GNCIRT Press Release

Reference: GNCIRT ALERT 2016-01

May 31, 2016

The Guyana National Computer Response Incident Team (GNCIRT) wishes to alert the general public of the rise in Business E-Mail Compromise (BEC) attacks being perpetrated on local business and agencies, transacting businesses online, via e-mail. In particular, transactions that involved wire transfers payments of invoices from suppliers.

Background

This type of attack is also known by different technical jargons, such as: “Man in the e-mail”, “Wire Transfer Fraud” and “E-mail Interception Fraud”, to name a few.

These recent attacks in Guyana are not new, as they are very prevalent around the world. As the use of Business Services, offered through the Internet, increases, so too are the associated risks. The Internet has made business-to-business transactions much more simplified and impersonal, but in doing so, has increased the risk of businesses becoming victims to fraudulent transactions. It is therefore necessary that more diligence and security-consciousness are required when conducting online business.

BEC is an international scam, targeting businesses and agencies conducting business-to-business transactions, using e-mails. This type of attack is usually carried out by first gathering information on the intended victims, and then use the information to intercept e-mail communications, pretending to act on behalf of legitimate business entities. Hence the name, “Man-in-the-e-mail”. In this type of attack, cybercriminals usually create domain names that are similar to the domain name of the company they intend to disguise as.

Example of these domain names are:

Legitimate domain	supligin.com
Fraudulent domain	suplegin.com or supligini.com or suppligin.com

Typical Approach

Cybercriminals also use the information gathered to determine how payments to suppliers are done and who are the key personnel involved. They subsequently use this information to manipulate invoices or wire transfer details. An e-mail will then be sent to the unsuspecting buyer, stating the changes in the details.

A typical e-mail correspondence will be as shown below:

Subject: Changes to Bank Transfer Details
From: johnsmith@suplegin.com
To: marysingh@unsuspectedcompany.com

Dear Mary

Please note the changes to the payment details. As from today, May 30, 2016, all payments for Supligin should be made to the bank account information shown below:

BANK NAME: Some Bank
BANK ADDRESS: Some address
SWIFT CODE: XOXOXOX
IBAN NUMBER: ADAD SDSD CDCD XOXO
BENEFICIARY NAME: Some company name
ADDRESS: Some beneficiary address

Thanks for your cooperation.

Regards
John Smith
Senior Financial Manager (ag)
SUPLIGIN

Also, it is not uncommon for perpetrators of this type of attack to use forged letterheads and forward correspondences, with forged signatures of key personnel, to convince their intended victims that these changes are legitimate.

Consequences

Businesses are usually not aware of this type of attack until they are contacted by the legitimate suppliers to follow-up on the status of their payments. It is only then that they realize that a fraud has been committed. More so, this type of attack constitutes a serious threat to the way business is done around the world and, by extension, the cost effectiveness of businesses and the growth of the local economy, as funds lost to international criminal networks are more than often irredeemable.

However, on the bright side, some businesses have been able to detect these cunning deceptions and, as such, halt the processing of payments and scrutinized every business transaction, to ensure legitimacy. Nonetheless, it is regrettable that businesses do not usually use the opportunity to gather information on the attackers with the intention to prosecute these criminals to the full extent of the law.

Recommendations

It is advised that due diligence must be taken to ensure that changes in transaction details are done with the right authorization and with persons that are known business associates. The most stringent scrutiny must be applied, as failure to be thorough may be consequential.

It is therefore imperative that persons and organizations be made aware of the risks involved in conducting business-to-business transactions over the Internet, especially when doing so impersonally, via e-mails.

Guyana is now in the process of enacting legislations governing cybercrimes (Cybercrime Act of 2016). It is therefore advised that such incidents be reported to the Guyana Police Force and the Guyana National Computer Incident Response Team before these criminals are alerted, so that evidence can be collected, preserved and presented in court, in an effort to bring these criminals to justice.