URGENT

No.CB/PHQ/COVID-19/II/2020/248

GOVERNMENT OF MIZORAM
POLICE HEADQUARTERS: AIZAWL

***

Dated Aizawl, the 22nd May, 2020.

To,

The Dy. Inspector General of Police (CID),
Mizoram, Aizawl.

Subjects: ***1. Drug trafficking associated with COVID-19.***
2. Cerberus is taking advantage of COVID-19 pandemic.

Sir,

Please find enclosed herewith copies of mail both dated 21st May, 2020 with its enclosures received from DD/ICPU, Interpol, New Delhi on the subjects cited above for favour of information and further necessary action from your end.

Enclo: *As above*.

Yours faithfully,

(ZOSANGLIANA) AIG(Hqrs.),
for Director General of Police,
Mizoram, Aizawl.
Tel No: 0389-2334355.

(24)

rediffmail

Mailbox of polmizo

Subject: Cerberus is taking advantage of COVID-19 Pandemic

From: Vijayendra Bidari DD Co. <ddco@cbi.gov.in> on Thu, 21 May 2020 15:26:48

To: "Police Headquarters UT JK PHQ UT JK Jammu and kashmir" <phqjk@jkpolice.gov.in>, "dgp" <dgp@tncctns.gov.in>, "polmizo" <polmizo@rediffmail.com>, "Director General of Police, Goa" <dgpgoa@goapolice.gov.in>, "dgpmp" <dgpmp@mppolice.gov.in>, "control-cid" <control-cid@jhpolice.gov.in>, "Director General of Police, Sikkim Sikkim Police" <dgp@sikkimpolice.nic.in>, "John Longkumer" <dgp.ngl@mha.gov.in>, "Rajiv Singh IC DGP Tripura" <dgp@tripurapolice.nic.in>, dgp@tspolice.gov.in, "DGP, Assam" <dgp@assampolice.gov.in>, "addlcpcrimehq" <addlcpcrimehq@gmail.com>, "DG Police, Cuttack" <dgp.odpol@nic.in>, "cidphqraipur" <cidphqraipur@gmail.com>

1 attachment(s) - Purple_Notice_No._968-4-2020__IPSG-CFC_Cerberus.pdf (478.34KB)

Sir,

Please find attached a copy of the Purple Notice regarding the use and dissemination of a **malicious software CERBERUS BANKING TROJAN.**

A banking Trojan known as **Cerberus is taking advantage of COVID-19 Pandemic** to impersonate and send SMS using the lure of COVID-19 related content to download the embedded malicious link, which deploys its malicious app. Usually spread via phishing campaigns to trick users into installing it on their smartphones, the Cerberus corona malicious .apk uses its connection with the actual virus name to help get more users infected.

This Trojan primarily focuses on stealing financial data such as credit card numbers. In addition, it can use overlay attacks to **trick victims into providing personal information and can capture two-factor authentication details.** An "official" twitter account is used to post promotional content about the malware.

As the Purple Notice disseminate important information in the present scenario, therefore, the same is forwarded for your information and necessary action, as deemed appropriate at your end.

IGP(HQ) / AIG(HQ) / DIG CID / Medical Cell.

Regards,
Vijayendra Bidari, IPS
DD/IPCU
INTERPOL-NEW DELHI

DIG, CBI,
International Police Cooperation Unit
5-B, 6th Floor, A Wing, , CGO Complex,
New Delhi - 110003
Ph. No. +91 11 24361683
e mail - ddco@cbi.gov.in

IGP (Hqrs.) 22/5/20

DGP (M) 21/5/20

PF of DGP (M) Receipt No. 2993 Date 22/5/20

1 IMP 22/5/20

246

Control No.: P-968/4-2020
Requesting country: IPSG
File No.: 2020/27743-1
Date of publication: 14 April 2020

INTERPOL
PURPLE NOTICE

MODUS OPERANDI

Type(s) of offence:	The use and dissemination of a malicious software. Cerberus banking Trojan threat and its update related to the Coronavirus pandemic.
Date of the offence:	From June 2019 until now
Country of offence:	Global
Circumstances of offence:	After a national service suffered a malfunctioning and was therefore being rendered inaccessible, the CFC has seen evidence that the threat actor(s) behind the banking Trojan known as Cerberus have taken advantage of this impediment to impersonate the entity and send SMS using the lure of COVID-19 related content to download the embedded malicious link, which deploys its malicious app. This comes from a new wave of attacks of Cerberus, which has been initiated by taking advantage of the COVID-19 pandemic. Usually spread via phishing campaigns to trick users into installing it on their smartphones, the Cerberus corona malicious .apk uses its connection with the actual virus name to help get more users infected. This Trojan primarily focuses on stealing financial data such as credit card numbers. In addition, it can use overlay attacks to trick victims into providing personal information and can capture two-factor authentication details.
Description of modus operandi:	First found in June 2019, Cerberus is an Android malware rented out on underground forums, offering a feature-set that enables successful exfiltration of personally identifiable information (PII) from infected devices. Cerberus was coded from scratch and the author(s) claimed to be using the Trojan for private operations for at least 2 years. Following availability to public, it can cost $2000 (1 month usage), $7000 (6 months) and up to $12,000 (12 months). An "official" twitter account is used to post promotional content about the malware. When Cerberus is first started on the device, it will begin by hiding its icon from the application drawer. Then it will ask for the accessibility service privilege. After the user grants the requested privilege, Cerberus starts to abuse it by granting itself additional permissions, such as permissions needed to send messages and make calls, without requiring any user interaction. It also disables Play Protect (Google's preinstalled antivirus solution) to prevent its discovery

and deletion in the future. After granting itself additional privileges and securing its persistence on the device, Cerberus registers the infected device in the botnet and waits for commands from the C2 server while also being ready to perform overlay attacks[1].

Cerberus malware has capabilities such as the use of overlay attacks, SMS control and contact list harvesting, as well as leverage keylogging to broaden the attack scope. Specifically, Cerberus embeds the following set of features that allows itself to remain under the radar and successfully perform attacks:

Overlaying: Dynamic (Local injects obtained from C2)
Keylogging
SMS harvesting: SMS listing
SMS harvesting: SMS forwarding
Device info collection
Contact list collection
Application listing
Location collection
Overlaying: Targets list update
SMS: Sending
Calls: USSD request making
Calls: Call forwarding
Remote actions: App installing
Remote actions: App starting
Remote actions: App removal
Remote actions: Showing arbitrary web pages
Remote actions: Screen-locking
Notifications: Push notifications
Self-protection: Hiding the App icon
Self-protection: Preventing removal
Self-protection: Emulation-detection

Upon installation, the malware will seek to target specific applications of interest.

2020 Update & COVID-19 Campaign

Cerberus banking Trojan seems to be heavily used during the Coronavirus pandemic, conducting phishing attacks through the use of banking Trojans to steal the victim's credit card information, SMS, contacts and call records.

A new variant of Cerberus was detected in mid-January 2020. This version has undergone refactoring of the code base and updates of the C2 communication

[1] An overlay attack happens is when an attacker places a window over a legitimate application on the device so users interact with the attacker rather than their own device.

protocol, but most notably it got enhanced with the Remote Access Trojan (RAT) feature to perform fraud from the infected device, and enabling the stealing of a devices screen-lock credentials (PIN code or swipe pattern) and 2FA tokens from the Google Authenticator application. When the app is running, the Trojan can get the content of the interface and can send it to the C2 server.

The RAT service is able to traverse the file system of the device and download its contents. On top of that, it can also launch TeamViewer and setup connections to it, providing threat actor's full remote access of the device.
Once TeamViewer is working, it provides actors with many possibilities, including changing device settings, installing or removing apps, but most notably using any app on the device (such as banking apps, messengers and social network apps), it can also provide valuable insight into victim's behaviour and habits; in case it would be used for espionage purposes.

The feature enabling theft of device's screen lock credentials (PIN and lock pattern) is powered by a simple overlay that will require the victim to unlock the device.

Points of contact:	INTERPOL Cyber Fusion Centre INTERPOL General Secretariat, Command and Coordination Centre
E-mail:	INTERPOL Cyber Fusion Centre CFC@interpol.int (Internet) CFC@gs.igcs.int (I-24/7) INTERPOL General Secretariat, Command and Coordination Centre os-ccc@interpol.int (Internet) os-ccc@gs.igcs.int (I-24/7)
Telephone:	INTERPOL General Secretariat, Command and Coordination Centre + 33 4 72 44 76 76
Fax:	INTERPOL General Secretariat, Command and Coordination Centre + 33 4 72 44 71 63

Recommended precautionary action:
It is strongly recommended that you circulate this purple notice to your country's law enforcement bodies and CERT organizations to alert them about this modus operandi and to allow them to take whatever preventive and precautionary measures they deem necessary. All recipients are strongly encouraged to share data, and provide any investigative information relating to this modus operandi.

IPSG Reference: PN-20-0004