Profiling & Disrupting an APT Spear Phishing Campaign Targeting Slack users in the Financial Sector

By Mauro Eldritch

Published: 2024-02-21 · Archived: 2026-04-05 17:37:03 UTC

@MauroEldritch, Quetzal Team @ Bitso — 2024

Press enter or click to view image in full size

Credits: Pixabay

Introduction

In January 2024, we first identified a Spear Phishing campaign targeting Slack users in the financial sector.

The threat actor used a template for the deceptive email with high attention to detail, making it highly convincing. However, part of its infrastructure is recycled, having been used in previous campaigns, and it shows activity consistent with an Advanced Persistent Threat (APT).

As of the date of this investigation, there are no public mentions of the indicators of this campaign, suggesting that we are among the first to discover and profile it [1].

Technical Analysis

The attacker uses Google email servers (108.177.16.4, 209.85.218.68 & 209.85.166.169), which are whitelisted on most security providers, to gain a reputational advantage and evade potential blocks based on SPAM lists (source: Cisco Talos).

The body of the email is static, but the subject and malicious action button links change per recipient. The template is highly sophisticated, with particular attention to detail, including links and buttons redirecting to official Slack application sites and social networks. However, the language used in the email body and the email subjects reveals the deceptive nature of the communication, as analyzed in the 'Language Analysis' section below.

Malicious domains used by the threat actor are hosted on PorkBun, similar to those used by QRLog. At the time of writing this report, all these domains display a "Maintenance" message, as seen below. This is likely a response to us releasing IOCs (Indicators of Compromise) on various intelligence platforms (available in the 'References' section).

Domains were created on January 3rd except for *slack-hub.com* which exists since May, 2021. All of them have none or positive reputation.

Language Analysis

Email Body

> Kindly acknowledge receiving of our deal!
>
> We urge you to immediately address the requirement to accept our recent updated deal through your company's messaging platform. Kindly enter your official communication account and promptly acknowledge your business's newest deal.

- Use of "receiving of" instead of "receipt of."
- Use of "recent updated" instead of "recently updated."
- Use of "kindly," a word uncommon in normal communications and very frequent in deceptive emails.

Subjects

> Take Immediate Action: Accept Your Latest Business Agreement on Slack!
>
> Action Needed: Log in and Consent to the Revised Agreement on Communication!
>
> Time-sensitive: Verify Your Company's New Slack Deal Immediately!
>
> Time's Running Out: Recognize Your Recently Company Agreement on Slack!
>
> URGENT: Approval Required for the Fresh Business Contract on Messaging!
>
> Critical Mission: Acknowledge Your Business's Latest Agreement on Communication!
>
> Vital Update: Accept Your Recent Company Pact on Slack!

> Crucial: Acknowledge the New Contract on Company’s Messaging!
>
> Don’t Miss Out on This: Acknowledge Your Company’s Newest Agreement on Slack!
>
> Act Now: Accept Your Newest Company Terms on Slack!
>
> VITAL: Approval Required for the New Company Pact on Slack!
>
> Respond Immediately: Validate Your Latest Corporate Agreement on Slack!
>
> Critical Assignment: Validate Your Company’s Most Recent Agreement on Slack!
>
> Critical Task: Confirm Your Company’s Newest Deal on Slack!
>
> Important Update: Accept Your Most Recent Company Deal on Slack!
>
> PRESSING: Approval Required for the New Company Agreement on Slack!
>
> Urgent: Login and Endorse the Updated Agreement on Slack!
>
> Essential Duty: Authorize Your Company’s Recent Contract on Messaging!

- Use of a common pattern: [Alert Phrase]: [Action Needed]!.
- Use of a common pattern attempting to deceive the user through a false sense of urgency.
- Use of unnecessary exclamation marks.
- Use of uncommon words and phrases in corporate communications such as “Pressing,” “Vital,” “Respond Immediately,” “Crucial.”
- Presumed generation of subjects by an LLM model like ChatGPT.

IOCs

PRIMARY

> Domain:slackcloud.network
>
> Domain:slack-hub.com
>
> Domain:slack-sso.com
>
> Domain:slack-protect.com
>
> Domain:gfylinks.com
>
> Domain:badtastecru.co.uk
>
> Domain:ssoslack.com
>
> Domain:slack.com.slackcloud.network
>
> Domain:slack.com.ssoslack.com

> Domain:com.ssoslack.com
>
> IP:44.227.65.245
>
> IP:44.227.76.166
>
> URL:http://com.ssoslack.com/signin
>
> URL:http://slack.com.ssoslack.com/signin
>
> URL:http://ssoslack.com/signin
>
> URL:https://badtastecru.co.uk/jxp8g
>
> URL:https://gfylinks.com/saa5l
>
> URL:https://slack.com.slackcloud.network/signin#/signin
>
> String:Take Immediate Action: Accept Your Latest Business Agreement on Slack!
>
> String:Action Needed: Log in and Consent to the Revised Agreement on Communication!
>
> String:Time-sensitive: Verify Your Company’s New Slack Deal Immediately!
>
> String:Time’s Running Out: Recognize Your Recently Company Agreement on Slack!
>
> String:URGENT: Approval Required for the Fresh Business Contract on Messaging!
>
> String:Critical Mission: Acknowledge Your Business’s Latest Agreement on Communication!
>
> String:Vital Update: Accept Your Recent Company Pact on Slack!
>
> String:Crucial: Acknowledge the New Contract on Company’s Messaging!
>
> String:Don’t Miss Out on This: Acknowledge Your Company’s Newest Agreement on Slack!
>
> String:Act Now: Accept Your Newest Company Terms on Slack!
>
> String:VITAL: Approval Required for the New Company Pact on Slack!
>
> String:Respond Immediately: Validate Your Latest Corporate Agreement on Slack!
>
> String:Critical Assignment: Validate Your Company’s Most Recent Agreement on Slack!
>
> String:Critical Task: Confirm Your Company’s Newest Deal on Slack!
>
> String:Important Update: Accept Your Most Recent Company Deal on Slack!
>
> String:PRESSING: Approval Required for the New Company Agreement on Slack!
>
> String:Urgent: Login and Endorse the Updated Agreement on Slack!

> String:Essential Duty: Authorize Your Company’s Recent Contract on Messaging!

SECONDARY / ASSOCIATED

> Domain:pa7ypal.com
>
> Domain:connect-jnj.com
>
> Domain:xhams6er.com
>
> Domain:cooporatestock.com
>
> Domain:whatsappweb.xyz
>
> Domain:acess-logon-security.com
>
> Domain:info-spedizioni-xme.com
>
> Domain:recent-check-info.com
>
> Domain:cpamvitaie-fr.com
>
> Domain:superimarkets.com
>
> Domain:covidvaxonline.com
>
> Domain:review-transaction-attempt.com
>
> Domain:pay7pal.com
>
> Domain:gokcsbus.com
>
> Domain:noblearab.com
>
> Domain:portail-espace-sante.com
>
> Domain:nqf279d0booy.fun
>
> Domain:noodagency.com
>
> Domain:cit1zens-portal.com
>
> Domain:bhuiridh-gauge.com
>
> Domain:revertinstruction.com
>
> Domain:4pcstar.com
>
> Domain:review-new-applogon.com
>
> Domain:prodigalaudio.com

> Domain:livespory.com
>
> Domain:camvaclimlted.com
>
> Domain:2kclass.com
>
> Domain:1jdm.com
>
> Domain:sykes-sso.com
>
> Domain:ask-jnj.com
>
> Domain:concrecapital.com
>
> Domain:baidru.com
>
> Domain:mo-s.online
>
> Domain:checked-mobile-logon.com
>
> Domain:hempenvalley.com
>
> Domain:thecovidconspiracy.com
>
> Domain:cryptochampion.game
>
> Domain:manage-cyber-security.com
>
> Domain:007.bond
>
> Domain:azureservicesapi.com
>
> Domain:palashtv.com
>
> Domain:shareena.net
>
> Domain:bagtroop.com
>
> Domain:pharmerica.bar
>
> Domain:mktrending.com
>
> Domain:russ1ano.xyz
>
> Domain:giftstrendy.com
>
> Domain:manage-storedpayees109.com
>
> Domain:rumat-circle.com
>
> Domain:change-manage-add.com

> Domain:jumphigherventures.com
>
> Domain:10hoursleepsounds.com
>
> Domain:02261988.xyz
>
> Domain:2ody.com
>
> Domain:2faweb3ga.xyz
>
> Domain:att-rsa.com
>
> Domain:02mbnwsxctgbp.xyz
>
> Domain:austinpublicradio.com
>
> Domain:deflsolutions.com
>
> Domain:12bet1gom.com
>
> Domain:13westy37.xyz
>
> Domain:288908.xyz
>
> Domain:german0.xyz
>
> Domain:manage-added-attempted.com
>
> Domain:dunyaservices.com
>
> Domain:360lifeinabox.com
>
> Domain:microsoft-sso.net
>
> Domain:1gomkubet.com
>
> Domain:orkney-circle.com
>
> Domain:wellmarkhealth.com
>
> Domain:226616.xyz
>
> Domain:symantecq.com
>
> Domain:bankbazaronline.com
>
> Domain:fssd11asdflokmn.xyz
>
> Domain:jeuriderspaceacprints.com
>
> Domain:4yqw.com

> Domain:new-info-added.com
>
> Domain:covidvaxasap.com
>
> Domain:uid-amazio0m.xyz
>
> Domain:1gomw88.com
>
> Domain:1drvmicrosoft.com
>
> Domain:iopta.com
>
> Domain:226616.com
>
> Domain:arthot.com
>
> Domain:covidvaxtoday.com
>
> Domain:conferma-anagrafe-bpercard.com
>
> Domain:rpoqgfw.xyz
>
> Domain:1tal1ano.xyz
>
> Domain:noticeyahoo-conf2.xyz
>
> Domain:covidvaxcolombia.com
>
> Domain:inside-aol.com
>
> Domain:nichon18.rest
>
> Domain:speculumlover.com
>
> Domain:giottmart.com
>
> Domain:0mud.quest
>
> Domain:ivancarabantes.com
>
> Domain:roysalbank.com
>
> Domain:eliminate-corona.com
>
> Domain:mon-portail-colissimo.com
>
> Domain:att-mfa.com
>
> Domain:acespec.org
>
> Domain:sportline.one

> Domain:viagrawallet.org
>
> Domain:noipv6.wtf
>
> Domain:sparkasse.wiki
>
> Domain:vtb-tech.info
>
> Domain:adaloappdocs.top
>
> Domain:usp-blauder.us
>
> Domain:nikologios.wiki
>
> Domain:discounthouse.zone
>
> Domain:walletmanagements.com
>
> Domain:dlsneyplus-at.info
>
> Domain:3fw51.buzz
>
> Domain:review-confirmation-app.info
>
> Domain:adam2christ.org
>
> Domain:batcoin.biz
>
> Domain:banca-sella.co
>
> Domain:usp-saco.us
>
> Domain:mlcrosoft.info
>
> Domain:ca-ref12786378993290038.cloud
>
> Domain:deny-logon-attempted.info
>
> Domain:16206.tel
>
> Domain:covidhistory.org
>
> Domain:bottom.wiki
>
> Domain:mon-espace-sfr.org
>
> Domain:1k67s.buzz
>
> Domain:1001tutorialjahitan.buzz
>
> Domain:vivaless.buzz

> Domain:jessica-and-daniel.nyc
>
> Domain:operation-handling.info
>
> Domain:aiou.io
>
> Domain:dlsneyplus-app.info
>
> Domain:usp-mingodix.us
>
> Domain:removeaddin.info
>
> Domain:anpost-review.info
>
> Domain:glass.house
>
> Domain:yd1s.top
>
> Domain:berrybull.us
>
> Domain:purbno.us
>
> Domain:usp-daliver.us
>
> Domain:check-active-app.info
>
> Domain:documentshare.info
>
> Domain:mathlab.info
>
> Domain:usp-yinoksuz.us
>
> Domain:analyze-resolve.info
>
> Domain:coviddeaths.foundation
>
> Domain:godofwar.buzz

Possible Attribution

The infrastructure used for this campaign is recycled, having been part of previous campaigns. While the domains are new, the linked IP addresses have more than 100 mentions on the AlienVault OTX platform [2] [3].

After an analysis with the bIOChip tool [6], I found links to Advance Persistent Threats (APTs) EVILNUM (mostly) [4] [5] and Lazarus (secondarily) [8] [9]. Remember that the domains used in the QRLog campaign by

Lazarus were also hosted on Porkbun, a noteworthy detail.

bIOChip Output

> ⚠️ Report for concrecapital.com: Malicious activity found.
>
> 🥷 Domain is linked to known adversaries:
>
> * Lazarus (1)
>
> ☣️ Domain is linked to malware activity:
>
> * WifiCloudWidget (1)
>
> * Targeted: Crypto.com (1)
>
> * Targeted: Coinbase (1)
>
> ⚠️ Report for superimarkets.com: Malicious activity found.
>
> ☣️ Domain is linked to malware activity:
>
> * VileLoader (1)
>
> * DeathStalker (1)
>
> * Stonefly (1)
>
> * Maui (1)
>
> * EVILNUM (1)
>
> ⚠️ Report for 1jdm.com: Malicious activity found.
>
> ☣️ Domain is linked to malware activity:
>
> * AM (1)
>
> * Agent Tesla (1)
>
> * Malware (1)
>
> * Tulach Malware (1)
>
> * adware.pcappstore/veryfast (1)
>
> * NSIS (1)
>
> * Static AI — Malicious PE (1)
>
> * HoneyPot (1)

> ⚠️ Report for azureservicesapi.com: Malicious activity found.
>
> ☣️ Domain is linked to malware activity:
>
> * VileLoader (1)
>
> * DeathStalker (1)
>
> * Stonefly (1)
>
> * Maui (1)
>
> * EVILNUM (1)
>
> ⚠️ Report for symantecq.com: Malicious activity found.
>
> ☣️ Domain is linked to malware activity:
>
> * VileLoader (1)
>
> * DeathStalker (1)
>
> * Stonefly (1)
>
> * Maui (1)
>
> * EVILNUM (1)
>
> ⚠️ Report for slack-sso.com: Malicious activity found.
>
> 🥷 Domain is linked to known adversaries:
>
> * Evilnum (1)
>
> ☣️ Domain is linked to malware activity:
>
> * EVILNUM (1)
>
> ⚠️ Report for slack-hub.com: Malicious activity found.
>
> 🥷 Domain is linked to known adversaries:
>
> * Evilnum (1)
>
> ☣️ Domain is linked to malware activity:
>
> * EVILNUM (1)
>
> ⚠️ Report for slack-protect.com: Malicious activity found.
>
> 🥷 Domain is linked to known adversaries:

> * Evilnum (1)
>
> ☣️ Domain is linked to malware activity:
>
> * EVILNUM (1)

About EVILNUM

Evilnum, DeathStalker, TA4563, or Knockout Spider is an advanced threat actor focused on victims in the financial sector and cryptocurrencies. First observed in 2017, it remains active. It is known for employing Spear Phishing among its TTPs (Tactics, Techniques, Procedures) and using its toolset, including PyVil RAT (a Python-written Trojan) and EVILNUM. It has also been observed using third-party tools like More_Eggs and open-source tools like LaZagne [7].

It has links with Golden Chickens, providers of MaaS (malware as a service).

Conclusions

In conclusion, this targeted Spear Phishing campaign demonstrated sophistication, affirming its bespoke nature over a random, mass-spamming attempt. The potential consequences were significant despite using less refined language and recycled infrastructure. The incident highlights the crucial role of threat intelligence, emphasizing the necessity for swift and extensive sharing to defend against advanced threats effectively.

We must remember that the “P” in APT is for “Persistent”, so it’s vital to predict that this campaign might change and come back with a different focus but still operated by the same actor.

Acknowledgments

Luis Noriega, Nelson Colón & Emilio Revelo from the Information Security Team actively participated in this investigation. Rob Harrop for his corrections.

References

1. AlienVault OTX Intelligence Pulse on the campaign
2. AlienVault OTX Intelligence Pulses on infrastructure
3. AlienVault OTX Intelligence Pulses on infrastructure
4. CrowdStrike Falcon profile of EVILNUM
5. EVILNUM profile on Mitre
6. bIOChip
7. EVILNUM Toolset on Mitre
8. Lazarus profile on Mitre
9. CrowdStrike Falcon profile of Lazarus: Labyrinth Chollima
