Feb 03 2024

NETMANAGEIT

Intelligence Report

VajraSpy: A Patchwork of espionage apps

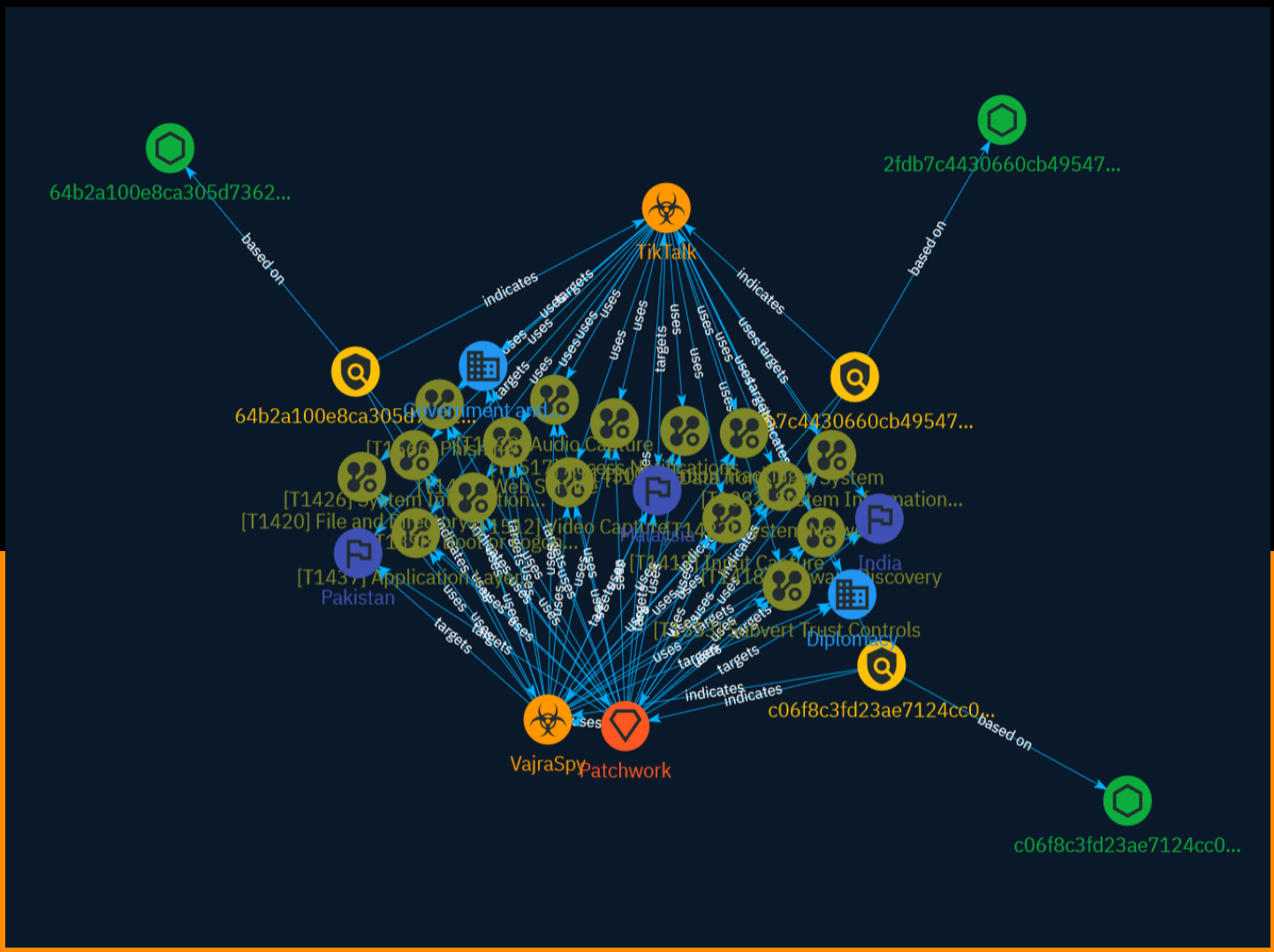

Table of contents

Overview

Entities

Observables

External References

Overview

Description

ESET researchers have identified 12 Android espionage apps that were available on Google Play between 2021 and 2023 and are still available in the wild, but not on alternative app stores, as previously thought.

Confidence

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

15 / 100

Content

N/A

Indicator

Name

c06f8c3fd23ae7124cc06eb63c0411418715bf99d3c9fa66525790b2b4c61858

Description

SHA256 of baf6583c54fc680aa6f71f3b694e71657a7a99d0

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'c06f8c3fd23ae7124cc06eb63c0411418715bf99d3c9fa66525790b2b4c61858']

Name

64b2a100e8ca305d7362eeb4858694156d676989b8c6d6d8d01cdebe84dafc7b

Description

SHA256 of e0d73c035966c02df7bce66e6ce24e016607e62e

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '64b2a100e8ca305d7362eeb4858694156d676989b8c6d6d8d01cdebe84dafc7b']

Name

2fdb7c4430660cb49547ac2828a631810d4e3d245a6501ce00825faa169cb7d0

Description

SHA256 of 3b27a62d77c5b82e7e6902632da3a3e5ef98e743

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '2fdb7c4430660cb49547ac2828a631810d4e3d245a6501ce00825faa169cb7d0']

Name

c06f8c3fd23ae7124cc06eb63c0411418715bf99d3c9fa66525790b2b4c61858

Description

SHA256 of baf6583c54fc680aa6f71f3b694e71657a7a99d0

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'c06f8c3fd23ae7124cc06eb63c0411418715bf99d3c9fa66525790b2b4c61858']

Name

64b2a100e8ca305d7362eeb4858694156d676989b8c6d6d8d01cdebe84dafc7b

Description

SHA256 of e0d73c035966c02df7bce66e6ce24e016607e62e

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '64b2a100e8ca305d7362eeb4858694156d676989b8c6d6d8d01cdebe84dafc7b']

Name

2fdb7c4430660cb49547ac2828a631810d4e3d245a6501ce00825faa169cb7d0

Description

SHA256 of 3b27a62d77c5b82e7e6902632da3a3e5ef98e743

Pattern Type

stix

Pattern

```
[file:hashes.'SHA-256' =
'2fdb7c4430660cb49547ac2828a631810d4e3d245a6501ce00825faa169cb7d0']
```

Malware

Name
VajraSpy

Name
TikTalk

Name
VajraSpy

Name
TikTalk

Attack-Pattern

Name
Video Capture
ID
T1512
Description
An adversary can leverage a device's cameras to gather information by capturing video recordings. Images may also be captured, potentially in specified intervals, in lieu of video files. Malware or scripts may interact with the device cameras through an available API provided by the operating system. Video or image files may be written to disk and exfiltrated later. This technique differs from [Screen Capture](https://attack.mitre.org/techniques/T1513) due to use of the device's cameras for video recording rather than capturing the victim's screen. In Android, an application must hold the `android.permission.CAMERA` permission to access the cameras. In iOS, applications must include the `NSCameraUsageDescription` key in the `Info.plist` file. In both cases, the user must grant permission to the requesting application to use the camera. If the device has been rooted or jailbroken, an adversary may be able to access the camera without knowledge of the user.
Name
Web Service
ID

T1481

Description

Adversaries may use an existing, legitimate external Web service as a means for relaying data to/from a compromised system. Popular websites and social media, acting as a mechanism for C2, may give a significant amount of cover. This is due to the likelihood that hosts within a network are already communicating with them prior to a compromise. Using common services, such as those offered by Google or Twitter, makes it easier for adversaries to hide in expected noise. Web service providers commonly use SSL/TLS encryption, giving adversaries an added level of protection. Use of Web services may also protect back-end C2 infrastructure from discovery through malware binary analysis, or enable operational resiliency (since this infrastructure may be dynamically changed).

Name

Input Capture

ID

T1417

Description

Adversaries may use methods of capturing user input to obtain credentials or collect information. During normal device usage, users often provide credentials to various locations, such as login pages/portals or system dialog boxes. Input capture mechanisms may be transparent to the user (e.g. [Keylogging](https://attack.mitre.org/techniques/T1417/001)) or rely on deceiving the user into providing input into what they believe to be a genuine application prompt (e.g. [GUI Input Capture](https://attack.mitre.org/techniques/T1417/002)).

Name

Application Layer Protocol

ID

T1437

Description

Adversaries may communicate using application layer protocols to avoid detection/network filtering by blending in with existing traffic. Commands to the mobile device, and often the results of those commands, will be embedded within the protocol traffic between the mobile device and server. Adversaries may utilize many different protocols, including those used for web browsing, transferring files, electronic mail, or DNS.

Name

Access Notifications

ID

T1517

Description

Adversaries may collect data within notifications sent by the operating system or other applications. Notifications may contain sensitive data such as one-time authentication codes sent over SMS, email, or other mediums. In the case of Credential Access, adversaries may attempt to intercept one-time code sent to the device. Adversaries can also dismiss notifications to prevent the user from noticing that the notification has arrived and can trigger action buttons contained within notifications.(Citation: ESET 2FA Bypass)

Name

Software Discovery

ID

T1418

Description

Adversaries may attempt to get a listing of applications that are installed on a device. Adversaries may use the information from [Software Discovery](https://attack.mitre.org/techniques/T1418) during automated discovery to shape follow-on behaviors, including whether or not to fully infect the target and/or attempts specific actions. Adversaries may attempt to enumerate applications for a variety of reasons, such as figuring out what security measures are present or to identify the presence of target applications.

Name

System Information Discovery

ID

T1426

Description

Adversaries may attempt to get detailed information about a device's operating system and hardware, including versions, patches, and architecture. Adversaries may use the information from [System Information Discovery](https://attack.mitre.org/techniques/T1426) during automated discovery to shape follow-on behaviors, including whether or not to fully infects the target and/or attempts specific actions. On Android, much of this information is programmatically accessible to applications through the `android.os.Build` class. (Citation: Android-Build) iOS is much more restrictive with what information is visible to applications. Typically, applications will only be able to query the device model and which version of iOS it is running.

Name

Data from Local System

ID

T1533

Description

Adversaries may search local system sources, such as file systems or local databases, to find files of interest and sensitive data prior to exfiltration. Access to local system data, which includes information stored by the operating system, often requires escalated privileges. Examples of local system data include authentication tokens, the device keyboard cache, Wi-Fi passwords, and photos. On Android, adversaries may also attempt to access files from external storage which may require additional storage-related permissions.

Name

Boot or Logon Initialization Scripts

ID

T1398

Description

Adversaries may use scripts automatically executed at boot or logon initialization to establish persistence. Initialization scripts are part of the underlying operating system and are not accessible to the user unless the device has been rooted or jailbroken.

Name

Audio Capture

ID

T1429

Description

Adversaries may capture audio to collect information by leveraging standard operating system APIs of a mobile device. Examples of audio information adversaries may target include user conversations, surroundings, phone calls, or other sensitive information.

Android and iOS, by default, require that applications request device microphone access from the user. On Android devices, applications must hold the `RECORD_AUDIO` permission to access the microphone or the `CAPTURE_AUDIO_OUTPUT` permission to access audio output. Because Android does not allow third-party applications to hold the `CAPTURE_AUDIO_OUTPUT` permission by default, only privileged applications, such as those distributed by Google or the device vendor, can access audio output.(Citation: Android Permissions) However, adversaries may be able to gain this access after successfully elevating their privileges. With the `CAPTURE_AUDIO_OUTPUT` permission, adversaries may pass the `MediaRecorder.AudioSource.VOICE_CALL` constant to `MediaRecorder.setAudioOutput`, allowing capture of both voice call uplink and downlink. (Citation: Manifest.permission) On iOS devices, applications must include the `NSMicrophoneUsageDescription` key in their `Info.plist` file to access the microphone. (Citation: Requesting Auth-Media Capture)

Name

System Network Configuration Discovery

ID

T1422

Description

Adversaries may look for details about the network configuration and settings, such as IP and/or MAC addresses, of operating systems they access or through information discovery of remote systems. On Android, details of onboard network interfaces are accessible to apps through the `java.net.NetworkInterface` class.(Citation: NetworkInterface) Previously, the Android `TelephonyManager` class could be used to gather telephony-related device identifiers, information such as the IMSI, IMEI, and phone number. However, starting with Android 10, only preloaded, carrier, the default SMS, or device and profile owner applications can access the telephony-related device identifiers.(Citation: TelephonyManager) On iOS, gathering network configuration information is not possible without root access. Adversaries may use the information from [System Network Configuration Discovery](https://attack.mitre.org/techniques/T1422) during automated discovery to shape follow-on behaviors, including determining certain access within the target network and what actions to do next.

Name

File and Directory Discovery

ID

T1420

Description

Adversaries may enumerate files and directories or search in specific device locations for desired information within a filesystem. Adversaries may use the information from [File and Directory Discovery](https://attack.mitre.org/techniques/T1420) during automated discovery to shape follow-on behaviors, including deciding if the adversary should fully infect the target and/or attempt specific actions. On Android, Linux file permissions and SELinux policies typically stringently restrict what can be accessed by apps without taking advantage of a privilege escalation exploit. The contents of the external storage directory are generally visible, which could present concerns if sensitive data is inappropriately stored there. iOS's security architecture generally restricts the ability to perform any type of [File and Directory Discovery](https://attack.mitre.org/techniques/T1420) without use of escalated privileges.

Name

Location Tracking

ID

T1430

Description

Adversaries may track a device’s physical location through use of standard operating system APIs via malicious or exploited applications on the compromised device. On Android, applications holding the `ACCESS_COAURSE_LOCATION` or `ACCESS_FINE_LOCATION` permissions provide access to the device’s physical location. On Android 10 and up, declaration of the `ACCESS_BACKGROUND_LOCATION` permission in an application’s manifest will allow applications to request location access even when the application is running in the background.(Citation: Android Request Location Permissions) Some adversaries have utilized integration of Baidu map services to retrieve geographical

location once the location access permissions had been obtained.(Citation: PaloAlto-SpyDealer)(Citation: Palo Alto HenBox) On iOS, applications must include the `NSLocationWhenInUseUsageDescription`, `NSLocationAlwaysAndWhenInUseUsageDescription`, and/or `NSLocationAlwaysUsageDescription` keys in their `Info.plist` file depending on the extent of requested access to location information.(Citation: Apple Requesting Authorization for Location Services) On iOS 8.0 and up, applications call `requestWhenInUseAuthorization()` to request access to location information when the application is in use or `requestAlwaysAuthorization()` to request access to location information regardless of whether the application is in use. With elevated privileges, an adversary may be able to access location data without explicit user consent with the `com.apple.locationd.preauthorized` entitlement key.(Citation: Google Project Zero Insomnia)

Name

Subvert Trust Controls

ID

T1553

Description

Adversaries may undermine security controls that will either warn users of untrusted activity or prevent execution of untrusted programs. Operating systems and security products may contain mechanisms to identify programs or websites as possessing some level of trust. Examples of such features would include a program being allowed to run because it is signed by a valid code signing certificate, a program prompting the user with a warning because it has an attribute set from being downloaded from the Internet, or getting an indication that you are about to connect to an untrusted site. Adversaries may attempt to subvert these trust mechanisms. The method adversaries use will depend on the specific mechanism they seek to subvert. Adversaries may conduct [File and Directory Permissions Modification](https://attack.mitre.org/techniques/T1222) or [Modify Registry](https://attack.mitre.org/techniques/T1112) in support of subverting these controls. (Citation: SpectorOps Subverting Trust Sept 2017) Adversaries may also create or steal code signing certificates to acquire trust on target systems.(Citation: Securelist Digital Certificates)(Citation: Symantec Digital Certificates)

Name

Phishing

ID

T1566

Description

Adversaries may send phishing messages to gain access to victim systems. All forms of phishing are electronically delivered social engineering. Phishing can be targeted, known as spearphishing. In spearphishing, a specific individual, company, or industry will be targeted by the adversary. More generally, adversaries can conduct non-targeted phishing, such as in mass malware spam campaigns. Adversaries may send victims emails containing malicious attachments or links, typically to execute malicious code on victim systems. Phishing may also be conducted via third-party services, like social media platforms. Phishing may also involve social engineering techniques, such as posing as a trusted source, as well as evasive techniques such as removing or manipulating emails or metadata/headers from compromised accounts being abused to send messages (e.g., [Email Hiding Rules](https://attack.mitre.org/techniques/T1564/008)).(Citation: Microsoft OAuth Spam 2022)(Citation: Palo Alto Unit 42 VBA Infostealer 2014) Another way to accomplish this is by forging or spoofing(Citation: Proofpoint-spoof) the identity of the sender which can be used to fool both the human recipient as well as automated security tools.(Citation: cyberproof-double-bounce) Victims may also receive phishing messages that instruct them to call a phone number where they are directed to visit a malicious URL, download malware,(Citation: sygnia Luna Month)(Citation: CISA Remote Monitoring and Management Software) or install adversary-accessible remote management tools onto their computer (i.e., [User Execution](https://attack.mitre.org/techniques/T1204)).(Citation: Unit42 Luna Moth)

Name

System Information Discovery

ID

T1082

Description

An adversary may attempt to get detailed information about the operating system and hardware, including version, patches, hotfixes, service packs, and architecture. Adversaries may use the information from [System Information Discovery](https://attack.mitre.org/techniques/T1082) during automated discovery to shape follow-on behaviors, including whether or not the adversary fully infects the target and/or attempts specific actions. Tools such as [Systeminfo](https://attack.mitre.org/software/S0096) can be used to gather detailed system information. If running with privileged access, a breakdown of system data can be gathered through the `systemsetup` configuration tool on macOS. As an example, adversaries with user-level access can execute the `df -aH` command to obtain currently mounted disks and associated freely available space. Adversaries may also leverage a [Network Device CLI](https://attack.mitre.org/techniques/T1059/008) on network devices to gather detailed system information (e.g. `show version`).(Citation: US-CERT-TA18-106A) [System Information Discovery](https://attack.mitre.org/techniques/T1082) combined with information gathered from other forms of discovery and reconnaissance can drive payload development and concealment.(Citation: OSX.FairyTale)(Citation: 20 macOS Common Tools and Techniques) Infrastructure as a Service (IaaS) cloud providers such as AWS, GCP, and Azure allow access to instance and virtual machine information via APIs. Successful authenticated API calls can return data such as the operating system platform and status of a particular instance or the model view of a virtual machine.(Citation: Amazon Describe Instance)(Citation: Google Instances Resource)(Citation: Microsoft Virutal Machine API)

Name

Video Capture

ID

T1512

Description

An adversary can leverage a device's cameras to gather information by capturing video recordings. Images may also be captured, potentially in specified intervals, in lieu of video files. Malware or scripts may interact with the device cameras through an available API provided by the operating system. Video or image files may be written to disk and exfiltrated later. This technique differs from [Screen Capture](https://attack.mitre.org/techniques/T1513) due to use of the device's cameras for video recording rather than capturing the victim's screen. In Android, an application must hold the `android.permission.CAMERA` permission to access the cameras. In iOS, applications must include the `NSCameraUsageDescription` key in the `Info.plist` file. In both cases, the user

must grant permission to the requesting application to use the camera. If the device has been rooted or jailbroken, an adversary may be able to access the camera without knowledge of the user.

Name

Web Service

ID

T1481

Description

Adversaries may use an existing, legitimate external Web service as a means for relaying data to/from a compromised system. Popular websites and social media, acting as a mechanism for C2, may give a significant amount of cover. This is due to the likelihood that hosts within a network are already communicating with them prior to a compromise. Using common services, such as those offered by Google or Twitter, makes it easier for adversaries to hide in expected noise. Web service providers commonly use SSL/TLS encryption, giving adversaries an added level of protection. Use of Web services may also protect back-end C2 infrastructure from discovery through malware binary analysis, or enable operational resiliency (since this infrastructure may be dynamically changed).

Name

Input Capture

ID

T1417

Description

Adversaries may use methods of capturing user input to obtain credentials or collect information. During normal device usage, users often provide credentials to various locations, such as login pages/portals or system dialog boxes. Input capture mechanisms may be transparent to the user (e.g. [Keylogging](https://attack.mitre.org/techniques/

T1417/001)) or rely on deceiving the user into providing input into what they believe to be a genuine application prompt (e.g. [GUI Input Capture](https://attack.mitre.org/techniques/T1417/002)).

Name

Application Layer Protocol

ID

T1437

Description

Adversaries may communicate using application layer protocols to avoid detection/network filtering by blending in with existing traffic. Commands to the mobile device, and often the results of those commands, will be embedded within the protocol traffic between the mobile device and server. Adversaries may utilize many different protocols, including those used for web browsing, transferring files, electronic mail, or DNS.

Name

Access Notifications

ID

T1517

Description

Adversaries may collect data within notifications sent by the operating system or other applications. Notifications may contain sensitive data such as one-time authentication codes sent over SMS, email, or other mediums. In the case of Credential Access, adversaries may attempt to intercept one-time code sent to the device. Adversaries can also dismiss notifications to prevent the user from noticing that the notification has arrived and can trigger action buttons contained within notifications.(Citation: ESET 2FA Bypass)

Name

Software Discovery

ID

T1418

Description

Adversaries may attempt to get a listing of applications that are installed on a device. Adversaries may use the information from [Software Discovery](https://attack.mitre.org/techniques/T1418) during automated discovery to shape follow-on behaviors, including whether or not to fully infect the target and/or attempts specific actions. Adversaries may attempt to enumerate applications for a variety of reasons, such as figuring out what security measures are present or to identify the presence of target applications.

Name

System Information Discovery

ID

T1426

Description

Adversaries may attempt to get detailed information about a device's operating system and hardware, including versions, patches, and architecture. Adversaries may use the information from [System Information Discovery](https://attack.mitre.org/techniques/T1426) during automated discovery to shape follow-on behaviors, including whether or not to fully infects the target and/or attempts specific actions. On Android, much of this information is programmatically accessible to applications through the `android.os.Build` class. (Citation: Android-Build) iOS is much more restrictive with what information is visible to applications. Typically, applications will only be able to query the device model and which version of iOS it is running.

Name

Data from Local System

ID

T1533

Description

Adversaries may search local system sources, such as file systems or local databases, to find files of interest and sensitive data prior to exfiltration. Access to local system data, which includes information stored by the operating system, often requires escalated privileges. Examples of local system data include authentication tokens, the device keyboard cache, Wi-Fi passwords, and photos. On Android, adversaries may also attempt to access files from external storage which may require additional storage-related permissions.

Name

Boot or Logon Initialization Scripts

ID

T1398

Description

Adversaries may use scripts automatically executed at boot or logon initialization to establish persistence. Initialization scripts are part of the underlying operating system and are not accessible to the user unless the device has been rooted or jailbroken.

Name

Audio Capture

ID

T1429

Description

Adversaries may capture audio to collect information by leveraging standard operating system APIs of a mobile device. Examples of audio information adversaries may target include user conversations, surroundings, phone calls, or other sensitive information. Android and iOS, by default, require that applications request device microphone access from the user. On Android devices, applications must hold the `RECORD_AUDIO` permission to access the microphone or the `CAPTURE_AUDIO_OUTPUT` permission to access audio output. Because Android does not allow third-party applications to hold the `CAPTURE_AUDIO_OUTPUT` permission by default, only privileged applications, such as those distributed by Google or the device vendor, can access audio output.(Citation: Android Permissions) However, adversaries may be able to gain this access after successfully elevating their privileges. With the `CAPTURE_AUDIO_OUTPUT` permission, adversaries may pass the `MediaRecorder.AudioSource.VOICE_CALL` constant to `MediaRecorder.setAudioOutput`, allowing capture of both voice call uplink and downlink. (Citation: Manifest.permission) On iOS devices, applications must include the `NSMicrophoneUsageDescription` key in their `Info.plist` file to access the microphone. (Citation: Requesting Auth-Media Capture)

Name

System Network Configuration Discovery

ID

T1422

Description

Adversaries may look for details about the network configuration and settings, such as IP and/or MAC addresses, of operating systems they access or through information discovery of remote systems. On Android, details of onboard network interfaces are accessible to apps through the `java.net.NetworkInterface` class.(Citation: NetworkInterface) Previously, the Android `TelephonyManager` class could be used to gather telephony-related device identifiers, information such as the IMSI, IMEI, and phone number. However, starting with

Android 10, only preloaded, carrier, the default SMS, or device and profile owner applications can access the telephony-related device identifiers.(Citation: TelephonyManager) On iOS, gathering network configuration information is not possible without root access. Adversaries may use the information from [System Network Configuration Discovery](https://attack.mitre.org/techniques/T1422) during automated discovery to shape follow-on behaviors, including determining certain access within the target network and what actions to do next.

Name

File and Directory Discovery

ID

T1420

Description

Adversaries may enumerate files and directories or search in specific device locations for desired information within a filesystem. Adversaries may use the information from [File and Directory Discovery](https://attack.mitre.org/techniques/T1420) during automated discovery to shape follow-on behaviors, including deciding if the adversary should fully infect the target and/or attempt specific actions. On Android, Linux file permissions and SELinux policies typically stringently restrict what can be accessed by apps without taking advantage of a privilege escalation exploit. The contents of the external storage directory are generally visible, which could present concerns if sensitive data is inappropriately stored there. iOS's security architecture generally restricts the ability to perform any type of [File and Directory Discovery](https://attack.mitre.org/techniques/T1420) without use of escalated privileges.

Name

Location Tracking

ID

T1430

Description

Adversaries may track a device's physical location through use of standard operating system APIs via malicious or exploited applications on the compromised device. On Android, applications holding the `ACCESS_COAURSE_LOCATION` or `ACCESS_FINE_LOCATION` permissions provide access to the device's physical location. On Android 10 and up, declaration of the `ACCESS_BACKGROUND_LOCATION` permission in an application's manifest will allow applications to request location access even when the application is running in the background.(Citation: Android Request Location Permissions) Some adversaries have utilized integration of Baidu map services to retrieve geographical location once the location access permissions had been obtained.(Citation: PaloAlto-SpyDealer)(Citation: Palo Alto HenBox) On iOS, applications must include the `NSLocationWhenInUseUsageDescription`, `NSLocationAlwaysAndWhenInUseUsageDescription`, and/or `NSLocationAlwaysUsageDescription` keys in their `Info.plist` file depending on the extent of requested access to location information.(Citation: Apple Requesting Authorization for Location Services) On iOS 8.0 and up, applications call `requestWhenInUseAuthorization()` to request access to location information when the application is in use or `requestAlwaysAuthorization()` to request access to location information regardless of whether the application is in use. With elevated privileges, an adversary may be able to access location data without explicit user consent with the `com.apple.locationd.preauthorized` entitlement key.(Citation: Google Project Zero Insomnia)

Name

Subvert Trust Controls

ID

T1553

Description

Adversaries may undermine security controls that will either warn users of untrusted activity or prevent execution of untrusted programs. Operating systems and security products may contain mechanisms to identify programs or websites as possessing some level of trust. Examples of such features would include a program being allowed to run because it is signed by a valid code signing certificate, a program prompting the user with a warning because it has an attribute set from being downloaded from the Internet, or

getting an indication that you are about to connect to an untrusted site. Adversaries may attempt to subvert these trust mechanisms. The method adversaries use will depend on the specific mechanism they seek to subvert. Adversaries may conduct [File and Directory Permissions Modification](https://attack.mitre.org/techniques/T1222) or [Modify Registry](https://attack.mitre.org/techniques/T1112) in support of subverting these controls. (Citation: SpectorOps Subverting Trust Sept 2017) Adversaries may also create or steal code signing certificates to acquire trust on target systems.(Citation: Securelist Digital Certificates)(Citation: Symantec Digital Certificates)

Name

Phishing

ID

T1566

Description

Adversaries may send phishing messages to gain access to victim systems. All forms of phishing are electronically delivered social engineering. Phishing can be targeted, known as spearphishing. In spearphishing, a specific individual, company, or industry will be targeted by the adversary. More generally, adversaries can conduct non-targeted phishing, such as in mass malware spam campaigns. Adversaries may send victims emails containing malicious attachments or links, typically to execute malicious code on victim systems. Phishing may also be conducted via third-party services, like social media platforms. Phishing may also involve social engineering techniques, such as posing as a trusted source, as well as evasive techniques such as removing or manipulating emails or metadata/headers from compromised accounts being abused to send messages (e.g., [Email Hiding Rules](https://attack.mitre.org/techniques/T1564/008)).(Citation: Microsoft OAuth Spam 2022)(Citation: Palo Alto Unit 42 VBA Infostealer 2014) Another way to accomplish this is by forging or spoofing(Citation: Proofpoint-spoof) the identity of the sender which can be used to fool both the human recipient as well as automated security tools.(Citation: cyberproof-double-bounce) Victims may also receive phishing messages that instruct them to call a phone number where they are directed to visit a malicious URL, download malware,(Citation: sygnia Luna Month)(Citation: CISA Remote Monitoring and Management Software) or install adversary-accessible remote management tools onto their computer (i.e., [User Execution](https://attack.mitre.org/techniques/T1204)).(Citation: Unit42 Luna Moth)

Name

System Information Discovery

ID

T1082

Description

An adversary may attempt to get detailed information about the operating system and hardware, including version, patches, hotfixes, service packs, and architecture. Adversaries may use the information from [System Information Discovery](https://attack.mitre.org/techniques/T1082) during automated discovery to shape follow-on behaviors, including whether or not the adversary fully infects the target and/or attempts specific actions. Tools such as [Systeminfo](https://attack.mitre.org/software/S0096) can be used to gather detailed system information. If running with privileged access, a breakdown of system data can be gathered through the `systemsetup` configuration tool on macOS. As an example, adversaries with user-level access can execute the `df -aH` command to obtain currently mounted disks and associated freely available space. Adversaries may also leverage a [Network Device CLI](https://attack.mitre.org/techniques/T1059/008) on network devices to gather detailed system information (e.g. `show version`).(Citation: US-CERT-TA18-106A) [System Information Discovery](https://attack.mitre.org/techniques/T1082) combined with information gathered from other forms of discovery and reconnaissance can drive payload development and concealment.(Citation: OSX.FairyTale)(Citation: 20 macOS Common Tools and Techniques) Infrastructure as a Service (IaaS) cloud providers such as AWS, GCP, and Azure allow access to instance and virtual machine information via APIs. Successful authenticated API calls can return data such as the operating system platform and status of a particular instance or the model view of a virtual machine.(Citation: Amazon Describe Instance)(Citation: Google Instances Resource)(Citation: Microsoft Virutal Machine API)

Intrusion-Set

Name

Patchwork

Description

[Patchwork](https://attack.mitre.org/groups/G0040) is a cyber espionage group that was first observed in December 2015. While the group has not been definitively attributed, circumstantial evidence suggests the group may be a pro-Indian or Indian entity. [Patchwork](https://attack.mitre.org/groups/G0040) has been seen targeting industries related to diplomatic and government agencies. Much of the code used by this group was copied and pasted from online forums. [Patchwork](https://attack.mitre.org/groups/G0040) was also seen operating spearphishing campaigns targeting U.S. think tank groups in March and April of 2018.(Citation: Cymmetria Patchwork) (Citation: Symantec Patchwork) (Citation: TrendMicro Patchwork Dec 2017)(Citation: Volexity Patchwork June 2018)

Name

Patchwork

Description

[Patchwork](https://attack.mitre.org/groups/G0040) is a cyber espionage group that was first observed in December 2015. While the group has not been definitively attributed, circumstantial evidence suggests the group may be a pro-Indian or Indian entity. [Patchwork](https://attack.mitre.org/groups/G0040) has been seen targeting industries related to diplomatic and government agencies. Much of the code used by this group was copied and pasted from online forums. [Patchwork](https://attack.mitre.org/groups/G0040) was also seen operating spearphishing campaigns targeting U.S. think tank groups

in March and April of 2018.(Citation: Cymmetria Patchwork) (Citation: Symantec Patchwork) (Citation: TrendMicro Patchwork Dec 2017)(Citation: Volexity Patchwork June 2018)

Country

Name
Pakistan
Name
India
Name
Malaysia
Name
Pakistan
Name
India
Name
Malaysia

Sector

Name
Government and administrations
Description
Civilian government institutions and administrations of the executive and legislative branches. The diplomatic and judicial branches are not included.
Name
Diplomacy
Description
Public or private entities which are actors of or involved in international relations activities.
Name
Government and administrations
Description
Civilian government institutions and administrations of the executive and legislative branches. The diplomatic and judicial branches are not included.

Name
Diplomacy
Description
Public or private entities which are actors of or involved in international relations activities.

StixFile

Value
c06f8c3fd23ae7124cc06eb63c0411418715bf99d3c9fa66525790b2b4c61858
64b2a100e8ca305d7362eeb4858694156d676989b8c6d6d8d01cdebe84dafc7b
2fdb7c4430660cb49547ac2828a631810d4e3d245a6501ce00825faa169cb7d0
c06f8c3fd23ae7124cc06eb63c0411418715bf99d3c9fa66525790b2b4c61858
64b2a100e8ca305d7362eeb4858694156d676989b8c6d6d8d01cdebe84dafc7b
2fdb7c4430660cb49547ac2828a631810d4e3d245a6501ce00825faa169cb7d0

External References

- https://www.welivesecurity.com/en/eset-research/vajraspy-patchwork-espionage-apps/
- https://otx.alienvault.com/pulse/65bcd94818f29ad82d83f035