Criminals spread malware using website contact forms with Google URLs

zdnet.com/article/criminals-spread-malware-using-website-contact-forms-with-google-urls

Liam Tung

Microsoft is warning businesses to beware of cyber criminals using company website contact forms to deliver the IcedID info-stealing banking trojan in email with Google URLs to employees.

Company website 'contact us' forms are an open doorway on the internet and criminals have recently started using them to reach workers who receive contact requests from the public.

A notable feature of the attack is that the crooks are using the contact forms to send employees legitimate Google URLs that require users to sign in with their Google username and password.

Microsoft considered the threat serious enough to report the attacks to Google's security teams to warn them that cyber criminals are using legitimate Google URLs to deliver malware. The Google URLs are useful to the attackers because they will bypass email security filters. The attackers appear to have also bypassed CAPTCHA challenges that are used to test whether the contact submission is from a human.

"Attackers are abusing legitimate infrastructure, such as websites' contact forms, to bypass protections, making this threat highly evasive. In addition, attackers use legitimate URLs, in this case Google URLs that require targets to sign in with their Google credentials," the Microsoft 365 Defender Threat Intelligence Team notes.

Microsoft is concerned by the technique used and has currently detected the criminals using the URLs in email to deliver IcedID malware. But it could just as easily be used to transmit other malware.

IcedID is a banking trojan and information stealer and can be used as an entry point for subsequent attacks, such as manually operated ransomware for high-value targets. Human-operated ransomware attacks are increasingly common and require the attacker to sit at the keyboard and orchestrate the attack, in contrast to an automated attack.

"We have already alerted security groups at Google to bring attention to this threat as it takes advantage of Google URLs," Microsoft said.

"We observed an influx of contact form emails targeted at enterprises by means of abusing companies' contact forms. This indicates that attackers may have used a tool that automates this process while circumventing CAPTCHA protections," the company added.

This is a tricky attack for companies and government agencies to detect since the email arrives to employees from their own contact form and email marketing systems.

"As the emails are originating from the recipient's own contact form on their website, the email templates match what they would expect from an actual customer interaction or inquiry," Microsoft notes.

The attackers use language that applies pressure on the employee to respond – false claims that the targeted website is using copyrighted images, for example. The email contains a link to a sites.google.com page where the employee is meant to view the supposedly infringing images.

If the employee does their job and investigates the claim by signing into the site, the sites.google.com page automatically downloads a ZIP file with a JavaScript file, which in turn downloads IcedID malware as a .DAT file. It also downloads a component of the penetration-testing kit, Cobalt Strike, that allows the attacker to control the device over the internet.