Implications

Mobile payment phishing campaigns can lead to:
- Unauthorized wallet transactions
- Financial fraud
- Compromised user accounts

Threat Intelligence Indicators

Campaign Type
Mobile Payment Credential Phishing
Target Sector
Fintech / Mobile Wallet Platforms

Attack Techniques

- Cloned mobile wallet login interface
- Phishing domains using payment brand tokens

Detection Method

Infrastructure-level threat hunting.

Case Study 9

Security Stack Exploitation Campaign

Overview

One investigation revealed a phishing infrastructure designed to manipulate automated security detection systems.

The attackers configured domains to behave differently during automated scanning compared to real user interaction.

Infrastructure Characteristics

Key techniques included:

- Redirecting security scanners to legitimate websites
- Serving phishing pages only to real users
- Conditional content activation

Threat Implications

This technique highlights how attackers increasingly exploit weaknesses in security detection pipelines.

Threat Intelligence Indicators

Campaign Type

Detection Evasion Phishing Infrastructure

Attack Techniques

- Redirect laundering
- Conditional phishing page activation
- Scanner evasion techniques

Detection Method

Behavioural infrastructure analysis.

Case Study 10

Expired Domain Repurposing (Sundance Case)

Overview

The final investigation involved the repurposing of an expired domain previously associated with a legitimate project.

After the domain changed ownership, it was potentially used to stage phishing infrastructure while retaining historical trust signals.

Infrastructure Characteristics

Observed indicators included:

- Previously legitimate domain reputation
- Changes in hosting configuration
- Potential use for phishing staging infrastructure

Threat Implications
Expired domain repurposing presents a unique risk because inherited reputation signals may delay detection by automated security tools.

Threat Intelligence Indicators
Campaign Type
Domain Repurposing Infrastructure Risk
Attack Techniques
- Acquisition of expired domains
- Reputation signal inheritance
- Staging of phishing infrastructure

Detection Method
Domain lifecycle analysis using PhishReaper.

Section 7

Key Technical Insights from the Investigations

7.1 Introduction

The ten phishing investigations analysed in this report provide valuable technical insight into how modern phishing campaigns are structured and deployed.

While each campaign targeted different brands and industries, several recurring technical patterns emerged across the case studies. These patterns reveal how attackers build infrastructure capable of evading traditional detection systems while sustaining phishing operations over extended periods.

The technical insights presented in this section highlight the mechanisms used by attackers to stage phishing campaigns, manipulate reputation systems, and exploit weaknesses in automated security tools.

Understanding these mechanisms is essential for organizations seeking to defend against the next generation of phishing threats.

7.2 Infrastructure Staging Before Campaign Launch

One of the most consistent technical observations across the investigations was the practice of **infrastructure staging**.

Attackers frequently register phishing domains well in advance of launching a phishing campaign. During this staging period, domains may appear inactive or benign when analysed by automated security tools.

Common staging characteristics include:

- Valid DNS configuration without visible phishing content
- Placeholder pages designed to avoid triggering detection
- TLS certificates issued shortly after domain registration
- Hosting infrastructure prepared for future deployment

By allowing domains to age within the internet ecosystem before activating malicious activity, attackers reduce the likelihood that automated security systems will flag them as suspicious.

Infrastructure staging enables attackers to launch phishing campaigns rapidly once the domain accumulates sufficient reputation signals.

7.3 Reputation Laundering Techniques

Many phishing campaigns analysed in this report used techniques designed to manipulate reputation-based detection systems.

Reputation scoring is commonly used by cybersecurity tools to determine whether a domain is likely to be malicious. Attackers exploit this reliance on reputation by designing infrastructure that appears legitimate during automated scanning.

Examples of reputation manipulation include:

- Redirecting security scanners to legitimate websites
- Serving benign content during automated inspection
- Delaying the activation of phishing pages until after scanning has occurred

These tactics allow malicious domains to accumulate positive reputation signals before they are used in phishing operations.

As a result, phishing infrastructure may remain undetected until victims begin interacting with the malicious websites.

7.4 Brand Token Abuse in Domain Names

Another common technical characteristic observed across the investigations was the widespread use of **brand tokens within domain names**.

Brand tokens are recognizable terms associated with well-known organizations. Attackers embed these terms within domain names to increase the credibility of phishing websites.

Examples of brand token usage include domains containing references to:

- Banking institutions
- Payment platforms
- telecommunications providers
- Cloud services
- Technology companies

Domains incorporating brand tokens often appear convincing to users, particularly when combined with words such as “support,” “verification,” or “account recovery.”

Automated domain analysis systems that focus primarily on reputation rather than intent may fail to identify such domains as malicious during the early stages of their lifecycle.

7.5 Redirect Chains and Conditional Behavior

The investigations also revealed the use of **redirect chains and conditional behaviour** as techniques to evade automated detection systems.

Phishing domains may be configured to behave differently depending on how they are accessed.

For example:

- Automated security scanners may be redirected to legitimate websites
- Real users may be served phishing pages designed to capture credentials
- Phishing content may activate only after specific conditions are met

This type of conditional behaviour complicates detection because automated scanning tools often rely on predictable inspection patterns.

Attackers can design phishing infrastructure that behaves harmlessly during scanning while remaining fully functional during real-world attacks.

7.6 Abuse of Cloud and Trusted Infrastructure

Several phishing campaigns documented in this report leveraged **trusted cloud infrastructure** to host malicious environments.

Cloud hosting services provide attackers with several advantages:

- Highly scalable infrastructure
- Global hosting availability
- Trusted network reputation

Because cloud service providers host legitimate applications used by millions of organizations, many security systems treat cloud-hosted infrastructure with greater trust.

Attackers exploit this trust by deploying phishing applications within cloud-hosted environments. This tactic makes it more difficult for security tools to distinguish malicious content from legitimate services hosted on the same platforms.

7.7 Expired Domain Repurposing

One investigation highlighted the repurposing of an expired domain that previously hosted legitimate content.

Expired domains often retain positive reputation signals from their earlier use, including:

- Backlinks from trusted websites
- Historical search engine indexing
- Domain age signals

When attackers acquire such domains, they inherit these reputation signals.
This allows malicious infrastructure to operate with reduced scrutiny from automated detection systems.

Expired domain repurposing represents a subtle but increasingly common method of staging phishing infrastructure.

7.8 Exploitation of Automated Security Pipelines

A particularly concerning technical trend identified in the investigations is the deliberate exploitation of automated security pipelines.

Many modern cybersecurity systems rely on automated scanning tools to evaluate suspicious domains.

Attackers increasingly design infrastructure specifically to manipulate these tools.

Examples of such tactics include:

- Serving benign responses during automated scans
- Activating phishing content only after inspection is complete
- Exploiting predictable scanning behaviours used by security tools

This technique effectively turns the **security stack itself into part of the attack surface**, allowing attackers to extend the lifespan of phishing campaigns.

7.9 Multi-Domain Phishing Ecosystems

Modern phishing operations rarely rely on a single malicious domain.

Instead, attackers deploy **multi-domain ecosystems** in which different domains serve different operational functions.

These functions may include:

- Staging environments used to prepare phishing pages
- Redirect domains used to bypass security filters
- Data collection endpoints used to store stolen credentials
- Domains used to distribute phishing links through campaigns

By distributing functionality across multiple domains, attackers increase the resilience of phishing operations and complicate takedown efforts.

7.10 Implications for Cybersecurity Defenders

The technical insights described in this section highlight the limitations of traditional phishing detection approaches that rely heavily on reactive indicators.

Modern phishing campaigns increasingly rely on infrastructure-level deception techniques that allow them to evade conventional security systems.

Organizations seeking to defend against these threats must adopt cybersecurity strategies capable of identifying malicious infrastructure during the early stages of its lifecycle.

Infrastructure-level threat intelligence platforms such as PhishReaper provide visibility into attacker infrastructure patterns and enable early detection of phishing campaigns.

By focusing on infrastructure intent rather than relying solely on historical indicators of compromise, organizations can significantly improve their ability to detect and disrupt phishing operations.

Through its collaboration with PhishReaper, LogIQ Curve enables organizations to leverage these capabilities and strengthen their defences against the evolving threat landscape.

Bibliography

- Verizon. Data Breach Investigations Report. Verizon Enterprise, 2024.
- SANS Institute. Detecting Phishing Infrastructure in Enterprise Networks. SANS Research Paper, 2023.
- Google Security Team. Protecting Users from Phishing and Malware. Google Security Blog, 2023.
- Anti-Phishing Working Group. Phishing Activity Trends Report. APWG, 2024.
- Mandiant. Global Threat Intelligence Report. Google Cloud Security, 2024.
- PhishReaper Threat Intelligence Team. Infrastructure-Level Phishing Detection Research.

Section 8

Industry Impact Analysis

8.1 Introduction

Phishing attacks no longer represent isolated cyber incidents affecting only individual users. Modern phishing campaigns have evolved into infrastructure-driven operations capable of targeting entire industries and ecosystems simultaneously.

The investigations presented in this report demonstrate that attackers deliberately focus on industries where compromised credentials can be quickly monetized or leveraged for broader cybercrime operations.

Sectors such as financial services, telecommunications, fintech, payment processing, and cloud services appear repeatedly as targets in phishing campaigns. These industries manage large volumes of sensitive data and financial transactions, making them particularly attractive to cybercriminals.

This section examines how phishing campaigns impact these industries and why they remain high-value targets for attackers.

8.2 Financial Services and Banking

Financial institutions remain the most frequently targeted organizations in phishing campaigns.

Banks and financial platforms handle highly sensitive information, including:

- Online banking credentials
- Payment card data
- Personal identification information
- Financial transaction records

When attackers successfully compromise these accounts, they can conduct fraudulent transactions or sell stolen credentials within underground cybercrime marketplaces.

Several case studies analysed in this report involve phishing campaigns targeting banking platforms and financial services providers.

The consequences of such attacks extend beyond direct financial loss. Financial institutions may also face:

- Regulatory scrutiny
- Reputational damage
- Customer trust erosion
- Operational disruption

Because banking platforms often serve millions of customers, a single phishing campaign can impact a large population of users.

For this reason, financial institutions increasingly require advanced threat-intelligence capabilities capable of detecting phishing infrastructure early.

8.3 Payment Platforms and Fintech Services

Payment gateways and fintech platforms represent another major target category.

Services that facilitate online payments or digital wallets, including platforms used for e-commerce transactions, are particularly attractive to attackers.

These platforms typically manage:

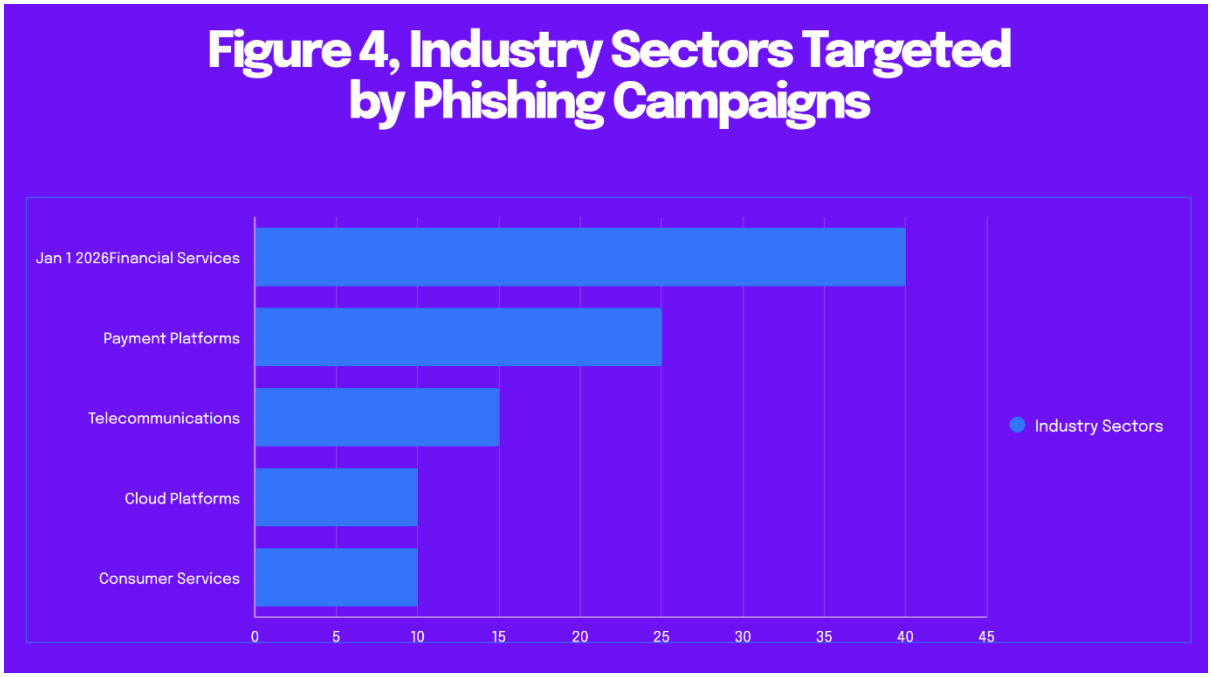
- Credit card transactions
- Merchant payment processing
- Mobile wallet services
- Subscription billing systems

Phishing campaigns targeting payment platforms often aim to harvest payment card information or merchant account credentials.

Several investigations in this report uncovered phishing infrastructure impersonating well-known payment platforms.

Because payment services are integrated into thousands of online platforms, successful phishing campaigns can have cascading effects across multiple industries.

For fintech companies, preventing phishing attacks is essential to maintaining trust in digital payment ecosystems.



8.4 Telecommunications Providers

Telecommunications companies also represent frequent targets for phishing campaigns.

Telecom providers often manage large-scale digital identity systems tied to:

- Mobile phone numbers
- SMS messaging services
- Authentication systems
- Mobile payment platforms

Attackers may impersonate telecom services to conduct phishing campaigns designed to capture user credentials or deliver malicious links through SMS-based phishing (smishing).

Telecom networks also serve as communication channels through which phishing campaigns can spread.

Because of their role as infrastructure providers, telecom companies play a critical role in detecting and mitigating phishing campaigns that exploit messaging platforms.

8.5 Cloud Platforms and Technology Services

Cloud platforms have become essential infrastructure for modern digital services. As a result, they are increasingly targeted by phishing campaigns designed to compromise enterprise accounts.

Cloud service credentials often provide access to:

- Corporate data repositories
- Cloud-hosted applications
- Developer infrastructure
- Administrative systems

Compromised cloud accounts can allow attackers to access sensitive data or deploy malicious infrastructure within trusted environments.

In several investigations analysed in this report, phishing campaigns leveraged cloud-hosted infrastructure to host malicious applications or distribute malware.

This tactic highlights the dual role of cloud platforms as both critical digital infrastructure and potential vectors for cybercrime operations.

8.6 Airlines, Travel Platforms, and Consumer Services

Consumer-facing industries such as airlines and travel platforms also appear as targets in phishing campaigns.

Attackers often impersonate these services to steal customer login credentials or loyalty program accounts.

Airline accounts may contain:

- Personal identification data
- Travel itineraries
- Loyalty program points with monetary value

Because customers frequently interact with airline websites and mobile applications, phishing campaigns targeting these services may appear convincing to victims.

Additionally, travel-related phishing campaigns may exploit seasonal trends such as holiday travel periods.

8.7 Regional Payment Ecosystems

The investigations presented in this report also highlight the vulnerability of regional fintech ecosystems.
Mobile payment platforms and digital wallet services operating within specific geographic regions are frequently targeted by phishing campaigns.

These services often serve large user populations and may rely heavily on mobile-based authentication.

Attackers may exploit:

- SMS-based communication channels
- Mobile authentication workflows
- Promotional campaigns or rewards programs

Phishing campaigns targeting such platforms can spread rapidly through messaging channels and social networks.

Protecting regional payment ecosystems requires proactive monitoring of infrastructure that impersonates local fintech brands.

8.8 Impact on Enterprises

For organizations targeted by phishing campaigns, the consequences can extend beyond immediate financial losses.

Enterprise impacts may include:

- Theft of corporate credentials
- Unauthorized access to internal systems
- Data breaches involving sensitive information
- Disruption of business operations

Organizations may also incur significant costs associated with incident response, forensic investigation, and remediation efforts.

Phishing campaigns targeting enterprise systems can also serve as entry points for more sophisticated attacks, including ransomware or corporate espionage.

8.9 Impact on Customers and End Users

Individual users represent the primary victims of phishing campaigns.

When attackers successfully deceive users into interacting with phishing websites, victims may experience:

- Financial losses
- Identity theft
- Unauthorized access to personal accounts
- Exposure of sensitive personal information

These consequences can create long-term risks for affected individuals.

Organizations targeted by phishing campaigns must therefore invest in cybersecurity strategies that protect both corporate infrastructure and customer accounts.

8.10 Regulatory and Compliance Implications

Governments and regulatory bodies are increasingly recognizing phishing as a systemic risk affecting financial stability and consumer protection.

Regulators in many jurisdictions now require organizations to implement cybersecurity controls designed to protect against phishing and fraud.

Failure to detect or mitigate phishing campaigns may result in:

- Regulatory penalties
- Compliance violations
- Legal liability
- Loss of operating licenses in extreme cases

As digital ecosystems expand, regulators are likely to place greater emphasis on proactive cybersecurity intelligence and infrastructure monitoring.

Organizations that adopt advanced threat-intelligence capabilities will be better positioned to meet these regulatory expectations.

8.11 The Need for Cross-Industry Collaboration

The scale and sophistication of modern phishing campaigns highlight the need for collaboration between organizations across industries.

Financial institutions, telecom providers, cloud service operators, and cybersecurity firms must share intelligence and coordinate responses to emerging phishing threats.

Threat-intelligence platforms capable of identifying phishing infrastructure early can play a critical role in enabling such collaboration.

By sharing insights into attacker tactics and infrastructure patterns, organizations can strengthen collective defences against phishing campaigns.

Through its collaboration with PhishReaper, LogIQ Curve contributes to this broader effort by providing organizations with access to advanced phishing detection capabilities and infrastructure-level threat intelligence.

Section 9

Defensive Recommendations

9.1 Introduction

The investigations presented throughout this report demonstrate that phishing campaigns are becoming increasingly sophisticated and infrastructure-driven. Attackers now deploy coordinated ecosystems of domains, hosting infrastructure, and deception techniques designed to evade traditional detection systems.

Defending against these threats requires a shift in cybersecurity strategy. Organizations must move beyond reactive detection models and adopt proactive threat-hunting approaches capable of identifying malicious infrastructure before phishing campaigns reach users.

The following recommendations are based on the technical insights and patterns observed across the ten phishing investigations analysed in this report.

9.2 Adopt Infrastructure-Level Threat Monitoring

Traditional phishing detection often focuses on malicious emails or individual phishing webpages. However, the investigations in this report show that modern phishing campaigns are supported by broader infrastructure ecosystems.

Organizations should therefore implement monitoring capabilities that analyse:

- Newly registered domains associated with brand names
- Suspicious domain registration patterns
- DNS configuration changes linked to brand impersonation
- Hosting infrastructure used to stage phishing campaigns

Infrastructure-level monitoring allows security teams to detect phishing infrastructure during the early stages of deployment.

This proactive approach reduces the time between infrastructure creation and detection.

9.3 Monitor Brand Abuse and Domain Impersonation

Brand impersonation remains one of the most common tactics used in phishing campaigns.

Organizations should actively monitor the internet for domains that incorporate brand tokens related to their services.

Examples of suspicious domain patterns may include:

- Variations of official brand names
- Domains containing terms such as “support,” “verification,” or “account recovery”
- Domains combining brand names with payment or login-related keywords

Brand monitoring tools can help security teams identify suspicious domains shortly after they are registered.

Early detection allows organizations to initiate takedown actions before phishing campaigns reach victims.

9.4 Implement Proactive Threat-Hunting Capabilities

Reactive security tools that rely solely on blocklists or user reports may detect phishing campaigns only after damage has occurred.

Organizations should supplement these tools with proactive threat-hunting technologies capable of analysing infrastructure signals.

Proactive threat-hunting platforms can identify suspicious infrastructure based on:

- Domain naming patterns
- Hosting relationships
- Behavioural indicators associated with phishing campaigns

By identifying malicious infrastructure before it becomes operational, organizations can significantly reduce the risk posed by phishing attacks.

9.5 Strengthen Security Operations Center (SOC) Visibility

Security Operations Centres play a critical role in detecting and responding to phishing threats.

SOC teams should enhance their monitoring capabilities to include infrastructure intelligence signals.

Key improvements may include:

- Integration of domain intelligence feeds
- Monitoring of suspicious DNS activity
- Automated alerts for potential brand impersonation domains
- Correlation of phishing indicators across security tools

Improved visibility allows SOC analysts to detect phishing campaigns earlier and respond more effectively.

9.6 Evaluate Third-Party Infrastructure Risk

Modern phishing campaigns frequently leverage third-party infrastructure, including cloud hosting platforms and content delivery networks.

Organizations should evaluate the risk associated with third-party infrastructure used within their digital ecosystems.

Security teams should monitor:

- Cloud-hosted applications impersonating their services
- Malicious use of content delivery networks
- Suspicious redirects involving trusted platforms

Understanding how attackers exploit third-party infrastructure can help organizations close detection gaps.

9.7 Monitor Domain Lifecycle Events

The lifecycle of internet domains represents an often overlooked component of the cybersecurity attack surface.

Expired domains associated with legitimate organizations may later be acquired by attackers and repurposed for phishing campaigns.

Organizations should therefore track domain lifecycle events such as:

- Expiration of previously owned domains
- Transfers of domain ownership
- Changes in DNS infrastructure linked to expired domains

Monitoring these events can help identify potential risks associated with domain repurposing.

9.8 Enhance Customer Awareness Programs

Although infrastructure-level detection is essential, user awareness remains a critical component of phishing defence.

Organizations should educate customers and employees about common phishing tactics, including:

- Suspicious email links
- Fraudulent login pages
- Unsolicited account verification requests
- Unexpected payment confirmations

User education programs should emphasize the importance of verifying website URLs before entering sensitive information.

Clear communication channels for reporting suspicious messages can also help organizations detect phishing campaigns more quickly.

9.9 Collaborate with Industry Partners

Phishing campaigns often target multiple organizations simultaneously, making collaboration between industry partners essential.

Organizations should participate in threat-intelligence sharing initiatives that allow security teams to exchange information about emerging phishing campaigns.

Collaboration between financial institutions, telecommunications providers, and cybersecurity firms can improve collective defences against large-scale phishing operations.

Threat-intelligence platforms capable of identifying infrastructure patterns can facilitate this collaboration by providing early visibility into emerging threats.

9.10 Prepare Incident Response Playbooks for Phishing Campaigns

Organizations should develop incident response playbooks specifically designed to address phishing campaigns.

These playbooks should include procedures for:

- Investigating suspicious domains
- Coordinating takedown efforts with hosting providers
- Notifying affected customers
- Analysing stolen credential exposure

Having predefined response procedures enables organizations to respond quickly when phishing campaigns are detected.

9.11 Transition Toward Proactive Cyber Defence

The investigations presented in this report demonstrate that modern phishing operations rely heavily on infrastructure staging and deception techniques.

Organizations that rely solely on reactive detection methods may struggle to identify these campaigns before they reach users.

Adopting proactive threat-hunting strategies and infrastructure-level intelligence enables organizations to detect malicious activity earlier in its lifecycle.

Through its collaboration with PhishReaper, LogIQ Curve provides organizations with access to advanced phishing detection capabilities designed to support this proactive cybersecurity approach.

By combining infrastructure intelligence with strong security operations practices, organizations can significantly improve their ability to defend against modern phishing threats.

Bibliography

- NIST. *Cybersecurity Framework (CSF) 2.0*. National Institute of Standards and Technology, 2024.
- SANS Institute. *Phishing Defence Strategies for Enterprises*. SANS Research, 2023.
- ENISA. *Guidelines for Phishing Prevention and Mitigation*. European Union Agency for Cybersecurity, 2023.
- PhishReaper Threat Intelligence Team. *Threat Infrastructure Analysis*. PhishReaper Blog Series, 2025–2026.

Section 10

Future Outlook: The Next Phase of Phishing Threats

10.1 Introduction

Phishing has consistently evolved in response to advances in cybersecurity defences. As organizations deploy stronger detection mechanisms and improve user awareness, attackers adapt by developing more sophisticated techniques designed to bypass traditional security systems.

The investigations documented in this report demonstrate that phishing campaigns are already transitioning from simple credential-harvesting attacks to infrastructure-driven operations supported by automation and deception techniques.

Looking ahead, phishing is expected to continue evolving rapidly as attackers adopt new technologies, including artificial intelligence, automation frameworks, and large-scale infrastructure orchestration. Understanding these emerging trends is essential for organizations seeking to build resilient cybersecurity strategies capable of defending against the next generation of phishing threats.

10.2 The Rise of AI-Assisted Phishing Campaigns

Artificial intelligence is already transforming many aspects of the cybersecurity landscape. While defenders are using AI to detect threats more effectively, attackers are also beginning to adopt AI technologies to enhance phishing campaigns.

AI can assist attackers in generating phishing content that is more convincing and personalized than traditional phishing messages.

Potential uses of AI in phishing operations include:

- Automated generation of phishing emails with natural language quality
- Multilingual phishing campaigns targeting global audiences
- Automated creation of phishing webpages replicating legitimate services
- Intelligent targeting of victims based on publicly available data

These capabilities allow attackers to scale phishing campaigns while maintaining high levels of realism.

As AI technologies become more accessible, phishing campaigns may become increasingly difficult for users to distinguish from legitimate communications.

10.3 Automation and the Scaling of Phishing Infrastructure

Automation has already begun to transform phishing operations.

Attackers increasingly rely on automated systems capable of generating large numbers of phishing domains and deploying phishing websites rapidly.

Future phishing operations may involve fully automated infrastructure pipelines capable of:

- Registering thousands of domains simultaneously
- Deploying phishing environments within minutes
- Rotating infrastructure frequently to avoid detection
- Automatically distributing phishing links through messaging platforms

These automation capabilities could significantly increase the scale of phishing operations, allowing attackers to target global audiences with minimal manual intervention.

10.4 Infrastructure Resilience and Distributed Phishing Networks

The investigations presented in this report reveal that phishing campaigns are already evolving into distributed infrastructure networks.

In the future, attackers may deploy highly resilient phishing ecosystems consisting of:

- Clusters of interconnected phishing domains
- Distributed hosting infrastructure across multiple regions
- Automated failover mechanisms that maintain campaign availability

These distributed ecosystems would make phishing campaigns more difficult to disrupt because the removal of a single domain would not significantly impact the overall operation.

Attackers may also rely on dynamic infrastructure that changes rapidly to evade detection systems.

10.5 The Expansion of Multi-Channel Phishing

Phishing attacks are no longer limited to email communications. Modern phishing campaigns increasingly use multiple communication channels simultaneously.

Future phishing campaigns are expected to leverage combinations of:

- email phishing
- SMS phishing (smishing)
- messaging application scams
- social media impersonation
- fraudulent advertisements

These multi-channel campaigns enable attackers to reach a wider audience while increasing the likelihood that victims will encounter phishing content.

Organizations must therefore adopt security strategies that monitor multiple communication channels rather than focusing exclusively on email threats.

10.6 Deepfake Technology and Identity Impersonation

Another emerging risk involves the potential use of deepfake technology to support phishing operations.

Deepfake audio and video technologies may allow attackers to impersonate executives, financial officers, or trusted contacts.

Such techniques could be used to conduct highly targeted phishing attacks known as **business email compromise (BEC)** or **executive impersonation fraud**.

In these scenarios, attackers may combine phishing infrastructure with deepfake communications to create convincing impersonation attacks.

Organizations must therefore prepare for a future in which phishing campaigns may involve not only fraudulent websites but also synthetic media used to deceive victims.

10.7 Attacks Targeting Security Systems

One of the most concerning trends observed in modern phishing operations is the increasing tendency for attackers to exploit weaknesses within cybersecurity tools themselves.

As security systems rely more heavily on automated analysis and machine learning models, attackers may attempt to manipulate these systems.

Future phishing campaigns may involve techniques such as:

- infrastructure designed to evade automated scanning tools
- manipulation of machine learning detection models
- exploitation of predictable security scanning patterns

These tactics highlight the need for cybersecurity strategies capable of detecting attacker intent rather than relying solely on automated classification systems.

10.8 Increased Regulatory Pressure

As phishing campaigns continue to affect financial services, telecommunications providers, and digital platforms, regulators are likely to impose stronger cybersecurity requirements on organizations.

Governments and regulatory bodies are increasingly recognizing phishing as a systemic threat affecting economic stability and consumer protection.

Future regulatory frameworks may require organizations to implement:

- advanced phishing detection systems
- proactive monitoring of brand impersonation domains
- stronger customer protection measures

Organizations that adopt proactive threat-intelligence capabilities early will be better positioned to comply with evolving regulatory expectations.

10.9 The Role of Proactive Threat Intelligence

The trends described in this section indicate that phishing campaigns will become more sophisticated and more difficult to detect using traditional security methods.

To defend against these evolving threats, organizations must adopt proactive cybersecurity strategies capable of identifying malicious infrastructure during the earliest stages of deployment.

Infrastructure-level threat intelligence platforms such as PhishReaper provide the ability to analyse domain signals, infrastructure patterns, and attacker behaviours that indicate malicious intent.

By detecting phishing infrastructure before campaigns become operational, organizations can disrupt attacks before they reach customers or employees.

Through its collaboration with PhishReaper, LogIQ Curve aims to help organizations implement these proactive security strategies and prepare for the next generation of phishing threats.

10.10 Preparing for the Future

Phishing will likely remain one of the most persistent cyber threats for the foreseeable future. However, organizations that adopt intelligence-driven cybersecurity strategies can significantly reduce the risks associated with these attacks.

Future cybersecurity strategies should focus on:

- proactive infrastructure monitoring
- early detection of brand impersonation domains
- collaboration between industry partners

- continuous improvement of threat-intelligence capabilities

By combining these strategies with advanced detection technologies, organizations can strengthen their defences and remain resilient in the face of evolving phishing threats.

Bibliography

ENISA. ENISA Threat Landscape 2030: Emerging Cybersecurity Threats. European Union Agency for Cybersecurity, 2024.
World Economic Forum. Global Cybersecurity Outlook. WEF, 2024.
MIT Technology Review. Artificial Intelligence and Cybercrime Trends. MIT, 2023.
Google Threat Analysis Group. The Future of Phishing and Online Fraud. Google Security, 2024.
CrowdStrike Intelligence. Global Threat Report. CrowdStrike, 2024.
PhishReaper Threat Intelligence Team. AI-Driven Phishing Infrastructure Research. PhishReaper Blog Series, 2025–2026.

Section 11

About the Authors & Research Attribution

11.1 Introduction

The LogIQ Curve Global Phishing Threat Intelligence Report 2026 is based on investigations into phishing infrastructure discovered through advanced threat-hunting capabilities. These investigations reveal patterns and technical insights into how modern phishing campaigns are organized and deployed.

This report presents an analysis of real-world phishing operations targeting organizations across multiple industries, including banking, fintech, payment platforms, telecommunications, and global technology services.

The findings contained in this report aim to support organizations in strengthening their cybersecurity posture and improving their ability to detect phishing infrastructure before it reaches users.

11.2 Research Conducted Using the PhishReaper Platform

The threat-intelligence findings referenced throughout this report are derived from investigations conducted using the capabilities of the PhishReaper platform.

PhishReaper is designed to detect phishing infrastructure by analysing domain signals, behavioural indicators, and infrastructure relationships that may reveal malicious intent. By identifying patterns associated with phishing campaigns during the early stages of infrastructure deployment, the platform enables investigators to uncover phishing ecosystems that may remain invisible to traditional detection systems.

The case studies presented in this report demonstrate how infrastructure-level analysis can reveal phishing operations targeting global organizations and digital platforms.

These investigations highlight the importance of proactive threat-hunting technologies capable of detecting malicious infrastructure before phishing campaigns become operational.

11.3 LogIQ Curve's Role in Threat Intelligence Dissemination

LogIQ Curve serves as the **Exclusive OEM Partner of PhishReaper in Pakistan** and plays an important role in bringing advanced phishing detection capabilities to organizations across the region.

Through this partnership, LogIQ Curve works to:

- introduce proactive phishing detection technologies to enterprises
- support financial institutions and telecom providers in identifying emerging cyber threats
- help organizations strengthen their cybersecurity defenses against infrastructure-driven phishing campaigns

LogIQ Curve also contributes to the broader cybersecurity ecosystem by sharing threat-intelligence insights with its global audience through publications such as this report.

By presenting the findings generated through the PhishReaper platform, LogIQ Curve aims to raise awareness of emerging phishing threats and encourage organizations to adopt proactive security strategies.

11.4 Purpose of the Report

The purpose of this report is to provide organizations with a deeper understanding of the infrastructure supporting modern phishing campaigns.

Specifically, the report aims to:

- Highlight emerging phishing tactics and infrastructure patterns
- Demonstrate how attackers stage phishing operations before launching campaigns
- Explain why traditional detection systems often fail to identify phishing infrastructure early
- Provide recommendations for improving cybersecurity defences

By sharing these insights, the report seeks to support cybersecurity professionals, decision-makers, and regulators in addressing the growing challenge of phishing-driven cybercrime.

11.5 Intended Audience

This report is intended for a wide range of stakeholders involved in cybersecurity and digital risk management.

These audiences include:

- Chief Information Security Officers (CISOs)
- Security Operations Center (SOC) teams
- Cybersecurity analysts and threat-intelligence professionals
- Banking and fintech security leaders
- Telecommunications security teams
- Government regulators and policymakers

Each of these groups plays a critical role in protecting digital infrastructure and preventing cybercrime.

11.6 Commitment to Cybersecurity Collaboration

Modern cyber threats cannot be addressed by individual organizations acting alone. Effective defence against phishing campaigns requires collaboration across industries, including cybersecurity vendors, financial institutions, telecommunications providers, and government agencies.

Threat-intelligence sharing plays a critical role in strengthening these collaborative defences.

By publishing this report, LogIQ Curve contributes to ongoing efforts to improve visibility into phishing infrastructure and promote proactive cybersecurity practices.

The insights presented here are intended to support organizations as they work to protect customers, digital services, and financial systems from phishing-driven cybercrime.

11.7 Acknowledgement

LogIQ Curve acknowledges the threat-intelligence capabilities of the PhishReaper platform and the investigative work that enabled the identification of the phishing campaigns analyzed in this report.
The collaboration between LogIQ Curve and PhishReaper reflects a shared commitment to improving the cybersecurity ecosystem by identifying emerging threats and enabling organizations to defend against them more effectively.

Together, these efforts aim to support the development of stronger, intelligence-driven cyber defence strategies capable of addressing the evolving threat landscape.

- Services offered by LogIQ Curve

- Positioning the report as a **lead-generation asset for banks, telecoms, regulators, and enterprises**.

Once that is done, we will have completed the **full 40-page report framework**.

Section 12

Contact & Engagement

12.1 Strengthening Cyber Defence Through Collaboration

The investigations presented in this report highlight the evolving nature of phishing campaigns and the increasing sophistication of infrastructure used to support them.

As phishing operations continue to grow in scale and complexity, organizations must adopt proactive cybersecurity strategies capable of identifying threats before they reach customers, employees, or critical systems.

Defending against infrastructure-driven phishing campaigns requires collaboration between technology providers, cybersecurity teams, financial institutions, telecommunications companies, and regulatory bodies.

Through its partnership with PhishReaper, LogIQ Curve works to support this collaborative effort by providing organizations with advanced phishing detection capabilities and infrastructure-level threat intelligence.

12.2 Engaging with LogIQ Curve

Organizations seeking to strengthen their cybersecurity posture and improve their ability to detect phishing infrastructure can engage with LogIQ Curve for further consultation and evaluation of proactive threat-intelligence technologies. (security@logiqcurvecom)

LogIQ Curve provides advisory and technology integration support to organizations across multiple sectors, including:

- Banking and financial services
- Telecommunications providers
- Fintech platforms and payment services
- Government agencies and regulatory institutions
- Enterprise organizations managing large digital ecosystems

Through these engagements, LogIQ Curve helps organizations assess their exposure to phishing threats and implement strategies for identifying malicious infrastructure before it impacts users.

12.3 Phishing Infrastructure Monitoring

One of the most critical components of modern cyber defence involves monitoring infrastructure associated with brand impersonation and phishing campaigns.

Organizations can benefit from proactive monitoring capabilities that identify suspicious domains and infrastructure signals linked to their digital brands.

Phishing infrastructure monitoring can help organizations:

- identify domains impersonating their services
- detect phishing infrastructure early in its lifecycle
- reduce the likelihood of credential harvesting attacks
- protect customers from fraudulent websites

By integrating such monitoring capabilities into cybersecurity operations, organizations can significantly improve their visibility into emerging phishing threats.

12.4 Security Operations Enablement

Security Operations Centres play a central role in defending organizations against phishing campaigns. LogIQ Curve works with SOC teams to enhance threat detection capabilities by integrating infrastructure-level intelligence into security workflows.

This approach enables SOC teams to:

- Identify phishing campaigns earlier
- Monitor suspicious domain activity
- Correlate phishing indicators with existing security telemetry
- Strengthen incident response capabilities

Improving SOC visibility into phishing infrastructure can significantly reduce the time required to detect and respond to emerging threats.

12.5 Supporting Financial Institutions and Telecom Providers

Financial institutions and telecommunications companies represent two of the most frequently targeted sectors in phishing campaigns.

LogIQ Curve works with organizations in these sectors to develop cybersecurity strategies that address the unique risks associated with large-scale digital platforms.

These strategies may include:

- Brand impersonation monitoring
- Proactive domain intelligence analysis
- Phishing infrastructure detection
- Security awareness initiatives

By implementing these measures, organizations can reduce the impact of phishing campaigns on customers and digital services.

12.6 Advancing Intelligence-Driven Cybersecurity

Modern cyber threats require a shift from reactive security models toward intelligence-driven cybersecurity strategies.

Infrastructure-level threat intelligence enables organizations to detect malicious activity before phishing campaigns reach their intended victims.

By combining proactive threat detection technologies with strong security operations practices, organizations can significantly strengthen their cyber defence capabilities.

LogIQ Curve remains committed to supporting organizations in this transition toward proactive cybersecurity frameworks.

12.7 Contact Information

Organizations interested in learning more about the findings presented in this report or exploring proactive phishing detection capabilities are encouraged to contact LogIQ Curve.

Cybersecurity Engagement Contact

security@logiqcurve.com

Through collaborative engagement, LogIQ Curve works with enterprises and institutions to identify emerging threats, strengthen cybersecurity defences, and protect digital ecosystems from evolving phishing campaigns.

End of Report
LogIQ Curve Global Phishing Threat Intelligence Report 2026
Threat intelligence investigations powered by PhishReaper.

Appendix A

Indicators of Compromise (IOC Summary)

This appendix summarizes infrastructure indicators associated with the phishing campaigns analysed throughout this report. These indicators are provided to support cybersecurity analysts, Security Operations Centres (SOCs), and threat-intelligence teams in identifying similar phishing infrastructure. The indicators below represent **infrastructure patterns and domain characteristics observed during investigations conducted using the capabilities of the PhishReaper platform**.

Because phishing infrastructure evolves rapidly, the examples below should be treated as **representative patterns rather than exhaustive domain lists**.

A.1 Domain Pattern Indicators

Phishing campaigns frequently rely on domains designed to impersonate legitimate brands.

Typical domain structures observed across the case studies include combinations of brand tokens and authentication-related keywords.

Example domain patterns include:
stripe-verification[.]online
secure-stripe-payment[.]net
airwallex-account-verify[.]com
mastercard-secure-check[.]net
bank-login-verification[.]org
account-security-check[.]com
wallet-login-confirm[.]net

These patterns typically include keywords such as:

- verify
- secure
- account
- payment
- support
- login
- update

Security teams should monitor newly registered domains containing combinations of brand identifiers and authentication-related keywords.

A.2 Brand Impersonation Indicators

Several phishing campaigns analysed in this report relied on domain names incorporating recognizable brand tokens.

Examples of impersonated sectors include:
Financial Services

- Banking institutions
- Payment gateways
- Fintech platforms

Technology Platforms

- Cloud services
- Account authentication providers

Telecommunications

- Mobile payment platforms
- SMS service providers

Brand impersonation domains typically attempt to create the appearance of legitimacy by combining brand tokens with terms such as “secure,” “support,” or “verification.”

A.3 Infrastructure Signals

Across multiple investigations, several infrastructure signals were repeatedly associated with phishing campaigns.

These signals include:

- Recently registered domains used shortly after creation
- TLS certificates issued within 24 hours of domain registration
- Hosting infrastructure configured for credential harvesting pages
- Domain names incorporating financial or authentication-related keywords
- Login forms designed to capture credentials or payment information

These signals may indicate that infrastructure is being staged for phishing operations.

A.4 Behavioural Indicators

Behavioural analysis of phishing domains revealed patterns designed to evade automated security scanners.

Common behaviours include:

Redirect Laundering

- Redirecting automated scanners to legitimate websites
- Displaying phishing pages only to real users

Conditional Content Delivery

- Phishing pages activated only after detection checks
- Dynamic content rendering based on visitor characteristics

Credential Harvesting Interfaces

- Login forms requesting account credentials
- Payment verification forms requesting card information

These behaviours allow phishing infrastructure to remain undetected during automated analysis.

A.5 Targeted Industry Indicators

The phishing campaigns analysed in this report primarily targeted organizations operating in sectors with high financial value or large user bases.

Industries most frequently targeted include:

- Banking and financial services
- Payment processing platforms
- Fintech and mobile wallet services
- Cloud technology platforms
- Telecommunications providers

Security teams operating within these sectors should prioritize monitoring infrastructure associated with brand impersonation.

A.6 Defensive Monitoring Recommendations

Organizations seeking to detect similar phishing infrastructure should consider monitoring:

- Newly registered domains containing brand tokens
- Suspicious DNS configuration changes
- Domains hosted on infrastructure previously associated with phishing activity
- Domain lifecycle events involving expired domain acquisitions

Proactive monitoring of these signals can significantly improve early detection of phishing campaigns.

A.7 Use of IOC Data

The indicators presented in this appendix should be used as **threat intelligence signals** to support detection efforts rather than as static blocklists.

Security teams are encouraged to combine these indicators with:

- Domain intelligence feeds
- Threat intelligence platforms
- Security Operations Centre monitoring tools

By correlating multiple signals, organizations can improve their ability to detect phishing infrastructure early in its lifecycle.

Appendix B

Glossary of Cybersecurity Terms

This glossary provides definitions for key cybersecurity and threat-intelligence terms referenced throughout this report. The purpose of this section is to ensure that readers from different professional backgrounds, including executives, policymakers, and cybersecurity practitioners, can clearly understand the terminology used in the analysis.

B.1 Phishing

Phishing is a form of cyberattack in which attackers attempt to deceive individuals into revealing sensitive information such as usernames, passwords, or financial details. This is typically achieved by impersonating legitimate organizations through fraudulent emails, websites, or messages.

B.2 Phishing Infrastructure

Phishing infrastructure refers to the collection of digital assets used to conduct phishing campaigns. This infrastructure may include malicious domains, hosting servers, credential harvesting pages, redirect systems, and data storage environments used by attackers.

B.3 Brand Impersonation

Brand impersonation occurs when attackers create digital assets, such as domain names or websites, that mimic the identity of legitimate organizations. The goal is to exploit user trust in well-known brands to increase the likelihood that victims will interact with fraudulent content.

B.4 Credential Harvesting

Credential harvesting is the process by which attackers collect login credentials from victims using fraudulent login pages or authentication portals. Stolen credentials may then be used to gain unauthorized access to accounts or systems.

B.5 Indicators of Compromise (IOC)

Indicators of Compromise (IOCs) are pieces of technical information that suggest a system or network may have been involved in malicious activity. Examples include suspicious domains, malicious IP addresses, or unusual system behaviours associated with cyberattacks.

B.6 Threat Intelligence

Threat intelligence refers to the collection and analysis of information related to current or emerging cyber threats. This information helps organizations understand attacker tactics, identify potential risks, and improve cybersecurity defences.

B.7 Infrastructure-Level Threat Detection

Infrastructure-level threat detection focuses on identifying malicious digital infrastructure, such as phishing domains or hosting environments, before they are actively used in attacks. This approach emphasizes detecting attacker intent rather than waiting for confirmed malicious activity.

B.8 Reputation Laundering

Reputation laundering is a technique used by attackers to make malicious infrastructure appear trustworthy. This may involve hosting benign content temporarily, redirecting automated scanners to legitimate websites, or allowing domains to age before launching attacks.

B.9 Redirect Laundering

Redirect laundering refers to the use of redirect chains that conceal malicious destinations. Security scanners may encounter harmless pages during automated inspection, while real users are redirected to phishing pages.

B.10 Security Operations Center (SOC)

A Security Operations Centre (SOC) is a centralized team responsible for monitoring, detecting, and responding to cybersecurity threats within an organization. SOC teams analyse security alerts and coordinate incident response activities.

B.11 Domain Lifecycle

The domain lifecycle refers to the stages through which an internet domain progresses, including registration, active use, expiration, and potential transfer of ownership. Attackers sometimes exploit expired domains to stage phishing infrastructure.

B.12 Infrastructure Staging

Infrastructure staging refers to the preparation of digital infrastructure, such as domain registrations and hosting environments, before launching an attack. Attackers may stage infrastructure weeks or months in advance to evade detection systems.

B.13 Multi-Domain Phishing Ecosystem

Modern phishing campaigns often rely on networks of multiple domains performing different roles, including phishing pages, redirect infrastructure, and credential collection endpoints. This structure creates a more resilient phishing ecosystem.

B.14 Conditional Content Delivery

Conditional content delivery occurs when a website behaves differently depending on the visitor. For example, a phishing site may display benign content to automated scanners while presenting credential-harvesting pages to real users.

B.15 Phishing Kit

A phishing kit is a pre-built software package used by attackers to quickly deploy phishing websites. These kits typically include cloned login pages, credential capture scripts, and control panels for managing stolen data.

B.16 Domain Intelligence

Domain intelligence refers to the analysis of domain registration patterns, hosting configurations, and infrastructure relationships to identify suspicious or malicious digital assets.

B.17 Threat Hunting

Threat hunting is a proactive cybersecurity practice in which analysts search for hidden or emerging threats within networks or infrastructure rather than waiting for automated alerts.

B.18 Infrastructure Signal

Infrastructure signals are observable technical characteristics that may indicate malicious intent. Examples include suspicious domain naming patterns, rapid DNS configuration changes, or hosting relationships linked to phishing campaigns.

B.19 Attack Surface

The attack surface represents the total set of digital assets that attackers may attempt to exploit. This may include websites, domains, cloud services, authentication systems, and communication channels.

B.20 Cyber Threat Intelligence Report

A cyber threat intelligence report is a structured document that analyses cybersecurity threats, attacker techniques, and infrastructure patterns to provide insights for organizations seeking to strengthen their security posture.

Disclaimer

This report has been prepared by LogIQ Curve based on threat-intelligence insights and investigations conducted using the capabilities of the PhishReaper.

The information presented in this report is intended for informational and research purposes only. While reasonable efforts have been made to ensure the accuracy of the analysis, the findings represent observations at the time of investigation and may evolve as threat actors change tactics and infrastructure.

The examples of domains, infrastructure patterns, and attack techniques referenced in this report are provided for cybersecurity awareness and defensive research. They should not be interpreted as an exhaustive list of malicious infrastructure.

LogIQ Curve and its partners do not assume liability for any actions taken based on the information presented in this report. Organizations are encouraged to conduct their own security assessments and consult professional cybersecurity experts when implementing defensive measures.