



NETMANAGEIT

Intelligence Report

Job Scams Using Bioscience Lures Target Universities

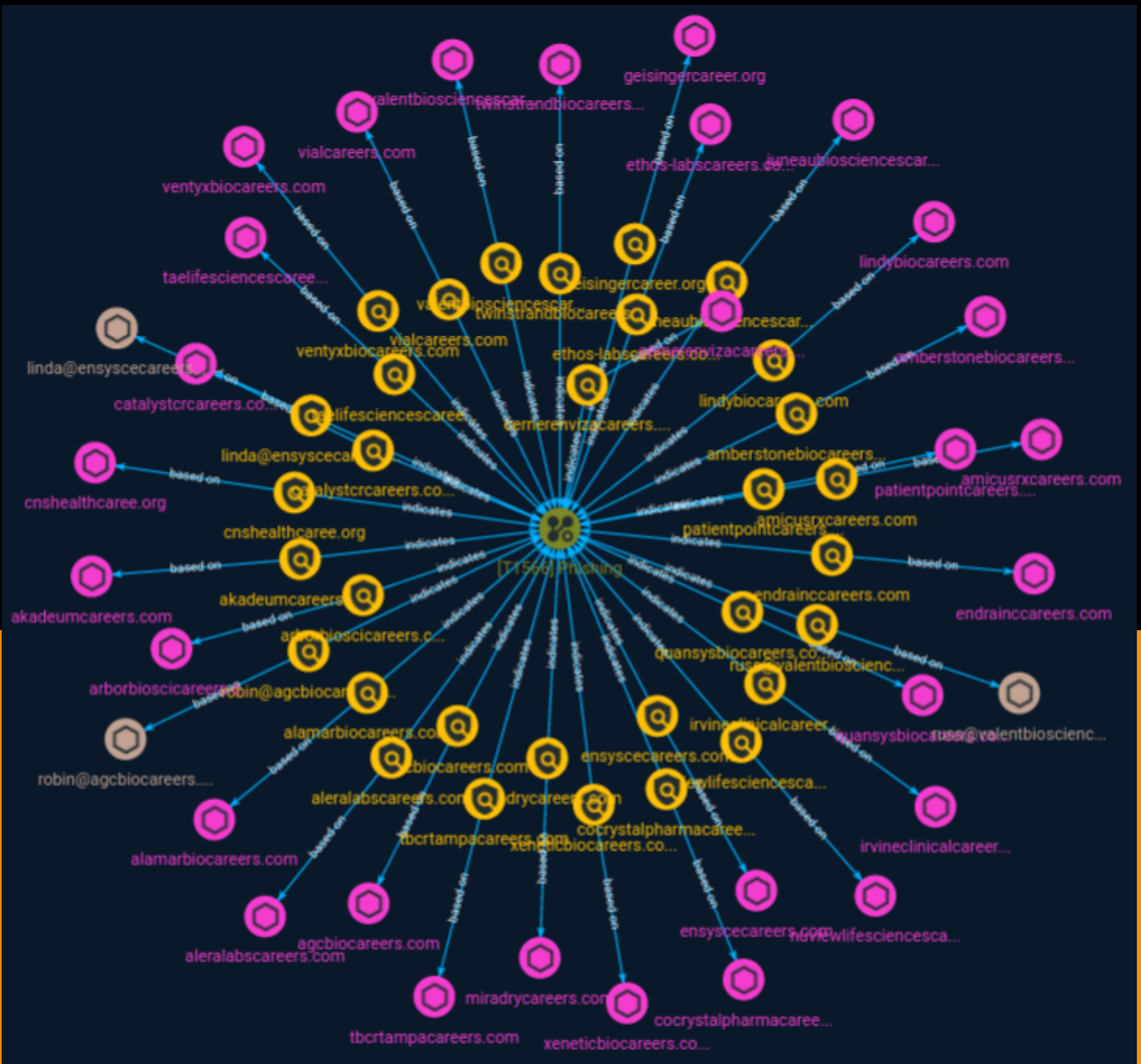


Table of contents

Overview

● Description	4
● Confidence	4

Entities

● Indicator	5
● Sector	16
● Attack-Pattern	17

Observables

● Domain-Name	18
● Email-Addr	20



External References

-
- External References

21

Overview

Description

As layoffs impact thousands of people across many different industries, threat actors continue to exploit the labor market with employment scams to attempt to steal money from job-hunters, based on Proofpoint research and analysis.

Confidence

This value represents the confidence in the correctness of the data contained within this report.

15 / 100

Indicator

Name

irvineclinicalcareers.com

Pattern Type

stix

Pattern

[domain-name:value = 'irvineclinicalcareers.com']

Name

robin@agcbiocareers.com

Pattern Type

stix

Pattern

[email-addr:value = 'robin@agcbiocareers.com']

Name

akadeumcareers.com

Pattern Type

stix

Pattern

[domain-name:value = 'akadeumcareers.com']

Name

geisingercareer.org

Pattern Type

stix

Pattern

[domain-name:value = 'geisingercareer.org']

Name

juneaubiosciencescareers.com

Pattern Type

stix

Pattern

[domain-name:value = 'juneaubiosciencescareers.com']

Name

lindybiocareers.com

Pattern Type

stix

Pattern

[domain-name:value = 'lindybiocareers.com']

Name

linda@ensyscecareers.com

Pattern Type

stix

Pattern

[email-addr:value = 'linda@ensyscecareers.com']

Name

alamarbiocareers.com

Pattern Type

stix

Pattern

[domain-name:value = 'alamarbiocareers.com']

Name

ensyscecareers.com

Pattern Type

stix

Pattern

[domain-name:value = 'ensyscecareers.com']

Name

amberstonebiocareers.com

Pattern Type

stix

Pattern

[domain-name:value = 'amberstonebiocareers.com']

Name

agcbiocareers.com

Pattern Type

stix

Pattern

[domain-name:value = 'agcbiocareers.com']

Name

vialcareers.com

Pattern Type

stix

Pattern

[domain-name:value = 'vialcareers.com']

Name

patientpointcareers.com

Pattern Type

stix

Pattern

[domain-name:value = 'patientpointcareers.com']

Name

cnshealthcaree.org

Pattern Type

stix

Pattern

[domain-name:value = 'cnshealthcaree.org']

Name

quansysbiocareers.com

Pattern Type

stix

Pattern

[domain-name:value = 'quansysbiocareers.com']

Name

russ@valentbiosciencescareers.com

Pattern Type

stix

Pattern

[email-addr:value = 'russ@valentbiosciencescareers.com']

Name

catalystrcareers.com

Pattern Type

stix

Pattern

[domain-name:value = 'catalystrcareers.com']

Name

taelifesciencescareers.com

Pattern Type

stix

Pattern

[domain-name:value = 'taelifesciencescareers.com']

Name

ethos-labscareers.com

Pattern Type

stix

Pattern

[domain-name:value = 'ethos-labscareers.com']

Name

xeneticbiocareers.com

Pattern Type

stix

Pattern

[domain-name:value = 'xeneticbiocareers.com']

Name

miradrycareers.com

Pattern Type

stix

Pattern

[domain-name:value = 'miradrycareers.com']

Name

nuviewlifesciencescareers.com

Pattern Type

stix

Pattern

[domain-name:value = 'nuviewlifesciencescareers.com']

Name

twinstrandbiocareers.com

Pattern Type

stix

Pattern

[domain-name:value = 'twinstrandbiocareers.com']

Name

cocystalpharmacareers.com

Pattern Type

stix

Pattern

[domain-name:value = 'cocystalpharmacareers.com']

Name

amicusrxcareers.com

Pattern Type

stix

Pattern

[domain-name:value = 'amicusrxcareers.com']

Name

arborbiosicareers.com

Pattern Type

stix

Pattern

[domain-name:value = 'arborbiosicareers.com']

Name

tbcrampacareers.com

Pattern Type

stix

Pattern

[domain-name:value = 'tbcrtampacareers.com']

Name

valentbiosciencescareers.com

Pattern Type

stix

Pattern

[domain-name:value = 'valentbiosciencescareers.com']

Name

cernerenvizacareers.com

Pattern Type

stix

Pattern

[domain-name:value = 'cernerenvizacareers.com']

Name

endrainccareers.com

Pattern Type

stix

Pattern

[domain-name:value = 'endrainccareers.com']

Name

ventyxbiocareers.com

Pattern Type

stix

Pattern

[domain-name:value = 'ventyxbiocareers.com']

Name

aleralabscareers.com

Pattern Type

stix

Pattern

[domain-name:value = 'aleralabscareers.com']

Sector

Name

Education

Description

Public or private entities operating to facilitate learning and acquiring knowledge and skills, composed of infrastructures and services to host teachers, students, and administrative services related to this activity. This does not include research activities.

Attack-Pattern

Name

Phishing

ID

T1566

Description

Adversaries may send phishing messages to gain access to victim systems. All forms of phishing are electronically delivered social engineering. Phishing can be targeted, known as spearphishing. In spearphishing, a specific individual, company, or industry will be targeted by the adversary. More generally, adversaries can conduct non-targeted phishing, such as in mass malware spam campaigns. Adversaries may send victims emails containing malicious attachments or links, typically to execute malicious code on victim systems. Phishing may also be conducted via third-party services, like social media platforms. Phishing may also involve social engineering techniques, such as posing as a trusted source, as well as evasive techniques such as removing or manipulating emails or metadata/headers from compromised accounts being abused to send messages (e.g., [Email Hiding Rules](<https://attack.mitre.org/techniques/T1564/008>)).(Citation: Microsoft OAuth Spam 2022)(Citation: Palo Alto Unit 42 VBA Infostealer 2014) Another way to accomplish this is by forging or spoofing(Citation: Proofpoint-spoof) the identity of the sender which can be used to fool both the human recipient as well as automated security tools.(Citation: cyberproof-double-bounce) Victims may also receive phishing messages that instruct them to call a phone number where they are directed to visit a malicious URL, download malware,(Citation: sygnia Luna Month)(Citation: CISA Remote Monitoring and Management Software) or install adversary-accessible remote management tools onto their computer (i.e., [User Execution](<https://attack.mitre.org/techniques/T1204>)).(Citation: Unit42 Luna Moth)

Domain-Name

Value

vialcareers.com

aleralabscareers.com

cnshealthcaree.org

taelifesciencescareers.com

ethos-labscareers.com

geisingercareer.org

amicusrxcareers.com

tbcrampacareers.com

catalystcrcareers.com

valentbiosciencescareers.com

endrainccareers.com

lindybiocareers.com

ensyscecareers.com

juneaubiosciencescareers.com

ventyxbiocareers.com

patientpointcareers.com

nuviewlifesciencescareers.com

cocrystalpharmacareers.com

quansysbiocareers.com

akadeumcareers.com

cernerenvizacareers.com

twinstrandbiocareers.com

irvineclinicalcareers.com

agcbiocareers.com

xeneticbiocareers.com

arborbiosciareers.com

amberstonebiocareers.com

alamarbiocareers.com

miradrycareers.com

Email-Addr

Value

robin@agcbiocareers.com

linda@ensyscecareers.com

russ@valentbiosciencescareers.com

External References

-
- <https://otx.alienvault.com/pulse/64b8f0cefed4e3dd9e0aca9d>
-
- <https://www.proofpoint.com/us/blog/threat-insight/job-scams-using-bioscience-lures-target-universities>