Jun 11 2024

Intelligence Report

test

Example Name
123 Main Street
Miami, FL 33101 USA
888.888.8888

intelligence_reports@example.com
https://example.com

Table of contents

Overview

Entities

Observables

Overview

Description

Confidence

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

100 / 100

Content

Just typing some text so that it's easy to understand how content mapping works.

Indicator

Name
39e8679e5efec3434258e8a4988b1555803c34031be46545de1c29200a70d1dd
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = '39e8679e5efec3434258e8a4988b1555803c34031be46545de1c29200a70d1dd']

Note

Name

Name

based-on

Name

Report

Name

Infrastructure Patterns Lead to More Than 30 Active APT29 C2 Servers

Description

Russian cyber-espionage group APT29 (The Dukes, Yttrium, Cozy Bear) is actively serving malware previously used in an espionage campaign in the UK, US and Canada. They attributed the malware used in the campaign, known as WellMess and WellMail, with APT29. Test This is an update

Name

Quasar RAT's Dual DLL Sideloading Technique

Description

Given the prevalence of sideloading techniques in malware campaigns, it's vital to understand their mechanisms to defend against them effectively. The case of QuasarRAT provides an insightful example.

Name

FireEye TRITON 2019

Description

Miller, S, et al. (2019, April 10). TRITON Actor TTP Profile, Custom Attack Tools, Detections, and ATT&CK Mapping. Retrieved April 16, 2019.

Artifact

Value
33480167a4cb3f0703e4f053b8ad83f9b2291a804e1cf6d14c27ac9272fce414a7a5793ff6ecd36c808a085fdb6e9b41b630322fa61de4fd2baff06847c7143b

StixFile

Value
39e8679e5efec3434258e8a4988b1555803c34031be46545de1c29200a70d1dd

External References