GNCIRT ALERT # 3: Business E-Mail Compromised

Date: 30th May, 2016

Affected Parties

- **All Business E-mail Users**

Overview

The Guyana National Computer Incident Response Team (GNCIRT) has been made aware of an increasing number of Business E-Mail Compromise (BEC) attacks being experienced by local businesses and agencies transacting businesses online, via e-mail.

This type of attack is also known by different names such as "Wire Transfer Scam / Fraud", "E-Mail Interception Fraud" and "Man in the E-Mail."

Description

Business E-Mail Compromise is an international fraud targeting businesses and agencies usually interacting with foreign suppliers. This type of attack is usually carried out by intercepting e-mail communications, where the attackers manipulate invoices and change the banking information for wire transfer payments. Unsuspecting employees conducting business with long established suppliers are deceived out of large sums of money/funds.

This type of attack is on the rise globally (please see links below)and has resulted in actual losses and attempted frauds of thousands of (United States) dollars locally.

Characteristics of BEC Incidents reported to CIRT:

Spoofed emails addresses are very similar to legitimate email addresses. Two examplesof the legitimate and fraudulent addresses are shown below.

Legitimate	Johndoe@guyana.gy
Fraudulent	John.doe@guyana.gy

Legitimate	Sallysmith@company.com
Fraudulent	Sallysmith@gmail.com

Fraudulent e-mail requests are similar to normal business transactions and attackers are familiar with names and designations of company personnel. This is a targeted attack, as attackers usually gather information about their intended victims. This information include knowledgeof the procurement process and payment details of the entities they are attacking. These attackers are so deceptive that Businesses are typically not aware of the fraud until their suppliers follow up on the status of their payment.

Suggestions for protection:

- Double check to confirm that e-mail addresses and banking information are correct
- Forward vs Reply: Do not use the Reply option to respond. Instead, use the Forward option and either type in the correct email address or select it from the email address book to ensure the intended recipient's correct email address is used.
- Use communication outside the email environment to avoid interception by hackers: Establish other communication channels such as telephone calls to verify significant transactions.
- Be extra-careful when processing changes to pertinent information (such as Bank Accounts) and cross check with existing contacts through pre-established channels.

GNCIRT recommends the following steps be taken to mitigate the impact if infected:

- Change passwords of all compromised e-mail accounts
- Contact all banks and financial agencies that maybe linked to the compromised e-mail addresses and inform them of pertinent information about the situation.
- Contact all suppliers and business associates that you communicate with via the compromised e-mail address and inform them of the situation.
- Contact all contacts that you communicate with via the compromised e-mail address and inform them of the situation. Use this time to provide them with an alternate means of communication such a fax number and / or another email address.
- Call GNCIRT, to report such incidents.

For further information, please visit:

1- **Federal Bureau of Investigation**
https://www.fbi.gov/phoenix/press-releases/2016/fbi-warns-of-dramatic-increase-in-business-e-mail-scams

2- **Symantec**
http://www.symantec.com/connect/blogs/business-email-compromise-campaigns-continue-targeting-c-level-employees-despite-warnings

3- **Trend Micro**
http://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/business-email-compromise-bec-schemes