

Loki Bot: On a hunt for corporate passwords

By Tatyana Shcherbakova

Published: 2018-08-29 · Archived: 2026-04-05 14:28:22 UTC



[Spam and phishing](#)

[Spam and phishing](#)

29 Aug 2018

1 minute read



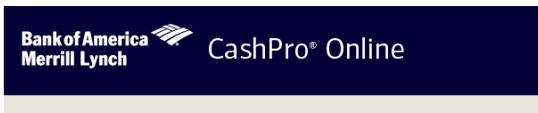
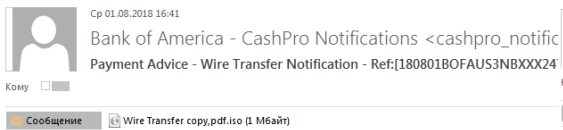
Starting from early July, we have seen malicious spam activity that has targeted corporate mailboxes. The messages discovered so far contain an attachment with an .iso extension that Kaspersky Lab solutions detect as Loki Bot. The malware's key objective is to steal passwords from browsers, messaging 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. 1 Fake notifications from well-known companies



Santander Rio Telegraph System Date: 2018-08-02

DEAR BENEFICIARY,

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

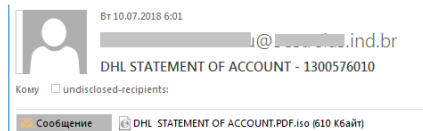
Wire Transfer Alert

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: XXXXXXXXXXXXX
 Beneficiary Account Number: XXXXXXXXXXXXX
 Beneficiary Bank: XXXXXXXXXXXXX
 Remitter Name: XXXXXXXXXXXXX
 Senders Reference Number: 187IH29014CT1A29
 Additional Beneficiary Information:

Document protected by security scanner Santander Rio SWIFT Avast
 PH: 0-800-599-2400 Contact us: www.santanderrio.com
 © 2018 Santander Rio International Payment



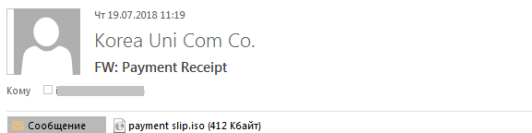
Dear Customer,

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.

2. 2 Fake notifications containing financial documents



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.

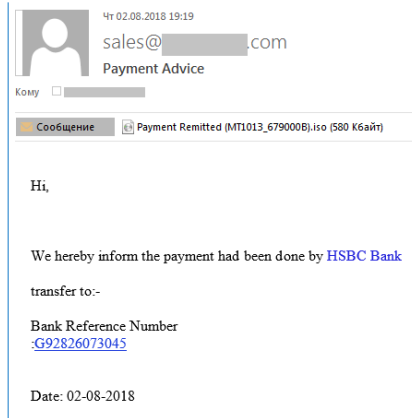
Good Day,
 My colleague is on leave, kindly confirm the attached invoice to enable me proceed with the payment.

Best Regards,
 Helen Addison
 Asst. Finance Manager

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

Waiting for your reply.

Thanks & regards,



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.

3. 3 Fake orders or offers

By 07.08.2018 14:34
Jim Achor <orders@██████████.com>
RFQ for PR 4509138184
Кому undisclosed-recipients:

Сообщение Products List_Quotation Sheet.xls.iso (760 Kбайт)

Hello.

Greetings from ██████████.

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,
██████████ ZIU
██████████
Reg. Impr. ██████████
Tel: ██████████ 4
email: ██████████.ch

By 24.07.2018 13:10
info@██████████
PURCHASE ORDER
Кому undisclosed-recipients:

Сообщение purchase order.iso (568 Kбайт)

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 ██████████.onltd@hotmail.com is highly appreciated.

Thank You! Best Regards,

Company name: ██████████
Address: ██████████, 127411
Mrs veronica lisa
Sales & Purchasing Manager
██████████

By 24.07.2018 8:00
Ivan Rakic <ronin@██████████>
PURCHASE ORDER # WI-HYT/18-32/0379
Кому Recipients

Сообщение INVSC4F-180700141.iso (416 Kбайт)

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.



Latest Posts

Latest Webinars

Reports

Kaspersky researchers analyze updated CoolClient backdoor and new tools and scripts used in HoneyMyte (aka Mustang Panda or Bronze President) APT campaigns, including three variants of a browser data stealer.

Kaspersky discloses a 2025 HoneyMyte (aka Mustang Panda or Bronze President) APT campaign, which uses a kernel-mode rootkit to deliver and protect a ToneShell backdoor.

Kaspersky GReAT experts analyze the Evasive Panda APT's infection chain, including shellcode encrypted with DPAPI and RC5, as well as the MgBot implant.

Kaspersky expert describes new malicious tools employed by the Cloud Atlas APT, including implants of their signature backdoors VBShower, VBCloud, PowerShower, and CloudAtlas.

Source: <https://securelist.com/loki-bot-stealing-corporate-passwords/87595/>