TA4557 Launches Targeted Recruitment Scam via Email | Proofpoint US

By Kelsey Merriman, Selena Larson, and Xavier Chambrier

Published: 2023-12-07 · Archived: 2026-04-05 15:15:14 UTC

What happened

Since at least October 2023, TA4557 began using a new technique of targeting recruiters with direct emails that ultimately lead to malware delivery. The initial emails are benign and express interest in an open role. If the target replies, the attack chain commences.

Previously, throughout most of 2022 and 2023, TA4557 typically applied to existing open job listings purporting to be a job applicant. The actor included malicious URLs, or files containing malicious URLs, in the application. Notably, the URLs were not hyperlinked and the user would have to copy and paste the URL text to visit the website. The legitimate job hosting sites would then generate and send email notifications to the prospective employers who posted the positions.

In recently observed campaigns, TA4557 used both the new method of emailing recruiters directly as well as the older technique of applying to jobs posted on public job boards to commence the attack chain.

Specifically in the attack chain that uses the new direct email technique, once the recipient replies to the initial email, the actor was observed responding with a URL linking to an actor-controlled website posing as a candidate resume. Alternatively, the actor was observed replying with a PDF or Word attachment containing instructions to visit the fake resume website.

From: William Lynch <william@wlynch.com>
Sent: Monday, October 23, 2023 7:03 PM
To: [redacted]com>
Subject: [EXTERNAL] SR ACCOUNTANT

Dear ,

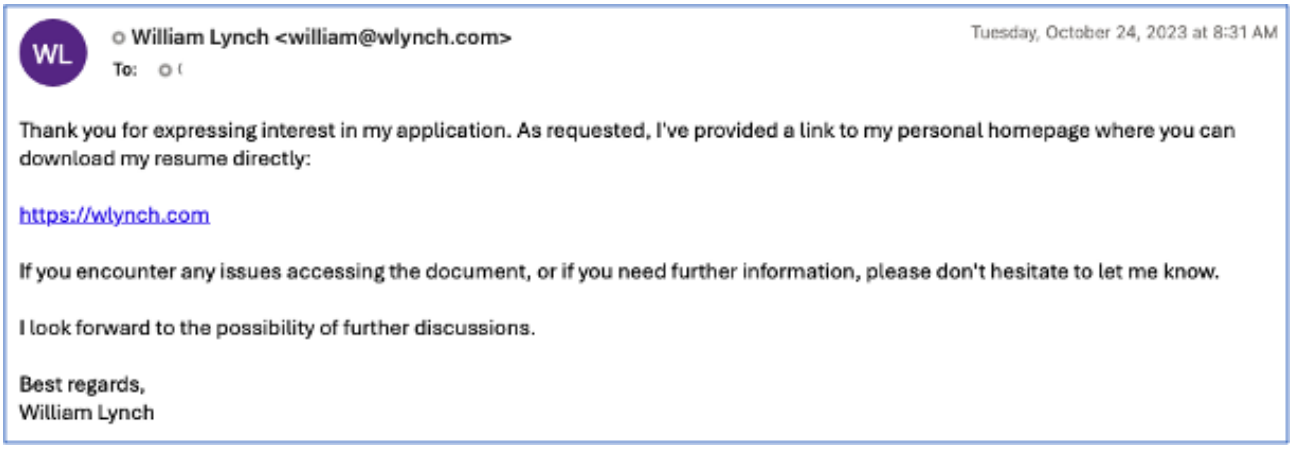
I'm William Lynch, and I'm interested in the accountant position at [redacted]. I've reviewed the job requirements and, with my experience, I believe I match them and can be a valuable addition to your team.

Is this role still available?

Please let me know if there's an opportunity to discuss this further.

Thanks,
William

Example initial outreach email by TA4557 to inquire about a job posting.

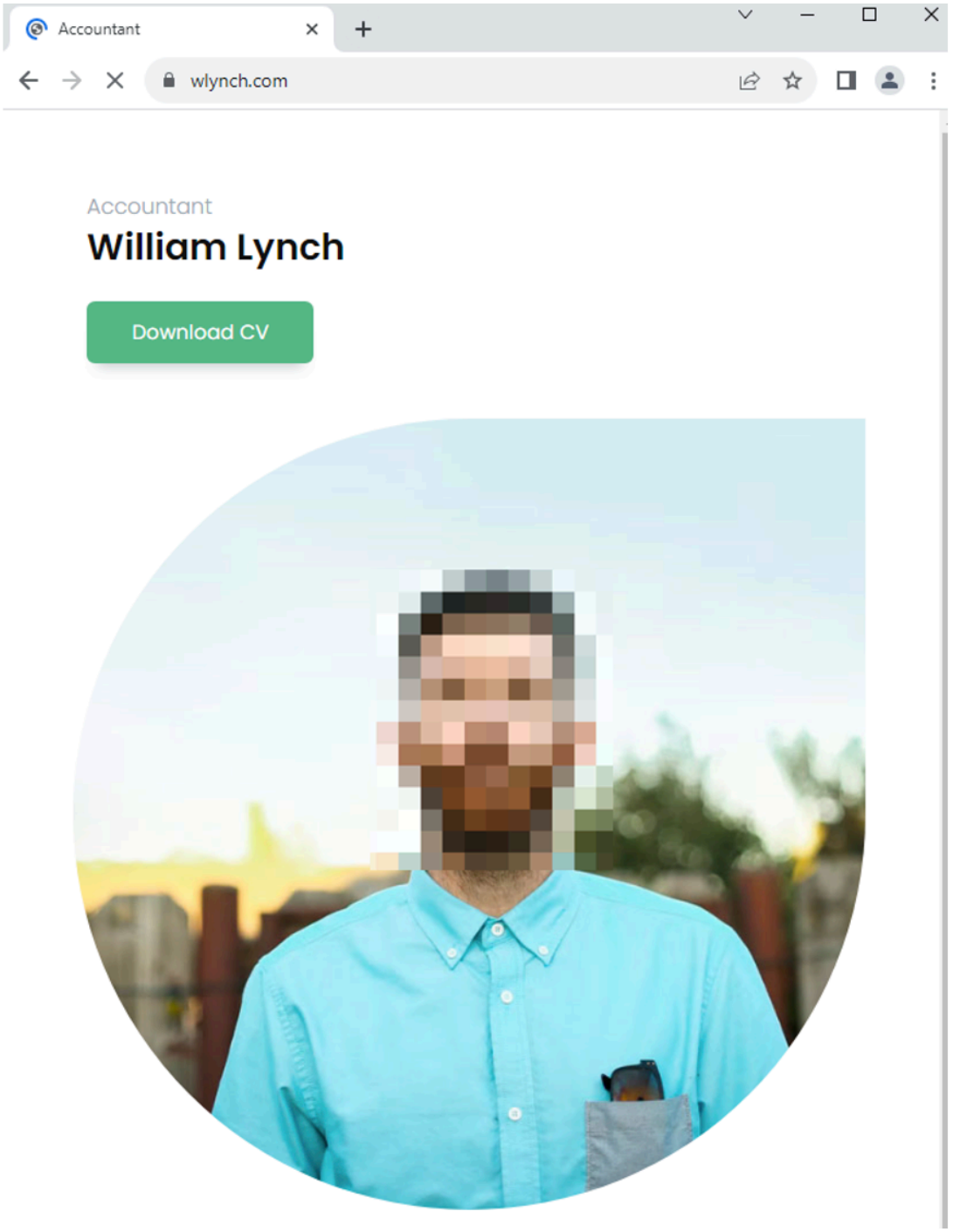


Example follow up email containing a URL linking to a fake resume website.

Very notably, in campaigns observed in early November 2023, Proofpoint observed TA4557 direct the recipient to "refer to the domain name of my email address to access my portfolio" in the initial email instead of sending the resume website URL directly in a follow up response. This is likely a further attempt to evade automated detection of suspicious domains.

Email purporting to be from a candidate directing the recipient to visit the domain in an email address.

If the potential victims visit the "personal website" as directed by the threat actor, the page mimics a candidate's resume or job site for the candidate (TA4557) applying for a posted role. The website uses filtering to determine whether to direct the user to the next stage of the attack chain.



Example of a fake candidate website operated by TA4557 that leads to download of a zip attachment.

If the potential victim does not pass the filtering checks, they are directed to a page containing a resume in plain text. Alternatively, if they pass the filtering checks, they are directed to the candidate website. The candidate website uses a CAPTCHA which, if completed, will initiate the download of a zip file containing a shortcut file (LNK). The LNK, if executed, abuses legitimate software functions in "ie4uinit.exe" to download and execute a scriptlet from a location stored in the "ie4uinit.inf" file. This technique is commonly referred to as "Living Off The Land" (LOTL).

The scriptlet decrypts and drops a DLL in the %APPDATA%\Microsoft folder. Next, it attempts to create a new regsrv32 process to execute the DLL using Windows Management Instrumentation (WMI) and, if that fails, tries

an alternative approach using the ActiveX Object Run method.

The DLL employs anti-sandbox and anti-analysis techniques. It incorporates a loop specifically designed to retrieve the RC4 key necessary for deciphering the More_Eggs backdoor. This loop is strategically crafted to extend its execution time, enhancing its evasion capabilities within a sandbox environment. Furthermore, the DLL employs multiple checks to determine if it is currently being debugged, utilizing the NtQueryInformationProcess function.

The DLL drops the More_Eggs backdoor along with the MSXSL executable. Subsequently, it initiates the creation of the MSXSL process using the WMI service. Once completed, the DLL deletes itself. More_Eggs can be used to establish persistence, profile the machine, and drop additional payloads.

Attribution

Proofpoint has been tracking TA4557 since 2018 as a skilled, financially motivated threat actor known to distribute the More_Eggs backdoor capable of profiling the endpoint and sending additional payloads.

TA4557 is notably different from other priority threat actors tracked by Proofpoint due to the unique tool and malware usage, campaign targeting, use of job candidate-themed lures, sophisticated evasive measures employed to prevent detection, distinct attack chains, and the actor-controlled infrastructure.

Activity attributed to TA4557 has historically overlapped with activity associated to cybercrime group FIN6 by third parties in external reporting. The malware suite used by TA4557 has also been observed to be used by the cybercrime groups Cobalt Group and Evilnum, and Proofpoint tracks these as distinct activity clusters which are not often observed in Proofpoint threat data.

Why it matters

TA4557 demonstrates sophisticated social engineering and tailors their lures to specific, legitimate job opportunities posted online. The tone and content of the emails suggest to the recipient the actor is a legitimate candidate, and because the actor specifically targets people who are involved in recruiting and hiring, the emails do not immediately seem suspicious.

Proofpoint has seen an increase in threat actors using benign messages to build trust and engage with a target before sending the malicious content, and TA4557 adopting this technique may convince recipients to be more trusting of the interaction and subsequent content shared with them. Additionally, the group is regularly changing their sender emails, fake resume domains, and infrastructure. This is done alongside building rapport with the target before sending a payload and poses a problem for defenders and automated security tools as it can be difficult to detect the content as malicious.

Organizations that use third-party job posting websites should be aware of this actor’s tactics, techniques, and procedures (TTPs) and educate employees, especially those in recruiting and hiring functions, about this threat.

Example Emerging Threats signatures

2852061 – ETPRO MALWARE Possible More_eggs Landing Page - Fake Resume/Profile Site

2850476 – ETPRO MALWARE More_eggs CnC Activity

Indicators of compromise

Indicator	Description
wlynch\.com	Domain
9d9b38dffe43b038ce41f0c48def56e92dba3a693e3b572dbd13d5fbc9abc1e4	SHA256
6ea619f5c33c6852d6ed11c52b52589b16ed222046d7f847ea09812c4d51916d	SHA256
annetterawlings\.com	Domain
010b72def59f45662150e08bb80227fe8df07681dcf1a8d6de8b068ee11e0076	SHA256
