Apr 14 2024

NETMANAGEIT

Intelligence Report

eXotic Visit campaign: Tracing the footprints of Virtual Invaders

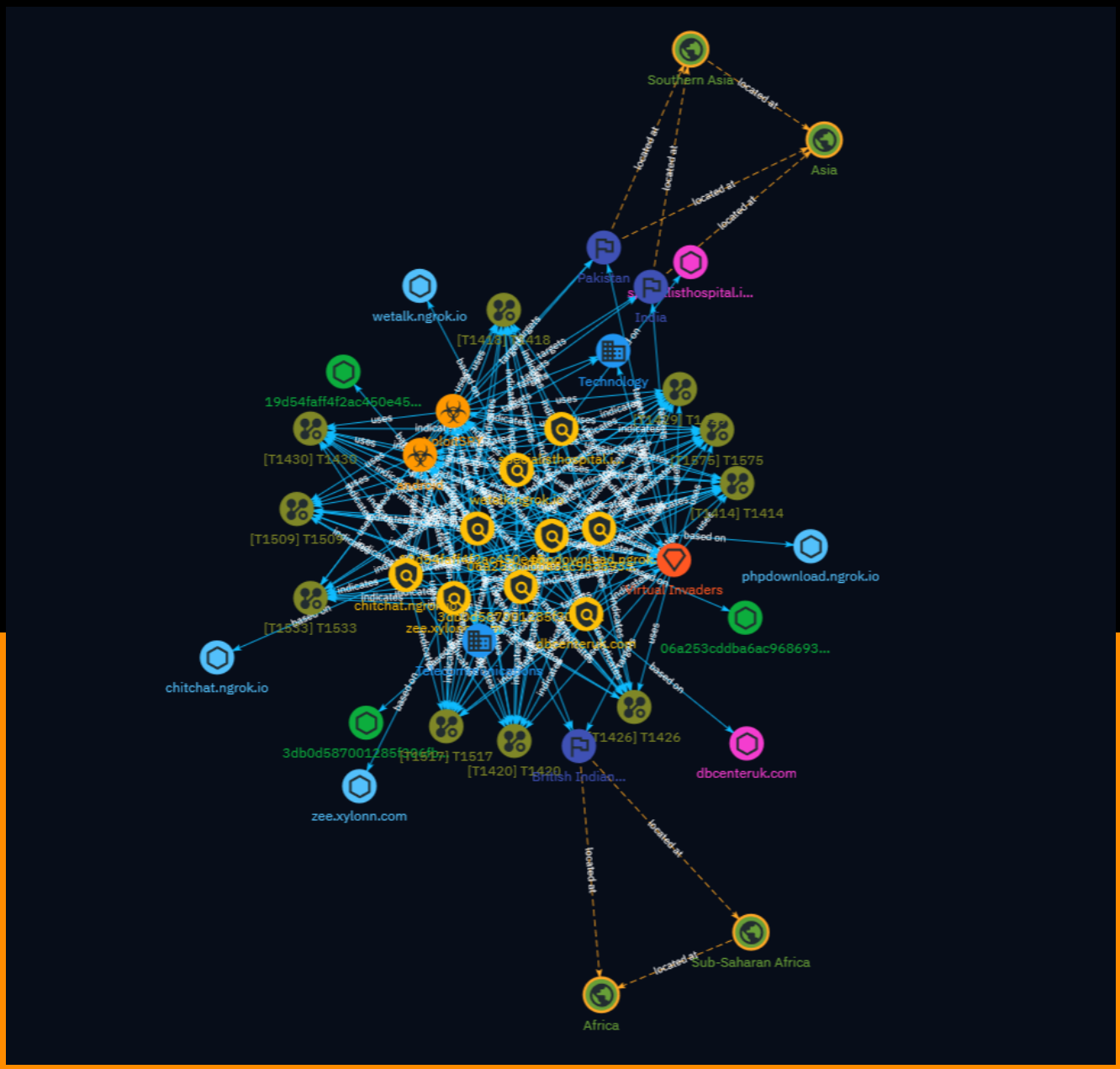

Table of contents

Overview

- Description 4
- Confidence 4
- Content 5

Entities

- Indicator 6
- Malware 10
- Intrusion-Set 11
- Attack-Pattern 12
- Country 18
- Region 19
- Sector 20

Observables

- StixFile 21
- Hostname 22
- Domain-Name 23

External References

- External References 24

Overview

Description

ESET researchers uncovered the eXotic Visit espionage campaign that targets users mainly in India and Pakistan with seemingly innocuous apps that provide messaging functionality but also contain malware. The apps are distributed through dedicated websites and Google Play. The malware is based on the open-source Android RAT XploitSPY and has been customized over time. The campaign has been active since late 2021.

Confidence

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

100 / 100

Content

N/A

Indicator

Name

3db0d587001285f306fbdd73d29ad62ee826a0c27585ebaaf1d993504fdacc5f

Description

SHA256 of 0d9f42ce346090f7957ca206e5dc5a393fb3513f

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '3db0d587001285f306fbdd73d29ad62ee826a0c27585ebaaf1d993504fdacc5f']

Name

19d54faff4f2ac450e4578109dc1e85325edecee8532214154784eca6806f7bf

Description

SHA256 of bb28ce23b3387de43efb08575650a23e32d861b6

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '19d54faff4f2ac450e4578109dc1e85325edecee8532214154784eca6806f7bf']

Name

06a253cddba6ac9686939527075e2235b7741ea6903349d86a1a33543af7fcfa

Description

SHA256 of c9ae3cd4c3742cc3353af353f96f5c9e8c663734

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '06a253cddba6ac9686939527075e2235b7741ea6903349d86a1a33543af7fcfa']

Name

zee.xylonn.com

Pattern Type

stix

Pattern

[hostname:value = 'zee.xylonn.com']

Name
wetalk.ngrok.io
Pattern Type
stix
Pattern
[hostname:value = 'wetalk.ngrok.io']
Name
phpdownload.ngrok.io
Pattern Type
stix
Pattern
[hostname:value = 'phpdownload.ngrok.io']
Name
chitchat.ngrok.io
Pattern Type
stix
Pattern
[hostname:value = 'chitchat.ngrok.io']

Name
specialisthospital.in
Pattern Type
stix
Pattern
[domain-name:value = 'specialisthospital.in']
Name
dbcenteruk.com
Pattern Type
stix
Pattern
[domain-name:value = 'dbcenteruk.com']

Malware

Name
XploitSPY

Name
android

Intrusion-Set

Name
Virtual Invaders

Attack-Pattern

Name
T1509
ID
T1509
Description
Adversaries may generate network traffic using a protocol and port pairing that are typically not associated. For example, HTTPS over port 8088 or port 587 as opposed to the traditional port 443. Adversaries may make changes to the standard port used by a protocol to bypass filtering or muddle analysis/parsing of network data.
Name
T1575
ID
T1575
Description
Adversaries may use Android's Native Development Kit (NDK) to write native functions that can achieve execution of binaries or functions. Like system calls on a traditional desktop operating system, native code achieves execution on a lower level than normal Android SDK calls. The NDK allows developers to write native code in C or C++ that is compiled

directly to machine code, avoiding all intermediate languages and steps in compilation that higher level languages, like Java, typically have. The Java Native Interface (JNI) is the component that allows Java functions in the Android app to call functions in a native library.(Citation: Google NDK Getting Started) Adversaries may also choose to use native functions to execute malicious code since native actions are typically much more difficult to analyze than standard, non-native behaviors.(Citation: MITRE App Vetting Effectiveness)

Name

T1517

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

T1418

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

T1426

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

T1533

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

T1429

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

T1420

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

T1430

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

T1414

ID

T1414

Description

Adversaries may abuse clipboard manager APIs to obtain sensitive information copied to the device clipboard. For example, passwords being copied and pasted from a password manager application could be captured by a malicious application installed on the device. (Citation: Fahl-Clipboard) On Android, applications can use the `ClipboardManager.OnPrimaryClipChangedListener()` API to register as a listener and monitor the clipboard for changes. However, starting in Android 10, this can only be used if the application is in the foreground, or is set as the device's default input method editor (IME).(Citation: Github Capture Clipboard 2019)(Citation: Android 10 Privacy Changes) On iOS, this can be accomplished by accessing the `UIPasteboard.general.string` field. However, starting in iOS 14, upon accessing the clipboard, the user will be shown a system notification if the accessed text originated in a different application. For example, if the user copies the text of an iMessage from the Messages application, the notification will read "application_name has pasted from Messages" when the text was pasted in a different application.(Citation: UIPPasteboard)

Country

Name
Pakistan
Name
India
Name
British Indian Ocean Territory

Region

Name
Southern Asia
Name
Asia
Name
Sub-Saharan Africa
Name
Africa

Sector

Name
Telecommunications
Description
Private and public entities involved in the production, transport and dissemination of information and communication signals.
Name
Technology
Description
Private entities related to the research, development, manufacturing and distribution of electronics, softwares, computers and products related to information technologies.

StixFile

Value
3db0d587001285f306fbdd73d29ad62ee826a0c27585ebaaf1d993504fdacc5f
19d54faff4f2ac450e4578109dc1e85325edecee8532214154784eca6806f7bf
06a253cddba6ac9686939527075e2235b7741ea6903349d86a1a33543af7fcfa

Hostname

Value
zee.xylonn.com
wetalk.ngrok.io
phpdownload.ngrok.io
chitchat.ngrok.io

Domain-Name

Value
specialisthospital.in
dbcenteruk.com

External References

- https://www.welivesecurity.com/en/eset-research/exotic-visit-campaign-tracing-footprints-virtual-invaders/
- https://otx.alienvault.com/pulse/6616fd0f9a1d112706f04e37