Breaking Down Credential Phishing Trends: How Can NDR Help?

Cybercriminals have changed tactics. Credential phishing has overtaken ransomware as the most common way to breach enterprise networks. What started as amateur email scams is now an industrial operation with nation-state precision. Phishing campaigns today mimic real user behavior so well that even trained employees fall for fake login pages, social engineering calls, and credential traps.

If attackers get credentials, they skip the noise and walk right through the digital front door. This blog breaks down how credential phishing works, why it's more dangerous than ever—and what Network Detection and Response (NDR) platforms like Fidelis Network are doing to stop it.

The Numbers Don't Lie

Credential theft is surging across sectors, fueled by automation, reused passwords, and a booming underground market. Let's put it in perspective:

- 703% surge in credential phishing attacks in H2 2024[1].
- Over 100 billion compromised records shared on underground forums in 2024[2].
- 15–16 billion stolen credentials circulating on the dark web as of 2025[3] [4].
- The most-used password, "123456," appeared over 3 million times and is cracked in less than one second.
- 49 of 50 most-traded passwords can be cracked in under one second.

Attackers pair these credentials with powerful bots that test logins across platforms—what we call credential stuffing. It's fast, scalable, and shockingly effective.

Why Are Mobile Users Easy Targets for Credential Theft?

Phishing attacks on mobile devices are a fast-growing threat vector. Even though many credential thefts begin on smartphones, their effects are felt inside enterprise networks—when those stolen credentials are used to breach business systems.

Mobile phishing (especially smishing) attacks are growing fast because smartphones weaken visibility and amplify urgency.

- Smishing increased by over 400% between 2020 and 2023[5]
- Mobile phishing tools mimic login pages flawlessly
- Small screens remove URL visibility and show fewer security cues

Touch interfaces = quick taps. Combine that with shortened URLs, spoofed brands, or a fake "your session expired" message—and users hand over their passwords faster than ever.

Once credentials are stolen from mobile devices, attackers often use them to log into enterprise systems, sometimes days or weeks after the original theft.

NDR plays a critical role here: it can spot the unusual login locations, device changes, and rapid, automated testing of these credentials in enterprise environments. This connection means mobile threats quickly become network problems, and NDR is uniquely positioned to identify and contain such attacks.

How Are Cybercriminals Launching Phishing Attacks So Easily?

Phishing is no longer just for elite hackers. Sophisticated phishing kits, AI-written lures, and automated tools make it easy for anyone to start stealing credentials at scale.

- Phishing kits are sold on dark web marketplaces
- AI models generate realistic copy and auto-translate attacks
- Credential harvesters automatically upload logs to attacker-controlled databases

A campaign that once took days now runs in minutes. And it only takes one set of valid credentials to breach an enterprise.

Can Hackers Bypass Multi-Factor Authentication?

Yes, organizations deployed multi-factor authentication (MFA) expecting bulletproof protection, but it’s no longer enough. While MFA adds an extra layer of protection by requiring users to verify their identity through multiple authentication methods, attackers have developed techniques to bypass even these advanced authentication methods.

No MFA method is immune. Even hardware tokens can be phished with social engineering. That’s why post-authentication detection is essential.

How Criminals Beat MFA:

Notification Bombing:

- Flood users with auth requests
- Users approve to stop the spam
- 34% success rate within one hour

Phone Number Hijacking

- Take over victim’s phone service
- Steal SMS codes in real-time
- Losses range from thousands to millions.

Fake IT Support:

- Pose as internal helpdesk

- Talk users into sharing codes
- Peak success: Monday mornings, Friday afternoons

Once MFA is bypassed, attackers gain access to a compromised account, which can then be exploited for further malicious activities.

While exact cost figures vary, failures in MFA are a significant contributor to rising cyberattack costs in 2024.

Where Do Stolen Credentials End Up After a Breach?

Over 15 billion stolen credentials are circulating on the dark web as of 2025.

Why Stolen Logins Stay Valuable:

- **Password recycling:** The average person reuses passwords across 7 accounts.
- **Automated testing:** Bots try stolen credentials against hundreds of sites.
- **Account takeovers:** One compromised login opens multiple systems.
- **Network infiltration:** Initial access enables deeper penetration.

These compromised credentials are frequently bought and sold on underground markets, fueling further attacks. This creates a thriving economy where valid credentials hold value for months or years.

How Does NDR Detect Attacks That Bypass Traditional Security?

Traditional security tries blocking everything bad at the network edge. Signature matching, URL filtering, email scanning—all focused on prevention.

Network Detection and Response operates on a different principle.

Rather than stopping every attack, NDR accepts that some will succeed. The focus shifts to detecting what happens after attackers gain initial access. This approach excels against credential-based attacks. NDR solutions often assign risk scores to suspicious activities, enabling security teams to prioritize responses. NDR also plays a crucial role in protecting credentials by detecting and responding to threats that bypass traditional defenses.

Why NDR Outperforms Traditional Tools:

- Old School: “Keep all threats outside”
- NDR: “Spot threats that got inside”

NDR’s advanced detection capabilities complement endpoint and email security, helping prevent credential phishing from resulting in successful breaches by identifying suspicious activity even after initial access.

From Alert Fatigue to Attack Precision: The NDR Playbook

- Automated investigations
- Incident correlation
- Real-time response

[Download Now]

Fidelis Network®: Purpose-Built for Credential Defense

Deep Session Inspection

Fidelis Network® dissects nested files using patented analysis technology:

Credential Theft Detection:

- Detects malicious scripts buried in email attachments.
- Uncovers phishing payloads hidden in compressed files.
- Monitors encrypted channels exfiltrating stolen credentials.
- Flags JavaScript keyloggers capturing form data.
- Identifies replay attacks by detecting repeated use of stolen credentials or tokens.

Live Analysis Features:

- Packet-level file structure examination.
- Content pattern recognition for credential theft.
- User authentication sequence monitoring.
- Access pattern anomaly identification.

Email Threat Intelligence

The platform intercepts credential theft attempts through comprehensive email analysis:

Pre-interaction Protection:

- Spots phishing emails before user clicks.
- Identifies malicious attachments with credential stealers.
- Catches suspicious links to fake websites targeting login pages.
- Recognizes email patterns from credential campaigns.

Internal Threat Monitoring:

- Tracks lateral phishing from compromised accounts.
- Identifies spray attacks targeting multiple users.
- Detects credential harvesting through email analysis.
- Monitors unauthorized access attempts via email.

Multi-vector Threat Correlation

Fidelis Network® connects attack dots across network segments using MITRE ATT&CK mapping:

Attack Chain Reconstruction:

- Follows progression from credential theft to privilege escalation.
- Maps lateral movement after successful credential compromise.
- Identifies brute force attacks against user accounts.
- Tracks unauthorized access attempts network-wide.

Intelligence-driven Detection:

- Merges network monitoring with endpoint telemetry.
- Combines email security with external threat feeds.
- Monitors for automated login attempts as part of threat correlation, helping to detect and mitigate malicious bot activity targeting login processes.
- Delivers complete attack visibility across infrastructure.
- Ranks threats by severity and progression speed.

Instant Response Automation

Fidelis Network® responds to credential threats without human delay:

Immediate Containment:

- Kills suspicious connections tied to credential theft.
- Quarantines devices showing credential misuse signs.
- Blocks IPs and URLs from phishing campaigns.
- Isolates network segments to stop lateral movement.

Smart Response Logic:

- Machine learning identifies high-confidence threats.
- Predefined rules trigger immediate automated actions.
- Complex scenarios escalate to human analysts.
- Forensic collection starts automatically for investigation.

How Can You Stop Stolen Credentials from Being Exfiltrated?

Fidelis Network® monitors credential exfiltration across multiple channels:

Credential Monitoring Scope:

- Unauthorized transmission of auth tokens, API keys, and OAuth tokens.
- Suspicious data flows containing credential information.
- Unusual access patterns to credential storage systems.
- OAuth token and session cookie extraction attempts.

Detection Methodology:

- Pattern matching for credential data structures.
- Behavioral analysis of data access sequences.
- Content inspection of structured and unstructured flows.
- Real-time authentication token usage monitoring.

How Do You Detect New Phishing Kits or Credential Stealers?

Cloud-based analysis examines suspicious content in isolated environments:

Zero-day Coverage:

- Identifies unknown phishing kits targeting credentials.
- Detects malicious payloads deploying credential harvesters.
- Discovers new credential theft malware variants.
- Uncovers advanced social engineering tactics in spear phishing.

Intelligence Operations:

- Live updates on emerging credential attack methods.
- Automated threat indicator sharing across security tools.
- Predictive analysis of upcoming credential campaigns.
- Collaborative defense against organized credential theft.

How Does Fidelis NDR Work With SIEM, SOAR, and IAM Tools?

Fidelis Network® connects with existing security investments:

Integration Function Value SIEM Centralized alert correlation Unified threat view EDR Comprehensive threat detection Enhanced endpoint coverage SOAR Automated incident response Faster threat resolution IAM Enhanced credential monitoring Improved access oversight

Connection Methods:

- APIs for bidirectional data exchange.
- Log forwarding through standard protocols.
- Real-time sharing between security platforms.
- Unified dashboard for centralized threat management.

Integration with IAM and other security platforms strengthens access controls across the organization, helping to prevent unauthorized access and improve overall security posture.

What Are the Deployment Options for NDR?

Organizations need deployment options that match their operational requirements.

Hardware Deployment:

- Dedicated appliances for maximum throughput.
- Data residency compliance for regulated industries.
- Complete organizational control over processing.
- Optimized for high-volume traffic analysis.

Virtual Implementation:

- VMware, Hyper-V, and cloud platform support.
- Scalable resource allocation matching network demands.
- Hybrid environment compatibility for complex infrastructures.
- Cost-effective deployment for resource-constrained organizations.

Cloud Services:

- Managed services with global threat intelligence.
- Automatic scaling based on traffic patterns.
- Reduced infrastructure management overhead.
- Enhanced threat intelligence through customer base sharing.

What Detection Methods Does Fidelis NDR Use?

Fidelis Network® combines multiple detection approaches for comprehensive credential attack identification:

Behavioral Analysis:

- User login pattern examination.
- Access timing anomaly detection.
- Geographic location verification.
- Device fingerprinting for authentication validation.

Machine Learning:

- Network traffic pattern analysis.
- Communication flow examination.
- Data access behavior modeling.
- Novel attack technique identification.

Signature Detection:

- Known credential phishing pattern matching.
- Malware signature identification.
- URL reputation analysis.
- File hash comparison against threat databases.

Anomaly Detection:

- Normal user behavior baseline establishment.
- Statistical authentication pattern analysis.
- Deviation identification from established baselines.
- Risk scoring using multiple behavioral factors.

How Are Credential-Based Attacks Changing in 2025?

Credential phishing continues evolving at breakneck speed. As attackers develop more sophisticated techniques, the risk of identity theft for both individuals and organizations increases, exposing them to significant personal and financial consequences.

AI-Enhanced Detection

- Advanced behavioral pattern analysis for legitimate users.
- Improved detection of unknown attack techniques.
- Predictive modeling for potential attack vectors.
- Automated response time reduction through intelligent analysis.

Zero Trust Implementation

- Every authentication request verification regardless of source.
- Continuous user identity validation throughout sessions.
- Micro-segmentation limiting credential attack impact.
- Comprehensive traffic monitoring for credential misuse indicators.

Threat Intelligence Evolution

- Real-time updates on emerging credential attack techniques.
- Automated threat indicator sharing across security platforms.
- Predictive analysis of credential attack campaigns.
- Collaborative defense against organized credential theft operations.

How Do NDR Tools Detect and Respond to Credential Theft?

NDR vs. Traditional Antivirus

Antivirus relies on signature matching for known malware. NDR monitors network behavior and user activities, catching unusual login patterns, data access behaviors, and lateral movement after credential theft through comprehensive behavioral analysis. NDR is a complement to, not a replacement for, endpoint protection.

Real-time Credential Stuffing Detection

***NDR platforms spot credential stuffing through distinctive patterns*:** high-volume login attempts from multiple IPs, rapid authentication sequences, and automated tool signatures in network traffic. Detection happens through statistical authentication pattern analysis and connection behavior monitoring.

Automated Credential Compromise Response

Systems terminate suspicious connections, isolate compromised devices, block malicious IPs, and alert security teams. Response speed advantages come from predefined automated actions and machine learning-driven threat classification.

Encrypted Traffic Analysis

NDR examines metadata, connection patterns, timing, and behavioral characteristics without decrypting traffic. Unusual access patterns, connection timings, and data transfer volumes indicate credential misuse through statistical analysis and baseline comparison, respecting privacy and compliance.

Infrastructure Integration Requirements

Modern NDR solutions integrate with existing infrastructure through physical hardware, virtual machines, or cloud deployment without major network modifications. Integration happens through APIs and standardized protocols rather than infrastructure replacement.

AI-generated Phishing Defense

NDR effectiveness comes from detecting post-phishing activity rather than analyzing initial phishing content. Behavioral patterns following credential theft remain detectable regardless of phishing sophistication through network activity monitoring and user behavior analysis.

What Makes Credential-Based Attacks So Effective and How Can You Stop Them?

Weak Password Exploitation

Organizations with weak passwords face constant brute force attacks. Credential stuffing operations specifically target accounts with predictable password patterns, making weak passwords a primary entry point for unauthorized parties seeking to steal sensitive information.

Automated Attack Tools

Modern cybercriminals deploy sophisticated automation tools across their IT environment to scale credential attacks. These tools systematically test stolen credentials against multiple systems until finding a successful attack vector. Each successful attack allows attackers to escalate privileges and move laterally through networks.

Privilege Elevation Risks

After initial credential compromise, attackers pursue privilege elevation through various techniques. Standard user accounts become stepping stones for accessing administrative systems, enabling attackers to deploy malware and establish persistent access throughout the IT environment.

The combination of weak passwords, automated attack tools, and privilege elevation creates a dangerous cycle where unauthorized parties can systematically steal sensitive information and maintain long-term access to compromised systems.

Key Steps to Strengthen Credential Defense with NDR

- Audit password policies and enforce unique credentials.
- Monitor for credential reuse and automate detection of stuffing attacks.
- Integrate NDR with SIEM, EDR, SOAR, and IAM for unified visibility.
- Regularly review and tune NDR detection rules.
- Conduct tabletop exercises simulating credential phishing scenarios.

References:

1. ^2024 Phishing Report Shows Credential Phishing Up By 703% in H2 | SlashNext
2. ^Fortinet Threat Report Reveals Record Surge in Automated Cyberattacks as Adversaries Weaponize AI and Fresh Techniques | Fortinet
3. ^15 billion stolen passwords on sale on the dark web, research reveals | The Independent | The Independent
4. ^16 billion passwords exposed in colossal data breach | Cybernews
5. ^Smishing Statistics Statistics: Market Data Report 2025