Tales from the Trenches: Loki Bot Malware

phishme.com/loki-bot-malware/

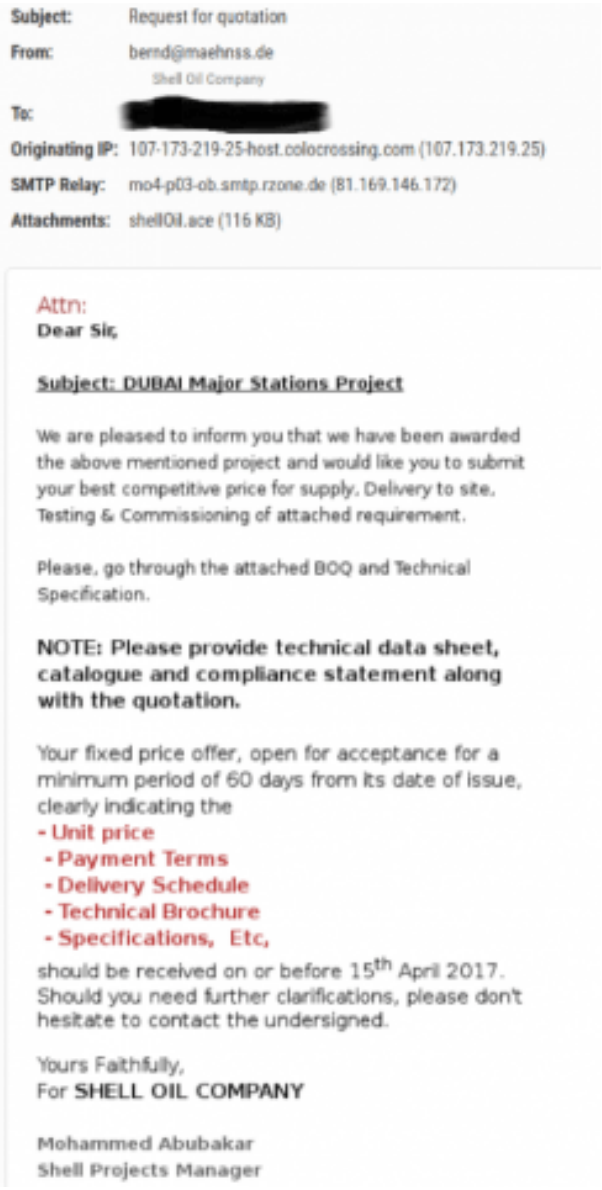
Cofense March 23, 2017

On March 15, 2017, our Phishing Defense Center observed several emails with the subject line “Request for quotation” pretending to award Shell Oil Company contracts – a very targeted subject tailored to the receiver. As with most phishing emails, there is a compelling call to action for the receiver, in this case a contract award from a well-known organization. And, an added bonus unknown to the receiver, the emails also contained a malicious attachment designed to siphon data from its targets.
Included is an example of one of these emails along with basic Triage header information.

Each email analyzed contained instructions to open an attached .ace archive file that when decompressed revealed a Windows executable containing Loki Bot Malware.

Loki Bot is a commodity **malware** sold on underground sites which is designed to steal private data from infected machines, and **then** submit that info to a command and control host via HTTP POST. This private data includes stored passwords, login credential information from Web browsers, and a variety of cryptocurrency wallets.

The following Loki Bot executable was identified during our analysis.



Subject: Request for quotation
From: bernd@maehnss.de
Shell Oil Company
To: [redacted]
Originating IP: 107-173-219-25-host.colocrossing.com (107.173.219.25)
SMTP Relay: mo4-p03-ob.smtp.rzone.de (81.169.146.172)
Attachments: shellOil.ace (116 KB)

Attn:
Dear Sir,

Subject: DUBAI Major Stations Project

We are pleased to inform you that we have been awarded the above mentioned project and would like you to submit your best competitive price for supply, Delivery to site, Testing & Commissioning of attached requirement.

Please, go through the attached BOQ and Technical Specification.

NOTE: Please provide technical data sheet, catalogue and compliance statement along with the quotation.

Your fixed price offer, open for acceptance for a minimum period of 60 days from its date of issue, clearly indicating the
- Unit price
- Payment Terms
- Delivery Schedule
- Technical Brochure
- Specifications, Etc,

should be received on or before 15th April 2017. Should you need further clarifications, please don't hesitate to contact the undersigned.

Yours Faithfully,
For **SHELL OIL COMPANY**

Mohammed Abubakar
Shell Projects Manager

Filename	MD5	Size
shellOil.ace	5d70858b154c8b0eb205e84ca7f27a04	118,473
Shell Oil.exe	6a95ae2c90a4a3c5a2c1ce3eaf399966	245,760

Upon infecting a machine, this malware performs a callback to the following command and control host reporting the new infection and submitting any private data stolen during the infection process.

Command and Control URL	IP Address	Location
hxxp://elmansy.net/pdf/fre.php	118.193.173.208	China

The command and control domain ‘elmansy.net’ was created almost exactly a year ago on 2016-03-18 with the email address sherif-elfmanns The IP address reveals that the domain is being hosted out of Jiangsu, China.

Take Away

As always, PhishMe cautions our customers to be wary of emails requesting information or promising reward. Specific to this sample, we recommend that customers be observant for emails containing the subject line “Request for quotation” or emails promising business with new or unknown businesses. PhishMe Simulator customers who feel this type of offer might be successful with its employees should consider launching simulations that follow this style of attack to further train their users.

Additionally, incident responders should consider blocking the domain and IP address mentioned above, as well as searching endpoint systems for the MD5’s if internal systems support it.

The Phishing Defense Center is the hub for our remotely managed PhishMe Triage services. The fully staffed center manages all internal reported emails for a number of organizations. All information shared has been cleansed of any identifiable data.

Don't miss out on any of our phishing updates! Subscribe to our blog.