Blox Tales #6: Subpoena-Themed Phishing With CAPTCHA Redirect

armorblox.com/blog/blox-tales-6-subpoena-themed-phishing-with-captcha-redirect/

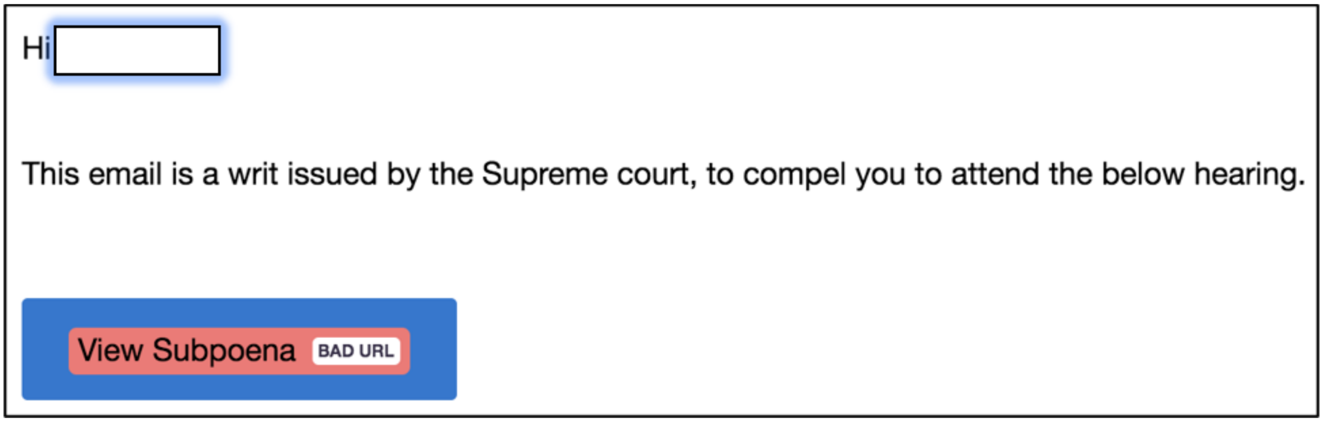
Back

Written by Abhishek Iyer
Threat Research / 5.21.20

Each Blox Tales blog will take a look at a targeted email attack, outline why it made its way into an inbox, and highlight how Armorblox was able to detect the attack. In this blog, we'll focus on a new variant of the subpoena phishing attack. This email used multiple redirects, **including a functioning CAPTCHA page**, to lure users into giving up their Office 365 credentials.

The Attack

A few days ago, we saw a credential phishing email hit multiple customer environments. This email claimed to come from the Supreme Court and included a zero-day link that was masked as a subpoena. Clicking the link took the targets through multiple redirects, including a fully-functioning CAPTCHA page that increased the legitimacy of the communication. The final credential phishing page resembled an Office 365 login portal, designed to make targets part with their Office 365 credentials. A snapshot of the email is given below:



Hi [redacted]

This email is a writ issued by the Supreme court, to compel you to attend the below hearing.

Fig: Email where attackers impersonate the Supreme Court and direct targets to view the subpoena

This attack is a variant of **last year's subpoena themed phishing attack** that surfaced in the UK, where attackers impersonated the UK Ministry of Justice. Last year's attack infected target endpoints with publicly-available information stealing malware called *Predator the Thief.*

This current variant of the attack is tougher to detect because it avoids known malware and instead opts for a zero-day credential phishing page.

Why The Attack Got Through

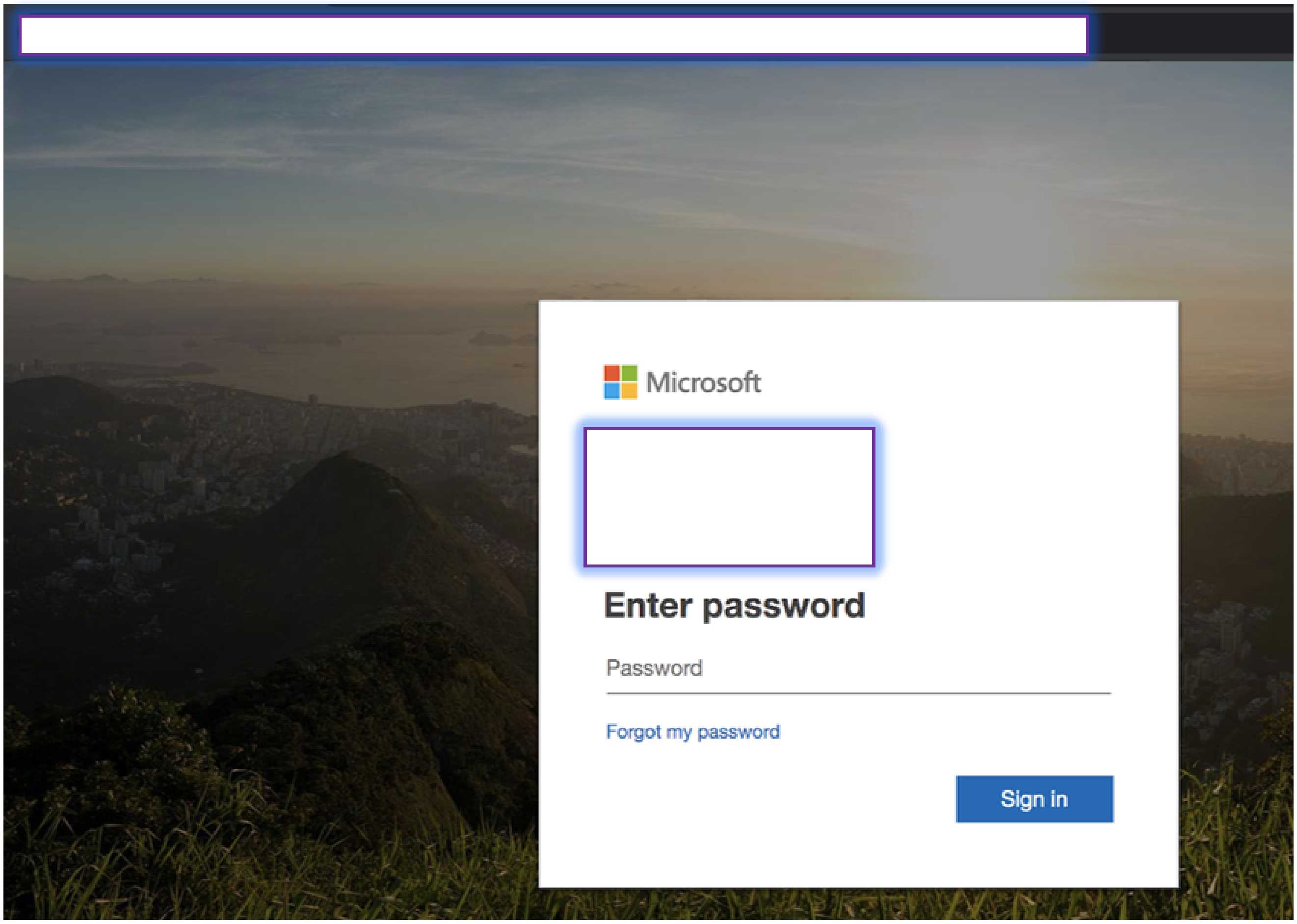
This email got past existing Office 365 and gateway security controls because it didn't follow the tenets of more traditional phishing attacks.

1. Not a mass email

Although multiple Armorblox customers were hit with this attack, this was not a bulk email. Only a few people in each target organization received it. This ensured that the email wasn't caught in the bulk email filters of Exchange Online Protection (EOP).

2. Zero-day link and lookalike website

The attacker created a new domain for the link in this email attack, so it got past any EOP filters that were created to block known bad links. The final credential phishing page was painstakingly made to resemble an Office 365 login page. A screenshot is presented below:



[redacted]

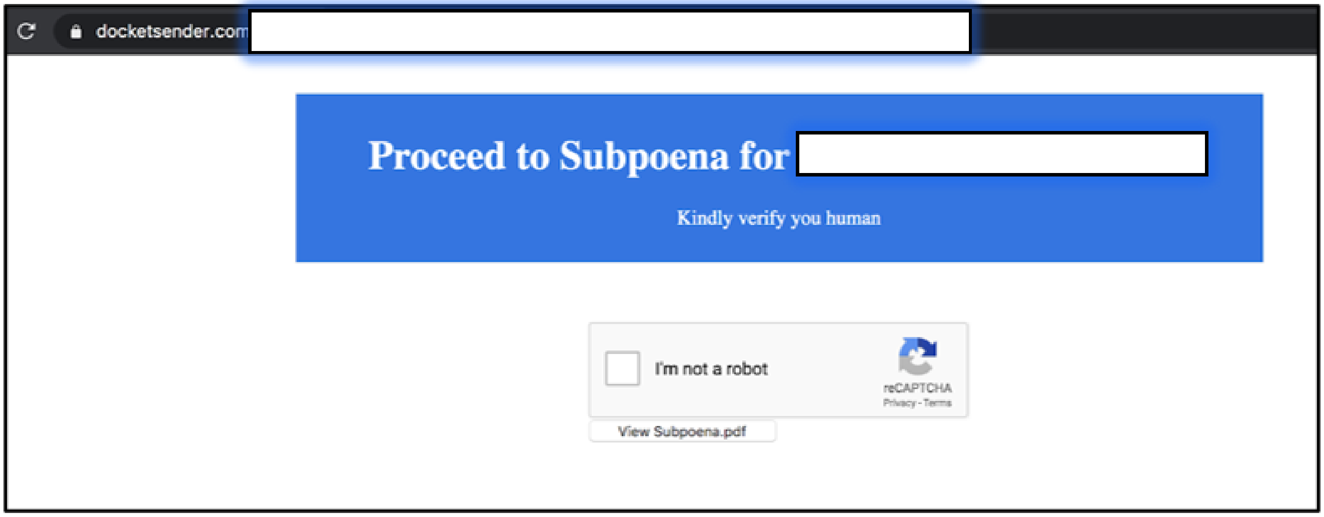
[redacted]

Fig: Final credential phishing page made to resemble an Office 365 login page

This page would pass most eye tests during busy mornings, with people happily assuming it to be a legitimate Microsoft page. A closer look at the domain reveals that this is a lookalike page built specifically for the target. The master domain for the page is ‘invoicesendernow[.]com’ which is clearly not a Microsoft page.

3. Leverages CAPTCHA for legitimacy

The penultimate URL redirect in this attack leads users to a fully functioning CAPTCHA page. Upon clicking the *‘I’m not a robot’* button, a real CAPTCHA image test pops up, stamping a clear seal of legitimacy on the email communication. The inclusion of CAPTCHA also makes it harder for security technologies relying just on URL redirection abilities to follow the URL to its final destination. Screenshots of both CAPTCHA pages are given below:

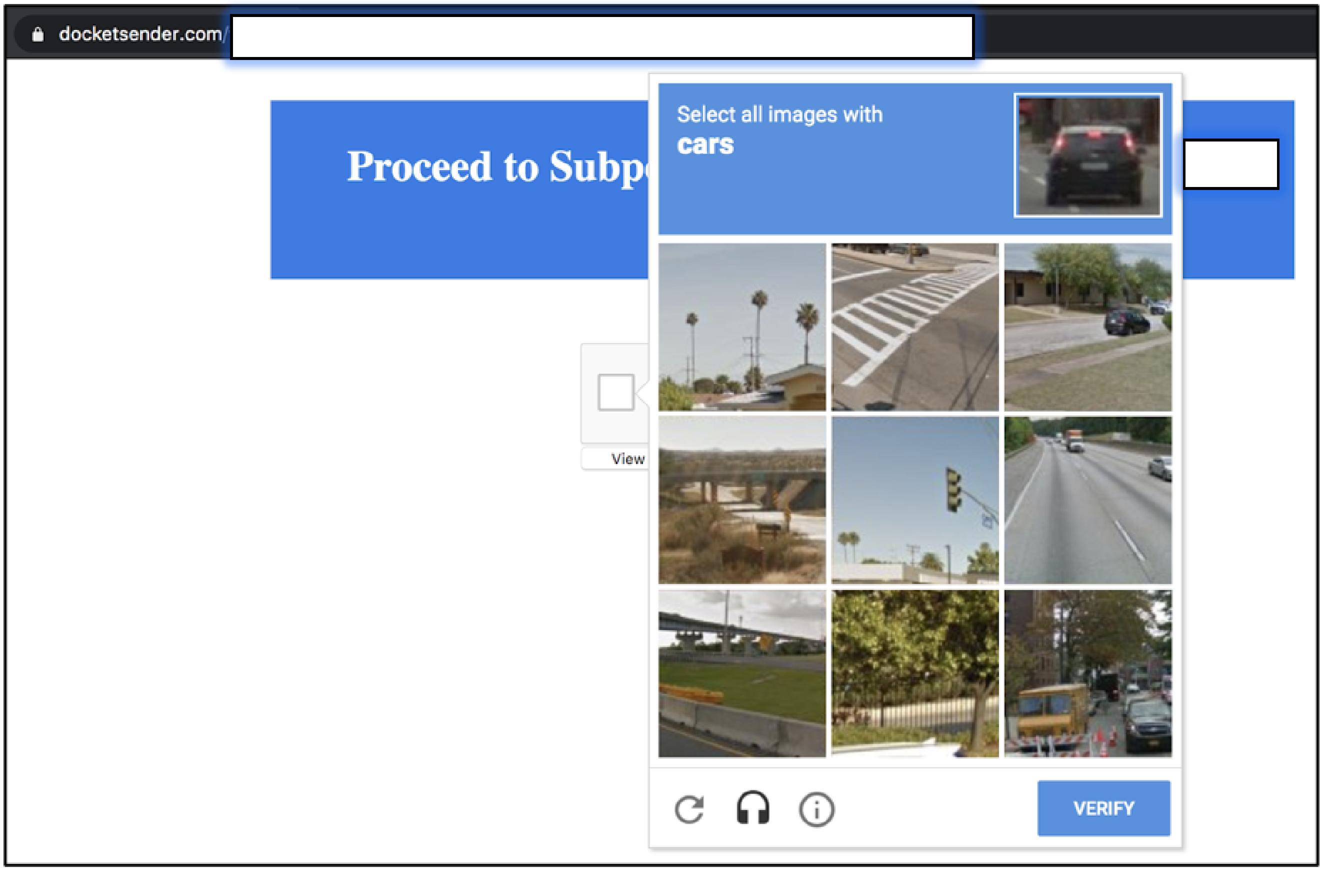


docketsender.com[redacted]

Proceed to Subpoena for [redacted]

Kindly verify you human

Fig: The page introducing the CAPTCHA test.



docketsender.com/[redacted]

Proceed to Subp [redacted]

Select all images with **cars**

Fig: Screenshot of the CAPTCHA test.

A closer look at both CAPTCHA pages reveals some irregularities. The master domain of the pages is ‘docketsender[.]com’ that, while not malicious, doesn’t seem like a legitimate domain. In the first screenshot, the subheading reads ‘*Kindly verify you human*’. This grammatical error tells users this is not a real CAPTCHA page, but unfortunately it’s a minor error that we’re likely to rush past in our daily lives.

4. Socially engineered

Unlike spray-and-pray email fraud attempts, this email was expressly created and sent to trigger the required response. The sender name impersonated the Supreme Court, making the email likely to get past eye tests when people glanced through it amidst hundreds of other emails in their overflowing mailboxes. The email language was terse and authoritative, including a CTA (call to action) in the email - *View Subpoena* - clearly describing the purpose of the email.

How Armorblox Detected The Attack

Armorblox was able to detect the email attack based on the following insights:

1. Language, intent, and tone

Armorblox language models have been trained on tons of data and further customized to suit every customer environment. These models analyzed the email body and detected that there was an unusual request made in the email (which is a common trait in **business email compromise** attacks).

2. Low communication history

Armorblox detected that the sender email in question had a low communication history with the victim's email account. While not a violation in itself, this insight is critical when compared with other unusual signals and can catch highly targeted attacks.

3. Low domain frequency

Armorblox ML models have three tiers - a global model, an organization-specific model, and a mailbox-specific model. While the mailbox-specific model was able to detect low communication history between the sender and the receiver, the organization-specific model also detected that the attacker's domain had not communicated with the target company as a whole.

Based on the insights above, along with many other detection signals, Armorblox flagged the email as a credential phishing threat. The email was automatically quarantined based on predetermined remediation actions for the credential phishing detection category.

Stay tuned for more Blox Tales! If you're interested to learn about Armorblox, you can **schedule a demo** with one of our email security experts.

To learn how Armorblox augments native Office 365 email security, download our whitepaper below.

Get Whitepaper