


Fresh Phish: Urgency, Mail Relay Serve Phishers Well on Craigslist

 inky.com/blog/urgency-mail-relay-serve-phishers-well-on-craigslist



Posted by Roger Kay

- [Tweet](#)
-

During her monolog on the Moth podcast back in 2011, Satori Shakoor described how she returned to dating sometime after mourning the deaths of both her mother and her son. “So, I went on Craigslist,” she told the live audience, “ 'cause Craigslist deliver right now.”

Craigslist, that old-fashioned website people still use to find things locally — and urgently — has become the latest phishing vector. In addition to the inherent time pressure of its marketplace, a feature on the site that appeals to phishers is the mail relay function. In the service of safety and anonymity, Craigslist lets people seeking or offering things send an email through the system to anyone else. What the recipient sees for a sender’s address is `<a long hex string>@<subdomain>.craigslist.org`. Craigslist knows the identities of everyone, but unless a correspondent discloses details, they are perfectly anonymous to others on the system.

This situation suits phishers just fine. They can shoot their poisoned arrows from behind a local mail proxy. And shoot they did — a number of times in early October.

Quick Takes: Attack Flow Overview

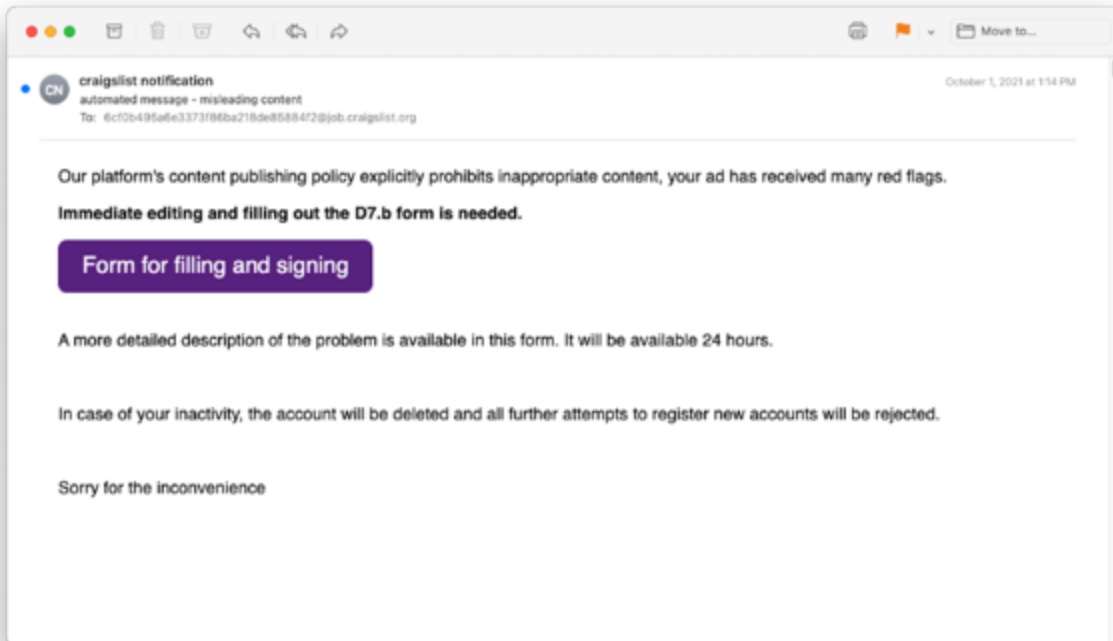
- Type: phishing
- Vector: fakes notifications sent from Craigslist
- Payload: malware hosted on abused OneDrive page
- Techniques: brand impersonation, abuse of the legitimate website
- Platform: Gsuite and Office365
- Target: Gsuite & Microsoft users

The Attack

In early October, several INKY users received real Craigslist email notifications informing them that a published ad of theirs included “inappropriate content” and violated Craigslist’s terms and conditions. The notifications gave false instructions on how to avoid having their accounts deleted.

In our analysis, we learned that a common thread among recipients of this particular phish was the fact that they were active Craigslist users. The notifications were “real” in the sense that they really did come from a Craigslist domain, but they were fake in the sense that Craigslist itself, either its humans or its machines, did not intend to send them. Without verification from Craigslist, we can't be sure, but it appears as if Craigslist was compromised since the recipients were not random (they posted ads on the platform) and the emails originated from Craigslist.

A sample email looked like this:

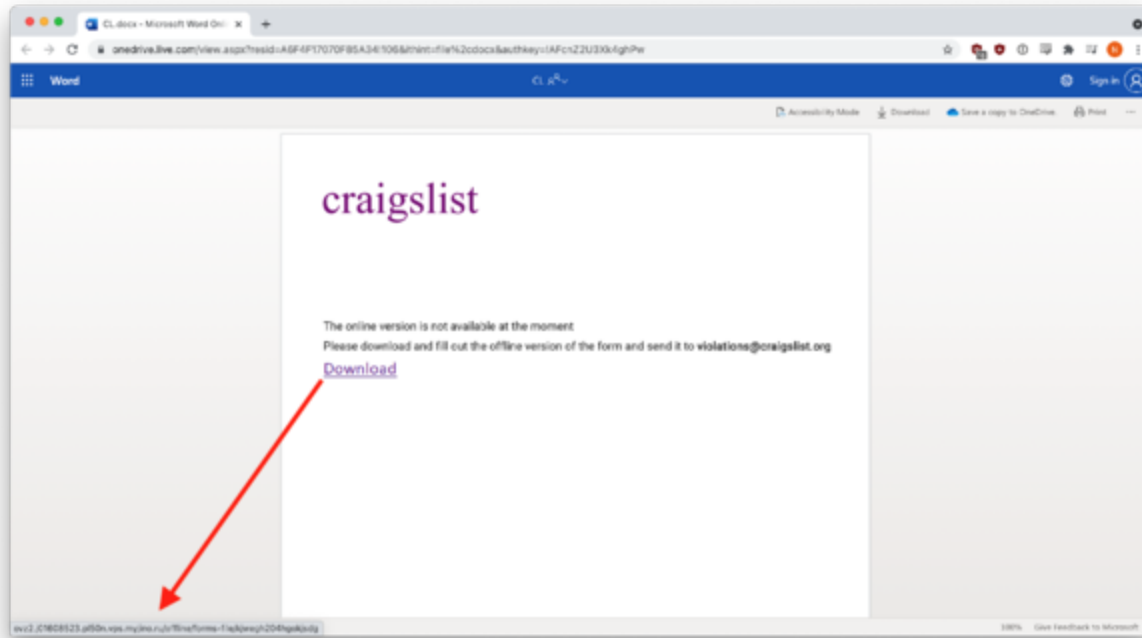


That

big purple button looks pretty tempting.

However, if a recipient tried to rectify this supposed problem by clicking on the big purple button, they were taken to a customized document uploaded to Microsoft OneDrive. It appears as if bad actors were able to manipulate the email's HTML to create that button and link it to OneDrive. Recipients were then instructed to use the "Download" link on OneDrive to fill out the form and return it to violations@craigslist.org.

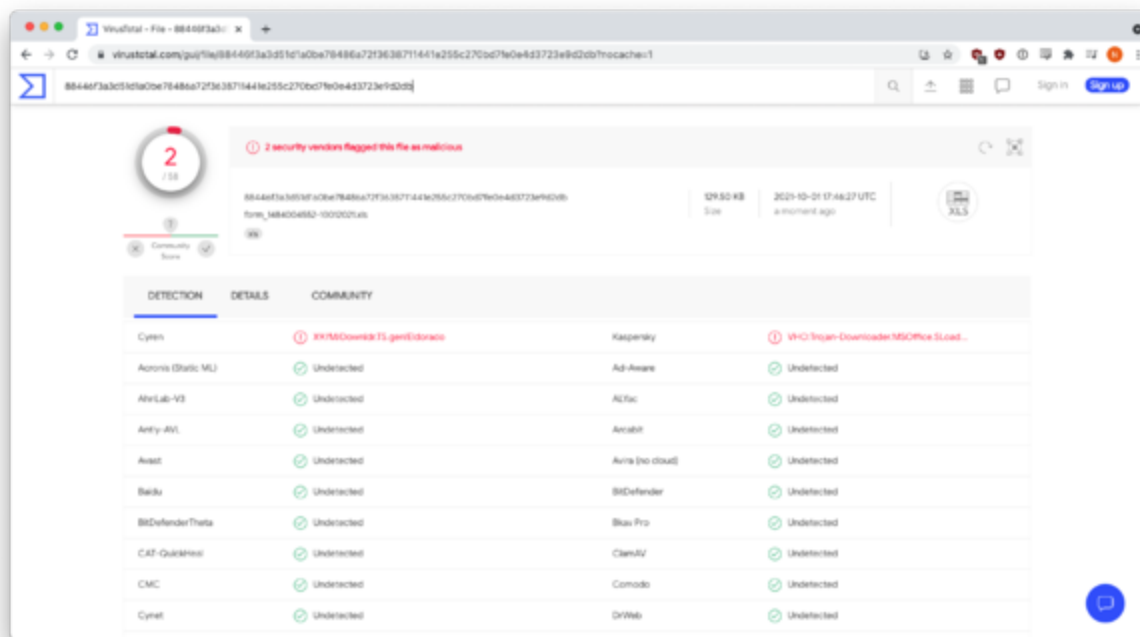
Hovering over the link revealed a Russian domain (myjino[.]ru).



Victims who clicked saw "The online version is not available at the moment" and were asked to download the form

Clicking on the link automatically downloaded a zip file named "form_1484004552-10012021.zip."

Uncompressing the file revealed a macro-enabled spreadsheet named "form_1484004552-10012021.xls," a document that had already been flagged by security vendors.



Not a good spreadsheet

The spreadsheet impersonated DocuSign and also used Norton and Microsoft logos to imply that the file was safe. DocuSign does not in fact have a service called “DocuSign Protect Service.” The company itself observed [this particular misuse](#) of its brand in a posting on the alerts section of its website from November 2020. It does have a service named “DocuSign Protect and Sign.”


DocuSign®

THIS DOCUMENT ENCRYPTED BY DOCUSIGN® PROTECT SERVICE

**This steps are required to fully decrypt the document,
encrypted by DocuSign**

1. If this document was downloaded from E-mail, then please click "Enable editing" in the yellow bar above.

example of notification

 **PROTECTED WARNING** This file originated from an internet location and might be unsafe. Click for more details.

2. Click to "Enable Content" to perform Microsoft Excel Decryption Core to start the decryption of the document.

example of notification

 **SECURITY WARNING** Macros have been disabled.

Why I can not open this document?

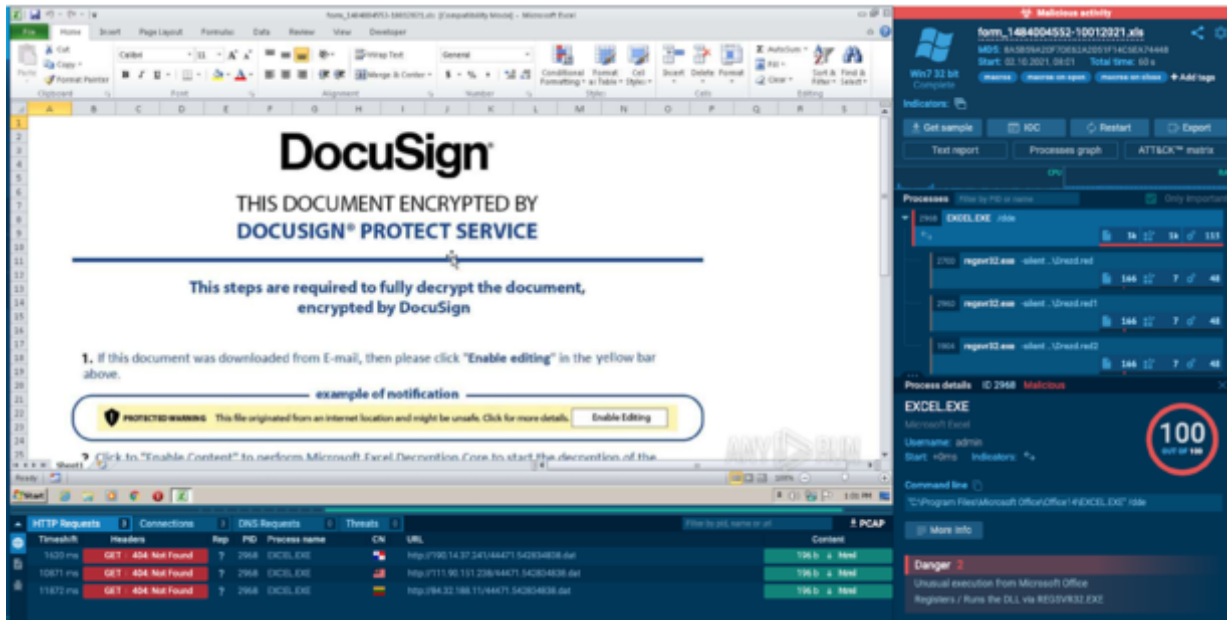
- You are using iOS or Android device. Please use Desktop PC.
- You are trying to view this document using Online Viewer.



Not DocuSign, nor Norton, much less Microsoft

Users who clicked on "Enable Editing" and "Enable Content" bypassed Microsoft Office security controls and allowed the macros to be executed.

We confirmed malicious activity in a malware sandbox. Files were created and modified. The malware also attempted to make external connections to download more components or exfiltrate data, but these attempts received a "404 not found" error.



from the sandbox

The error was likely due to a mistake on the part of the bad actors, or it's possible that the malicious content was discovered on those hosts and had already been taken down.

If this attack had been successful, some of the possible outcomes could have been:

- The installation of a remote access tool;
- A full-blown ransomware attack;
- The launching of Emotet to compromise an email account and use it to spam other recipients;
- The exfiltration of saved login credentials from a browser; or
- The installation of a keylogger.

Techniques

Sent from an authentic Craigslist IP address (208.82.237.105), these attacks looked like real Craigslist email notifications, which, because they appeared to be legitimate, were able to pass standard email authentication (SPF, DKIM, and DMARC).

```
bh=6YmcfLu5zTpv0B054niFvILLM551gqvETmFDVTm3c=;
b-IDjEKmV2jD1zxP/YS4RdMtCKcM0gEG8A@wa3AS19wf1hAkIp8ertK/tf7HUHT1q6z
h2Axgl0t8ZeD7NLPC17rZTTn/CQyxFO/P2c rNNxXSs+kpoDZ255Q99r2LC9sHXoNe2xX
RFU5oEpbCxFgQh3LI0xfUgAaHaKo+MruxuF3EN63Z8LdLyoivRf9V+FnuTBkdwd1jHe
AHZJ/ZUc@zyG/TVd9QFfkHhMxCALd59X3MHqUKfUJVL61Pk99In5xSnb1BBF7@x8+IcL
xf7nmE+rBaRaYvRXoLLKBRKsxxHxFcnhbPUKbZYJ5Ehpp0bKfg8nm58mhXoaEpJQk9e
Kymms
ARC-Authentication-Results: i=1; mx.google.com;
dkim=pass header.i=@reply.craigslislist.org header.s=reply-20200514-220940-0jgy50o3 header.b=h7GryYct;
spf=pass (google.com: domain of bounce-anon-@craigslislist.org designates 200.82.237.105 as permitted sender)
smtp.mailfrom="bounce-anon-@craigslislist.org";
dmarc=pass (p=REJECT sp=REJECT dis=NONE) header.from=reply.craigslislist.org
Received: from outbound.ashburn.craigslislist.org (mx10a.craigslislist.org. [200.82.237.105])
by mx.google.com with ESMTPS id g6s11595274vsq.417.2021.10.01.18.14.16
for <>
(version=TLS1_2 cipher=ECDHE-ECDSA-AES128-GCM-SHA256 bits=128/128);
Fri, 01 Oct 2021 10:14:16 -0700 (PDT)
Received-SPF: pass (google.com: domain of bounce-anon-@craigslislist.org designates 200.82.237.105 as permitted sender)
client-ip=200.82.237.105;
Authentication-Results: mx.google.com;
dkim=pass header.i=@reply.craigslislist.org header.s=reply-20200514-220940-0jgy50o3 header.b=h7GryYct;
spf=pass (google.com: domain of bounce-anon-@craigslislist.org designates 200.82.237.105 as permitted sender)
smtp.mailfrom="bounce-anon-@craigslislist.org";
dmarc=pass (p=REJECT sp=REJECT dis=NONE) header.from=reply.craigslislist.org
Received: outbound
DKIM-Filter: OpenDKIM Filter v2.11.0 outbound.ashburn.craigslislist.org C00A51800214
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed;
d=reply.craigslislist.org; s=reply-20200514-220940-0jgy50o3;
t=1633180456; bh=6YmcfLu5zTpv0B054niFvILLM551gqvETmFDVTm3c=;
h=From:To:Subject:Date:From;
b=h7GryYct56fx2TC/Q5VTHv5B1ej16gN0e1515JNM36yeh+72EM9czdWLP1aykEJyn
dpYxj+KnQTWwVQZVt8KwWxnQ9TAdgR4b7Kn2LNbUsyRZenQdfpJTHRZ7GF62CHn+4h
HuPK2-bXdkD9s9Vw+RJk8/JtsmsPpy@aFXPLeu0U=
From: "craigslislist notification" <6cf0b495a6e3373f86ba218de85884f2@reply.craigslislist.org>
To: 6cf0b495a6e3373f86ba218de85884f2@job.craigslislist.org
Subject: automated message - misleading content
Date: Fri, 01 Oct 2021 11:14:05 -0600
```

SPF & DKIM pass for craigslist.org

Header analysis showing legit sender

In this case, the recipient (the potential victim) had indeed posted a help-wanted listing, seeking a housekeeper in Moscow.

```
Original craigslist post:
https://pullman.craigslislist.org/lab/d/moscow-housekeeper-laundry-worker/7375197253.html
About craigslist mail:
https://craigslislist.org/about/help/email-relay
Please flag unwanted messages (spam, scam, other):
https://post.craigslislist.org/mailflag?flagCode=34&smtpid=2339b04fe9b42d653d0a44a5b80a532602be41d0.1
```

Indication of original Craigslist posting

The phishers were able to manipulate the Craigslist email system to send a fake violation notification to that individual. Since the URL to resolve the issue hosted a customized document placed on Microsoft OneDrive, it did not appear on any threat intelligence feed, allowing it to slip past most security vendors.

Recap of Techniques:

- Brand impersonation — a macro-enabled spreadsheet festooned with logos of DocuSign, Microsoft, and Norton implies safety and trust
- Abuse of cloud and web resources — bad actors send fake violation emails from Craigslist and lead victims to a legitimate but abused Microsoft OneDrive site that hosts a customized document with a malware download link
- Malware — macro-enabled spreadsheet manipulates files, attempts to download more malware from an external source to infect the victim’s machine

Best Practices: Guidance and Recommendations

Recipients should be on the lookout for unusual requests. A red flag ought to go up right away if a violation notice comes in that doesn't correspond to any recipient behavior on the platform in question.

Another red flag is the mixing of platforms. It doesn't make sense to resolve a Craigslist issue through a document uploaded to OneDrive.

Recipients should also be suspicious about the indirect way they are being asked to sign the form. Proper protocol would have the form attached directly to the email rather than requiring a trip up to OneDrive and an additional link-click there.

Fresh Phish examples were discovered and analyzed initially by Bukar Alibe, Data Analyst, INKY

Look for the next edition of INKY's Fresh Phish blog coming soon.

About INKY

Headquartered in College Park, Maryland, INKY leads the industry in mail protection powered by unique computer vision, artificial intelligence, and machine learning. The company's flagship product, INKY Phish Fence, uses these novel techniques to "see" each email much like a human does, to block phishing attacks that get through every other system. INKY founder Dave Baggett also co-founded ITA Software, the industry-leading airfare search company purchased by Google in 2011 for \$730M, which now powers Google Flights®. For more information, please visit <https://INKY.com/>.