ShinyHunters-Linked Social Engineering and Identity-Targeting Campaign

Aug 24, 2026

WHITE

View Alert

On August 22, 2026, threat actors linked to the extortion group ShinyHunters executed a targeted social engineering campaign against ReliaQuest using voice phishing and lookalike single sign-on (SSO) infrastructure.

Although the attacker briefly established an authenticated identity dashboard session through harvested credentials and MFA push approval, subsequent lateral movement was blocked by device-trust access controls. The incident was successfully contained with zero unauthorized access to internal applications, enterprise systems, customer environments, or telemetry data.

Health-ISAC provides this information to increase situational awareness and encourage organizations to assess their risk exposure to this activity.

Additional Info

Analysis:

The threat actor conducted a coordinated voice phishing (vishing) campaign combined with credential harvesting. The adversary registered a typosquatted domain hosted behind a content delivery network (CDN) to mirror the organization's corporate SSO authentication portal. Posing as a named internal security staff member, the attacker contacted several employees to create a sense of urgency and directed them to the malicious login page. During the interaction, one employee submitted corporate

credentials into the fake portal and subsequently approved a multi-factor authentication (MFA) push notification on their mobile device.

The harvested credentials and approved MFA token granted the attacker an active web session strictly limited to the organization's central identity provider (IdP) dashboard. This level of access allowed the threat actor to view only the top-level application launch tiles configured within the employee's identity interface. Because the session was initiated from an unmanaged, external device, the adversary was unable to establish persistence or manipulate account configurations before automated detection and defensive mechanisms engaged.

The overall impact of the incident was negligible due to layered conditional access policies and zero-trust controls. When the adversary attempted to pivot from the dashboard into internal applications and corporate systems, access was systematically denied because the requests originated from non-compliant, unmanaged endpoints. Incident response teams isolated the compromised identity, revoked active session tokens, and verified that no data exfiltration, service disruption, or access to customer environments occurred, rendering subsequent extortion claims published on the actor's leak site unsubstantiated.

This campaign reflects the continued evolution of extortion groups like ShinyHunters and related loose-knit ecosystems (such as Scattered Spider), which prioritize identity compromise, SaaS-layer access, and mobile-targeted social engineering over traditional malware deployment. By pairing personalized phone-led interactions with reverse-proxy phishing kits, threat actors regularly bypass standard MFA implementations. This incident underscores that identity verification alone is insufficient without strong device-context verification and defense-in-depth architecture.

Recommendations and Mitigations:

Health-ISAC recommends organizations review and assess their risk exposure to this activity and implement the following:

- Restrict SaaS applications, internal portals, and APIs to corporate-managed devices verified via client certificates, EDR health checks, or MDM profiles.
- Track lookalike domain registrations, newly observed domains (NODs), and branded subdomains targeting corporate single sign-on services.

- Train IT, security, and admin personnel to identify voice impersonation, caller ID spoofing, and unsolicited login verification requests.
- Set session timeouts that effectively support user workflows and ensure security, restrict IdP visibility for non-compliant endpoints, and alert on simultaneous logins from anomalous geographies or IPs.
- Reviewing the Health Industry Cybersecurity Practices (HICP): Managing Threats and Protecting Patients resources.

<hr size=1 width="100%" align=center>

Alert Id	04207192
Category	Cyber Incidents
References	cyberinsider bleepingcomputer reliaquest hhs
Tags	Vishing, ShinyHunters, Social Engineering

Access the Health-ISAC Threat Intelligence Portal
Enhance your personalized information-sharing community with improved threat visibility, alert notifications, and incident sharing in a trusted environment delivered to you via email and mobile apps. Contact membership@h-isac.org for access to Health-ISAC Threat Intelligence Portal (HTIP).

For Questions or Comments
Please email us at toc@h-isac.org

Please provide your feedback

Like Dislike

Download the App

Available on iOS, Android and Web

For more updates and alerts, visit: **https://health-isac.cyware.com/webapp/**
Health-ISAC is an invite only platform. Please DO NOT forward this email to anyone. If you are not supposed to receive this email, please report to **toc@h-isac.org**

--
You received this message because you are subscribed to the Google Groups "TLP Green - Health-ISAC Partners" group.
To unsubscribe from this group and stop receiving emails from it, send an email to health-isac-partners+unsubscribe@h-isac.org.
To view this discussion visit https://groups.google.com/a/h-isac.org/d/msgid/health-isac-partners/010001a034786b65-a073a33c-852b-4555-9d73-bff808630f6c-000000%40email.amazonses.com.