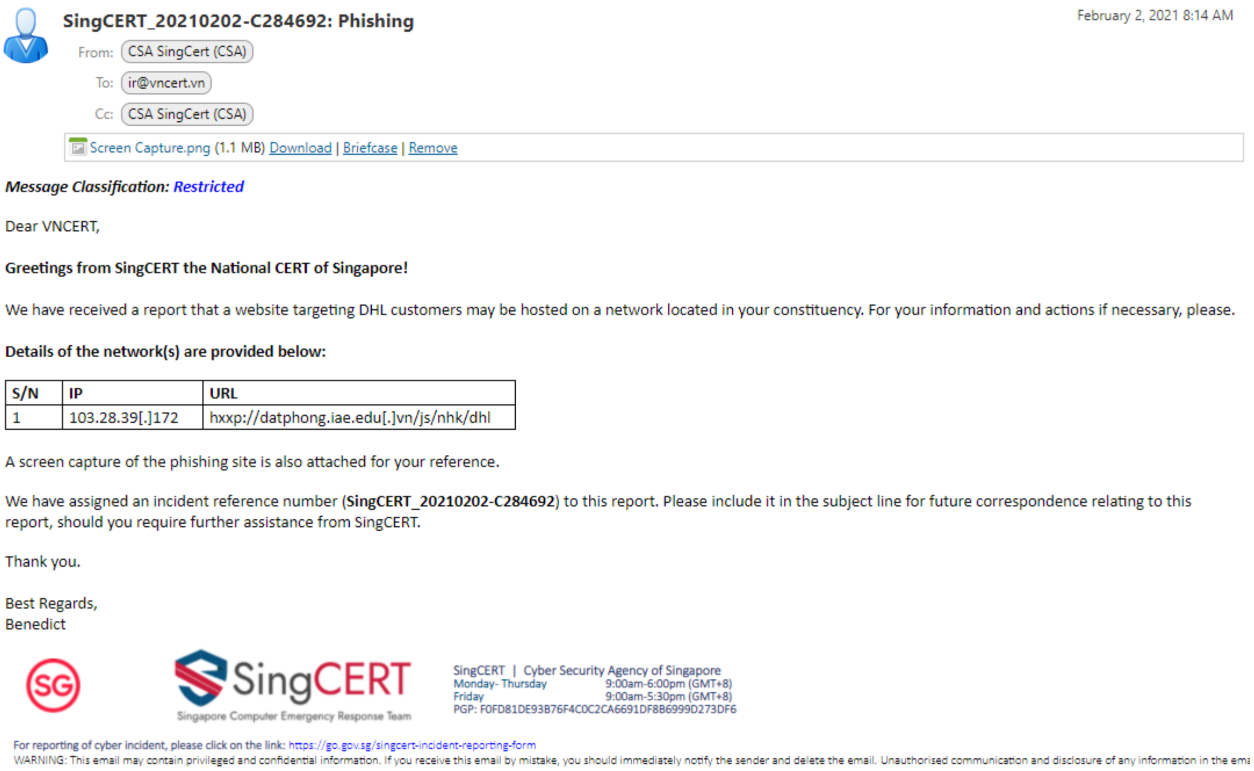
Information Sharing Brazil, ThaiCert email



SingCERT_20210202-C284692: Phishing

February 2, 2021 8:14 AM

From: CSA SingCert (CSA)

To: ir@vncert.vn

Cc: CSA SingCert (CSA)

Screen Capture.png (1.1 MB) Download | Briefcase | Remove

Message Classification:* *Restricted

Dear VNCERT,

Greetings from SingCERT the National CERT of Singapore!

We have received a report that a website targeting DHL customers may be hosted on a network located in your constituency. For your information and actions if necessary, please.

Details of the network(s) are provided below:

S/N	IP	URL
1	103.28.39[.]172	hxxp://datphong.iae.edu[.]vn/js/nhk/dhl

A screen capture of the phishing site is also attached for your reference.

We have assigned an incident reference number (**SingCERT_20210202-C284692**) to this report. Please include it in the subject line for future correspondence relating to this report, should you require further assistance from SingCERT.

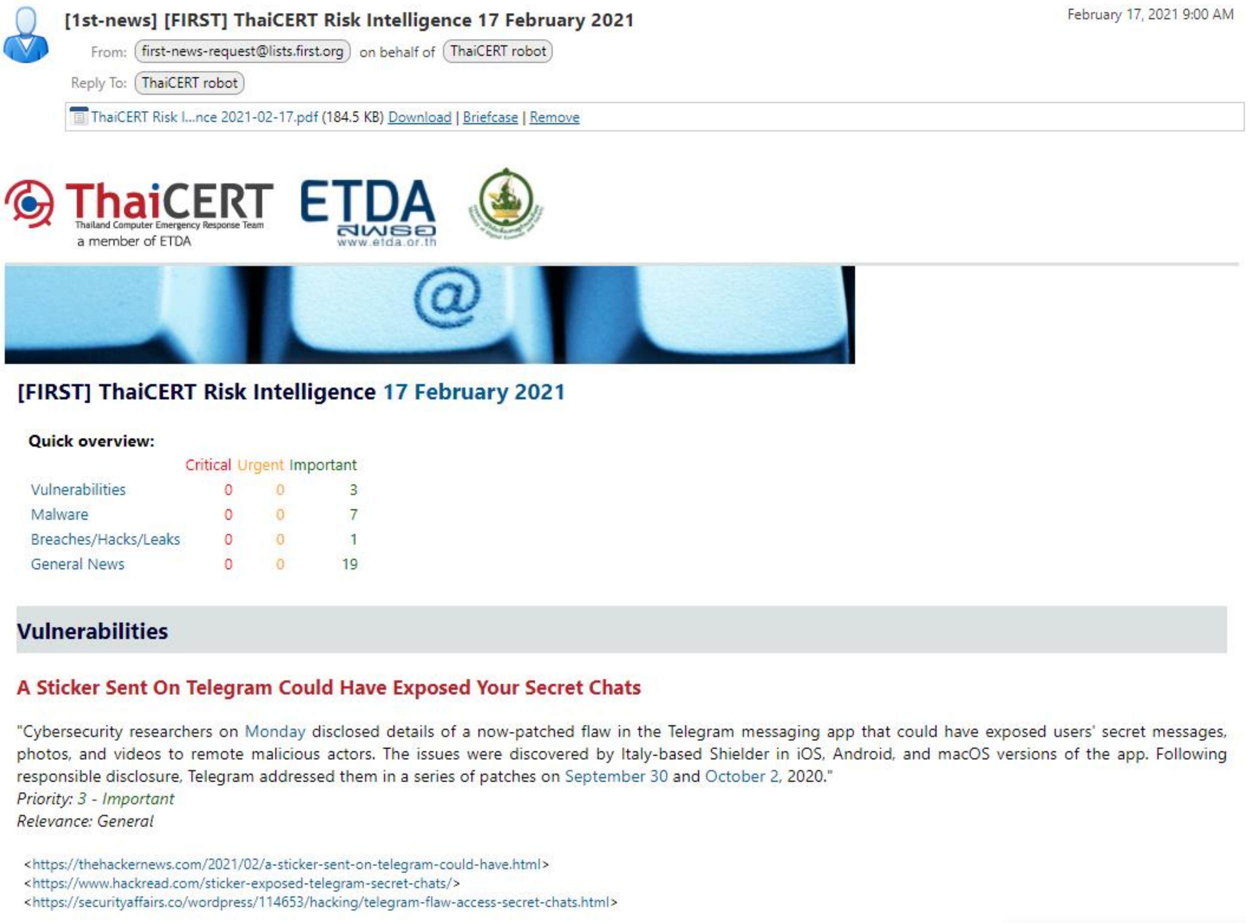
Thank you.

Best Regards,
Benedict

SingCERT
Singapore Computer Emergency Response Team

SingCERT | Cyber Security Agency of Singapore
Monday- Thursday 9:00am-6:00pm (GMT+8)
Friday 9:00am-5:30pm (GMT+8)
PGP: F0FD81DE93B76F4C0C2CA6691DF8B6999D273DF6

For reporting of cyber incident, please click on the link: https://go.gov.sg/singcert-incident-reporting-form
WARNING: This email may contain privileged and confidential information. If you receive this email by mistake, you should immediately notify the sender and delete the email. Unauthorised communication and disclosure of any information in the ema



[1st-news] [FIRST] ThaiCERT Risk Intelligence 17 February 2021

February 17, 2021 9:00 AM

From: first-news-request@lists.first.org on behalf of ThaiCERT robot

Reply To: ThaiCERT robot

ThaiCERT Risk I...nce 2021-02-17.pdf (184.5 KB) Download | Briefcase | Remove

ThaiCERT
Thailand Computer Emergency Response Team
a member of ETDA

ETDA
www.etda.or.th

[FIRST] ThaiCERT Risk Intelligence 17 February 2021

Quick overview:

	Critical	Urgent	Important
Vulnerabilities	0	0	3
Malware	0	0	7
Breaches/Hacks/Leaks	0	0	1
General News	0	0	19

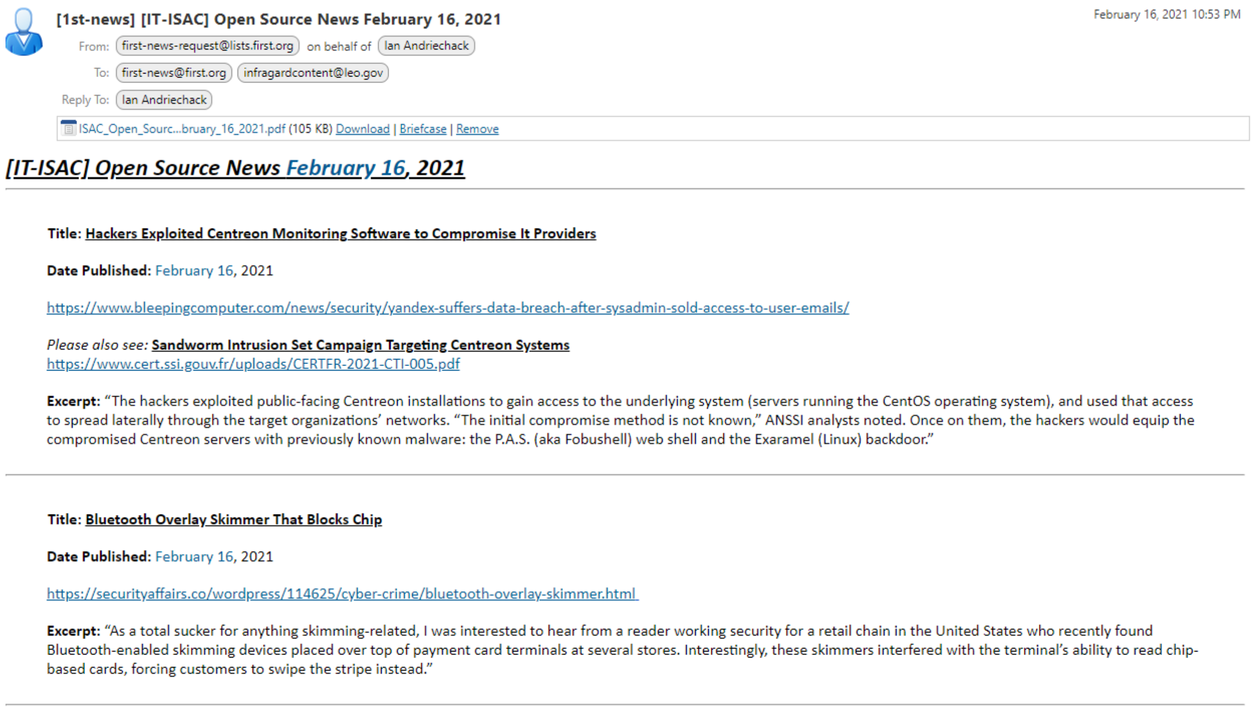
Vulnerabilities

A Sticker Sent On Telegram Could Have Exposed Your Secret Chats

"Cybersecurity researchers on Monday disclosed details of a now-patched flaw in the Telegram messaging app that could have exposed users' secret messages, photos, and videos to remote malicious actors. The issues were discovered by Italy-based Shielder in iOS, Android, and macOS versions of the app. Following responsible disclosure, Telegram addressed them in a series of patches on September 30 and October 2, 2020."
Priority: 3 - Important
Relevance: General

<https://thehackernews.com/2021/02/a-sticker-sent-on-telegram-could-have.html>
<https://www.hackread.com/sticker-exposed-telegram-secret-chats/>
<https://securityaffairs.co/wordpress/114653/hacking/telegram-flaw-access-secret-chats.html>

Information Sharing FIRST IT-ISAC email



[1st-news] [IT-ISAC] Open Source News February 16, 2021

February 16, 2021 10:53 PM

From: first-news-request@lists.first.org on behalf of Ian Andriechack

To: first-news@first.org infragardcontent@leo.gov

Reply To: Ian Andriechack

ISAC_Open_Sourc...bruary_16_2021.pdf (105 KB) Download | Briefcase | Remove

[IT-ISAC] Open Source News February 16, 2021

Title: **Hackers Exploited Centreon Monitoring Software to Compromise It Providers**

Date Published: February 16, 2021

https://www.bleepingcomputer.com/news/security/yandex-suffers-data-breach-after-sysadmin-sold-access-to-user-emails/

Please also see: **Sandworm Intrusion Set Campaign Targeting Centreon Systems**
https://www.cert.ssi.gouv.fr/uploads/CERTFR-2021-CTI-005.pdf

Excerpt: "The hackers exploited public-facing Centreon installations to gain access to the underlying system (servers running the CentOS operating system), and used that access to spread laterally through the target organizations' networks. "The initial compromise method is not known," ANSSI analysts noted. Once on them, the hackers would equip the compromised Centreon servers with previously known malware: the P.A.S. (aka Fobushell) web shell and the Exaramel (Linux) backdoor."

Title: **Bluetooth Overlay Skimmer That Blocks Chip**

Date Published: February 16, 2021

https://securityaffairs.co/wordpress/114625/cyber-crime/bluetooth-overlay-skimmer.html

Excerpt: "As a total sucker for anything skimming-related, I was interested to hear from a reader working security for a retail chain in the United States who recently found Bluetooth-enabled skimming devices placed over top of payment card terminals at several stores. Interestingly, these skimmers interfered with the terminal's ability to read chip-based cards, forcing customers to swipe the stripe instead."