cybersecurity associates

Android Malware: Rogue

Threat Hunting Report

Dated: 12th April 2021

By Zachary Goggins

This report contains Threat Hunting research carried out by CSA analysts to outline the subject threat to the reader. It highlights information about current and emerging threats to identify countermeasures which can be put into place to thwart the threat.

Contents

Android Malware: Rogue

Threat Hunting Report

Executive Summary

The purpose of this report is to document the current form and methodologies used by the Rogue Malware. The information documented is then used by Cyber Security Associates Ltd (CSA) Cyber Analysts to hunt for the threat within the client environment through the use of our supported SIEM's BorderPoint and LogRhythm and advise on counter measures to monitor and detect for the subject threat.

This report documents the lifecycle of the Rogue Malware and how it operates, with supporting evidence and recommendations to mitigate the emerging threat. The report also includes a list of identified indicators of compromise and references where the information within this report was identified from.

Summary

A new malware dubbed Rogue is able to provide hackers with near-full access to a targeted smartphone. Researchers have found this malware being distributed on the dark web. It is a Remote Administration Tool (RAT) that infects victims with a keylogger, this allows attackers to monitor the use of websites and apps which allows them to steal passwords and usernames, including more sensitive information such as financial data.

This malware can initiate a full-scale takeover of the infected smartphone, it will also monitor the GPS location on the target, using the camera to take pictures and secretly recording audio from calls. This can happen while the virus is hidden from the owner of the smartphone. A malicious actor can use their own smartphone to send commands to the infected device. Security experts have linked Rogue to two previous Android RATs, Cosmos and Hawkshaw.

Rogue was developed by the darknet threat actors known as Triangulum and HeXaGoN Dev. Security experts have noted that it appears to be a combination of Triangulum's social marketing skills and HeXaGoN Dev's programming skills that have enabled this malware to pose a legitimate threat. The RAT will take advantage of a targeted devices Android Accessibility Services, this is designed to assist users with disabilities. Hackers can access these services to gain control over a device without the victim knowing. Rogue is being offered for as little as $29 a month, whereas lifetime access is being offered for $189.

Tactics, Techniques, Procedures

Tactics, Techniques, and Procedures (TTP) describes an approach of analysing an APT's operation or can be used as means of profiling a certain threat actor.

Tactics is meant to outline the way an adversary chooses to carry out his attack from the beginning till the end. Technological approach of achieving intermediate results during the campaign is described by Techniques the attacker uses. Lastly, the organizational approach of the attack is defined by procedures which are used by the threat actor.

In order to understand and fight the enemy one has to understand the Tactics, Techniques and Procedures (TTP) the attacker uses. Understanding the Tactics of an adversary can help in predicting the upcoming attacks and detect those in early stages. Identifying the Techniques used during an attack allows to identify an organisation's blind spots and implement countermeasures in advance. Finally, the analysis of the procedures used by the adversary can help to understand what the adversary is looking for within their target's infrastructure.

TTPs that are described within this research are based of the information which CSA analysts have been able to identify prior to the release of this document. The threat may change and adapt as it matures to increase its likelihood of evading defence.

Hackers
A 'hacker' is a person who finds it interesting to interfere with computer systems. Often seen as a challenge, a hacker will attempt to breach a system because it tests their skills and knowledge.

Hacktivists
A 'hacktivist' is a person who gains unauthorized access to computer files or networks in order to further social or political ends.

Insider Threats
An employee or 'insider' is a person within a group or organisation, especially someone with knowledge of information unavailable to others.

State Sponsored
A 'state actor' is a person who is acting on behalf of a governmental body and is therefore subject to regulation under their human rights.

Organised Crime
A 'criminal gang' is a group of people that take part in organised unlawful activity. They may target a business to gather information on customers or to gather financial data which could be sold.

Phase 1: Initial Access: Phishing

Rogue can gain access to systems by utilising multiple infection methods. Researchers have so far found that this entails malicious applications, phishing or possibly something else. After it has been downloaded onto a smartphone, it will ask for permissions so that the hacker can access the victim's smartphone remotely, from their own smartphone. If the permissions are not granted, Rogue will keep asking the user to grant them until they do.

Phase 2: Persistence: Abuse Services

Rogue abuses Google's Firebase platform to target and compromise as many Android devices as possible. Firebase incorporates some services that will help developers create mobile and web applications. Rogue will use the following services:

- Cloud Messaging - receives commands from the C2.
- Realtime Database - uploads data from the device.
- Cloud Firestore - to upload files.

MITRE ATT&CK

MITRE developed the Adversarial Tactics, Techniques and Common Knowledge framework (ATT&CK), which is used to track various techniques attackers use throughout the different stages of cyberattack to infiltrate a network and exfiltrate data.

The framework defines the following tactics that are used in a cyberattack:

- Initial Access
- Execution
- Persistence
- Privilege Escalation
- Defence Evasion
- Credential Access
- Discovery
- Lateral Movement
- Collection
- Exfiltration
- Command and Control

It will also disguise its malicious intent and pretend to be a legitimate service by registering as the system administrator. When Rogue has obtained all the required permissions from the victim, it is hidden from the owner of the infected device which makes it difficult to remove. If the victim tries to revoke administrative privileges, a message is displayed by the malware: "Are you sure to wipe all the data?", this attempts to scare victims from removing the malware.

Rogue can compare specific pre-defined values of the system which enables it to detect a virtual environment, this could lead to an abort or delay of its malicious actions.

Phase 3: Command & Control (C2): Exfiltration

Rogue will use Firebase's services as a C2 server, this means that all of the information stolen by the malware is delivered using the Firebase infrastructure; the same infrastructure is used to deliver the commands that control the malware. In the malware's manifest file there is a field called 'APP_VERSION'. Depending on the value of that field, Rogue can run on 'MINIMUM' configuration, this is designed to draw the minimum amount of attention.

Android's accessibility service can be adapted by Rogue to suit its own needs. This service is the Operating System (OS) assistive service that is used to mimic the user's screen clicks which can automate user interactions with the device. Rogue will use this service to get around OS security restrictions. The accessibility service is used for documenting and logging the user's actions which will then upload the collected data to the cloud C2 server. The following user actions are logged:

- TYPE_VIEW_TEXT_CHANGED
- TYPE_VIEW_FOCUSED
- TYPE_VIEW_CLICKED

Cyber Kill-Chain

The cyber kill chain is a process that traces the stages of a cyberattack. This starts at the early reconnaissance stages that eventually leads to data exfiltration.

The kill chain can help one to understand and combat ransomware, advanced persistent threats (APTs) and security breaches.

The cyber kill-chain defines the following tactics that are used in a cyberattack:

- Reconnaissance
- Intrusion
- Exploitation
- Privilege Escalation
- Lateral Movement
- Obfuscation/ Anti-forensics
- Denial of Service
- Exfiltration

Rogue can monitor every notification that pops up on the infected device. It does this by registering its own notification service and every notification that is triggered is saved to a local predetermined database. This is later uploaded to the Firebase Database. The notifications are parsed into the following fields:

- Message Body
- Sender
- Timestamp
- TYPE_VIEW_CLICKED

A 'Block List' is used for phone numbers by Rogue and it will choose which numbers are in the list. If it detects a call to one of these numbers, either incoming or outgoing, it will drop the call. To achieve this, a call receiver called 'me.hawkshaw.receiver.CallReceiver' is registered and it will use 'CallBlock' to block a certain call. If a call is accepted, each call can be recorded and Rogue will then leak it to the Firebase Cloud Store.

Conclusion

Once a smartphone has been infected, Rogue asks for many different permissions that the attackers need to gain direct access to the infected device. If a victim decides not to grant the permissions, Rogue will ask profusely for permissions to be granted until the user gives in. It will then abuse Androids services so that it can disguise itself as a legitimate service, this is how it evades Androids defences and gains persistence.

More businesses are working from home now due to Covid-19. This means that employees can access internal business networks and potentially sensitive data by using mobiles. Attackers now have an increased chance to compromise networks by using infected mobiles as an attack vector. This can happen due to poor security configurations on mobile or by exploiting unpatched vulnerabilities (caused from not updating the device).

The price of $29 a month means that this malware is widely available for anyone to use, but depending on the person that buys the malware, different infection methods may be used.

Advice

The IOC's identified within this report are monitored by our SIEM solution, BorderPoint, if a host were to demonstrate any of the characteristics CSA would ensure to alarm you. It is imperative that there is a backup strategy in place that is tested and that it also covers worst-case scenarios. CSA recommends:

- Regular backups must be kept offline; this is the only way to protect against a determined threat actor.
- Regularly test backups for their integrity and if they can be recovered. Scan backups for registry persistence.
- Critical data should be written on WORMs (Write Once Read Many). This write protection ensures that the data cannot be tampered with once it is written to the device.
- Disable all macros, except those that are digitally signed. This will display a security notification for macros that were developed by a certified publisher, allowing one to decide whether to enable or disable them.
- Implement filters at the email gateway. Filter out emails with known malspam indicators and block suspicious IP addresses at the firewall.
- Educate and train employees on social engineering and phishing. This is a common infection method for malware and ransomware, training employees in this area can reduce the risk of a compromise though emails.
- Adhere to the Principle of Least Privilege (PLP). Ensure that users have the minimum level of access required to accomplish their duties. Limit administrative credentials to designated admins.

- **Use antivirus programs on clients and servers**. Keep it up to date with automatic updates of signatures and software. This should also apply to mobile devices.
- **If there is not a policy regarding suspicious emails, consider creating one.** Specify that all suspicious emails should be reported to the security and/or IT departments. Using CSA's tool AppGuard will prevent interaction with the system space.
- **Inform users of mobile risks.** A mobile is a computer and should be treated like one, consider the source of an app or game. For example, if it asks for more than what it needs to do its job, do not install it.
- **Prevent users from jailbreaking their mobiles.** This is the process of removing security limitations that is imposed by the operating systems vendor, by gaining full access to the OS and its features. This allows all apps including malicious ones, to access the data owned by other applications.
- **Encrypt devices.** If a device is lost, strong encryption would make it incredibly difficult for someone to break into it and steal the data. Set strong passwords for the device and SIM card.
- **Mobile security policies should fit into overall security framework.** If a device does not comply with security policies, it should not be allowed to connect to the corporate network and access corporate data. IT departments need to communicate which devices are allowed.

Indicators of Compromise

Domain Names:

- https[:]//bald-panel[.]firebaseio[.]com
- https[:]//hawkshaw-cae48[.]firebaseio[.]com
- https[:]//spitfirepanel[.]firebaseio[.]com
- https[:]//phoenix-panel[.]firebaseio[.]com

Firebase Accounts:

In the code of the Rogue malware, there are hidden Firebase accounts:

- GUARDIAO
- PHOENIX
- SPITFIRE
- AVIRTEK
- HAWKSHAW

Commands:

Command	Description
getLocation	Add current location and current timestamp to the Firebase Database.
getMessages	SMS messages and the current timestamp are added to the Firebase Database.
makeCall	Application initiates a phone call to a provided phone number.
getImages	Make thumbnails of an album with its name and upload thumbnails to the Firebase Cloud Store. A list of uploaded thumbnails is stored in the Firebase Database.
deleteCallLog	Removes records from the provided type of call-log.
fileExplorer	Store a list of directories by a provided path in the Firebase Database.
recordCamera	Starts recording from selected cameras and for a provided duration. The video is recorded to a local file. After recording, the video-file is uploaded to the Firebase Cloud Store.
installApp	Installs an application from a provided URL.
syncWhatsappMessages	Upload messages collected from chat programs to the Firebase Database.
fileDownloadToLocal	Downloads a file from a provided URL to a provided local path.
deviceAdmin	Activates the device admin permission for an application.
openApp	Launches an application with a provided name.
getContacts	Uploads all contacts and call logs to the Firebase Database.
root	Executes a shell command. The output of the command is stored in the Firebase Database.
takePicture	Takes a photo from a selected camera (back or front) and uploads the photo to the Firebase Cloud Store.
deleteFile	Deletes a file or directory per the provided path.
downloadFile / uploadFile	Uploads a file by a provided path to the Firebase Cloud Store.
sendMessage	Sends a custom SMS message to a specified number.

recordScreen	Records a video of the device's screen. The video is recorded to a local file. After recording, the video-file is uploaded to the Firebase Cloud Store.
deleteContact	Deletes a specified contact.
updateCallBlockList	Updates the local list of call blocked numbers with a list from the Firebase Database.
takeScreenShot	Takes a screenshot of the current screen. The screenshot is uploaded to the Firebase Cloud Store.
recordAudio	Starts recording from a microphone for a provided duration. The audio is recorded to a local file. After recording, the audio-file is uploaded to the Firebase Cloud Store.
deviceInfo	Collects information about the device: • Phone number • Network provider • Username • List of device user accounts • SDK version • User-visible version string • Device serial number • Device name, brand, board, manufacturer • IMEI • Battery level • Network connection status • WiFi connection information, DHCP status • WiFi scan results with available Access Points • IPv4 and IPv6 addresses The information is stored in the Firebase Database.
cancelScheduledCommand	Cancels the execution of a scheduled pending command.
usageStats	Gets statistics of the device's applications usage. The following fields are sent to the C&C server: · Package name · Foreground time · Timestamp of first time used

	• Timestamp of last time used System applications are eliminated from the statistics. The information is stored in the Firebase Database.
getInstalledApps	Stores the current timestamp and list of installed applications in the Firebase Database.
deleteFiles	Deletes files from the device by a provided path.
openBrowser	Opens the Chrome browser and navigates to a specific URL.
zipFiles	Zips files in a specified path. The resulting zip-file is uploaded to the Firebase Cloud Store.
addContact	Creates a new contact.
login	Attempts to log back into the Firebase account with a provided email and password.
getAllScheduledTasks	Dumps all scheduled tasks into a log and uploads it to the C&C server.
cancelAllScheduledCommands	Similar to “cancelScheduledCommand” but for all pending commands.
addCallLog	Adds a new record to the call log with a provided number, the duration, date, and the type of the call.
updateFCMToken	Updates the token that is used for the Firebase service.
deleteApp	Uninstalls application by a provided package name.
clearWhatsappMessages	Removes saved sniffed IM messages from applications in the local database. It is possible to remove all messages or only messages that belong to one of the sniffed applications (e.g. “com.whatsapp”).
runJobScheduler	Starts a scheduler for executing jobs scheduled by the “scheduleCommand” command.

Hashes:

SHA256:

- 1f5850b3a38df372cc40987b376cbf093ed5dd5d9e99e3ead61b24aa8cc82976
- 28a74b00f590cc85578dad296271ed0a91225b876c088a4fae2a7e9d06636347
- 2beb5e9d9ba93acc1d5f858c3e4fdeee04e0741eb44ab0a3a5a98ce2687f38a7
- 36ebc45ee083d8478372916a7d9bf4f7f26bdd1cd8f10765ec6e375bf73962f4
- 3dc2f2a200630294fc0af904ddf611f9ecfe8a4c65899aff8d6b56aed53177f8
- 3ead4a167d118105164e9c13de0fa14d06ea0dc32d02c861bde4c8bef4e0bd07
- 41ad6c0c6eb93877adb8a319520bba43a334cae463379feccb5b6df3bb94b530
- 4478a2e8a952529bbe1bf0a1f1d98f197ff1717f1dab1635cfe151c4771d3561
- 49b353ac2ba897672644ea6aff8edc69ac7fc195b96c069c338f7da588674871
- 4ad6b698cfd2af542fca2316b94e1f213025d48e0895f1a127dec789c4b4dded
- 4d24880ac70f7d7b3997316ca01854413de0d8df5bb30ce757280a28713ae7e4
- 4e0bcfc83f8a2714acbf1725262827ec17f61c5826cd5cf0837d1642fdc5b25e
- 5a8de8e601fb1577321ded7475b28f8c72157bb6bcf2857c99cbc7a39489c71a
- 5de7799e1d95daaaceb6e158dfb27e44fd93021c7676f728b0e157e1bd2099c7
- 62078c7099dd3485b45ac8bec8fcecbc2662f6c21d3b309dc7a865df6a822794
- 64905ad7b0f635efb0402d57d0b0d7d31832ca66afac2fe17379877004a32e73
- 6ad406fa29e2f327d9672e1f8578d89aa1f1cc242c7a9ee83ede3cebd313ca09
- 6e89e0e52fec1bff8175742570d9a40cb32be6c869e885077db9b13b1e39ef80
- 71cc0cd5979cce2ee72073e81c47262465fd8158d10a7d29cd86cae6ffa12607
- 72c60de4ae67237bbcdc8d9bdda38c2374cb0d4a1364239ecb9ef4992a6253e2
- 734c9146be56c9c1e1abb7dfa533d8ebec77ceae8550d7918dd7e38e4f4dc721
- 7a6c738f4bdecffcbfa8a29eae1091876f34d9c91cd21b51a7e51896a69be3ac
- 7bea11940ef818db0b3284c5e6b651e8551b5f2662808e3c48e2e92a55156ff3
- 82c07ab7460204b60e4cd4c2f5e263db538e128382341f8dfa727800d3e0c980
- 901c93ee5bc2a474c20379bd07eac08cc27266a39b3b6b563c0ffa7dfcebec88
- 928cdc76250852b5161ca0ca418b82cf3033e1b21d419a9654a29a68b43e4aa5
- 974615a4902d920895b4fe03e4f987f56471f003daf82d2930c9fdbdc56bc048
- 9eb556a52bf26e284a6c333f09d576e61fad9f76d4d4b7abb86cfe099108b8a0
- a08db81e33f978da7b540228d04ddce47f447b4501b9f70fba46f5acf74e038a
- a1002512a86d7af9c4fd5579f87baee7d377e84373cae475a83beb9438eb17e7

- ae3afac1ddbf6853845c8a62f9adaaa5ea872141da2dd8be5a6d61b84bf1da9a
- af89e25c4add8bc5a5d5cd1a16479ecd8f40577766d8ea8e42eb6bcae7d3ba9d
- b93ba6614762120f200efdee98ba2f5f3f3f55f152279c70422d2014f770cf8e
- bcd53e2e363daf5eb719c0892d49d15261189fe8711adc9ad40fcbe646956622
- c2893c0cdb3e67f3052fe3f819f03f5d52610d0904dad11aa353db202ead6c00
- caa38f6ae2969e885757ff0cfce69b7981d4c115740f12cd18b4088b47a97dee
- cf519a751ea25f59f99d7f90dfba82c109b11725fe9cbeb479c3ec358f124e99
- d910ff3e1ff1c8355d603113dfdf6de3859e206bdd704b83a75c7efb7ab7a594
- dfd18ac31b4b90ac72649de6ed663fa2fd8719606cd4da7126098e58288693ce
- e0e1fb9d914d0626c4e7b4999afdd02f070cea1bc5a446f7073566d94493161f
- e2f611c47efd760a41090293792ad8ebe6ae972c75fe136639c4cc98561b4e98
- f47d06ddf3525e244f5d58e9c3ea5f1977845c917b84fca28363d1797d70715e
- fa7fcbf01a252e1f0d3028512e5d58ab18674bc415d4956e28d1e3fea835d724
- 10988044a6db87ff8a526aa4a5004c9fafb8631d4373bf3e7ec76e5e47690eb9
- cb1cbb2cadb2f265b38fae9bad0d622cdf4d7c071924a0346679fb3decafa95c
- 4105f8c46caa7b715d003a8d39ecf2d22b107000961a232538766830a741657b
- a4058e6e6f81ec4c8bb234b5df11ad9b459221cc7d1b0acba733ffd6e1f1f930
- b790affd3fc6591779fa0c06f6c8e47fbc1b2b76399842f12fbd792edb8bb98c

References

https://www.zdnet.com/article/this-android-malware-claims-to-give-hackers-full-control-of-your-smartphone/

https://www.indiatimes.com/technology/news/android-malware-rogue-can-give-hackers-full-access-of-your-phone-and-is-actively-spreading-531874.html

https://www.news18.com/news/tech/rogue-is-an-android-malware-that-gives-hackers-full-control-over-a-phone-heres-what-we-know-3282122.html

https://securityaffairs.co/wordpress/113369/malware/rogue-android-rat-darkweb.html#:~:text=Rogue%20is%20a%20new%20mobile,code%20on%20the%20darknet%20marketplaces

https://research.checkpoint.com/2021/going-rogue-a-mastermind-behind-android-malware-returns-with-a-new-rat/

https://blog.checkpoint.com/2021/01/12/going-rogue-a-mastermind-behind-android-malware-returns-with-a-new-rat/

https://latestnews-live.com/rogue-is-an-android-malware-that-gives-hackers-full-control-over-a-phone-heres-what-we-know/

https://thegreaterindia.in/technology/rogue-is-an-android-malware-that-gives-hackers-full-control-over-a-phone-heres-what-we-know/

https://3rd-strike.com/check-point-research-discovers-aggressive-android-malware-named-rogue/

https://securitybrief.co.nz/story/check-point-exposes-android-malware-vendor-using-dark-net-to-rebrand-products

https://techviral.net/rogue-android-malware-allows-hackers-to-access-your-phone/

https://www.amfrontier.net/2021/01/27/rogue-malware-is-an-android-users-worst-nightmare/

https://www.sophos.com/en-us/security-news-trends/security-trends/malware-goes-mobile.aspx