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

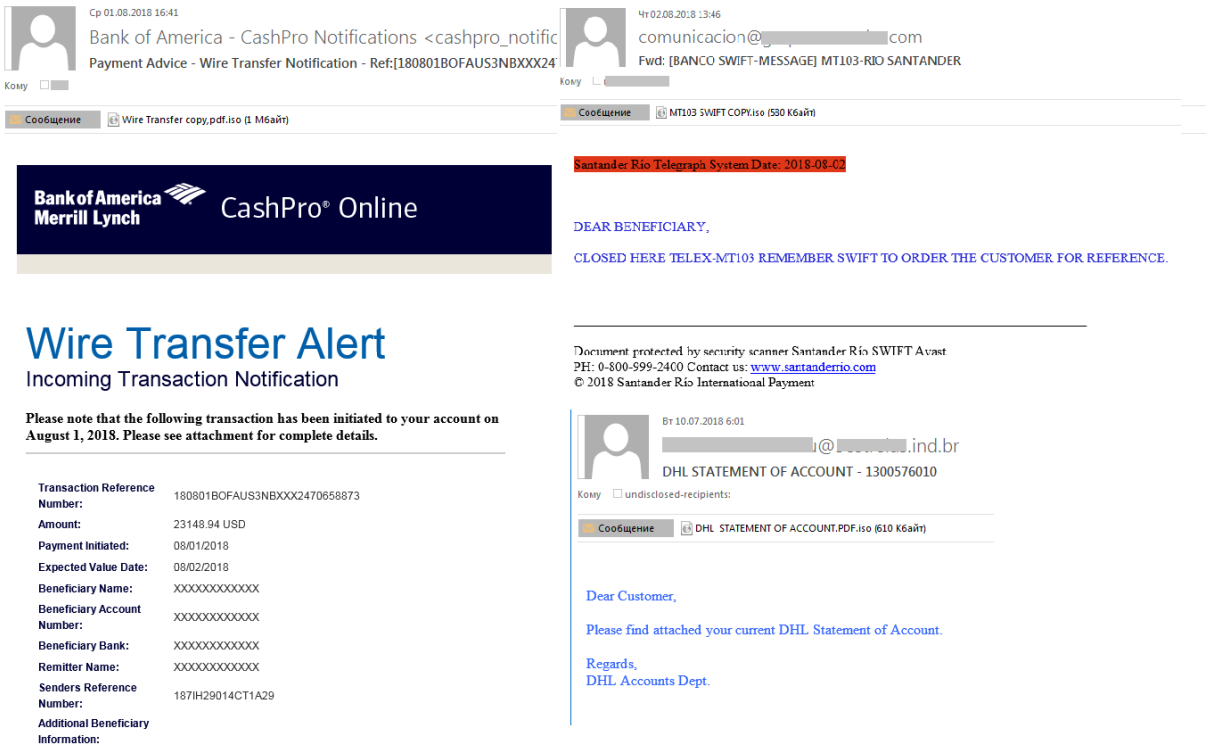
Starting from early July, we have seen malicious spam activity that has targeted corporate mailboxes. The messages discovered so far contain an attachment with an .iso extension that Kaspersky Lab solutions detect as Loki Bot. The malware's key objective is to steal passwords from browsers, messaging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

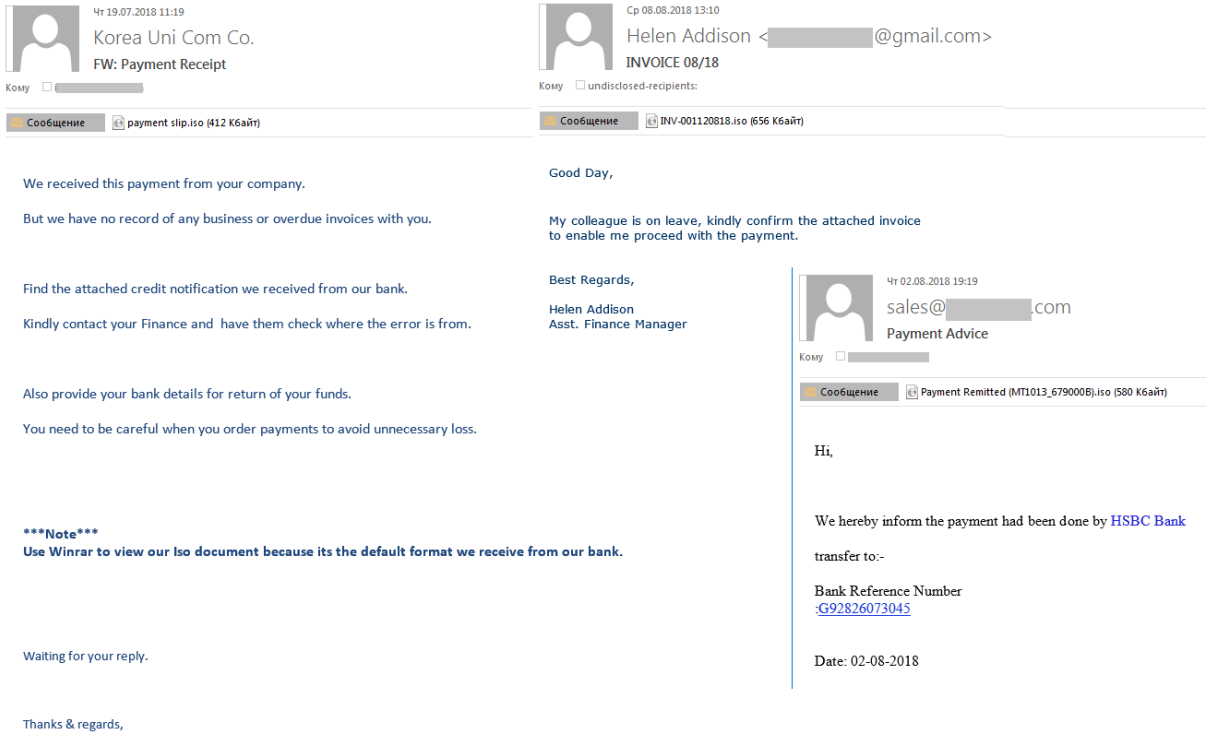
The emailed messages were notably diverse:

1. 1 Fake notifications from well-known companies



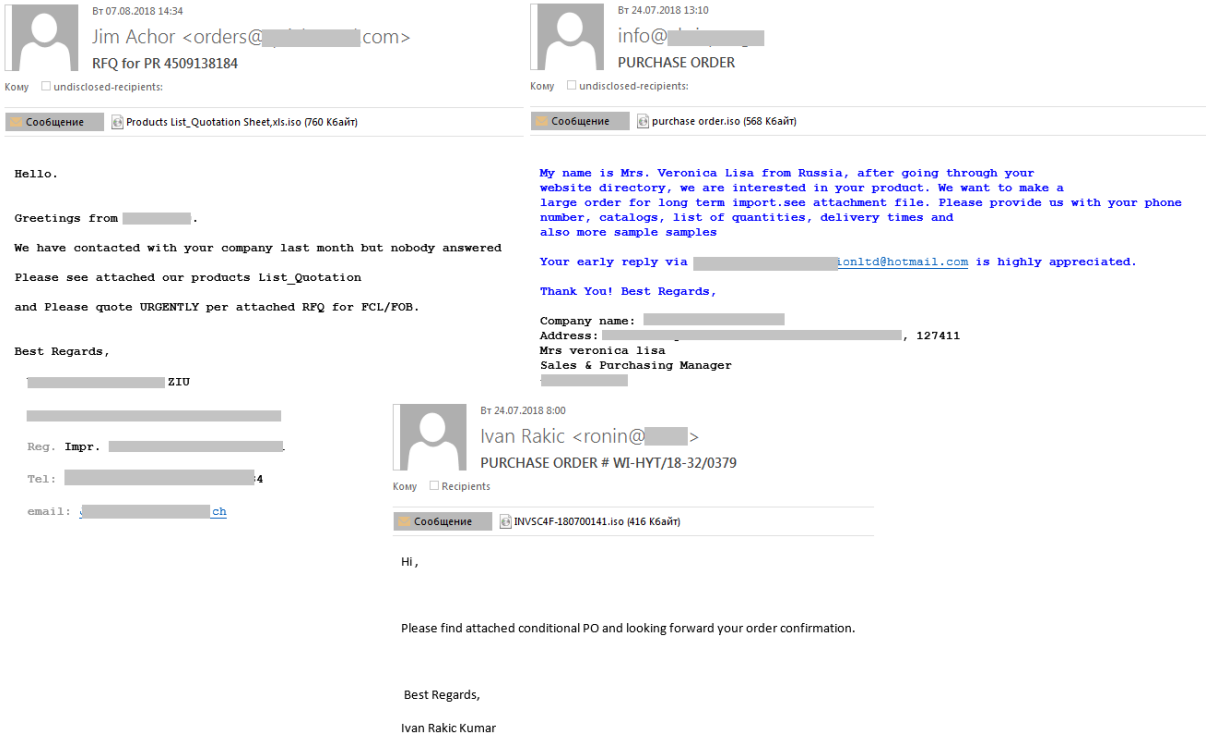
Imitating messages from well-known corporations is one of the most popular tricks in the hackers' arsenal. Interestingly enough, fake emails used to be directed mostly at common users and customers, whereas now companies are increasingly the target.

2. 2 Fake notifications containing financial documents



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



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.

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.
