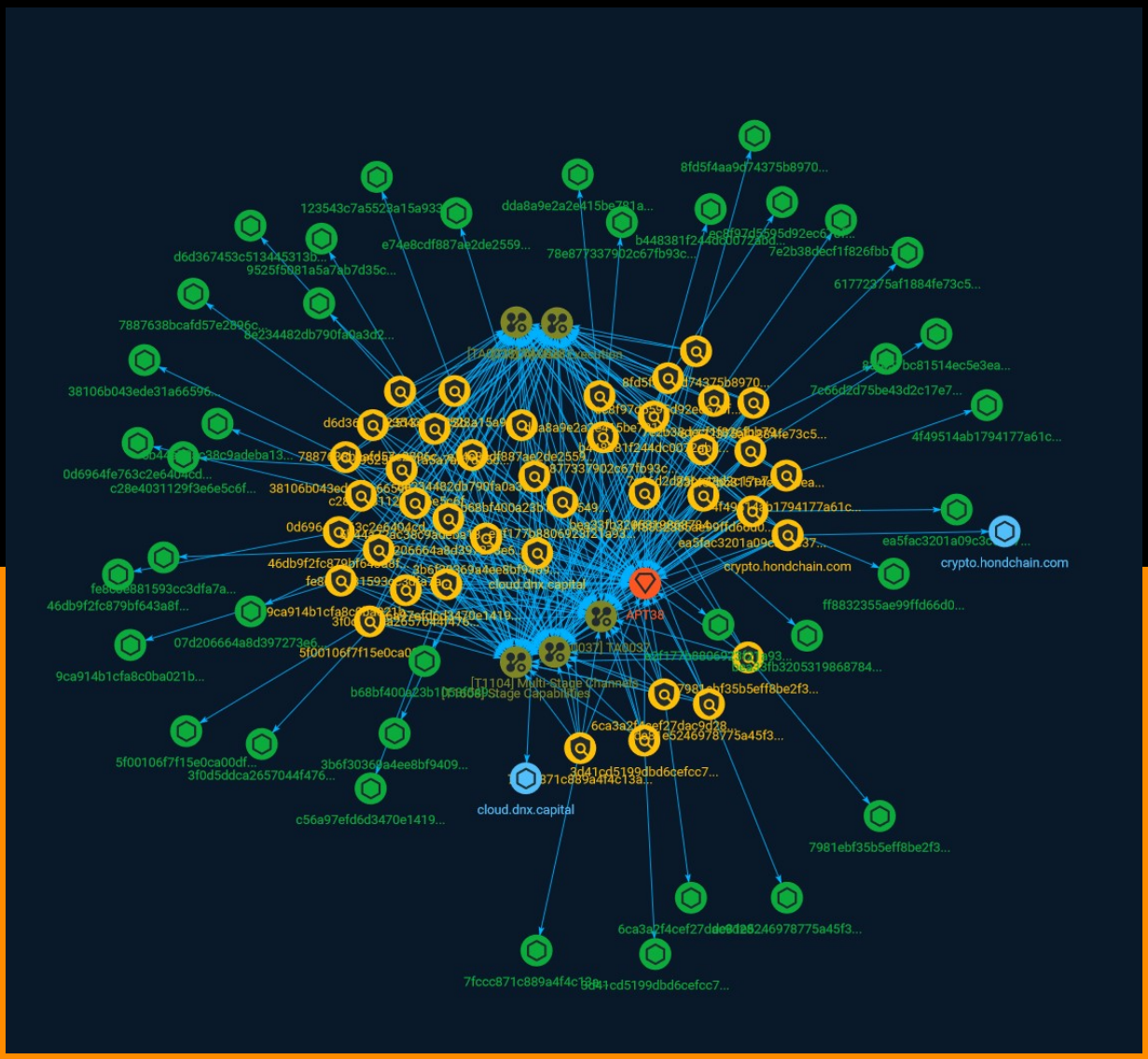
Jul 05 2023

NETMANAGEIT

# Intelligence Report

# BlueNoroff | How DPRK's macOS RustBucket Seeks to Evade Analysis and Detection



# Table of contents

## Overview



## Entities



## Observables

# External References

# Overview

## Description

Back in April, researchers at JAMF detailed a sophisticated APT campaign targeting macOS users with multi-stage malware that culminated in a Rust backdoor capable of downloading and executing further malware on infected devices. ‘RustBucket’, as they labeled it, was attributed with strong confidence to the BlueNoroff APT, generally assumed to be a subsidiary of the wider DPRK cyber attack group known as Lazarus.

## Confidence

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

15 / 100

# Indicator

**Name**

ea5fac3201a09c3c5c3701723ea9a5fec8bbc4f1f236463d651303f40a245452

**Description**

SHA256 of 9121509d674091ce1f5f30e9a372b5dcf9bcd257

**Pattern Type**

stix

**Pattern**

[file:hashes.'SHA-256' = 'ea5fac3201a09c3c5c3701723ea9a5fec8bbc4f1f236463d651303f40a245452']

**Name**

c56a97efd6d3470e14193ac9e194fa46d495e3dddc918219cca530b90f01d11e

**Description**

SHA256 of 7a5d57c7e2b0c8ab7d60f7a7c7f4649f33fea8aa

**Pattern Type**

stix

**Pattern**

[file:hashes.'SHA-256' = 'c56a97efd6d3470e14193ac9e194fa46d495e3dddc918219cca530b90f01d11e']

**Name**

3f0d5ddca2657044f4763ae53c4f33c8a7814ba451b60d24430a126674125624

**Description**

SHA256 of 338af1d91b846f2238d5a518f951050f90693488

**Pattern Type**

stix

**Pattern**

[file:hashes.'SHA-256' = '3f0d5ddca2657044f4763ae53c4f33c8a7814ba451b60d24430a126674125624']

**Name**

5f00106f7f15e0ca00df4dbb0eeccd57930b4b81bc9aa3fca0c5af4eda339ab7

**Description**

multiple_versions SHA256 of 7f8f43326f1ce505a8cd9f469a2ded81fa5c81be

**Pattern Type**

stix

**Pattern**

[file:hashes.'SHA-256' = '5f00106f7f15e0ca00df4dbb0eeccd57930b4b81bc9aa3fca0c5af4eda339ab7']

**Name**

3b6f30369a4ee8bf9409d141b6d1b3fb4286c34984b5de005ed7431df549b17e

**Description**

SHA256 of 5304031dc990790a26184b05b3019b2c5fa7022a

**Pattern Type**

stix

**Pattern**

[file:hashes.'SHA-256' = '3b6f30369a4ee8bf9409d141b6d1b3fb4286c34984b5de005ed7431df549b17e']

**Name**

8e234482db790fa0a3d2bf5f7084ec4cfb74bffd5f6cbdc5abdbc1350f58e3fe

**Description**

multiple_versions SHA256 of 469236d0054a270e117a2621f70f2a494e7fb823

**Pattern Type**

stix

**Pattern**

[file:hashes.'SHA-256' = '8e234482db790fa0a3d2bf5f7084ec4cfb74bffd5f6cbdc5abdbc1350f58e3fe']

**Name**

7c66d2d75be43d2c17e75d37c39344a9b5d29ee5c5861f178aa7d9f34208eb48

**Description**

SHA256 of dabb4372050264f389b8adcf239366860662ac52

**Pattern Type**

stix

**Pattern**

[file:hashes.'SHA-256' = '7c66d2d75be43d2c17e75d37c39344a9b5d29ee5c5861f178aa7d9f34208eb48']

**Name**

ff8832355ae99ffd66d0fe9eda2d74efdf3ed87bb2a4c215b93ade93165f7c0b

**Description**

SHA256 of e2bcdfbda85c55a4d6070c18723ba4adb7631807

**Pattern Type**

stix

**Pattern**

[file:hashes.'SHA-256' = 'ff8832355ae99ffd66d0fe9eda2d74efdf3ed87bb2a4c215b93ade93165f7c0b']

**Name**

123543c7a5523a15a933e32477b8cba4cd79a680bb69ef2dba178700bfb9ec07

**Description**

multiple_versions SHA256 of e7158bb75adf27262ec3b0f2ca73c802a6222379

**Pattern Type**

stix

**Pattern**

[file:hashes.'SHA-256' = '123543c7a5523a15a933e32477b8cba4cd79a680bb69ef2dba178700bfb9ec07']

**Name**

e74e8cdf887ae2de25590c55cb52dad66f0135ad4a1df224155f772554ea970c

**Description**

SHA256 of e0e42ac374443500c236721341612865cd3d1eec

**Pattern Type**

stix

**Pattern**

[file:hashes.'SHA-256' = 'e74e8cdf887ae2de25590c55cb52dad66f0135ad4a1df224155f772554ea970c']

**Name**

78e877337902c67fb93c5fdc3b1d9710292a29b97dc98f3cc319ac3edbb760a4

**Description**

SHA256 of b02922869e86ad06ff6380e8ec0be8db38f5002b

**Pattern Type**

stix

**Pattern**

[file:hashes.'SHA-256' = '78e877337902c67fb93c5fdc3b1d9710292a29b97dc98f3cc319ac3edbb760a4']

**Name**

38106b043ede31a66596299f17254d3f23cbe1f983674bf9ead5006e0f0bf880

**Description**

SHA256 of 72167ec09d62cdfb04698c3f96a6131dceb24a9c

**Pattern Type**

stix

**Pattern**

[file:hashes.'SHA-256' = '38106b043ede31a66596299f17254d3f23cbe1f983674bf9ead5006e0f0bf880']

**Name**

b68bf400a23b1053f54911a2b826d341f6bf87c26bea5e6cf21710ee569a7aab

**Description**

SHA256 of 0738687206a88ecbee176e05e0518effa4ca4166

**Pattern Type**

stix

**Pattern**

[file:hashes.'SHA-256' = 'b68bf400a23b1053f54911a2b826d341f6bf87c26bea5e6cf21710ee569a7aab']

**Name**

cloud.dnx.capital

**Pattern Type**

stix

**Pattern**

[hostname:value = 'cloud.dnx.capital']

**Name**

d6d367453c513445313be7339666e4faeeebeae71620c187012ea5ae2901df34

**Description**

SHA256 of d5971e8a3e8577dbb6f5a9aad248c842a33e7a26

**Pattern Type**

stix

**Pattern**

[file:hashes.'SHA-256' = 'd6d367453c513445313be7339666e4faeeebeae71620c187012ea5ae2901df34']

**Name**

6ca3a2f4cef27dac9d28c1ec2b29a8fa09dfc6dbbaf58e00dddbf5c1dd3b3cc3

**Description**

SHA256 of 7e1870a5b24c78a5e357568969aae3a5e7ab857d

**Pattern Type**

stix

**Pattern**

[file:hashes.'SHA-256' = '6ca3a2f4cef27dac9d28c1ec2b29a8fa09dfc6dbbaf58e00dddbf5c1dd3b3cc3']

**Name**

9525f5081a5a7ab7d35cf2fb2d7524e0777e37fe3df62730e1e7de50506850f7

**Description**

SHA256 of ca59874172660e6180af2815c3a42c85169aa0b2

**Pattern Type**

stix

**Pattern**

[file:hashes.'SHA-256' = '9525f5081a5a7ab7d35cf2fb2d7524e0777e37fe3df62730e1e7de50506850f7']

**Name**

61772375af1884fe73c5d154b8637dd62f26d23bc38d18462a88e2bbed483fd7

**Description**

SHA256 of 9a5f6a641cc170435f52c6a759709a62ad5757c7

**Pattern Type**

stix

**Pattern**

[file:hashes.'SHA-256' = '61772375af1884fe73c5d154b8637dd62f26d23bc38d18462a88e2bbed483fd7']

**Name**

3d41cd5199dbd6cefcc78d53bb44a2ecbea716de2bc8e547ead7c2aebd9925f0

**Description**

multiple_versions SHA256 of 7e69cb4f9c37fad13de85e91b5a05a816d14f490

**Pattern Type**

stix

**Pattern**

[file:hashes.'SHA-256' = '3d41cd5199dbd6cefcc78d53bb44a2ecbea716de2bc8e547ead7c2aebd9925f0']

**Name**

c28e4031129f3e6e5c6fbd7b1cebd8dd21b6f87a8564b0fb9ee741a9b8bc0197

**Description**

SHA256 of 9676f0758c8e8d0e0d203c75b922bcd0aeaa0873

**Pattern Type**

stix

**Pattern**

[file:hashes.'SHA-256' = 'c28e4031129f3e6e5c6fbd7b1cebd8dd21b6f87a8564b0fb9ee741a9b8bc0197']

**Name**

b448381f244dc0072abd4f52e01ca93efaebb2c0a8ea8901c4725ecb1b2b0656

**Description**

SHA256 of a1a85cba1bc4ac9f6eafc548b1454f57b4dff7e0

**Pattern Type**

stix

**Pattern**

[file:hashes.'SHA-256' = 'b448381f244dc0072abd4f52e01ca93efaebb2c0a8ea8901c4725ecb1b2b0656']

**Name**

0d6964fe763c2e6404cde68af2c5f86d34cf50a88bd81bc06bba739010821db0

**Description**

SHA256 of d9f1392fb7ed010a0ecc4f819782c179efde9687

**Pattern Type**

stix

**Pattern**

[file:hashes.'SHA-256' = '0d6964fe763c2e6404cde68af2c5f86d34cf50a88bd81bc06bba739010821db0']

**Name**

dda8a9e2a2e415be781a39fdf41f1551af2344f1b1a0ddf921d8aeba90343d1b

**Description**

SHA256 of 5933f1a20117d48985b60b10b5e42416ac00e018

**Pattern Type**

stix

**Pattern**

[file:hashes.'SHA-256' = 'dda8a9e2a2e415be781a39fdf41f1551af2344f1b1a0ddf921d8aeba90343d1b']

**Name**

bea33fb3205319868784c028418411ee796d6ee3dfe9309f143e7e8106116a49

**Description**

SHA256 of fd1cef5abe3e0c275671916a1f3a566f13489416

**Pattern Type**

stix

**Pattern**

[file:hashes.'SHA-256' = 'bea33fb3205319868784c028418411ee796d6ee3dfe9309f143e7e8106116a49']

**Name**

46db9f2fc879bf643a8f05e2b35879b235cbb04aa06fe548f0bc7c7c02483cf3

**Description**

SHA256 of 963a86aab1e450b03d51628797572fe9da8410a2

**Pattern Type**

stix

**Pattern**

[file:hashes.'SHA-256' = '46db9f2fc879bf643a8f05e2b35879b235cbb04aa06fe548f0bc7c7c02483cf3']

**Name**

83f457bc81514ec5e3ea123fc237811a36da6ce7f975ad56d62e34af4d1f37c0

**Description**

SHA256 of 89301dfdc5361f1650796fecdac30b7d86c65122

**Pattern Type**

stix

**Pattern**

[file:hashes.'SHA-256' = '83f457bc81514ec5e3ea123fc237811a36da6ce7f975ad56d62e34af4d1f37c0']

**Name**

e2f177b8806923f21a93952b61aedbeb02d829a67a820a7aab5ee72512e3d646

**Description**

SHA256 of 27b101707b958139c32388eb4fd79fcd133ed880

**Pattern Type**

stix

**Pattern**

[file:hashes.'SHA-256' = 'e2f177b8806923f21a93952b61aedbeb02d829a67a820a7aab5ee72512e3d646']

**Name**

07d206664a8d397273e69ce37ef7cf933c22e93b62d95b673d6e835876feba06

**Description**

multiple_versions SHA256 of be234cb6819039d6a1d3b1a205b9f74b6935bbcc

**Pattern Type**

stix

**Pattern**

[file:hashes.'SHA-256' = '07d206664a8d397273e69ce37ef7cf933c22e93b62d95b673d6e835876feba06']

**Name**

7e2b38decf1f826fbb792d762d9e6a29147e9ecb44eb2ad2c4dc08e7ee01a140

**Description**

SHA256 of 0be69bb9836b2a266bfd9a8b93bb412b6e4ce1be

**Pattern Type**

stix

**Pattern**

[file:hashes.'SHA-256' = '7e2b38decf1f826fbb792d762d9e6a29147e9ecb44eb2ad2c4dc08e7ee01a140']

**Name**

5b44a72ac38c9adeba133b516250f53d3cd13f4018cff7daf44a328ebc6c5ad0

**Description**

SHA256 of 0df7e1d3b3d54336d986574441778c827ff84bf2

**Pattern Type**

stix

**Pattern**

[file:hashes.'SHA-256' = '5b44a72ac38c9adeba133b516250f53d3cd13f4018cff7daf44a328ebc6c5ad0']

**Name**

8fd5f4aa9d74375b8970844a9d6c479bc7dfa257132ee8a25d5cd404e19168c8

**Description**

SHA256 of 7f9694b46227a8ebc67745e533bc0c5f38fdfa59

**Pattern Type**

stix

**Pattern**

[file:hashes.'SHA-256' = '8fd5f4aa9d74375b8970844a9d6c479bc7dfa257132ee8a25d5cd404e19168c8']

**Name**

7981ebf35b5eff8be2f3849c8f3085b9cec10d9759ff4d3afd46990520de0407

**Description**

SHA256 of ac08406818bbf4fe24ea04bfd72f747c89174bdb

**Pattern Type**

stix

**Pattern**

[file:hashes.'SHA-256' = '7981ebf35b5eff8be2f3849c8f3085b9cec10d9759ff4d3afd46990520de0407']

**Name**

7887638bcafd57e2896c7c16698e927ce92fd7d409aae698d33cdca3ce8d25b8

**Description**

SHA256 of ed4f16b36bc47a701814b63e30d8ea7a226ca906

**Pattern Type**

stix

**Pattern**

[file:hashes.'SHA-256' = '7887638bcafd57e2896c7c16698e927ce92fd7d409aae698d33cdca3ce8d25b8']

**Name**

crypto.hondchain.com

**Pattern Type**

stix

**Pattern**

[hostname:value = 'crypto.hondchain.com']

**Name**

fe8c0e881593cc3dfa7a66e314b12b322053c67cbc9b606d5a2c0a12f097ef69

**Description**

SHA256 of 69f24956fb75beb9b93ef974d873914500e35601

**Pattern Type**

stix

**Pattern**

[file:hashes.'SHA-256' = 'fe8c0e881593cc3dfa7a66e314b12b322053c67cbc9b606d5a2c0a12f097ef69']

**Name**

ec8f97d5595d92ec678ffbf5ae1f60ce90e620088927f751c76935c46aa7dc41

**Description**

SHA256 of 3cc19cef767dee93588525c74fe9c1f1bf6f8007

**Pattern Type**

stix

**Pattern**

[file:hashes.'SHA-256' = 'ec8f97d5595d92ec678ffbf5ae1f60ce90e620088927f751c76935c46aa7dc41']

**Name**

de81e5246978775a45f3dbda43e2716aaa1b1c4399fe7d44f918fccecc4dd500

**Description**

SHA256 of 8a1b32ab8c2a889985e530425ae00f4428c575cc

**Pattern Type**

stix

**Pattern**

[file:hashes.'SHA-256' = 'de81e5246978775a45f3dbda43e2716aaa1b1c4399fe7d44f918fccecc4dd500']

**Name**

9ca914b1cfa8c0ba021b9e00bda71f36cad132f27cf16bda6d937badee66c747

**Description**

MacOS:Nukesped-A\ [Drp] SHA256 of 182760cbe11fa0316abfb8b7b00b63f83159f5aa

**Pattern Type**

stix

**Pattern**

[file:hashes.'SHA-256' = '9ca914b1cfa8c0ba021b9e00bda71f36cad132f27cf16bda6d937badee66c747']

**Name**

4f49514ab1794177a61c50c63b93b903c46f9b914c32ebe9c96aa3cbc1f99b16

**Description**

SHA256 of cd8f41b91e8f1d8625e076f0a161e46e32c62bbf

**Pattern Type**

stix

**Pattern**

[file:hashes.'SHA-256' = '4f49514ab1794177a61c50c63b93b903c46f9b914c32ebe9c96aa3cbc1f99b16']

**Name**

7fccc871c889a4f4c13a977fdd5f062d6de23c3ffd27e72661c986fae6370387

**Description**

SHA256 of 831dc7bc4a234907d94a889bcb60b7bedf1a1e13

| Pattern Type |
| --- |
| stix |

| Pattern |
| --- |
| [file:hashes.'SHA-256' = '7fccc871c889a4f4c13a977fdd5f062d6de23c3ffd27e72661c986fae6370387'] |

# Attack-Pattern

| Name |
| --- |
| TA0028 |
| **ID** |
| TA0028 |
| **Name** |
| TA0037 |
| **ID** |
| TA0037 |
| **Name** |
| Stage Capabilities |
| **ID** |
| T1608 |
| **Description** |
| Adversaries may upload, install, or otherwise set up capabilities that can be used during targeting. To support their operations, an adversary may need to take capabilities they |

developed ([Develop Capabilities](https://attack.mitre.org/techniques/T1587)) or obtained ([Obtain Capabilities](https://attack.mitre.org/techniques/T1588)) and stage them on infrastructure under their control. These capabilities may be staged on infrastructure that was previously purchased/rented by the adversary ([Acquire Infrastructure](https://attack.mitre.org/techniques/T1583)) or was otherwise compromised by them ([Compromise Infrastructure](https://attack.mitre.org/techniques/T1584)). Capabilities may also be staged on web services, such as GitHub or Pastebin, or on Platform-as-a-Service (PaaS) offerings that enable users to easily provision applications.(Citation: Volexity Ocean Lotus November 2020)(Citation: Dragos Heroku Watering Hole)(Citation: Malwarebytes Heroku Skimmers)(Citation: Netskope GCP Redirection)(Citation: Netskope Cloud Phishing) Staging of capabilities can aid the adversary in a number of initial access and post-compromise behaviors, including (but not limited to): * Staging web resources necessary to conduct [Drive-by Compromise](https://attack.mitre.org/techniques/T1189) when a user browses to a site.(Citation: FireEye CFR Watering Hole 2012)(Citation: Gallagher 2015)(Citation: ATT ScanBox) * Staging web resources for a link target to be used with spearphishing.(Citation: Malwarebytes Silent Librarian October 2020)(Citation: Proofpoint TA407 September 2019) * Uploading malware or tools to a location accessible to a victim network to enable [Ingress Tool Transfer](https://attack.mitre.org/techniques/T1105).(Citation: Volexity Ocean Lotus November 2020) * Installing a previously acquired SSL/TLS certificate to use to encrypt command and control traffic (ex: [Asymmetric Cryptography](https://attack.mitre.org/techniques/T1573/002) with [Web Protocols](https://attack.mitre.org/techniques/T1071/001)).(Citation: DigiCert Install SSL Cert)

# Intrusion-Set

## Name

APT38

## Description

[APT38](https://attack.mitre.org/groups/G0082) is a North Korean state-sponsored threat group that specializes in financial cyber operations; it has been attributed to the Reconnaissance General Bureau.(Citation: CISA AA20-239A BeagleBoyz August 2020) Active since at least 2014, [APT38](https://attack.mitre.org/groups/G0082) has targeted banks, financial institutions, casinos, cryptocurrency exchanges, SWIFT system endpoints, and ATMs in at least 38 countries worldwide. Significant operations include the 2016 Bank of Bangladesh heist, during which [APT38](https://attack.mitre.org/groups/G0082) stole $81 million, as well as attacks against Bancomext (2018) and Banco de Chile (2018); some of their attacks have been destructive.(Citation: CISA AA20-239A BeagleBoyz August 2020) (Citation: FireEye APT38 Oct 2018)(Citation: DOJ North Korea Indictment Feb 2021)(Citation: Kaspersky Lazarus Under The Hood Blog 2017) 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.

# StixFile

| Value |
| --- |
| e2f177b8806923f21a93952b61aedbeb02d829a67a820a7aab5ee72512e3d646 |
| c28e4031129f3e6e5c6fbd7b1cebd8dd21b6f87a8564b0fb9ee741a9b8bc0197 |
| 7e2b38decf1f826fbb792d762d9e6a29147e9ecb44eb2ad2c4dc08e7ee01a140 |
| bea33fb3205319868784c028418411ee796d6ee3dfe9309f143e7e8106116a49 |
| 3b6f30369a4ee8bf9409d141b6d1b3fb4286c34984b5de005ed7431df549b17e |
| 78e877337902c67fb93c5fdc3b1d9710292a29b97dc98f3cc319ac3edbb760a4 |
| 7c66d2d75be43d2c17e75d37c39344a9b5d29ee5c5861f178aa7d9f34208eb48 |
| 3f0d5ddca2657044f4763ae53c4f33c8a7814ba451b60d24430a126674125624 |
| 83f457bc81514ec5e3ea123fc237811a36da6ce7f975ad56d62e34af4d1f37c0 |
| c56a97efd6d3470e14193ac9e194fa46d495e3dddc918219cca530b90f01d11e |
| b448381f244dc0072abd4f52e01ca93efaebb2c0a8ea8901c4725ecb1b2b0656 |
| ea5fac3201a09c3c5c3701723ea9a5fec8bbc4f1f236463d651303f40a245452 |
| b68bf400a23b1053f54911a2b826d341f6bf87c26bea5e6cf21710ee569a7aab |

123543c7a5523a15a933e32477b8cba4cd79a680bb69ef2dba178700bfb9ec07

3d41cd5199dbd6cefcc78d53bb44a2ecbea716de2bc8e547ead7c2aebd9925f0

d6d367453c513445313be7339666e4faeeebeae71620c187012ea5ae2901df34

9525f5081a5a7ab7d35cf2fb2d7524e0777e37fe3df62730e1e7de50506850f7

46db9f2fc879bf643a8f05e2b35879b235cbb04aa06fe548f0bc7c7c02483cf3

8e234482db790fa0a3d2bf5f7084ec4cfb74bffd5f6cbdc5abdbc1350f58e3fe

8fd5f4aa9d74375b8970844a9d6c479bc7dfa257132ee8a25d5cd404e19168c8

dda8a9e2a2e415be781a39fdf41f1551af2344f1b1a0ddf921d8aeba90343d1b

7981ebf35b5eff8be2f3849c8f3085b9cec10d9759ff4d3afd46990520de0407

5f00106f7f15e0ca00df4dbb0eeccd57930b4b81bc9aa3fca0c5af4eda339ab7

38106b043ede31a66596299f17254d3f23cbe1f983674bf9ead5006e0f0bf880

61772375af1884fe73c5d154b8637dd62f26d23bc38d18462a88e2bbed483fd7

6ca3a2f4cef27dac9d28c1ec2b29a8fa09dfc6dbbaf58e00dddbf5c1dd3b3cc3

0d6964fe763c2e6404cde68af2c5f86d34cf50a88bd81bc06bba739010821db0

ff8832355ae99ffd66d0fe9eda2d74efdf3ed87bb2a4c215b93ade93165f7c0b

e74e8cdf887ae2de25590c55cb52dad66f0135ad4a1df224155f772554ea970c

5b44a72ac38c9adeba133b516250f53d3cd13f4018cff7daf44a328ebc6c5ad0

07d206664a8d397273e69ce37ef7cf933c22e93b62d95b673d6e835876feba06

# Hostname

| Value |
| --- |
| cloud.dnx.capital |

# External References

- https://otx.alienvault.com/pulse/64a5a12895965c20e52afd15
- https://www.sentinelone.com/blog/bluenoroff-how-dprks-macos-rustbucket-seeks-to-evade-analysis-and-detection/