VOTIRO

UPS Billing Center
Your new invoice is now available.
Thank you for your business.
Reply
Reply all
Forward

How Novel UPS, FedEx, and DHL Phishing Attacks Evaded Antivirus Protection

Table of Contents

How Novel UPS, FedEx, and DHL Phishing Attacks

Evaded Antivirus Protection

In April 2020, Votiro's Research Team discovered a malicious macro that delivers a Dridex malware 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. The IP address on this website, at the time when this attack was identified, pointed to a server in Russia.

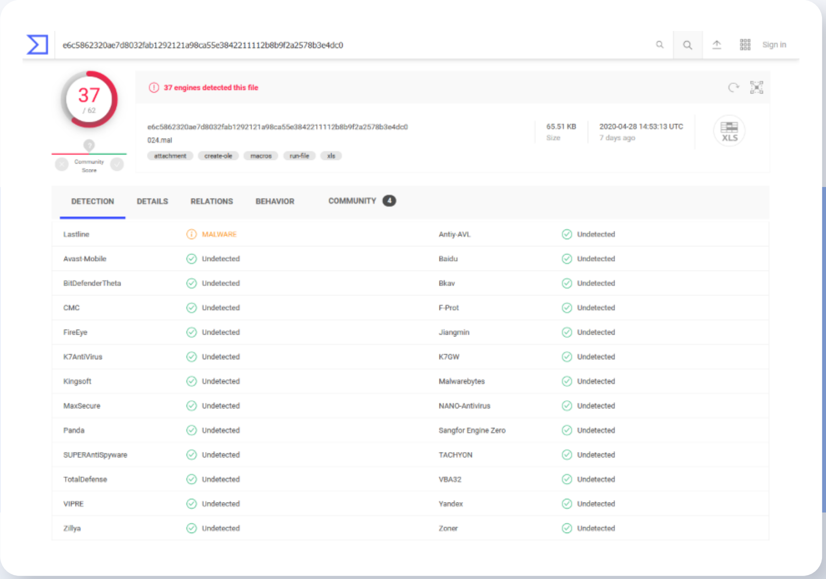
Upon opening the file, which is a multi-threat document, the user has no insight into the automatic execution of the macro. The hacker is using a tool called Evil Clippy to hide the macro from being viewed or analyzed by static analysis tools. Evil Clippy is a cross-platform assistant for creating malicious 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 ransomware.

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.

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 because the macro was novel and not included in existing threat signature databases. As of 2pm ET on May 5th, 2020 – *weeks* after the first campaign – VirusTotal reported several email protection and antivirus services that would still miss the UPS and FedEx email. This improves the chances that the attack makes it to business and personal inboxes.



e6c5862320ae7d8032fab1292121a98ca55e3842211112b8b9f2a2578b3e4dc0

37 / 62

37 engines detected this file

e6c5862320ae7d8032fab1292121a98ca55e3842211112b8b9f2a2578b3e4dc0
024.mal

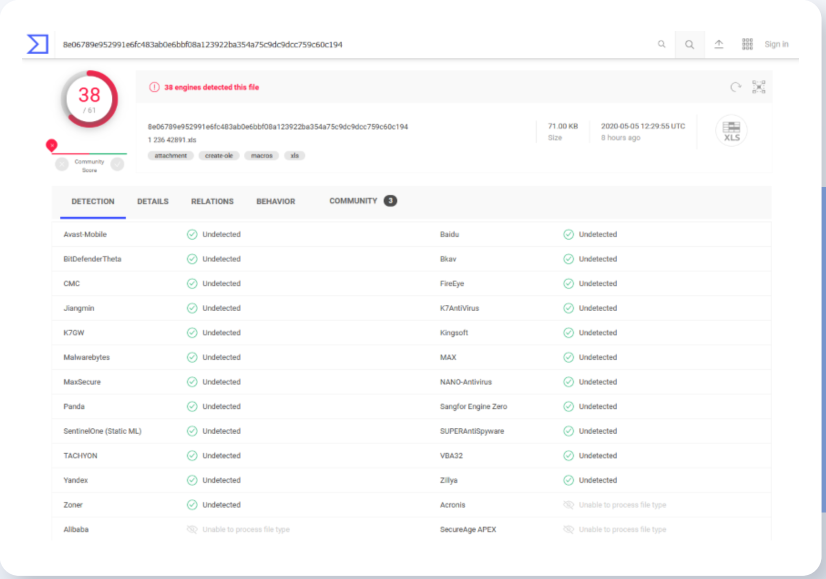
attachment create-ole macros run-file xls

65.51 KB
Size

2020-04-28 14:53:13 UTC
7 days ago

XLS

Lastline	MALWARE	Antiy-AVL	Undetected
Avast-Mobile	Undetected	Baidu	Undetected
BitDefenderTheta	Undetected	Bkav	Undetected
CMC	Undetected	F-Prot	Undetected
FireEye	Undetected	Jiangmin	Undetected
K7AntiVirus	Undetected	K7GW	Undetected
Kingsoft	Undetected	Malwarebytes	Undetected
MaxSecure	Undetected	NANO-Antivirus	Undetected
Panda	Undetected	Sangfor Engine Zero	Undetected
SUPERAntiSpyware	Undetected	TACHYON	Undetected
TotalDefense	Undetected	VBA32	Undetected
VIPRE	Undetected	Yandex	Undetected
Zillya	Undetected	Zoner	Undetected



8e06789e952991e6fc483ab0e6bbf08a123922ba354a75c9dc9dcc759c60c194

38 / 61

38 engines detected this file

8e06789e952991e6fc483ab0e6bbf08a123922ba354a75c9dc9dcc759c60c194
1 236 42891.xls

attachment create-ole macros xls

71.00 KB
Size

2020-05-05 12:29:55 UTC
8 hours ago

XLS

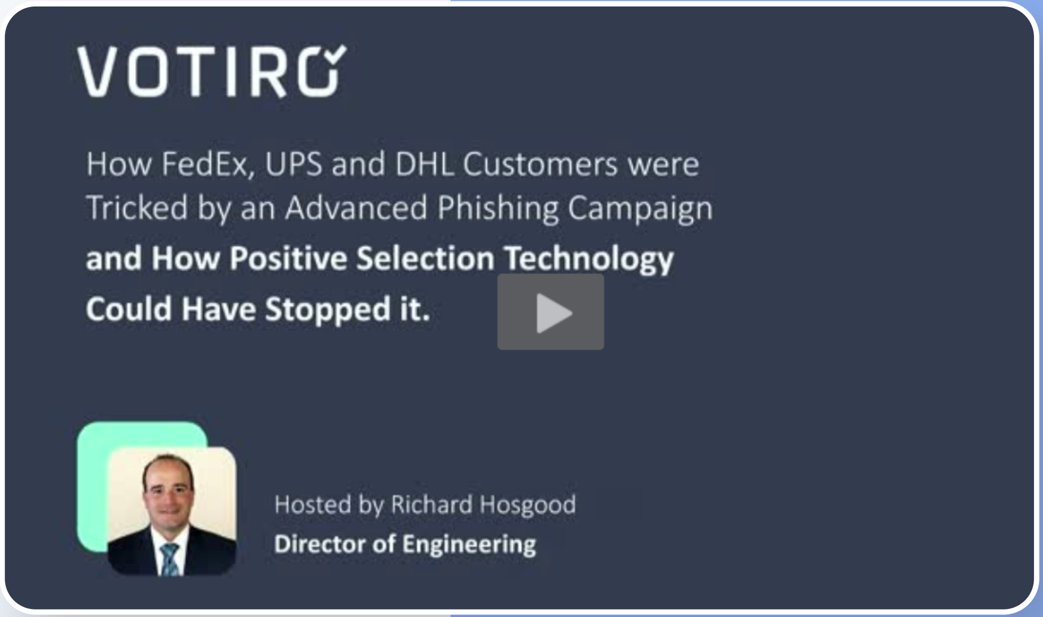
Avast-Mobile	Undetected	Baidu	Undetected
BitDefenderTheta	Undetected	Bkav	Undetected
CMC	Undetected	FireEye	Undetected
Jiangmin	Undetected	K7AntiVirus	Undetected
K7GW	Undetected	Kingsoft	Undetected
Malwarebytes	Undetected	MAX	Undetected
MaxSecure	Undetected	NANO-Antivirus	Undetected
Panda	Undetected	Sangfor Engine Zero	Undetected
SentinelOne (Static ML)	Undetected	SUPERAntiSpyware	Undetected
TACHYON	Undetected	VBA32	Undetected
Yandex	Undetected	Zillya	Undetected
Zoner	Undetected	Acronis	Unable to process file type
Alibaba	Unable to process file type	SecureAge APEX	Unable to process file type

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.

About the Attacks

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



VOTIRO

How FedEx, UPS and DHL Customers were Tricked by an Advanced Phishing Campaign **and How Positive Selection Technology Could Have Stopped it.**

Hosted by Richard Hosgood
Director of Engineering

UPS Phishing Email

This message contained server names as if it originated directly from UPS (sent from upsbillingcenter4@ups.com).

The return path on the message header points 398094.20200420134554@ZUJOHUR.FODEWOX.njppsagent8.ups.com, which is a legitimate UPS server in Matawan, NJ.

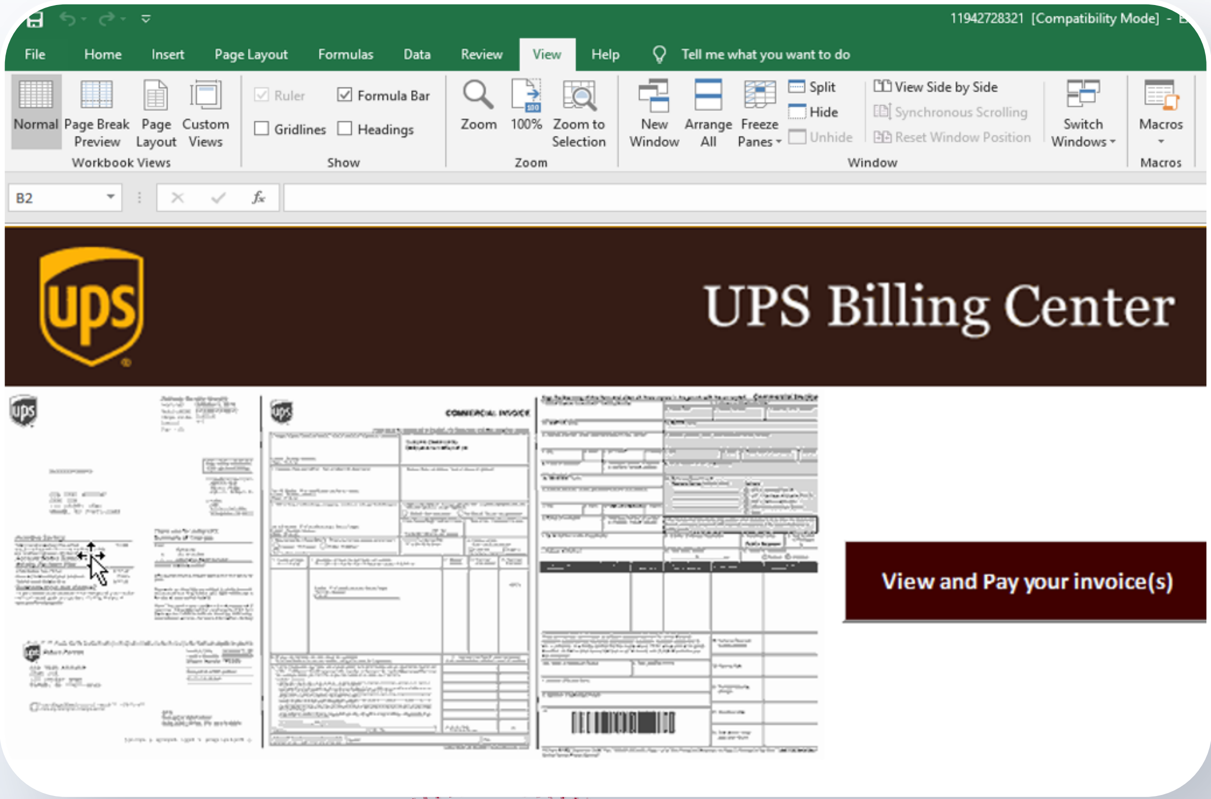
Inside this email was a legitimate-looking message from UPS with the logo and links that lead to ups.com. This email included an Excel spreadsheet that consists of a macro that automatically executes a PowerShell code, which exploits the user's computer.

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. 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 (sent from upsbillingcenter4@ups.com).**

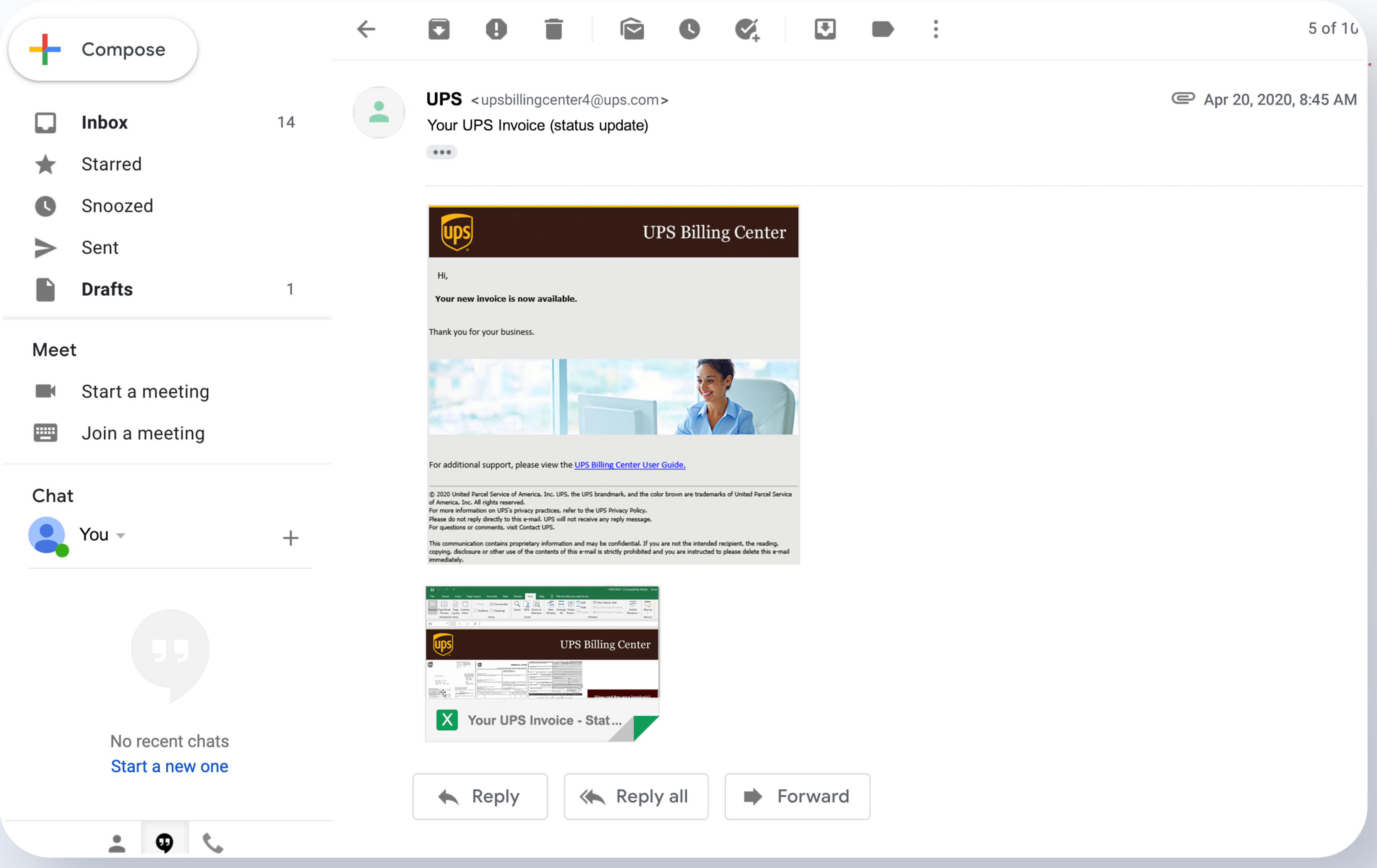
UPS Attack Hash:

e6c5862320ae7d8032fab1292121a98ca55e3842211112b8b9f2a2578b3e4dc0



Malicious Excel Attached from UPS Phishing Email

UPS Phishing Email



UPS <upsbillingcenter4@ups.com>

Apr 20, 2020, 8:45 AM

Your UPS Invoice (status update)

UPS Billing Center

Hi,

Your new invoice is now available.

Thank you for your business.

For additional support, please view the UPS Billing Center User Guide.

© 2020 United Parcel Service of America, Inc. UPS, the UPS brandmark, and the color brown are trademarks of United Parcel Service of America, Inc. All rights reserved.
For more information on UPS's privacy practices, refer to the UPS Privacy Policy.
Please do not reply directly to this e-mail. UPS will not receive any reply message.
For questions or comments, visit Contact UPS.

This communication contains proprietary information and may be confidential. If you are not the intended recipient, the reading, copying, disclosure or other use of the contents of this e-mail is strictly prohibited and you are instructed to please delete this e-mail immediately.

UPS Billing Center

Your UPS Invoice - Stat...

UPS Phishing Email

FedEx Phishing Email

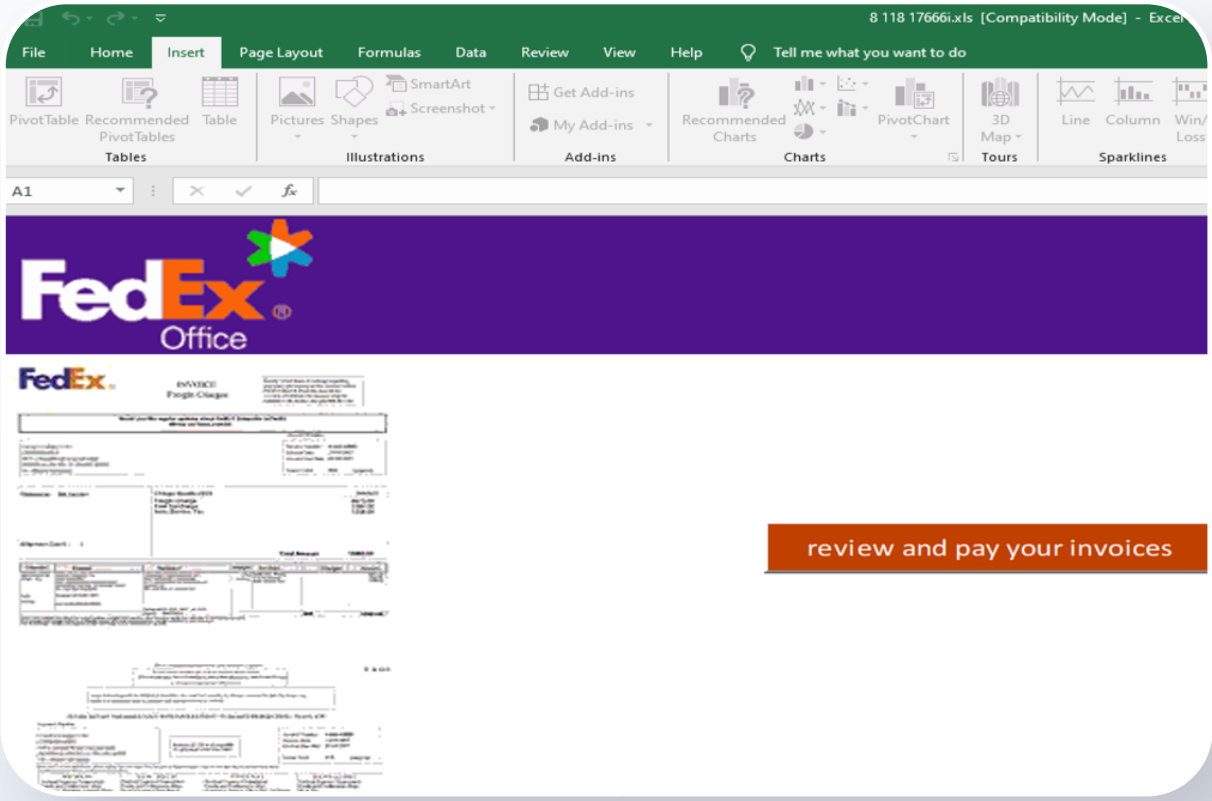
A legitimate-looking email that appeared to come from Fedex.com was sent from **116.17.62.149**, which traces back to Shaping, Guangdong, China. This email was received by Votiro on April 27, 2020 at 9:40am. The return path on the message header points sinai25@pvma00009.prod.fedex.com, and this is a 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

This Excel was included in the email →

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

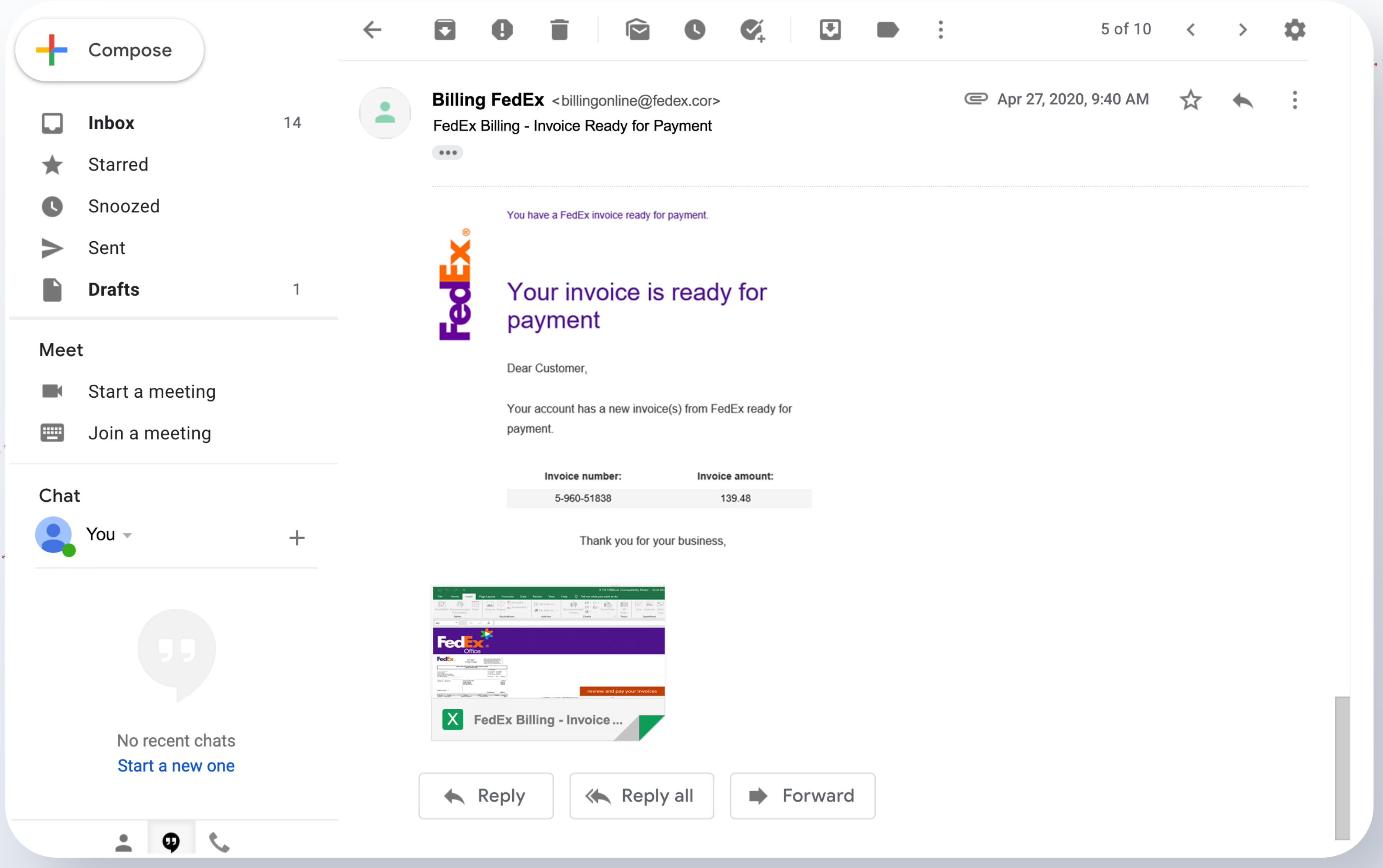
FedEx Attack Hash:
8e06789e952991e6fc483ab0e6bbf08a123922ba354a75c9dc9dcc759c60c194



8 118 17666i.xls [Compatibility Mode] - Excel

Malicious Excel Attached from FedEx Phishing Email

FedEx Phishing Email



Billing FedEx <billingonline@fedex.cor>

FedEx Billing - Invoice Ready for Payment

Apr 27, 2020, 9:40 AM

You have a FedEx invoice ready for payment.

Your invoice is ready for payment

Dear Customer,

Your account has a new invoice(s) from FedEx ready for payment.

Invoice number:	Invoice amount:
5-960-51838	139.48

Thank you for your business,

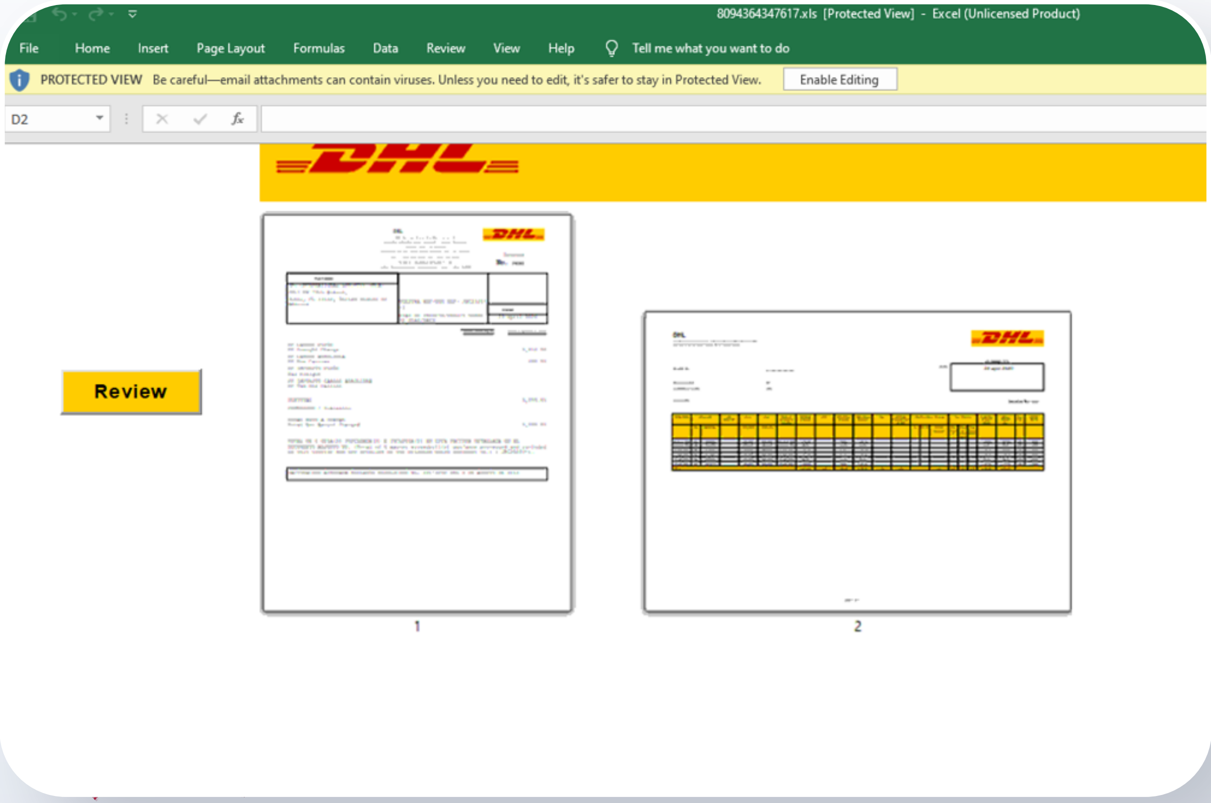
FedEx Phishing Email

DHL Phishing Email

The DHL phishing email was received on April 29th at 10:32am ET. 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 easy to miss.

The below Excel was included in the email →

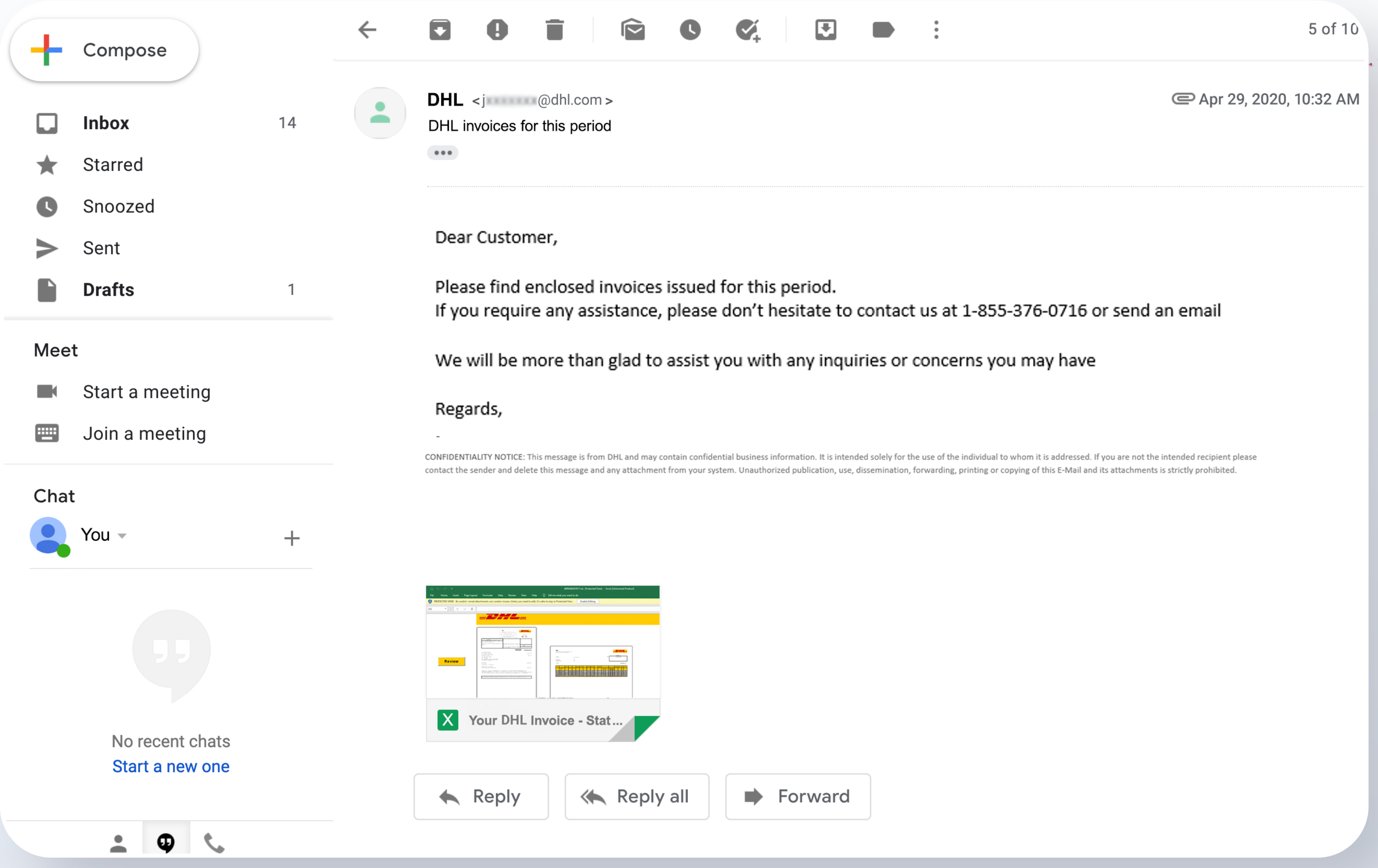


8094364347617.xls [Protected View] - Excel (Unlicensed Product)

PROTECTED VIEW Be careful—email attachments can contain viruses. Unless you need to edit, it's safer to stay in Protected View.

Malicious Excel Attached from DHL Phishing Email

DHL Phishing Email



DHL <j[redacted]@dhl.com>

Apr 29, 2020, 10:32 AM

DHL invoices for this period

Dear Customer,

Please find enclosed invoices issued for this period.
If you require any assistance, please don't hesitate to contact us at 1-855-376-0716 or send an email

We will be more than glad to assist you with any inquiries or concerns you may have

Regards,

-

CONFIDENTIALITY NOTICE: This message is from DHL and may contain confidential business information. It is intended solely for the use of the individual to whom it is addressed. If you are not the intended recipient please contact the sender and delete this message and any attachment from your system. Unauthorized publication, use, dissemination, forwarding, printing or copying of this E-Mail and its attachments is strictly prohibited.

Your DHL Invoice - Stat...

DHL Phishing Email

How to Prevent File-Borne Attacks Like These

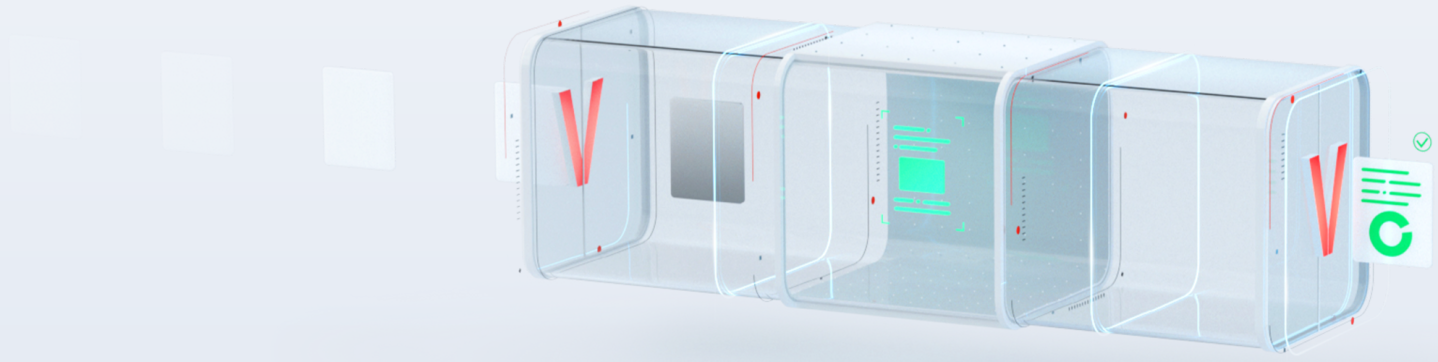
Votiro Cloud: Protection From Weaponized Files

Votiro introduces the **Votiro Cloud:** the only solution that protects from weaponized files without detection or slowing business. Unlike detection-based file security solutions that scan for suspicious elements and block some malicious files, Votiro's revolutionary Positive Selection™ technology singles out *only the safe elements of each file*, ensuring every file that enters your organization is safe to use.

When an email containing a malicious file enters an enterprise's communications network, Positive Selection technology rebuilds the file, transferring over only the vendor-approved, known good content. This leaves the malicious code behind while allowing the file to retain its full usability and functionality.

All the functionality that users need for working with a file, such as copying text, handling bookmarks, keeping content on the original pages, using active content and embedded objects, running macros, and searching, is preserved.

Founded in 2010 by leading file security experts, Votiro's new approach to file security works invisibly in the background, completely eliminating threats while ensuring zero interruption to business.



Completely Secure Files, No Matter the Source

Votiro Cloud API For Email:

Completely secure every email that enters your organization.

Votiro Cloud API For Web Downloads:

Secure everything employees download, no matter what it is or where it came from.

Votiro Cloud API For Web Uploads & Applications:

Secure all file uploads and receive documents completely risk-free.

Experience Zero Trust File Security For Yourself

See for yourself how easy it is to safeguard your organization with the Votiro Cloud.

Sign up for a live demo