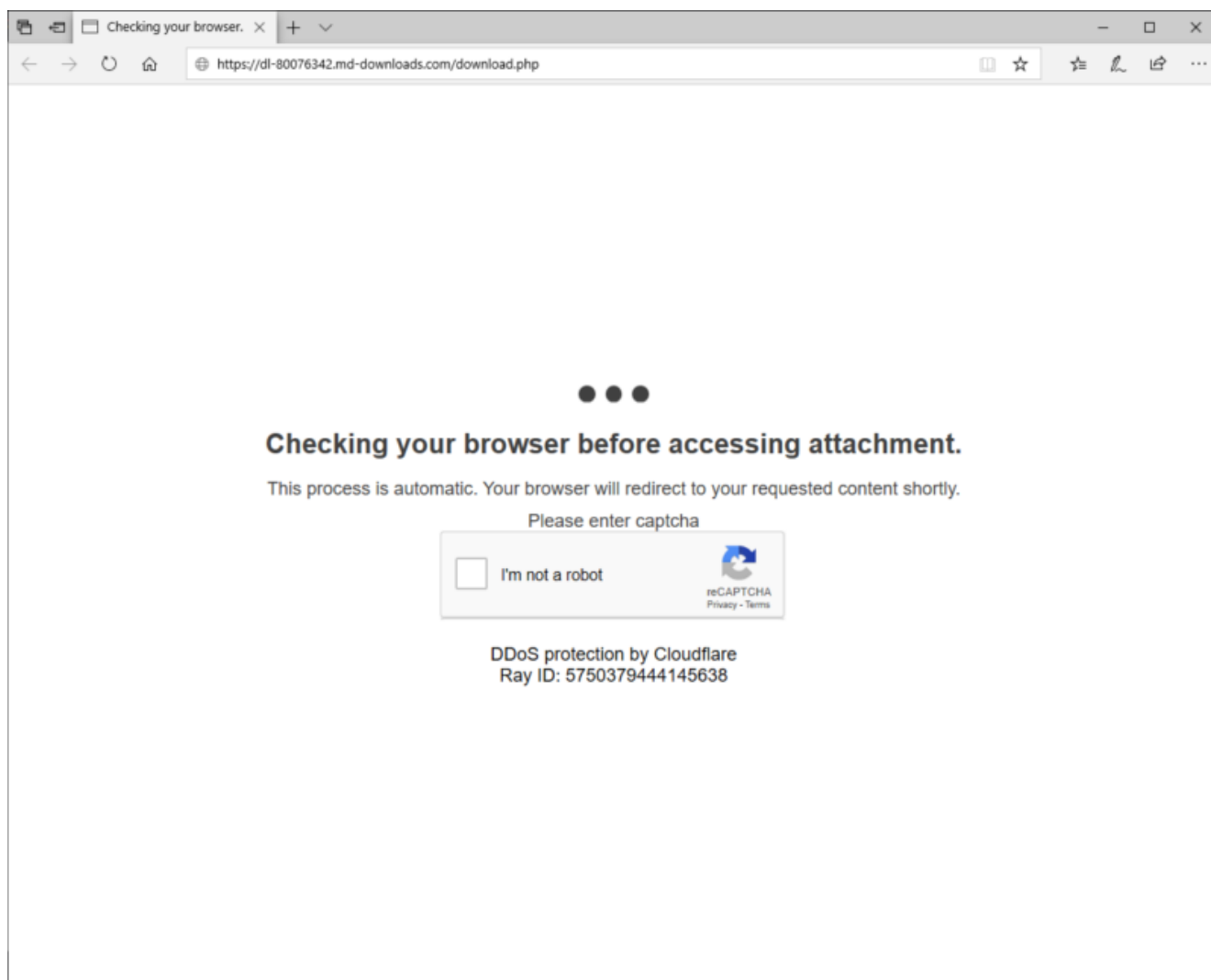


To evade detection, hackers are requiring targets to complete CAPTCHAs



Microsoft Security Intelligence

reader comments

48 with 37 posters participating

Share this story

CAPTCHAs, those puzzles with muffled sounds or blurred or squiggly letters that websites use to filter out bots (often unsuccessfully), have been annoying end users for more than a

decade. Now, the challenge-and-response tests are likely to vex targets in malware attacks.

Microsoft recently spotted an attack group distributing a malicious Excel document on a site requiring users to complete a CAPTCHA, most likely in an attempt to thwart automated detection by good guys. The Excel file contains macros that, when enabled, install GraceWire, a trojan that steals sensitive information such as passwords. The attacks are the work of a group Microsoft calls Chimborazo, which company researchers have been tracking since at least January.

Previously, Microsoft observed Chimborazo distributing the Excel file in attachments included in phishing messages and later spreading through embedded Web links. In recent weeks, the group has begun sending phishing emails that change things up again. In some cases, the phishes include links that lead to redirector sites (usually legitimate sites that have been compromised). In other cases, the emails have an HTML attachment that contains a malicious iframe tag.

Either way, clicking on the link or attachment leads to a site where targets download the malicious file, but only after completing the CAPTCHA (which is short for completely automated public Turing test to tell computers and humans apart). The purpose: to thwart automated analysis defenders use to detect and block attacks and get attack campaigns shut down. Typically the analysis is performed by what are essentially bots that download malware samples and run and analyze them in virtual machines.

Requiring the successful completion of a CAPTCHA means analysis will only happen when a live human being downloads the sample. Without the automation, the chances of the malicious file flying under the radar are much better. Microsoft has dubbed Chimborazo's ongoing attack campaign Duedear.

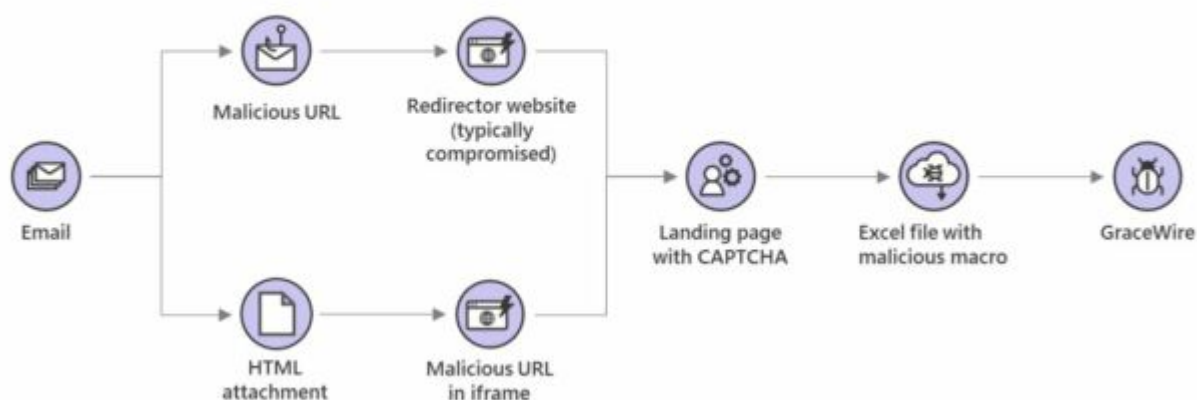
“CHIMBORAZO, the group behind Dudear campaigns that deploy the info-stealing Trojan GraceWire, evolved their methods once again in constant pursuit of detection evasion,” Microsoft’s Security Intelligence group wrote in a Tweet on Wednesday. “The group is now using websites with CAPTCHA to avoid automated analysis.”

CHIMBORAZO, the group behind Dudear campaigns that deploy the info-stealing Trojan GraceWire, evolved their methods once again in constant pursuit of detection evasion. The group is now using websites with CAPTCHA to avoid automated analysis. pic.twitter.com/Kz3cdwYDd7

– Microsoft Security Intelligence (@MsftSecIntel) June 17, 2020

The attack flow looks like this:

CHIMBORAZO attack chain (June 2020)



Microsoft Security Intelligence

In a campaign the Security Intelligence group covered in January, Chimborazo used an IP traceback service to track the IP addresses of machines that download the malicious Excel file, presumably to also evade automated detection. Back then, it was the first time Microsoft had seen Chimborazo use redirector sites.

Jérôme Segura, head of threat intelligence at security provider Malwarebytes, said using CAPTCHAs in malware attacks is rare but not unprecedented. He pointed to this tweet from late December that was doing the same thing. In that case attackers required targets to complete a CAPTCHA that was a knock off of Google's reCAPTCHA service. While fake, it served the same purpose as a real one—to thwart automated analysis by requiring a real person to download the file.

The CAPTCHA spotted by Microsoft may also be a fake reCAPTCHA. The evidence: as seen in the image at the top of this post, it says reCAPTCHA and below that claims to provide “DDoS protection by Cloudflare.” Those are two separate services. (Then again, as one commenter points out, it's possible the attackers used both services separately.) Google representatives didn't immediately respond to an email seeking comment for this post.

Periodically changing up attack routines is one way attackers stay ahead of defenders, creating a never-ending back-and-forth process that requires constant vigilance for defenders to stay on top of. It's likely the attack group will change course again in the coming months.

Post updated to add comments in the second-to-last paragraph.

<https://arstechnica.com/?p=1684769>