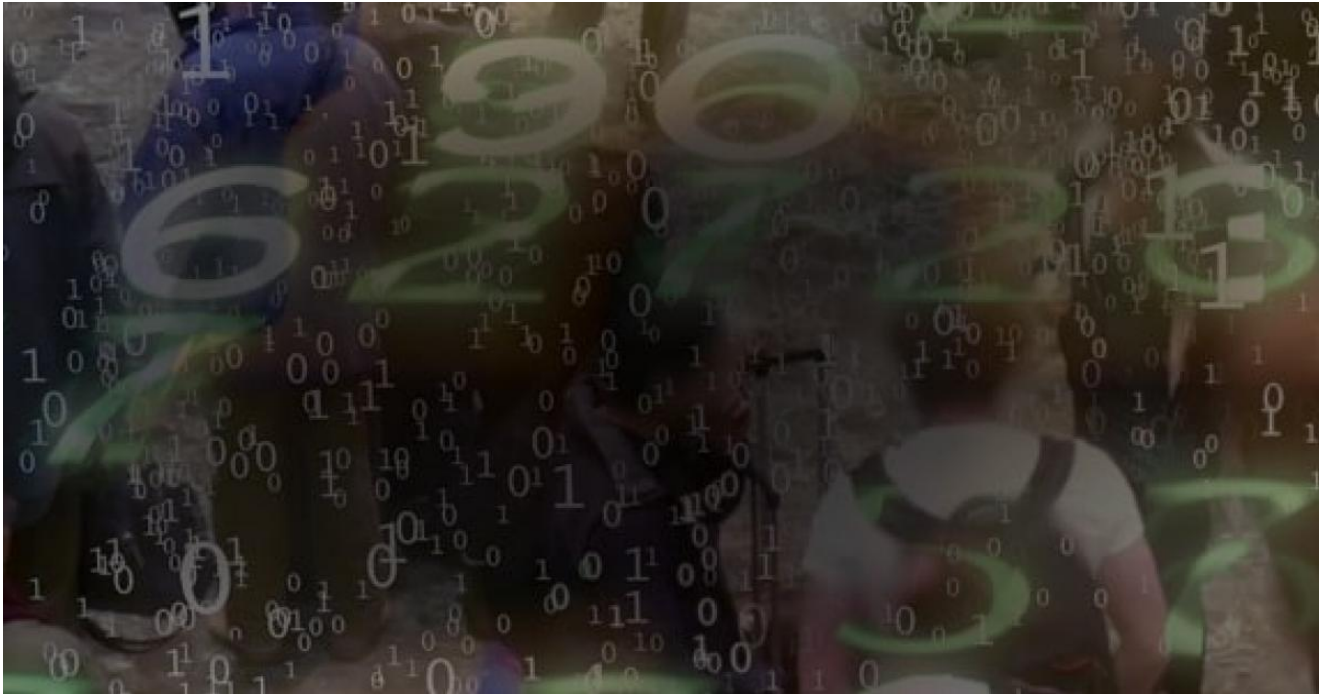


# Security Brief: TA547 Pivots from Ursnif Banking Trojan to Ransomware in Australian Campaign

 [proofpoint.com/us/blog/security-briefs/ta547-pivots-ursnif-banking-trojan-ransomware-australian-campaign](https://proofpoint.com/us/blog/security-briefs/ta547-pivots-ursnif-banking-trojan-ransomware-australian-campaign)

July 16, 2020





[Blog](#)

[Threat Insight](#)

Security Brief: TA547 Pivots from Ursnif Banking Trojan to Ransomware in Australian Campaign



July 17, 2020 Sherrod DeGrippe and the Proofpoint Threat Research Team

Proofpoint researchers have identified a ransomware and banking trojan campaign that occurred July 12-14, 2020 and targeted multiple verticals in Australia. The campaign pivoted from distributing the Ursnif banking trojan in early messages to later distributing Adhubllka ransomware, which encrypts files on compromised systems. While this campaign was widely distributed across industries, construction, transportation, entertainment and media, aerospace, and manufacturing were among the most commonly observed.

Proofpoint researchers believe this campaign is the work of TA547, an actor known for abusing email service providers and distributing banking trojans across various geographic regions. This campaign is also the latest example of TA547 targeting Australians. A prior effort included a ZLoader banking malware campaign disguised as job applicant emails.

In this case over 2,000 messages were sent during July 12-14 with lures informing intended recipients that their order “has been processed” and urging them to their view their “order details.” The subject lines contained “salesforce.com Order Confirmation” followed by a fake order number.

The messages contain Microsoft Excel attachments (Figure 1) or URLs linking to Excel documents hosted by an email service provider (Figure 2).

info@printmycup.com ☆ To [redacted].au> ☆  
salesforce.com Order Confirmation 81515/500 -AU 12/07/2020 à 23:57

Your Quote# Q-81515500 has been processed. Order# 81515/500 was activated on 7/12/2020 2:16 PM. Your Contract Start Date is 7/13/2020 and your Contract End Date is 6/20/2021.

Your order details attached below.

Thank you for your business.

1 attachment: QO-81515500.xlsb 40,8 KB Save


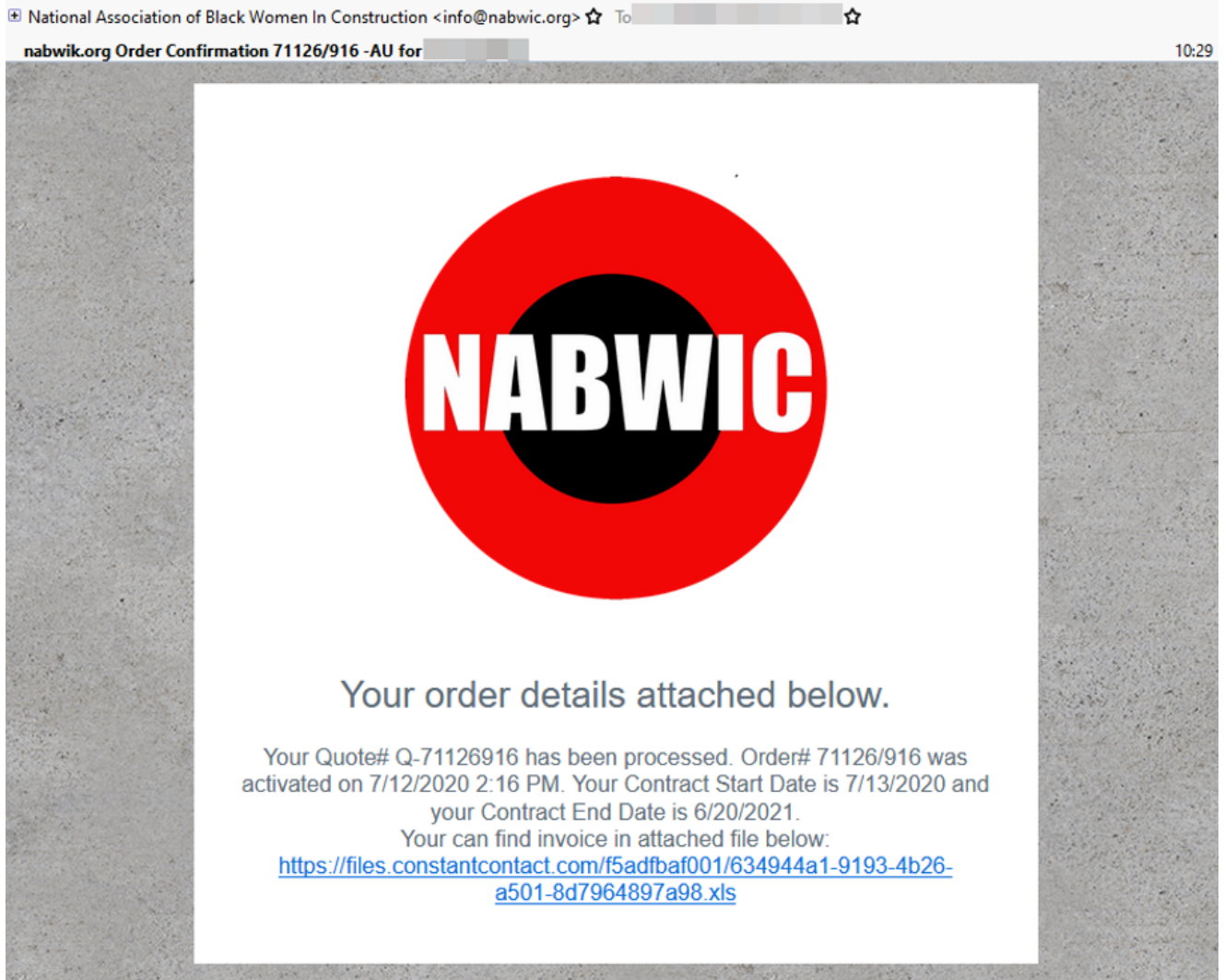
 QO-81515500.xlsb 40,8 KB

Figure 1: Malicious Microsoft Excel attachment



National Association of Black Women In Construction | 6600 NW 27th Avenue, Suite 208,  
Miami, FL 33147-7220

[Unsubscribe](#)

[Update Profile](#) | [About Constant Contact](#)

Sent by info@nabwic.org in collaboration with

**Constant Contact**

Try email marketing for free today!

Figure 2: Link to malicious Excel document

The email lure with malware attached (Figure 1) is not particularly interesting or customized, but the lure that contains a link to the malware (Figure 2) is a bit more creative. It contains a lure with branding for a construction workers' resource group, which is notable because the construction industry was one of the sectors most targeted in this campaign.

In initial messages, the files used XL4 macros (Figure 3) to download Ursnif but shifted to downloading Adhubllka ransomware on July 13 around 08:00am GMT (Figure 4).

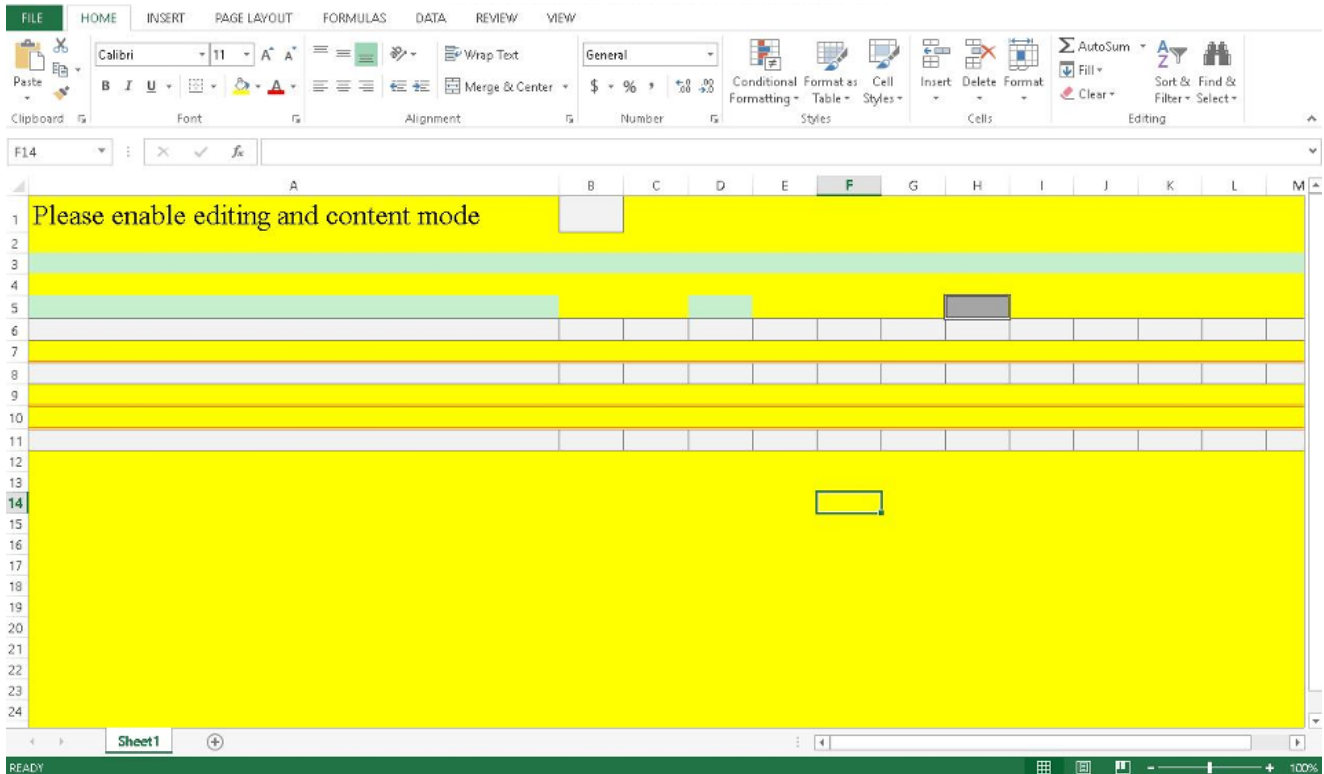


Figure 3: Excel document containing malicious macros

The pivot to delivering a new payload isn't unusual on its own, but it is unclear why the actor switched away from using highly valuable crimeware like Ursnif to Adhubble ransomware.

```
Attention!  
  
All your files, documents, photos, databases and other important files are encrypted  
  
The only method of recovering files is to purchase an unique decryptor. Only we can give you this decryptor and only we can recover your files.  
  
The server with your decryptor is in a closed network TOR. You can get there by the following ways:  
  
-----  
1. Download Tor browser - https://www.torproject.org/  
2. Install Tor browser  
3. Open Tor Browser  
4. Open link in TOR browser: http://7rzpvw3hflwe2c7h.onion/?  
5. Follow the instructions on this page  
  
-----  
  
On our page you will see instructions on payment and get the opportunity to decrypt 1 file for free.  
  
Alternate communication channel here: http://helpgvxg3cc5mvp3.onion/
```

Figure 4: Ransomware note

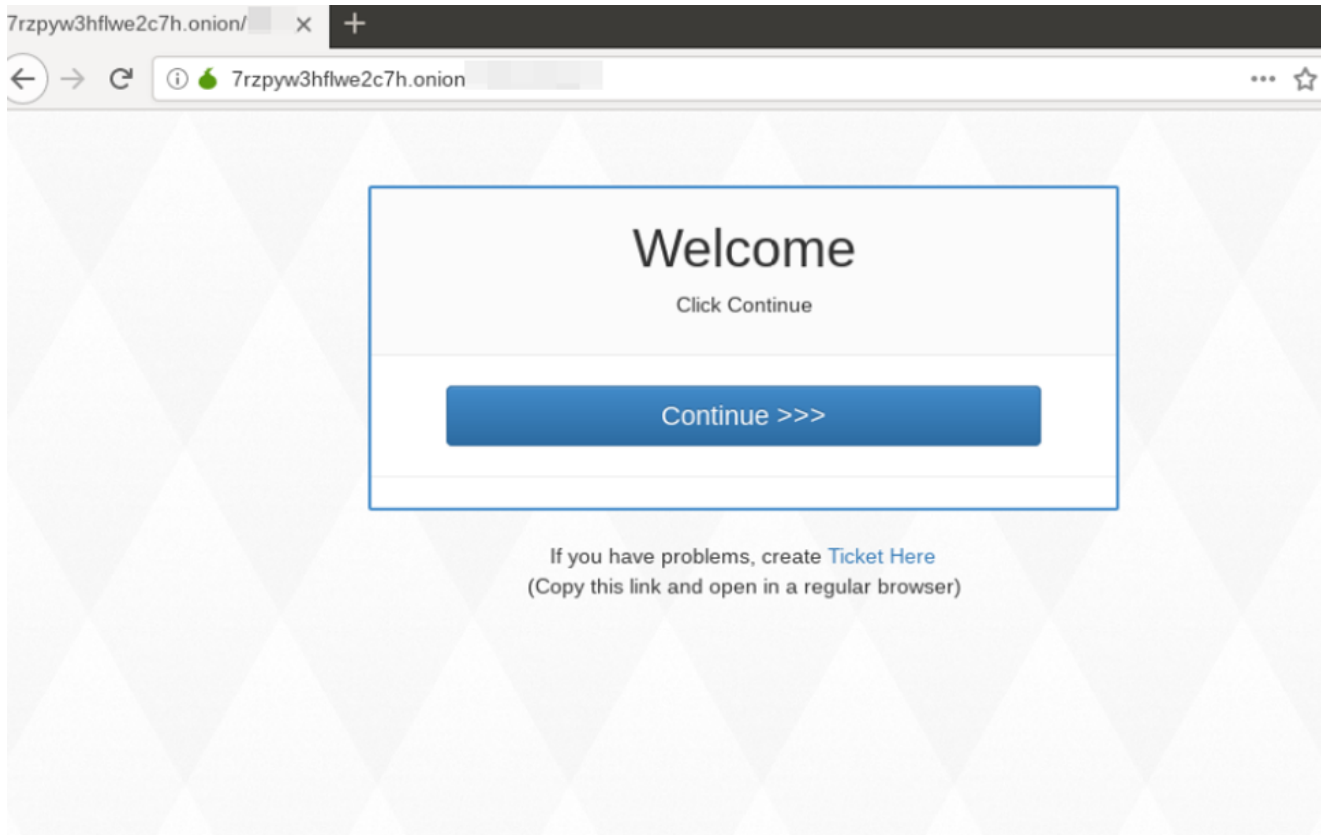


Figure 5: Ransomware payment page

The initial payment page for Adhubllka includes a link to a Freshdesk ticketing software instance. The link is behind a URL shortener that collects the victim's IP address if they visit the link to report an issue. The actor might be suggesting the victim visit the ticketing site in a browser other than Tor because it isn't a .onion link, but this could also be an attempt to collect the victim's unmasked IP address.

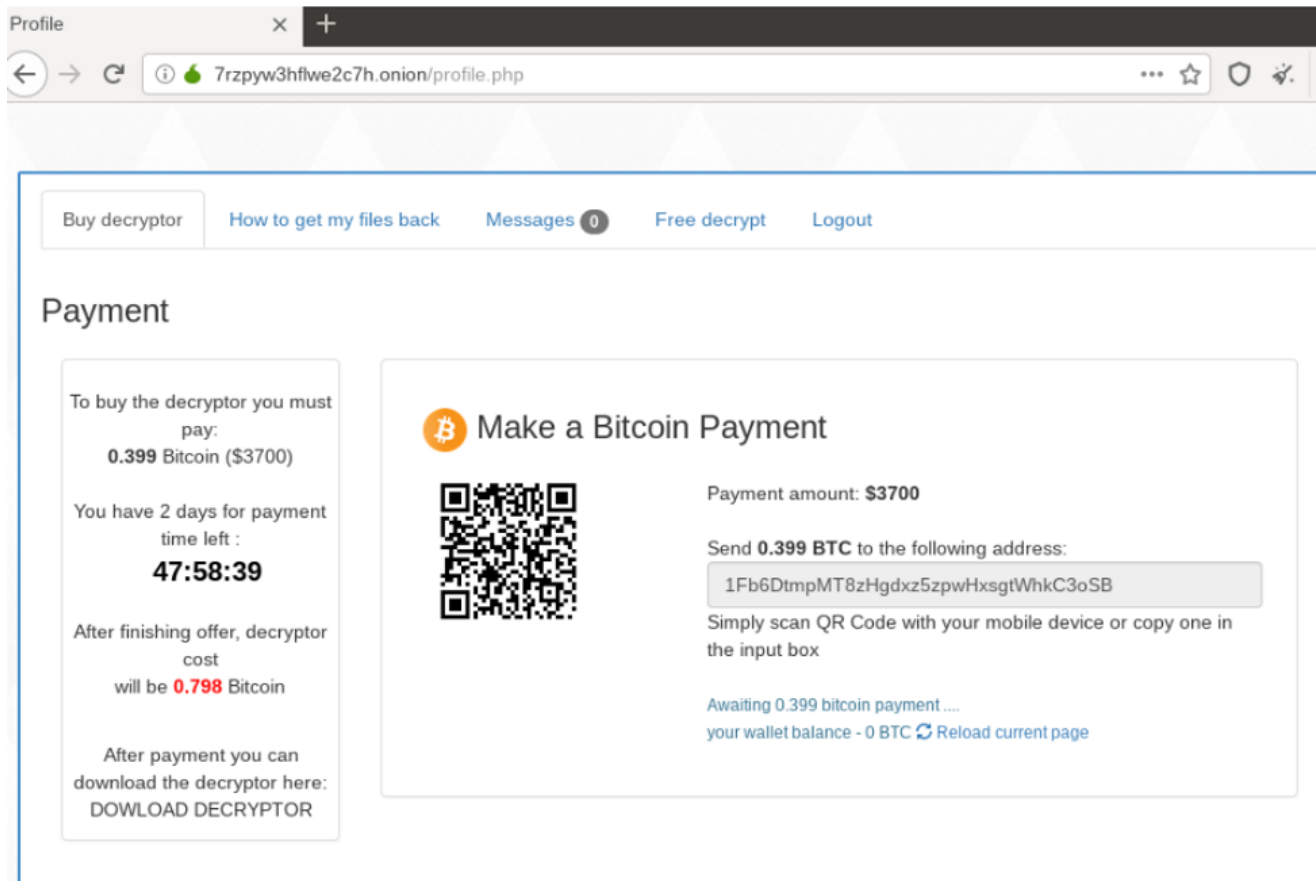


Figure 6: Ransomware payment portal

The ransom of \$3,700 is requested in bitcoin, complete with a QR code to facilitate the transaction. Instructions for creating a bitcoin wallet are found on the “How to get my files back” tab of the site.

As of this publication, the Tor site is still online, though no transactions involving associated bitcoin addresses appear to have taken place.

The techniques used in this campaign are not uncommon for TA547, but the mid-campaign payload switch is unusual. While the motivation for the switch isn’t immediately clear, it’s possible that the actor is experimenting with different payloads, or simply wants different types of infections at their disposal.

Subscribe to the Proofpoint Blog