Sep 21 2023

NETMANAGEIT

Intelligence Report

Cado Security Labs Researchers Witness a 600X Increase in P2Pinfect Traffic

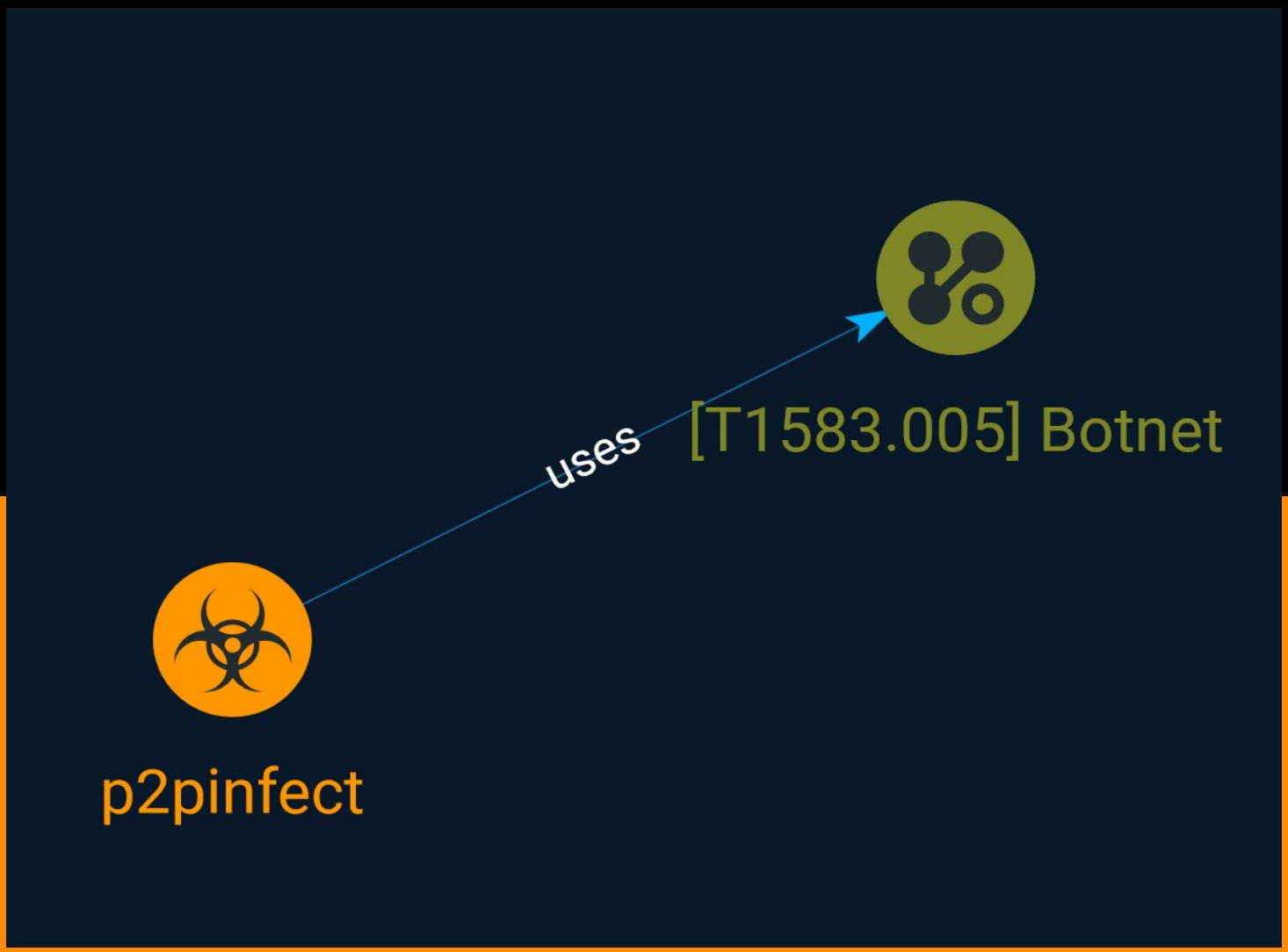

Table of contents

Overview

Entities

External References

Overview

Description

Cado Security Labs has been tracking the P2Pinfect botnet since August 2023. P2Pinfect's developers are committed to maintaining and iterating on the functionality of their malicious payloads, while simultaneously scaling the botnet across continents and cloud providers at a rapid rate. Given the current size of the botnet, its geographical spread, self-updating capability, and its rapid growth, this would be considered a lucrative asset for most threat actors.

Confidence

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

15 / 100

Attack-Pattern

Name
Botnet
ID
T1583.005
Description
Adversaries may buy, lease, or rent a network of compromised systems that can be used during targeting. A botnet is a network of compromised systems that can be instructed to perform coordinated tasks.(Citation: Norton Botnet) Adversaries may purchase a subscription to use an existing botnet from a booter/stresser service. With a botnet at their disposal, adversaries may perform follow-on activity such as large-scale [Phishing] (https://attack.mitre.org/techniques/T1566) or Distributed Denial of Service (DDoS). (Citation: Imperva DDoS for Hire)(Citation: Krebs-Anna)(Citation: Krebs-Bazaar)(Citation: Krebs-Booter)

Malware

Name
p2pinfect

External References

- https://otx.alienvault.com/pulse/650afe46e917ac8a71adc2f2
- https://www.cadosecurity.com/cado-security-labs-researchers-witness-a-600x-increase-in-p2pinfect-traffic/