BazaFlix: BazaLoader Fakes Movie Streaming Service | Proofpoint US

By May 26, 2021 Selena Larson and Matthew Mesa

Published: 2021-05-24 · Archived: 2026-04-05 17:21:12 UTC

Key Findings

1. BazaLoader affiliates continue to use elaborate infection chains requiring significant victim interaction to distribute BazaLoader malware.
2. Emails directed the victim to call a customer service line which sent them to a website containing malicious content.
3. The threat actor created a robust fake movie streaming service called BravoMovies, complete with fake movie titles as a landing page.

Overview

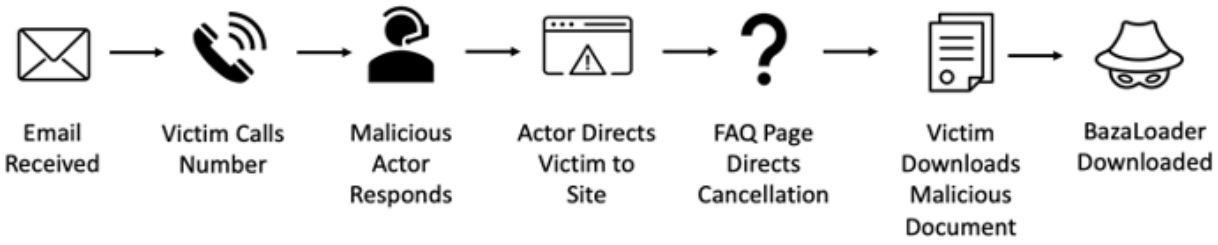
Proofpoint researchers identified a BazaLoader campaign requiring significant human interaction to execute and install the BazaLoader backdoor. The threat actor leveraged phone-based customer service representatives to direct victims to unknowingly download and install the malware. This campaign is representative of a broader trend leveraged by the BazaLoader threat actors using call centers as part of an intricate attack chain.

The entertainment-themed campaign was first observed in early May 2021 and masqueraded as a streaming entertainment service, complete with a slick website featuring fake movies. The campaign demonstrates an inversely proportional relationship between successful infection rates and asking people to complete complicated steps – the more steps required by the user, the less likely they are to complete the attack chain. However, despite being counterintuitive, the techniques used by the threat actors in this, and similar, campaigns help bypass fully automated threat detection systems. Additionally, leveraging a streaming service cancellation lure preys on a growing trend of users cancelling online entertainment following major growth in the industry during 2020.

Campaign Details

BazaLoader is a downloader written in C++ that is used to download and execute additional modules. Proofpoint first observed BazaLoader in April 2020. It is currently used by multiple threat actors and frequently serves as a loader for disruptive malware including Ryuk and Conti ransomware. Proofpoint assesses with high confidence there is a strong overlap between the distribution and post-exploitation activity of BazaLoader and threat actors behind The Trick malware, also known as Trickbot.

Infection Chain



In the recent BazaLoader campaign, messages purport to be from various senders with subjects such as:

- Your trial period M0012064753012345 is going to be expired soon. Thankfully you made a decision to stick with us!
- Demo stage is expired! Your account #M0272028060812345 will be automatically transferred to premium plan!

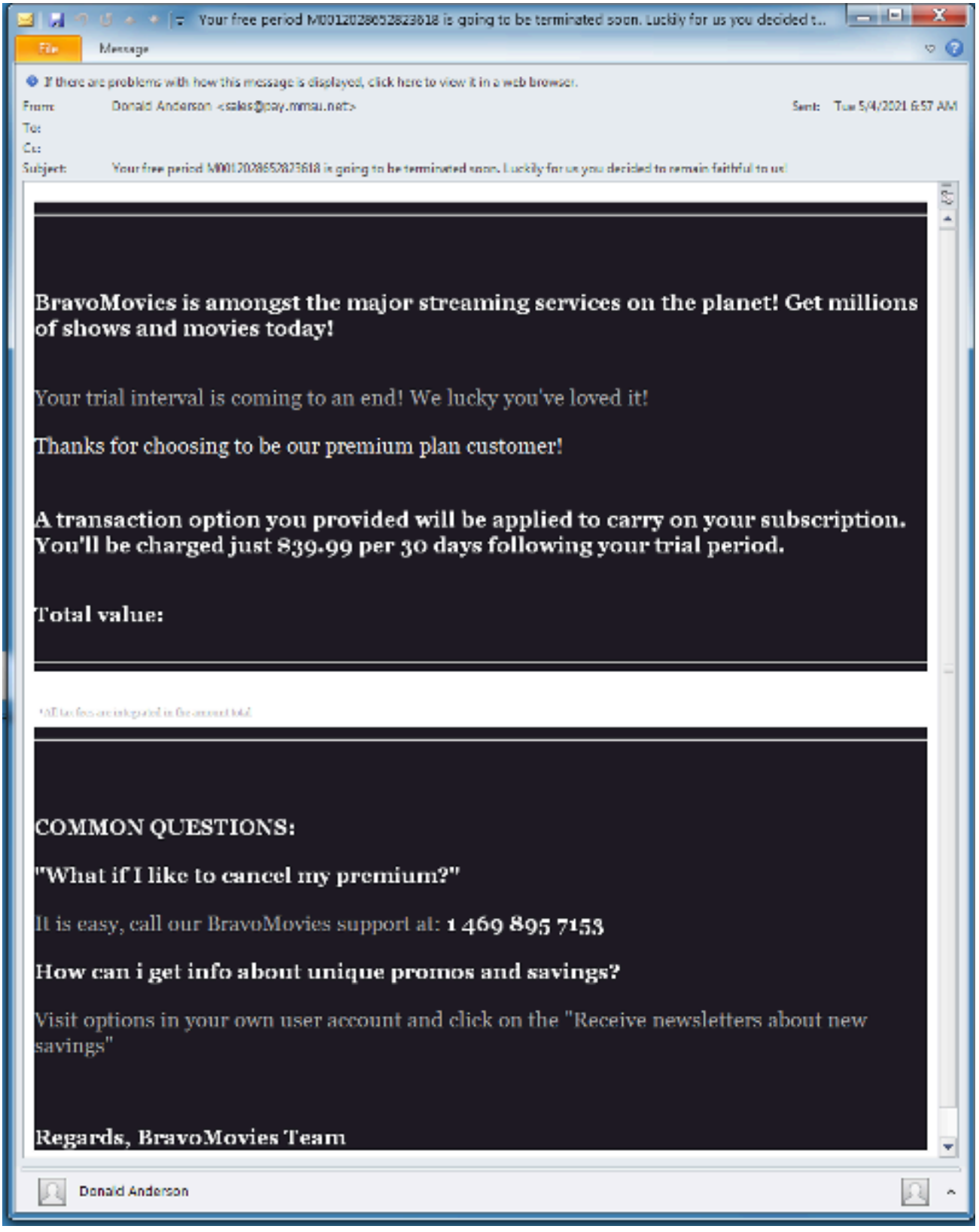
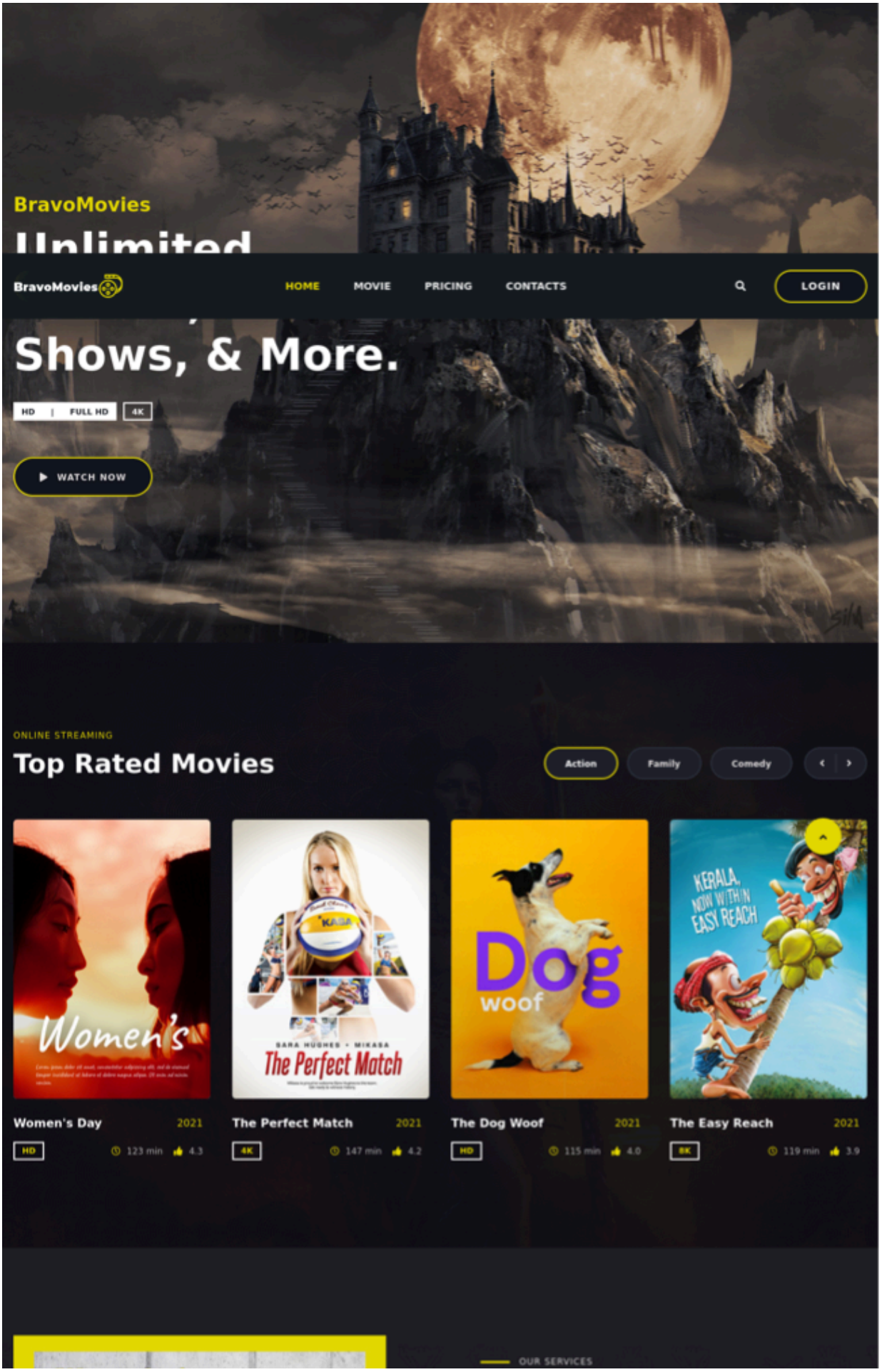


Figure 1: Initial BazaLoader email masquerading as an entertainment streaming service

The emails contain phone numbers and references to the "BravoMovies" company. The messages purport to inform the target their credit card will be charged unless they cancel their subscription to the service. If the user calls the phone number provided in the email, a customer service representative will verbally guide the user to the company's alleged website. The website is a convincing representation of a movie and television streaming service. The threat actors used

fake movie posters obtained from various open-source resources including an advertising agency, the creative social network Behance, and the book “How to Steal a Dog.”


BravoMovies
Unlimited
BravoMovies
HOME
MOVIE
PRICING
CONTACTS
LOGIN
Shows, & More.
HD | FULL HD
4K
WATCH NOW
ONLINE STREAMING
Top Rated Movies
Action
Family
Comedy
Women's
SARA HUGHES • MIKASA
The Perfect Match
Dog
woof
KERALA,
NOW WITHIN
EASY REACH
Women's Day
2021
HD
123 min
4.3
The Perfect Match
2021
4K
147 min
4.2
The Dog Woof
2021
HD
115 min
4.0
The Easy Reach
2021
8K
119 min
3.9
OUR SERVICES

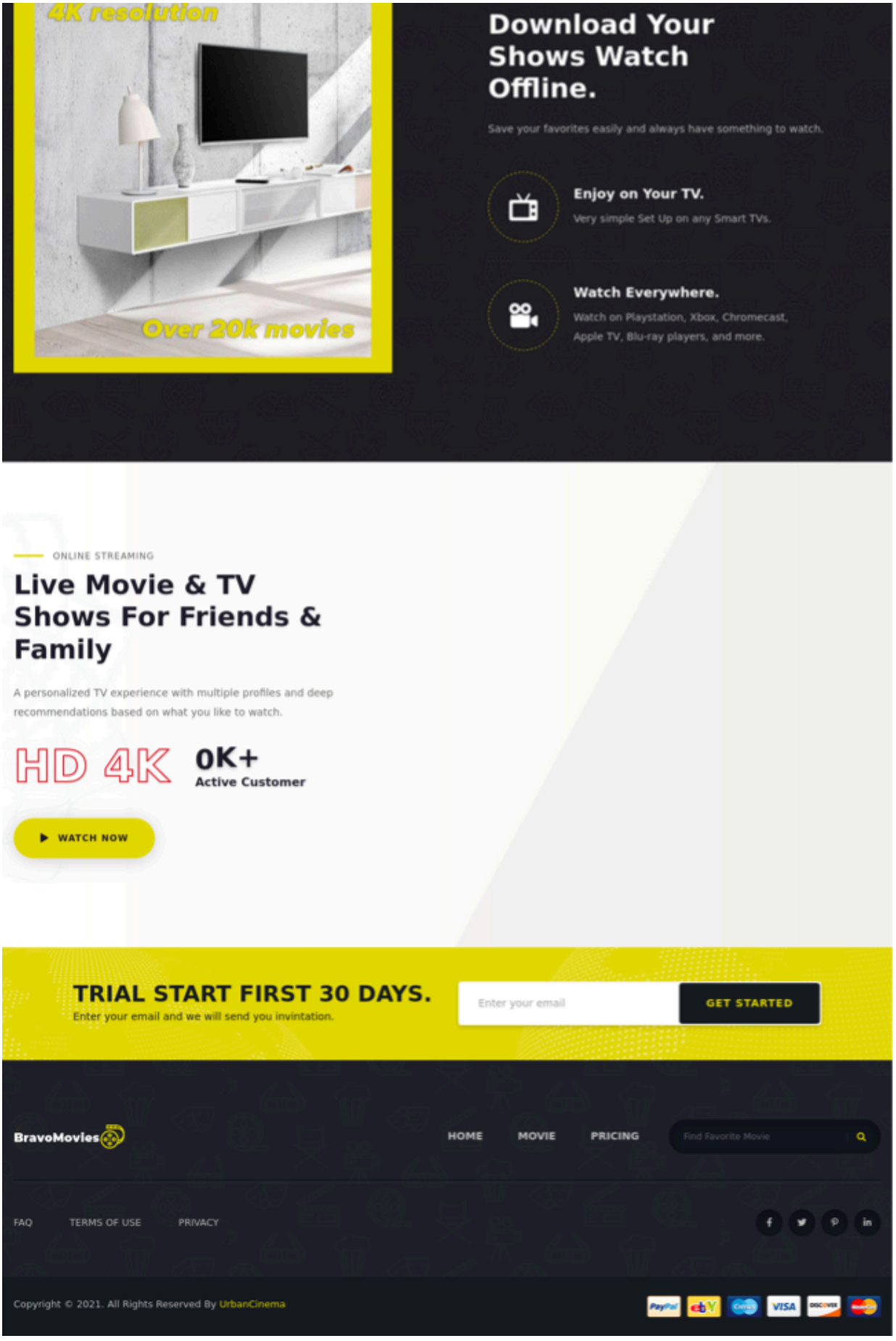
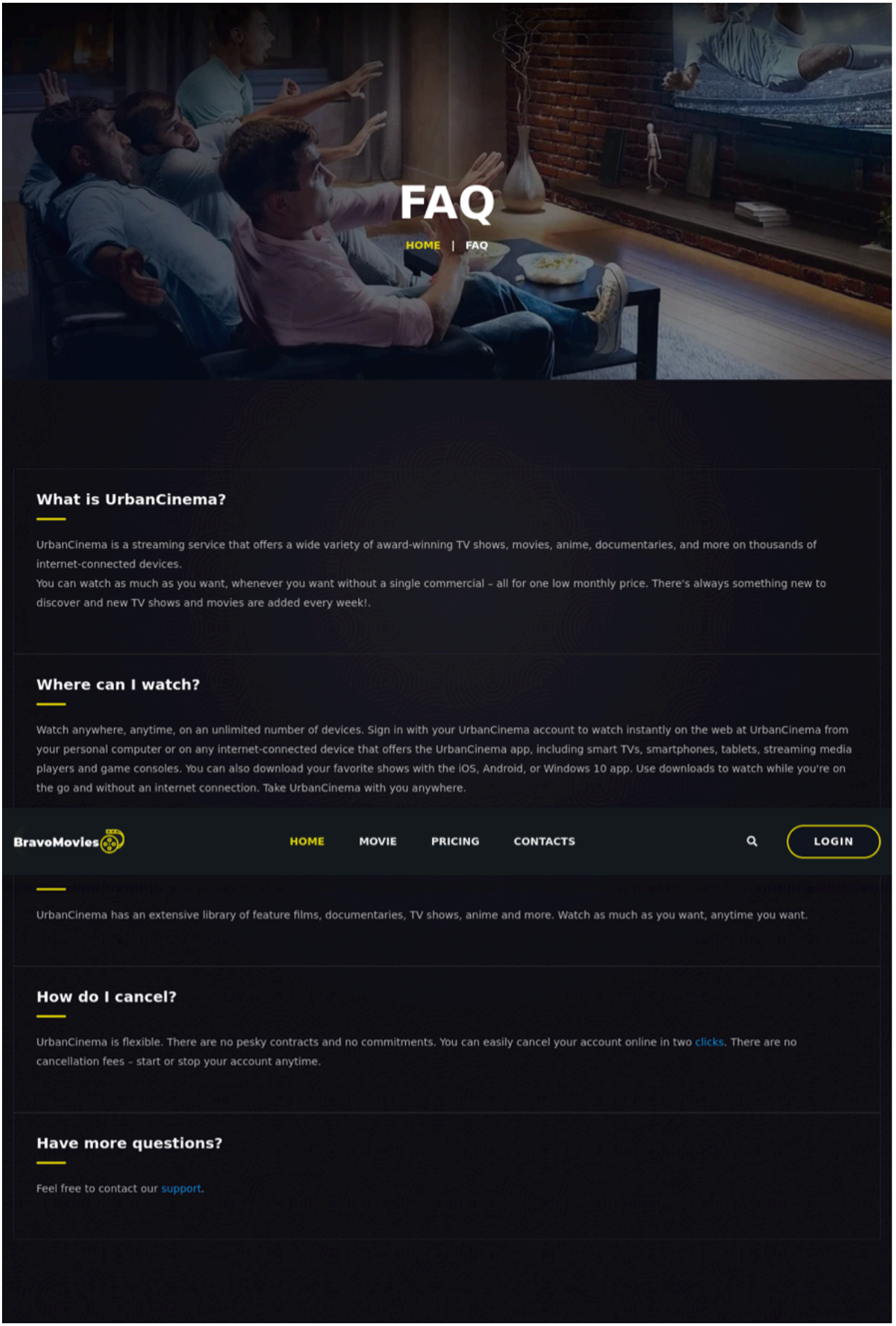


Figure 2: BravoMovies landing page

When the user visits the site mentioned, navigates to the Frequently Asked Questions component of the website, and follows the directions to unsubscribe via the “Subscribtion” page, they will be directed to the download of an Excel

Sheet.


FAQ
HOME | FAQ
What is UrbanCinema?
UrbanCinema is a streaming service that offers a wide variety of award-winning TV shows, movies, anime, documentaries, and more on thousands of internet-connected devices.
You can watch as much as you want, whenever you want without a single commercial – all for one low monthly price. There's always something new to discover and new TV shows and movies are added every week!.
Where can I watch?
Watch anywhere, anytime, on an unlimited number of devices. Sign in with your UrbanCinema account to watch instantly on the web at UrbanCinema from your personal computer or on any internet-connected device that offers the UrbanCinema app, including smart TVs, smartphones, tablets, streaming media players and game consoles. You can also download your favorite shows with the iOS, Android, or Windows 10 app. Use downloads to watch while you're on the go and without an internet connection. Take UrbanCinema with you anywhere.
BravoMovies
HOME
MOVIE
PRICING
CONTACTS
LOGIN
UrbanCinema has an extensive library of feature films, documentaries, TV shows, anime and more. Watch as much as you want, anytime you want.
How do I cancel?
UrbanCinema is flexible. There are no pesky contracts and no commitments. You can easily cancel your account online in two clicks. There are no cancellation fees – start or stop your account anytime.
Have more questions?
Feel free to contact our support.

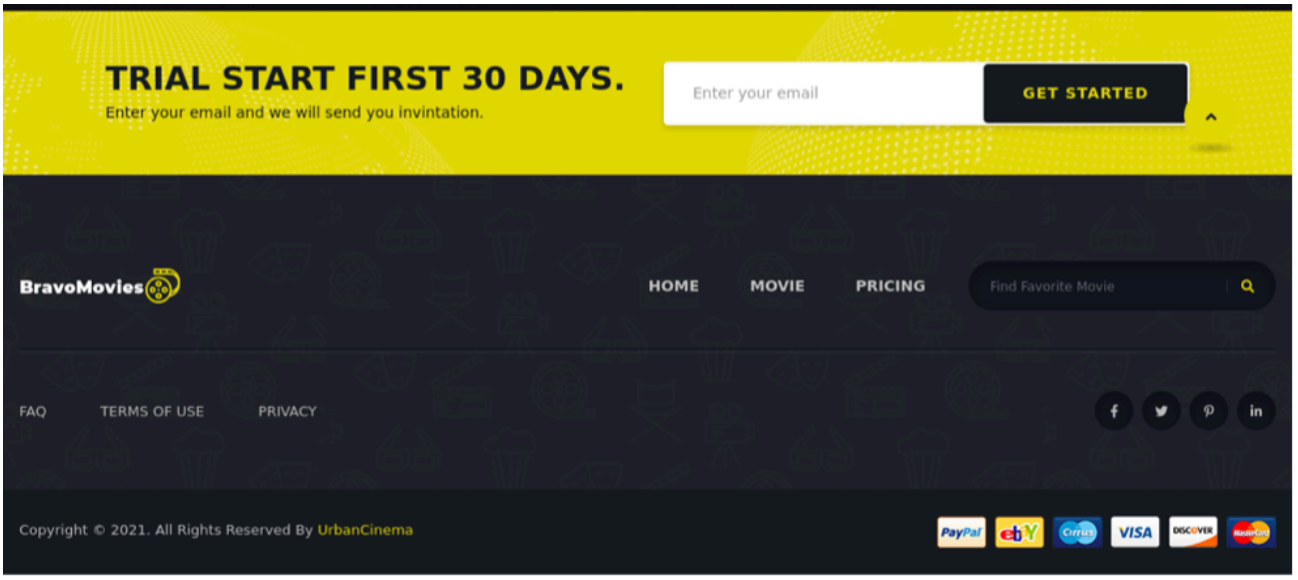


Figure 3: FAQ page with cancellation instructions

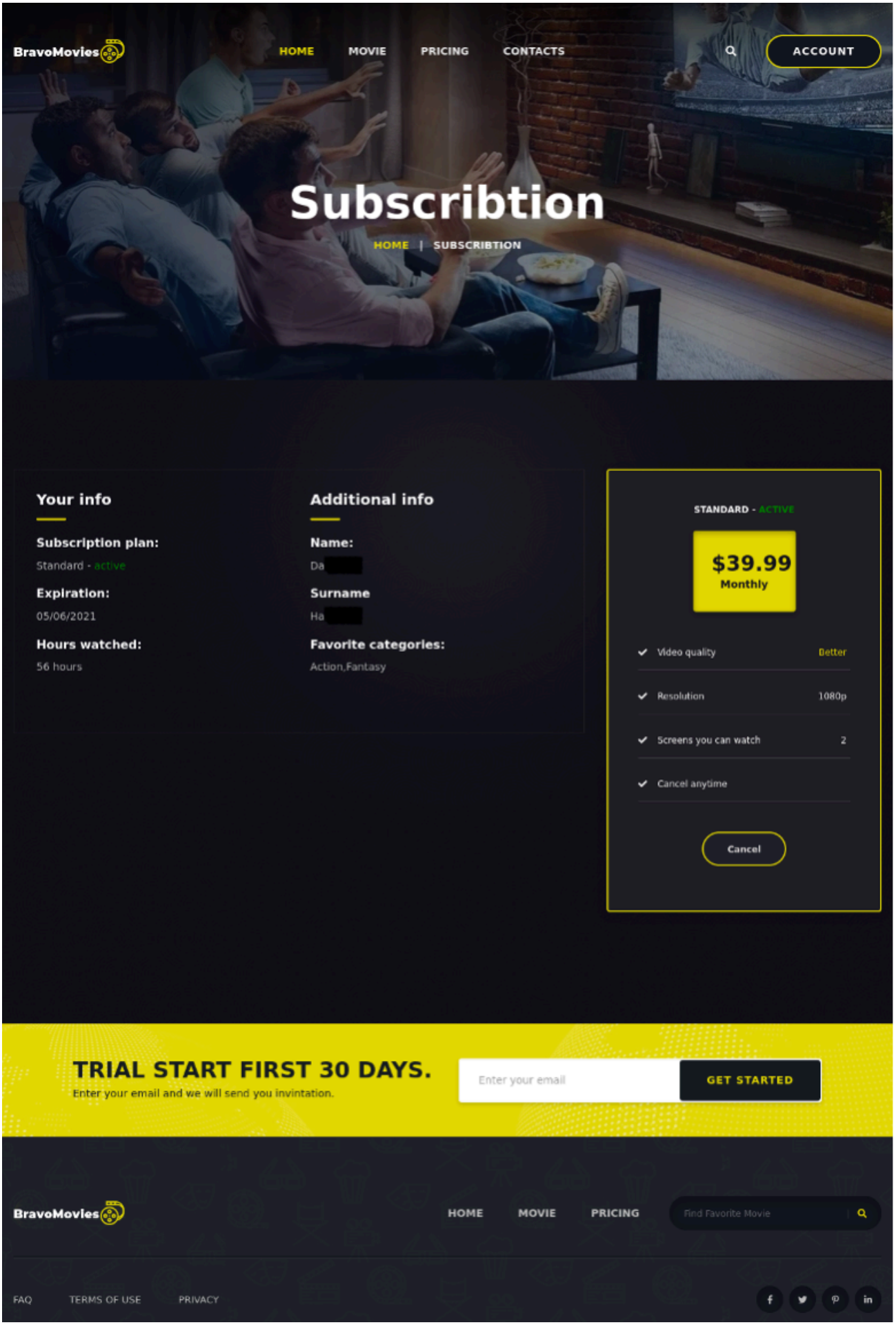

BravoMovies
HOME
MOVIE
PRICING
CONTACTS
ACCOUNT
Subscribtion
HOME | SUBSCRIBTION
Your info
Subscription plan:
Standard - active
Expiration:
05/06/2021
Hours watched:
56 hours
Additional info
Name:
Da
Surname
Ha
Favorite categories:
Action,Fantasy
STANDARD - ACTIVE
$39.99
Monthly
Video quality
Better
Resolution
1080p
Screens you can watch
2
Cancel anytime
Cancel
TRIAL START FIRST 30 DAYS.
Enter your email and we will send you invintation.
Enter your email
GET STARTED
BravoMovies
HOME
MOVIE
PRICING
Find Favorite Movie
FAQ
TERMS OF USE
PRIVACY

Figure 4: Fake subscription cancellation page

The Excel sheet contains macros that, if enabled, will download BazaLoader.

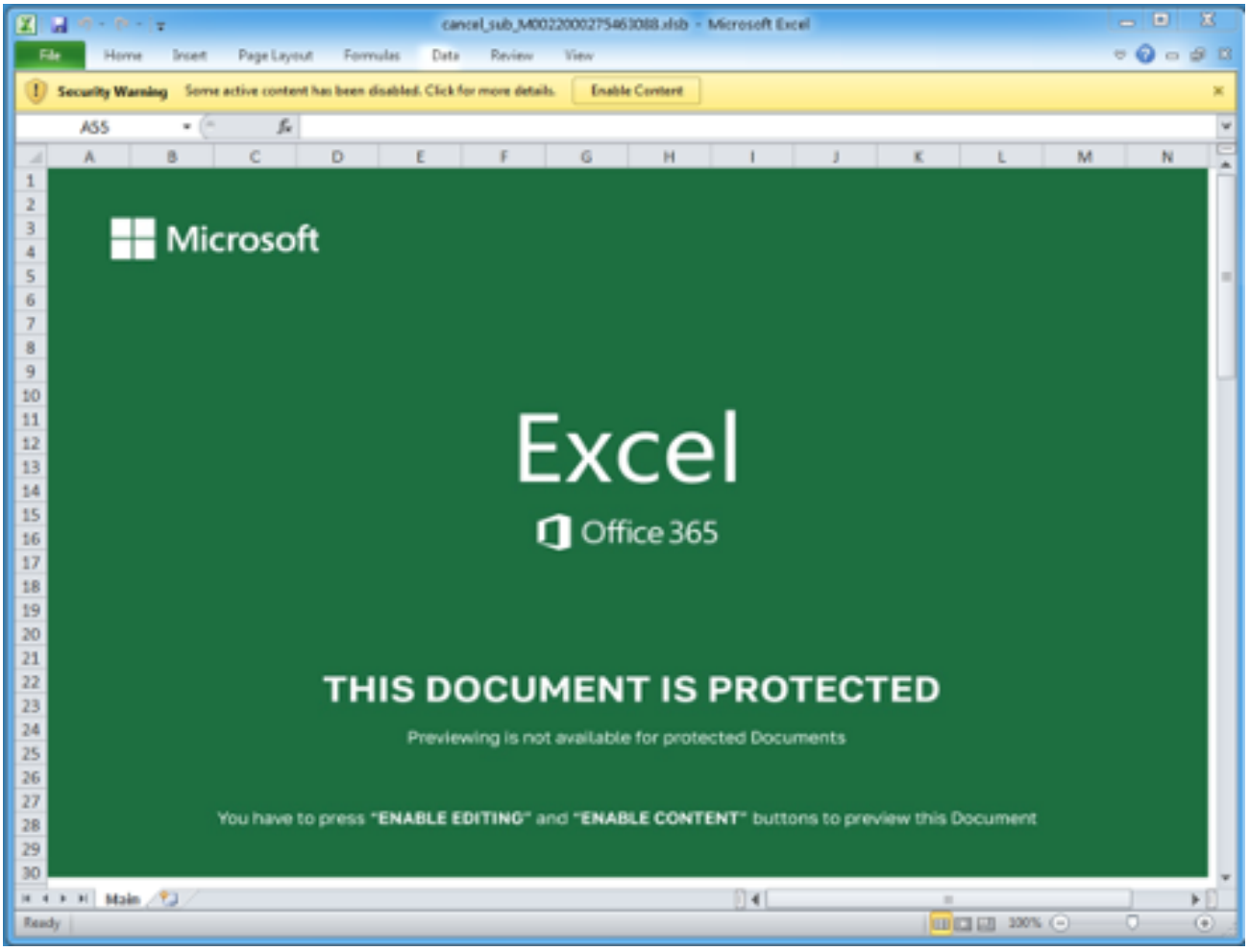


Figure 5: Malicious Excel Sheet

At this time, Proofpoint has not observed the second-stage payload in this campaign.

Related Campaigns

Proofpoint has observed BazarLoader threat actors using the method of phone-based customer service representatives to direct malicious downloads since February 2021. Security researchers have dubbed this method "BazarCall". Proofpoint has previously observed BazaLoader email threat campaigns requiring significant human interaction in order to execute the malware. The previous campaigns included subscription pharmaceutical services and lingerie and flower orders.

Additionally, Proofpoint researchers have observed similar infection chains leading to the distribution of The Trick instead of BazaLoader. By leveraging attack chains that require a lot of human interaction, threat actors can bypass some automated threat detection services that only flag on malicious links or attachments in email. Proofpoint anticipates the threat actors behind BazaLoader and The Trick will continue to use these techniques in future campaigns.

Conclusion

Using entertainment subscription themes may be a timely and effective method for convincing users to engage with the email content and follow-on malicious documents. During the COVID-19 pandemic in 2020, subscriptions to online streaming services skyrocketed, surpassing one billion users globally last year. But according to recent 2021 data, consumers are using fewer services while churning through free subscriptions and cancelling when their trials run out. BazaLoader threat actors are taking advantage of this human behavior trend in the identified campaign.

Indicators of Compromise

IOC	IOC Type	Description	First Observed
urbancinema[.]net	Domain	Landing Page	2021-05-05
bravomovies[.]net	Domain	Landing Page	2021-05-01
bvcinema[.]net	Domain	Landing Page	2021-05-06
47.91.77[.]83	IP	BravoMovies Website Host	2021-05-05
8.209.65[.]249	IP	BravoMovies Website Host	2021-05-01
8.209.92[.]183	IP	BravoMovies Website Host	2021-05-04
8.209.75[.]180	IP	BravoMovies Website Host	2021-05-04
8.211.4[.]26	IP	BravoMovies Website Host	2021-05-06

8.211.6[.]4	IP	BravoMovies Website Host	2021-05-06
8.209.67[.]183	IP	BravoMovies Website Host	2021-05-10
47.91.74[.]88	IP	BravoMovies Website Host	2021-05-15
176.111.174[.]60	IP	BazaLoader Excel Payload Host	2021-05-04
hxxps://18.237.242[.]195/g1_262/bt_64_g1_262	URL	BazaLoader C2	2021-05-04
hxxp://noise1[.]xyz/campo/n/o	URL	BazaLoader Excel Payload	2021-05-04
9663dc275239aa93ceccedae7a0d54e10def18dd177d231264a323a4175a23d4	SHA256	BazaLoader Hash	2020-04-25

ET Signatures:

2033033 - ET TROJAN BazaLoader CnC Activity

2033034 - ET TROJAN Observed Malicious SSL Cert

Subscribe to the Proofpoint Blog
