TA575 criminal group using 'Squid Game' lures for Dridex malware

By Written by Jonathan Greig, ContributorContributor Oct. 29, 2021 at 1:36 p.m. PT

Archived: 2026-04-05 15:52:52 UTC

ZDNET Recommends

Cybersecurity firm Proofpoint has found evidence of a prolific cybercrime group using the popularity of Netflix hit "Squid Game" to spread the Dridex malware.

In a blog post, Proofpoint said TA575 -- a "large cybercrime actor" -- has sent emails pretending to be someone working on the show, urging people to download malicious attachments or fill out forms with sensitive information.

The emails come with subject lines saying things like: "Squid Game is back, watch new season before anyone else," "Invite for Customer to access the new season," "Squid game new season commercials casting preview," and "Squid game scheduled season commercials talent cast schedule."

Proofpoint said it found thousands of emails using the lures that targeted a variety of industries in the US. Some of the emails try to lure victims in by saying they could be in the show if they download a document and fill it out.

Proofpoint

"The attachments are Excel documents with macros that, if enabled, will download the Dridex banking trojan affiliate id '22203' from Discord URLs," Proofpoint researchers Axel F and Selena Larson wrote.

Sherrod DeGrippo, vice president of threat detection and response at Proofpoint, told *ZDNet* that Dridex is a banking trojan used to siphon money directly from the victim's bank account.

"But Dridex is also used for information gathering or as a malware loader that can lead to follow-on infections such as ransomware," DeGrippo added.

Proofpoint has been tracking TA575 since late 2020, noting that the group typically distributes Dridex through "malicious URLs, Microsoft Office attachments, and password-protected files." The gang uses a variety of lures to get victims to click on links or download documents, often playing off of pop culture or deploying invoice-related language in emails.

"On average, TA575 sends thousands of emails per campaign, impacting hundreds of organizations. TA575 also uses the Discord content delivery network (CDN) to host and distribute Dridex," the Proofpoint researchers said, adding that Discord has become a "popular malware-hosting service for cybercriminals."

Cybersecurity experts like ThreatModeler CEO Archie Agarwal said the TA575 criminal group is made up of prolific, financially-motivated opportunists who specialize in Dridex malware and operate swaths of Cobalt Strike servers.

Both the Dridex malware and Cobalt Strike servers are examples of repurposing the work of others, Agarwal said, explaining that Dridex dates back as far as 2015 and was known for specializing in banking credentials theft.

Hank Schless, Lookout senior manager of security solutions, said that throughout the COVID-19 pandemic, cybercriminals have used a variety of hooks related to the vaccine or government aid as a lure for emails with malicious attachments.

Lookout data shows threat actors are heavily targeting users through mobile channels such as SMS, social media platforms, third-party messaging apps, gaming, and even dating apps. He added that one of the most interesting parts of the report is that TA575 uses the Discord CDN to host and deliver the malware.

"This practice of using legitimate services as an intermediary command and control server is becoming more common. We frequently see it with data storage platforms like Dropbox as well. Attackers do this because it may help them slip by any detections more easily if the traffic looks legitimate," Schless said.

Security
