Luna Moth: The Actors Behind the Recent False Subscription Scams

blog.sygnia.co/luna-moth-false-subscription-scams

Over the last few months, Sygnia's Incident Response team has been methodically tracking the 'Luna Moth' ransom group. Their modus-operandi resembles scammers, with the twist of corporate data theft, leveraging the threat of publication to demand millions of dollars in ransom.

key points

- The Sygnia Incident Response team identified a relatively new threat group, which has been operating since the end of March 2022. Sygnia refers to this threat actor as 'Luna Moth' or TG2729.
- 'Luna Moth' focuses on Data Breach extortion attacks, threatening to leak stolen information if the demanded ransom is not paid.
- The initial compromise is achieved by deceiving victims in a phishing campaign under the theme of Zoho MasterClass and Duolingo subscriptions, leading to the installation of an initial tool on the compromised host.
- The group uses commercial remote administration tools (RATs) and publicly available tools to operate on compromised devices and maintain persistency, demonstrating once more the simplicity and effectiveness of ransom attacks.
- The group acts and operates in an opportunistic way: even if there are no assets or devices to compromise in the network, they exfiltrate any data that is accessible; this emphasizes the importance of managing sensitive corporate information.

the 'luna moth' group

With the rise in ransomware activity over the past years, the security industry has become used to hearing about double extortion, and even triple extortion attacks, and new crime groups of all kinds. In this blog post, we shed light on a relatively new threat actor which goes by the name of the ‘Silent Ransom Group’ (or ‘SRG’) and was dubbed 'Luna Moth' by Sygnia. By launching a phishing campaign with a wide coverage area, 'Luna Moth' infiltrates and compromises victim devices. These attacks can be categorized as data breach ransom attacks, in which the main focus of the group is to gain access to sensitive documents and information, and demand payment to withhold publication of the stolen data. Simple as they may be, these attacks can create serious issues for victims if sensitive data and information is stolen in this way.

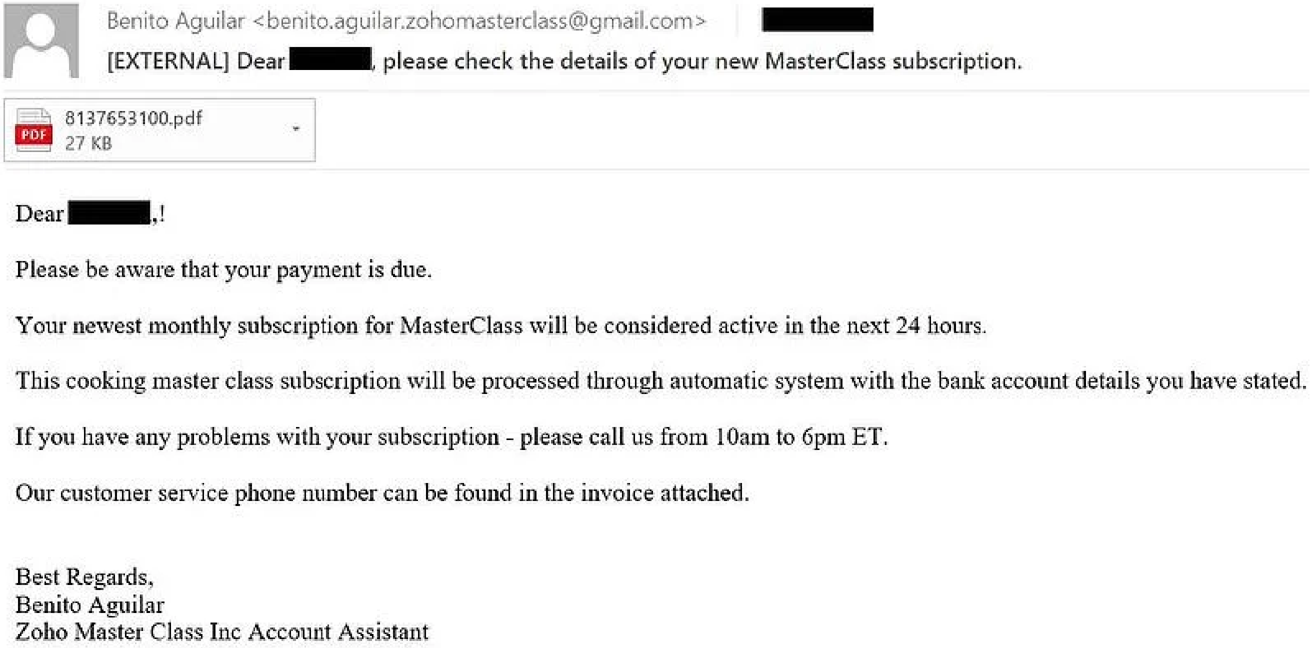
Although the group is not widely known, they have been active in the past months, attempting to build their reputation as a ransom gang. Their modus-operandi resembles scammers, with the twist of corporate data theft, leveraging the threat of publication to demand millions of dollars in ransom.

gaining initial accesss

Over the past three months, the ‘Luna Moth' group operated a large-scale phishing campaign under the theme of MasterClass and Duolingo subscriptions, by impersonating Zoho MasterClass Inc and Duolingo. Although claiming to be related to the Zoho Corporation or Duolingo, the phishing emails are sent from Gmail addresses that are altered to resemble the legitimate company email addresses:

- {FIRST-NAME}.{LAST-NAME}.zohomasterclass@gmail.com
- {FIRST-NAME}.{LAST-NAME}.duolingo@gmail.com

This is a classic phishing scam: the email claims that the recipient of the email purchased a subscription to a legitimate service, and that payment is due. To complete the scam, an invoice PDF file is attached to the email, and the victim is recommended to call a phone number, which the email states can be found within the attached file, if there are any issues with the subscription.



Benito Aguilar <benito.aguilar.zohomasterclass@gmail.com> [redacted]

[EXTERNAL] Dear [redacted], please check the details of your new MasterClass subscription.

8137653100.pdf
27 KB

Dear [redacted],!

Please be aware that your payment is due.

Your newest monthly subscription for MasterClass will be considered active in the next 24 hours.

This cooking master class subscription will be processed through automatic system with the bank account details you have stated.

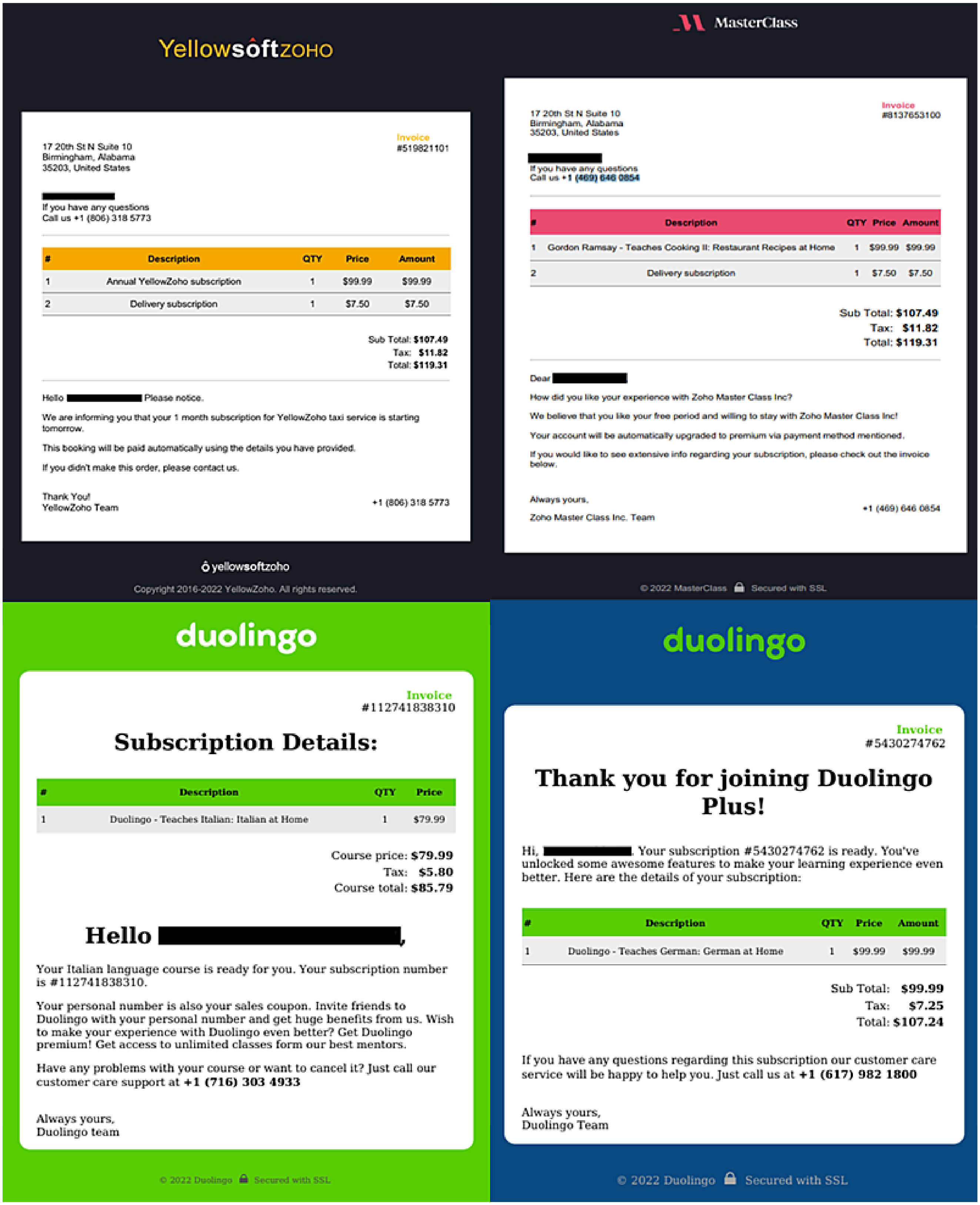
If you have any problems with your subscription - please call us from 10am to 6pm ET.

Our customer service phone number can be found in the invoice attached.

Best Regards,
Benito Aguilar
Zoho Master Class Inc Account Assistant

Image 1

: An example of a Zoho Masterclass themed phishing email



YellowsoftZOHO

17 20th St N Suite 10
Birmingham, Alabama
35203, United States

Invoice
#519821101

[redacted]
If you have any questions
Call us +1 (806) 318 5773

#	Description	QTY	Price	Amount
1	Annual YellowZoho subscription	1	$99.99	$99.99
2	Delivery subscription	1	$7.50	$7.50

Sub Total: **$107.49**
Tax: **$11.82**
Total: **$119.31**

Hello [redacted] Please notice.

We are informing you that your 1 month subscription for YellowZoho taxi service is starting tomorrow.

This booking will be paid automatically using the details you have provided.

If you didn't make this order, please contact us.

Thank You!
YellowZoho Team

+1 (806) 318 5773

yellowsoftzoho

Copyright 2016-2022 YellowZoho. All rights reserved.

MasterClass

17 20th St N Suite 10
Birmingham, Alabama
35203, United States

Invoice
#8137653100

[redacted]
If you have any questions
Call us +1 **(469) 646 0854**

#	Description	QTY	Price	Amount
1	Gordon Ramsay - Teaches Cooking II: Restaurant Recipes at Home	1	$99.99	$99.99
2	Delivery subscription	1	$7.50	$7.50

Sub Total: **$107.49**
Tax: **$11.82**
Total: **$119.31**

Dear [redacted]

How did you like your experience with Zoho Master Class Inc?

We believe that you like your free period and willing to stay with Zoho Master Class Inc!

Your account will be automatically upgraded to premium via payment method mentioned.

If you would like to see extensive info regarding your subscription, please check out the invoice below.

Always yours,

Zoho Master Class Inc. Team

+1 (469) 646 0854

© 2022 MasterClass 🔒 Secured with SSL

duolingo

Invoice
#112741838310

Subscription Details:

#	Description	QTY	Price
1	Duolingo - Teaches Italian: Italian at Home	1	$79.99

Course price: **$79.99**
Tax: **$5.80**
Course total: **$85.79**

Hello [redacted],

Your Italian language course is ready for you. Your subscription number is #112741838310.

Your personal number is also your sales coupon. Invite friends to Duolingo with your personal number and get huge benefits from us. Wish to make your experience with Duolingo even better? Get Duolingo premium! Get access to unlimited classes form our best mentors.

Have any problems with your course or want to cancel it? Just call our customer care support at **+1 (716) 303 4933**

Always yours,
Duolingo team

© 2022 Duolingo 🔒 Secured with SSL

duolingo

Invoice
#5430274762

Thank you for joining Duolingo Plus!

Hi, [redacted]. Your subscription #5430274762 is ready. You've unlocked some awesome features to make your learning experience even better. Here are the details of your subscription:

#	Description	QTY	Price	Amount
1	Duolingo - Teaches German: German at Home	1	$99.99	$99.99

Sub Total: **$99.99**
Tax: **$7.25**
Total: **$107.24**

If you have any questions regarding this subscription our customer care service will be happy to help you. Just call us at **+1 (617) 982 1800**

Always yours,
Duolingo Team

© 2022 Duolingo 🔒 Secured with SSL

Image 2-5: Examples of invoices attached as PDF files to the phishing emails

If the victim wishes to refute the purchase, they are required to join a Zoho remote support session. At this point, the threat actor uses the native Zoho Assist functionality to send another email, entitled “Zoho Assist - Remote Support session”, which guides the user to download and install the Zoho Assist application. The group then invites the victim to the support session using Zoho Assist accounts that are tied to protonmail emails.

During this short yet effective Zoho Assist session, the threat actor is able to trick the user into downloading and installing Atera on their device; this is a remote administration tool commonly used by threat actors. Once Atera is installed on the device, the threat actor can access the device and operate freely.

tools in the arsenal

The examples shown above demonstrate that both the activities and the toolset of 'Luna Moth' are fairly unsophisticated. The main tools used by the threat actor consist of remote administration tools (RATs) that allow them to control compromised devices; these include Atera, Splashtop, Syncro, and AnyDesk. These tools also provide the threat actors with some redundancy and persistence: if one of the RATs is removed from the system, it can be reinstalled by the others.

Additional tools used by the group include off-the-shelf tools such as SoftPerfect Network Scanner, SharpShares, and Rclone. The tools are stored on compromised machines under false names masquerading as legitimate binaries. These tools, in addition to the RATs, provide the threat actors with the means to conduct basic reconnaissance activities, access additional available assets, and exfiltrate data from compromised networks.

campaign infrastructure

The infrastructure used by 'Luna Moth' as part of the subscription scams can be mapped to two main clusters of domains and IPs:

- Exfiltration domains: Domains under the XYZ TLD, such as maaays[.]xyz. These domains are used by the group as part of the Rclone exfiltration process; the domains are the target to which the exfiltrated data is sent.
- Phishing domains that appear to be related to Zoho or Duolingo – for example, masterzohoclass[.]com. Most of these domains have a very short lifespan of about four hours.

The first identified domain related to the campaign was registered during April 2022. Both the exfiltration and phishing domains are hosted by the provider Hostwinds, and registered under Namecheap.

Domain	IP Address	Registration Date	Type
dictumst[.]xyz	23[.]254[.]229[.]90	18/04/2022 08:46	Exfiltration Server
tincidunt[.]xyz	192[.]119[.]110[.]47	18/04/2022 08:53	Exfiltration Server
deserunt[.]xyz	192[.]119[.]110[.]22	18/04/2022 08:54	Exfiltration Server
mczoho[.]com	192[.]119[.]111[.]25	18/04/2022 14:27	Infrastructure
masterzohoclass[.]com	192[.]236[.]178[.]3	19/04/2022 13:54	Infrastructure
zohocook[.]com	192[.]236[.]177[.]251	20/04/2022 10:42	Infrastructure
molestie[.]xyz	192[.]236[.]193[.]152	21/04/2022 07:21	Exfiltration Server
adipiscing[.]xyz	192[.]236[.]193[.]150	21/04/2022 07:21	Exfiltration Server
fringilla[.]xyz	192[.]236[.]193[.]148	21/04/2022 13:18	Exfiltration Server
volutpat[.]xyz	192[.]236[.]193[.]151	21/04/2022 13:19	Exfiltration Server
ultrices[.]xyz	192[.]236[.]193[.]149	21/04/2022 13:19	Exfiltration Server

cookwithzoho[.]com	192[.]236[.]193[.]141	21/04/2022 13:34	Infrastructure
cookingbyzoho[.]com	192[.]236[.]193[.]140	22/04/2022 12:15	Infrastructure
massay[.]xyz	192[.]236[.]177[.]20	25/04/2022 11:28	Exfiltration Server
masaay[.]xyz	192[.]236[.]176[.]79	25/04/2022 11:28	Exfiltration Server
myaaas[.]xyz	192[.]236[.]192[.]84	25/04/2022 11:29	Exfiltration Server
myaasa[.]xyz	192[.]236[.]179[.]76	25/04/2022 11:29	Exfiltration Server
myasaa[.]xyz	192[.]236[.]178[.]135	25/04/2022 11:29	Exfiltration Server
masyaa[.]xyz	192[.]236[.]193[.]86	25/04/2022 11:30	Exfiltration Server
maysaa[.]xyz	192[.]236[.]193[.]81	25/04/2022 11:30	Exfiltration Server
msaaay[.]xyz	192[.]236[.]192[.]215	25/04/2022 11:30	Exfiltration Server
maaays[.]xyz	192[.]236[.]194[.]2	25/04/2022 11:35	Exfiltration Server
maaasy[.]xyz	192[.]236[.]194[.]31	25/04/2022 11:36	Exfiltration Server
cookingzoho[.]com	192[.]236[.]195[.]42	25/04/2022 12:50	Infrastructure
zohomclass[.]com	192[.]236[.]195[.]83	26/04/2022 13:02	Infrastructure

zohocooking[.]com	192[.]236[.]198[.]22	27/04/2022 12:12	Infrastructure
studyzoho[.]com	192[.]236[.]198[.]23	28/04/2022 11:02	Infrastructure
molesste[.]xyz	192[.]236[.]208[.]56	28/04/2022 20:53	Exfiltration Server
zohocookingmeals[.]com	192[.]236[.]199[.]2	29/04/2022 10:49	Infrastructure
zohokitchen[.]com	192[.]236[.]192[.]2	02/05/2022 13:12	Infrastructure
ullamm[.]xyz	23[.]254[.]227[.]79	02/05/2022 16:36	Exfiltration Server
zohokitchenmaster[.]com	192[.]236[.]192[.]9	03/05/2022 10:54	Infrastructure
zohoteachingmaster[.]com	192[.]236[.]192[.]69	04/05/2022 12:42	Infrastructure
zohoteaching[.]com	192[.]236[.]192[.]73	05/05/2022 14:02	Infrastructure
tincidut[.]xyz	142[.]11[.]215[.]104	06/05/2022 13:48	Exfiltration Server
masterclassgold[.]com	142[.]11[.]215[.]25	09/05/2022 14:42	Infrastructure
proodee[.]xyz	192[.]236[.]179[.]217	09/05/2022 16:07	Exfiltration Server
zohocookingclass[.]com	198[.]54[.]117[.]244	10/05/2022 07:53	Infrastructure
zohoclasspro[.]com	142[.]11[.]215[.]212	10/05/2022 11:42	Infrastructure
deerunt[.]xyz	142[.]11[.]206[.]153	14/05/2022 08:40	Exfiltration Server
nostuud[.]xyz	192[.]236[.]147[.]234	14/05/2022 14:27	Exfiltration Server

aliuuip[.]xyz	23[.]254[.]228[.]211	14/05/2022 14:28	Exfiltration Server
zohoduolingo[.]com	192[.]236[.]209[.]36	16/05/2022 13:11	Infrastructure
duolingoclass[.]com	192[.]236[.]209[.]34	17/05/2022 13:24	Infrastructure
acsyruse[.]xyz	192[.]236[.]155[.]81	17/05/2022 20:56	Exfiltration Server
zoholanguageclass[.]com	142[.]11[.]209[.]198	18/05/2022 12:40	Infrastructure
zoholanguage[.]com	104[.]168[.]164[.]244	19/05/2022 13:40	Infrastructure
duo-lingo-class[.]com	104[.]168[.]204[.]231	23/05/2022 12:27	Infrastructure
caaom[.]xyz	192[.]236[.]155[.]151	23/05/2022 14:04	Exfiltration Server
caaof[.]xyz	192[.]236[.]155[.]106	23/05/2022 14:05	Exfiltration Server
caaog[.]xyz	192[.]236[.]155[.]138	23/05/2022 14:05	Exfiltration Server
caaor[.]xyz	192[.]236[.]155[.]103	23/05/2022 14:06	Exfiltration Server
caaon[.]xyz	192[.]236[.]155[.]102	23/05/2022 14:28	Exfiltration Server
duolingo-class[.]com	192[.]236[.]192[.]33	24/05/2022 12:29	Infrastructure
studyduolingo[.]com	192[.]236[.]177[.]18	25/05/2022 12:32	Infrastructure
masterclass-cook[.]com	192[.]236[.]193[.]171	31/05/2022 13:43	Infrastructure

duuis[.]xyz	192[.]236[.]249[.]78	01/06/2022 09:43	Exfiltration Server
eeeaa[.]xyz	192[.]236[.]249[.]80	01/06/2022 09:43	Exfiltration Server
veelit[.]xyz	192[.]236[.]249[.]79	01/06/2022 09:44	Exfiltration Server
eesse[.]xyz	192[.]236[.]249[.]76	01/06/2022 09:44	Exfiltration Server
moolit[.]xyz	192[.]236[.]249[.]75	01/06/2022 09:45	Exfiltration Server
premiumduolingo[.]com	104[.]168[.]201[.]129	01/06/2022 12:49	Infrastructure
cook-masterclass[.]com	104[.]168[.]201[.]121	01/06/2022 12:50	Infrastructure
yourduolingo[.]com	104[.]168[.]201[.]87	02/06/2022 11:55	Infrastructure
masterclasscooking[.]com	192[.]119[.]111[.]51	03/06/2022 12:20	Infrastructure
duolingoeducation[.]com	192[.]119[.]111[.]21	03/06/2022 12:20	Infrastructure
educationduolingo[.]com	192[.]119[.]111[.]197	06/06/2022 11:32	Infrastructure
masterclass-chef[.]com	104[.]168[.]201[.]100	06/06/2022 11:33	Infrastructure
allduolingo[.]com	192[.]236[.]194[.]113	07/06/2022 13:02	Infrastructure
allredoo[.]xyz	192[.]236[.]194[.]42	07/06/2022 16:02	Exfiltration Server
aredo[.]xyz	192[.]236[.]160[.]132	07/06/2022 16:03	Exfiltration Server

aeedo[.]xyz	192[.]236[.]193[.]182	07/06/2022 16:03	Exfiltration Server
allreedo[.]xyz	104[.]168[.]218[.]242	07/06/2022 16:04	Exfiltration Server
alloout[.]xyz	104[.]168[.]135[.]71	07/06/2022 17:16	Exfiltration Server
subscriptionduolingo[.]com	192[.]236[.]195[.]74	08/06/2022 12:33	Infrastructure
germanbyduolingo[.]com	192[.]236[.]208[.]44	10/06/2022 11:59	Infrastructure
duolingo-italianclass[.]com	104[.]168[.]171[.]231	21/06/2022 12:43	Infrastructure
aeecc[.]xyz	23[.]238[.]40[.]29	22/06/2022 19:25	Exfiltration Server
eceee[.]xyz	23[.]238[.]40[.]28	22/06/2022 19:25	Exfiltration Server
aeocc[.]xyz	23[.]238[.]40[.]31	22/06/2022 19:26	Exfiltration Server
aedcc[.]xyz	23[.]238[.]40[.]30	22/06/2022 19:26	Exfiltration Server
aeucc[.]xyz	23[.]238[.]40[.]32	22/06/2022 19:27	Exfiltration Server
duolingoitalian[.]com	192[.]236[.]155[.]243	23/06/2022 13:05	Infrastructure
duolingoit[.]com	192[.]236[.]176[.]197	24/06/2022 12:48	Infrastructure
duolingoitclass[.]com	104[.]168[.]171[.]104	27/06/2022 13:09	Infrastructure
duolingo-it[.]com	192[.]236[.]176[.]199	28/06/2022 13:07	Infrastructure

italian-duolingo[.]com	192[.]119[.]110[.]112	29/06/2022 13:27	Infrastructure
masterclass-design[.]com	192[.]119[.]110[.]166	29/06/2022 15:26	Infrastructure

If you were impacted by this attack or are seeking guidance on how to prevent similar attacks, please contact us at contact@sygnia.co or our 24-hour hotline +1-877-686-8680.

Contributors: Oren Biderman, Tomer Lahiyani, Noam Lifshitz.