Jun 21 2023

NETMANAGEIT

Intelligence Report

Analyzing a YouTube Sponsorship Phishing Mail and Malware Targeting Content Creators

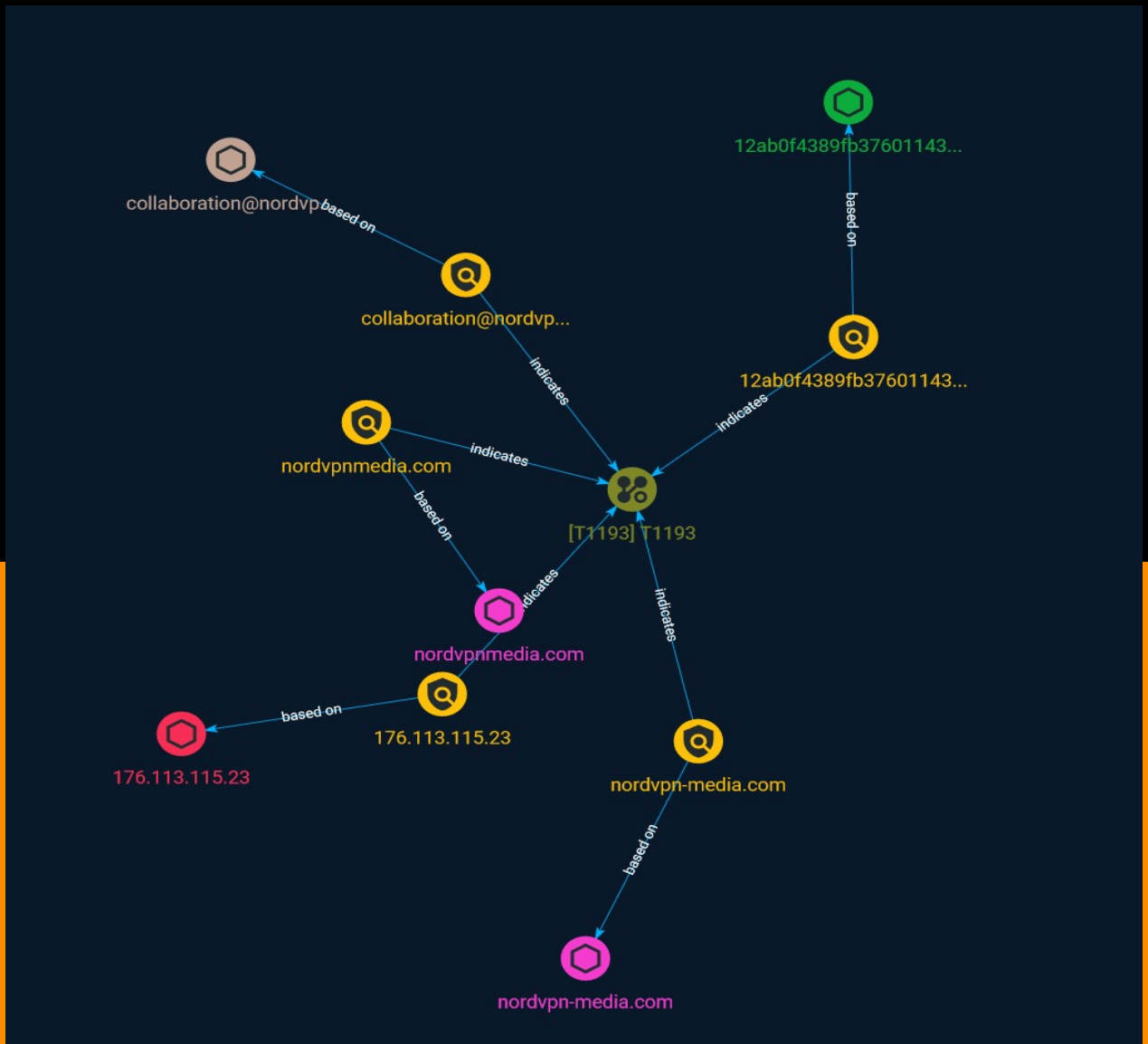

Table of contents

Overview

Entities

Observables

External References

Overview

Description

Analysis of a spear-phishing e-mail masqueraded as an individual representing NordVPN.

Confidence

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

15 / 100

Attack-Pattern

Name
T1193
ID
T1193

Indicator

Name
collaboration@nordvpn-media.com
Pattern Type
stix
Pattern
[email-addr:value = 'collaboration@nordvpn-media.com']
Name
nordvpn-media.com
Pattern Type
stix
Pattern
[domain-name:value = 'nordvpn-media.com']
Name
nordvpnmedia.com

Pattern Type

stix

Pattern

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

Name

12ab0f4389fb376011431b9ffc35cd90447edc980b75574b6b376ef0fd50fd59

Description

ALF:Trojan:MSIL/AgentTesla.KM

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '12ab0f4389fb376011431b9ffc35cd90447edc980b75574b6b376ef0fd50fd59']

Name

176.113.115.23

Description

CC=HK ASN=AS57678 Cat Technologies Co. Limited

Pattern Type

stix
Pattern
[ipv4-addr:value = '176.113.115.23']

Domain-Name

Value
nordvpn-media.com
nordvpnmedia.com

Email-Addr

Value
collaboration@nordvpn-media.com

StixFile

Value
12ab0f4389fb376011431b9ffc35cd90447edc980b75574b6b376ef0fd50fd59

IPv4-Addr

Value
176.113.115.23

External References

- https://otx.alienvault.com/pulse/6492f49bc15b4eb8a929d20e
- https://isc.sans.edu/diary/rss/29966