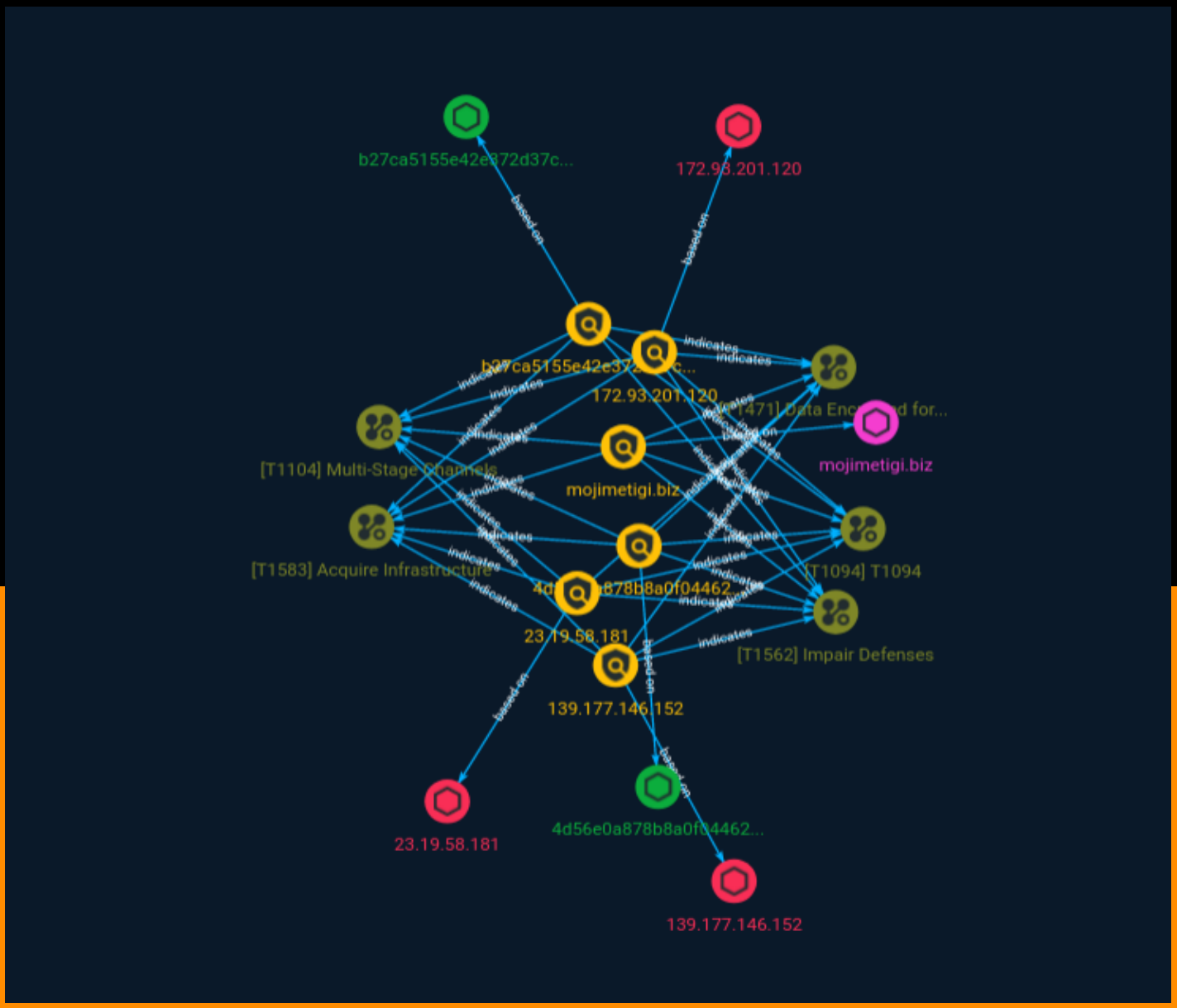
Aug 03 2023

NETMANAGEIT

# Intelligence Report

# Report: Ransomware Command-and-Control Providers Unmasked



# Table of contents

## Overview



## Entities



## Observables

# External References

# Overview

## Description

The Halcyon Research and Engineering Team has published new research that details novel techniques used to unmask yet another Ransomware Economy player that is facilitating ransomware attacks and state-sponsored APT operations: Command-and-Control Providers (C2P) who sell services to threat actors while assuming a legal business profile.

## Confidence

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

15 / 100

# Indicator

| Name |
| --- |
| 4d56e0a878b8a0f04462e7aa2a47d69a6f3a31703563025fb40fb82bab2a2f05 |
| **Pattern Type** |
| stix |
| **Pattern** |
| [file:hashes.'SHA-256' = '4d56e0a878b8a0f04462e7aa2a47d69a6f3a31703563025fb40fb82bab2a2f05'] |
| **Name** |
| 139.177.146.152 |
| **Description** |
| CC=US ASN=AS14956 -Reserved AS |
| **Pattern Type** |
| stix |
| **Pattern** |

[ipv4-addr:value = '139.177.146.152']

**Name**

b27ca5155e42e372d37cf2bcbb1f159627881ecbae2e51d41f414429599d37a7

**Pattern Type**

stix

**Pattern**

[file:hashes.'SHA-256' = 'b27ca5155e42e372d37cf2bcbb1f159627881ecbae2e51d41f414429599d37a7']

**Name**

23.19.58.181

**Description**

CC=GB ASN=AS205544 Leaseweb Uk Limited

**Pattern Type**

stix

**Pattern**

[ipv4-addr:value = '23.19.58.181']

**Name**

mojimetigi.biz

| Pattern Type |
| --- |
| stix |
| **Pattern** |
| [domain-name:value = 'mojimetigi.biz'] |
| **Name** |
| 172.93.201.120 |
| **Description** |
| CC=US ASN=AS20278 NEXEON |
| **Pattern Type** |
| stix |
| **Pattern** |
| [ipv4-addr:value = '172.93.201.120'] |

# Attack-Pattern

| Name |
| --- |
| T1094 |
| **ID** |
| T1094 |
| **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**

Data Encrypted for Impact

**ID**

T1471

**Description**

An adversary may encrypt files stored on a mobile device to prevent the user from accessing them. This may be done in order to extract monetary compensation from a victim in exchange for decryption or a decryption key (ransomware) or to render data permanently inaccessible in cases where the key is not saved or transmitted.

**Name**

Impair Defenses

**ID**

T1562

**Description**

Adversaries may maliciously modify components of a victim environment in order to hinder or disable defensive mechanisms. This not only involves impairing preventative defenses, such as firewalls and anti-virus, but also detection capabilities that defenders can use to audit activity and identify malicious behavior. This may also span both native defenses as well as supplemental capabilities installed by users and administrators. Adversaries may also impair routine operations that contribute to defensive hygiene, such as blocking users from logging out of a computer or stopping it from being shut down. These restrictions can further enable malicious operations as well as the continued propagation of incidents.(Citation: Emotet shutdown) Adversaries could also target event aggregation and analysis mechanisms, or otherwise disrupt these procedures by altering other system components.

**Name**

Multi-Stage Channels

**ID**

T1104

**Description**

Adversaries may create multiple stages for command and control that are employed under different conditions or for certain functions. Use of multiple stages may obfuscate the command and control channel to make detection more difficult. Remote access tools will call back to the first-stage command and control server for instructions. The first stage may have automated capabilities to collect basic host information, update tools, and upload additional files. A second remote access tool (RAT) could be uploaded at that point to redirect the host to the second-stage command and control server. The second stage will likely be more fully featured and allow the adversary to interact with the system through a reverse shell and additional RAT features. The different stages will likely be hosted separately with no overlapping infrastructure. The loader may also have backup first-stage callbacks or [Fallback Channels](https://attack.mitre.org/techniques/T1008) in case the original first-stage communication path is discovered and blocked.

# Domain-Name

| Value |
| --- |
| mojimetigi.biz |

# StixFile

| Value |
| --- |
| 4d56e0a878b8a0f04462e7aa2a47d69a6f3a31703563025fb40fb82bab2a2f05 |
| b27ca5155e42e372d37cf2bcbb1f159627881ecbae2e51d41f414429599d37a7 |

# IPv4-Addr

| Value |
| --- |
| 23.19.58.181 |
| 172.93.201.120 |
| 139.177.146.152 |

# External References

- https://otx.alienvault.com/pulse/64caa604c4ce91eb26b74912
- https://www.halcyon.ai/blog/report-ransomware-command-and-control-providers-unmasked-by-halcyon-researchers