Loki Bot: On a hunt for corporate passwords

SL securelist.com/loki-bot-stealing-corporate-passwords/87595/

Spam and phishing mail

Spam and phishing mail

29 Aug 2018

minute read

Authors

Tatyana Shcherbakova

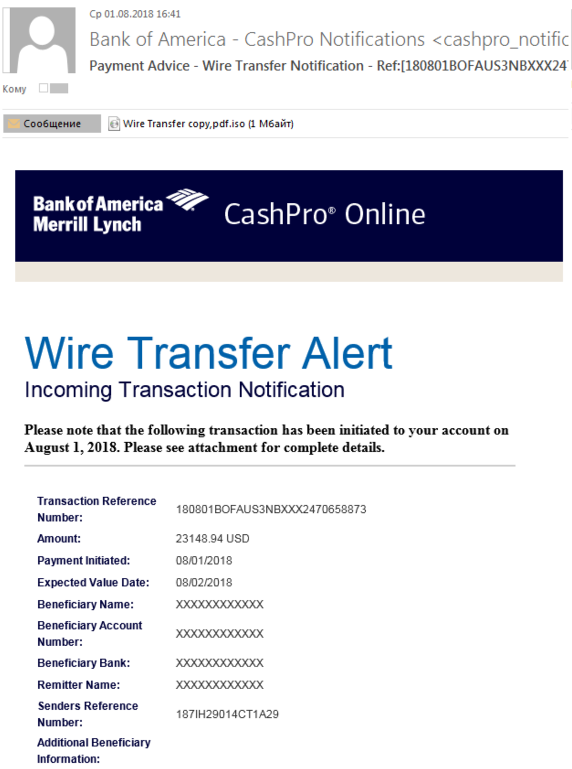
Starting from early July, we have seen malicious spam activity that has targeted corporate mailboxes. The messages discovered so far contain an attachment with an .iso extension that Kaspersky Lab solutions detect as Loki Bot. The malware's key objective is to steal passwords from browsers, messaging applications, mail and FTP clients, and cryptocurrency wallets. Loki Bot dispatches all its loot to the malware owners.

ISO images are copies of optical discs that can be mounted in a virtual CD/DVD drive to be used in the same way as the originals. Whereas in days of yore users needed dedicated software to open this type of image, today's operating systems support the format out of the box, and if you want to access the contents of the file, all you need to do is double-click. Malicious spam uses this type of file as a container for delivering malware, albeit rarely.

As mentioned above, hackers were sending out copies of Loki Bot to company email addresses that could be obtained from public sources or from the companies' own websites.

The emailed messages were notably diverse:

1. Fake notifications from well-known companies



Ср 01.08.2018 16:41

Bank of America - CashPro Notifications <cashpro_notific

Payment Advice - Wire Transfer Notification - Ref:[180801BOFAUS3NBXXX24

Кому □ [redacted]

Сообщение | Wire Transfer copy,pdf.iso (1 Мбайт)

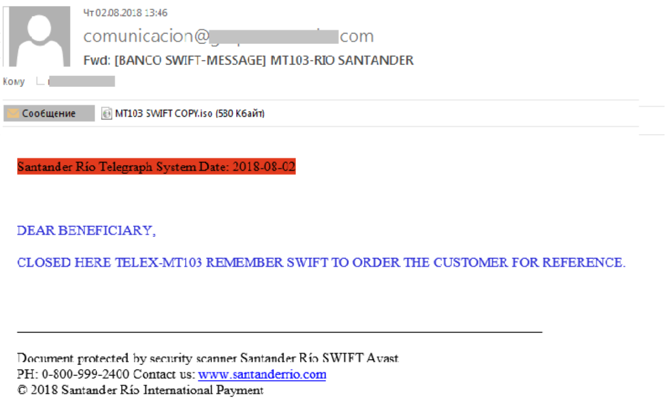
Bank of America Merrill Lynch CashPro® Online

Wire Transfer Alert

Incoming Transaction Notification

Please note that the following transaction has been initiated to your account on August 1, 2018. Please see attachment for complete details.

Transaction Reference Number:	180801BOFAUS3NBXXX2470658873
Amount:	23148.94 USD
Payment Initiated:	08/01/2018
Expected Value Date:	08/02/2018
Beneficiary Name:	XXXXXXXXXXXX
Beneficiary Account Number:	XXXXXXXXXXXX
Beneficiary Bank:	XXXXXXXXXXXX
Remitter Name:	XXXXXXXXXXXX
Senders Reference Number:	187IH29014CT1A29
Additional Beneficiary Information:	



Чт 02.08.2018 13:46

comunicacion@[redacted]com

Fwd: [BANCO SWIFT-MESSAGE] MT103-RIO SANTANDER

Кому [redacted]

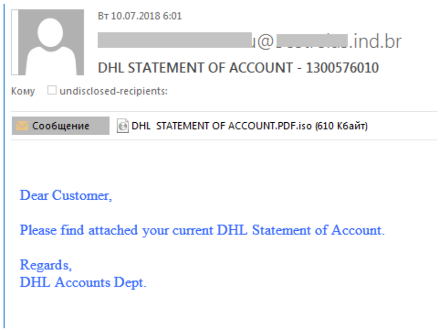
Сообщение | MT103 SWIFT COPY.iso (530 Кбайт)

Santander Río Telegraph System Date: 2018-08-02

DEAR BENEFICIARY,

CLOSED HERE TELEX-MT103 REMEMBER SWIFT TO ORDER THE CUSTOMER FOR REFERENCE.

Document protected by security scanner Santander Río SWIFT Avast
PH: 0-800-999-2400 Contact us: www.santanderrio.com
© 2018 Santander Río International Payment



Вт 10.07.2018 6:01

[redacted]u@[redacted].ind.br

DHL STATEMENT OF ACCOUNT - 1300576010

Кому □ undisclosed-recipients:

Сообщение | DHL STATEMENT OF ACCOUNT.PDF.iso (610 Кбайт)

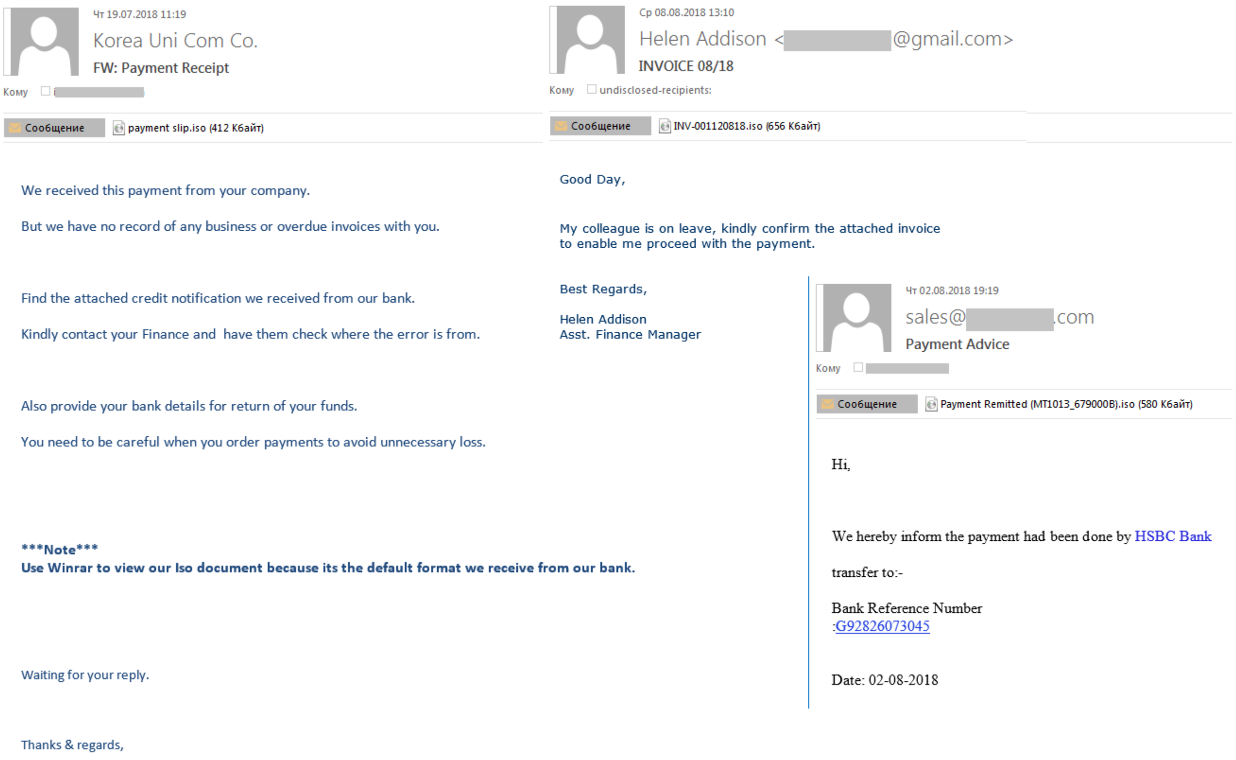
Dear Customer,

Please find attached your current DHL Statement of Account.

Regards,
DHL Accounts Dept.

Imitating messages from well-known corporations is one of the most popular tricks in the hackers’ arsenal. Interestingly enough, fake emails used to be directed mostly at common users and customers, whereas now companies are increasingly the target.

1. Fake notifications containing financial documents



Korea Uni Com Co.

FW: Payment Receipt

Кому [redacted]

payment slip.iso (412 Кбайт)

We received this payment from your company.

But we have no record of any business or overdue invoices with you.

Find the attached credit notification we received from our bank.

Kindly contact your Finance and have them check where the error is from.

Also provide your bank details for return of your funds.

You need to be careful when you order payments to avoid unnecessary loss.

*****Note*****
Use Winrar to view our Iso document because its the default format we receive from our bank.

Waiting for your reply.

Thanks & regards,

Helen Addison <[redacted]@gmail.com>

INVOICE 08/18

Кому undisclosed-recipients:

INV-001120818.iso (656 Кбайт)

Good Day,

My colleague is on leave, kindly confirm the attached invoice
to enable me proceed with the payment.

Best Regards,

Helen Addison
Asst. Finance Manager

sales@[redacted].com

Payment Advice

Кому [redacted]

Payment Remitted (MT1013_679000B).iso (580 Кбайт)

Hi,

We hereby inform the payment had been done by HSBC Bank

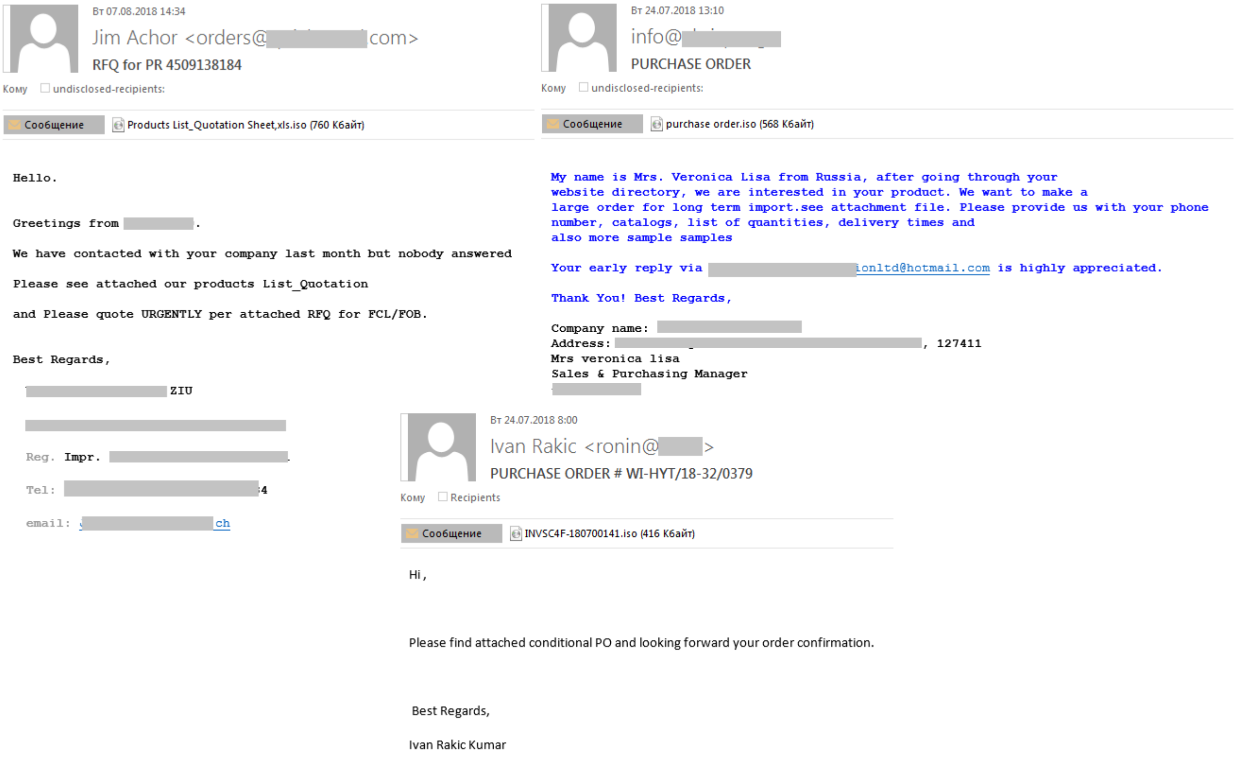
transfer to:-

Bank Reference Number
:G92826073045

Date: 02-08-2018

The scammers passed off malicious files as financial documents: invoices, transfers, payments, etc. This is a fairly popular malicious spamming technique, with the message body usually no more than a few lines and the subject mentioning what exactly is purported to be attached.

1. Fake orders or offers



Вт 07.08.2018 14:34

Jim Achor <orders@[redacted]com>

RFQ for PR 4509138184

Кому □ undisclosed-recipients:

Сообщение | Products List_Quotation Sheet,xls.iso (760 Кбайт)

```
Hello.

Greetings from [redacted].

We have contacted with your company last month but nobody answered

Please see attached our products List_Quotation

and Please quote URGENTLY per attached RFQ for FCL/FOB.

Best Regards,

  [redacted] ZIU

  [redacted]

  Reg. Impr. [redacted]

  Tel: [redacted]4

  email: [redacted]ch
```

Вт 24.07.2018 13:10

info@[redacted]

PURCHASE ORDER

Кому □ undisclosed-recipients:

Сообщение | purchase order.iso (568 Кбайт)

```
My name is Mrs. Veronica Lisa from Russia, after going through your
website directory, we are interested in your product. We want to make a
large order for long term import.see attachment file. Please provide us with your phone
number, catalogs, list of quantities, delivery times and
also more sample samples

Your early reply via [redacted]ionltd@hotmail.com is highly appreciated.

Thank You! Best Regards,

Company name: [redacted]
Address: [redacted], 127411
Mrs veronica lisa
Sales & Purchasing Manager
[redacted]
```

Вт 24.07.2018 8:00

Ivan Rakic <ronin@[redacted]>

PURCHASE ORDER # WI-HYT/18-32/0379

Кому □ Recipients

Сообщение | INVSC4F-180700141.iso (416 Кбайт)

Hi ,

Please find attached conditional PO and looking forward your order confirmation.

Best Regards,

Ivan Rakic Kumar

Phishers may pose as customers placing an order, or a vendor offering their goods or services.

Every year we observe an increase in spam attacks on the corporate sector. The perpetrators have used phishing and malicious spam, including forged business emails, in their pursuit of confidential corporate information: intellectual property, authentication data, databases, bank accounts, etc. That's why today it's essential for corporate security measures to include both technical protection and training for employees, because their actions may cause irreparable damage to the business.

- Phishing
- Spam Letters
- Spammer techniques

Authors

Expert Tatyana Shcherbakova

Loki Bot: On a hunt for corporate passwords

Your email address will not be published. Required fields are marked *

GReAT webinars

13 May 2021, 1:00pm

GReAT Ideas. Balalaika Edition

26 Feb 2021, 12:00pm
17 Jun 2020, 1:00pm
26 Aug 2020, 2:00pm
22 Jul 2020, 2:00pm
From the same authors

Spam and phishing in Q1 2020

Every little bitcoin helps

The Rio Olympics: Scammers Already Competing

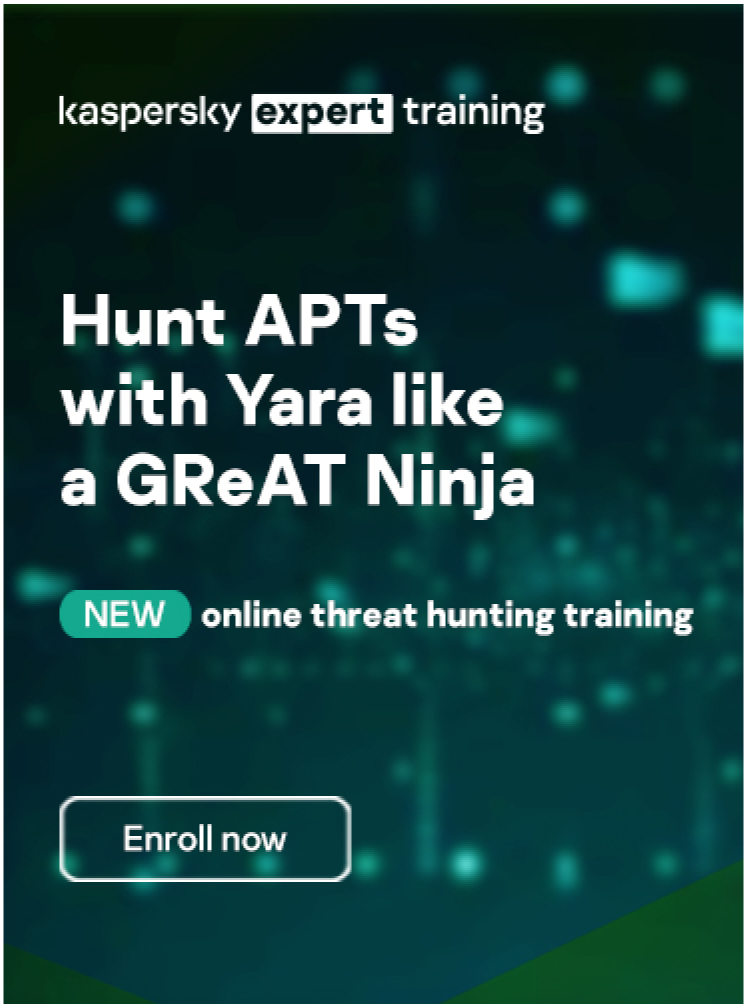
[Spammers all geared up for Euro 2016!]

[Arabian tales by ‘Nigerians’]

Subscribe to our weekly e-mails

The hottest research right in your inbox

-


kaspersky expert training
Hunt APTs with Yara like a GReAT Ninja
NEW online threat hunting training
Enroll now

Reports

APT trends report Q1 2022

This is our latest summary of advanced persistent threat (APT) activity, focusing on events that we observed during Q1 2022.

Lazarus Trojanized DeFi app for delivering malware

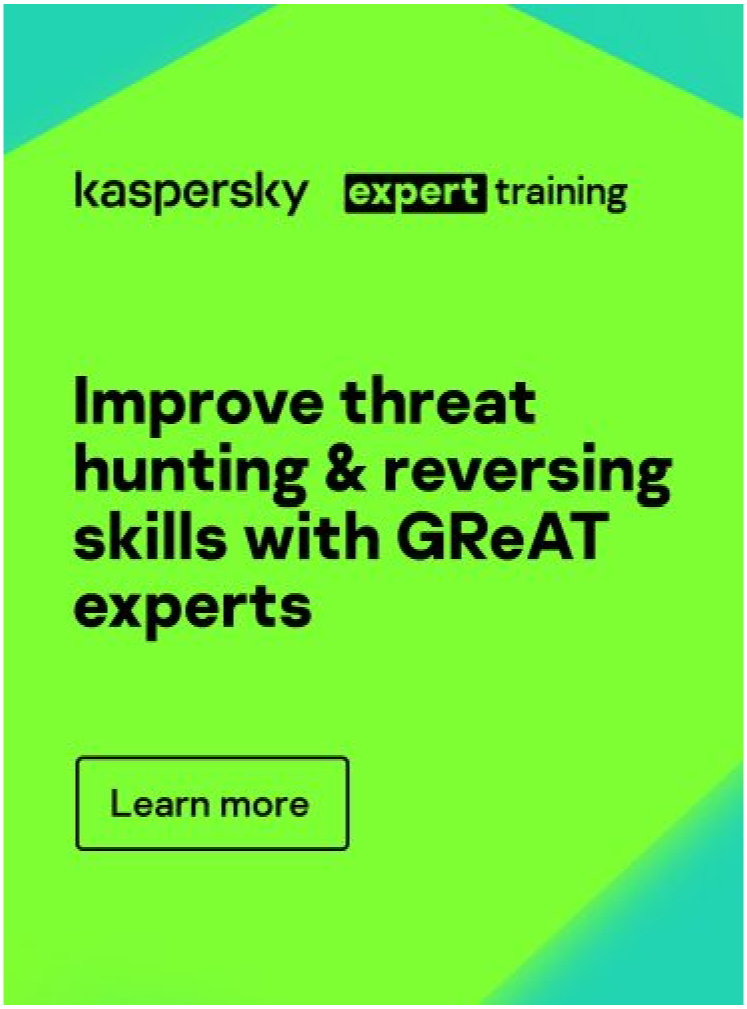
We recently discovered a Trojanized DeFi application that was compiled in November 2021. This application contains a legitimate program called DeFi Wallet that saves and manages a cryptocurrency wallet, but also implants a full-featured backdoor.

MoonBounce: the dark side of UEFI firmware

At the end of 2021, we inspected UEFI firmware that was tampered with to embed a malicious code we dub MoonBounce. In this report we describe how the MoonBounce implant works and how it is connected to APT41.

The BlueNoroff cryptocurrency hunt is still on

It appears that BlueNoroff shifted focus from hitting banks and SWIFT-connected servers to solely cryptocurrency businesses as the main source of the group's illegal income.



Subscribe to our weekly e-mails

The hottest research right in your inbox