Nov 03 2023

NETMANAGEIT

Intelligence Report

Analysis of activities of suspected APT-C-36 (Blind Eagle) organization launching Amadey botnet Trojan

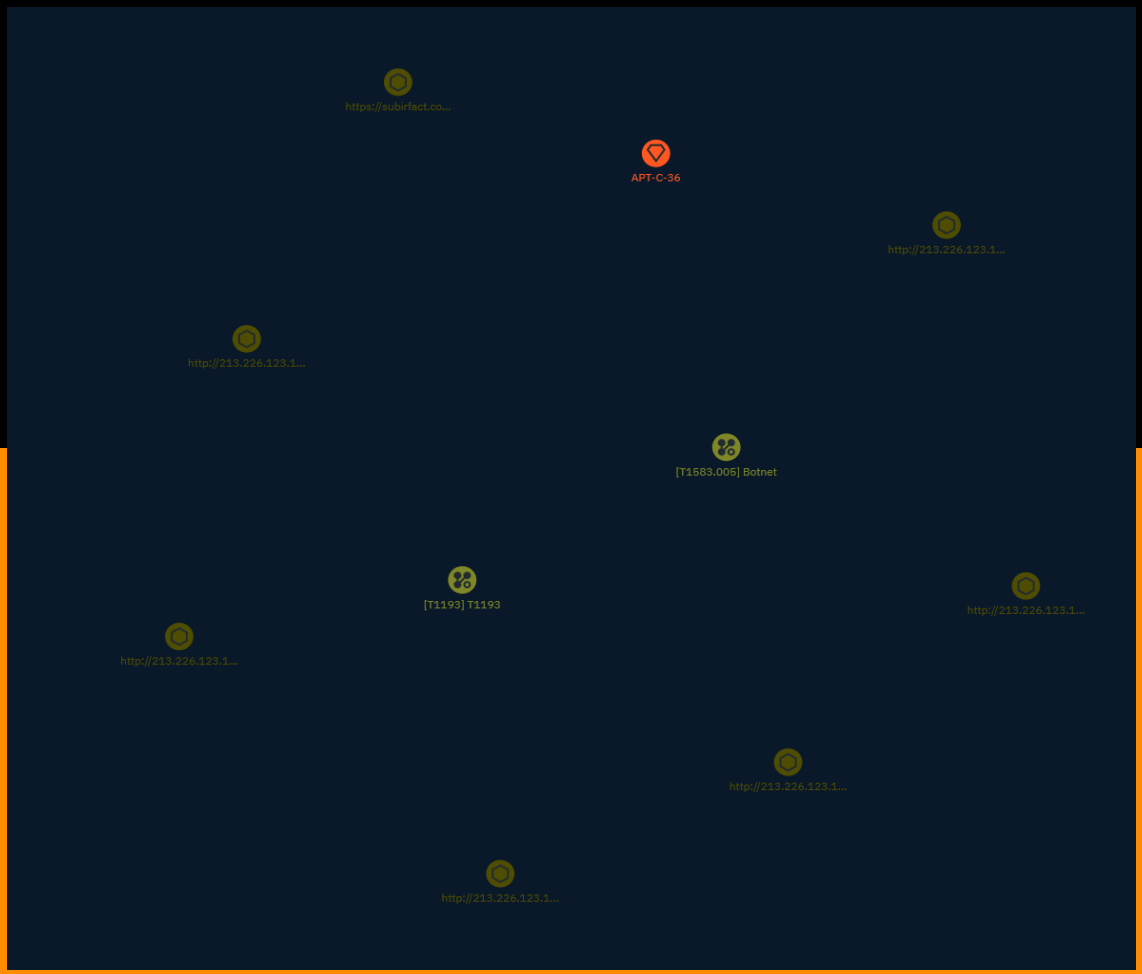

Table of contents

Overview

Entities

Observables

External References

Overview

Description

In daily hunting activities, Weixin discovered that the APT-C-36 organization recently attempted to add the Amadey botnet Trojan to its usual PDF spear phishing attack flow. The Amadey botnet Trojan is a modular botnet Trojan that appeared for sale on Russian hacker forums around October 2018. It has the capabilities of intranet traversal, information theft, remote command execution, script execution, and DDos attacks.

Confidence

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

15 / 100

Content

N/A

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)
Name
T1193
ID
T1193

Intrusion-Set

Name
APT-C-36

Description
[APT-C-36](https://attack.mitre.org/groups/G0099) is a suspected South America espionage group that has been active since at least 2018. The group mainly targets Colombian government institutions as well as important corporations in the financial sector, petroleum industry, and professional manufacturing.(Citation: QiAnXin APT-C-36 Feb2019)

Url

Value
http://213.226.123.14/8bmeVwqx/index.php?scr=1
http://213.226.123.14/8bmeVwqx/Plugins/cred.dll
http://213.226.123.14/8bmeVwqx/Plugins/clip64.dll
http://213.226.123.14/8bmeVwqx/Plugins/cred64.dll
https://subirfact.com/onLyofFicED.bat
http://213.226.123.14/8bmeVwqx/index.php
http://213.226.123.14/8bmeVwqx/Plugins/clip.dll

External References

- https://otx.alienvault.com/pulse/6544c4c1db5b0874008a4f12
- https://mp.weixin.qq.com/s/-7U1-NTP0EdVOtptzbHUsg