OPERATIONS

3/10/2016
12:30 PM

# Hackers' Typo Foils Their $1 Billion Wire Transfer Heist

**Stolen credentials are no use without good spelling.**

Let this be a lesson in the importance of good editors. Attackers successfully breached Bangladesh Bank's systems and stole its credentials for payment transfers, yet the small typo they made in a wire transfer request ultimately undid their efforts to steal $1 billion.

As Reuters reports today, after obtaining the credentials, attackers "bombarded the Federal Reserve Bank of New York with nearly three dozen requests to move money from the Bangladesh Bank's account there to entities in the Philippines and Sri Lanka."

The first four transfers, totaling about $81 million, went through, but the fifth time:

> Hackers misspelled "foundation" in the NGO's name as "fandation," prompting a routing bank, Deutsche Bank, to seek clarification from the Bangladesh central bank, which stopped the transaction, one of the officials said.

This, plus the number and size of the transfers being sent to private entities instead of other banks raised the suspicions of The Fed. Although the initial $80 million was not recovered, between $850 to $870 million of attempted transactions were stopped.

Read more at Reuters.

*Dark Reading's Quick Hits delivers a brief synopsis and summary of the significance of breaking news events. For more information from the original source of the news item, please follow the link provided in this article. View Full Bio*

Dark Reading Staff
Quick Hits

6 COMMENTS
COMMENT NOW

Login
100% 0%

Like Tweet Share

COMMENT | EMAIL THIS | PRINT | RSS



## COMMENTS

NEWEST FIRST | OLDEST FIRST | THREADED VIEW

**zdondadaz,**
User Rank: Apprentice
6/3/2016 | 3:33:54 PM
Login 50% 50%

**Re: Irony is so bitter sweet**
Who's to say it wasn't a distraction? Keep them distracted with the 800 million transaction while they clear up loose ends and make off with the 80 million transaction... Yeah, I don't think it was a mistake.. Pople that hack into banks and steal 80mil DON'T MAKE MISTAKES.

REPLY | POST MESSAGE | MESSAGES LIST | START A BOARD

**KeithB787,**
User Rank: Apprentice
3/11/2016 | 5:56:11 PM
Login 50% 50%

**Irony is so bitter sweet**
People tend to say that only death and taxes are constant. It seems like irony is another given. At least I've seen it many times in the past and continue to see it, even today. It's definitely ironic that the hackers probably spent a lot of time to figure out exactly how to hack into the Bangladesh bank only to see a significant portion of their efforts wasted due to a spelling mistake. In addition, it seems strange that while the bank's network was breached through a Hi-Tech exploit, a simple low tech request for spelling clarification/validation resulted in foiling a significant financial portion of the plot.

REPLY | POST MESSAGE | MESSAGES LIST | START A BOARD

**RyanSepe,**
User Rank: Ninja
3/11/2016 | 2:47:25 PM
Login 50% 50%

**Group**
I know this fairly new but has this been tracked to a group/individual or has there been any data scraped to suggest origin of the attack?

REPLY | POST MESSAGE | MESSAGES LIST | START A BOARD

**RyanSepe,**
User Rank: Ninja
3/11/2016 | 2:45:43 PM
Login 50% 50%

**Re: c'mon...makes you think that their cat jumped on the keyboard. I wonder how many times those furry critters foil plans like this seriously.**
You think that they would do a much stricter job of spell checking when trying to exfiltrate hundreds of millions.

REPLY | POST MESSAGE | MESSAGES LIST | START A BOARD

**Kelly Jackson Higgins,**
User Rank: Strategist
3/11/2016 | 7:35:20 AM
Login 100% 0%

**Re: c'mon...makes you think that their cat jumped on the keyboard. I wonder how many times those furry critters foil plans like this seriously.**
Stupid hacker tricks.

REPLY | POST MESSAGE | MESSAGES LIST | START A BOARD

**hewenthatway,**
User Rank: Strategist
3/11/2016 | 3:50:51 AM
Login 50% 50%

**c'mon...makes you think that their cat jumped on the keyboard. I wonder how many times those furry critters foil plans like this seriously.**
c'mon...makes you think that their cat jumped on the keyboard. I wonder how many times those furry critters foil plans like this seriously.

REPLY | POST MESSAGE | MESSAGES LIST | START A BOARD

HOT TOPICS | EDITORS' CHOICE

**Many Ransomware Attacks Can be Stopped Before They Begin** (3)
Jai Vijayan, Contributing Writer, 3/17/2020

**This Tax Season, Save the Scorn and Protect Customers from Phishing Scams** (2)
Dr. Salvatore Stolfo, Founder & CTO, Allure Security, 3/17/2020

**Fewer Vulnerabilities in Web Frameworks, but Exploits Remain Steady** (1)
Robert Lemos, Contributing Writer, 3/16/2020



TWITTER FEED

BUG REPORT

ENTERPRISE VULNERABILITIES
From DHS/US-CERT's National Vulnerability Database

- **CVE-2019-14872**
  PUBLISHED: 2020-03-19
  The _dtoa_r function of the newlib libc library, prior to version 3.3.0, performs multiple memory allocations without checking their return value. This could result in NULL pointer dereference.
- **CVE-2019-20485**
  PUBLISHED: 2020-03-19
  qemu/qemu_driver.c in libvirt before 6.0.0 mishandles the holding of a monitor job during a query to a guest agent, which allows attackers to cause a denial of service (API blockage).
- **CVE-2019-19677**
  PUBLISHED: 2020-03-18
  arxes-tolina 3.0.0 allows User Enumeration.
- **CVE-2019-19676**
  PUBLISHED: 2020-03-18
  A CSV injection in arxes-tolina 3.0.0 allows malicious users to gain remote control of other computers. By entering formula code in the following columns: Kundennummer, Firma, Street, PLZ, Ort, Zahlziel, and Bemerkung, an attacker can create a user with a name that contains malicious code. Other use...
- **CVE-2020-10365**
  PUBLISHED: 2020-03-18
  LogicalDoc before 8.3.3 allows SQL Injection. LogicalDoc populates the list of available documents by querying the database. This list could be filtered by modifying some of the parameters. Some of them are not properly sanitized which could allow an authenticated attacker to perform arbitrary queri...