Jan 12 2024

NETMANAGEIT

Intelligence Report

Exploring FBot | Python-Based Malware Targeting Cloud and Payment Services

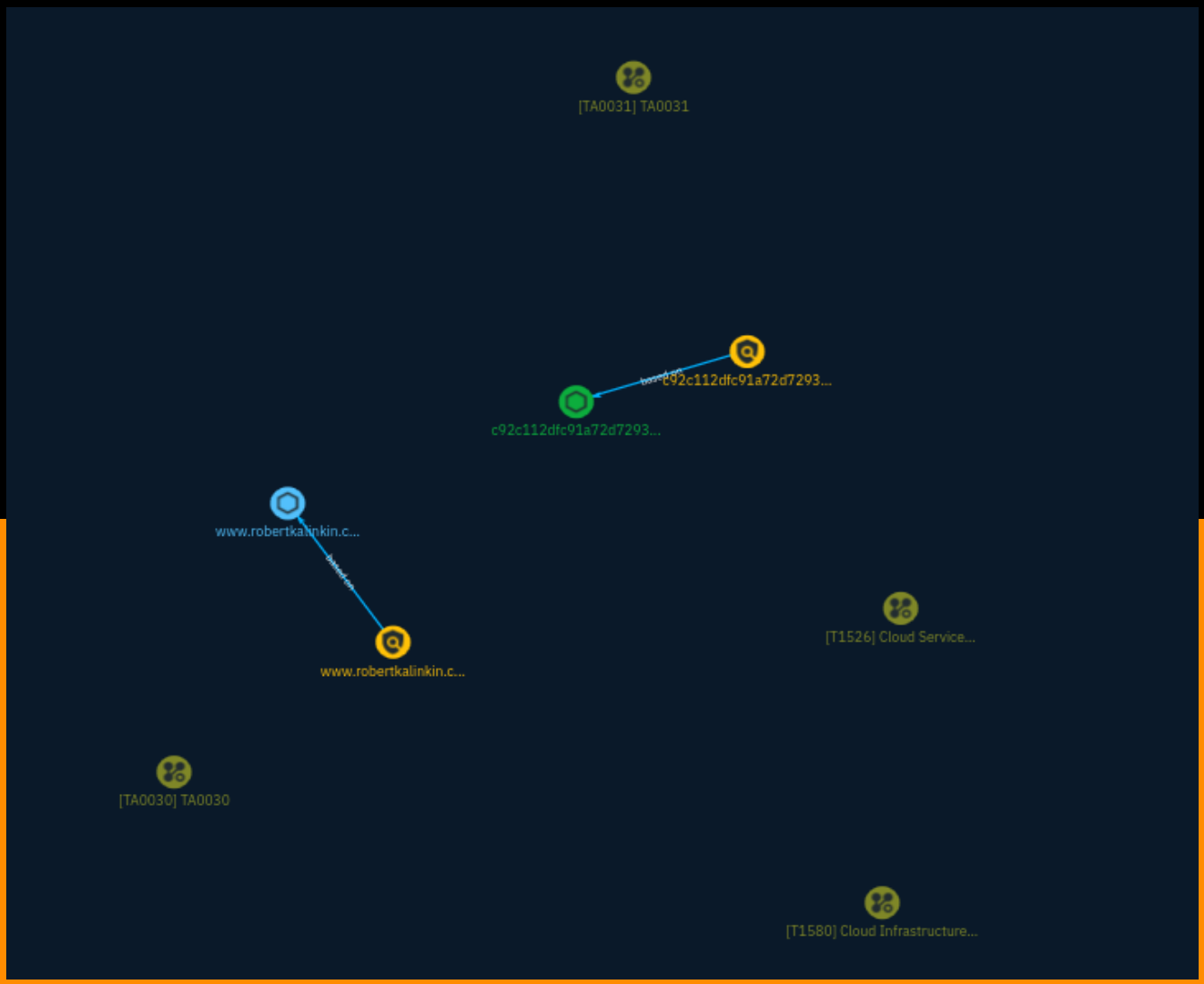

Table of contents

Overview

Entities

Observables

External References

Overview

Description

FBot is a Python-based hacking tool distinct from other cloud malware families, targeting web servers, cloud services, and SaaS platforms like AWS, Office365, PayPal, Sendgrid, and Twilio. FBot does not utilize the widely-used Androxgh0st code but shares similarities with the Legion cloud infostealer in functionality and design.Key features include credential harvesting for spamming attacks, AWS account hijacking tools, and functions to enable attacks against PayPal and various SaaS accounts.FBot is characterized by a smaller footprint compared to similar tools, indicating possible private development and a more targeted distribution approach.

Confidence

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

15 / 100

Content

N/A

Attack-Pattern

Name
Cloud Service Discovery
ID
T1526
Description
An adversary may attempt to enumerate the cloud services running on a system after gaining access. These methods can differ from platform-as-a-service (PaaS), to infrastructure-as-a-service (IaaS), or software-as-a-service (SaaS). Many services exist throughout the various cloud providers and can include Continuous Integration and Continuous Delivery (CI/CD), Lambda Functions, Azure AD, etc. They may also include security services, such as AWS GuardDuty and Microsoft Defender for Cloud, and logging services, such as AWS CloudTrail and Google Cloud Audit Logs. Adversaries may attempt to discover information about the services enabled throughout the environment. Azure tools and APIs, such as the Azure AD Graph API and Azure Resource Manager API, can enumerate resources and services, including applications, management groups, resources and policy definitions, and their relationships that are accessible by an identity.(Citation: Azure - Resource Manager API)(Citation: Azure AD Graph API) For example, Stormspotter is an open source tool for enumerating and constructing a graph for Azure resources and services, and Pacu is an open source AWS exploitation framework that supports several methods for discovering cloud services.(Citation: Azure - Stormspotter)(Citation: GitHub Pacu) Adversaries may use the information gained to shape follow-on behaviors, such as targeting data or credentials from enumerated services or evading identified defenses through [Disable or Modify Tools](https://attack.mitre.org/techniques/T1562/001) or [Disable or Modify Cloud Logs](https://attack.mitre.org/techniques/T1562/008).

Name
TA0030
ID
TA0030
Name
TA0031
ID
TA0031
Name
Cloud Infrastructure Discovery
ID
T1580
Description
An adversary may attempt to discover infrastructure and resources that are available within an infrastructure-as-a-service (IaaS) environment. This includes compute service resources such as instances, virtual machines, and snapshots as well as resources of other services including the storage and database services. Cloud providers offer methods such as APIs and commands issued through CLIs to serve information about infrastructure. For example, AWS provides a `DescribeInstances` API within the Amazon EC2 API that can return information about one or more instances within an account, the `ListBuckets` API that returns a list of all buckets owned by the authenticated sender of the request, the `HeadBucket` API to determine a bucket's existence along with access permissions of the request sender, or the `GetPublicAccessBlock` API to retrieve access block configuration for a bucket.(Citation: Amazon Describe Instance)(Citation: Amazon Describe Instances API)

(Citation: AWS Get Public Access Block)(Citation: AWS Head Bucket) Similarly, GCP's Cloud SDK CLI provides the `gcloud compute instances list` command to list all Google Compute Engine instances in a project (Citation: Google Compute Instances), and Azure's CLI command `az vm list` lists details of virtual machines.(Citation: Microsoft AZ CLI) In addition to API commands, adversaries can utilize open source tools to discover cloud storage infrastructure through [Wordlist Scanning](https://attack.mitre.org/techniques/T1595/003).(Citation: Malwarebytes OSINT Leaky Buckets - Hioureas) An adversary may enumerate resources using a compromised user's access keys to determine which are available to that user.(Citation: Expel IO Evil in AWS) The discovery of these available resources may help adversaries determine their next steps in the Cloud environment, such as establishing Persistence.(Citation: Mandiant M-Trends 2020)An adversary may also use this information to change the configuration to make the bucket publicly accessible, allowing data to be accessed without authentication. Adversaries have also may use infrastructure discovery APIs such as `DescribeDBInstances` to determine size, owner, permissions, and network ACLs of database resources. (Citation: AWS Describe DB Instances) Adversaries can use this information to determine the potential value of databases and discover the requirements to access them. Unlike in [Cloud Service Discovery](https://attack.mitre.org/techniques/T1526), this technique focuses on the discovery of components of the provided services rather than the services themselves.

Indicator

Name
c92c112dfc91a72d7293772b741c2eab3bc42ee539ed5881f2edcc3e5cb669f3
Description
SHA256 of 2becd32162b2b0cb1afc541e33ace3a29dad96f1
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = 'c92c112dfc91a72d7293772b741c2eab3bc42ee539ed5881f2edcc3e5cb669f3']
Name
www.robertkalinkin.com
Pattern Type
stix
Pattern

```
[hostname:value = 'www.robertkalinkin.com']
```

StixFile

Value
c92c112dfc91a72d7293772b741c2eab3bc42ee539ed5881f2edcc3e5cb669f3

Hostname

Value
www.robertkalinkin.com

External References

- https://otx.alienvault.com/pulse/65a0778b1b5ad66b6a11bf50
- https://www.sentinelone.com/labs/exploring-fbot-python-based-malware-targeting-cloud-and-payment-services/