New UPS Phishing Variant!

2021-08-27 - Don Guilbeault - Comments (0) - General

Waiting for a package? Don't click this phony UPS email

Malicious message takes you to real UPS website, but don't trust it

A clever crook has been dropping malware on unsuspecting victims who get tricked into clicking a legitimate looking UPS tracking number link that leads to the real UPS.com website. Normally, you can avoid phishing and malware scams by checking the URL, or web address, of the site they take you to. It's usually a dead giveaway when the URL and purported site don't match. But in this case, reports say, the victim lands on the real UPS website, and hence may be more inclined to trust the malicious Word document that gets downloaded as the tracking number page is opened. That Word doc itself is deliberately unreadable until the reader clicks "Enable Content", which downloads yet more files. This has been quoted as "one of the best phishing emails seen in a long time."

UPS.com has since fixed the particular flaw that permitted the crook to inject malicious code right into the company website, and most of the best antivirussoftware detects the malicious Word doc. But it won't be the last time this method is used in phishing and "malspam" (malicious spam) campaigns.

How the phish works — and how to avoid it

The deception begins with a convincing-looking email message notifying you that "your package has experienced an exception," defined as "when a package or shipment encounters an unforeseen event." You are invited to "download and print out the invoice to pick up the package at the UPS Store" or to click the tracking number link. The only tip off that this is bogus is the

address of the email sender, which includes "unitedparcelservice" but has a different (dot)com name. However, it wouldn't be that difficult for the sender to "spoof" a legitimate UPS.com email address if they wanted to. Normally, you can avoid email based phishing scams by hovering your mouse cursor over the link in the body of the message. That will display the destination URL at the bottom of your screen. But in this case, you'll see a real UPS.com web address when you hover over the tracking number or the invoice link. Click on either, and you land on a page on the UPS website telling you that "Your download will start shortly." The crook has exploited a cross site scripting (XSS) flaw in the UPS site to add their own code, which reaches out to another website to fetch and deliver a Word document to the site visitor.

Malicious macro

Here's where this scheme becomes more of a regular phishing/malspam scam, and where it's easiest to avoid. Open that Word doc, and the text will be so blurry that you won't be able to read it. Microsoft Word will tell you that macros — small scripts that can run in Office files — have been disabled, but the Word file tells you to "Enable Content" to see the text. Needless to say, you should never Enable Content on some random Word, Excel or PowerPoint document downloaded from the internet. But if you do, a macro in the Word doc downloads a possibly malicious .png image that would contain an executable script to install backdoor access to your PC allow the would be hacker remote access to your data.

Remember when in doubt, always delete…

Don Guilbeault
IT Analyst
Westview Co-operative Association Limited

P. 403.556.3335 Option 2, 8| C. 403.899.9752 | F. 403.507.2405
P.O. Box 3970, Olds AB. T4H 1P6, Canada
don.guilbeault@westviewcoop.ca | www.westviewco-op.crs

Integrity | Excellence | Responsibility | Community