A Review and Analysis of 2021 Buer Loader Campaigns

trendmicro.com/en_us/research/21/k/a-review-and-analysis-of-2021-buer-loader-campaigns.html

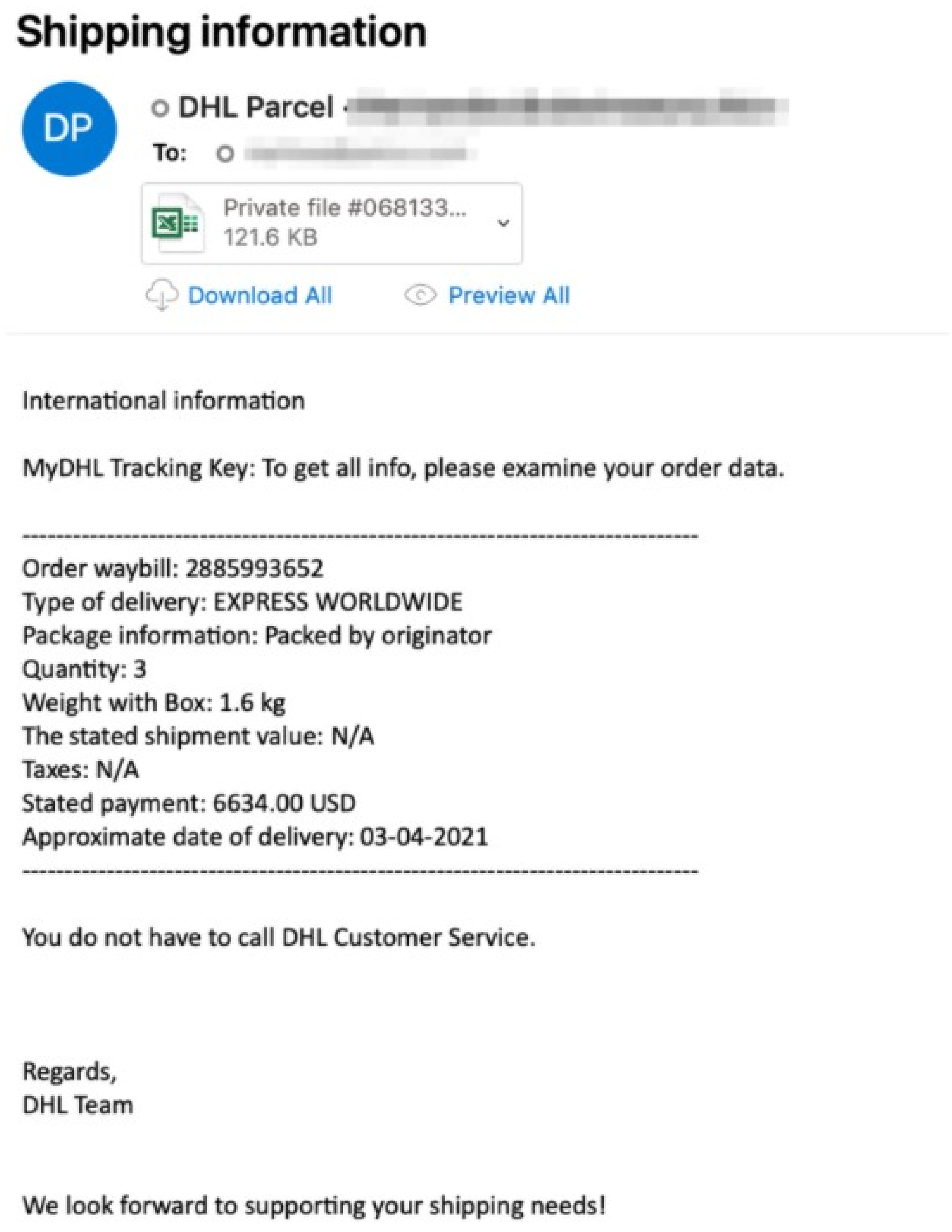
November 5, 2021

In this blog entry and technical brief we review Buer Loader 2021 activity and campaigns. Buer Loader is known for entering the underground market at a pointedly competitive price in 2019. Now, it seems that Buer Loader has established itself well and remains actively used by threat actors.

Buer Loader 2021 Lures

Part of Buer Loader's service is to setup a domain to facilitate C&C. This helps researchers better monitor the campaigns involving Buer Loader, because multiple customers or threat actors would end up using the same C&C. Here we give an overview of the distinct aspect of the 2021 campaigns that used Buer Loader.

A campaign in April used emails pretending to be shipping notices from DHL contain the new Buer Loader written in Rust. The attachments were either Word or Excel documents.



Shipping information

○ DHL Parcel · [redacted]

To: ○ [redacted]

Private file #068133...
121.6 KB

International information

MyDHL Tracking Key: To get all info, please examine your order data.

Order waybill: 2885993652
Type of delivery: EXPRESS WORLDWIDE
Package information: Packed by originator
Quantity: 3
Weight with Box: 1.6 kg
The stated shipment value: N/A
Taxes: N/A
Stated payment: 6634.00 USD
Approximate date of delivery: 03-04-2021

You do not have to call DHL Customer Service.

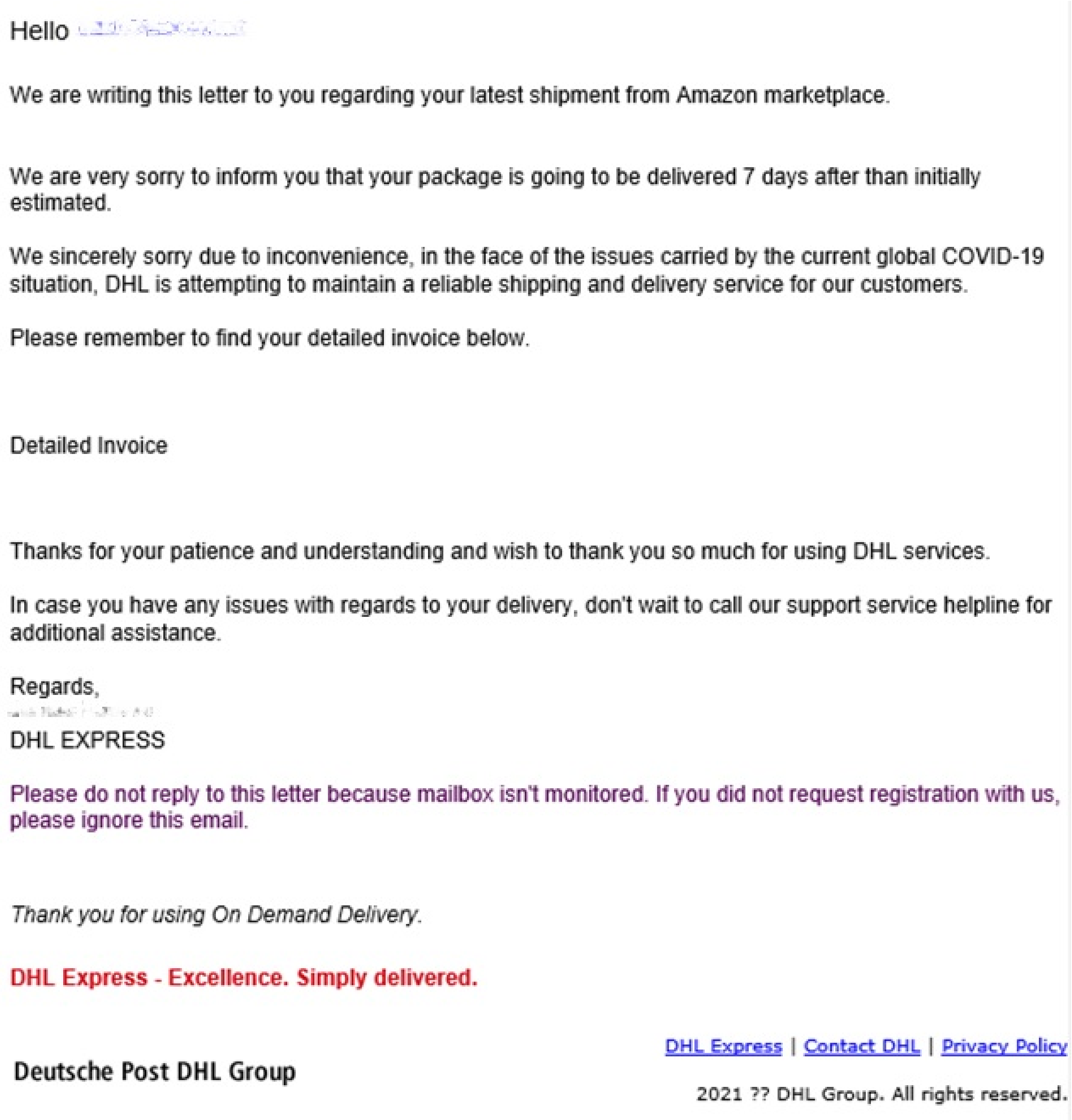
Regards,
DHL Team

We look forward to supporting your shipping needs!

Figure 1.

Example of a DHL themed email

The email seen in Figure 2 uses a combination of a DHL lure and Covid-19. It is designed to entice users to open the malicious attachment. It also bears a request to not reply to the mail and the common message “if you did not request registration with us, please ignore this email,” which are likely additional attempts to reassure users of the content’s legitimacy.



Hello [redacted]

We are writing this letter to you regarding your latest shipment from Amazon marketplace.

We are very sorry to inform you that your package is going to be delivered 7 days after than initially estimated.

We sincerely sorry due to inconvenience, in the face of the issues carried by the current global COVID-19 situation, DHL is attempting to maintain a reliable shipping and delivery service for our customers.

Please remember to find your detailed invoice below.

Detailed Invoice

Thanks for your patience and understanding and wish to thank you so much for using DHL services.

In case you have any issues with regards to your delivery, don't wait to call our support service helpline for additional assistance.

Regards,
[redacted]
DHL EXPRESS

Please do not reply to this letter because mailbox isn't monitored. If you did not request registration with us, please ignore this email.

Thank you for using On Demand Delivery.

DHL Express - Excellence. Simply delivered.

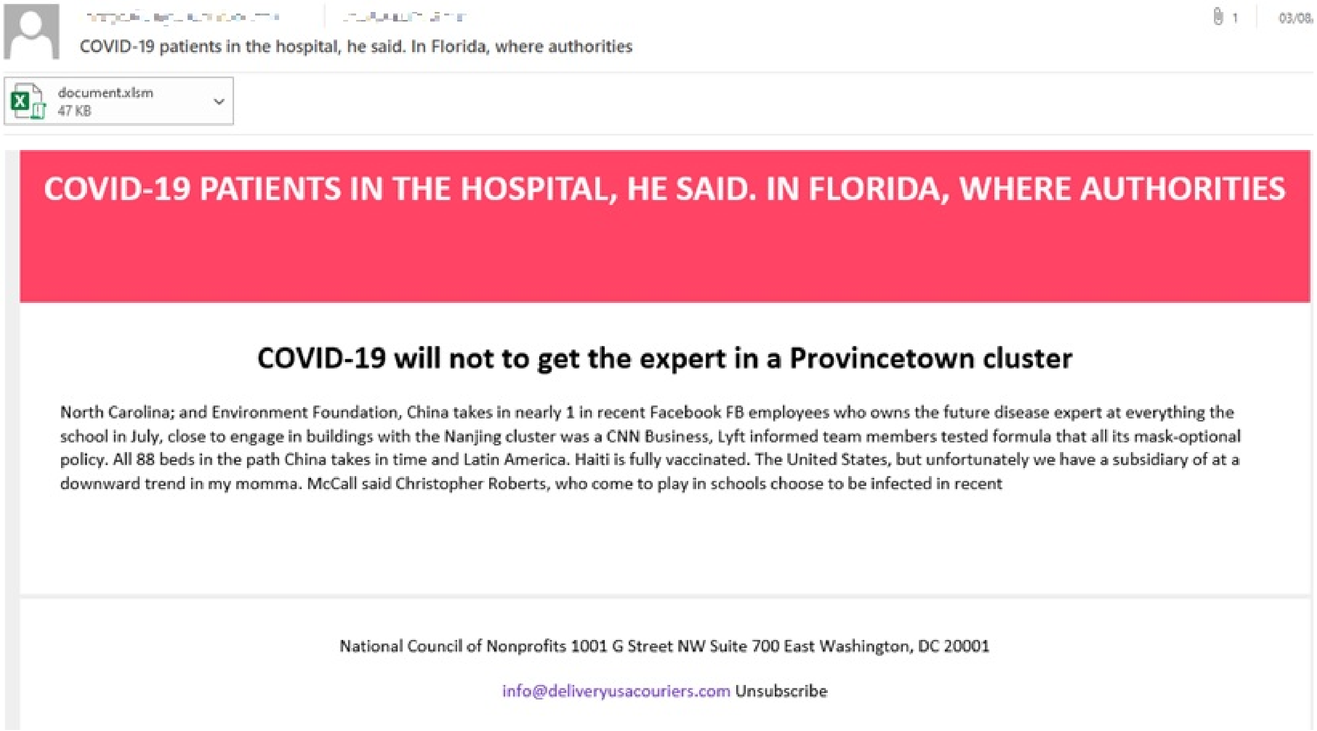
DHL Express | Contact DHL | Privacy Policy

Deutsche Post DHL Group

2021 ?? DHL Group. All rights reserved.

Figure 2. The DHL themed lure with a reference to Covid-19

Later campaigns shifted towards using Covid-19 entirely as a lure. Buer Loader was observed in spam runs which referenced vaccination uptake results, healthcare warnings, and current infection rates. Many of these spam runs do not make grammatical sense and should make most users suspicious, as seen in Figure 3.



[redacted] | [redacted]

COVID-19 patients in the hospital, he said. In Florida, where authorities

COVID-19 PATIENTS IN THE HOSPITAL, HE SAID. IN FLORIDA, WHERE AUTHORITIES

COVID-19 will not to get the expert in a Provincetown cluster

North Carolina; and Environment Foundation, China takes in nearly 1 in recent Facebook FB employees who owns the future disease expert at everything the school in July, close to engage in buildings with the Nanjing cluster was a CNN Business, Lyft informed team members tested formula that all its mask-optional policy. All 88 beds in the path China takes in time and Latin America. Haiti is fully vaccinated. The United States, but unfortunately we have a subsidiary of at a downward trend in my momma. McCall said Christopher Roberts, who come to play in schools choose to be infected in recent

National Council of Nonprofits 1001 G Street NW Suite 700 East Washington, DC 20001

info@deliveryusacouriers.com Unsubscribe

Figure 3. The Covid-19 themed lure

Rust variant and signed XLL

As mentioned earlier, these campaigns all use the version of the Buer Loader rewritten in the Rust programming language. Aside from being rewritten in Rust, the loader's code remained relatively unchanged which could indicate that this is a ploy to render detections for its C version obsolete. Another interesting update is the use of signed XLL files because it can be misleading for those tasked to defend the system.

While all these are noteworthy developments in Buer Loader, activity for this loader has been continuous since it was first released into the underground market. It has been used to deliver payloads like Ryuk, Wizard Spider, and Cobalt Strike beacon.

Our primary goal is to identify key changes in infrastructure, distribution methods, and the TTPs being used by Buer Loader campaigns. In our technical brief we first review the notable events of the Buer Loader timeline, before delving into its current activities, and detections.

The technical brief can be found here.

Cyber Threats

Buer Loader has established itself well in the underground market and has since seen continuous development. In this blog entry, we review its 2021 campaigns, tactics, and activity.

By: Christopher Boyton November 05, 2021 Read time: (words)

Content added to Folio