Jul 03 2023

NETMANAGEIT

Intelligence Report

Detecting Popular Cobalt Strike Malleable C2 Profile Techniques

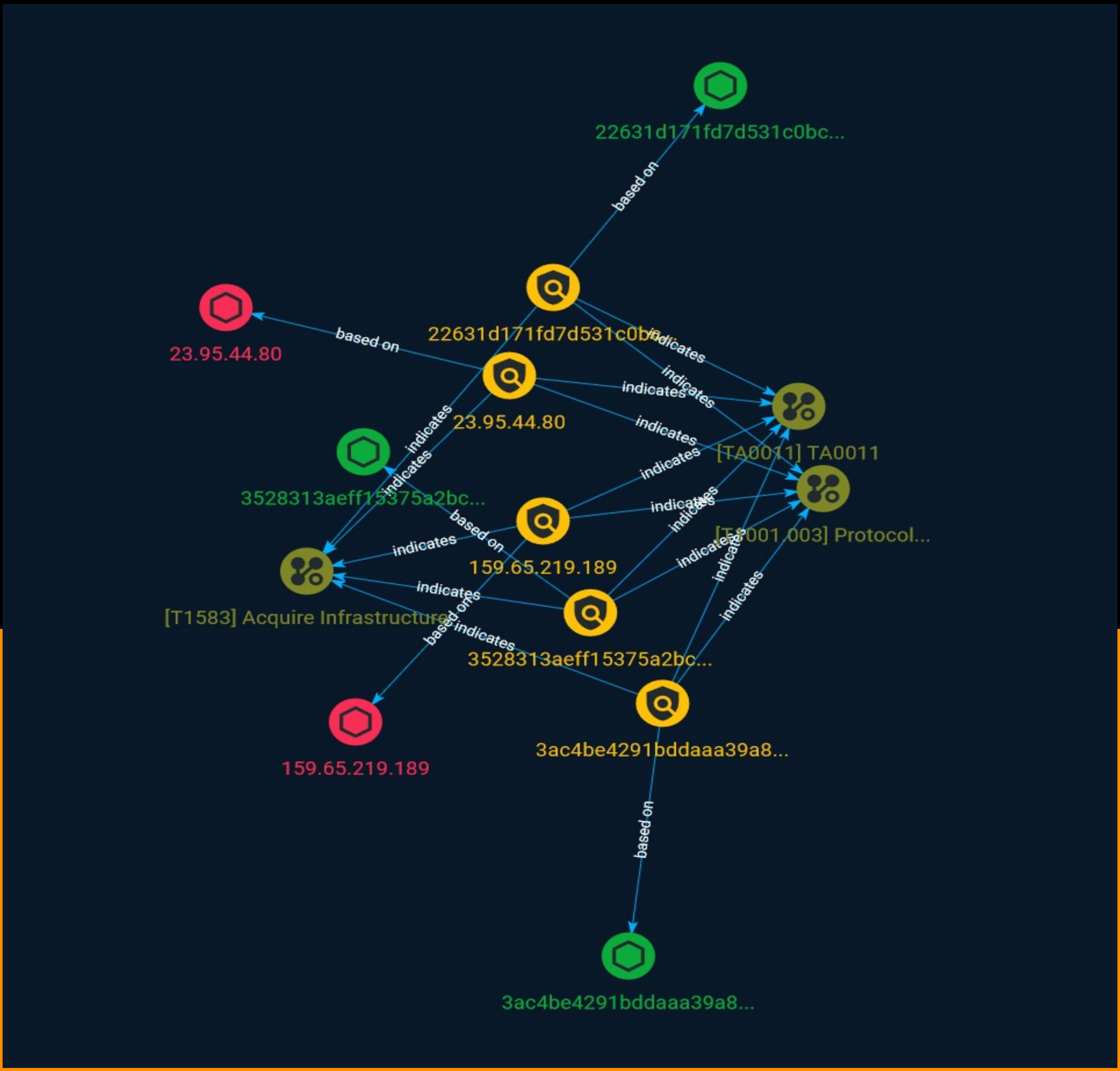

Table of contents

Overview

Entities

Observables

External References

Overview

Description

We identified Team Server instances connected to the internet that host Beacon implants and provide command-and-control (C2) functionality. We have also extracted the Malleable C2 profile configuration from the Beacon binary to help us understand the various methods used to evade conventional detections.

Confidence

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

15 / 100

Indicator

Name

23.95.44.80

Description

CC=US ASN=AS36352 AS-COLOCROSSING

Pattern Type

stix

Pattern

[ipv4-addr:value = '23.95.44.80']

Name

3528313aeff15375a2bce7b7587b188dcf1befb1e50c9db65d46e81a77a4a096

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' =
'3528313aeff15375a2bce7b7587b188dcf1befb1e50c9db65d46e81a77a4a096']

Name

22631d171fd7d531c0bc083a5335a910a95257e3194b50d8b471740d3a91fe34

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' =
'22631d171fd7d531c0bc083a5335a910a95257e3194b50d8b471740d3a91fe34']

Name

3ac4be4291bddaaa39a815cc05ece6d611cd69a1604fec8dec0f7e5451659cfa

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' =
'3ac4be4291bddaaa39a815cc05ece6d611cd69a1604fec8dec0f7e5451659cfa']

Name

159.65.219.189

Description

CC=US ASN=AS14061 DIGITALOCEAN-ASN

Pattern Type

stix

Pattern

[ipv4-addr:value = '159.65.219.189']

Attack-Pattern

Name
Protocol Impersonation
ID
T1001.003
Description
Adversaries may impersonate legitimate protocols or web service traffic to disguise command and control activity and thwart analysis efforts. By impersonating legitimate protocols or web services, adversaries can make their command and control traffic blend in with legitimate network traffic. Adversaries may impersonate a fake SSL/TLS handshake to make it look like subsequent traffic is SSL/TLS encrypted, potentially interfering with some security tooling, or to make the traffic look like it is related with a trusted entity.
Name
Acquire Infrastructure
ID
T1583
Description
Adversaries may buy, lease, or rent infrastructure that can be used during targeting. A wide variety of infrastructure exists for hosting and orchestrating adversary operations.

Infrastructure solutions include physical or cloud servers, domains, and third-party web services.(Citation: TrendmicroHideoutsLease) Additionally, botnets are available for rent or purchase. Use of these infrastructure solutions allows adversaries to stage, launch, and execute operations. Solutions may help adversary operations blend in with traffic that is seen as normal, such as contacting third-party web services or acquiring infrastructure to support [Proxy](https://attack.mitre.org/techniques/T1090).(Citation: amnesty_nso_pegasus) Depending on the implementation, adversaries may use infrastructure that makes it difficult to physically tie back to them as well as utilize infrastructure that can be rapidly provisioned, modified, and shut down.

Name
TA0011

ID
TA0011

StixFile

Value
22631d171fd7d531c0bc083a5335a910a95257e3194b50d8b471740d3a91fe34
3ac4be4291bddaaa39a815cc05ece6d611cd69a1604fec8dec0f7e5451659cfa
3528313aeff15375a2bce7b7587b188dcf1befb1e50c9db65d46e81a77a4a096

IPv4-Addr

Value
159.65.219.189
23.95.44.80

External References

- https://otx.alienvault.com/pulse/64a2dfe24c04a40592744e60
- https://unit42.paloaltonetworks.com/cobalt-strike-malleable-c2/