NETMANAGEIT

Intelligence Report

Security alert: social engineering campaign targets technology industry employees
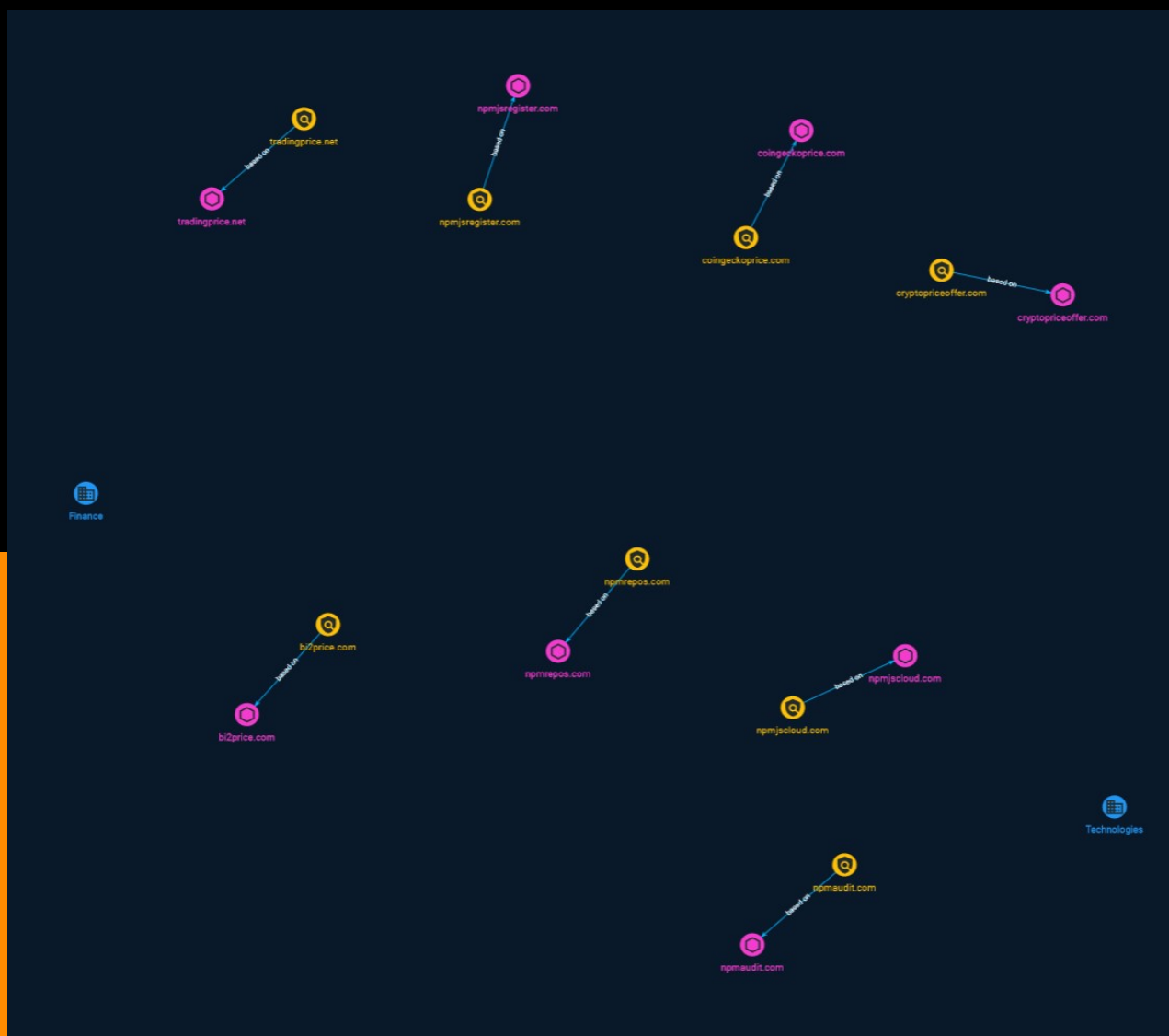
Table of contents

Overview

Entities

Observables

External References

Overview

Description

GitHub has identified a low-volume social engineering campaign that targets the personal accounts of employees of technology firms. No GitHub or npm systems were compromised in this campaign.

Confidence

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

15 / 100

Indicator

Name
coingeckoprice.com

Pattern Type
stix

Pattern
[domain-name:value = 'coingeckoprice.com']

Name
bi2price.com

Pattern Type
stix

Pattern
[domain-name:value = 'bi2price.com']

Name
cryptopriceoffer.com

Pattern Type

stix

Pattern

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

Name

npmaudit.com

Pattern Type

stix

Pattern

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

Name

npmjsregister.com

Pattern Type

stix

Pattern

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

Name

npmrepos.com

Pattern Type

stix

Pattern

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

Name

npmjscloud.com

Pattern Type

stix

Pattern

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

Name

tradingprice.net

Pattern Type

stix

Pattern

[domain-name:value = 'tradingprice.net']

Sector

Name

Technologies

Description

Private entities related to the research, development, manufacturing and distribution of electronics, softwares, computers and products related to information technologies.

Name

Finance

Description

Public and private entities involved in the allocation of assets and liabilities over space and time.

Domain-Name

Value
npmjscloud.com
bi2price.com
coingeckoprice.com
npmaudit.com
tradingprice.net
cryptopriceoffer.com
npmrepos.com
npmjsregister.com

External References

- https://otx.alienvault.com/pulse/64ba889899df4b7ce2fd19bc

- https://github.blog/2023-07-18-security-alert-social-engineering-campaign-targets-technology-industry-employees/#indicators