Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

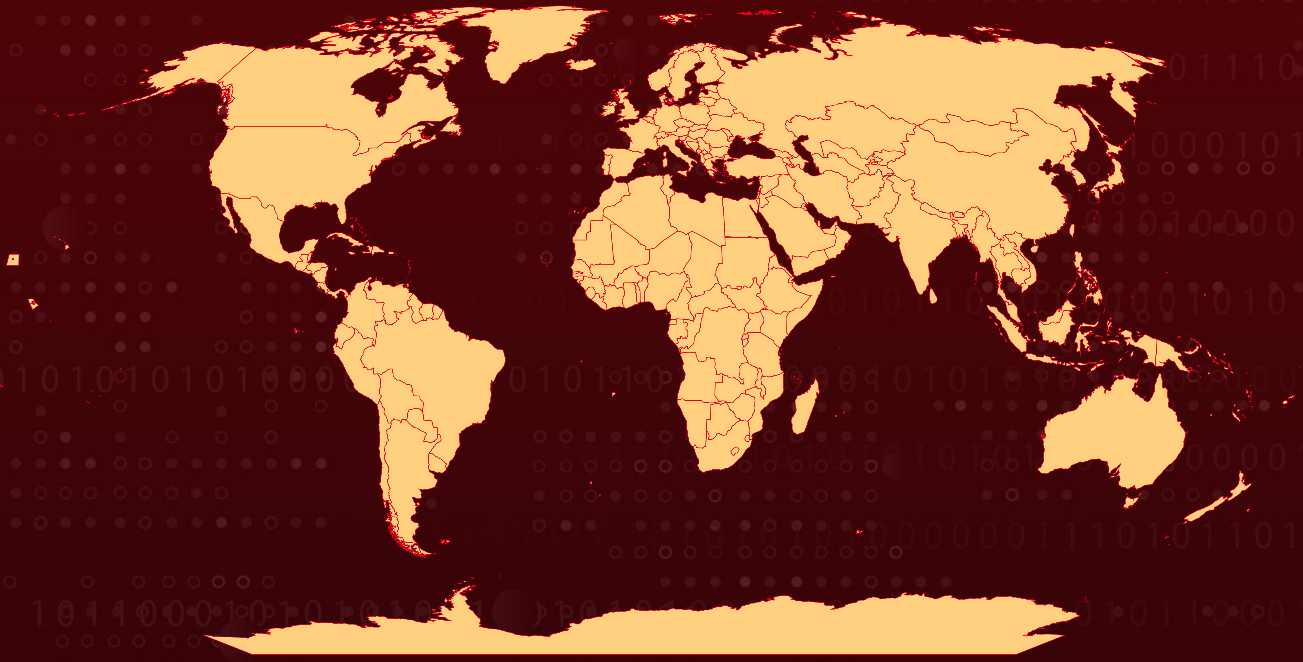
ErrorFather: A Multi-Stage Cerberus Attack on Android

Date of Publication	Admiralty Code	TA Number
October 16, 2024	A1	TA2024395

Summary

Attack Began: September 2024
Campaign Name: ErrorFather
Malware: Cerberus
Affected Platform: Android
Targeted Region: Worldwide
Attack: The ErrorFather campaign uses a sophisticated variant of the Cerberus Banking Trojan to target Android users. The campaign employs a multi-stage infection process to bypass detection and steal financial information. The attackers have been actively targeting users, indicating a sustained and ongoing threat. Android users are advised to be vigilant and take necessary precautions to protect their devices.

Attack Regions



Powered by Bing
© Australian Bureau of Statistics, GeoNames, Microsoft, Navinfo, Open Places, OpenStreetMap, TomTom, Zenrin

Attack Details

#1

The ErrorFather campaign is an advanced Android-targeted cyberattack that repurposes the Cerberus Banking Trojan, a malware originally designed to steal financial data through keylogging, VNC, and overlay attacks. Cerberus, first detected in 2019, became a prominent tool for financial fraud, but after its source code was leaked, multiple threat actors used it to create new banking trojans such as Alien, ERMAC, and Phoenix. ErrorFather follows this trend by utilizing a heavily modified version of Cerberus, demonstrating the adaptability of cybercriminals in reusing known malware.

#2

This campaign uses a two-stage infection process. The first APK, acting as a dropper, installs a secondary payload known as "final-signed.apk," which carries the main malicious functionalities. This secondary payload uses advanced obfuscation techniques, allowing it to evade traditional antivirus engines. ErrorFather's deployment of this modified Cerberus strain shows how the group has adapted older malware to bypass modern security defenses.

#3

To ensure resilience, ErrorFather employs a Domain Generation Algorithm (DGA) for its command and control (C&C) operations. This allows the malware to dynamically update its C&C servers, ensuring continuity even if primary servers are taken down. The DGA used is based on the Istanbul timezone, making it difficult for law enforcement to neutralize the malware's infrastructure. This sophisticated C&C approach enhances the malware's persistence.

#4

The malicious capabilities of Cerberus include keylogging, overlay attacks for phishing, and remote control of infected devices through VNC functionality. These tools allow attackers to harvest sensitive data and remotely manage compromised devices. The malware can also send the names of installed applications to its C&C server and retrieve phishing HTML files, further enabling its wide range of malicious activities.

#5

The campaign saw a marked increase in activity during September and October 2024, indicating ongoing targeting efforts by the threat actors involved. This campaign exemplifies how cybercriminals continue to repurpose older malware strains like Cerberus to create new threats. Despite being based on previously known malware, its sophisticated infection methods and evasion techniques pose significant risks to users.

Recommendations

Download Apps Only from Trusted Sources: Always install apps from official platforms like Google Play Store, which implements security checks. Avoid downloading apps from unknown or third-party websites that could host malicious APKs.

Use Strong Security Software: Install reputable mobile security or antivirus software that can detect malware, even those designed to evade traditional detection like ErrorFather. Make sure the software is regularly updated to protect against the latest threats.

Enable Google Play Protect: Google Play Protect scans your device for harmful apps. Ensure it is enabled to automatically check for suspicious apps and behaviors, including unknown APKs.

Keep Your Device and Apps Updated: Regularly update your Android device's operating system and apps, as updates often contain security patches that can fix vulnerabilities exploited by malware like Cerberus.

Implement Strong Authentication Practices: Use strong, unique passwords for your accounts and enable multi-factor authentication (MFA) wherever possible to enhance security.

Be Cautious with Permissions: Review app permissions carefully before granting them. Only allow permissions that are essential for the app's functionality.

Potential MITRE ATT&CK TTPs

TA0027 Initial Access	TA0041 Execution	TA0030 Defense Evasion	TA0035 Collection
TA0032 Discovery	TA0035 Collection	TA0037 Command and Control	TA0036 Exfiltration
T1521.001 Symmetric Cryptography	T1521 Encrypted Channel	T1646 Exfiltration Over C2 Channel	T1637 Dynamic Resolution

T1660 Phishing	**T1575** Native API	**T1655.001** Match Legitimate Name or Location	**T1655** Masquerading
T1418 Application Discovery	**T1630.001** Uninstall Malicious Application	**T1630** Indicator Removal on Host	**T1516** Input Injection
T1417.001 Keylogging	**T1417** Input Capture	**T1418** Software Discovery	**T1426** System Information Discovery
T1513 Screen Capture	**T1429** Audio Capture	**T1616** Call Control	**T1636.003** Contact List
T1636 Protected User Data	**T1636.004** SMS Messages	**T1637.001** Domain Generation Algorithms	

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	4c7f90d103b54ba78b85f92d967ef4cdcc0102d3756e1400383e774d2f27bb2e, 8f3e3a2a63110674ea63fb6abe4a1889fc516dd6851e8c47298c7987e67ff9b6, c570e075f9676e79a1c43e9879945f4fe0f54ef5c78a5289fe72ce3ef6232a14, a2c701fcea4ed167fdb3131d292124eb55389bc746fcef8ca2c8642ba925895c, 8faa93be87bb327e760420b2faa33f0f972899a47c80dc2bc07b260c18dfcb14, ee87b4c50e5573cba366efaa01b8719902b8bed8277f1903e764f9b4334778d0, 136d00629e8cd59a6be639b0eaef925fd8cd68cbcbdb71a3a407836c560b8579, 516282073b7d81c630d4c5955d396e1e47a2f476f03dea7308461fa62f465c11, 5bd21d0007d34f67faeb71081309e25903f15f237c1f7b094634584ca9dd873e,

TYPE	VALUE
SHA256	6b8911dfdf1961de9dd2c3f9b141a6c5b1029311c66e9ded9bca4d21635c0c49, befe69191247abf80c5a725e1f1024f7195fa85a7af759db2546941711f6e6ae, 9d966baefa96213861756fde502569d7bba9c755d13e586e7aaca3d0949cbdc3, 0c27ec44ad5333b4440fbe235428ee58f623a878baefe08f2dcdad62ad5ffce7, 880c9f65c5e2007bfed3a2179e64e36854266023a00e1a7066cbcf8ee6c93cbc, 6c045a521d4d19bd52165ea992e91d338473a70962bcfded9213e592cea27359
SHA1	cb6f9bcd4b491858583ee9f10b72c0582bf94ab1, 9373860987c13cff160251366d2c6eb5cbb3867e, c7ebf2adfd6482e1eb2c3b05f79cdff5c733c47b
MD5	0544cc3bcd124e6e3f5200416d073b77, d9763c68ebbfaeef4334cfefc54b322f, f9d5b402acee67675f87d33d7d52b364
URLs	hxxp[://]cmsspain[.]homes, hxxp[://]consulting-service-andro[.]ru, hxxp[://]cmscrocospain[.]shop, hxxp[://]cmsspain[.]lol, hxxp[://]cmsspain[.]shop, hxxp[://]elstersecure-plus[.]online, hxxps[://]secure-plus[.]online/ElsterSecure[.]apk, hxxps[://]api[.]telegram[.]org/bot7779906180:AAE3uTyuoDX0YpV1DBJyz5zgwvvVg-up4xo/sendMessage?chat_id=5915822121&text=

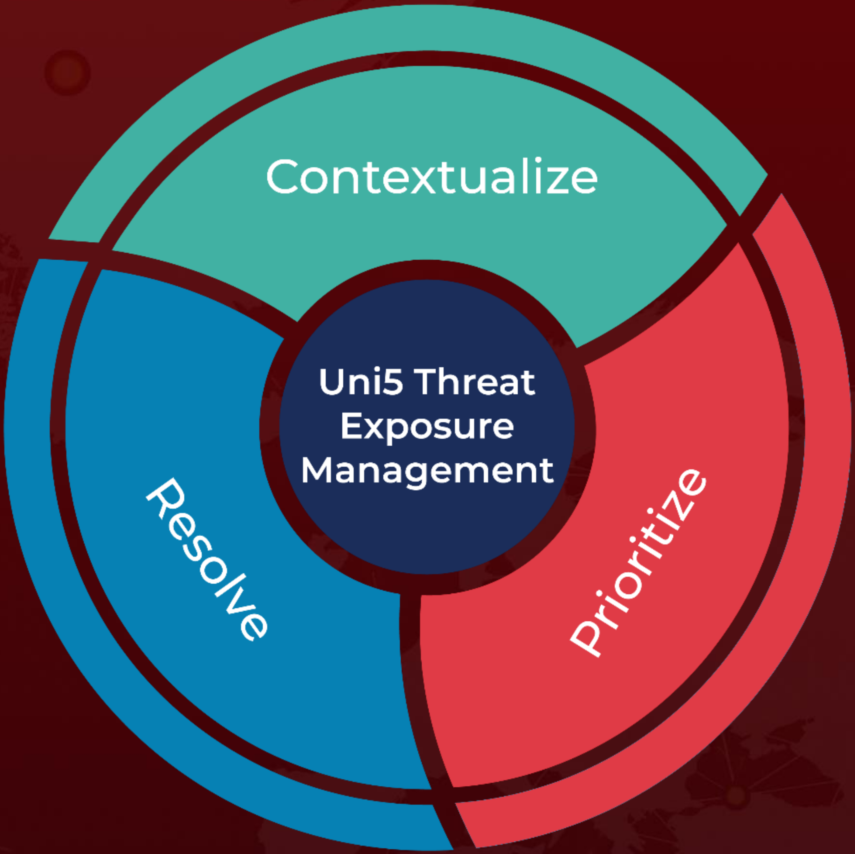
References

https://cyble.com/blog/hidden-in-plain-sight-errorfathers-deadly-deployment-of-cerberus/

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with **HivePro Uni5**: Threat Exposure Management Platform.



REPORT GENERATED ON

October 16, 2024 • 4:30 AM

More at www.hivepro.com