LARES
A DAMOVO COMPANY

WHITE PAPER

THE LARES ASSUMED BREACH VISHING METHODOLOGY

Testing voice-based trust after the attacker already has a foothold.

ABOUT LARES

Lares is a security consulting firm that helps companies secure electronic, physical, intellectual, and financial assets through a unique blend of assessment, testing, and coaching since 2008.

For more information, visit lares.com, contact us at (720) 600-0329, or follow Lares on X @Lares_.

LARES
A DAMOVO COMPANY

www.lares.com

CONTACT INFORMATION

1580 N. Logan St. Ste 660, PMB 79199, Denver, CO 80203, USA

+1 (720) 600-0329
sales@lares.com

Executive Summary

A more realistic model for voice-based compromise

Voice phishing is often tested as though the attacker starts with nothing. That model is useful, but it is incomplete. Many real attacks begin after the attacker has already acquired a small amount of trusted context, such as an employee identifier, an order number, a support case, or a vendor reference.

Once that happens, the security problem changes. The question is no longer whether an employee can recognize a suspicious caller. The question is whether the organization still enforces meaningful controls once the caller sounds legitimate.

The Lares Assumed Breach Vishing Methodology is designed to test that condition. It measures how voice-based workflows perform when an adversary begins with limited but credible business context and uses it to move deeper into support processes, escalation paths, and identity-dependent actions.

“The question is whether the organization still enforces meaningful controls once the caller sounds legitimate.”

WHY IT MATTERS

This methodology does not replace traditional vishing. It builds on it. A black box baseline still matters because it shows how an organization handles unsolicited external callers. The assumed breach phase then tests what happens after a caller has just enough context to be treated differently.

Together, those two views produce a more realistic assessment of voice-based risk.

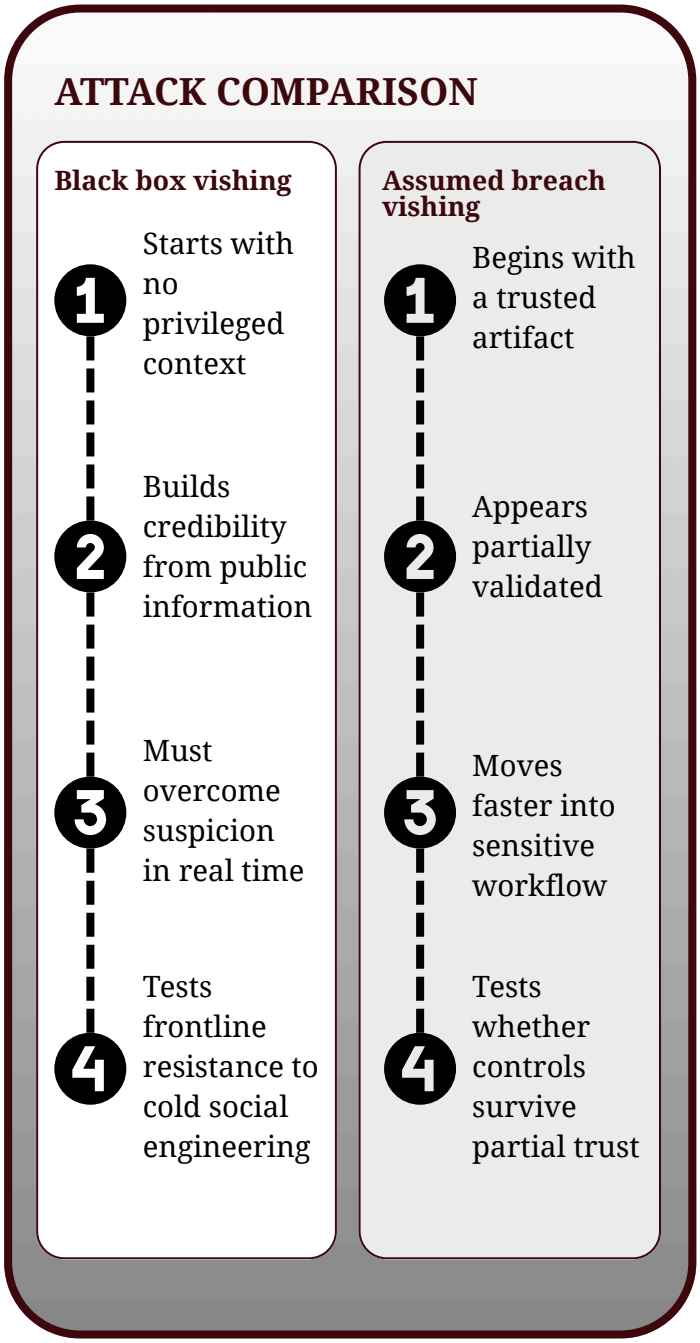
Why black box vishing is not enough

THE TRUST PROBLEM

Most support operations are designed to solve problems quickly. Help desks restore access. Customer support resolves issues. Service teams route requests and keep business moving. That creates a predictable tension between service and security.

That tension becomes most visible when a caller arrives with plausible context. In many environments, one or two trusted details are enough to change the interaction. None of those signals should be sufficient to authorize sensitive action on their own, but in practice they often lower the level of scrutiny the caller receives.

This is where many organizations fail. Teams may understand that vishing exists and documented procedures may require verification, but once a caller presents a believable artifact, the interaction often shifts from screening to problem solving before trust has actually been earned.



What assumed breach means in practice

In this methodology, an assumed breach does not imply a full internal compromise. It does not mean administrative access, insider status, or broad privileged knowledge. It means the attacker begins with a small amount of realistic business context that many teams would interpret as a sign of legitimacy.

These are not arbitrary props. They are the kinds of artifacts that are commonly exposed, reused, or inferred in real environments. More importantly, they are the kinds of details that often lower skepticism during live support interactions.

CORE PREMISE

If a small amount of context materially changes how a caller is treated, the real weakness lies not only in the employee's judgment. It lies in the design of the process itself.

COMMON TRUST ARTIFACTS

ID

Employee ID
A valid employee identifier that makes the caller feel known.

#

Order number
A transaction reference that lowers skepticism in service workflows.

CS

Case or ticket
A support reference that makes the issue appear immediately legitimate.

SH

Shipment detail
Fulfillment or logistics context tied to a live workflow.

MG

Manager context
A name, team, or reporting detail that signals internal familiarity.

VN

Partner context
Known vendor or third-party details that anchor a believable pretext.

Methodology Overview

The methodology is structured to measure both external resistance and post-foothold resilience. It begins with planning, establishes a black box baseline, and then transitions to a controlled assumed breach scenario.

Phase 0
Engagement Design and Planning

Objectives, scope boundaries, deconfliction, disruption guardrails, and the assumed breach starting condition.

Phase I
Reconnaissance and Intelligence Gathering

Mapping public footprint, support channels, naming conventions, and the context that makes calls believable.

Phase II
Black Box Vishing Baseline

Testing external resistance without approved artifacts to establish the baseline.

Phase III
Assumed Breach Transition

Introducing preapproved trust artifacts selected during planning.

Phase IV
Assumed Breach Execution

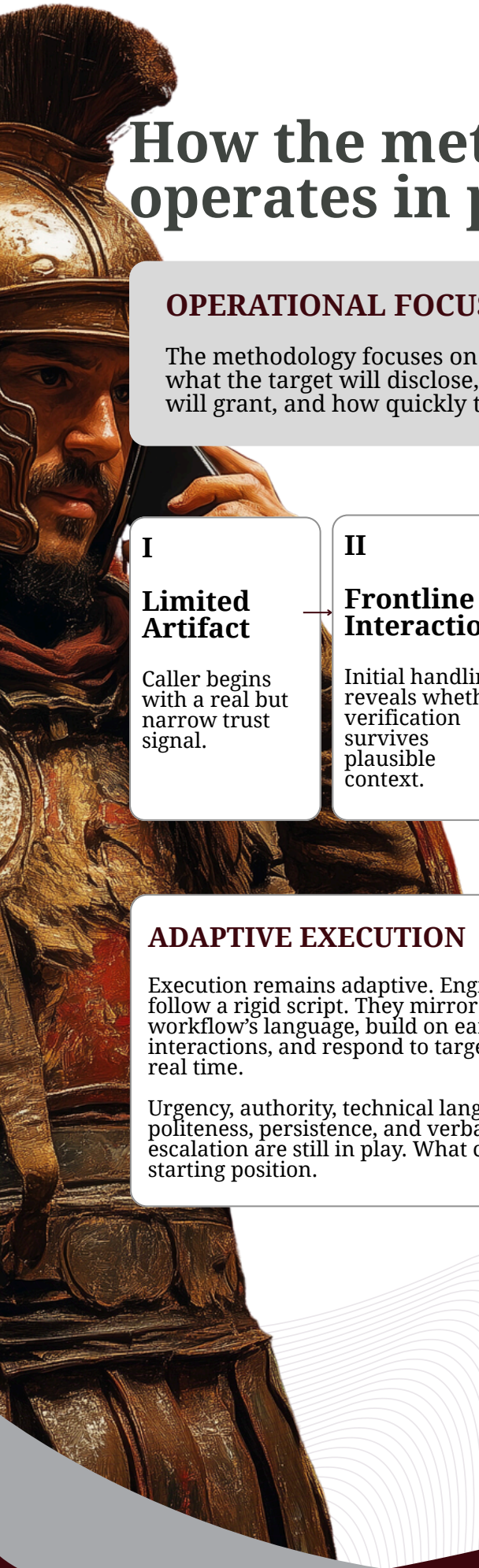
Targeted calls that measure disclosure, action, exception handling, and escalation behavior.

Phase V
Analysis and Reporting

Explaining which trust signals changed posture, where verification weakened, and how to reduce risk.

ASSESSMENT VALUE

Without a black box baseline, it is difficult to distinguish weaknesses caused by the foothold from weaknesses that already exist in the handling of unauthenticated callers. The assumed breach phase then shows what changes when the caller is treated differently.



How the methodology operates in practice

OPERATIONAL FOCUS

The methodology focuses on process abuse, not just conversation success. It measures what the target will disclose, what actions they will perform, what exceptions they will grant, and how quickly they route the caller into more sensitive workflows.

I

Limited Artifact

Caller begins with a real but narrow trust signal.

→

II

Frontline Interaction

Initial handling reveals whether verification survives plausible context.

→

III

Handoff or Escalation

Introducing preapproved trust artifacts selected during planning.

→

IV

Sensitive Workflow

Reset, disclosure, exception, reroute, or identity-dependent action.

→

V

Analysis

Lares maps where trust expanded and why the process allowed it.

ADAPTIVE EXECUTION

Execution remains adaptive. Engineers do not follow a rigid script. They mirror the workflow's language, build on earlier interactions, and respond to target behavior in real time.

Urgency, authority, technical language, politeness, persistence, and verbal privilege escalation are still in play. What changes is the starting position.

REPORTING FOCUS

A strong report does more than log successful or unsuccessful calls. It explains which trust signals changed posture, where verification weakened, where escalation created risk, and how the attacker progressed.

That distinction is what makes the findings useful for security leadership and workflow owners.

Use cases and failure patterns

IT HELP DESK

The help desk is one of the highest-value targets in voice-based assessment because it sits close to identity, access, account recovery, and operational urgency.

Assumed breach testing shows how much employee context is enough to move the help desk from validation to remediation.

CUSTOMER SUPPORT

Customer support environments are built around service continuity and rapid resolution. That makes them vulnerable to callers who possess real transaction context.

This use case exposes whether ordinary business details are being treated as trust anchors.

COMMON FAILURE PATTERNS

Overreliance on knowledge-based authentication

One or two data points materially change handling because the process relies on information that is easy to steal, infer, or buy.

Trust expansion during handoffs

One team performs a reasonable check, but the next assumes validation has already happened.

Policy drift

Documented procedures for callback verification or approval paths are stronger on paper than in live support interactions.

Cumulative privilege through conversation

A caller begins with one legitimate detail and ends with a much richer set of internal knowledge to use later.

What to do with the results

The purpose of this methodology is not to prove that support teams can be manipulated. That is already well understood. The purpose is to identify where the process grants trust too early and how to reduce that trust without harming the business.

Stronger verification

Sensitive actions should require stronger forms of verification than shared knowledge or contextual details.

Escalation discipline

Receiving teams should know what has and has not been verified and should not assume earlier validation was sufficient.

Role-based training

Help desks, customer support teams, payroll teams, and partner-facing teams face different pressures and should be trained accordingly.

Process instrumentation

Controls should detect unusual patterns across multiple calls because attackers often accumulate trust gradually.

CLOSING VIEW

By combining a black box baseline with a controlled assumed breach scenario, this methodology shows where support processes relax too early, where verification depends too heavily on context, and where ordinary business workflows can be manipulated into access, action, or deeper compromise.

ADDITIONAL RESOURCES

Lares Vishing Methodology
Lares Insider Threat Methodology

ABOUT LARES

Lares is a security consulting firm that helps companies secure electronic, physical, intellectual, and financial assets through a unique blend of assessment, testing, and coaching since 2008.

For more information, visit lares.com, contact us at (720) 600-0329, or follow Lares on X @Lares_.

LARES
A DAMOVO COMPANY

CONTACT INFORMATION

1580 N. Logan St. Ste 660, PMB 79199, Denver, CO 80203, USA

+1 (720) 600-0329
sales@lares.com