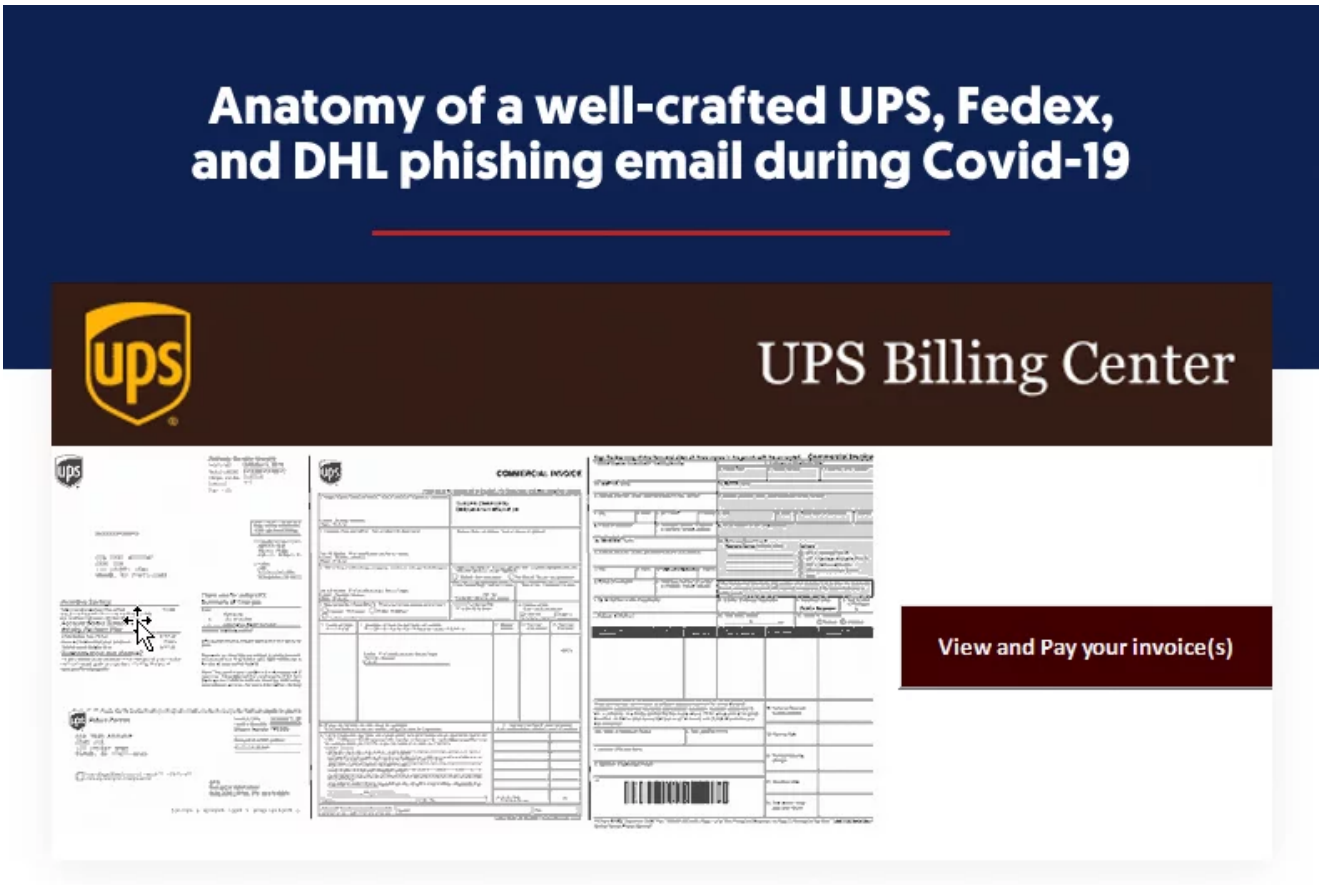
How UPS, FedEx, and DHL Phishing Emails Work

votiro.com/blog/anatomy-of-a-well-crafted-ups-fedex-and-dhl-phishing-email-during-covid-19/

May 5, 2020



What happened:

Votiro's Research Team has discovered a malicious macro that delivers a Dridex trojan payload hiding in Microsoft Excel spreadsheets delivered via phishing emails appearing to be from UPS, FedEx, and DHL. The Excel spreadsheet includes an obfuscated macro that launches PowerShell in hidden mode and downloads the payload from geronaga.com, a website that is registered with a Chinese website register https://now.cn. The IP address on this website, at the time when this attack was identified, pointed to a server in Russia.

Upon opening the file, which is a multi-threat document, the user has no insight into the automatic execution of the macro. The hacker is using a tool called Evil Clippy to hide the macro from being viewed or analyzed by static analysis tools. Evil Clippy is a cross-platform assistant for creating malicious Microsoft Office documents. This tool was released during a BlackHat Asia talk on March 28, 2019.

Once the file is opened, and the user either enables editing or clicks on the link within the Excel to “View & Pay the Invoice,” it executes an obfuscated PowerShell command that downloads the payload from a website and executes the attack. This attack is a multi-staged attack—using a sophisticated technique that evades email protection software and using advanced tactics that make it look like it came from these UPS, FedEx, and DHL shipping companies in separate messages.

No time to read now? Download the FedEx, UPS, DHL Case Study here.

Who is affected:

People and businesses – even people who are aware of phishing emails – are susceptible to this email campaign. This email campaign was missed by SaaS email protection providers because the macro was hidden and the macro was novel and not included in existing signature databases. As of 2pm ET on May 5th, 2020, VirusTotal reports several email protection services that would still miss the UPS and FedEx email. This improves the chances that the attack makes it to business and personal inboxes.

The attacker wanted to make a phishing email appear as if it came from either FedEx, UPS, or DHL by injecting their servers into the header of the messages. Even a well-trained person could be fooled by this phishing attack, as it makes the email sender appear to be legitimate.

If an unsuspecting person received one of these legitimate-looking emails with a Microsoft Excel spreadsheet attached, it is highly likely that they would open the attached Excel spreadsheet and compromise their systems.

Video Version

In the below video, Votiro Director of Engineering – North America, Rich Hosgood, dissects the UPS, FedEx, and DHL emails and Excel Attachments.

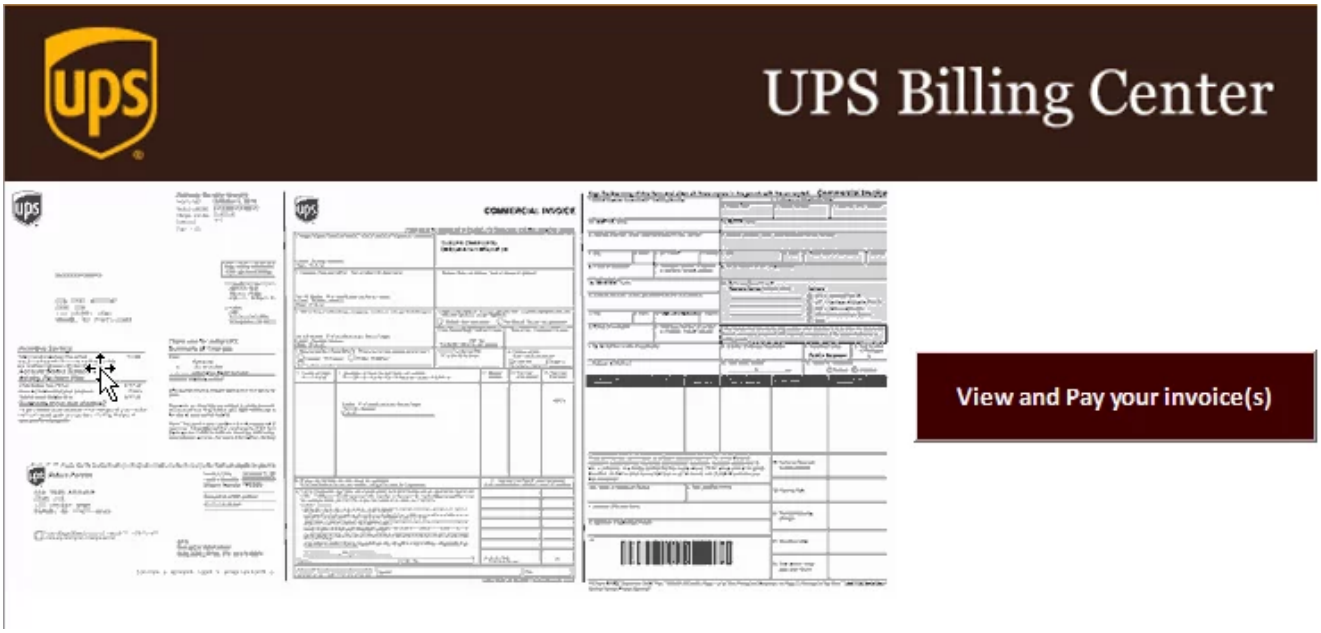
Additional information about each hack:

UPS Phishing Email

A legitimate looking email that appeared to come from the UPS website was sent from host242-180-static.131-212-b.business.telecomitalia.it, which is an Italian telco. The return path on the message header points 398094.20200420134554@ZUJOHUR.FODEWOX.njppsagent8.ups.com, which is a UPS server in Matawan, NJ. Inside this email was a legitimate-looking message from UPS with the logo and links that lead to ups.com. This email included an Excel spreadsheet that consists of a macro that automatically executes a PowerShell code, which exploits the user’s computer.

This attack was identified by Votiro on April 20, 2020 at 8:45am. It was uploaded to VirusTotal on April 22, 2020 at 5:14pm. A second UPS phishing email was received on April 22, 2020 at 1:42pm. The hash for this is included at the bottom of the post.

This email also included an Excel spreadsheet attachment with an auto-execution macro. That attachment looked like this.

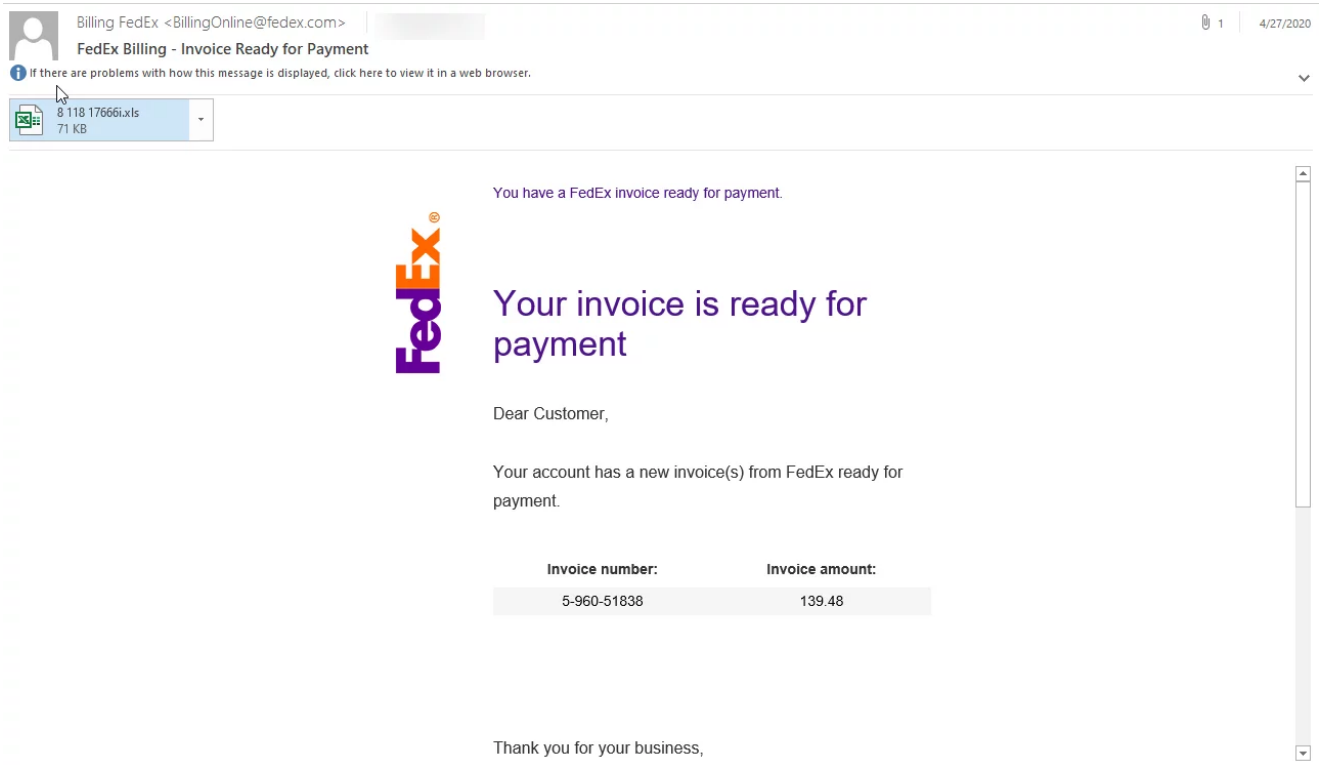


Every email message received by end-users contains header information. **This message contained server names as if it originated directly from UPS**. Even a well-trained person in cybersecurity could be fooled by this phishing attempt.

FedEx Phishing Email

A legitimate-looking email that appeared to come from Fedex.com was sent from 116.17.62.149, which traces back to Shaping, Guangdong, China. This email was received by Votiro on April 27, 2020 at 8:45am. The return path on the message header points sinai25@pvma00009.prod.fedex.com, and this is a server owned by FedEx in Collierville, Tennessee. Inside this email was a legitimate-looking message from FedEx with the logo and links pointing to FedEx.

Received: from 116.17.62.149 China IP https://ipinfo.io/116.17.62.149
From: Billing FedEx <BillingOnline@fedex.com>
Return-Path: sinai25@pvma00009.prod.fedex.com



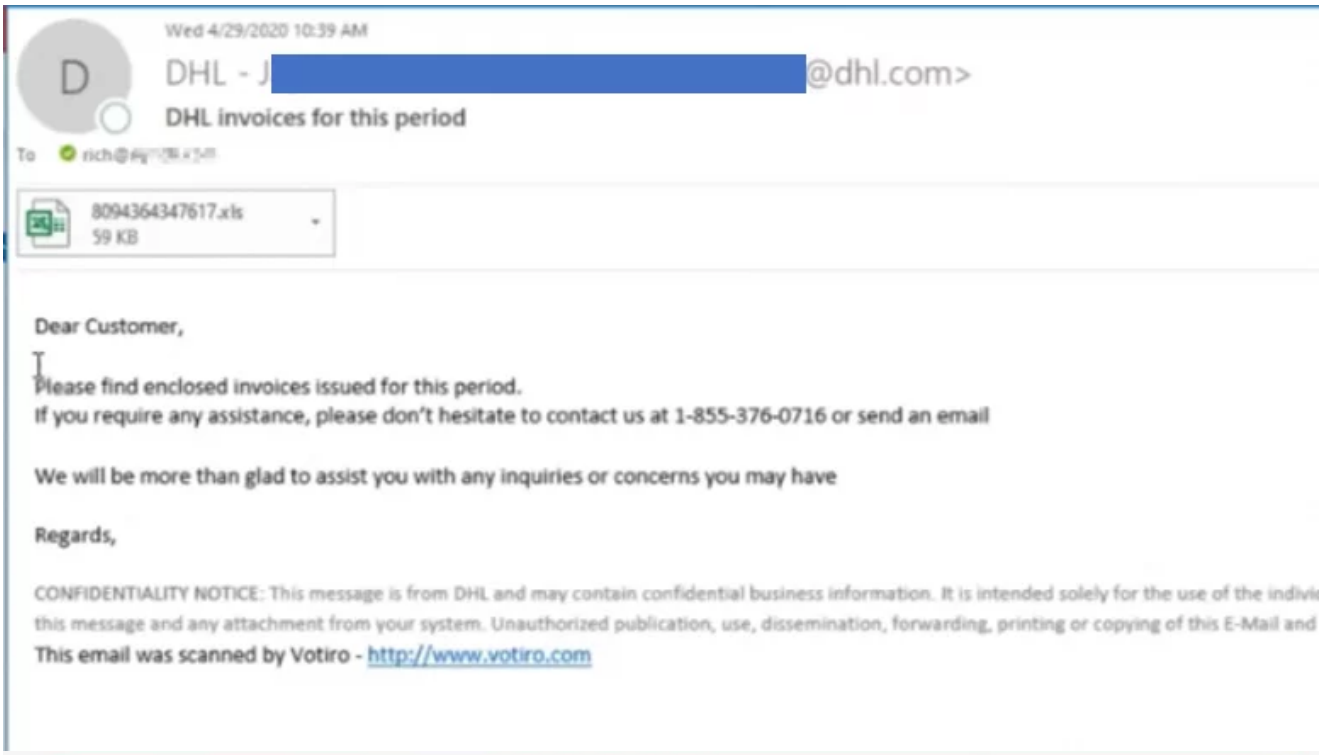
The below Excel was included in the email.

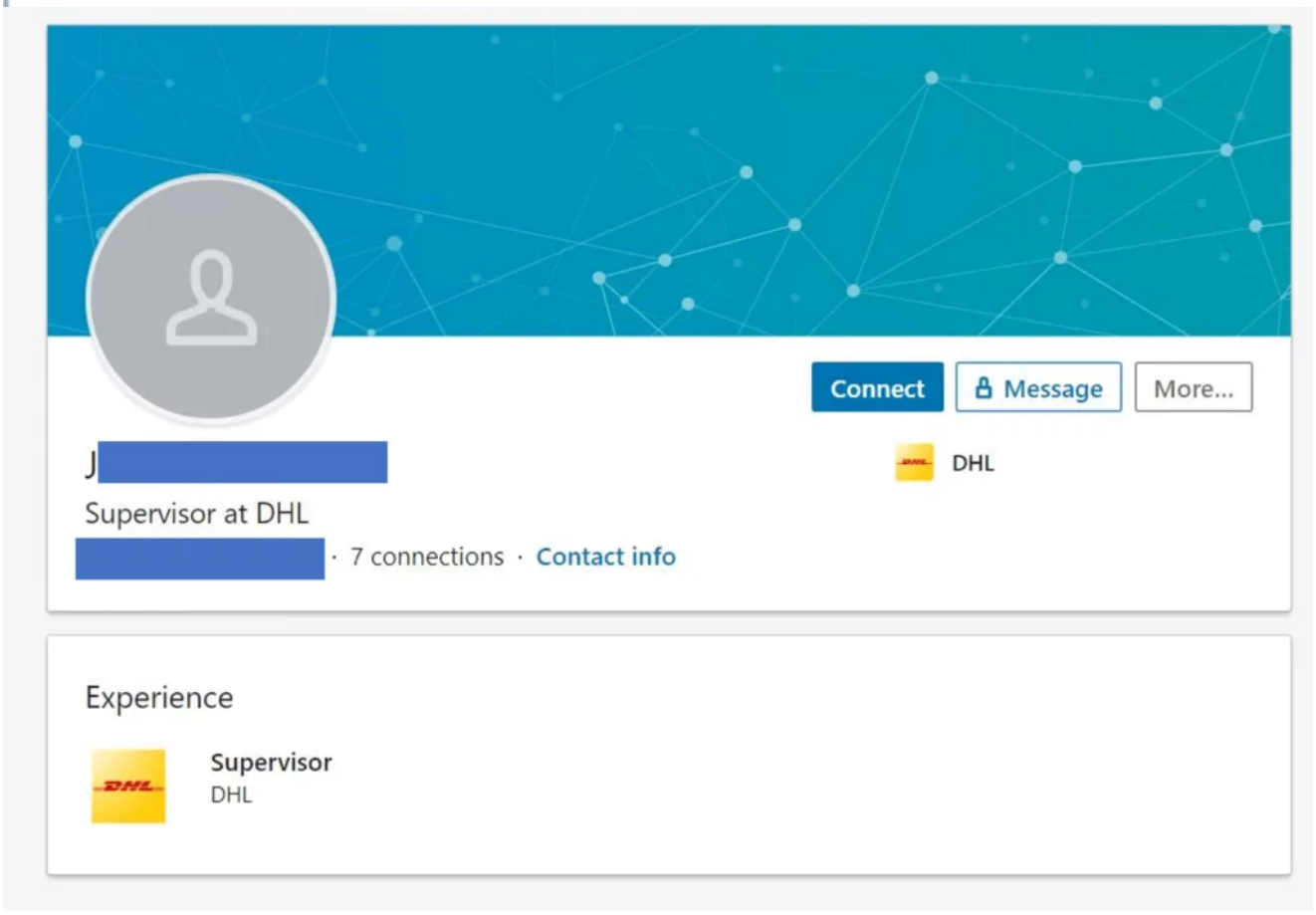
This message contained server names as if it originated directly from FedEx.

DHL Phishing Email

The DHL phishing email was less branded than the other emails. But it is important to note that the sender appears to be legitimate, with a firstname.lastname@dhl.com email address appearing to be the sender.

An individual—who has a name within one letter of the one used as a spoofed DHL email address—exists on LinkedIn, and their profile lists them as working at DHL. The profile has very few details. While the profile may not be from the attackers, it helps add legitimacy to the email, as even though the attacks contain a slightly different spelling of their name, the single letter difference can be hard to miss.





Hashes

UPS: e6c5862320ae7d8032fab1292121a98ca55e3842211112b8b9f2a2578b3e4dc0

FedEx: 8e06789e952991e6fc483ab0e6bbf08a123922ba354a75c9dc9dcc759c60c194

Want to stay up to date on the latest file-borne threats? Sign up to receive blog posts to your inbox below.