How to Slam a Door on the Cutwail Botnet: Enforce DMARC

mimecast.com/blog/how-to-slam-a-door-on-the-cutwail-botnet-enforce-dmarc/

Key Points

- The Cutwail botnet continues to be very active and often spoofs the brands of well-known organizations via email as part of its attacks.
- Though many well-known organizations use DMARC to limit abuse of their brands via email, not enough email receiving organizations are enforcing on DMARC.
- While not a magic bullet, DMARC can be an important contributor to improved security when used more broadly and in conjunction with other security controls.

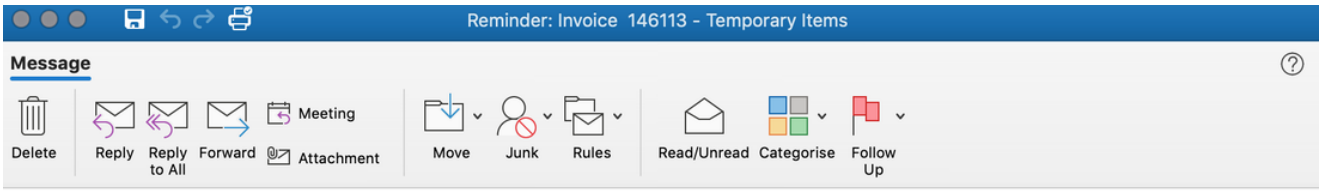
First discovered in 2007, Cutwail is a large botnet comprised of infected windows hosts. By 2009, it was determined that the Cutwail botnet was the largest botnet of its kind based on the number of infected hosts. Cutwail is still active today, and its primary aim is to turn infected hosts into spambots capable of generating high volumes of malicious and otherwise unwanted email. In the past, Cutwail has been responsible for pushing out well-known malware families like Gozi, URLZone and Dridex.

Over the past couple of months, Cutwail has become more active and has been sending email-borne attacks loaded with malicious URLs and Excel file attachments. These attacks have often been sent out spoofing the domains and brands of well-known global organizations, such as Intuit, UPS, FedEx and ADP. Well-known brands are extremely useful, in particular to spammy services such as Cutwail, given the vast majority of people that receive them will at minimum recognize them, if not also regularly do business with them, and thus be more likely to trust and engage with the emails.

The good news is that all of these companies, as well as many others, have done the right thing to stop the email-borne exploitation of their online brands; They have implemented DMARC and also have set the “p” values of their DMARC DNS entries to “reject.” This means that any email security system that receives these fraudulent emails should be able to analyze and reject them as imposters. Implementing DMARC is not a trivial IT project, and thus we should give credit where credit is due to those domain owners that have successfully done it.

The bad news is that many of these emails continue to land at their intended targets and apparently are being acted on. Why? Unfortunately, not enough organizations are enforcing on DMARC on their inbound email and thus the DMARC action request flag of “p=reject” is falling on the security equivalent of deaf ears. This issue of lack of DMARC enforcement is not new. In fact, it was recently reported by SC Magazine that attacks spoofing Microsoft.com were ironically being delivered to organizations that were using Microsoft 365 as their email provider. Evidently, many organizations using Microsoft 365 are not enforcing DMARC, even though Microsoft has Microsoft.com set to DMARC “reject.”

Let’s look at a couple recent examples of the malicious emails that are being sent by the Cutwail botnet.



Reminder: Invoice 146113

A

Accounting <quickbooks@notification.intuit.com>

To:

Thursday, 29 October 2020 at 20:56

intuit quickbooks

Order will be delivered upon payment receipt.

Thanks for your business!

INVOICE 146113

DUE 29/10/2020

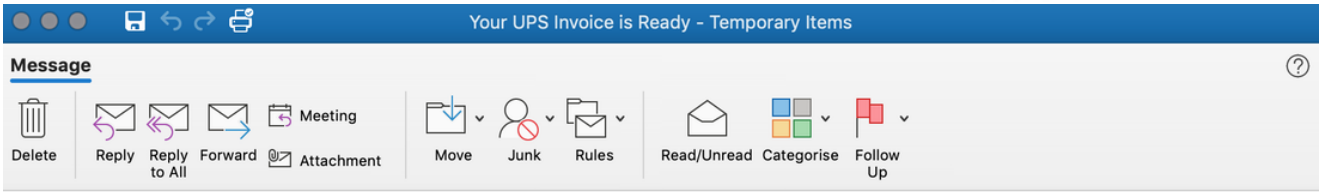
$1,230.00

Pay invoice

Powered by QuickBooks

https://msc-cunds.de/permit.php

If you receive an email that seems fraudulent, please check with the business owner before paying.



Your UPS Invoice is Ready

U

upsbillingcenter@ups.com

To:

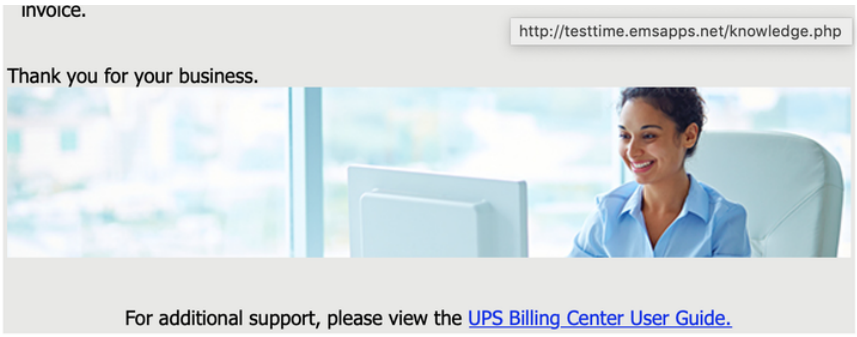
Tuesday, 3 November 2020 at 17:38

UPS Billing Center

view and pay your invoice

Hi,

Your new invoice is now available. Please visit the UPS Billing Center to view and pay your



Note in these examples that these Cutwail generated emails are not using *similar* sending domains to UPS and Intuit; Cutwail is using the *actual* domains of the spoofed organizations – intuit.com & ups.com. It does this, combined with the appropriate branding and text, to increase the credibility of the email and thus improve engagement with the receiver. In addition, compelling email subjects also play a role in gaining trust and engagement.

Example subjects:

- *FedEx Billing Online - Invoice Ready for Payment*
- *Your UPS Invoice is Ready*
- *ADP Payroll Invoice(s) 04-NOV-2020: 193987187*
- *FBA Inbound Shipment Bill of Lading Ready (FBA855RXJZV9)*
- *Invoice 419665*
- *Electronic Invoice (#05250943)*
- *Reminder: Invoice 625953*

Unfortunately, engagement with any of these emails *rewards* the target with the download of the Dridex trojan from one of these locations:

hxxp://declareeducation[.]com/zzp9nf57e.zip
hxxp://demo[.]linuxuatwebspiders[.]com/hwlkzsx.zip
hxxp://dekowood-dev[.]uzor[.]group/kz70ctm.zip
hxxp://personnel[.]districtweb[.]ca/lqicoh.zip
hxxp://sl-elite[.]net/cuiq5y2.zip
hxxp://testtime[.]emsapps[.]net/raistmat.zip
hxxp://sparkasse[.]africamojatours[.]co[.]za/fcm6rtep.txt
hxxp://organisme[.]districtweb[.]ca/jp3x5s1w.txt
hxxp://e2mblog2[.]linuxuatwebspiders[.]com/iejvut.txt
hxxp://sentable[.]cz/fj5oilayy.txt
hxxp://simplvid[.]xpleomedia[.]com/emkbnc6.txt
hxxp://bary[.]sz4h[.]com/g6g9tu4.gif
hxxp://bancomext[.]demasys[.]net/vj0g4rl.gif

hxxp://officehelp[.]uzor[.]group/pguip0gny.gif
hxxp://businessdebthelper[.]com/yozcw4.pdf
hxxp://cafeplus[.]districtweb[.]ca/g6fb8jcz9.pdf
hxxp://casadosirmaos[.]bitnetbr[.]com/n1c9hq9ps.jpg
hxxp://pc[.]helloconci[.]com/wpbhvi8.jpg
hxxp://metal-test[.]cn/rmjiyy1.jpg
hxxp://bajajclasses[.]com/jw4kb9.jpg
hxxp://chickencode[.]appsdesignstudio[.]com/ihmkigi.jpg
hxxp://ctalk[.]helloconci[.]com/a5goz2s.rar

With the Dridex trojan installed, the attackers have a lot of flexibility as to what comes next. Unfortunately, the delivery of ransomware in the next stage of the attack has recently been shown to be very popular.

The Bottom Line

While there are many ways Cutwail botnet initiated attacks can be stopped, such as with security awareness training to address user engagement and sophisticated endpoint protections to block the installation of the malware, it is particularly frustrating that a control specifically designed to make this type of phishing more difficult for the phisher — DMARC — has not yet been more broadly implemented. The domain owners have done their part, what about everyone else in the world of email?

Note: Mimecast's defenses on behalf of our customers against these Cutwail generated emails have proven to be effective.

Primary research conducted by Samantha Clarke, Mimecast Threat Research Engineer

Up Next

Brand Protection | Apr 19, 2021

ROI Analysis: Keeping Brands Safe from Digital Impersonation