TALES FROM THE SOC

SOCIAL ENGINEERING · HIGH PRIORITY

Email Bombing & Account Compromise

IT support impersonation via Microsoft Teams Quick Assist, leveraging living-off-the-land techniques.

Incident Overview

Threat Type: IT support impersonation campaign delivered via email bombing and Microsoft Teams Quick Assist, leveraging living-off-the-land techniques to evade file-reputation defenses.

Time to Containment: 13 minutes from initial escalation to confirmed customer remediation of all four affected users.

Attack Characteristics: An attacker email-bombed four users to create confusion, then posed as IT Support via Microsoft Teams using a lookalike account. The attacker gained interactive remote access to at least one endpoint via Quick Assist and executed a chain of Microsoft-signed, VirusTotal-clean binaries — QuickAssist.exe, powershell.exe, and tar.exe — to extract a password-protected archive into a suspicious user profile path. Every tool in the chain was purpose-built to pass standard file-reputation checks.

Detection & Escalation

Detection: Microsoft Defender XDR flagged a Teams impersonation campaign following the mail-bombing event. Critical Start SOCAI enriched each alert with IOC lookups, sign-in activity, and a structured risk summary — enabling analysts to move straight to decision-making rather than starting from raw telemetry.

SOC Escalation: Medium priority, escalated to High. Analysts recognized three separate alerts — mail bombing, Teams impersonation, and Quick Assist endpoint activity — as a single coordinated campaign. Because sign-in evidence was incomplete and MFA confirmation was absent, the team declined to close the alert as benign and escalated for customer visibility, consistent with documented investigation standards.

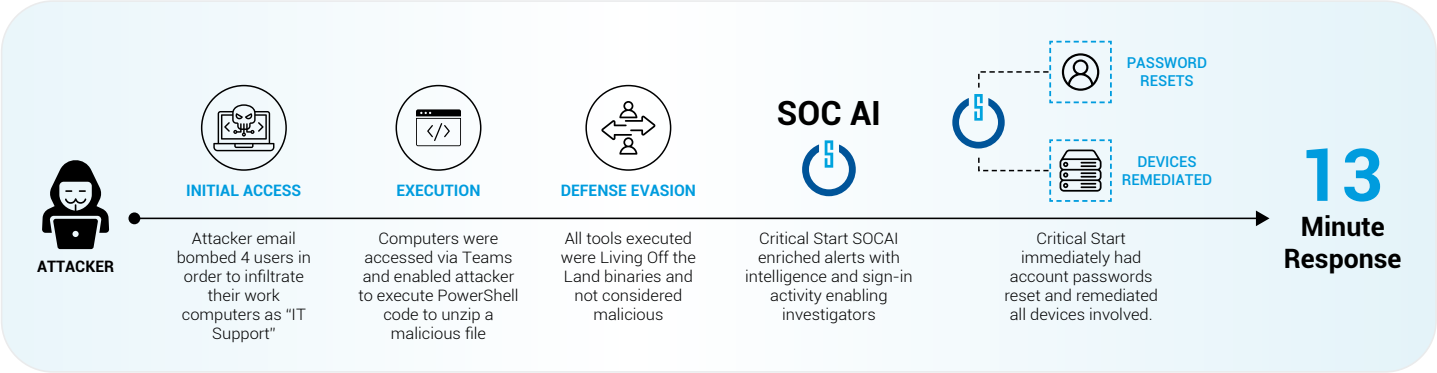
Depth of Investigation

The Critical Start SOC tied five distinct alerts into a single coordinated campaign. Analysts identified the impersonation account as linked to an external IP via a commercial hosting provider, cross-referenced mail-bombing targets with endpoint activity, and correctly flagged the Quick Assist process chain as a living-off-the-land abuse pattern — despite every binary being signed by Microsoft and returning clean on VirusTotal. Recognizing this activity required adversarial pattern recognition, not just automated tooling.

A critical investigation detail: the affected users were hybrid identities, meaning password resets and account disables had to be routed through the Defender XDR console rather than standard Active Directory tooling. Analysts identified this early and applied the correct remediation path without delay — a nuance that could have stalled containment in a less experienced SOC.

Critical Start SOCAI accelerated the investigation by surfacing enriched intelligence and sign-in context upfront, allowing human analysts to focus on adversarial judgment. The team worked the customer phone tree twice before reaching the client, who confirmed full remediation for all four affected users within 13 minutes of escalation.

Attack Sequence



Outcome

In 13 minutes, the Critical Start SOC confirmed a coordinated impersonation campaign, walked the customer's team through remediation for all four affected users, and ensured passwords were reset, sessions revoked, and accounts disabled. By treating three separate alerts as one campaign — and applying the correct hybrid-identity remediation path — the team prevented what could have escalated into interactive endpoint access, credential theft, or broader lateral movement. The customer's team noticed.

> **"We had a true positive event trigger on 07/2/2026 and the Critical Start Team was all over it, including escalating where necessary. Thanks for everything you do to protect us and great job on this one!"**
>
> — Customer, energy sector