Dec 22 2023

NETMANAGEIT

Intelligence Report

Android Banking Trojan Chameleon can now bypass any Biometric Authentication

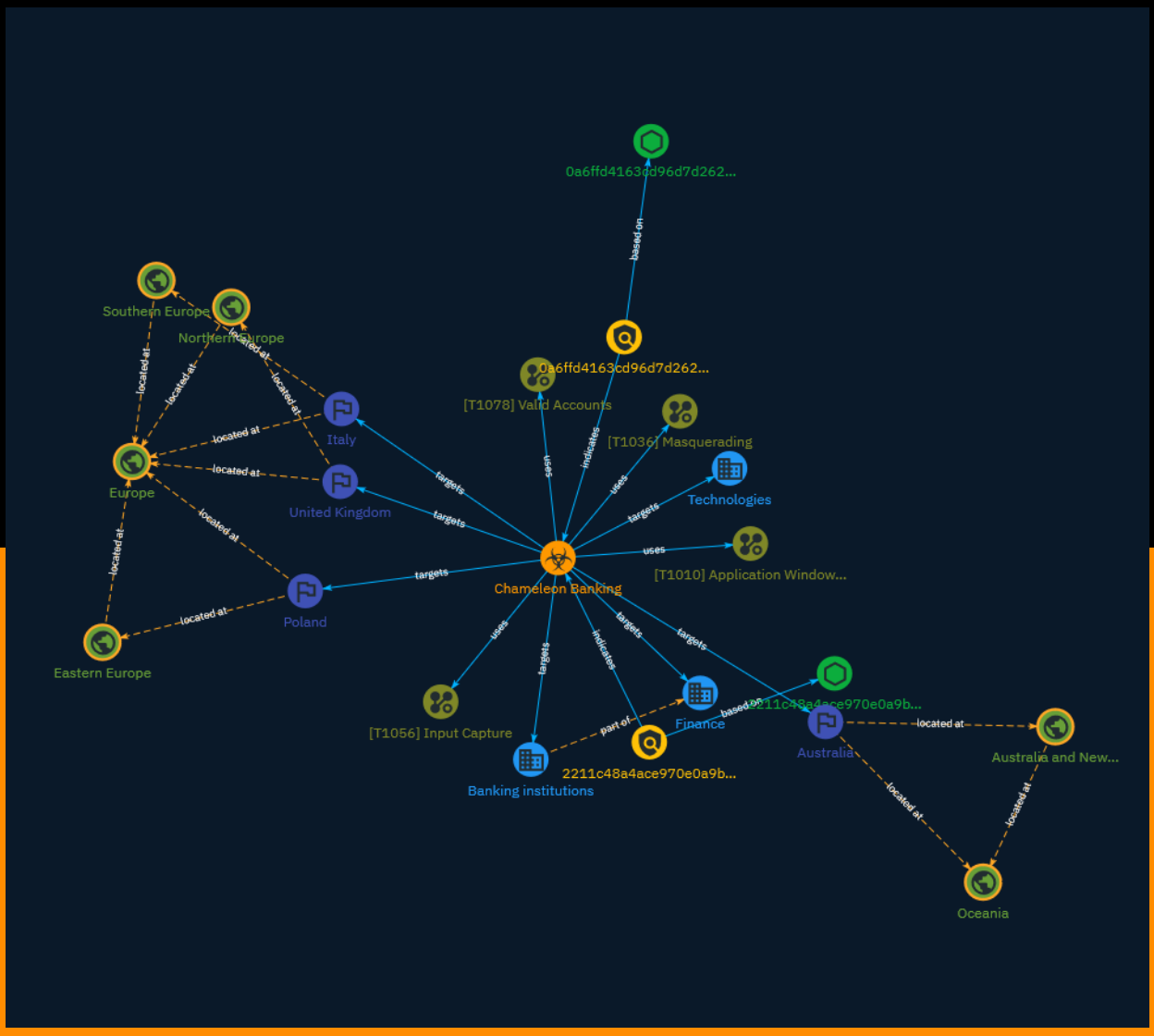

Table of contents

Overview

Entities

Observables

External References

Overview

Description

A refined iteration of the Chameleon banking trojan has emerged, and has expanded its target region to the UK and Italy, according to research conducted by ThreatFabric in December 2023.

Confidence

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

15 / 100

Content

N/A

Attack-Pattern

Name
Valid Accounts
ID
T1078
Description
Adversaries may obtain and abuse credentials of existing accounts as a means of gaining Initial Access, Persistence, Privilege Escalation, or Defense Evasion. Compromised credentials may be used to bypass access controls placed on various resources on systems within the network and may even be used for persistent access to remote systems and externally available services, such as VPNs, Outlook Web Access, network devices, and remote desktop.(Citation: volexity_0day_sophos_FW) Compromised credentials may also grant an adversary increased privilege to specific systems or access to restricted areas of the network. Adversaries may choose not to use malware or tools in conjunction with the legitimate access those credentials provide to make it harder to detect their presence. In some cases, adversaries may abuse inactive accounts: for example, those belonging to individuals who are no longer part of an organization. Using these accounts may allow the adversary to evade detection, as the original account user will not be present to identify any anomalous activity taking place on their account.(Citation: CISA MFA PrintNightmare) The overlap of permissions for local, domain, and cloud accounts across a network of systems is of concern because the adversary may be able to pivot across accounts and systems to reach a high level of access (i.e., domain or enterprise administrator) to bypass access controls set within the enterprise.(Citation: TechNet Credential Theft)
Name

Input Capture

ID

T1056

Description

Adversaries may use methods of capturing user input to obtain credentials or collect information. During normal system usage, users often provide credentials to various different locations, such as login pages/portals or system dialog boxes. Input capture mechanisms may be transparent to the user (e.g. [Credential API Hooking](https://attack.mitre.org/techniques/T1056/004)) or rely on deceiving the user into providing input into what they believe to be a genuine service (e.g. [Web Portal Capture](https://attack.mitre.org/techniques/T1056/003)).

Name

Masquerading

ID

T1036

Description

Adversaries may attempt to manipulate features of their artifacts to make them appear legitimate or benign to users and/or security tools. Masquerading occurs when the name or location of an object, legitimate or malicious, is manipulated or abused for the sake of evading defenses and observation. This may include manipulating file metadata, tricking users into misidentifying the file type, and giving legitimate task or service names. Renaming abusable system utilities to evade security monitoring is also a form of [Masquerading](https://attack.mitre.org/techniques/T1036).(Citation: LOLBAS Main Site) Masquerading may also include the use of [Proxy](https://attack.mitre.org/techniques/T1090) or VPNs to disguise IP addresses, which can allow adversaries to blend in with normal network traffic and bypass conditional access policies or anti-abuse protections.

Name

Application Window Discovery

ID

T1010

Description

Adversaries may attempt to get a listing of open application windows. Window listings could convey information about how the system is used.(Citation: Prevailion DarkWatchman 2021) For example, information about application windows could be used identify potential data to collect as well as identifying security tooling ([Security Software Discovery](https://attack.mitre.org/techniques/T1518/001)) to evade.(Citation: ESET Grandoreiro April 2020) Adversaries typically abuse system features for this type of enumeration. For example, they may gather information through native system features such as [Command and Scripting Interpreter](https://attack.mitre.org/techniques/T1059) commands and [Native API](https://attack.mitre.org/techniques/T1106) functions.

Sector

Name
Finance
Description
Public and private entities involved in the allocation of assets and liabilities over space and time.
Name
Banking institutions
Description
Credit institutions whose business consists in receiving repayable funds from the public and granting credit. As the bank of banks, central banks are included in this scope.
Name
Technologies
Description
Private entities related to the research, development, manufacturing and distribution of electronics, softwares, computers and products related to information technologies.

Indicator

Name
2211c48a4ace970e0a9b3da75ac246bd9abaaaf4f0806ec32401589856ea2434
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = '2211c48a4ace970e0a9b3da75ac246bd9abaaaf4f0806ec32401589856ea2434']
Name
0a6ffd4163cd96d7d262be5ae7fa5cfc3affbea822d122c0803379d78431e5f6
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = '0a6ffd4163cd96d7d262be5ae7fa5cfc3affbea822d122c0803379d78431e5f6']

Country

Name
Poland
Name
Australia
Name
United Kingdom
Name
Italy

Region

Name
Europe
Name
Northern Europe
Name
Southern Europe
Name
Oceania
Name
Australia and New Zealand
Name
Eastern Europe

Malware

Name
Chameleon Banking

StixFile

Value
0a6ffd4163cd96d7d262be5ae7fa5cfc3affbea822d122c0803379d78431e5f6
2211c48a4ace970e0a9b3da75ac246bd9abaaaf4f0806ec32401589856ea2434

External References

- https://otx.alienvault.com/pulse/6585a108d98cf0b320927060
- https://www.threatfabric.com/blogs/android-banking-trojan-chameleon-is-back-in-action