Dec 11 2023

NETMANAGEIT

Intelligence Report

Analysis of North Korean Hackers' Targeted Phishing Scams on Telegram

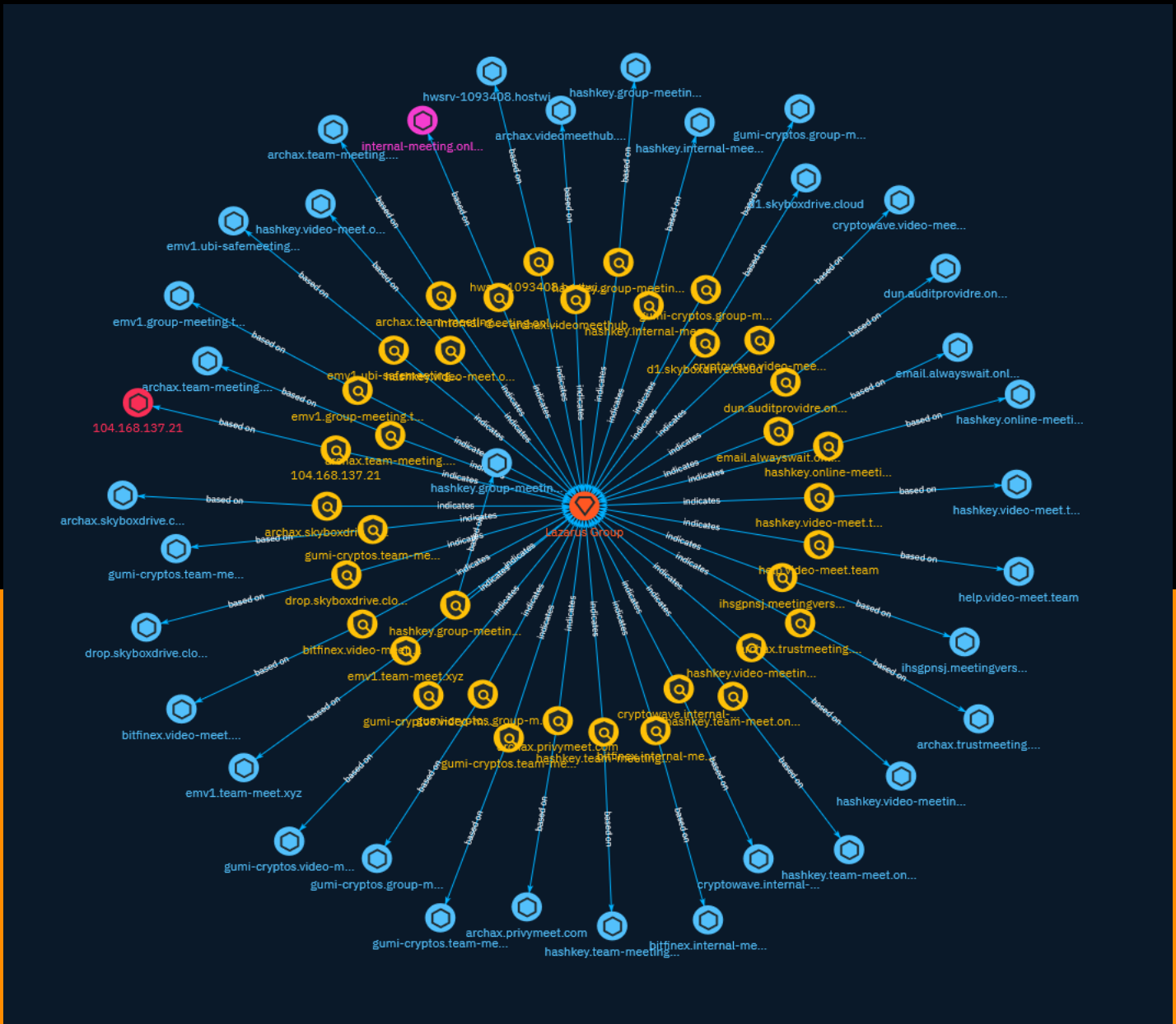

Table of contents

Overview

Entities

Observables

External References

Overview

Description

North Korean hacker group Lazarus initiated a widespread phishing operation on Telegram, specifically targeting the cryptocurrency industry. More recently, these hackers have escalated their tactics by posing as reputable investment institutions to execute phishing scams against various cryptocurrency project teams.

Confidence

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

15 / 100

Content

N/A

Indicator

Name
emv1.ubi-safemeeting.live
Pattern Type
stix
Pattern
[hostname:value = 'emv1.ubi-safemeeting.live']
Name
archax.team-meeting.xyz
Pattern Type
stix
Pattern
[hostname:value = 'archax.team-meeting.xyz']
Name
ihsgpnsj.meetingverse.app

Pattern Type
stix
Pattern
[hostname:value = 'ihsgpnsj.meetingverse.app']
Name
gumi-cryptos.team-meeting.xyz
Pattern Type
stix
Pattern
[hostname:value = 'gumi-cryptos.team-meeting.xyz']
Name
hashkey.team-meet.online
Pattern Type
stix
Pattern
[hostname:value = 'hashkey.team-meet.online']
Name
104.168.137.21

Description

ISP: Hostwinds LLC. **OS:** None ---------- Hostnames: - hwsrv-1093408.hostwindsdns.com - email.alwayswait.online ---------- Domains: - hostwindsdns.com - alwayswait.online ---------- Services: **443:** ``` HTTP/1.1 404 Not Found Server: nginx/1.22.1 Date: Thu, 07 Dec 2023 03:59:52 GMT Content-Type: text/plain; charset=utf-8 Content-Length: 19 Connection: keep-alive X-Content-Type-Options: nosniff ``` HEARTBLEED: 2023/12/07 04:00:01 104.168.137.21:443 - SAFE ---------- **3389:** ``` Remote Desktop Protocol \x03\x00\x00\x13\x0e\xd0\x00\x00\x124\x00\x02\x1f\x08\x00\x02\x00\x00\x00 Remote Desktop Protocol NTLM Info: OS: Windows 10 (version 1809)/Windows Server 2019 (version 1809) OS Build: 10.0.17763 Target Name: HWC-HWP-7779700 NetBIOS Domain Name: HWC-HWP-7779700 NetBIOS Computer Name: HWC-HWP-7779700 DNS Domain Name: hwc-hwp-7779700 FQDN: hwc-hwp-7779700 ``` ----------

Pattern Type

stix

Pattern

[ipv4-addr:value = '104.168.137.21']

Name

hashkey.internal-meeting.online

Pattern Type

stix

Pattern

[hostname:value = 'hashkey.internal-meeting.online']

Name

hwsrv-1093408.hostwindsdns.com

Pattern Type

stix

Pattern

[hostname:value = 'hwsrv-1093408.hostwindsdns.com']

Name

emv1.group-meeting.team

Pattern Type

stix

Pattern

[hostname:value = 'emv1.group-meeting.team']

Name

archax.privymeet.com

Pattern Type

stix

Pattern

[hostname:value = 'archax.privymeet.com']

Name

help.video-meet.team

Pattern Type

stix

Pattern

[hostname:value = 'help.video-meet.team']

Name

email.alwayswait.online

Pattern Type

stix

Pattern

[hostname:value = 'email.alwayswait.online']

Name

internal-meeting.online

Pattern Type

stix

Pattern

[domain-name:value = 'internal-meeting.online']

Name

hashkey.video-meet.team

Pattern Type

stix

Pattern

[hostname:value = 'hashkey.video-meet.team']

Name

drop.skyboxdrive.cloud

Pattern Type

stix

Pattern

[hostname:value = 'drop.skyboxdrive.cloud']

Name

hashkey.group-meeting.online

Pattern Type

stix

Pattern

[hostname:value = 'hashkey.group-meeting.online']

Name

emv1.team-meet.xyz

Pattern Type

stix

Pattern

[hostname:value = 'emv1.team-meet.xyz']

Name

bitfinex.video-meet.online

Pattern Type

stix

Pattern

[hostname:value = 'bitfinex.video-meet.online']

Name

cryptowave.video-meet.online

Pattern Type

stix

Pattern

[hostname:value = 'cryptowave.video-meet.online']

Name

gumi-cryptos.group-meeting.online

Pattern Type

stix

Pattern

[hostname:value = 'gumi-cryptos.group-meeting.online']

Name

archax.skyboxdrive.cloud

Pattern Type

stix

Pattern

[hostname:value = 'archax.skyboxdrive.cloud']

Name

hashkey.online-meeting.team

Pattern Type

stix

Pattern

[hostname:value = 'hashkey.online-meeting.team']

Name

archax.team-meeting.pro

Pattern Type

stix

Pattern

[hostname:value = 'archax.team-meeting.pro']

Name

hashkey.video-meet.online

Pattern Type

stix

Pattern

[hostname:value = 'hashkey.video-meet.online']

Name

bitfinex.internal-meeting.online

Pattern Type

stix

Pattern

[hostname:value = 'bitfinex.internal-meeting.online']

Name

cryptowave.internal-meeting.online

Pattern Type

stix

Pattern

[hostname:value = 'cryptowave.internal-meeting.online']

Name

d1.skyboxdrive.cloud

Pattern Type

stix

Pattern

[hostname:value = 'd1.skyboxdrive.cloud']

Name

hashkey.team-meeting.xyz

Pattern Type

stix

Pattern

[hostname:value = 'hashkey.team-meeting.xyz']

Name

gumi-cryptos.group-meeting.team

Pattern Type

stix

Pattern

[hostname:value = 'gumi-cryptos.group-meeting.team']

Name

archax.videomeethub.online

Pattern Type

stix

Pattern

[hostname:value = 'archax.videomeethub.online']

Name

hashkey.group-meeting.team

Pattern Type

stix

Pattern

[hostname:value = 'hashkey.group-meeting.team']

Name

gumi-cryptos.team-meet.online

Pattern Type

stix

Pattern

[hostname:value = 'gumi-cryptos.team-meet.online']

Name

hashkey.video-meeting.team

Pattern Type

stix

Pattern

[hostname:value = 'hashkey.video-meeting.team']

Name

dun.auditprovidre.online

Pattern Type

stix

Pattern

[hostname:value = 'dun.auditprovidre.online']

Name

archax.trustmeeting.live

Pattern Type

stix

Pattern

[hostname:value = 'archax.trustmeeting.live']

Name

gumi-cryptos.video-meet.team

Pattern Type

stix

Pattern

[hostname:value = 'gumi-cryptos.video-meet.team']

Intrusion-Set

Name

Lazarus Group

Description

[Lazarus Group](https://attack.mitre.org/groups/G0032) is a North Korean state-sponsored cyber threat group that has been attributed to the Reconnaissance General Bureau. (Citation: US-CERT HIDDEN COBRA June 2017)(Citation: Treasury North Korean Cyber Groups September 2019) The group has been active since at least 2009 and was reportedly responsible for the November 2014 destructive wiper attack against Sony Pictures Entertainment as part of a campaign named Operation Blockbuster by Novetta. Malware used by [Lazarus Group](https://attack.mitre.org/groups/G0032) correlates to other reported campaigns, including Operation Flame, Operation 1Mission, Operation Troy, DarkSeoul, and Ten Days of Rain. (Citation: Novetta Blockbuster) North Korean group definitions are known to have significant overlap, and some security researchers report all North Korean state-sponsored cyber activity under the name [Lazarus Group](https://attack.mitre.org/groups/G0032) instead of tracking clusters or subgroups, such as [Andariel](https://attack.mitre.org/groups/G0138), [APT37](https://attack.mitre.org/groups/G0067), [APT38](https://attack.mitre.org/groups/G0082), and [Kimsuky](https://attack.mitre.org/groups/G0094).

Domain-Name

Value
internal-meeting.online

Hostname

Value
cryptowave.internal-meeting.online
archax.skyboxdrive.cloud
hashkey.online-meeting.team
archax.privymeet.com
archax.team-meeting.xyz
hashkey.video-meeting.team
bitfinex.video-meet.online
archax.team-meeting.pro
hashkey.team-meeting.xyz
d1.skyboxdrive.cloud
dun.auditprovidre.online
gumi-cryptos.video-meet.team
drop.skyboxdrive.cloud

archax.trustmeeting.live

hashkey.video-meet.online

email.alwayswait.online

ihsgpnsj.meetingverse.app

emv1.ubi-safemeeting.live

hashkey.video-meet.team

gumi-cryptos.group-meeting.online

cryptowave.video-meet.online

hashkey.team-meet.online

emv1.group-meeting.team

gumi-cryptos.group-meeting.team

gumi-cryptos.team-meeting.xyz

hwsrv-1093408.hostwindsdns.com

help.video-meet.team

emv1.team-meet.xyz

hashkey.internal-meeting.online

bitfinex.internal-meeting.online

archax.videomeethub.online

hashkey.group-meeting.team
gumi-cryptos.team-meet.online
hashkey.group-meeting.online

IPv4-Addr

Value
104.168.137.21

External References

- https://otx.alienvault.com/pulse/65773dc2466c7161e66b3d07
- https://slowmist.medium.com/analysis-of-north-korean-hackers-targeted-phishing-scams-on-telegram-872db3f7392b