INNOVATIVE SOLUTIONS

Date: 16-5-2017

EXECUTIVE SUMMARY

On the **16th May 2017 at 5:31 PM** Innovative Solutions Managed Security Services (MSS) received information on a new wave of attacks that involved sending Phishing emails to multiple clients. The malicious email had the subject of "*Aramco Top Urgent RFQ 4202283220*". A 1 MB Microsoft Word file was also attached to with malicious email titled "*Print Out.doc*".

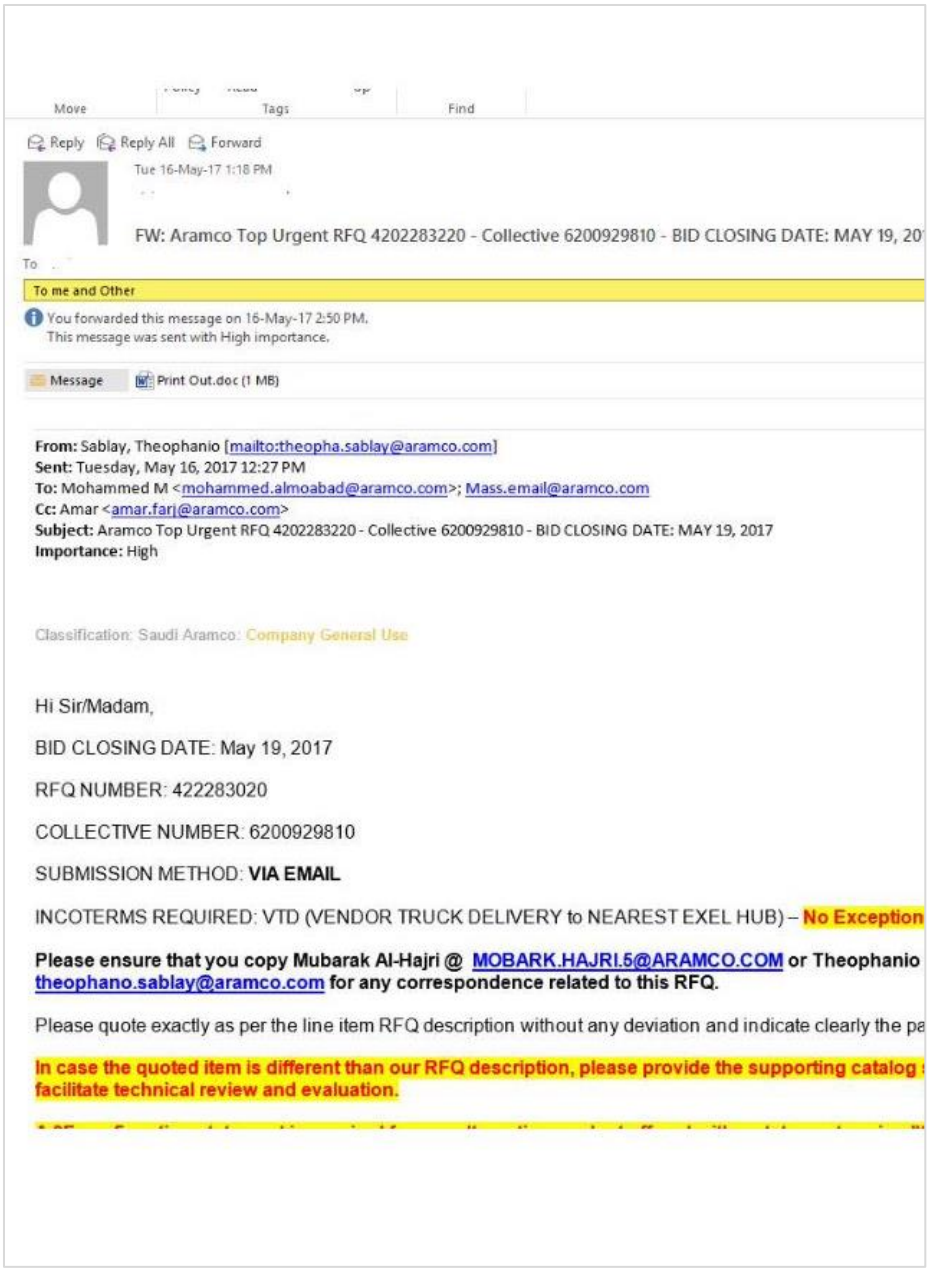
The MSS team was able to immediately block the threat using Innovative Solutions state-of-the-art Managed Endpoint Protection Service. This prompt response ensured that the file is completely banned from being executed at clients' environments.

Further details will be shared as we receive further information and sample for analysis.

Details	
FILE Name	Print Out.doc
MD5 Hash Identifier	26DEDC60B7EB64F59012F473AA9694ED
SHA-1 Hash Identifier	E2483D5DD4E030978152AB5DA95A9B9CA2C1BEDE
SHA-256 Hash Identifier	A5FD22029110E5C42DC4136BF8E31435EE7A55639DA07020721 EA19F71E24 A78
Action Taken	**BLOCKED**
Present Network Status	**SECURED**
Association to Attack Campaign	Currently Unknown
Malware Behavior	Currently Unknown

Initial findings:

- Email is spoofed.
- Attachment is a MS word document with obfuscated macro.
- Macro calls a compromised Saudi domain that is now used as a malware download point www . alkhalaf-group.com / Cc / [[words.exe]]
- The executable file (.exe) is identified as Trojan.Win32.AutoIt that was first identified in 2003.
- It's very much like AgentTesla in harvesting access credentials for various apps.



Move Tags Find

Reply Reply All Forward

Tue 16-May-17 1:18 PM

FW: Aramco Top Urgent RFQ 4202283220 - Collective 6200929810 - BID CLOSING DATE: MAY 19, 20

To

To me and Other

You forwarded this message on 16-May-17 2:50 PM.
This message was sent with High importance.

Message Print Out.doc (1 MB)

From: Sablay, Theophanio [mailto:theopha.sablay@aramco.com]
Sent: Tuesday, May 16, 2017 12:27 PM
To: Mohammed M <mohammed.almoabad@aramco.com>; Mass.email@aramco.com
Cc: Amar <amar.farj@aramco.com>
Subject: Aramco Top Urgent RFQ 4202283220 - Collective 6200929810 - BID CLOSING DATE: MAY 19, 2017
Importance: High

Classification: Saudi Aramco: Company General Use

Hi Sir/Madam,

BID CLOSING DATE: May 19, 2017

RFQ NUMBER: 422283020

COLLECTIVE NUMBER: 6200929810

SUBMISSION METHOD: **VIA EMAIL**

INCOTERMS REQUIRED: VTD (VENDOR TRUCK DELIVERY to NEAREST EXEL HUB) – **No Exception**

Please ensure that you copy Mubarak Al-Hajri @ MOBARK.HAJRI.5@ARAMCO.COM or Theophanio theophano.sablay@aramco.com for any correspondence related to this RFQ.

Please quote exactly as per the line item RFQ description without any deviation and indicate clearly the pa

In case the quoted item is different than our RFQ description, please provide the supporting catalog facilitate technical review and evaluation.

Figure 1: Screenshot of the malicious email