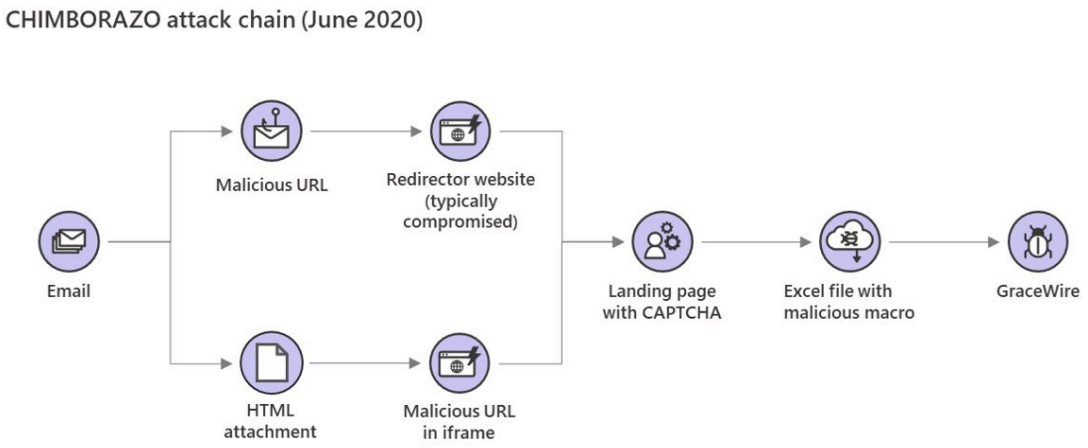
To evade detection, hackers are requiring targets to complete CAPTCHAs

By Dan Goodin

Published: 2020-06-18 · Archived: 2026-04-05 20:36:07 UTC

“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.”

The attack flow looks like this:



Credit: Microsoft Security Intelligence

Credit: 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.
