


TA575 Uses 'Squid Game' Lures to Distribute Dridex malware

 proofpoint.com/us/blog/threat-insight/ta575-uses-squid-game-lures-distribute-dridex-malware

October 28, 2021





[Blog](#)

[Threat Insight](#)

TA575 Uses 'Squid Game' Lures to Distribute Dridex malware



October 28, 2021 Axel F and Selena Larson

Proofpoint identified the large cybercrime actor TA575 distributing Dridex malware using Squid Game lures. The threat actor is purporting to be entities associated with the Netflix global phenomenon using emails enticing targets to get early access to a new season of Squid Game or to become a part of the TV show casting.

On October 27, 2021, Proofpoint observed thousands of emails targeting all industries primarily in the United States. The emails used subjects such as:

- Squid Game is back, watch new season before anyone else.
- Invite for Customer to access the new sesason. [sic]
- Squid game new season commercials casting preview
- Squid game scheduled season commercials talent cast schedule

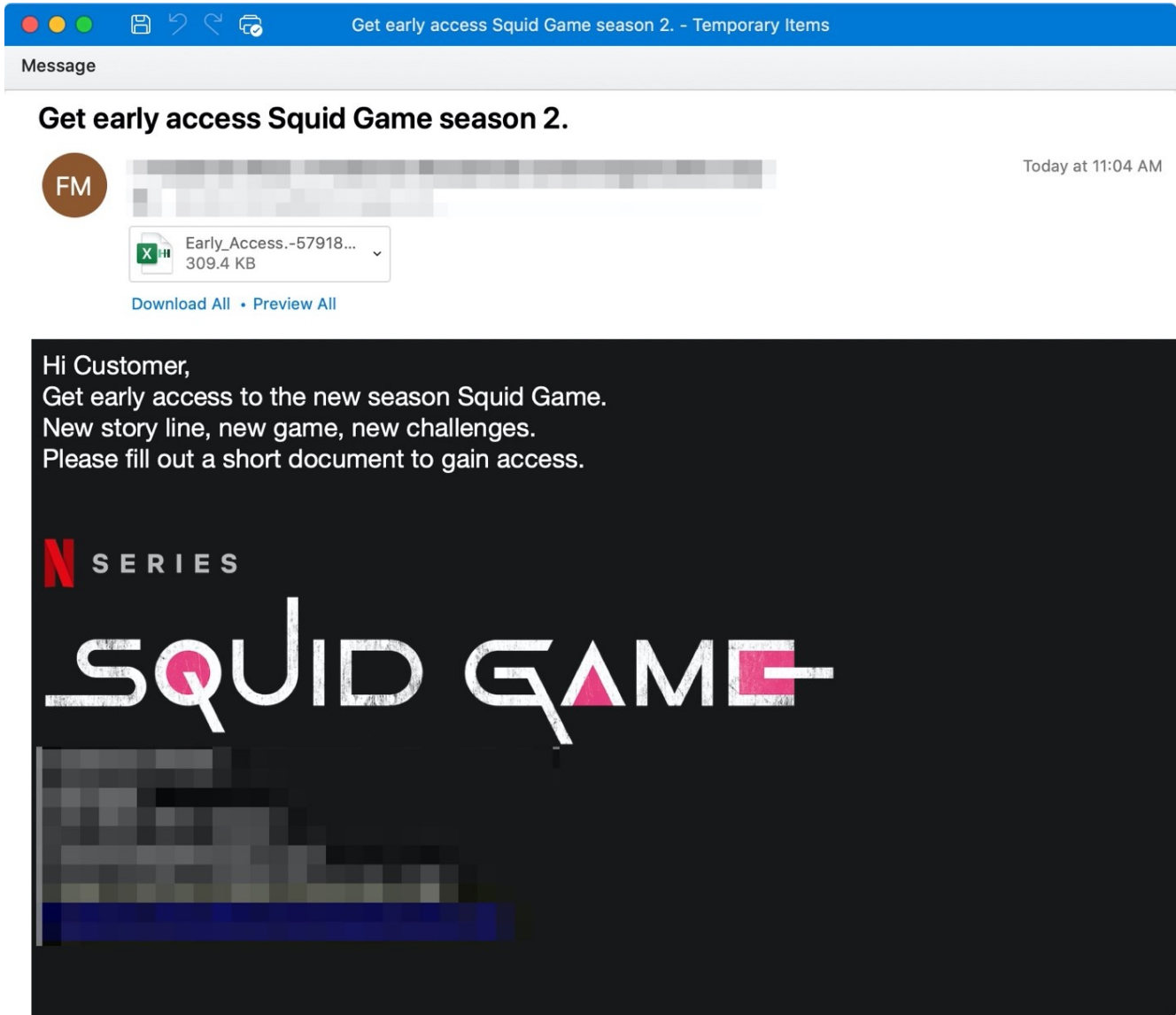


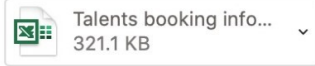
Figure 1: Netflix Squid Game email lure inviting customers to get early access to a new season

Message

Squid game upcoming season commercials talent casting



Yesterday at 11:11 AM



[Download All](#) • [Preview All](#)

Adult Talent Onboarding/Registration

Become a part of [redacted]'s legendary casting platform. Registration for background casting in [redacted] is free and easy. Complete both steps so you can get booked on next season of Squid Game TV show.



Make a reservation

Gather your [required documentation](#), then fill in casting papers of a reservation for a Talent Onboarding session.



Figure 2: Netflix Squid Game email lure soliciting actors and background talent to apply to be on the show or show commercials

The emails tell the victim to fill out either an attached document to get early access to the new season of the show or a talent form to become part of the background casting. The attachments are Excel documents with macros that, if enabled, will download the Dridex banking trojan affiliate id "22203" from Discord URLs. Dridex is a prolific banking trojan distributed by multiple affiliates that can lead to data theft and installation of follow-on malware such as ransomware.

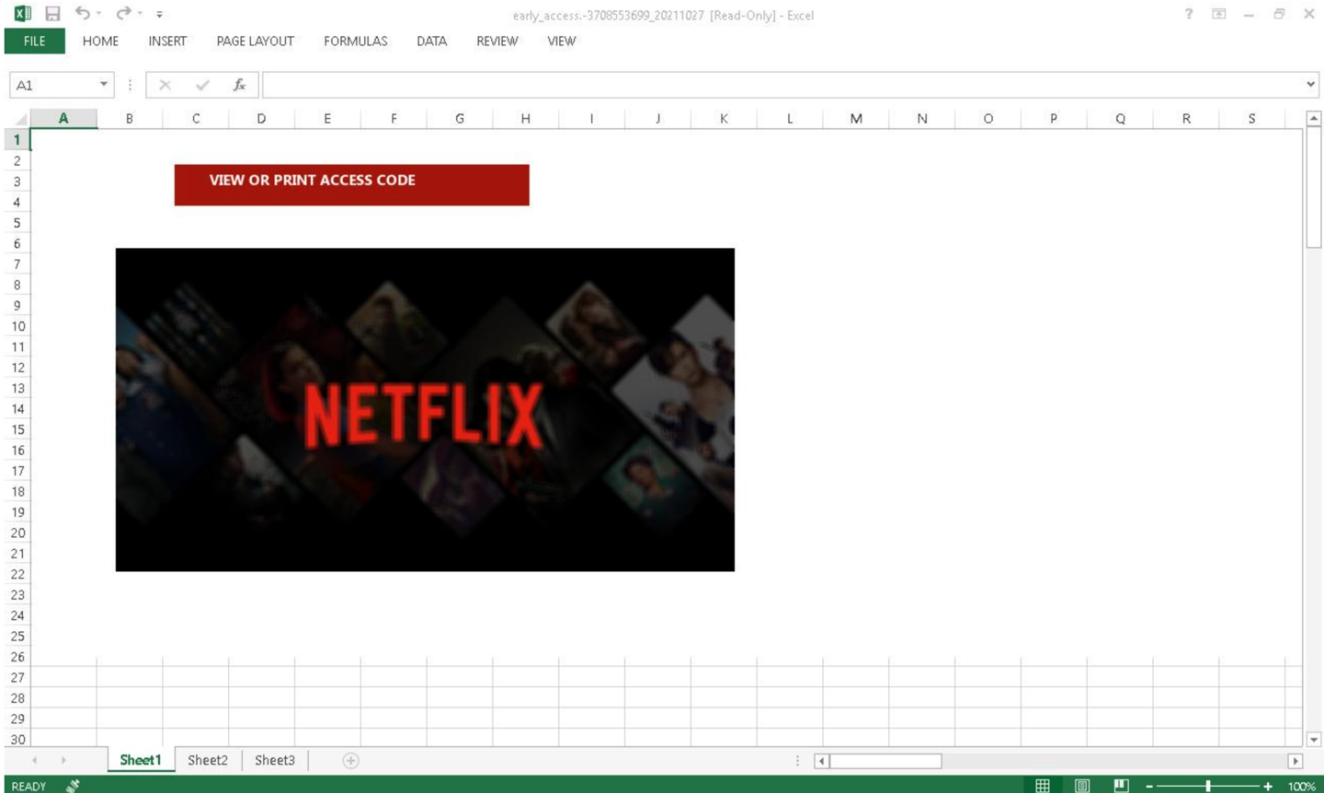


Figure 3: One of the several Excel attachment lures observed in this campaign

TA575 is a Dridex affiliate tracked by Proofpoint since late 2020. This group distributes malware via malicious URLs, Microsoft Office attachments, and password-protected files. 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. Discord, a communications platform with consumer and enterprise uses, is an increasingly popular malware hosting service for cybercriminals.

TA575 themes generally include invoicing and payments, but occasionally include popular news, events, and cultural references. Cybercriminal threat actors in general have pounced on Squid Game as a popular lure and malware theme. This makes sense; as Squid Game is Netflix's "biggest ever" series, the pool of potential victims who would inadvertently interact with malicious content associated with it is higher than a general lure theme. TA575 is betting the invitation to be part of the upcoming season will entice more users to interact with the malicious Microsoft Excel file.

Proofpoint observed the following indicators of compromise:

Indicator	Description
85d2fe6405aac0816f7286bc26174151ae69a08210aec78fea5628862489d8ac	Dridex SHA256
149[.]202[.]179[.]100:443	Dridex C2
66[.]147[.]235[.]111:6891	Dridex C2

81[.]0[.]236[.]89:13786	Dridex C2
hxxps[:]//cdn[.]discordapp[.]com/ attachments/902882967184113677/902908322359959602/xEljRErMuphgnb[.]dll	Excel Payload
hxxps[:]//cdn[.]discordapp[.]com/ attachments/902882967184113677/902903501724725280/TgrWe[.]dll	Excel Payload
hxxps[:]//cdn[.]discordapp[.]com/ attachments/902882967184113677/902907845887012875/nmQxwiMDXToNFO[.]dll	Excel Payload

Subscribe to the Proofpoint Blog