Mar 29 2024

NETMANAGEIT

Intelligence Report

Out of the shadows - ’darcula’ iMessage and RCS smishing attacks target USPS and global postal services

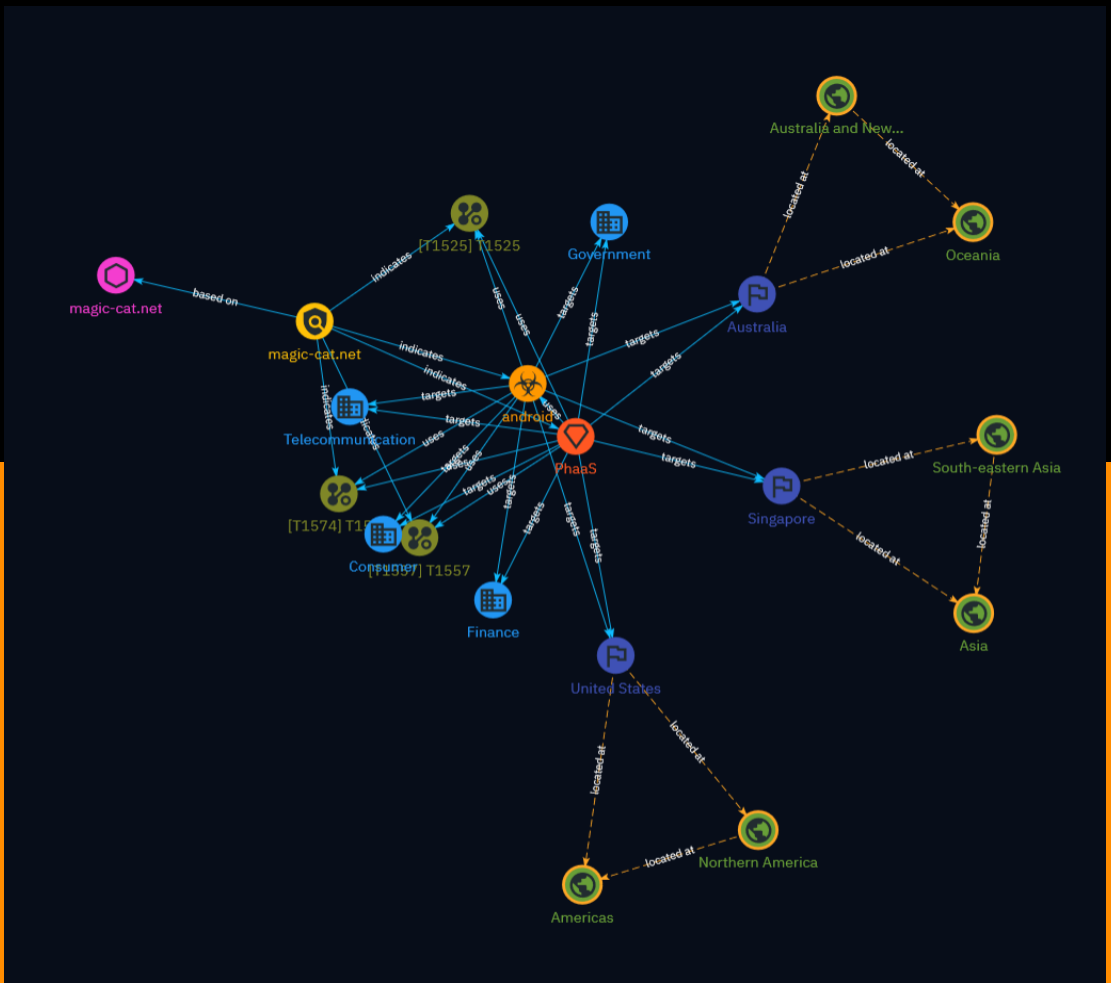

Table of contents

Overview

Entities

Observables

External References

Overview

Description

Confidence

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

100 / 100

Content

N/A

Indicator

Name
magic-cat.net
Pattern Type
stix
Pattern
[domain-name:value = 'magic-cat.net']

Intrusion-Set

Name
PhaaS

Sector

Name
Consumer
Name
Telecommunication
Description
Private and public entities involved in the production, transport and dissemination of information and communication signals.
Name
Government
Description
Civilian government institutions and administrations of the executive and legislative branches. The diplomatic and judicial branches are not included.
Name
Finance
Description

Public and private entities involved in the allocation of assets and liabilities over space and time.

Malware

Name
android

Attack-Pattern

Name
T1574
ID
T1574
Description
Adversaries may execute their own malicious payloads by hijacking the way operating systems run programs. Hijacking execution flow can be for the purposes of persistence, since this hijacked execution may reoccur over time. Adversaries may also use these mechanisms to elevate privileges or evade defenses, such as application control or other restrictions on execution. There are many ways an adversary may hijack the flow of execution, including by manipulating how the operating system locates programs to be executed. How the operating system locates libraries to be used by a program can also be intercepted. Locations where the operating system looks for programs/resources, such as file directories and in the case of Windows the Registry, could also be poisoned to include malicious payloads.
Name
T1525
ID
T1525

Description

Adversaries may implant cloud or container images with malicious code to establish persistence after gaining access to an environment. Amazon Web Services (AWS) Amazon Machine Images (AMIs), Google Cloud Platform (GCP) Images, and Azure Images as well as popular container runtimes such as Docker can be implanted or backdoored. Unlike [Upload Malware](https://attack.mitre.org/techniques/T1608/001), this technique focuses on adversaries implanting an image in a registry within a victim's environment. Depending on how the infrastructure is provisioned, this could provide persistent access if the infrastructure provisioning tool is instructed to always use the latest image.(Citation: Rhino Labs Cloud Image Backdoor Technique Sept 2019) A tool has been developed to facilitate planting backdoors in cloud container images.(Citation: Rhino Labs Cloud Backdoor September 2019) If an adversary has access to a compromised AWS instance, and permissions to list the available container images, they may implant a backdoor such as a [Web Shell](https://attack.mitre.org/techniques/T1505/003).(Citation: Rhino Labs Cloud Image Backdoor Technique Sept 2019)

Name

T1557

ID

T1557

Description

Adversaries may attempt to position themselves between two or more networked devices using an adversary-in-the-middle (AiTM) technique to support follow-on behaviors such as [Network Sniffing](https://attack.mitre.org/techniques/T1040), [Transmitted Data Manipulation](https://attack.mitre.org/techniques/T1565/002), or replay attacks ([Exploitation for Credential Access](https://attack.mitre.org/techniques/T1212)). By abusing features of common networking protocols that can determine the flow of network traffic (e.g. ARP, DNS, LLMNR, etc.), adversaries may force a device to communicate through an adversary controlled system so they can collect information or perform additional actions.(Citation: Rapid7 MiTM Basics) For example, adversaries may manipulate victim DNS settings to enable other malicious activities such as preventing/redirecting users from accessing legitimate sites and/or pushing additional malware.(Citation: ttint_rat)(Citation: dns_changer_trojans)(Citation: ad_blocker_with_miner) Adversaries may also manipulate DNS and leverage their position in order to intercept user credentials and session cookies.

(Citation: volexity_0day_sophos_FW) [Downgrade Attack](https://attack.mitre.org/techniques/T1562/010)s can also be used to establish an AiTM position, such as by negotiating a less secure, deprecated, or weaker version of communication protocol (SSL/TLS) or encryption algorithm.(Citation: mitm_tls_downgrade_att)(Citation: taxonomy_downgrade_att_tls)(Citation: tlseminar_downgrade_att) Adversaries may also leverage the AiTM position to attempt to monitor and/or modify traffic, such as in [Transmitted Data Manipulation](https://attack.mitre.org/techniques/T1565/002). Adversaries can setup a position similar to AiTM to prevent traffic from flowing to the appropriate destination, potentially to [Impair Defenses](https://attack.mitre.org/techniques/T1562) and/or in support of a [Network Denial of Service](https://attack.mitre.org/techniques/T1498).

Country

Name
Australia
Name
Singapore
Name
United States

Region

Name
Australia and New Zealand
Name
Oceania
Name
South-eastern Asia
Name
Asia
Name
Northern America
Name
Americas

Domain-Name

Value
magic-cat.net

External References

- https://www.netcraft.com/blog/darcula-smishing-attacks-target-usps-and-global-postal-services/
- https://otx.alienvault.com/pulse/6606bc441ee0ee30e8cdf771